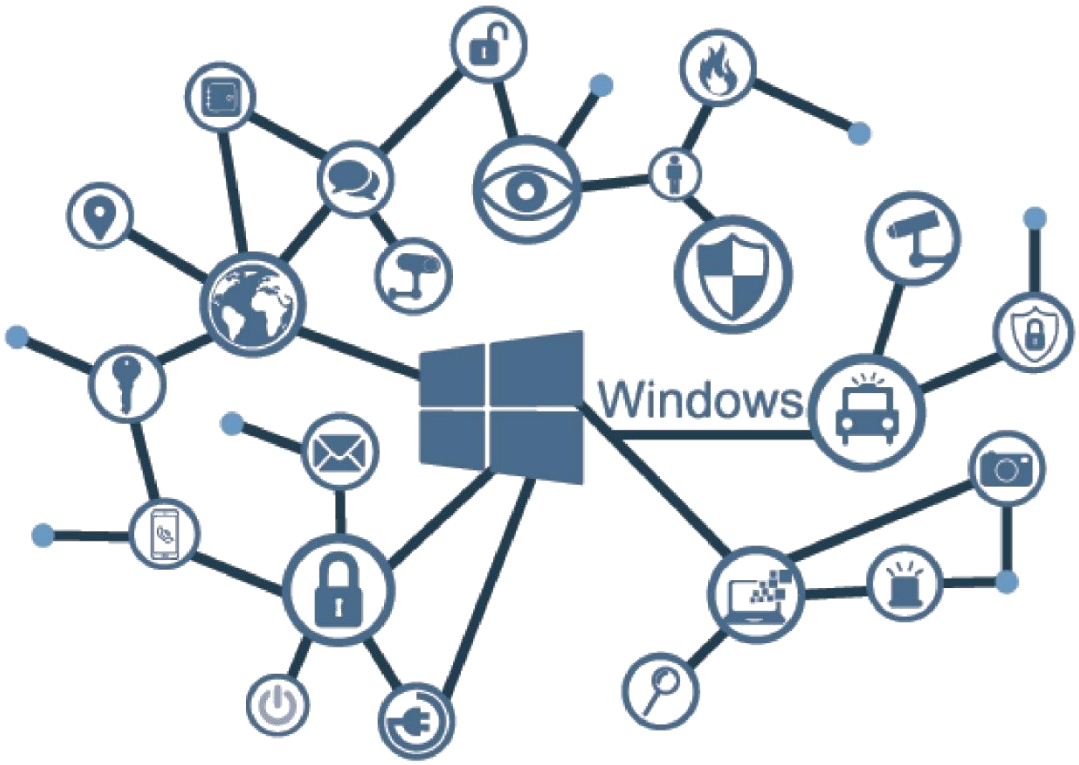
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 599AB23

PERFILADO DE SEGURIDAD PARA WINDOWS CLIENTE (CLIENTE MIEMBRO O CLIENTE INDEPENDIENTE)



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
2025.01.29 12:55:58 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-168-4
Fecha de Edición: mayo de 2024

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

INDICE

1. INTRODUCCIÓN

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

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

Por ejemplo, en el caso de un entorno para un cliente miembro de un dominio con Microsoft Windows 10, en el que se instale Microsoft Office 2016, deberán aplicarse las siguientes guías:

a) Guía CCN-STIC-599AB23 en el cliente miembro con Windows 10.

b) Guía CCN-STIC-585 Microsoft Office 2016 sobre Windows 10.

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 Cliente.

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 Cliente, 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 **equipos basados en un sistema operativo "Microsoft Windows Cliente"**, instalados en español, bien actuando como **cliente miembro de un dominio** o bien como un **cliente independiente**.

El documento no se centrará en una edición y versión concreta del sistema operativo, como pueda ser Windows 10 o Windows 11, sino que será de utilidad para **cualquier edición y versión cliente de Windows** (siendo recomendable su aplicación desde la edición Windows 10 Enterprise LTSC 2019 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 11 Pro, Versión 22H2.

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 Cliente 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.

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

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 Cliente.

   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 Cliente, 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 un sistema de archivos que permita 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 equipo va a ser cliente miembro de un dominio, se debe proceder de la siguiente manera:

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

   ii. Si el equipo es un cliente independiente, se debe proceder de la siguiente forma:

      - Revisar e implementar el apartado correspondiente a la aplicación de seguridad sobre un cliente independiente.

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 Cliente, 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 Cliente.

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 Cliente

En total, según se puede apreciar en la tabla, es posible la aplicación directa de catorce (14) medidas de seguridad de forma técnica a los sistemas operativos Windows Cliente. 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 los sistemas operativos Windows Cliente 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 Cliente, 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 Cliente, 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
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

[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.2	Configuración de seguridad	Categoría	aplica	aplica	aplica	+ R1 + R2 + R3+ R4 + R5 + R6 + R7 + R8 + R9 + R10 + R11 + R12
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

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
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 Cliente 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 a los sistemas operativos Windows Cliente. 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 los sistemas operativos Windows Cliente y su aplicación a nivel técnico.

ANEXO A. CONFIGURACIÓN SEGURA DE CLIENTES WINDOWS MIEMBRO DE DOMINIO

ANEXO A.1. PASO A PASO DE CONFIGURACIÓN BASE DE SEGURIDAD SOBRE CLIENTES MIEMBRO

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento de los equipos clientes miembro de un dominio, 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 la 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:

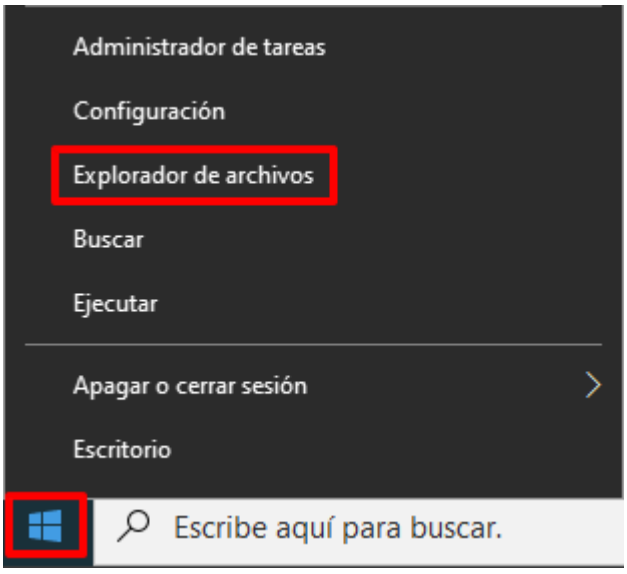
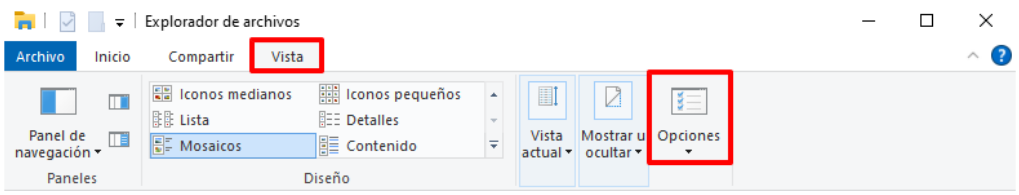
a) Clientes miembro del dominio: Aplicable a aquellos equipos que utilicen cualquier tipo de servicio dentro del dominio, se definirán medidas de seguridad mediante objetos GPO y se ejecutarán acciones manuales y automatizadas para finalizar las labores de configuración segura.

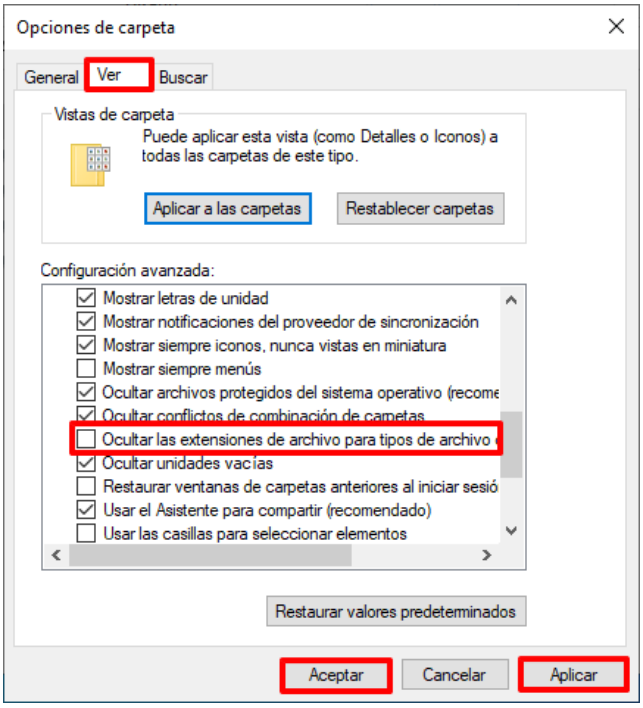
b) Configuraciones individuales: Es necesario indicar que ciertas medidas de seguridad no pueden ser aplicadas por medio de objetos GPO o configuraciones exactas a nivel de Windows. Esto es debido a que deben ser personalizadas por cada organización o adaptadas a esta. Por ello, se han dedicado apartados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

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

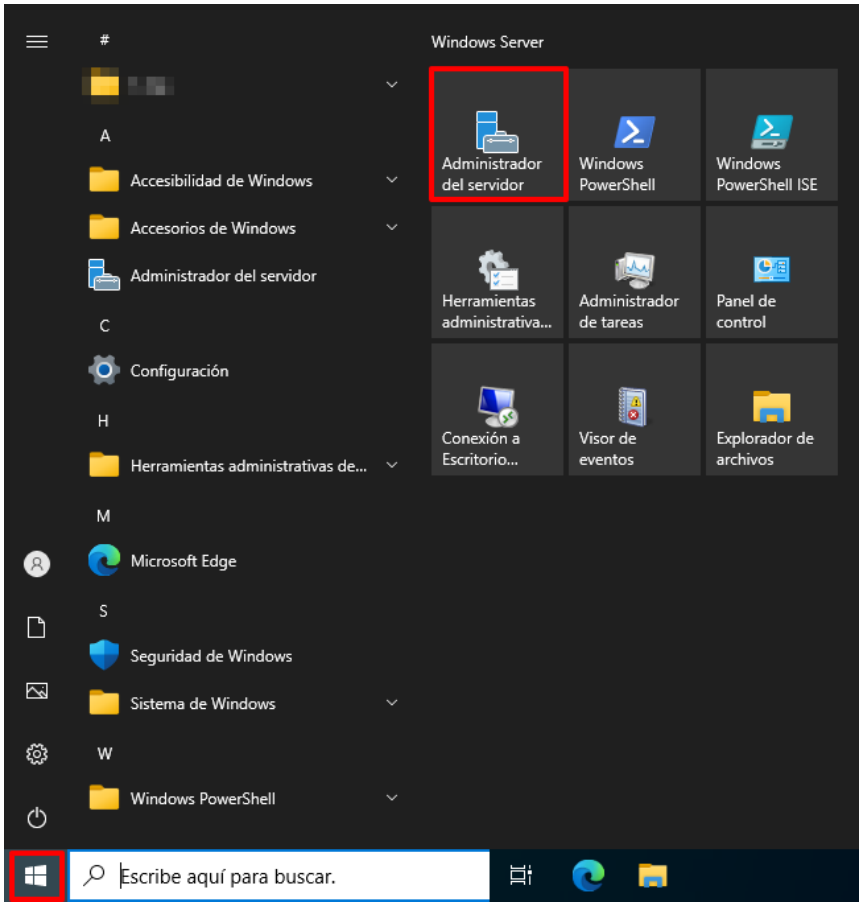
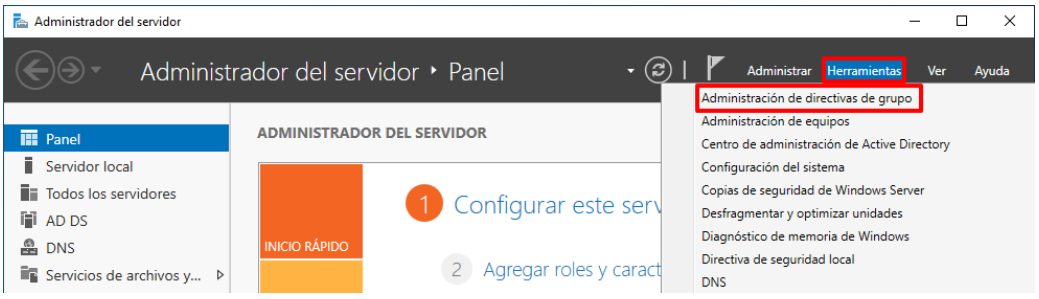
ANEXO A.1.1. PREPARACIÓN DEL DOMINIO

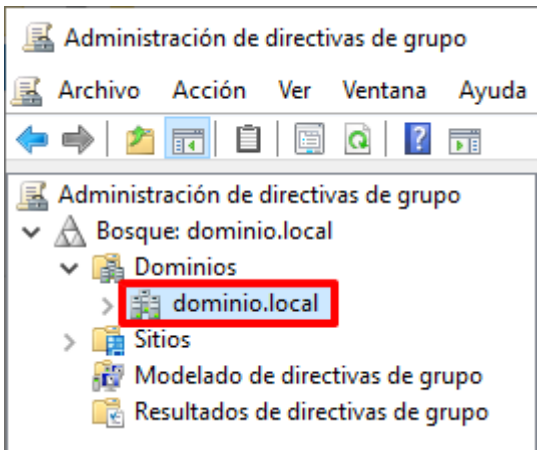
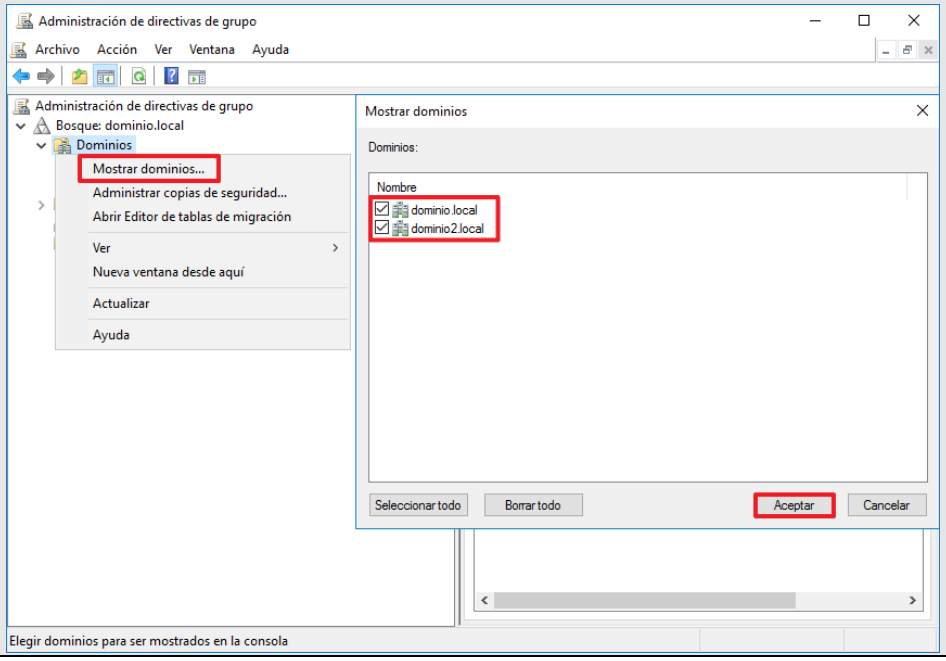
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se realizará la implementación de las medidas de seguridad mediante objetos GPO. Solo es necesario realizar este procedimiento una (1) vez.

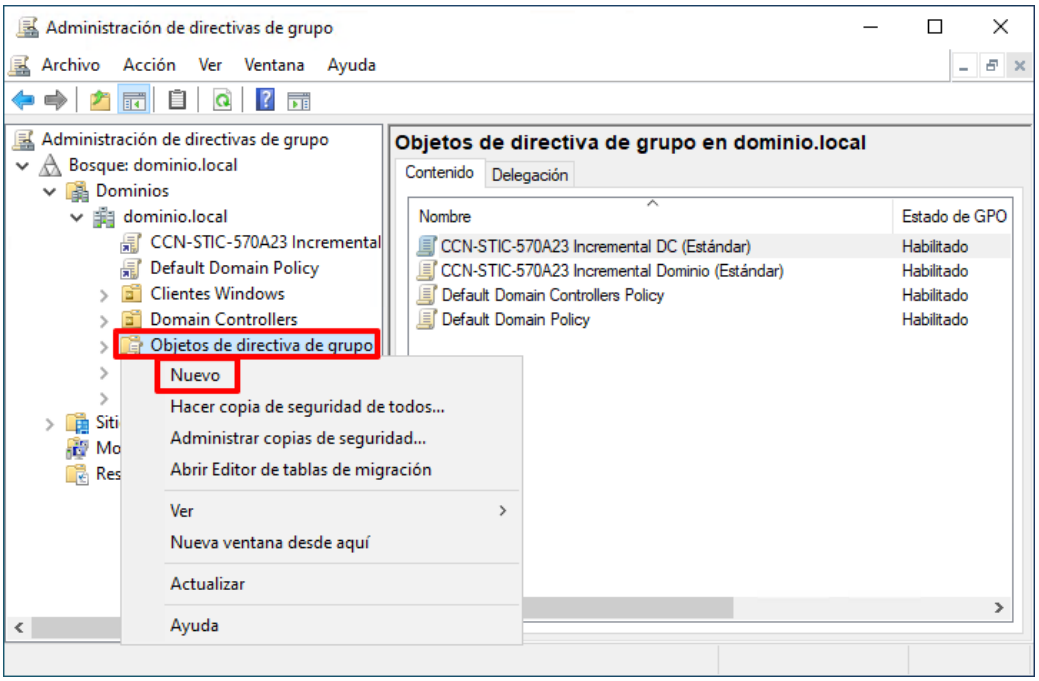
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad C:\.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts". **Nota:** Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599AB23\CLIENTES MIEMBRO”.
4.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 

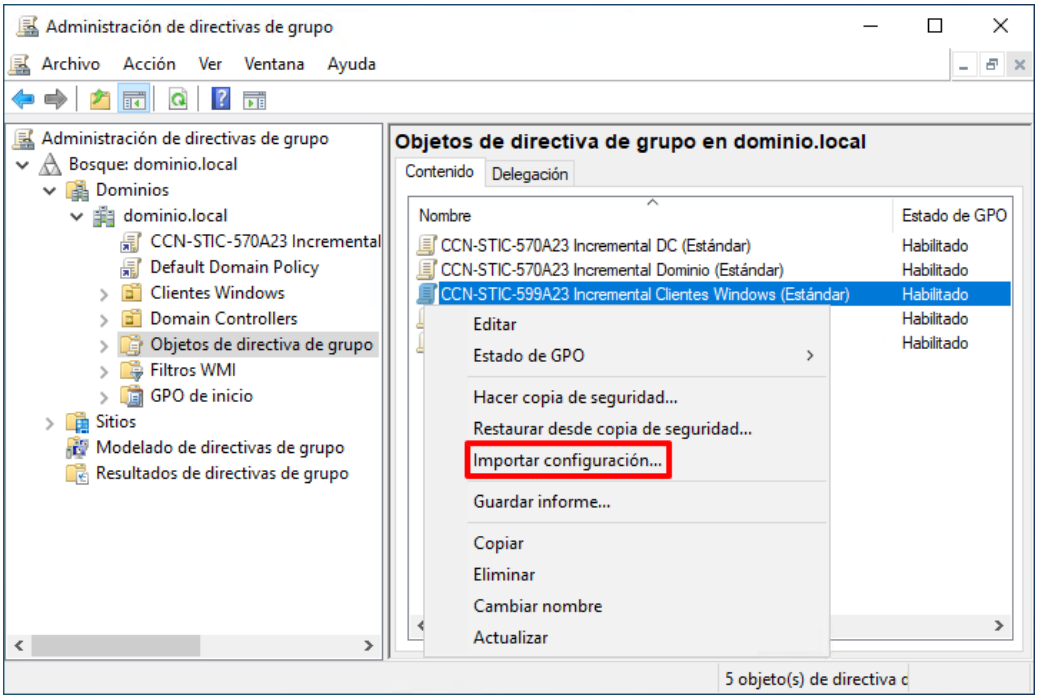
Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – ESTANDAR/USO OFICIAL/MATERIAS CLASIFICADAS • CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-599A23 Incremental Actualizaciones WU [Directorio] • CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-599A23 Incremental Control Dispositivos [Directorio] • CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).inf • CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).wfw • CCN-STIC-599A23 Incremental Actualizaciones WU.inf

