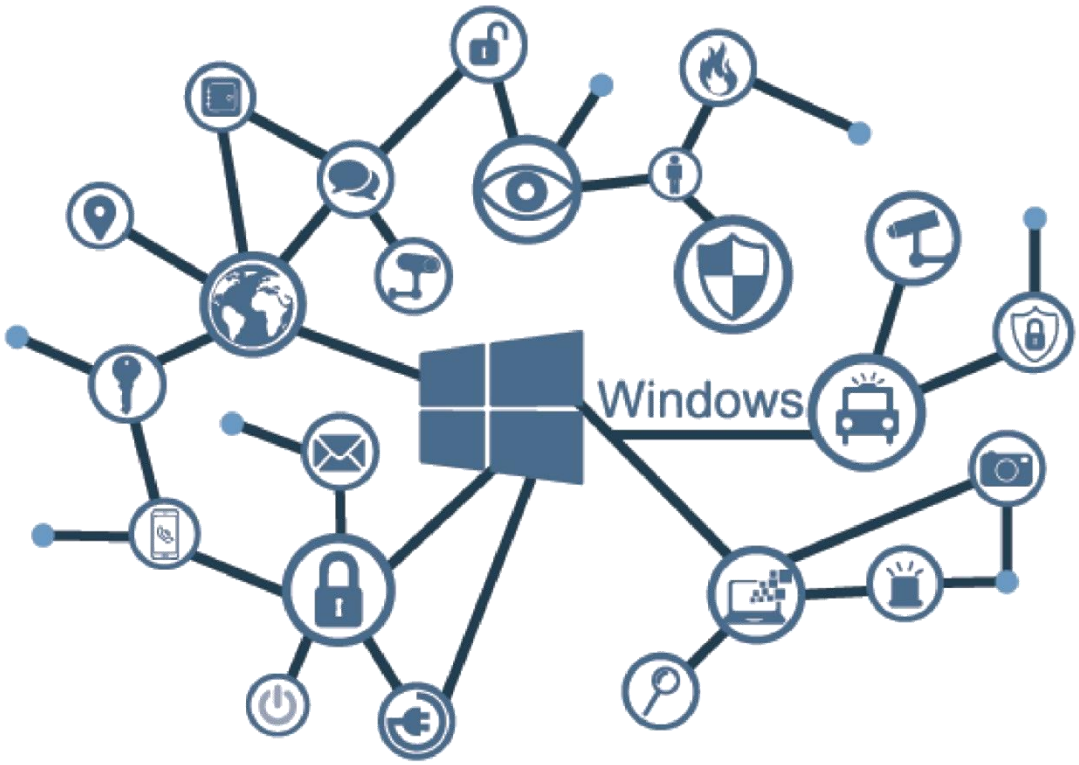
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 570A23

PERFILADO DE SEGURIDAD PARA WINDOWS SERVER (CONTROLADOR DE DOMINIO O SERVIDOR MIEMBRO)



JULIO 2023

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.25 17:53:40 +02'00'

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: julio de 2023
NIPO: 083-23-194-3

INDICE

1. INTRODUCCIÓN

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

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

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

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

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

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

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

2. OBJETO

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

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

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

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

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

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

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

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

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

3. ALCANCE

La guía se ha elaborado para proporcionar información específica sobre cómo implementar las distintas configuraciones según diferentes escenarios. En particular, se incluirá la configuración para asegurar **servidores basados en un sistema operativo "Microsoft Windows Server"**, instalados en español con la versión completa del producto (experiencia de escritorio), bien actuando con el **rol de controlador de dominio** o bien como **servidor miembro de un dominio**. Así mismo, se establecerán los mecanismos para asegura el entorno de dominio asociado.

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

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

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

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

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

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

Este documento incluye:

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

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

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

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

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

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

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

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

4. DESCRIPCIÓN DE USO DE ESTA GUÍA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   ii. No instalar otros sistemas operativos en el equipo.

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

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

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

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

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

   - ESTÁNDAR.
   - USO OFICIAL.
   - MATERIAS CLASIFICADAS.

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

   - BÁSICA
   - MEDIA
   - ALTA
   - SISTEMAS CLASIFICADOS

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

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

Tabla 1. Selección de perfil de medidas de seguridad

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

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

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

   i. Si el servidor va a ser un controlador de dominio, se debe proceder de la siguiente manera:

      - Debido a la existencia de un dominio, será necesario revisar y aplicar el apartado correspondiente a la seguridad de Active Directory.
      - Revisar e implementar el apartado correspondiente a la aplicación de seguridad sobre un controlador de dominio.

   ii. Si el servidor es un servidor miembro del dominio, se debe proceder de la siguiente forma:

      - Revisar e implementar el apartado correspondiente a la aplicación de seguridad sobre un servidor miembro.

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

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

5. PERFIL DE CUMPLIMIENTO TÉCNICO ESPECÍFICO ENS

El presente apartado recoge el conjunto de medidas de aplicación técnica que es posible aplicar según las necesidades descritas por el ENS a los sistemas operativos Windows Server, independientemente de la calificación de la información y/o la categoría asociada al sistema de información TIC.

Los elementos descritos a continuación es lo que se considera el Perfil de Cumplimiento Técnico Específico (PCTE), asociado a los sistemas operativos Windows Server.

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

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2

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

En total, según se puede apreciar en la tabla, es posible la aplicación directa de catorce (14) medidas de seguridad de forma técnica al sistema operativo Windows Server. Estás serán identificadas en los apartados posteriores, así como definidas a nivel técnico.

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

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

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

6. PERFIL DE CUMPLIMIENTO TÉCNICO ESPECÍFICO CCN-STIC

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

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

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

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

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.acc.1	Identificación	T A	aplica	+ R1	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1	+ R1 + R2
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1	+ R1 + R2 + R3 + R4 + R6 + R7

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica	+ R1
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5 + R6 + R7

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9	+ [R1[1] o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9 + R10
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica	+ R1 + R2 + R3+ R4 + R5 + R6 + R7 + R8 + R9 + R10 + R11 + R12

[1] Se han establecido controles adicionales en el uso de contraseñas como elemento de autenticación.

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad			
			BAJO	MEDIO	ALTO	MC
			Categoría de seguridad del sistema			
			BÁSICA	MEDIA	ALTA	MC
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6 + R7
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5 + R6
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5	+ R1 + R2 + R3 + R4 + R5 + R6 + R7 + R8
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2	+ R1 + R2
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5 + R6
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2	+ R1 + R2

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

En total, según se puede apreciar en la tabla, es posible la aplicación directa de catorce (14) medidas de seguridad de forma técnica al sistema operativo Windows Server. Estás serán identificadas en los apartados posteriores, así como definidas a nivel técnico.

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

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

ANEXO A. PASO A PASO DE CONFIGURACIÓN BASE DE SEGURIDAD SOBRE WINDOWS SERVER

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

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

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

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

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

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

a) Dominio: Aplicación de elementos de seguridad sobre el conjunto de objetos pertenecientes al dominio mediante configuraciones de objetos GPO.

b) Controladores de Dominio (Domain Controllers): Se definirán acciones manuales y automáticas para asegurar los equipos que cumplen la función de Controlador de Dominio dentro de un dominio. De igual modo se aplicarán medidas de seguridad a los objetos del dominio mediante objetos GPO.

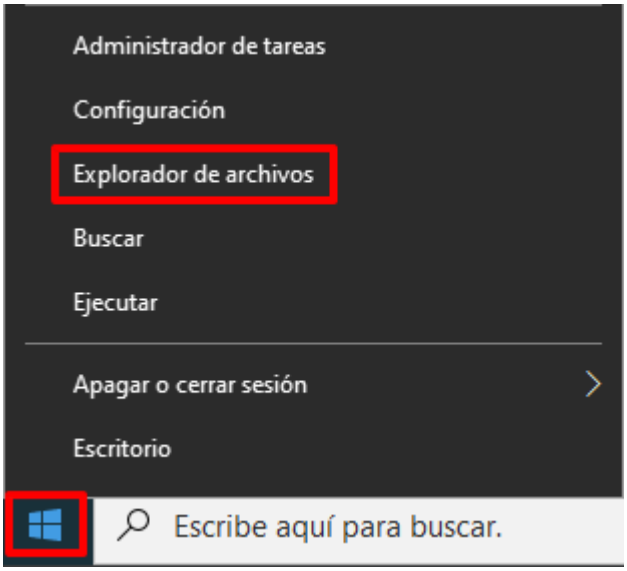
c) Servidores miembro del dominio: Aplicable a aquellos equipos que proporcionen cualquier tipo de servicio dentro del dominio, se definirán medidas de seguridad mediante objetos GPO y al igual que en las configuraciones para Controladores de Dominio se ejecutarán acciones manuales y automatizadas para finalizar las labores de configuración segura.

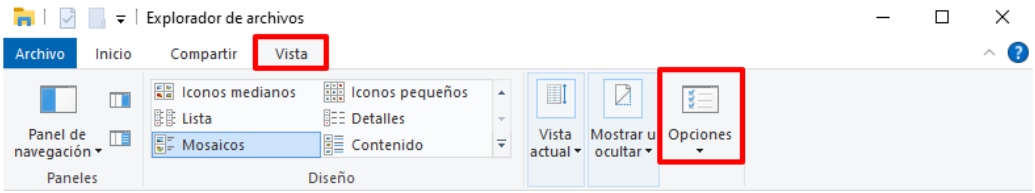
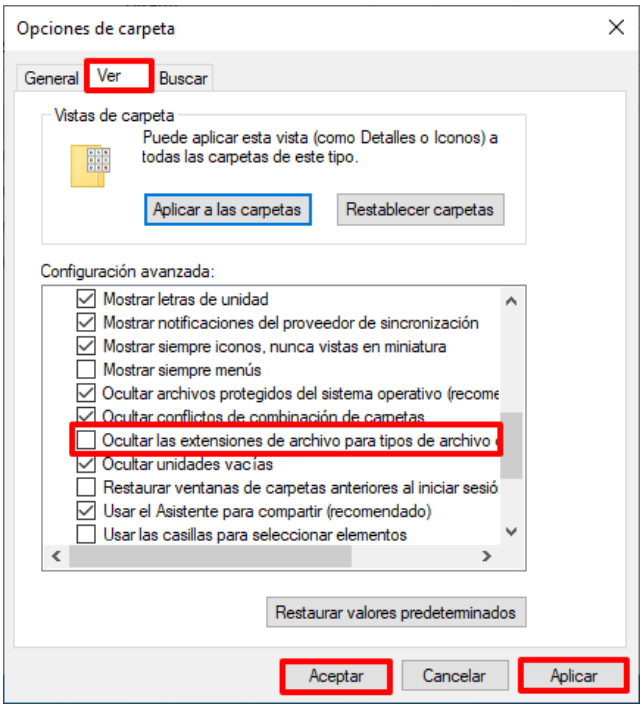
d) Configuraciones individuales: Es necesario indicar que ciertas medidas de seguridad no pueden ser aplicadas por medio de objetos GPO o configuraciones exactas a nivel de Windows. Esto es debido a que deben ser personalizadas por cada organización o adaptadas a esta. Por ello, se han dedicado apartados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

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

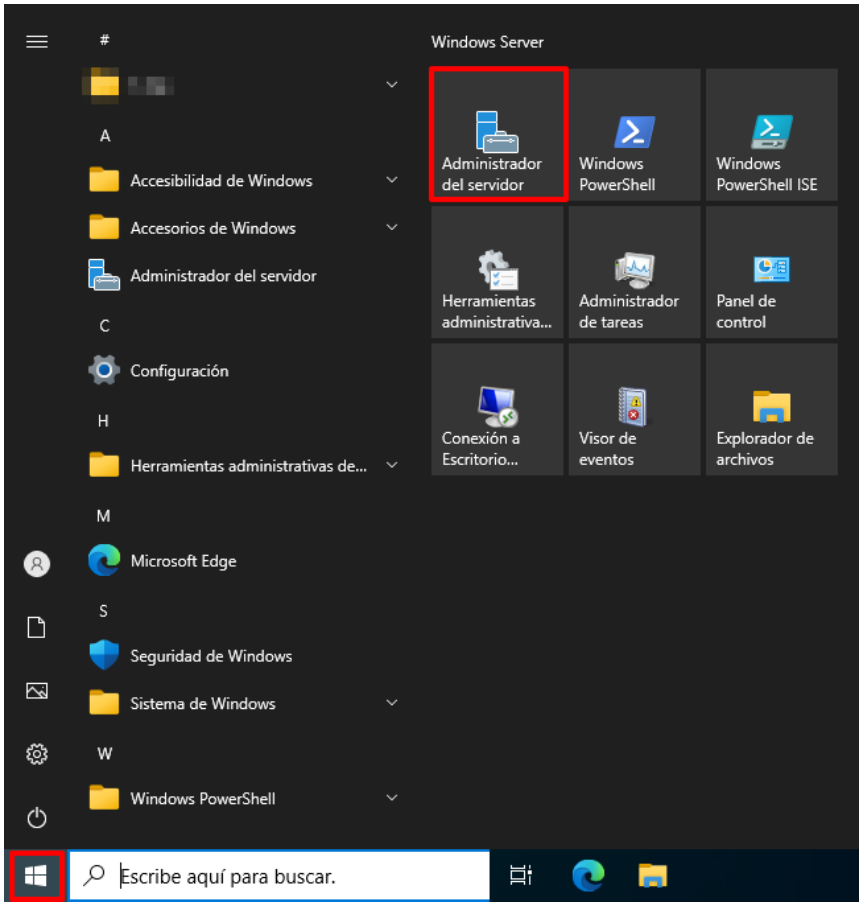
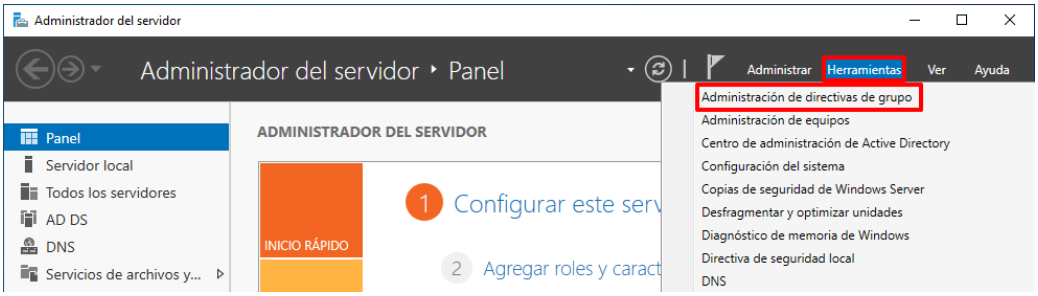
ANEXO A.1. PREPARACIÓN DEL DOMINIO

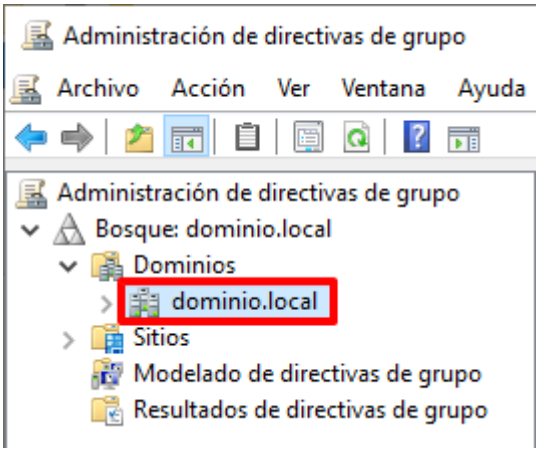
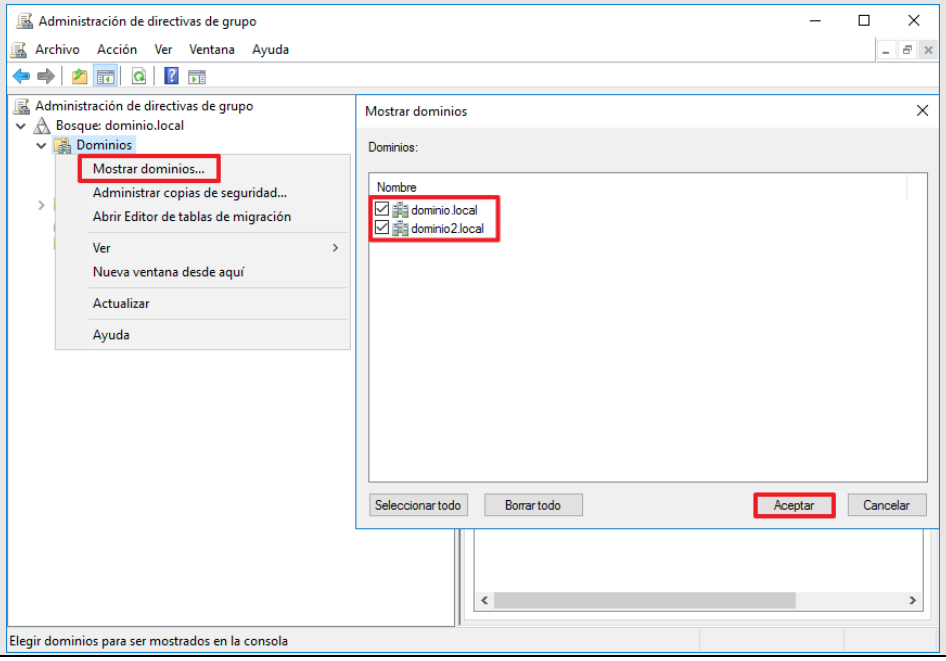
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las medidas de seguridad mediante objetos GPO. Solo es necesario realizar este procedimiento una (1) vez.

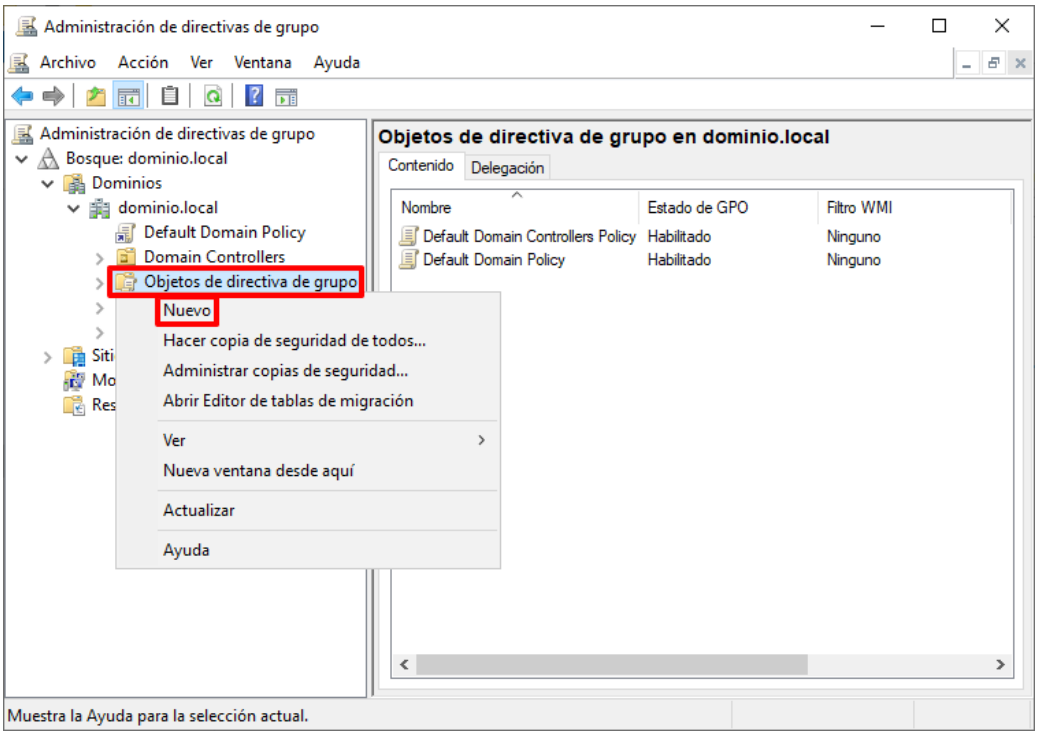
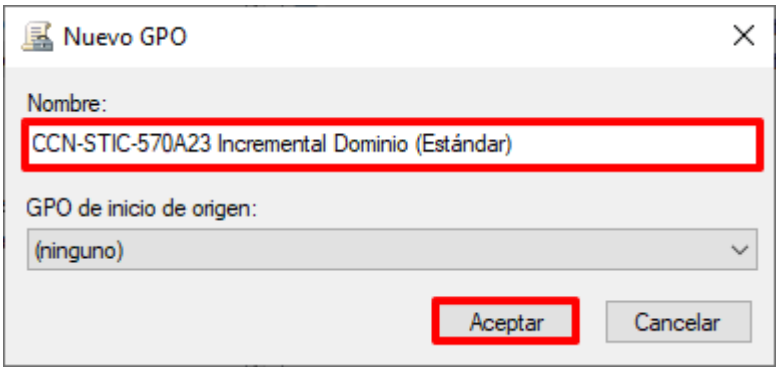
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad C:\.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio “Scripts-570A23”.
4.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 

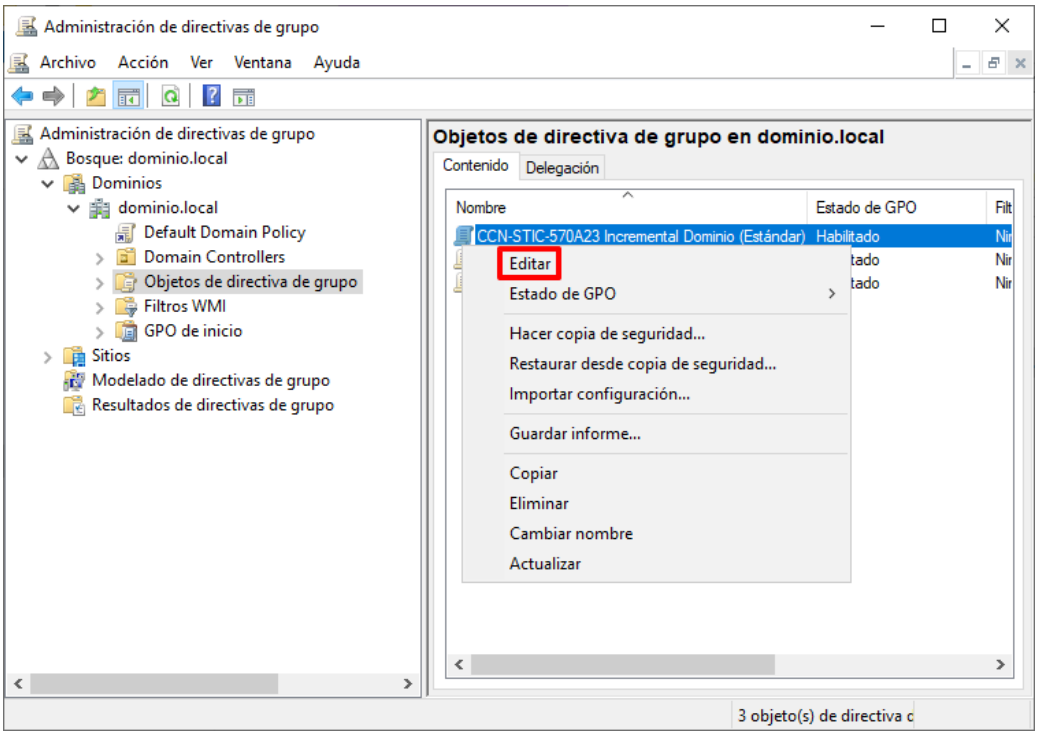
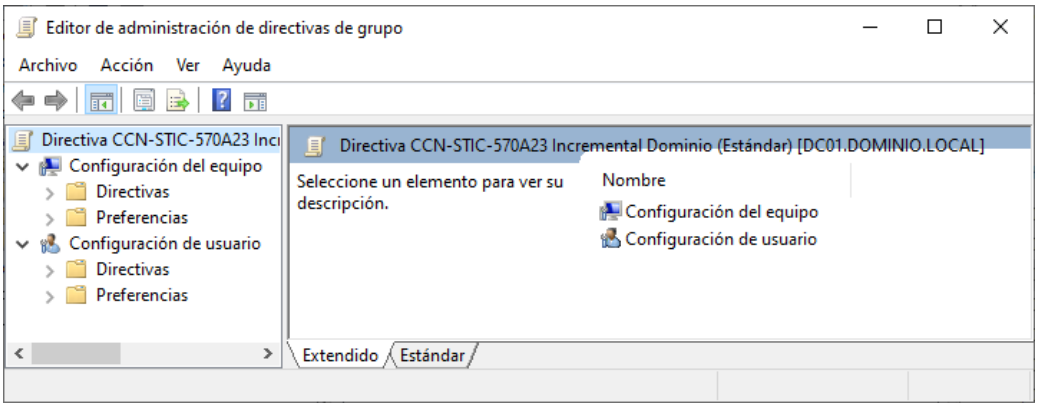
Paso	Descripción
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – ESTANDAR/USO OFICIAL/MATERIAS CLASIFICADAS • CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-570A23 Incremental Actualizaciones WU [Directorio] • CCN-STIC-570A23 Incremental Control Dispositivos [Directorio] • CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) [Directorio]

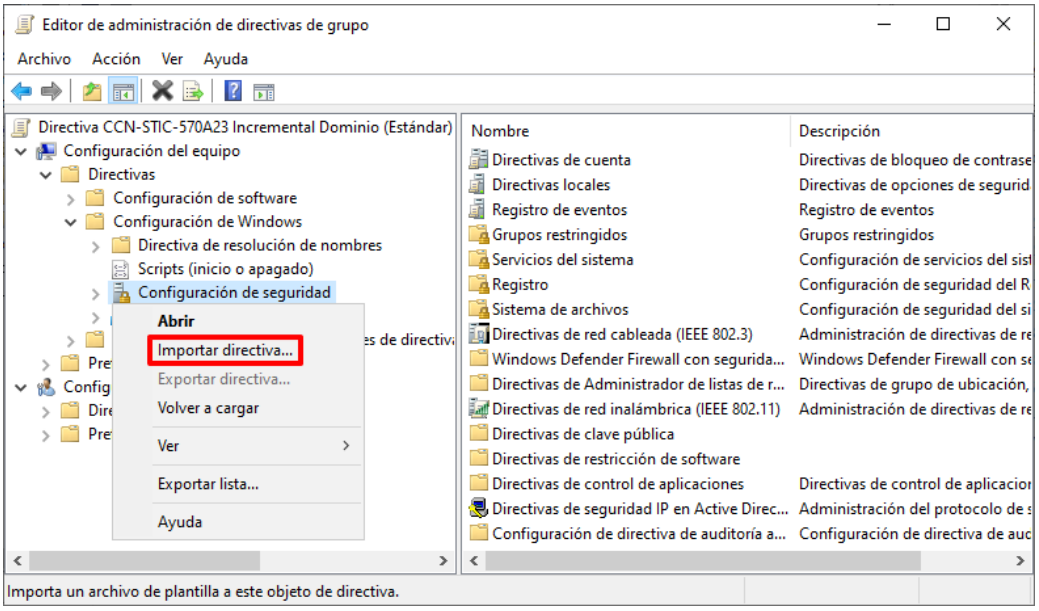
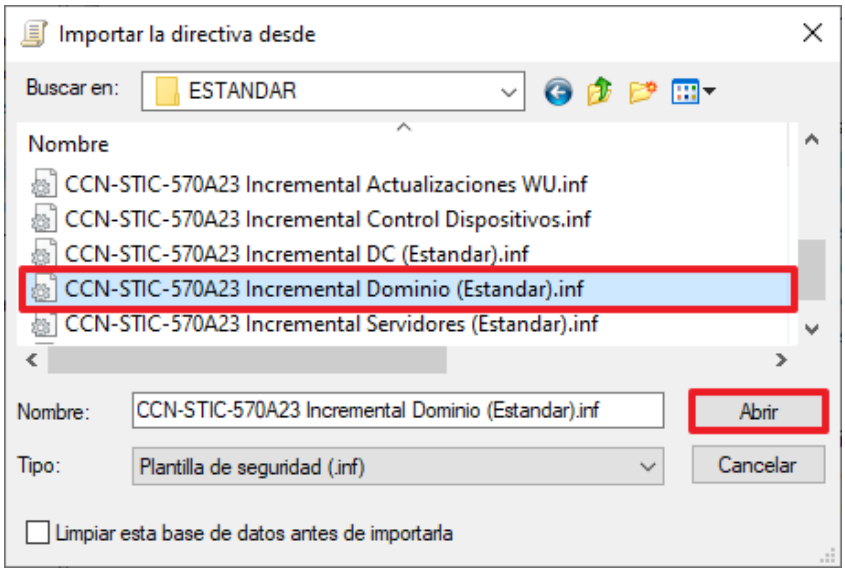
Paso	Descripción
	• CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).inf • CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).wfw • CCN-STIC-570A23 Incremental Actualizaciones WU.inf • CCN-STIC-570A23 Incremental Control Dispositivos.inf • CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]).inf • CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]).wfw • CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO]).inf • CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]).inf • CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]).wfw • CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO]).inf • CCN-STIC-570A23 Incremental BitLocker [Directorio] (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) • CCN-STIC-570A23 Incremental BitLocker.inf (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) – CCN-STIC-570A23 Controlador de Dominio - Configuración de Credenciales Admins.bat – CCN-STIC-570A23 Controlador de Dominio – Desinstalar roles y características.bat – CCN-STIC-570A23 Controlador de Dominio – Segregación de roles.bat – CCN-STIC-570A23 Controlador de Dominio – Suspensión de cuentas por no utilización.bat – CCN-STIC-570A23 Servidor Miembro – Desinstalar roles y características.bat – CCN-STIC-570A23 Windows Defender - Análisis de dispositivos USB.bat – CCN-STIC-570A23 Windows Defender - Análisis de integridad de ficheros.bat – CCN-STIC-570A23 Windows Defender - Análisis en el arranque.bat – CCN-STIC-570A23_Analisis_arranque_OS.xml – CCN-STIC-570A23_Analisis_dispositivos_USB.xml – CCN-STIC-570A23_Configuracion_credenciales.ps1 – CCN-STIC-570A23_Desinstala_roles_y_caracteristicas_DC.ps1 – CCN-STIC-570A23_Desinstala_roles_y_caracteristicas_servidor.ps1 – CCN-STIC-570A23_Integridad_ficheros.xml – CCN-STIC-573A23_Analisis_arranque.ps1

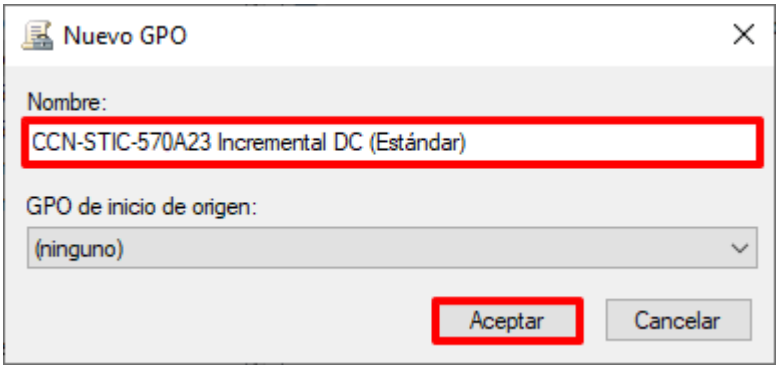
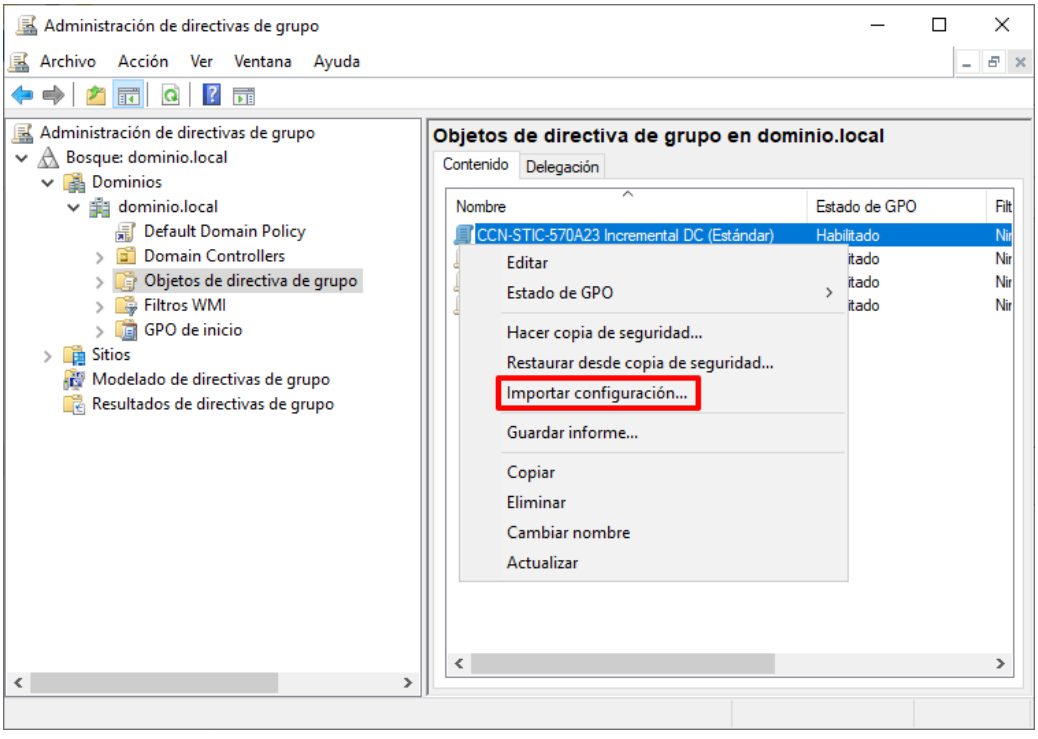
Paso	Descripción
	– CCN-STIC-573A23_Analisis_USBs.ps1 – CCN-STIC-573A23_Habilitar_registro_conexion_USBs.ps1 – CCN-STIC-570A23_Suspension_por_no_utilizacion.ps1
8.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.
9.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 

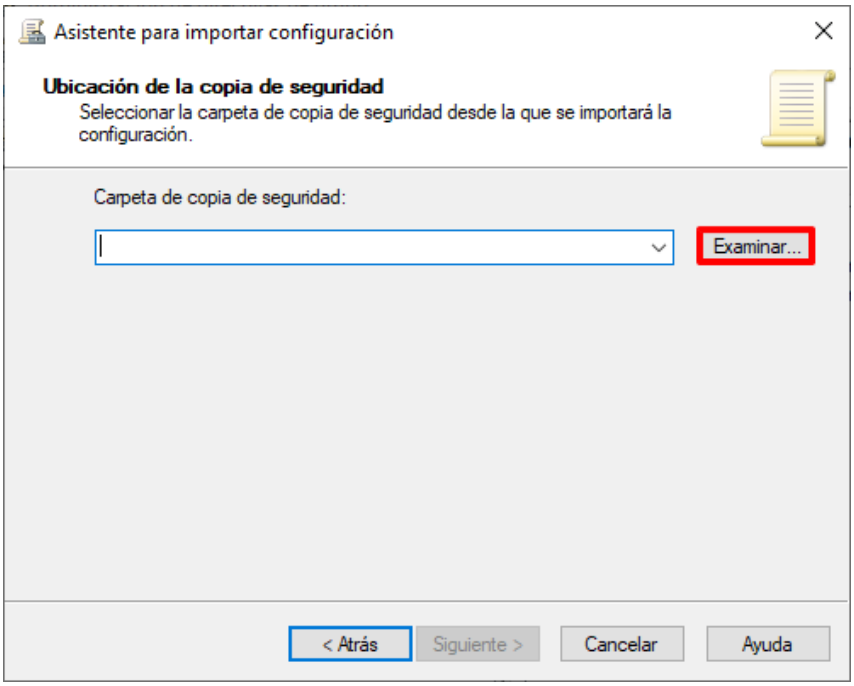
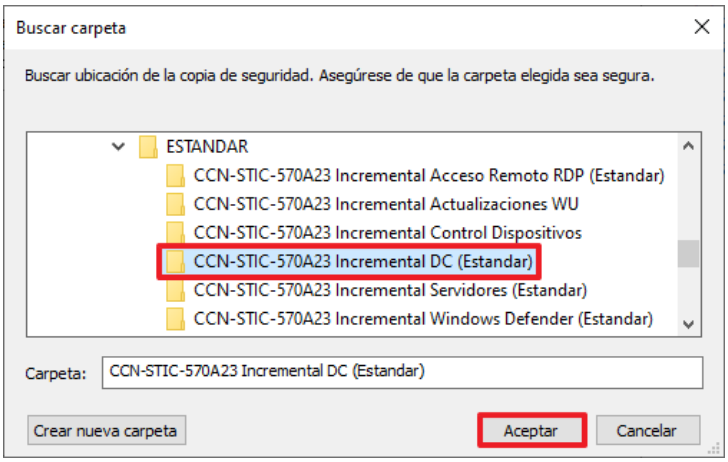
Paso	Descripción
10.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

Paso	Descripción
11.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
12.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO])**" y pulse el botón "Aceptar".  **Nota:** Defina el nombre del objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

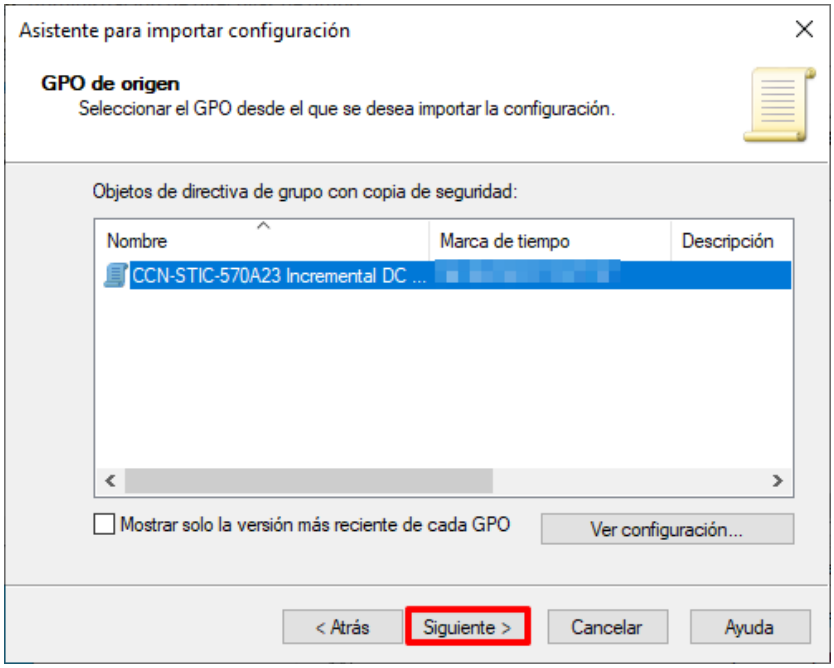
Paso	Descripción
13.	Seleccione con el botón derecho el GPO recién creado, “CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
14.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO. 

Paso	Descripción
15.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. Seleccione con el botón derecho el nodo "Configuración de seguridad" y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 
16.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO]).inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

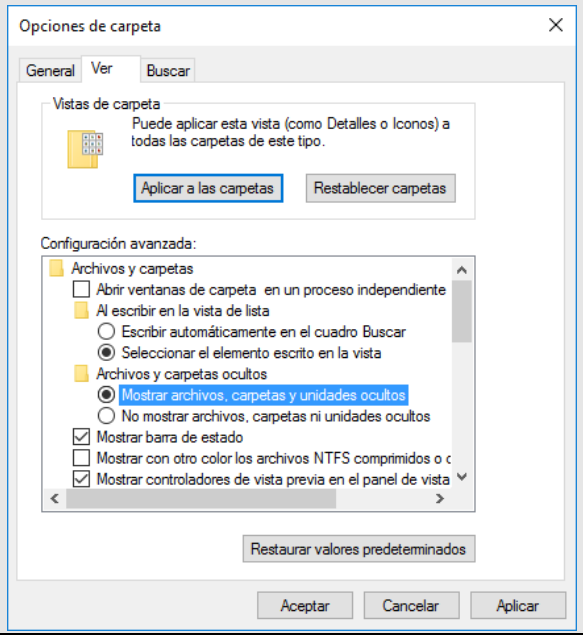
Paso	Descripción
17.	Con eso habrá quedado importada la plantilla en el objeto GPO. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada sobre los objetos requeridos. Cierre la ventana "Editor de administración de directivas de grupo".
18.	De nuevo en la consola "Administración de directivas de grupo", seleccione con el botón derecho el contenedor "Objetos de directiva de grupo" y seleccione la opción "Nuevo" del menú contextual que aparecerá". Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])**".  **Nota:** Defina el nombre del objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
19.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre "Importar configuración…" del menú contextual que aparecerá. 

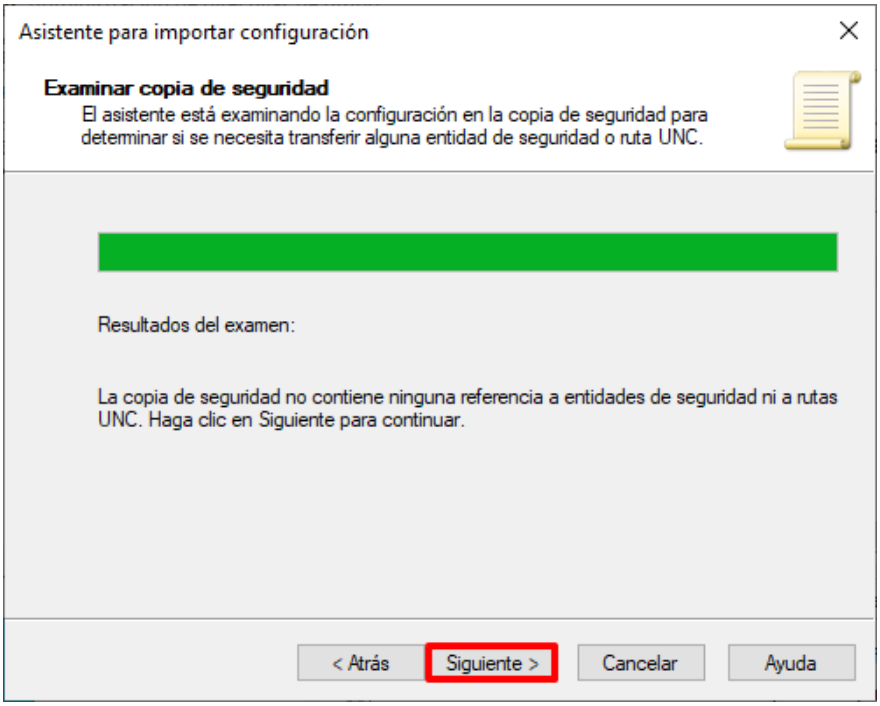
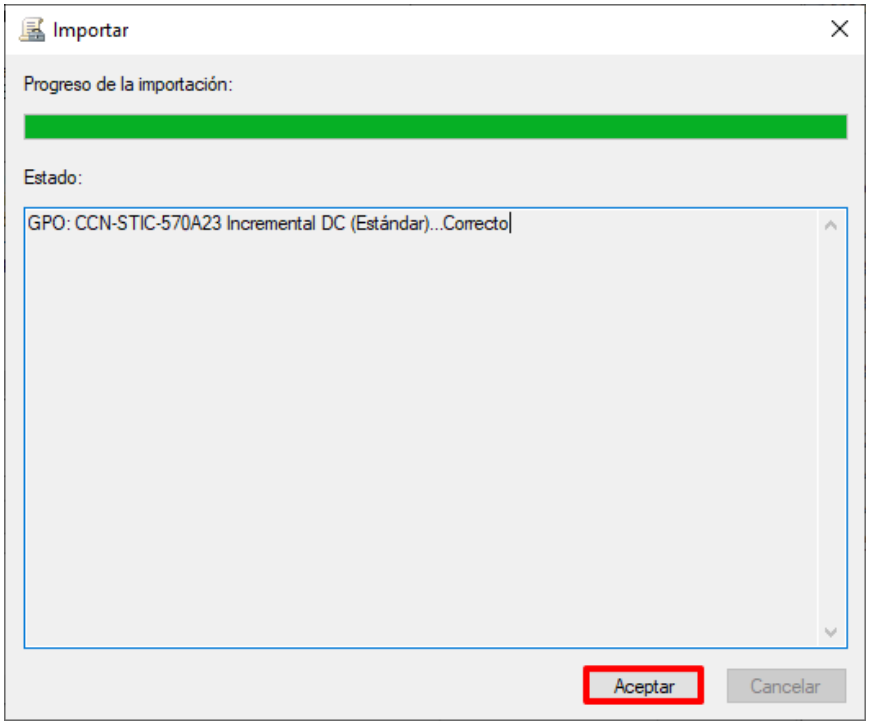
Paso	Descripción
20.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
21.	En la sección “Hacer copia de seguridad de GPO” pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad puesto que la política se encuentra vacía.
22.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
23.	Seleccione la carpeta “CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

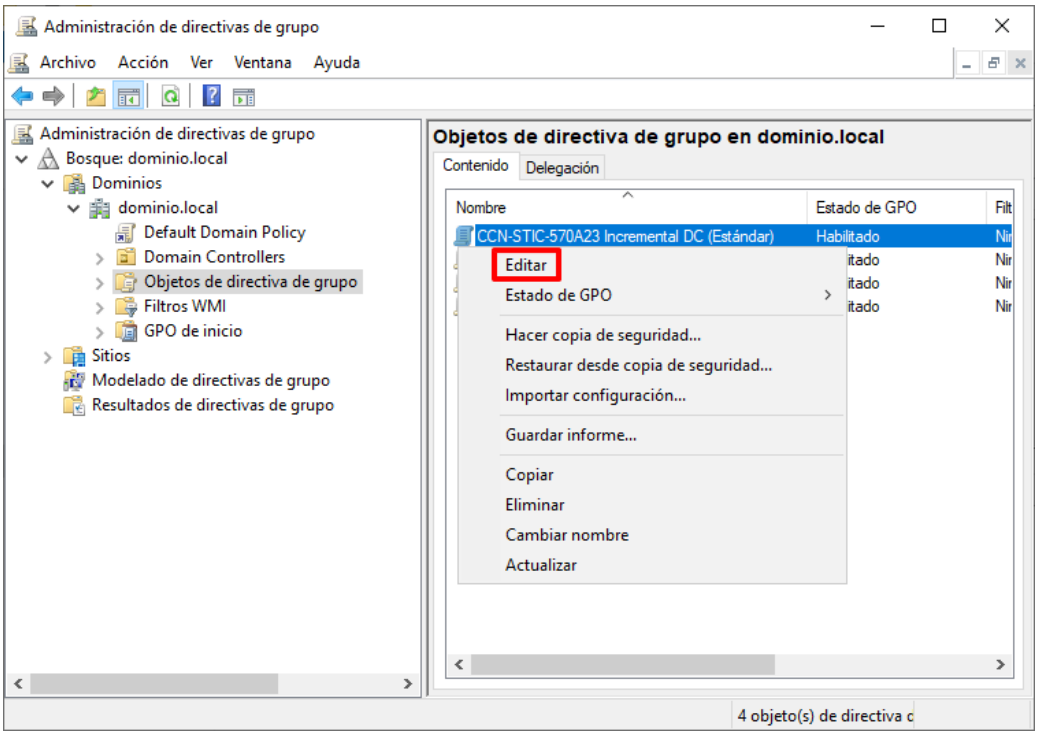
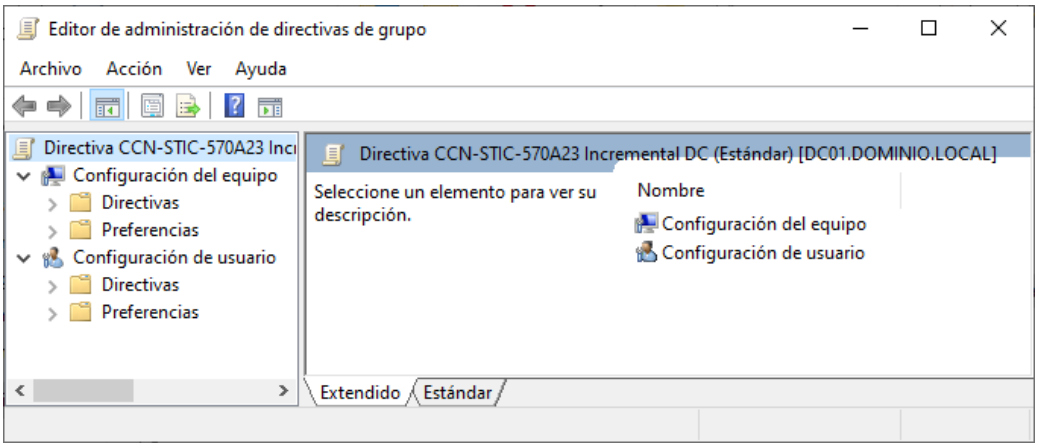
Paso	Descripción
24.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.
25.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])” y pulse “Siguiente >”.

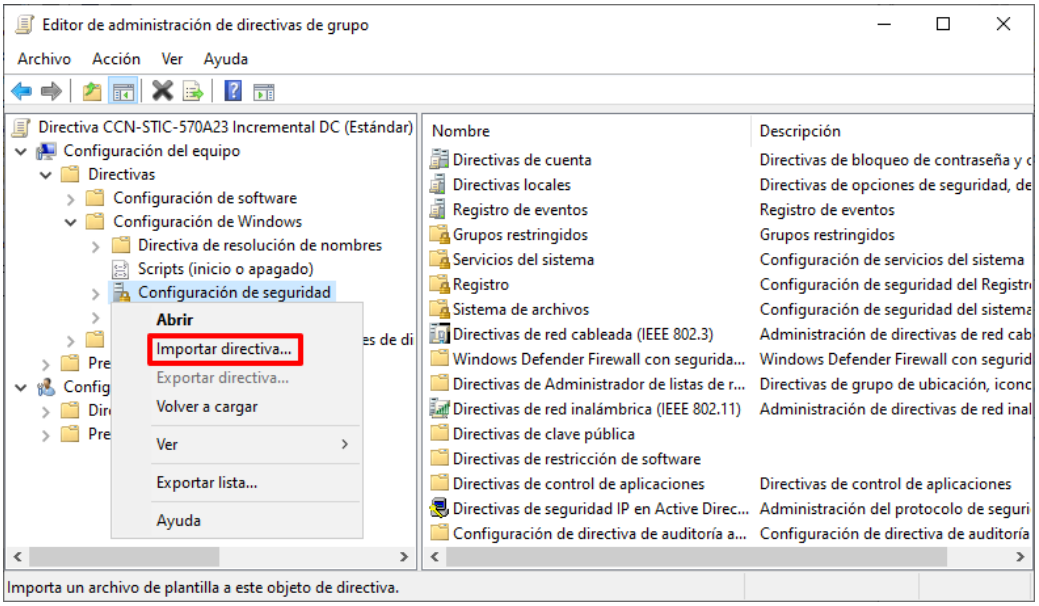
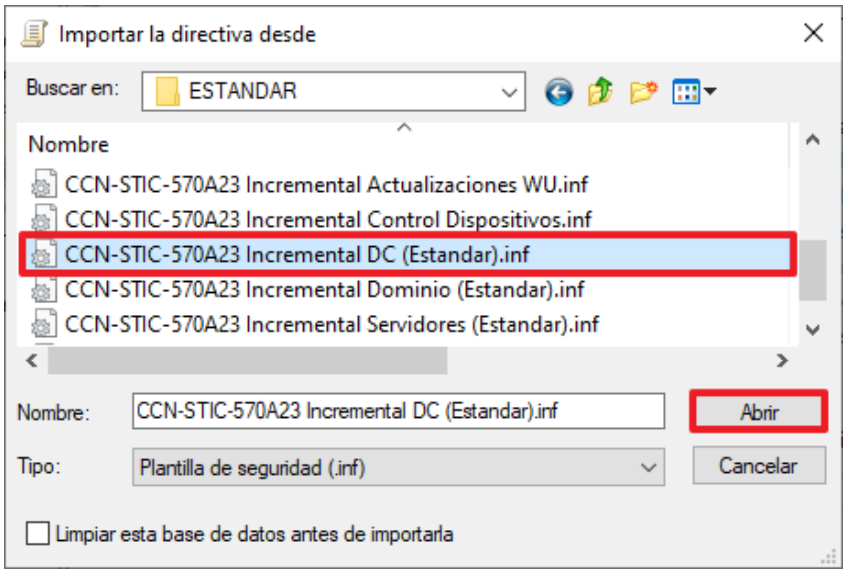


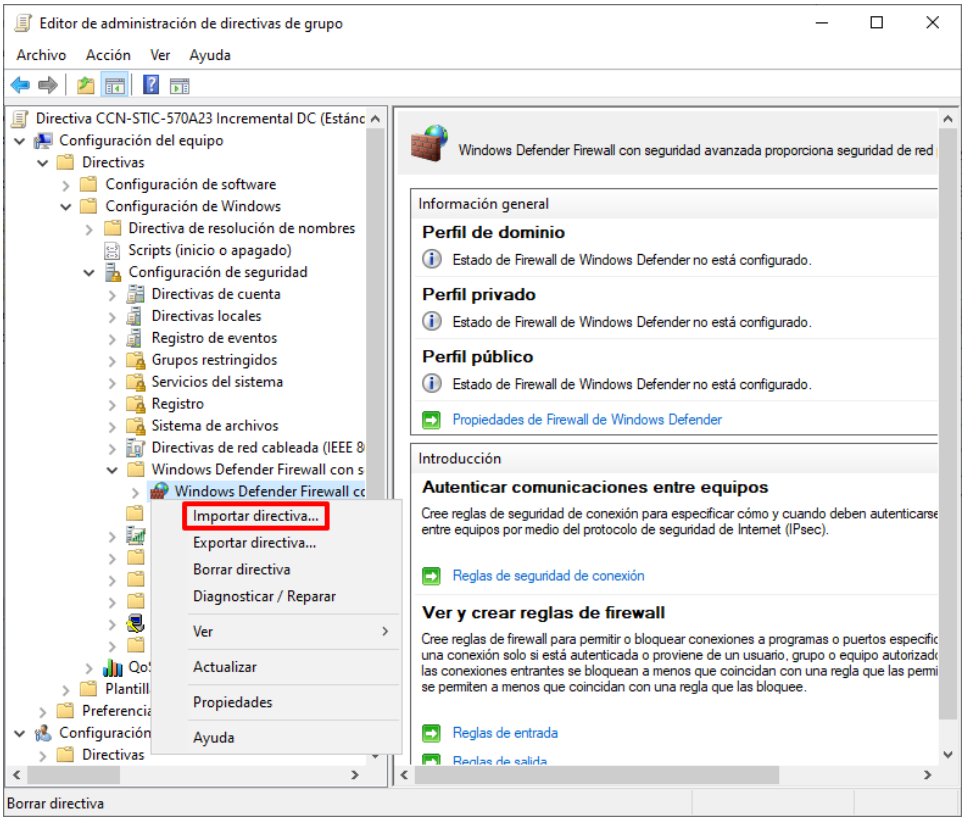
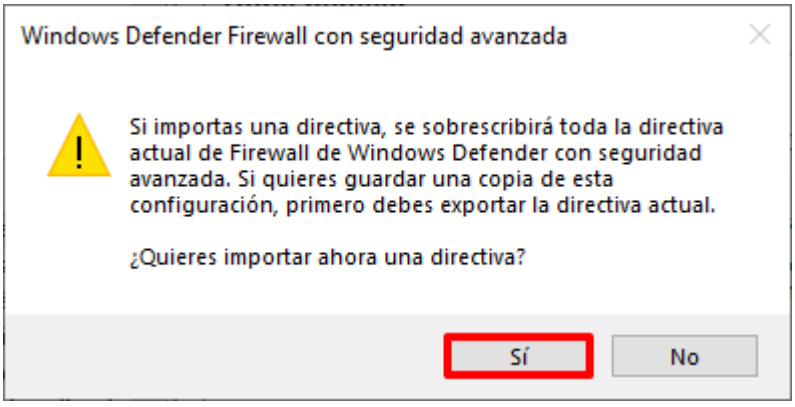
Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”.

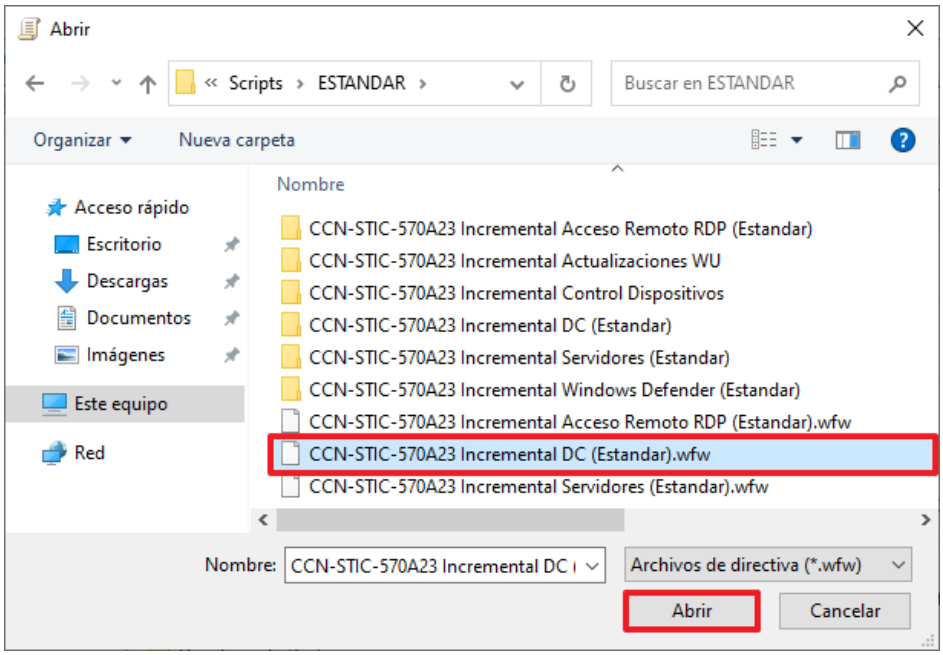
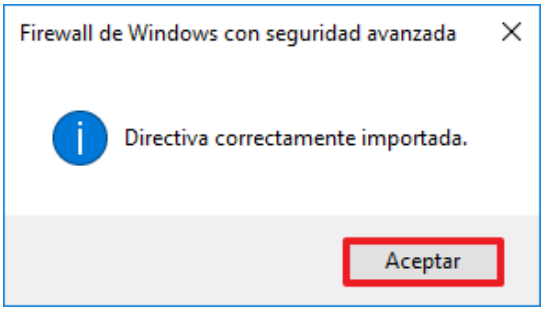


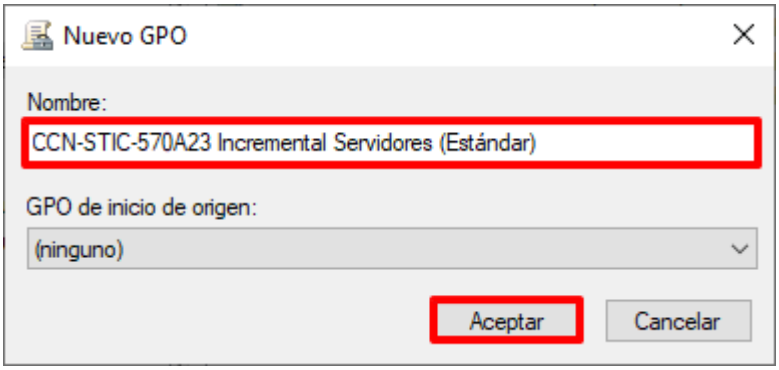
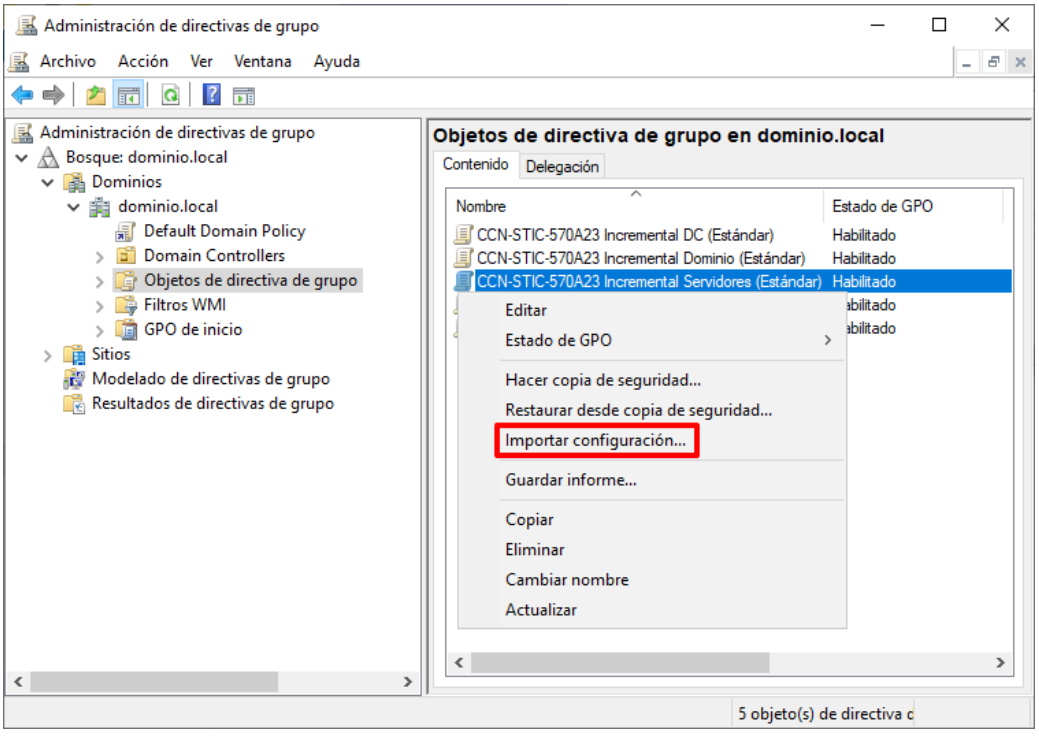
Paso	Descripción
26.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
27.	Para completar el asistente pulse sobre el botón “Finalizar”.
28.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

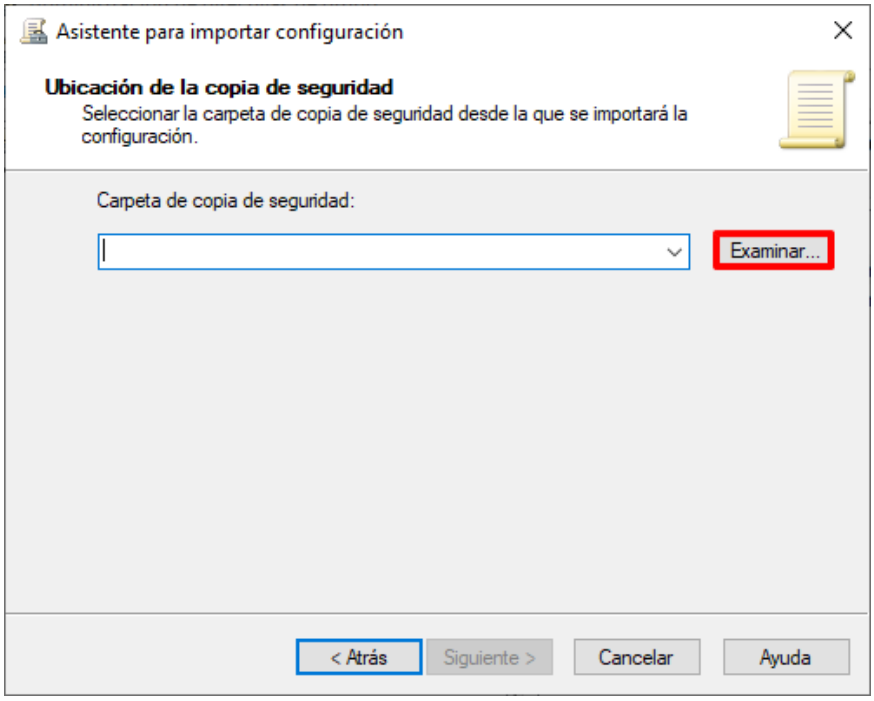
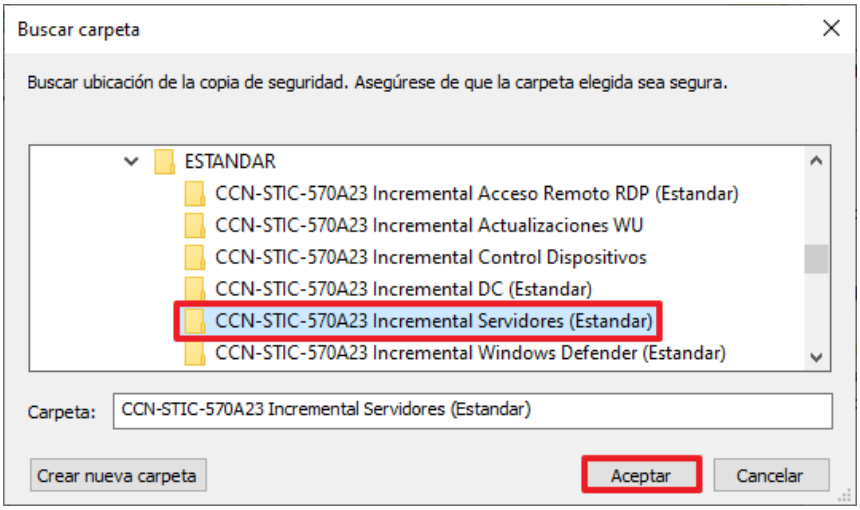
Paso	Descripción
29.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
30.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO. 

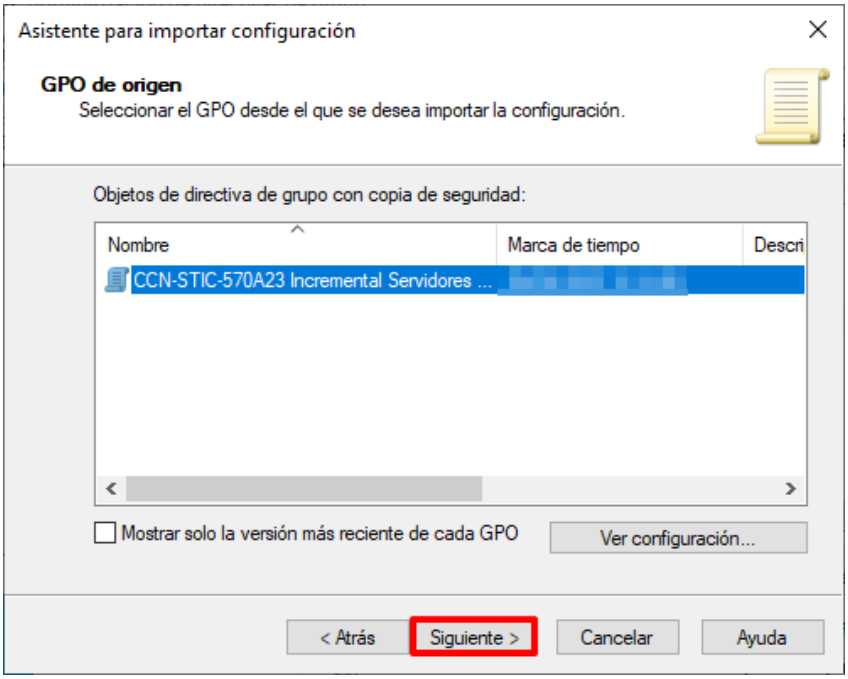
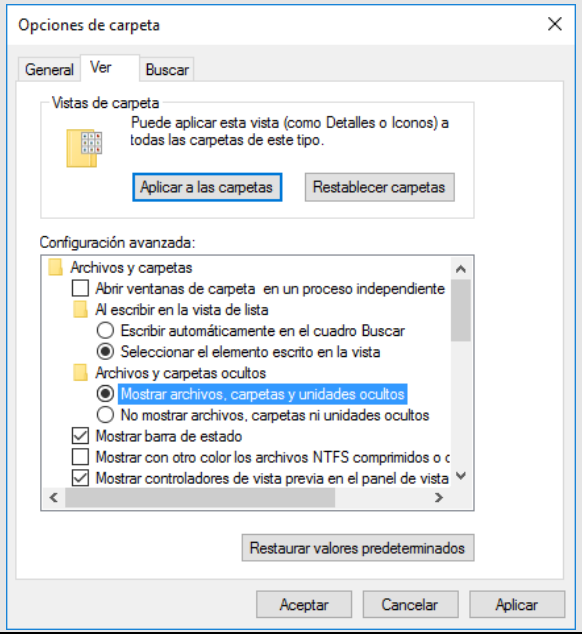
Paso	Descripción
31.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. Seleccione con el botón derecho el nodo "Configuración de seguridad" y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 
32.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]).inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

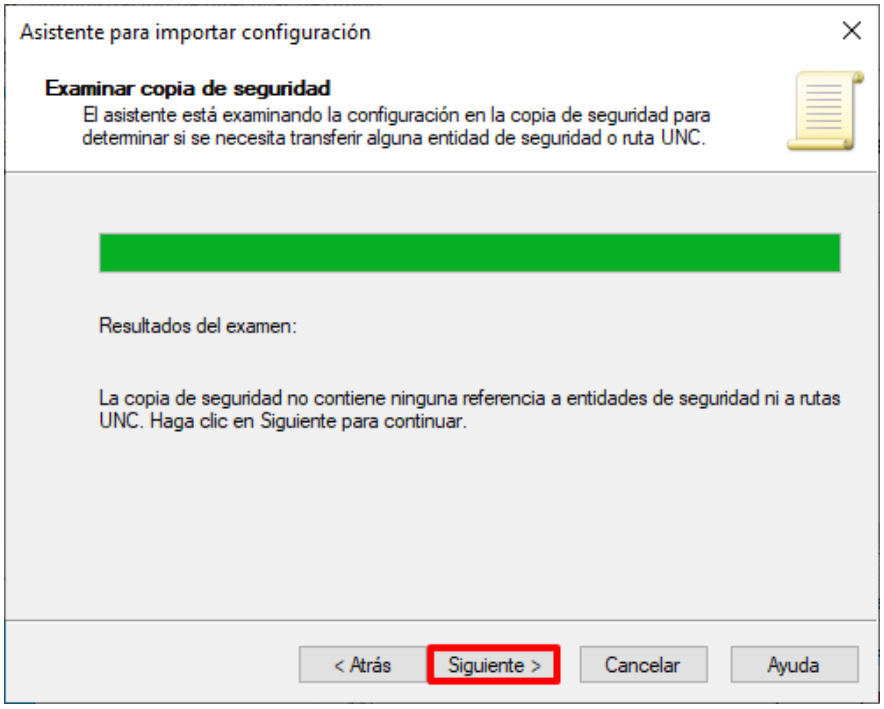
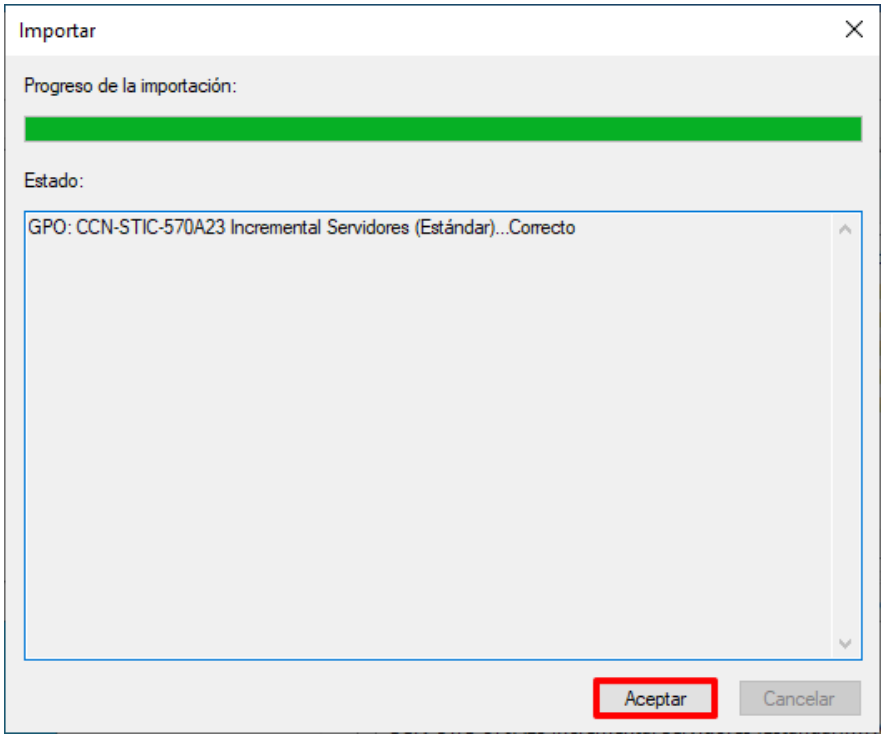
Paso	Descripción
33.	En la misma ventana del editor de administración de directivas de grupo, seleccione el siguiente nodo: "**Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada - LDAP://CN={<SID>},CN=POLICIES,CN=SYSTEM,DC=<su nombre de dominio>**". A continuación, pulse con el botón derecho sobre el nodo desplegado y seleccione la opción "Importar directiva…" del menú contextual que aparecerá. 
34.	Responda "Sí" a la pregunta de confirmación "¿Desea importar ahora una directiva? 

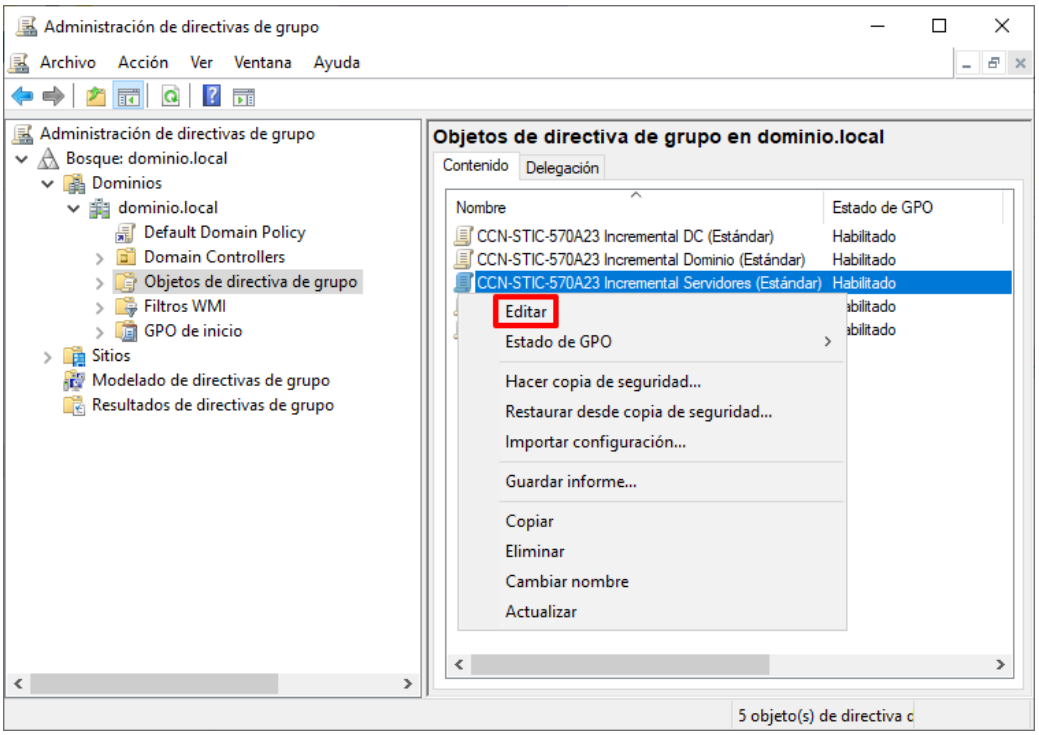
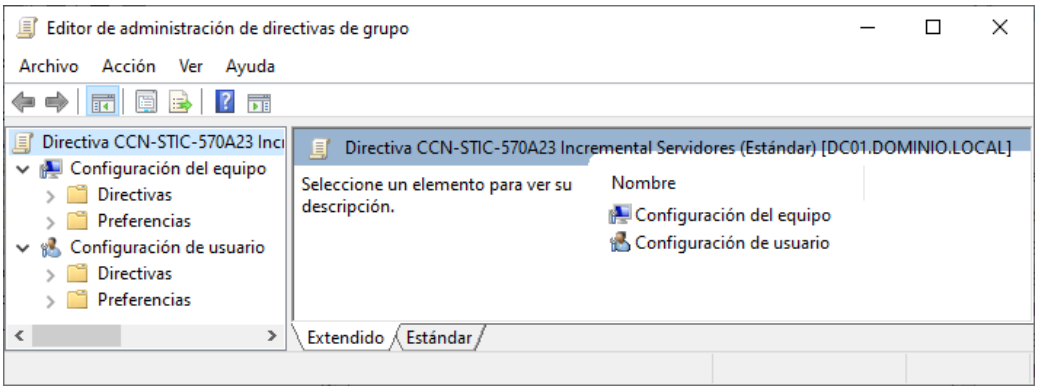
Paso	Descripción
35.	En el cuadro de diálogo que aparecerá, seleccione la directiva "C:\Scripts\[TIPO DE PERFILADO]\CCN-STIC-570A Incremental DC ([TIPO DE PERFILADO]).wfw" y pulse el botón "Abrir".  **Nota:** Seleccione la configuración de firewall acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
36.	Al finalizar correctamente la importación de la directiva de firewall aparecerá la siguiente ventana con el mensaje de confirmación "Directiva correctamente importada". Pulse el botón “Aceptar” para cerrar la ventana y poder continuar. 
37.	Con eso habrá quedado importada la plantilla en el objeto GPO. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada sobre los objetos requeridos. Cierre la ventana “Editor de administración de directivas de grupo”.
38.	A continuación, se ejecutarán los mismos pasos para la creación e importación de configuración de seguridad que será aplicada a los servidores miembro del dominio.

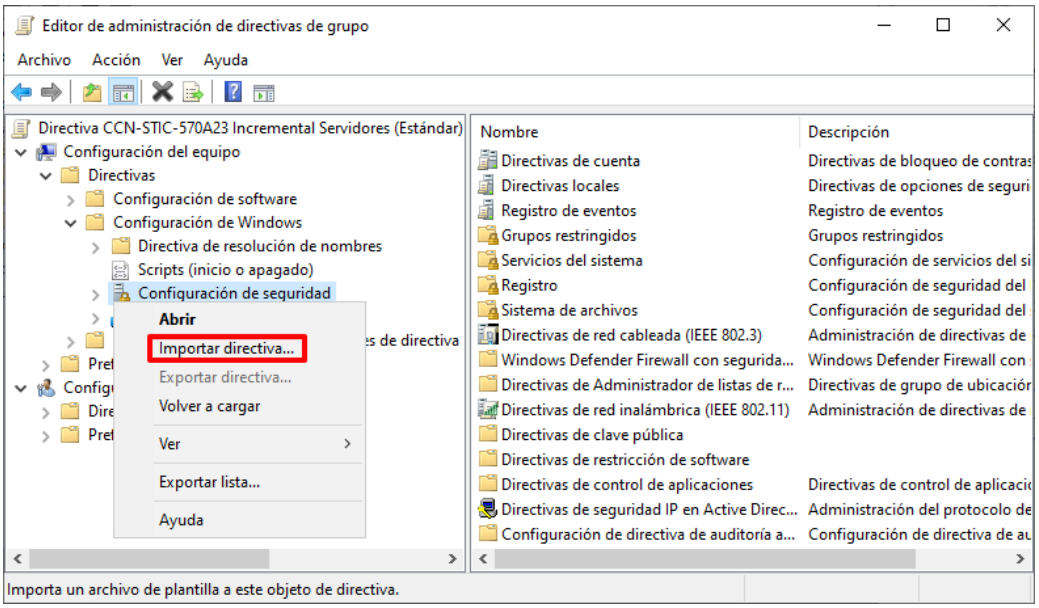
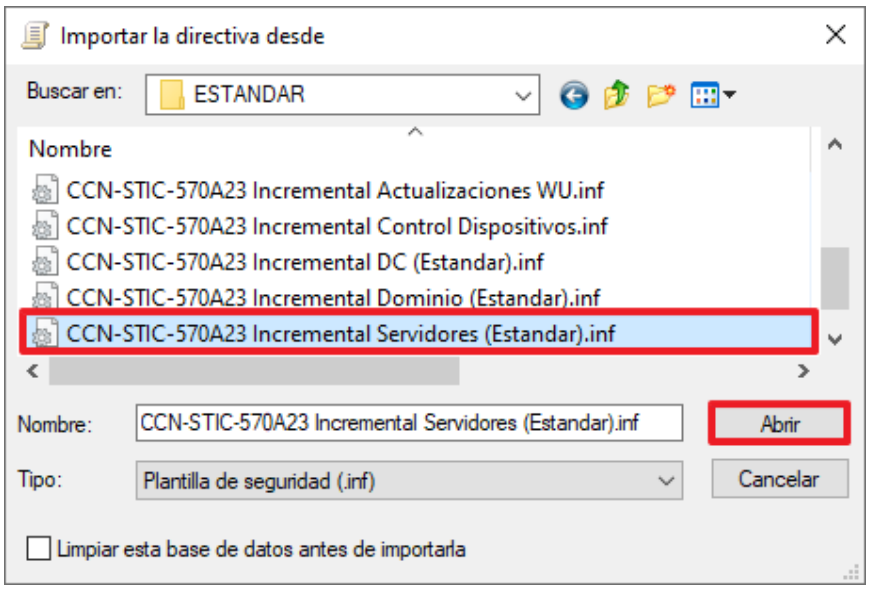
Paso	Descripción
39.	De nuevo en la consola “Administración de directivas de grupo”, seleccione con el botón derecho el contenedor “Objetos de directiva de grupo” y seleccione la opción “Nuevo” del menú contextual que aparecerá”. Asigne el siguiente nombre al nuevo objeto GPO: “**CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])**”.  **Nota:** Defina el nombre del objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
40.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
41.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.

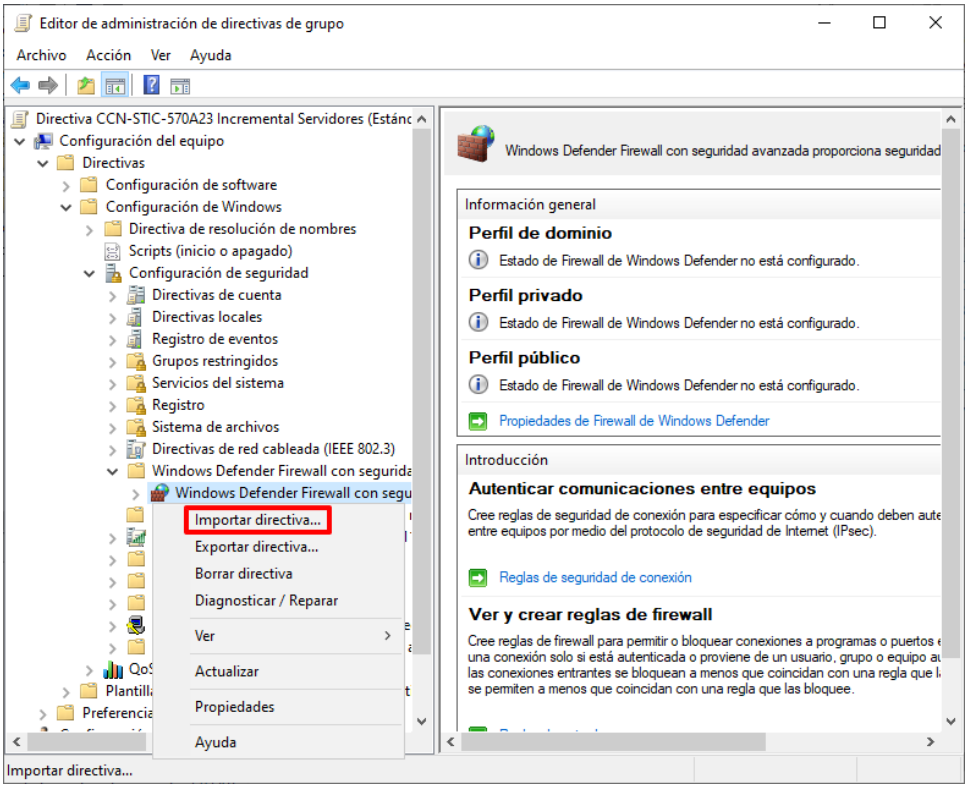
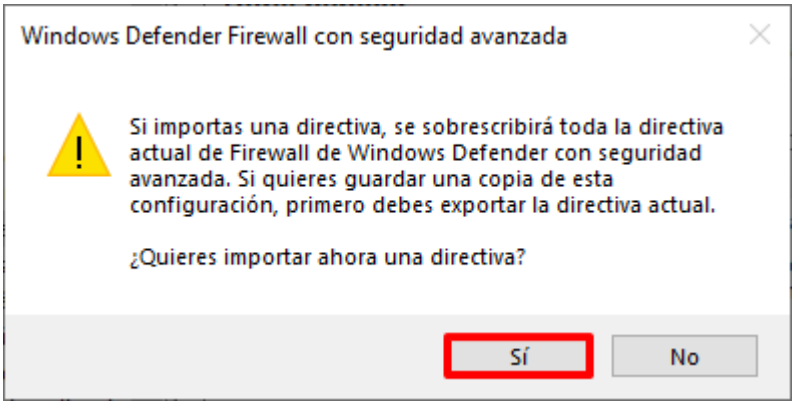
Paso	Descripción
42.	En la sección “Hacer copia de seguridad de GPO” pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad puesto que la política se encuentra vacía.
43.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
44.	Seleccione la carpeta “CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\ [TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

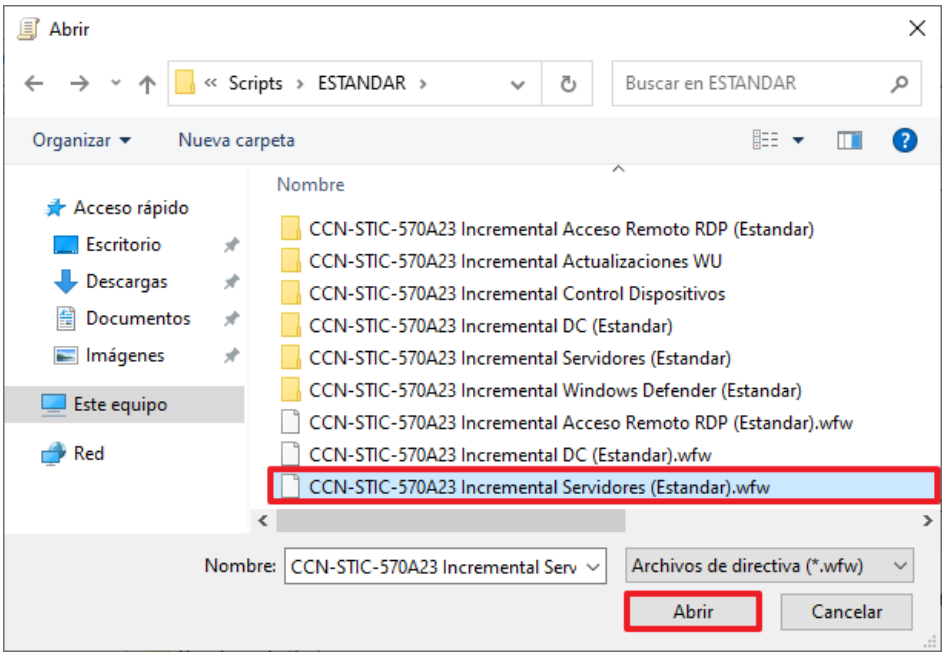
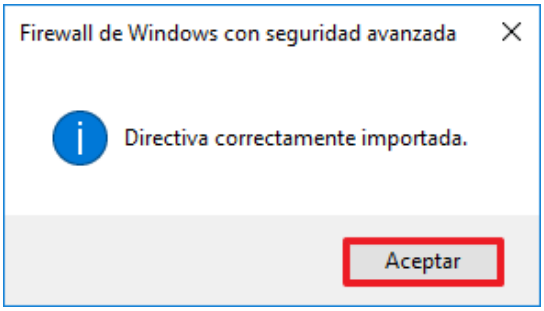
Paso	Descripción
45.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.
46.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

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

Paso	Descripción
50.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
51.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO. 

Paso	Descripción
52.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. Seleccione con el botón derecho el nodo "Configuración de seguridad" y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 
53.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\ [TIPO DE PERFILADO]" denominada "CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]).inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

Paso	Descripción
54.	En la misma ventana del editor de administración de directivas de grupo, seleccione el siguiente nodo: "**Directiva CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada - LDAP://CN={<SID>},CN=POLICIES,CN=SYSTEM,DC=<su nombre de dominio>**". A continuación, pulse con el botón derecho sobre el nodo desplegado y seleccione la opción "Importar directiva…" del menú contextual que aparecerá. 
55.	Responda "Sí" a la pregunta de confirmación "¿Desea importar ahora una directiva? 

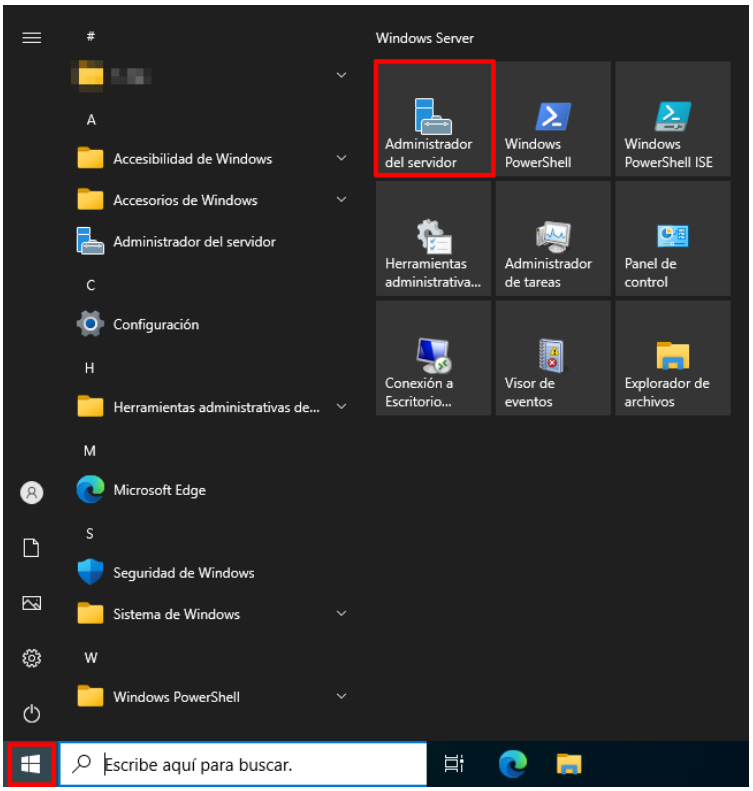
Paso	Descripción
56.	En el cuadro de diálogo que aparecerá, seleccione la directiva "C:\Scripts\[TIPO DE PERFILADO]\CCN-STIC-570A Incremental Servidores ([TIPO DE PERFILADO]).wfw" y pulse el botón "Abrir".  **Nota:** Seleccione la configuración de firewall acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
57.	Al finalizar correctamente la importación de la directiva de firewall aparecerá la siguiente ventana con el mensaje de confirmación "Directiva correctamente importada". Pulse el botón “Aceptar” para cerrar la ventana y poder continuar. 
58.	Con eso habrá quedado importada la plantilla en el objeto GPO. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada sobre los objetos requeridos. Cierre la ventana “Editor de administración de directivas de grupo”.

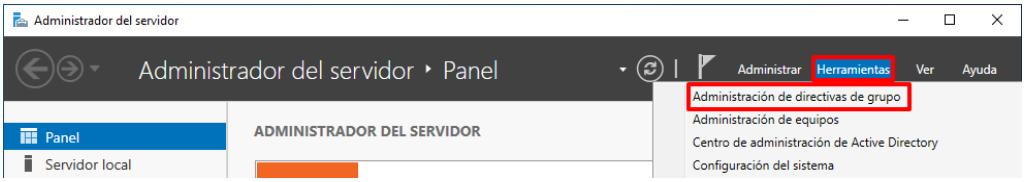
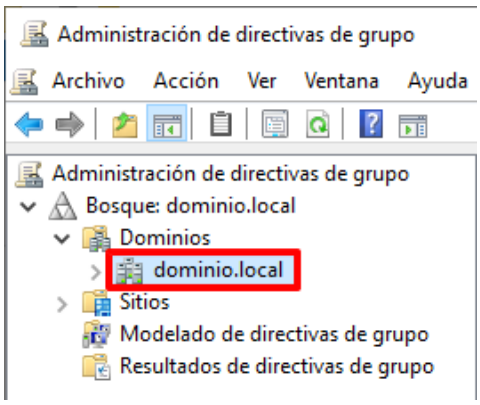
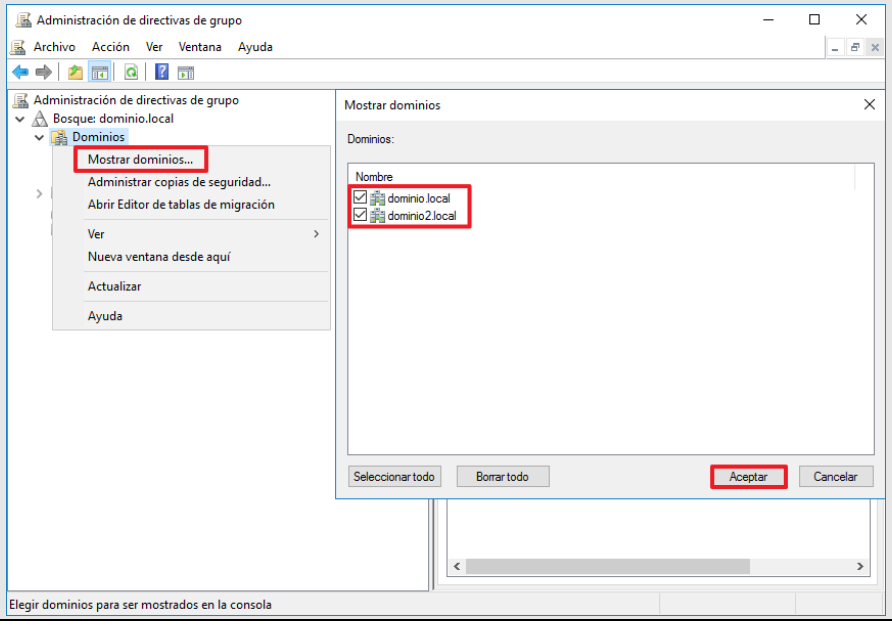
ANEXO A.2. CONFIGURACIÓN DE SEGURIDAD EN CONTROLADOR DE DOMINIO

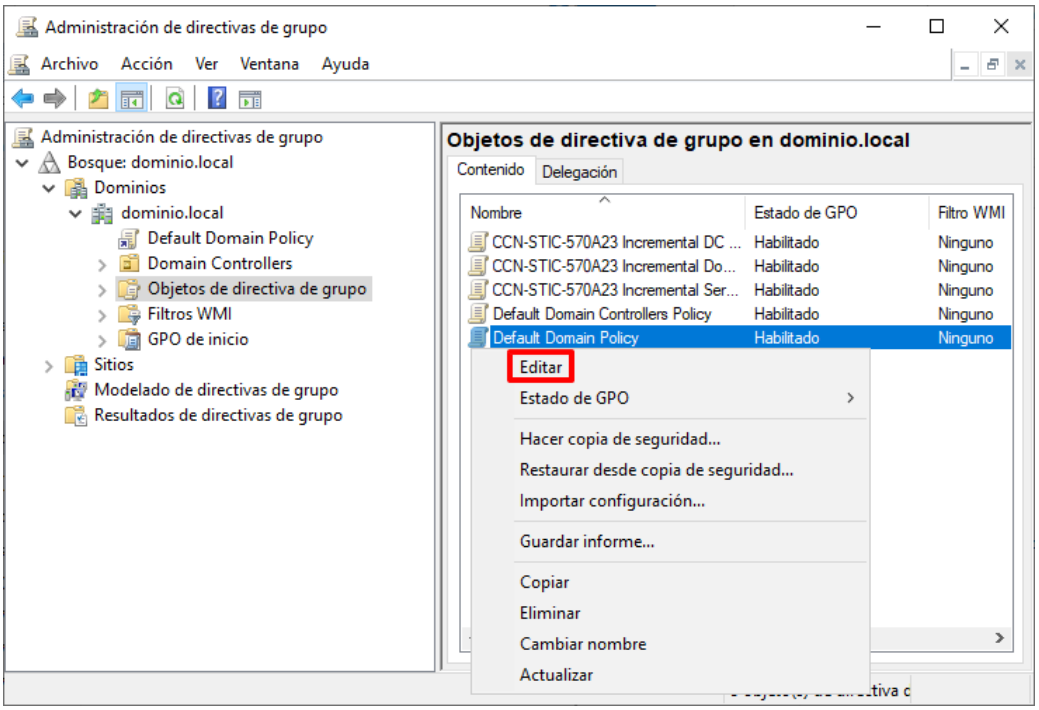
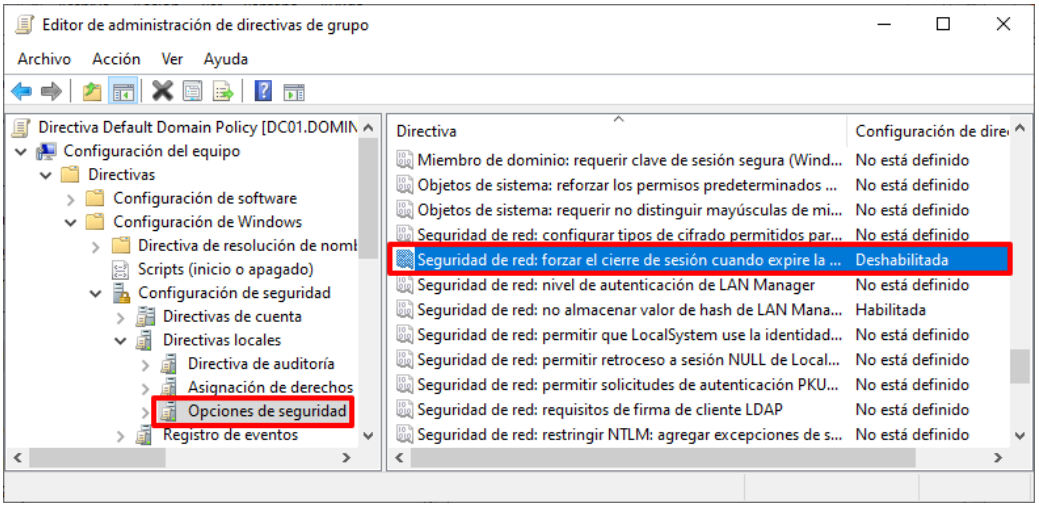
Una vez realizada la preparación de la configuración de seguridad necesaria a implementar, será necesario su aplicación sobre los objetos correspondientes, así como la ejecución de labores adicionales para cubrir todos los aspectos necesarios de seguridad.

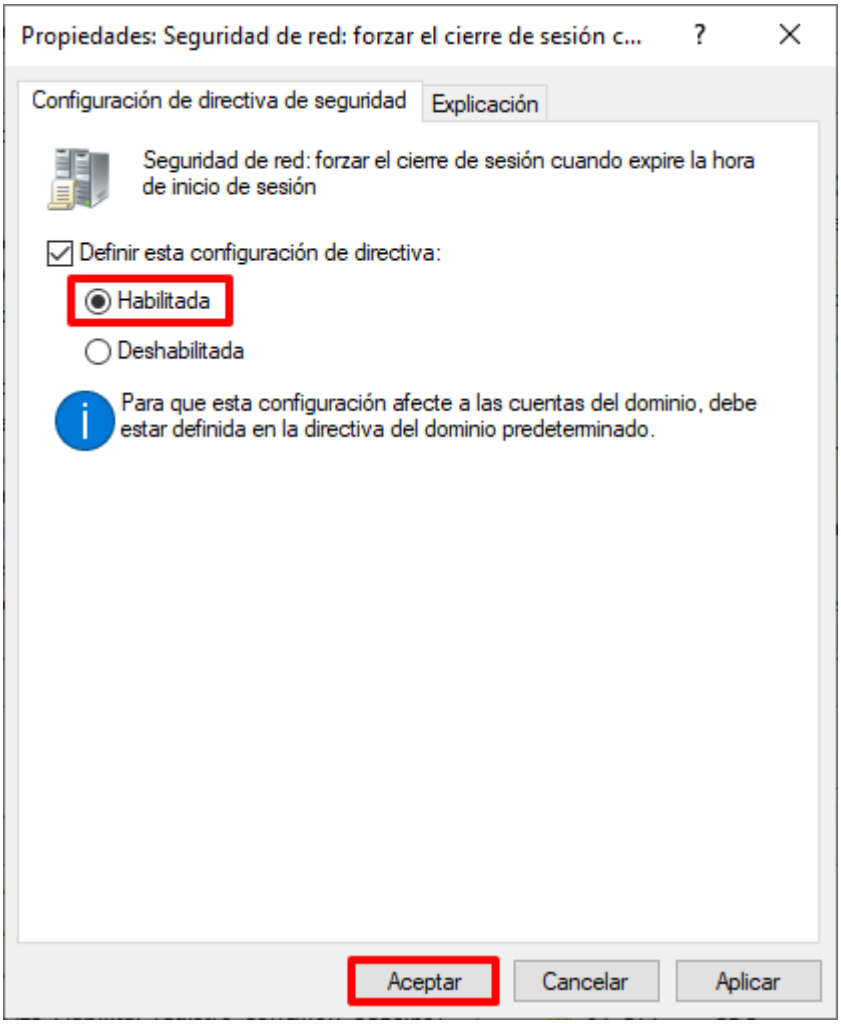
ANEXO A.2.1. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

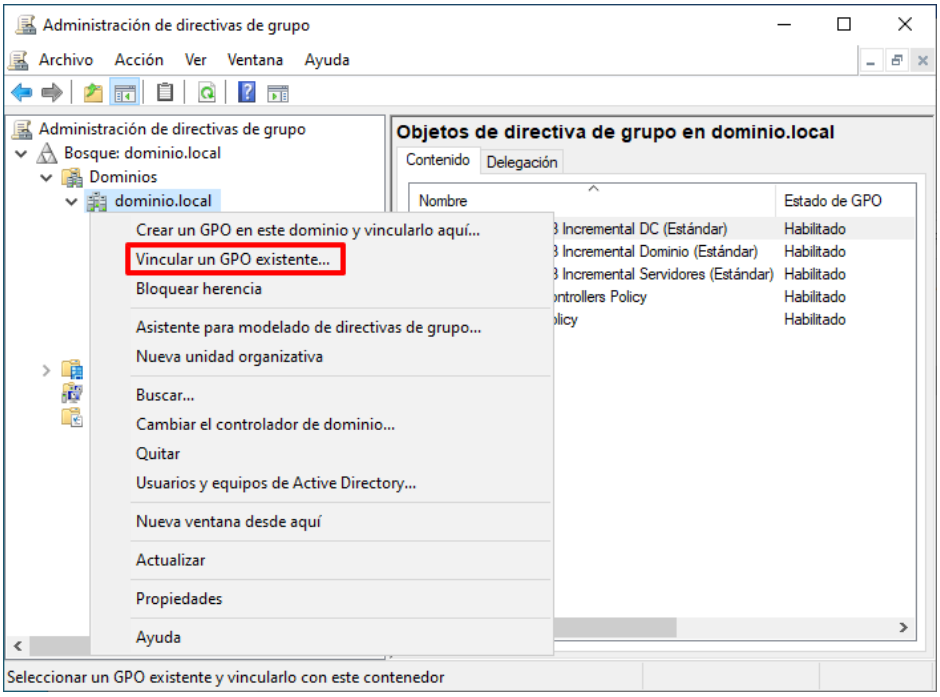
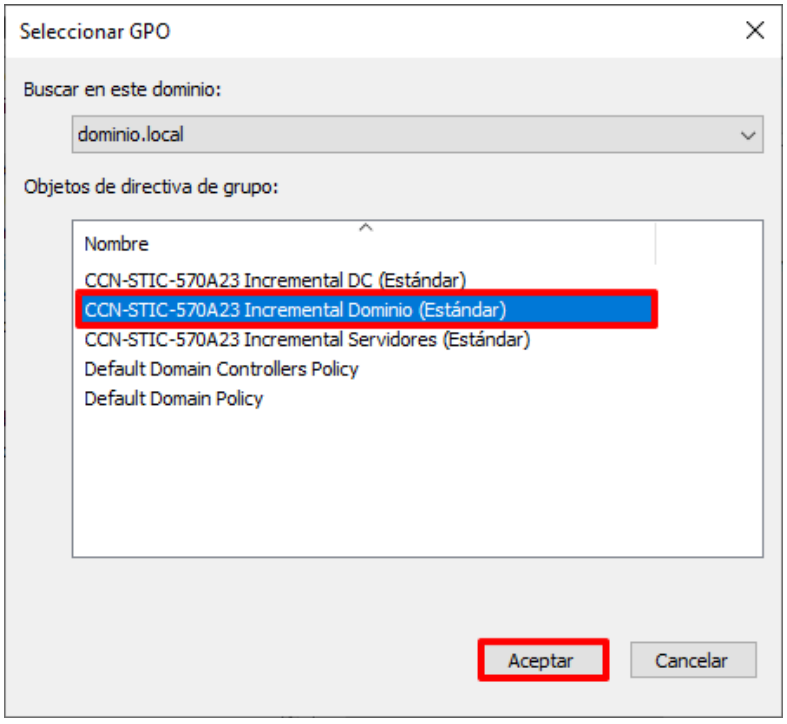
A continuación, se definen los pasos a seguir para la adecuada aplicación de las políticas generadas en el punto anterior para aplicar la configuración de seguridad sobre el dominio y sobre los objetos de tipo Domain Controller. Solo es necesario realizar este procedimiento una (1) vez.

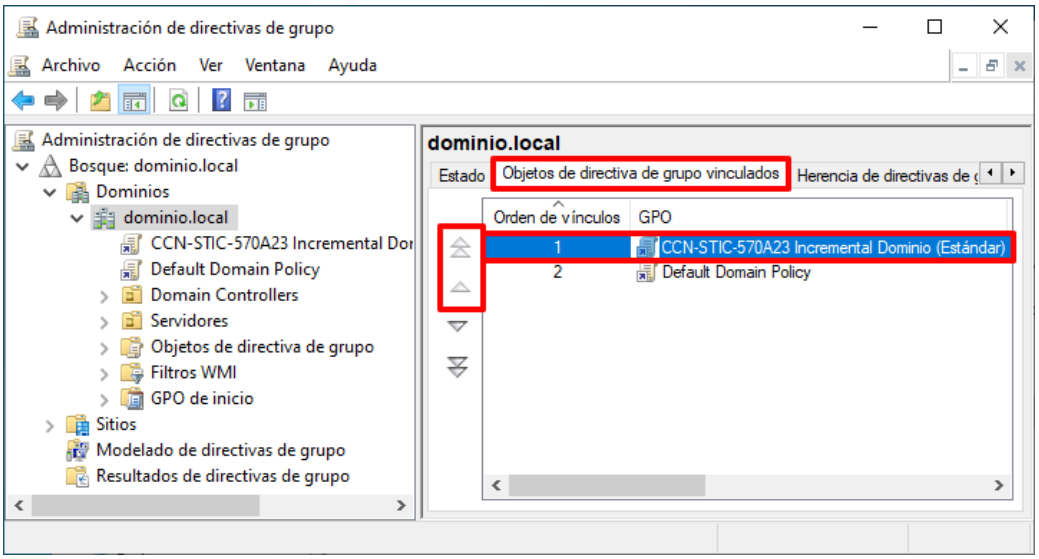
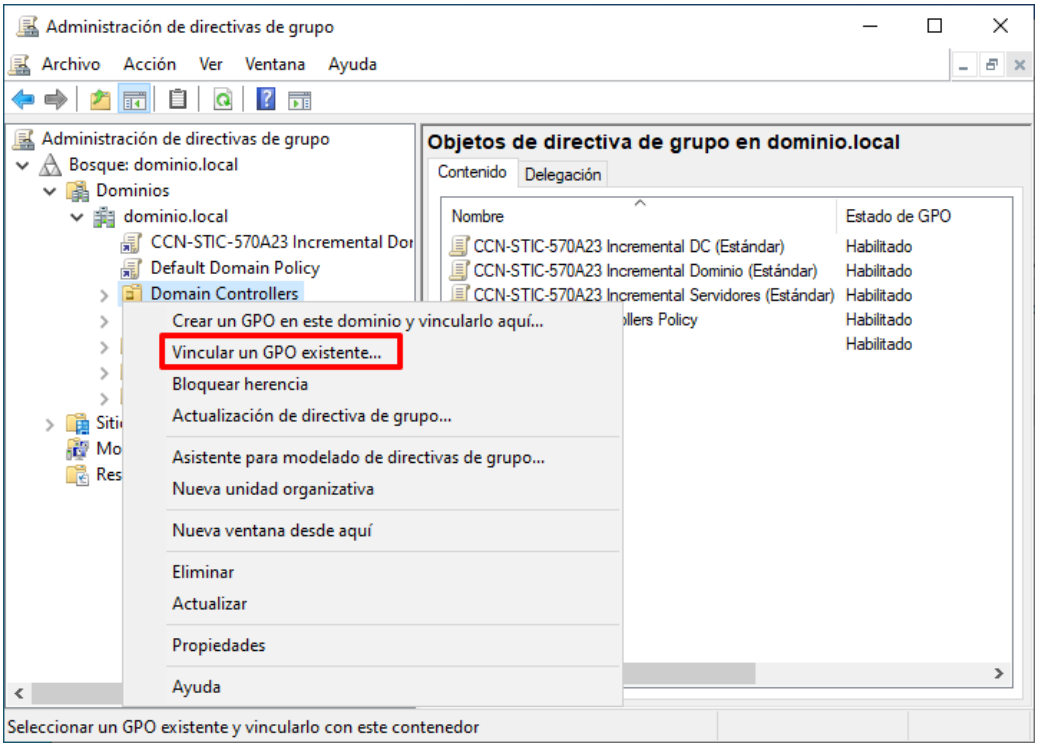
Paso	Descripción
59.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
60.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.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

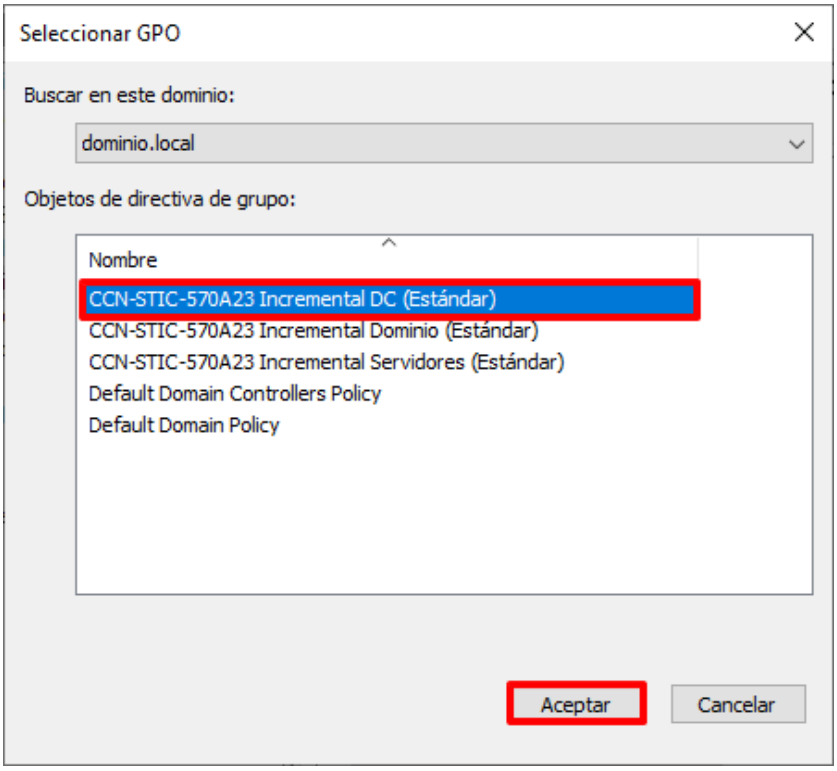
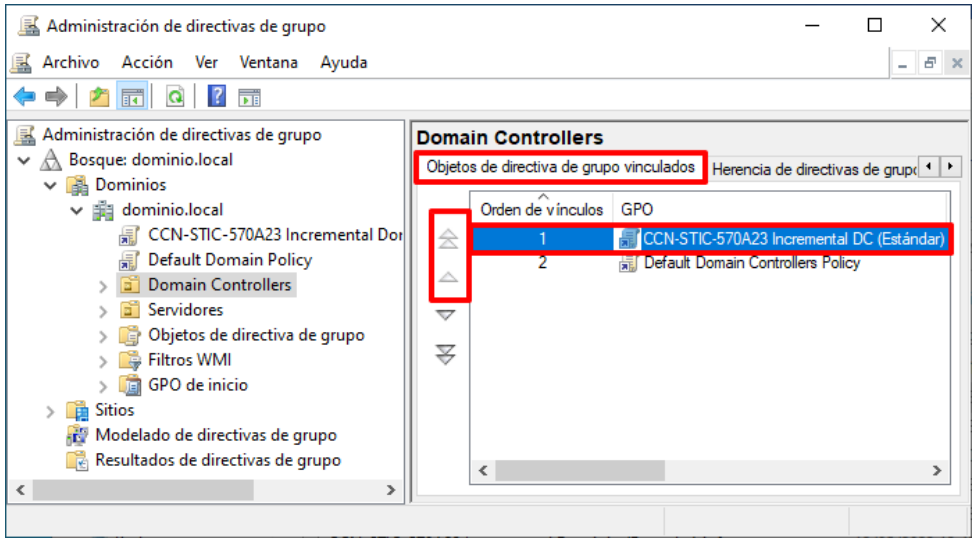
Paso	Descripción
61.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
62.	Una vez abierta la consola, seleccione: **“Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. Hasta que se indique lo contrario,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

Paso	Descripción
63.	Seleccione en el contenedor “Objetos de directiva de grupo” el objeto GPO creado por defecto “Default Domain Policy” con el botón derecho y elija la opción “Editar” en el menú contextual que aparecerá. 
64.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva Default Domain Policy → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**. Identifique en el panel derecho la directiva “**Seguridad de red: Forzar el cierre de sesión cuando expire la hora de inicio de sesión**” y haga doble clic sobre ella. 

Paso	Descripción
65.	En la nueva ventana emergente, establezca la configuración de la directiva en “Habilitada” y pulse sobre el botón “Aceptar”. 
66.	Cierre el editor de directivas de grupo.

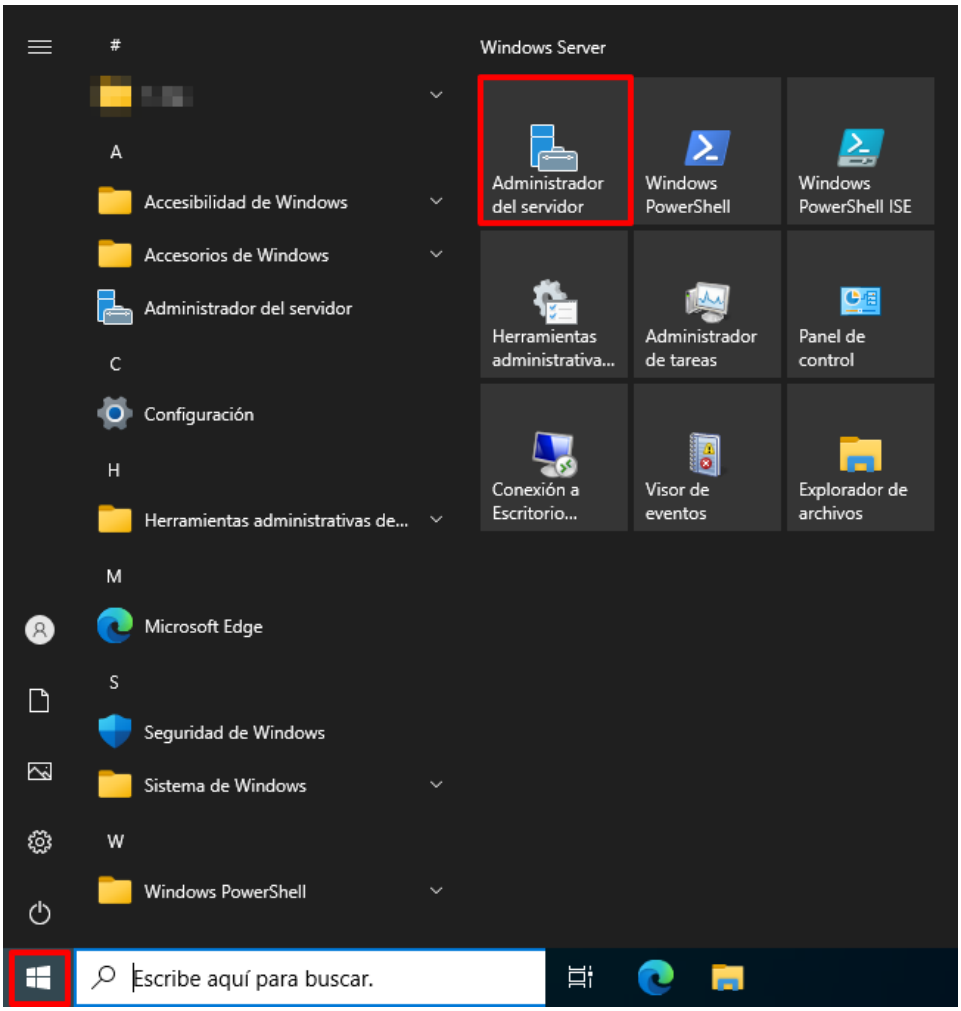
Paso	Descripción
67.	A continuación, haga clic derecho sobre el contenedor del dominio y seleccione la opción del menú contextual “Vincular un GPO existente…”. 
68.	A continuación, seleccione el objeto GPO “CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO])” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

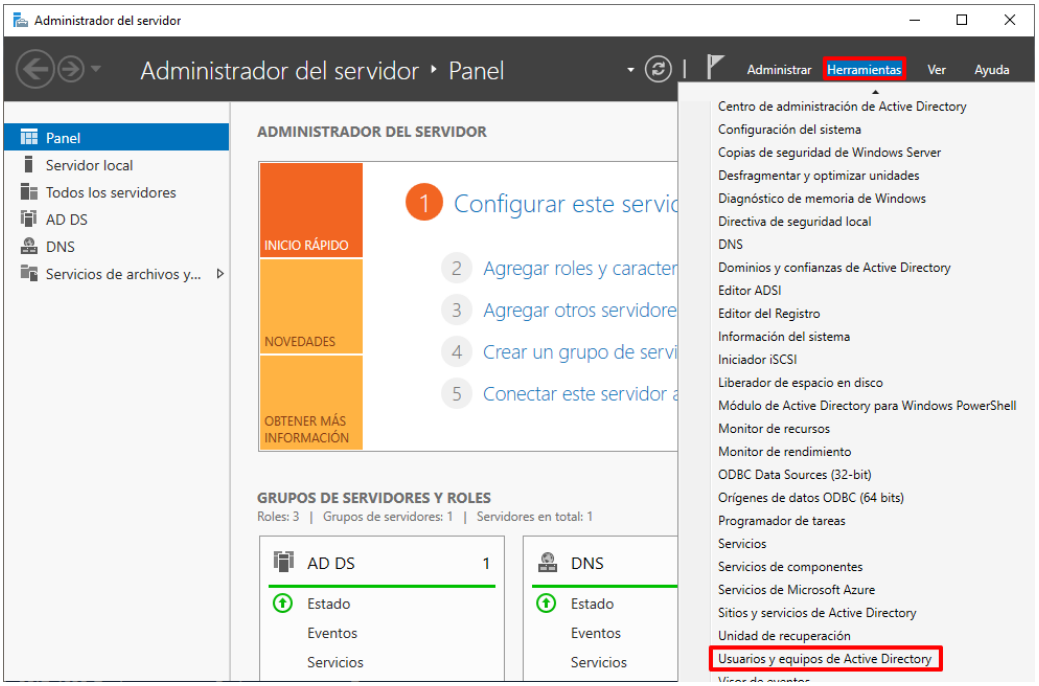
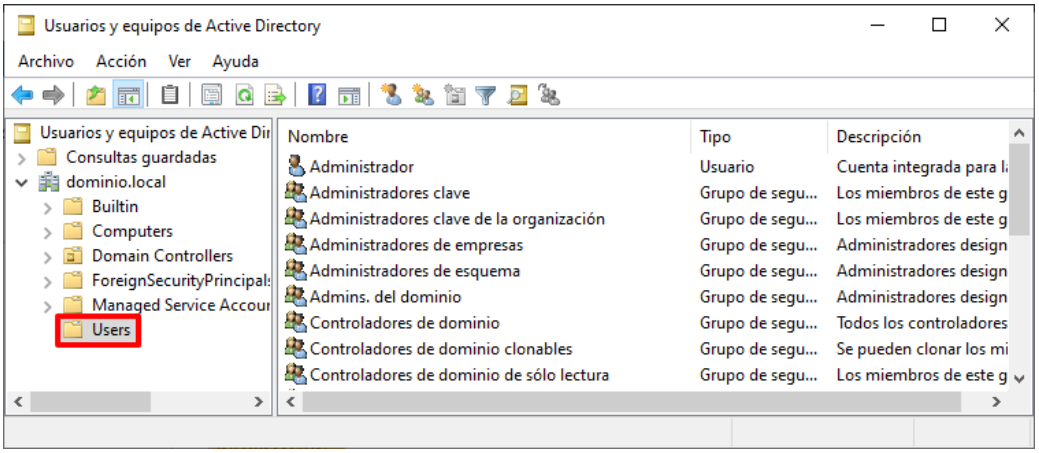
Paso	Descripción
69.	Seleccione el contenedor sobre el que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 
70.	A continuación, haga clic derecho sobre el contenedor "Domain Controllers" y seleccione la opción del menú contextual "Vincular un GPO existente…". 

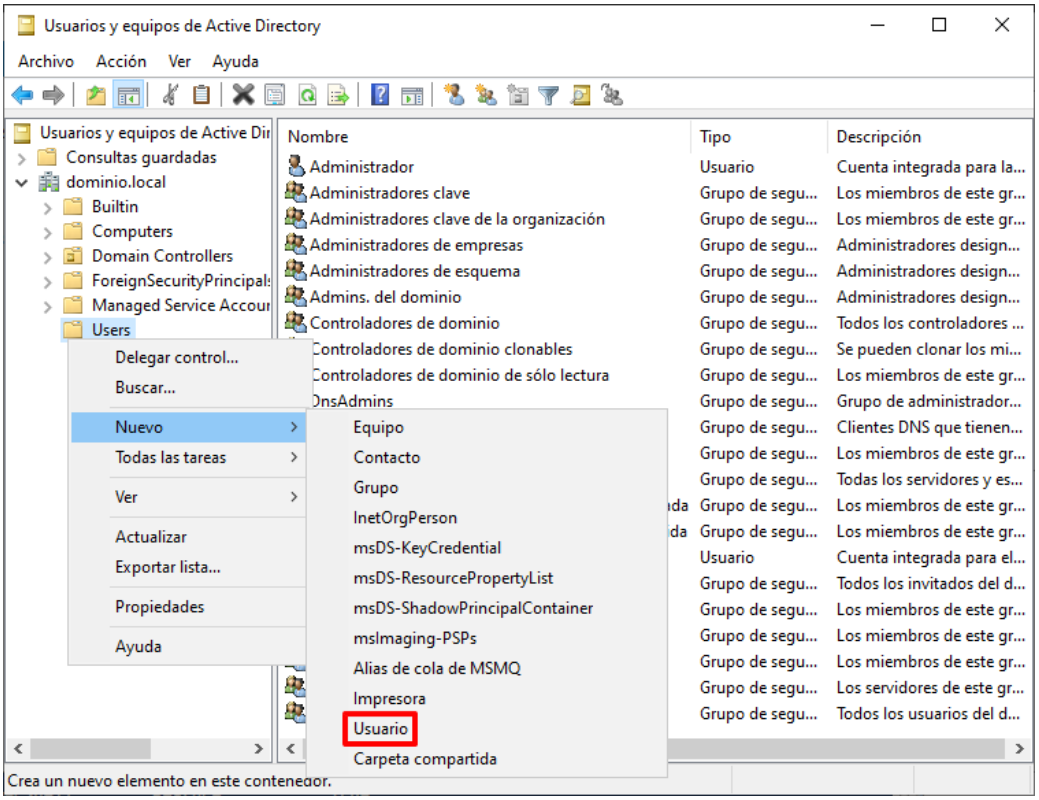
Paso	Descripción
71.	Seleccione el objeto GPO "CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])" y pulse "Aceptar".  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
72.	Seleccione el contenedor sobre el que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

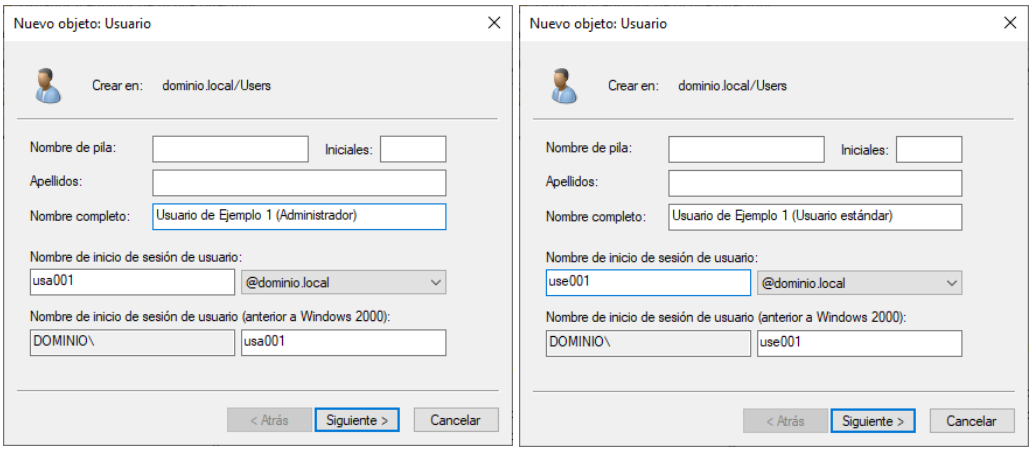
ANEXO A.2.2. IDENTIFICACIÓN

En el presente apartado se definirán las directrices para realizar una correcta gestión de identidades dentro de un entorno de Active Directory. Esta actividad deberá llevarse a cabo de forma principal sobre uno de los Domain Controllers pero extensible a los servidores miembro del dominio cuando se haga uso de cuentas locales. En el apartado correspondiente se describirán y pondrán ejemplos de estas labores.

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

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

Paso	Descripción
77.	Pulse con el botón derecho sobre el contenedor “Users” o bien sobre un espacio en blanco del panel derecho y seleccione “Nuevo → Usuario”. 

Paso	Descripción
78.	Sobre la nueva ventana emergente “Nuevo objeto: Usuario” deberá completar los campos solicitados teniendo en consideración los siguientes aspectos: – Nombre de inicio de sesión de usuario: Este campo será el utilizado por el usuario para iniciar sesión en los equipos pertenecientes al dominio. Se debe tener en consideración que dicho campo deberá **utilizar un identificador único para cada usuario**. Además de lo anterior, dicho **identificador deberá identificar los roles o funciones** de dicho usuario, pero sin revelar sus privilegios y/o permisos. – Varios usuarios para diferentes roles: Cuando la misma persona aúne **dos (2) o más funciones** dentro del mismo sistema deberá disponer de **dos (2) o más usuarios diferenciados** los cuales dispondrán de privilegios y permisos diferentes. – Nombre Completo: Singularizar a la persona asociada al identificador de nombre de inicio de sesión, así como sus responsabilidades en el sistema, será la función de este campo. Se considera optimo la utilización de información única de la persona, como su nombre y apellidos, DNI o similares. **Nota:** Es posible el uso del resto de campos, siempre que se cumplan las condiciones expresadas anteriormente. A continuación, se muestra un par de ejemplo sobre dos tipos diferentes de usuarios (con diferentes roles) asociados a la misma persona. En este caso se trata de un usuario administrador y un usuario sin privilegios. 

Paso	Descripción
79.	En este paso a paso se hace uso de una **nomenclatura de usuarios de ejemplo**, la cual **deberá ser adaptada a cada organización en función de las necesidades**. En este ejemplo se ha seguido la siguiente fórmula: – Usa001 → us = Usuario | a = Administrador | 001 = Número correlativo – Use001 → us = Usuario | e = Estándar | 001 = Número correlativo
80.	Esta acción, no solo deberá ser llevada a cabo para aquellos usuarios nuevos, sino también para los usuarios ya generados pero que no cumplan con las necesidades descritas anteriormente.

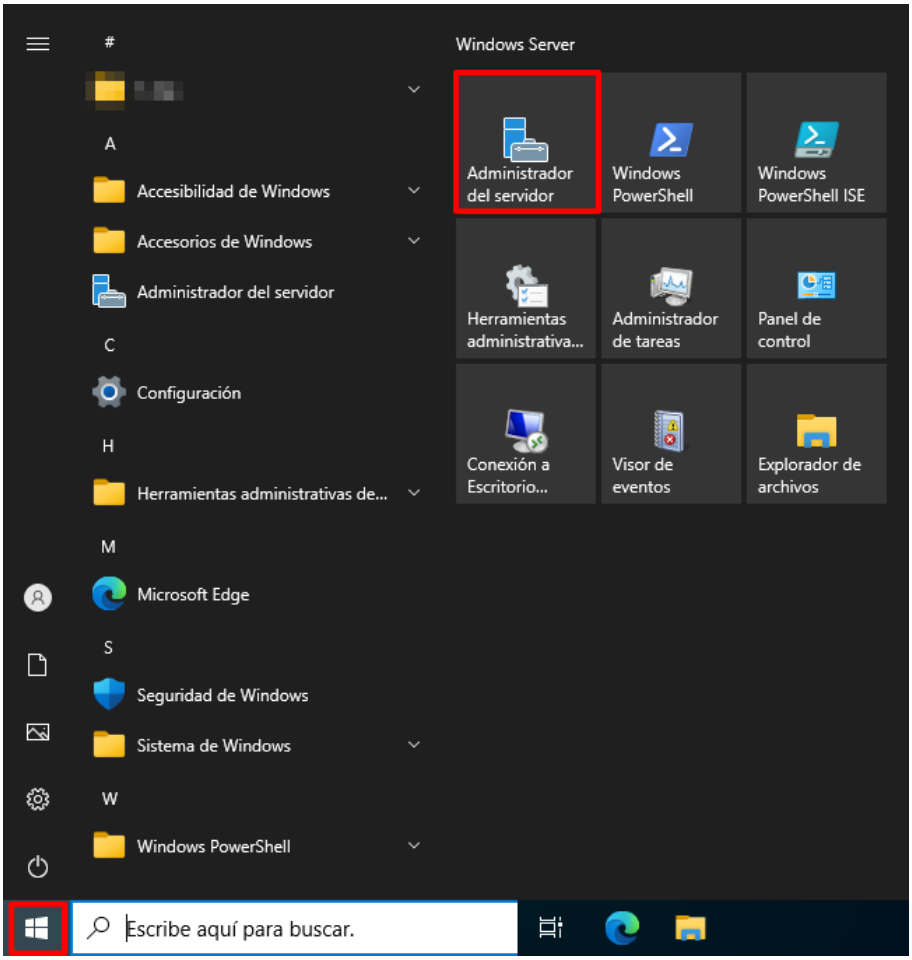
ANEXO A.2.3. SEGREGACIÓN DE FUNCIONES Y TAREAS

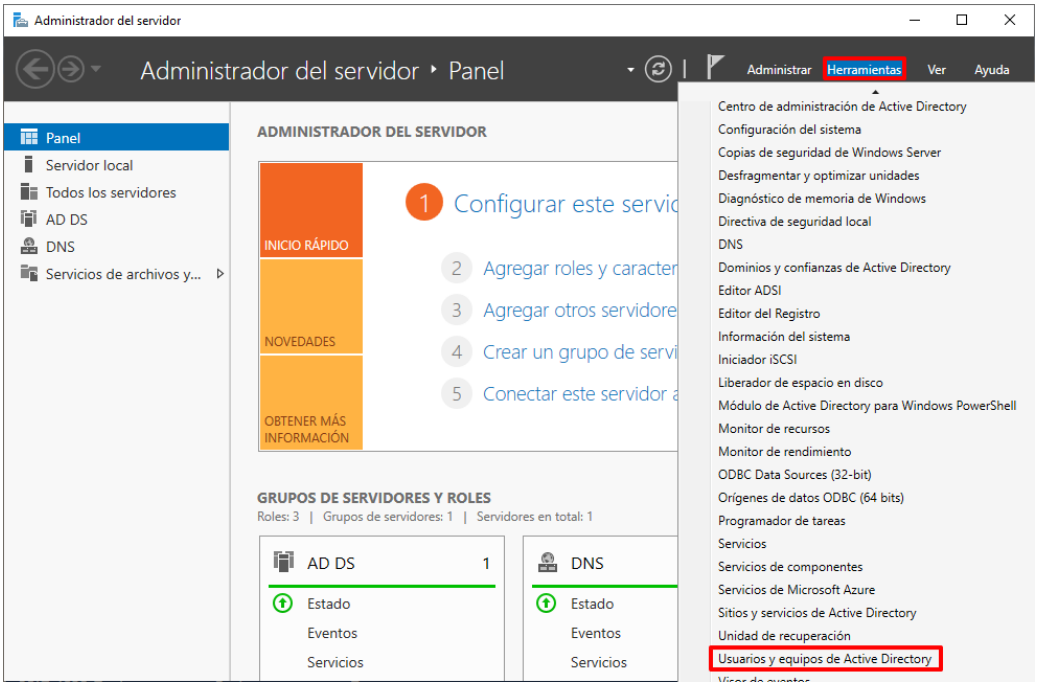
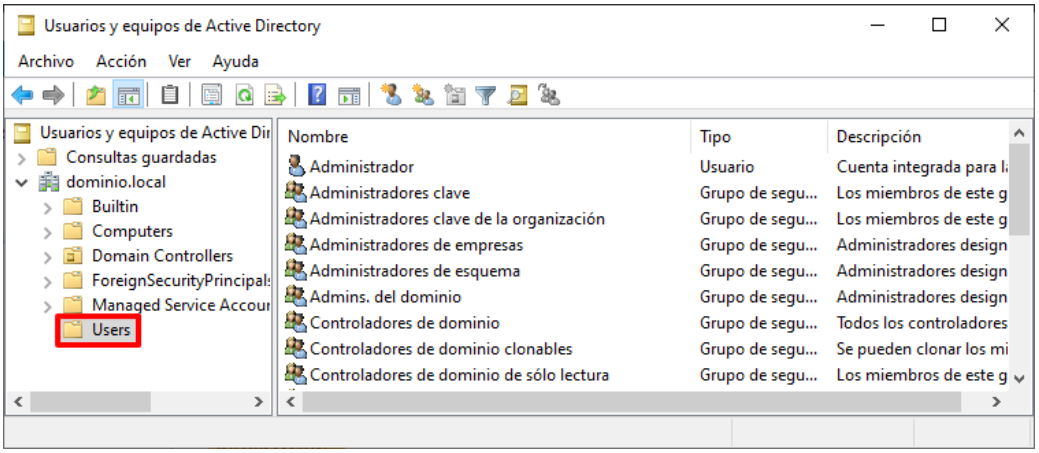
A continuación, se definirán las acciones para disponer de una adecuada segregación de funciones dentro de los sistemas operativos Windows Server y aplicable sobre los equipos de tipo Domain Controller.

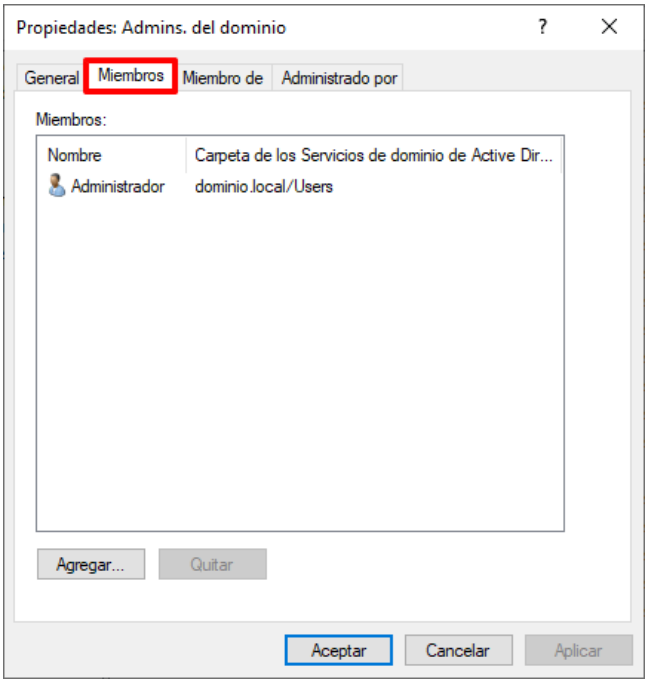
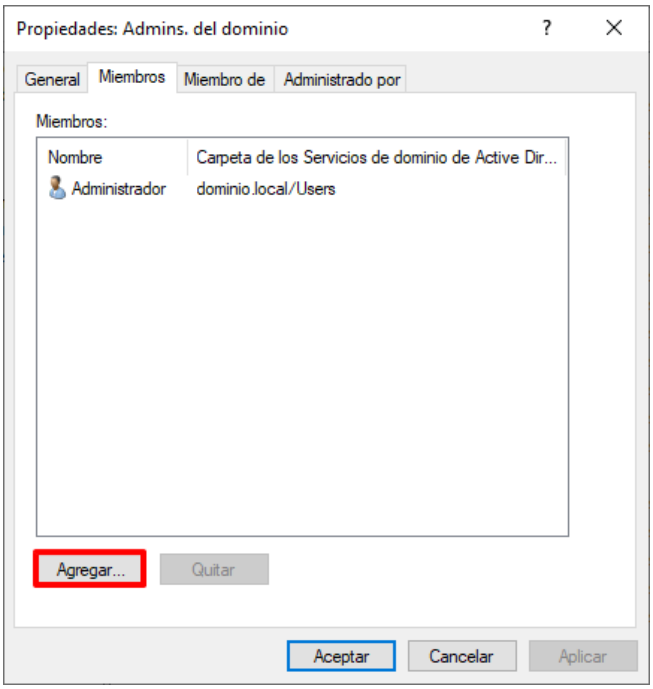
En primer lugar, se va a evaluar que al menos se disponen de dos (2) usuarios con suficientes privilegios de modo que toda la responsabilidad y capacidad de gestión no quede aunada en una persona y no sea posible abusar de dichos derechos.

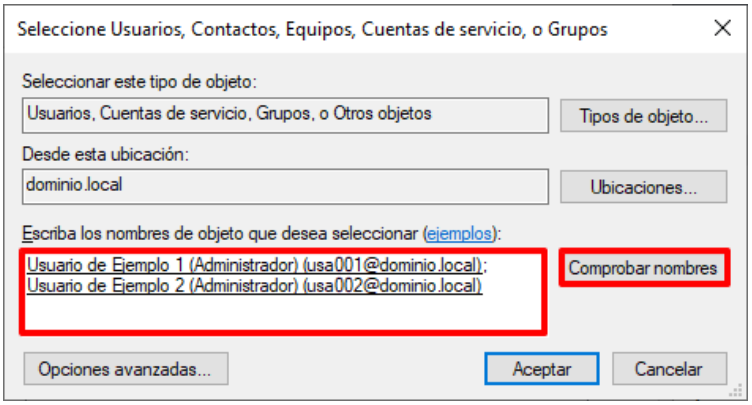
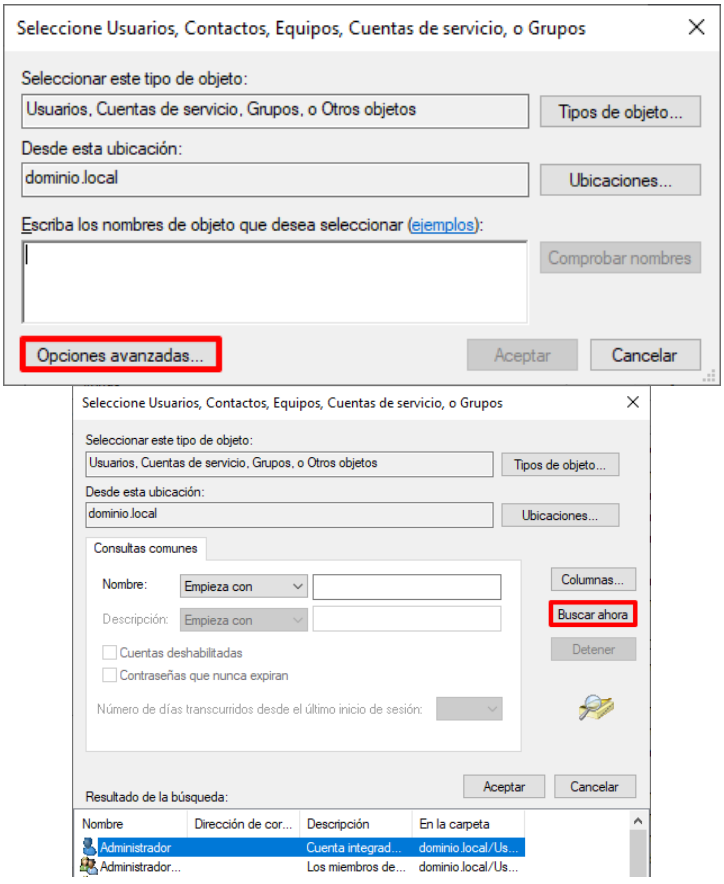
Nota: Los pasos descritos a continuación son un ejemplo de cómo segregar ciertas tareas, sin rechazar o validar la gestión por medio de consolas o herramientas adicionales que una organización pudiera disponer. Cada organización deberá adaptar los pasos descritos en el presente apartado en función de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

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

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

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

Paso	Descripción
85.	Haga doble clic sobre el grupo “Admins. del dominio” y sitúese a continuación sobre la pestaña “Miembros”. 
86.	Evalúe que **al menos existen dos (2) usuarios** unidos a este grupo y de igual modo evalúe que no existe un exceso de usuario o grupos unidos.
87.	En este ejemplo se va a añadir un par de usuarios adicionales al usuario integrado “Administrador”. Para ello, pulse sobre el botón “Agregar…” de la ventana “Propiedades: Admins. del dominio”. 

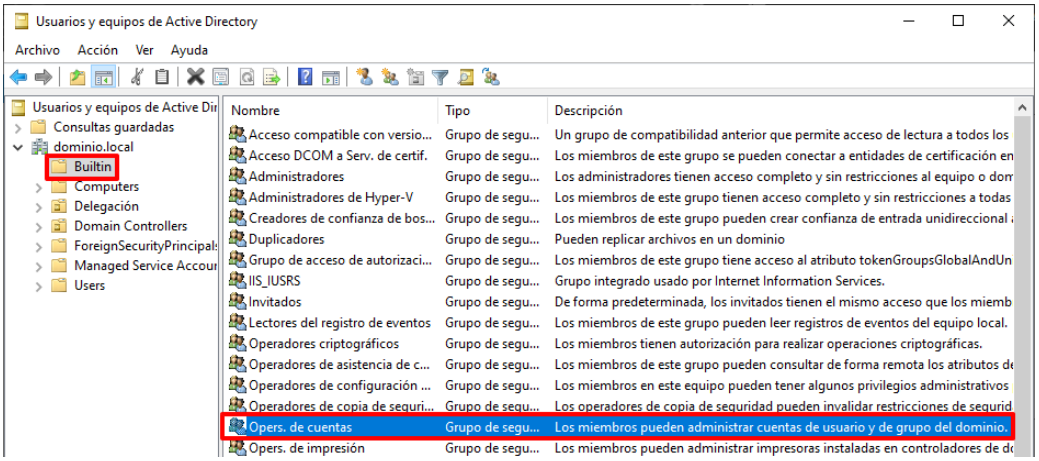
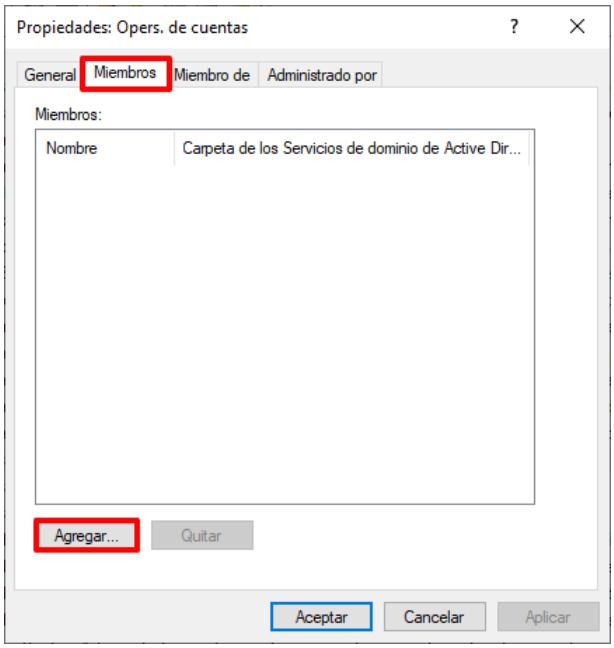
Paso	Descripción
88.	En la nueva ventana emergente introduzca el nombre de aquellas cuentas de usuario que desee que posean privilegios de administración en el dominio. Puede hacer uso del botón “Comprobar nombres” para identificar la cuenta de forma exacta y puede incluir varias cuentas separada por punto y coma (;).  **Nota:** En este ejemplo se hace uso de los usuarios: **usa001** y **usa002**. Deberá evaluar que usuarios de su organización deben pertenecer a este grupo.
89.	Si desconoce las cuentas de usuario puede hacer uso del botón “Opciones avanzadas…” y en la nueva ventana “Buscar ahora” para listar todos los usuarios. Pulse “Aceptar” cuando haya finalizado de incluir a los usuarios. 

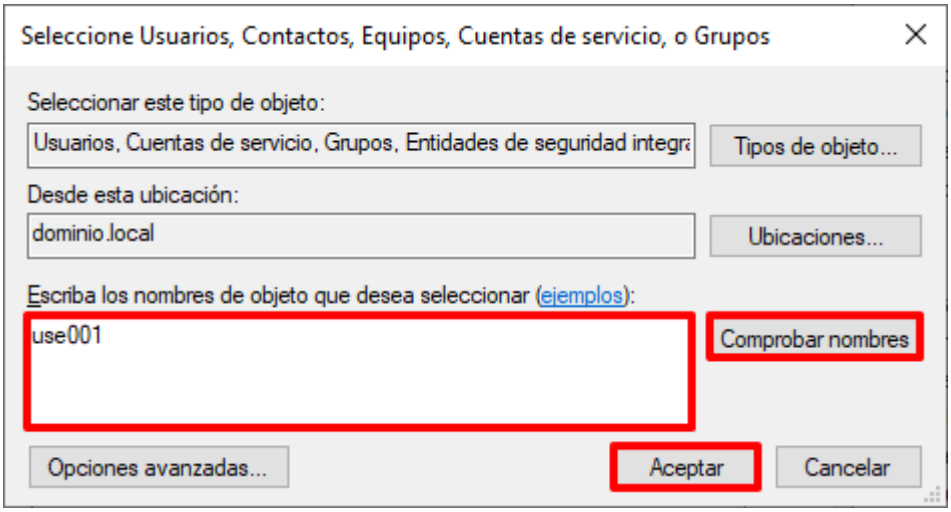
Realizada esta labor, a continuación, se ofrecerán ejemplos de cómo delegar tareas sobre usuarios o grupos de usuarios de forma que estos no requieran privilegios de administración en el dominio. Concretamente se delegarán privilegios para las siguientes labores:

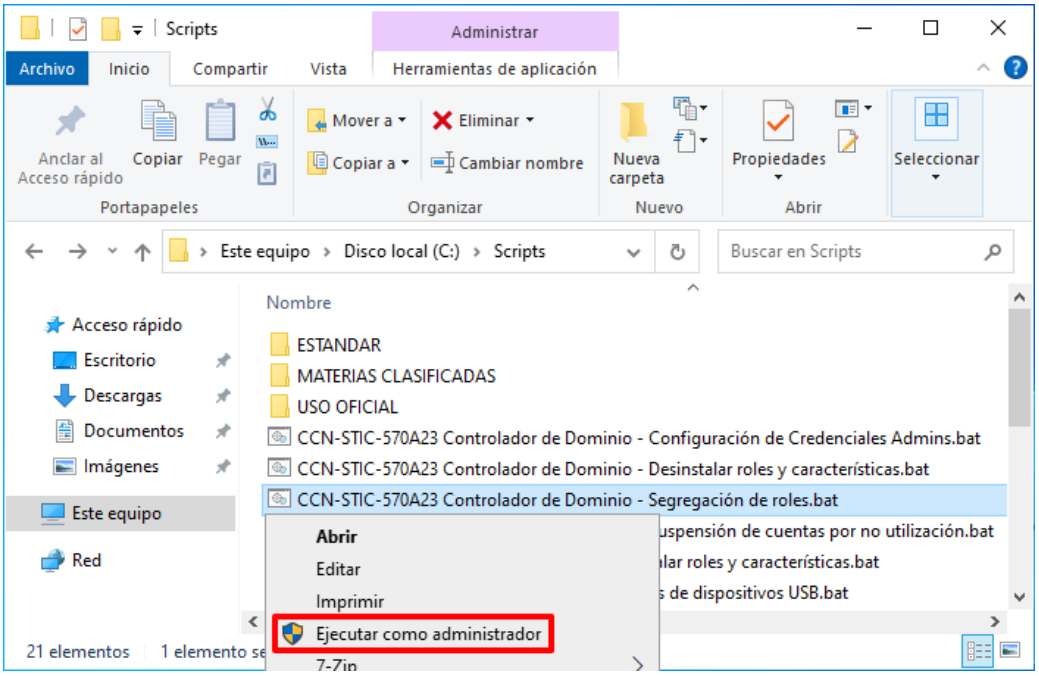
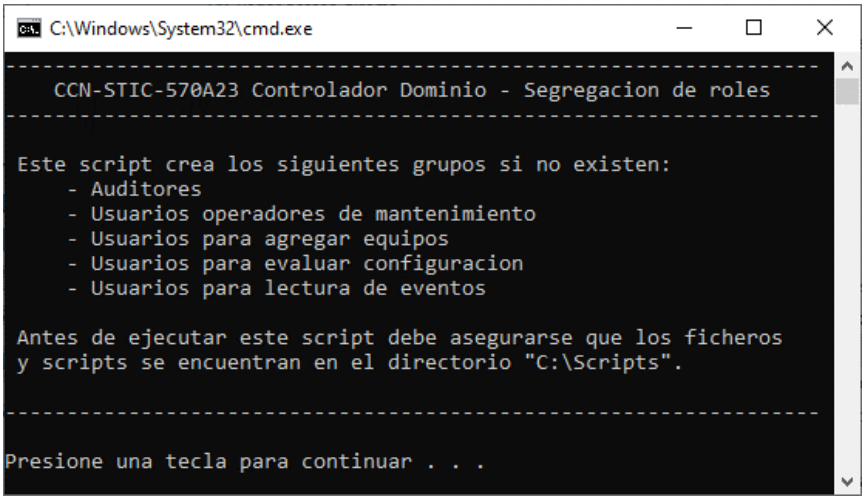
a) Crear usuarios del dominio y restablecer sus credenciales.

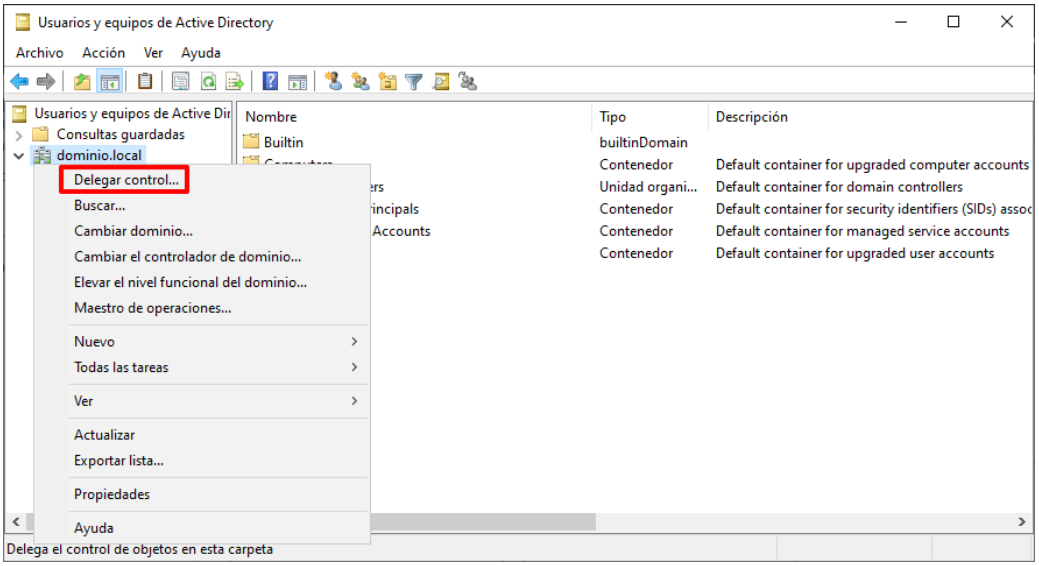
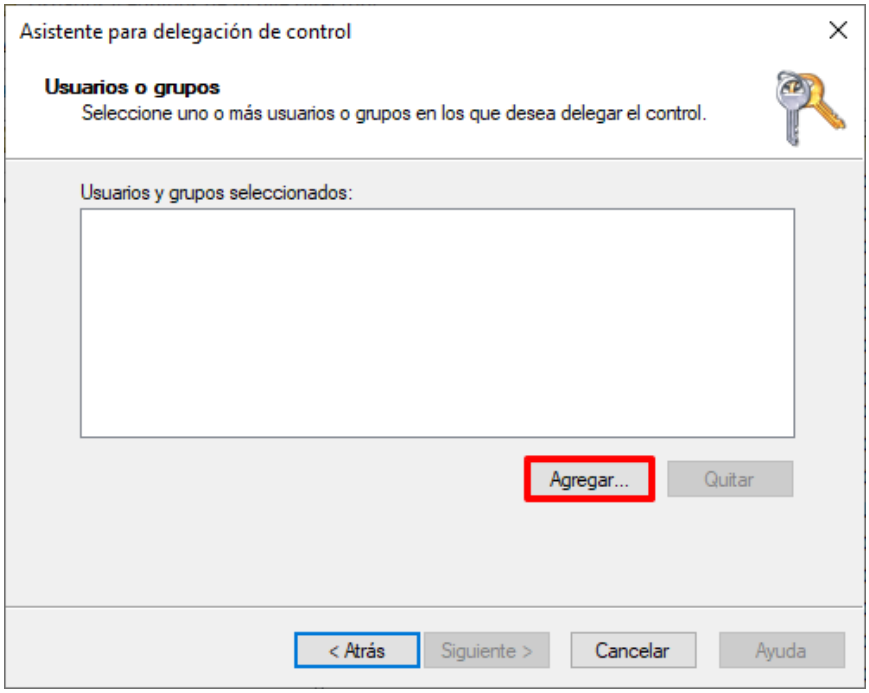
b) Agregar equipos al dominio.

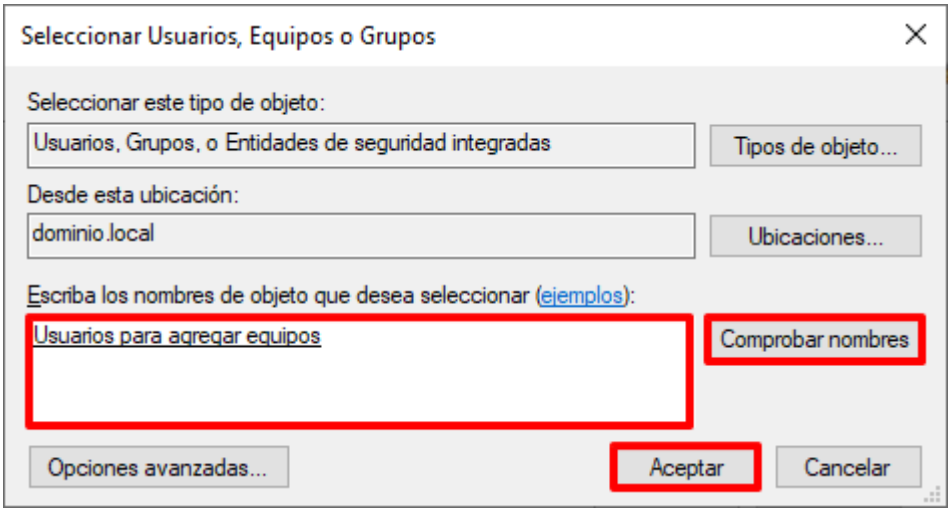
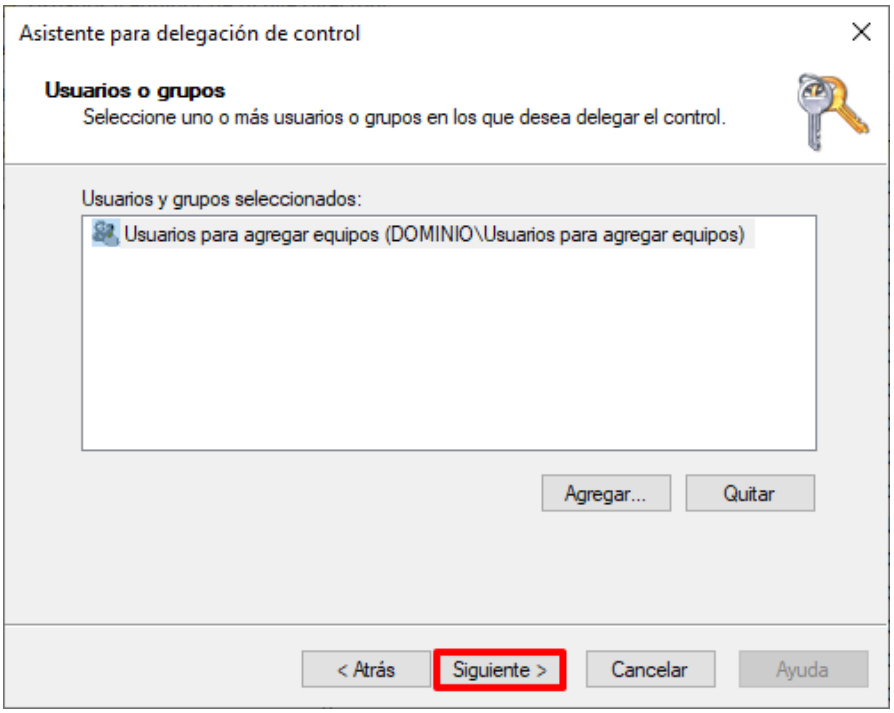
Nota: Existen diversas posibilidades para realizar esta labor, siendo la mostrada a continuación una de ellas.

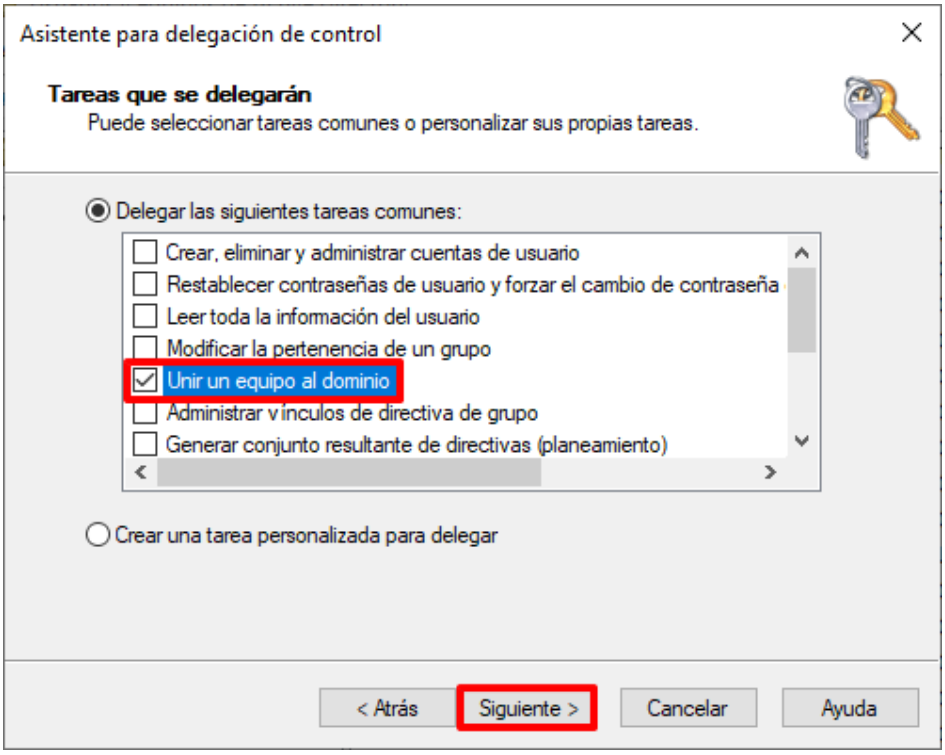
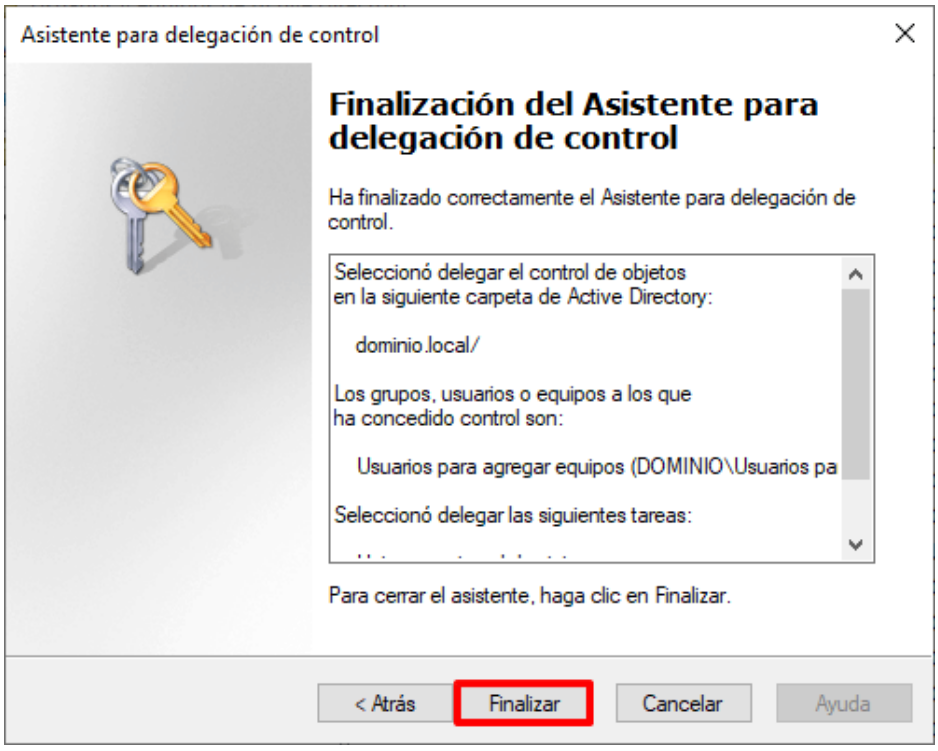
Paso	Descripción
90.	Sobre la consola "Usuarios y equipos de Active Directory", seleccione y despliegue el nodo "<nombre de su dominio> → Builtin". Identifique el grupo definido por defecto "Opers. de cuentas" y haga doble clic sobre él. 
91.	Seleccione la pestaña "Miembros" y pulse sobre el botón "Agregar…". 

Paso	Descripción
92.	En la nueva ventana emergente, incluya los usuarios o grupos los cuales desea agregar al grupo separados por punto y coma (;). Haga uso del botón "Comprobar nombres" para completar la información del usuario y pulse "Aceptar".  **Nota:** En este ejemplo se va a hacer uso del usuario estándar generado en el punto anterior dedicado a identificación, "use001" (Usuario de Ejemplo 1 (Usuario estándar)).
93.	Pulse "Aceptar" sobre la ventana de propiedades del grupo para finalizar la configuración.
94.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo el inicio de sesión sobre los equipos de tipo Domain Controller y acceso a las consolas de administración, aunque solo con acceso de escritura sobre la herramienta administrativa "Usuarios y equipos de Active Directory". **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.
95.	Para la siguiente labor, será necesario la creación de grupos dedicados de modo que la gestión de identidades quede simplificada en la pertenencia a grupos.

Paso	Descripción
96.	Si no desea realizar una creación de grupos personalizada o no dispone de estos grupos, diríjase al directorio “C:\Scripts” y ejecute el script “CCN-STIC-570A23 Controlador de Dominio – Segregación de roles.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
97.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsar cualquier botón para finalizar la ejecución del script. 
98.	Tras la ejecución del script, entre los grupos generados se puede encontrar el siguiente grupo: – Usuarios para agregar equipos.

Paso	Descripción
99.	De forma similar a lo realizado anteriormente, ejecute los pasos “90” a “93” para agregar a los usuarios necesarios al grupo recién creado que vayan a disponer de esta capacidad.
100.	A continuación, en la misma consola de “Usuarios y equipos de Active Directory” abierta en pasos anteriores, seleccione su dominio (<nombre de su dominio>) con el botón derecho y pulse sobre “Delegar control…”. 
101.	En la ventana “Asistente para delegación de control” pulse sobre el botón “Siguiente >”.
102.	En la siguiente ventana del asistente haga clic sobre el botón “Agregar…”. 

Paso	Descripción
103.	Escriba el nombre del grupo sobre el que desea delegar esta tarea. En este ejemplo será el generado a través del script ejecutado en pasos anteriores ("Usuarios para agregar equipos"). Pulse sobre "Comprobar nombres" para completar el nombre y pulse "Aceptar". 
104.	A continuación, pulse sobre "Siguiente >". 

Paso	Descripción
105.	En la ventana “Tareas que se delegarán” seleccione “Unir equipo al dominio”. Pulse “Siguiente >” para continuar. 
106.	Pulse “Finalizar” para acabar con el proceso. 

Paso	Descripción
107.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo unir objetos de tipo equipo al dominio sin disponer de privilegios de administración sobre este. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.

ANEXO A.2.3.1. SEGREGACIÓN DE FUNCIONES Y TAREAS (USO OFICIAL – MATERIAS CLASIFICADAS)

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

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

a) Creación de configuraciones.

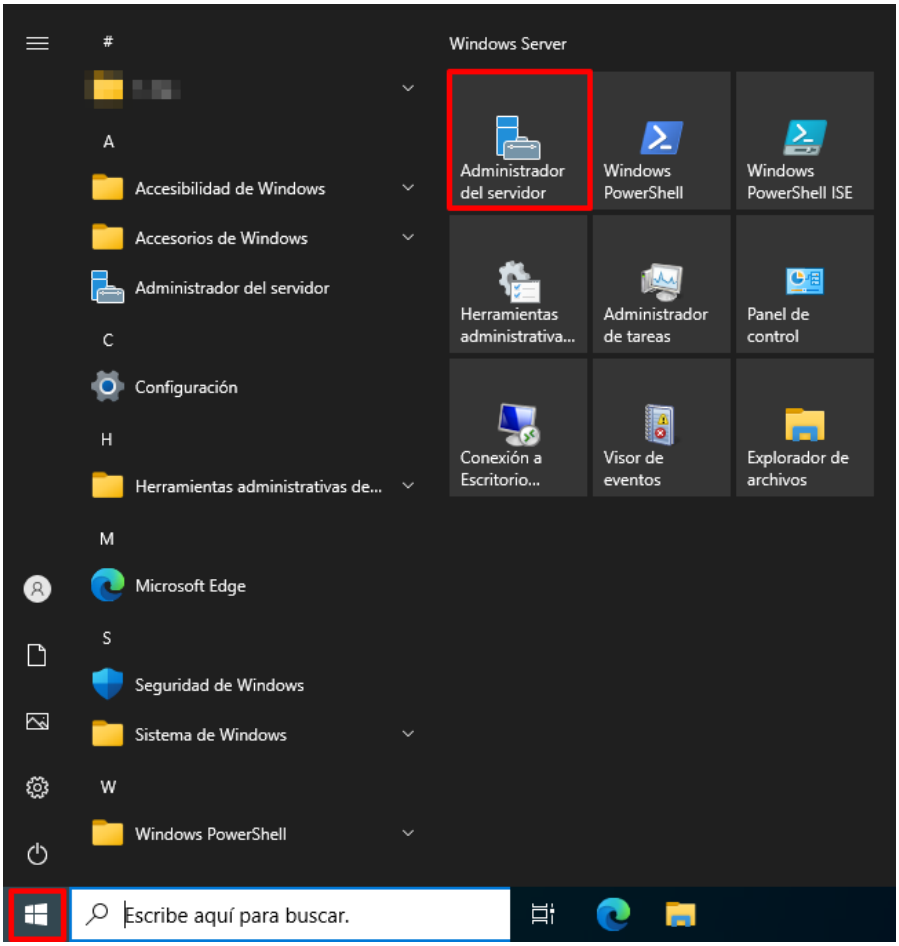
b) Evaluación de configuraciones resultantes.

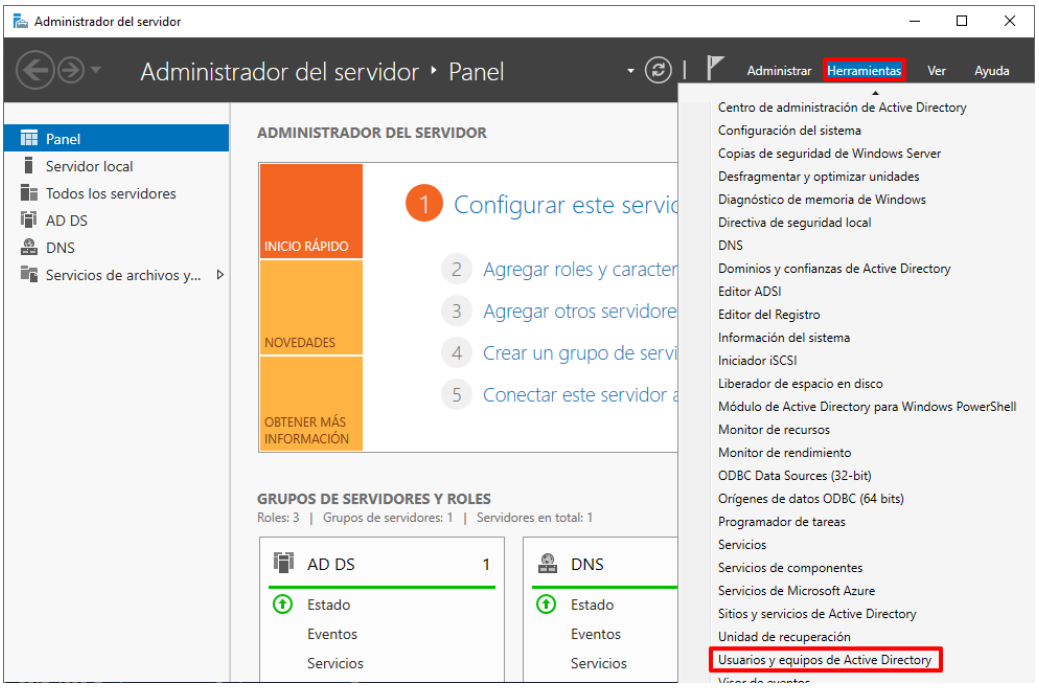
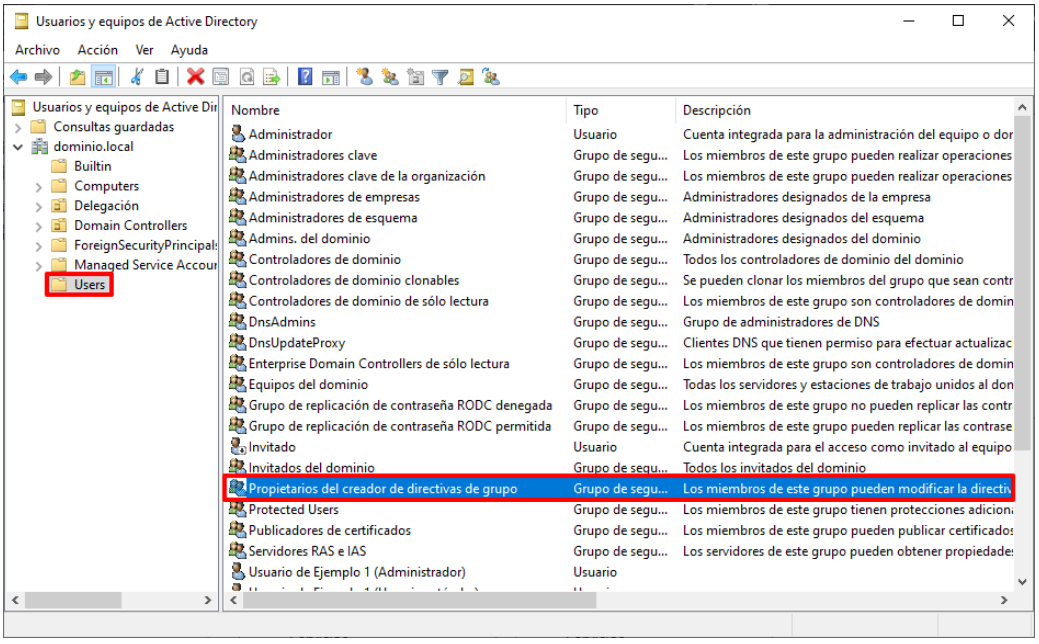
c) Revisión del registro de eventos.

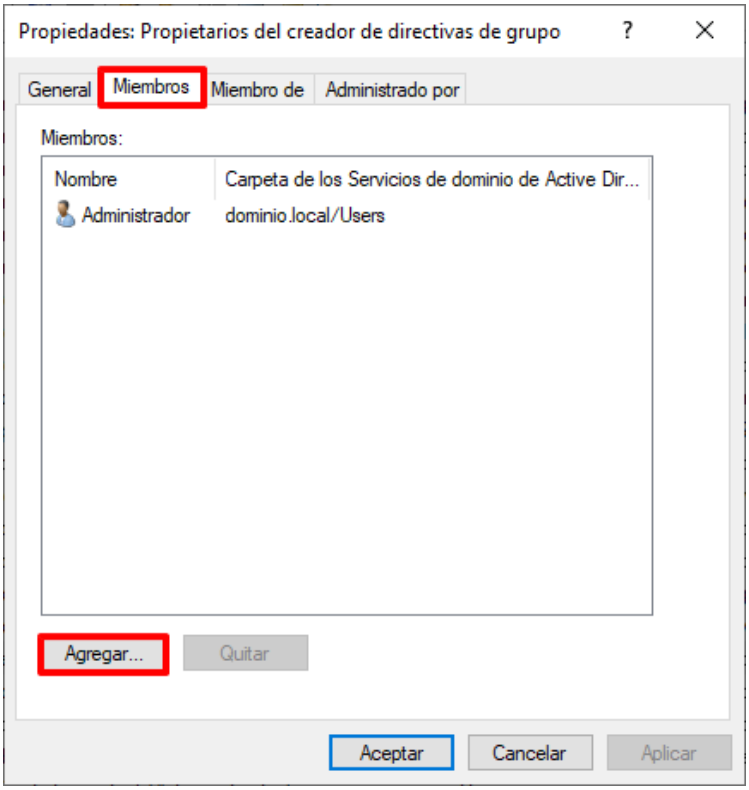
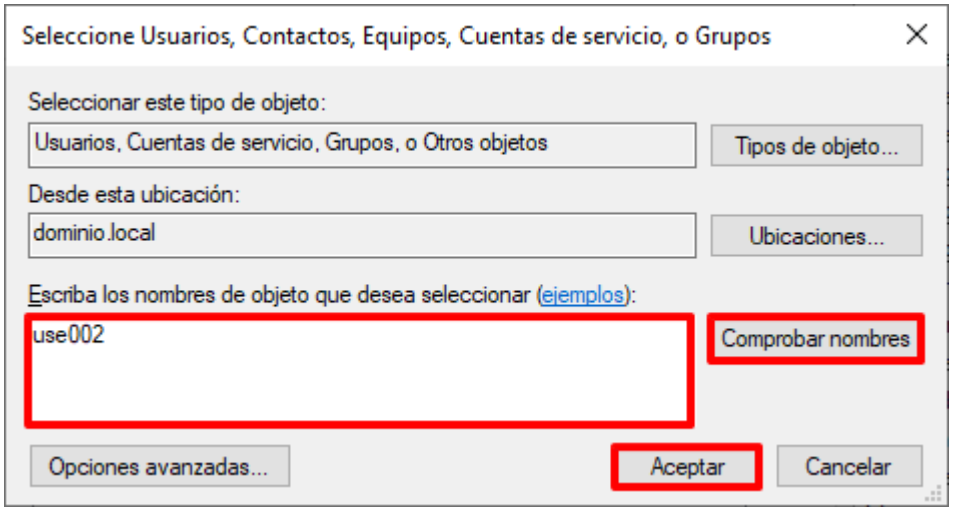
d) Operación de mantenimiento.

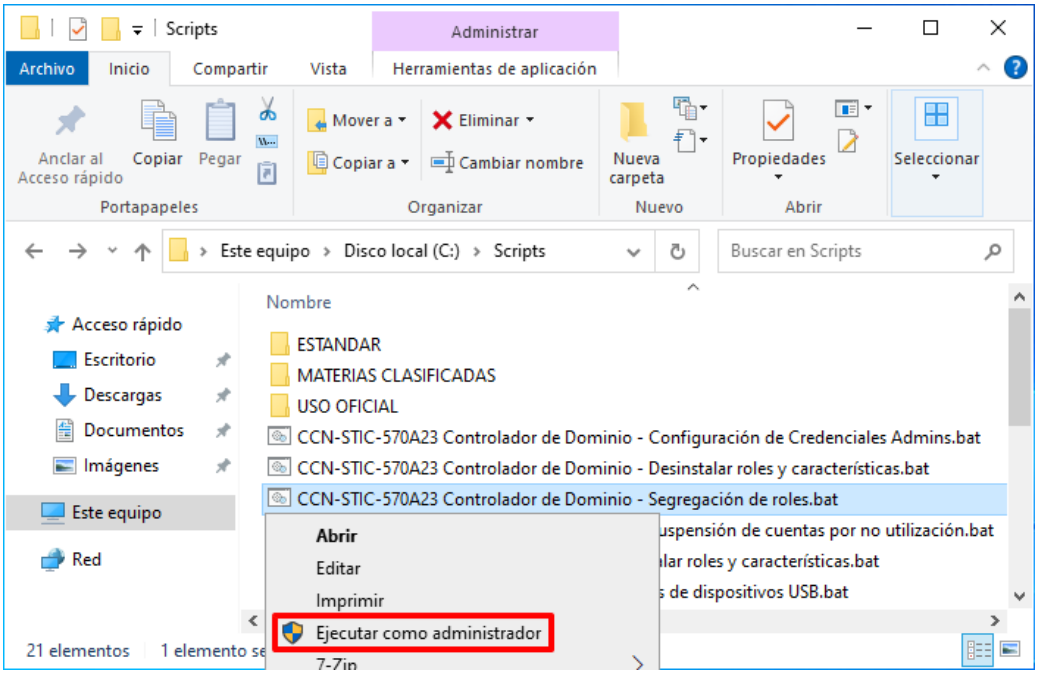
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

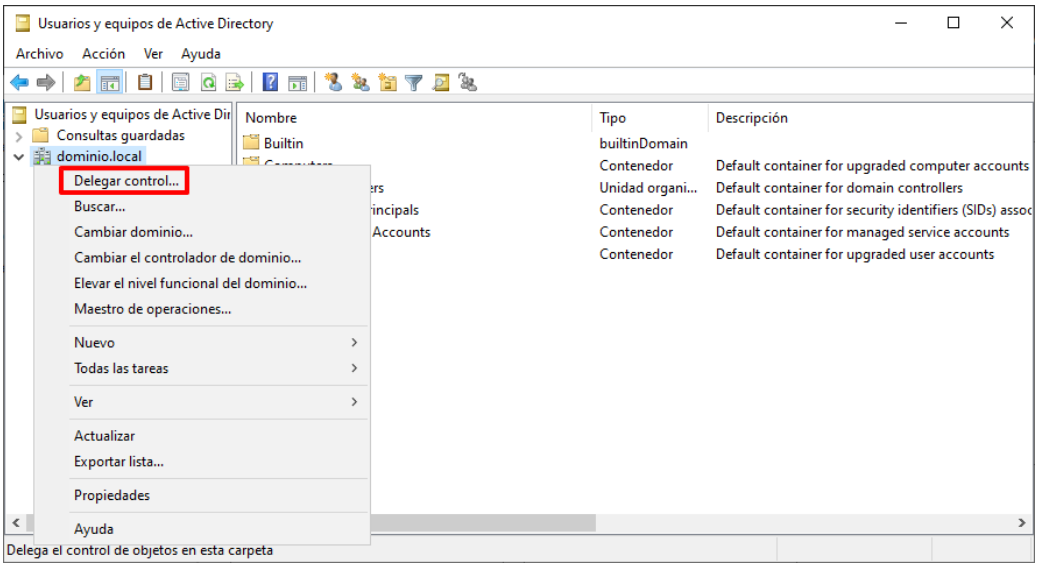
Paso	Descripción
108.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

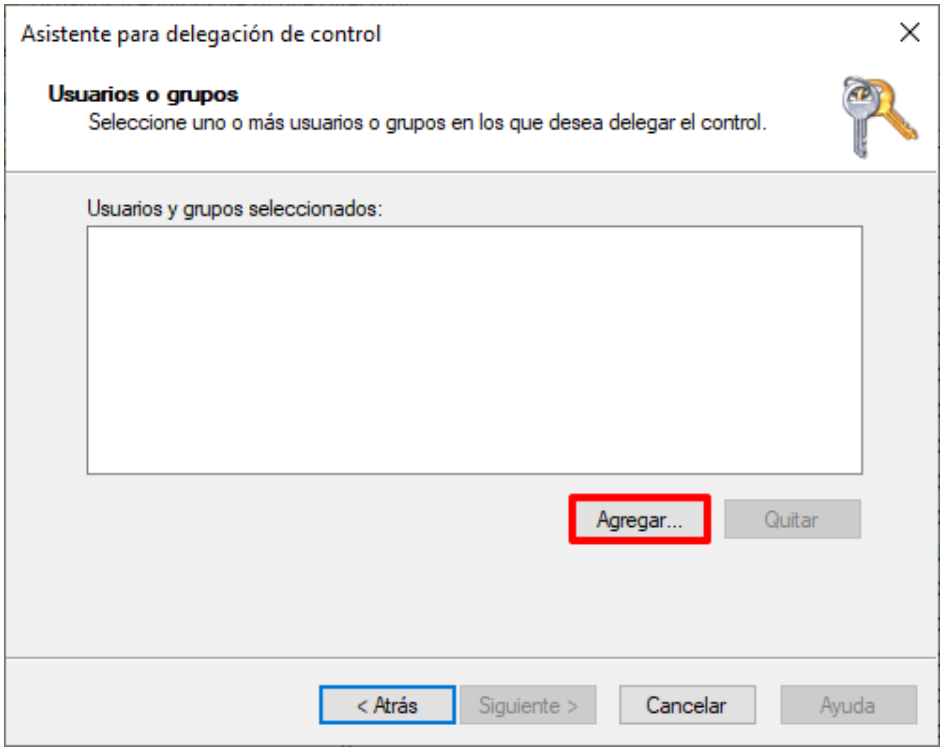
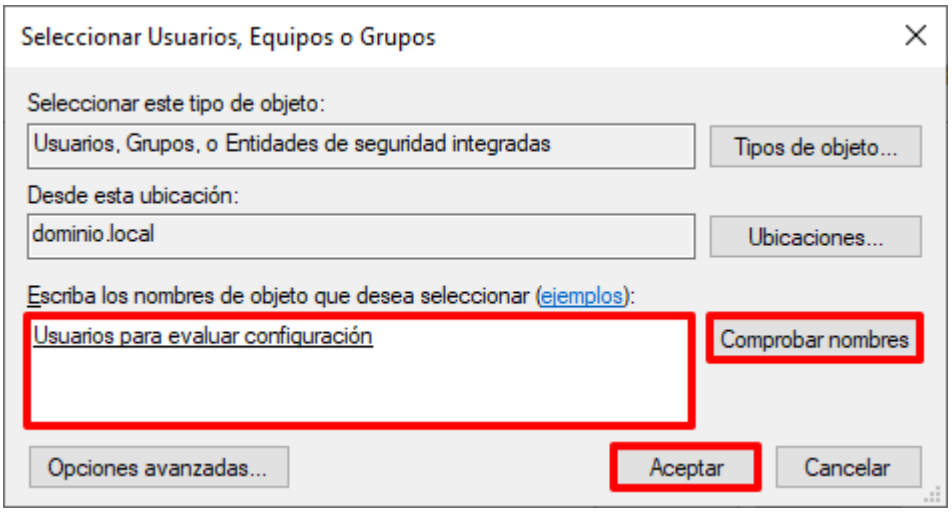
Paso	Descripción
109.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

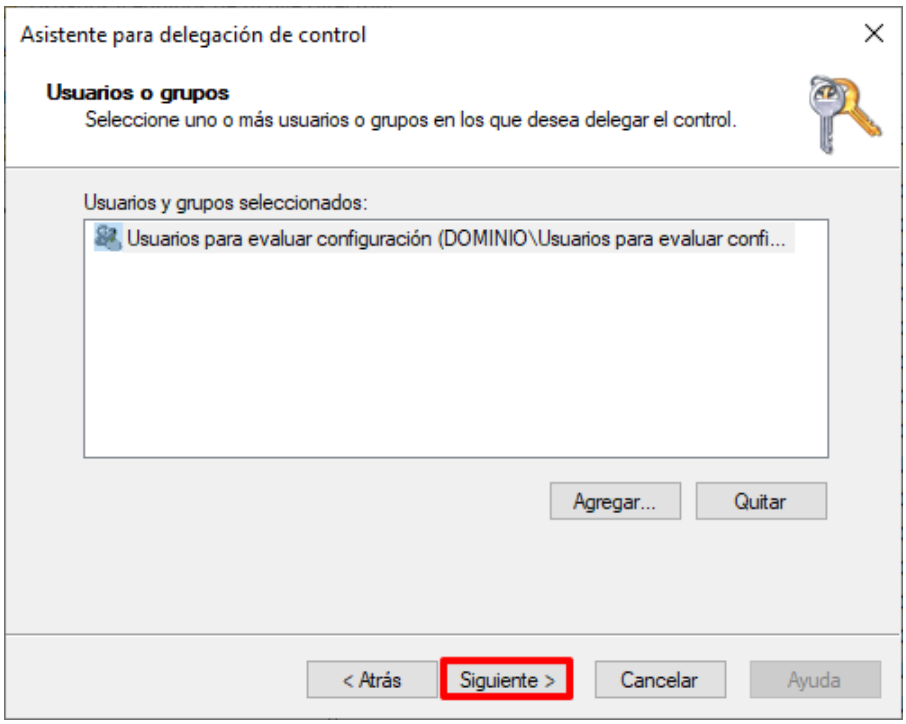
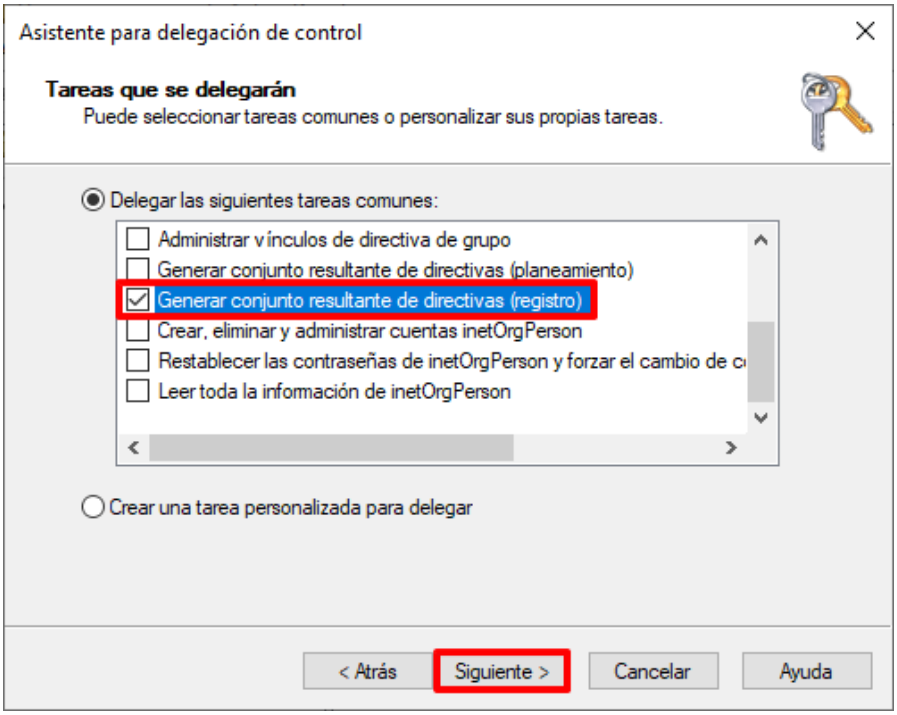
Paso	Descripción
110.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Usuarios y equipos de Active Directory”. 
111.	Sobre la consola “Usuarios y equipos de Active Directory”, seleccione y despliegue el nodo “<nombre de su dominio> → Users”. Identifique el grupo definido por defecto “Propietarios del creador de directivas de grupo” y haga doble clic sobre él. 

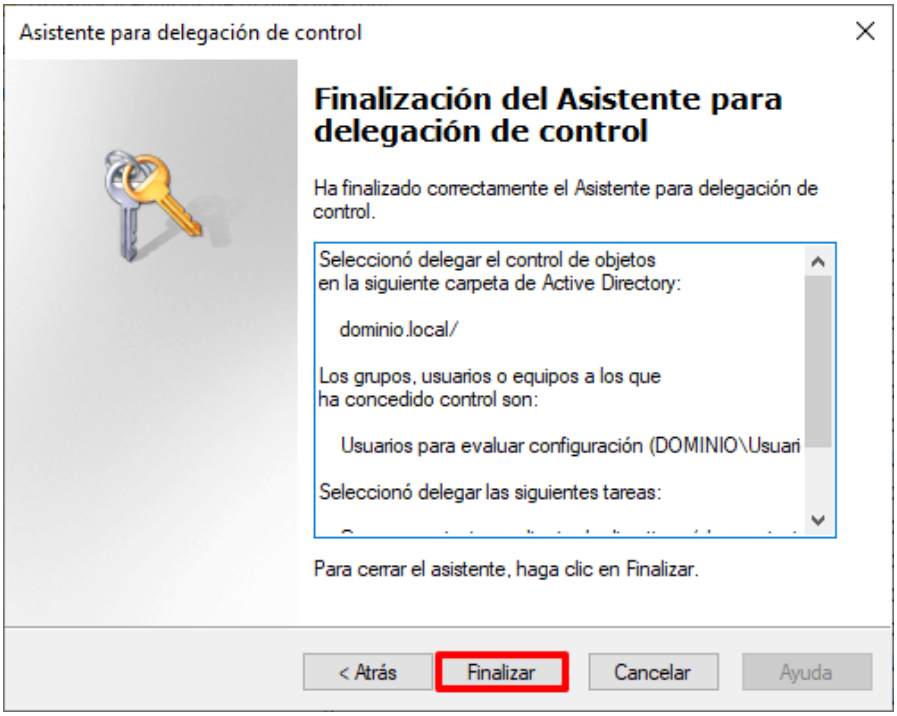
Paso	Descripción
112.	Seleccione la pestaña “Miembros” y pulse sobre el botón “Agregar…”. 
113.	En la nueva ventana emergente, incluya los usuarios o grupos los cuales desea agregar al grupo separados por punto y coma (;). Haga uso del botón “Comprobar nombres” para completar la información del usuario y pulse “Aceptar”.  **Nota:** En este ejemplo se va a hacer uso del usuario estándar generado en el punto anterior dedicado a identificación, “use002” (Usuario de Ejemplo 2 (Usuario estándar)).

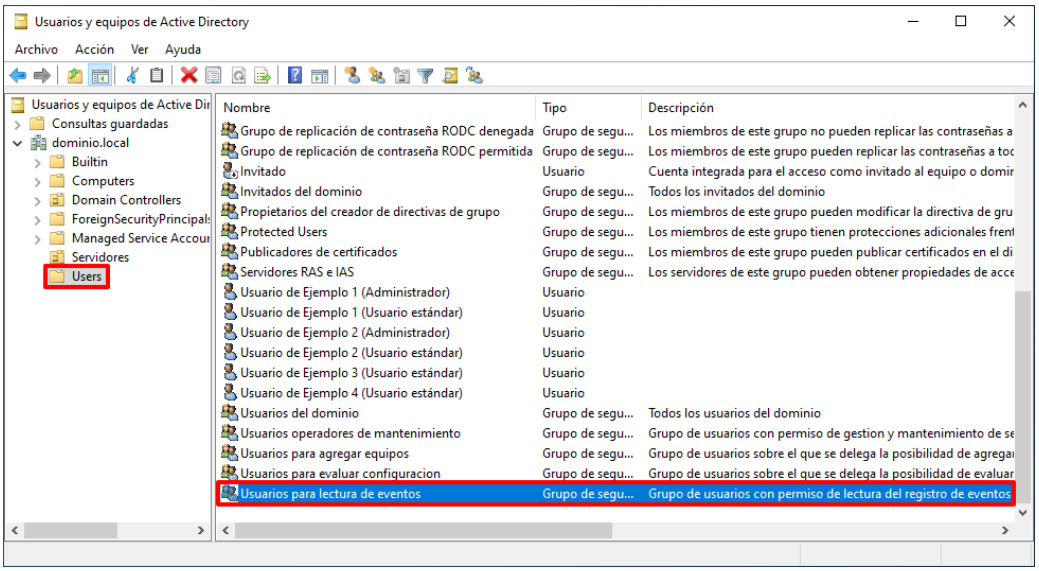
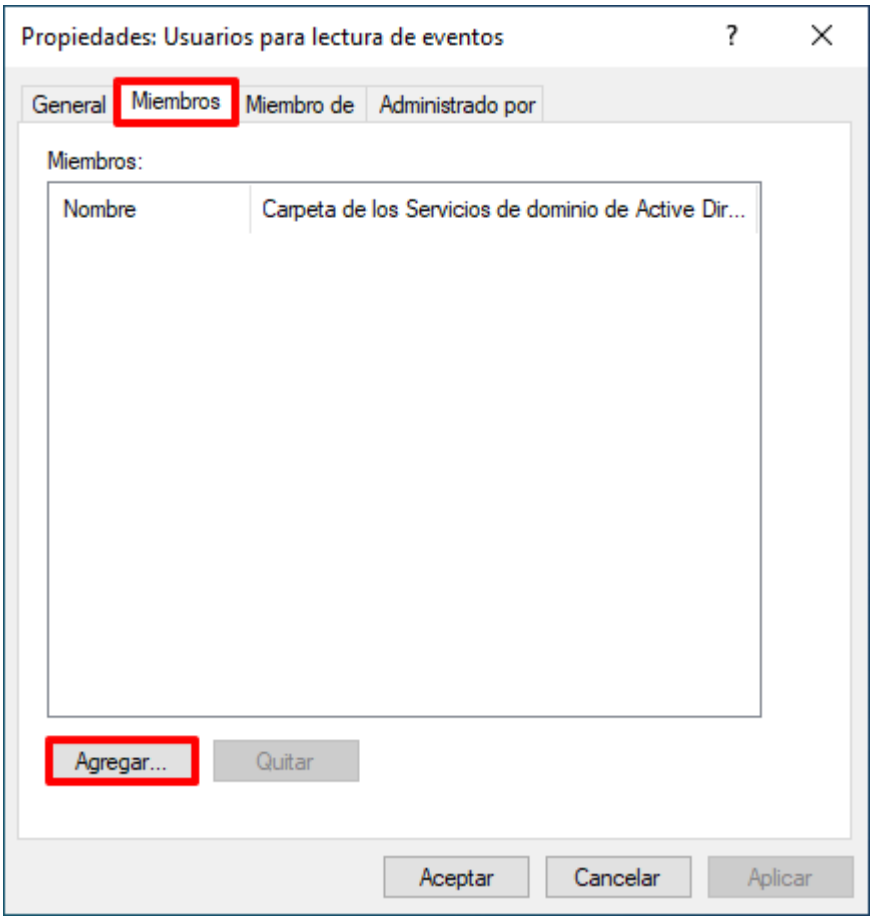
Paso	Descripción
114.	Pulse “Aceptar” sobre la ventana de propiedades del grupo para finalizar la configuración.
115.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo el acceso a las consolas de administración, aunque solo con acceso de escritura sobre la herramienta administrativa “Administración de directivas de grupo”. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.
116.	Para la siguiente labor, será necesario la creación de grupos dedicados de modo que la gestión de identidades quede simplificada en la pertenencia a grupos. **Nota:** Si ya ejecutó anteriormente el Script “CCN-STIC-570A23 Controlador de Dominio – Segregación de roles” en el “Paso 96” del presente apartado, continue en el “Paso 121”. En caso contrario continúe en el siguiente punto.
117.	Si no desea realizar una creación de grupos personalizada o no dispone de estos grupos, diríjase al directorio “C:\Scripts” y ejecute el script “CCN-STIC-570A23 Controlador de Dominio – Segregación de roles.bat”. Para ello, haga clic derecho sobre el script y seleccione la opción “Ejecutar como Administrador” del menú contextual que aparecerá. 
118.	Pulse cualquier botón para iniciar la ejecución del script y vuelva a pulsa cualquier botón para finalizar la ejecución del script.

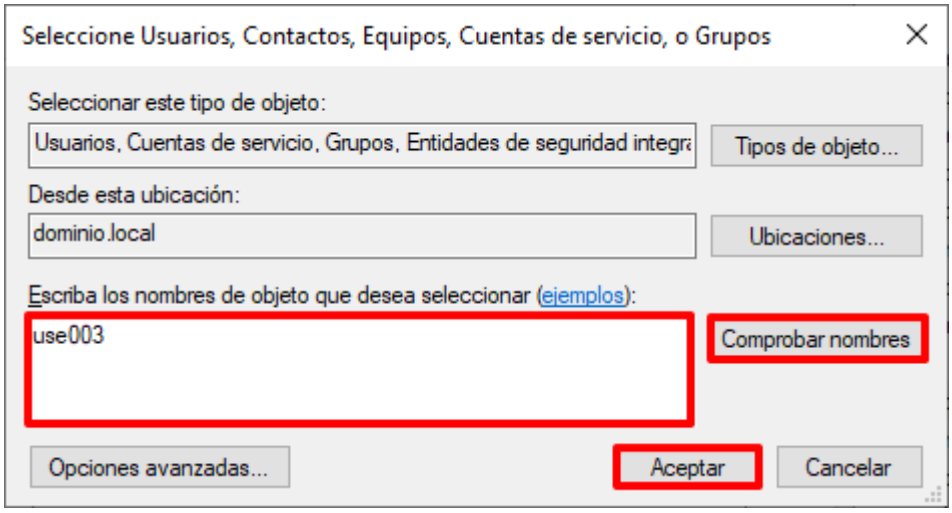
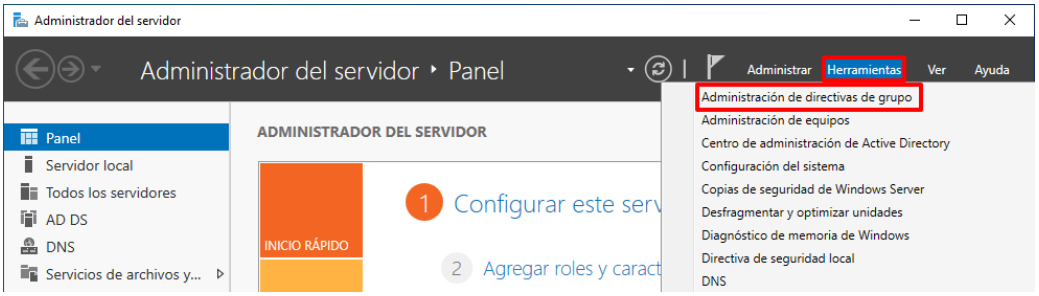
Paso	Descripción
119.	Tras la ejecución del script, entre los grupos generados se pueden encontrar los siguientes grupos: – Usuarios para evaluar configuración. – Usuarios para lectura de eventos. – Usuarios operadores de mantenimiento.
120.	De forma similar a lo realizado anteriormente, ejecute los pasos “111” a “114” para agregar a los usuarios necesarios al grupo “Usuarios para evaluar configuración” que vayan a disponer de esta capacidad.
121.	A continuación, en la misma consola de “Usuarios y equipos de Active Directory” abierta en pasos anteriores, seleccione su dominio (<nombre de su dominio>) con el botón derecho y pulse sobre “Delegar control…”. 
122.	En la ventana “Asistente para delegación de control” pulse sobre el botón “Siguiente >”.

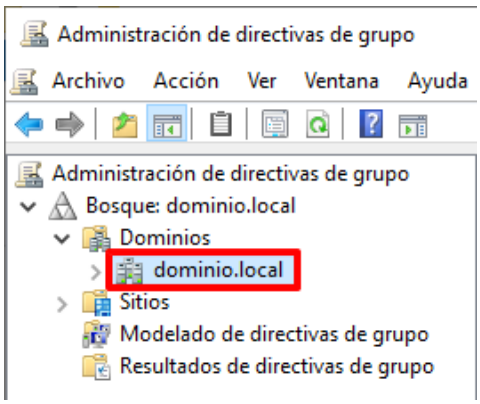
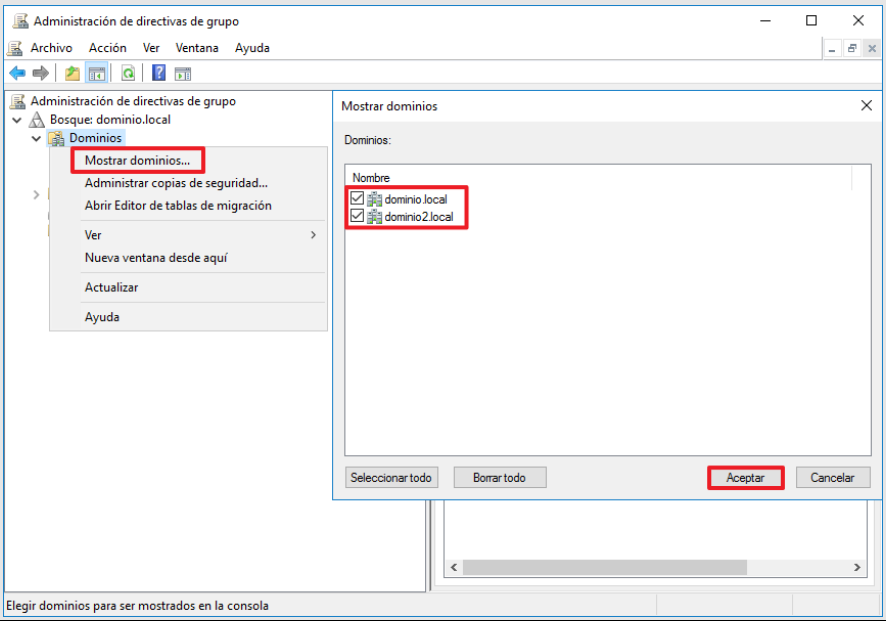
Paso	Descripción
123.	En la siguiente ventana del asistente haga clic sobre el botón “Agregar…”. 
124.	Escriba el nombre del grupo sobre el que desea delegar esta tarea. En este ejemplo será el generado a través del script ejecutado en pasos anteriores (“Usuarios para evaluar configuración”). Pulse sobre “Comprobar nombres” para completar el nombre y pulse “Aceptar”. 

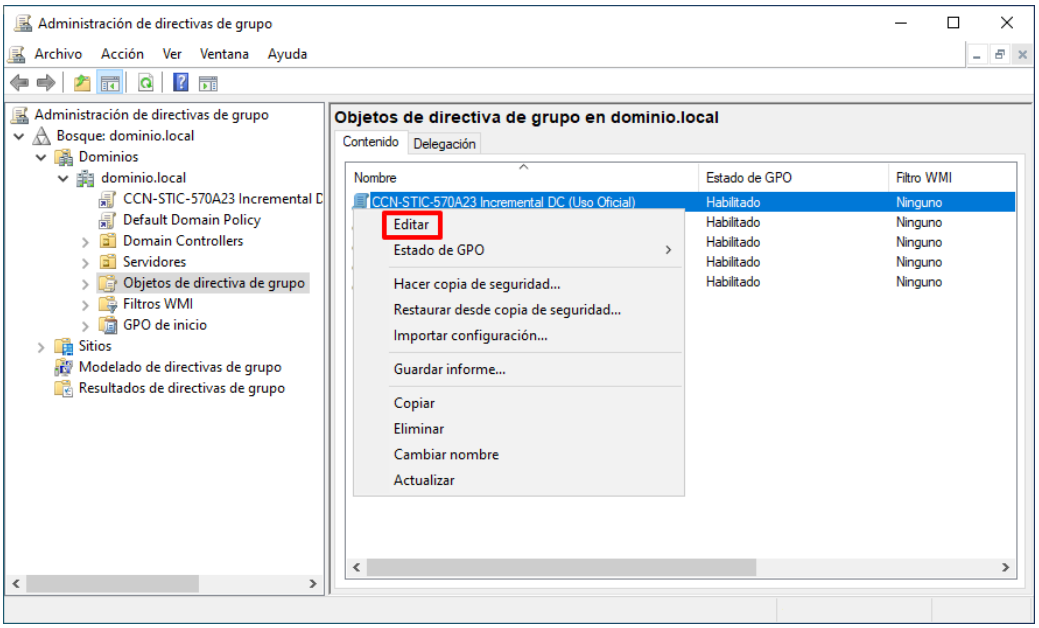
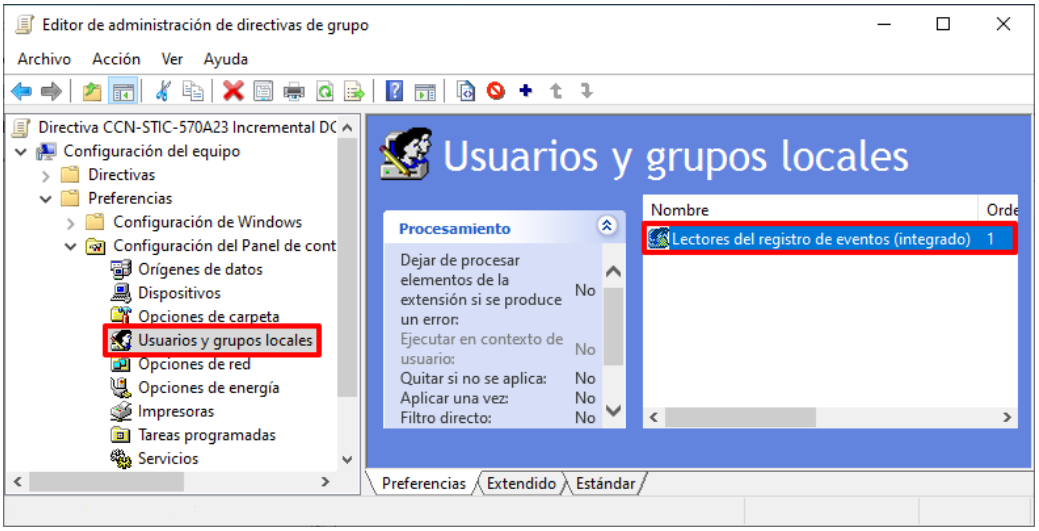
Paso	Descripción
125.	A continuación, pulse sobre “Siguiente >”. 
126.	En la ventana “Tareas que se delegarán” seleccione: – “Generar conjunto resultante de directivas (registro)” Pulse “Siguiente >” para continuar. 

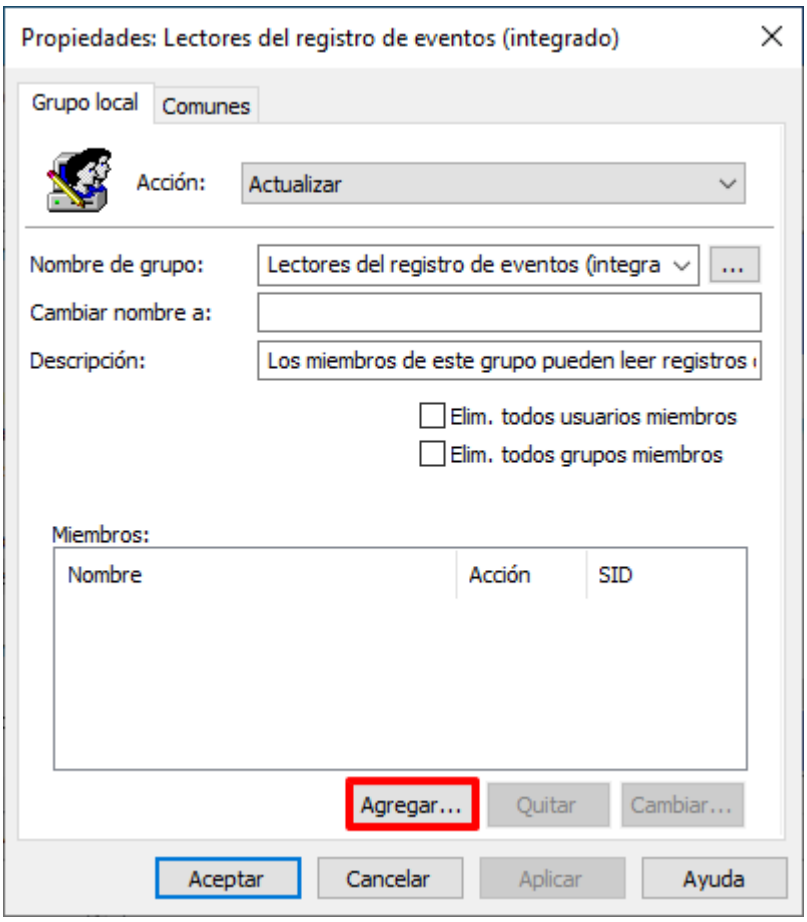
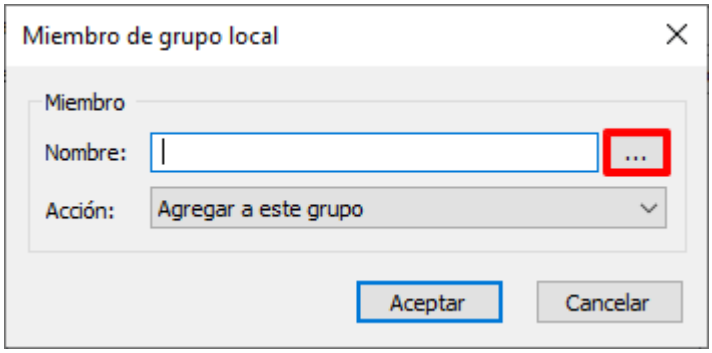
Paso	Descripción
127.	Pulse “Finalizar” para acabar con el proceso. 
128.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo la capacidad de obtener el estado de la configuración aplicada sobre los equipos finales en un entorno de dominio, sin la capacidad de administración sobre dicho equipo. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.

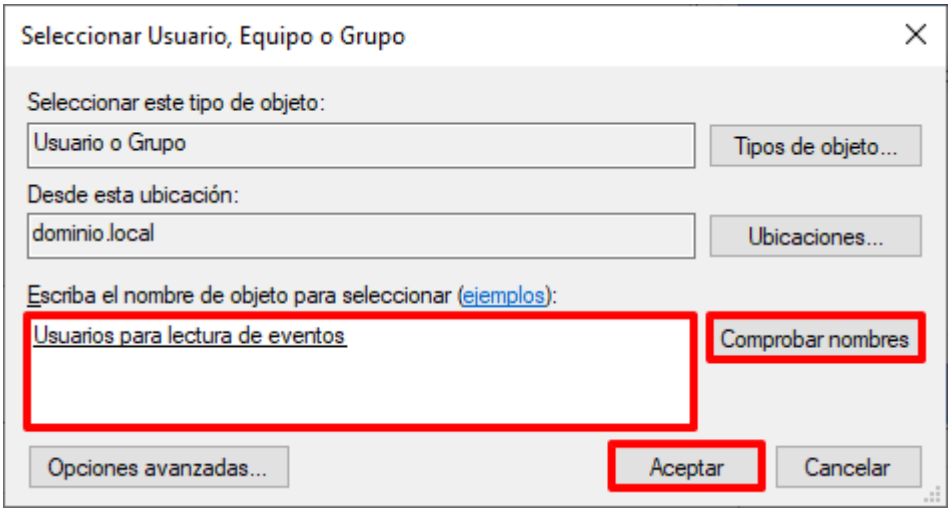
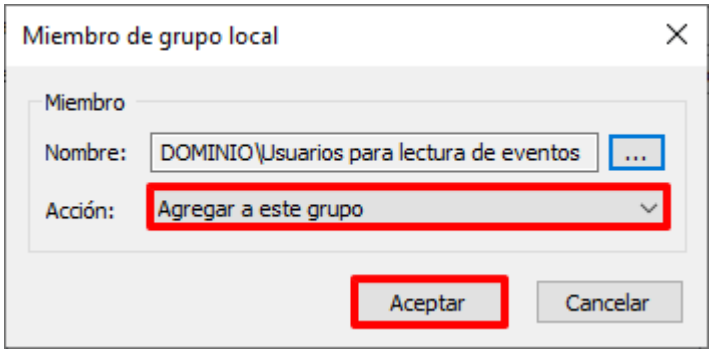
Paso	Descripción
129.	Por otro lado, de nuevo en la consola “Usuarios y equipos de Active Directory”, seleccione y despliegue el nodo “<nombre de su dominio> → Users”. Identifique el grupo generado “Usuarios para lectura de eventos” y haga doble clic sobre él. 
130.	Seleccione la pestaña “Miembros” y pulse sobre el botón “Agregar…”. 

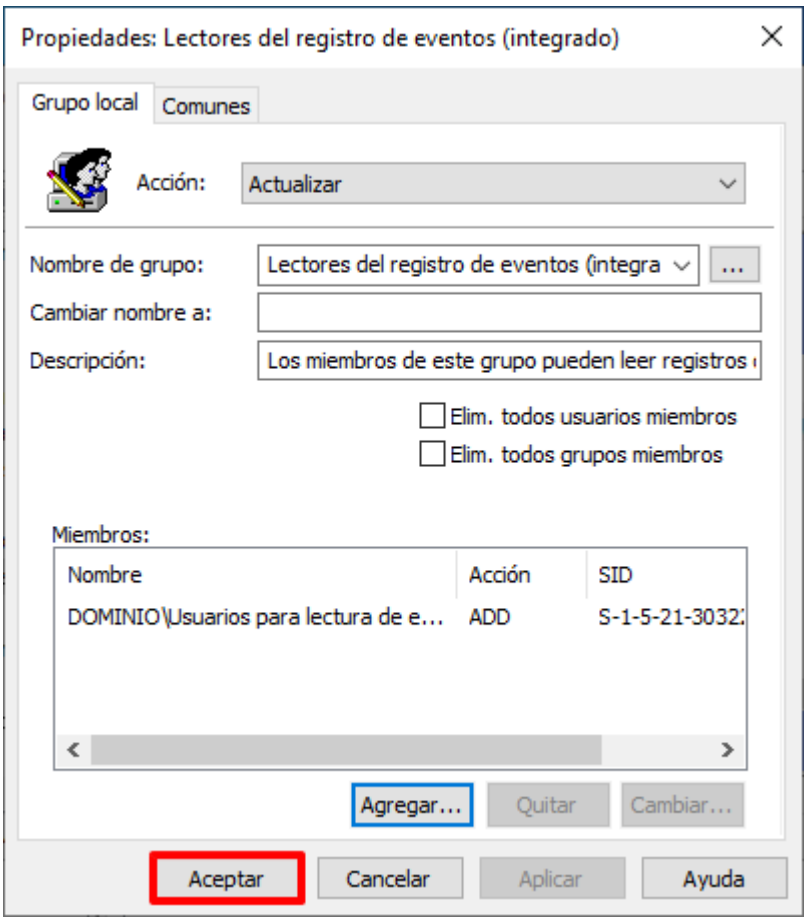
Paso	Descripción
131.	En la nueva ventana emergente, incluya los usuarios o grupos los cuales desea agregar al grupo separados por punto y coma (;). Haga uso del botón "Comprobar nombres" para completar la información del usuario y pulse "Aceptar".  **Nota:** En este ejemplo se va a hacer uso del usuario estándar generado según la nomenclatura definida en el punto anterior dedicado a identificación, "use003" (Usuario de Ejemplo 3 (Usuario estándar)).
132.	A continuación, en el "Administrador del servidor", en la parte superior derecha pulse sobre el botón "Herramientas" y seleccione "Administración de directivas de grupo". 

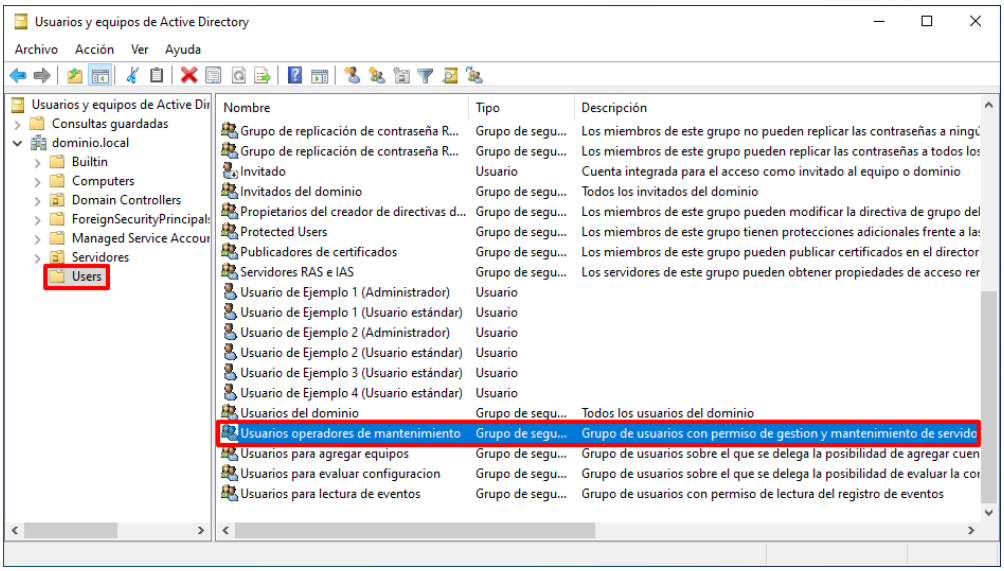
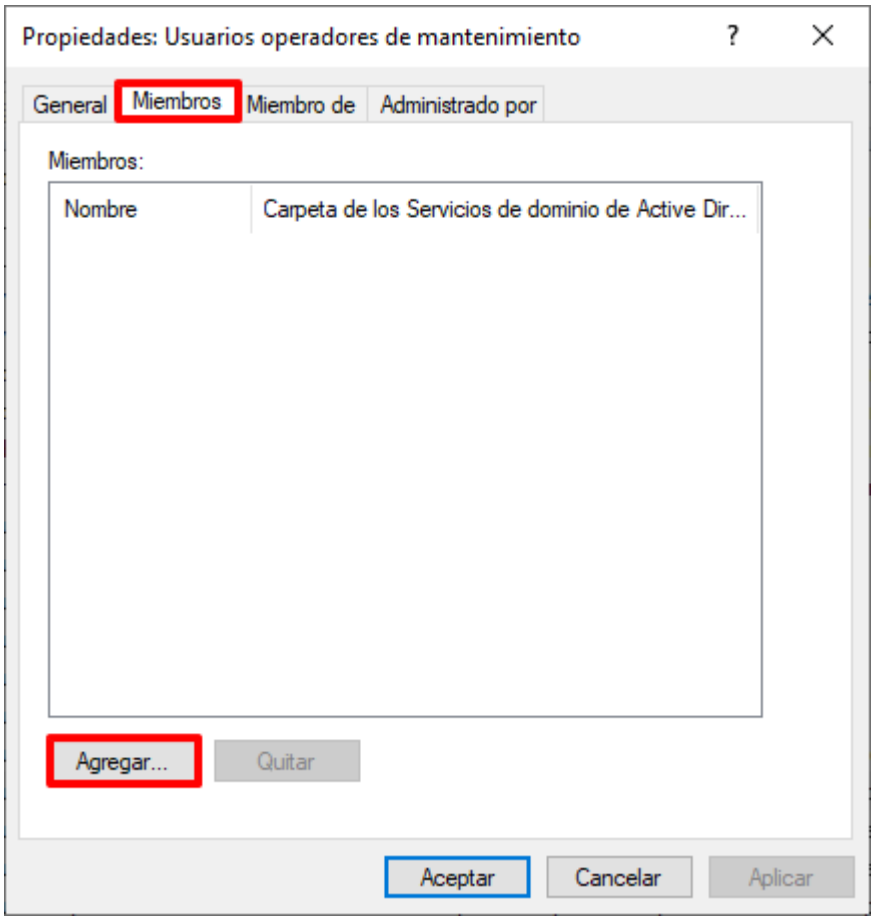
Paso	Descripción
133.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

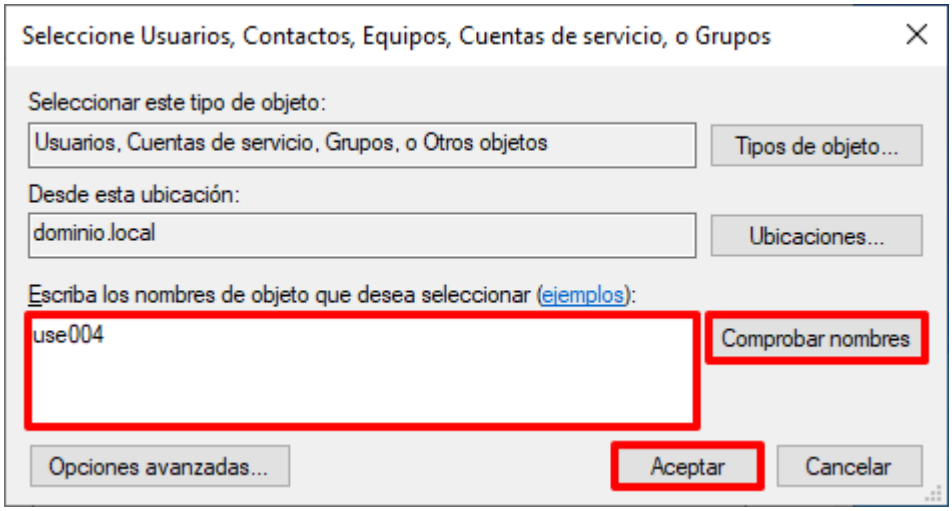
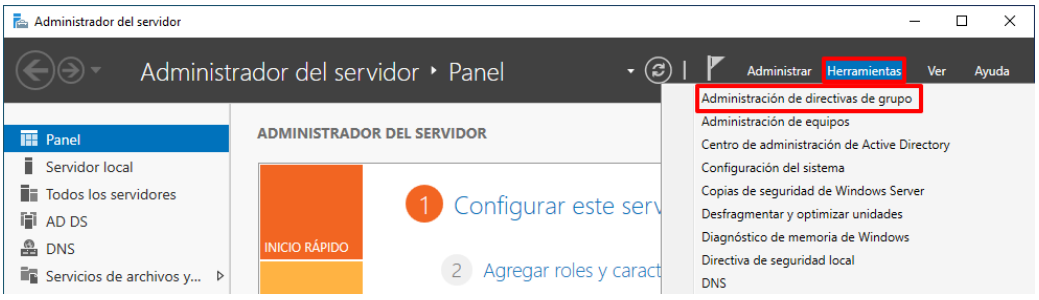
Paso	Descripción
134.	Seleccione con el botón derecho el objeto GPO “CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
135.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Preferencias → Configuración del Panel de control → Usuarios y grupos locales”**. En el panel derecho identifique el grupo “Lectores del registro de eventos (integrado)” y haga doble clic sobre el mismo. 

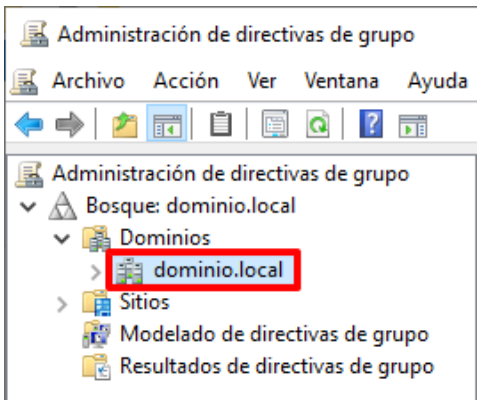
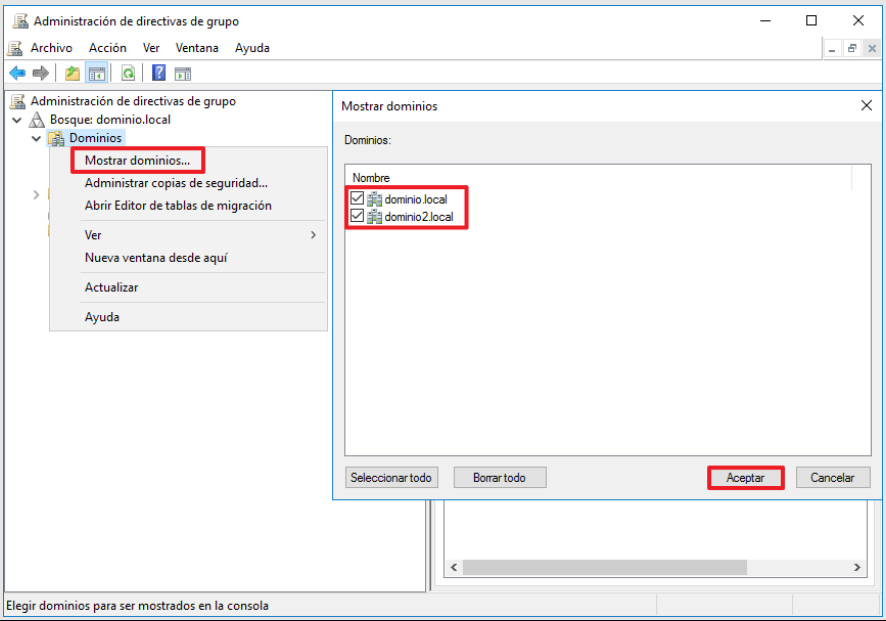
Paso	Descripción
136.	Pulse sobre el botón “Agregar…” para continuar. 
137.	En la nueva ventana emergente pulse sobre el botón “…”. 