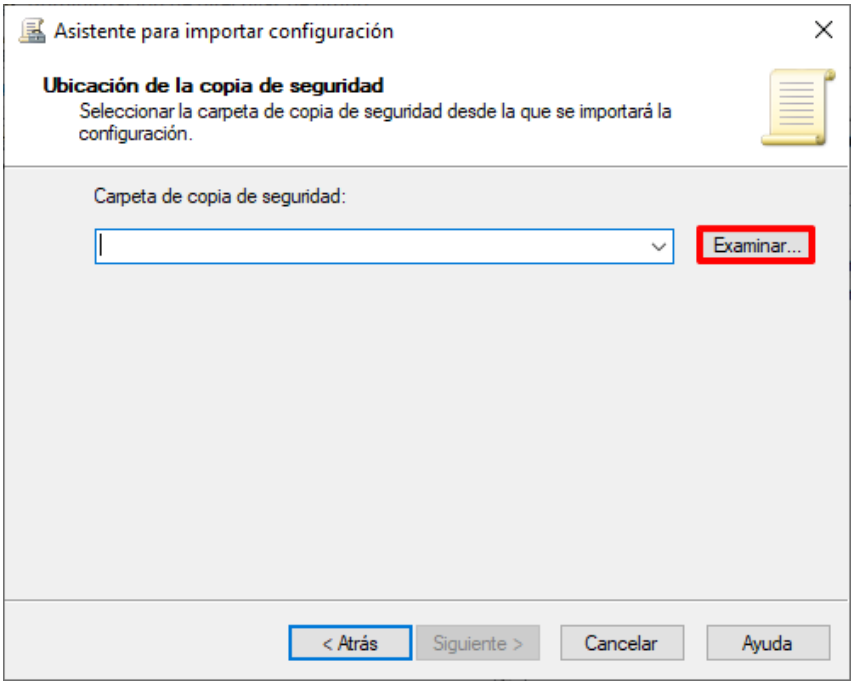
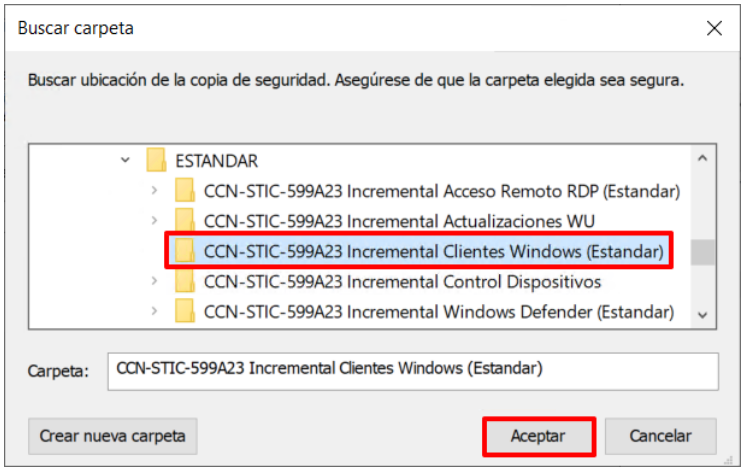
Paso	Descripción
	• CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]).inf • CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]).wfw • CCN-STIC-599A23 Incremental Control Dispositivos.inf • CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO]).inf • CCN-STIC-599A23 Incremental BitLocker [Directorio] (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) • CCN-STIC-599A23 Incremental BitLocker.inf (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) – CCN-STIC-599A23 Cliente Miembro – Desinstalar características.bat – CCN-STIC-599A23 Cliente Miembro – Eliminar aplicaciones aprovisionadas.bat – CCN-STIC-599A23 Menu contextual Windows 11.bat – CCN-STIC-599A23 Windows Defender - Análisis de dispositivos USB.bat – CCN-STIC-599A23 Windows Defender - Análisis de integridad de ficheros.bat – CCN-STIC-599A23 Windows Defender - Análisis en el arranque.bat – CCN-STIC-599A23_Analisis_arranque.ps1 – CCN-STIC-599A23_Analisis_arranque_OS.xml – CCN-STIC-599A23_Analisis_dispositivos_USB.xml – CCN-STIC-599A23_Analisis_USBs.ps1 – CCN-STIC-599A23_Antiguo_menu_contextual.ps1 – CCN-STIC-599A23_Desinstala_caracteristicas.ps1 – CCN-STIC-599A23_Eliminar_aplicaciones_aprovisionadas.ps1 – CCN-STIC-599A23_Habilitar_registro_conexion_USBs.ps1 – CCN-STIC-599A23_Integridad_ficheros.xml

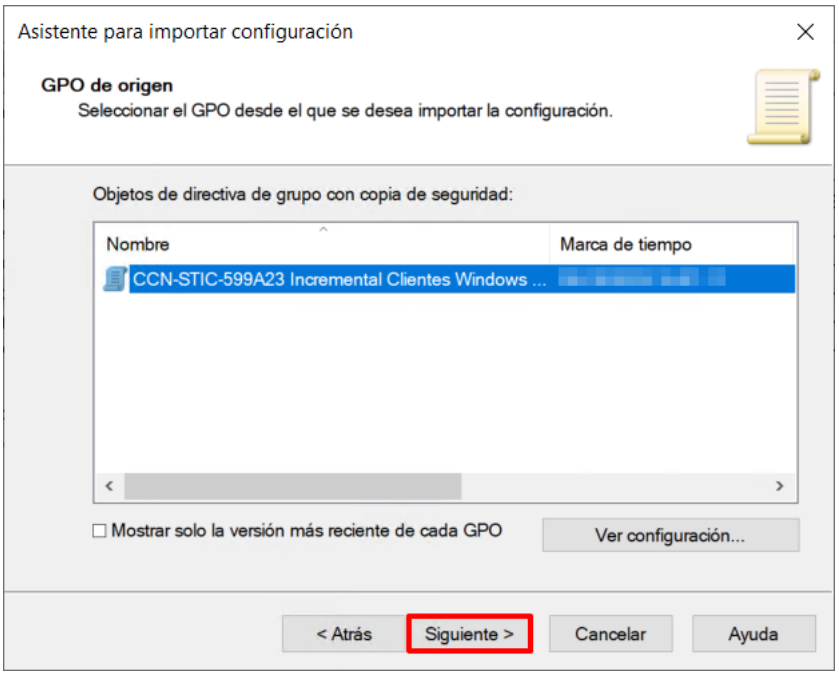
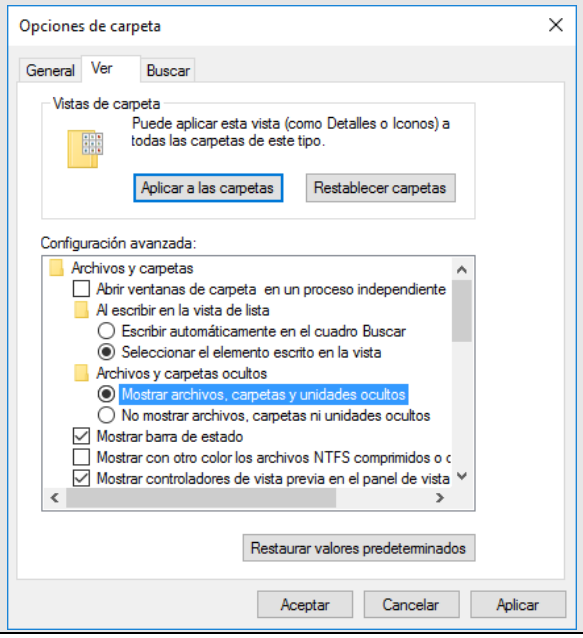
Paso	Descripción
8.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

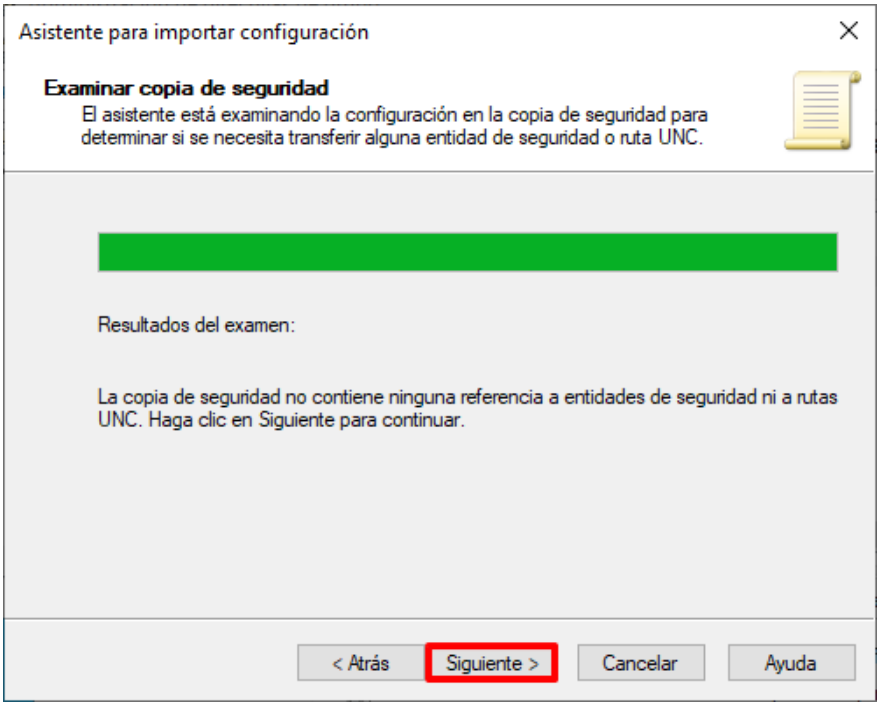
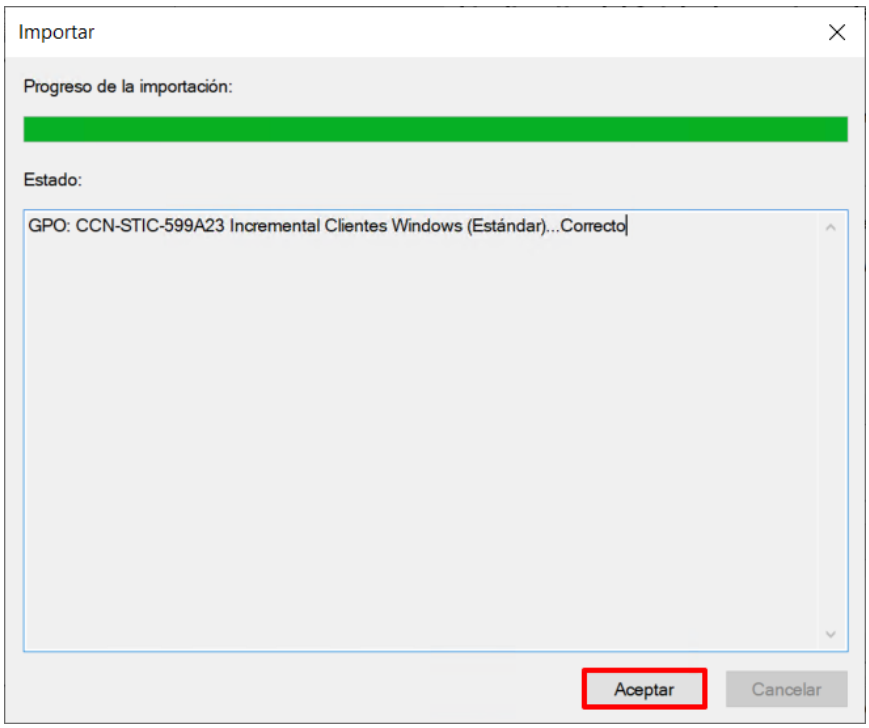
Paso	Descripción
10.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:**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

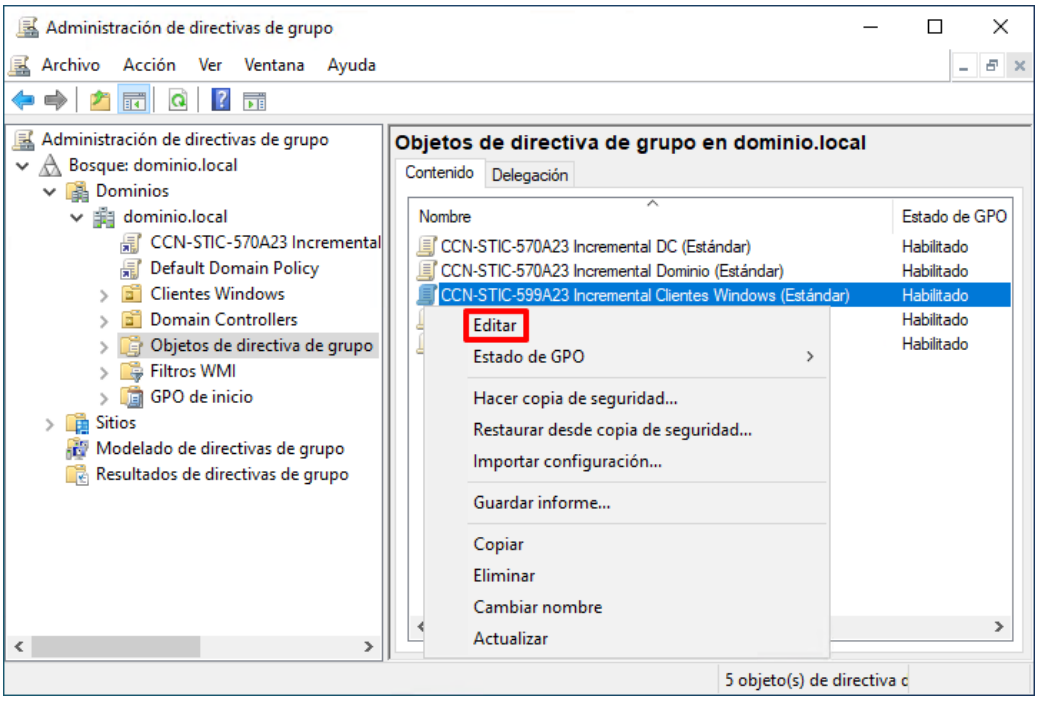
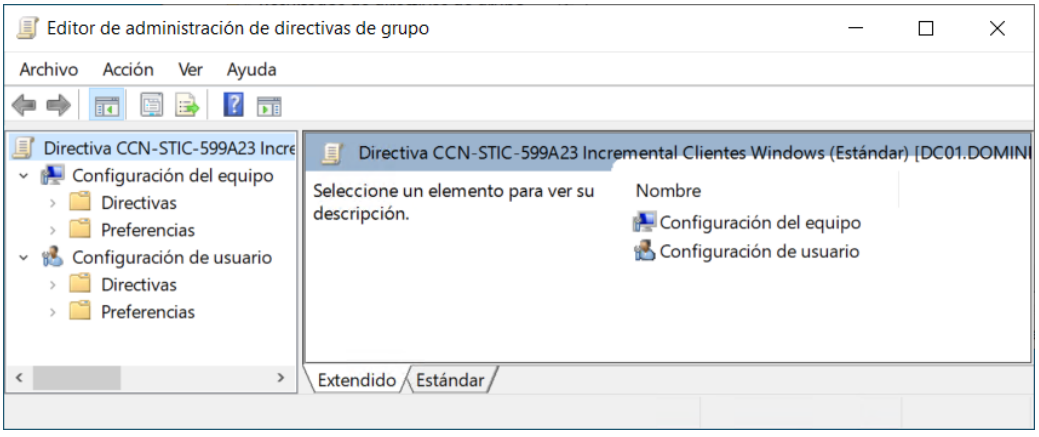
Paso	Descripción
11.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
12.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO])**" 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".
13.	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".

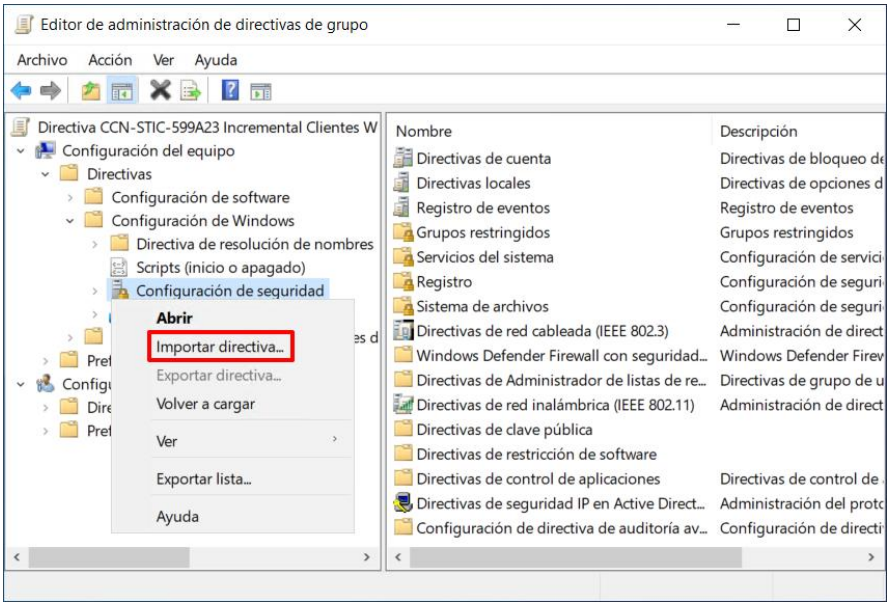
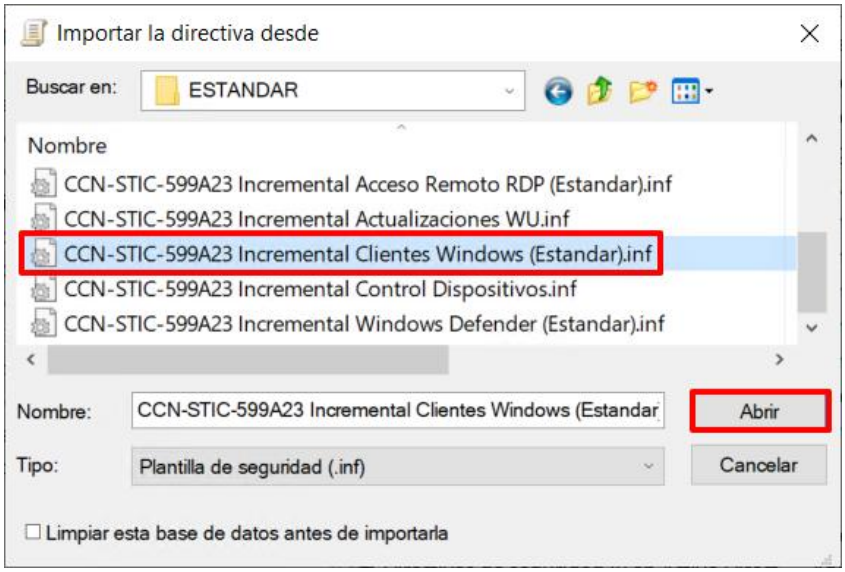
Paso	Descripción
14.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
15.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
16.	En la sección “Hacer copia de seguridad de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

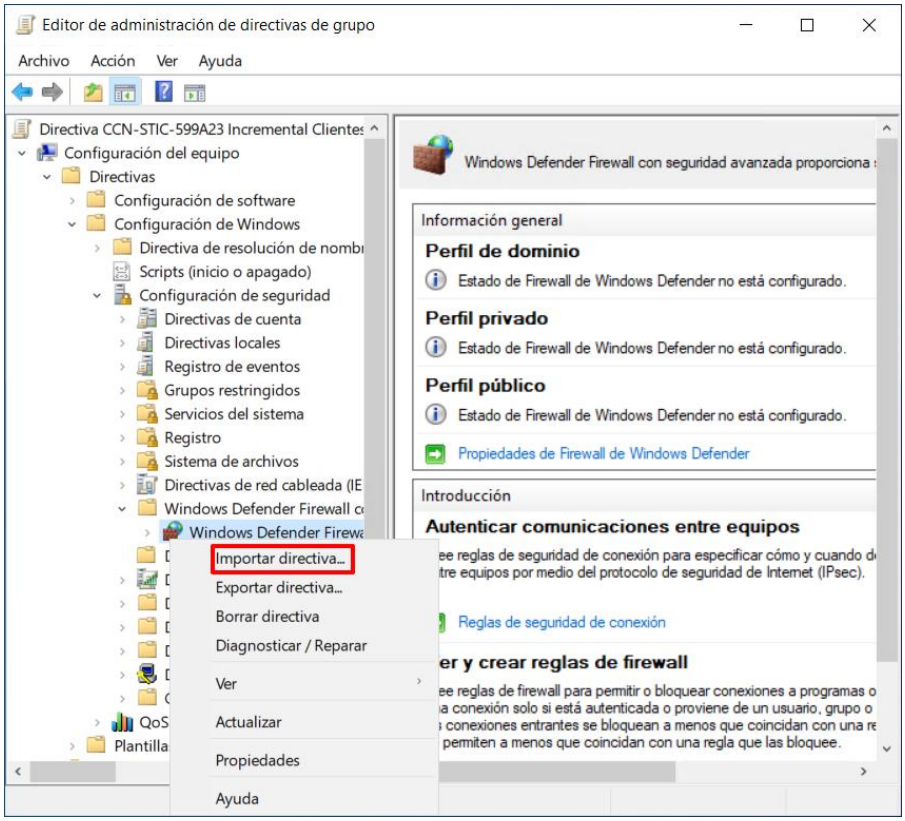
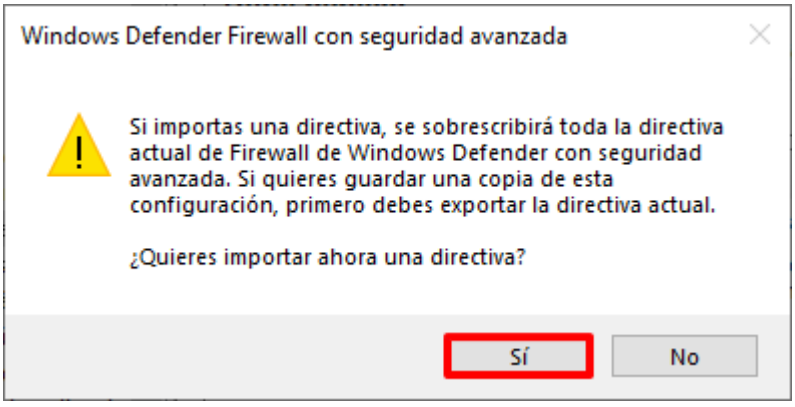
Paso	Descripción
17.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
18.	Seleccione la carpeta “CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
19.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.