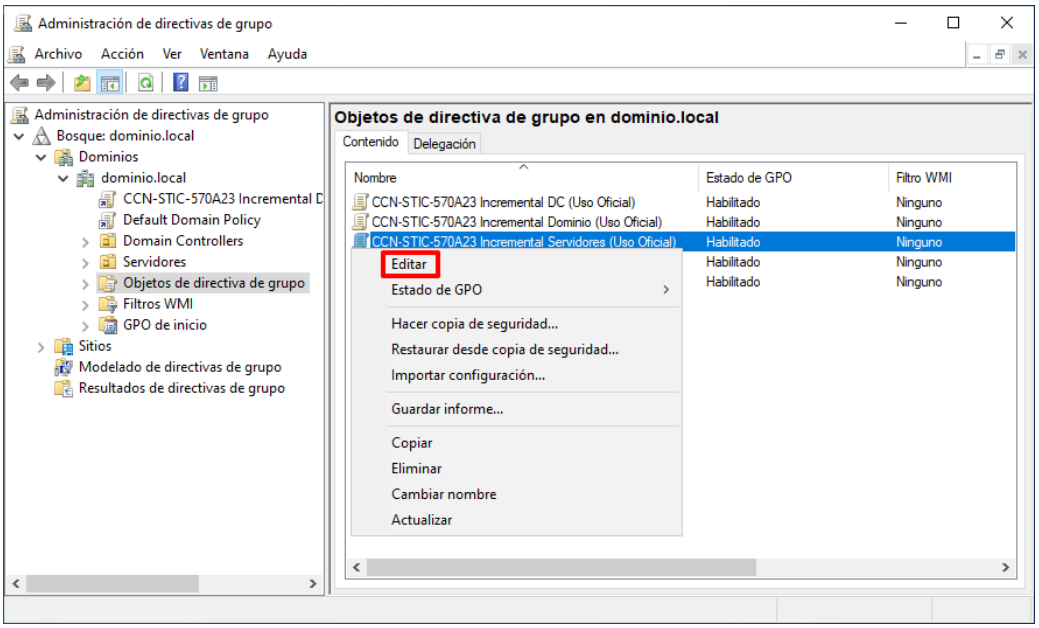
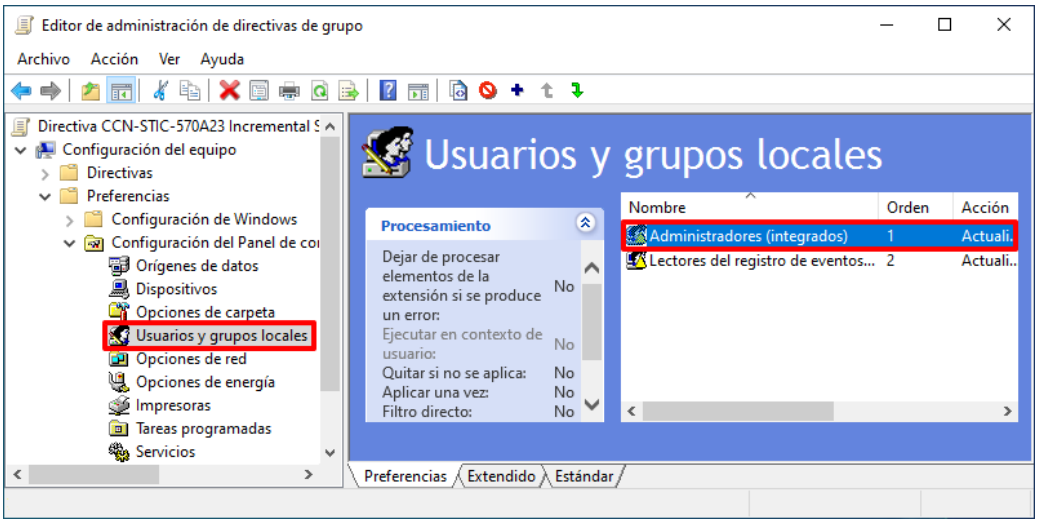
Paso	Descripción
138.	Escriba el nombre del grupo que desea incluir en el grupo integrado “Lectores del registro de eventos”. En este ejemplo, será el generado a través del script ejecutado en pasos anteriores (“Usuarios para lectura de eventos”). Pulse sobre “Comprobar nombres” para completar el nombre y pulse “Aceptar”. 
139.	En la anterior ventana emergente asegúrese de que la acción a realizar es “Agregar a este grupo” y pulse el botón de “Aceptar”. 

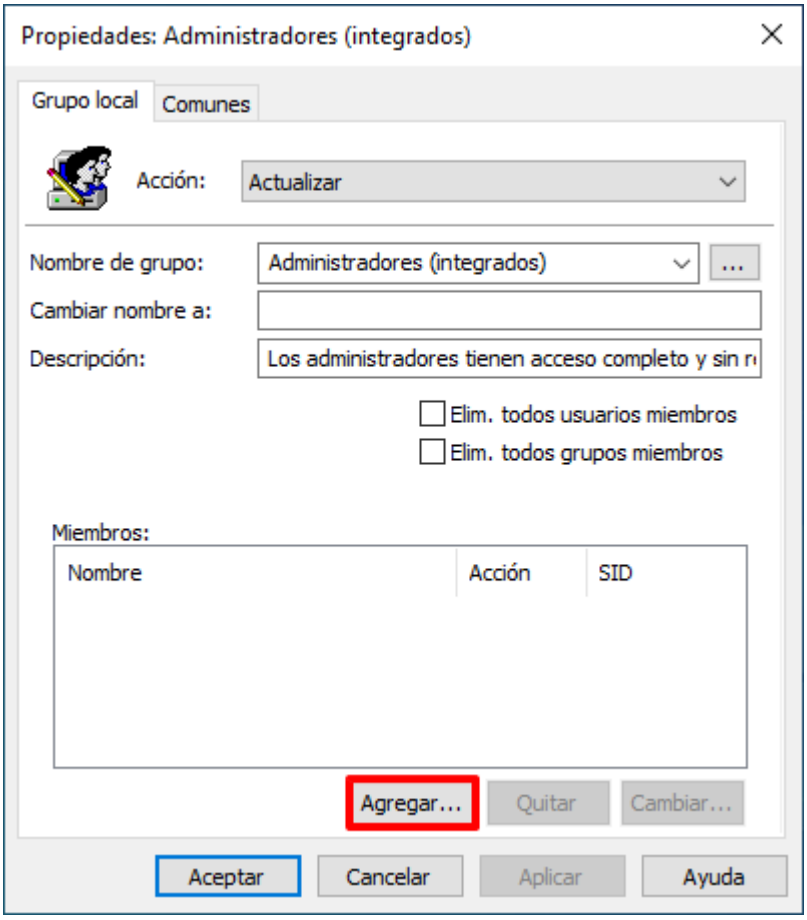
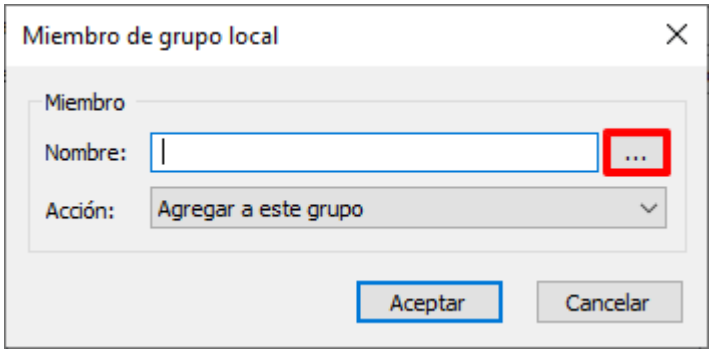
Paso	Descripción
140.	Para finalizar, pulse de nuevo sobre el botón de “Aceptar”. 
141.	Ejecute de nuevo los pasos 135 a 140 sobre el objeto GPO “CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])”, con el objetivo de añadir en el mismo el grupo deseado al grupo integrado “Lectores del registro de eventos”.
142.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes a este grupo el acceso a la consola de eventos del sistema operativo, pero sin la capacidad de administración sobre el equipo. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados.

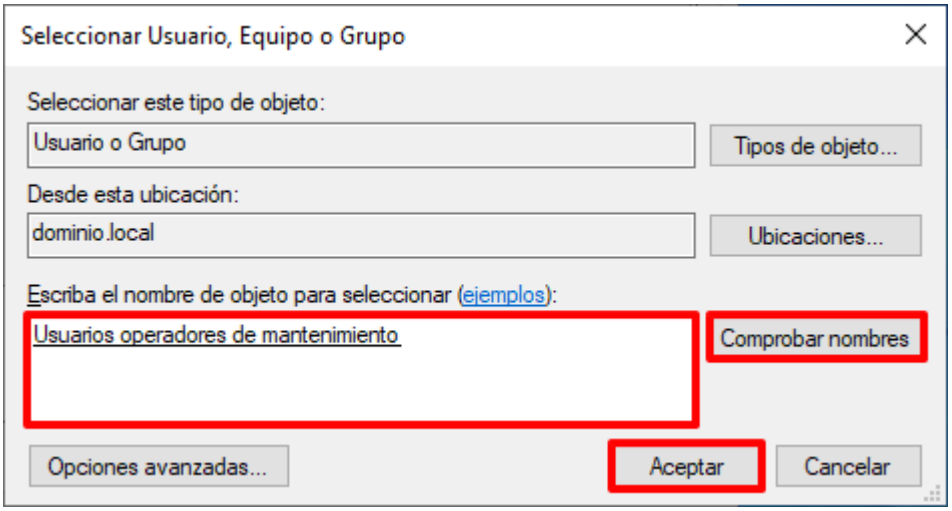
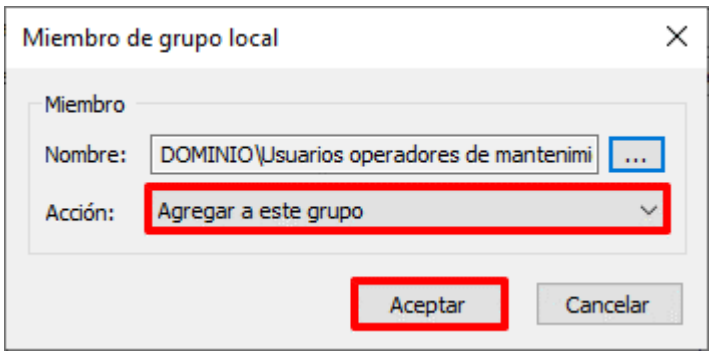
Paso	Descripción
143.	De nuevo en la consola “Usuarios y equipos de Active Directory”, seleccione y despliegue el nodo “<nombre de su dominio> → Users”. Identifique el grupo generado “Usuarios operadores de mantenimiento” y haga doble clic sobre él. 
144.	Seleccione la pestaña “Miembros” y pulse sobre el botón “Agregar…”. 

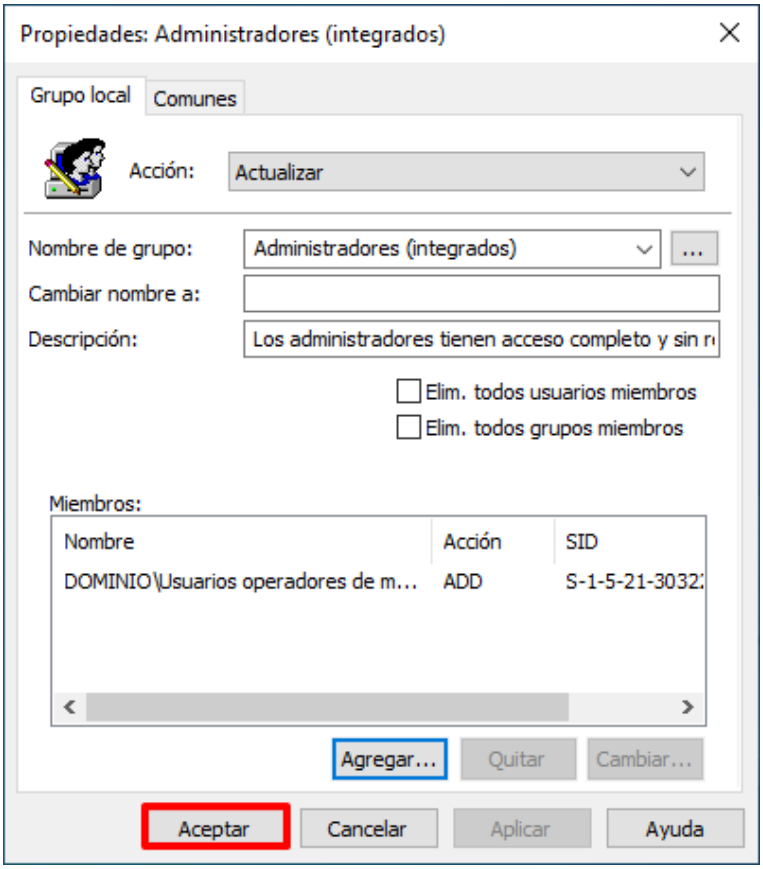
Paso	Descripción
145.	En la nueva ventana emergente, incluya los usuarios o grupos los cuales desea agregar al grupo separados por punto y coma (;). Haga uso del botón "Comprobar nombres" para completar la información del usuario y pulse "Aceptar".  **Nota:** En este ejemplo se va a hacer uso del usuario estándar generado según la nomenclatura definida en el punto anterior dedicado a identificación, "use004" (Usuario de Ejemplo 4 (Usuario estándar)).
146.	A continuación, en el "Administrador del servidor", en la parte superior derecha pulse sobre el botón "Herramientas" y seleccione "Administración de directivas de grupo". 

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

Paso	Descripción
148.	Seleccione con el botón derecho el objeto GPO “CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
149.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) → Configuración del equipo → Preferencias → Configuración del Panel de control → Usuarios y grupos locales”**. En el panel derecho identifique el grupo “Administradores (integrado)” y haga doble clic sobre el mismo. 

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

Paso	Descripción
152.	Escriba el nombre del grupo que desea incluir en el grupo integrado "Administradores". En este ejemplo, será el generado a través del script ejecutado en pasos anteriores ("Usuarios operadores de mantenimiento"). Pulse sobre "Comprobar nombres" para completar el nombre y pulse "Aceptar". 
153.	En la anterior ventana emergente asegúrese de que la acción a realizar es "Agregar a este grupo" y pulse el botón de "Aceptar". 

Paso	Descripción
154.	Para finalizar, pulse de nuevo sobre el botón de “Aceptar”. 
155.	Tenga en consideración que esta configuración permitirá a los usuarios pertenecientes al grupo incluido en los pasos previos el inicio de sesión sobre los equipos de tipo Servidor Miembro y realizar un mantenimiento, no basado en actualizaciones automáticas, con privilegios administrativos elevados. Esto supone que a efectos prácticos disponen de capacidad de administración sobre el equipo y los elementos que contiene. Deberá limitar el acceso a aplicaciones y herramientas para evitar que estos usuarios puedan realizar tareas sobre estas. **Nota:** No es objeto de esta guía definir los procesos idóneos de gestión por medio de herramientas o consolas adicionales de administración dentro de un dominio a través de equipos o puntos de acceso dedicados. En el paso a paso, dicha labor solo se ha delegado sobre los servidores miembro por cuestiones de operabilidad y no así sobre equipos de tipo Controlador de Dominio para preservar la seguridad en este componente crítico del Active Directory.

ANEXO A.2.4. CONFIGURACIÓN DE SEGURIDAD

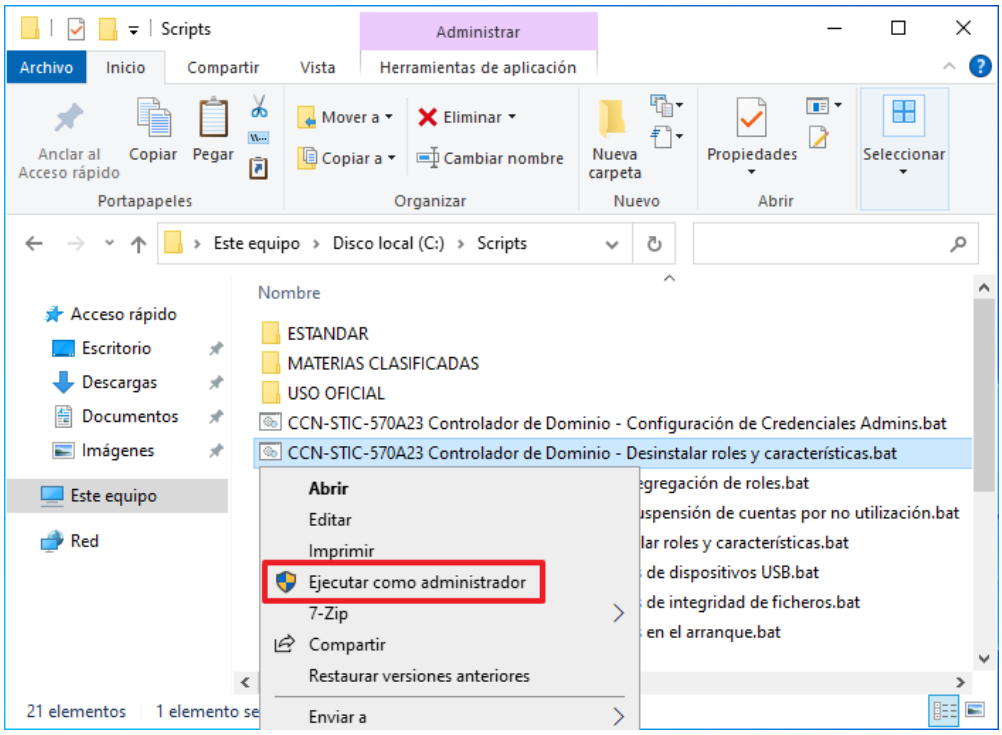
En el presente apartado, se definirán los pasos y acciones que tiene como objetivo cumplir la regla de "mínima funcionalidad".

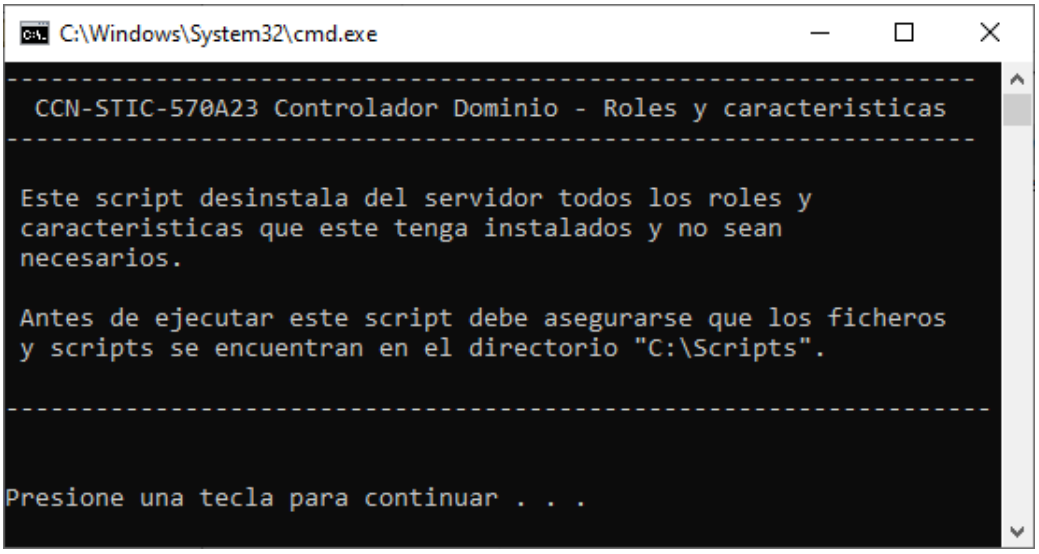
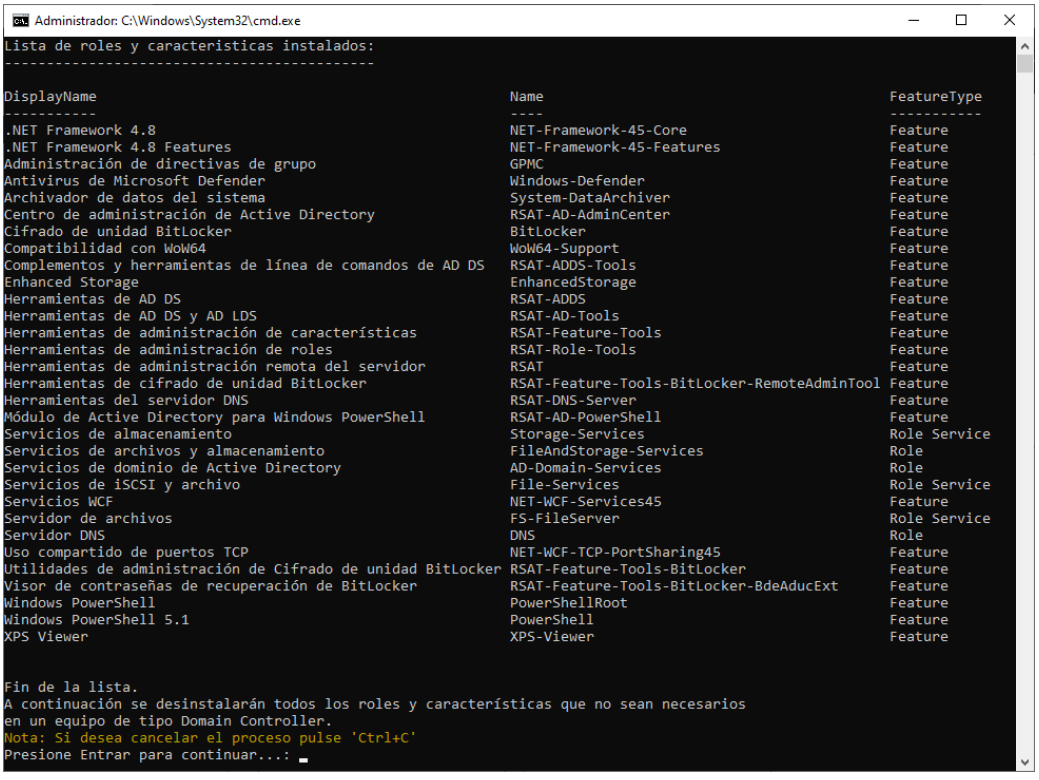
Para lograr el objetivo anterior se describen dos alternativas:

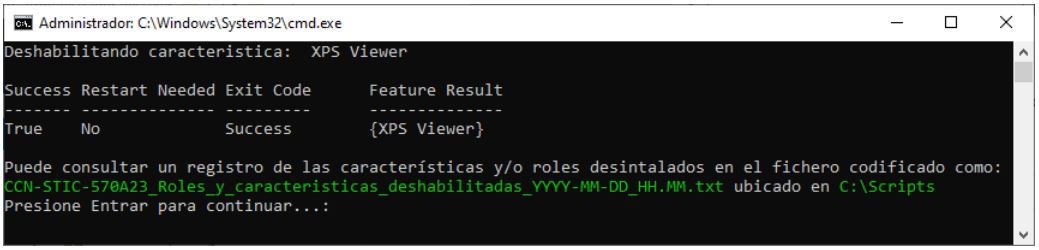
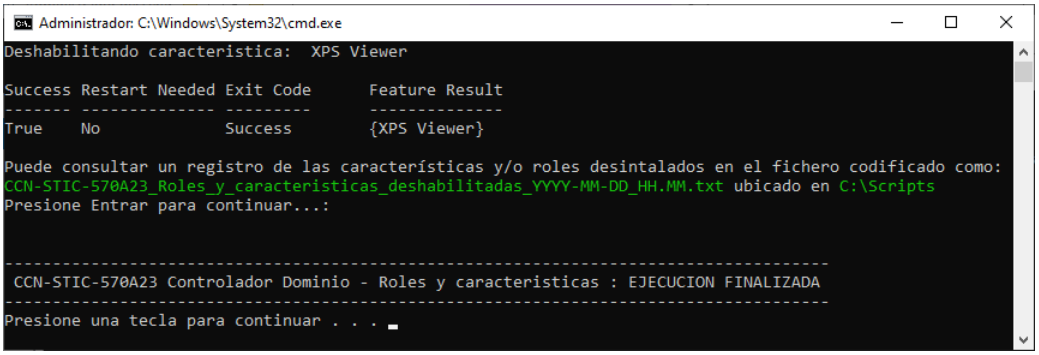
a) Por un lado, se facilitará un script que permita desinstalar aquellos roles y características consideradas no necesarias dentro de un equipo de tipo Domain Controller.

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

Nota: Si desea solo ejecutar esta acción de forma manual, vaya al "Paso 163" de este apartado.

Paso	Descripción
156.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
157.	Diríjase al directorio "C:\Scripts", haga clic derecho sobre el fichero "CCN-STIC-570A23 Controlador de Dominio – Desinstalar roles y características.bat" y seleccione la opción del menú contextual "Ejecutar como Administrador". 

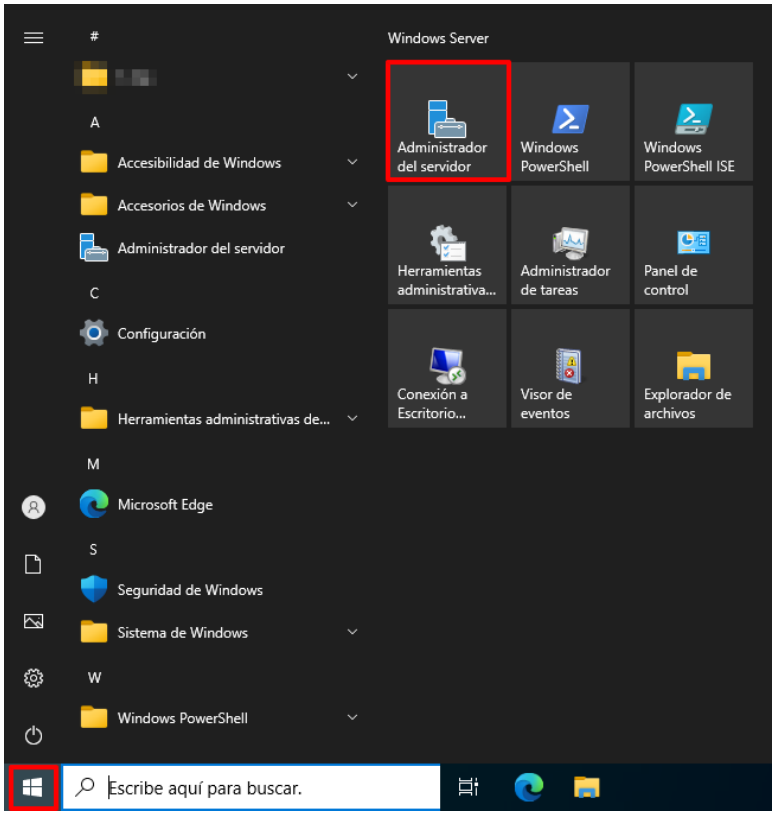
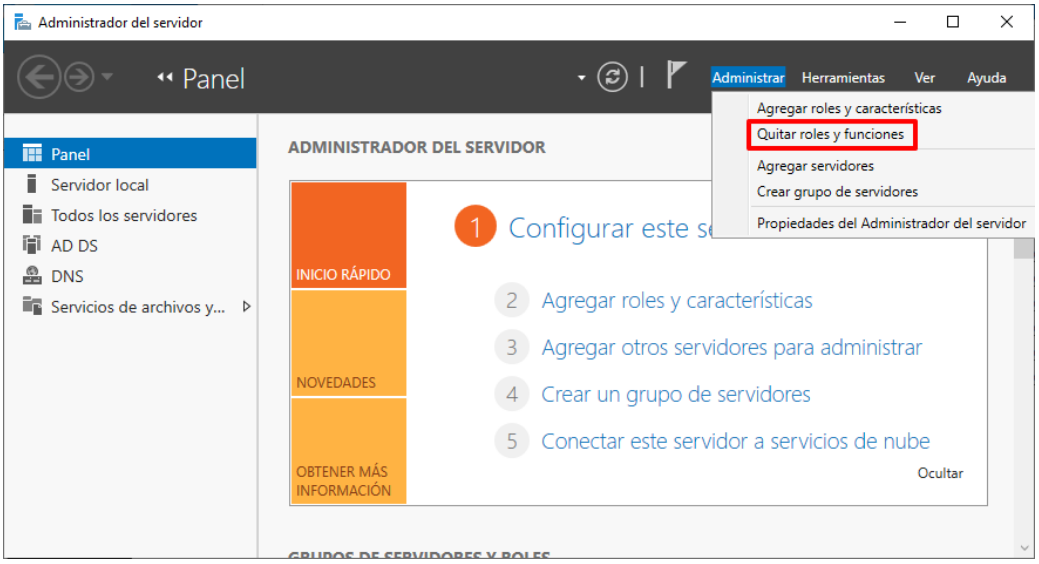
Paso	Descripción
158.	Pulse cualquier tecla para continuar. 
159.	A continuación, se recopilará y mostrarán los roles y características instalados en el equipo. Deberá pulsar sobre la tecla “Enter” para continuar y dar comienzo a la desinstalación de los roles y características no necesarias. 

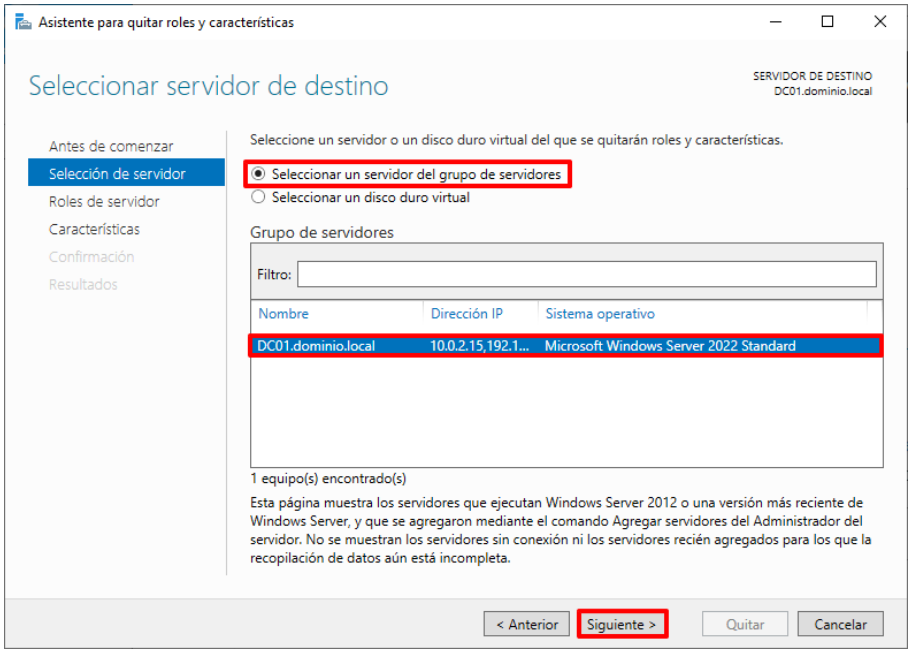
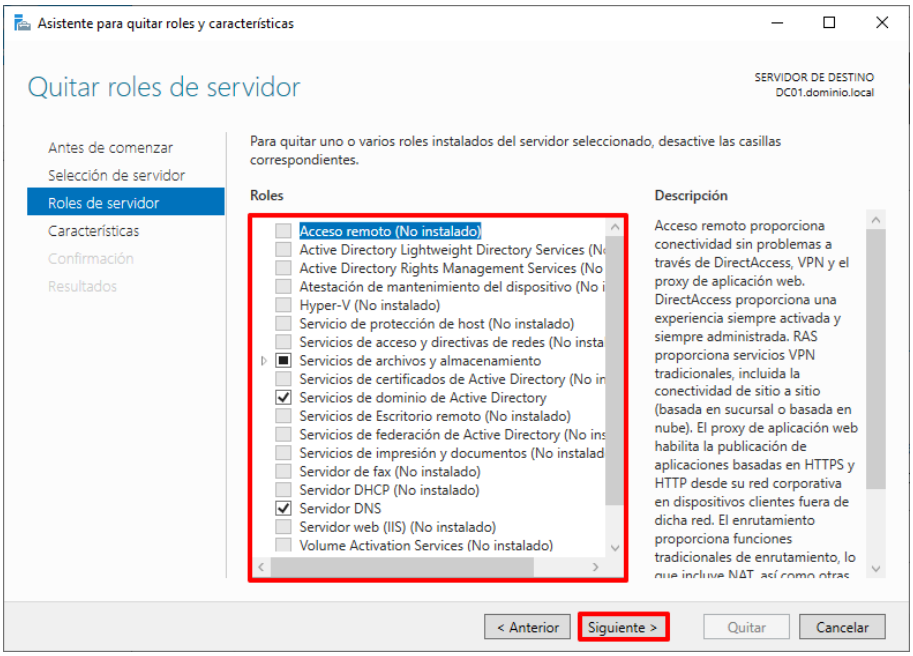
Paso	Descripción
160.	Cuando el proceso haya finalizado, podrá evaluar las características y roles desinstalados. Pulse de nuevo la tecla “Enter” para continuar. 
161.	El servidor se reiniciará a continuación para asegurar la adecuada desinstalación de roles y/o características. Pulse cualquier tecla para finalizar la ejecución del script. 
162.	Con esto se habrá finalizado la eliminación de roles y características no necesarias en un equipo de tipo Domain Controller.

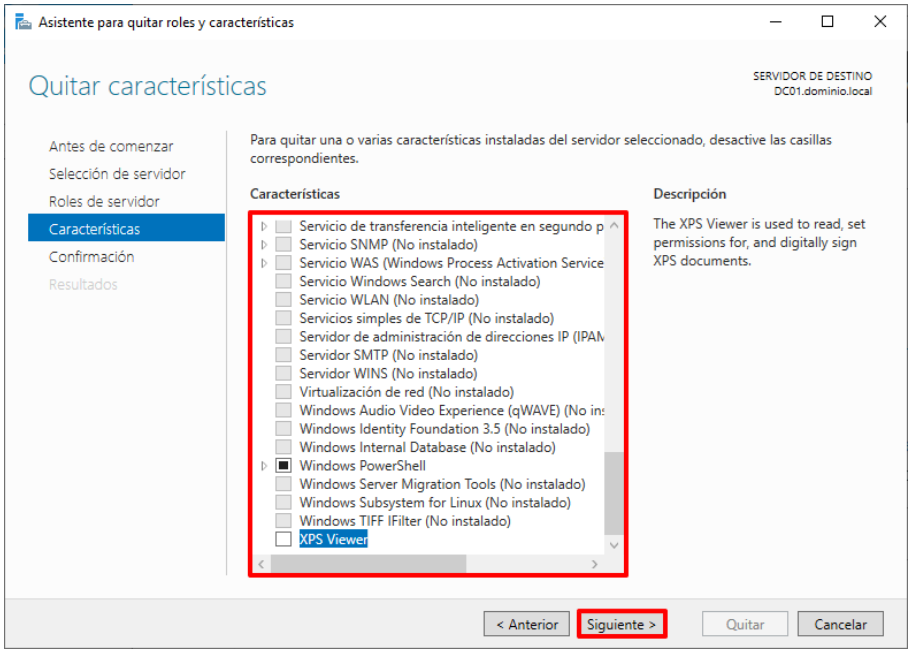
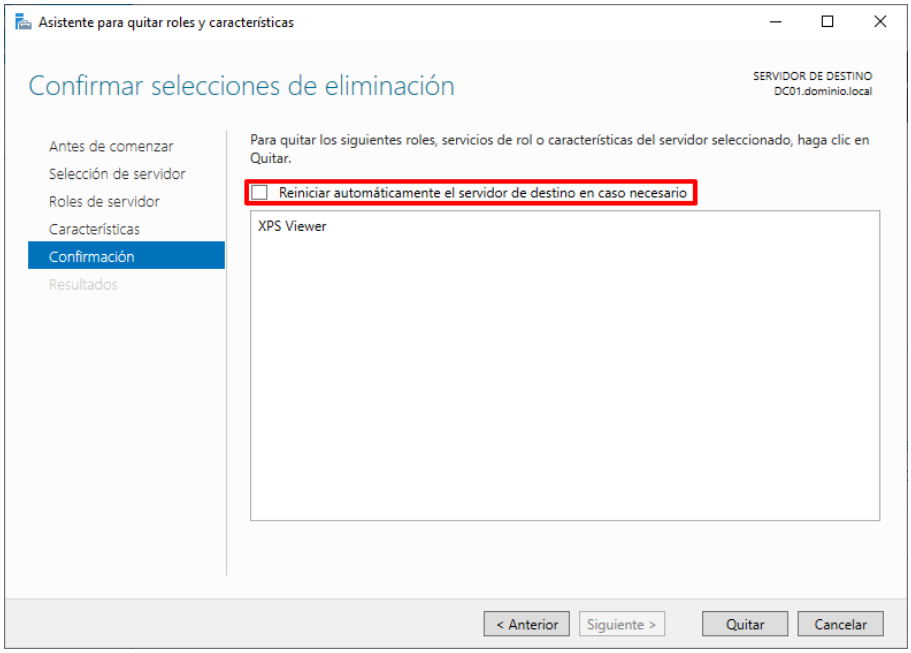
A continuación, se describen los pasos para realizar una desinstalación manual de roles y/o características implementadas en un equipo de tipo Domain Controller.

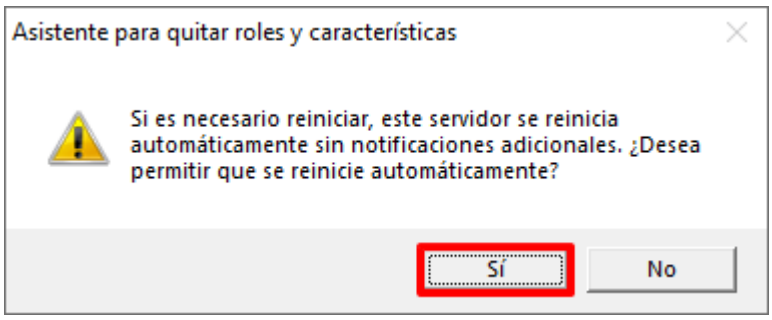
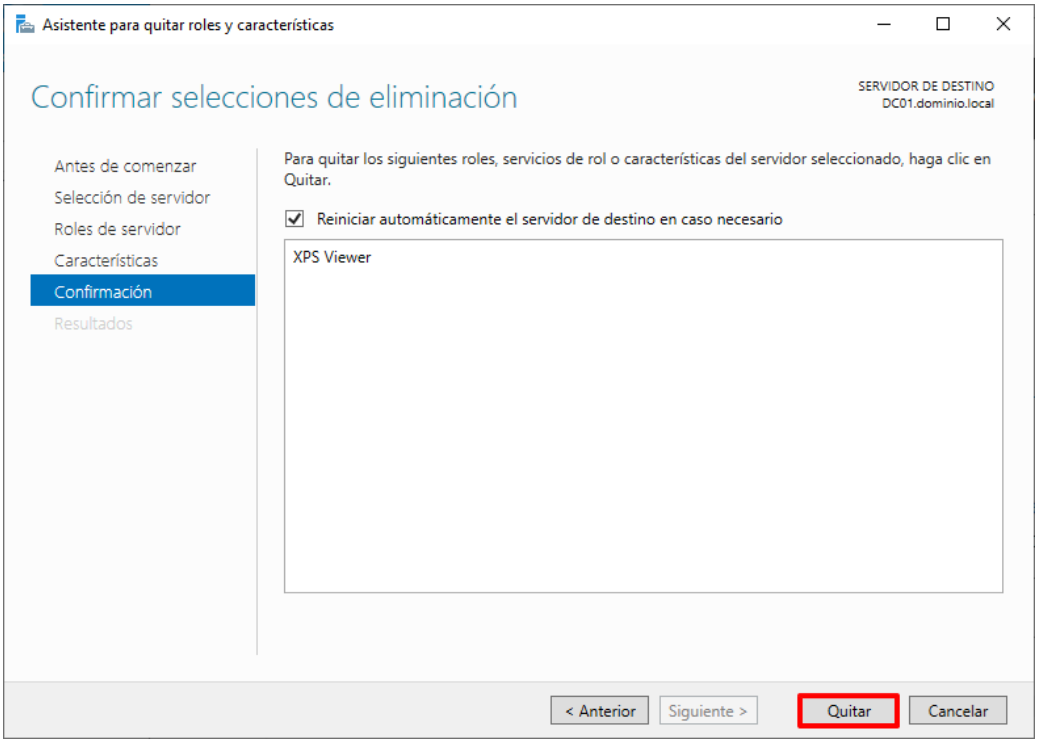
Nota: Para este ejemplo se desinstalará el visor XPS.

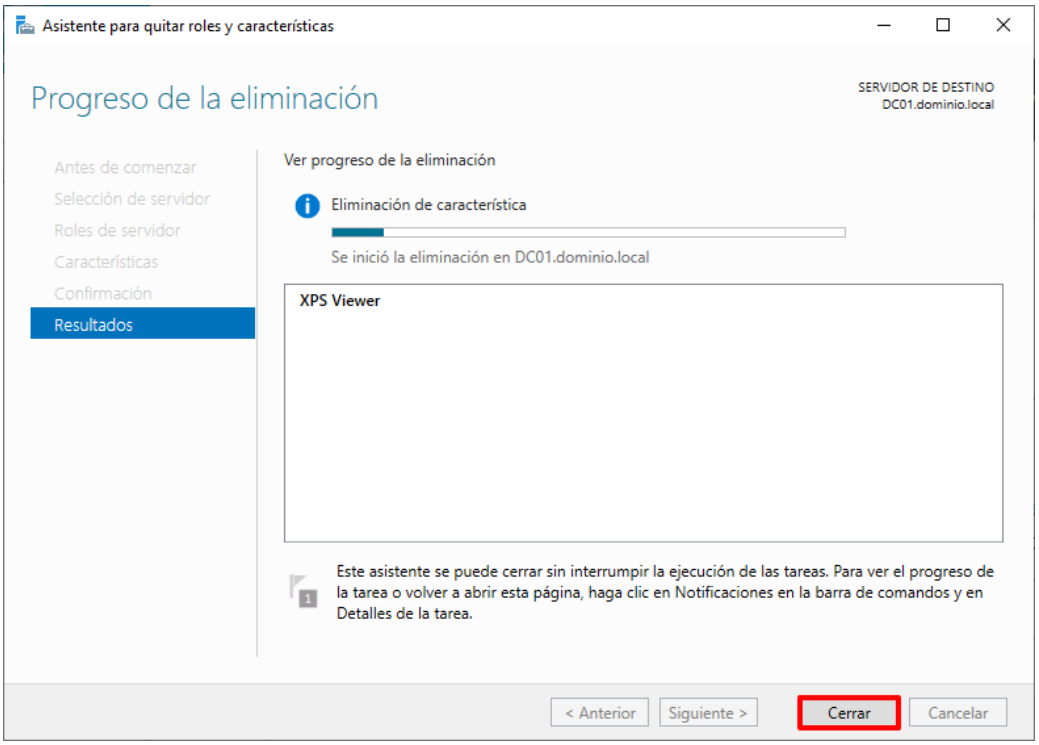
Paso	Descripción
163.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
164.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar el “Administrador del servidor”.
165.	En la parte superior derecha de la ventana “Administrador del servidor” pulse sobre “Administrar → Quitar roles y funciones”. 

Paso	Descripción
166.	En el asistente de instalación que se abrirá pulse “Siguiente >” en la primera ventana.
167.	A continuación, mantenga la opción “Seleccionar un servidor del grupo de servidores”, seleccione el equipo afectado en el apartado “Grupo de servidores” y pulse “Siguiente >”. 
168.	En el siguiente apartado del asistente, “Roles de servidor”, identifique aquellos que no son necesarios y desmárquelos. Pulse “Siguiente >” para continuar. 

Paso	Descripción
169.	Realice la misma acción que en el paso anterior, pero en el apartado del asistente "Características". Si apareciera una ventana para eliminar roles o características dependientes deberá pulsar en dicha ventana sobre "Quitar características". Pulse "Siguiente >" para continuar.  **Nota:** En este ejemplo se desinstala la característica "XPS Viewer".
170.	En la siguiente sección marque la opción "Reiniciar automáticamente el servidor de destino en caso necesario". 

Paso	Descripción
171.	Pulse “Sí” ante el mensaje de advertencia. 
172.	Pulse sobre el botón “Quitar” para dar comienzo a la desinstalación. 

Paso	Descripción
173.	A partir de ese momento el proceso dará comienzo. Pulse sobre el botón "Cerrar" cuando haya finalizado. En caso de ser necesario un reinicio el sistema advertirá de dicha necesidad. 

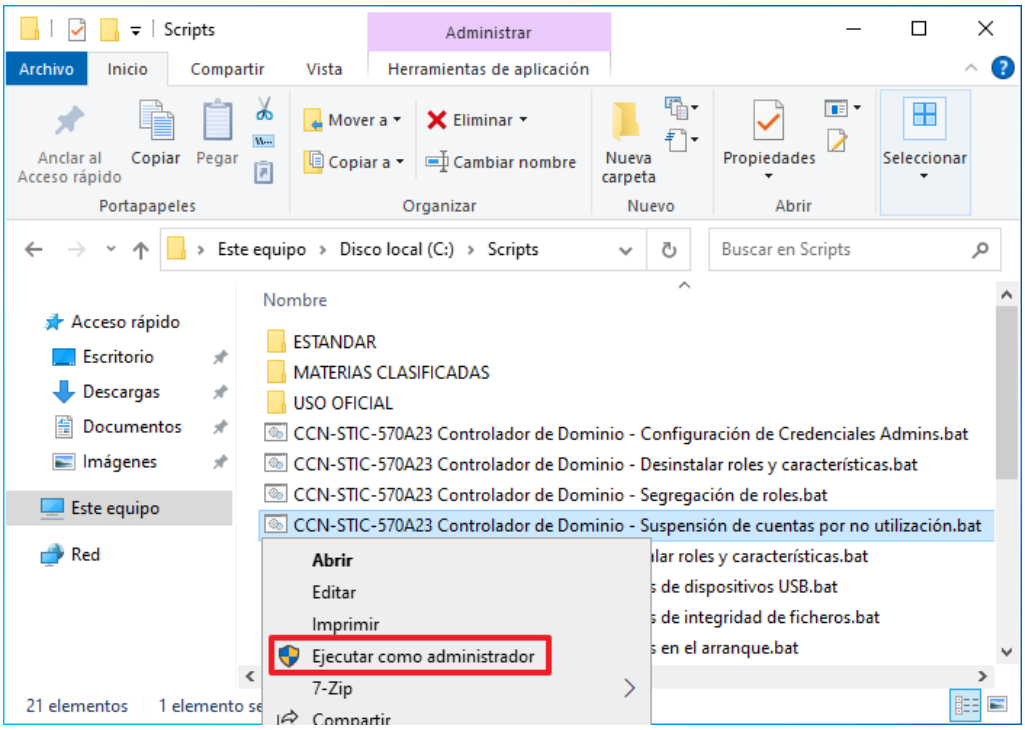
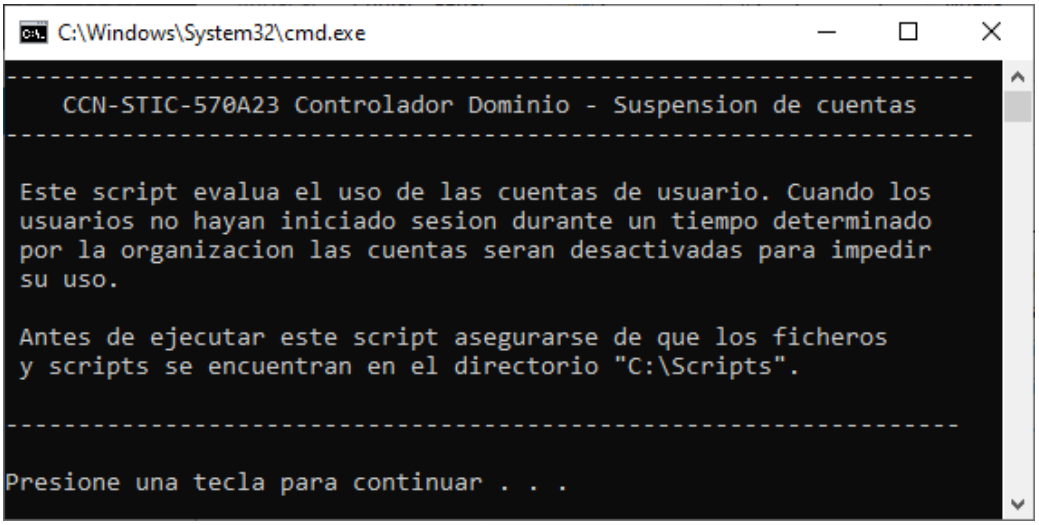
ANEXO A.2.5. MECANISMOS DE AUTENTICACIÓN (USO OFICIAL – MATERIAS CLASIFICADAS)

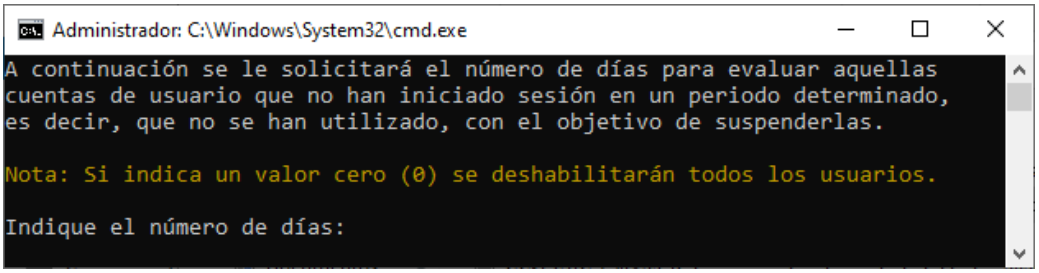
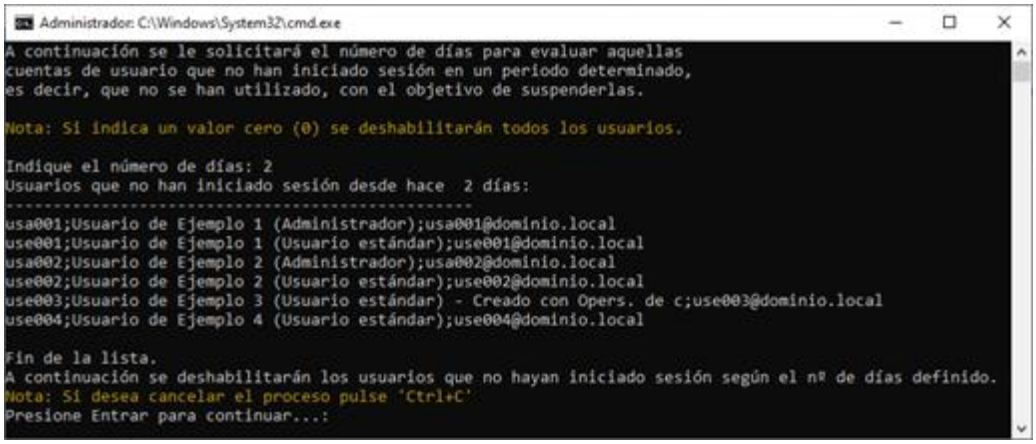
El presente punto tiene como objetivo ayudar a los administradores del sistema operativo a evaluar el estado de las cuentas de los diferentes usuarios. Cuando existan cuentas, tanto que ya hayan iniciado sesión, como cuentas nuevas que nunca lo hayan hecho, será necesario comprobar su uso en el tiempo de modo que tras un periodo de no uso determinado por la organización, dichas cuentas sean deshabilitadas.

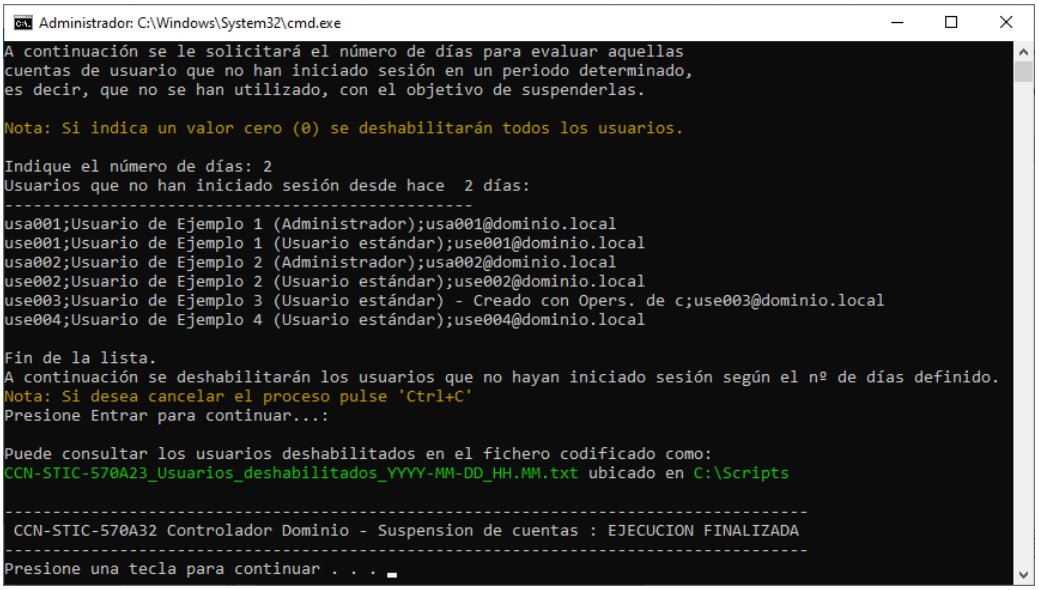
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

A continuación, se definen los pasos para llevar a efecto la labor indicada con anterioridad.

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

Paso	Descripción
175.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-570A23 Controlador de Dominio –Suspensión de cuentas por no utilización.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
176.	Pulse cualquier tecla para continuar. 

Paso	Descripción
177.	A continuación, deberá introducir un número de días, los cuales determinarán que todas las cuentas de usuario que no hayan iniciado sesión en los días indicados queden deshabilitadas. El número de días introducido se adaptará a la política de la organización. Se tendrán en cuenta tanto cuentas que ya hayan iniciado sesión, como cuentas creadas, en las cuales no se ha iniciado sesión, y se omitirán aquellas cuentas por defecto del sistema operativo que no requieran este control. Pulse "Enter" cuando haya indicado el número.  **Nota:** El número indicado deberá ser determinado por la organización en función de su política de seguridad. Noventa (90) días, es decir, tres (3) meses, se define como un valor recomendado a utilizar.
178.	Tras la ejecución se informará al usuario de las cuentas que han sido deshabilitadas y se habrá generado un fichero en el directorio "C:\Scripts" a modo de registro. Pulse de nuevo la tecla "Enter" para continuar la ejecución del script.  **Nota:** Para este paso a paso se han creado usuarios de ejemplo y se ha indicado un número que permita mostrar usuarios coincidentes con la necesidad.

Paso	Descripción
179.	Cuando la ejecución haya finalizado pulse cualquier tecla para finalizar. 
180.	Tenga en consideración que la ejecución de este script podrá ser automatizada por medio de las diferentes herramientas de los sistemas operativos de modo que no sea necesario realizar su ejecución de una forma periódica por un administrador. **Nota:** No es objeto del presente documento la automatización o definición de procesos de evaluación periódicos en la organización.

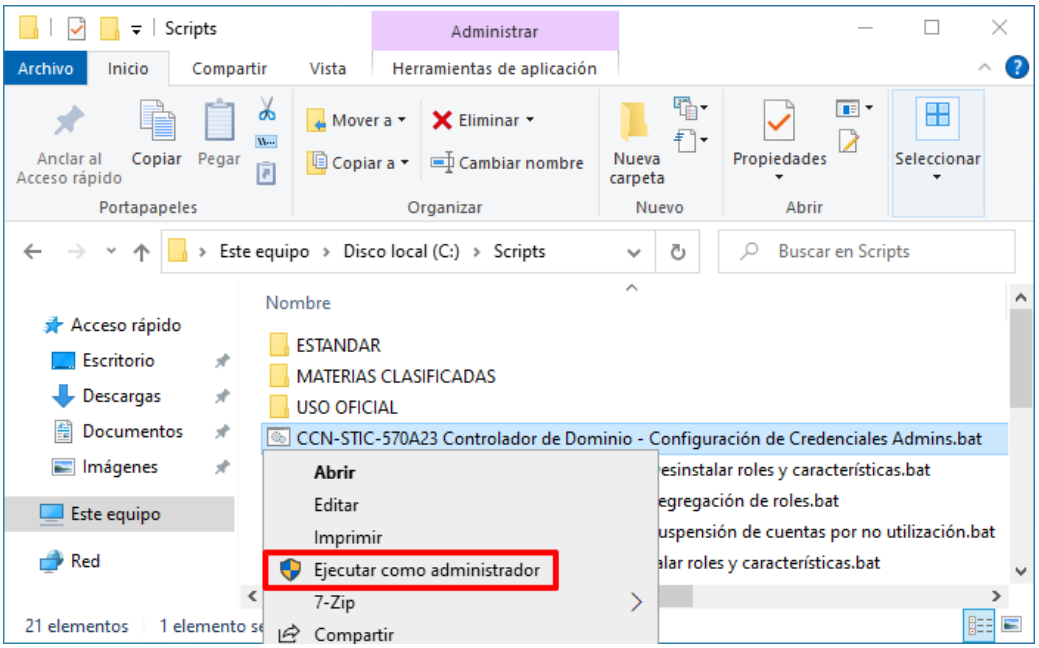
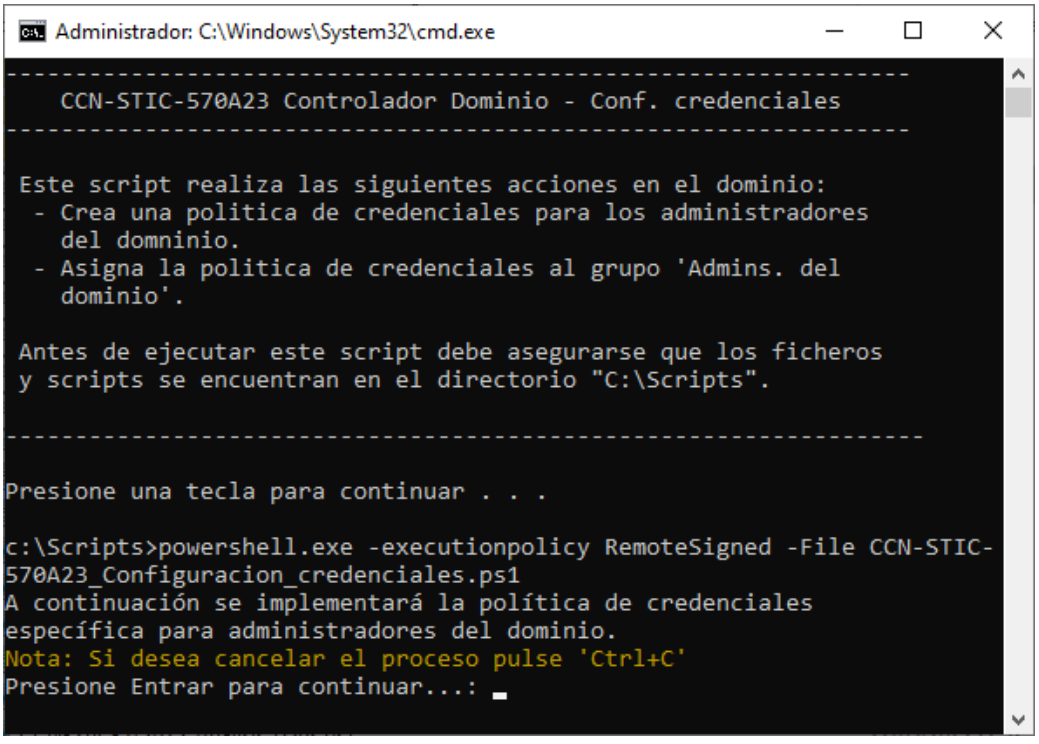
ANEXO A.2.5.1. MECANISMOS DE AUTENTICACIÓN (MATERIAS CLASIFICADAS)

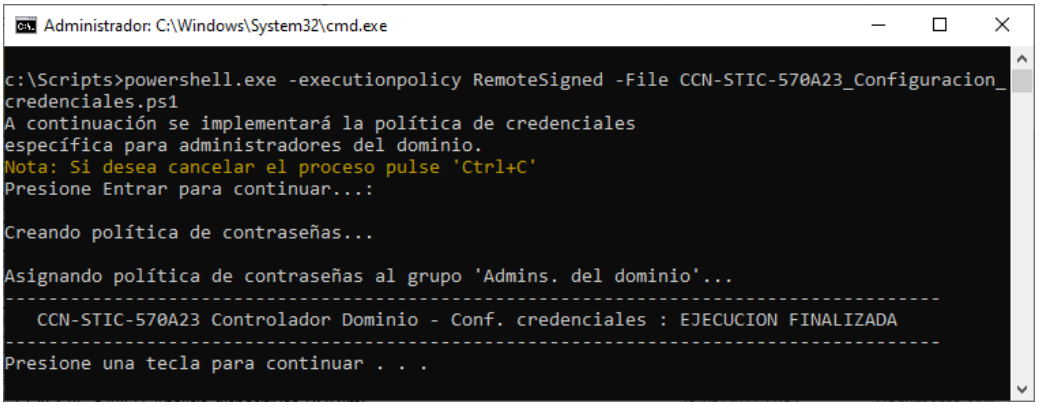
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso del perfil MATERIAS CLASIFICADAS.

A continuación, se definirán los pasos que permitan a los administradores establecer una política de credenciales específica para los administradores del dominio la cual es más estricta dados los privilegios que este tipo de cuentas poseen.

Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Materias Clasificadas**, no siendo obligatorio en ningún otro perfilado.

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

Paso	Descripción
182.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-570A23 Controlador de Dominio –Configuración de Credenciales Admins.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
183.	Pulse cualquier tecla para continuar y pulse la tecla “Enter” para dar comienzo al proceso y espere a que finalice. 

Paso	Descripción
184.	Cuando haya finalizado la ejecución del script pulse cualquier tecla para finalizar. 

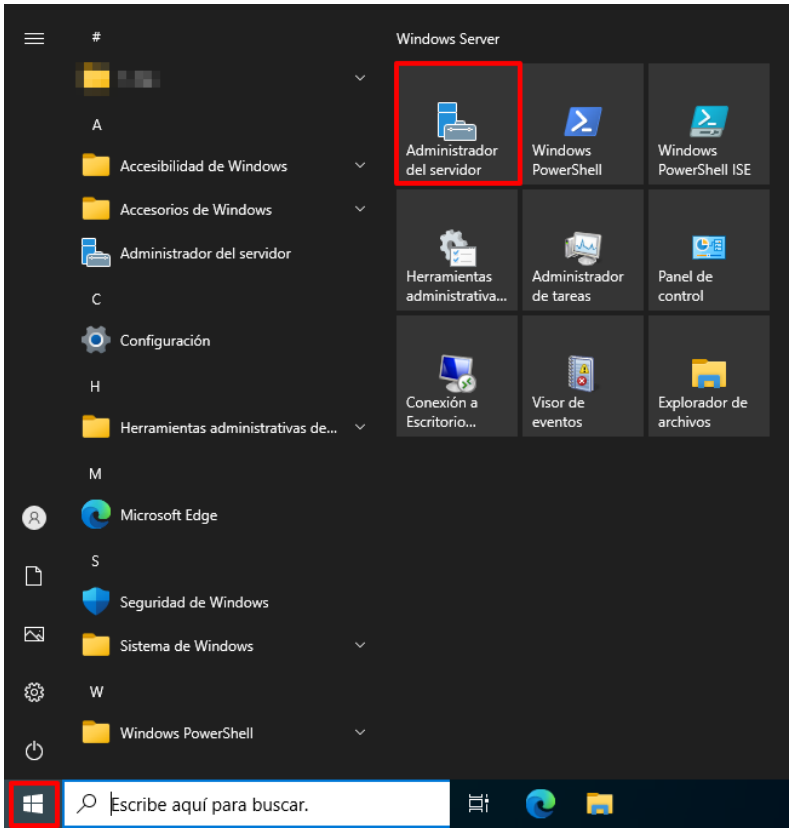
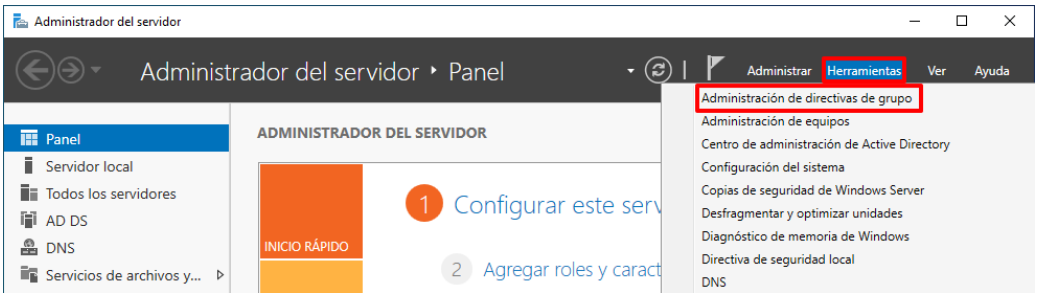
ANEXO A.3. CONFIGURACIÓN DE SEGURIDAD EN SERVIDOR MIEMBRO

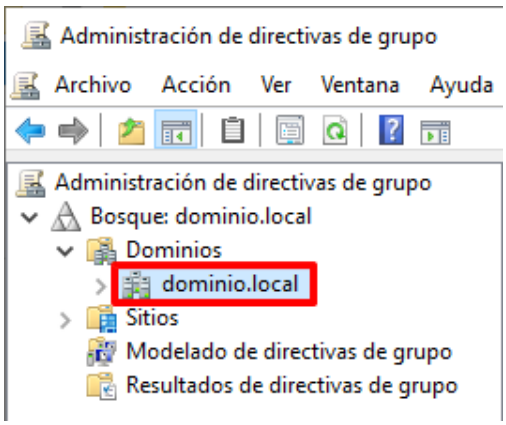
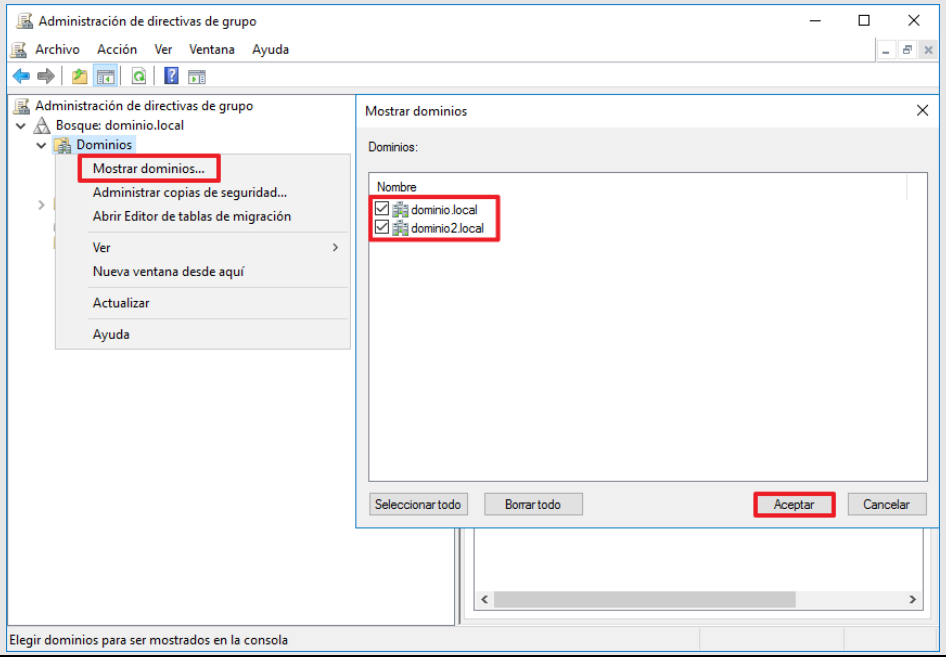
Una vez realizada la preparación de la configuración de seguridad necesaria a implementar, será necesario su aplicación sobre los objetos correspondientes, así como la ejecución de labores adicionales para cubrir todos los aspectos necesarios de seguridad.

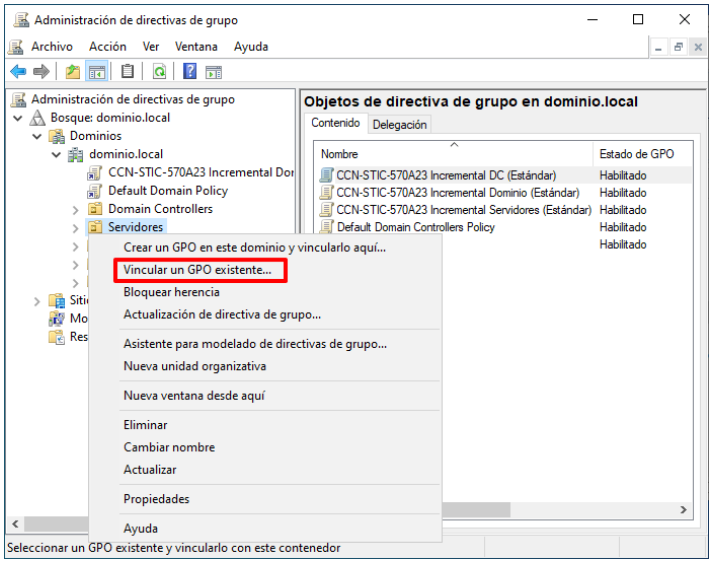
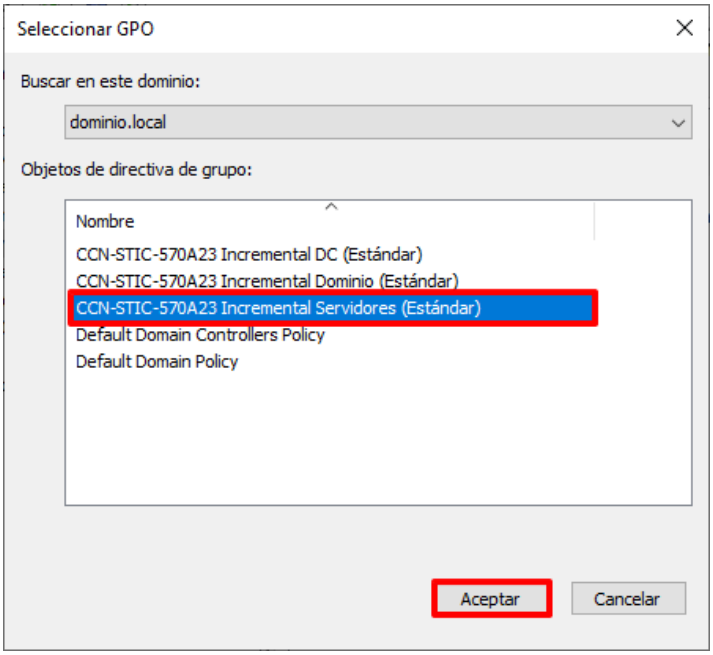
ANEXO A.3.1. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

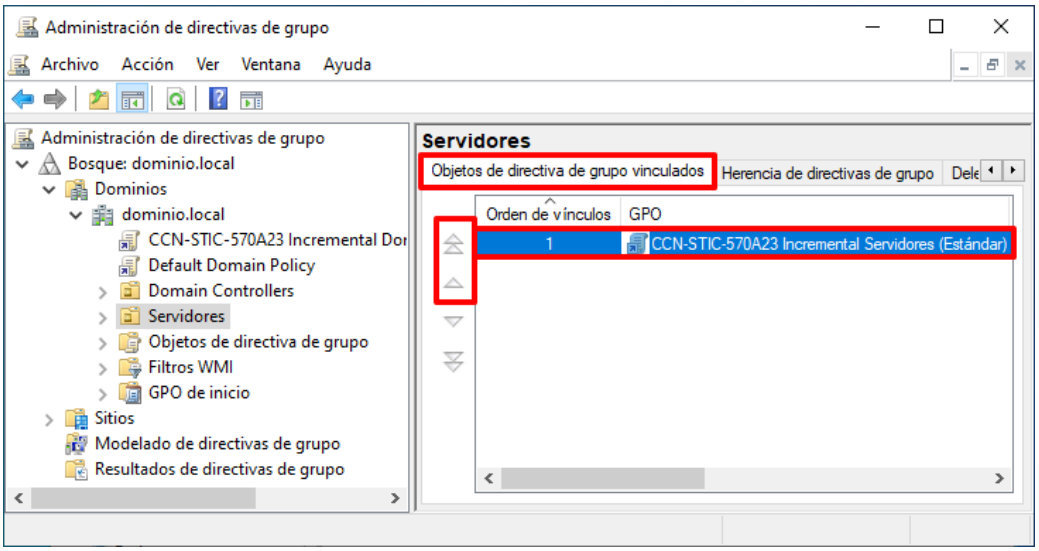
A continuación, se definen los pasos a seguir para la adecuada aplicación de las políticas generadas en el punto anterior para aplicar la configuración de seguridad sobre los objetos de tipo Servidor Miembro, pertenecientes al dominio. Solo es necesario realizar este procedimiento una (1) vez.

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

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

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

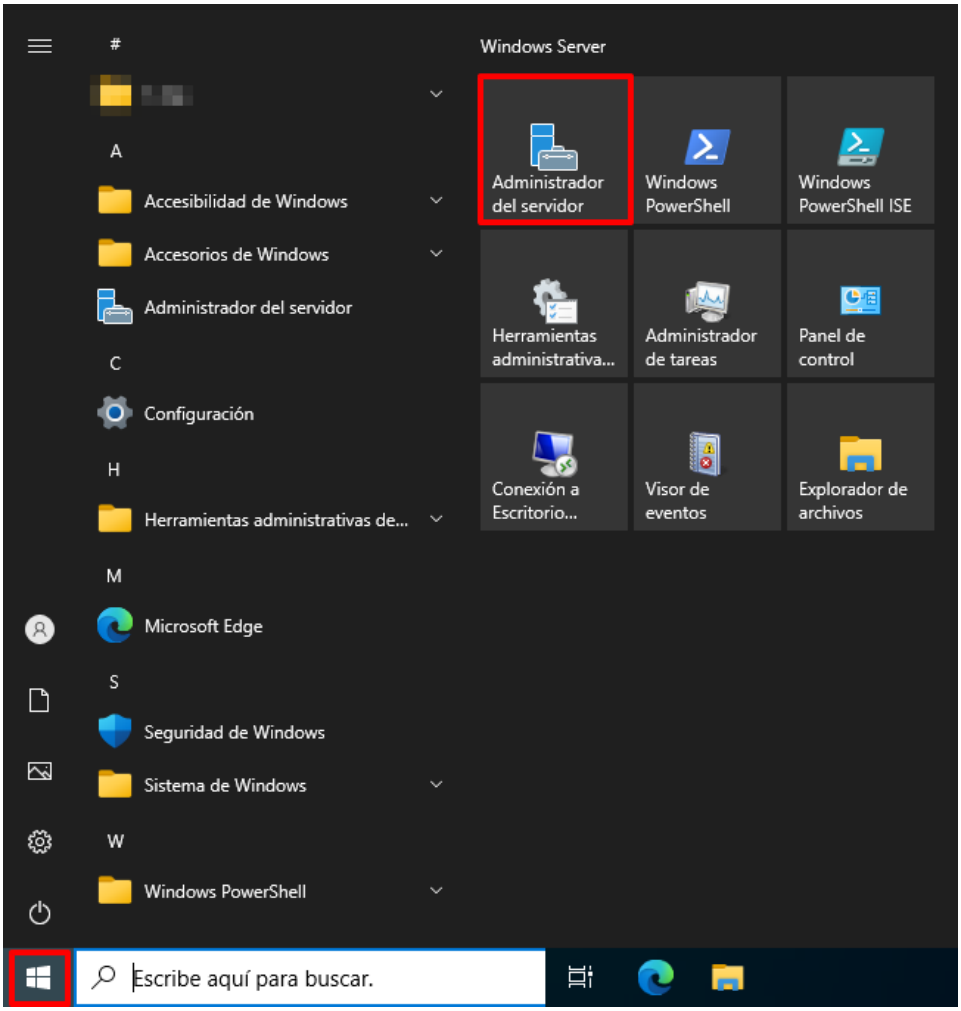
Paso	Descripción
5.	Identifique aquellas unidades organizativas donde se alojen aquellos objetos de tipo servidor que se pretenden asegurar, y haciendo clic derecho sobre el contenedor seleccione la opción del menú contextual "Vincular un GPO existente…".  **Nota:** En este ejemplo se hace uso de la unidad organizativa "Servidores" creada para alojar los objetos de tipo servidor miembro del dominio. Deberá adaptar este paso a las necesidades de su organización.
6.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])" y pulse "Aceptar".  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

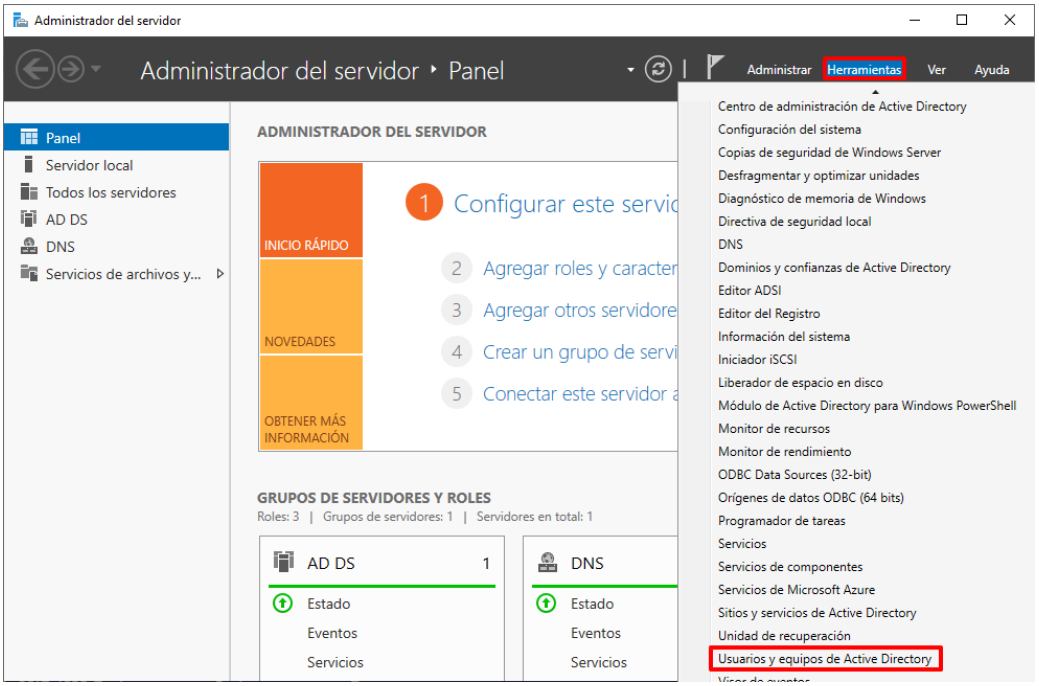
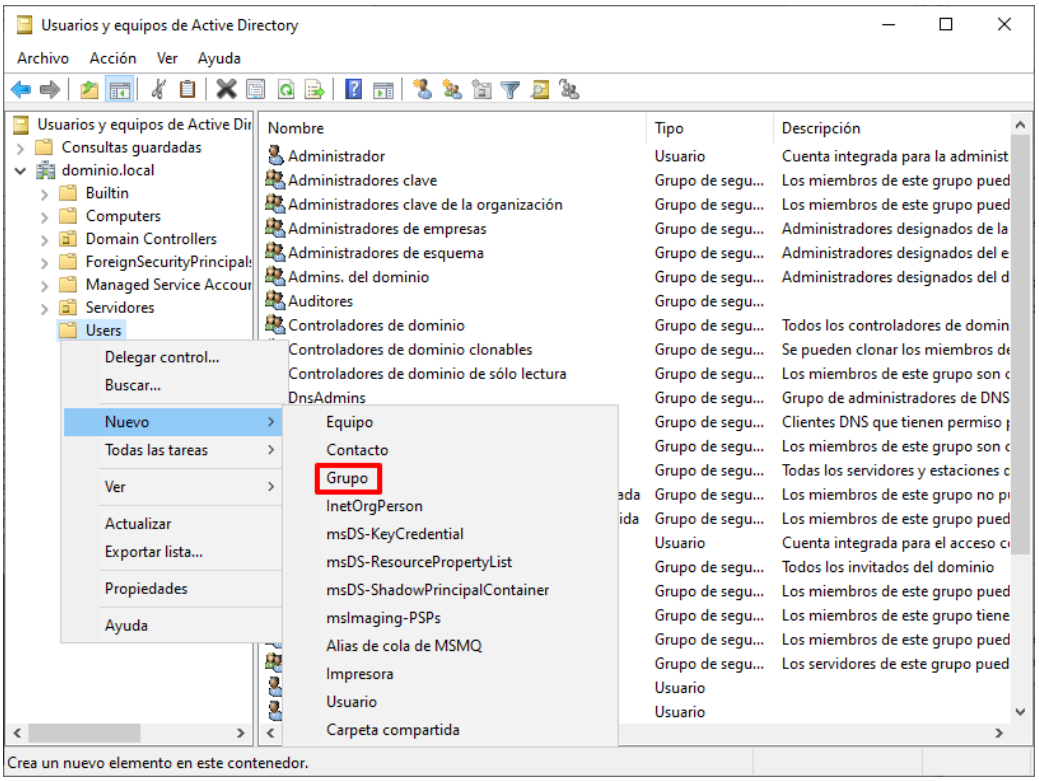
Paso	Descripción
7.	Seleccione el contenedor sobre el que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 
8.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

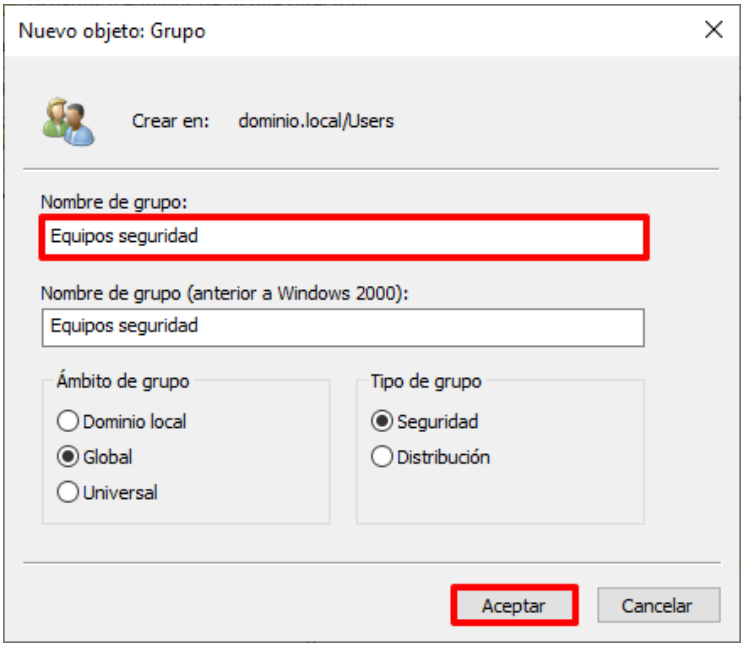
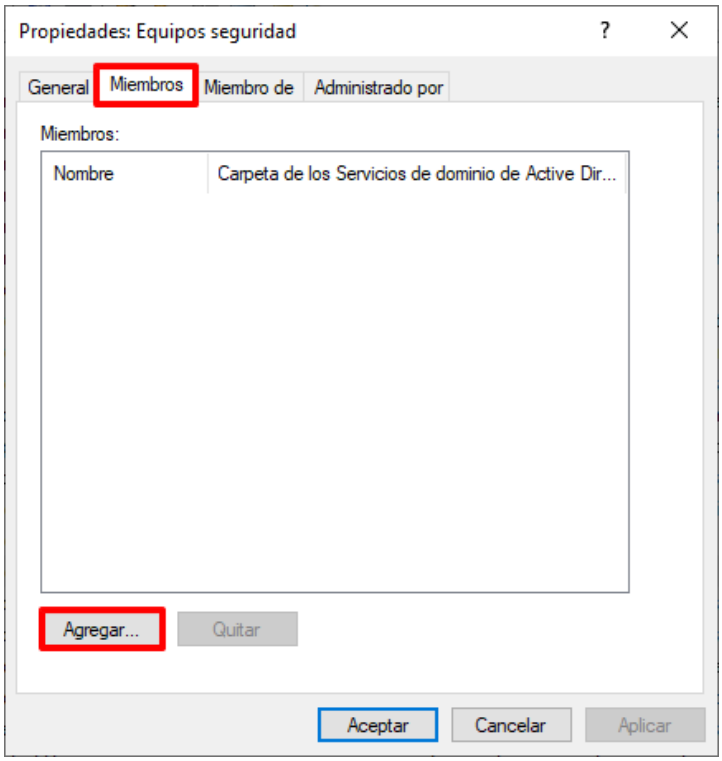
ANEXO A.3.2. FILTRADO DE SEGURIDAD DE OBJETOS GPO

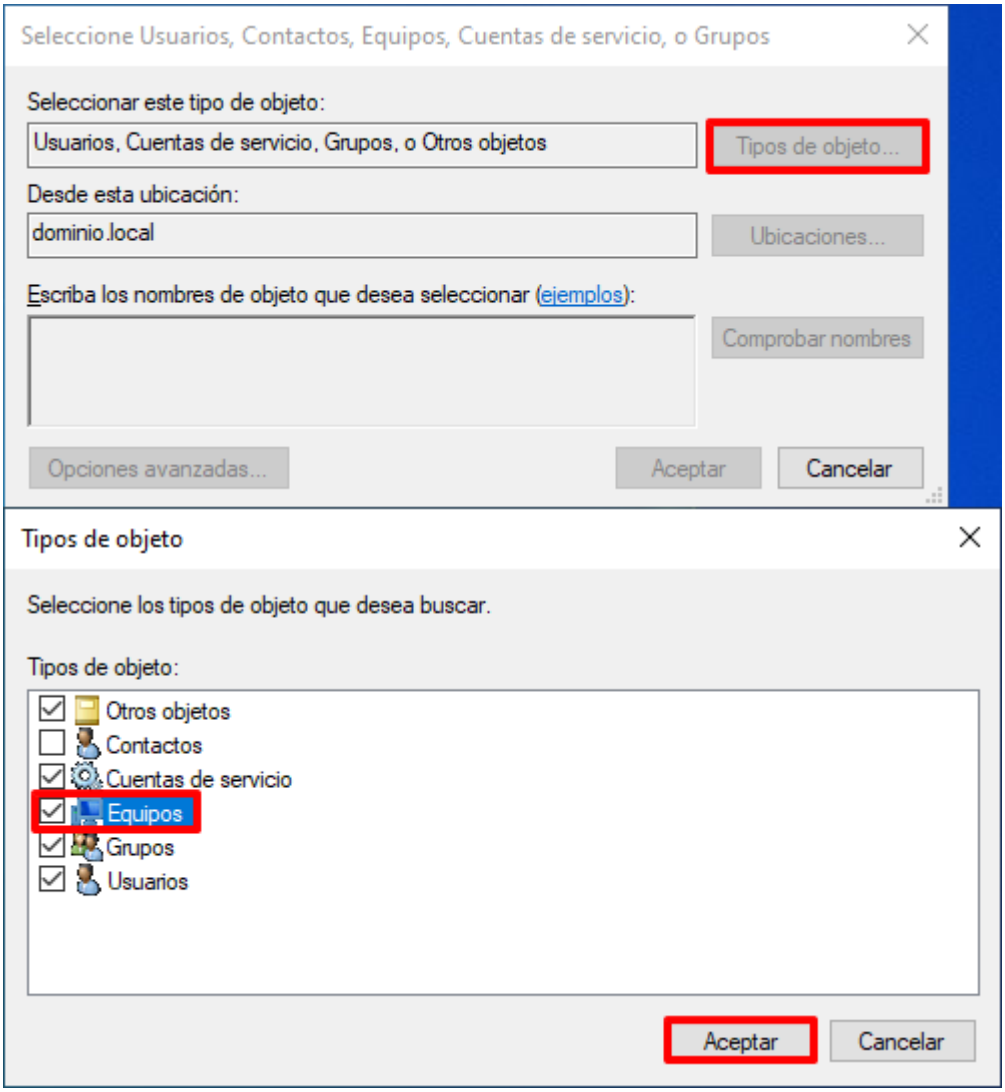
El presente apartado tiene como objetivo realizar una creación de un grupo de seguridad sobre el que aplicar el objeto GPO. Esto permitirá que solo se aplique el objeto GPO a los objetos incluidos dentro de dicho grupo, aunque en la unidad organizativa que se aplica el objeto GPO existan más objetos.

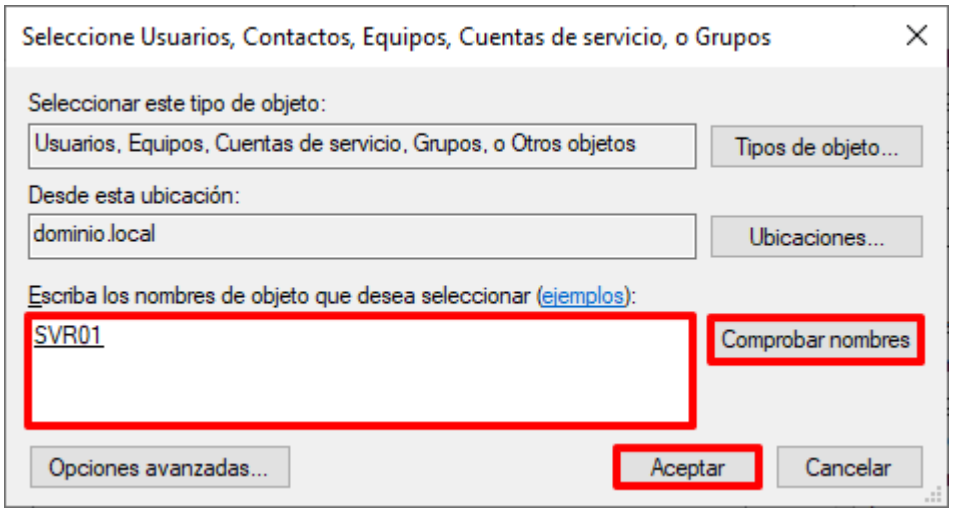
Nota: Estos pasos son opcionales y solo en caso de hacer uso de este tipo de filtrado para la aplicación de objetos GPO.

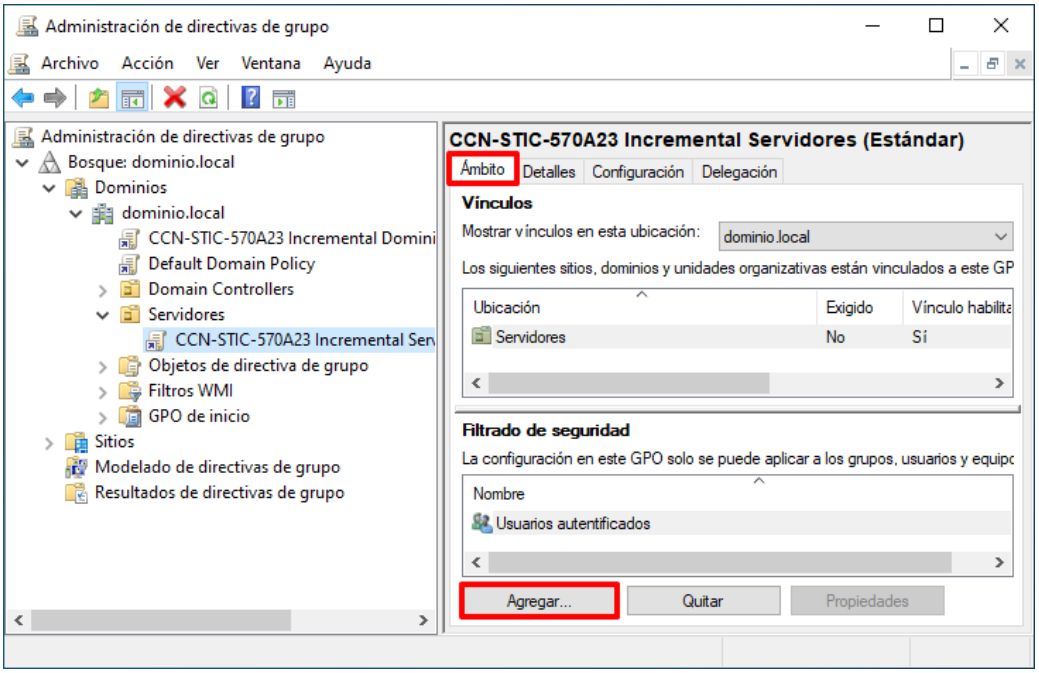
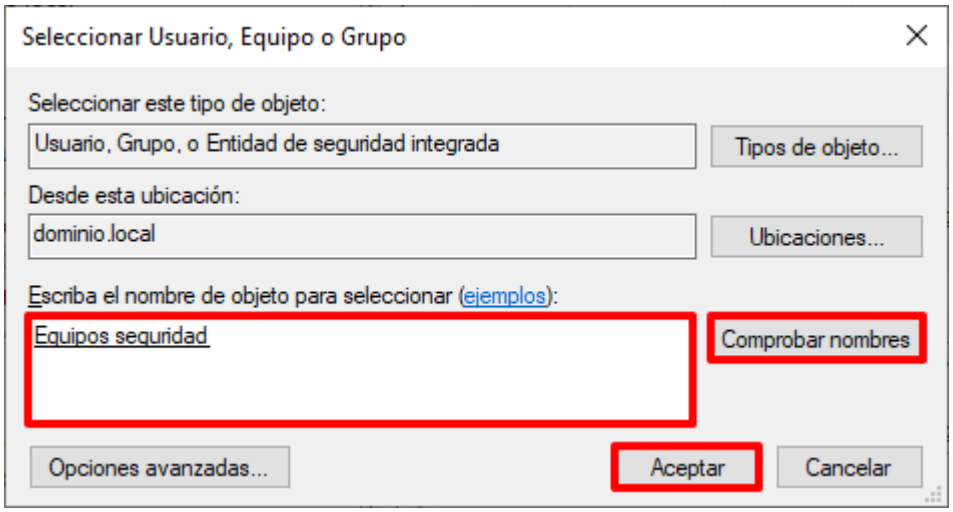
Paso	Descripción
9.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
10.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.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

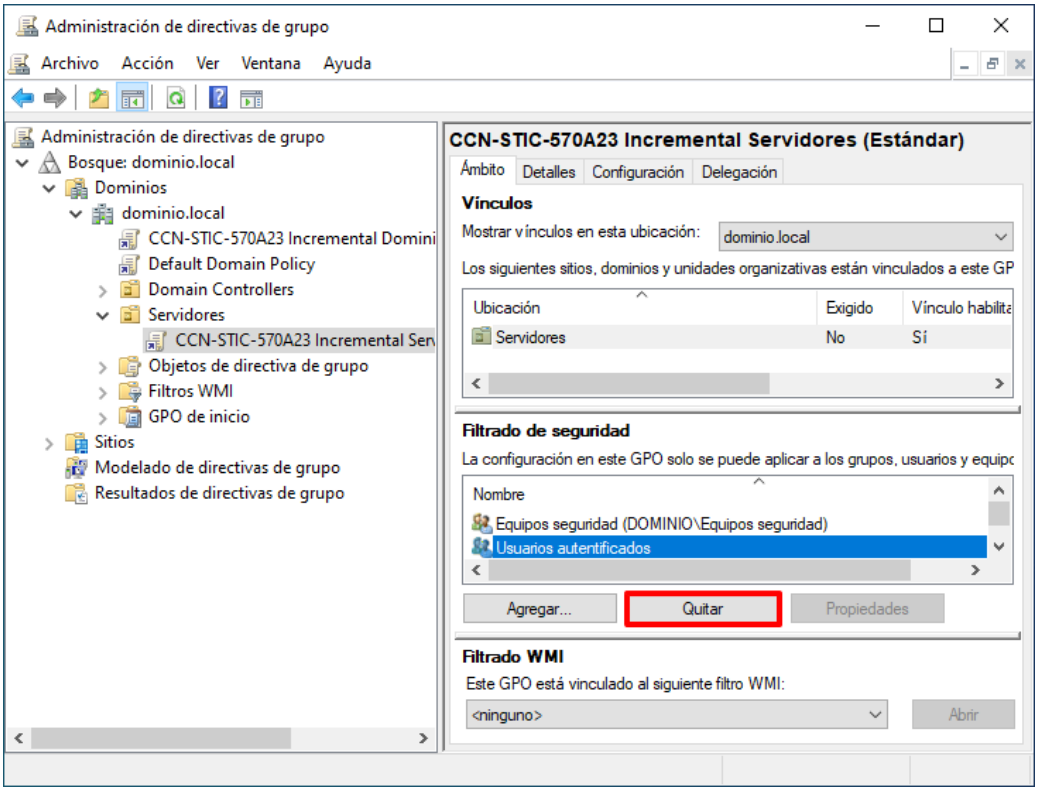
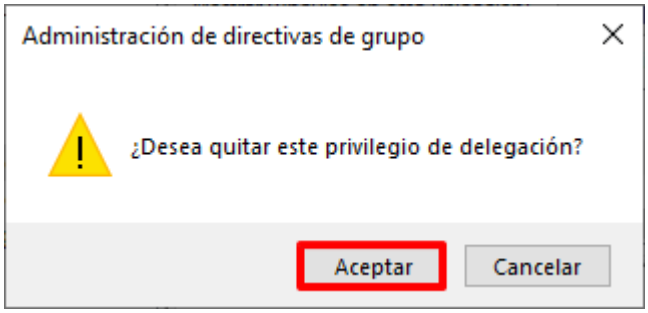
Paso	Descripción
11.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Usuarios y equipos de Active Directory”. 
12.	En la consola “Usuarios y equipos de Active Directory”, despliegue y seleccione el nodo “<nombre de su dominio> → Users” y haciendo clic derecho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

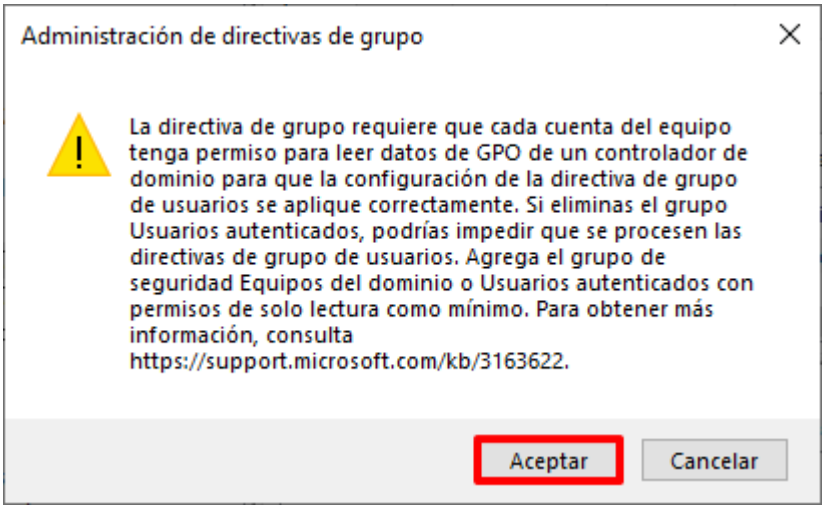
Paso	Descripción
13.	En la ventana “Nuevo objeto: Grupo”, indique el nombre del grupo y pulse “Aceptar”  **Nota:** En este ejemplo se ha hecho uso del nombre “Equipos seguridad”.
14.	Haga doble clic sobre el grupo recién creado y sobre la ventana “Propiedades: [GRUPO CREADO]” acceda a la pestaña “Miembros”.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

Paso	Descripción
15.	Pulse en la nueva ventana emergente sobre “Tipos de objeto…” y marque la opción “Equipos”. Pulse “Aceptar” para continuar. 

Paso	Descripción
16.	Incluya los equipos los cuales desea agregar al grupo separados por punto y coma (;). Haga uso del botón "Comprobar nombres" para completar la información del equipo y pulse "Aceptar".  **Nota:** Para este ejemplo se ha hecho uso del objeto de tipo equipo "SVR01". Deberá reiniciar los equipos incluidos en el grupo para que estos adquieran la membresía de grupo necesaria.
17.	A continuación, sobre la consola "Administración de directivas de grupo", diríjase a la unidad organizativa donde se encuentra vinculado el objeto GPO el cual se desea filtrar y selecciónelo. **Nota:** Para este ejemplo se hace uso del objeto GPO "CCN-STIC-570A23 Incremental Servidores (Estándar)".

Paso	Descripción
18.	En el panel derecho, seleccione la pestaña ámbito y en el apartado “Filtrado de seguridad” pulse sobre “Agregar…”. 
19.	En la ventana que se abrirá, incluya el grupo creado con anterioridad. Haga uso del botón “Comprobar nombres” para completar la información del grupo y pulse “Aceptar”. 

Paso	Descripción
20.	Posteriormente sobre el mismo apartado seleccione “Usuarios autentificados” y pulse sobre el botón “Quitar”. 
21.	Pulse sobre el botón “Aceptar” en el mensaje de advertencia. 

Paso	Descripción
22.	Pulse de nuevo sobre el botón “Aceptar” ante el siguiente mensaje de advertencia. 

ANEXO A.3.3. CONFIGURACIÓN DE SEGURIDAD

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

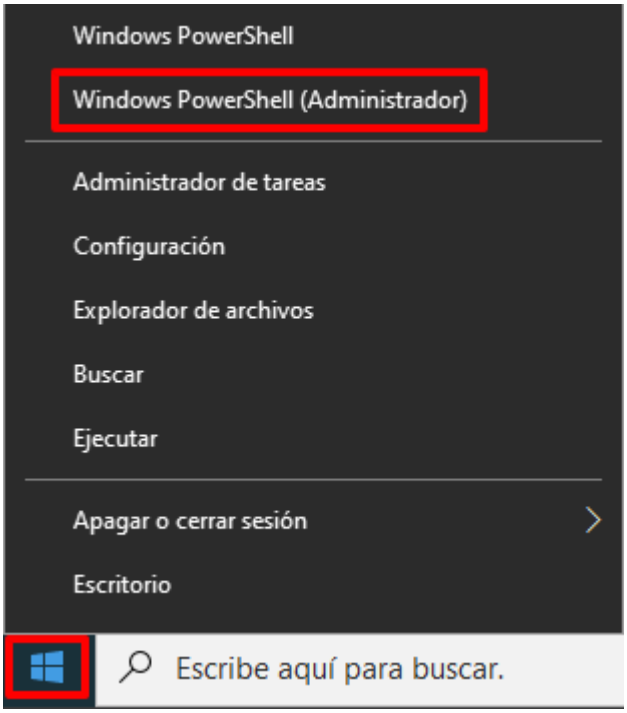
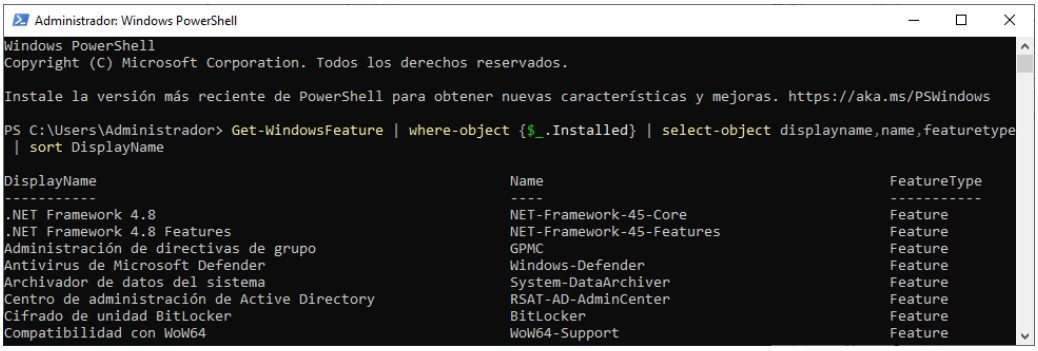
Para lograr el objetivo anterior se describen dos alternativas:

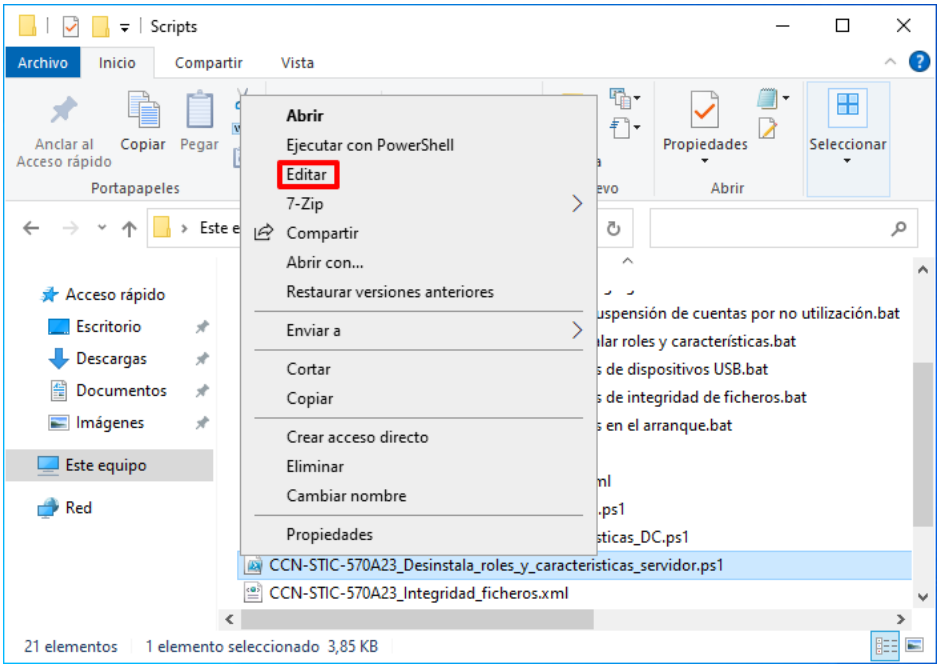
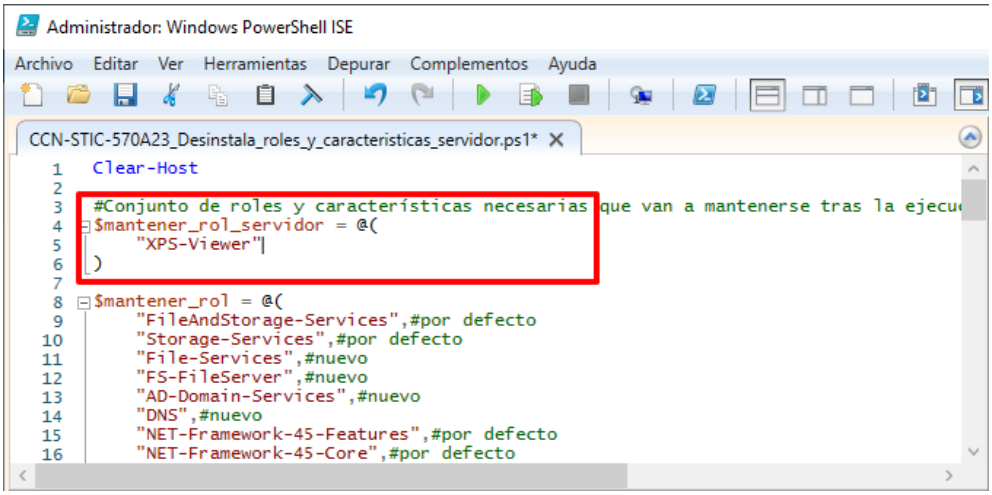
a) Por un lado, se facilitará un script que permita desinstalar aquellos roles y características consideradas no necesarias dentro de un equipo de tipo Servidor Miembro de un dominio.

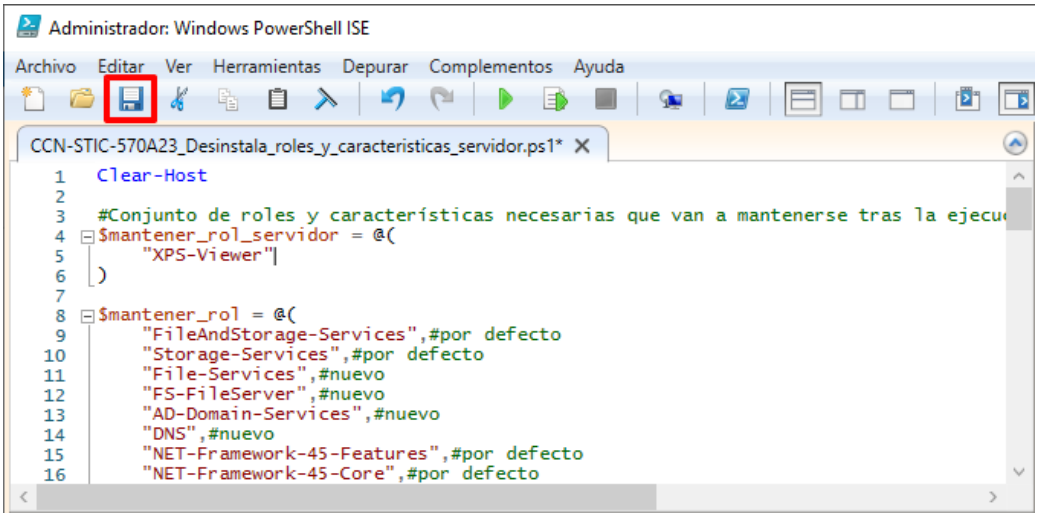
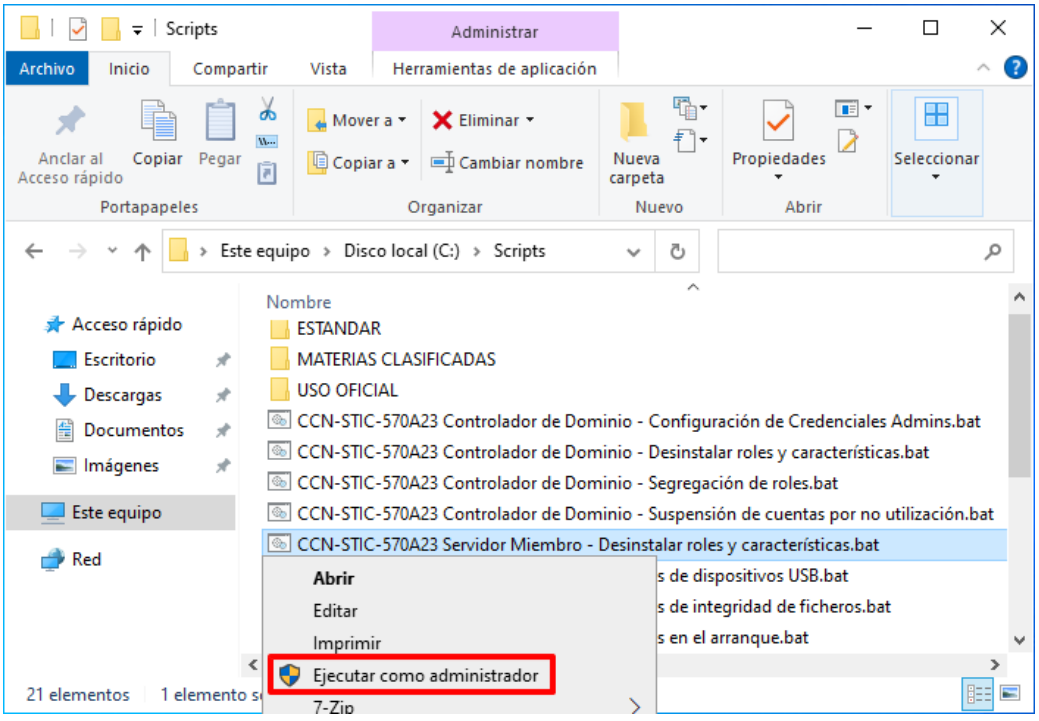
b) Por otra parte, se facilitará un paso a paso con información sobre como desinstalar roles y/o características de forma gráfica y manual.

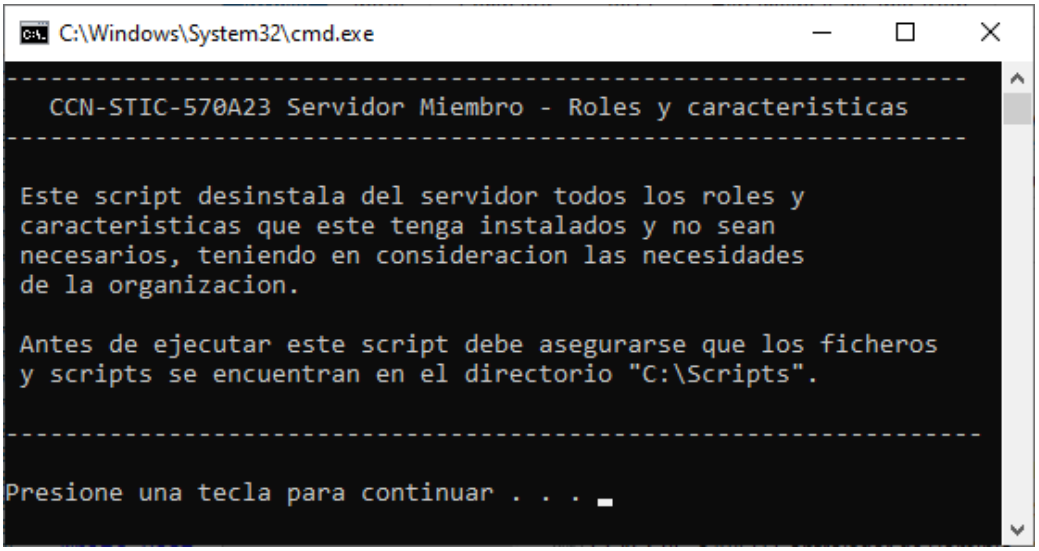
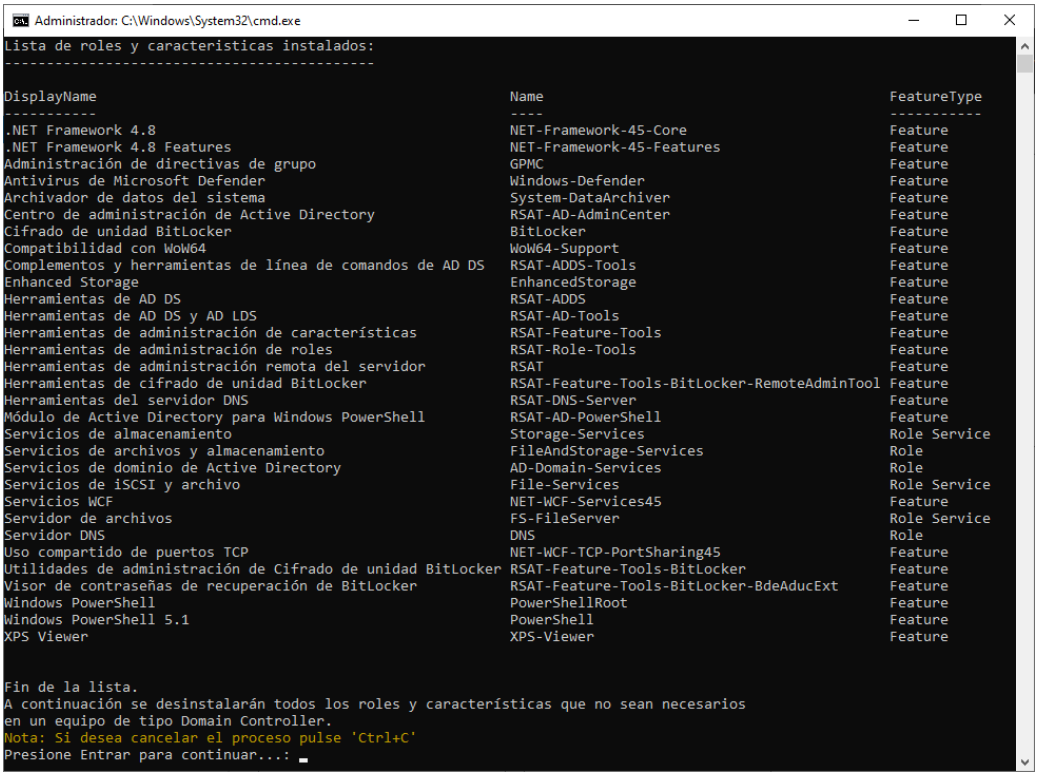
Nota: Si desea solo ejecutar esta acción de forma manual, vaya al “Paso 36” de este apartado.

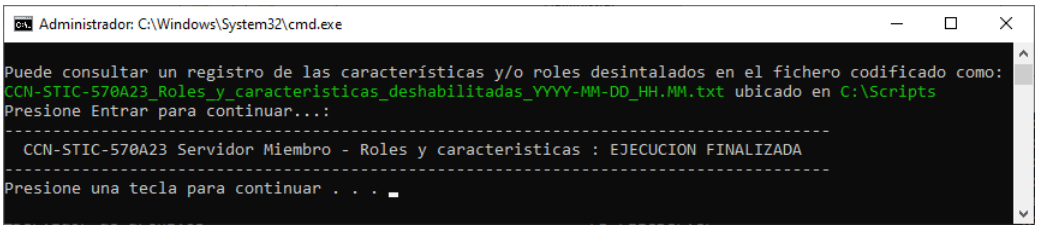
Paso	Descripción
23.	Inicie sesión en un servidor miembro del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
24.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Windows PowerShell (Administrador)”. 
25.	En la consola de PowerShell ejecute el siguiente comando para conocer aquellos roles y características instaladas en el equipo. > Get-WindowsFeature | Where-Object {$_.Installed} | Select-Object DisplayName,Name,FeatureType | Sort DisplayName  **Nota:** Puede redirigir la salida del comando a un fichero si lo desea con el objetivo de evaluar mejor la información mostrada.
26.	A continuación, **EVALÚE** y **DETERMINE** aquellos roles y características **QUE NO SON NECESARIAS ELIMINAR** y anótelos. Deberá anotar los elementos ubicados en la columna “Name”.

Paso	Descripción
27.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-570A23_Desinstala_roles_y_caracteristicas_servidor.ps1” y seleccione la opción del menú contextual “Editar”. Con ello se abrirá una ventana de Windows PowerShell ISE. 
28.	Dentro de la ventana de PowerShell ISE, al inicio del script identifique la línea donde se indica “$mantener_rol_servidor”. Dentro de la citada línea deberá incluir aquellos roles y características anotadas en pasos anteriores. Deberá **incluir los nombres entre comillas (“”) y separados por comas**.  **Nota:** En este ejemplo se ha incluido la característica “XPS-Viewer”. Tenga en consideración que ya existen otros roles y/o características que ya han sido determinadas como necesarias y no se desinstalarán.

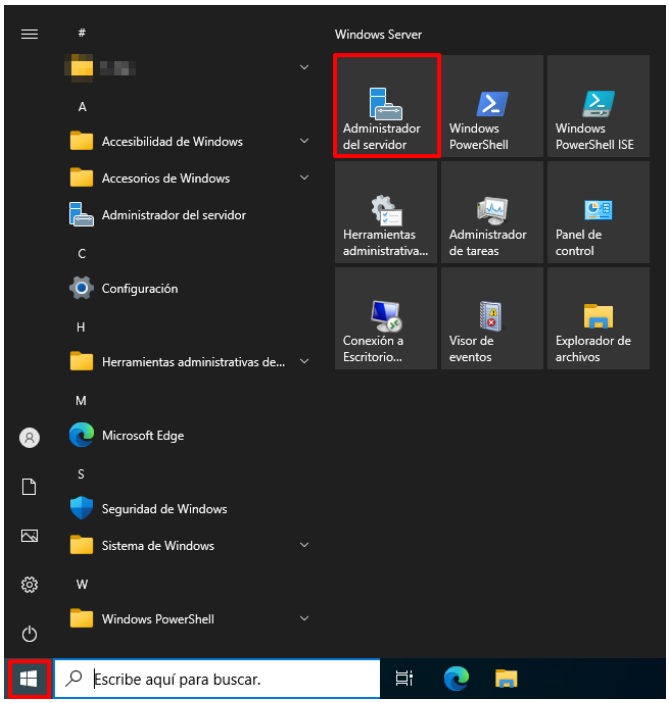
Paso	Descripción
29.	Cuando haya finalizado pulse sobre el botón “Guardar” en la parte superior izquierda. 
30.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-570A23 Servidor Miembro – Desinstalar roles y características.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 

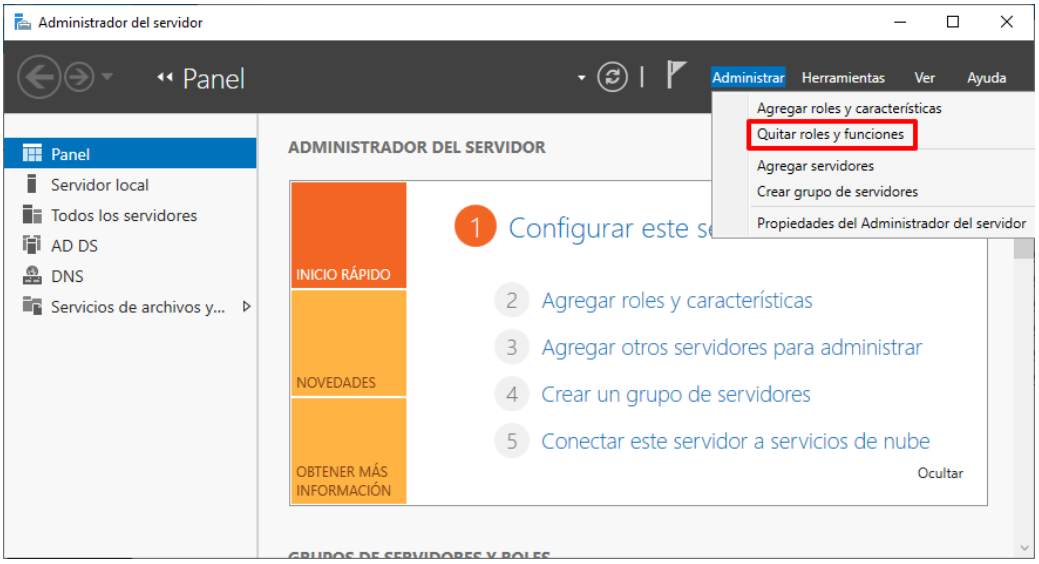
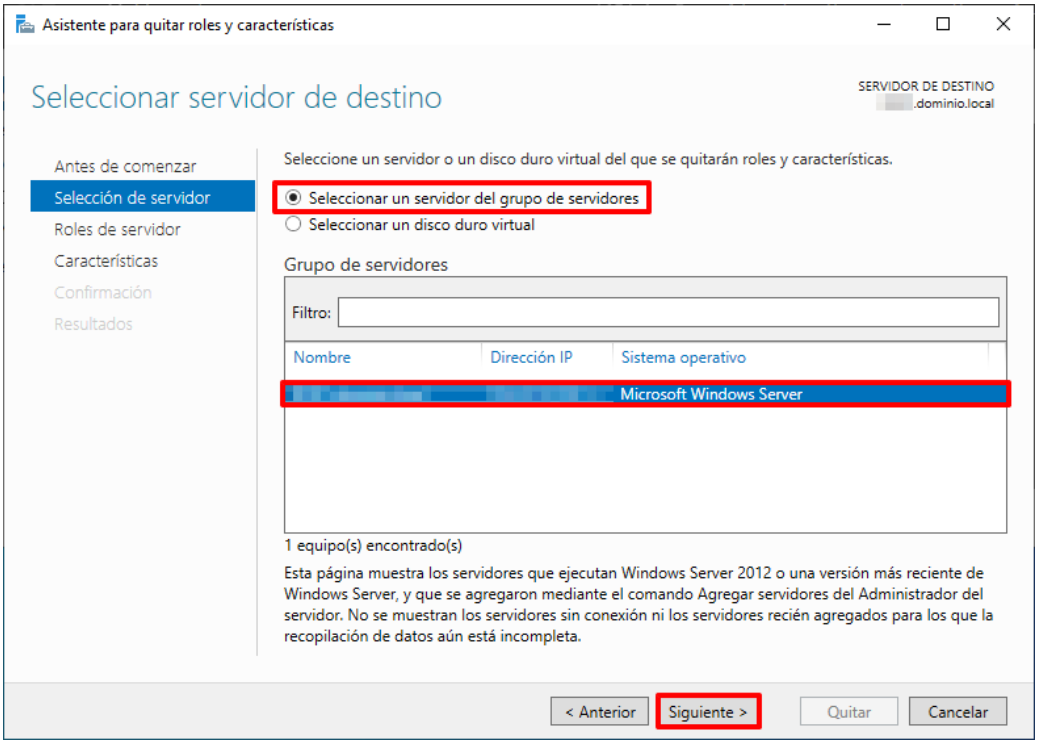
Paso	Descripción
31.	Pulse cualquier tecla para continuar. 
32.	A continuación, se recopilará y mostrarán los roles y características instalados en el equipo. Deberá pulsar la tecla “Enter” para continuar y dar comienzo a la desinstalación de los roles y características no necesarias. 
33.	Cuando el proceso haya finalizado, podrá evaluar las características y roles desinstalados. Pulse de nuevo la tecla “Enter” para continuar.

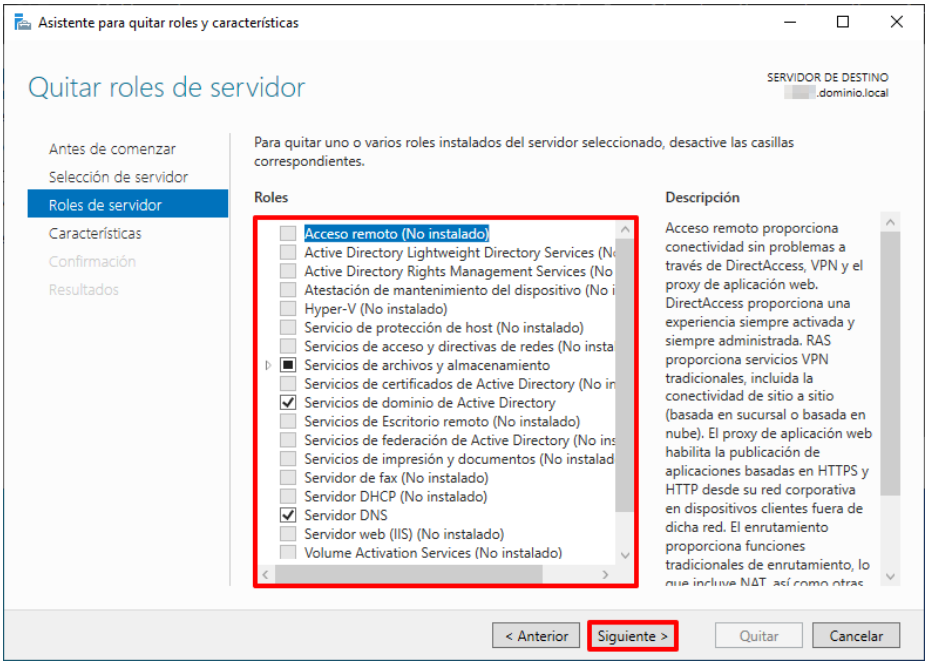
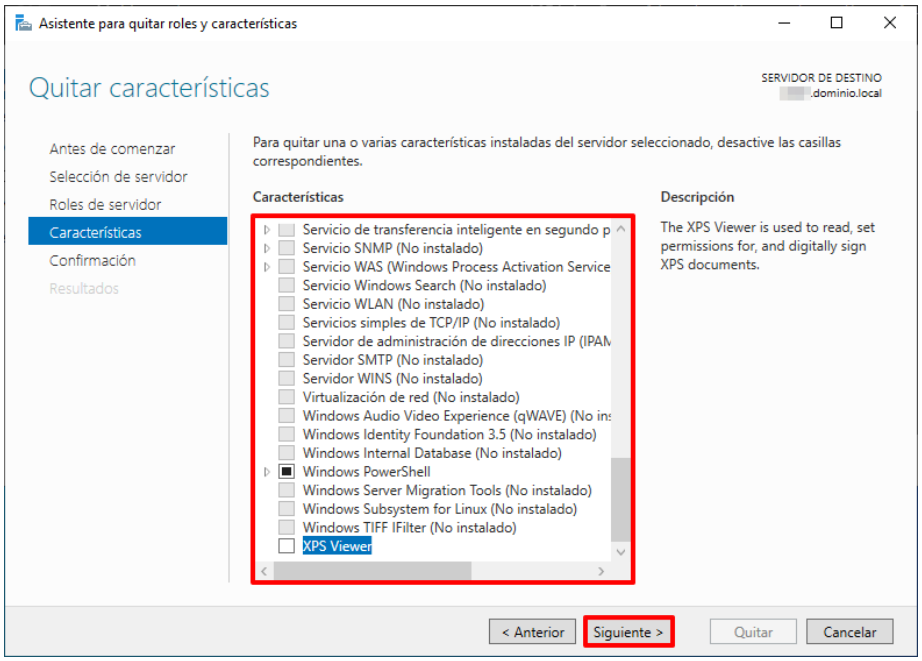
Paso	Descripción
34.	El servidor se reiniciará a continuación para asegurar la adecuada desinstalación de roles y/o características. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
35.	Con esto se habrá finalizado la eliminación de roles y características no necesarias en un equipo de tipo Servidor Miembro.

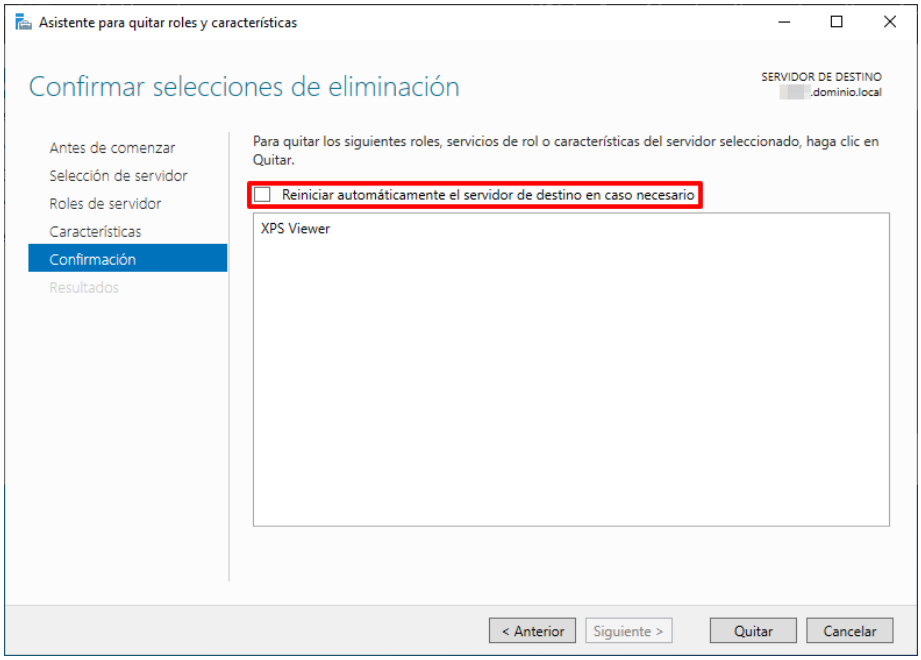
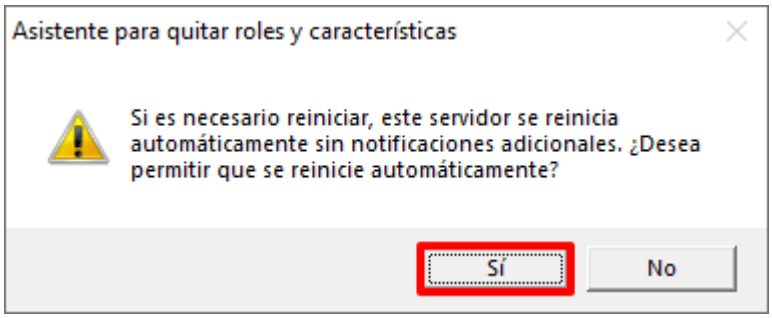
A continuación, se describen los pasos para realizar una desinstalación manual de roles y/o características implementadas en un equipo de tipo Servidor Miembro.

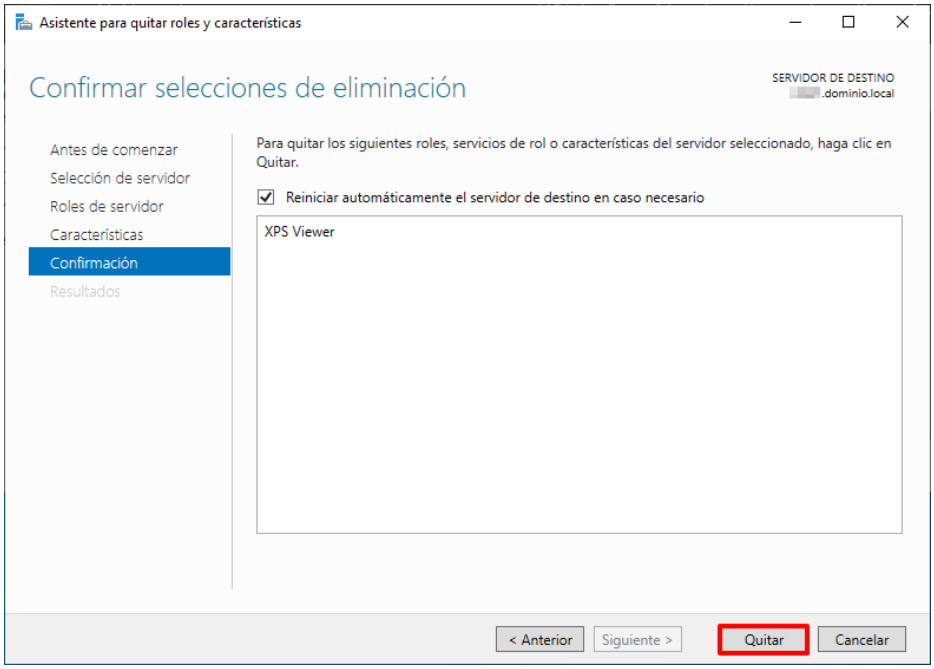
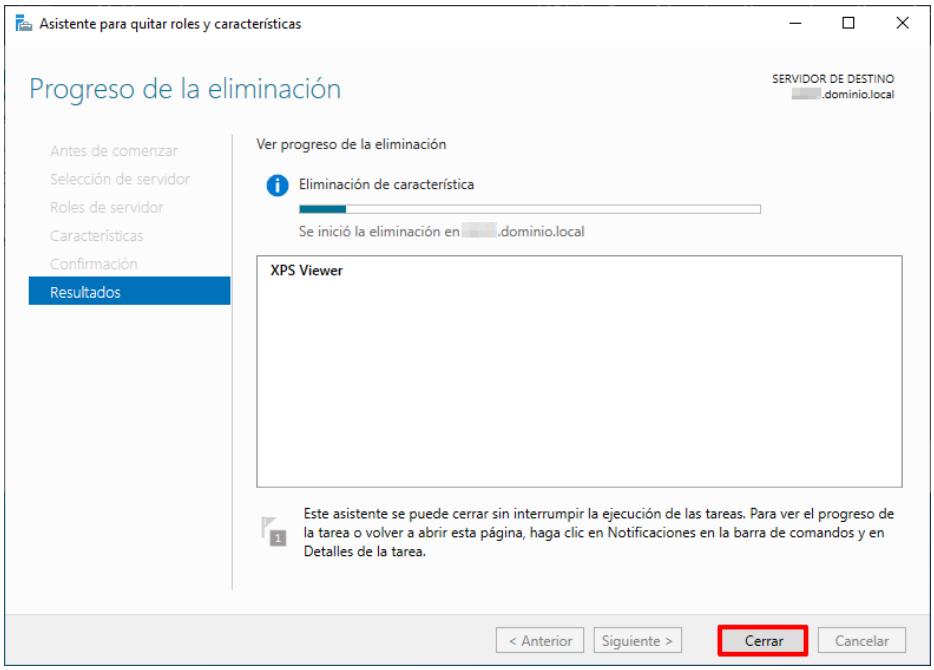
Nota: Para este ejemplo se desinstalará el visor XPS.

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

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

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

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

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

ANEXO B. CONFIGURACIONES ADICIONALES

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

ANEXO B.1. ACCESO REMOTO

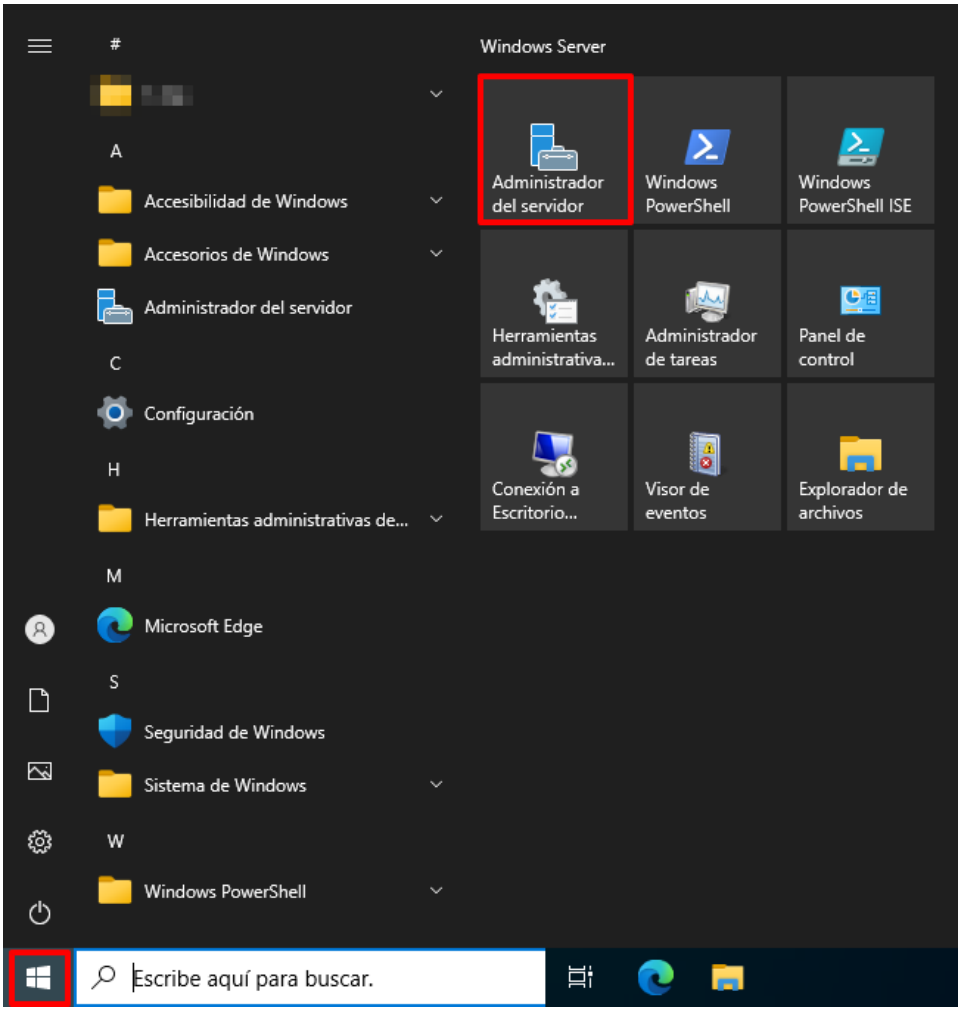
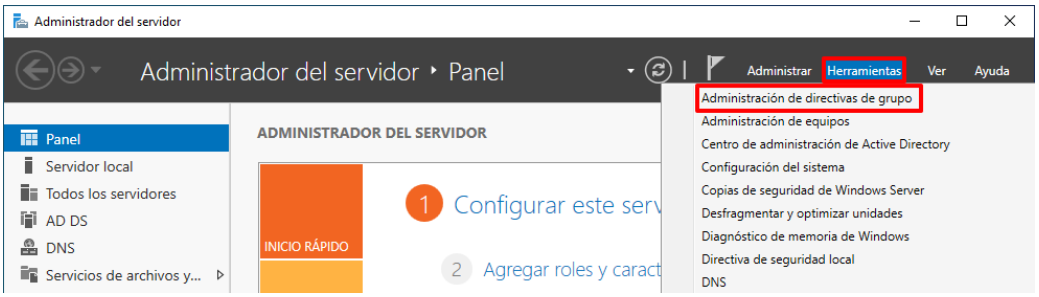
El objetivo del siguiente apartado tiene como misión establecer las configuraciones adecuadas sobre aquellos elementos a los que se les esté permitido el acceso remoto por medio de los elementos nativos de Windows. En este caso se hace referencia a Remote Desktop Connection (RDP).

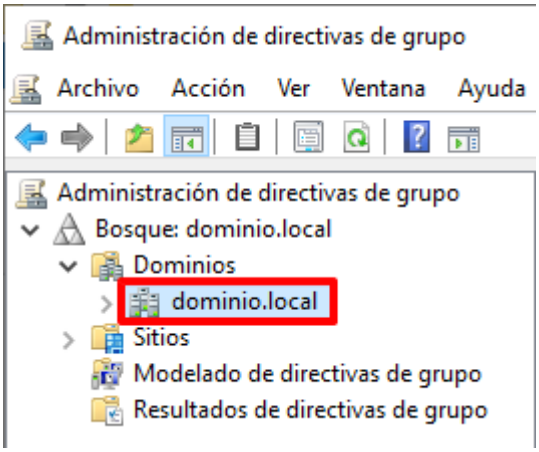
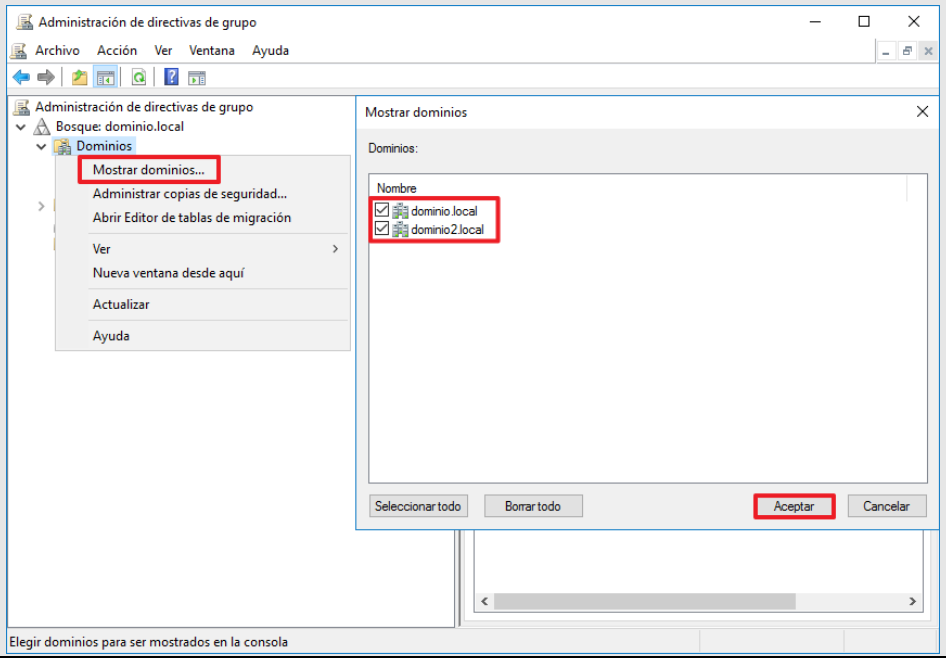
Este sistema de conectividad remota, aunque muy extendido y conocido por los usuarios, no se considera en ningún caso seguro cuando se hace uso de él fuera de un entorno o red local. Por ello, deberán utilizarse elementos adicionales de comunicación y seguridad como una VPN cuando se esté configurando un acceso remoto desde una ubicación diferente en la que se encuentre el sistema operativo.

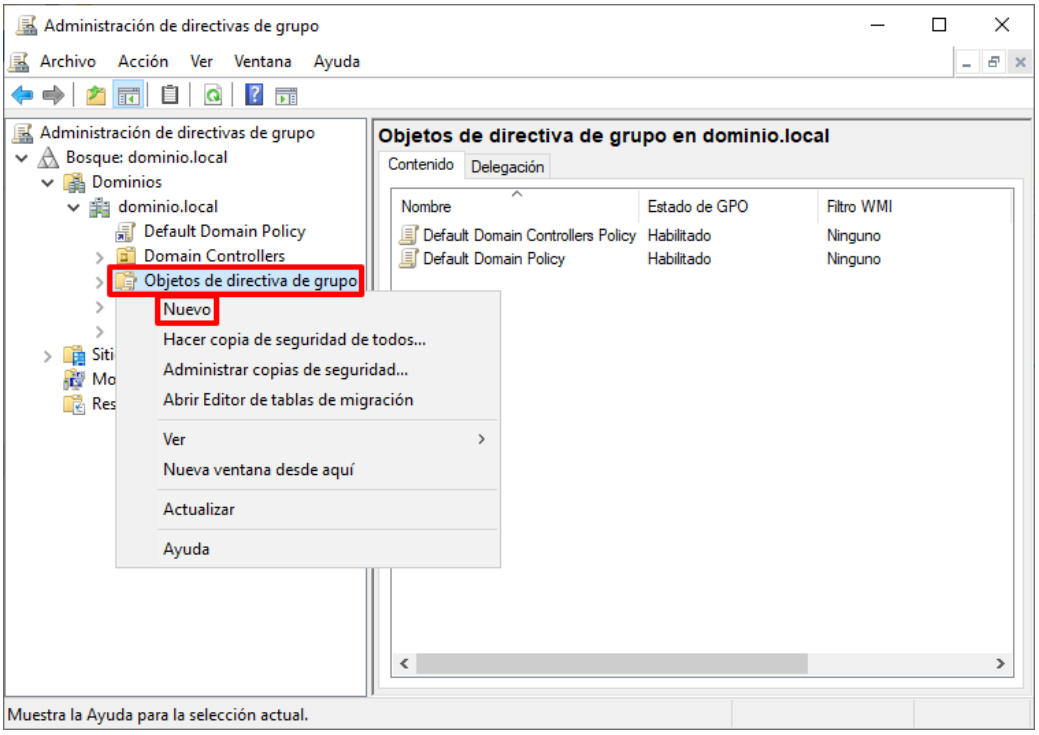
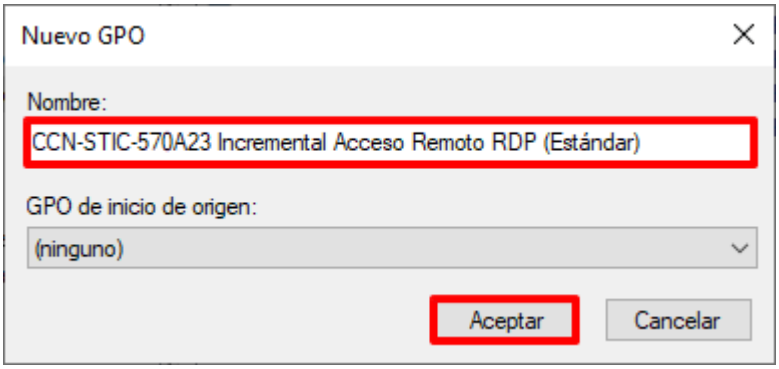
Nota: Si en su organización no hace uso de este elemento puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

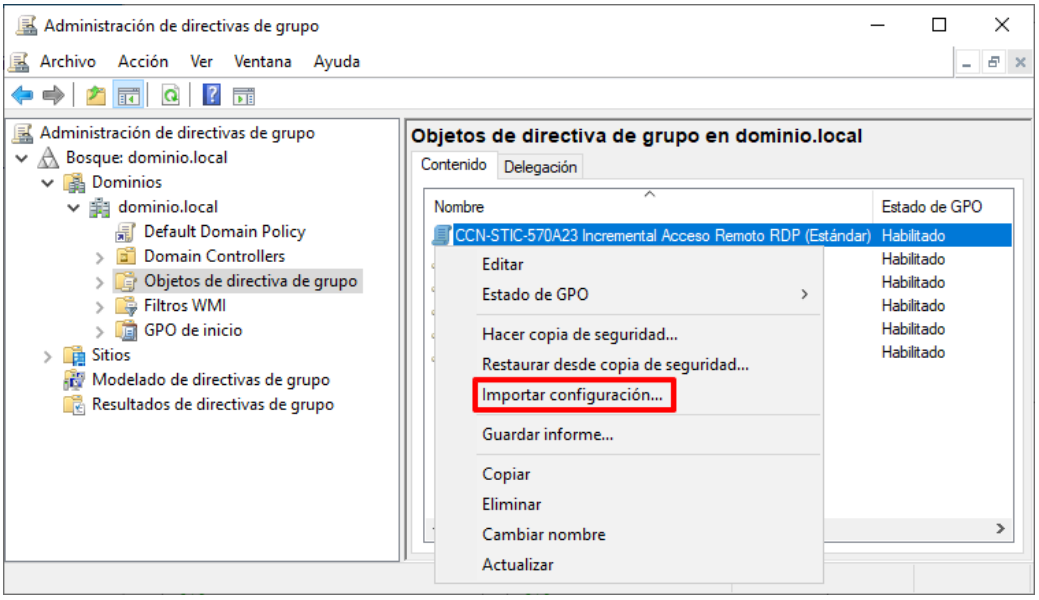
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

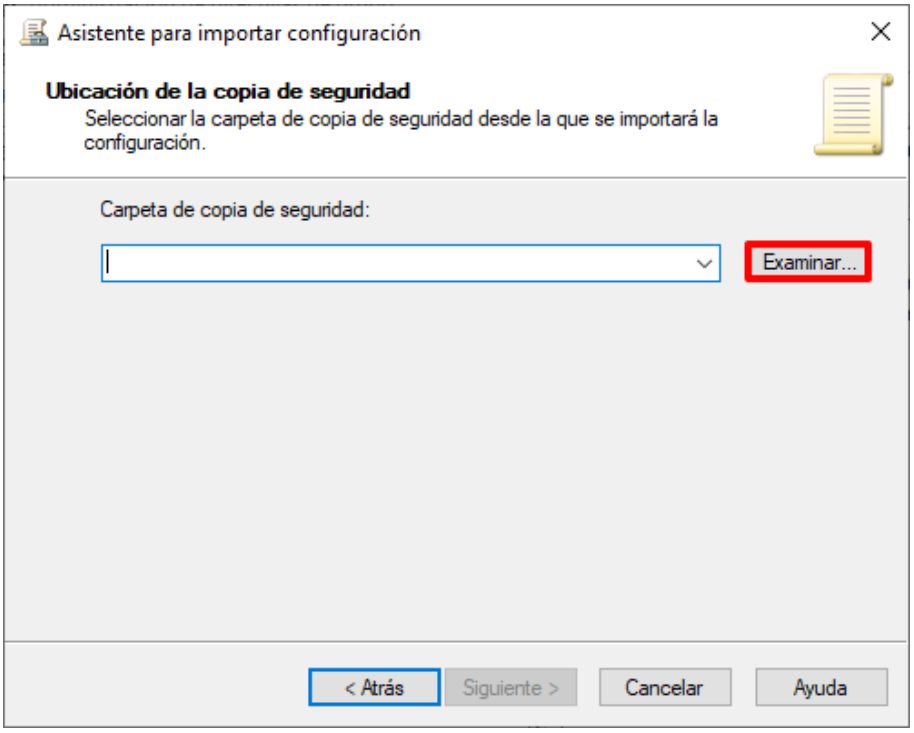
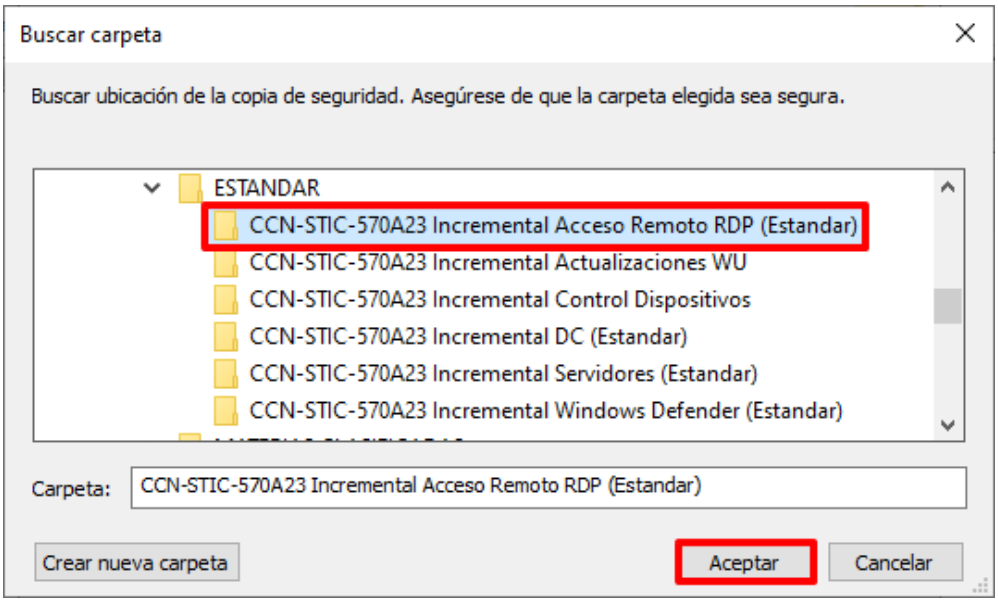
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

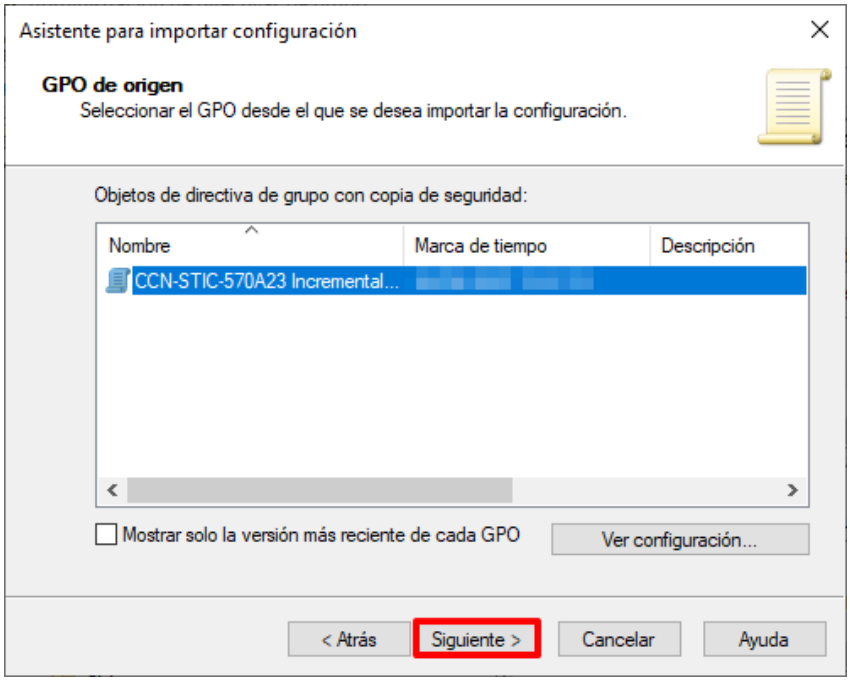
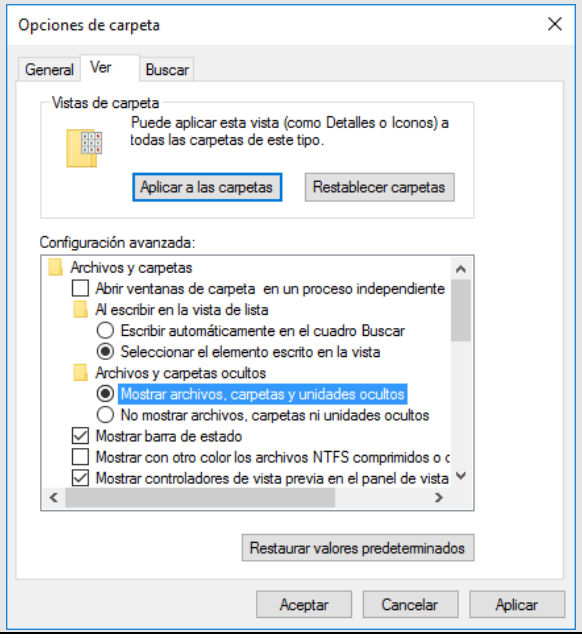
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

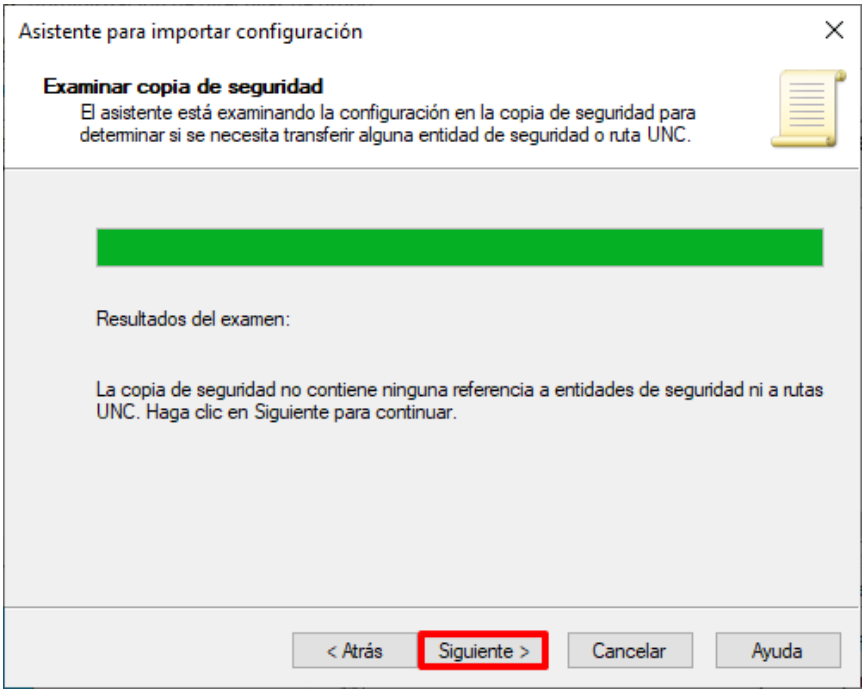
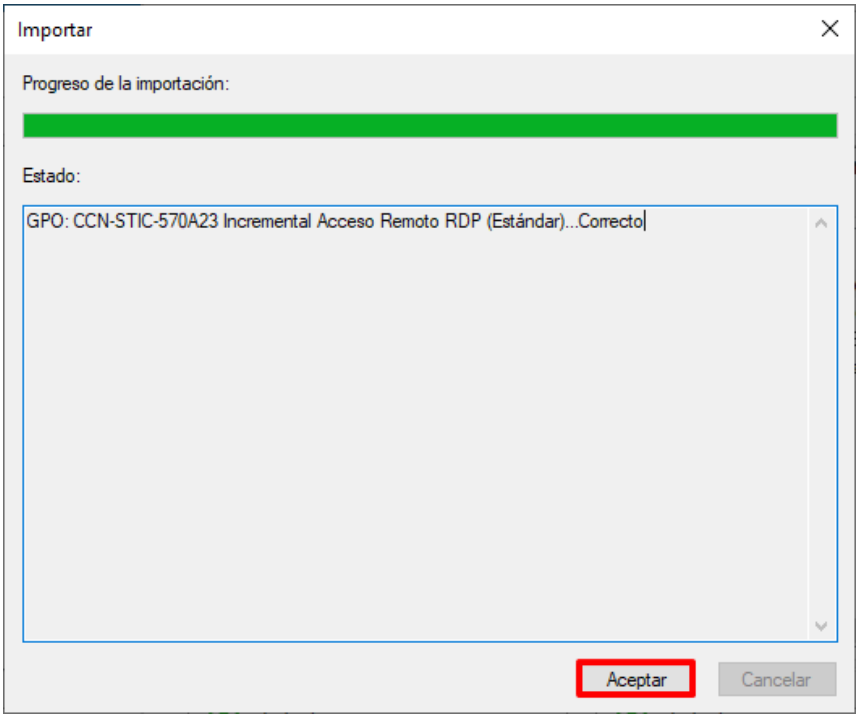
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

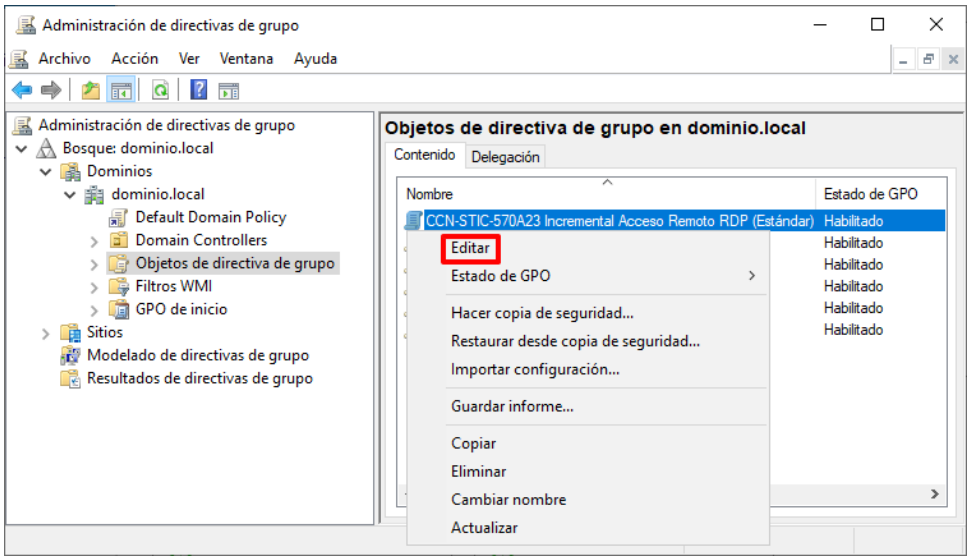
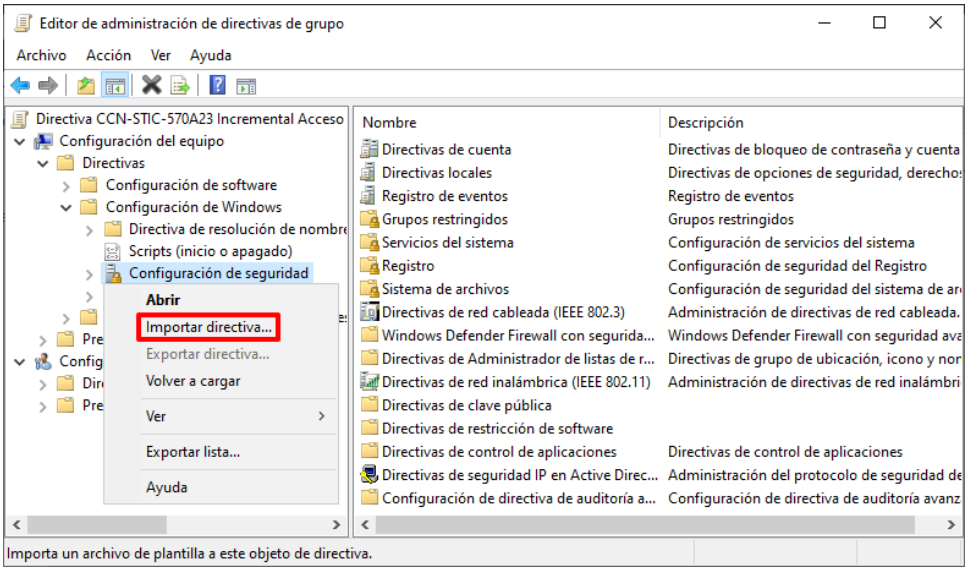
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])**" y pulse el botón "Aceptar".  **Nota:** Defina el nombre del objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

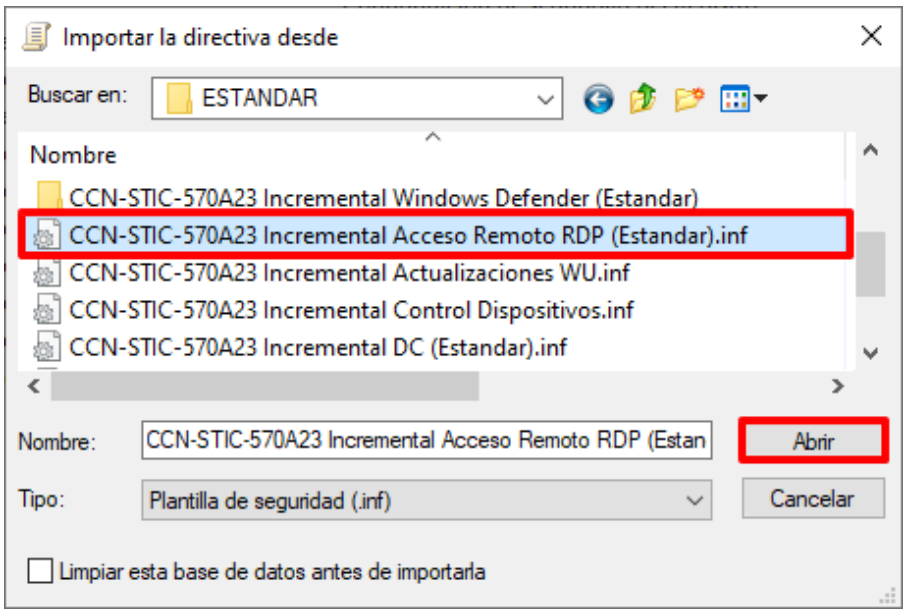
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

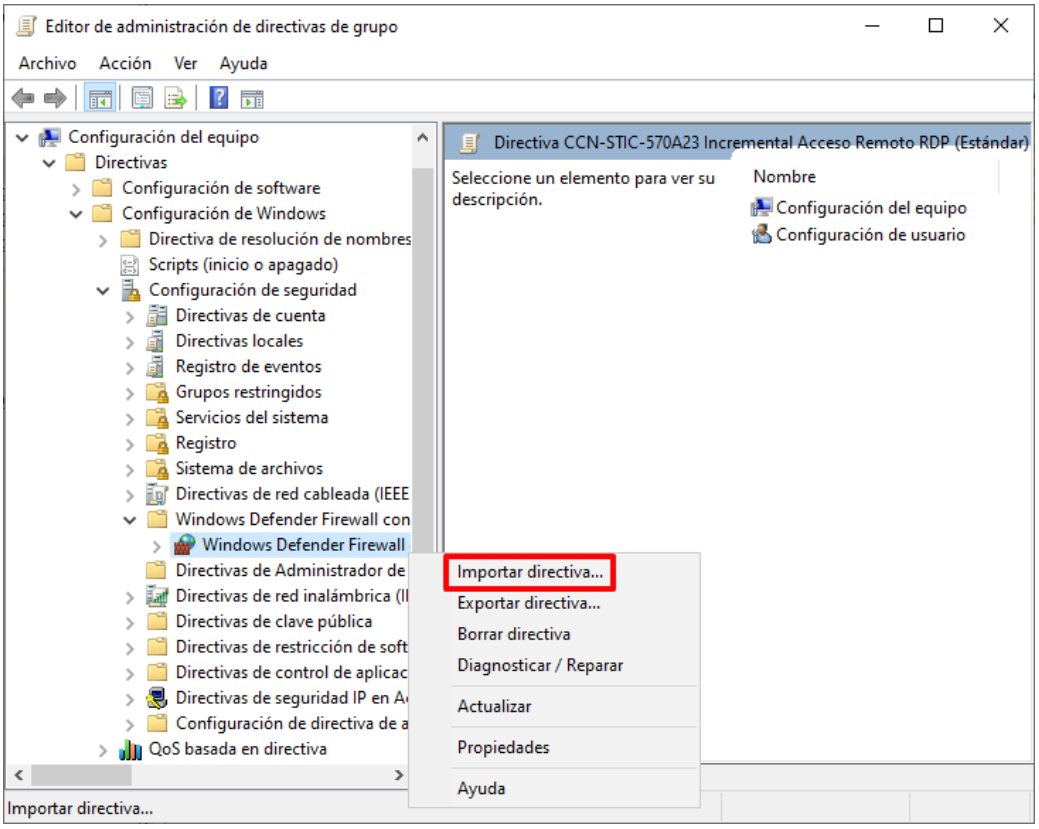
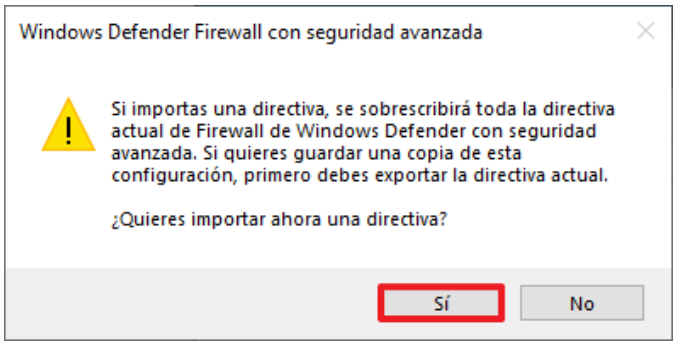
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

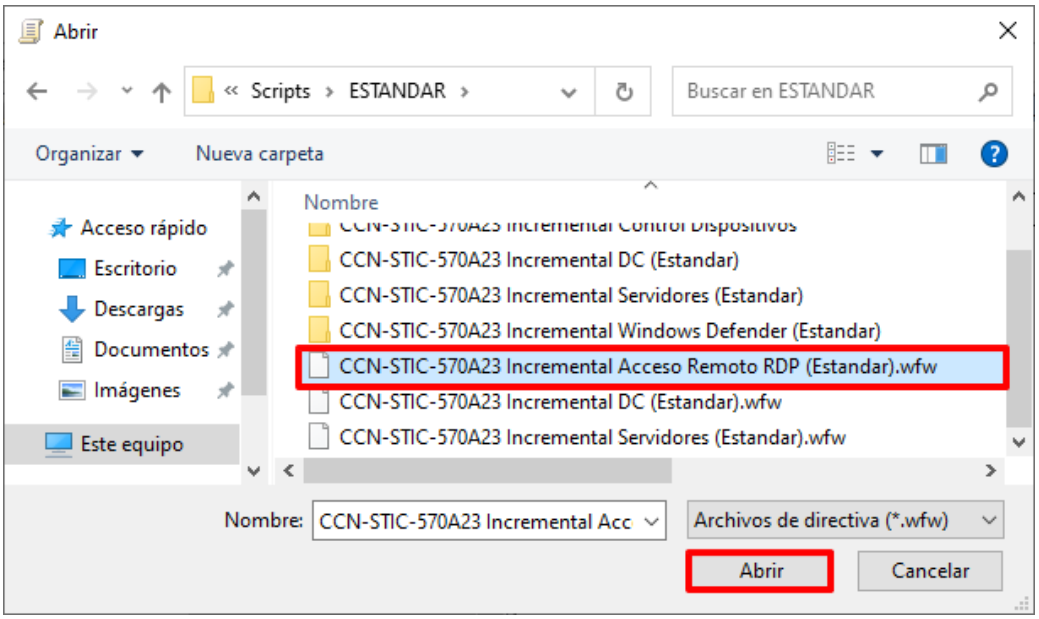
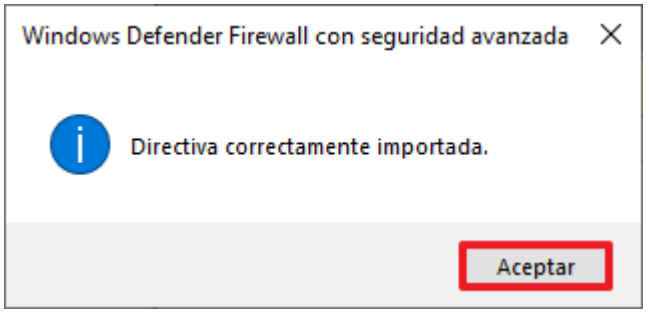
Paso	Descripción
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

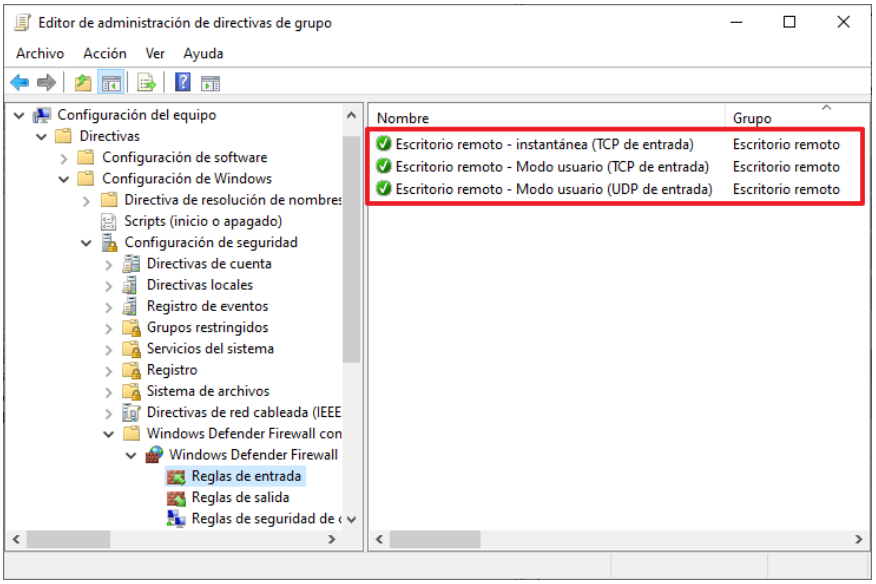
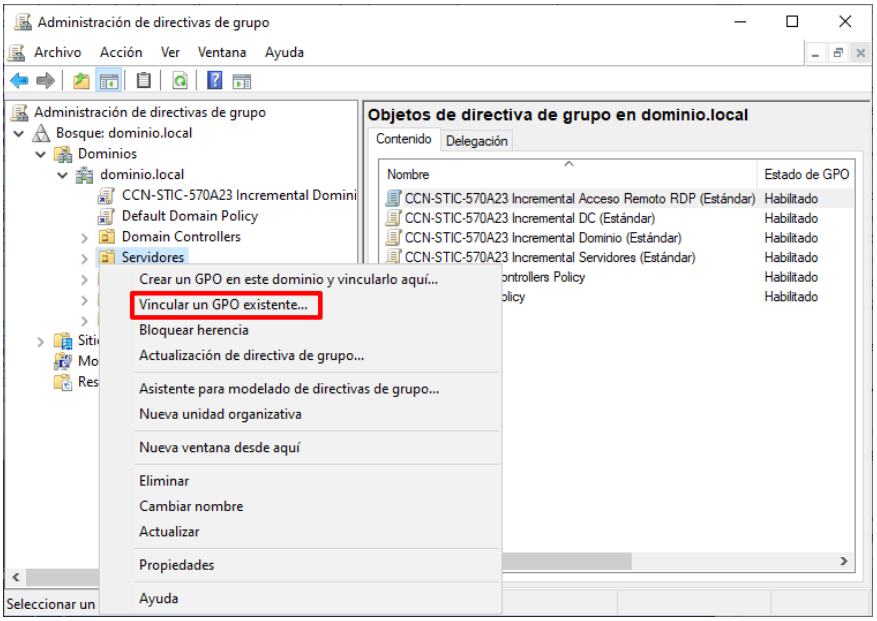
Paso	Descripción
14.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
15.	Para completar el asistente pulse sobre el botón “Finalizar”.
16.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

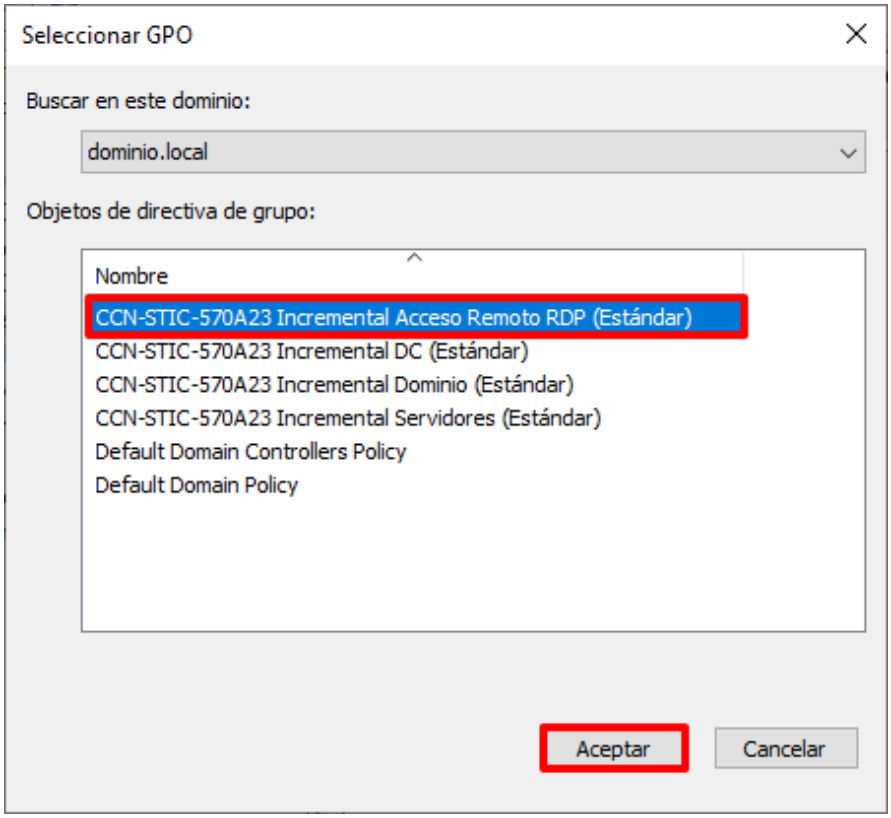
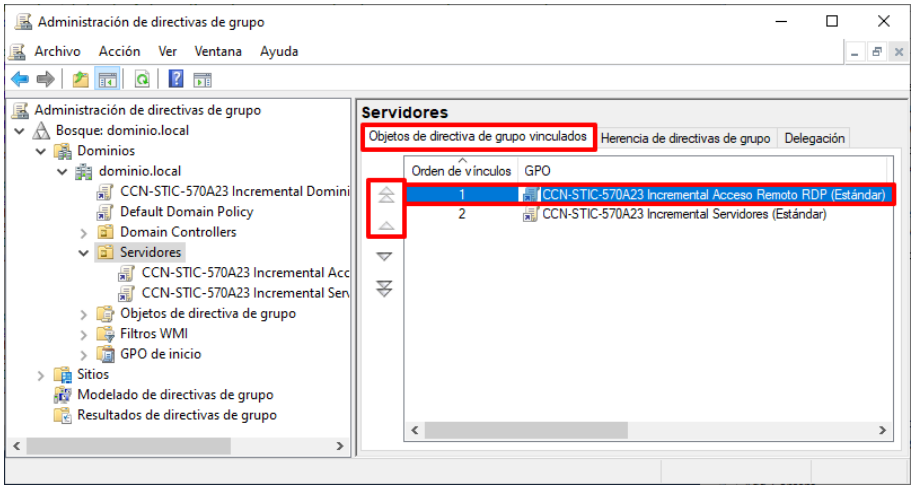
Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad”**. Seleccione con el botón derecho el nodo “Configuración de seguridad” y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 

Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en “C:\Scripts\[TIPO DE PERFILADO]” denominada “CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).inf”. A continuación, pulse sobre el botón “Abrir”.  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

Paso	Descripción
21.	En la misma ventana del editor de administración de directivas de grupo, seleccione el siguiente nodo: "**Directiva CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada - LDAP://CN={<SID>},CN=POLICIES,CN=SYSTEM,DC=<su nombre de dominio>**". A continuación, pulse con el botón derecho sobre el nodo desplegado y seleccione la opción "Importar directiva…" del menú contextual que aparecerá. 
22.	Pulse "Sí" para continuar. 

Paso	Descripción
23.	Seleccione el archivo de configuración “CCN-STIC-570A23 Incremental Acceso Remoto RDP (TIPO DE PERFILADO).wfw” ubicado en “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Abrir”.  **Nota:** Seleccione la configuración de firewall acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
24.	Pulse “Aceptar” para continuar. 

Paso	Descripción
25.	Despliegue el nodo “Reglas de entrada” y confirme que las reglas se han importado correctamente. 
26.	Cierre la ventana “Editor de administración de directivas de grupo”.
27.	Por último, identifique las unidades organizativas y objetos que requieran el acceso remoto y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración. En este ejemplo se hace uso de la Unidad Organizativa “Servidores”, creada para tal fin.

Paso	Descripción
28.	A continuación, seleccione el objeto GPO “CCN-STIC-570A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO configurado acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
29.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña “Objetos de directiva de grupo vinculados”, seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

Paso	Descripción
30.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.

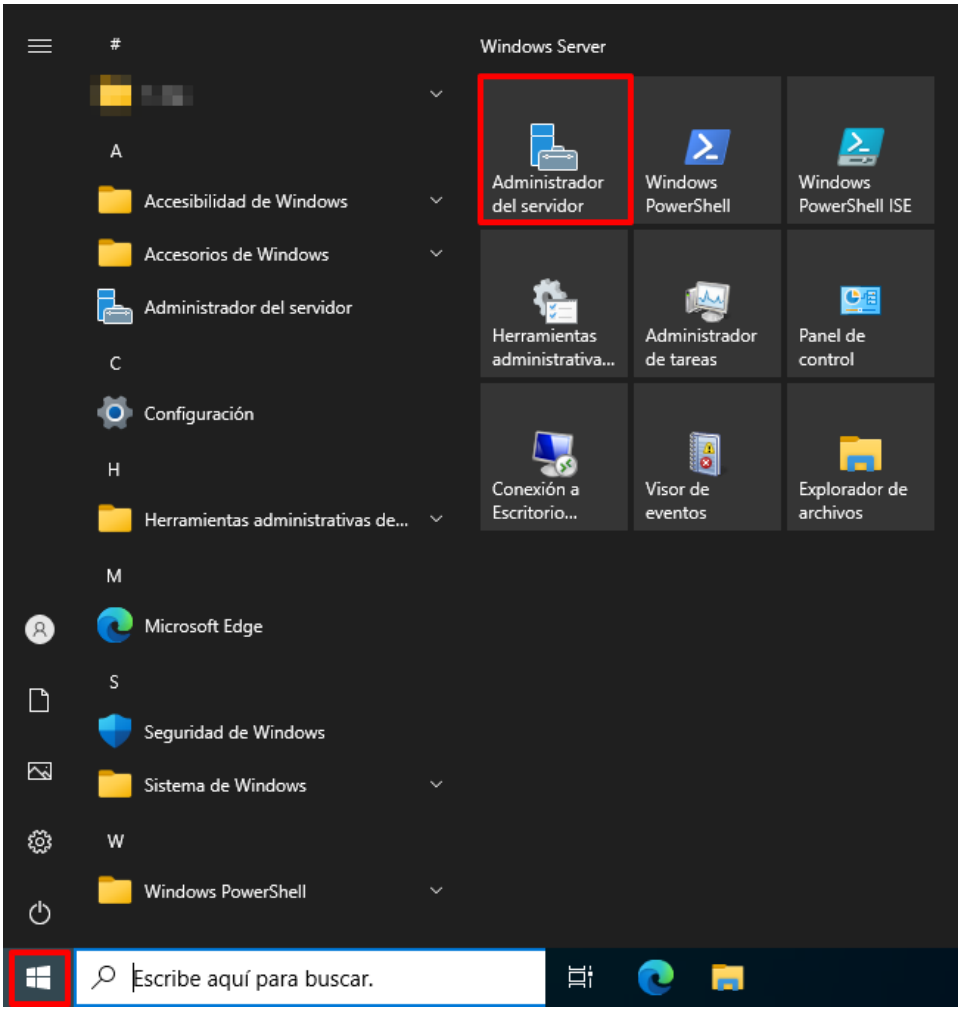
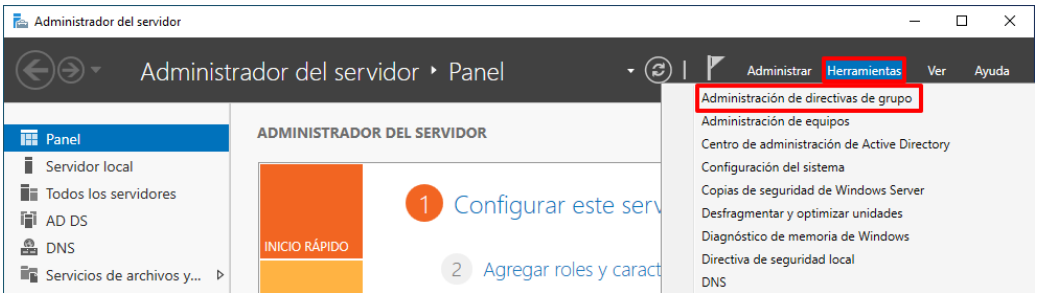
ANEXO B.2. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

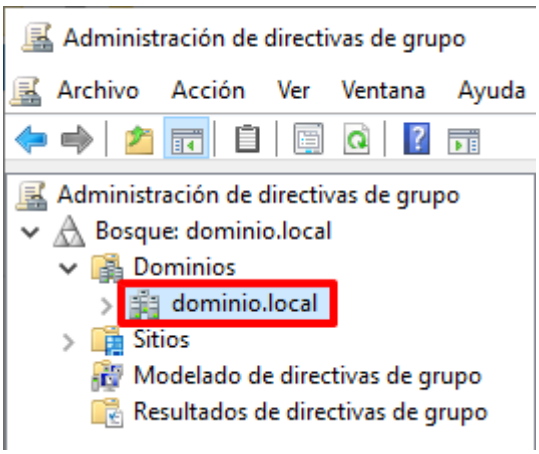
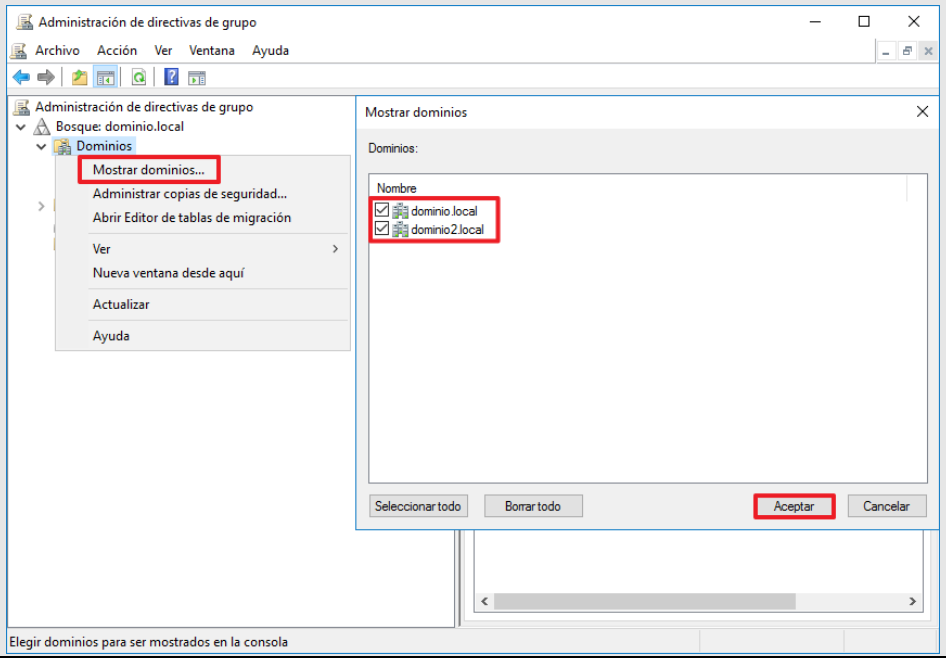
A través de la siguiente sección y su paso a paso, se definirán las acciones para dotar al sistema operativo Windows Server de un servicio de actualizaciones automáticas completamente configurado.

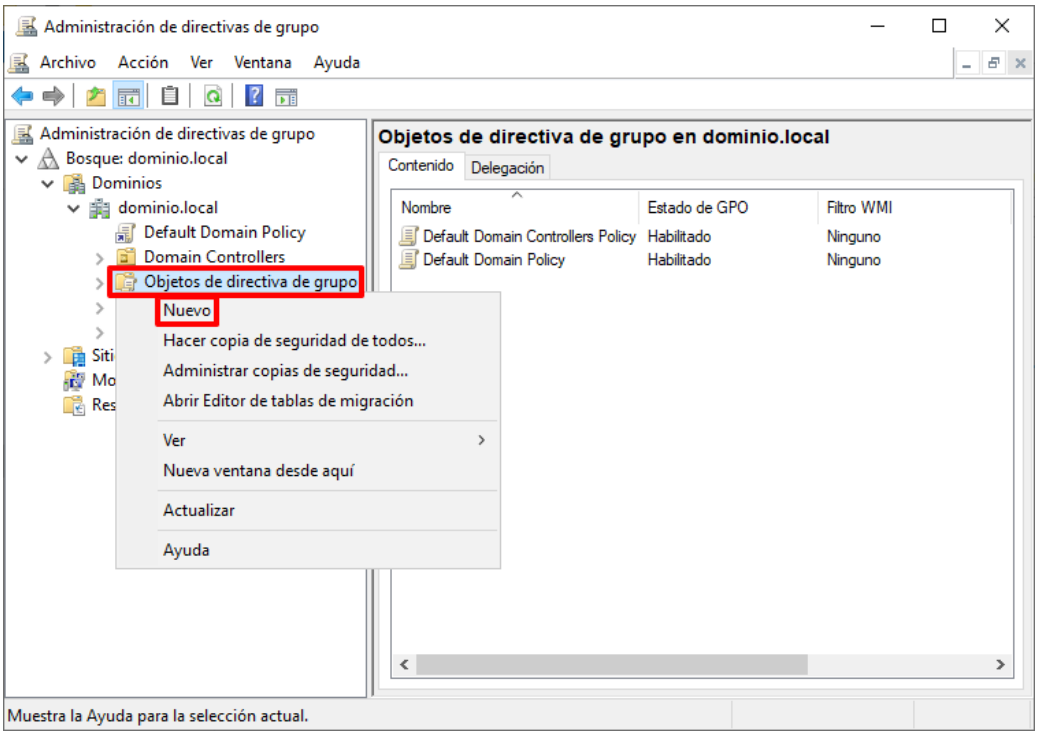
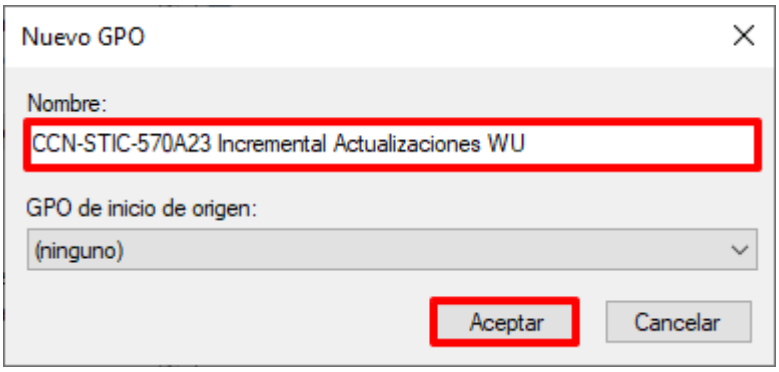
Nota: Si en su organización ya dispone de un producto o servicio para la actualización y mantenimiento del sistema operativo, como el servicio de WSUS, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

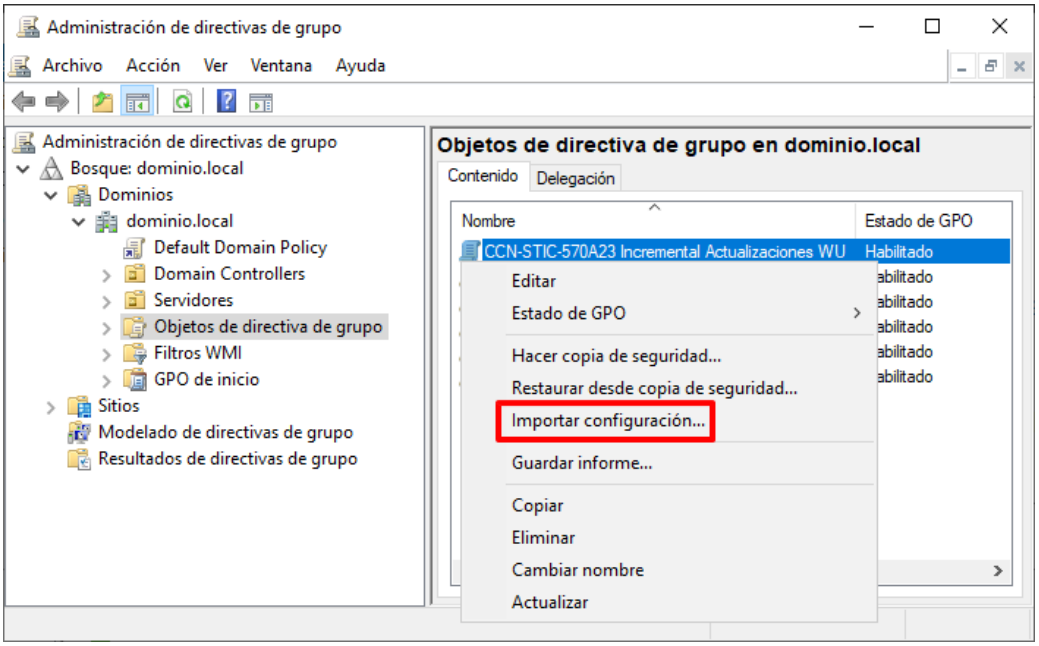
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

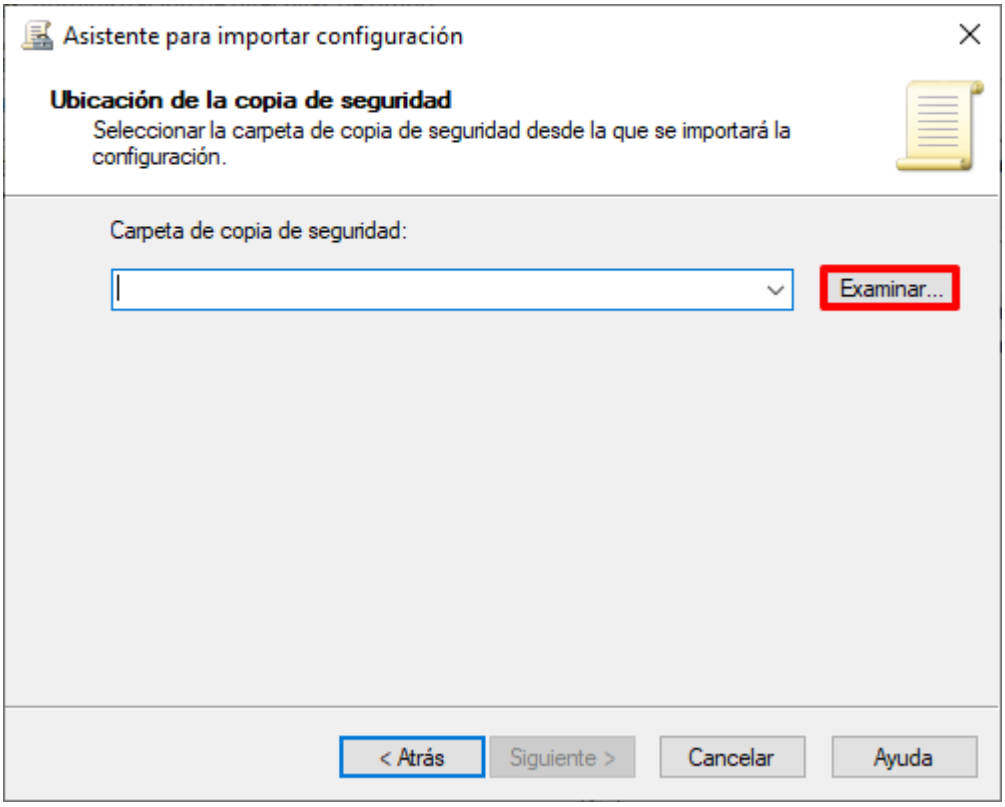
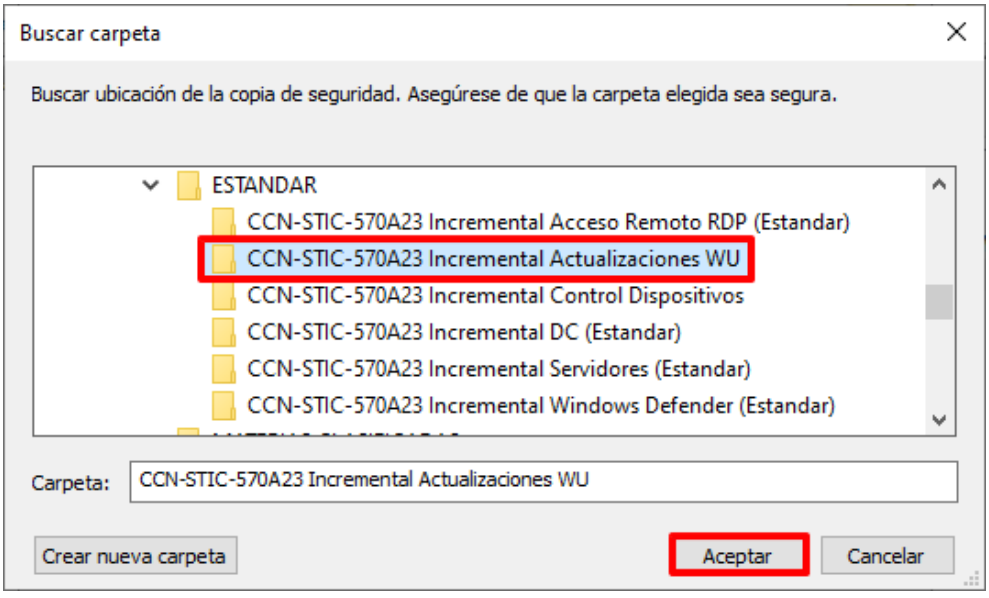
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

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

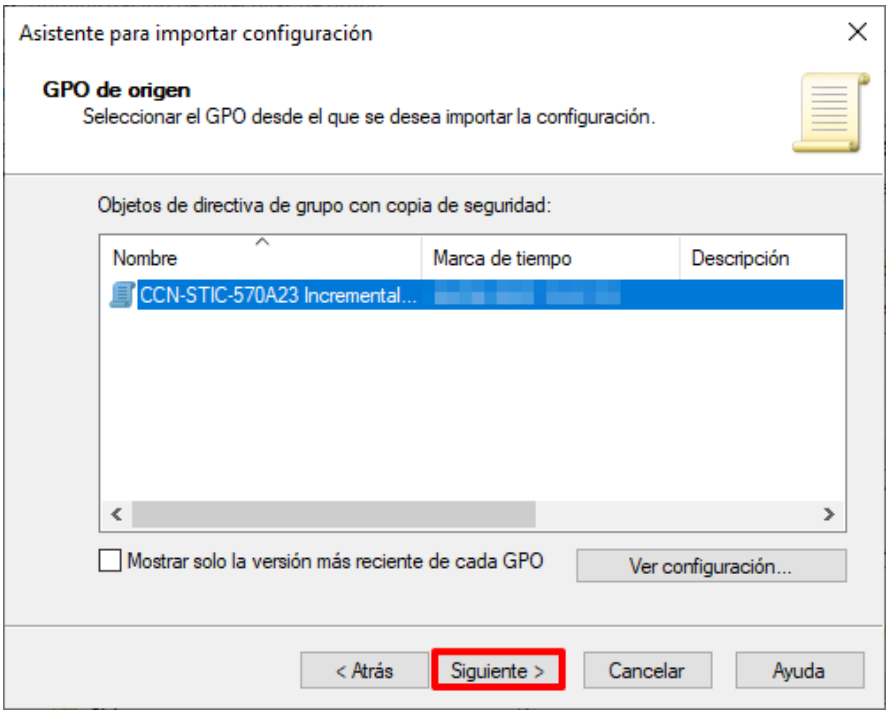
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Actualizaciones WU**" y pulse el botón "Aceptar". 

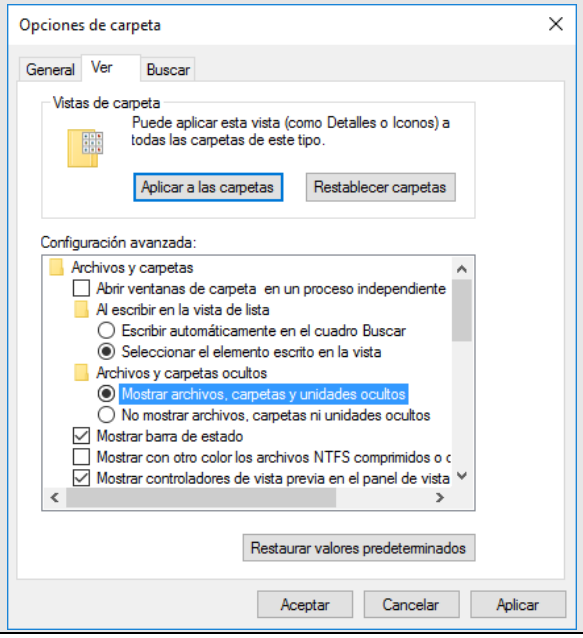
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

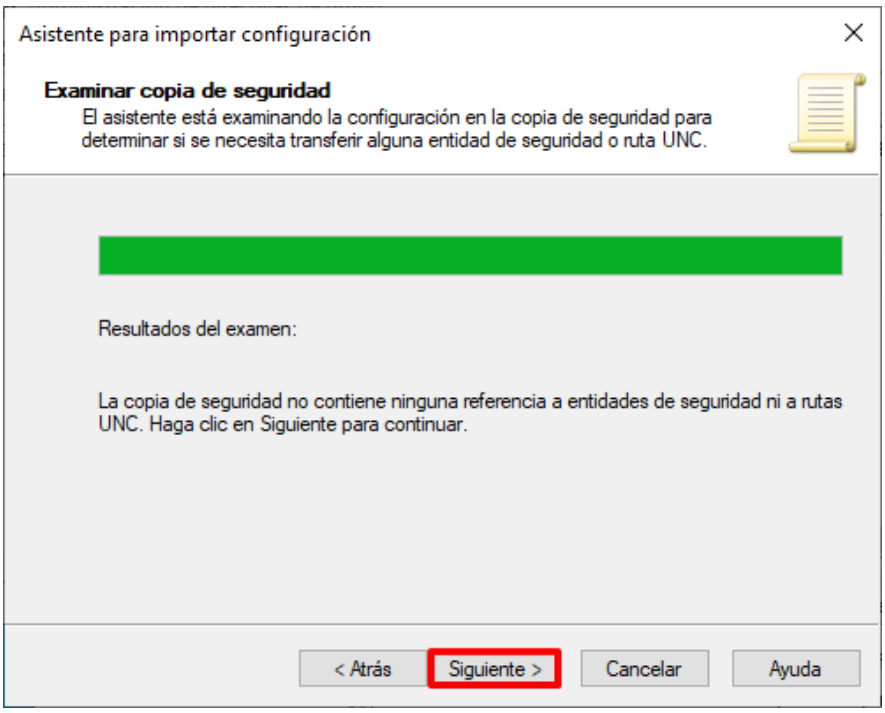
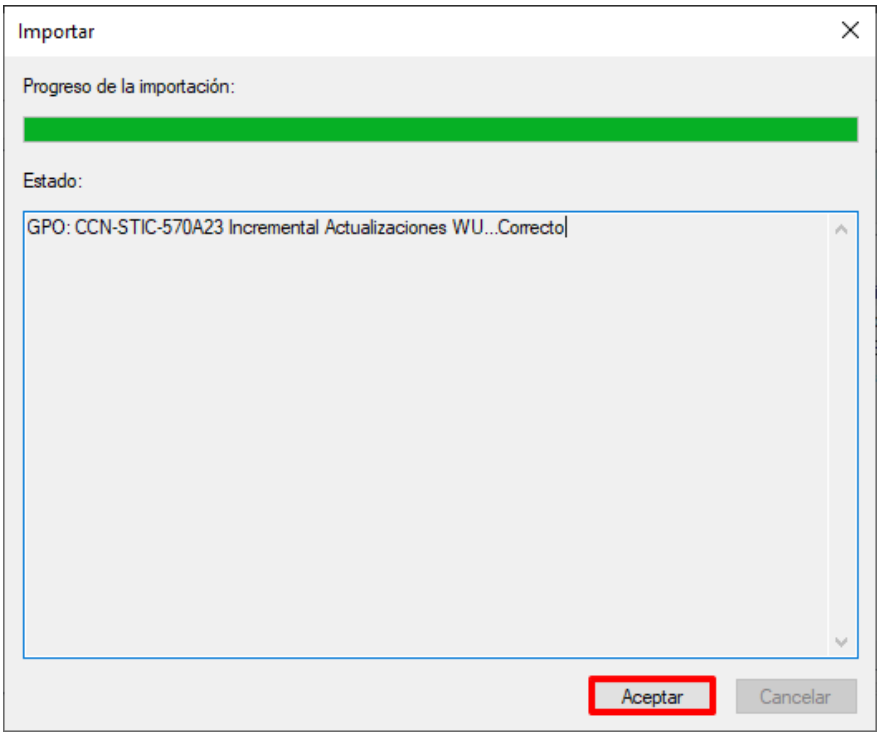
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-570A23 Incremental Actualizaciones WU” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

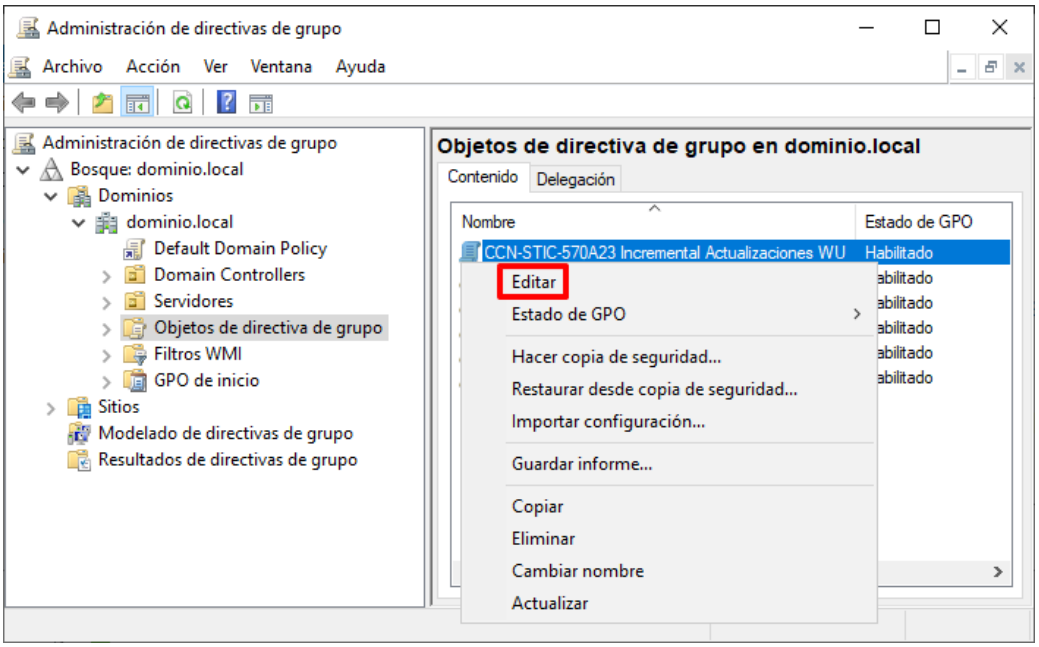
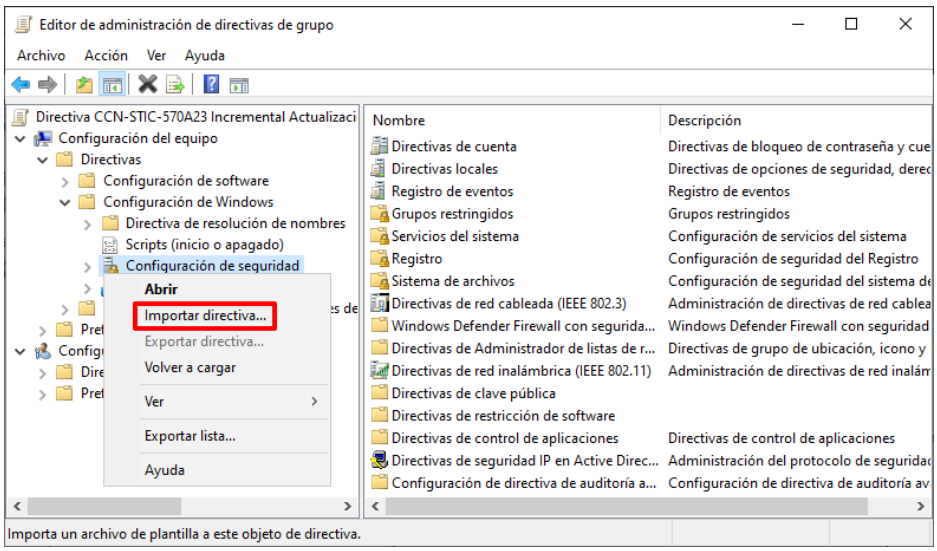
Paso	Descripción
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental Actualizaciones WU” y pulse “Siguiente >”.

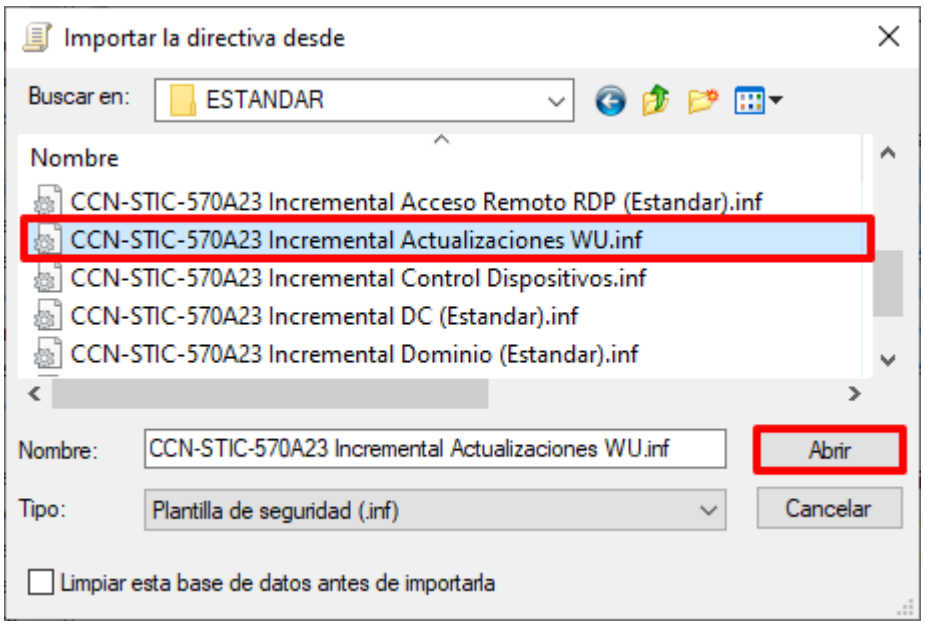
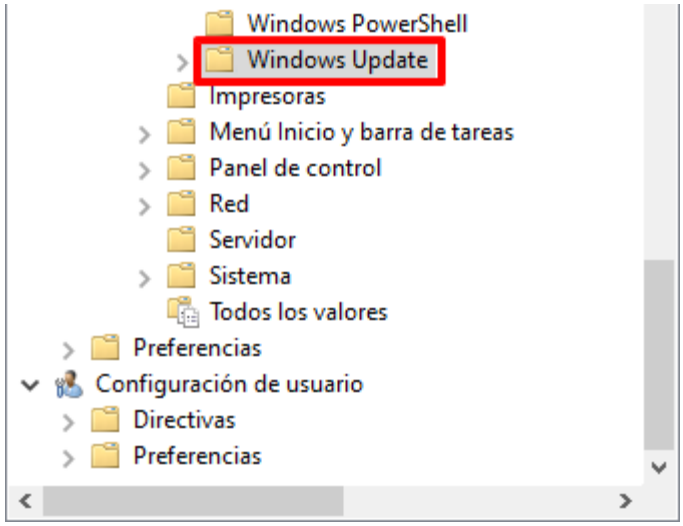


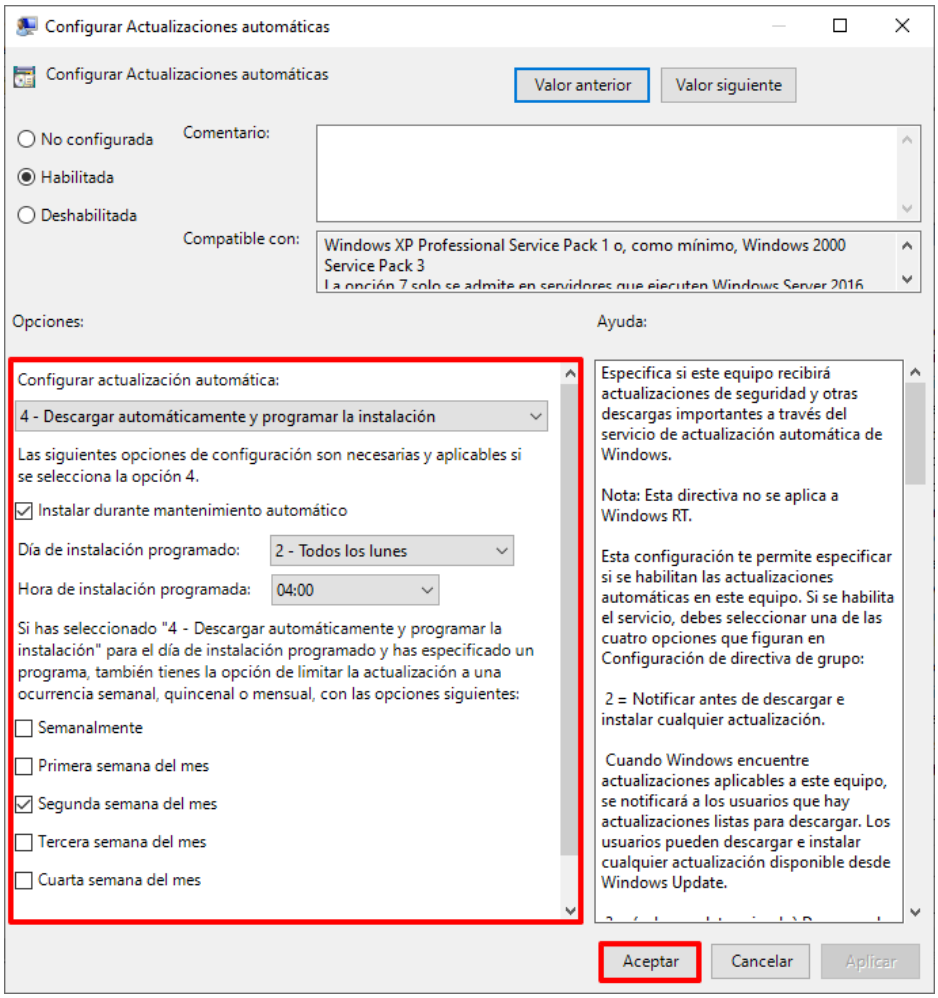
Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”.

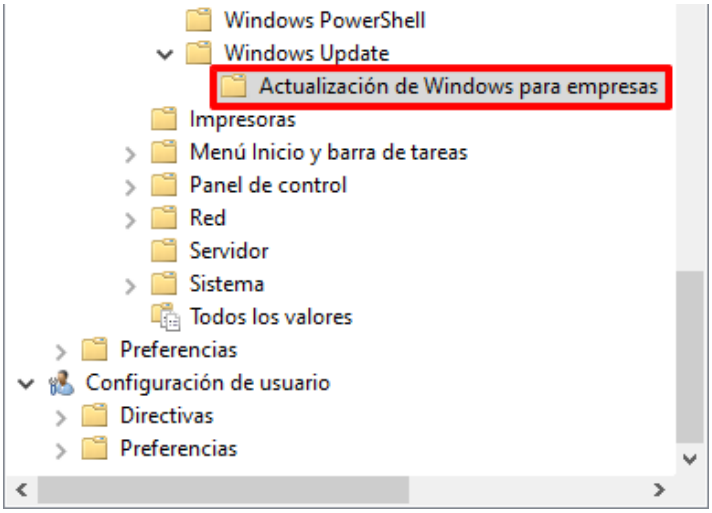
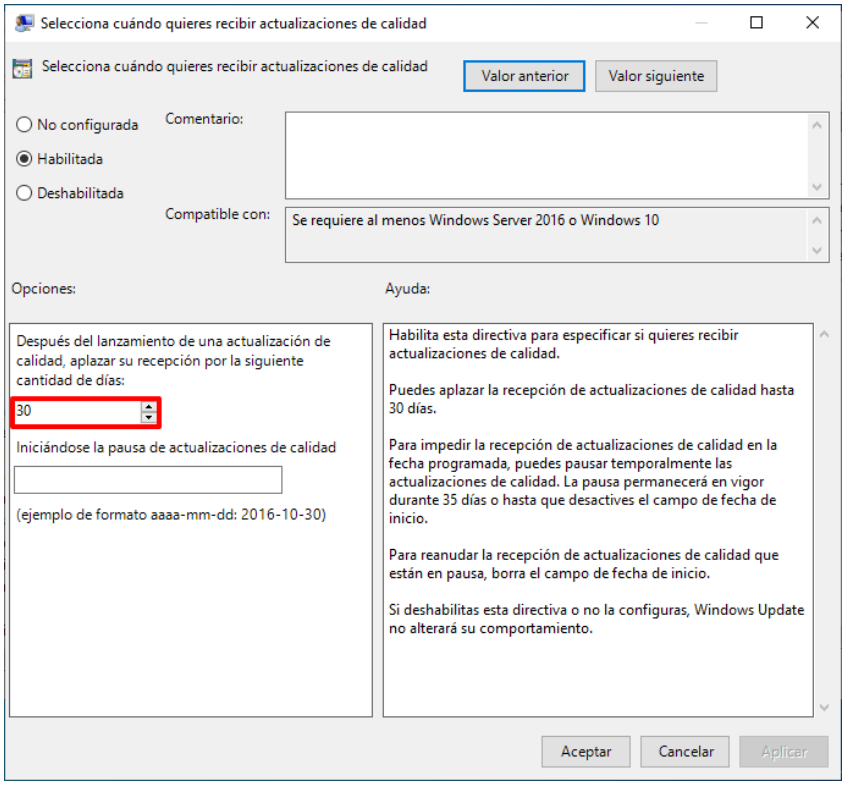


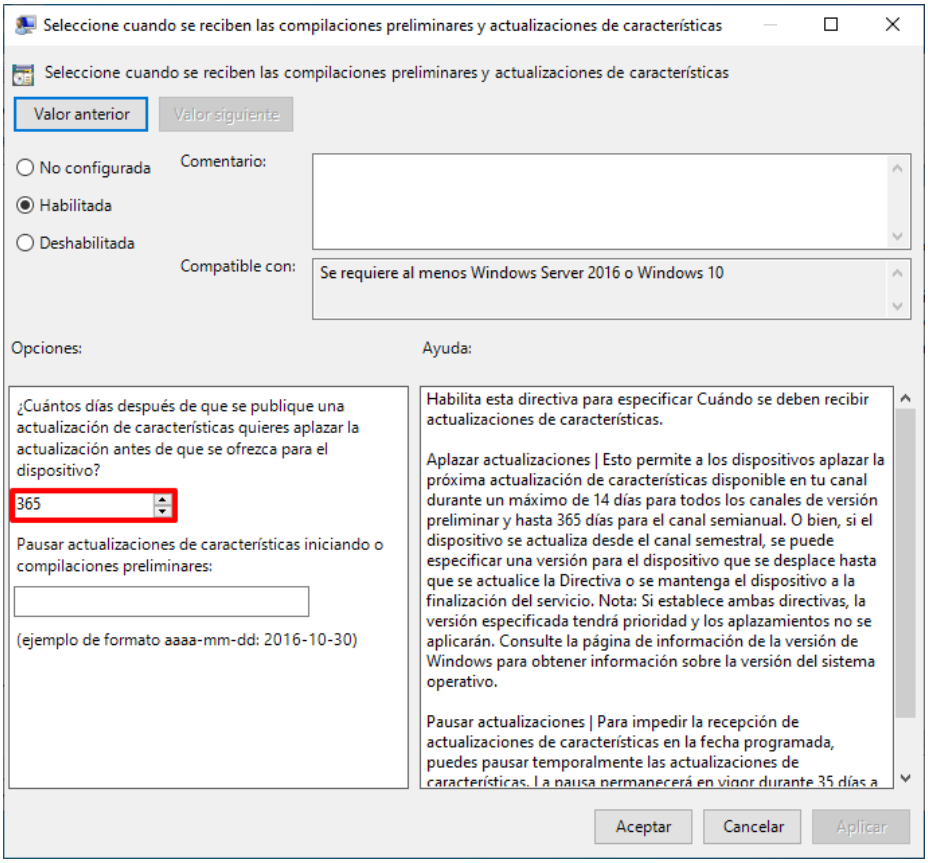
Paso	Descripción
14.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
15.	Para completar el asistente pulse sobre el botón “Finalizar”.
16.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

Paso	Descripción
17.	Seleccione de nuevo el objeto GPO "CCN-STIC-570A23 Incremental Actualizaciones WU" con el botón derecho y seleccione la opción "Editar" del menú contextual que aparecerá. 
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"CCN-STIC-570A23 Incremental Actualizaciones WU → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. Seleccione con el botón derecho el nodo "Configuración de seguridad" y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 

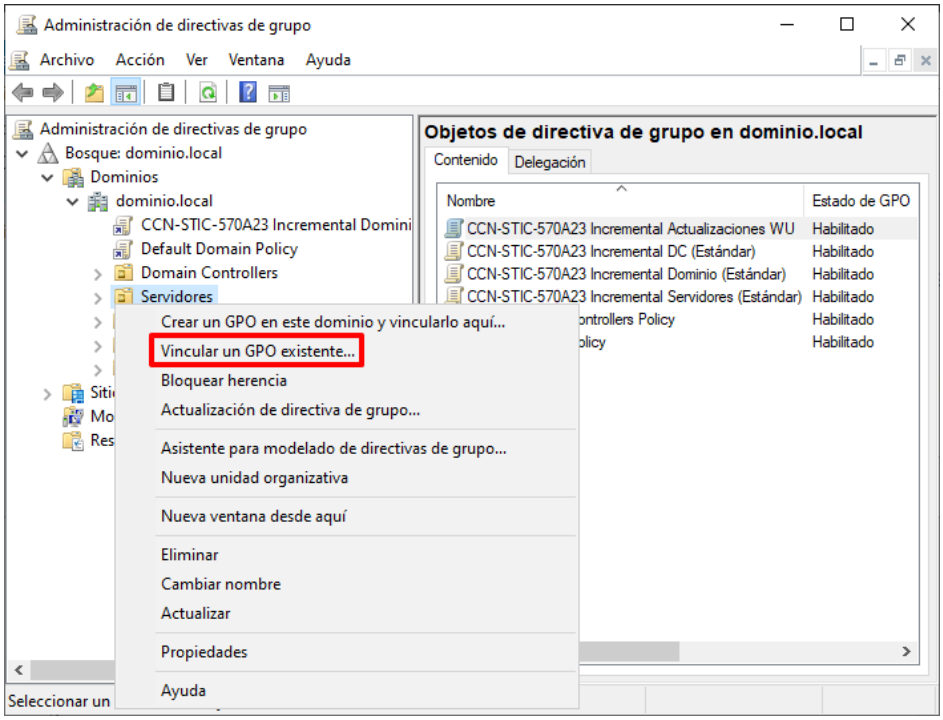
Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-570A23 Incremental Actualizaciones WU.inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
21.	A continuación, despliegue el nodo: **"CCN-STIC-570A23 Incremental Actualizaciones WU → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Windows Update"** 

Paso	Descripción
22.	En el panel derecho identifique y haga doble clic sobre la directiva “Configurar Actualizaciones automáticas”. Evalúe y adapte la configuración ofrecida acorde a las necesidades de su organización. 

Paso	Descripción
23.	A continuación, despliegue el nodo: **"CCN-STIC-570A23 Incremental Actualizaciones WU → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas".** 
24.	En el panel derecho haga doble clic sobre la directiva: **"Selecciona cúando quieres recibir actualizaciones de calidad"**. En la nueva ventana emergente deberá editar el número de días establecido.  **Nota:** En la configuración expuesta se ha indicado el máximo número de días. Puede de igual modo establecer la fecha desde que será de aplicación la pausa.

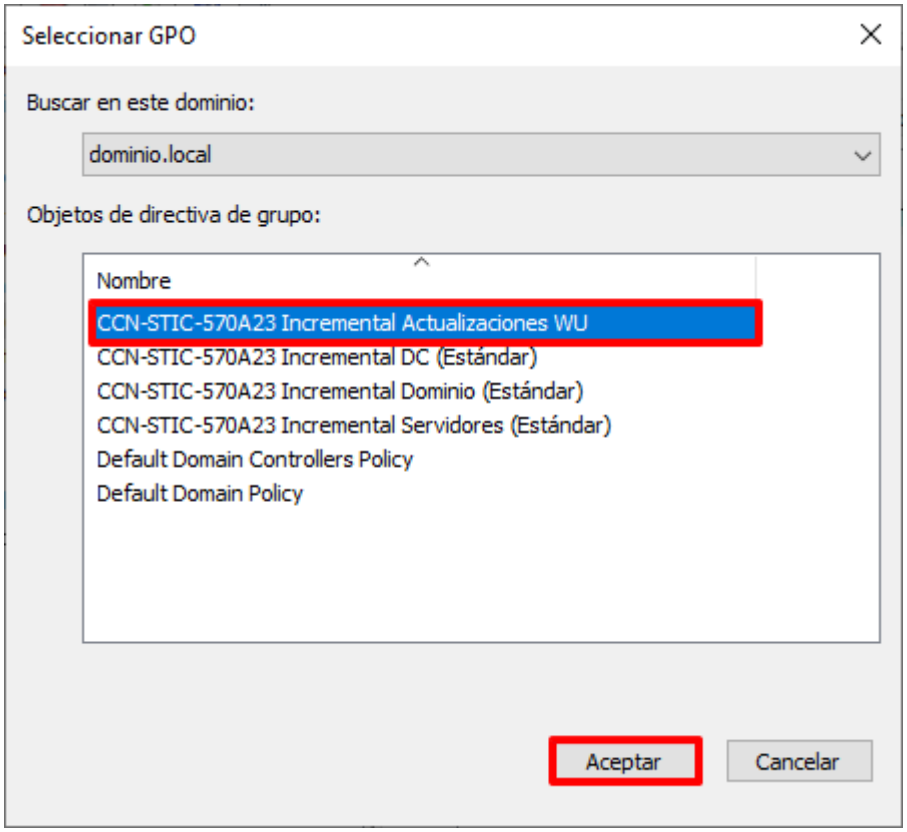
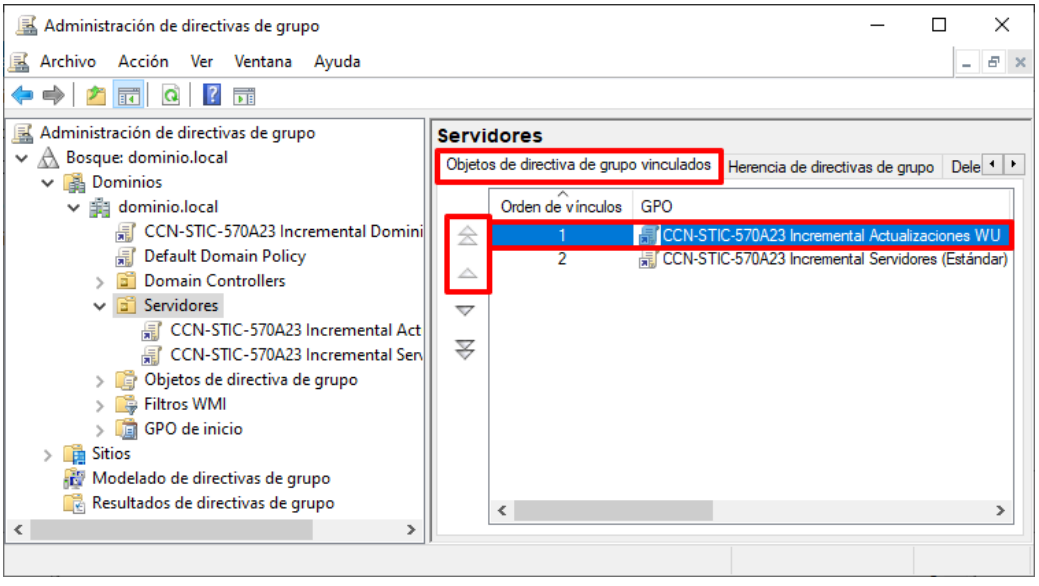
Paso	Descripción
25.	De forma análoga a lo realizado en los pasos anteriores, haga doble clic sobre la directiva **"Seleccione cuando se reciben las compilaciones preliminares y actualizaciones de características"**. En la nueva ventana emergente deberá editar el número de días establecido.  **Nota:** En la configuración expuesta se ha indicado el máximo número de días. Puede de igual modo establecer la fecha desde que será de aplicación la pausa.
26.	Cierre la ventana "Editor de administración de directivas de grupo".

Paso	Descripción
27.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de actualizaciones y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción “Vincular un GPO existente…”.



Nota: Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración.

En este ejemplo se hace uso de la Unidad Organizativa “Servidores”, creada para tal fin.

Paso	Descripción
28.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental Actualizaciones WU" y pulse "Aceptar". 
29.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

Paso	Descripción
30.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.