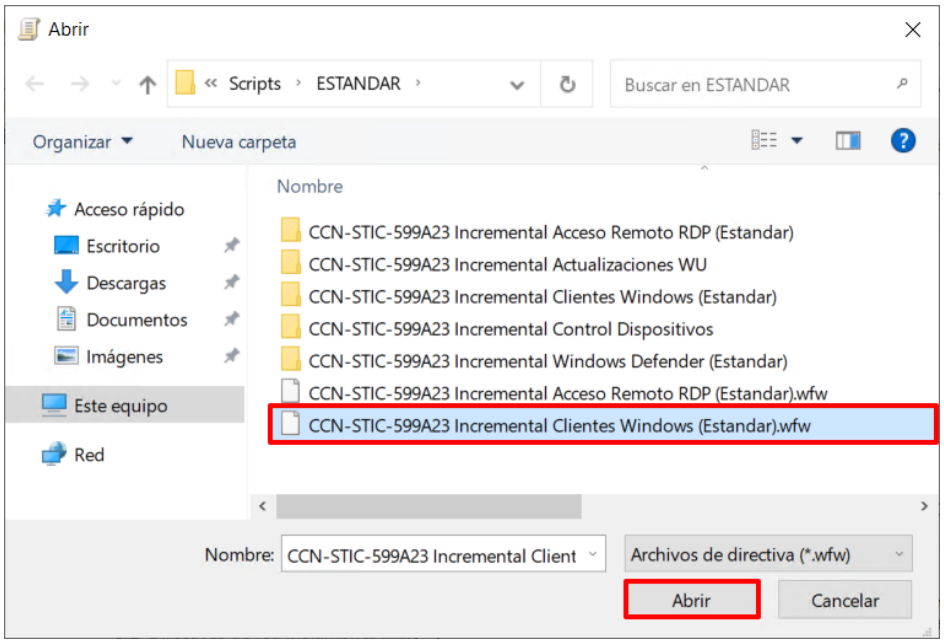
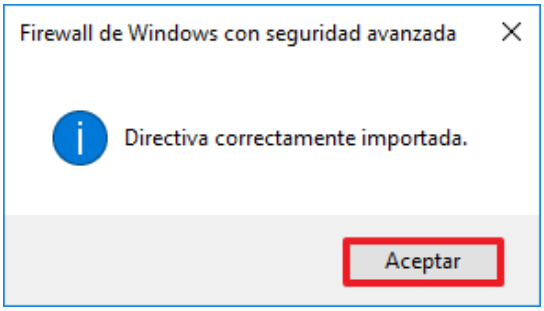
Paso	Descripción
20.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe 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
21.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
22.	Para completar el asistente pulse sobre el botón “Finalizar”.
23.	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
24.	Seleccione de nuevo el objeto GPO “CCN-STIC-599A23 Incremental Clientes Windows ([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”.
25.	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
26.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-599A23 Incremental Clientes Windows ([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. 
27.	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-599A23 Incremental Clientes Windows ([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
28.	En la misma ventana del editor de administración de directivas de grupo, seleccione el siguiente nodo: "**Directiva CCN-STIC-599A23 Incremental Clientes Windows ([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. 
29.	Responda "Sí" a la pregunta de confirmación "¿Desea importar ahora una directiva? 

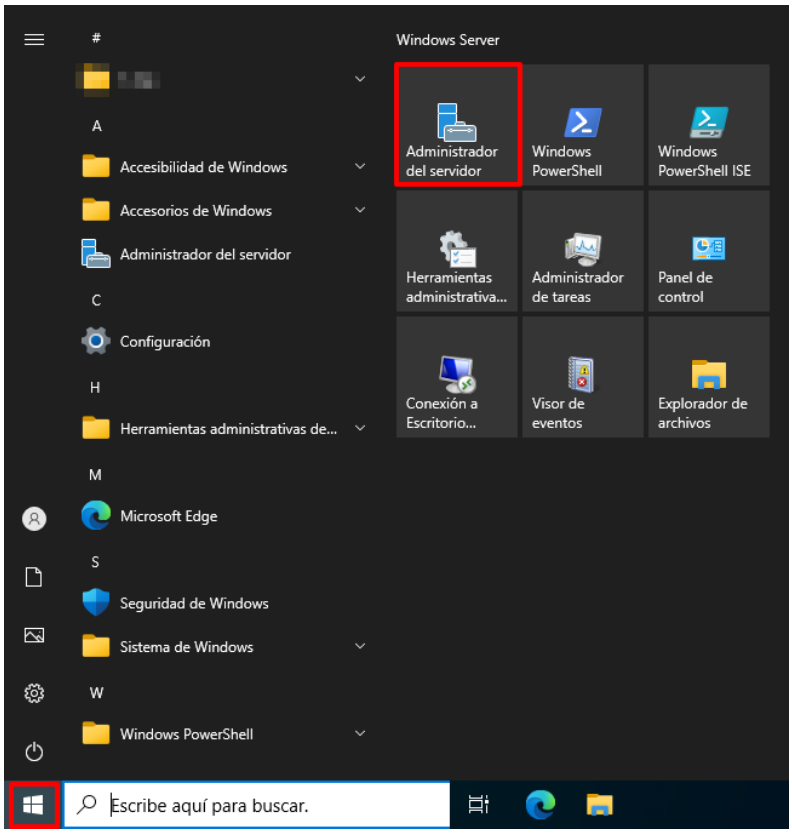
Paso	Descripción
30.	En el cuadro de diálogo que aparecerá, seleccione la directiva "C:\Scripts\[TIPO DE PERFILADO]\CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]).wfw" y pulse el botón "Abrir".  **Nota:** Seleccione la configuración de firewall acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
31.	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. 
32.	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”.

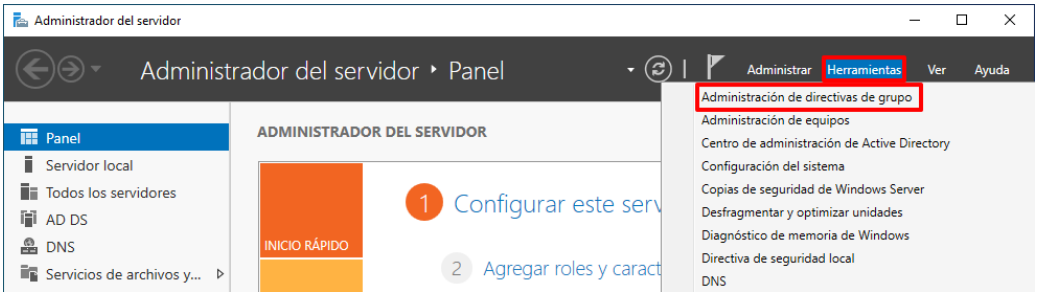
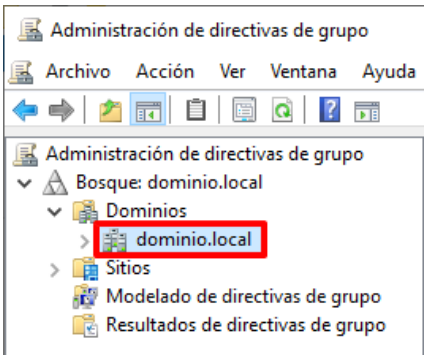
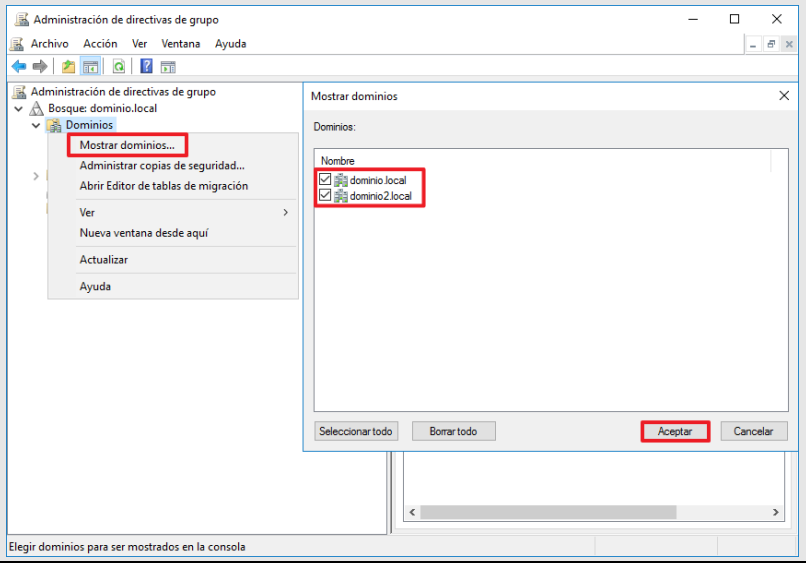
ANEXO A.1.2. CONFIGURACIÓN DE SEGURIDAD EN CLIENTES MIEMBRO

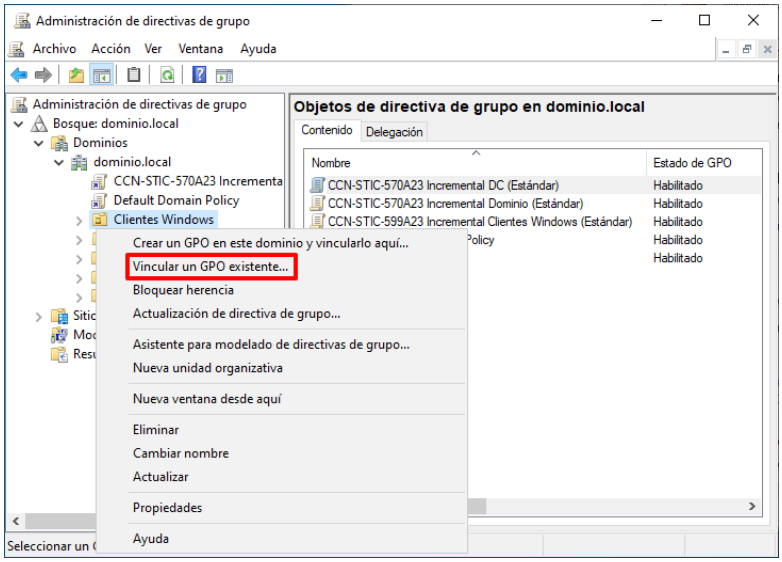
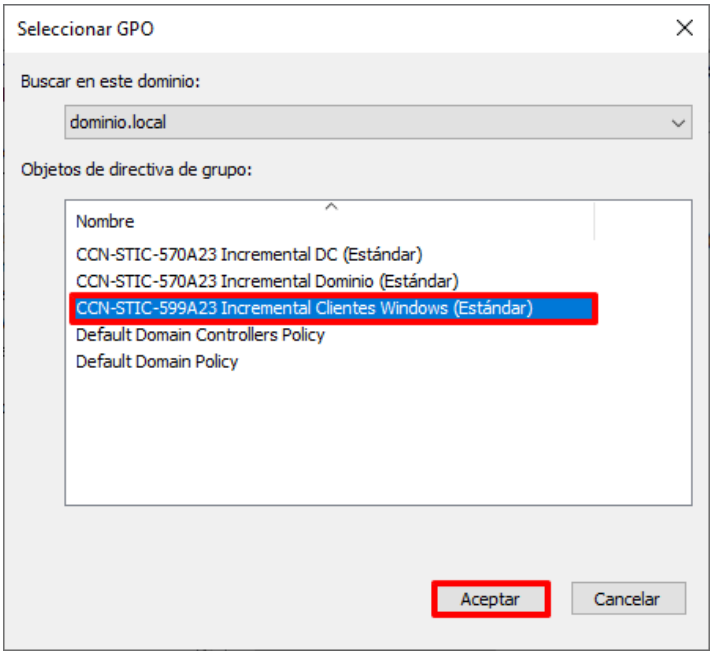
Una vez realizada la preparación de la configuración de seguridad necesaria a implementar, será necesario su aplicación sobre los objetos correspondientes, así como la ejecución de labores adicionales para cubrir todos los aspectos necesarios de seguridad.

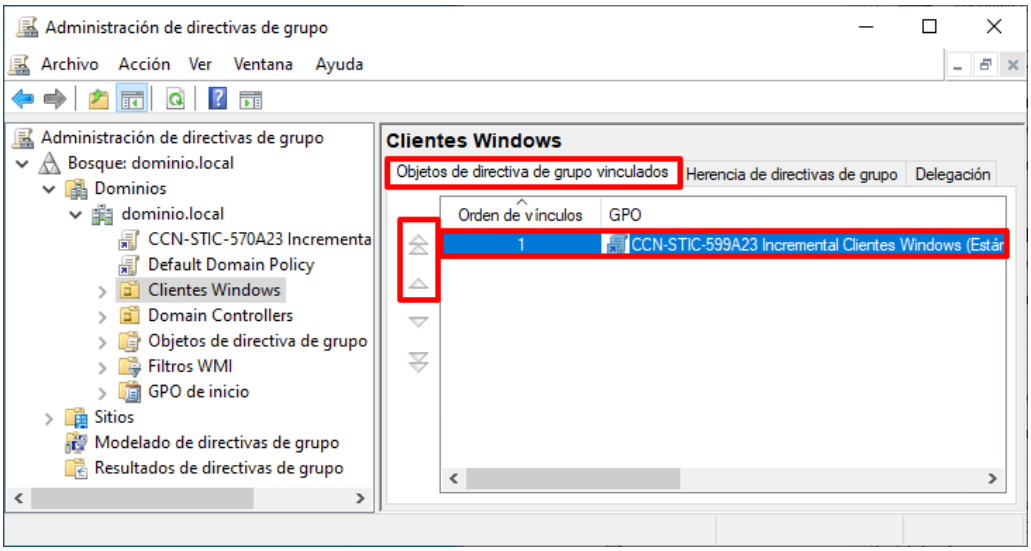
ANEXO A.1.2.1. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

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 los objetos de tipo Cliente 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.
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. 

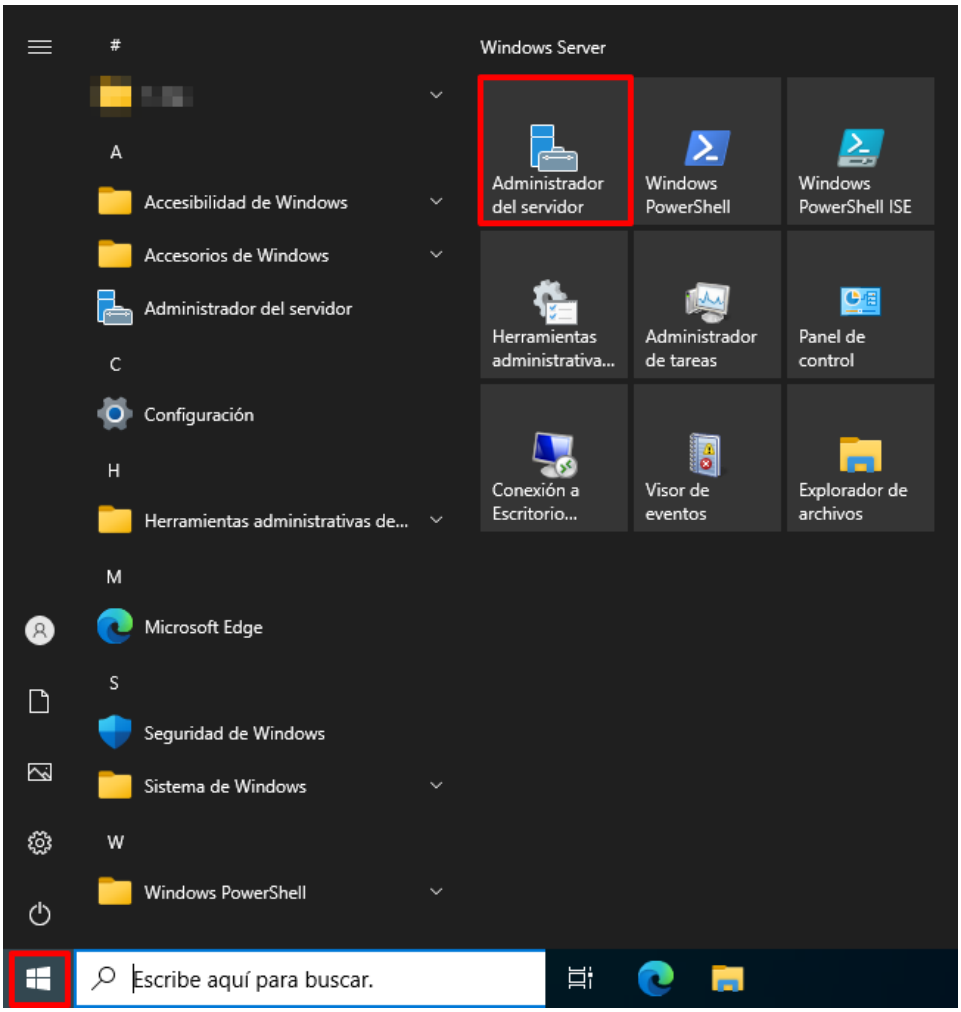
Paso	Descripción
5.	Identifique aquellas unidades organizativas donde se alojen aquellos objetos de tipo cliente miembro que se pretenden asegurar, y haciendo clic derecho sobre el contenedor seleccione la opción del menú contextual “Vincular un GPO existente…”.  **Nota:** En este ejemplo se hace uso de la unidad organizativa “Clientes Windows” creada para alojar los objetos de tipo cliente miembro del dominio. Deberá adaptar este paso a las necesidades de su organización.
6.	A continuación, seleccione el objeto GPO “CCN-STIC-599A23 Incremental Clientes Windows ([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”.

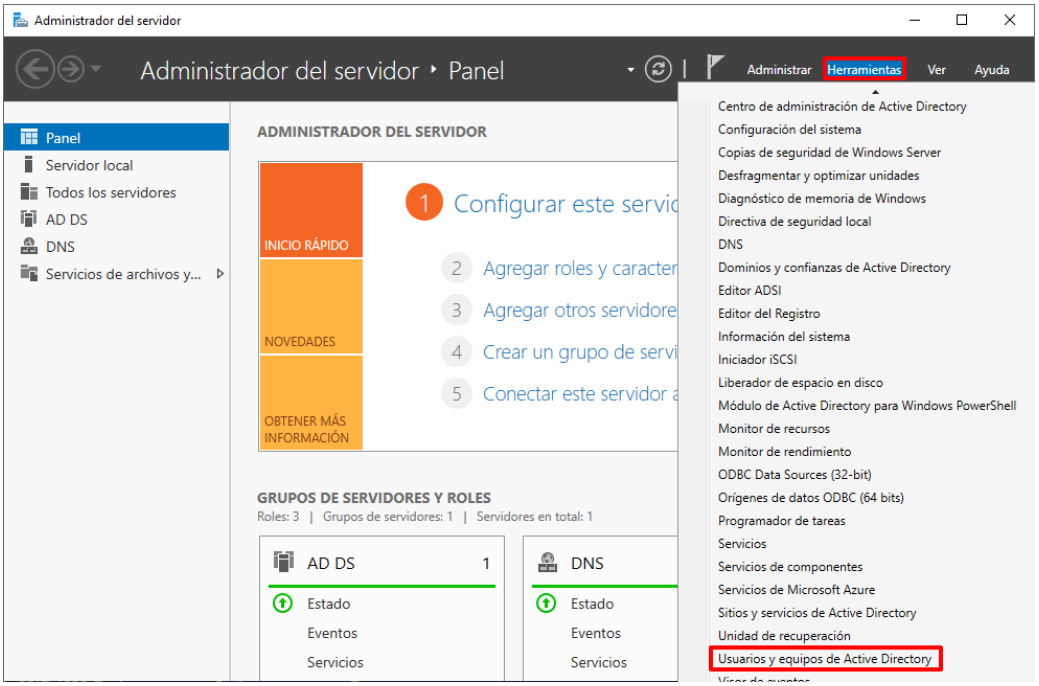
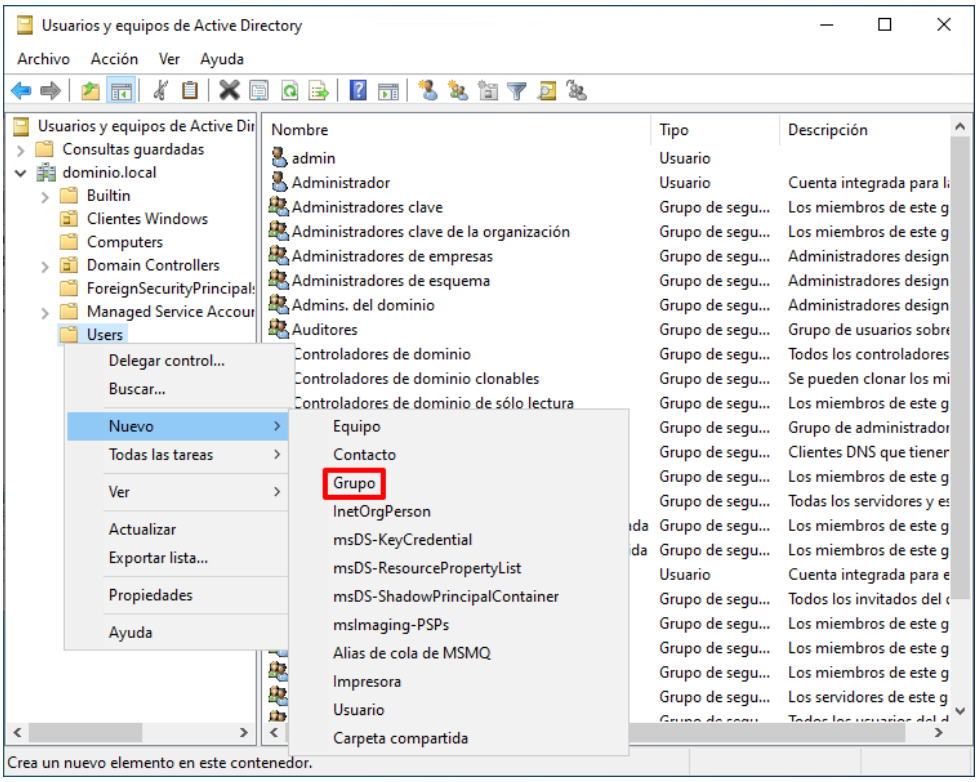
Paso	Descripción
7.	Seleccione el contenedor sobre el que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 
8.	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.

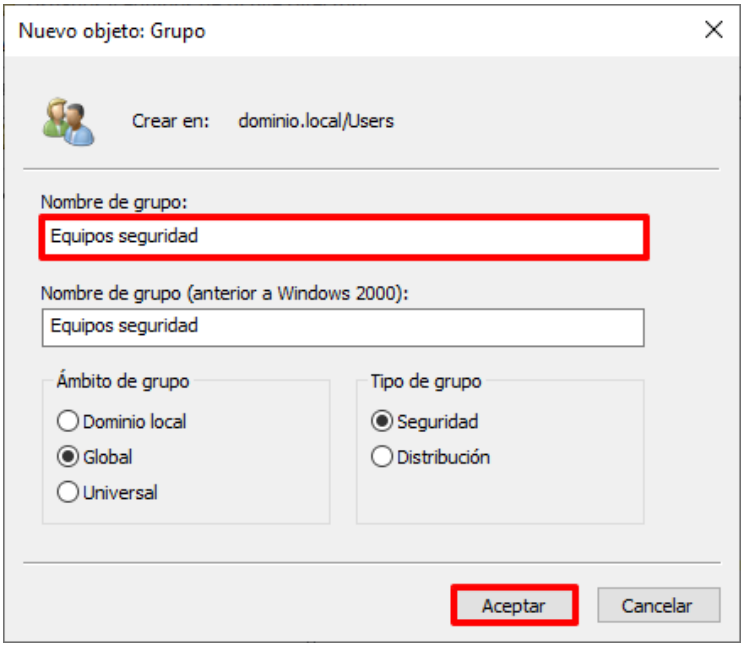
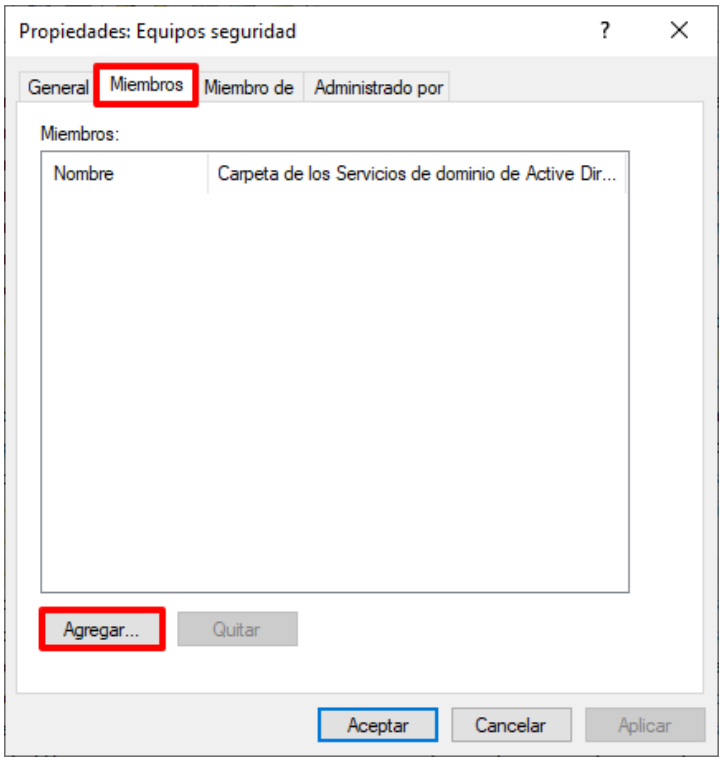
ANEXO A.1.2.2. FILTRADO DE SEGURIDAD DE OBJETOS GPO

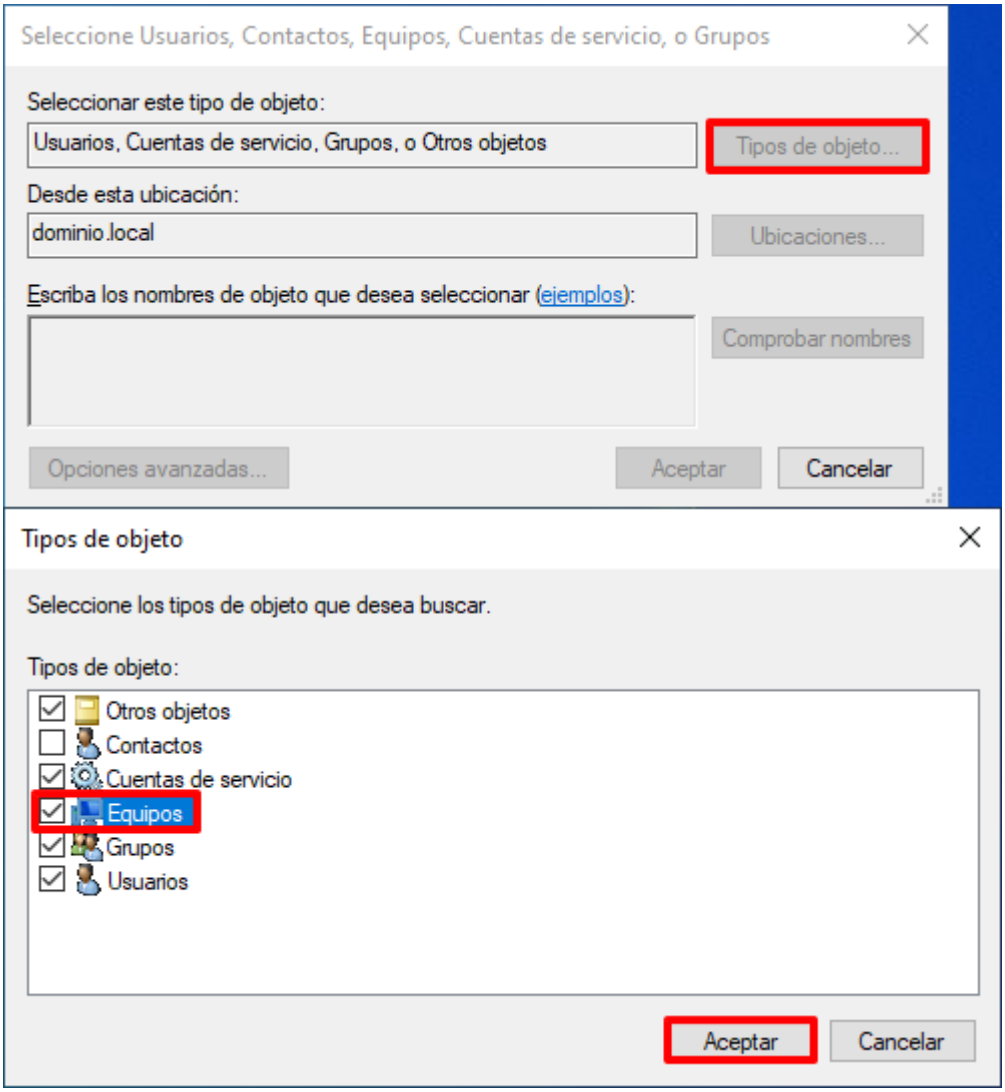
El presente apartado tiene como objetivo realizar una creación de un grupo de seguridad sobre el que aplicar el objeto GPO. Esto permitirá que solo se aplique el objeto GPO a los objetos incluidos dentro de dicho grupo, aunque en la unidad organizativa que se aplica el objeto GPO existan más objetos.

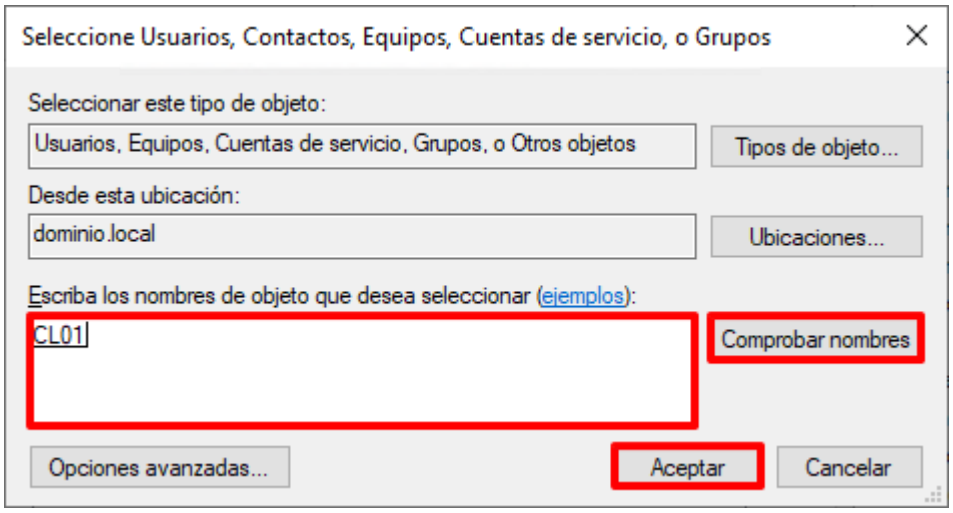
Nota: Estos pasos son opcionales y solo en caso de hacer uso de este tipo de filtrado para la aplicación de objetos GPO.

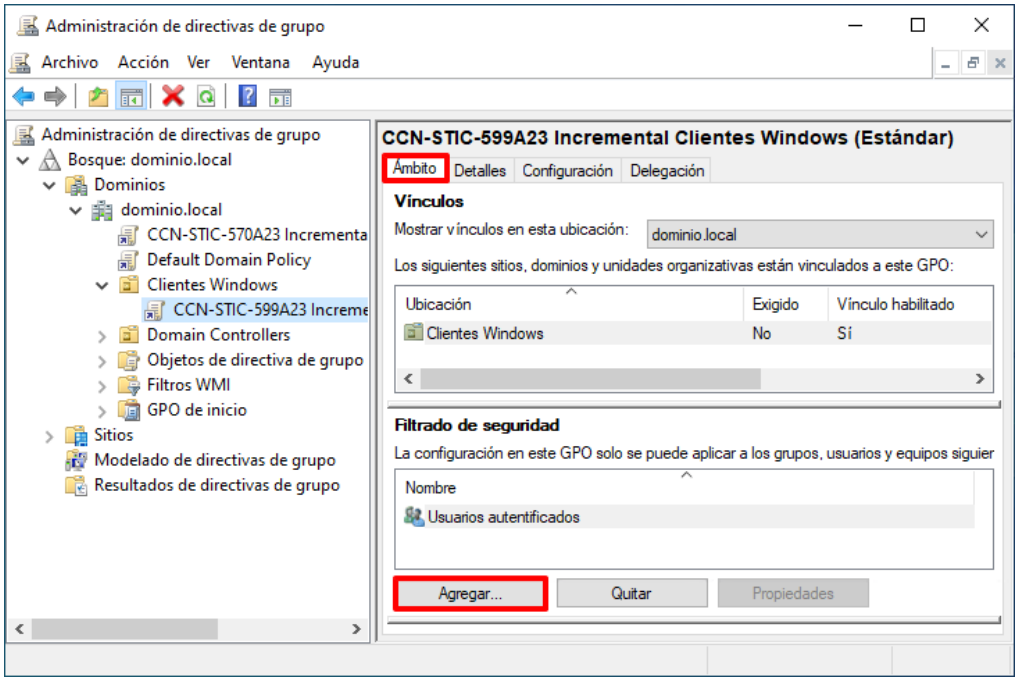
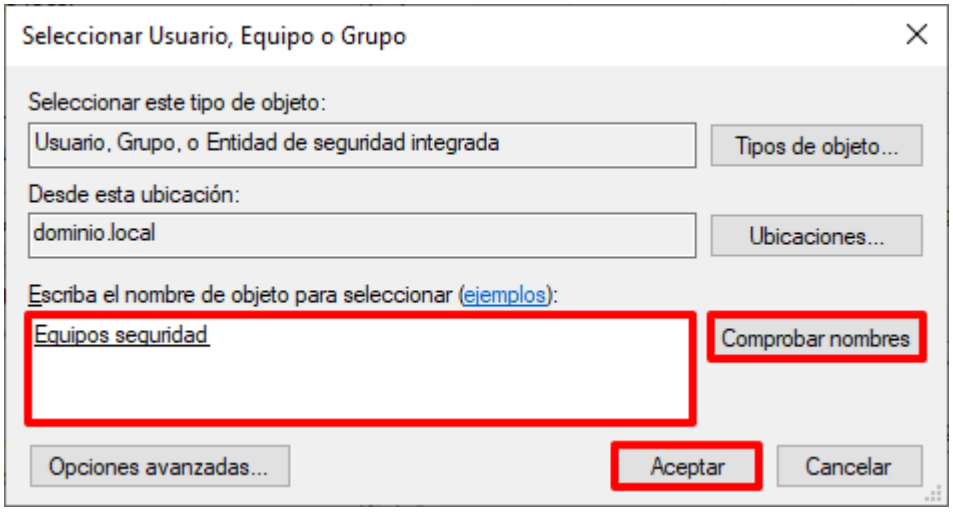
Paso	Descripción
9.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
10.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **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".

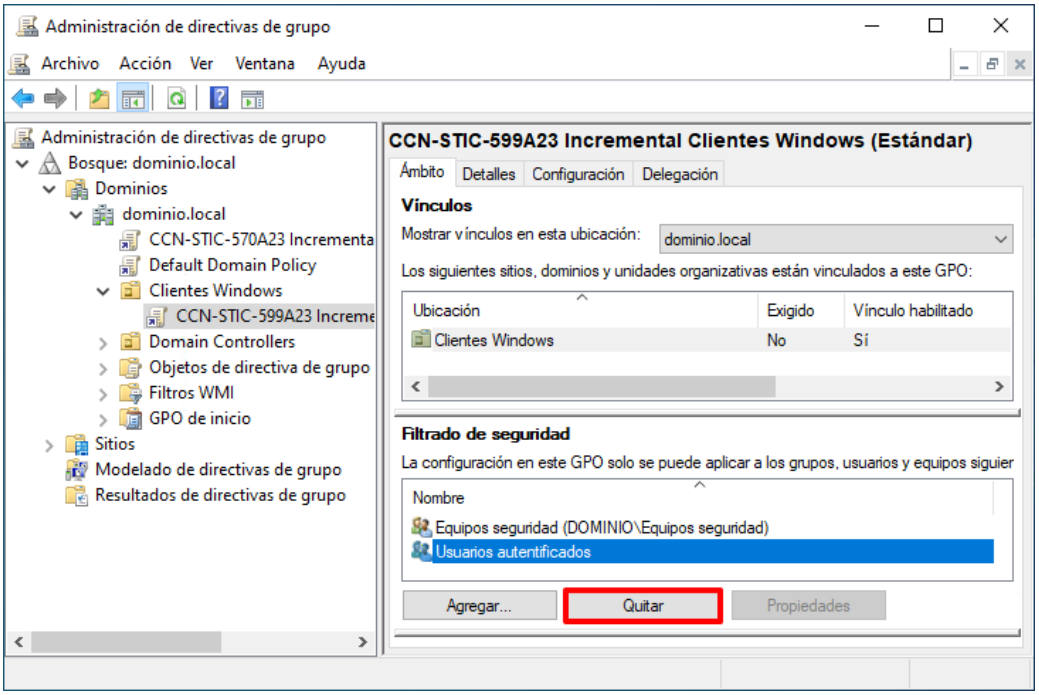
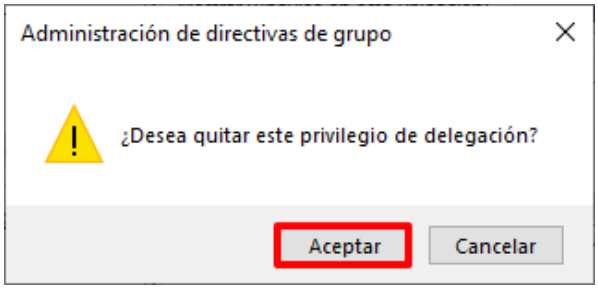
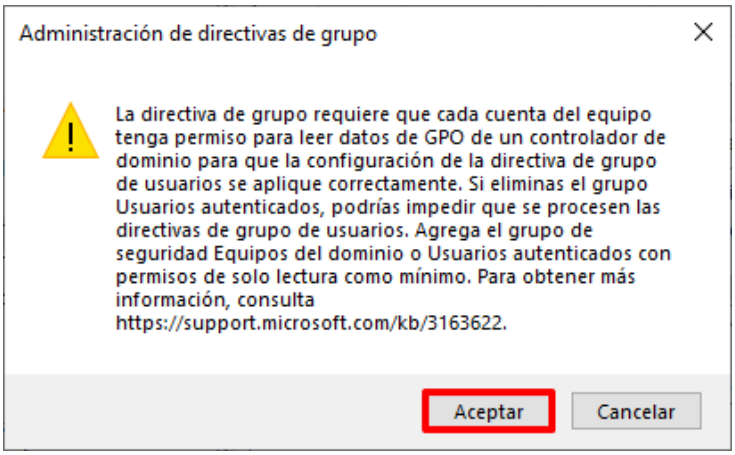
Paso	Descripción
11.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Usuarios y equipos de Active Directory”. 
12.	En la consola “Usuarios y equipos de Active Directory”, despliegue y seleccione el nodo “<nombre de su dominio> → Users” y haciendo clic derecho 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 "CL01". 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-599A23 Incremental Clientes Windows (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. 
22.	Pulse de nuevo sobre el botón “Aceptar” ante el siguiente mensaje de advertencia. 

ANEXO A.1.2.3. SEGREGACIÓN DE FUNCIONES Y TAREAS (USO OFICIAL – MATERIAS CLASIFICADAS)

A continuación, se definirán las acciones para disponer de una adecuada segregación de funciones dentro de los sistemas operativos Windows Cliente, con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

Es un requisito previo necesario haber **realizado el paso a paso del anexo homónimo en el documento "CCN-STIC-570A23 Perfilado de seguridad para Windows Server"**. Si no ha seguido dicho apartado en el documento indicado, los siguientes pasos no podrán ser llevados a cabo de forma óptima.

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.

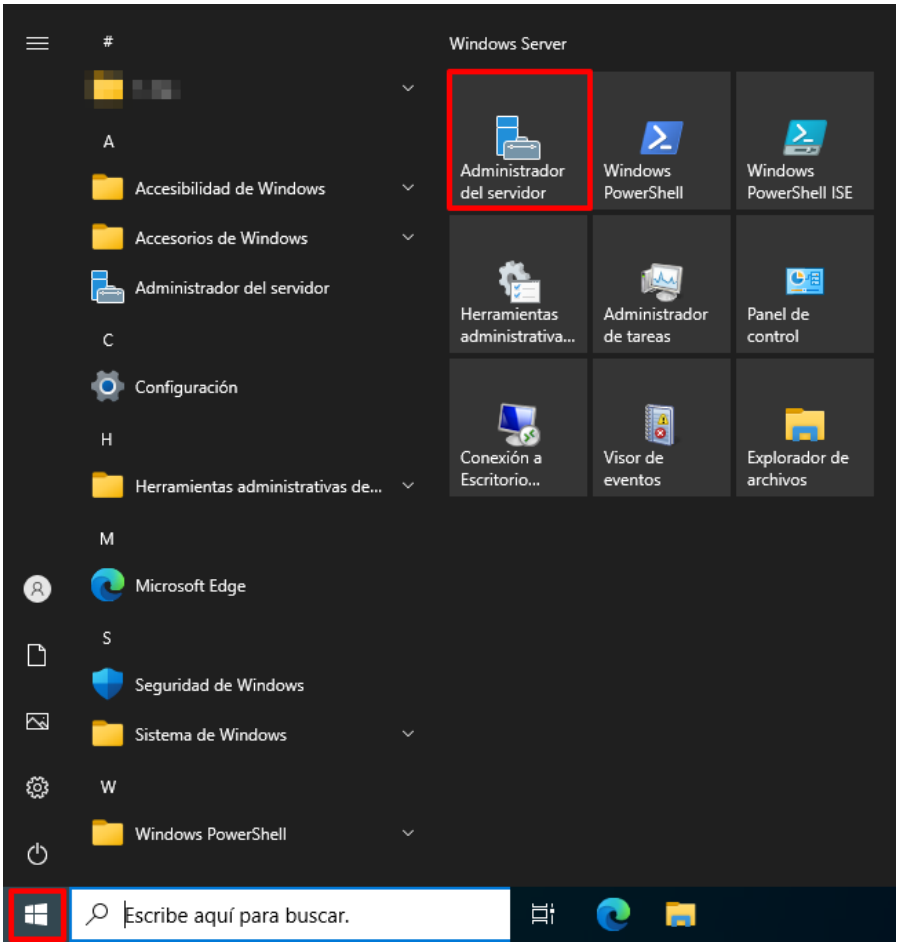
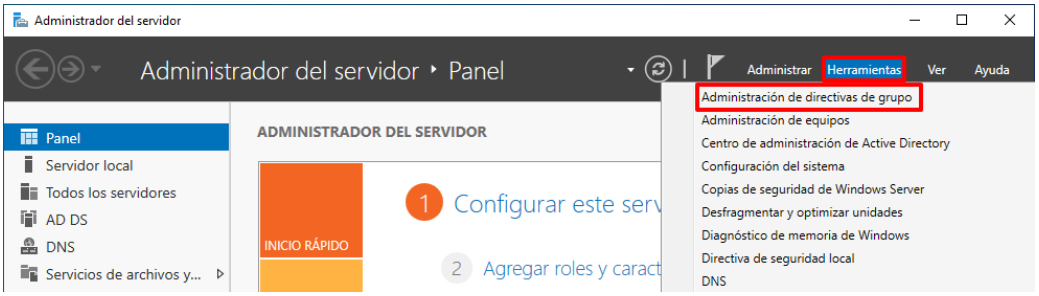
Los pasos que permiten realizar la siguiente segregación de funciones se disponen a continuación:

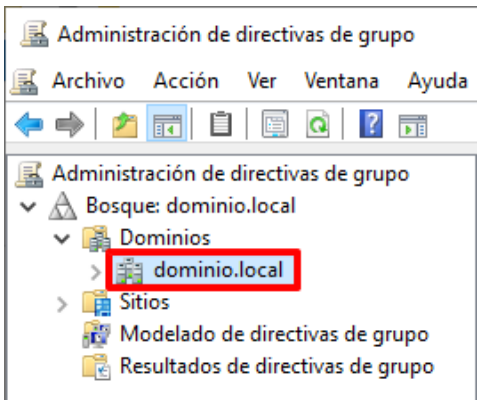
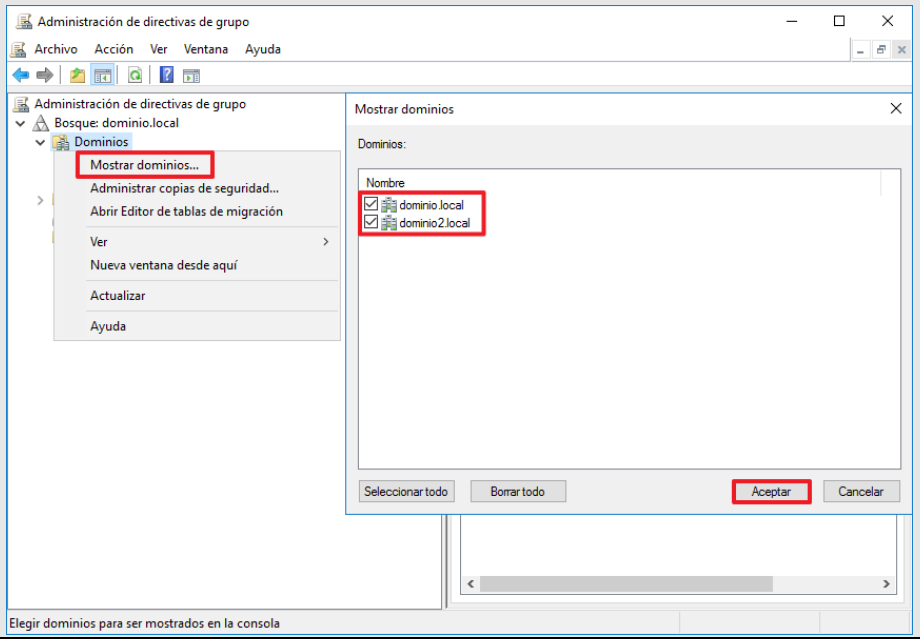
a) Revisión del registro de eventos.