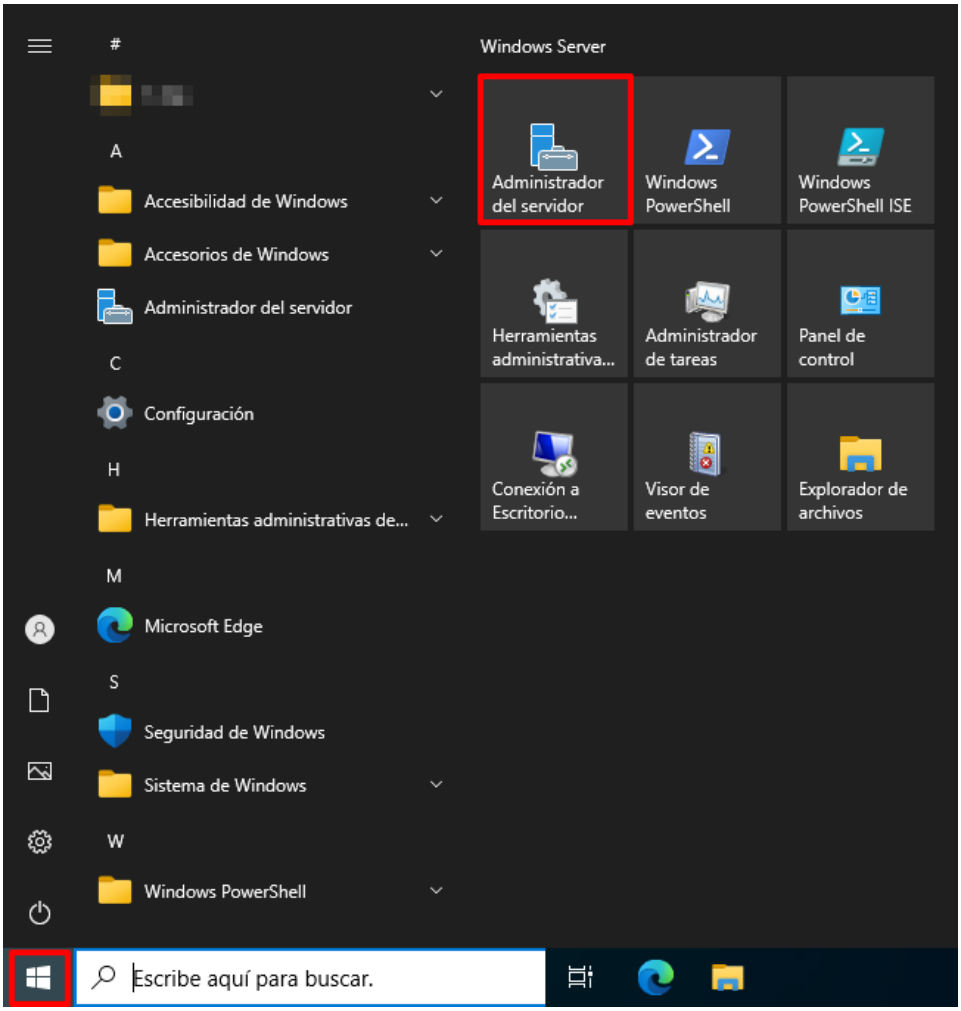
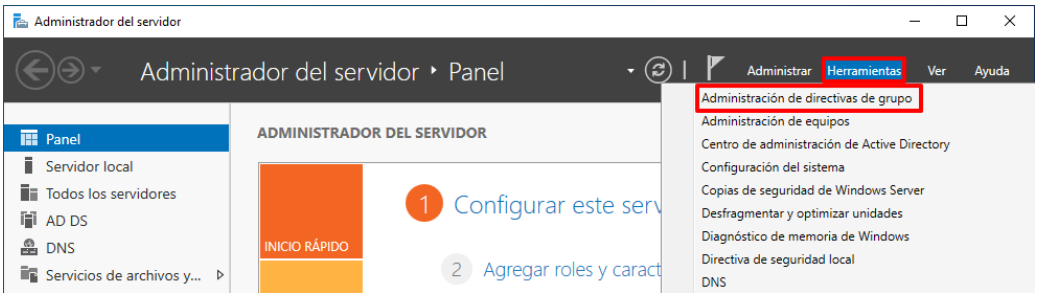
ANEXO B.3. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

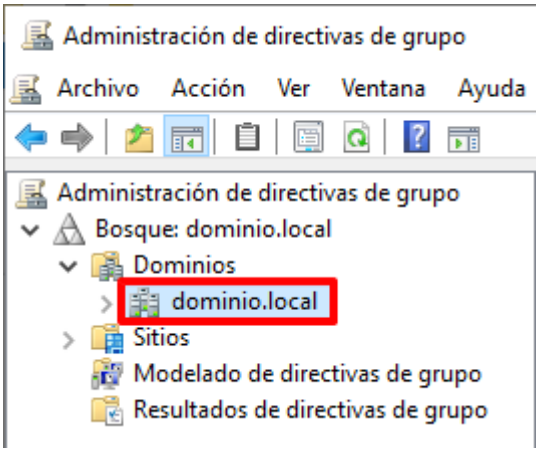
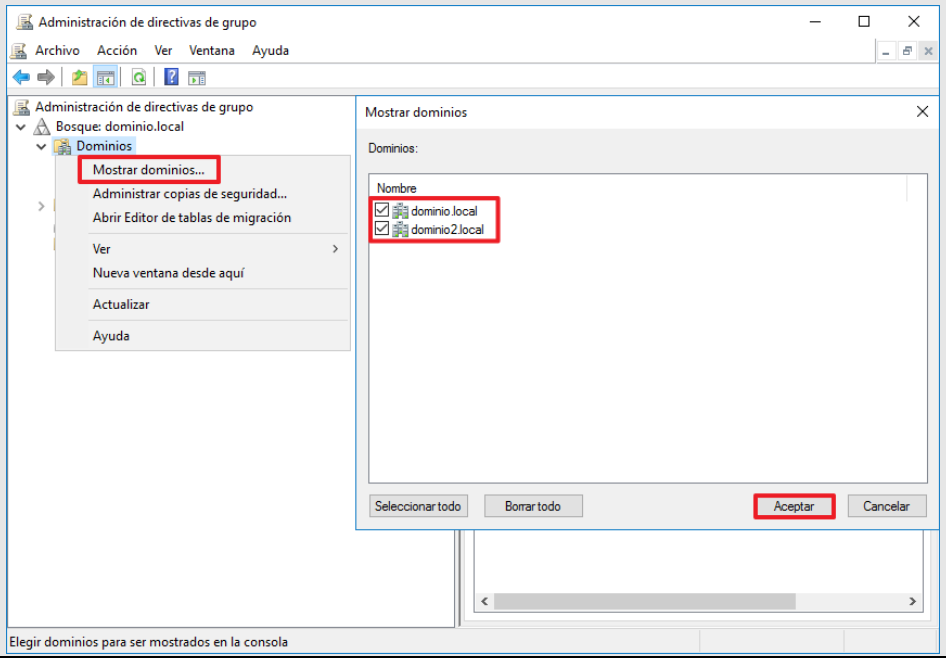
La sección y los pasos descritos a continuación, permiten establecer la configuración sobre el software frente a protección de código dañino incluido por defecto en los sistemas operativo Windows Server.

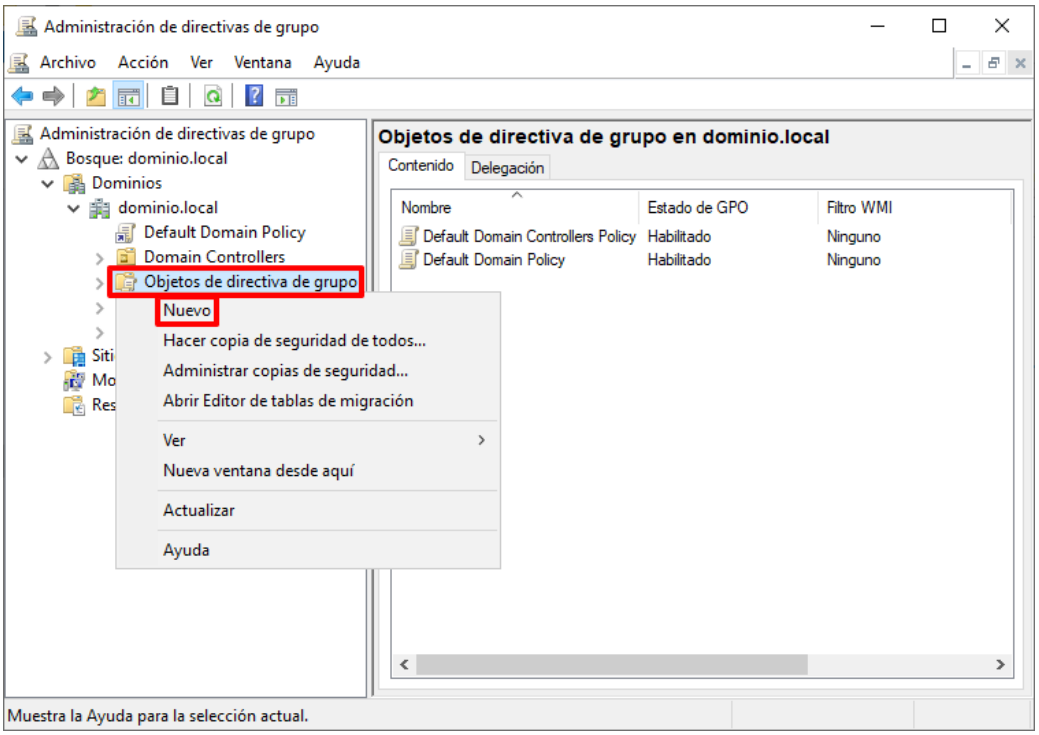
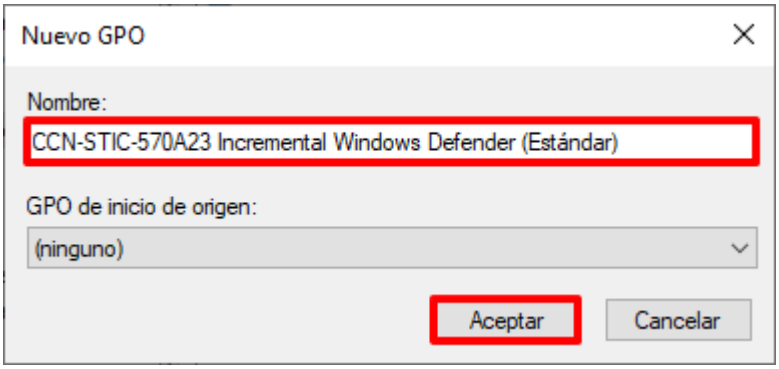
Nota: Si en su organización ya dispone de un producto o servicio frente a código dañino en el sistema operativo, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

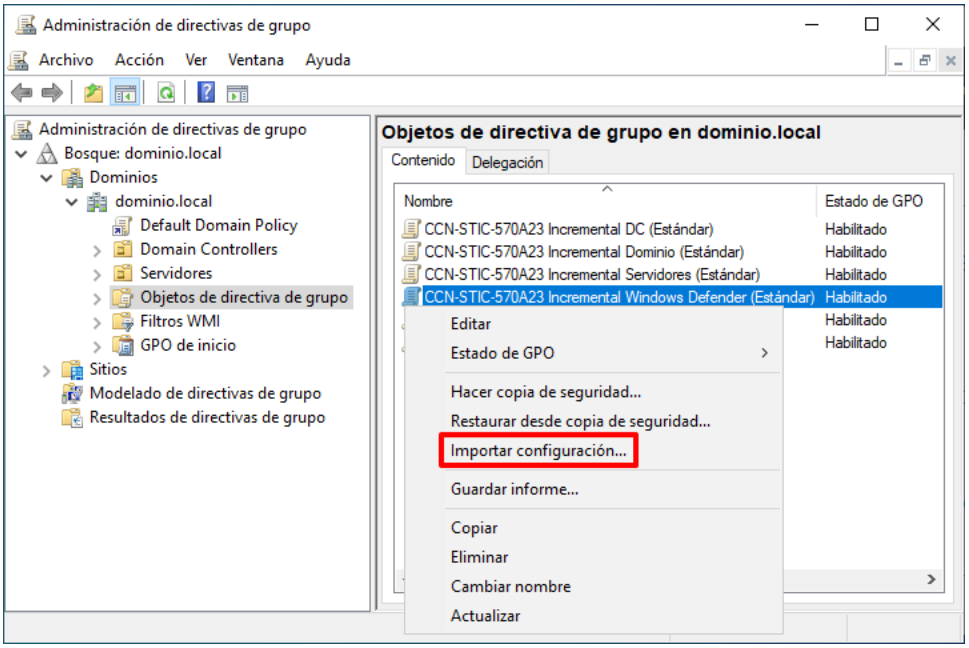
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

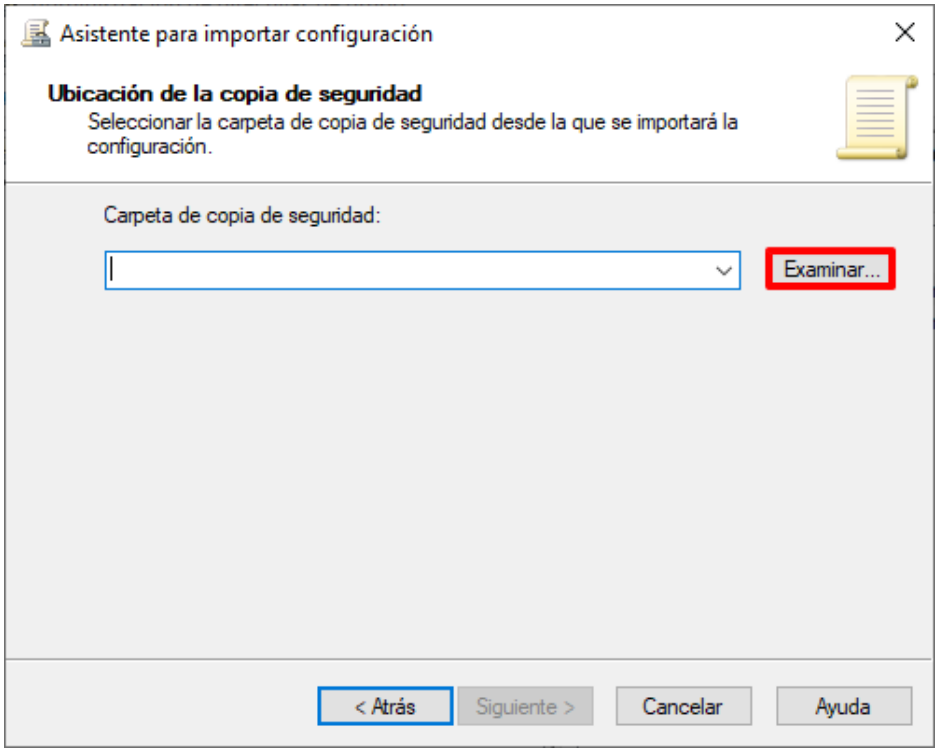
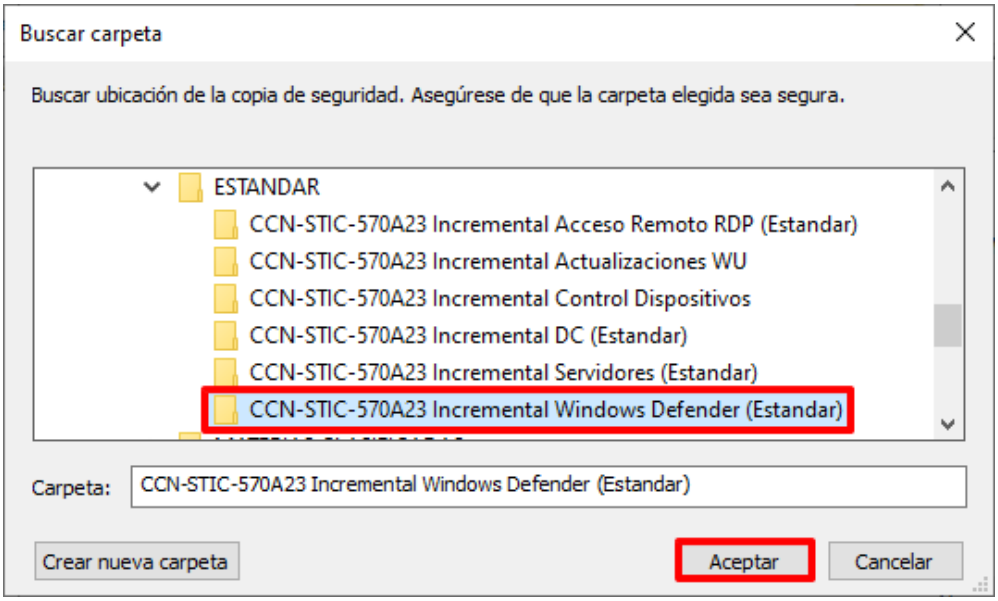
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

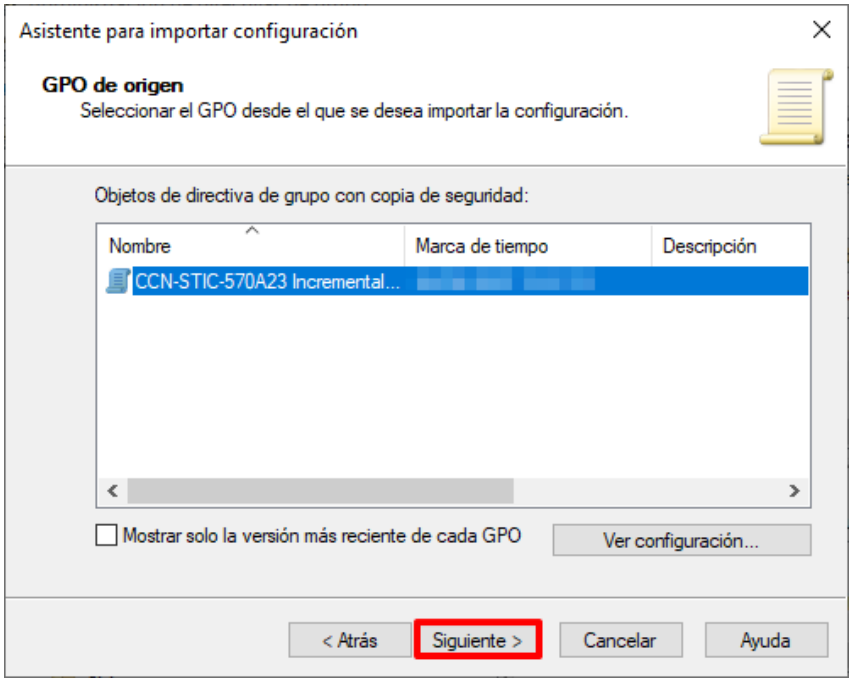
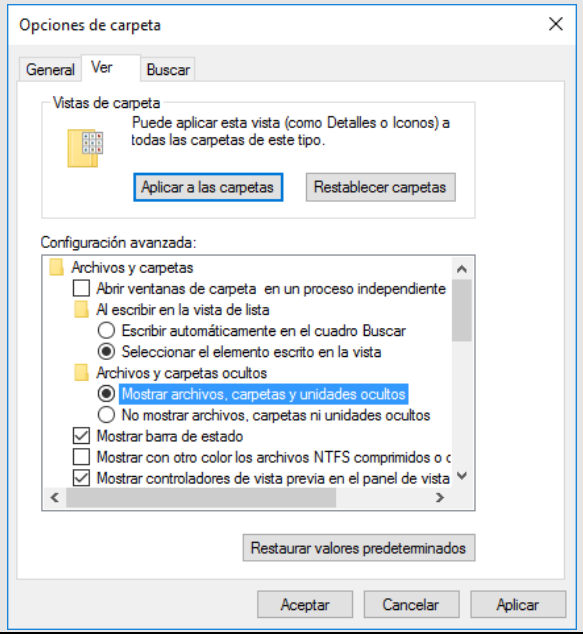
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

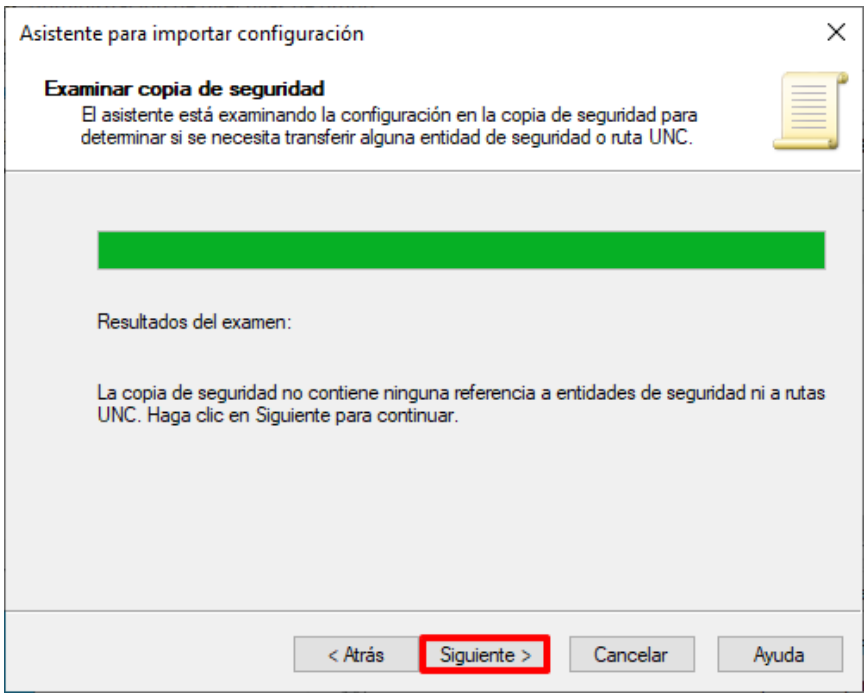
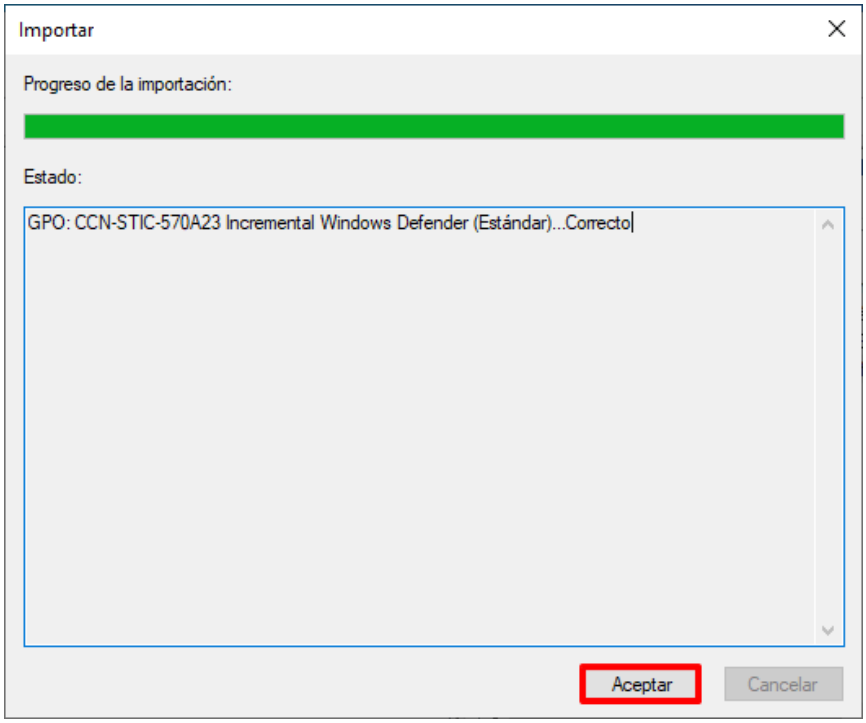
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

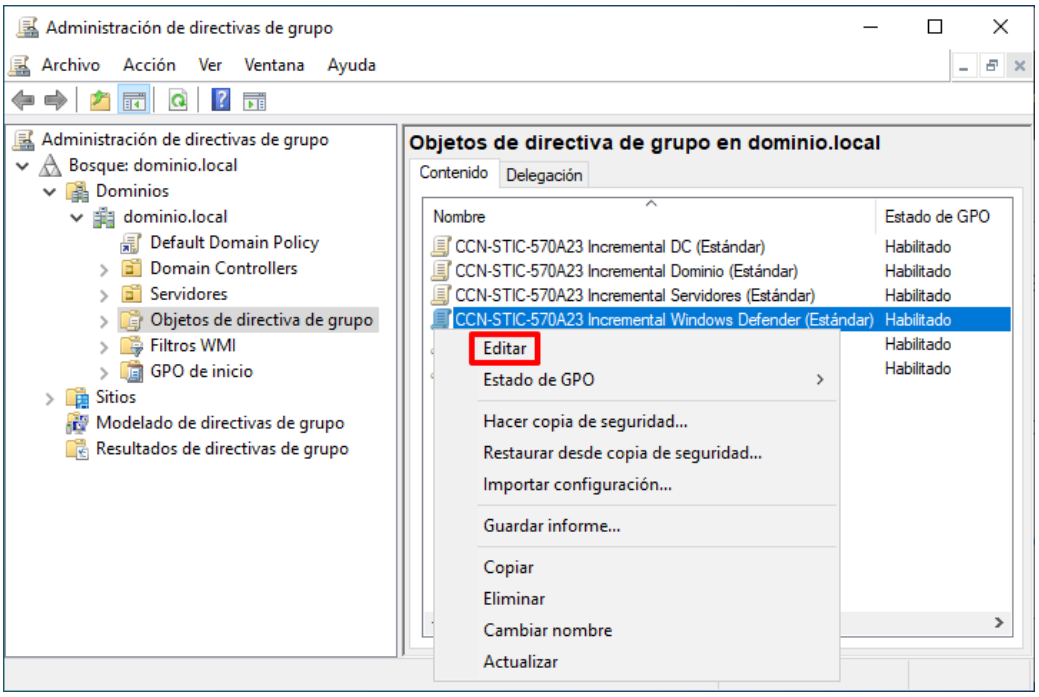
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO])**" y pulse el botón "Aceptar". 

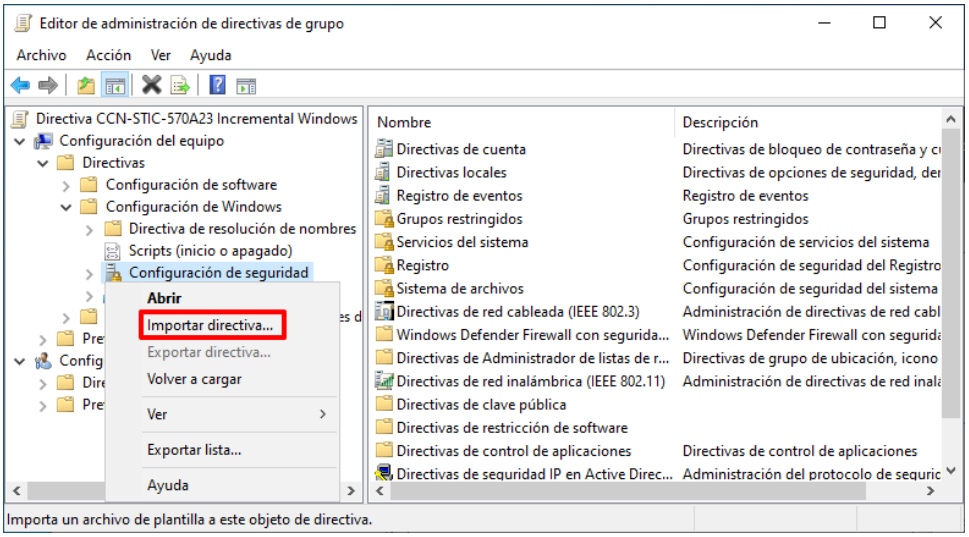
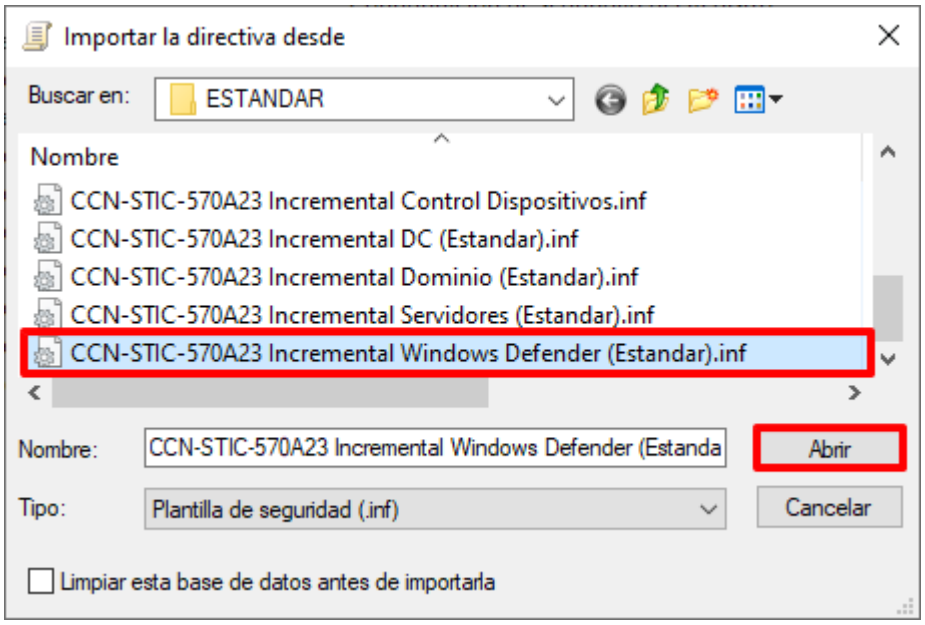
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

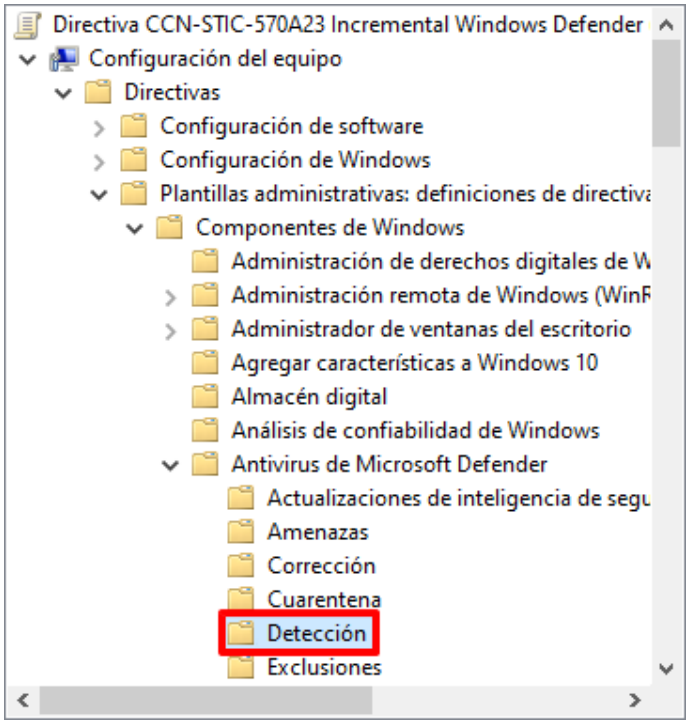
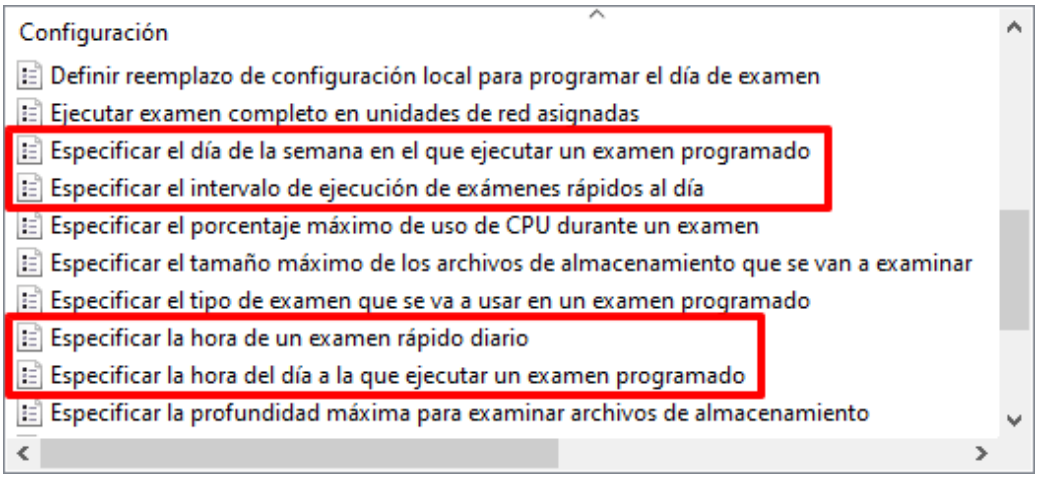
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

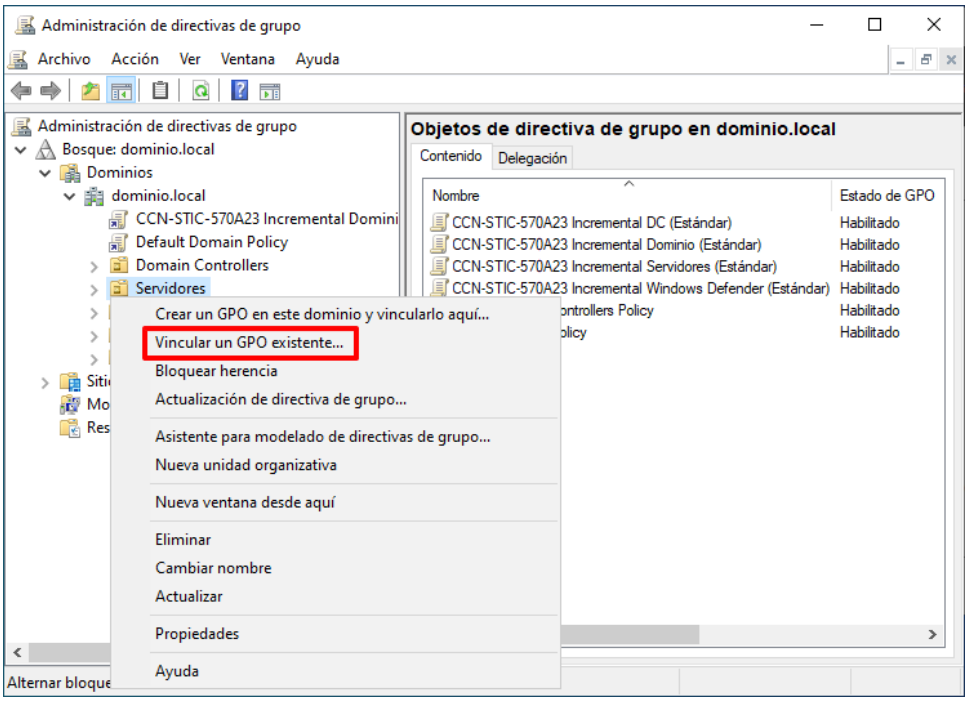
Paso	Descripción
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

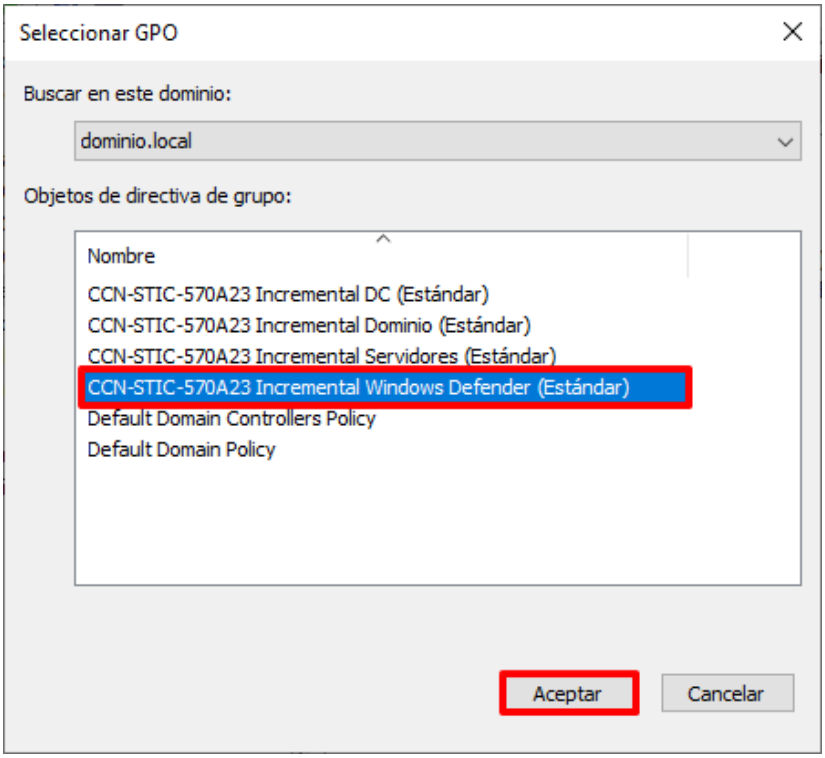
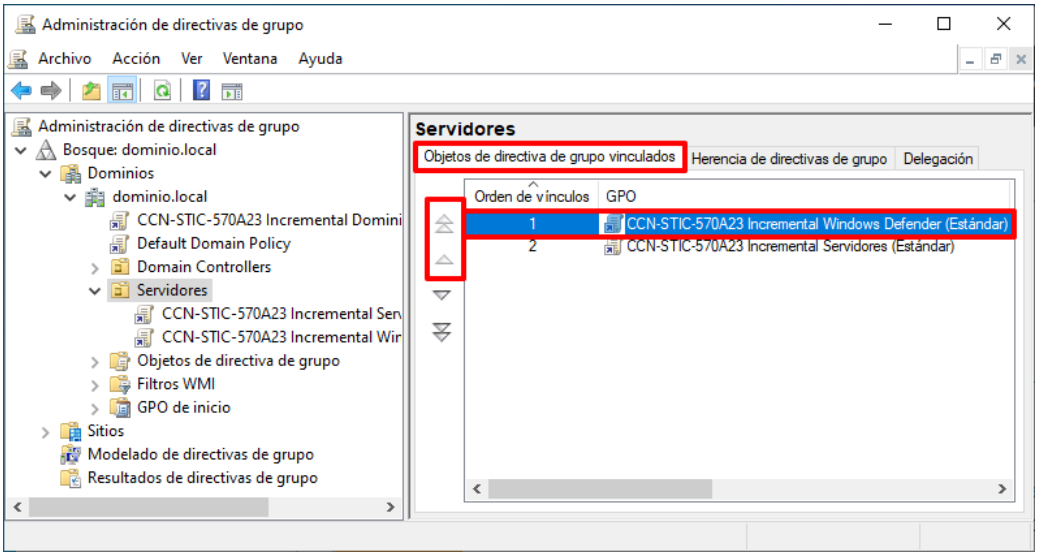
Paso	Descripción
14.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
15.	Para completar el asistente pulse sobre el botón “Finalizar”.
16.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

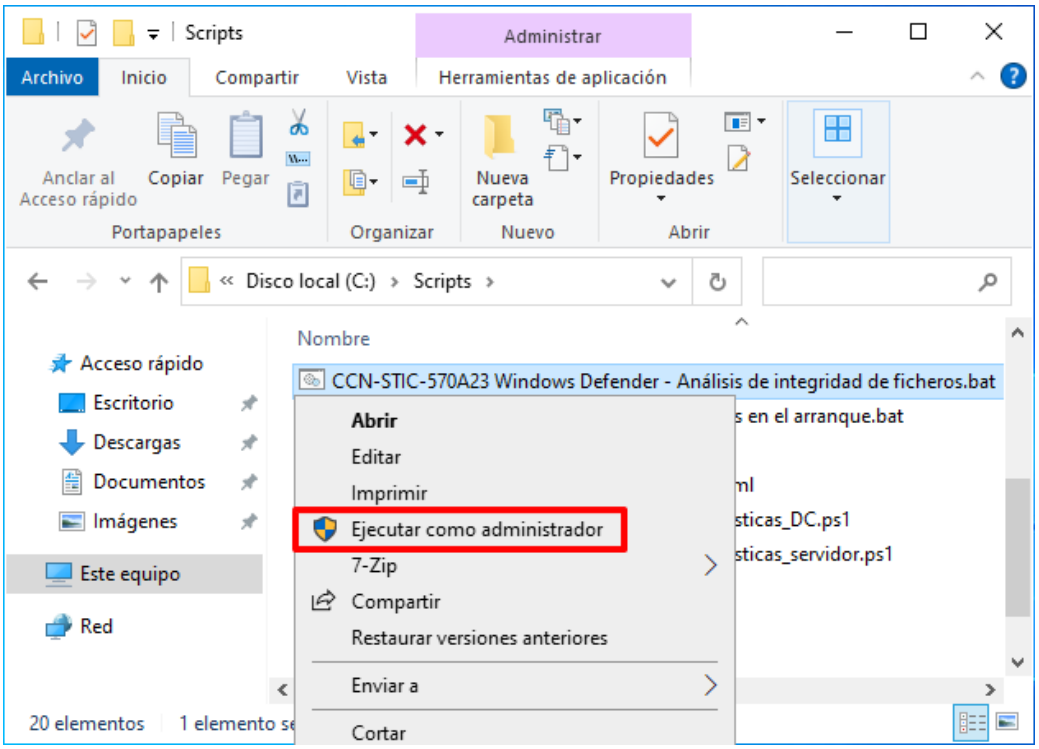
Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.

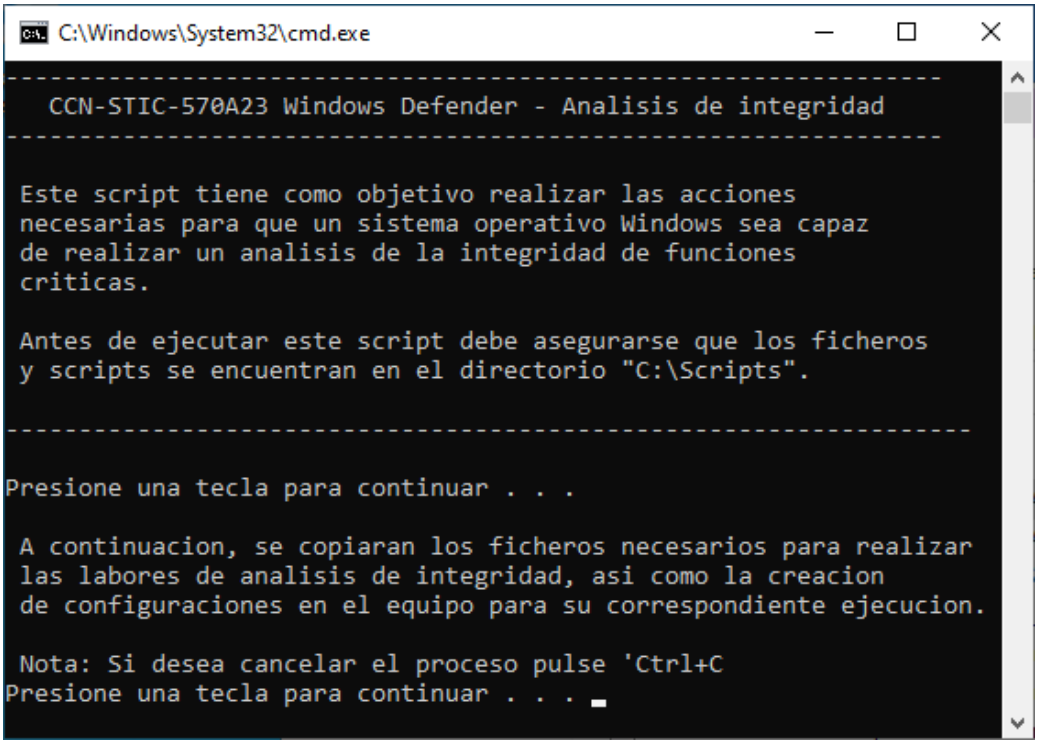
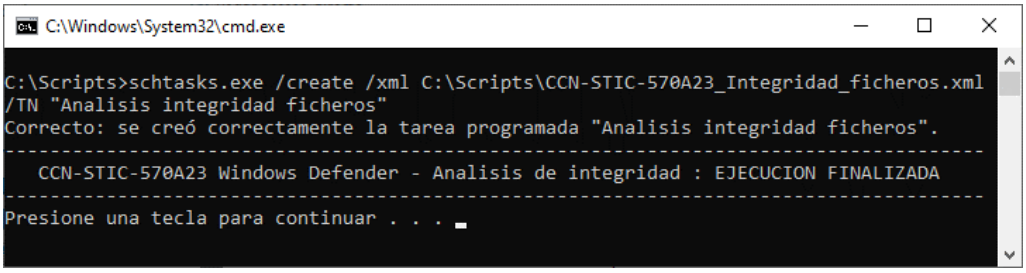
Paso	Descripción
19.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**. Seleccione con el botón derecho el nodo "Configuración de seguridad" y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO]).inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

Paso	Descripción
21.	A continuación, despliegue el nodo: **"CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Detección".** 
22.	En el panel derecho detecte las siguientes directivas. Deberá editar cada una de ellas, para definir la configuración que más se adecúe a su organización, de cara a la programación adecuada de los análisis de Windows Defender: – Especificar el día de la semana en el que ejecutar un examen programado – Especificar el intervalo de ejecución de exámenes rápidos al día – Especificar la hora de un examen rápido diario – Especificar la hora del día a la que ejecutar un examen programado 

Paso	Descripción
23.	Las directivas configuradas anteriormente se encuentran definida del siguiente modo: – Especificar el día de la semana en el que ejecutar un examen programado: Domingo – Especificar el intervalo de ejecución de exámenes rápidos al día: 24 horas – Especificar la hora de un examen rápido diario: 60 (1:00 [formato 24 horas]) – Especificar la hora del día a la que ejecutar un examen programado: 120 (2:00 [formato 24 horas])
24.	Cierre la ventana “Editor de administración de directivas de grupo”.
25.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de antivirus y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración. En este ejemplo se hace uso de la Unidad Organizativa “Servidores”, creada para tal fin.

Paso	Descripción
26.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO])" y pulse "Aceptar".  **Nota:** Seleccione el objeto GPO configurado acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
27.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

Paso	Descripción
28.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.
29.	A continuación, diríjase al directorio "C:\Scripts", haga clic derecho sobre el fichero "CCN-STIC-570A23 Windows Defender – Análisis de integridad de ficheros.bat" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Identifique los servidores y Controladores de Dominio que requieran la configuración del servicio de antivirus y ejecute el fichero en cada uno de los mismos.
30.	Pulse una tecla para continuar.

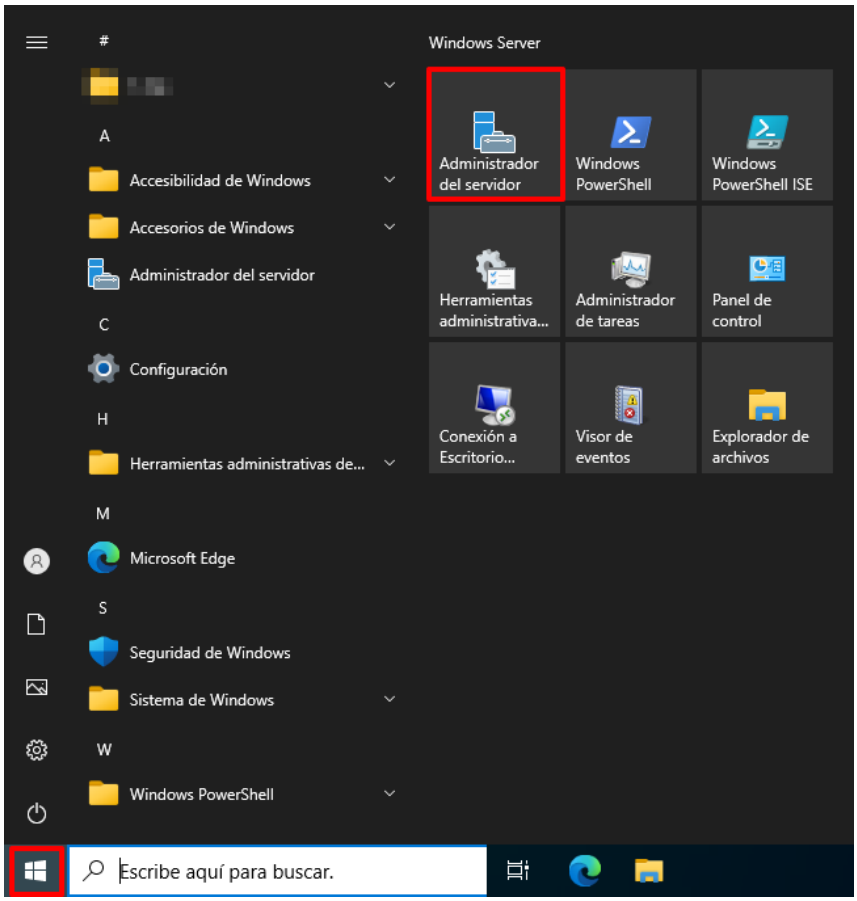
Paso	Descripción
31.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 
32.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
33.	Con esto habrá configurado el equipo para que se realice una comprobación de la integridad de ficheros esenciales del sistema operativo. **Nota:** Podrá editar la tarea programa generada con el objetivo de incluir cualquier fichero que desee analizar y comprobar.

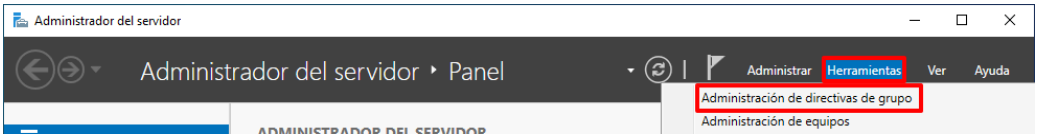
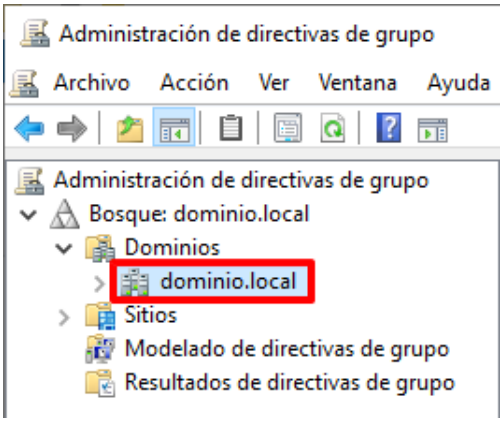
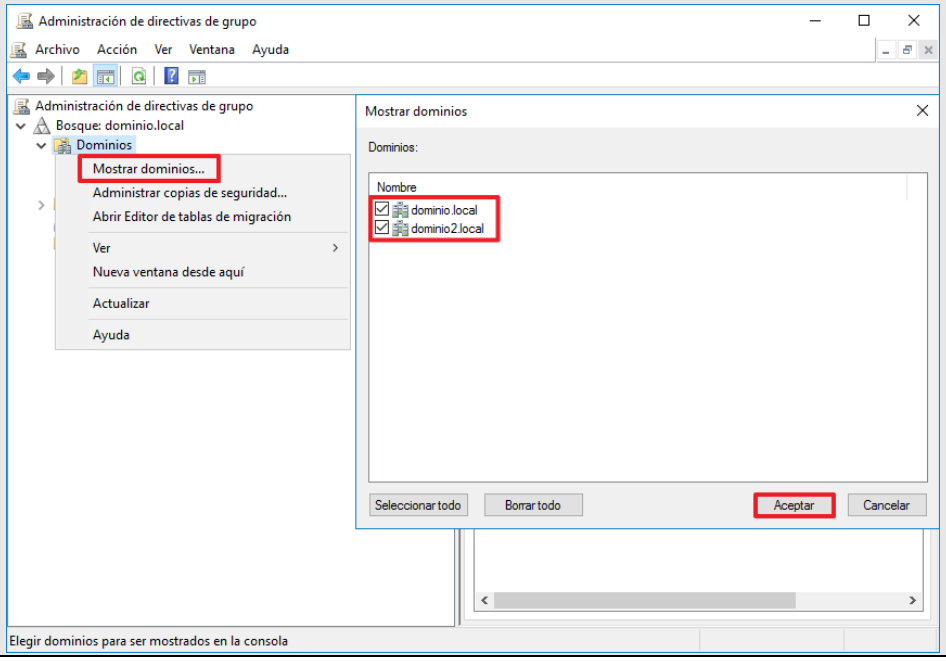
ANEXO B.3.1. PROTECCIÓN FRENTE A CÓDIGO DAÑINO (USO OFICIAL – MATERIAS CLASIFICADAS)

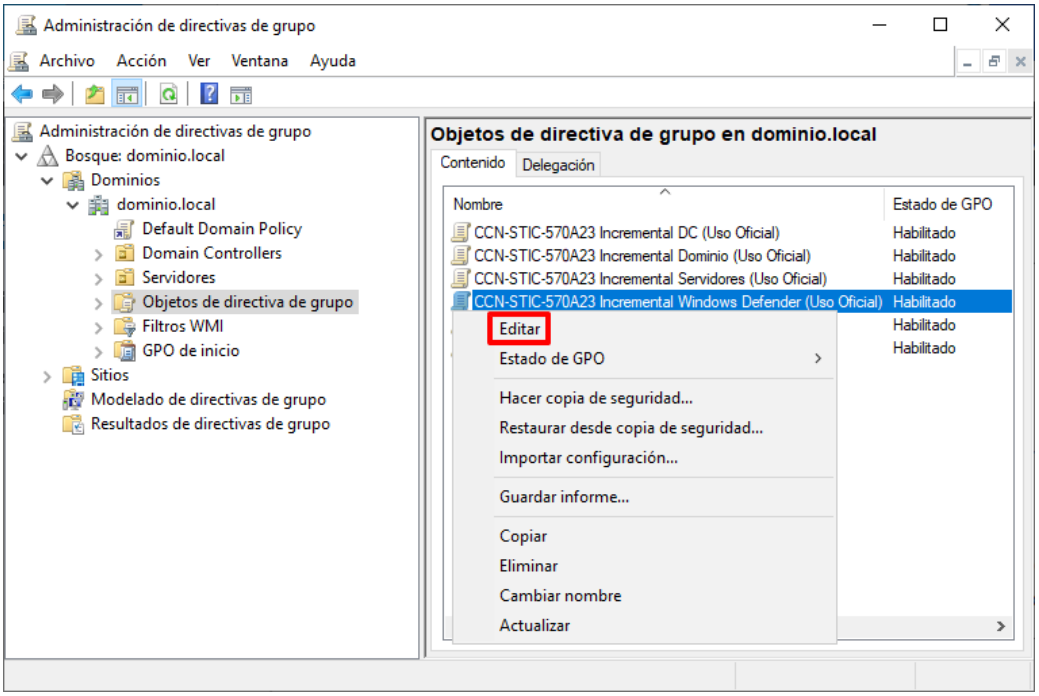
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

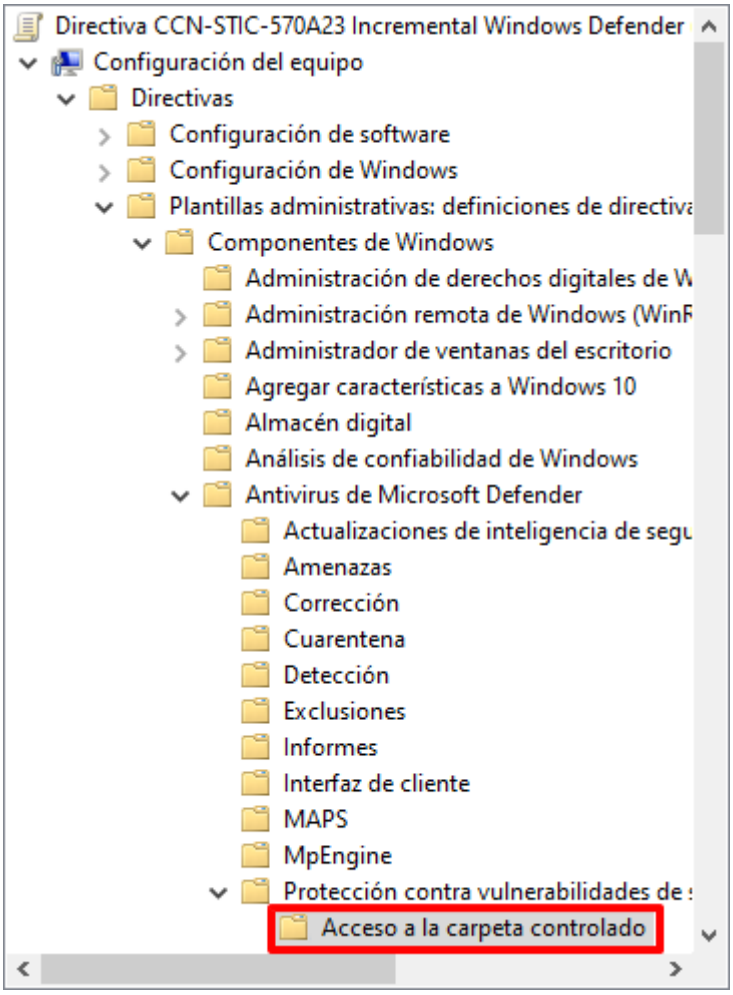
Las configuraciones definidas bajo el presente apartado tratan de impedir las modificaciones no autorizadas bajo directorios protegidos por el software contra código dañino, evitando de este modo la infección contra ramsonware.

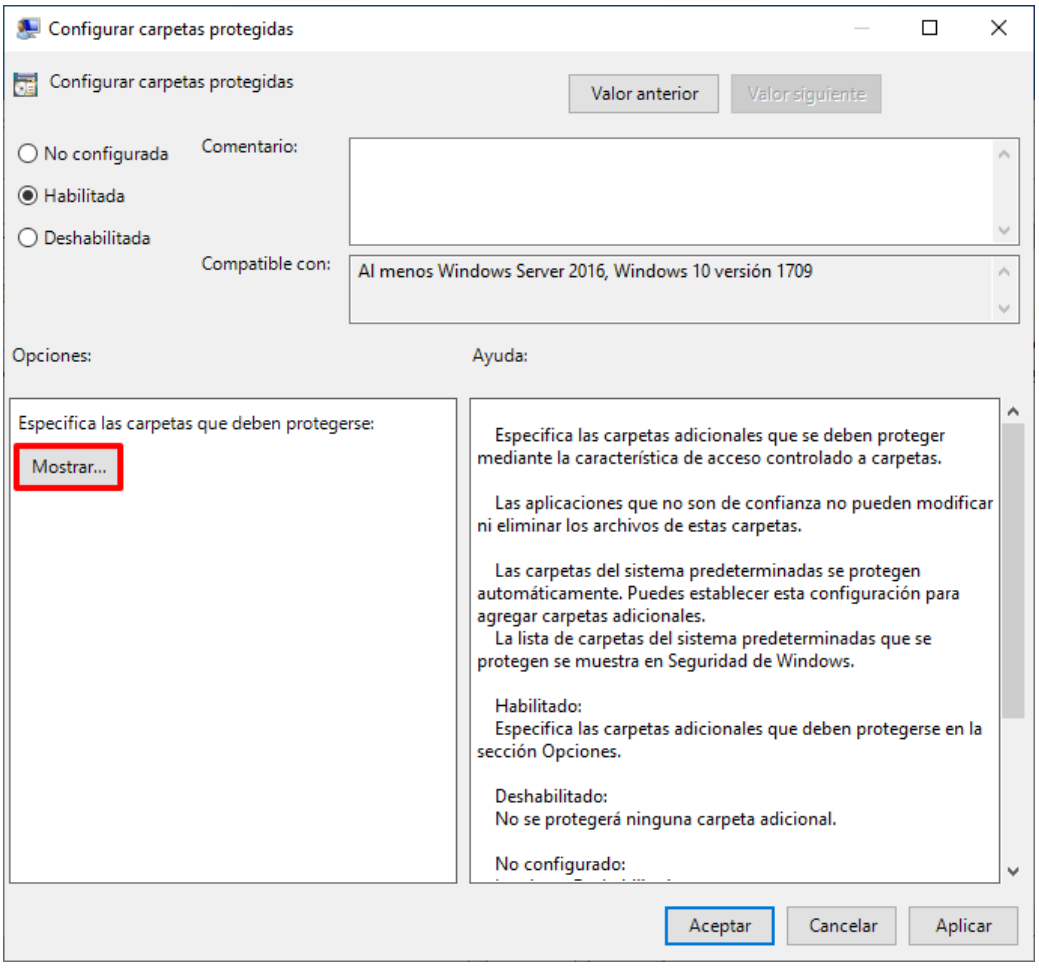
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

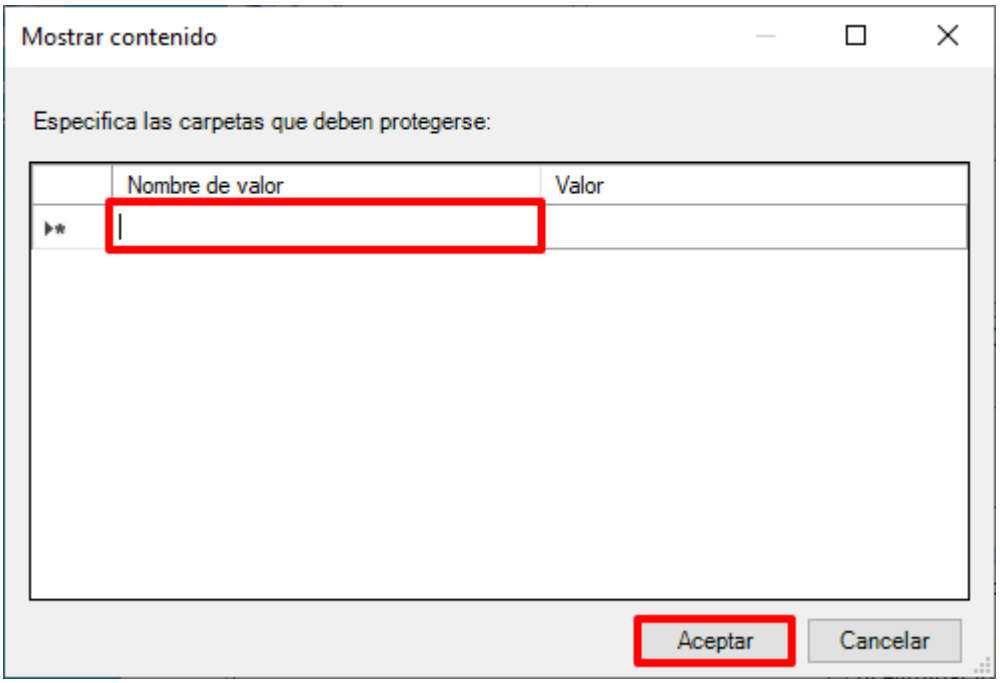
Paso	Descripción
34.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
35.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.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

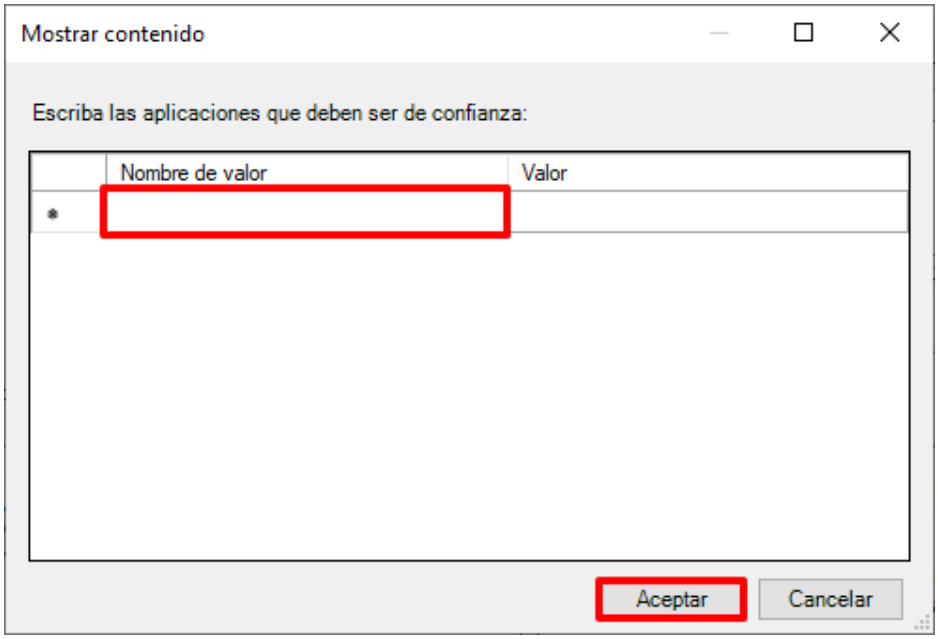
Paso	Descripción
36.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
37.	Una vez abierta la consola, seleccione: **“Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. Hasta que se indique lo contrario,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

Paso	Descripción
38.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
39.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.

Paso	Descripción
40.	A continuación, despliegue el nodo: **"CCN-STIC-570A23 Incremental Windows Defender ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Protección contra vulnerabilidades de seguridad de Microsoft Defender → Acceso a la carpeta controlado".** 

Paso	Descripción
41.	En el panel derecho haga doble clic sobre la directiva: **"Configurar carpetas protegidas"**. En la nueva ventana emergente pulse sobre el botón "Mostrar…". 

Paso	Descripción
42.	A continuación, sobre la ventana “Mostrar contenido”, deberá incluir las rutas absolutas de aquellas carpetas que considere que deban estar protegidas. Pulse “Aceptar” cuando haya finalizado.  **Nota:** Por defecto, el sistema operativo protege las siguientes rutas: - C:\Users\<username>\Documents - C:\Users\Public\Documents - C:\Users\<username>\Pictures - C:\Users\Public\Pictures - C:\Users\Public\Videos - C:\Users\<username>\Videos - C:\Users\<username>\Music - C:\Users\Public\Music - C:\Users\<username>\Favorites
43.	De forma análoga a lo realizado en los pasos anteriores, haga doble clic sobre la directiva **“Configurar aplicaciones permitidas”** y a continuación pulse sobre el botón “Mostrar…”.

Paso	Descripción
44.	A continuación, defina las aplicaciones que desee que Microsoft Defender excluya de su bloqueo de ejecución. Pulse “Aceptar” cuando haya finalizado  **Nota:** Tenga en consideración que el Antivirus de Microsoft Defender determina automáticamente que aplicaciones son de confianza. Por ello, esta configuración pretende excluir aquellas aplicaciones que el antivirus bloquee pero que se requieran de su ejecución.
45.	Cierre la ventana “Editor de administración de directivas de grupo”.

ANEXO B.3.2. PROTECCIÓN FRENTE A CÓDIGO DAÑINO (MATERIAS CLASIFICADAS)

El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso del perfil MATERIAS CLASIFICADAS.

Las configuraciones definidas bajo el presente apartado son las siguientes:

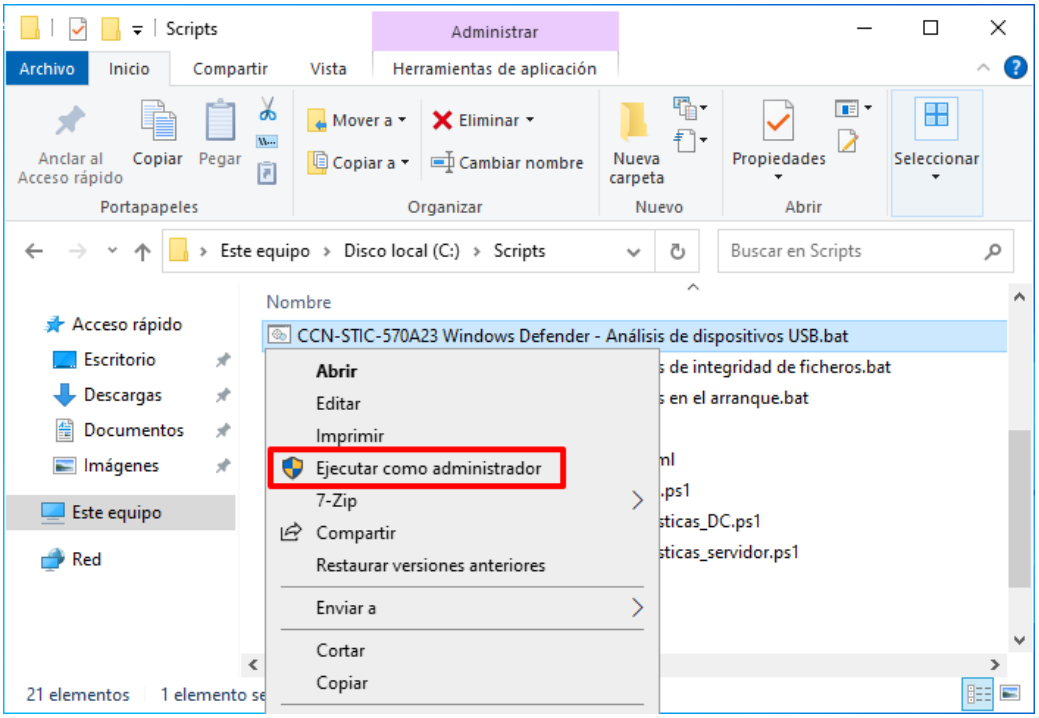
a) Análisis de dispositivos de almacenamiento extraíble cuando estos se conectan al equipo.

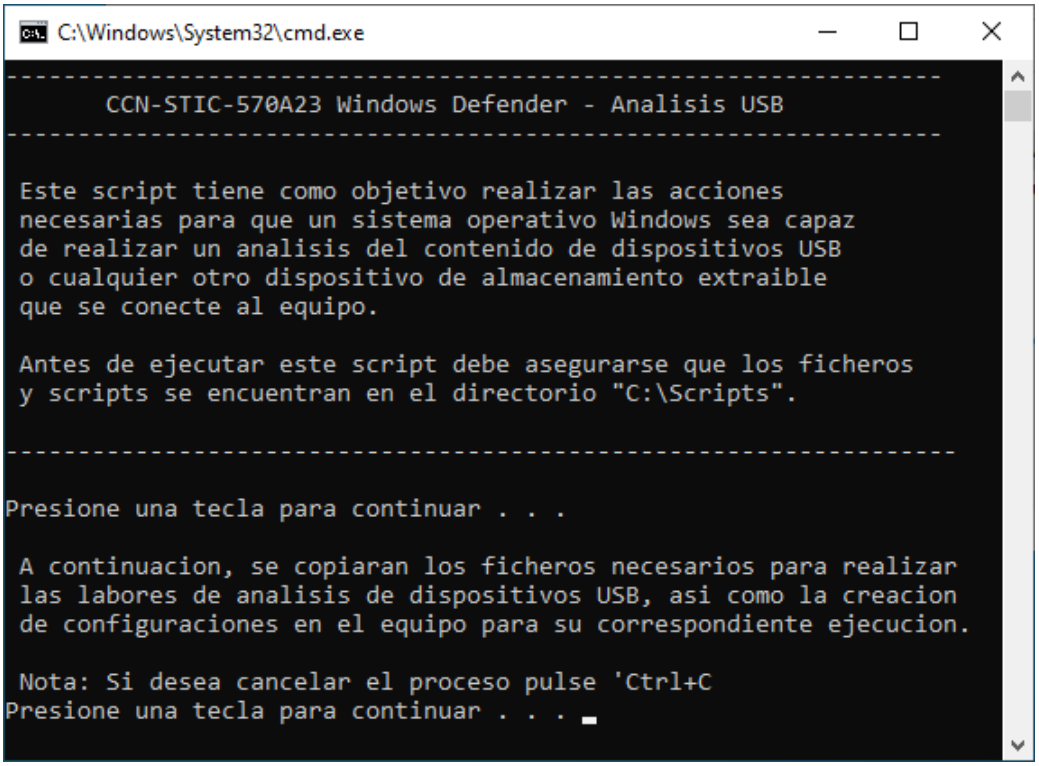
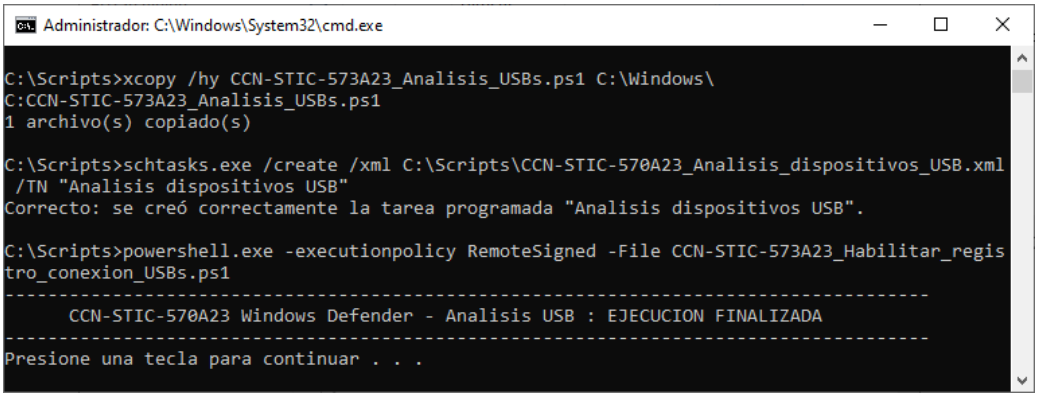
b) Análisis del sistema operativo en el arranque del sistema.

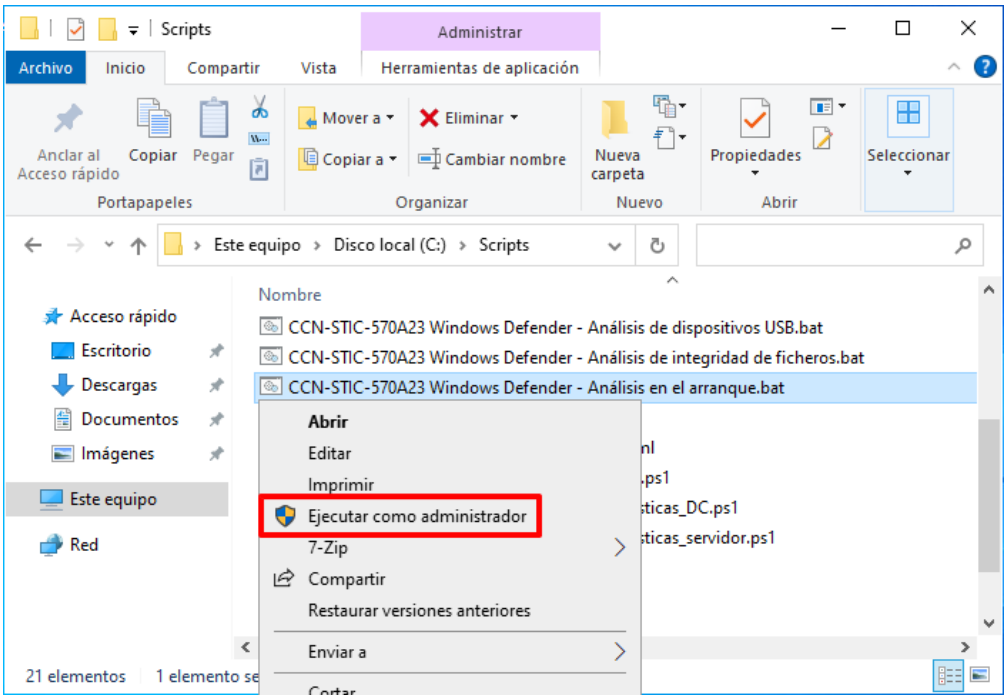
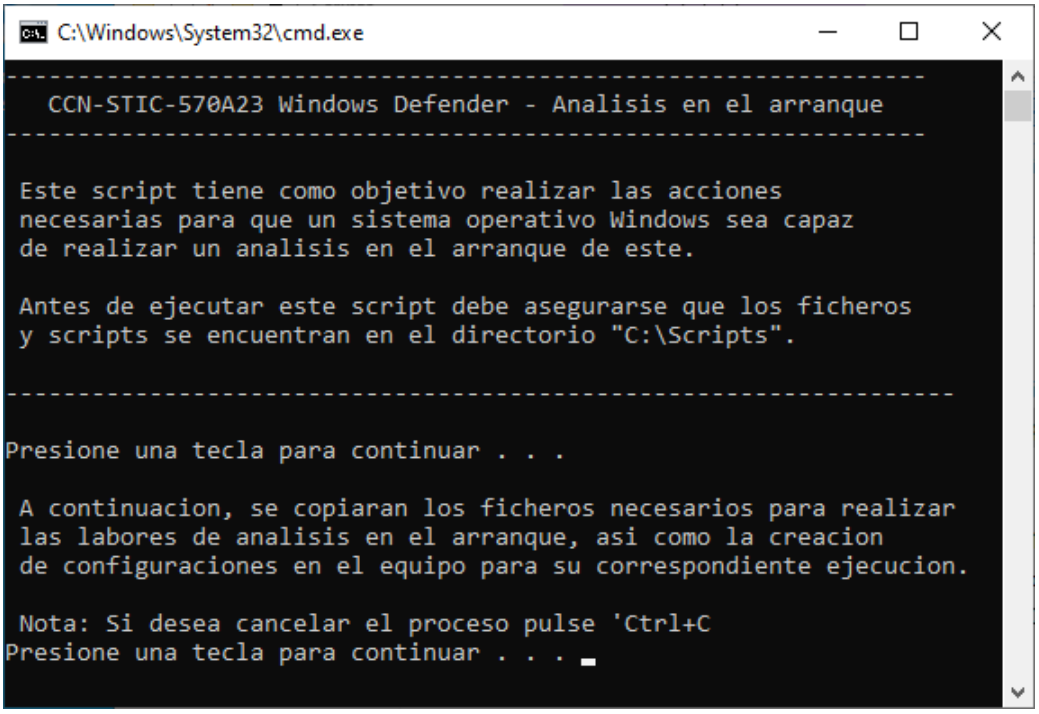
No se considera de aplicación las configuraciones del presente apartado si no se han aplicado el resto de configuraciones de esta herramienta según el punto ANEXO B.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO.

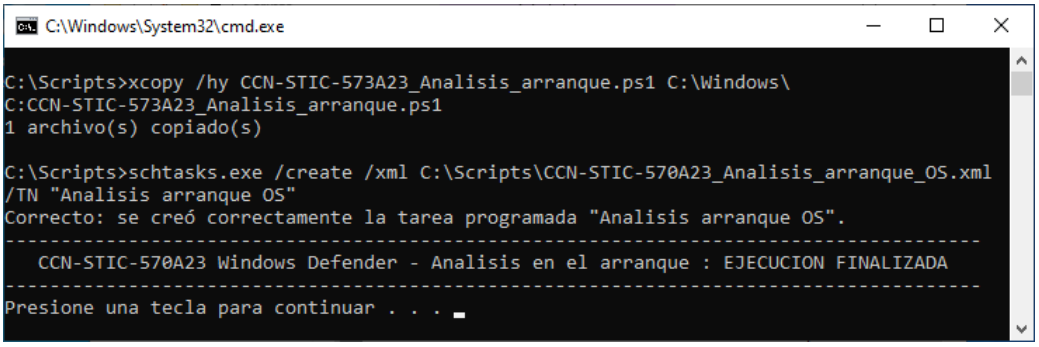
Tenga en consideración que estas configuraciones pueden afectar al rendimiento del sistema operativo.

Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Materias Clasificadas**, no siendo obligatorio en ningún otro perfilado.

Paso	Descripción
1.	Inicie sesión en un servidor perteneciente al dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-570A23 Windows Defender – Análisis de dispositivos USB.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
3.	Pulse cualquier tecla para continuar.

Paso	Descripción
4.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 
5.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
6.	Con esto habrá configurado el equipo para que se realice un análisis de los dispositivos de almacenamiento extraíble cada vez que se conecten al equipo.

Paso	Descripción
7.	De nuevo, en el directorio “C:\Scripts” haga clic derecho sobre el fichero “CCN-STIC-570A23 Windows Defender – Análisis en el arranque.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
8.	Pulse una tecla para continuar.
9.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 

Paso	Descripción
10.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
11.	Con esto habrá configurado el equipo para que se realice un análisis nada más se inicie el sistema operativo, así como los sectores de arranque de este.

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

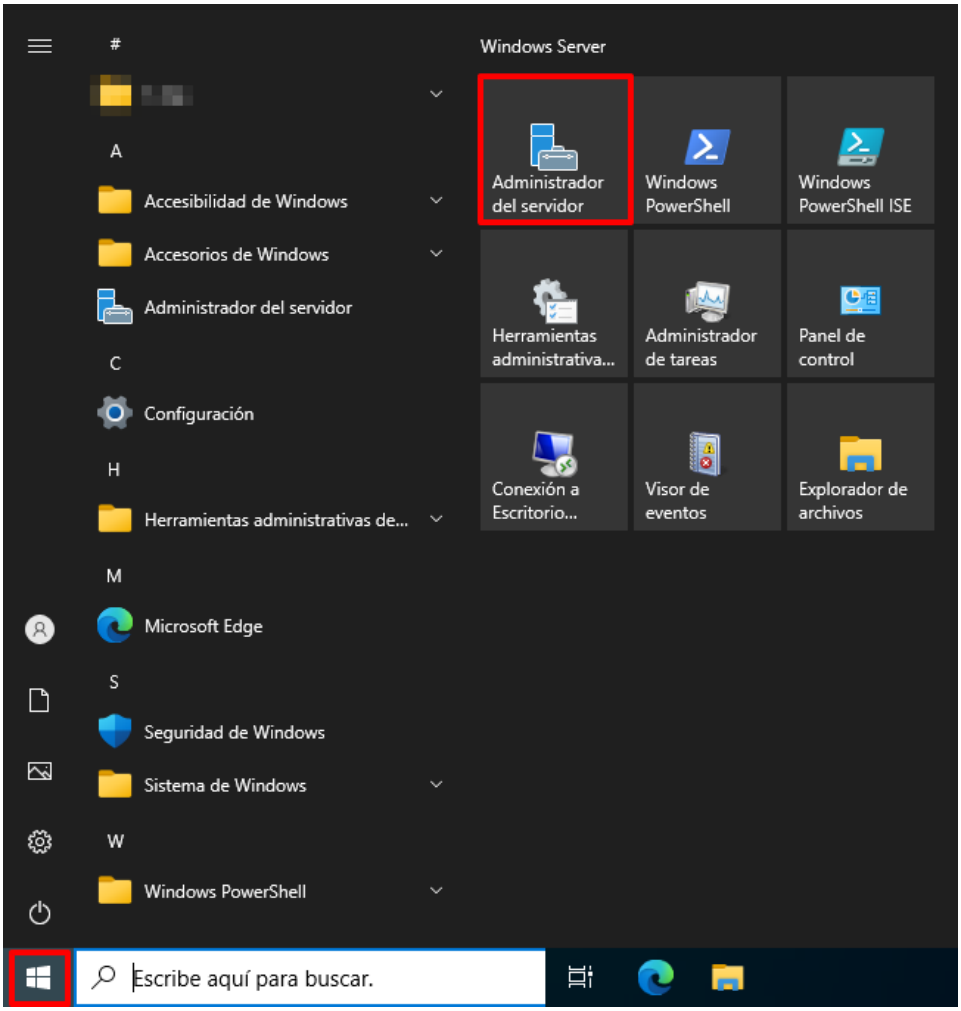
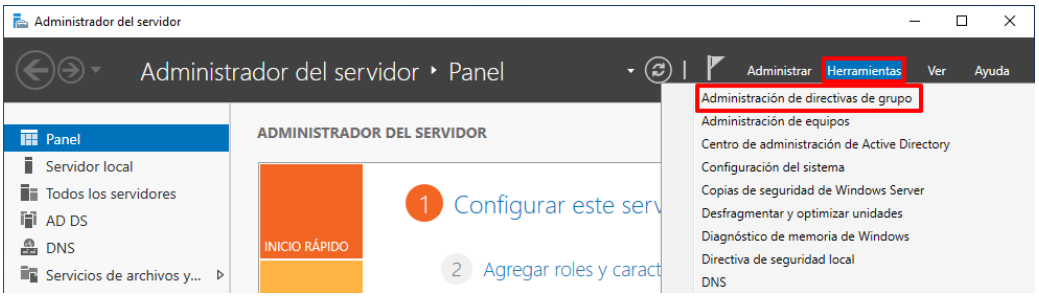
El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación del cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los servidores Windows Server.

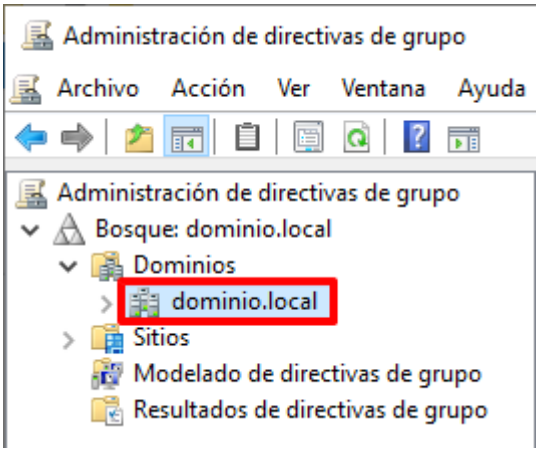
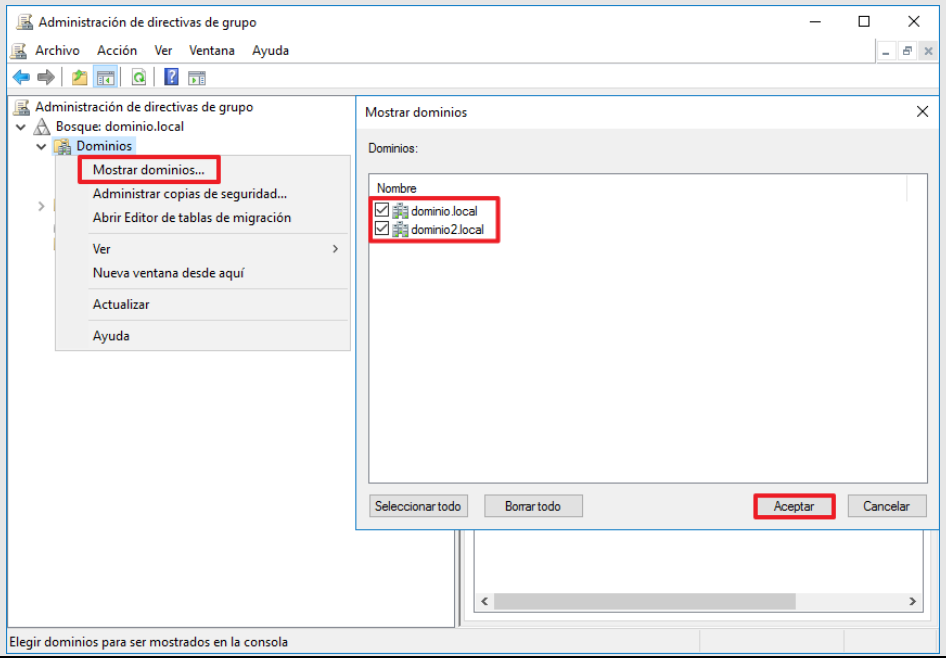
Debe tenerse en consideración que la implementación de un firewall de servidor dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que éste ofrece a la infraestructura. No se tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, en un servidor que actúe como Controlador de Dominio que en otro que funcione como servidor de ficheros exclusivamente.

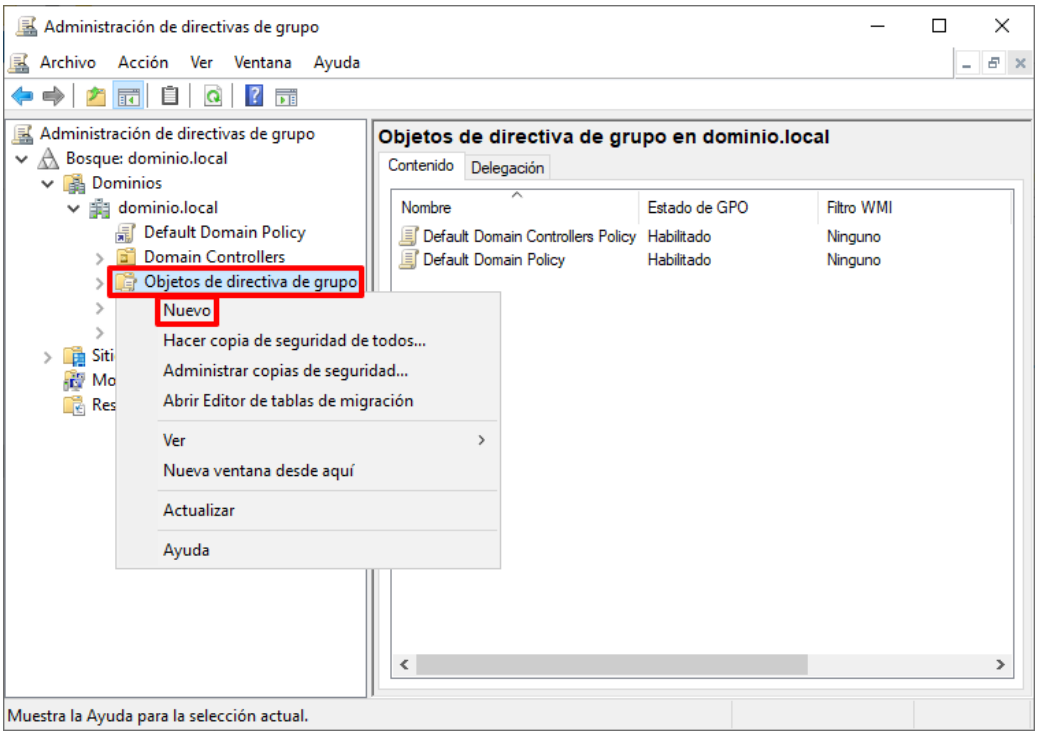
Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos para un conjunto de servidores web que sirven aplicaciones web por los puertos 80 y 443.

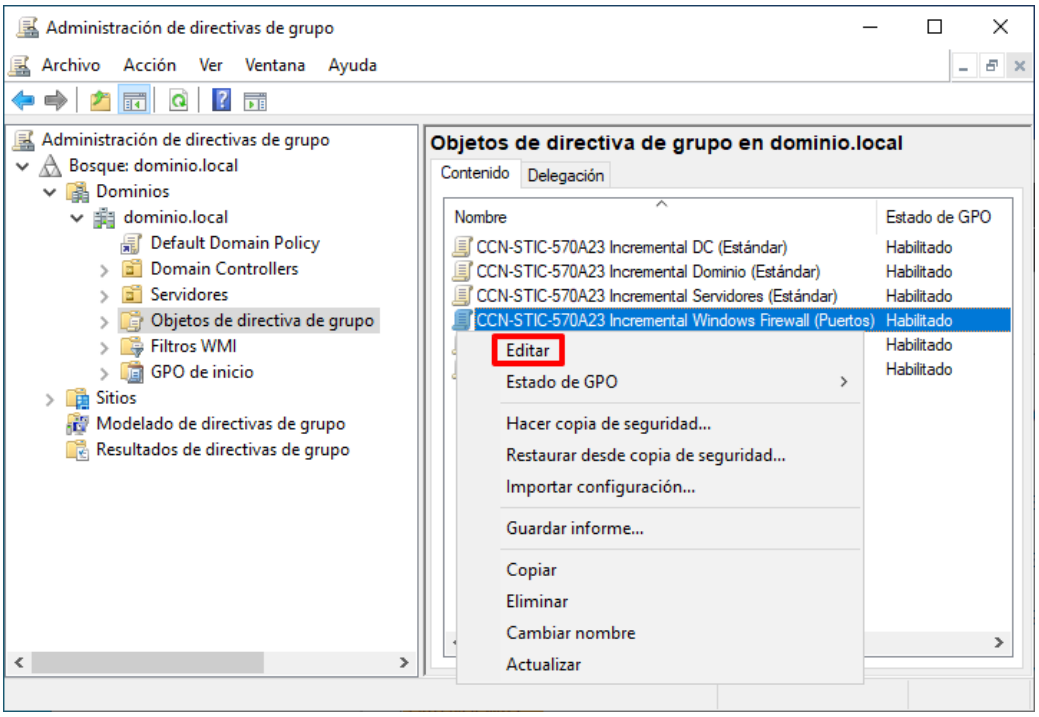
Por otro lado, si en su organización dispone de otro software que sustituya el firewall por defecto de Windows y este se encuentra habilitado y configurado podrá ignorar los siguientes pasos y continuar en el siguiente punto.

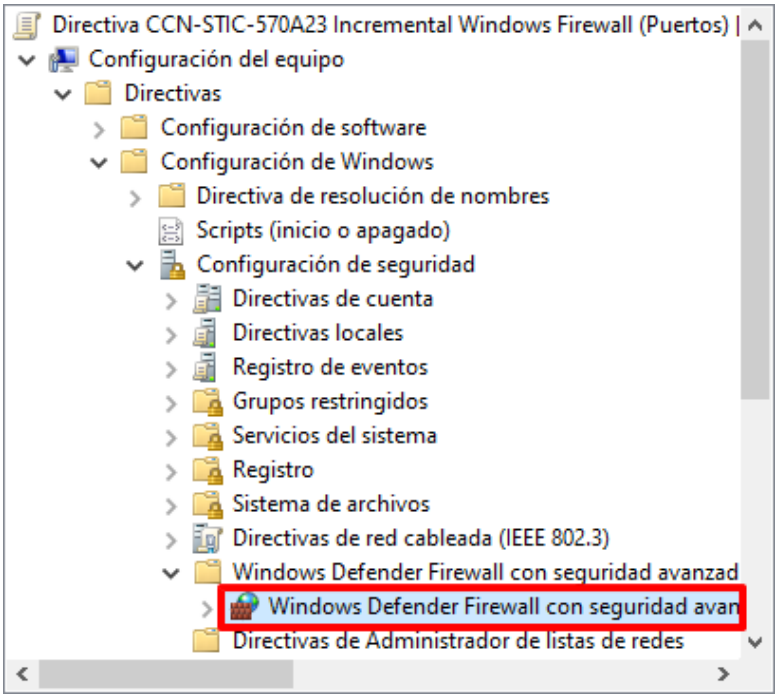
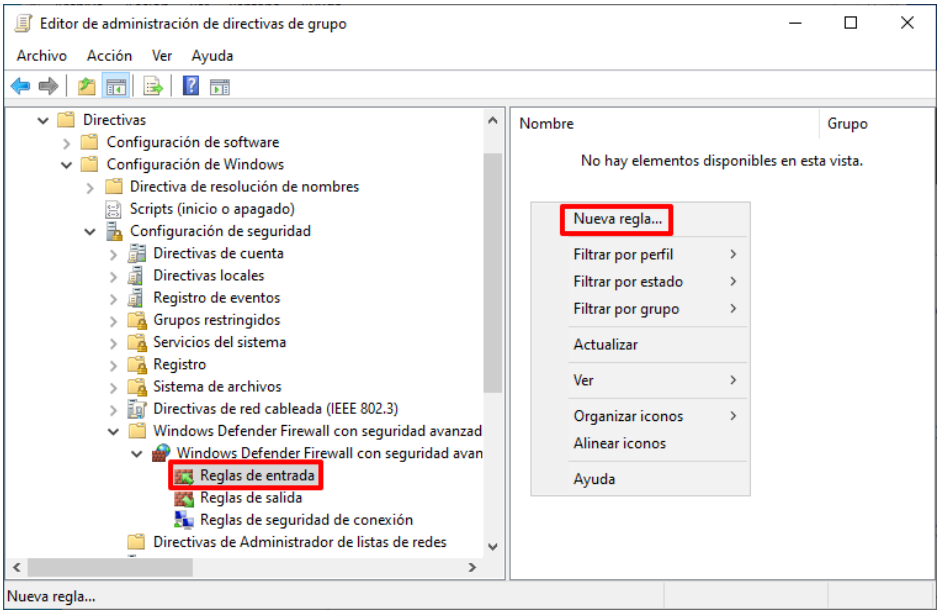
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

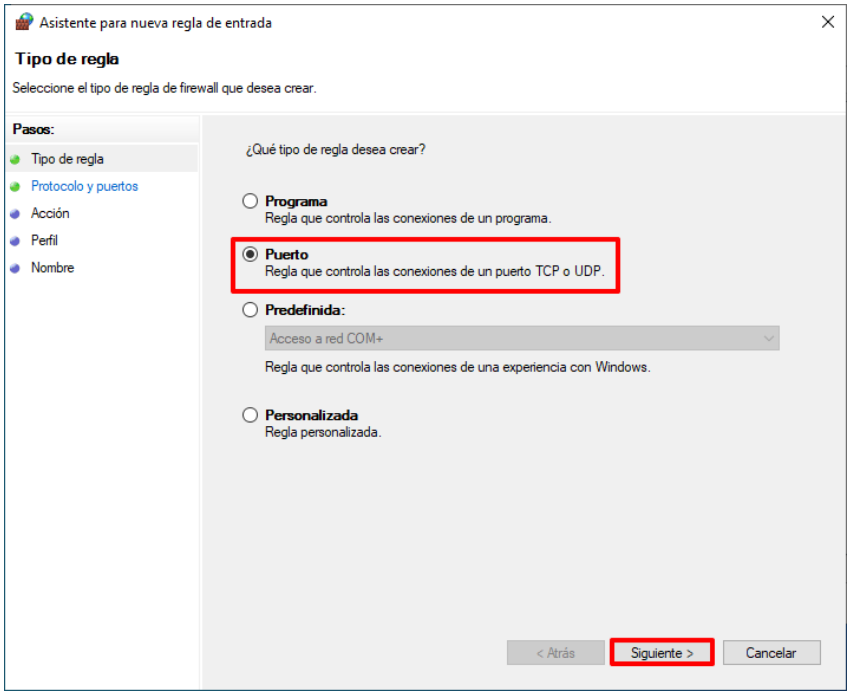
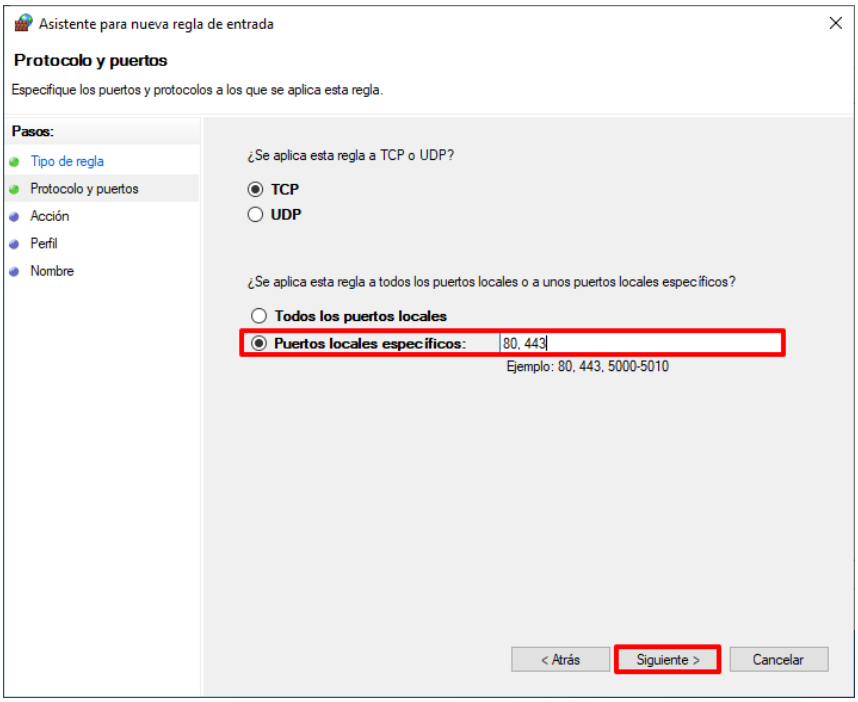
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

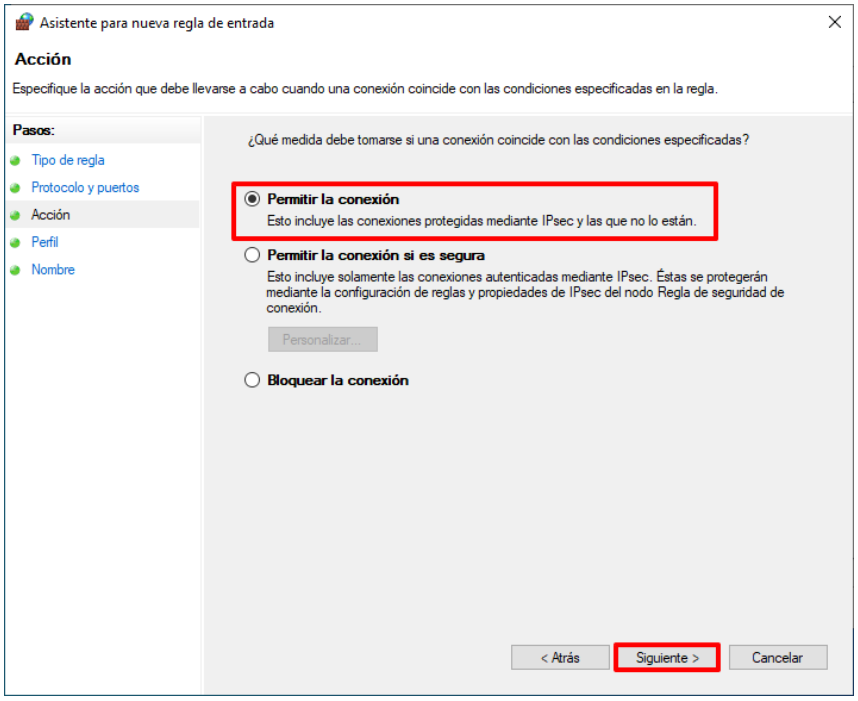
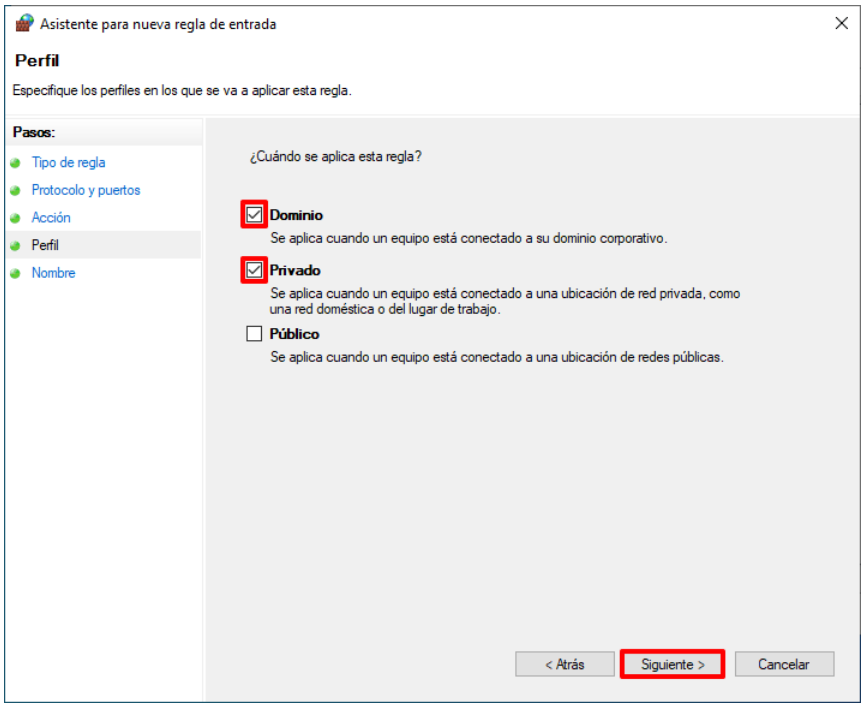
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

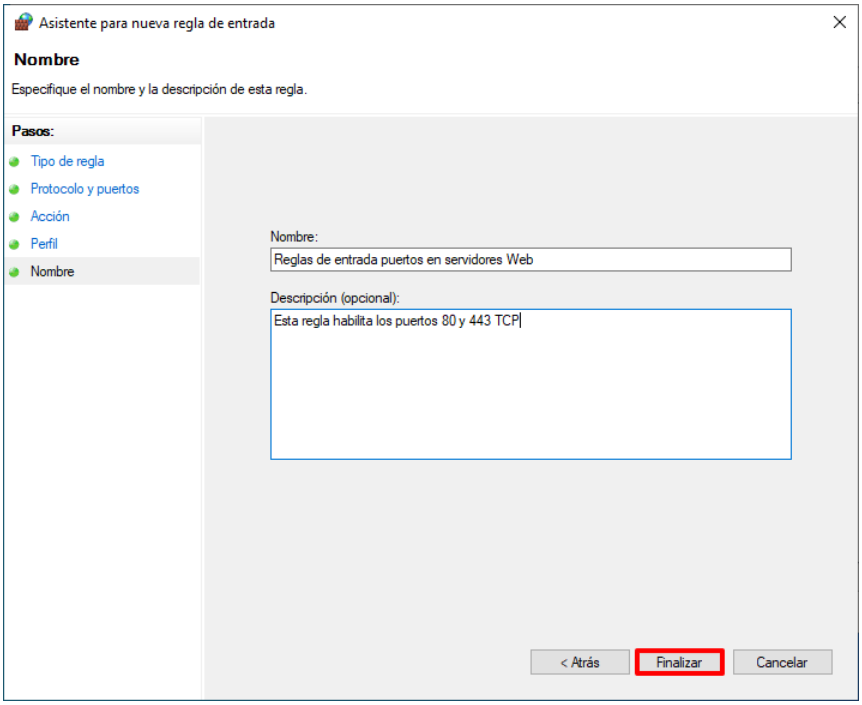
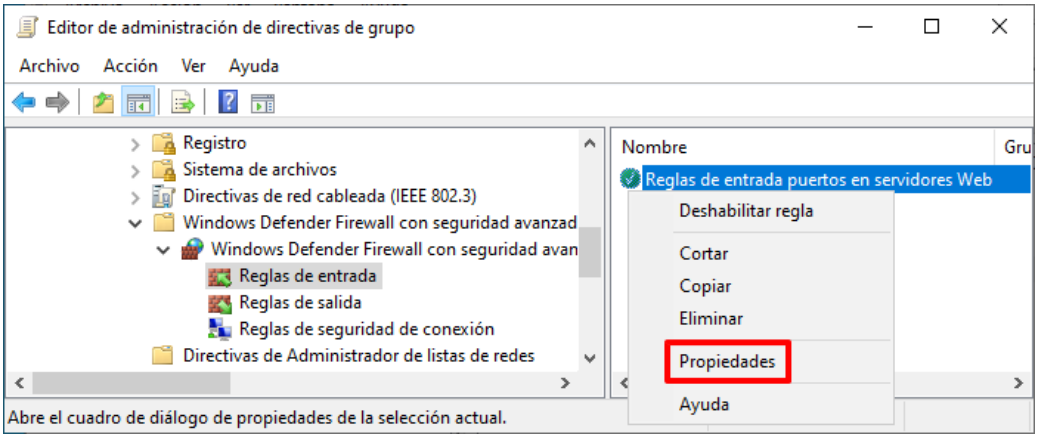
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Windows Firewall (Puertos)**" y pulse el botón "Aceptar". 

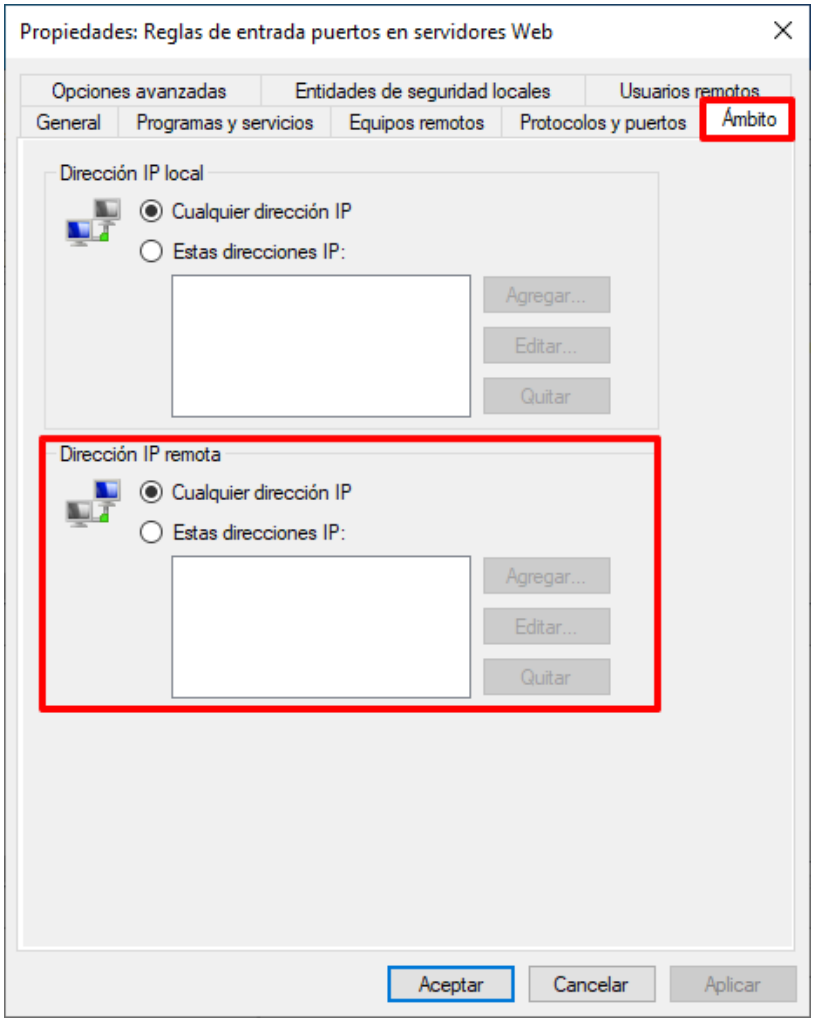
Paso	Descripción
7.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Windows Firewall (Puertos)” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá. 
8.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.

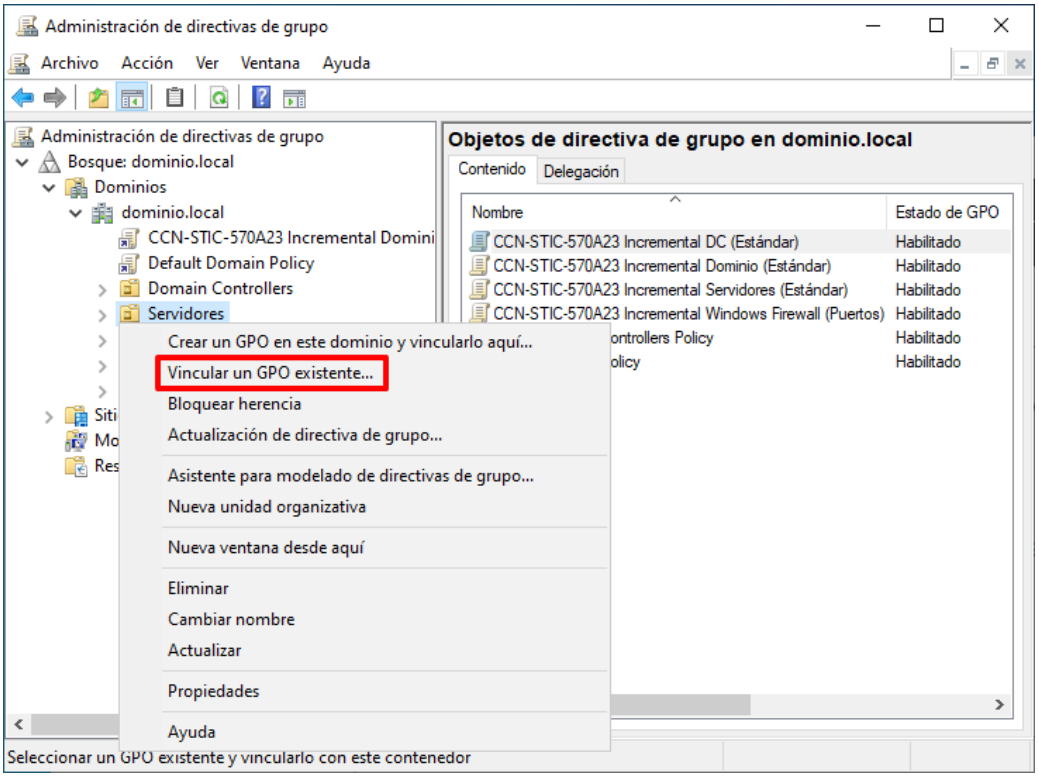
Paso	Descripción
9.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"CCN-STIC-570A23 Incremental Windows Firewall (Puertos) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada – LDAP://CN=..."**. 
10.	Despliegue el nodo "Windows Defender Firewall con seguridad avanzada y seleccione "Reglas de entrada". A continuación, pulse sobre con el botón derecho sobre un espacio en blanco en el panel derecho de la consola y seleccione "Nueva regla…". 

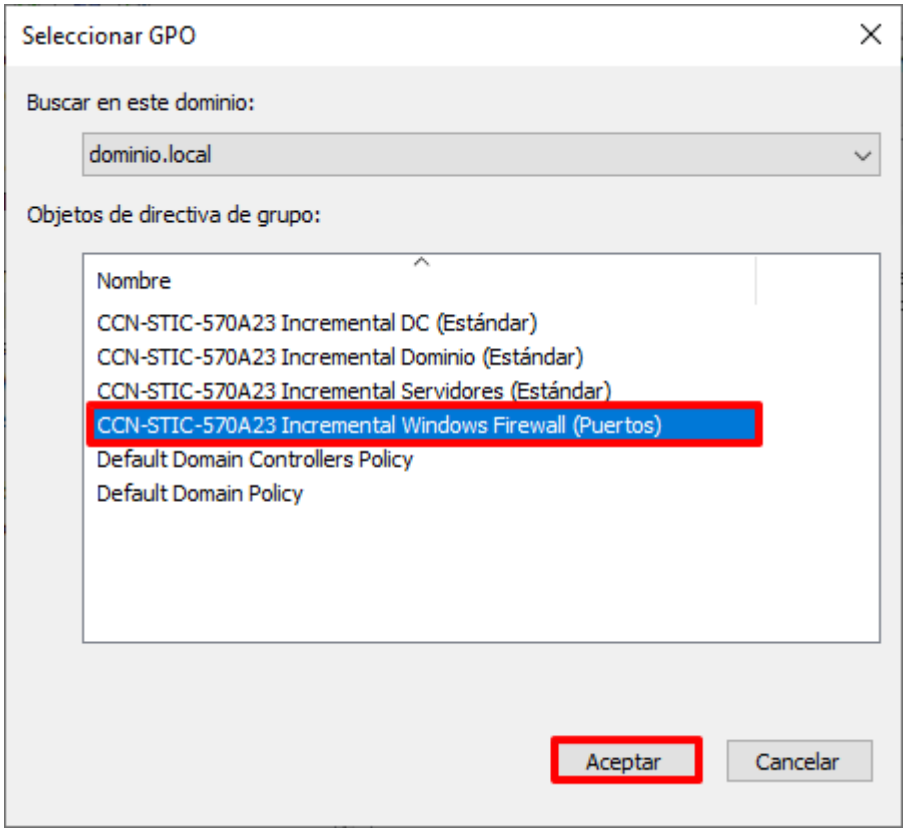
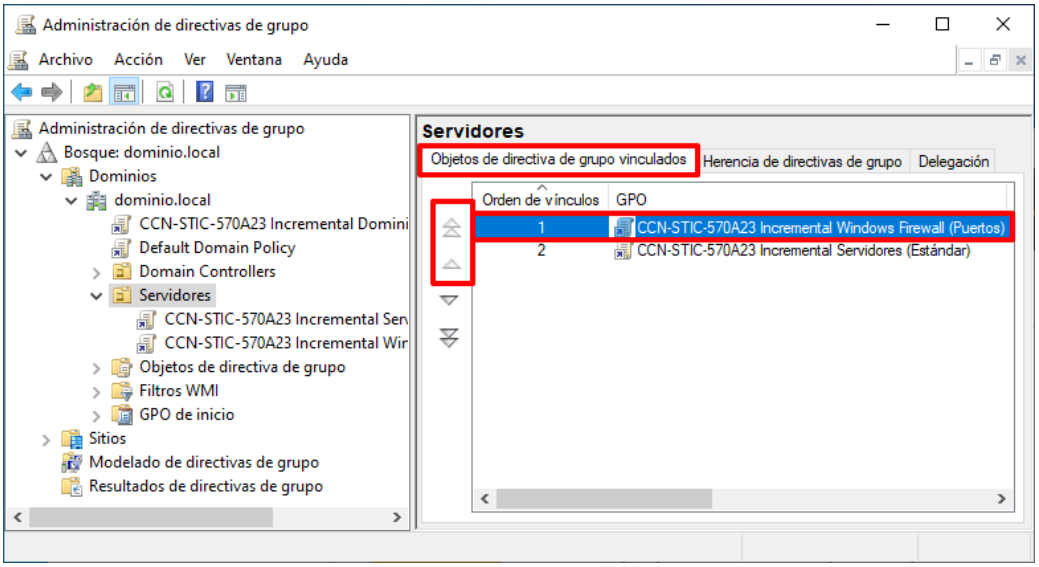
Paso	Descripción
11.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 
12.	En la opción de “Puertos locales específicos” introduzca “80, 443”. Si los servidores web escucharan peticiones por otros puertos, debería introducir también dichos puertos. Pulse el botón “Siguiente >”.  **Nota:** Deberá tener en consideración el protocolo, siendo en este ejemplo TCP.