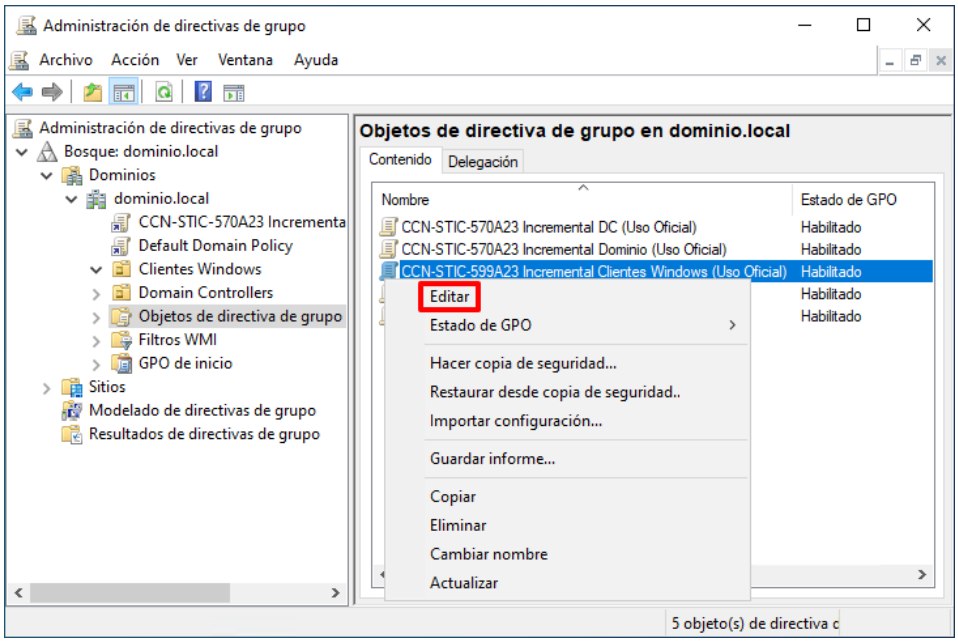
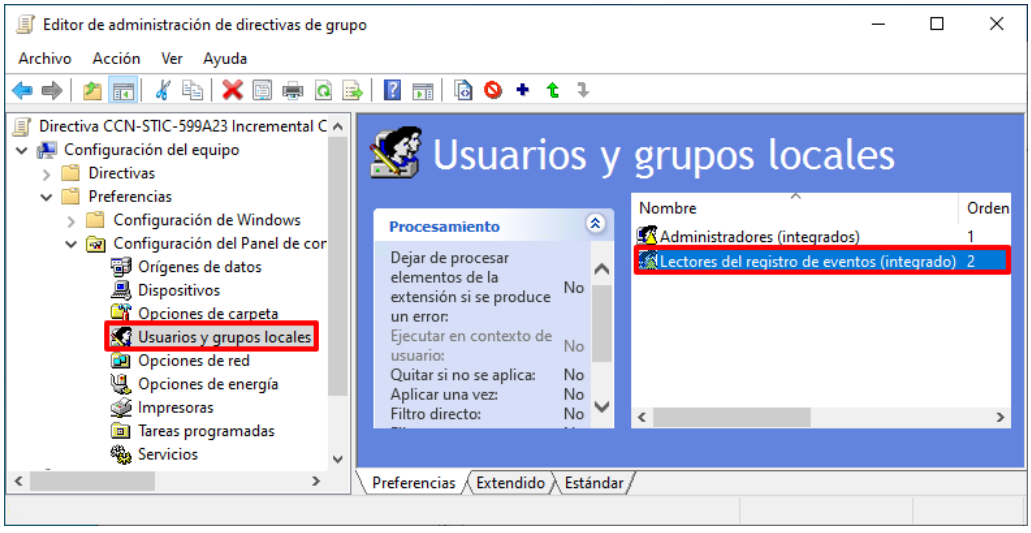
b) Operación de mantenimiento.

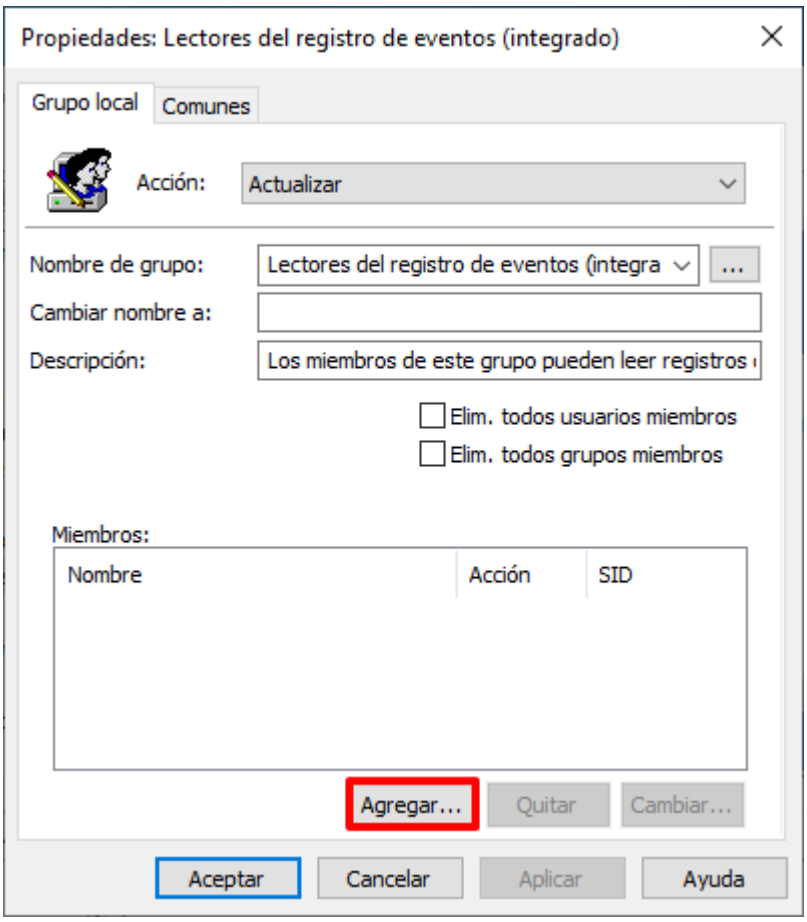
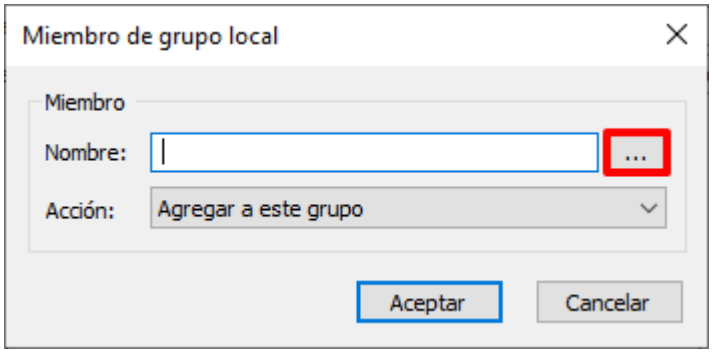
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

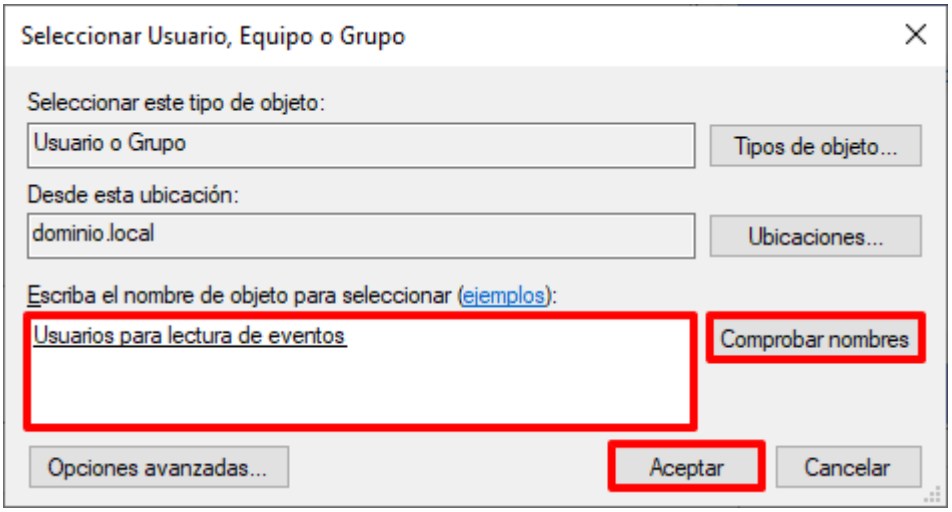
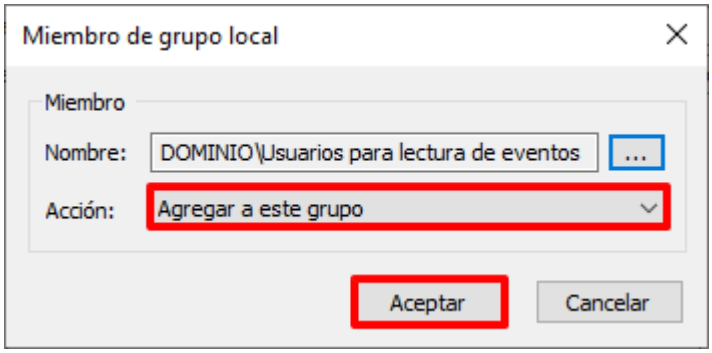
Paso	Descripción
23.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

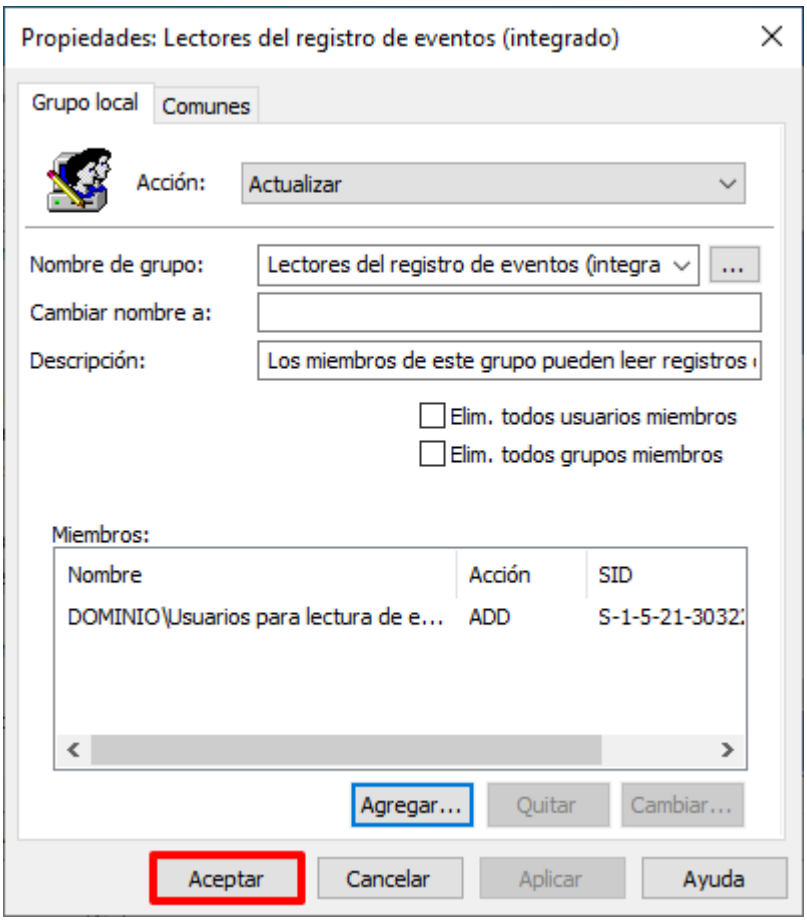
Paso	Descripción
24.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

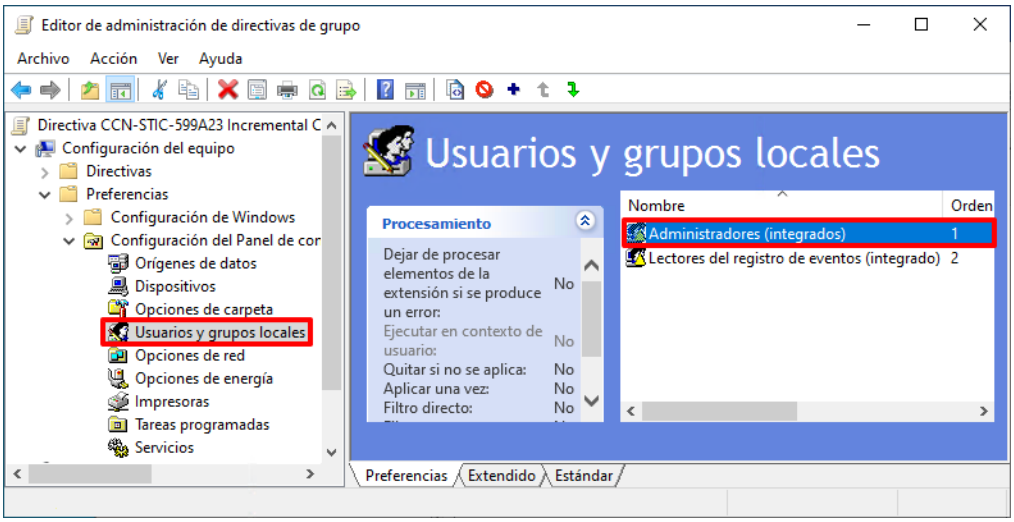
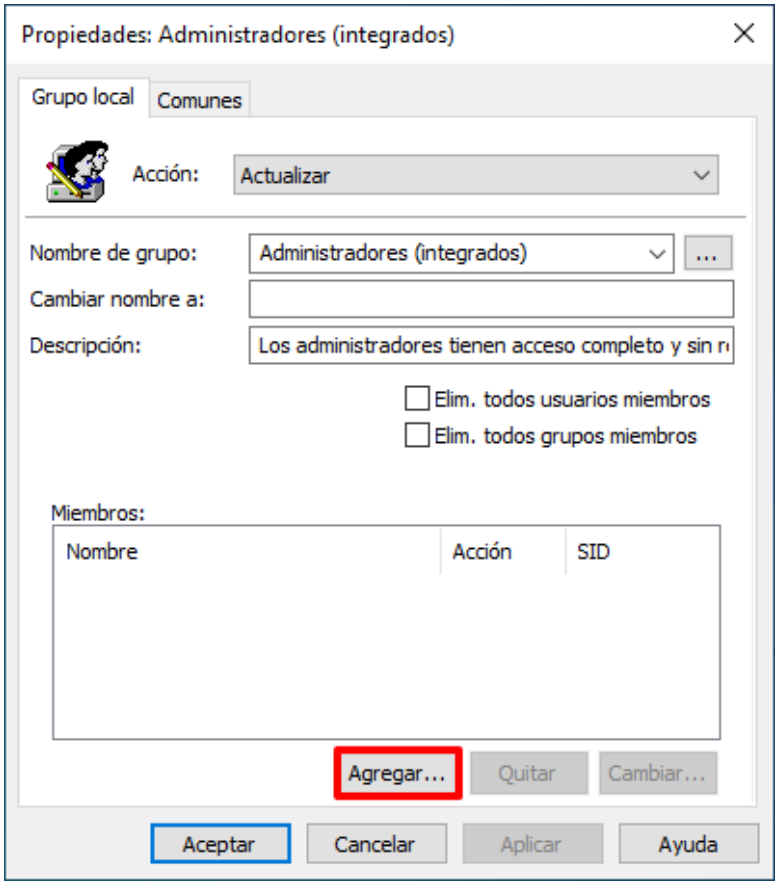
Paso	Descripción
26.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

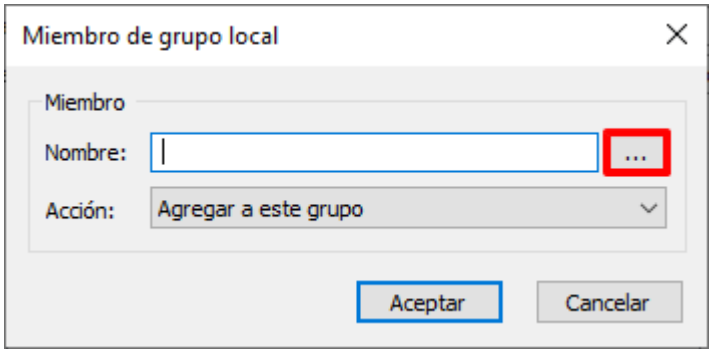
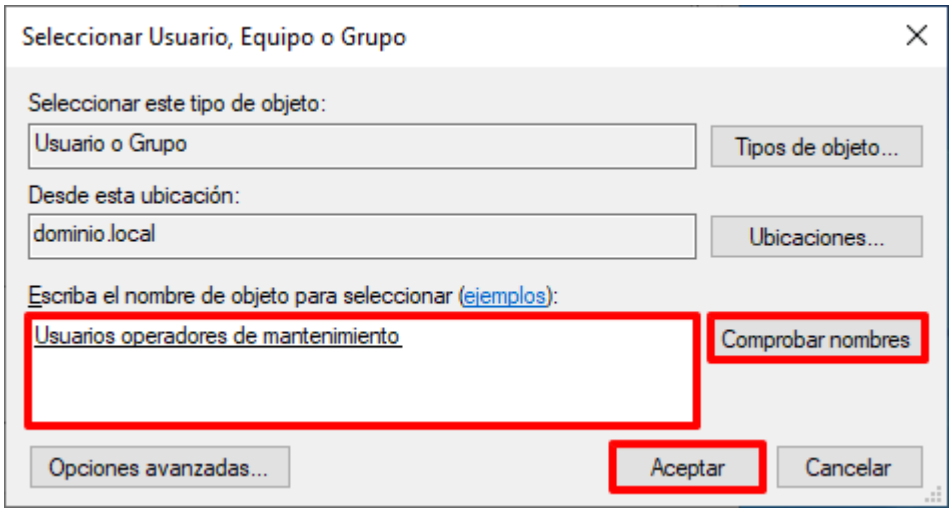
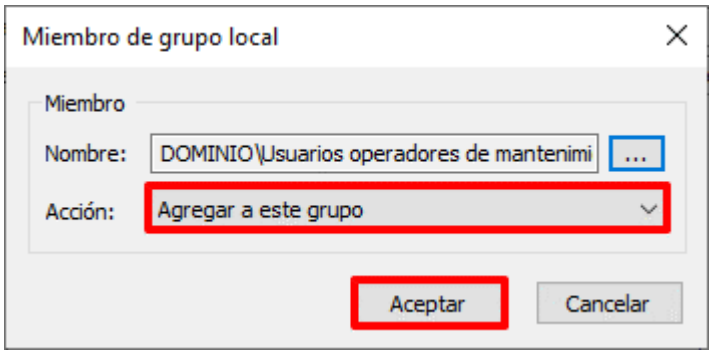
Paso	Descripción
27.	Seleccione con el botón derecho el objeto GPO “CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO])”, y elija la opción "Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Uso Oficial”.
28.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([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. 

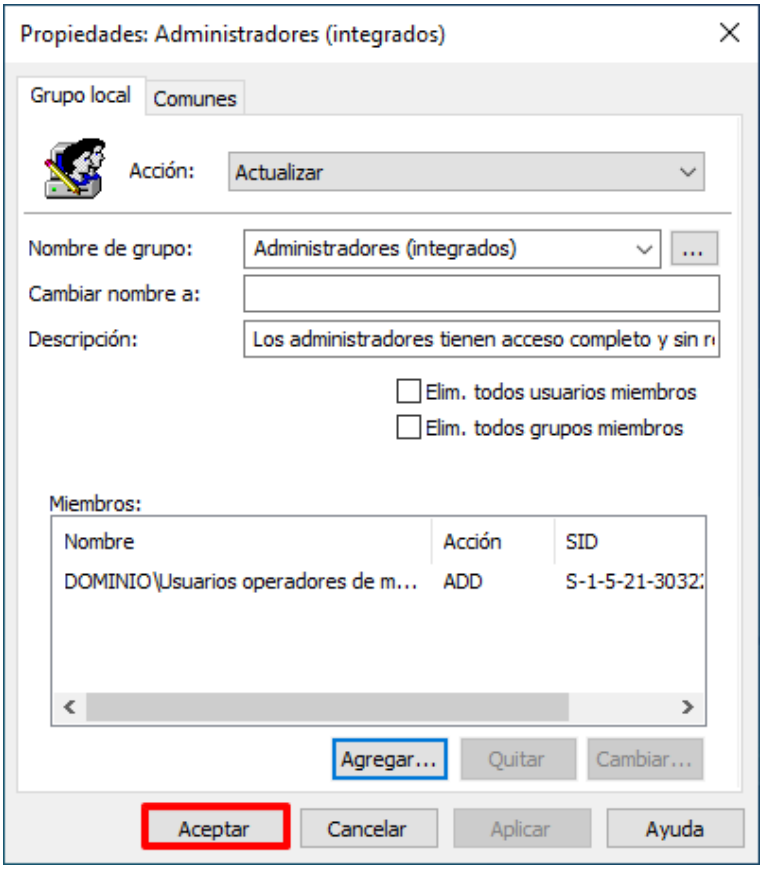
Paso	Descripción
29.	Pulse sobre el botón “Agregar…” para continuar. 
30.	En la nueva ventana emergente pulse sobre el botón “…”. 

Paso	Descripción
31.	Escriba el nombre del grupo que desea incluir en el grupo integrado “Lectores del registro de eventos”. En este ejemplo, se utilizará el grupo “Usuarios para lectura de eventos”, generado mediante el paso a paso del documento codificado como “CCN-STIC-570A23”. Pulse sobre “Comprobar nombres” para completar el nombre y pulse “Aceptar”. 
32.	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
33.	Para finalizar, pulse de nuevo sobre el botón de “Aceptar”. 
34.	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
35.	De nuevo, en la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-599A23 Incremental Clientes Windows ([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. 
36.	Pulse sobre el botón "Agregar…" para continuar. 

Paso	Descripción
37.	En la nueva ventana emergente pulse sobre el botón "…". 
38.	Escriba el nombre del grupo que desea incluir en el grupo integrado "Administradores". En este ejemplo, se utilizará el grupo "Usuarios operadores de mantenimiento", generado mediante el paso a paso del documento codificado como "CCN-STIC-570A23". Pulse sobre "Comprobar nombres" para completar el nombre y pulse "Aceptar". 
39.	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
40.	Para finalizar, pulse de nuevo sobre el botón de “Aceptar”. 
41.	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 Cliente 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.

ANEXO A.1.2.4. CONFIGURACIÓN DE SEGURIDAD

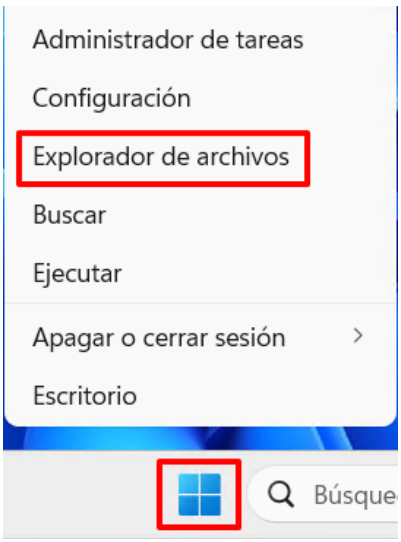
En el presente apartado, se definirán los pasos y acciones que tienen como objetivo cumplir la regla de “mínima funcionalidad”.

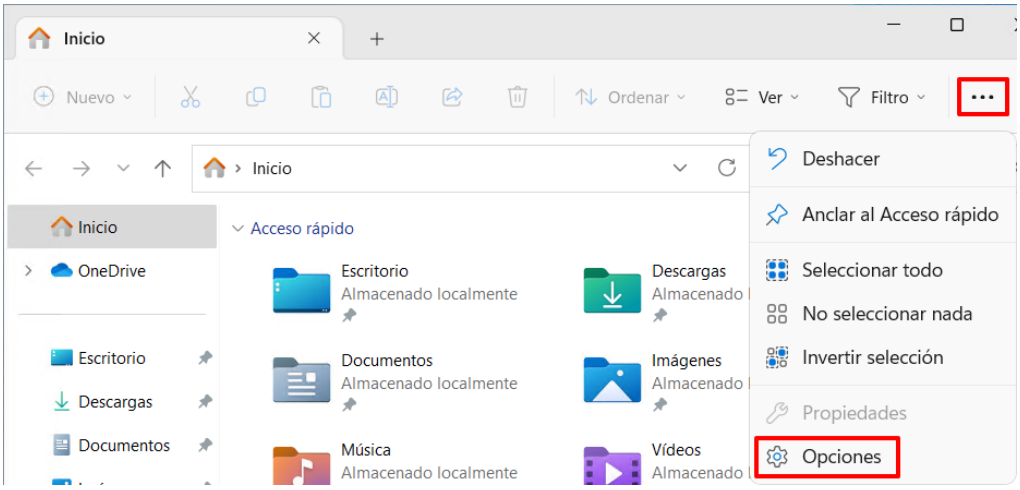
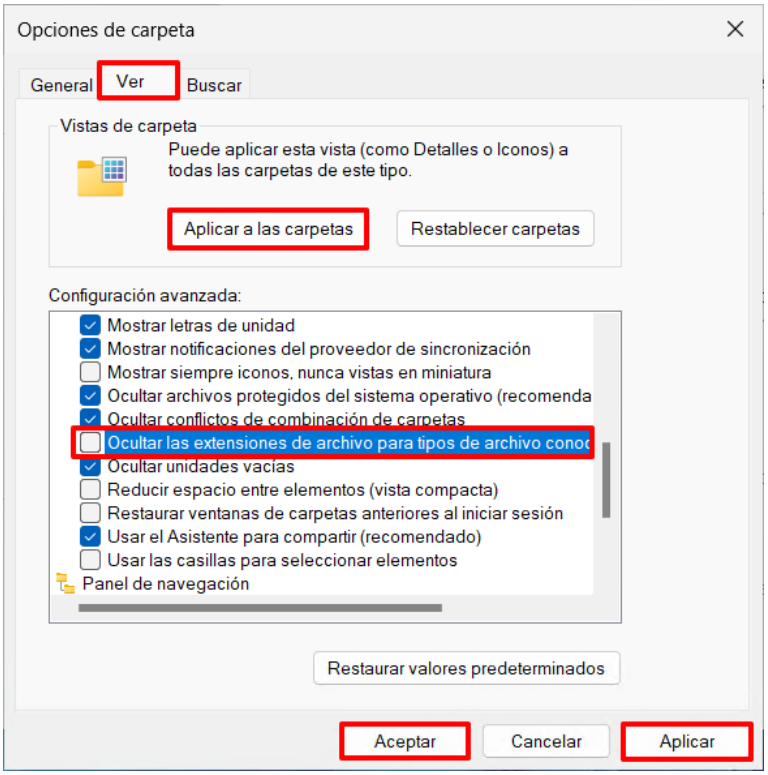
Para lograr el objetivo anterior se describen dos alternativas:

a) Por un lado, se facilitarán varios scripts que permitan desinstalar aquellas características y aplicaciones aprovisionadas consideradas no necesarias dentro de un equipo de tipo Cliente Miembro de un dominio.

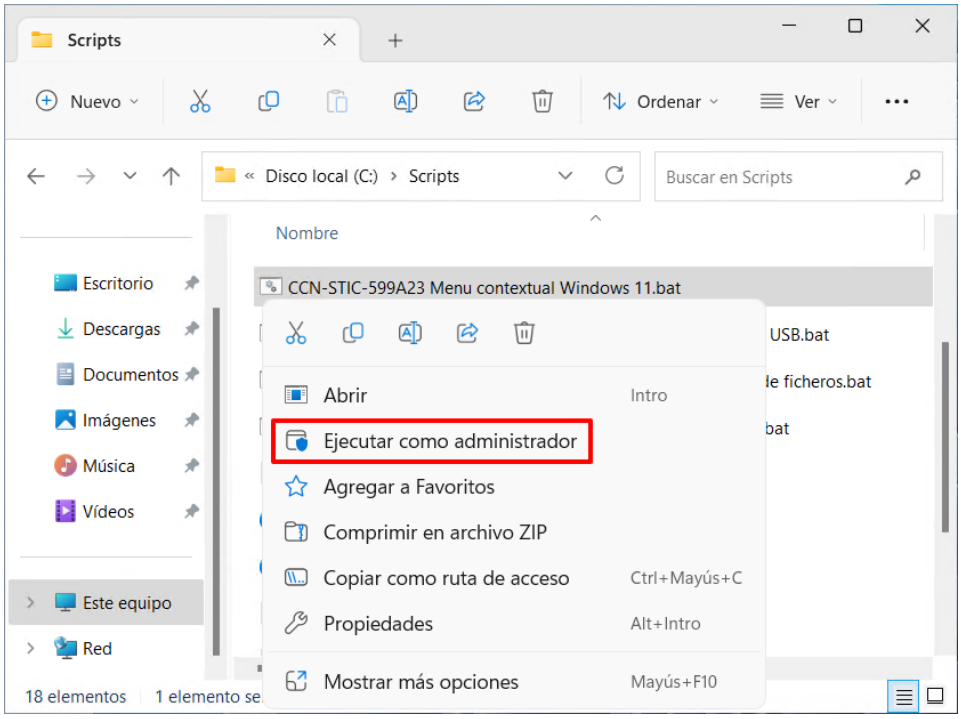
b) Por otra parte, se facilitará un paso a paso con información sobre como desinstalar características de forma gráfica y manual.

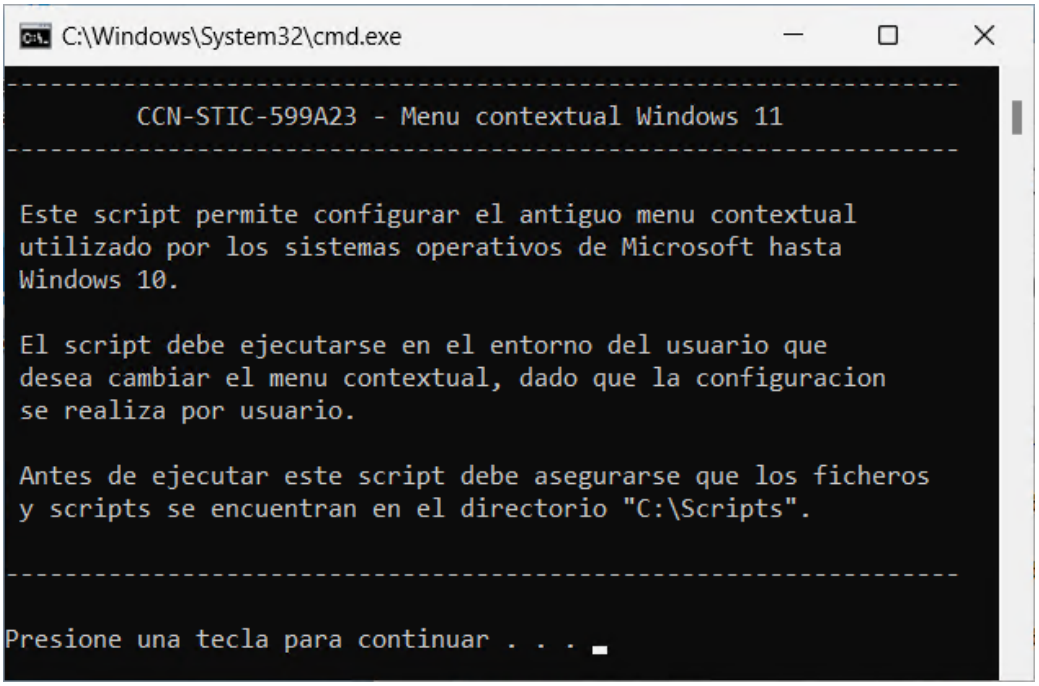
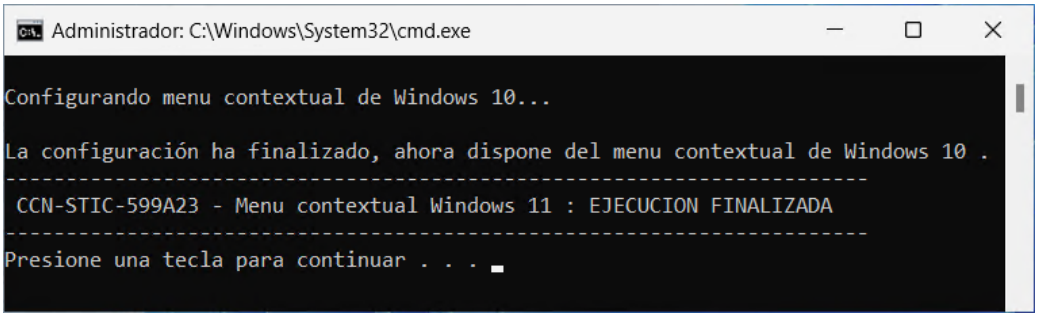
De forma preliminar a la configuración de seguridad, es necesario seguir los pasos que se describen a continuación, con el objetivo de poder llevar a cabo tanto los pasos del presente apartado como los siguientes. Solo es necesario realizar este procedimiento una (1) vez por Cliente Miembro a configurar.

Paso	Descripción
42.	Inicie sesión en un cliente miembro del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
43.	Cree el directorio “Scripts” en la unidad C:\.
44.	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-599AB23\CLIENTES MIEMBRO”.
45.	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
46.	En el "Explorador de archivos" pulse sobre el botón "…" del menú superior y seleccione el icono de "Opciones". 
47.	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". 

48.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del cliente miembro del dominio: – ESTANDAR/USO OFICIAL/MATERIAS CLASIFICADAS • CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-599A23 Incremental Actualizaciones WU [Directorio] • CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-599A23 Incremental Control Dispositivos [Directorio] • CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO]) [Directorio] • CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).inf • CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).wfw • CCN-STIC-599A23 Incremental Actualizaciones WU.inf • CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]).inf • CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]).wfw • CCN-STIC-599A23 Incremental Control Dispositivos.inf • CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO]).inf • CCN-STIC-599A23 Incremental BitLocker [Directorio] (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) • CCN-STIC-599A23 Incremental BitLocker.inf (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) – CCN-STIC-599A23 Cliente Miembro – Desinstalar características.bat – CCN-STIC-599A23 Cliente Miembro – Eliminar aplicaciones aprovisionadas.bat – CCN-STIC-599A23 Menu contextual Windows 11.bat – CCN-STIC-599A23 Windows Defender - Análisis de dispositivos USB.bat – CCN-STIC-599A23 Windows Defender - Análisis de integridad de ficheros.bat – CCN-STIC-599A23 Windows Defender - Análisis en el arranque.bat – CCN-STIC-599A23_Analisis_arranque.ps1 – CCN-STIC-599A23_Analisis_arranque_OS.xml – CCN-STIC-599A23_Analisis_dispositivos_USB.xml – CCN-STIC-599A23_Analisis_USBs.ps1 – CCN-STIC-599A23_Antiguo_menu_contextual.ps1

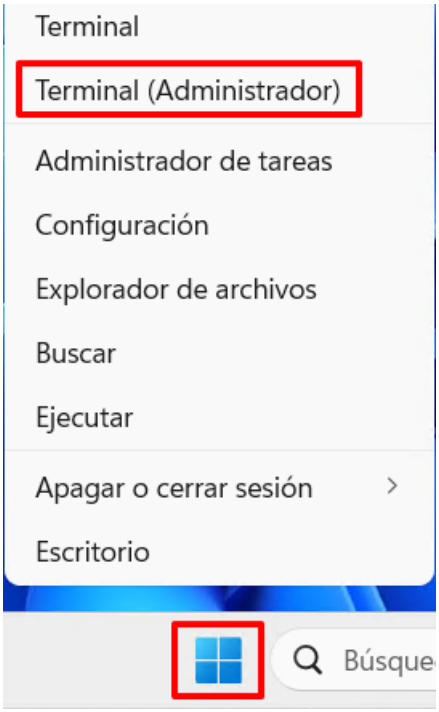
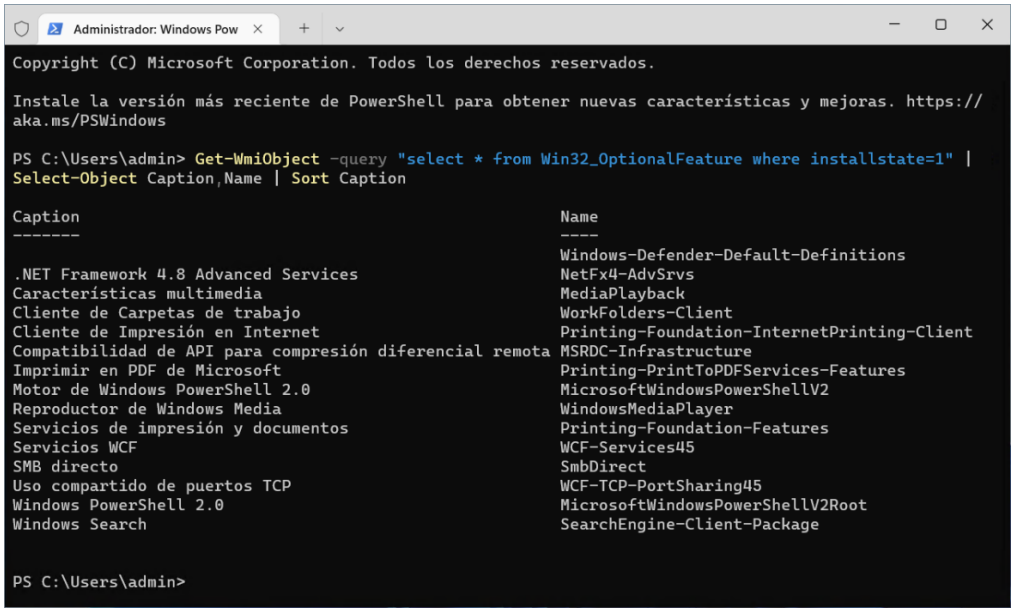
Paso	Descripción
	– CCN-STIC-599A23_Desinstala_caracteristicas.ps1 – CCN-STIC-599A23_Eliminar_aplicaciones_aprovisionadas.ps1 – CCN-STIC-599A23_Habilitar_registro_conexion_USBs.ps1 – CCN-STIC-599A23_Integridad_ficheros.xml
49.	A continuación, diríjase al directorio "C:\Scripts", haga clic derecho sobre el fichero "CCN-STIC-599A23 Menu contextual Windows 11.bat" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** El presente script solamente es necesario ejecutarlo en el caso de que el sistema operativo del cliente miembro del dominio se corresponda con la versión Windows 11. Si su sistema operativo es Windows 10, o si quiere mantener el uso del nuevo menú contextual incluido en Windows 11, vaya al "Paso 52" de este apartado. Tenga en consideración que para la elaboración del presente documento se ha ejecutado el script indicado y en los ejemplos se mostrará el antiguo menú contextual.

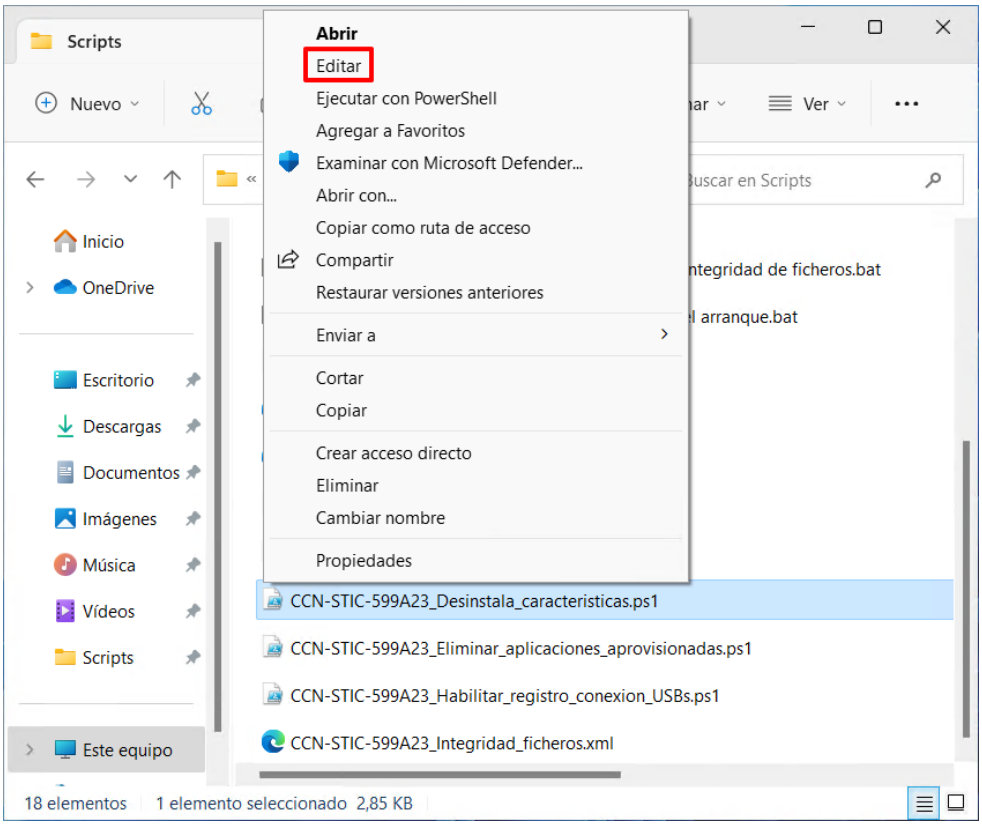
Paso	Descripción
50.	A continuación, se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar. 
51.	Espere a que finalice la ejecución y pulse una tecla para finalizar.  **Nota:** Durante la ejecución del script se reiniciará la interfaz gráfica del sistema.