Paso	Descripción
13.	En la pantalla de “Acción”, mantenga la configuración “Permitir la conexión” y pulse el botón “Siguiente >”. 
14.	En la ventana “Perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 

Paso	Descripción
15.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”. Puede asignar una descripción si lo desea. 
16.	La nueva regla ya se encuentra creada. Puede editarla pulsando con el botón derecho del ratón sobre la misma y seleccionando la opción “Propiedades”. 

Paso	Descripción
17.	Podría, por ejemplo, limitarse las IP remotas o rangos de redes que podrían conectarse a los servidores a través de los puertos 80 y 443. De forma predeterminada, se admite cualquier IP, pero podría establecerse un límite a las mismas mediante la pestaña “Ámbito”. 
18.	Podrá repetir los pasos anteriores en caso de necesidad de habilitar otros puertos de conexión.
19.	Cierre la ventana “Editor de administración de directivas de grupo”.

Paso	Descripción
20.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de cortafuegos y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración. En este ejemplo se hace uso de la Unidad Organizativa “Servidores”, creada para tal fin.

Paso	Descripción
21.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental Windows Firewall (Puertos)" y pulse "Aceptar". 
22.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

Paso	Descripción
23.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.

ANEXO B.5. COPIAS DE SEGURIDAD

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

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

Antes de continuar tenga en consideración los siguientes aspectos:

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

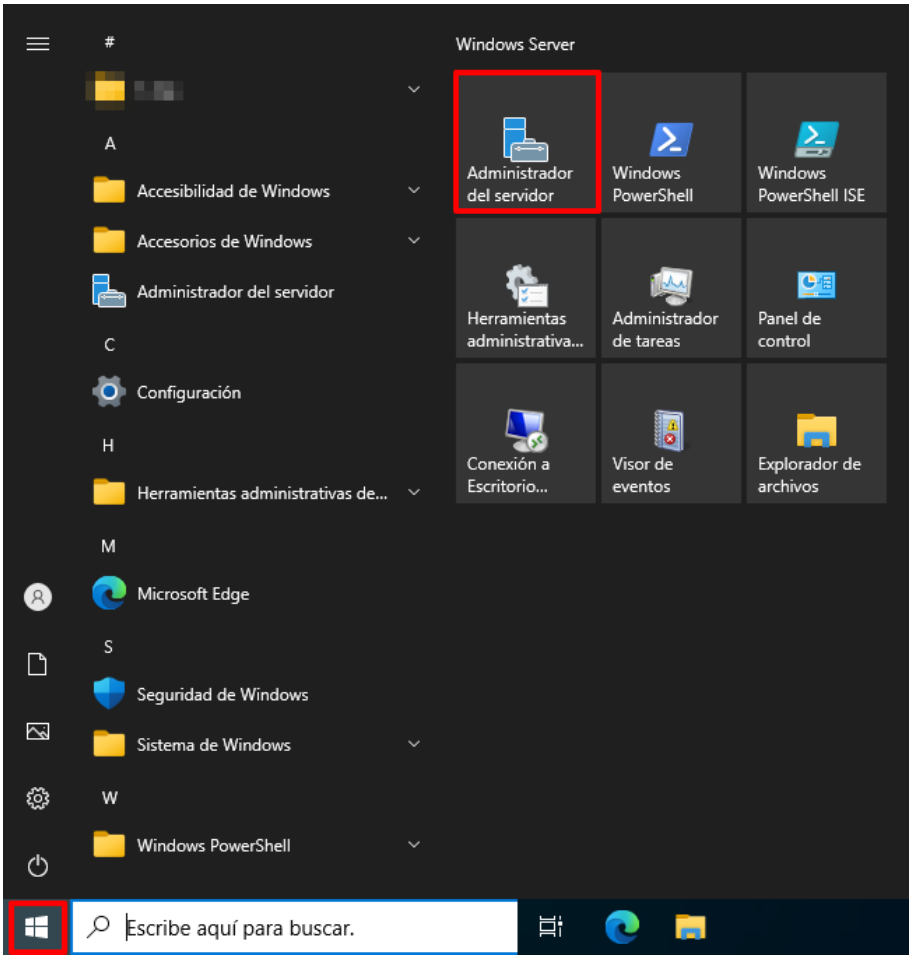
b) La característica "Copias de seguridad de Windows Server" deberá encontrarse implementada en los equipos donde se desea realizar la copia de seguridad.

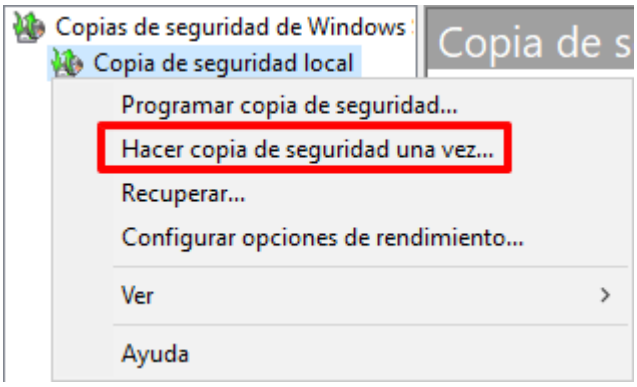
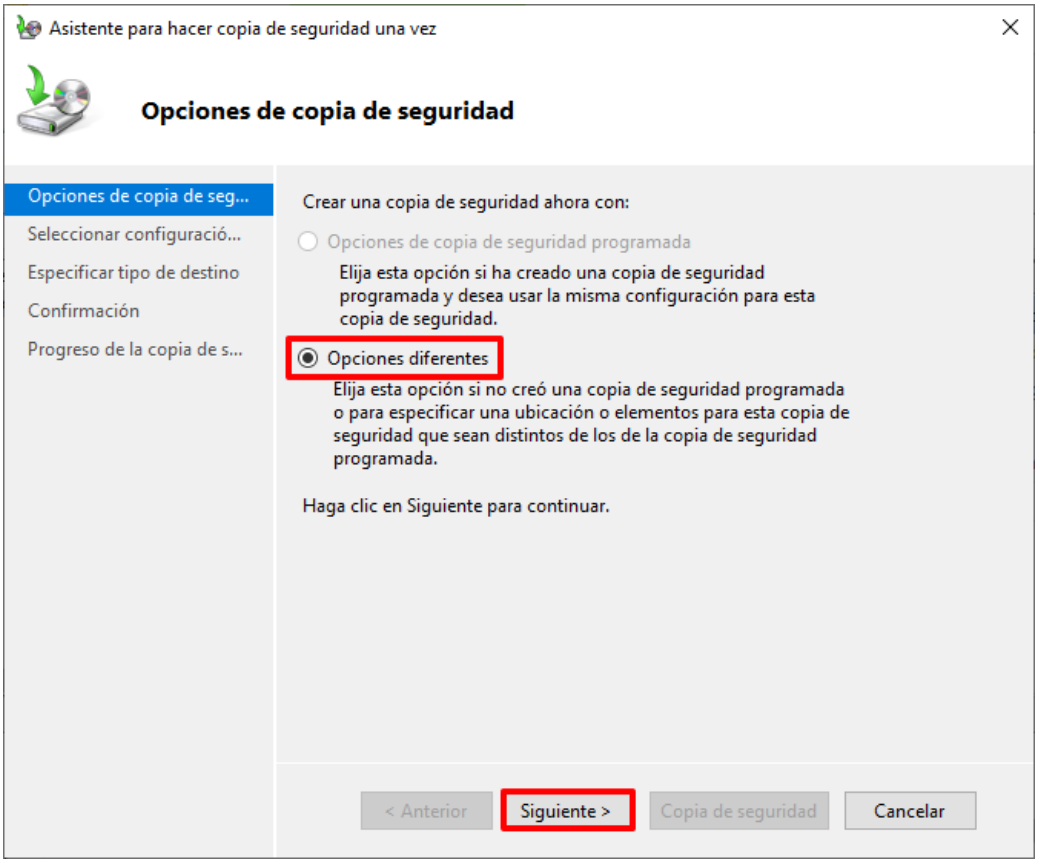
c) El uso de esta herramienta es de uso local por lo que no podrá utilizarse como mecanismo central de gestión de copias, aunque existe la posibilidad de programar dichas copias y alojarlas todas en una misma ubicación remota, de modo que estas se encuentren centralizadas.

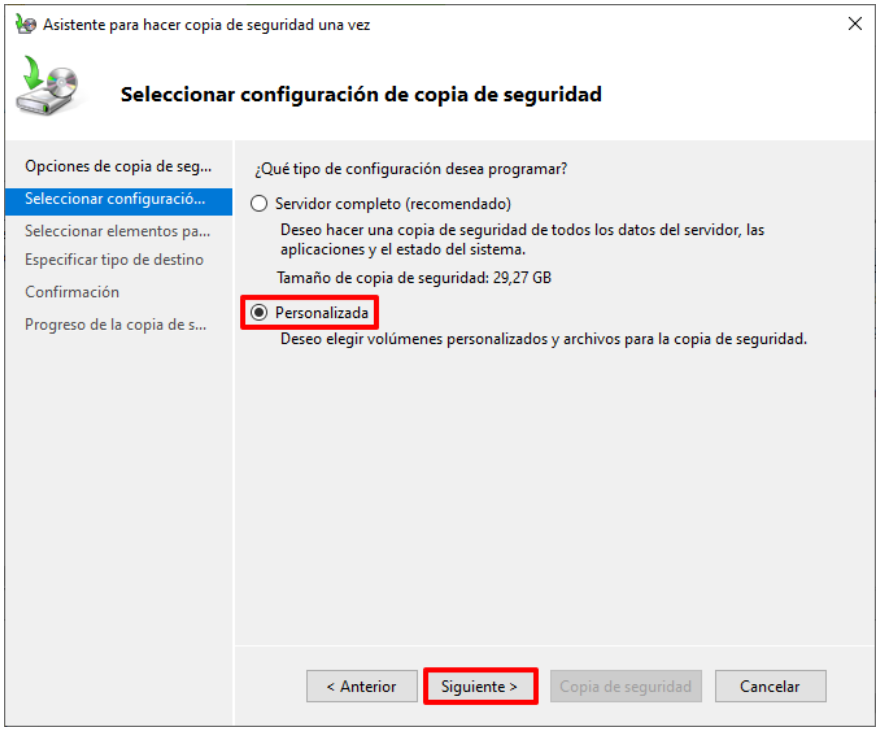
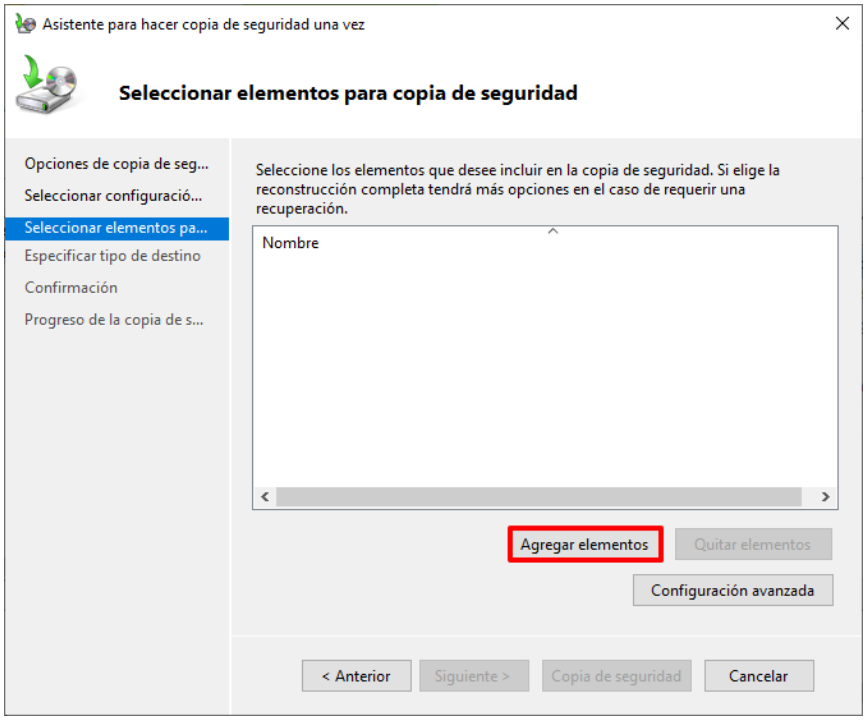
d) Si previamente ha seguido los pasos de Requisitos de Acceso presentes en la guía, para ejecutar de forma correcta los pasos indicados a continuación, deberá deshabilitar temporalmente el objeto GPO "CCN-STIC-570A23 Incremental Control Dispositivos" en las Unidades Organizativas donde se haya vinculado,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

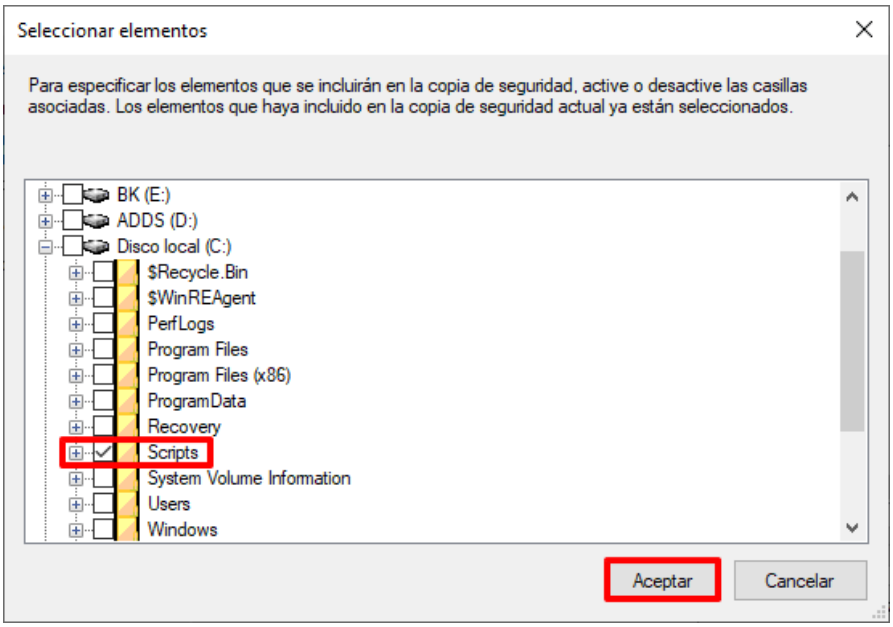
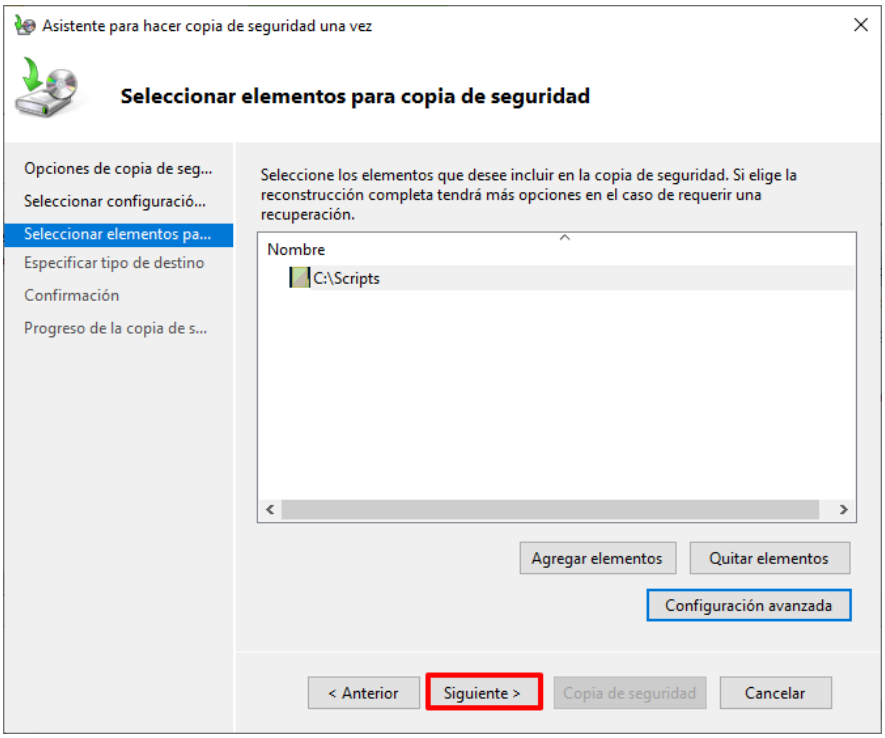
Nota: En este ejemplo se va a realizar una copia de seguridad puntual en el tiempo de una carpeta de datos alojada en un equipo de tipo Domain Controller.

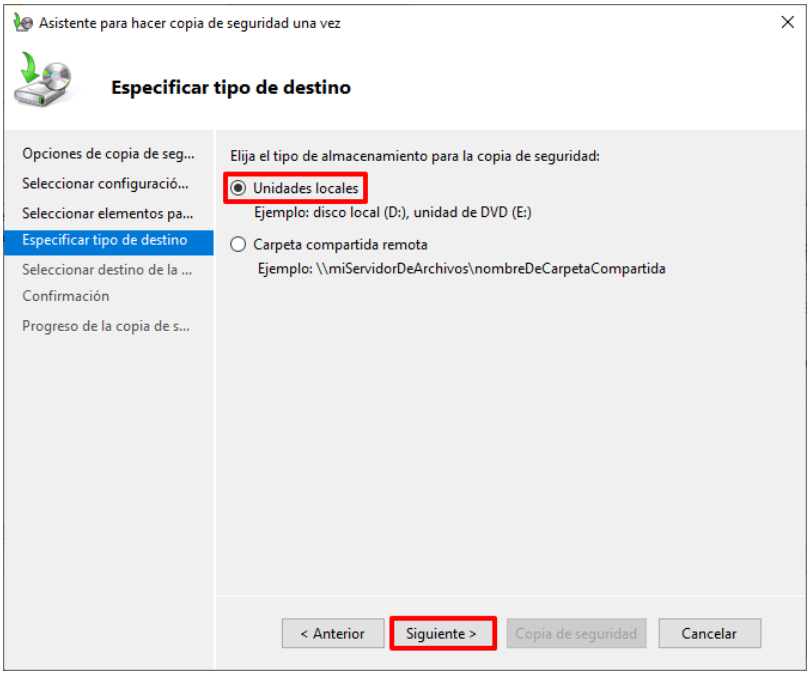
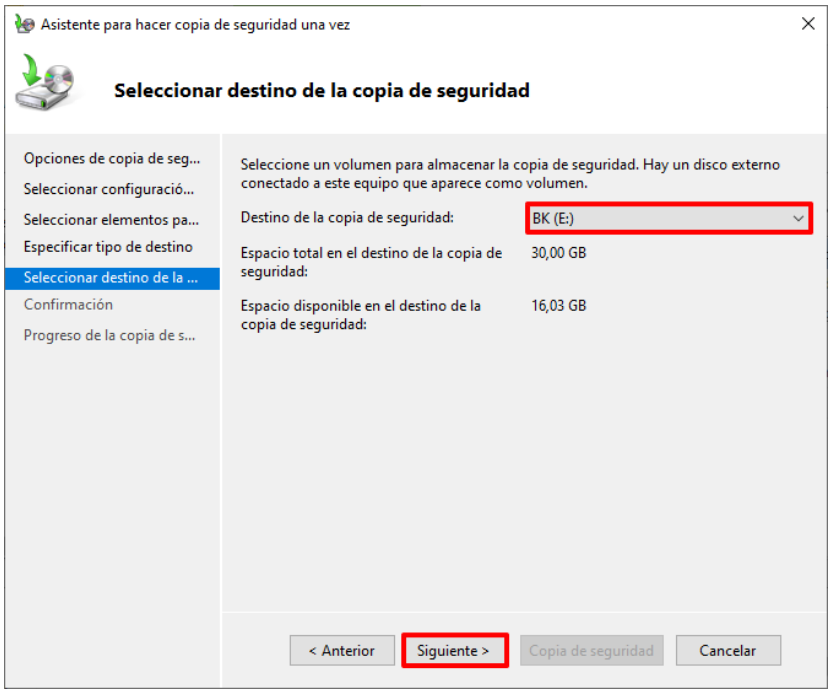
Se recomienda establecer una copia de seguridad programada con el objetivo de que esta se realice de una forma periódica acorde a las políticas de la organización, tomando en consideración su configuración (Completa, Incremental, etc.).

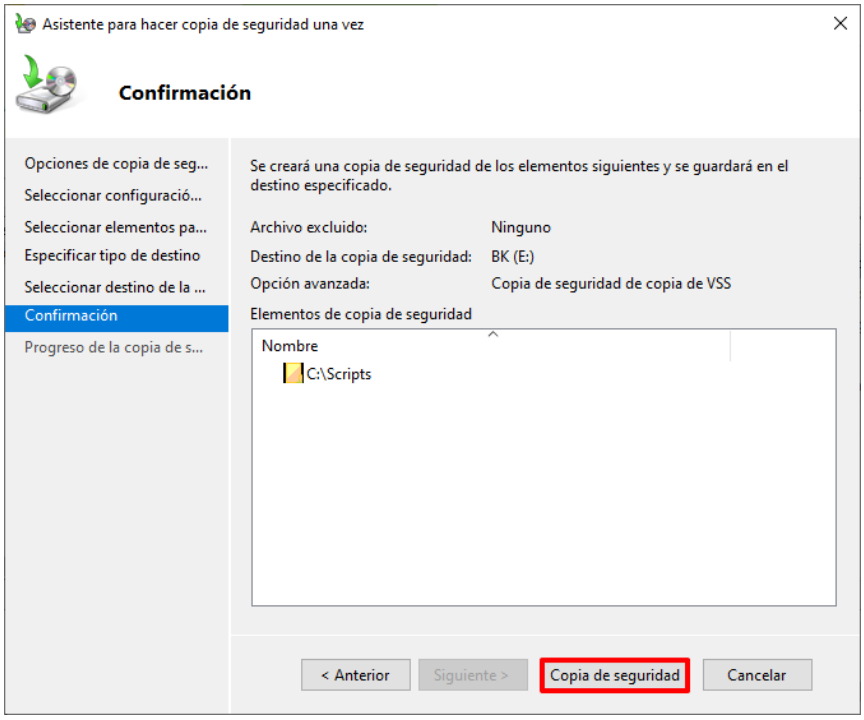
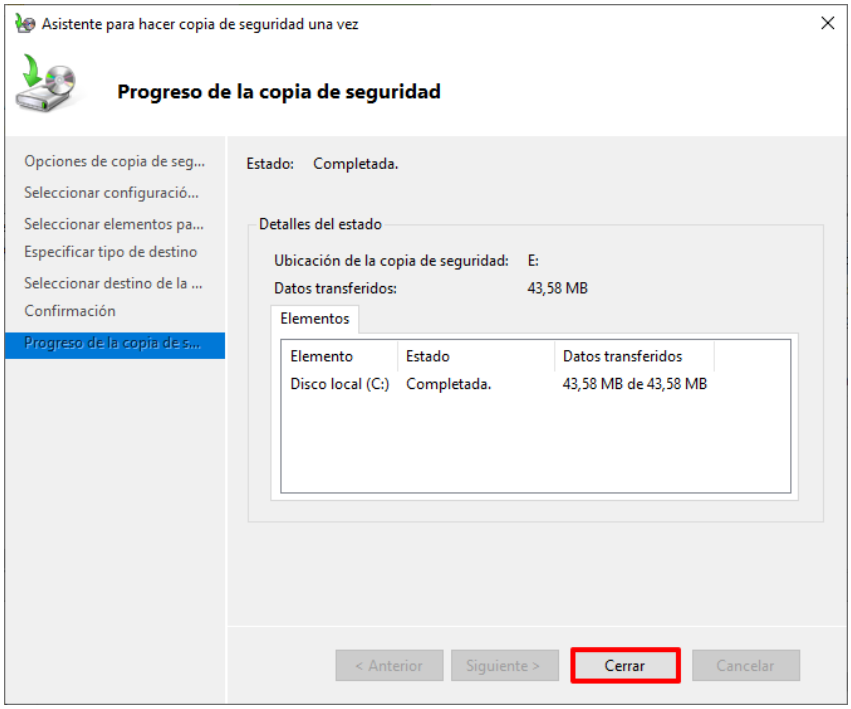
Paso	Descripción
1.	Inicie sesión en el equipo donde desea realizar la copia de seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de "Inicio" para ejecutar el "Administrador del servidor".
3.	En la parte superior derecha pulse sobre el botón "Herramientas" y a continuación seleccione "Copias de seguridad de Windows Server". 

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

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

Paso	Descripción
8.	En la nueva ventana emergente deberá seleccionar aquellos directorios y ficheros sobre los que desee realizar dicha copia de seguridad. Pulse “Aceptar” cuando haya finalizado.  **Nota:** En este ejemplo se ha seleccionado el directorio C:\Scripts.
9.	Pulse “Siguiente >” en la ventana “Seleccionar elementos para copia de seguridad”. 

Paso	Descripción
10.	Mantenga seleccionada la opción “Unidades locales” y pulse “Siguiente >”.  **Nota:** Dependiendo de la configuración o ubicación donde se desea alojar la copia de seguridad deberá adaptar este paso.
11.	En la opción “Destino de la copia de seguridad” seleccione la unidad donde desea alojar la copia de seguridad y pulse “Siguiente >”.  **Nota:** En este ejemplo se selecciona la unidad “E:” dedicada a la realización de copias de seguridad.

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

ANEXO B.6. PROTECCIÓN DE DISPOSITIVOS PORTÁTILES (USO OFICIAL - MATERIAS CLASIFICADAS)

La presente sección tiene como objetivo la configuración y aplicación de directivas de modo que sea posible el cifrado del sistema operativo Windows Server, o de dispositivos portátiles, bajo el producto BitLocker.

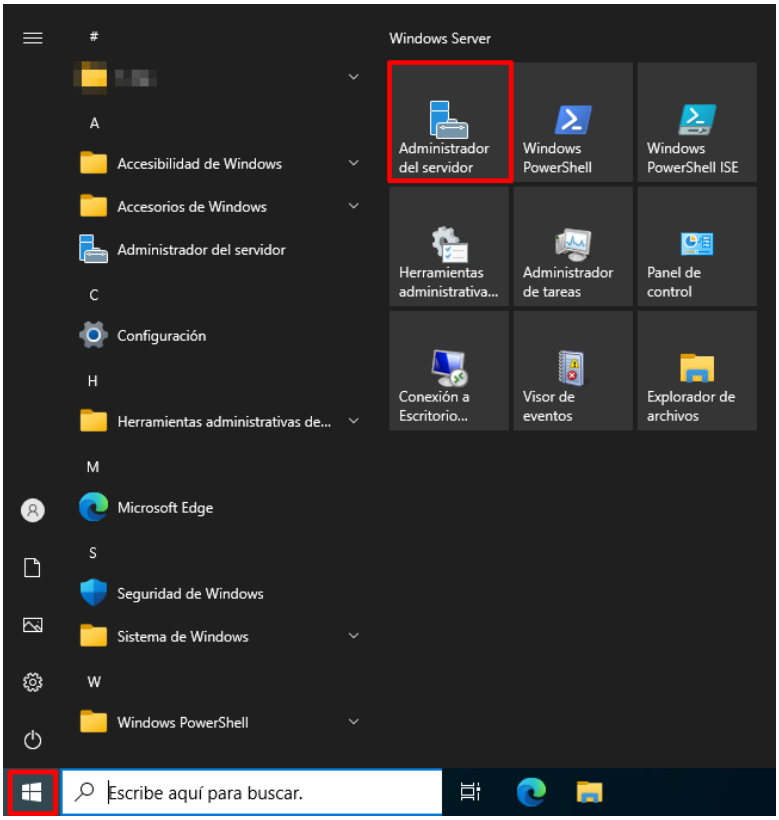
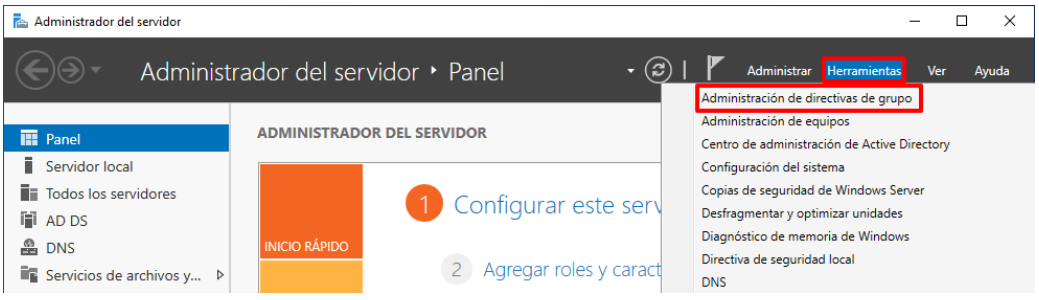
Deberá tener en consideración que para poder utilizar el producto BitLocker en los servidores o Controladores del Dominio, la característica "Cifrado de unidad BitLocker" deberá encontrarse implementada en los equipos donde se desea realizar el cifrado.

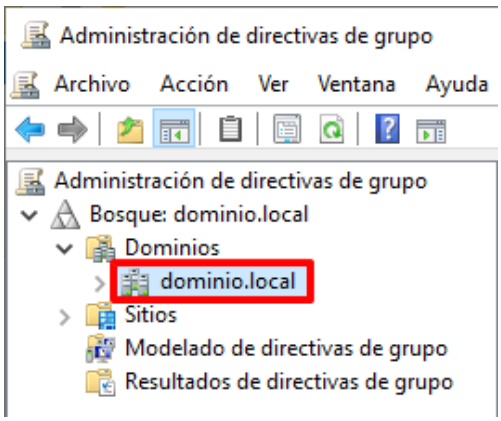
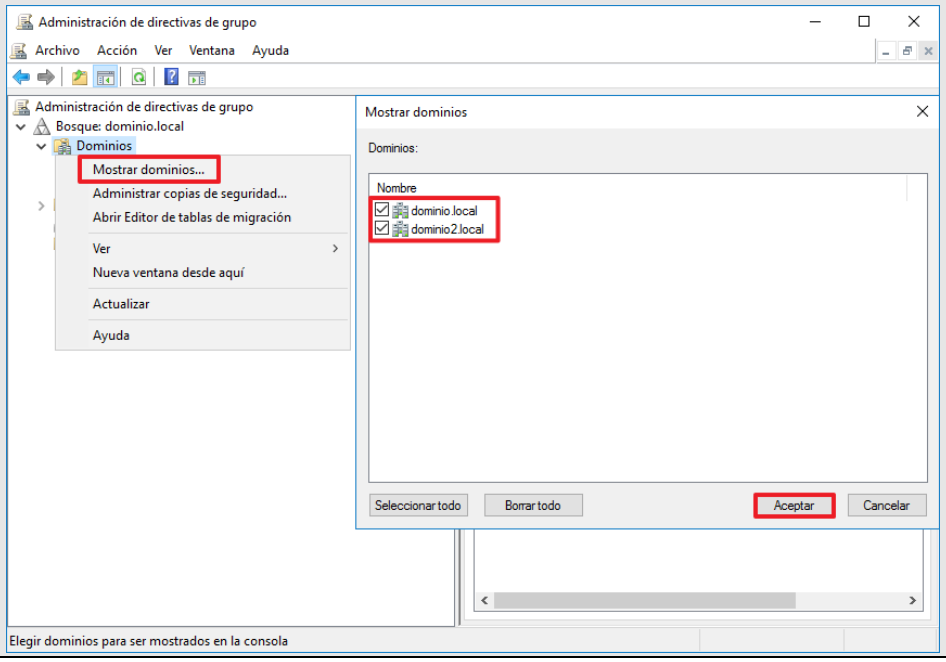
Nota: Si en su organización dispone de otro producto de cifrado, o bien su sistema operativo se encuentra implementado en un entorno protegido, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

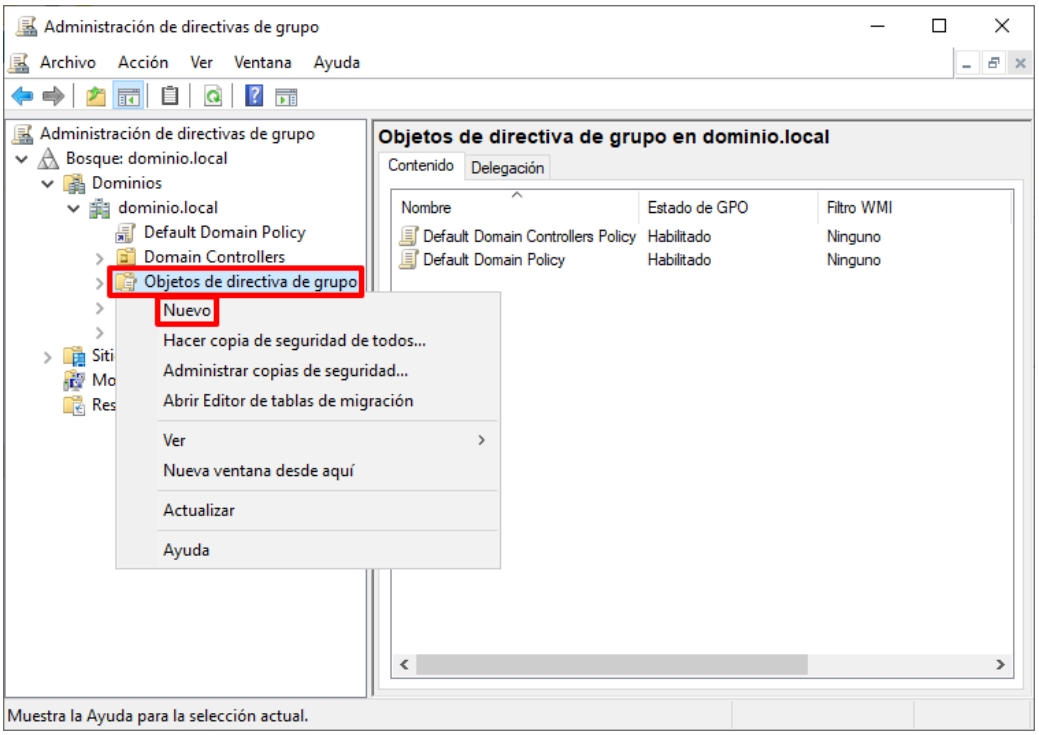
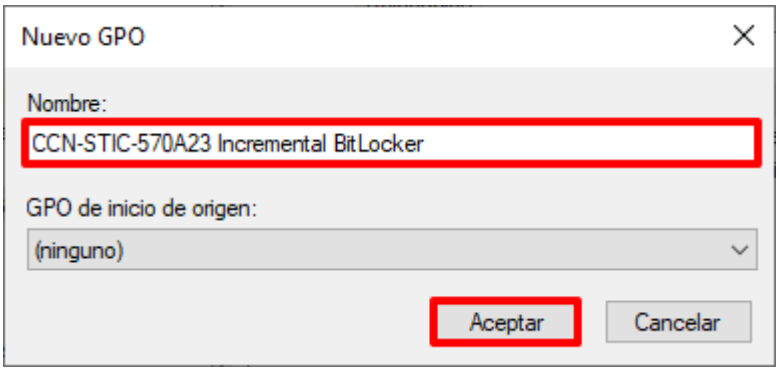
Se considera un entorno protegido, aquel entorno donde se disponga de un acceso controlado a salvo de hurtos y/o miradas indiscretas dentro de la organización.

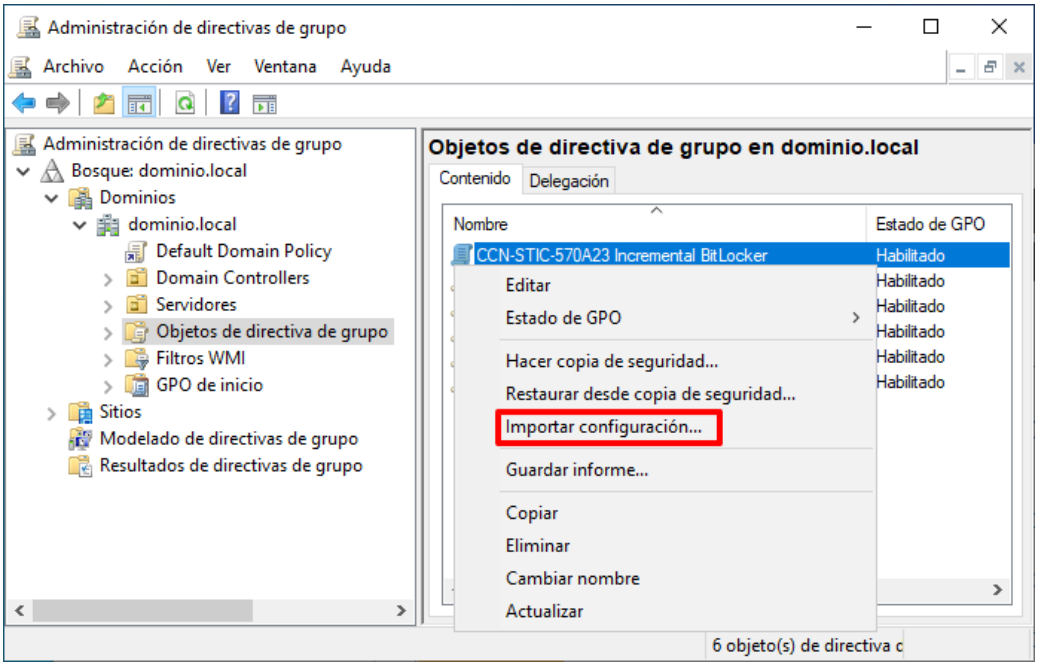
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

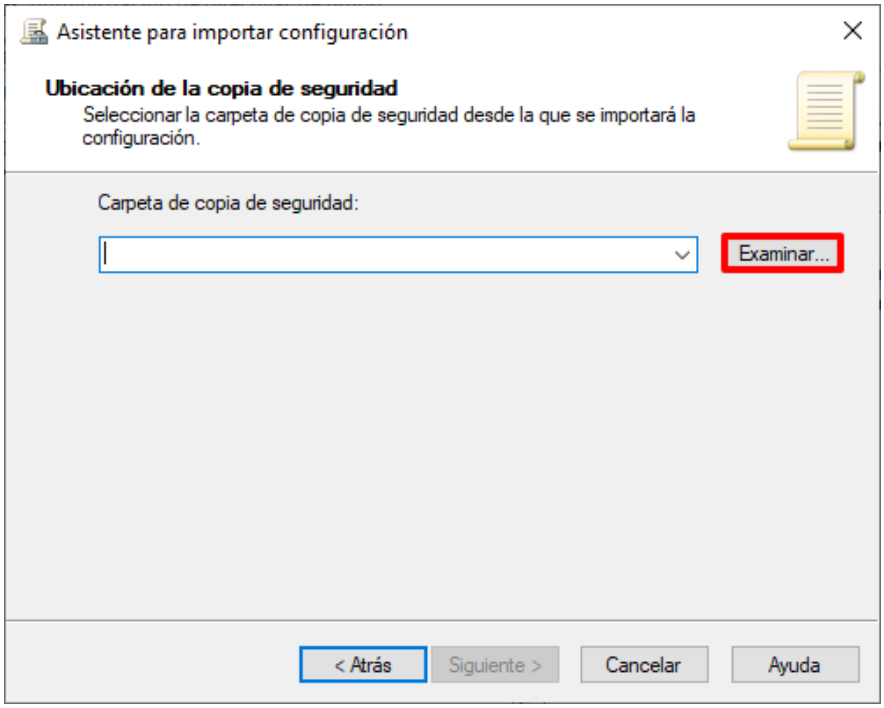
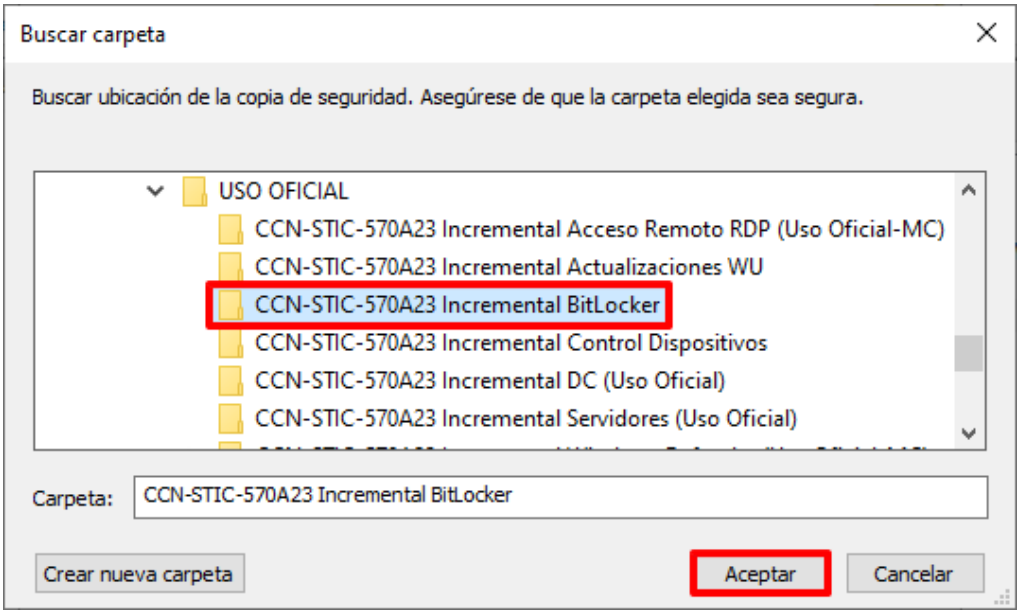
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

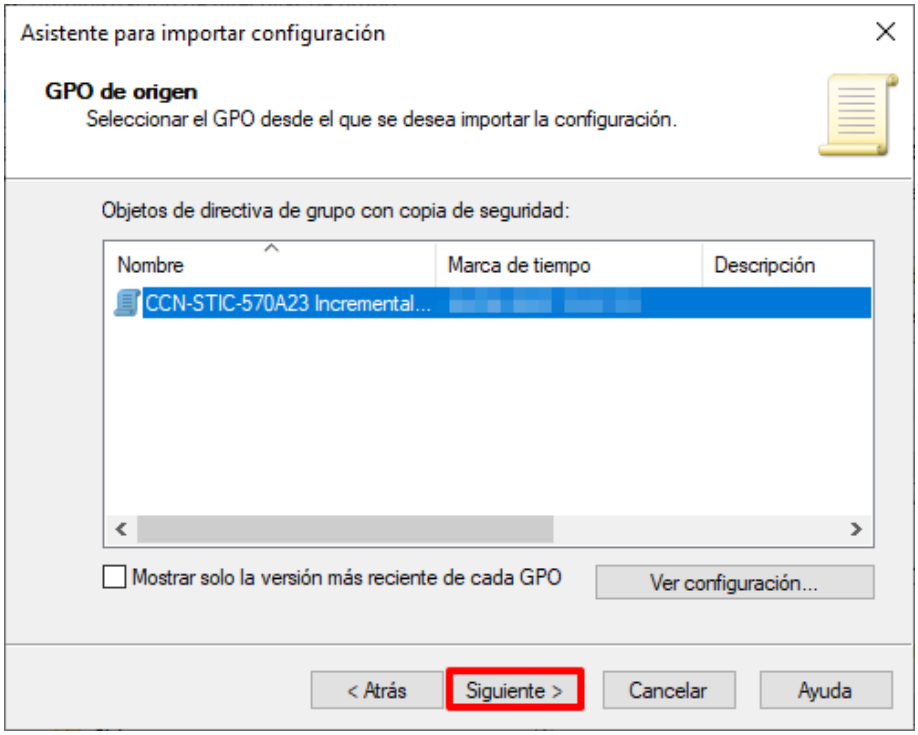
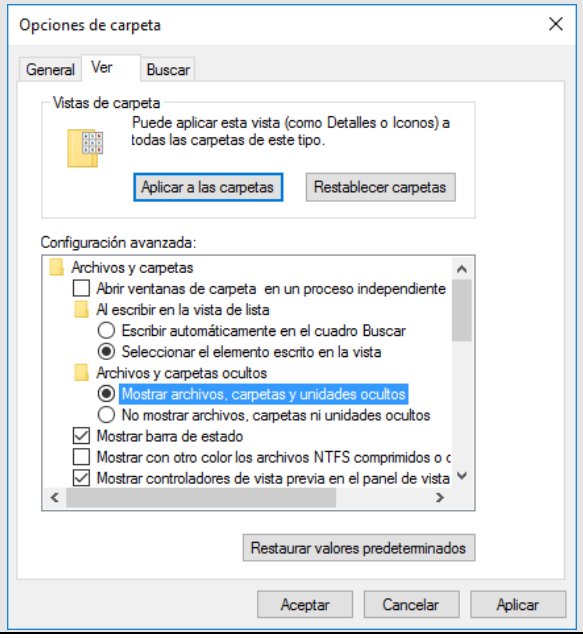
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

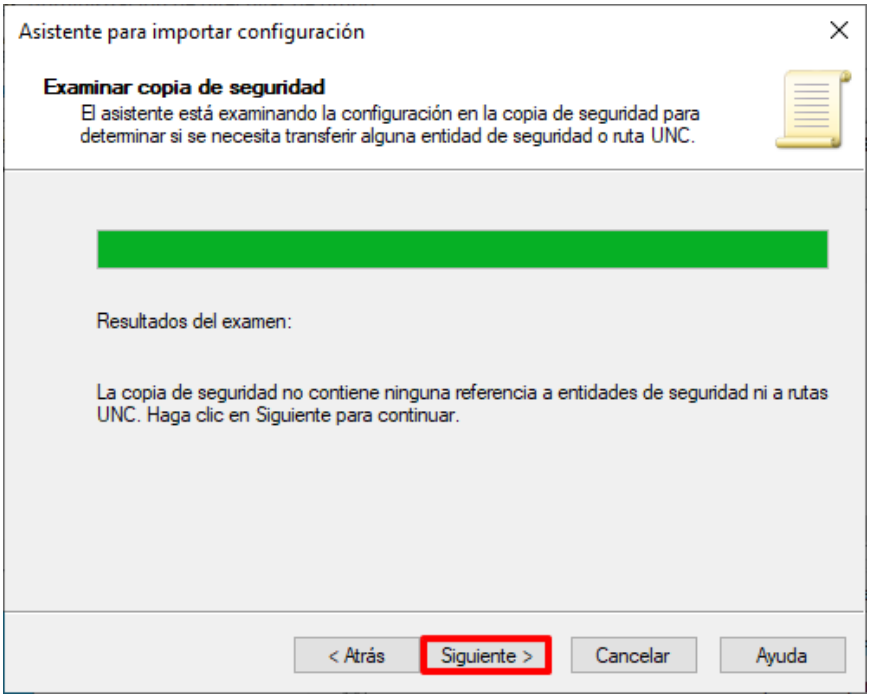
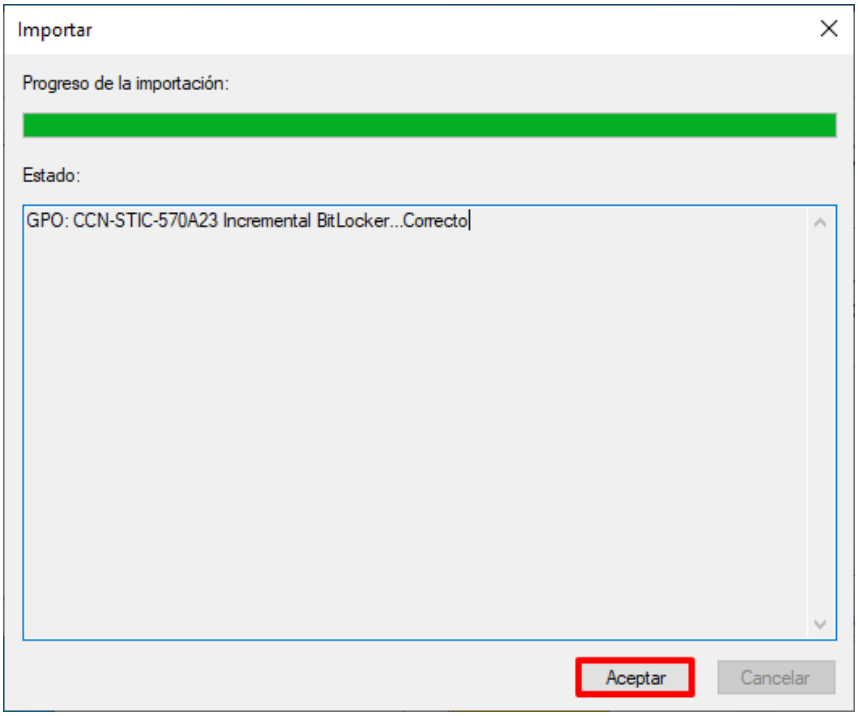
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

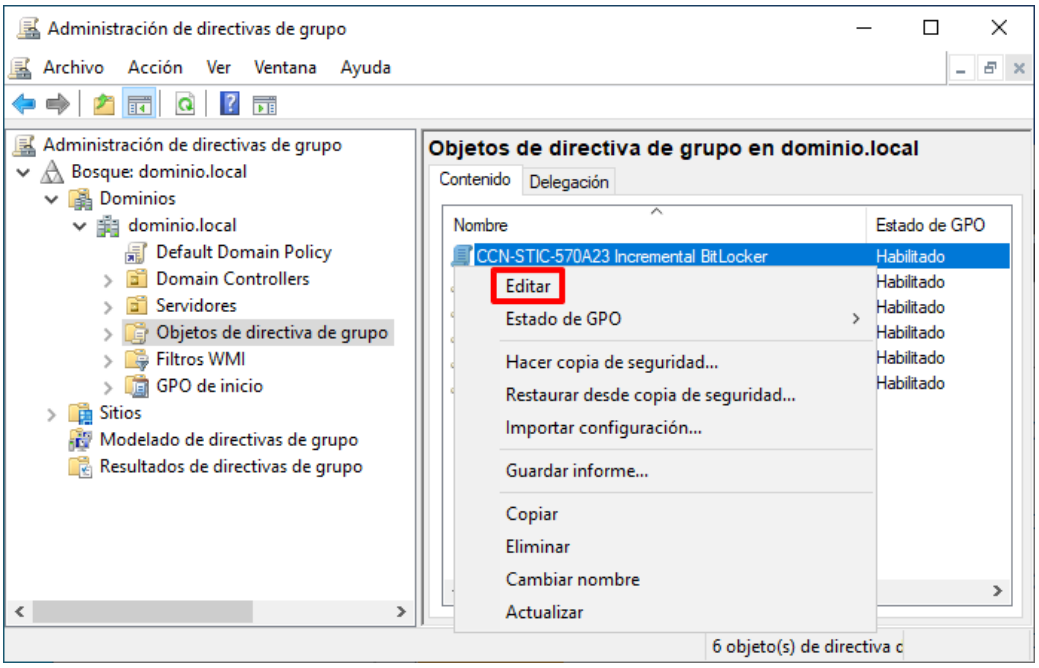
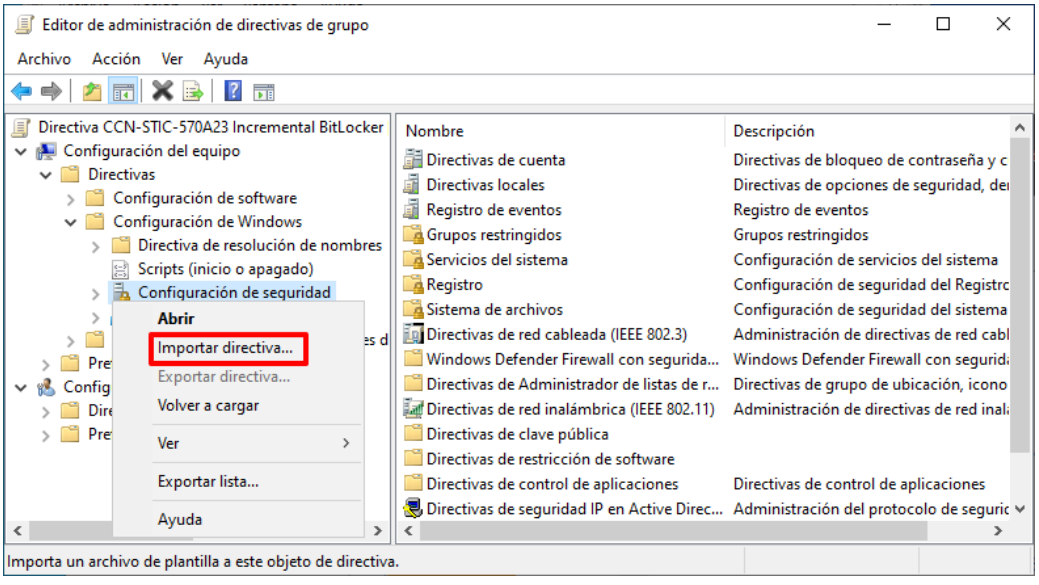
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental BitLocker**" y pulse el botón "Aceptar". 

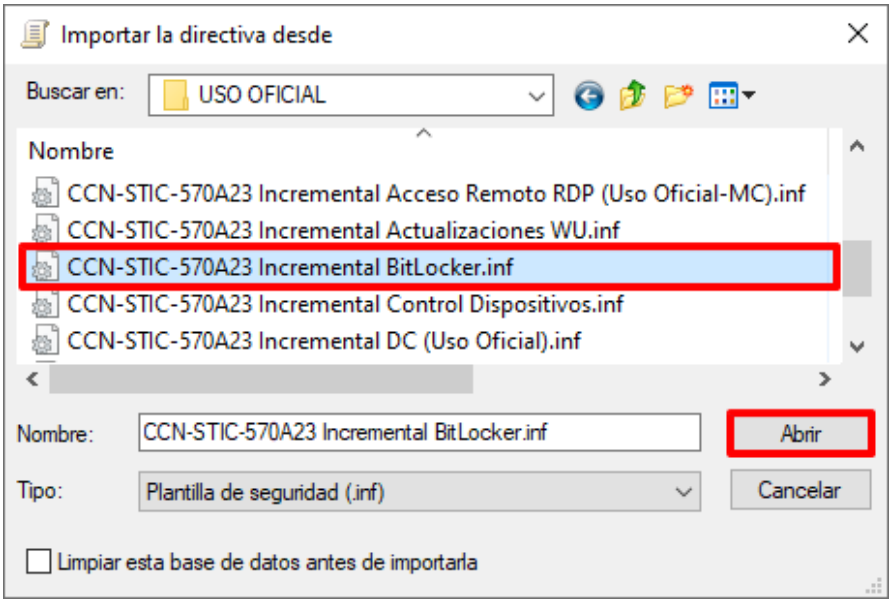
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

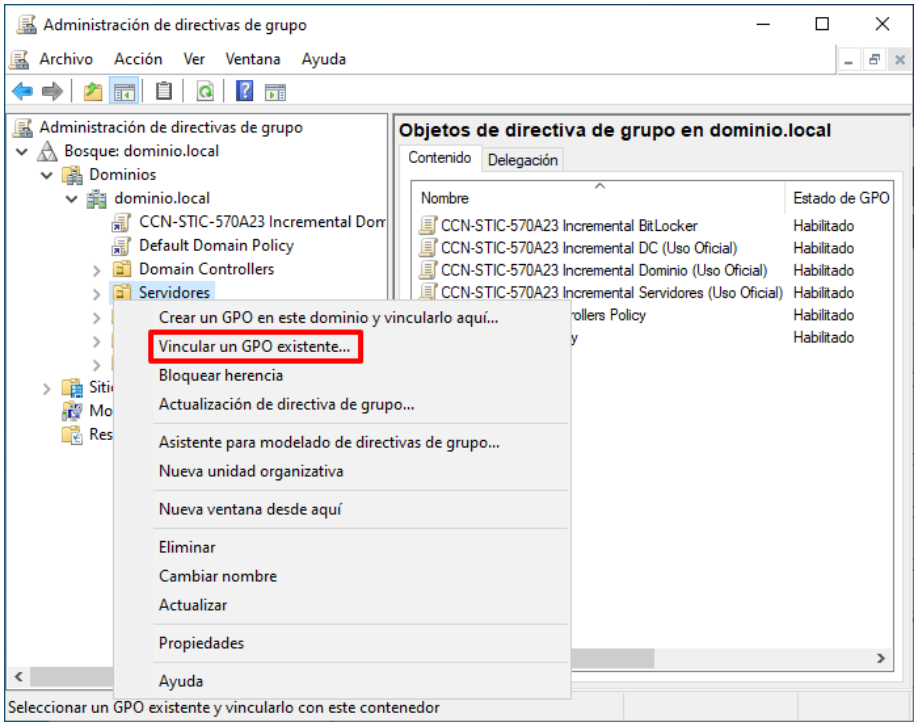
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-570A23 Incremental BitLocker” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Defina el nombre del objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.

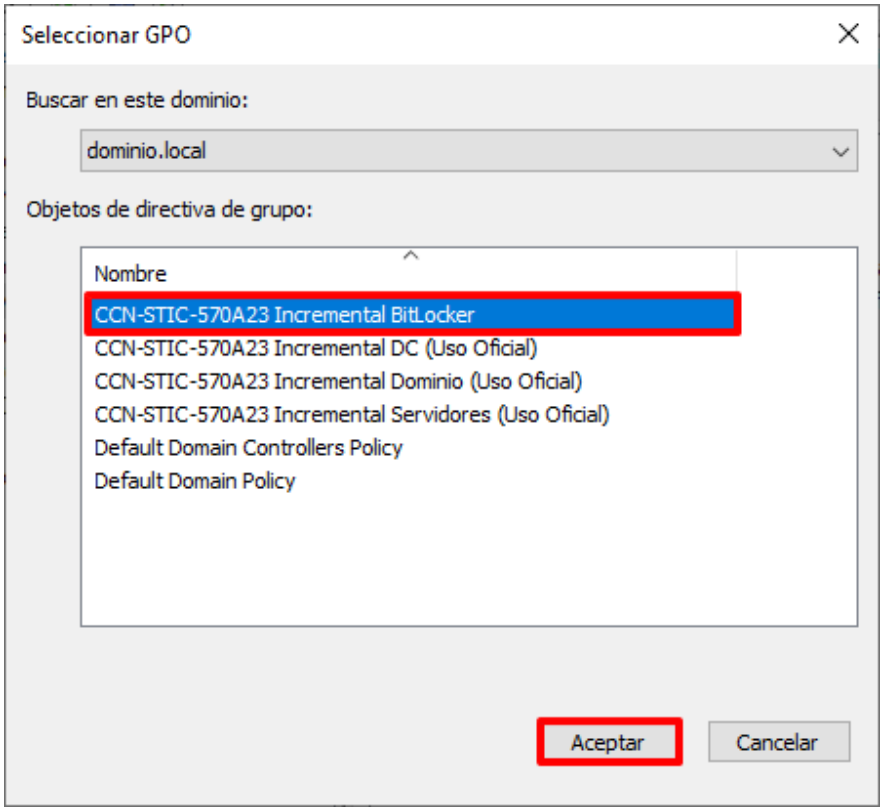
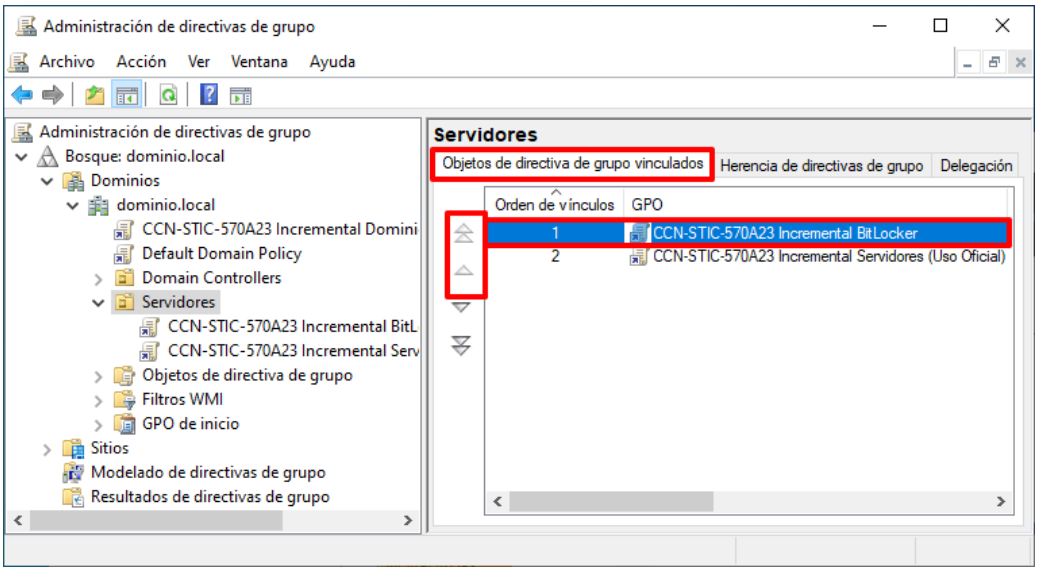
Paso	Descripción
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental BitLocker” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

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

Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental BitLocker” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá. 
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“CCN-STIC-570A23 Incremental BitLocker → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad”**. Seleccione con el botón derecho el nodo “Configuración de seguridad” y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 

Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en “C:\Scripts\[TIPO DE PERFILADO]” denominada “CCN-STIC-570A23 Incremental BitLocker.inf”. A continuación, pulse sobre el botón “Abrir”.  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
21.	Cierre la ventana “Editor de administración de directivas de grupo”.

Paso	Descripción
22.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de actualizaciones y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción “Vincular un GPO existente…”.  **Nota:** Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración. En este ejemplo se hace uso de la Unidad Organizativa “Servidores”, creada para tal fin.

Paso	Descripción
23.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental BitLocker" y pulse "Aceptar". 
24.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

Paso	Descripción
25.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.

ANEXO B.7. REQUISITOS DE ACCESO (MATERIAS CLASIFICADAS)

El siguiente apartado tiene como objetivo ayudar a los administradores con el control y uso de dispositivos conectados sobre los equipos de tipo servidor, independientemente de su rol, dentro de un dominio.

El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso del perfil MATERIAS CLASIFICADAS.

Nota: Si en su organización dispone de otro producto que realice las labores de control de acceso a dispositivos de almacenamiento extraíble puede ignorar el presente paso a paso y continuar en el siguiente apartado.

Se debe tener en consideración que tras la aplicación de los siguientes puntos se limitará la instalación de cualquier tipo de dispositivo, no solo dispositivos USB si no cualquier otro elemento como disco duro, tarjeta de red, etc., que haga uso de controladores (drivers).

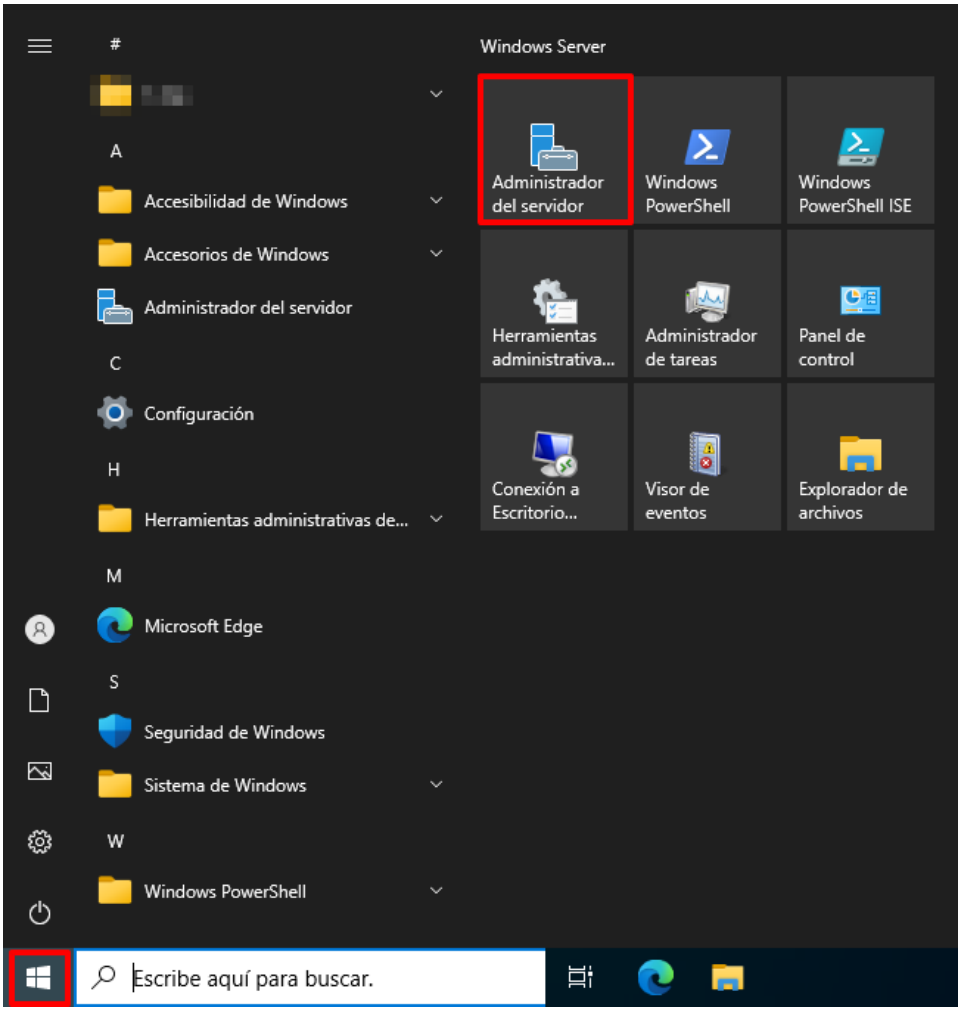
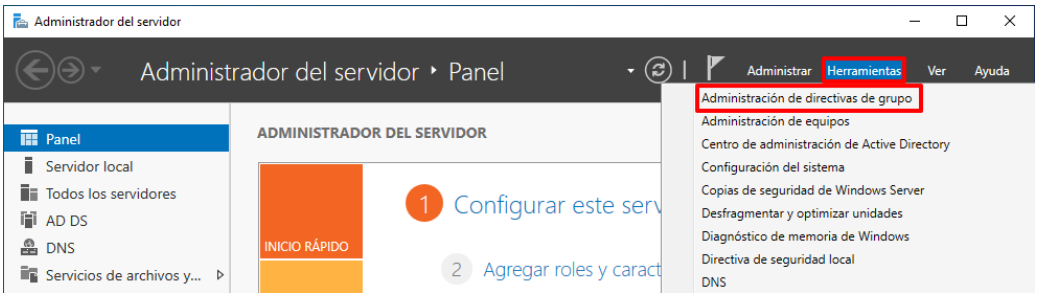
Realizadas las acciones descritas en el presente punto se presentarán dos formas de instalar controladores para el uso de dispositivos.

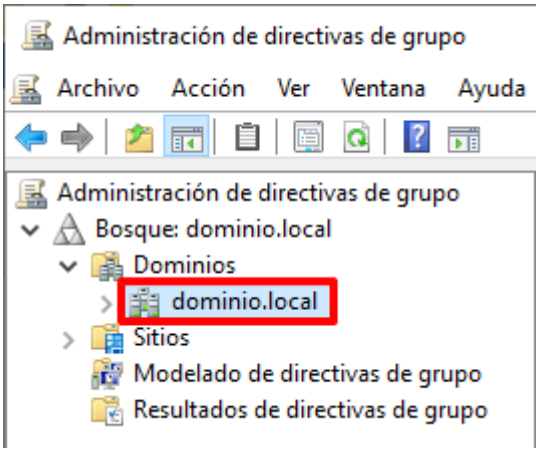
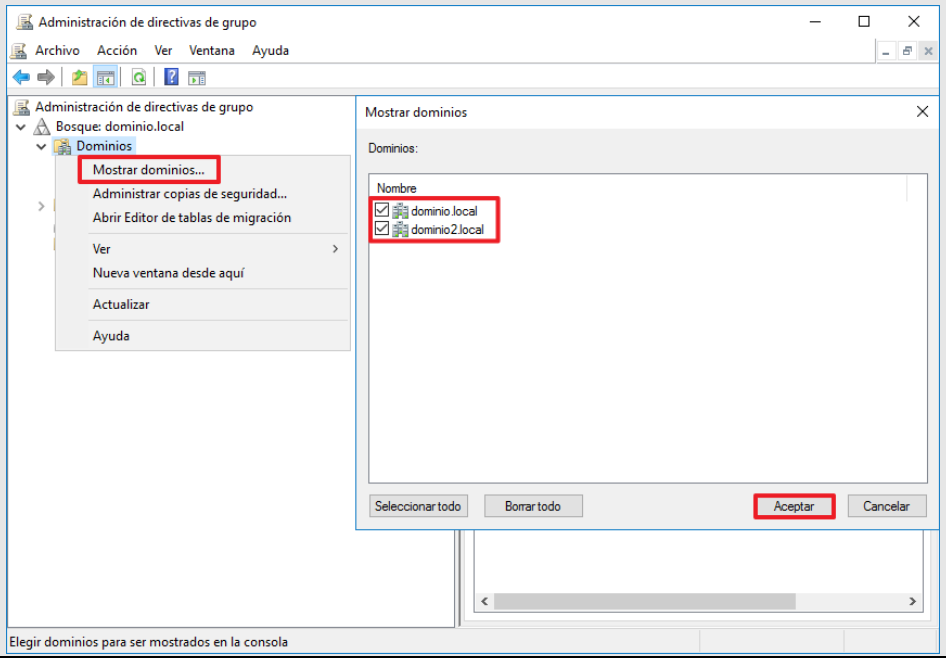
a) Actualización automática de controladores por parte de usuario con privilegios de administrador.

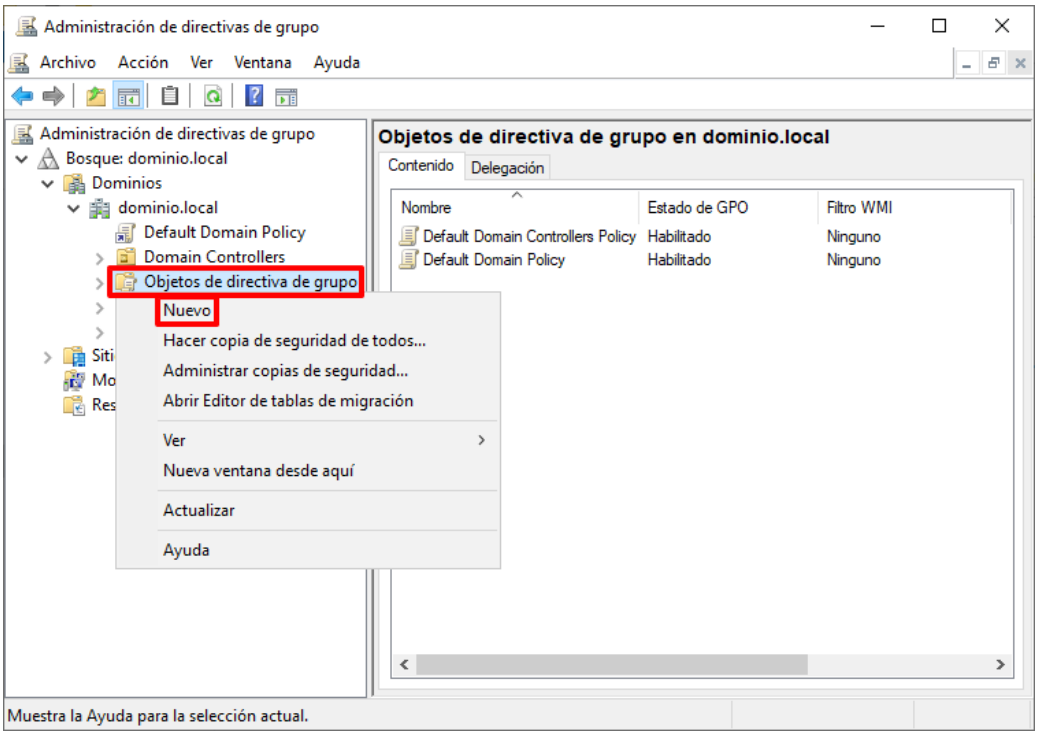
b) Alta de dispositivos por medio de identificadores únicos de los dispositivos.

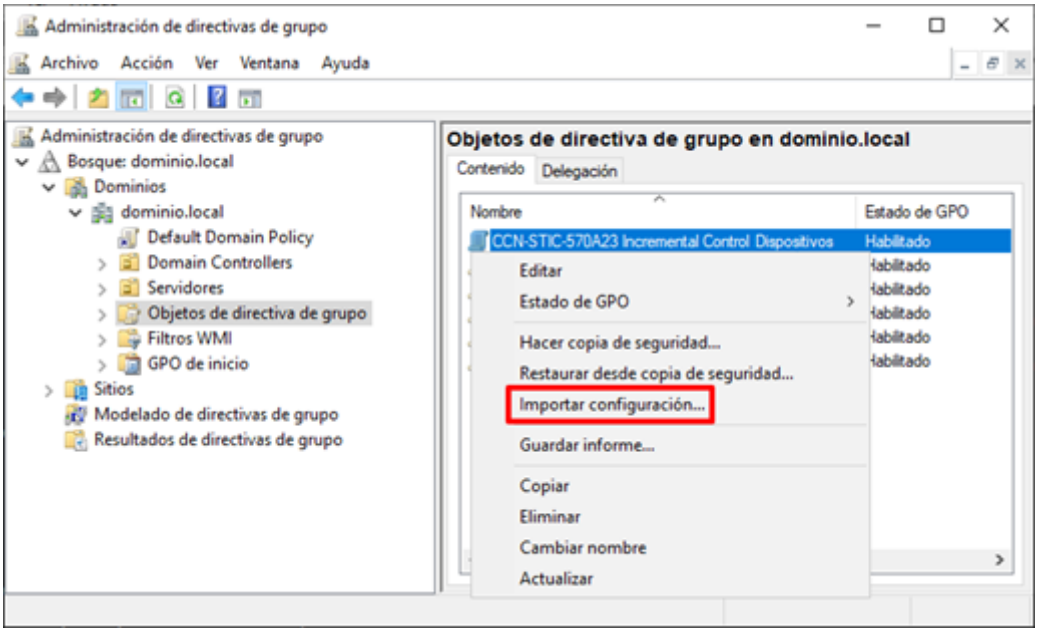
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Materias Clasificadas**, no siendo obligatorio en ningún otro perfilado.

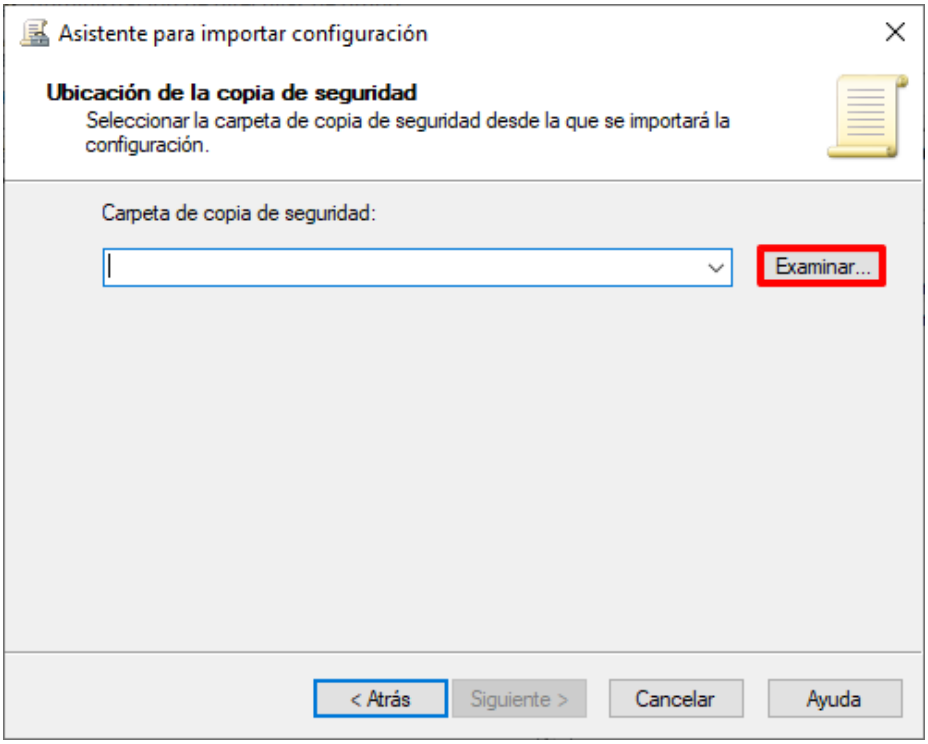
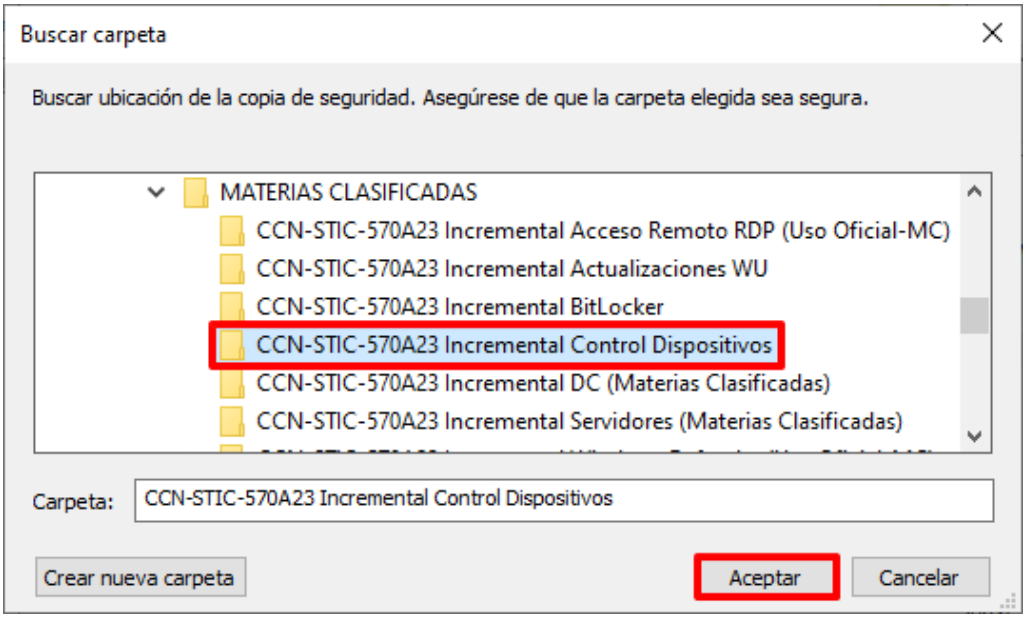
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

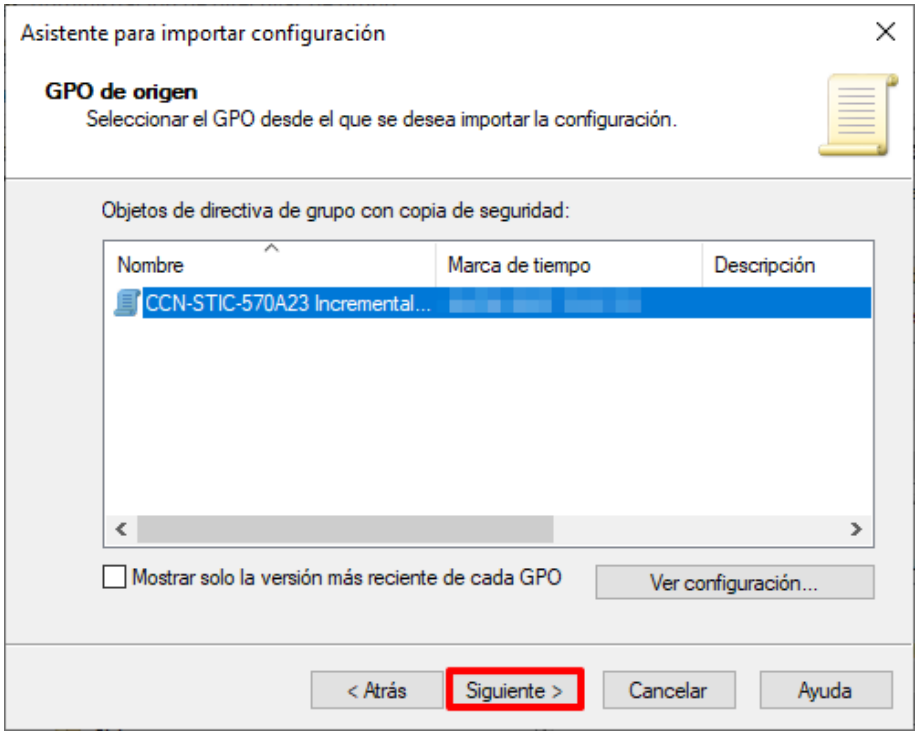
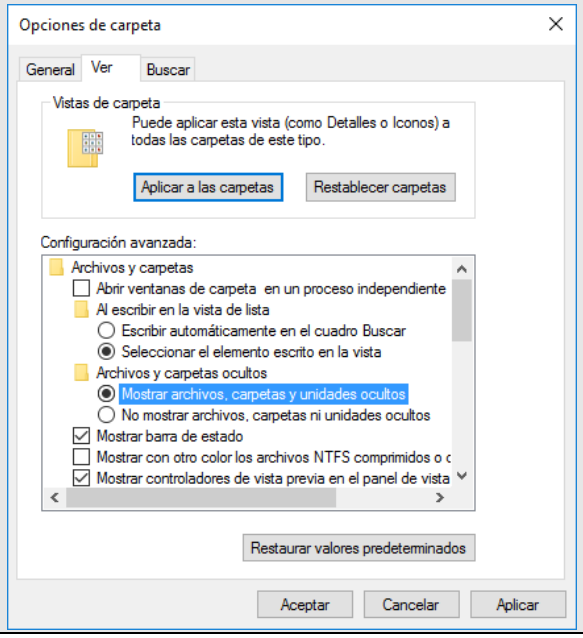
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

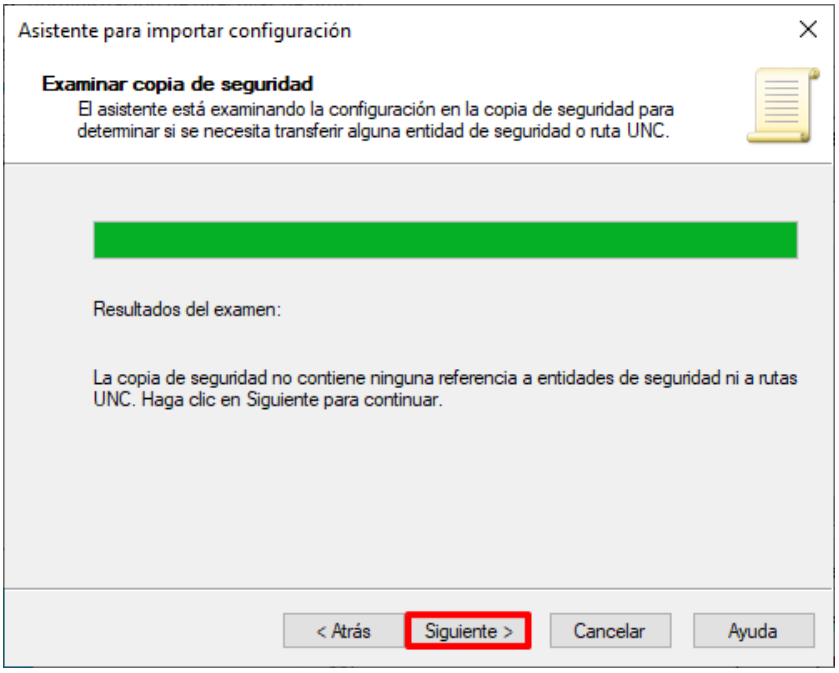
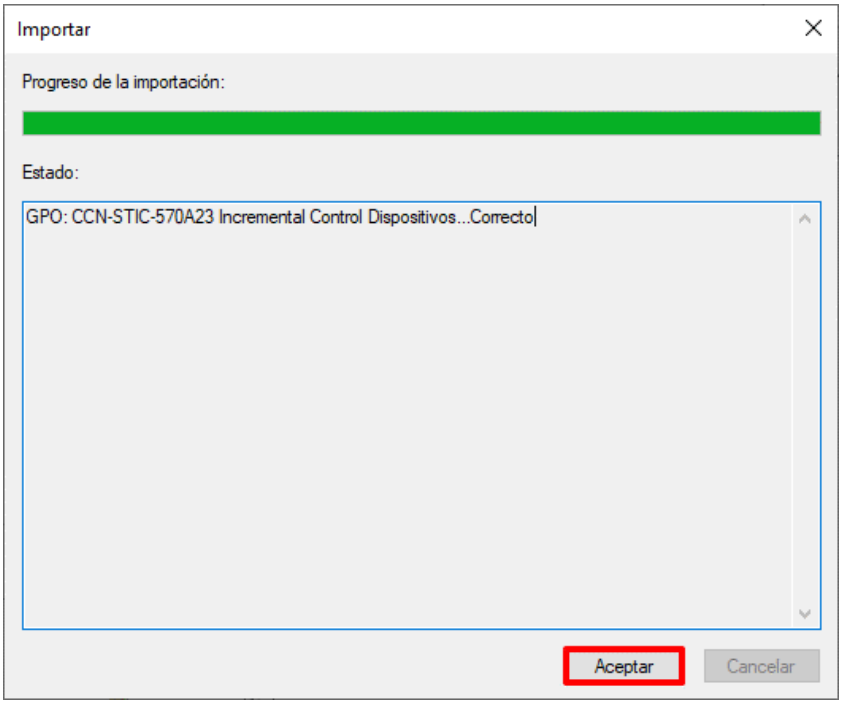
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

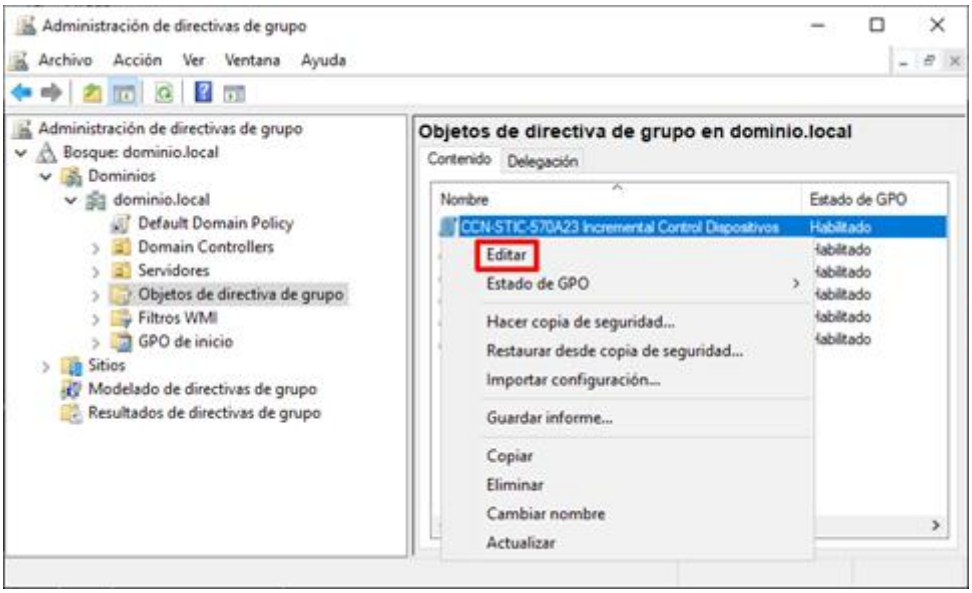
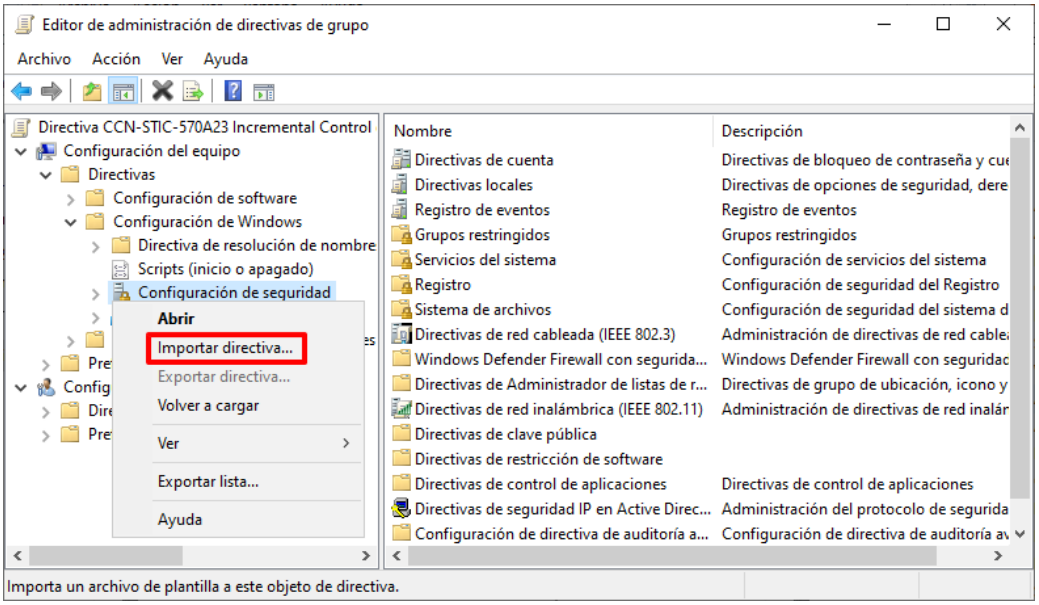
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Control Dispositivos**" y pulse el botón "Aceptar". 

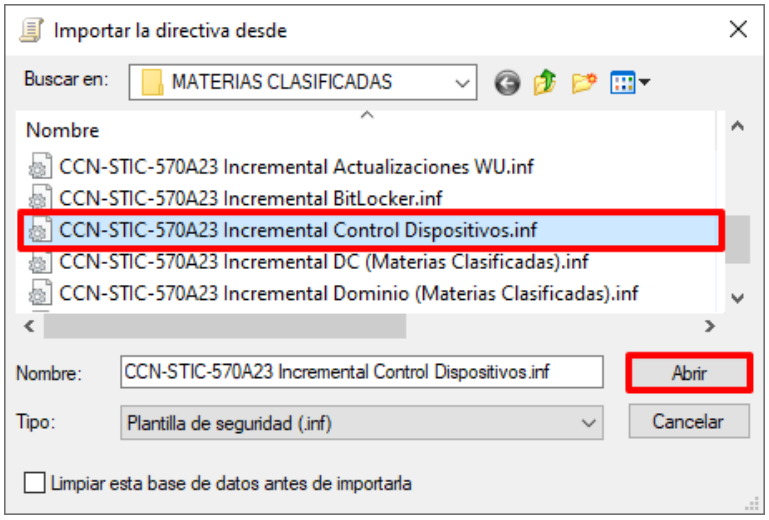
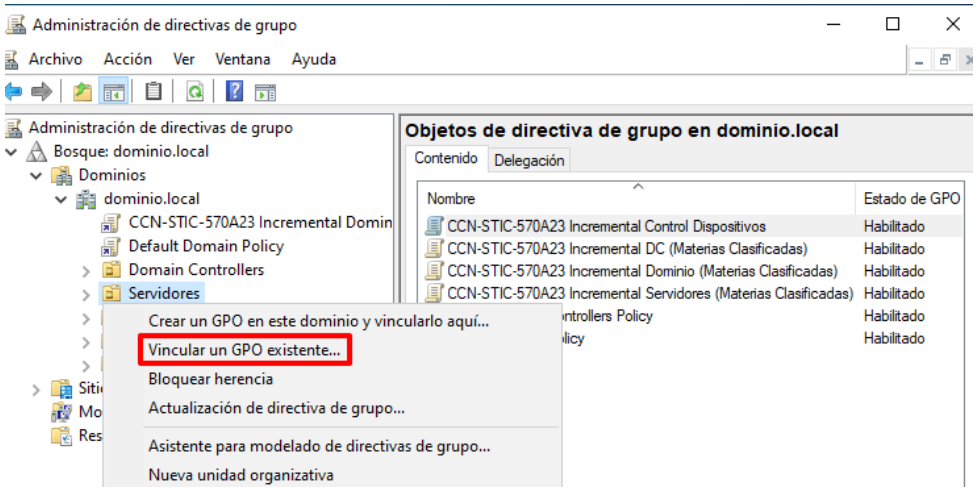
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

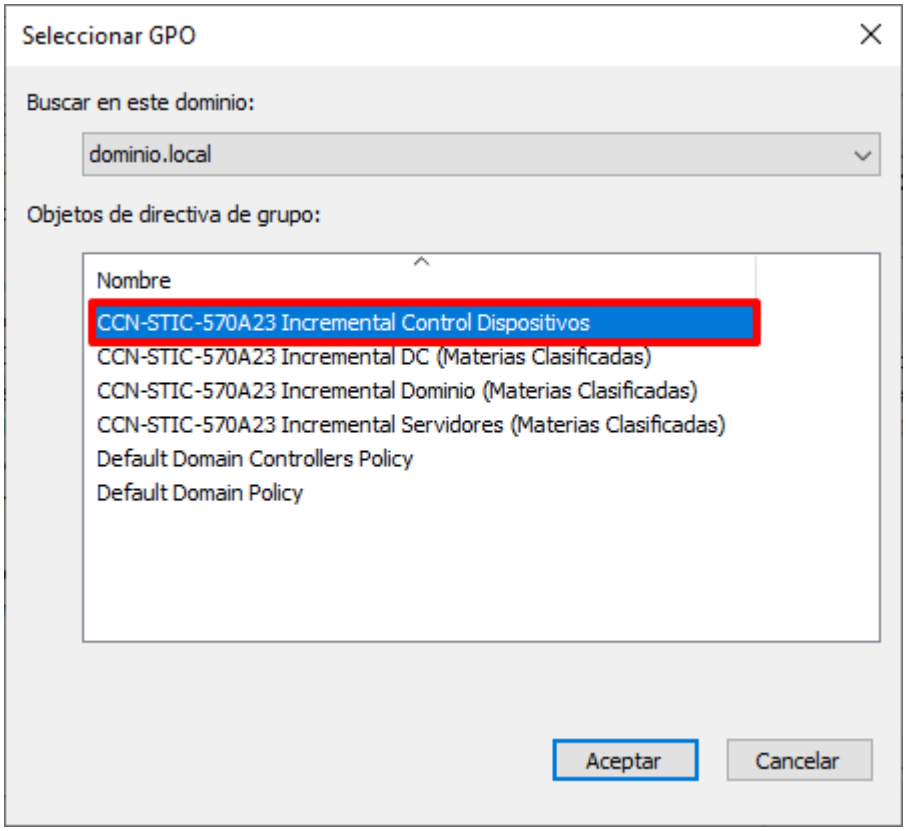
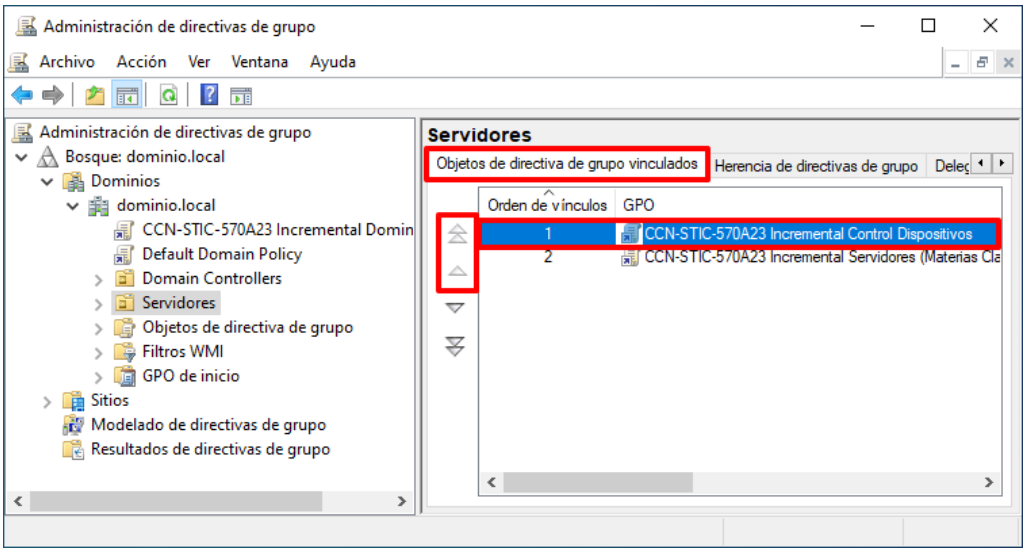
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-570A23 Incremental Control Dispositivos” situada en el directorio “C:\Scripts\MATERIAS CLASIFICADAS” y pulse “Aceptar”. 
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.

Paso	Descripción
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental Control Dispositivos” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

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

Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Control Dispositivos” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá. 
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“CCN-STIC-570A23 Incremental Control Dispositivos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad”**. Seleccione con el botón derecho el nodo “Configuración de seguridad” y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 

Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\MATERIAS CLASIFICADAS" denominada "CCN-STIC-570A23 Incremental Control Dispositivos.inf". A continuación, pulse sobre el botón "Abrir". 
21.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de actualizaciones y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción "Vincular un GPO existente…".  **Nota:** Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración. En este ejemplo se hace uso de la Unidad Organizativa "Servidores", creada para tal fin.

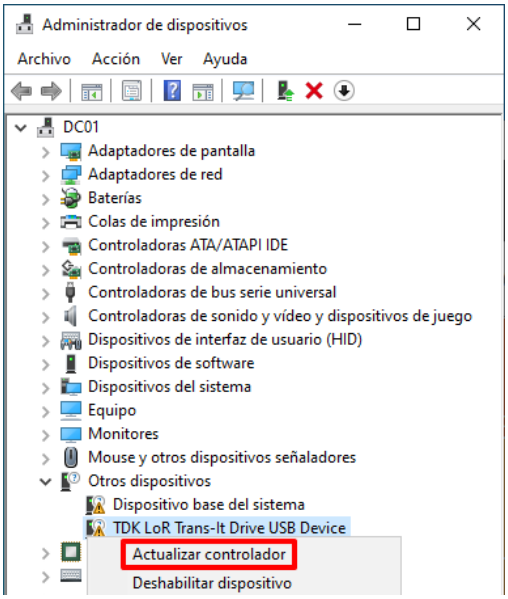
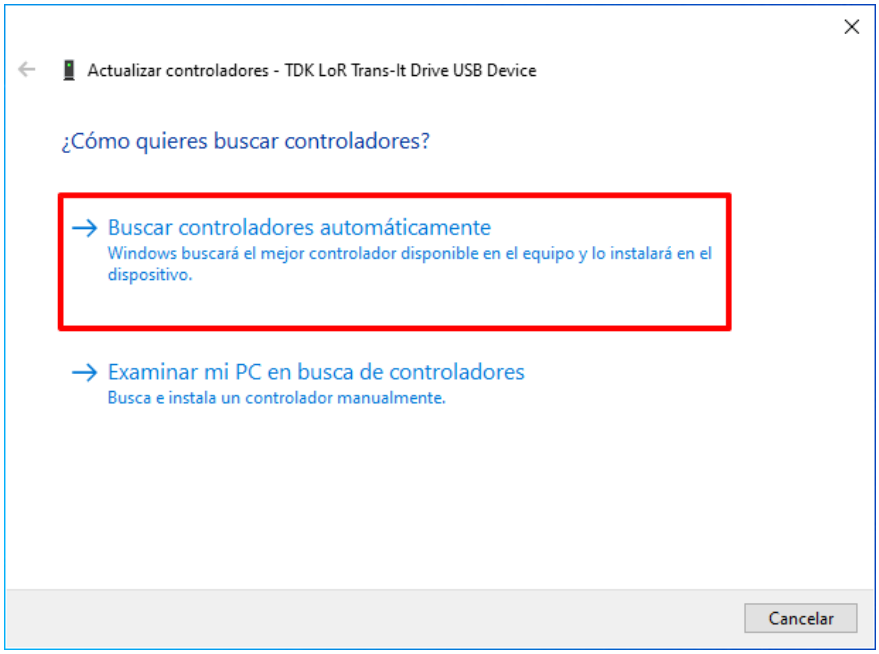
Paso	Descripción
22.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental Control Dispositivos" y pulse "Aceptar". 
23.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

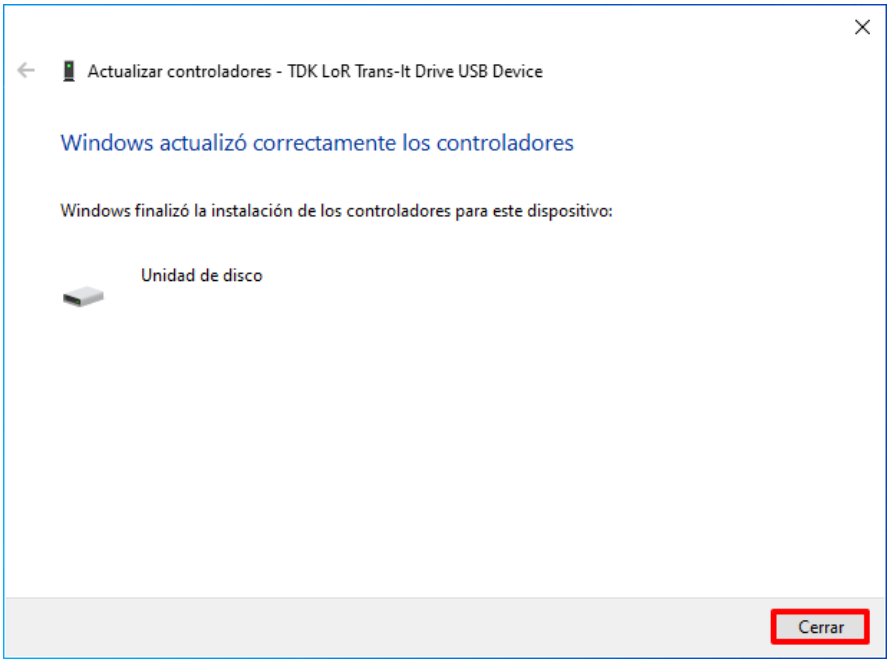
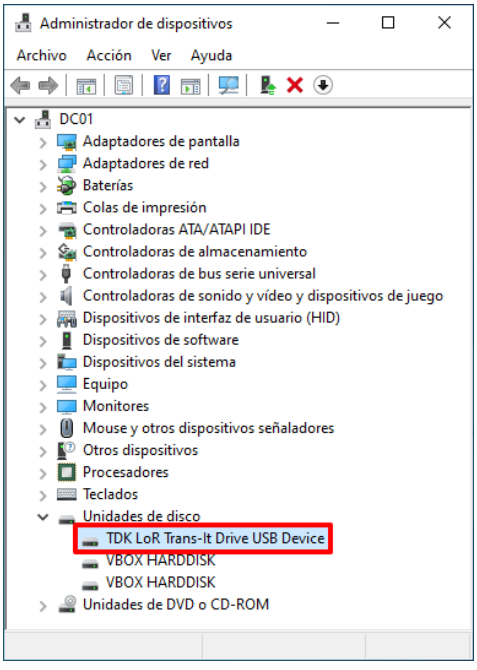
Paso	Descripción
24.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.

ANEXO B.7.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES

Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del dominio en el cual se está habilitando el uso de dispositivos USB.

Paso	Descripción
1.	Inicie sesión en el equipo servidor donde pretende habilitar el uso de un dispositivo USB.
2.	Haga clic derecho sobre el botón de "Inicio" y seleccione "Administrador de dispositivos". 

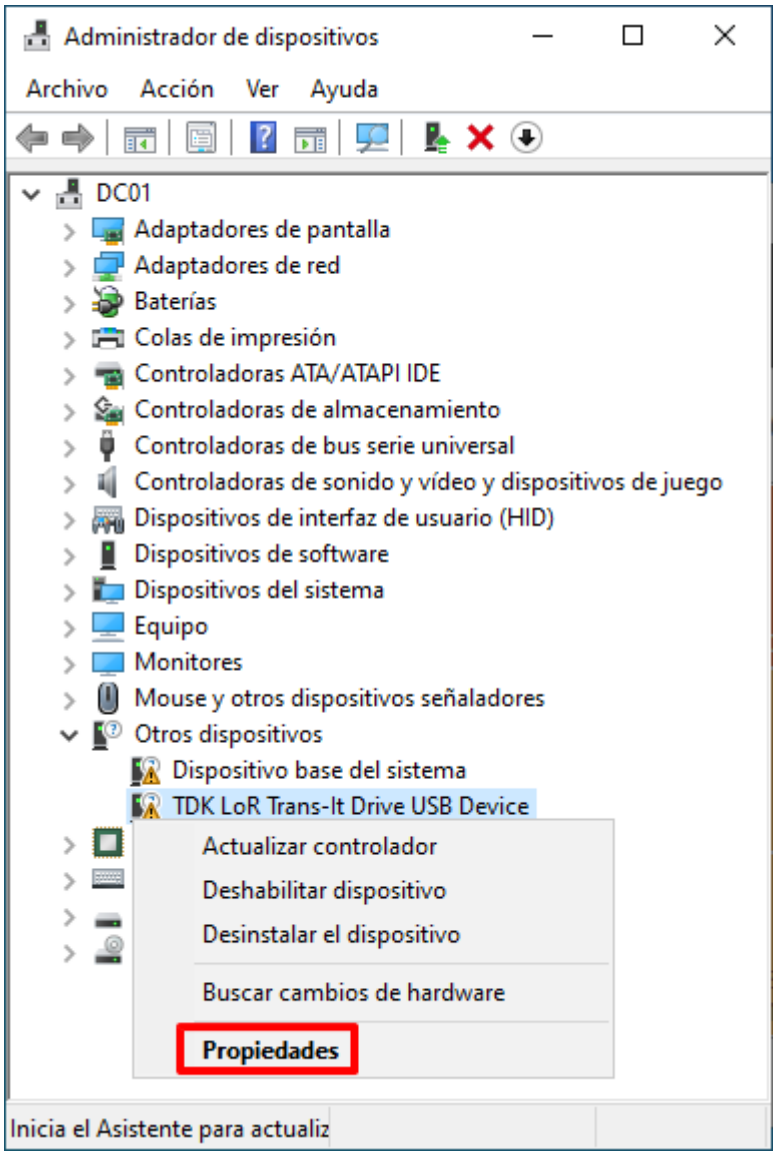
Paso	Descripción
3.	Despliegue en el "Administrador de dispositivos" el nodo "Otros dispositivos" y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual "Actualizar controlador".  **Nota:** Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de "Dispositivo desconocido".
4.	A continuación, se iniciará el asistente para instalar del software necesario. Seleccione la opción "Buscar software de controlador actualizado automáticamente". 

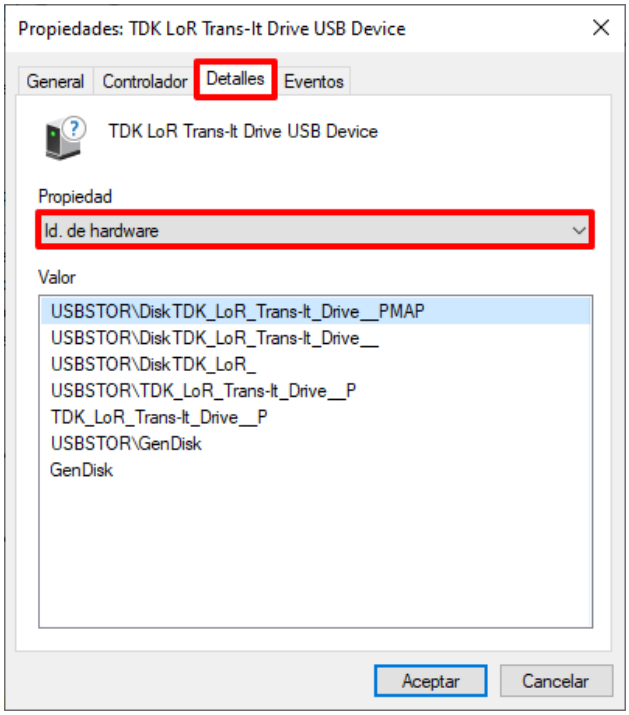
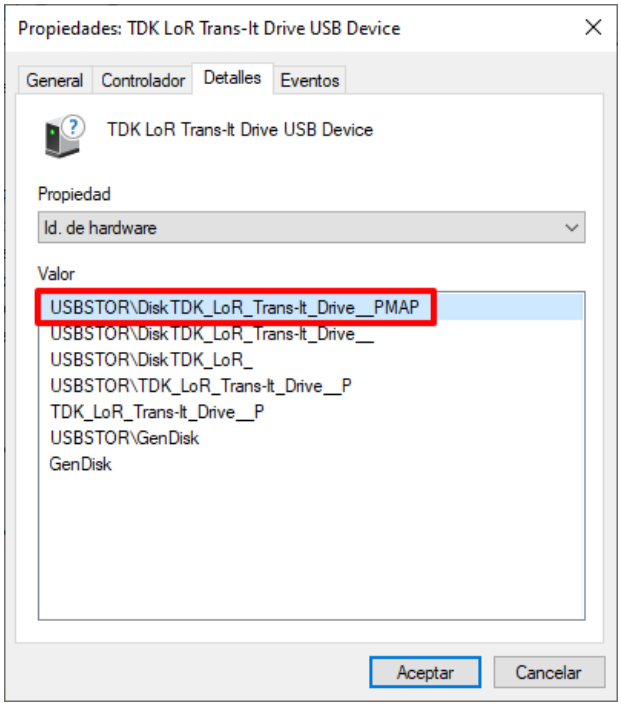
Paso	Descripción
5.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  **Nota:** No cierre el “Administrador de dispositivos” todavía.
6.	Ejecute los mismos pasos anteriores (pasos 3 a 5) hasta que el dispositivo aparezca en el apartado “Unidades de disco” y no exista ningún otro controlador dependiente en el apartado “Otros dispositivos”. Podrá corroborar que no existe ningún controlador necesario adicional cuando el dispositivo aparezca en el explorador de archivos de Windows. 