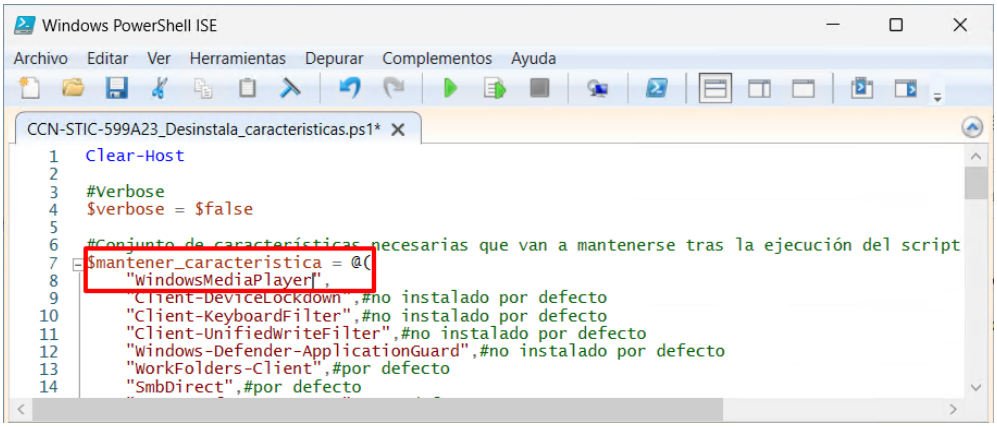
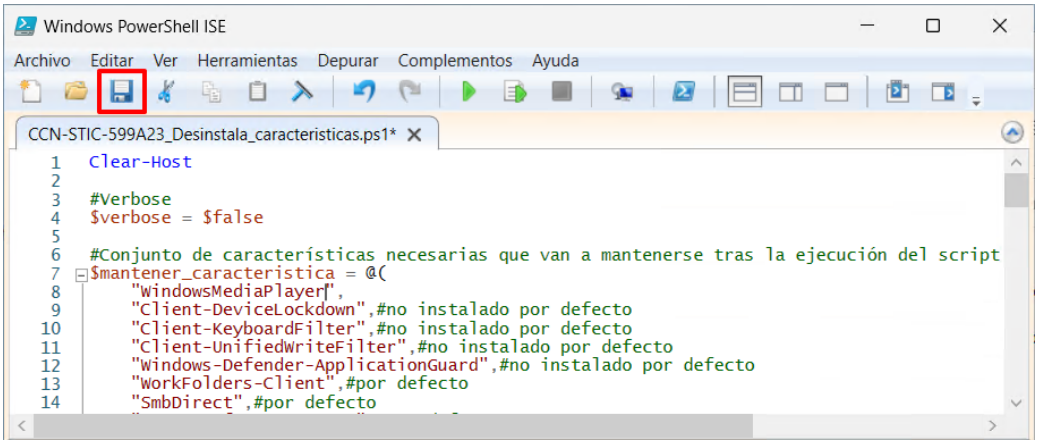
A continuación, se describen los pasos para realizar una desinstalación de características, mediante los scripts correspondientes, implementadas en un equipo de tipo Cliente Miembro.

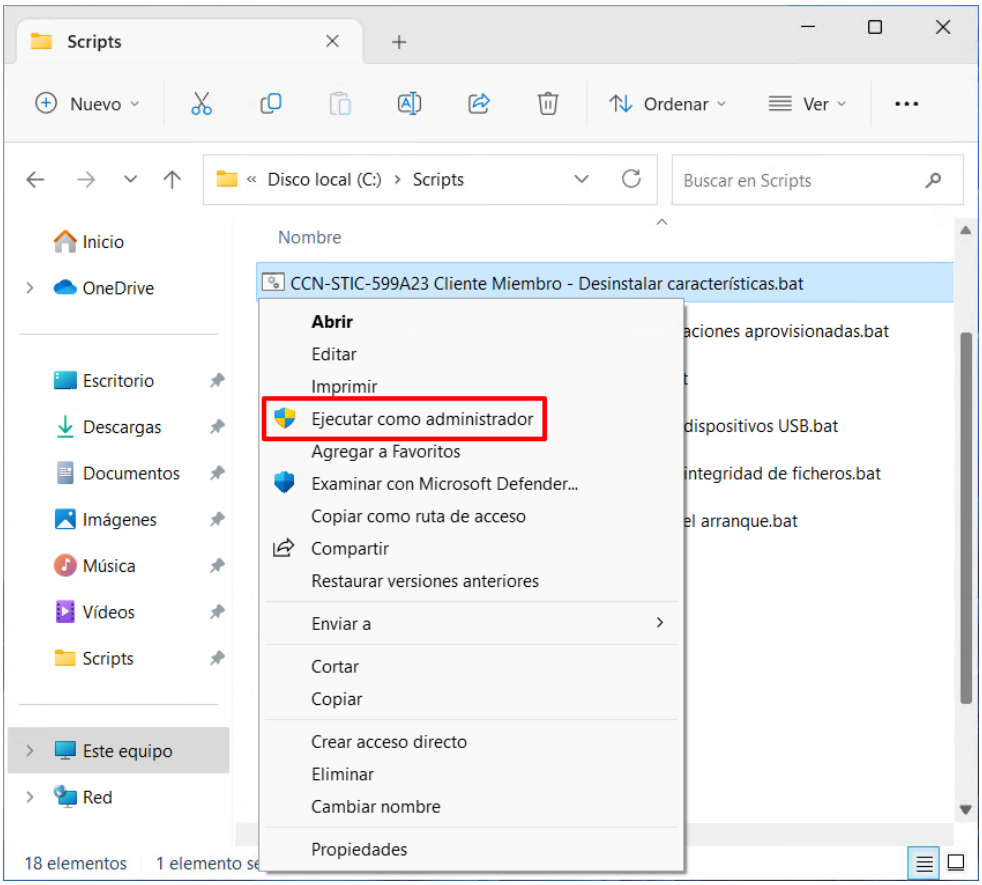
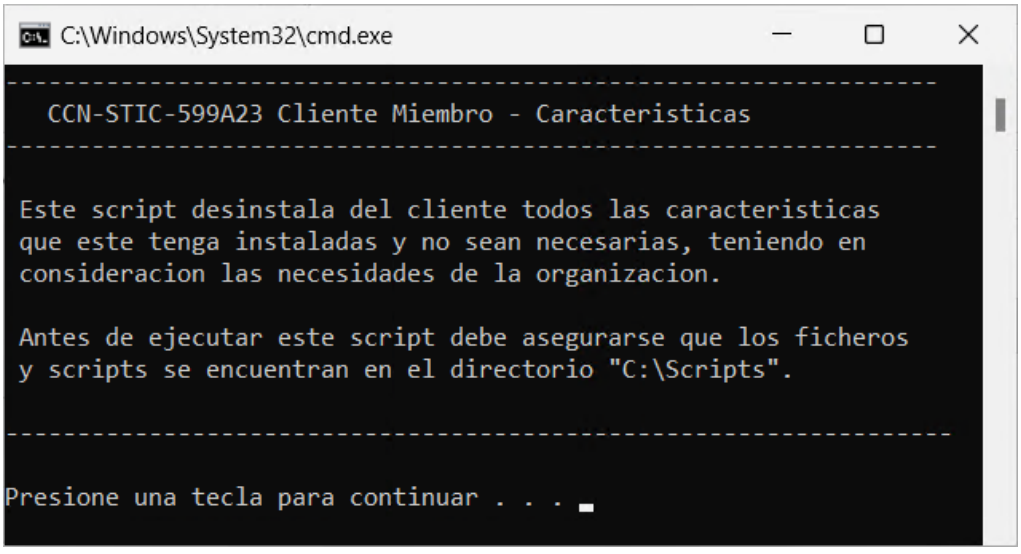
Nota: Si desea solo ejecutar esta acción de forma manual, vaya al “Paso 64” de este apartado.

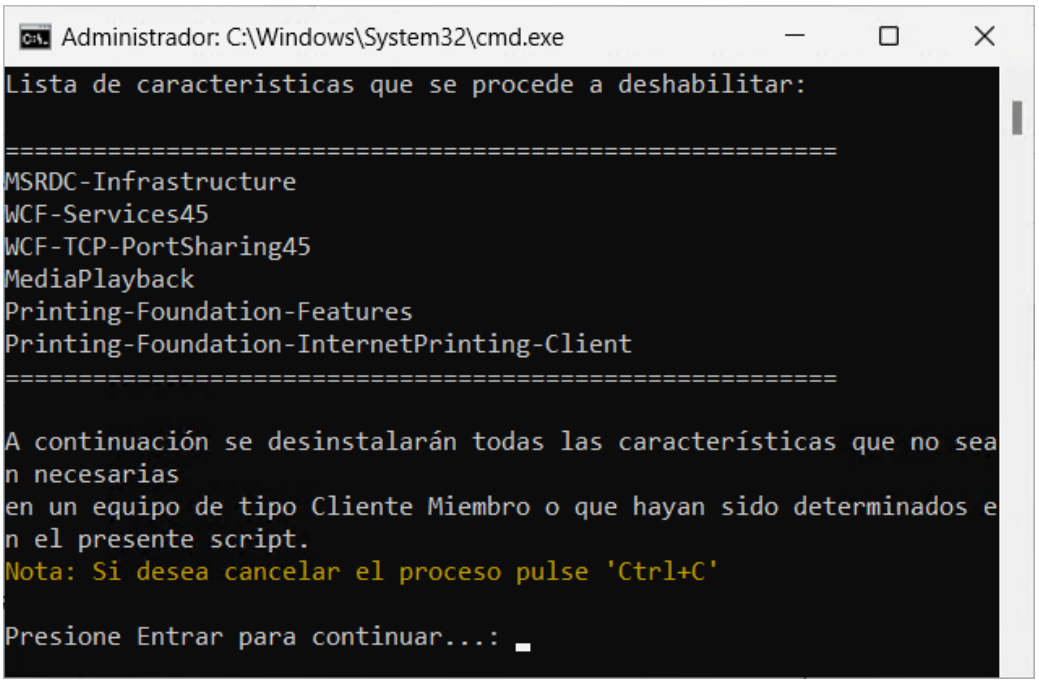
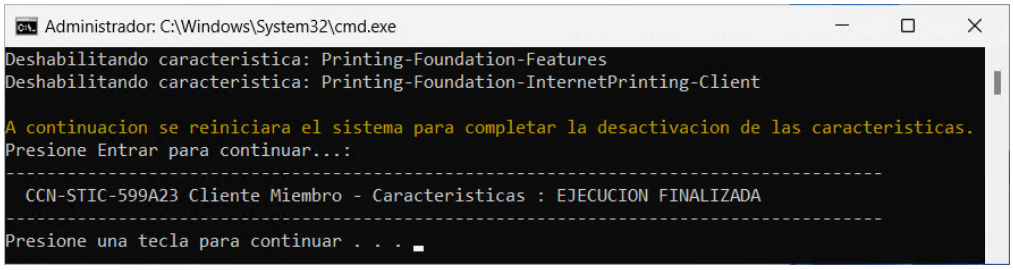
Paso	Descripción
52.	Inicie sesión en un cliente miembro del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
53.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
54.	En la consola de PowerShell ejecute el siguiente comando para conocer aquellas características instaladas en el equipo. > Get-WmiObject -query "select * from Win32_OptionalFeature where installstate= 1" | Select-Object Caption,Name | Sort Caption  **Nota:** Puede redirigir la salida del comando a un fichero si lo desea con el objetivo de evaluar mejor la información mostrada.

Paso	Descripción
55.	A continuación, **EVALÚE** y **DETERMINE** aquellas características **QUE NO SON NECESARIAS ELIMINAR** y anótelas. Deberá anotar los elementos ubicados en la columna “Name”.
56.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-599A23_Desinstala_caracteristicas.ps1” y seleccione la opción del menú contextual “Editar”. Con ello se abrirá una ventana de Windows PowerShell ISE. 

Paso	Descripción
57.	Dentro de la ventana de PowerShell ISE, al inicio del script identifique la línea donde se indica "$mantener_caracteristica". Dentro de la citada línea deberá incluir aquellas características anotadas en pasos anteriores, sin modificar las características que ya vienen incluidas en el script por defecto. Deberá **incluir los nombres entre comillas ("") y separados por comas**.  **Nota:** En este ejemplo se ha incluido la característica "WindowsMediaPlayer". Tenga en consideración que ya existen otras características que ya han sido determinadas como necesarias y no se desinstalarán.
58.	Cuando haya finalizado pulse sobre el botón "Guardar" en la parte superior izquierda y cierre el editor. 

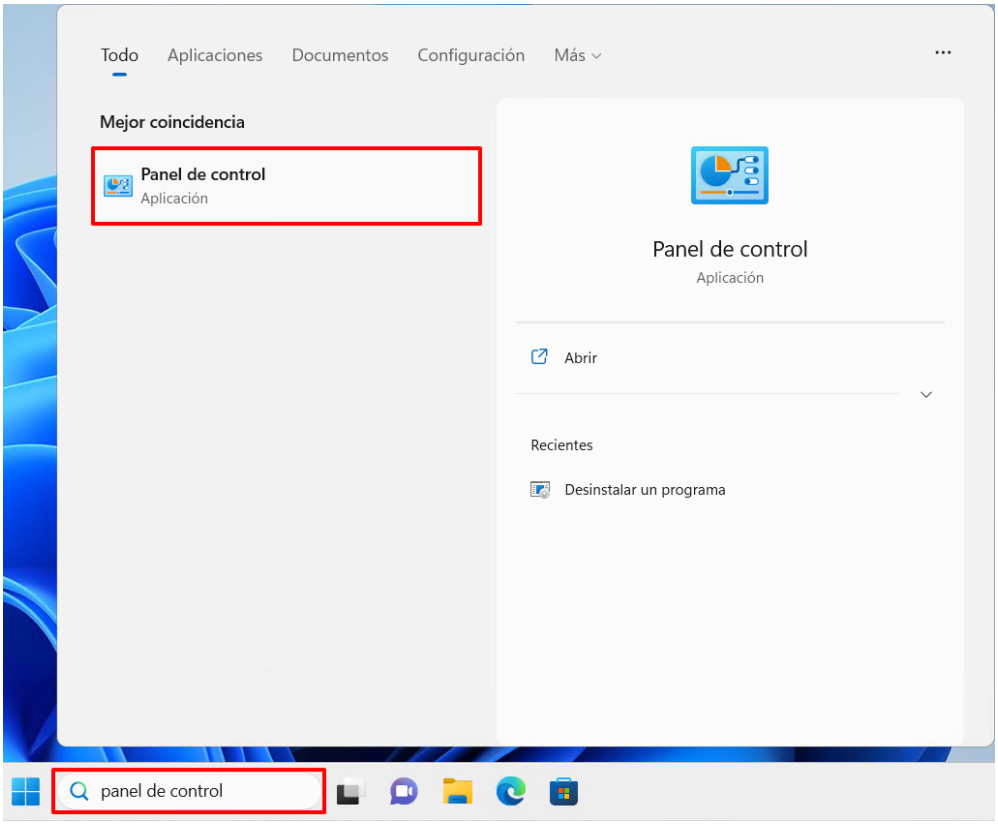
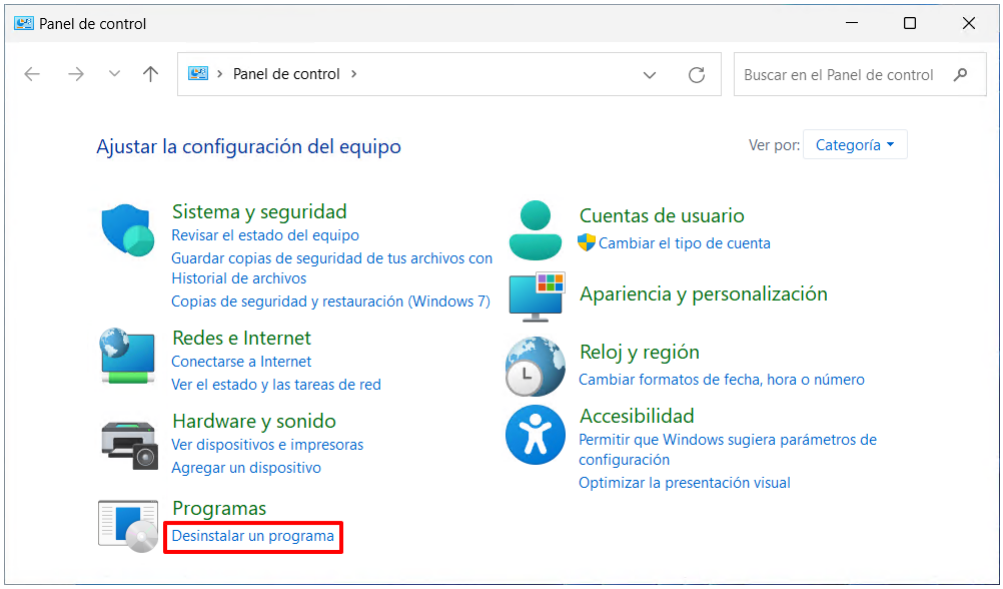
Paso	Descripción
59.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-599A23 Cliente Miembro – Desinstalar características.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
60.	Pulse cualquier tecla para continuar. 

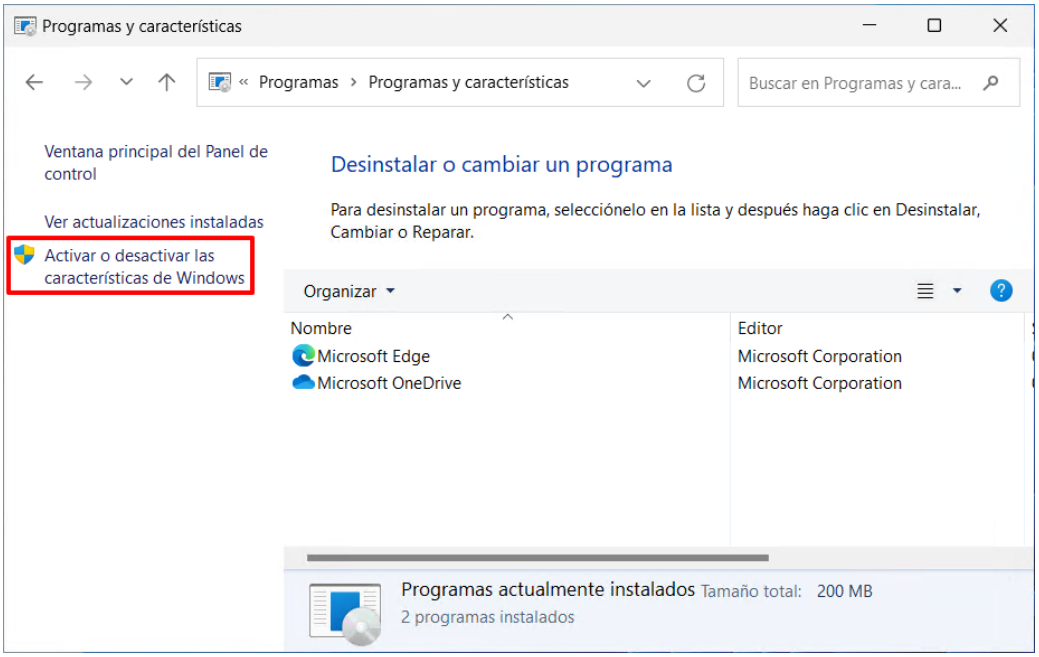
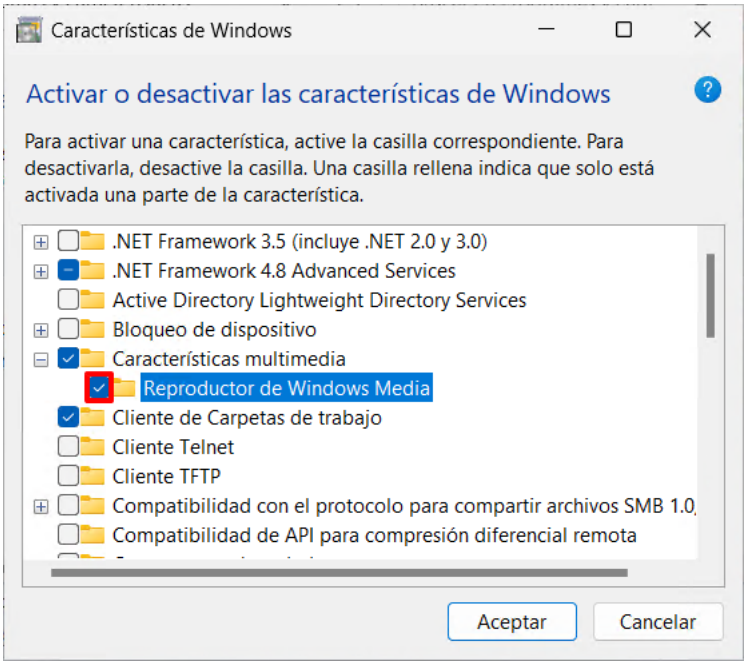
Paso	Descripción
61.	A continuación, se recopilará y mostrarán las características instaladas en el equipo. Deberá pulsar la tecla "Enter" para continuar y dar comienzo a la desinstalación de las características no necesarias. 
62.	El equipo se reiniciará a continuación para asegurar la adecuada desinstalación de características. Pulse de nuevo la tecla "Enter" para aceptar dicho reinicio, posteriormente pulse cualquier tecla para finalizar la ejecución del script. 
63.	Con esto se habrá finalizado la eliminación de características no necesarias en un equipo de tipo Cliente Miembro.

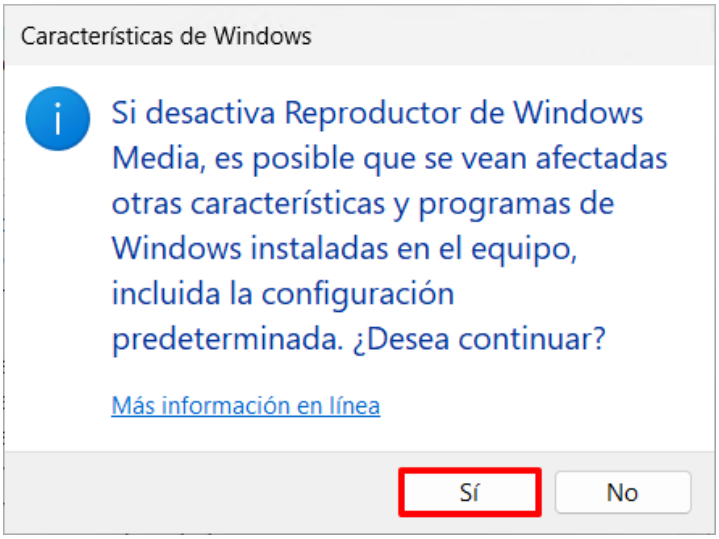
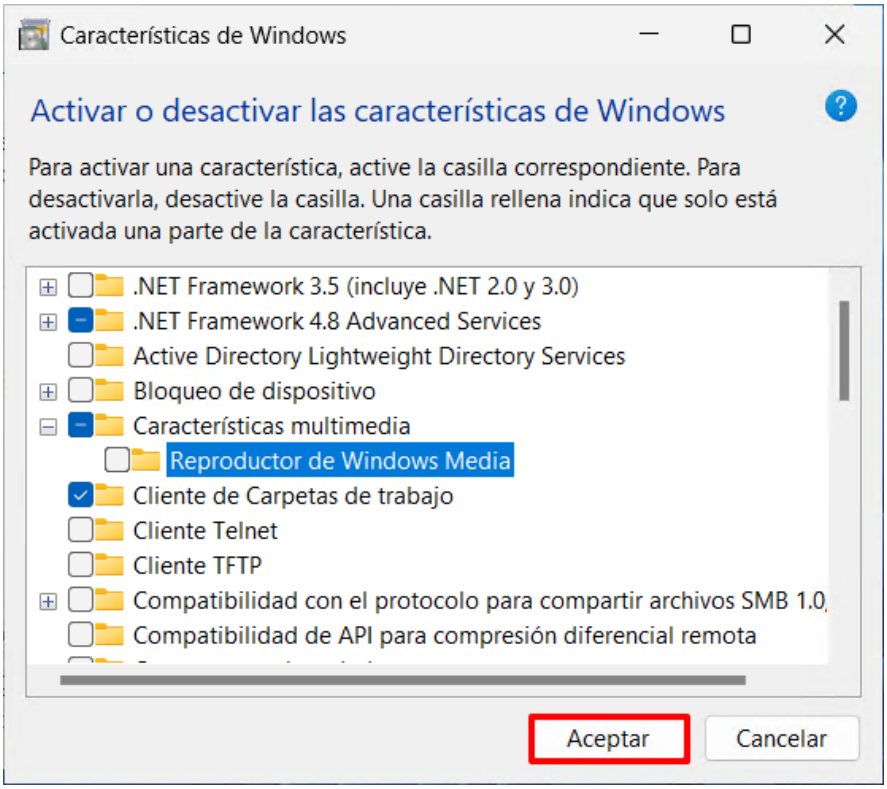
A continuación, se describen los pasos para realizar una desinstalación manual de características implementadas en un equipo de tipo Cliente Miembro.