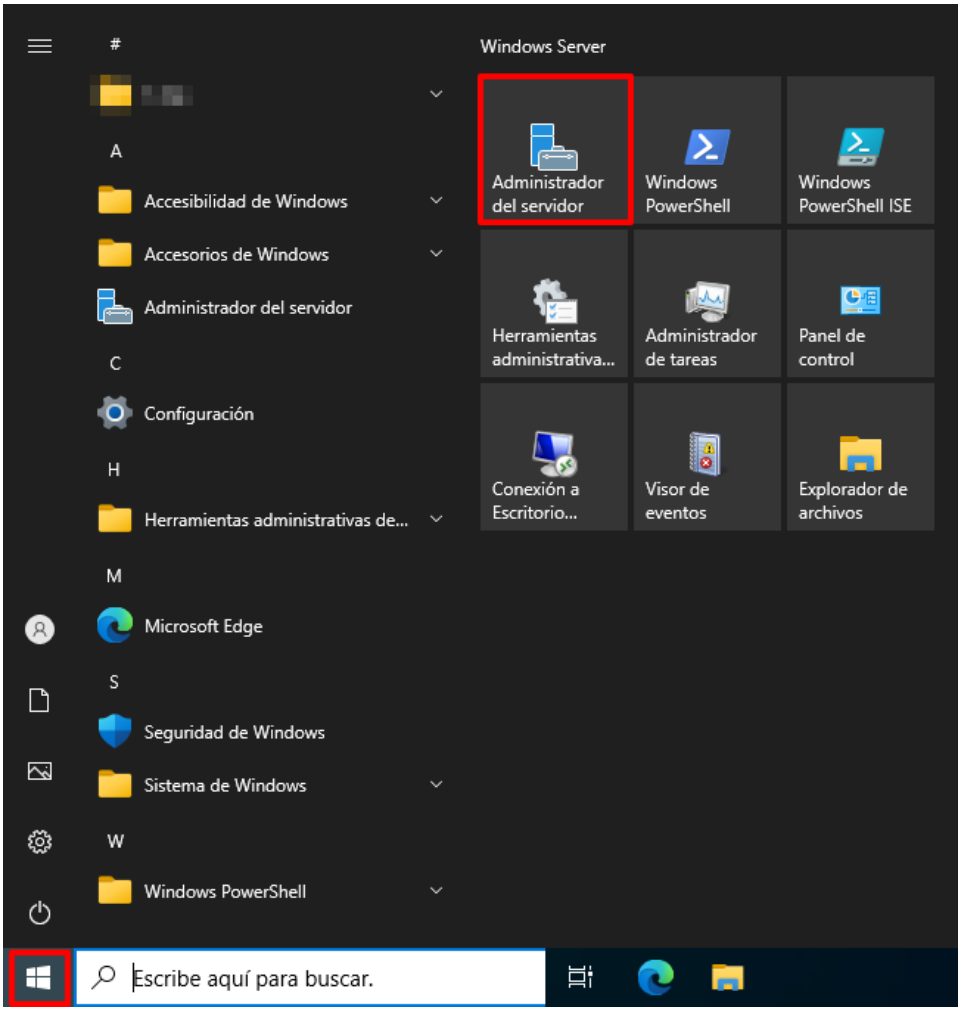
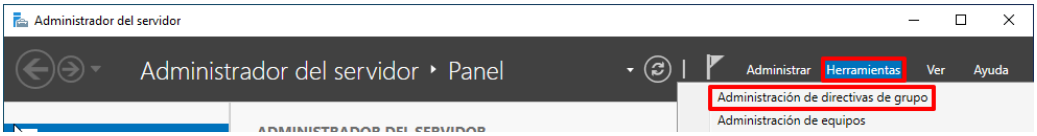
ANEXO B.7.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

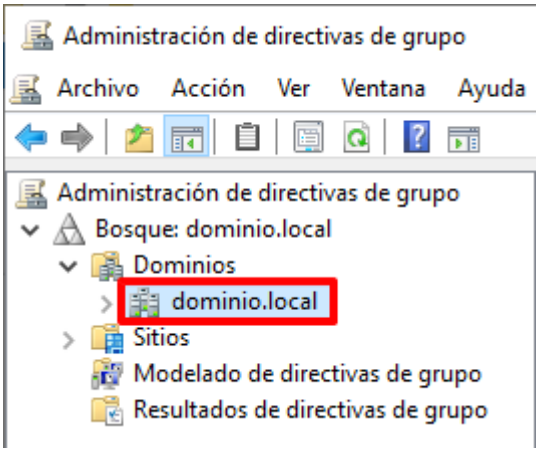
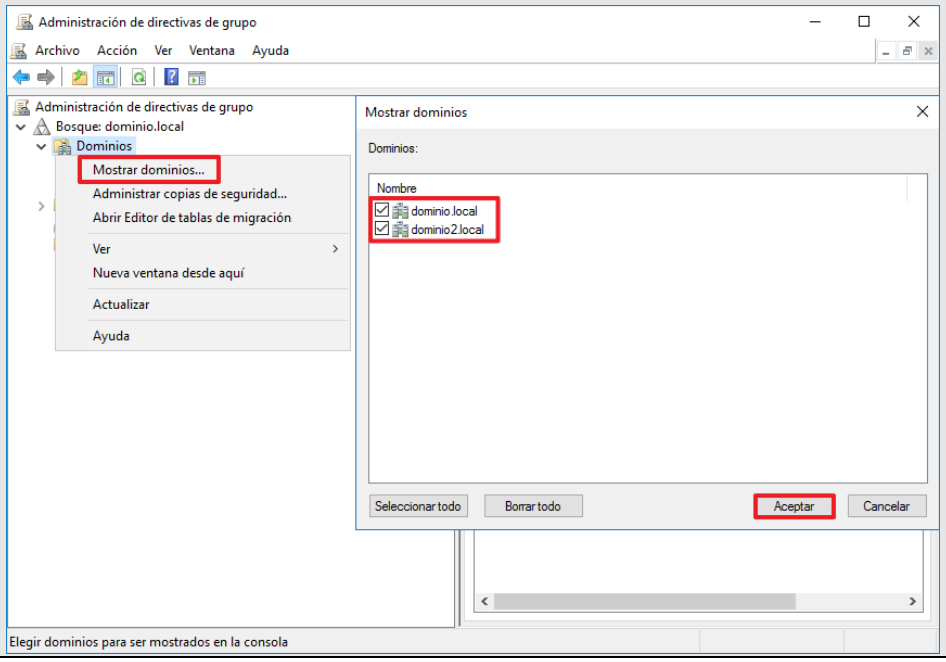
Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del dominio en el cual se está habilitando el uso de dispositivos USB y sobre un Controlador de Dominio perteneciente al dominio.

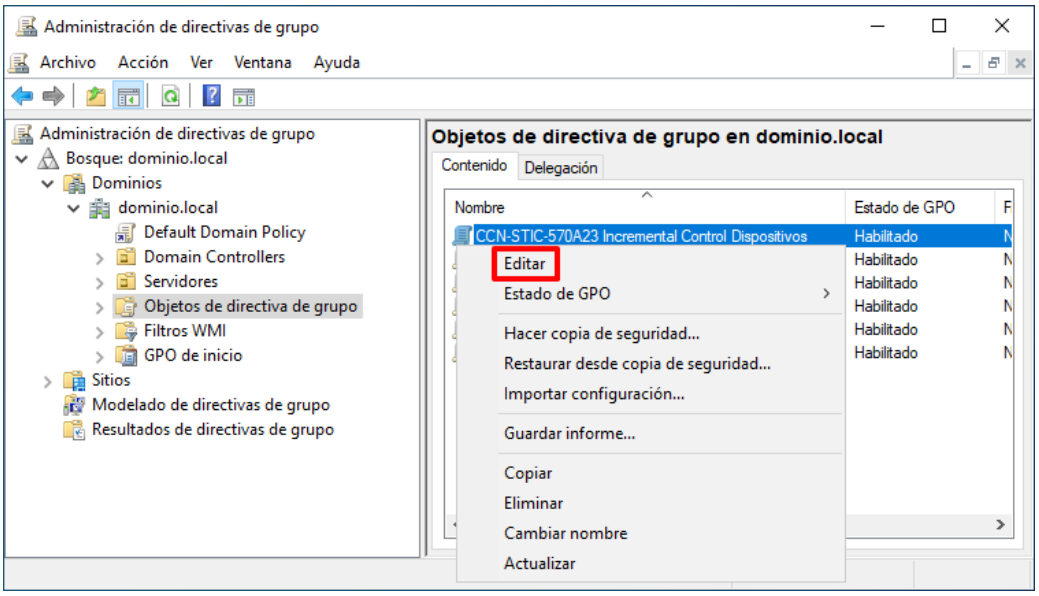
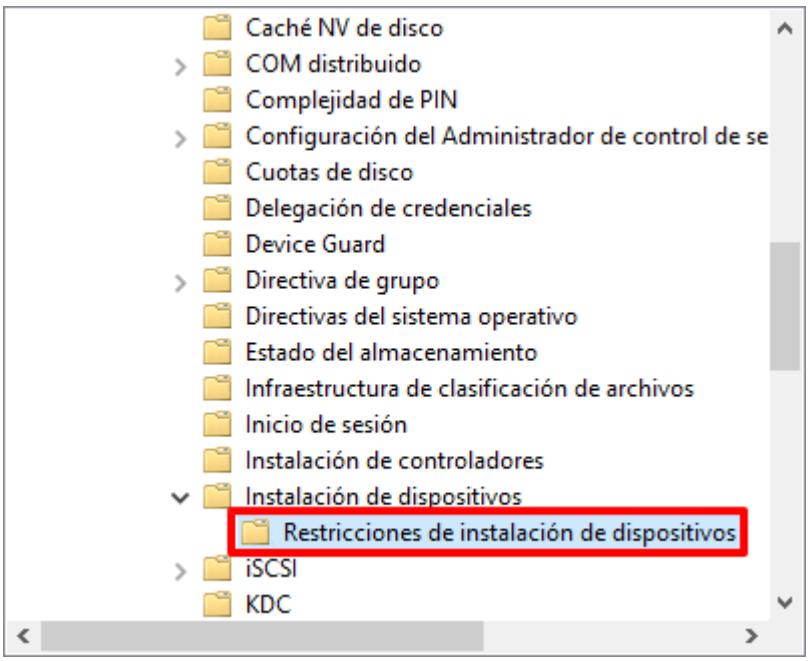
Paso	Descripción
1.	Inicie sesión en el equipo servidor donde pretende habilitar el uso de un dispositivo USB.
2.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

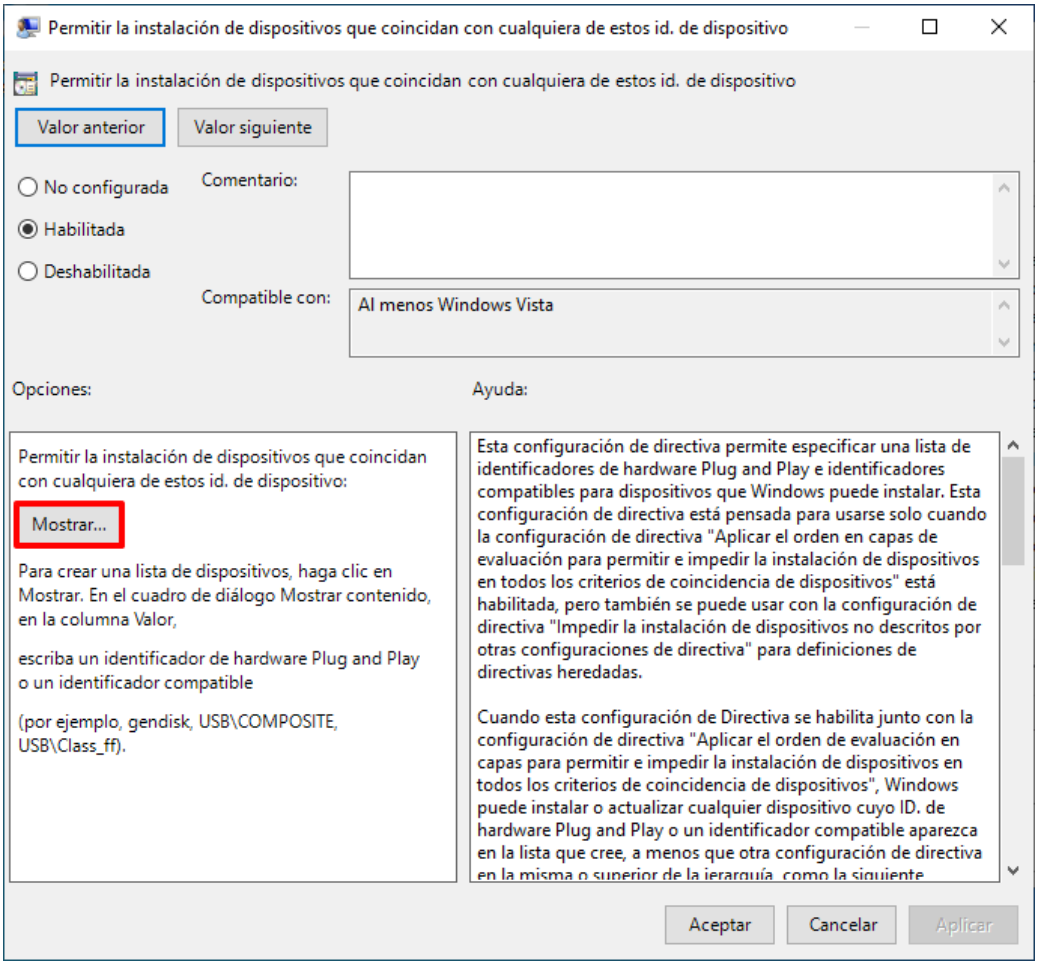
Paso	Descripción
3.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Propiedades”.  **Nota:** Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de “Dispositivo desconocido”.

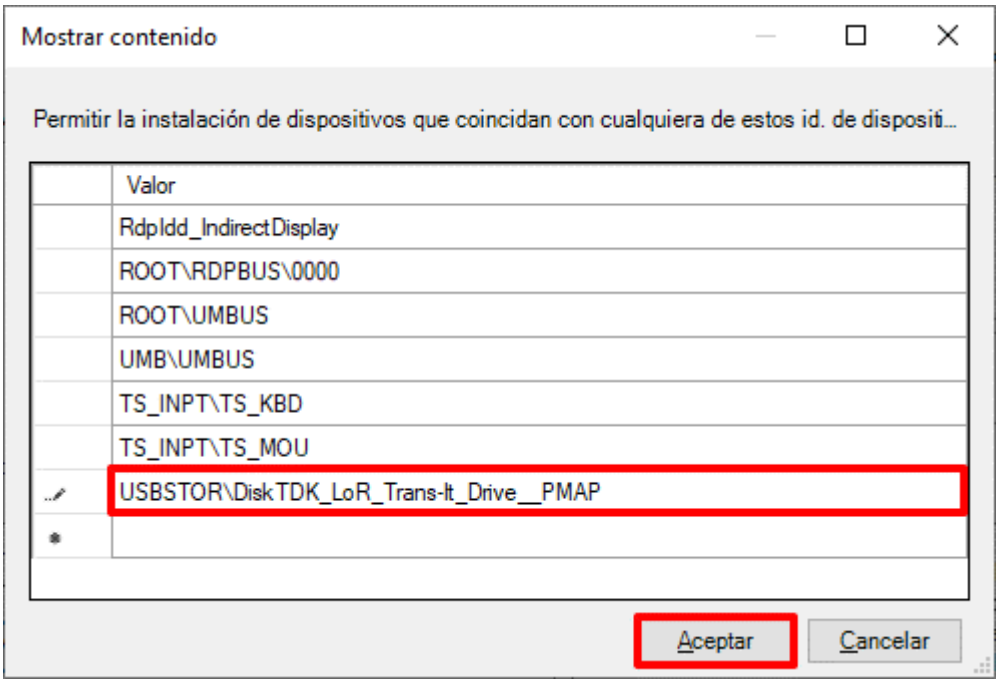
Paso	Descripción
4.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Id. de hardware”. 
5.	Seleccione el identificador que se encuentre en primer lugar y anótelo para poder introducirlo más adelante.  **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

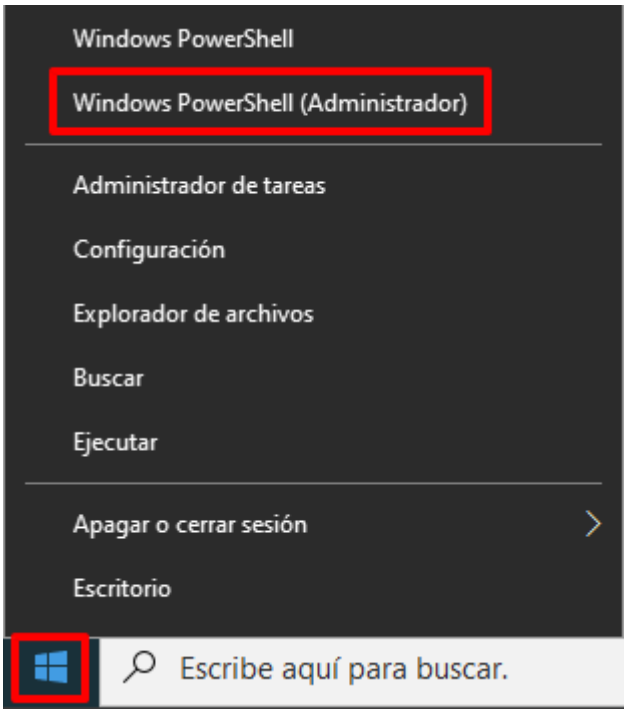
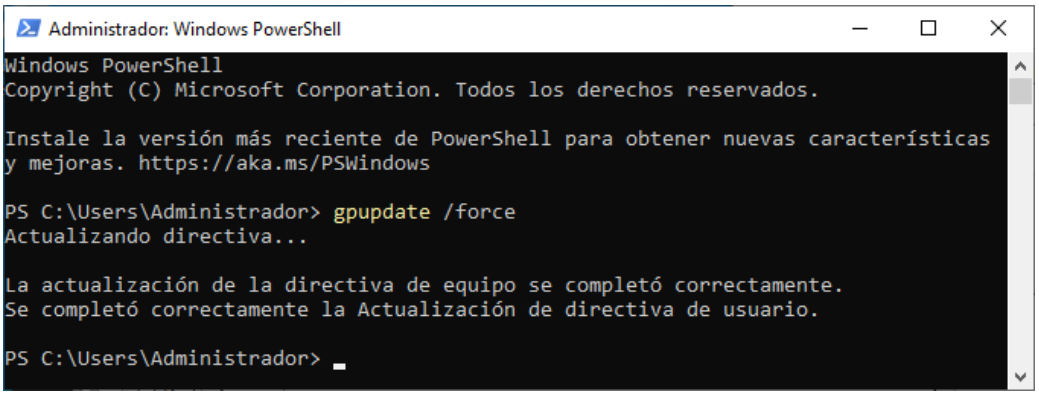
Paso	Descripción
6.	Inicie sesión en un servidor Controlado de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
7.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de "Inicio" para ejecutar el "Administrador del servidor".
8.	En la parte superior derecha pulse sobre el botón "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

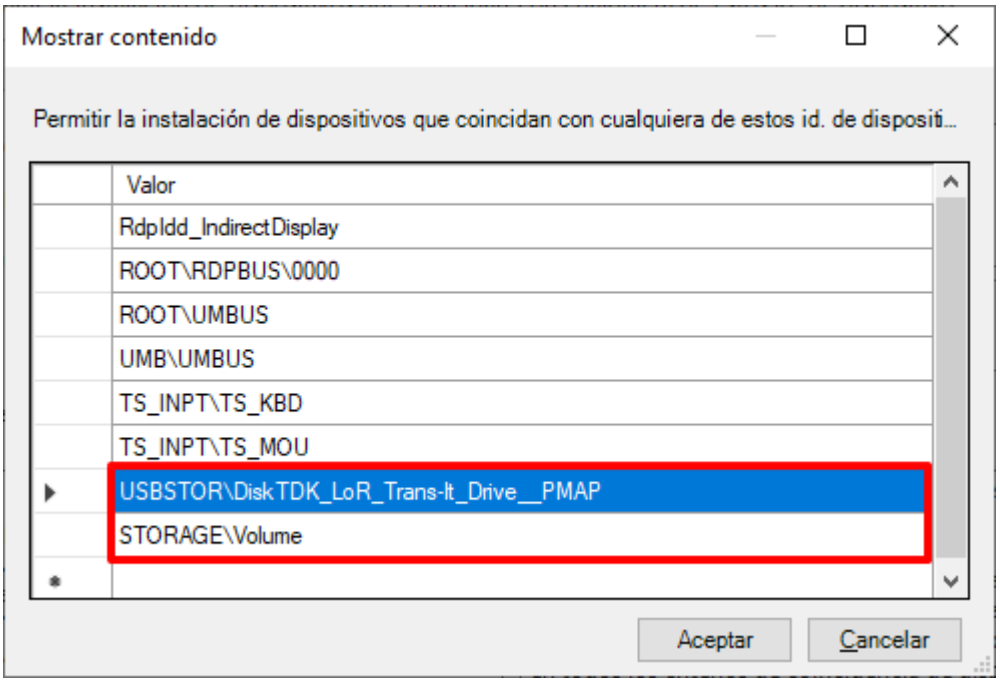
Paso	Descripción
9.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

Paso	Descripción
10.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-570A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
11.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

Paso	Descripción
12.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar…”. 

Paso	Descripción
13.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la última línea para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Verifique el identificador introducido y pulse “Aceptar” para continuar.  **Nota:** No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto funcionamiento del sistema.
14.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.
15.	Sin cerrar el “Editor de directivas de grupo local”, continue con el siguiente paso.

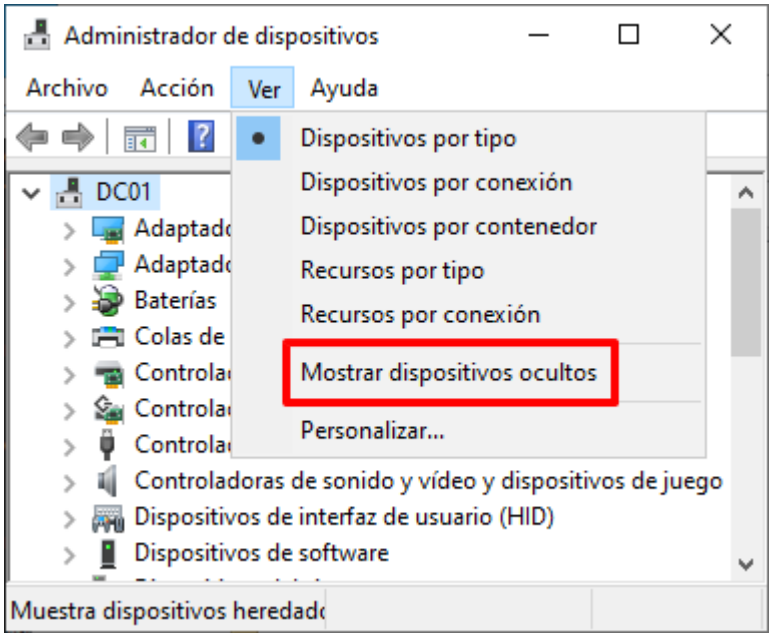
Paso	Descripción
16.	Sobre el equipo destino en el que se desea el uso de un dispositivo USB, haga clic derecho sobre el botón de "Inicio" y pulse sobre "PowerShell (Administrador)". 
17.	Ejecute el siguiente comando en la consola y espere a que finalice. > gpupdate /force 

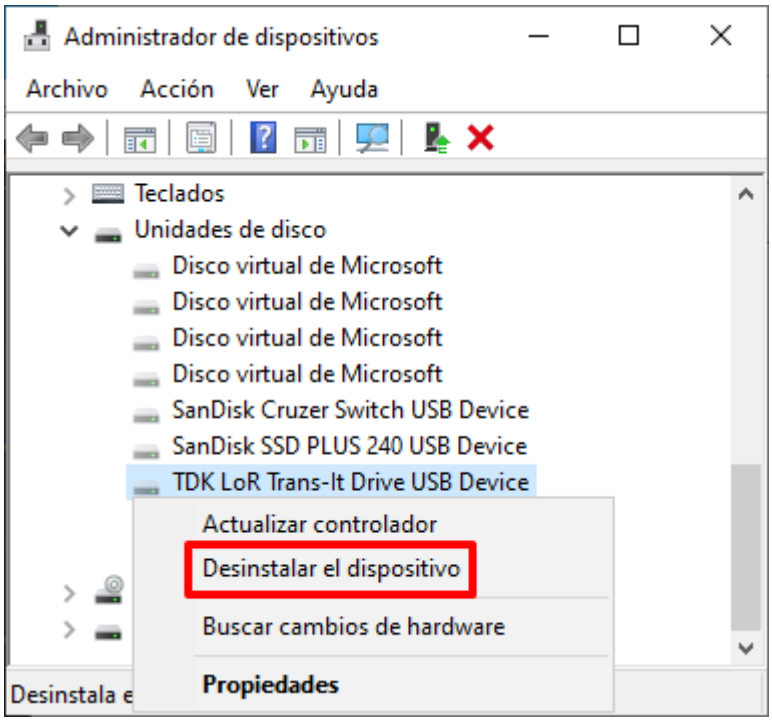
Paso	Descripción
18.	Ejecute de nuevo los pasos 3 a 17 con el objetivo de añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows. 

ANEXO B.7.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

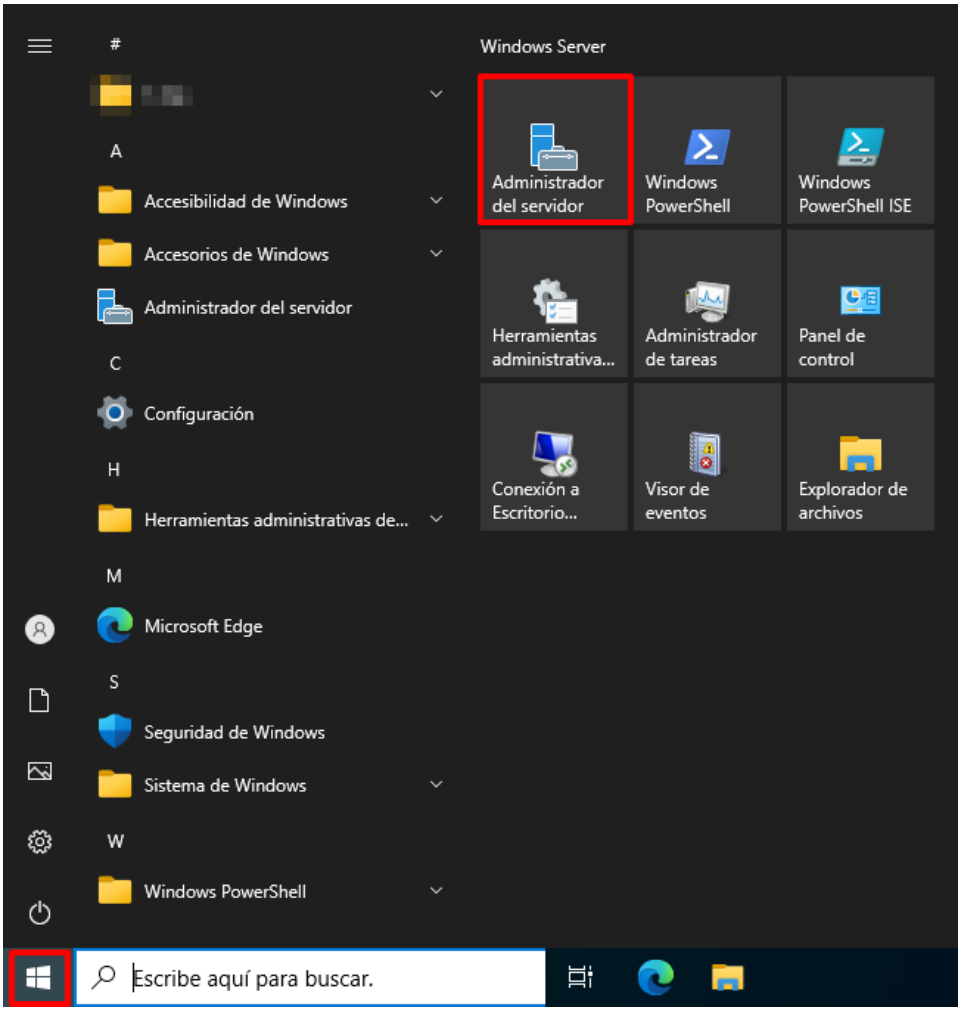
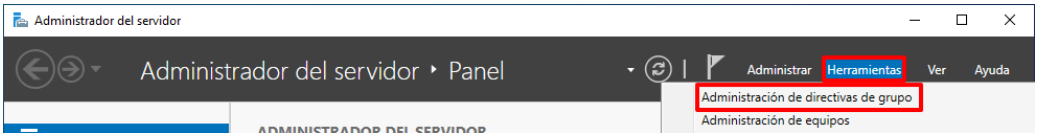
Tras la instalación del dispositivo y su posterior uso, es posible volver al estado anterior de bloqueo del uso de dispositivos USB dado de alta previamente. Para ello deberán seguir los siguientes pasos.

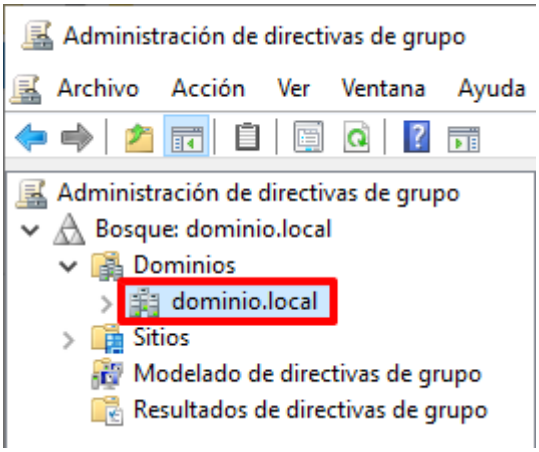
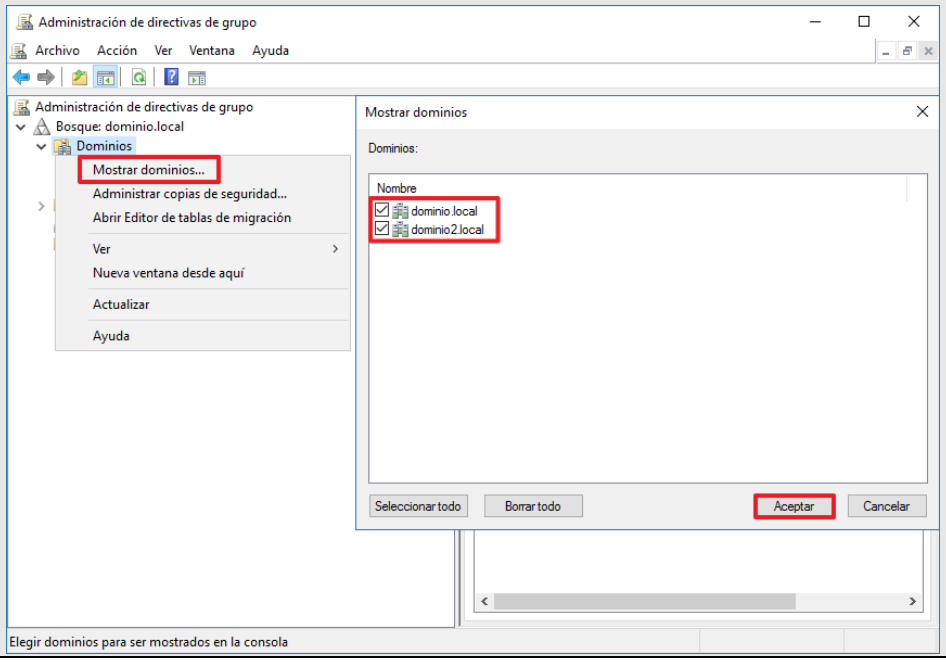
Paso	Descripción
1.	Inicie sesión en el equipo servidor donde pretende eliminar el uso de un dispositivo USB.

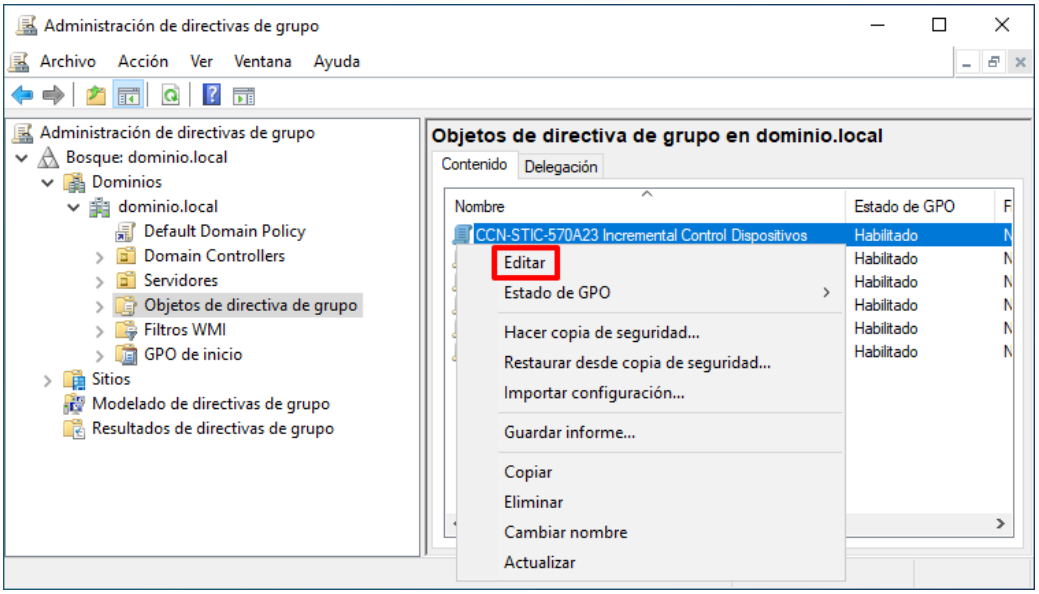
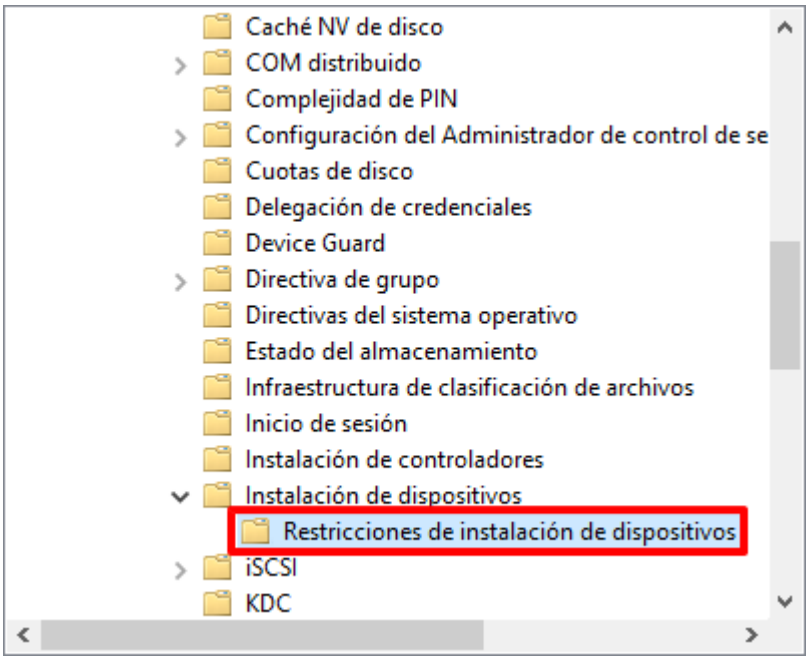
Paso	Descripción
2.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 
3.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

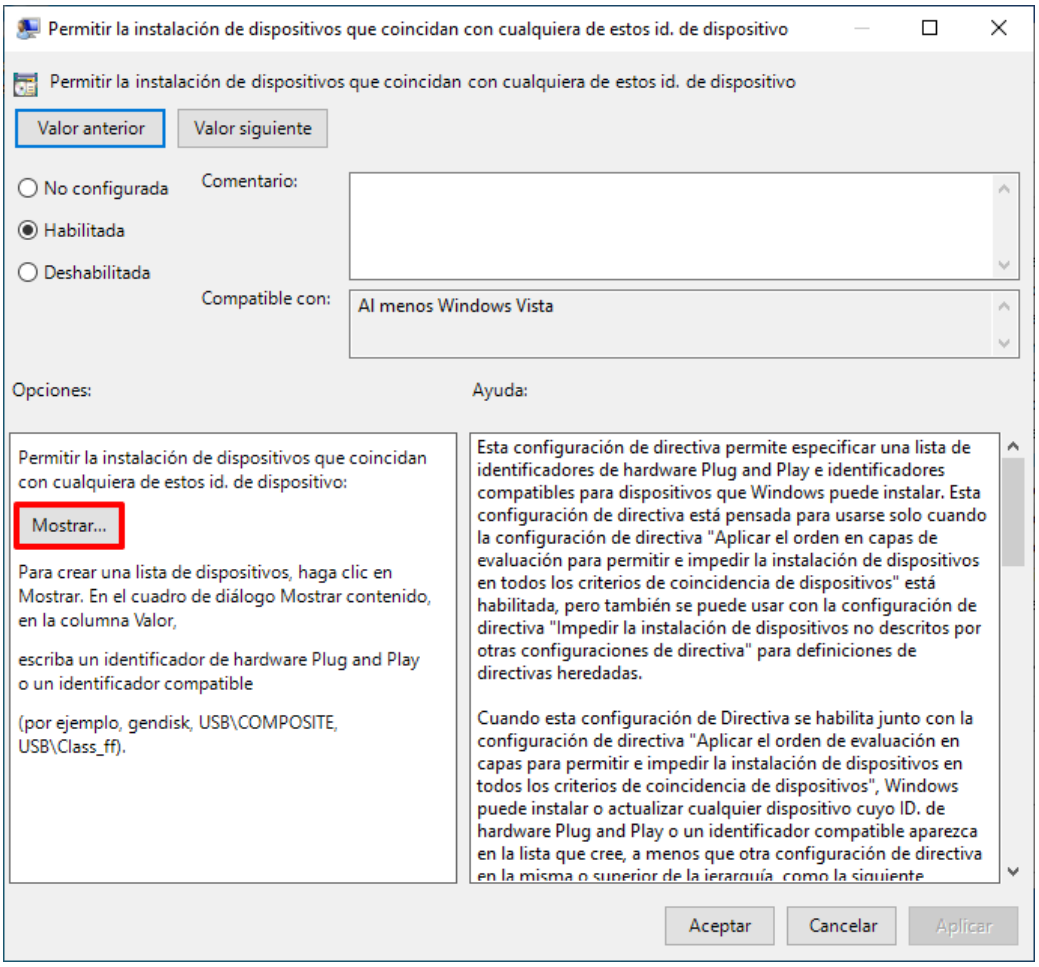
Paso	Descripción
4.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. A continuación, haga clic derecho sobre el mismo y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
5.	Pulse “Desinstalar” ante la advertencia emergente.  **Nota:** Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

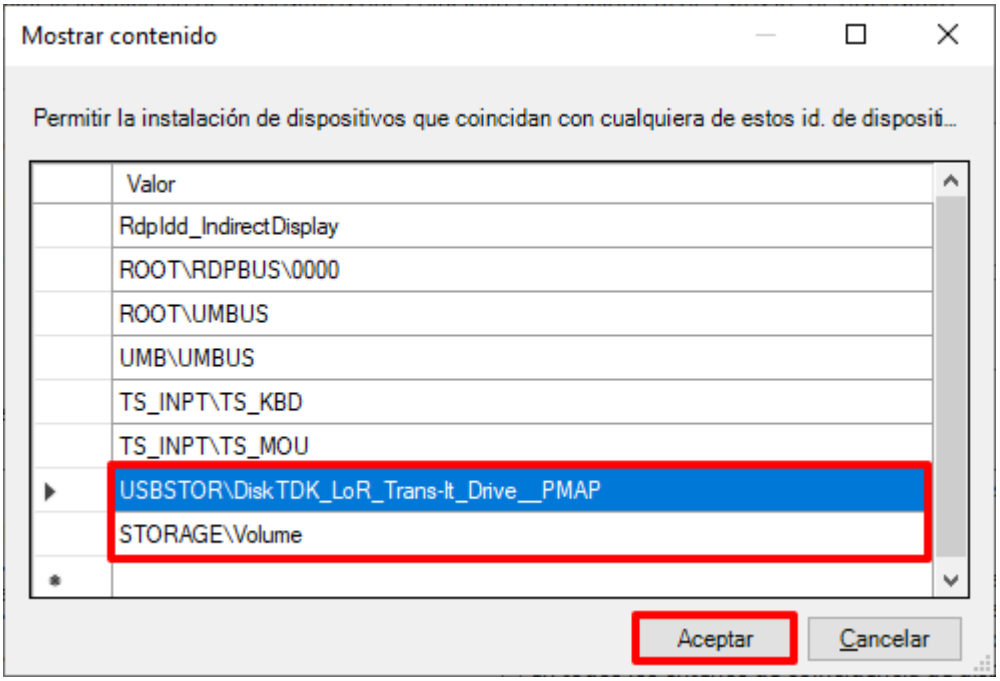
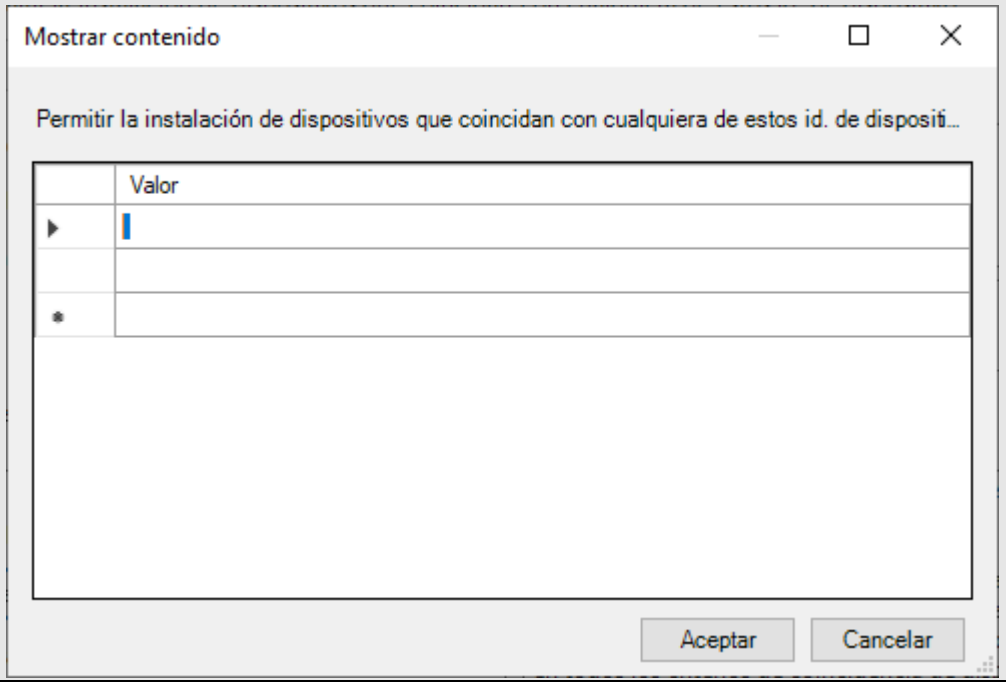
Los siguientes pasos solo serán necesarios en caso de haber hecho uso de la instalación mediante el uso de identificadores únicos de USB.

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

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

Paso	Descripción
5.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-570A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
6.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

Paso	Descripción
7.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar…”. 

Paso	Descripción
8.	En la ventana emergente “Mostrar contenido” elimine los identificadores correspondientes a los dispositivos sobre los cuales ya no se desea su uso. Pulse “Aceptar” para continuar.  **Nota:** No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto funcionamiento del sistema. En caso de necesitar eliminar todas las líneas, debe dejarse al menos una línea con un espacio en blanco para poder cerrar la configuración de la directiva. En caso contrario se mostrará un error. 

ANEXO C. CONFIGURACIONES DE MEJORA

El presente apartado define aquellas configuraciones que, sin ser obligatorias, permiten agregar un nivel de refuerzo adicional.

ANEXO C.1. REQUISITOS DE ACCESO (CONTROL DE ACCESO A DISPOSITIVOS)

El siguiente apartado tiene como objetivo ayudar a los administradores con el control y uso de dispositivos conectados sobre los equipos de tipo servidor independientemente de su rol dentro de un dominio.

Nota: Se debe tener en consideración que tras la aplicación de los siguientes puntos se limitará la instalación de cualquier tipo de dispositivo, no solo dispositivos USB si no cualquier otro elemento como disco duro, tarjeta de red, etc.

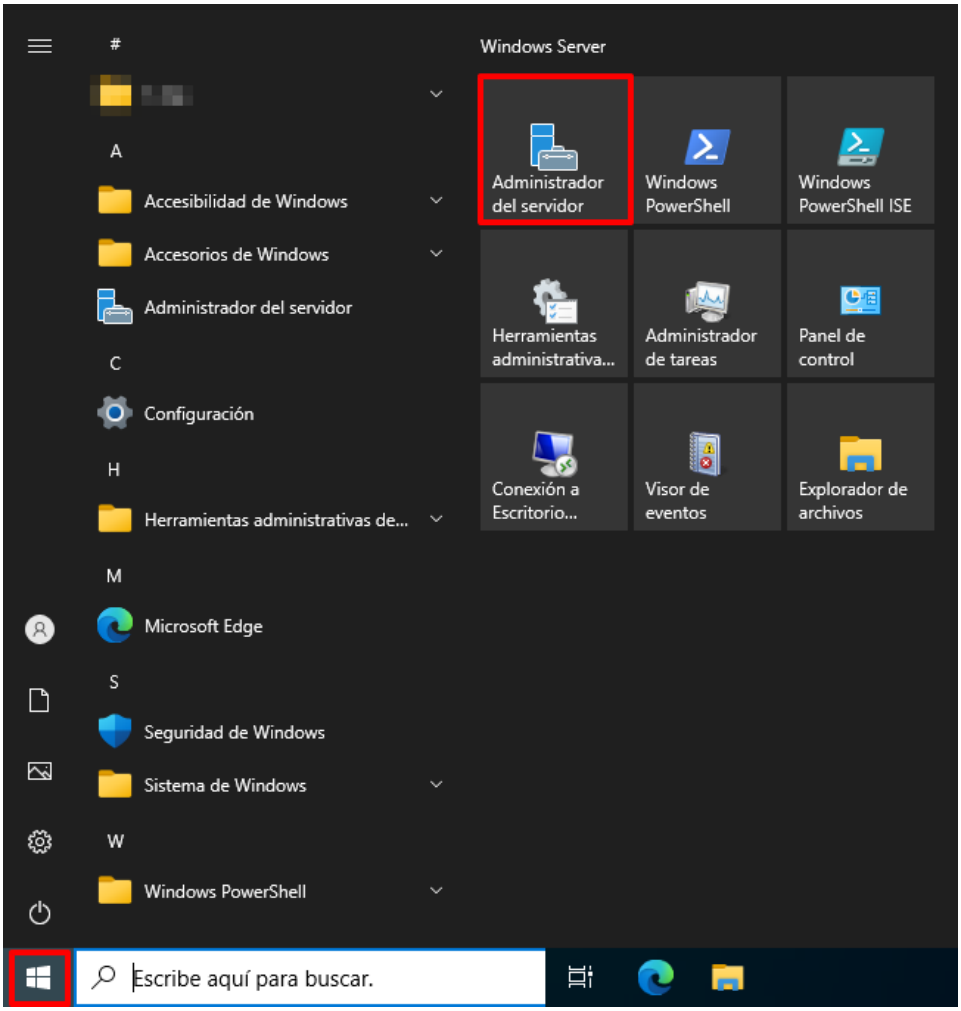
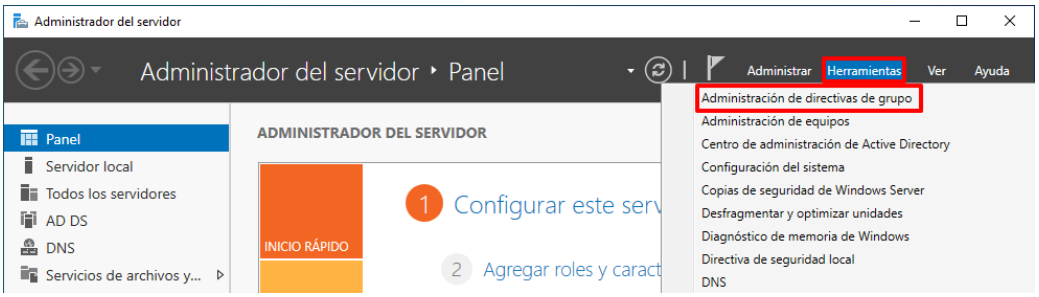
Realizadas las acciones descritas en el presente punto se presentarán dos formas de instalar controladores para el uso de dispositivos.

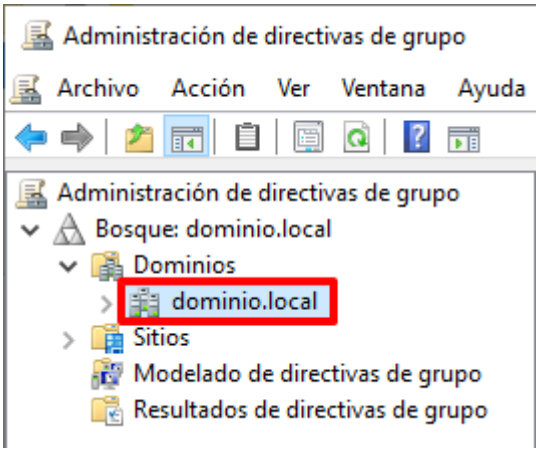
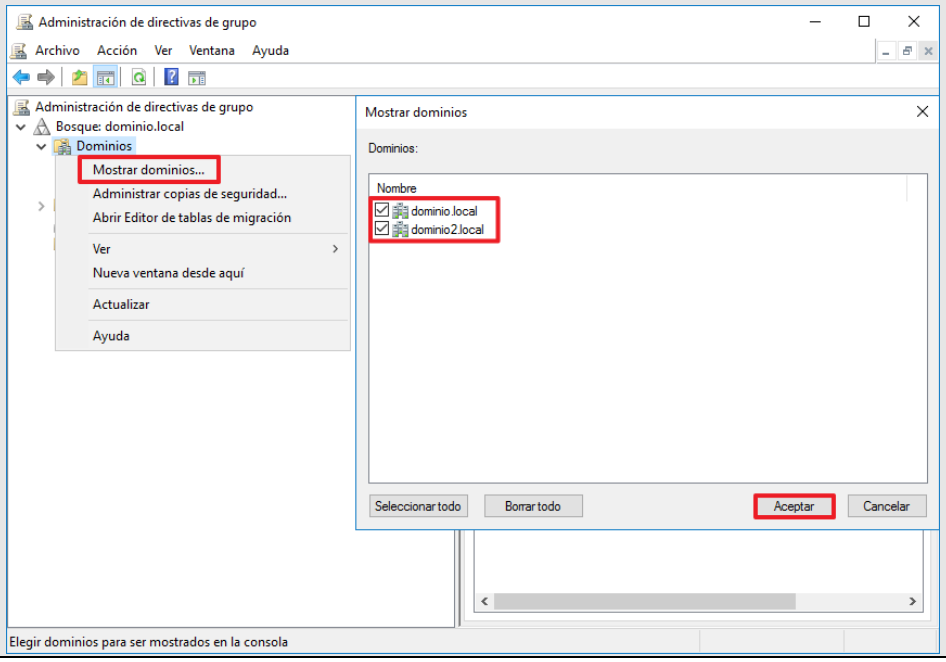
a) Actualización automática de controladores por parte de usuario con privilegios de administrador.

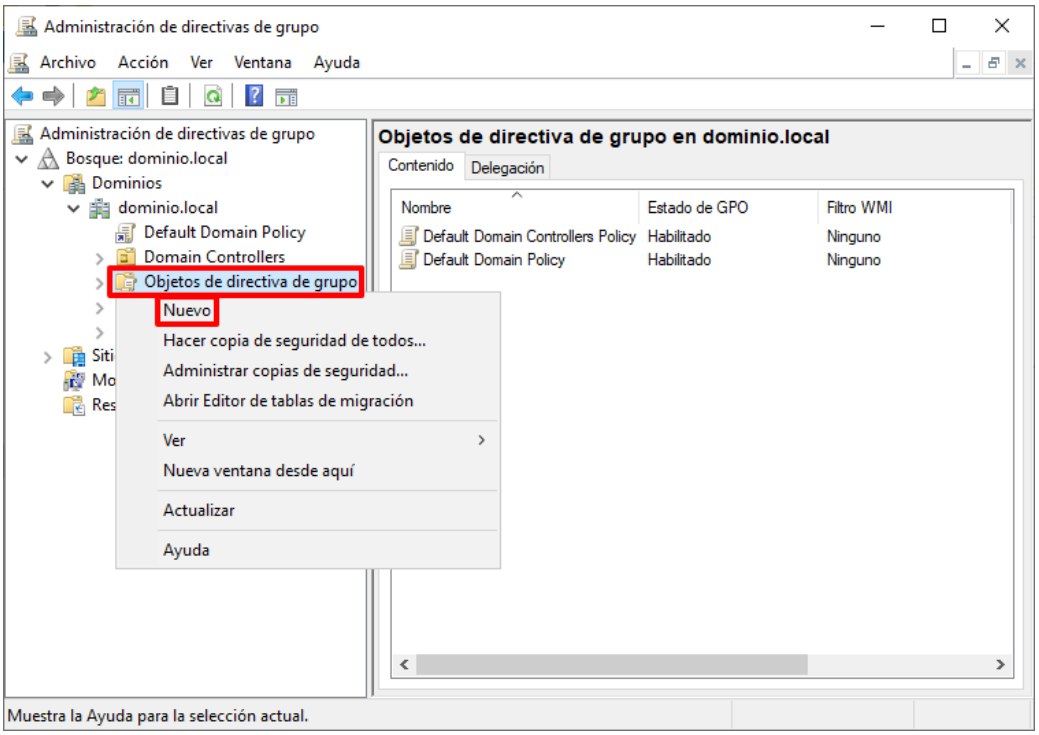
b) Alta de dispositivos por medio de identificadores únicos de los dispositivos.

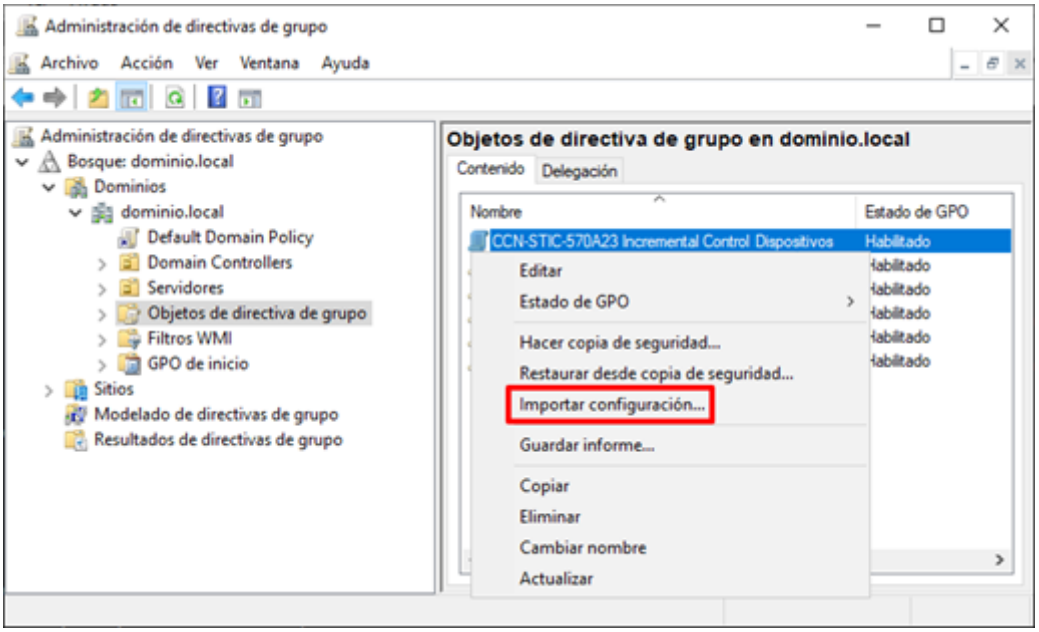
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. A pesar de esto, las configuraciones y pasos descritos a continuación son válidos para el perfil "Uso Oficial" y obligatorio para el perfil "Materias Clasificadas", tal y como se expone en el anexo correspondiente.

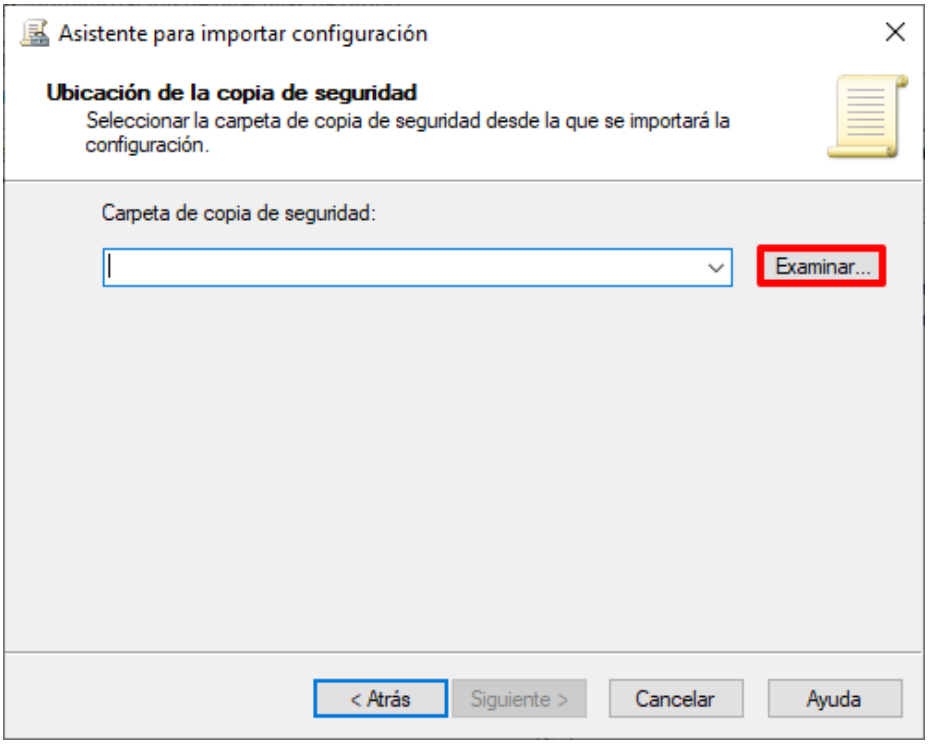
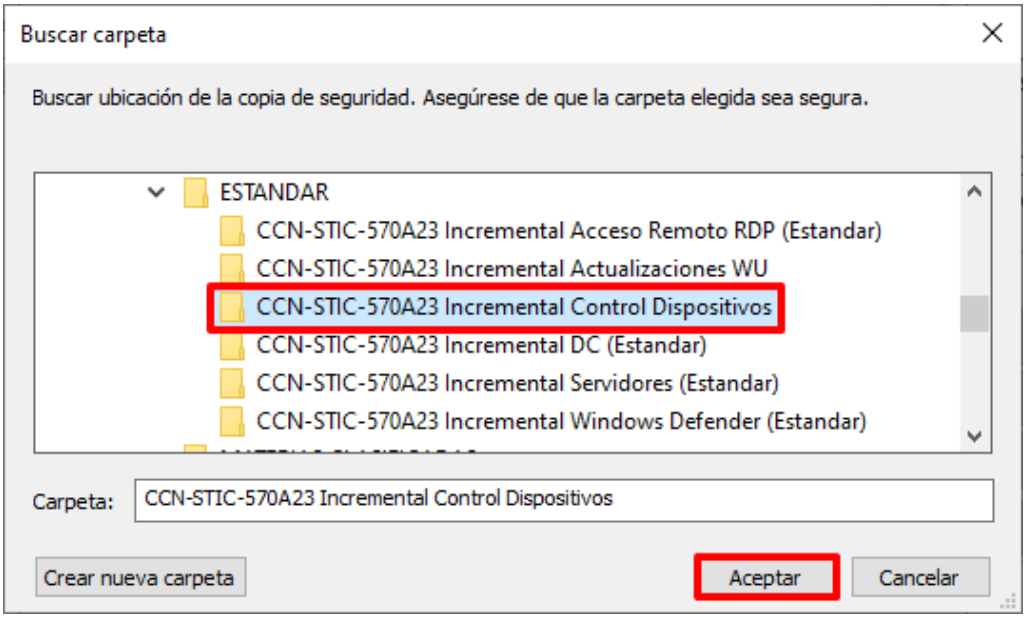
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

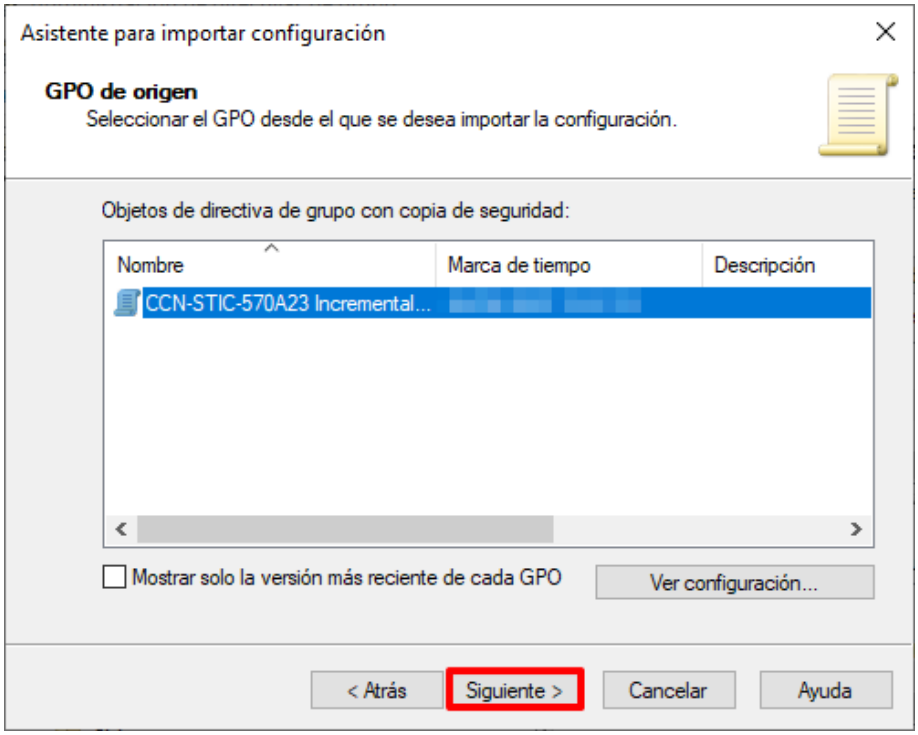
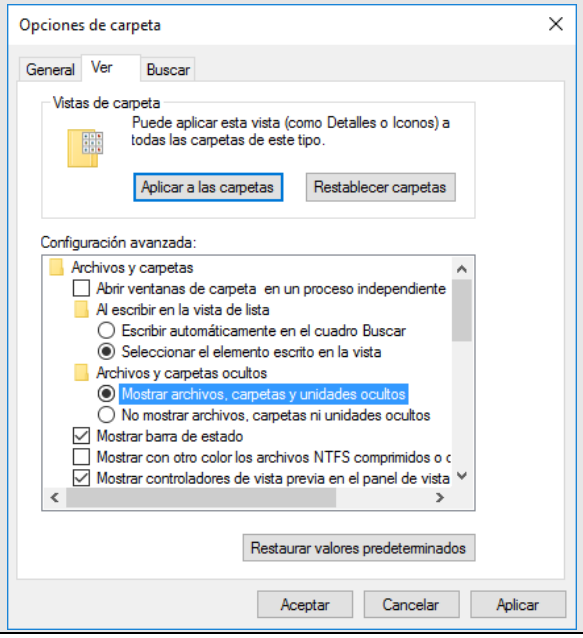
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

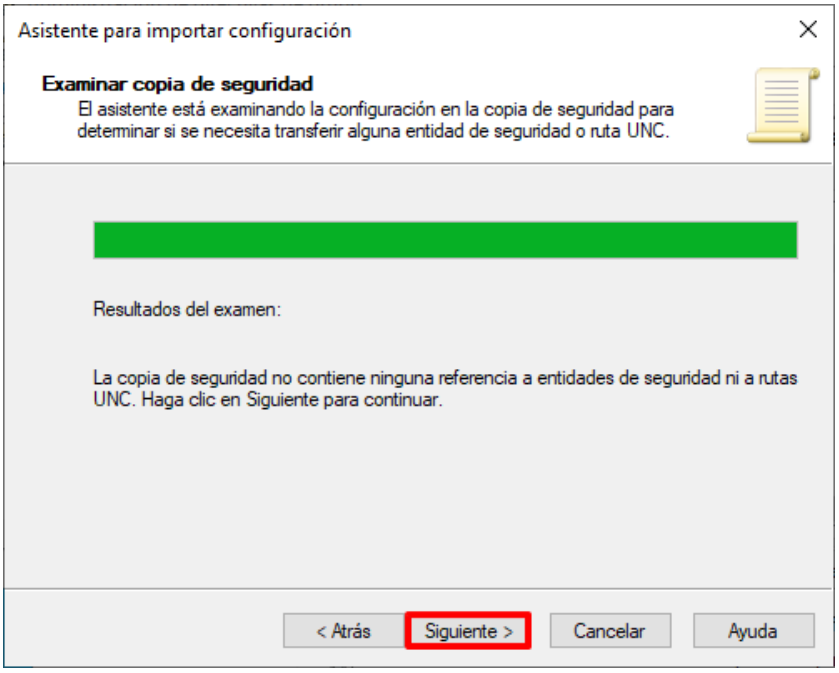
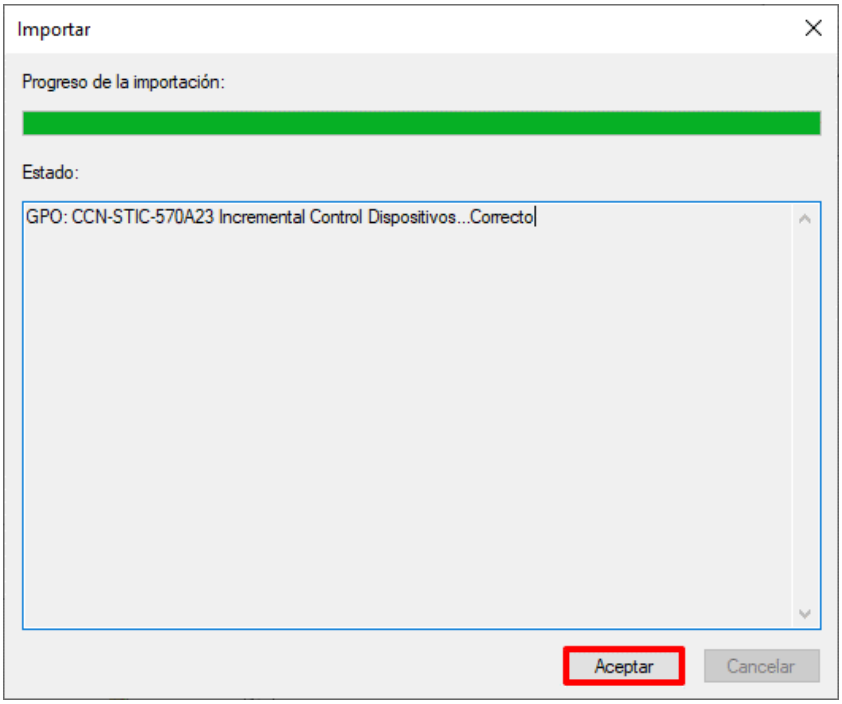
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

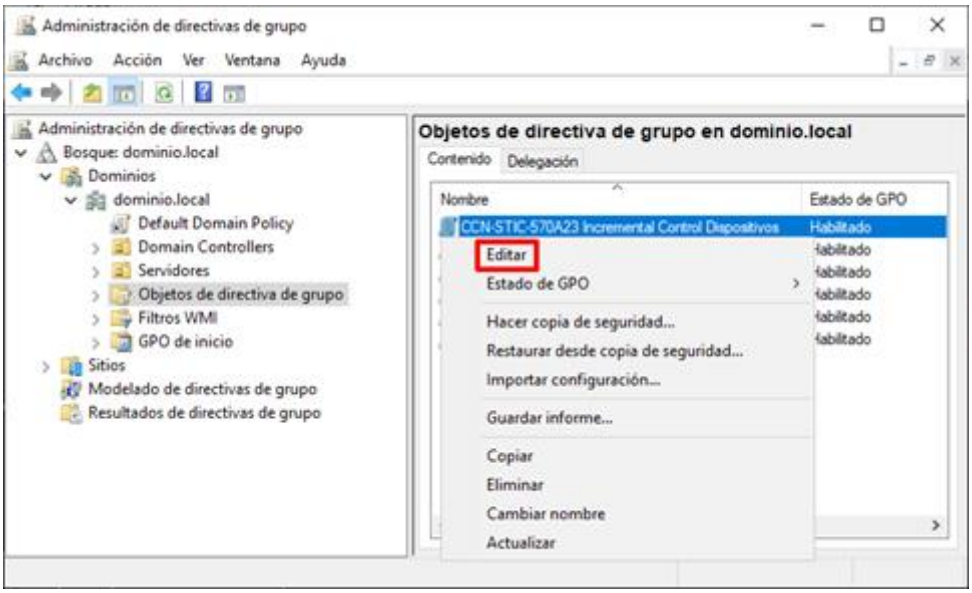
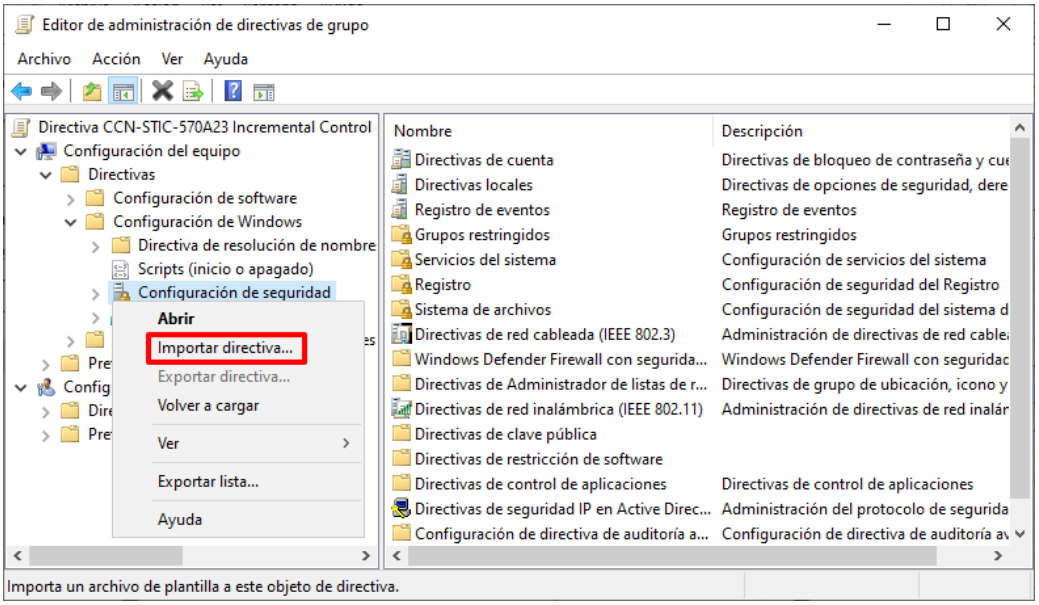
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-570A23 Incremental Control Dispositivos**" y pulse el botón "Aceptar". 

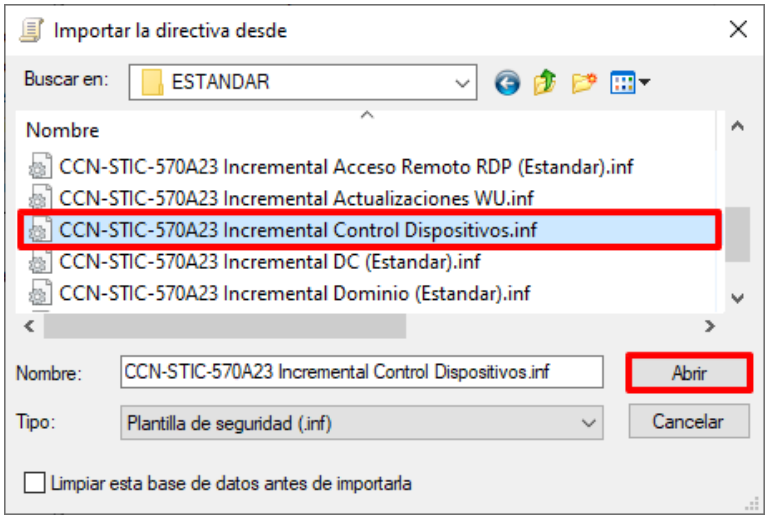
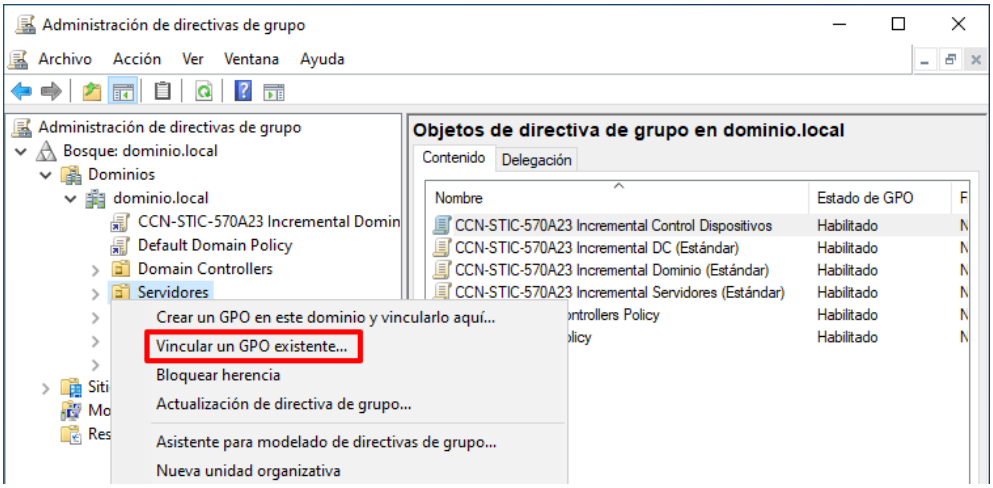
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

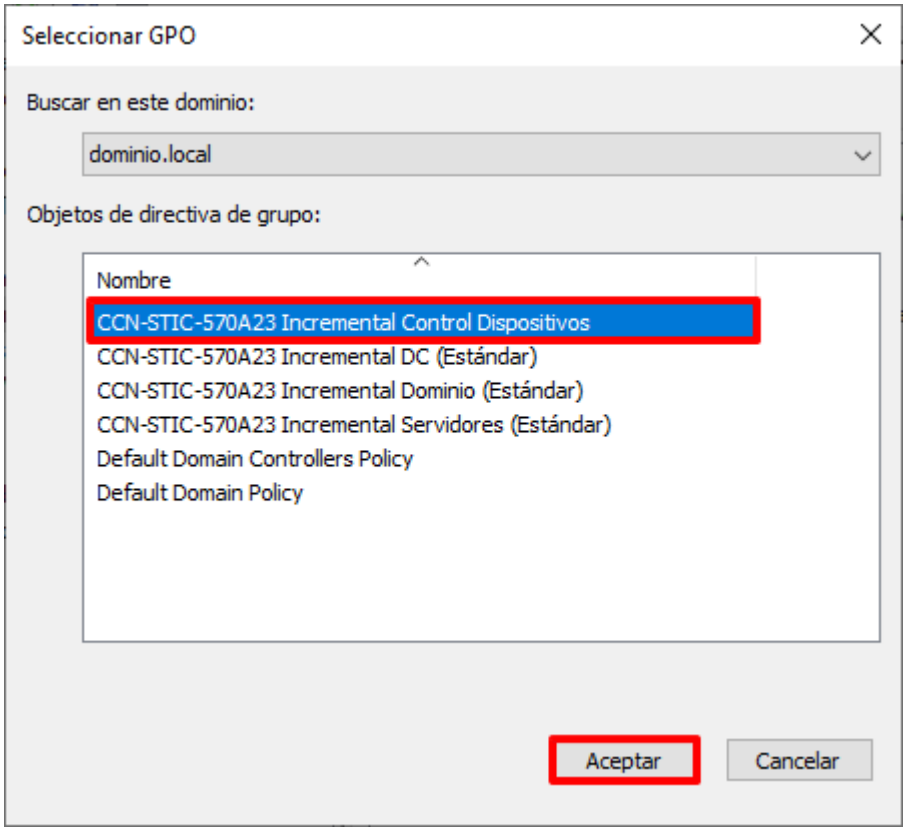
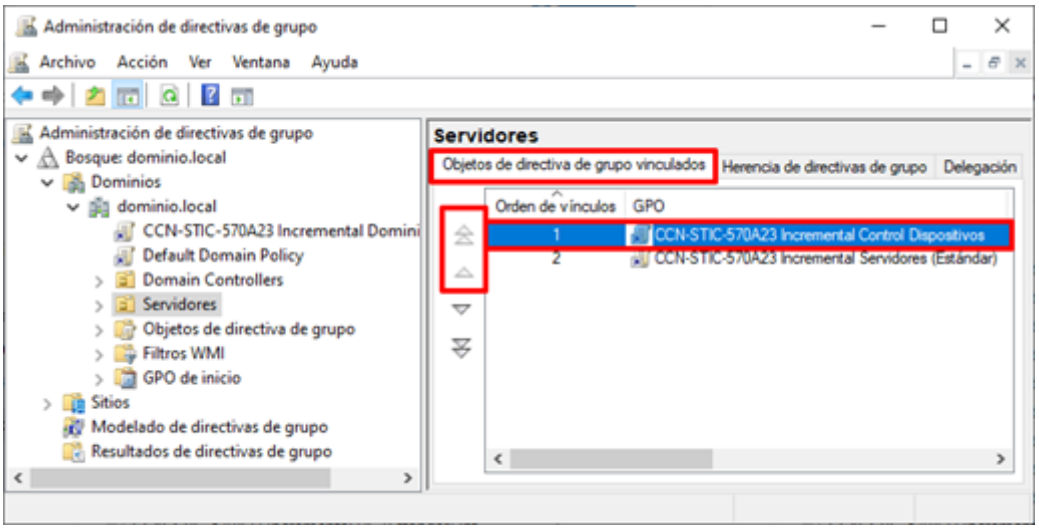
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-570A23 Incremental Control Dispositivos” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.

Paso	Descripción
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-570A23 Incremental Control Dispositivos” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior del explorador de archivos) la opción “Mostrar archivos, carpetas y unidades ocultos”. 

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

Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-570A23 Incremental Control Dispositivos” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá. 
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“CCN-STIC-570A23 Incremental Control Dispositivos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad”**. Seleccione con el botón derecho el nodo “Configuración de seguridad” y seleccione la opción "Importar directiva..." del menú contextual que aparecerá. 

Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-570A23 Incremental Control Dispositivos.inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** Seleccione la plantilla de seguridad acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
21.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de actualizaciones y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho sobre la unidad organizativa y seleccione la opción "Vincular un GPO existente…".  **Nota:** Vincule el objeto GPO a nivel de dominio si desea que se aplique sobre todos los objetos del dominio, pero teniendo en consideración la posibilidad de que existan objetos GPO en un nivel inferior que modifiquen dicha configuración. En este ejemplo se hace uso de la Unidad Organizativa "Servidores", creada para tal fin.

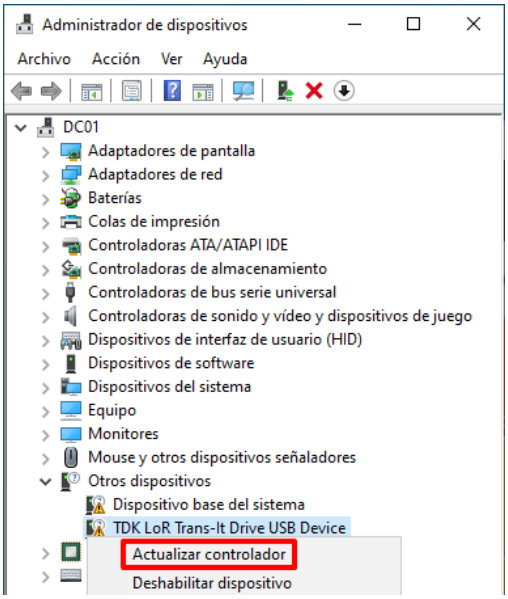
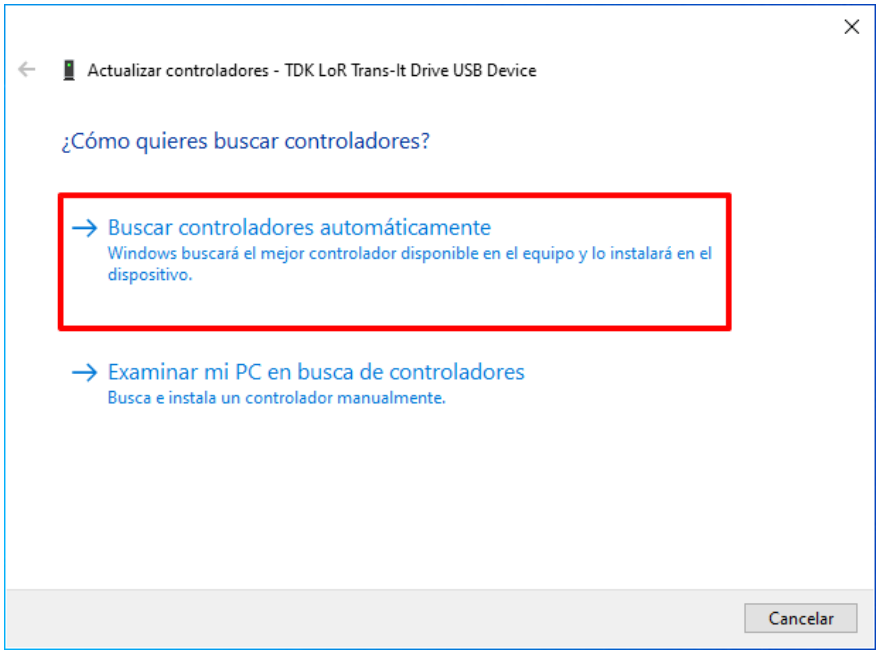
Paso	Descripción
22.	A continuación, seleccione el objeto GPO "CCN-STIC-570A23 Incremental Control Dispositivos" y pulse "Aceptar". 
23.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

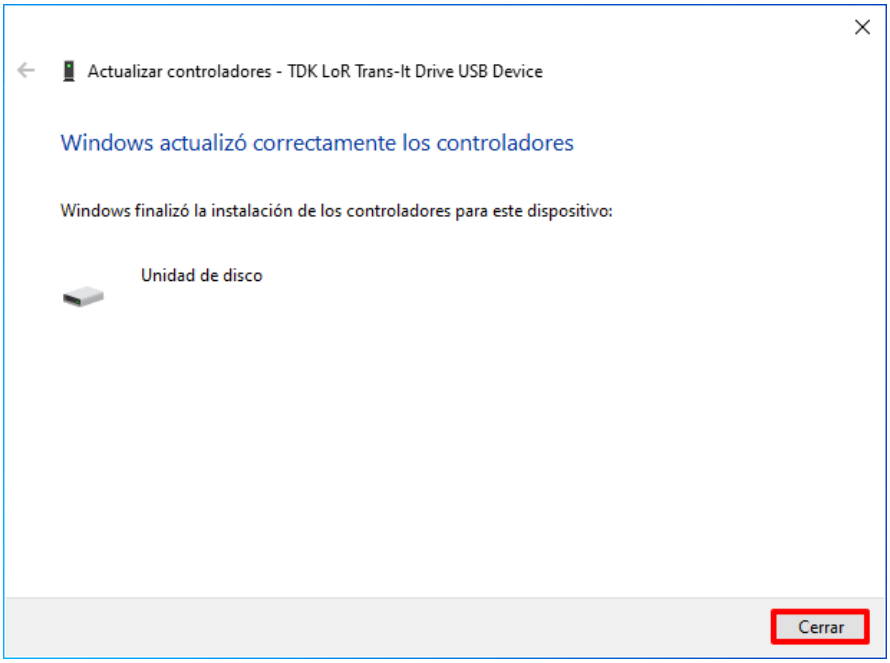
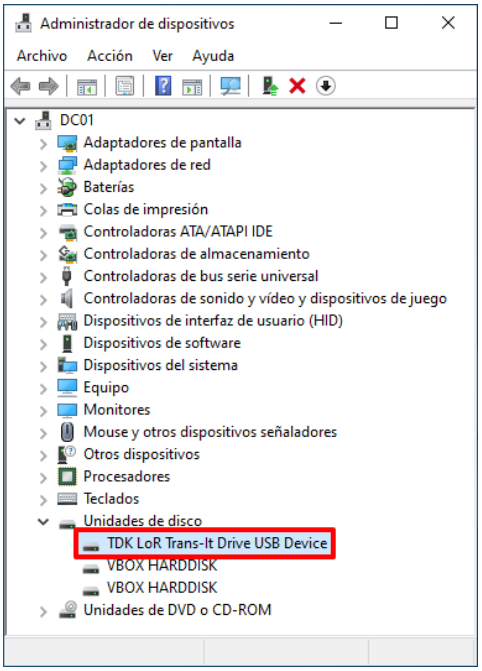
Paso	Descripción
24.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación de otra unidad organizativa anidada sobre la principal de modo que el objeto GPO creado se vincule exclusivamente sobre dicha unidad organizativa y no sobre la principal. – Generación de un grupo que aúne los equipos afectados y su configuración dentro del filtrado de seguridad dentro del objeto GPO. **Nota:** Puede consultar el apartado "ANEXO A.3.2 FILTRADO DE SEGURIDAD DE OBJETOS GPO" para conocer cómo realizar un filtrado en la aplicación de un objeto GPO por medio del uso de un grupo de seguridad.

ANEXO C.1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES

Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del dominio en el cual se está habilitando el uso de dispositivos USB.

Paso	Descripción
1.	Inicie sesión en el equipo servidor donde pretende habilitar el uso de un dispositivo USB.
2.	Haga clic derecho sobre el botón de "Inicio" y seleccione "Administrador de dispositivos". 

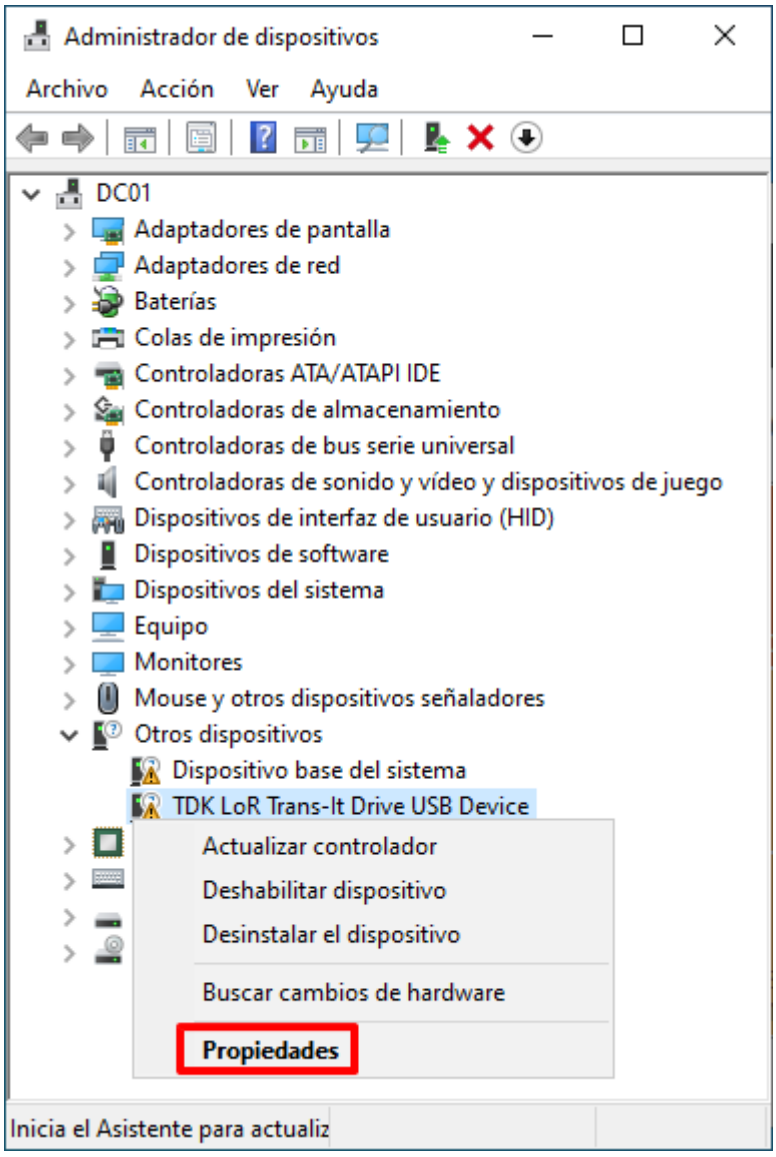
Paso	Descripción
3.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”.  **Nota:** Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de “Dispositivo desconocido”.
4.	A continuación, se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 

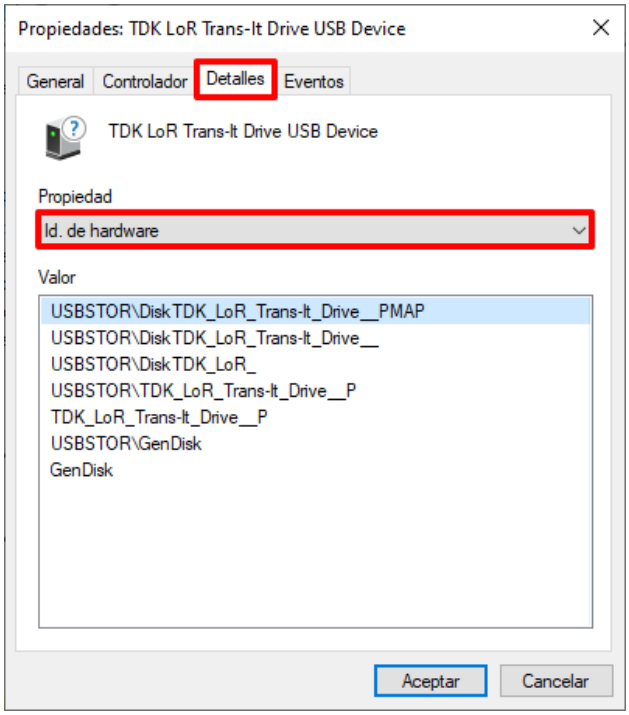
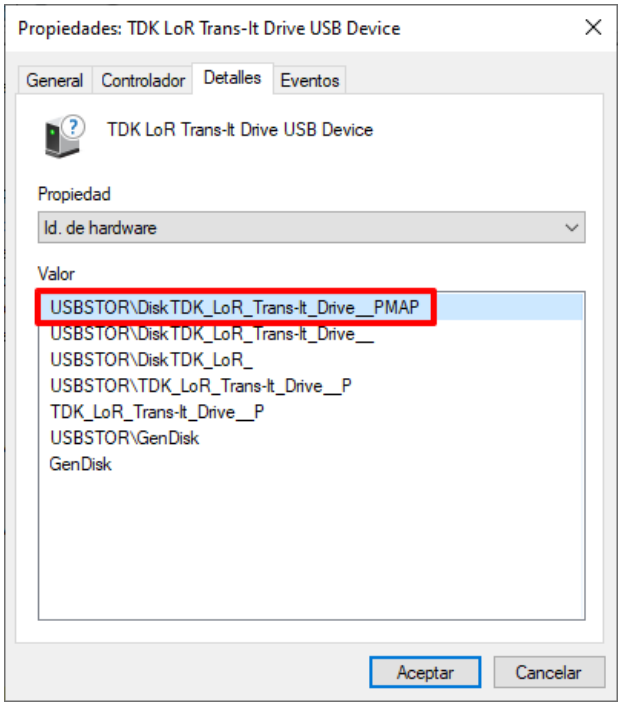
Paso	Descripción
5.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  **Nota:** No cierre el “Administrador de dispositivos” todavía.
6.	Ejecute los mismos pasos anteriores (pasos 3 a 5) hasta que el dispositivo aparezca en el apartado “Unidades de disco” y no exista ningún otro controlador dependiente en el apartado “Otros dispositivos”. Podrá corroborar que no existe ningún controlador necesario adicional cuando el dispositivo aparezca en el explorador de archivos de Windows. 

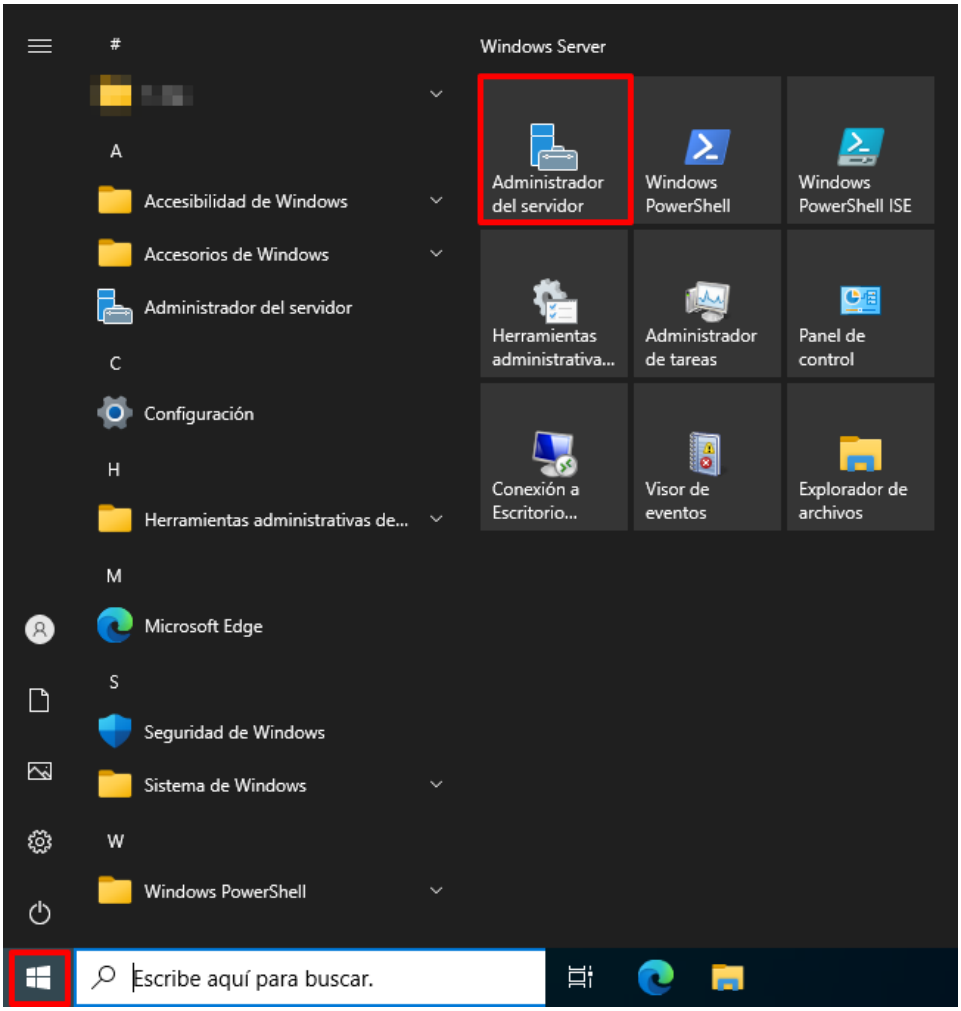
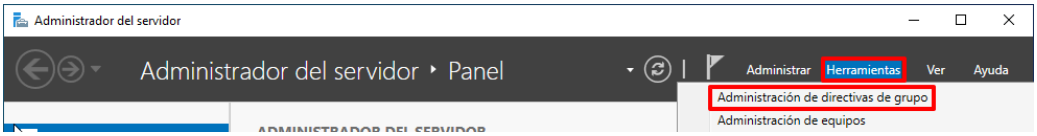
ANEXO C.1.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

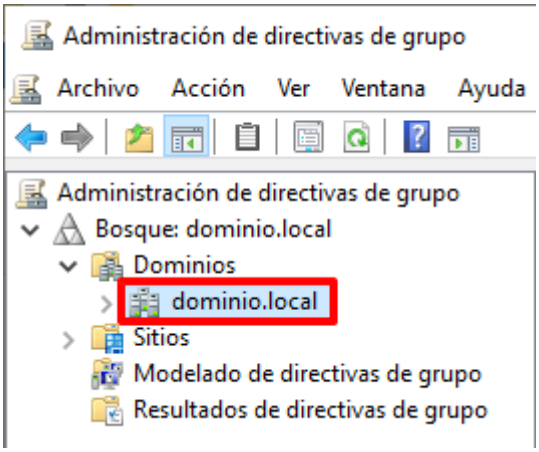
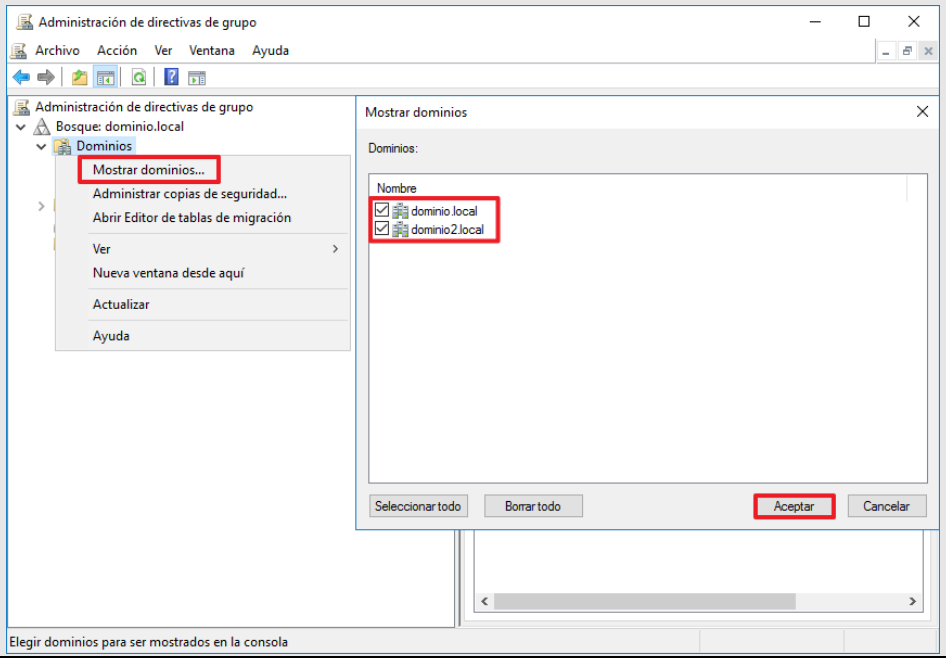
Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del dominio en el cual se está habilitando el uso de dispositivos USB y sobre un Controlador de Dominio perteneciente al dominio.

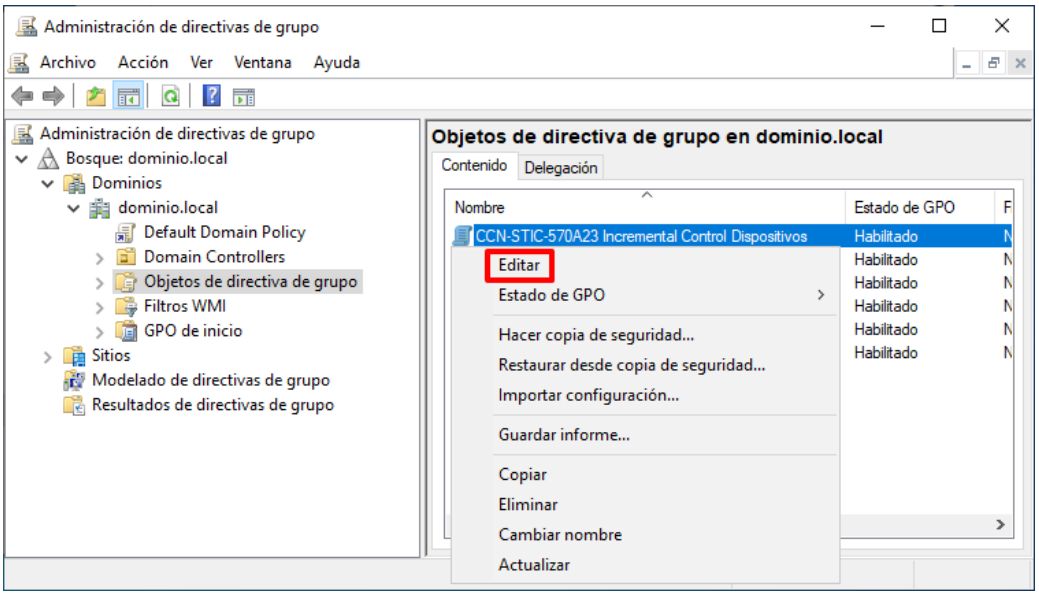
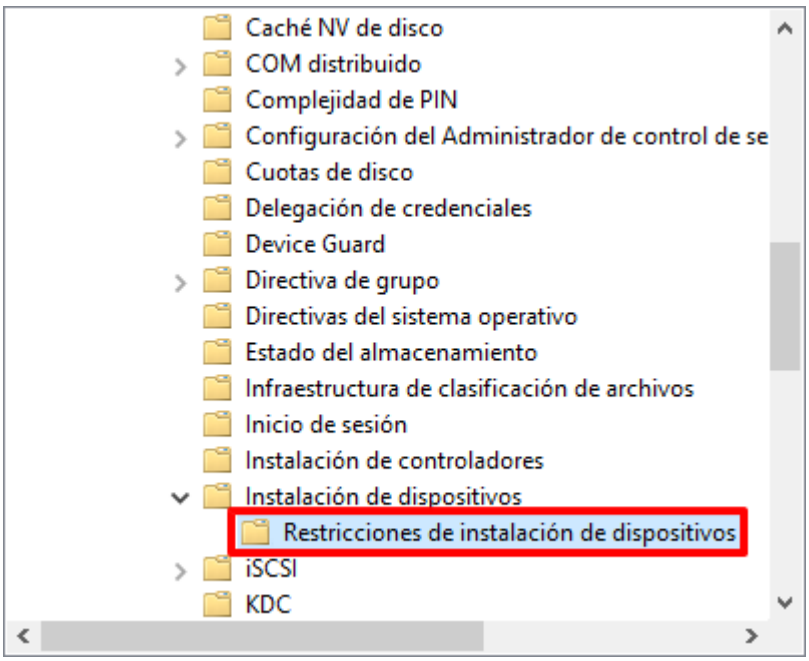
Paso	Descripción
1.	Inicie sesión en el equipo servidor donde pretende habilitar el uso de un dispositivo USB.
2.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

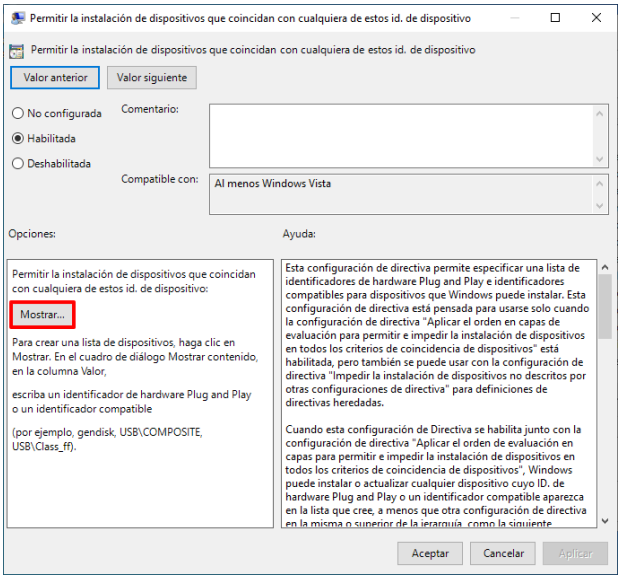
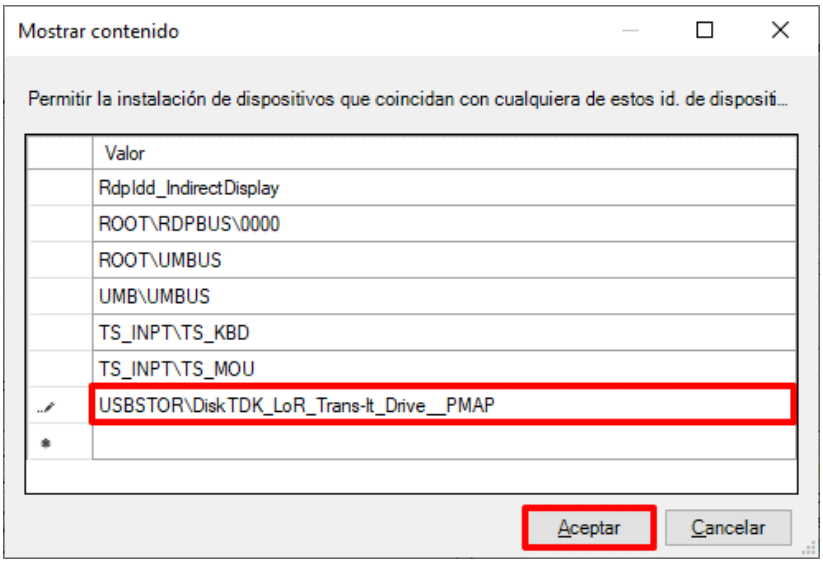
Paso	Descripción
3.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Propiedades”.  **Nota:** Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de “Dispositivo desconocido”.

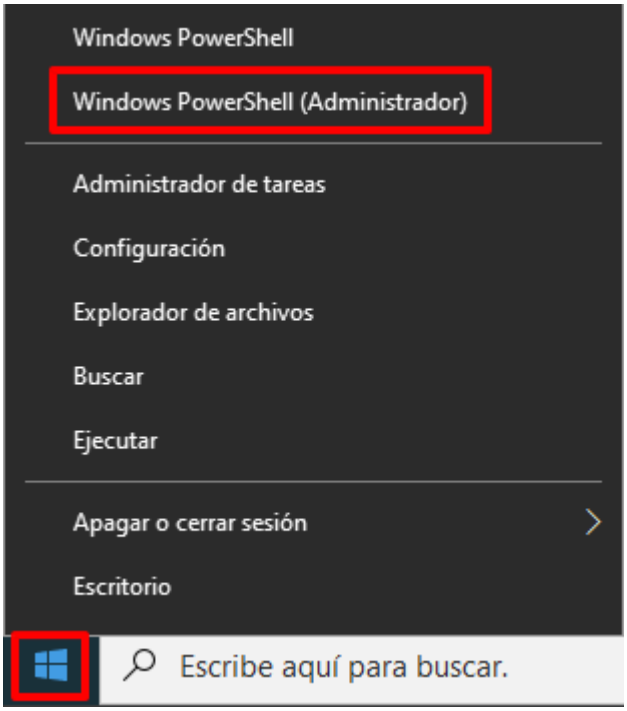
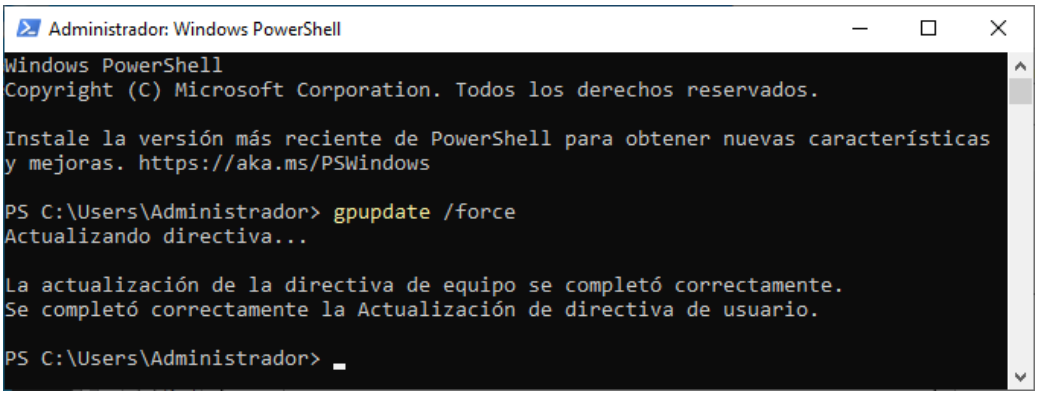
Paso	Descripción
4.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Id. de hardware”. 
5.	Seleccione el identificador que se encuentre en primer lugar y anótelo para poder introducirlo más adelante.  **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

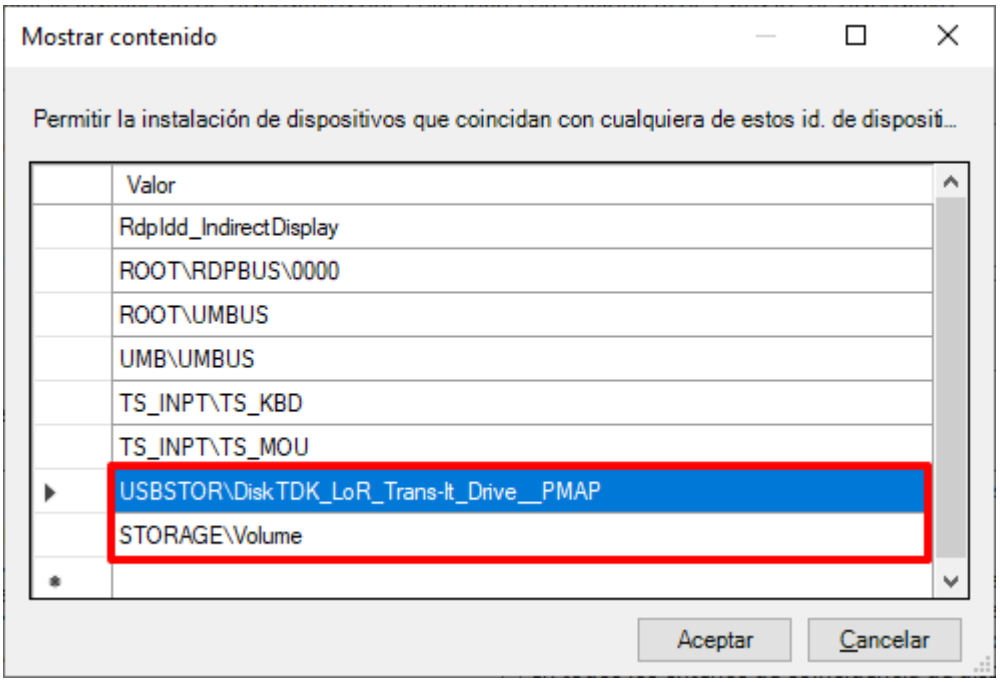
Paso	Descripción
6.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
7.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.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

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

Paso	Descripción
10.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-570A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
11.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

Paso	Descripción
12.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar…”. 
13.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la última línea para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Verifique el identificador introducido y pulse “Aceptar” para continuar.  **Nota:** No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto funcionamiento del sistema.
14.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.

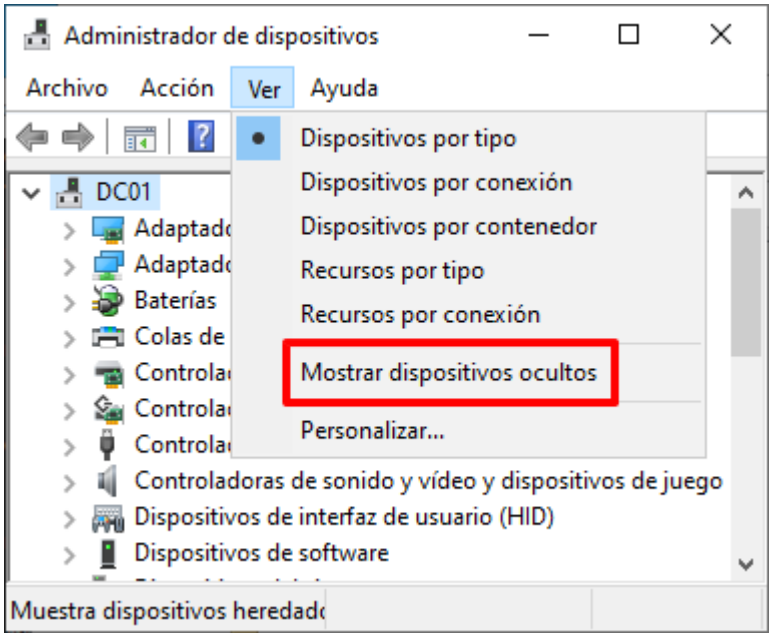
Paso	Descripción
15.	Sin cerrar el “Editor de directivas de grupo local”, continue con el siguiente paso.
16.	Sobre el equipo destino en el que se desea el uso de un dispositivo USB, haga clic derecho sobre el botón de “Inicio” y pulse sobre “PowerShell (Administrador)”. 
17.	Ejecute el comando el siguiente comando en la consola y espere a que finalice. > gpupdate /force 

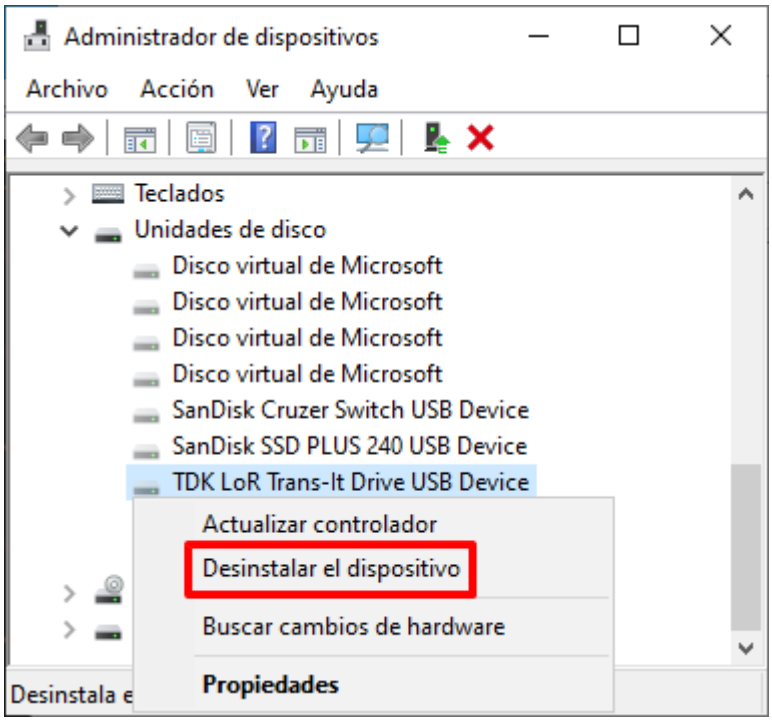
Paso	Descripción
18.	Ejecute de nuevo los pasos 3 a 17 con el objetivo de añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows. 

ANEXO C.1.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

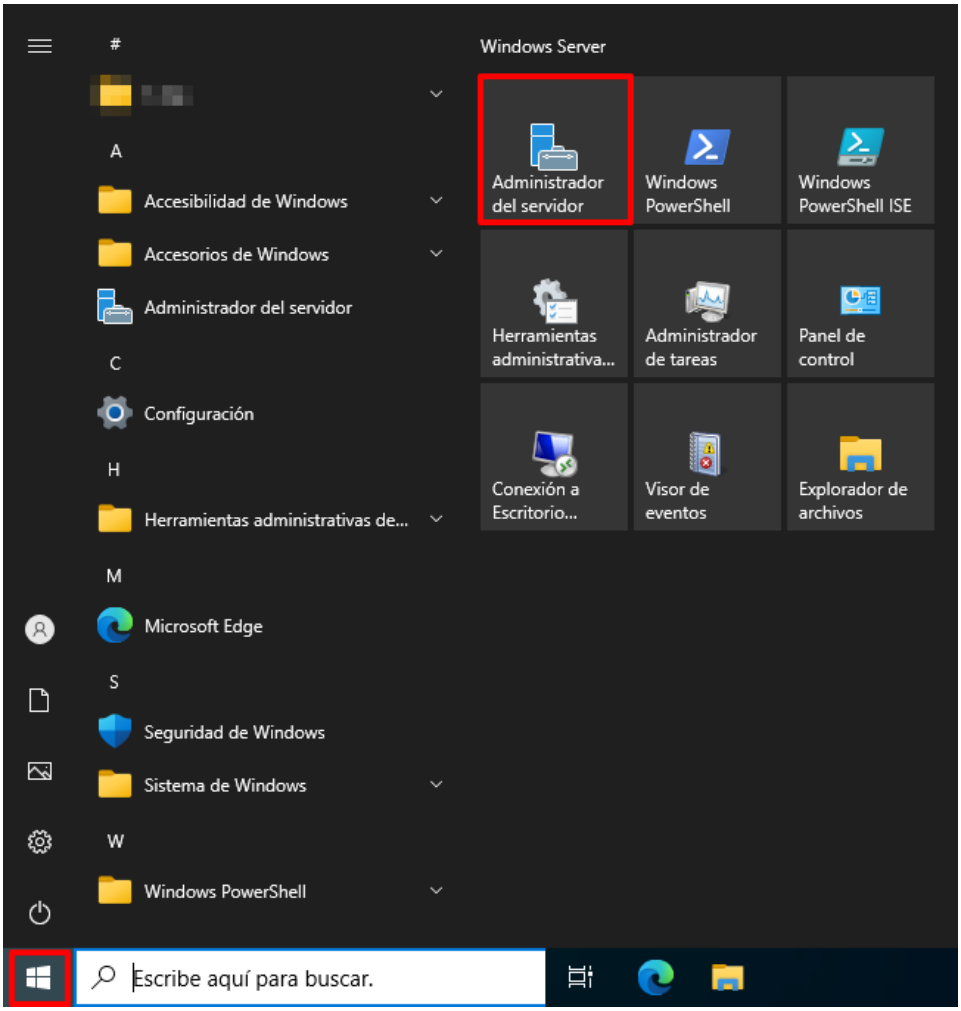
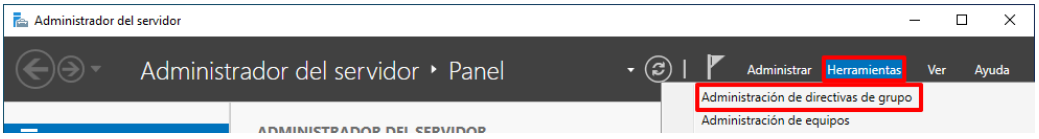
Tras la instalación del dispositivo y su posterior uso, es posible volver al estado anterior de bloqueo del uso de dispositivos USB dado de alta previamente. Para ello deberán seguir los siguientes pasos.

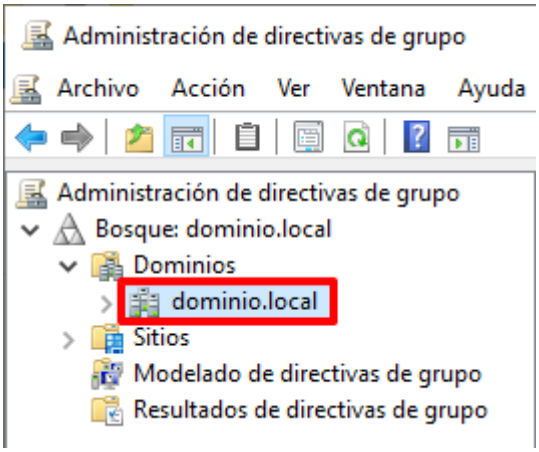
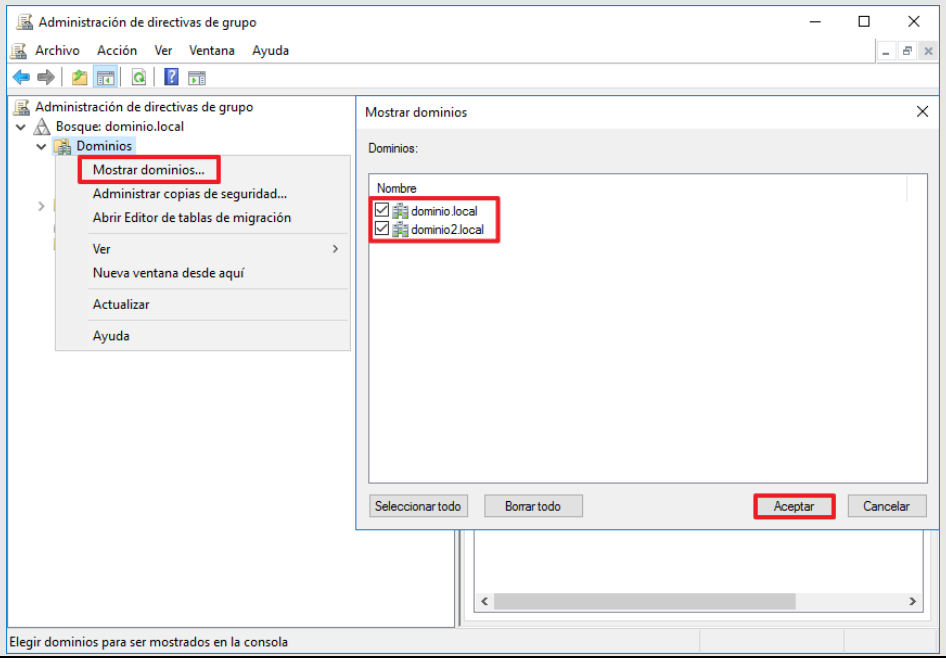
Paso	Descripción
1.	Inicie sesión en el equipo servidor donde pretende eliminar el uso de un dispositivo USB.

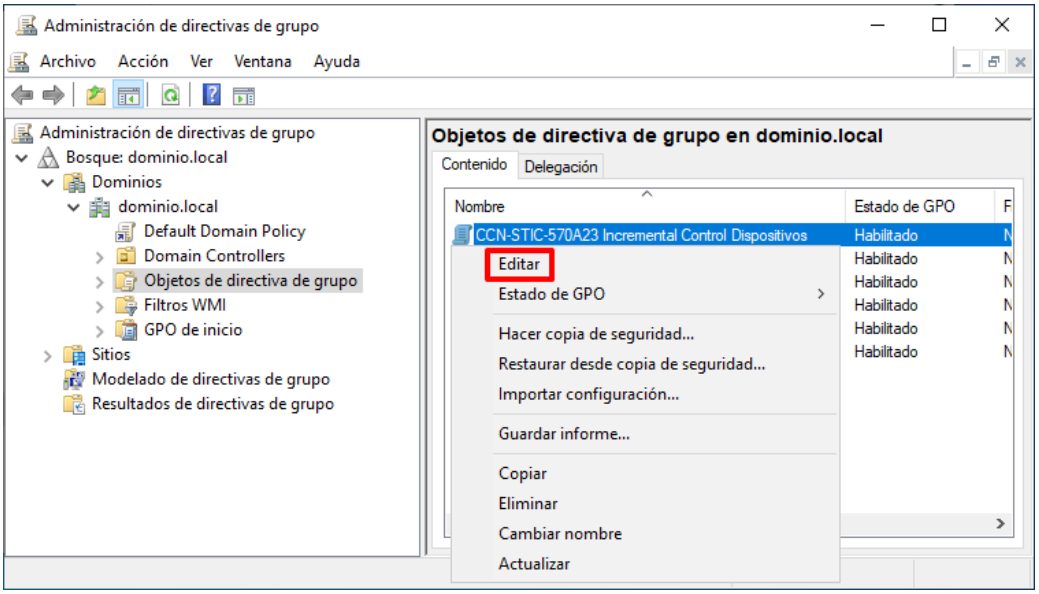
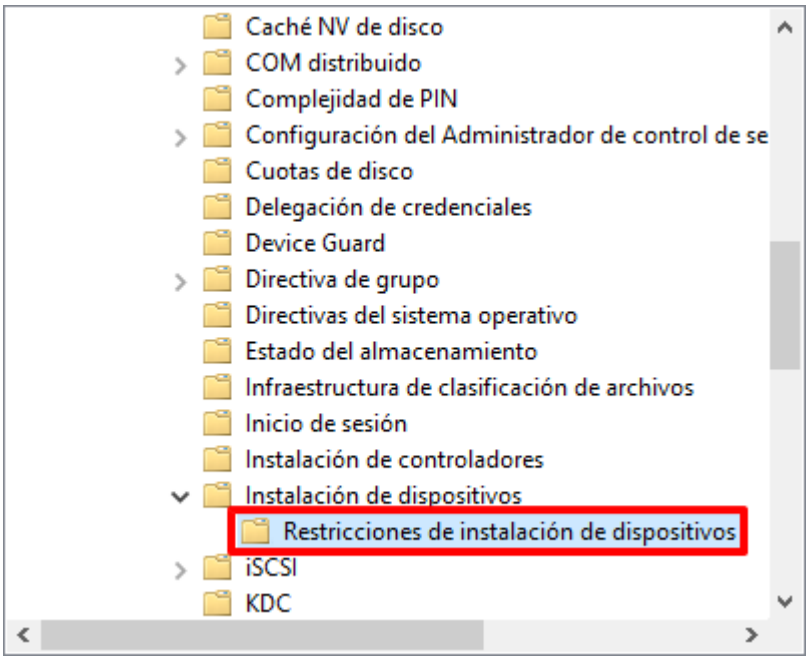
Paso	Descripción
2.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 
3.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

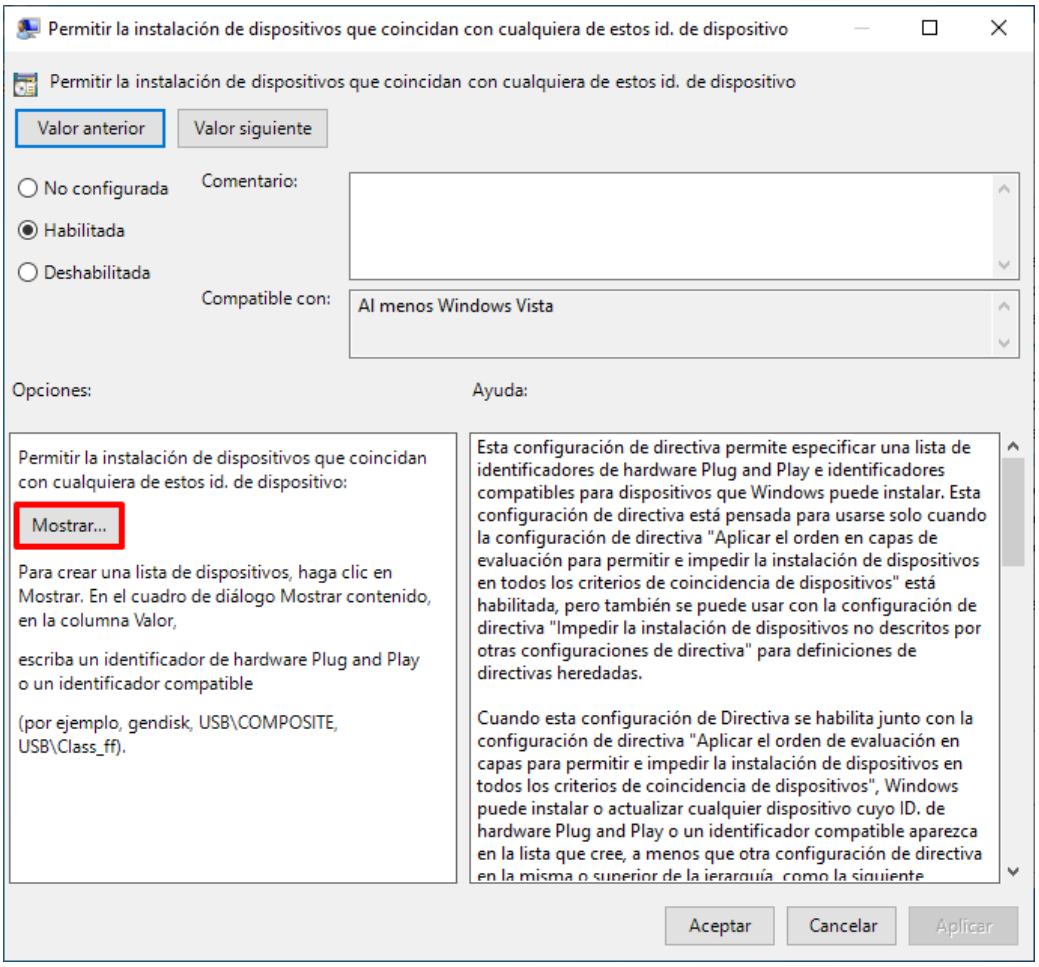
Paso	Descripción
4.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. A continuación, haga clic derecho sobre el mismo y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
5.	Pulse “Desinstalar” ante la advertencia emergente.  **Nota:** Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

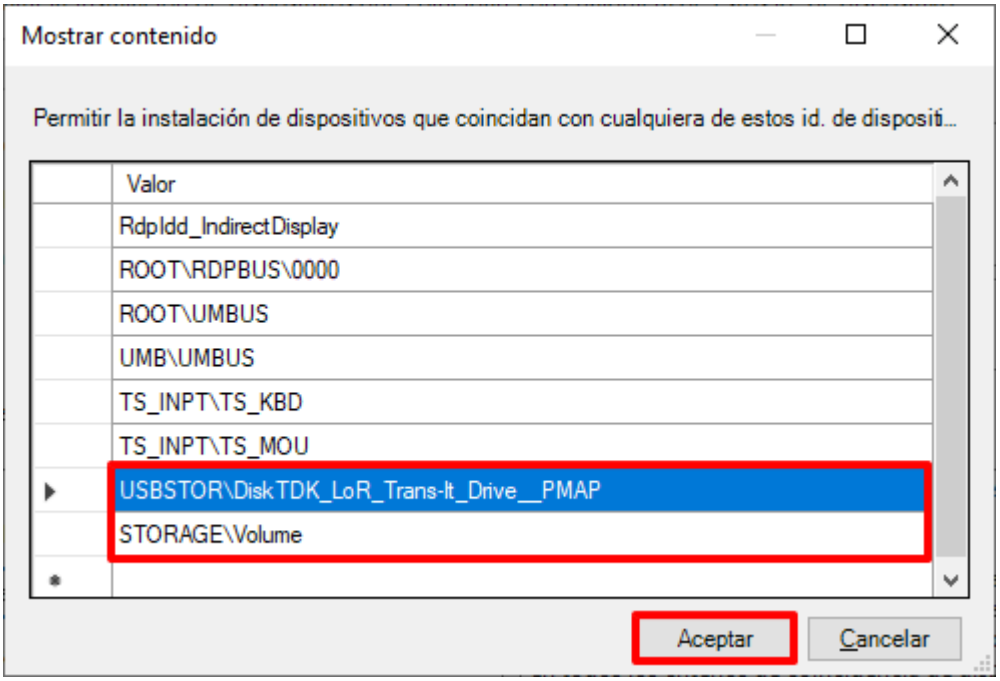
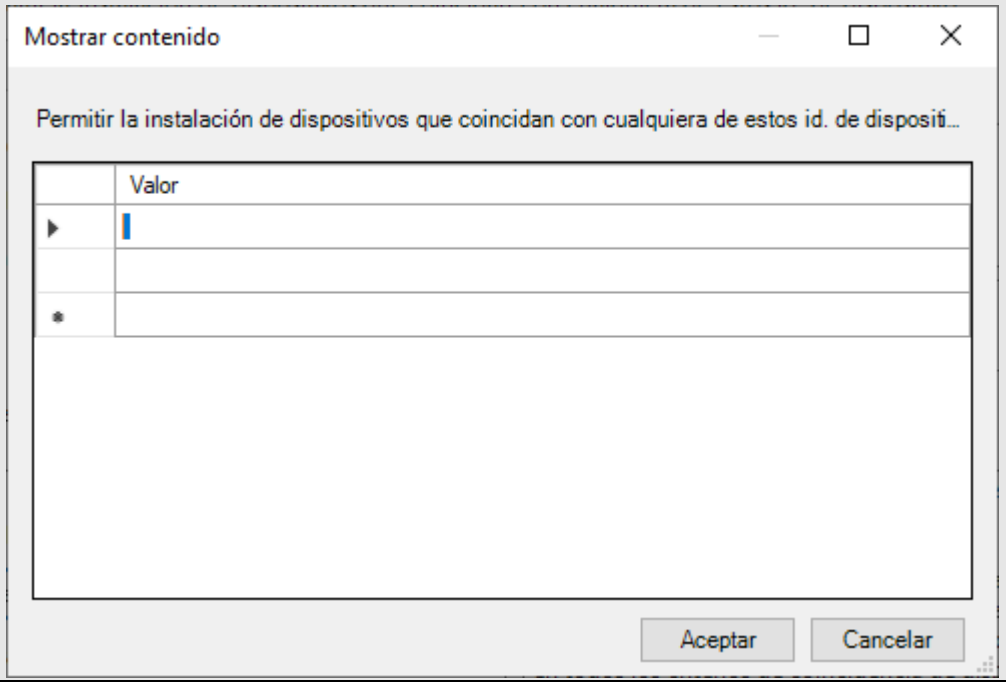
Los siguientes pasos solo serán necesarios en caso de haber hecho uso de la instalación mediante el uso de identificadores únicos de USB.

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

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

Paso	Descripción
5.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-570A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
6.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

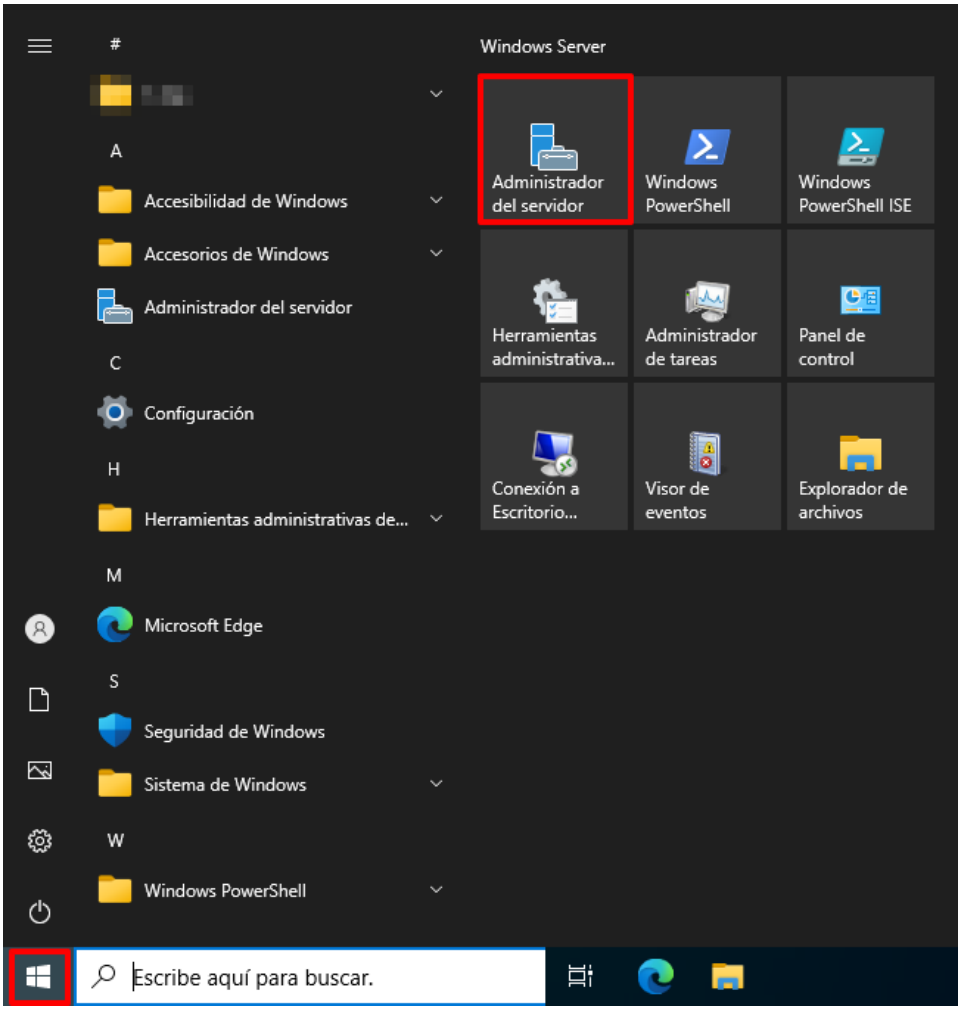
Paso	Descripción
7.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar…”. 

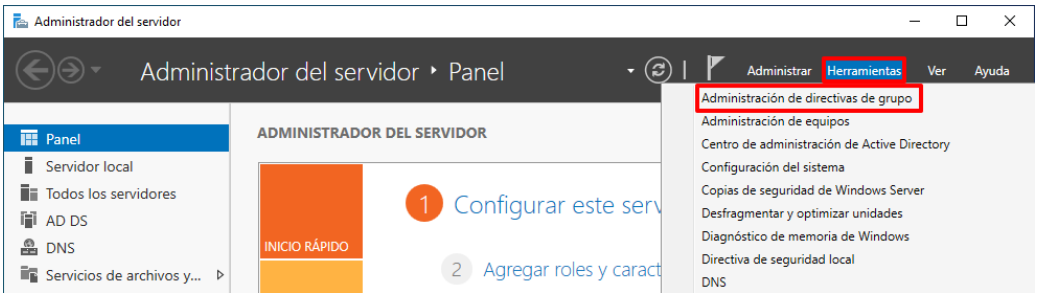
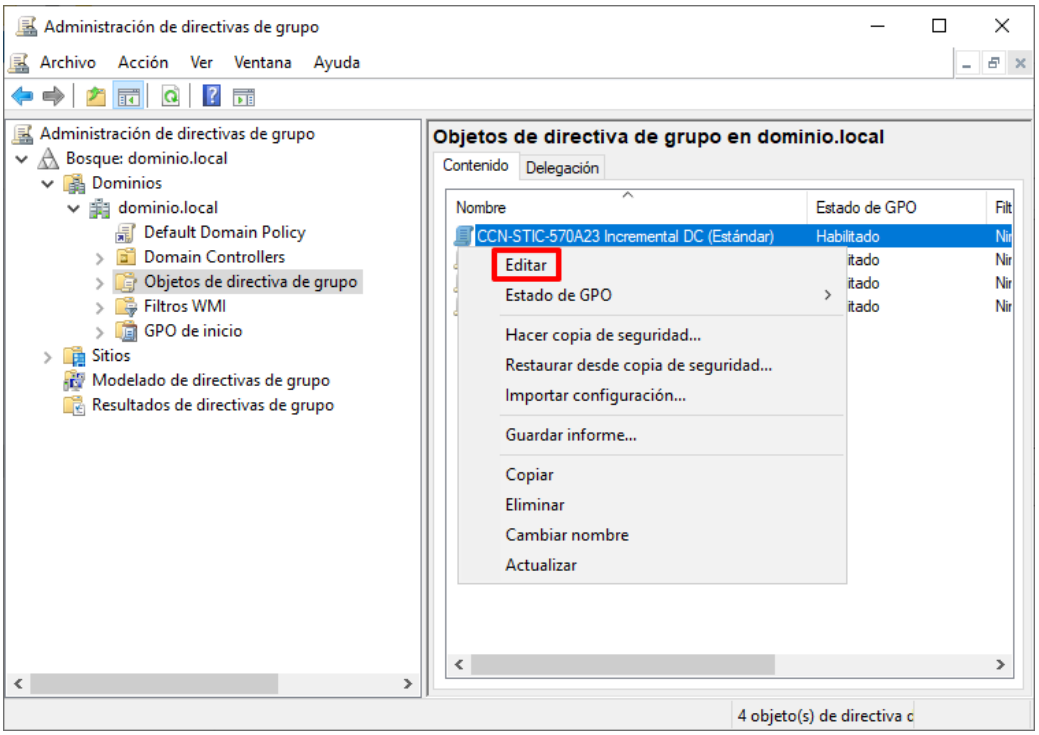
Paso	Descripción
8.	En la ventana emergente “Mostrar contenido” elimine los identificadores correspondientes a los dispositivos sobre los cuales ya no se desea su uso. Pulse “Aceptar” para continuar.  **Nota:** No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto funcionamiento del sistema. En caso de eliminar todas las líneas debe dejarse al menos una línea con un espacio en blanco para poder cerrar la configuración de la directiva. En caso contrario se mostrará un error. 

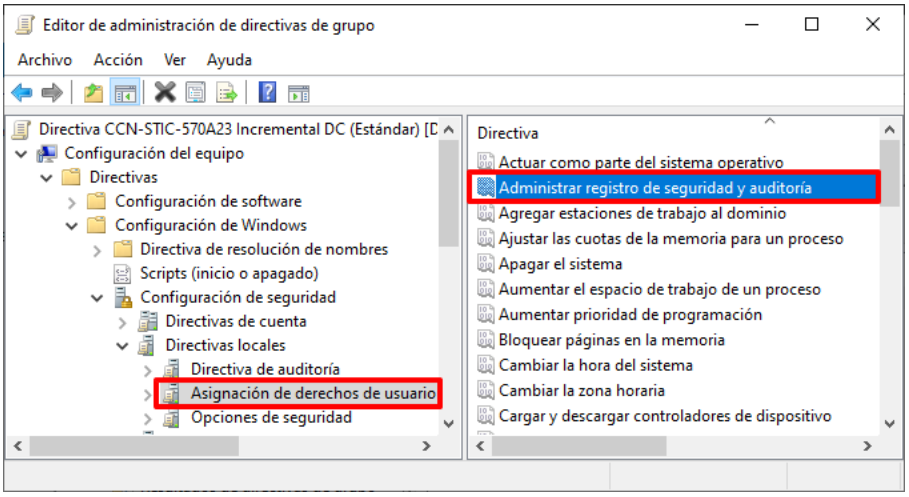
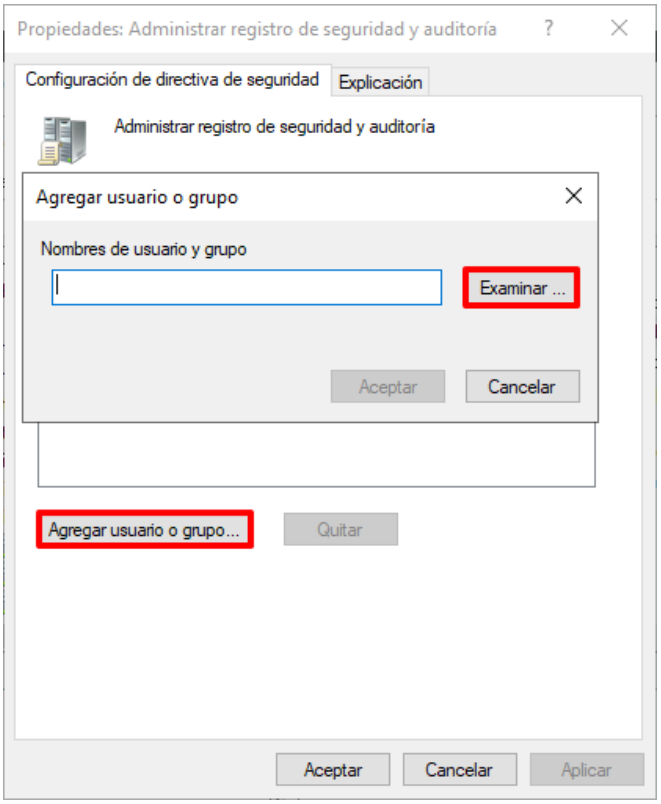
ANEXO C.2. SEGREGACIÓN DE FUNCIONES Y TAREAS (PRIVILEGIOS DE AUDITORÍA)

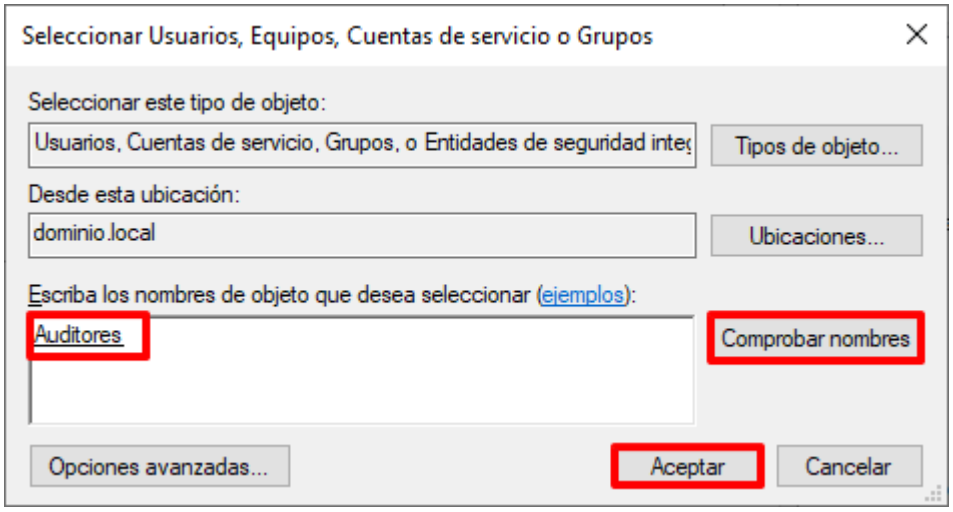
Los siguientes pasos definen las labores para permitir que solo aquellas cuentas deseadas sean capaces de generar auditorías en el sistema operativo Windows Server.

Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. A pesar de esto, las configuraciones y pasos descritos a continuación son válidos para los perfiles "Uso Oficial" y "Materias Clasificadas".

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

Paso	Descripción
3.	En la consola “Administrador del servidor”, en la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
4.	Seleccione el objeto GPO “CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

Paso	Descripción
5.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"**. A continuación, haga doble clic sobre la directiva **"Administrar registro de seguridad y auditoría"**. 
6.	En la ventana emergente, pulse sobre "Agregar usuario o grupo…". Pulse a continuación sobre "Examinar…". 

Paso	Descripción
7.	Introduzca el nombre del grupo “Auditores”, haga uso del botón “Comprobar nombres” para completar la información y pulse “Aceptar”.  **Nota:** El grupo “Auditores” habrá sido generado de forma automatizada si ha ejecutado previamente el script “CCN-STIC-570A23 Controlador de Dominio – Segregación de roles.bat”. En caso contrario puede ejecutar este script o bien crear el grupo de forma manual.
8.	Realice los mismos pasos (4 a 7), sobre el objeto GPO “CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO])”.

ANEXO C.3. PROTECCIÓN FRENTE A CÓDIGO DAÑINO (CONFIGURACIÓN DE LA HERRAMIENTA DE DETECCIÓN DE CÓDIGO DAÑINO)

El paso a paso definido a continuación tiene como objetivo realizar una configuración avanzada de la herramienta de código dañino configurada durante el punto “ANEXO B.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO”. Las configuraciones definidas bajo el presente apartado son las siguientes:

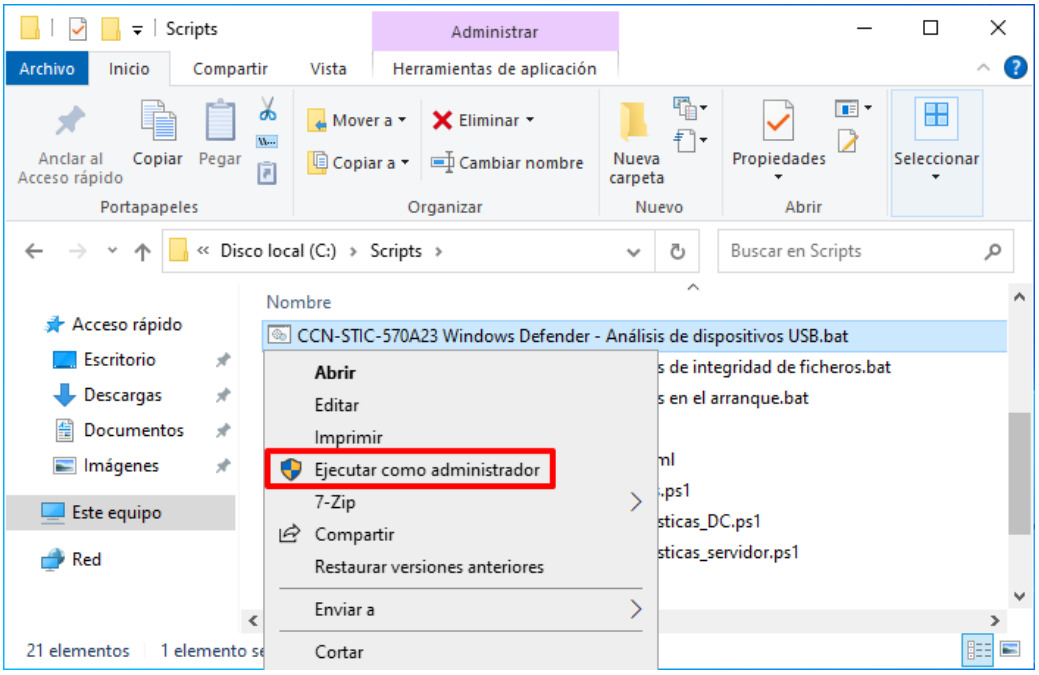
a) Análisis de dispositivos de almacenamiento extraíble cuando estos se conectan al equipo.

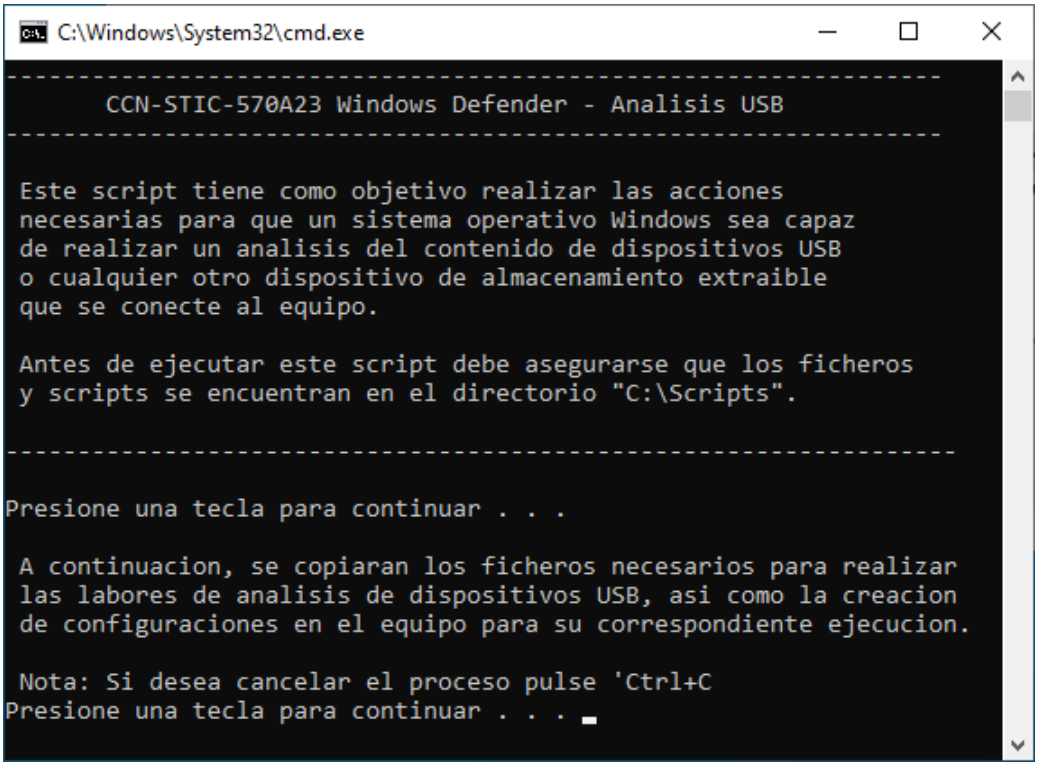
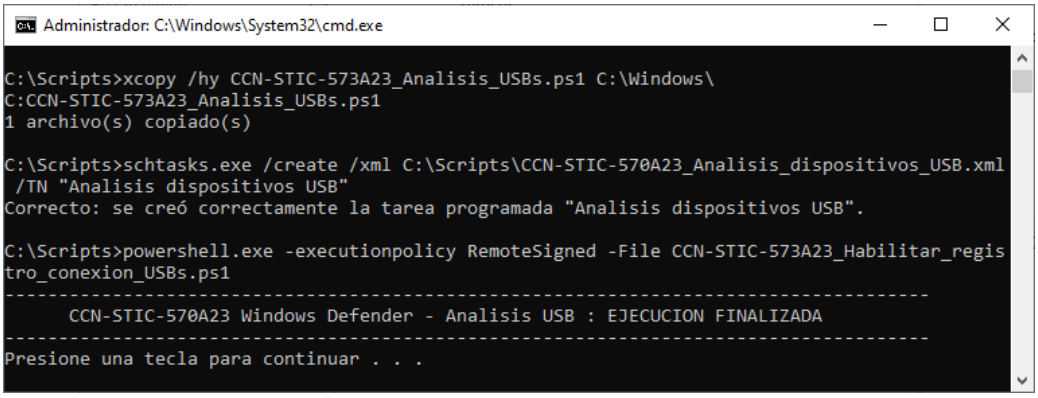
b) Análisis del sistema operativo en el arranque del sistema.

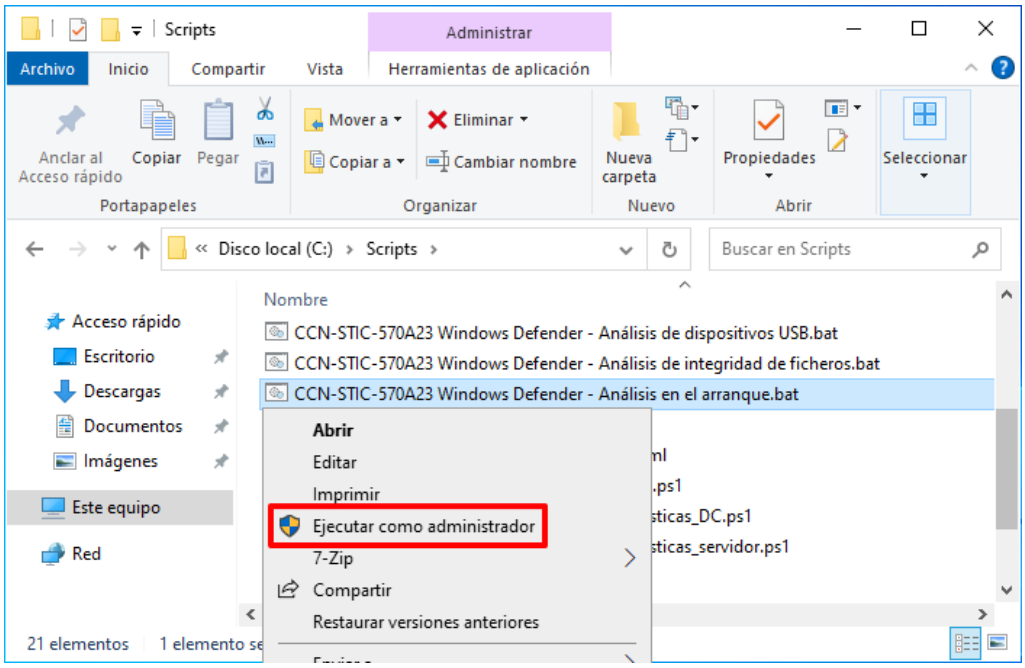
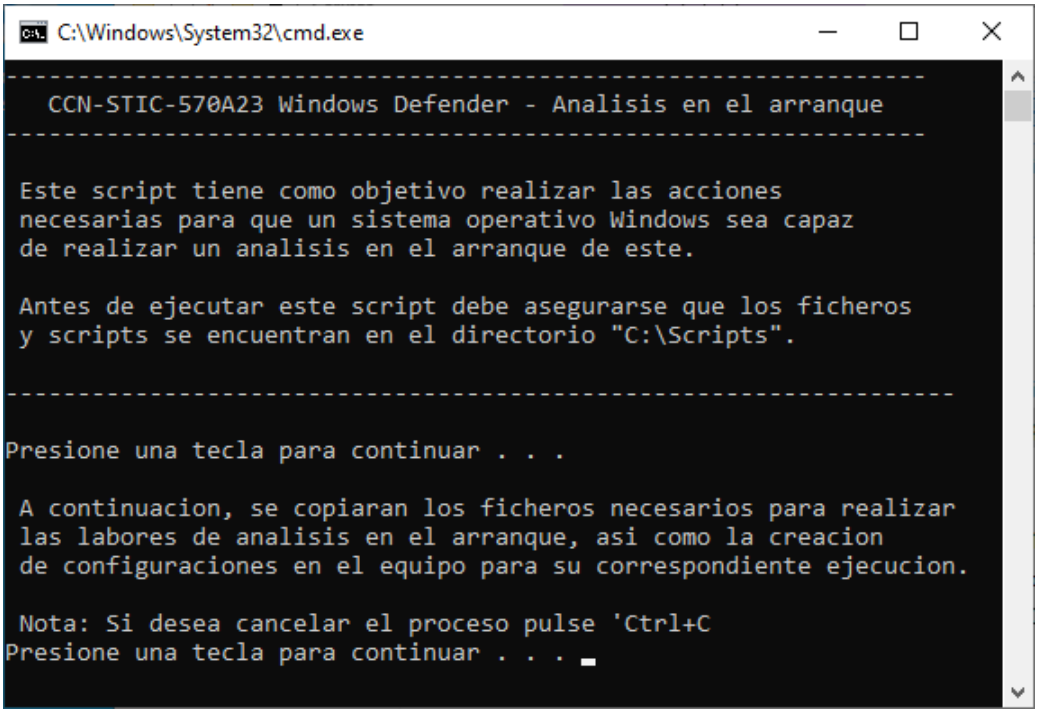
Nota: No se considera de aplicación las configuraciones del presente apartado si no se han aplicado el resto de configuraciones de esta herramienta según el punto indicado con anterioridad.

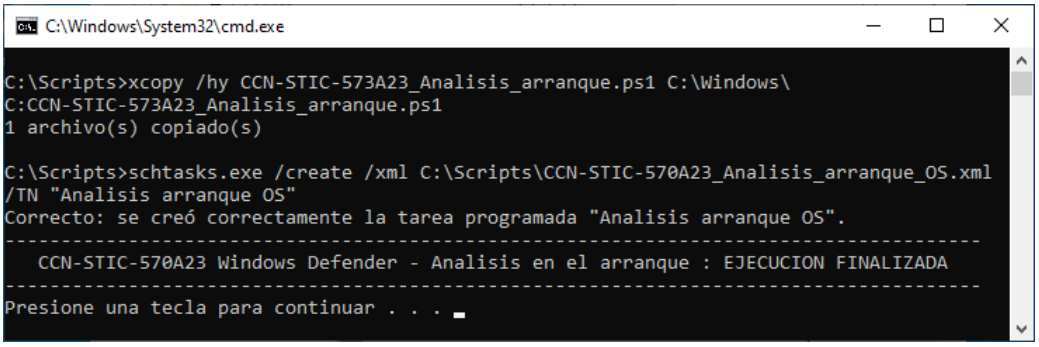
Deberá decidir si implementar toda o parte de la configuración según se expone en el presente paso a paso.

Tenga en consideración que estas configuraciones pueden afectar al rendimiento del sistema operativo.

Paso	Descripción
1.	Inicie sesión en un servidor perteneciente al dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-570A23 Windows Defender – Análisis de dispositivos USB.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
3.	Pulse cualquier tecla para continuar.

Paso	Descripción
4.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 
5.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
6.	Con esto habrá configurado el equipo para que se realice un análisis de los dispositivos de almacenamiento extraíble cada vez que se conecten al equipo.

Paso	Descripción
7.	De nuevo, en el directorio “C:\Scripts” haga clic derecho sobre el fichero “CCN-STIC-570A23 Windows Defender – Análisis en el arranque.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
8.	Pulse una tecla para continuar.
9.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 

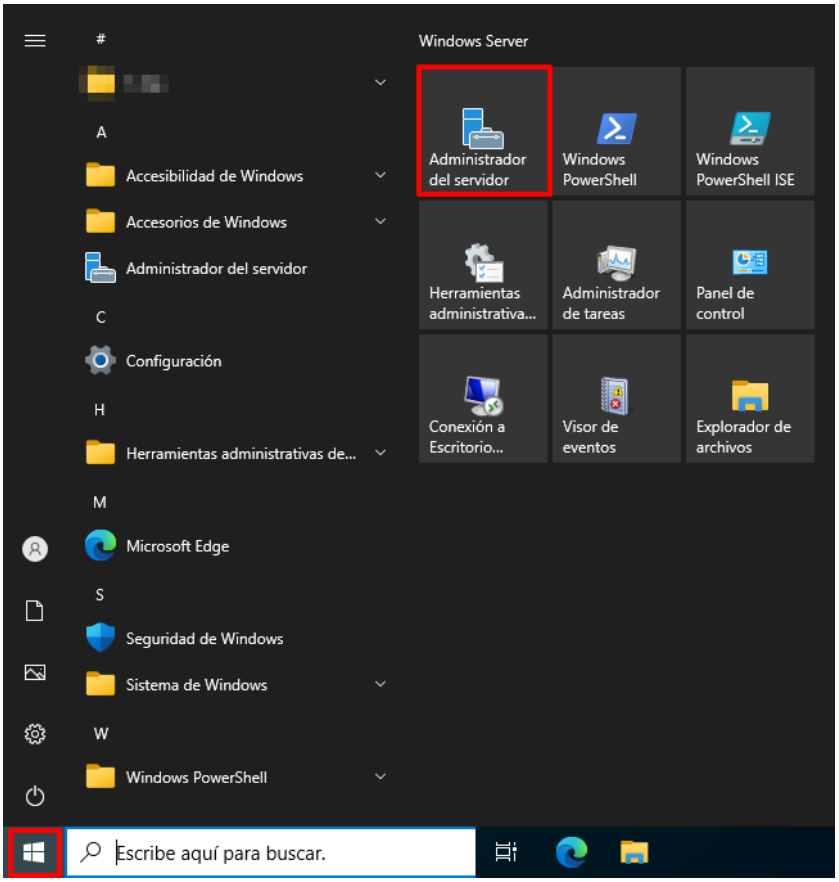
Paso	Descripción
10.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
11.	Con esto habrá configurado el equipo para que se realice un análisis nada más se inicie el sistema operativo, así como los sectores de arranque de este.

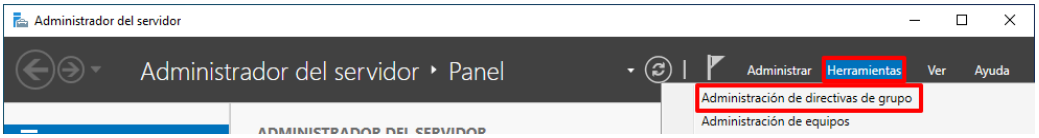
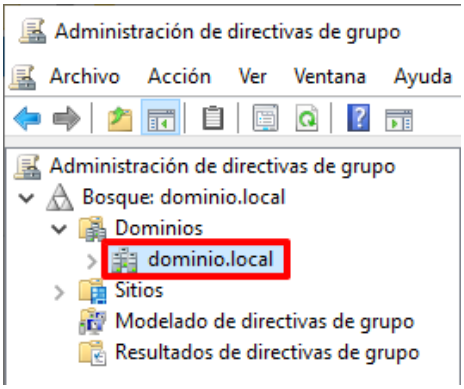
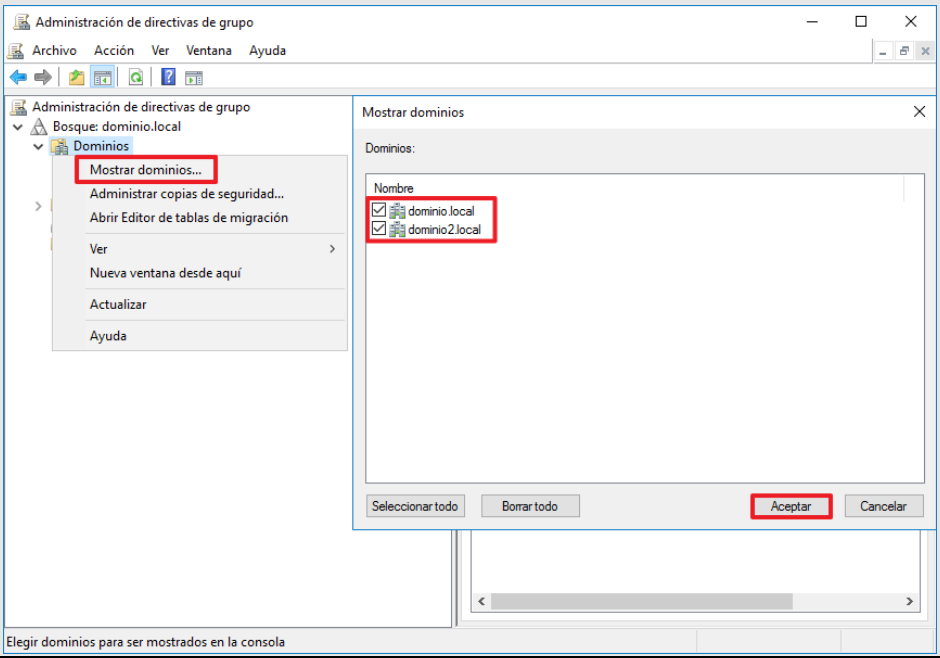
ANEXO D. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

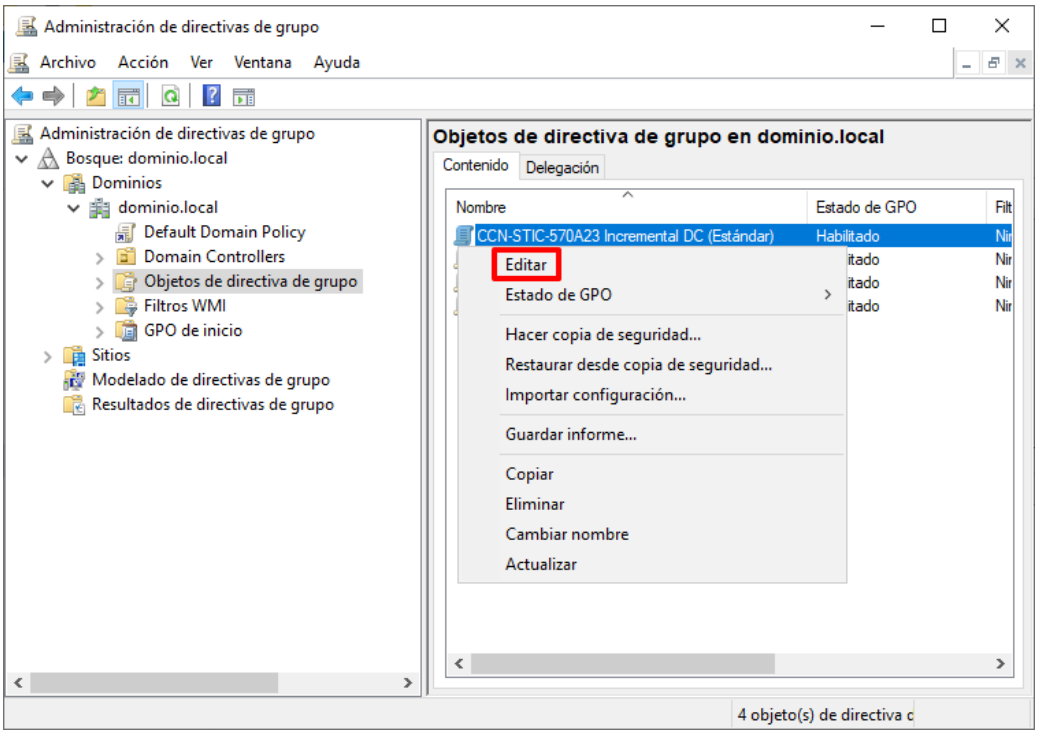
ANEXO D.1. INFORMACIÓN DE OBLIGACIONES

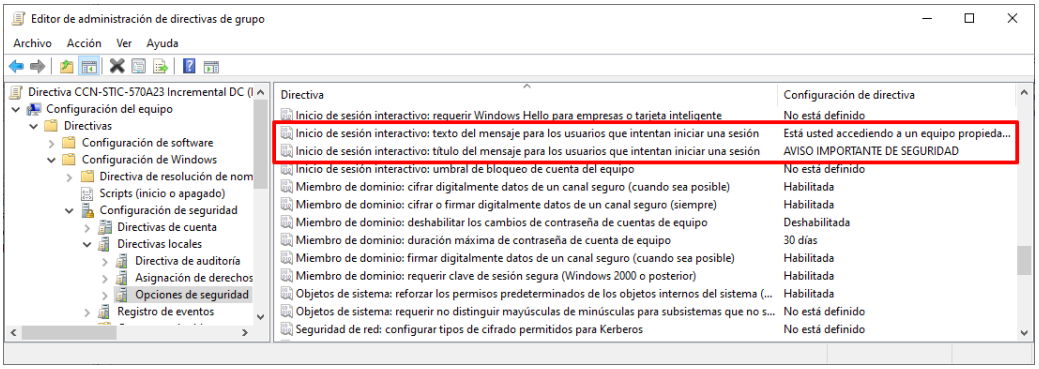
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a los mecanismos de autenticación, es necesario informar al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso al sistema.

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

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

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

Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique los dos (2) siguientes objetos GPO en función de donde desee adecuar los parámetros información sobre derechos y obligaciones de los usuarios: – CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) – CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre “Editar”.  **Nota:** En este ejemplo se hace uso del objeto GPO “CCN-STIC-570A23 Incremental DC (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.

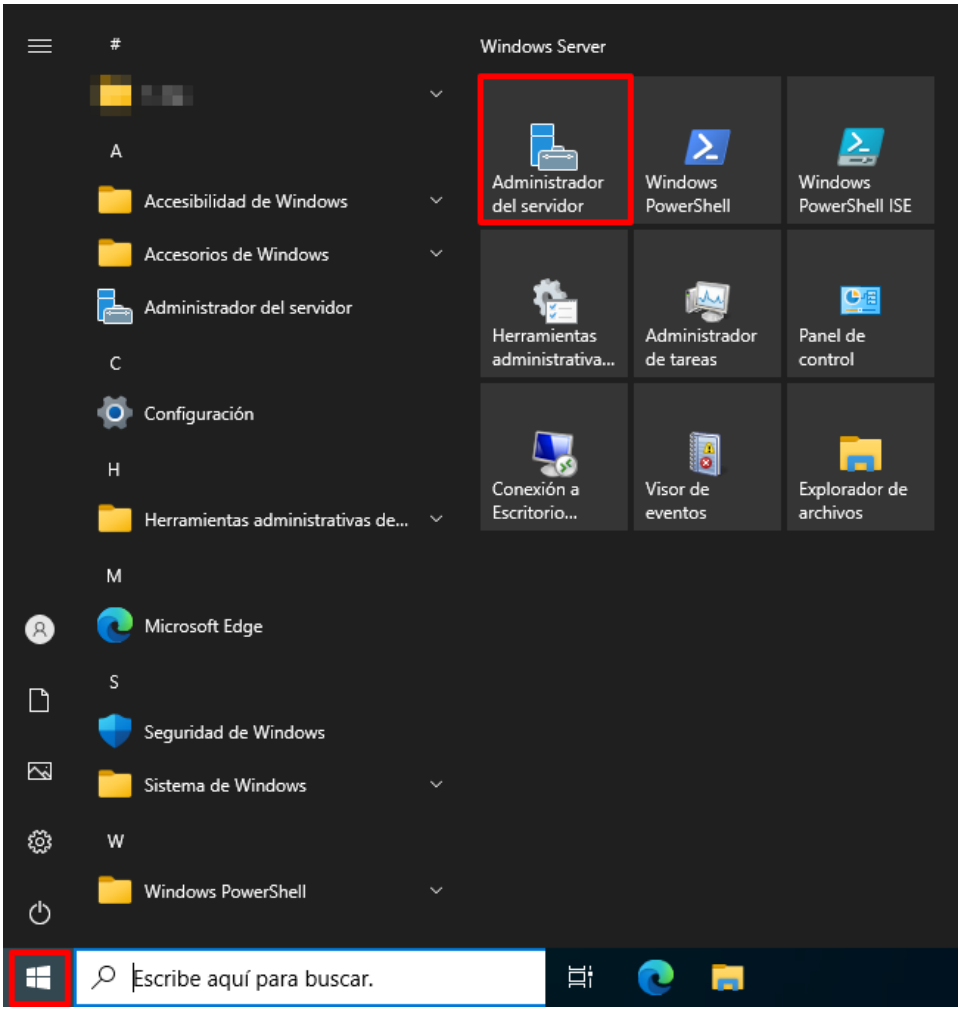
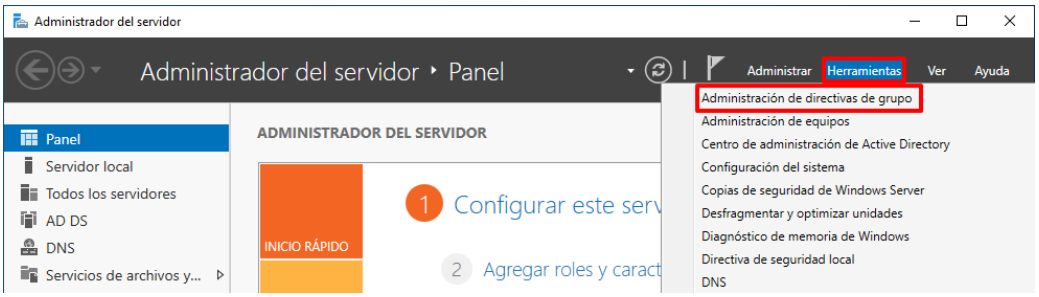
Paso	Descripción
8.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión – Inicio de sesión interactivo: título del mensaje para los usuarios que intentan inicia una sesión 
9.	La configuración establecida expone un mensaje tipo, el cual trata de cubrir los aspectos más generales de cara al uso de los sistemas de información. Deberá adaptar este apartado acorde a las necesidades de su organización tomando en consideración que siempre deberá informar al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso al sistema.

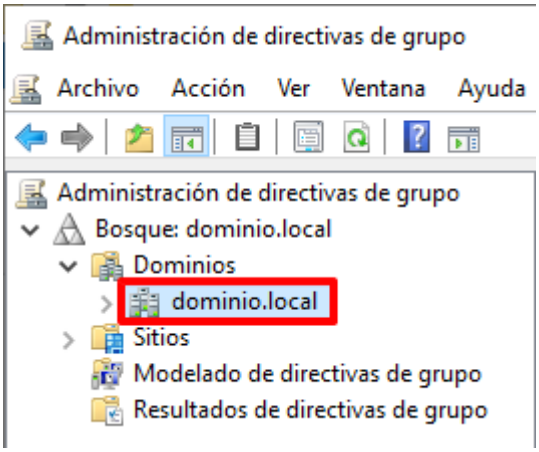
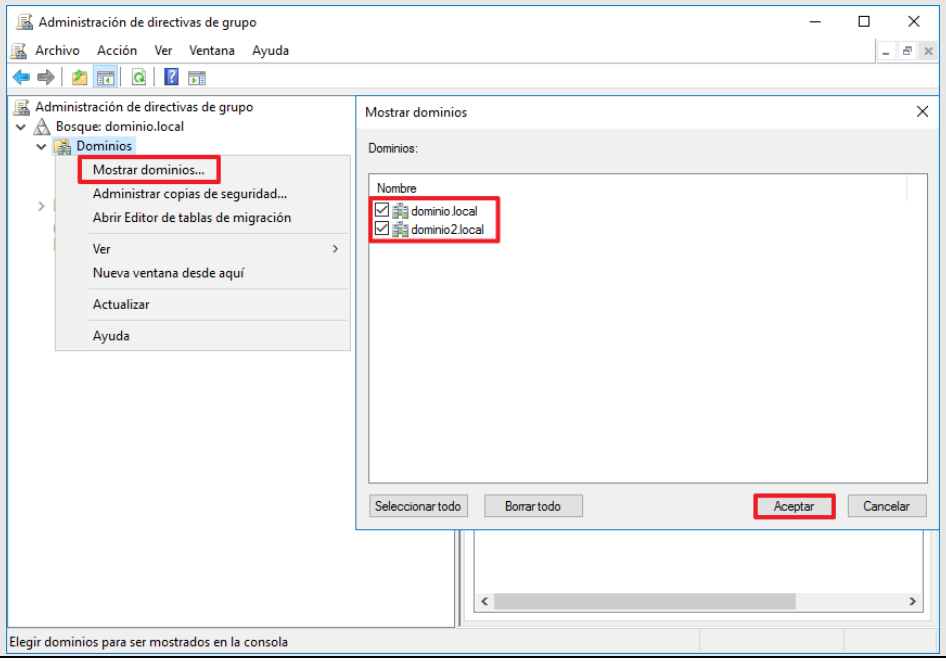
ANEXO D.2. RETENCIÓN DE REGISTROS DE ACTIVIDAD

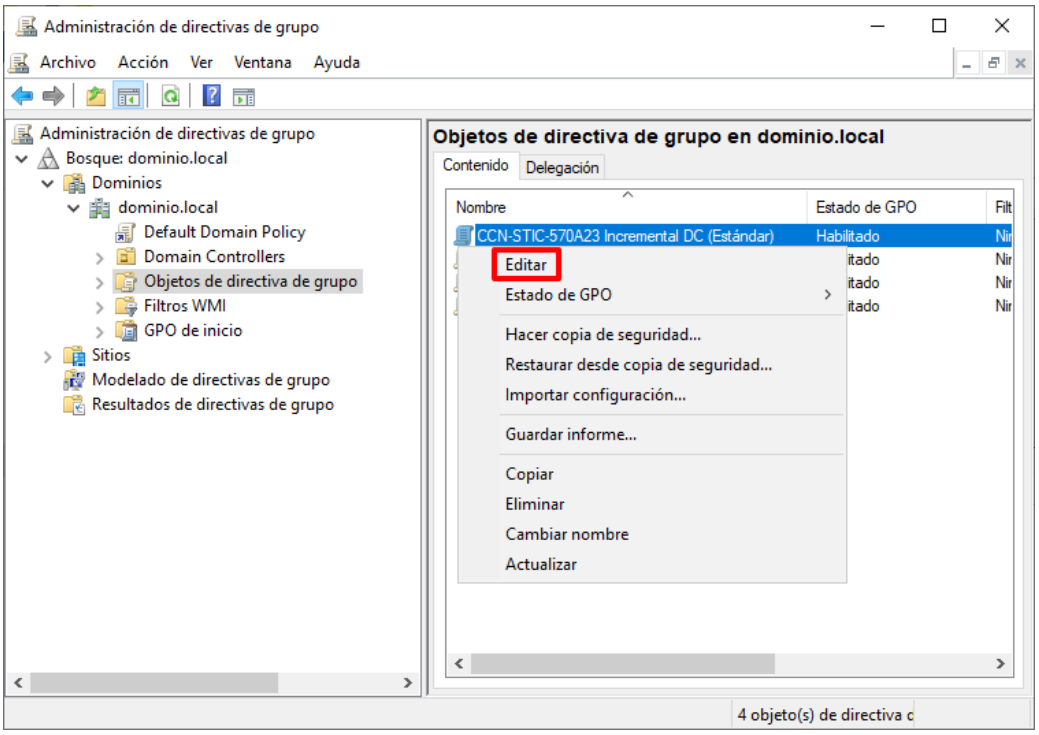
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a los registros de actividad y conforme a lo descrito en su refuerzo número tres (3), es necesario realizar una retención de los eventos auditados antes de que estos sean eliminados.

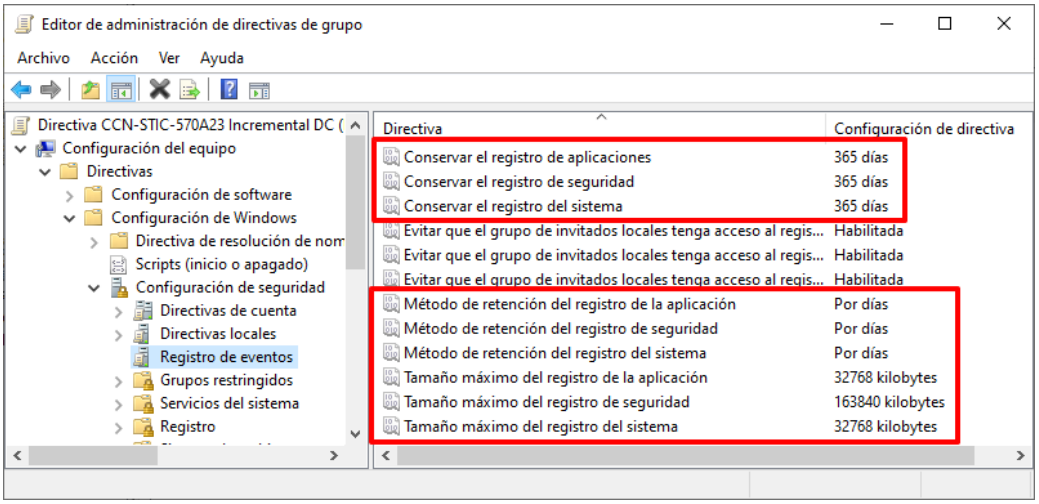
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a modificar y/o adaptar la configuración establecida en los apartados anteriores del presente documento.

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

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

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

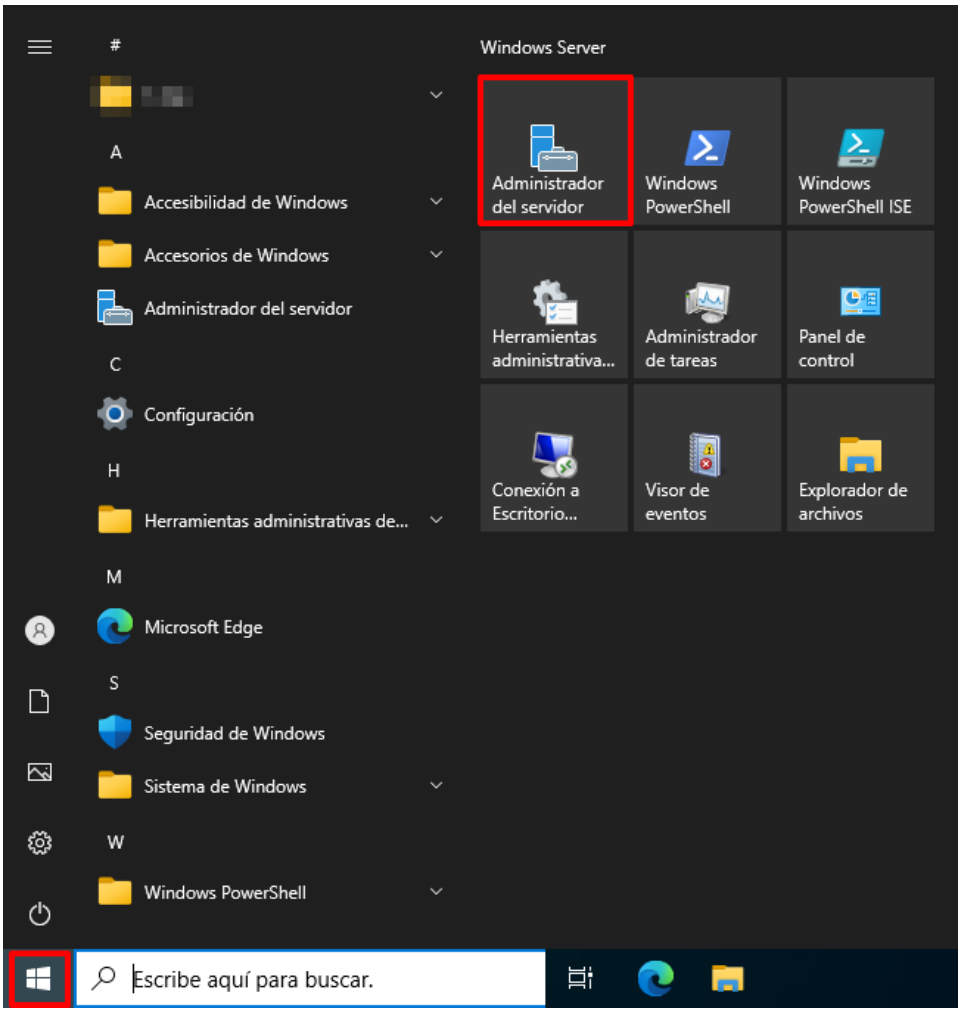
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique los dos (2) siguientes objetos GPO en función de donde desee adecuar los parámetros de retención: – CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) – CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre “Editar”.  **Nota:** En este ejemplo se hace uso del objeto GPO “CCN-STIC-570A23 Incremental DC (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”**.

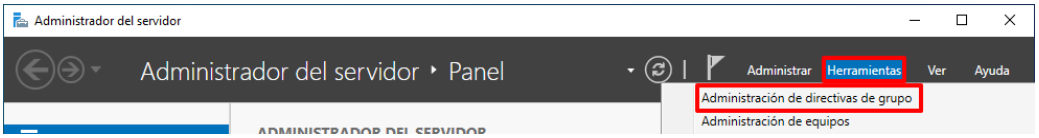
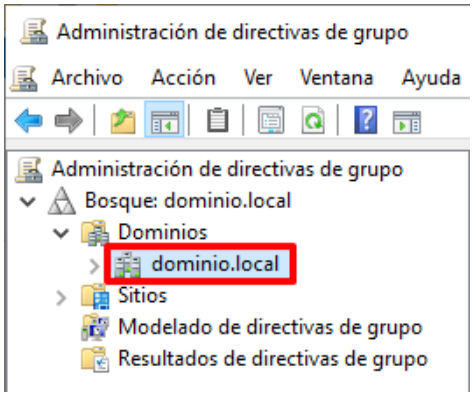
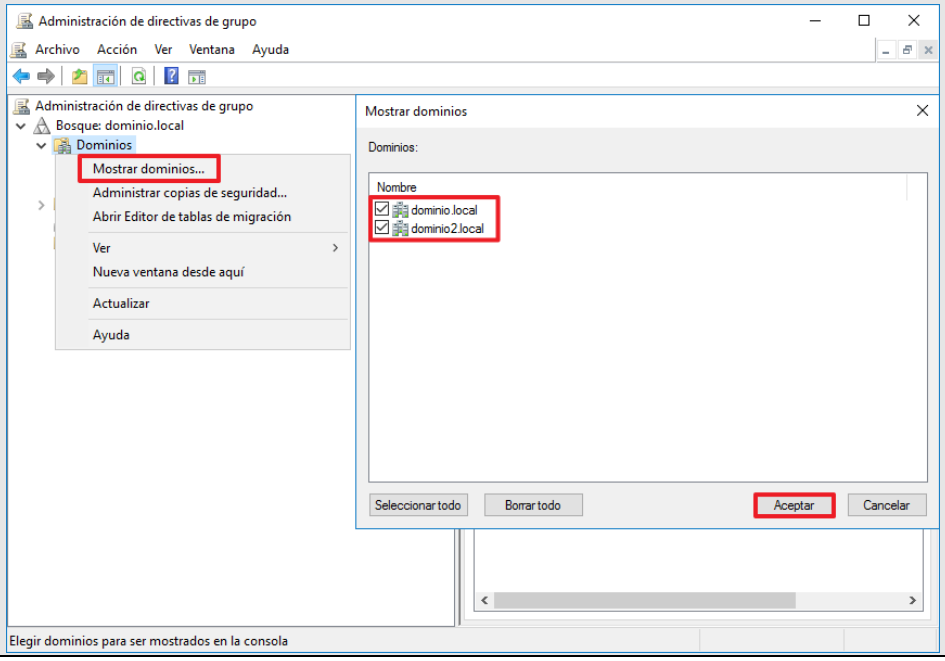
Paso	Descripción
8.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Conservar el registro de aplicaciones – Conservar el registro de seguridad – Conservar el registro del sistema – Método de retención del registro de la aplicación – Método de retención del registro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

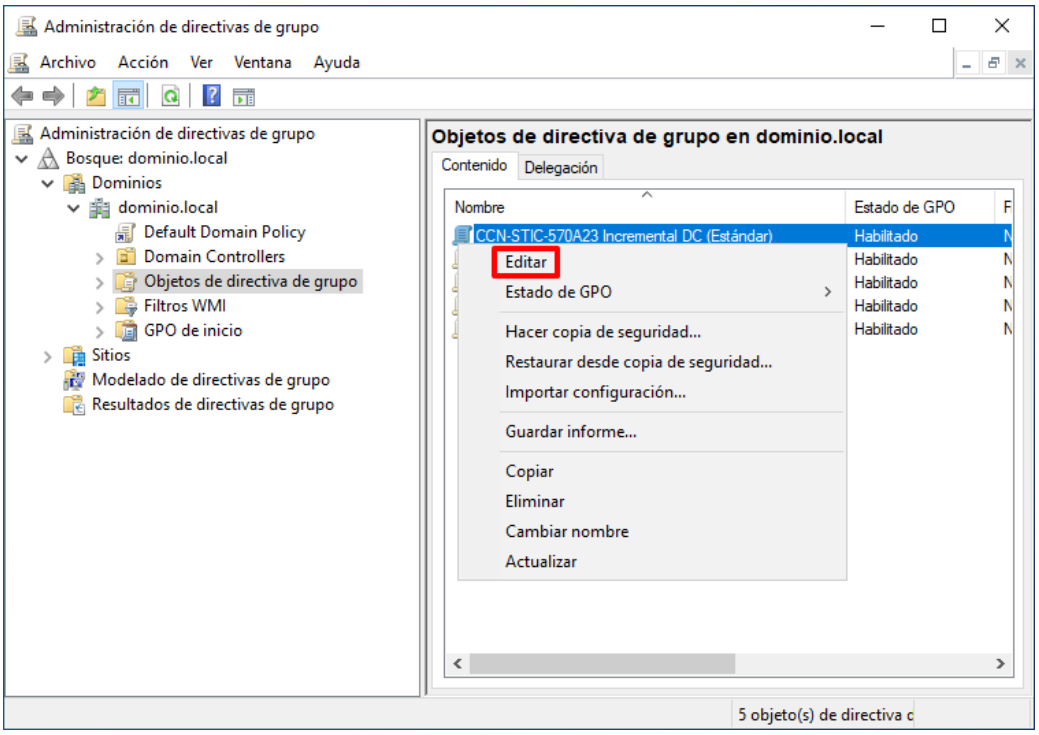
ANEXO D.3. PRIVILEGIOS

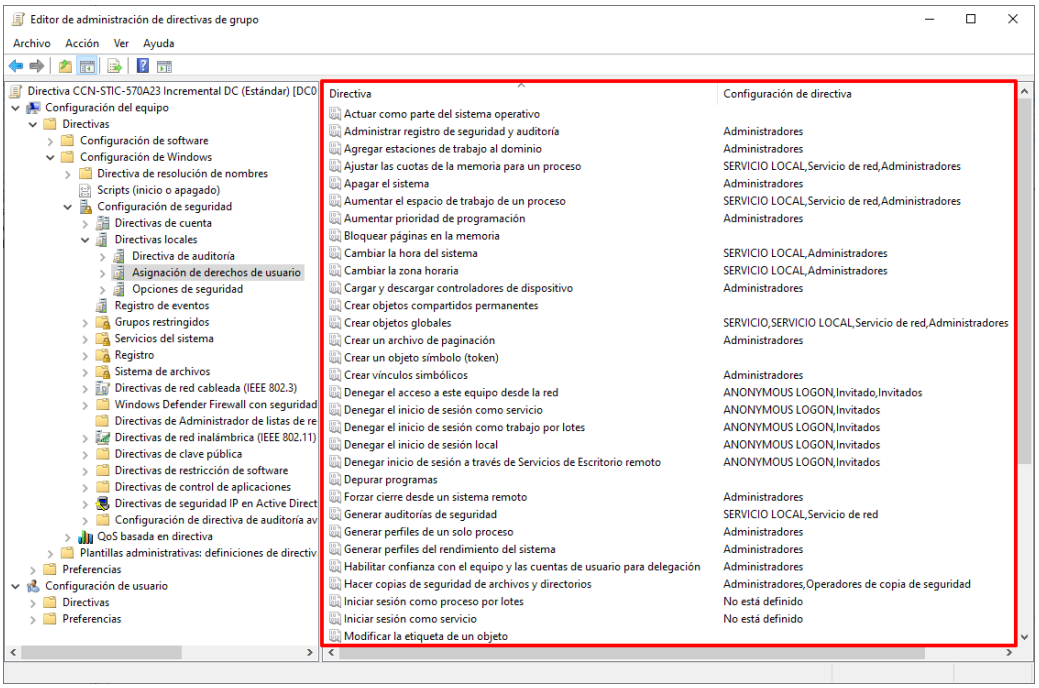
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a la identificación y el acceso a los sistemas de información, es necesario establecer los privilegios adecuados en función de las necesidades.

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

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

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

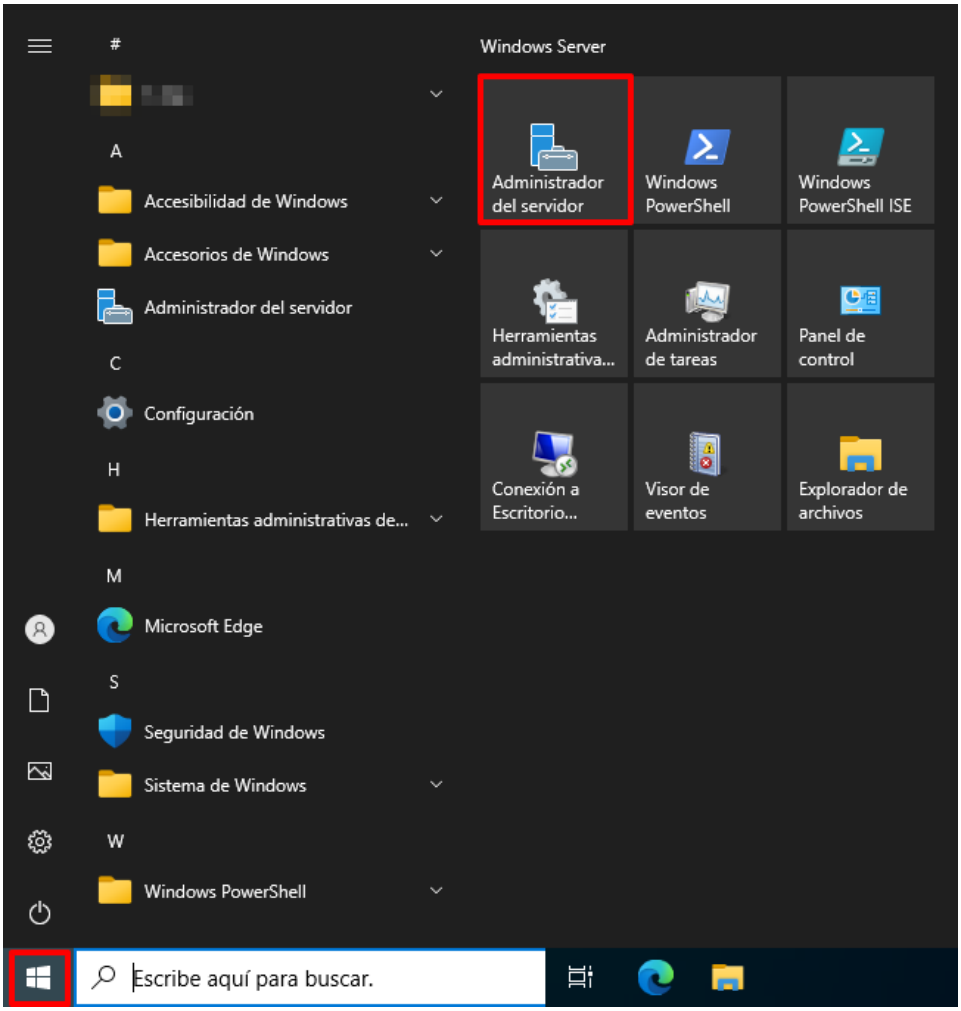
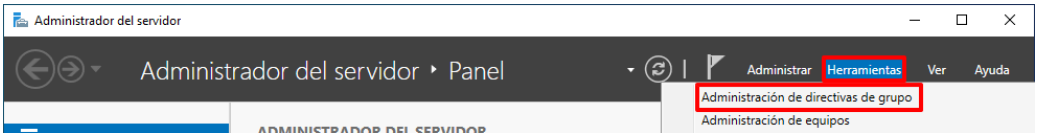
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique los dos (2) siguientes objetos GPO en función de donde desee adecuar los parámetros de privilegios: – CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) – CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre “Editar”.  **Nota:** En este ejemplo se hace uso del objeto GPO “CCN-STIC-570A23 Incremental DC (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”**.

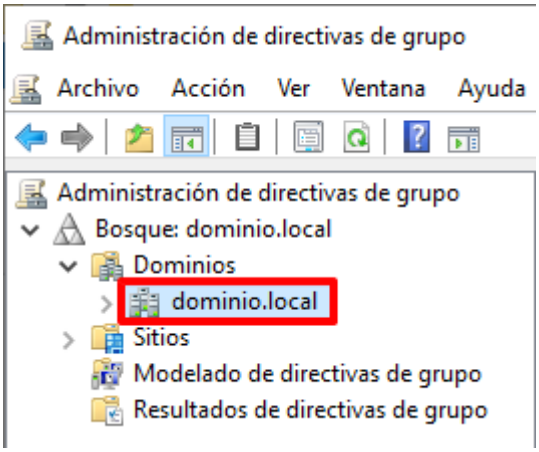
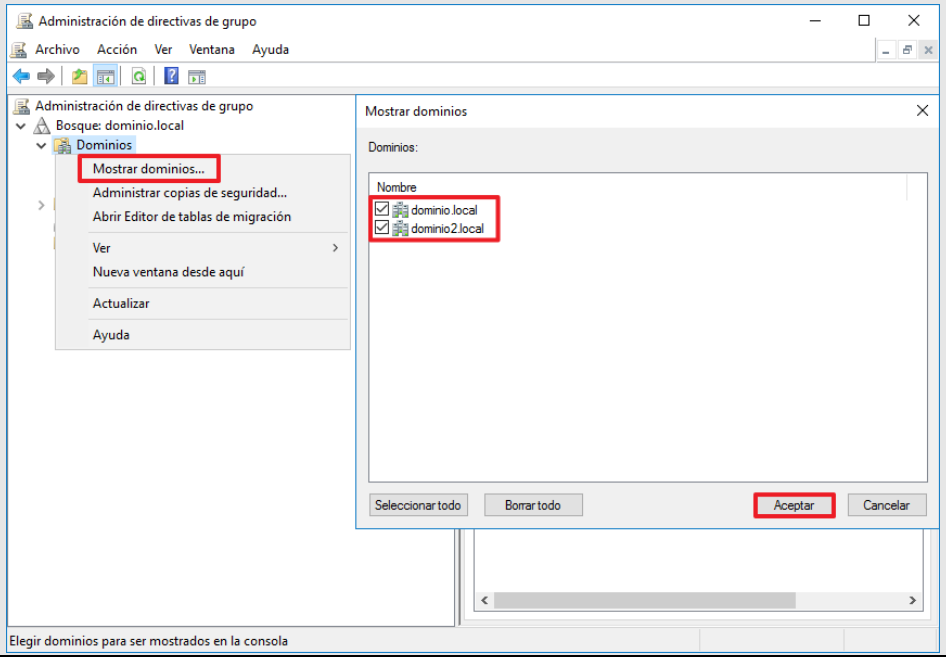
Paso	Descripción
8.	En el panel derecho evalúe todas las directivas de privilegios y edítelas a continuación. Tenga especial consideración con las siguientes directivas orientadas a los tipos de inicio de sesión, sobre todo cuando se realicen procesos automatizados en los sistemas de información o en los servidores Windows Server que ejercen el rol de servidor miembro del dominio. – Iniciar sesión como servicio – Iniciar sesión como proceso por lotes – Permitir el inicio de sesión local – Permitir inicio de sesión a través de Servicios de Escritorio remoto 
9.	La configuración establecida trata de restringir todo lo posible los privilegios de los usuarios, pero manteniendo la usabilidad dentro de los sistemas, poniendo especial atención sobre los sistemas operativos Windows Server que ejercen el rol de Domain Controller.

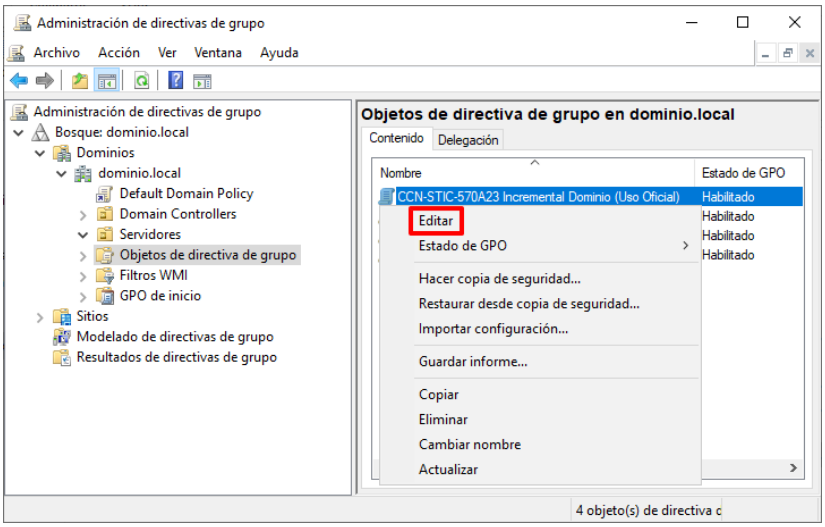
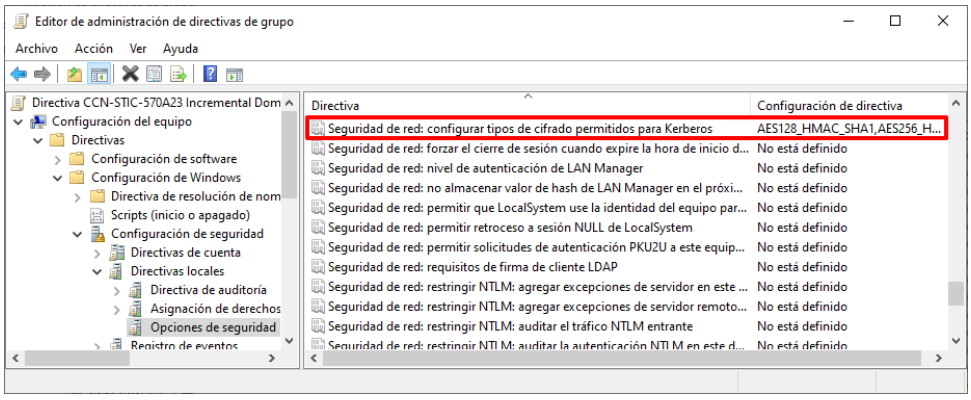
ANEXO D.4. CIFRADOS PERMITIDOS PARA KERBEROS

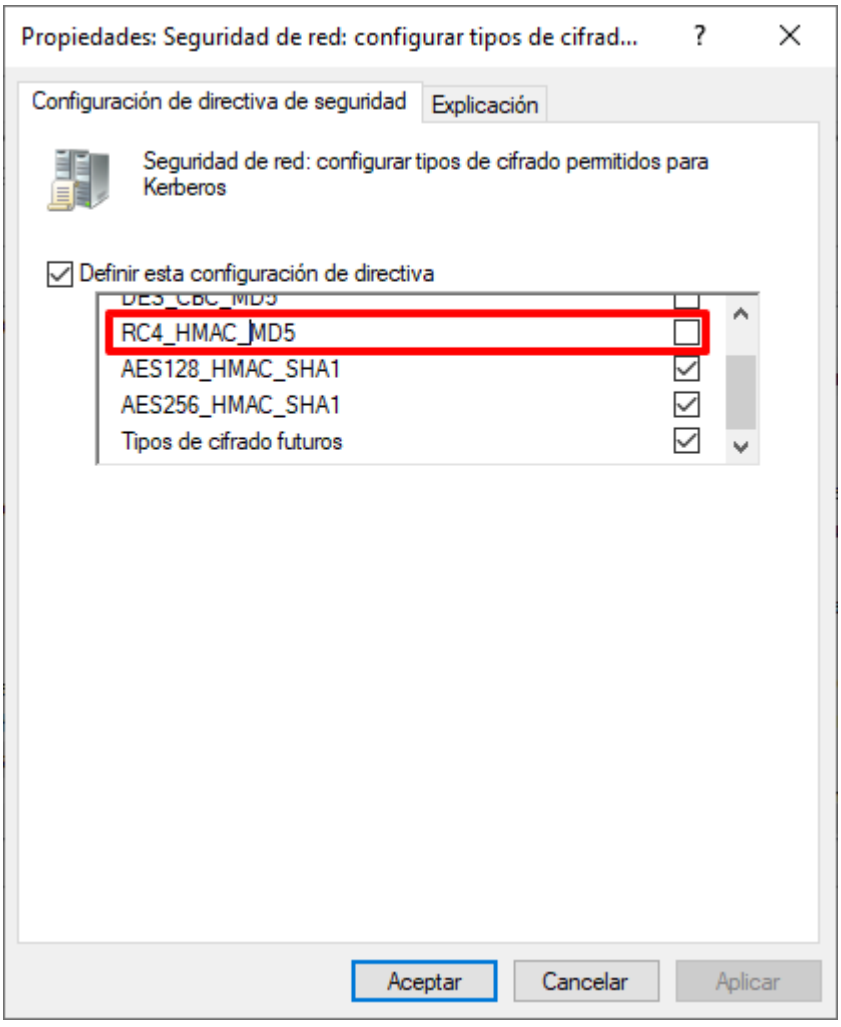
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a la protección de la integridad y la autenticidad, se definen los mecanismos autorizados para una comunicación segura entre los sistemas de información.

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

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

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

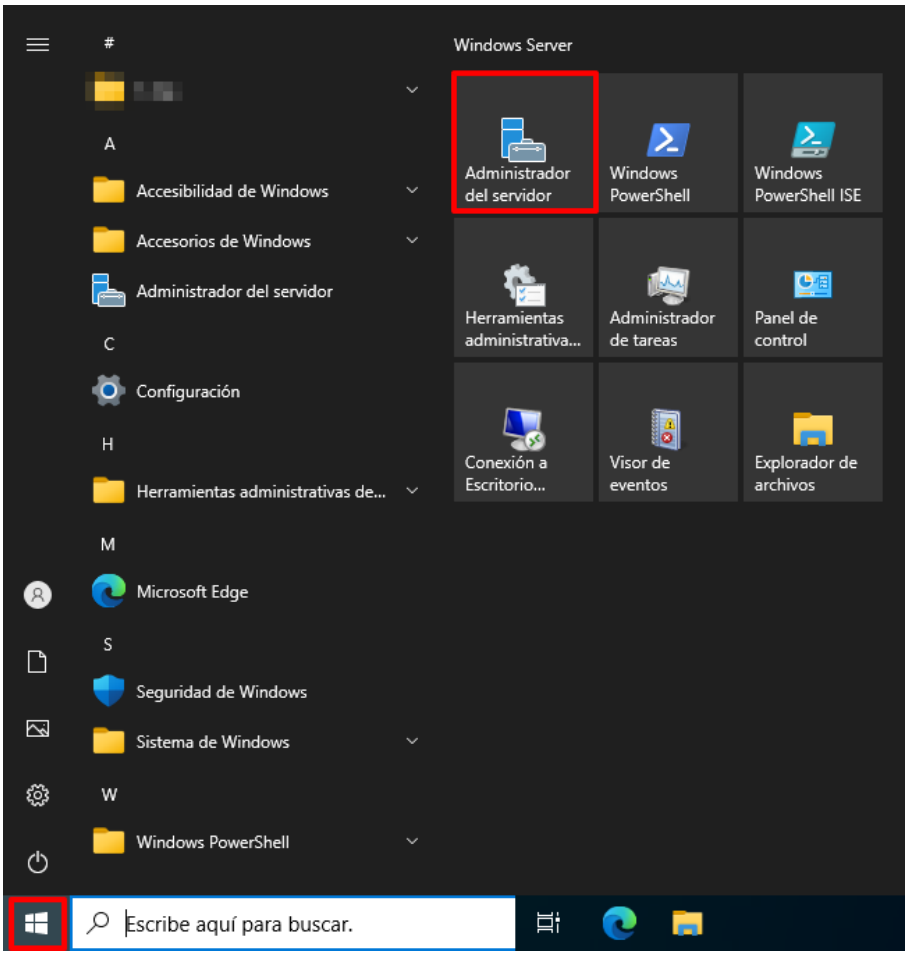
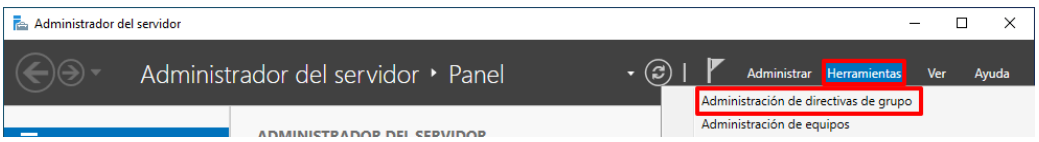
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de cifrado: – CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre “Editar”.  **Nota:** En este ejemplo se hace uso del objeto GPO “CCN-STIC-570A23 Incremental Dominio (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental Dominio ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.
8.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Seguridad de red: configurar tipos de cifrado permitidos para Kerberos 

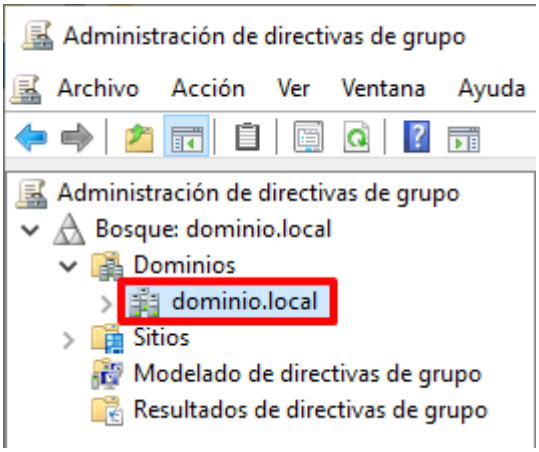
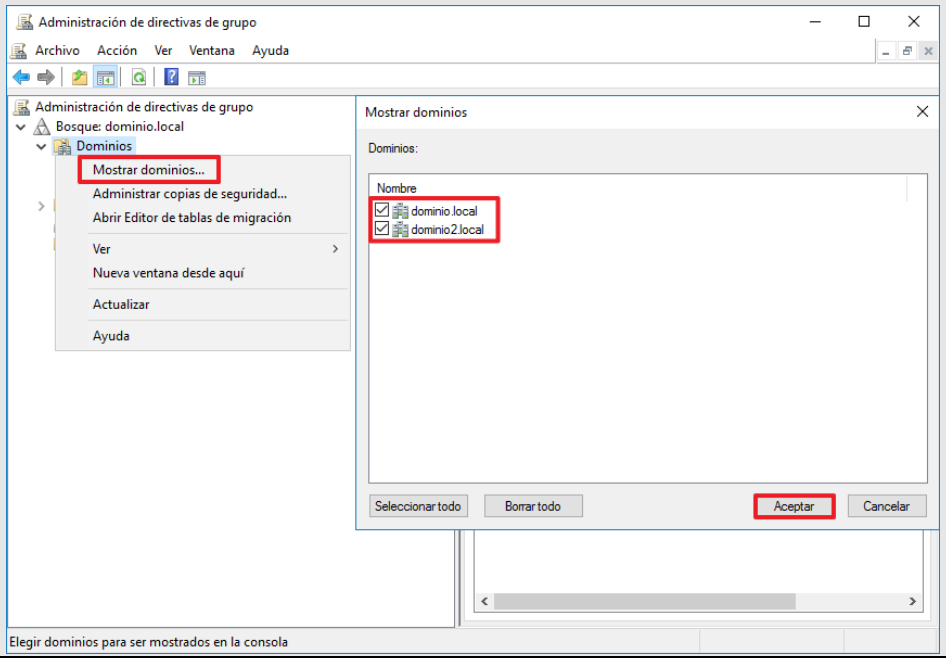
Paso	Descripción
9.	Cuando su sistema de información disponga de productos antiguos, o incluso obsoletos, es posible que para evitar problemas de conectividad entre sí requiera activar cifrados considerados inseguros. En este caso deberá marcar la opción “RC4_HMAC_MD5”. Independientemente de ello, deberá actualizar los sistemas más antiguos u obsoletos con el fin de poder retirar este tipo de cifrado del entorno de dominio.  **Nota:** Tenga en consideración que esta configuración se aplica a todos los objetos del dominio, independientemente si pueden hacer uso de cifrados más seguros.

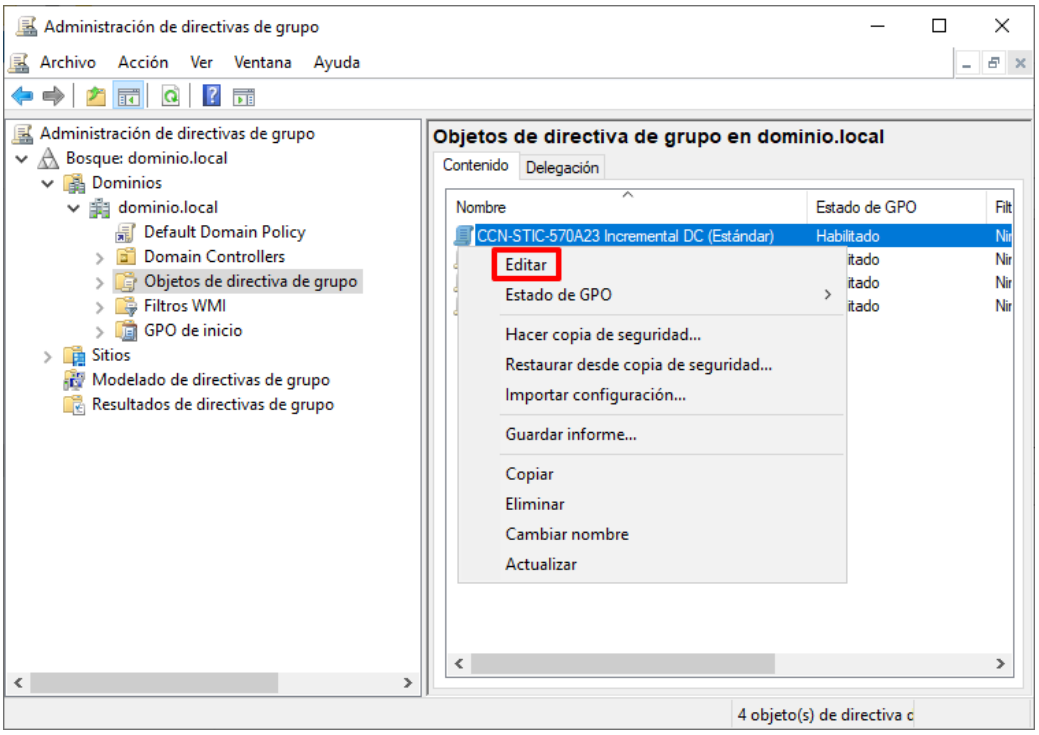
ANEXO D.5. BLOQUEO DE SESIÓN ANTE INACTIVIDAD

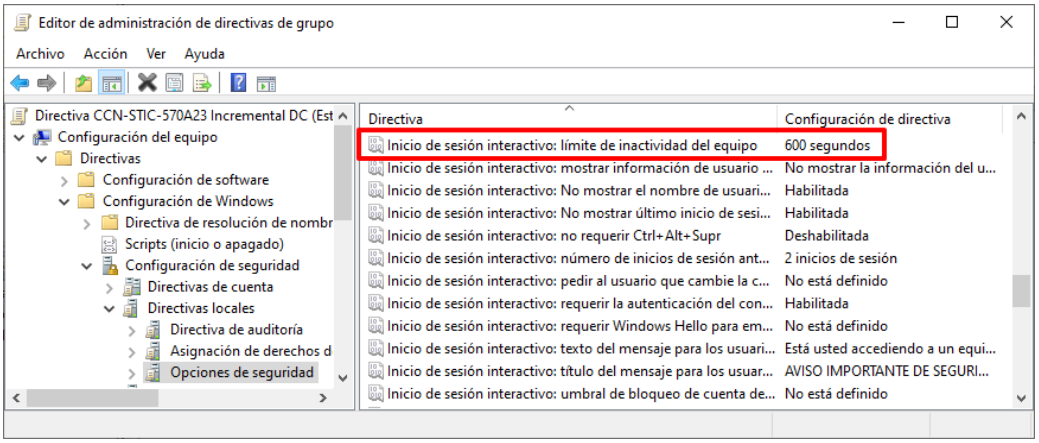
Dados los requisitos del ENS, tal y como se expone en la medida dedicada al bloqueo de puesto de trabajo, es necesario que este quede bloqueado pasado un tiempo prudencial de modo que requiera una nueva autenticación del usuario para el uso del mismo.

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

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

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

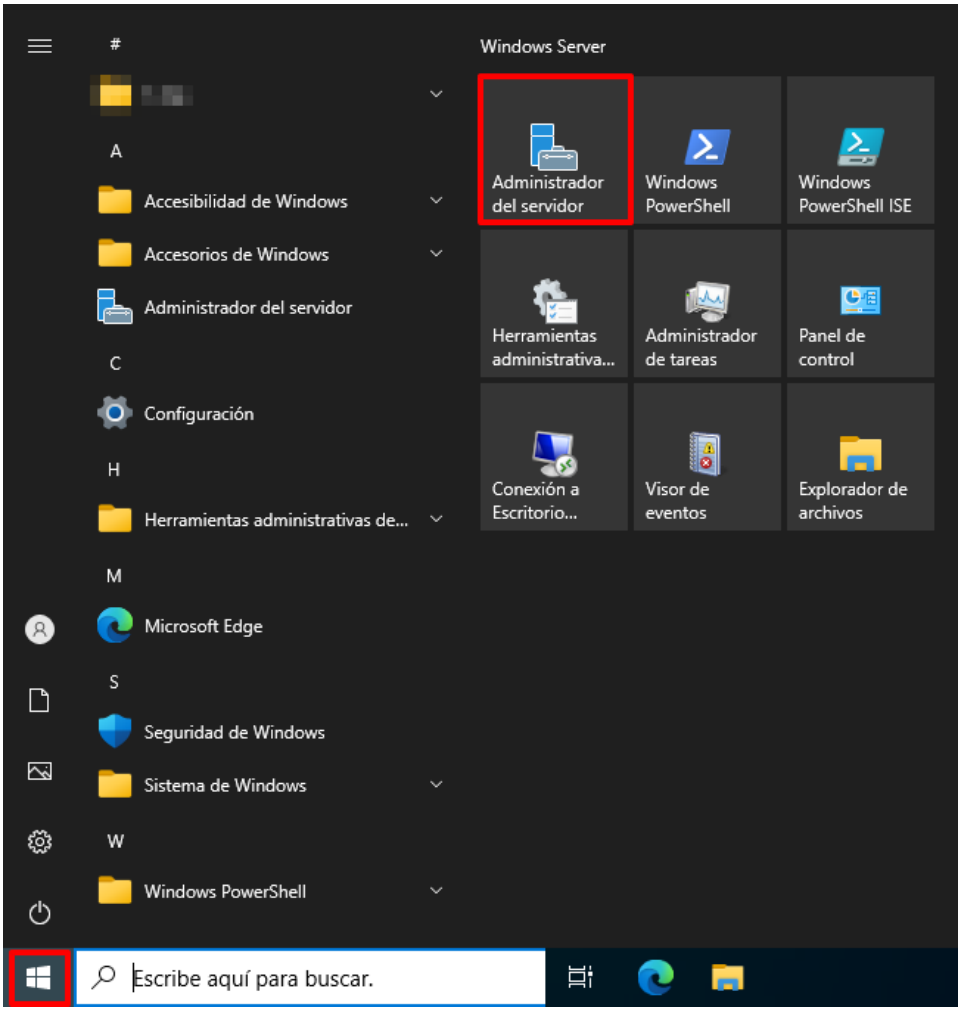
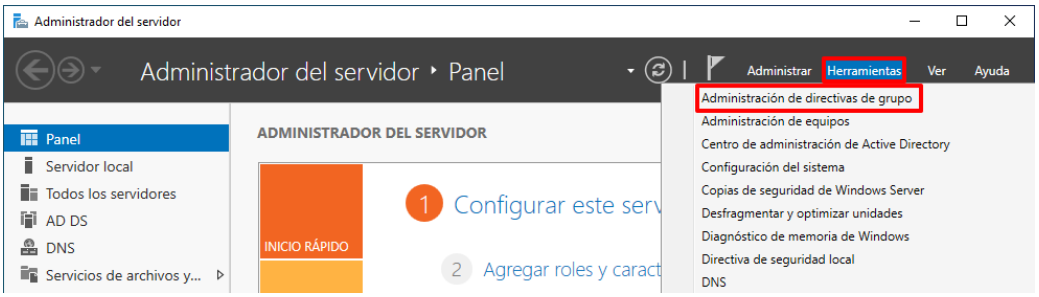
Paso	Descripción
5.	Dentro del nodo "Objetos de directiva de grupo" identifique los dos (2) siguientes objetos GPO en función de donde desee adecuar los parámetros de bloqueo de puesto de trabajo: – CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) – CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre "Editar".  **Nota:** En este ejemplo se hace uso del objeto GPO "CCN-STIC-570A23 Incremental DC (Estándar)".
7.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**.

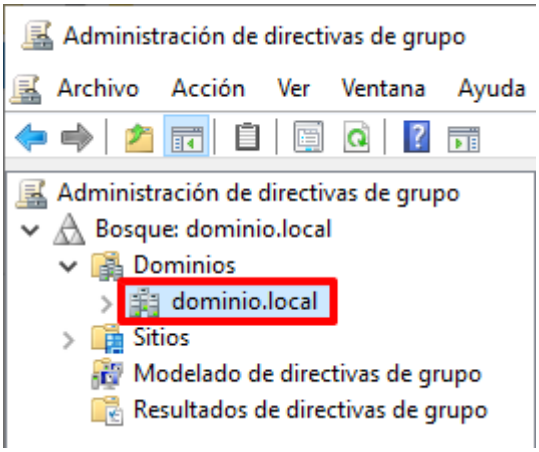
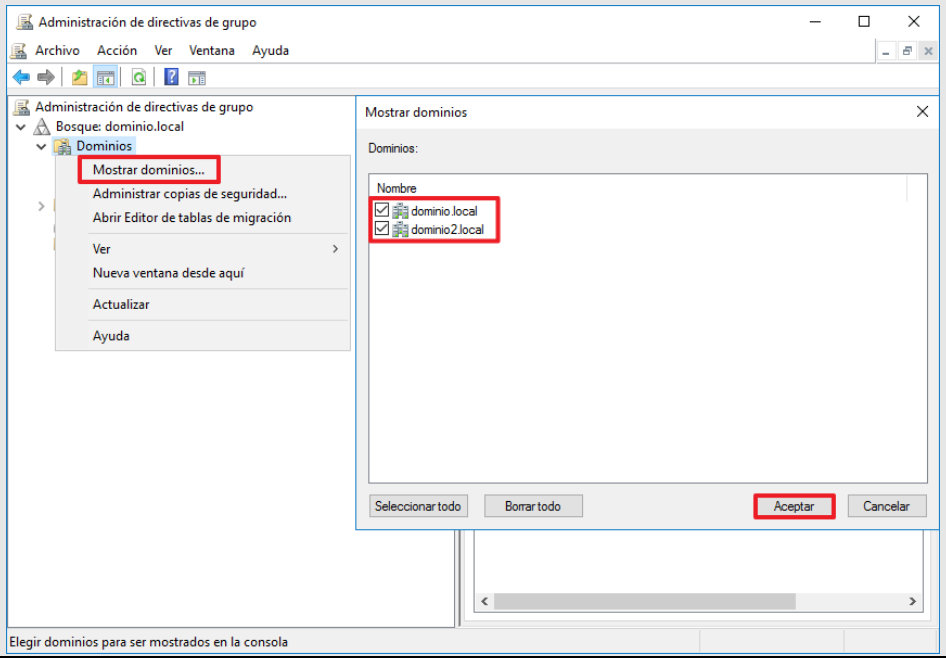
Paso	Descripción
8.	En el panel derecho identifique la siguiente directiva y edítela a continuación: – Inicio de sesión interactivo: límite de inactividad del equipo 
9.	La configuración establecida expone un tiempo prudencial el cual puede ser adaptado en función de la política de la organización.

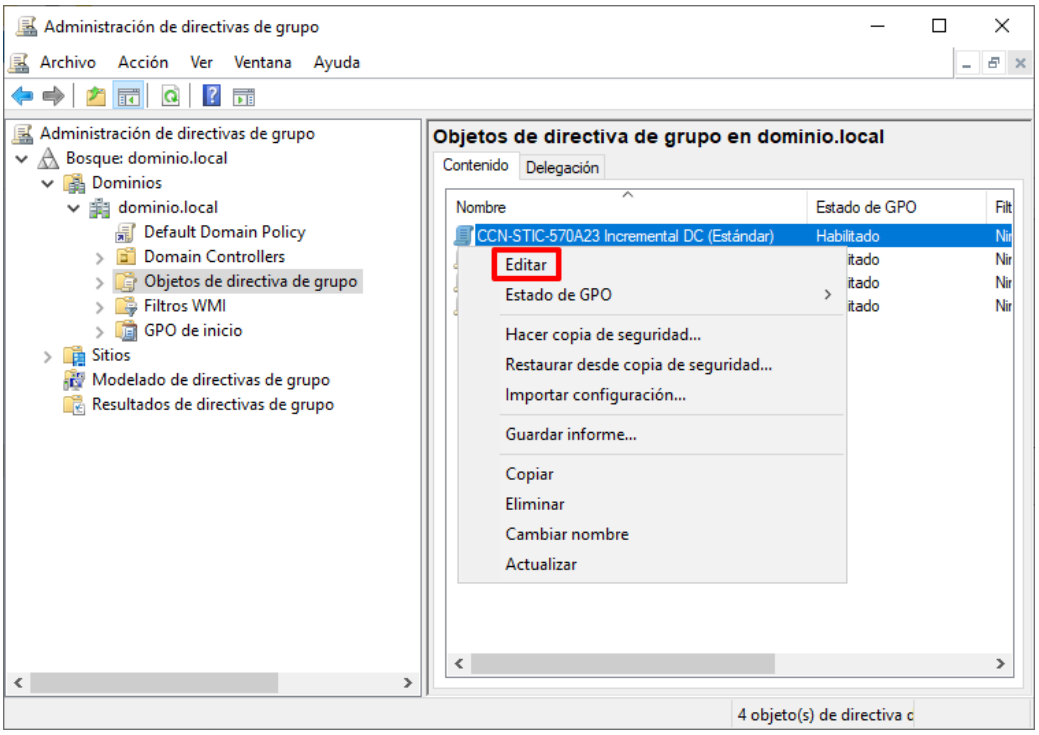
ANEXO D.6. OPCIONES DE SEGURIDAD

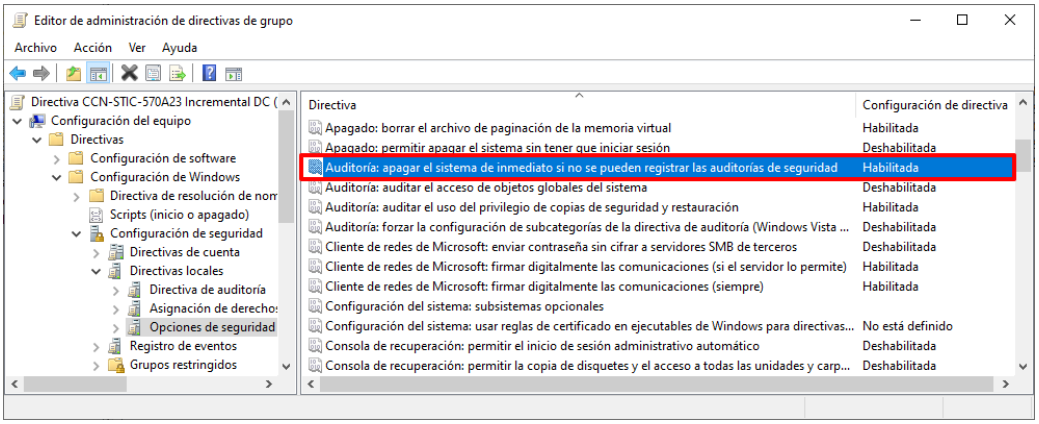
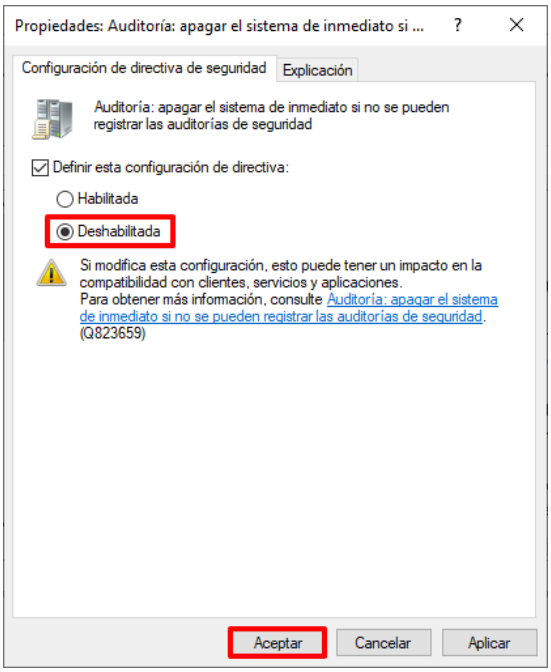
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a modificar y/o adaptar la configuración establecida en los apartados anteriores del presente documento.

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

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

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

Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique los dos (2) siguientes objetos GPO en función de donde desee adecuar los parámetros de opciones de seguridad: – CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) – CCN-STIC-570A23 Incremental Servidores ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.
6.	A continuación, haga clic derecho sobre el objeto deseado y pulse sobre “Editar”.  **Nota:** En este ejemplo se hace uso del objeto GPO “CCN-STIC-570A23 Incremental DC (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-570A23 Incremental DC ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.

Paso	Descripción
8.	En el panel derecho identifique la directiva “Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad”. 
9.	Cuando los recursos hardware en los sistemas TIC son aprovisionados de una forma muy limitada, pueden producirse situaciones en las que el uso de estos sistemas impida que la auditoría de seguridad se registre adecuadamente. En estas situaciones el sistema operativo colapsará para protegerse y lanzará un llamado “pantallazo azul” cuando la directiva anterior está configurada. Si debido a las limitaciones hardware se producen muchos de estos eventos, edite la directiva indicada en el paso anterior y establezca su configuración en “Deshabilitada”.  **Nota:** Tenga en consideración que alterar esta directiva puede impedirá que se registren ciertos eventos de seguridad que pueden ser cruciales de cara a la trazabilidad de alguna acción realizada en el sistema operativo.

PUBLICACIONES DE DEFENSA

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