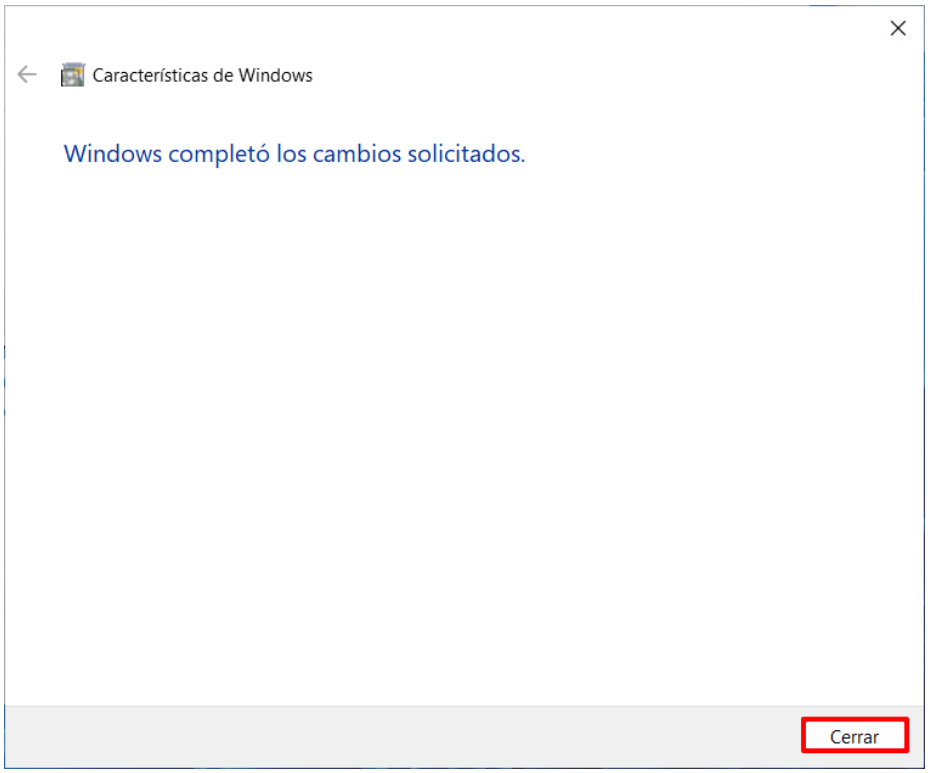
Nota: Para este ejemplo se desinstalará el Reproductor de Windows Media.

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

Paso	Descripción
65.	En el cuadro de búsqueda busque la aplicación “Panel de control” y una vez encontrada, haga clic sobre la misma. 
66.	En la parte inferior izquierda del “Panel de control”, pulse sobre “Desinstalar un programa” en el apartado “Programas”. 

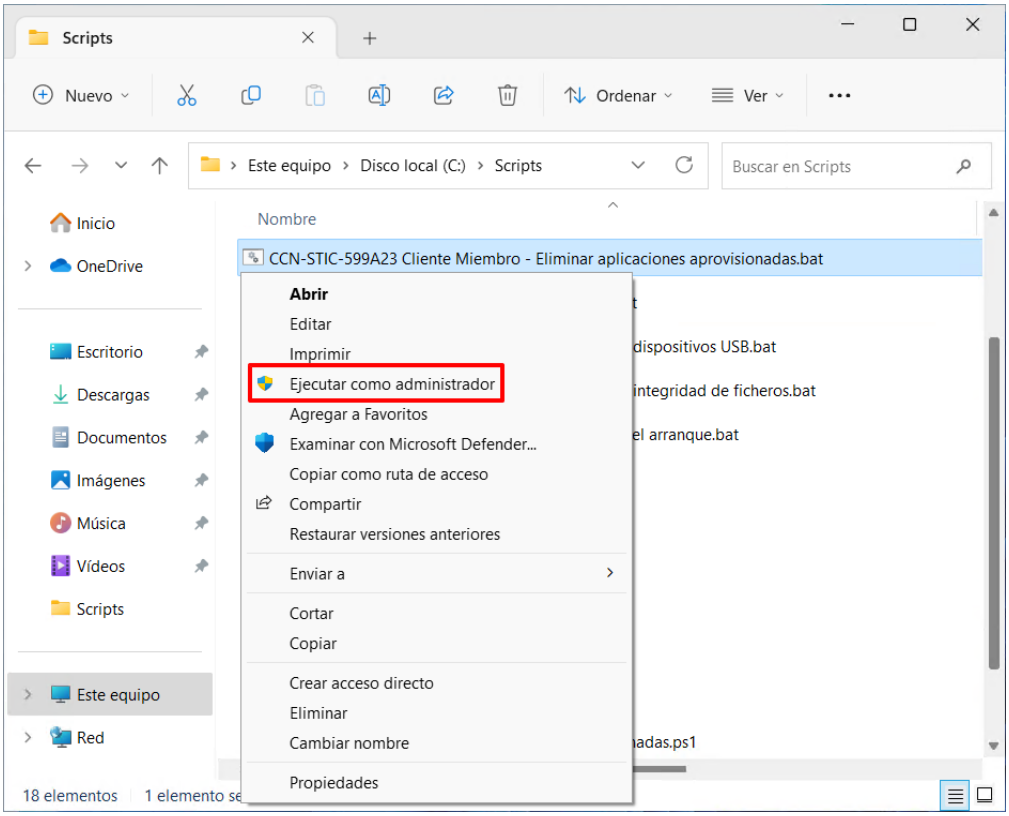
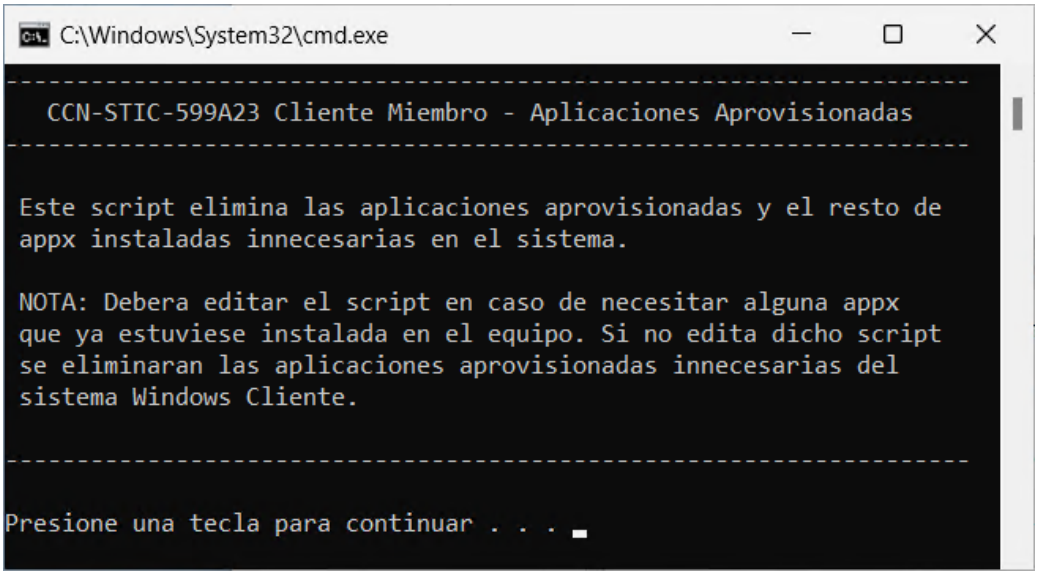
Paso	Descripción
67.	A continuación, seleccione la opción “Activar o desactivar las características de Windows” del menú ubicado en la parte izquierda de la ventana. 
68.	En la nueva ventana emergente, “Activar o desactivar las características de Windows”, identifique aquellas que no son necesarias y desmárquelas.  **Nota:** En este ejemplo se desinstala la característica “Reproductor de Windows Media”.

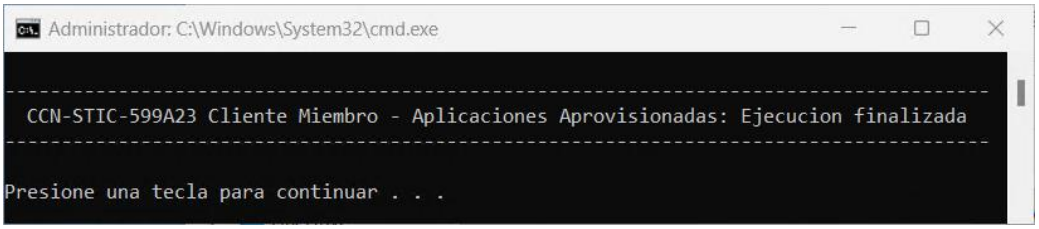
Paso	Descripción
69.	Pulse “Sí” ante el mensaje de advertencia. 
70.	Pulse sobre el botón “Aceptar” para continuar con la desinstalación. 

Paso	Descripción
71.	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. 

A continuación, se describen los pasos para realizar una desinstalación de las aplicaciones aprovisionadas implementadas en un equipo de tipo Cliente Miembro.

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

Paso	Descripción
73.	A continuación, diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-599A23 Cliente Miembro – Eliminar aplicaciones aprovisionadas.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
74.	Pulse cualquier tecla para comenzar con el proceso de desinstalación de aplicaciones aprovisionadas del sistema. 

Paso	Descripción
75.	Espere a que finalice la ejecución y pulse una tecla para finalizar.  **Nota:** En caso de que el sistema muestre errores puede ignorarlos y continuar.

ANEXO A.2. 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.

En caso de que haya configurado las diferentes herramientas mostradas en los siguientes apartados, siguiendo el documento codificado como "CCN-STIC-570A23", en sistemas operativos del tipo Windows Server, **podrá utilizar los mismos objetos GPO generados para dichos sistemas**. Aun así, tendrá que **seguir los siguientes pasos para ejecutar todas las acciones manuales** sobre los equipos del tipo Cliente Miembro.

ANEXO A.2.1. ACCESO REMOTO

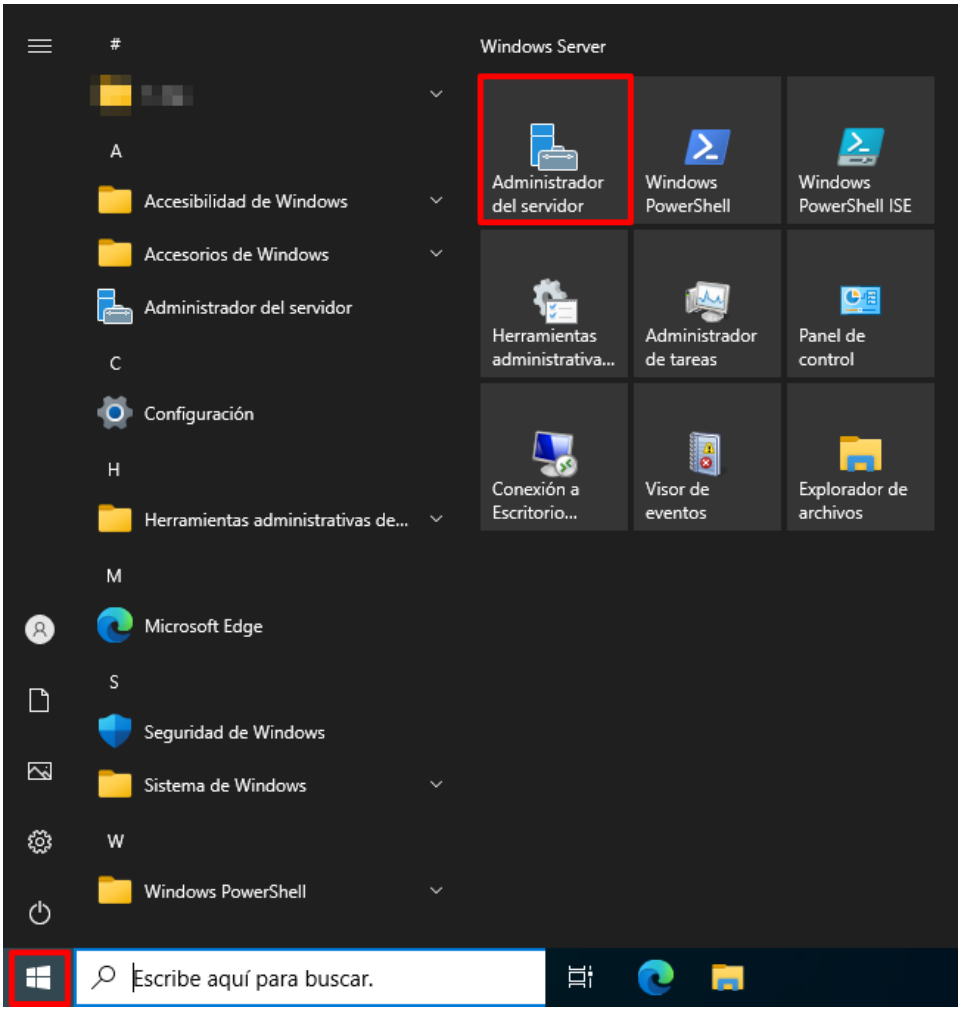
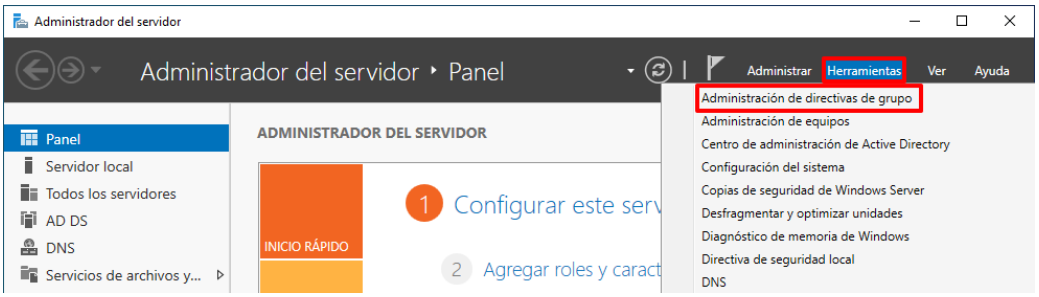
El objetivo del siguiente apartado tiene como misión establecer las configuraciones adecuadas sobre aquellos elementos a los que se les esté permitido el acceso remoto por medio de los elementos nativos de Windows. En este caso se hace referencia a Remote Desktop Connection (RDP).

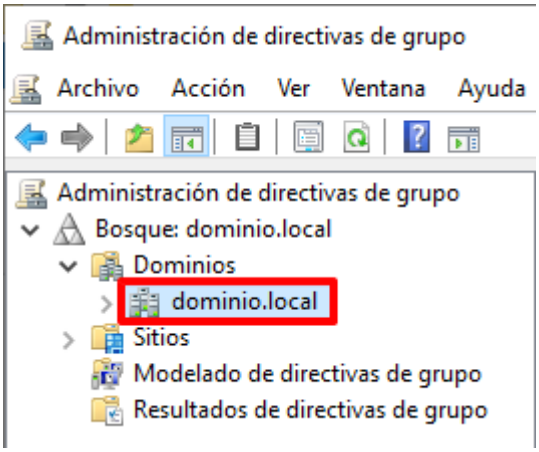
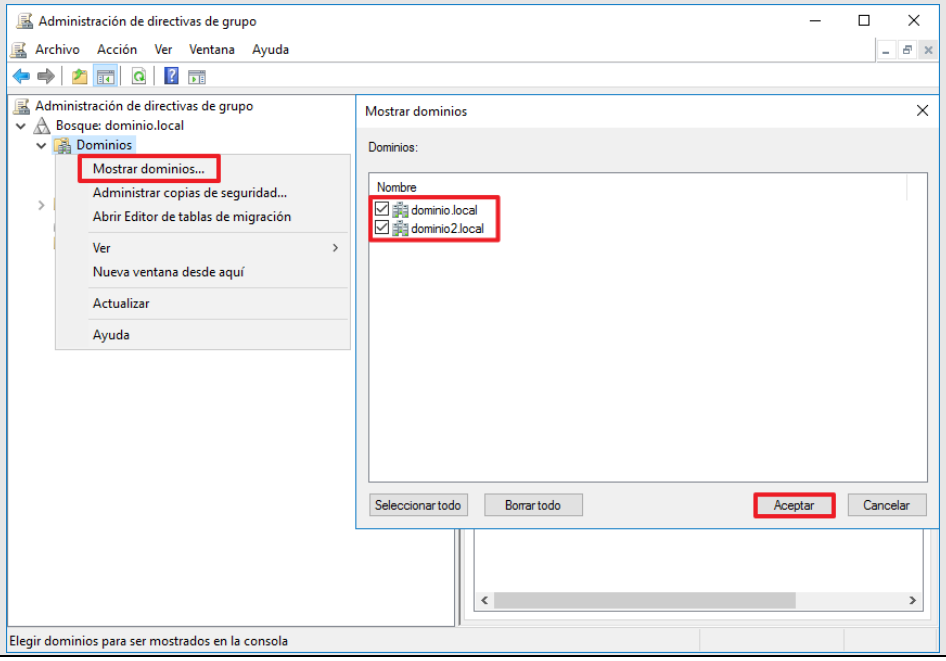
Este sistema de conectividad remota, aunque muy extendido y conocido por los usuarios, no se considera en ningún caso seguro cuando se hace uso de él fuera de un entorno o red local. Por ello, deberán utilizarse elementos adicionales de comunicación y seguridad como una VPN cuando se esté configurando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

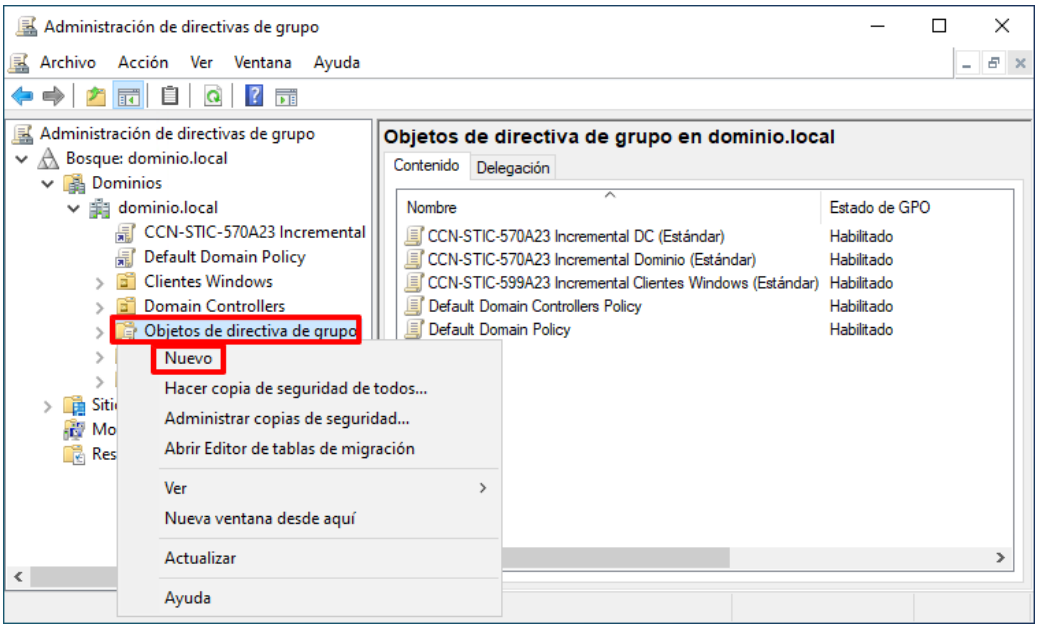
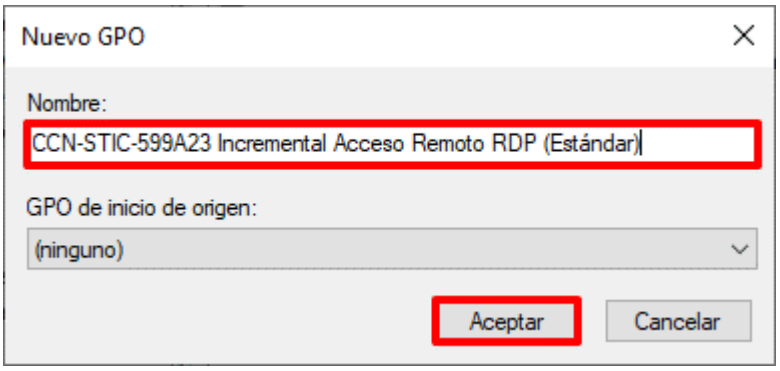
Nota: Si en su organización no hace uso de este elemento puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

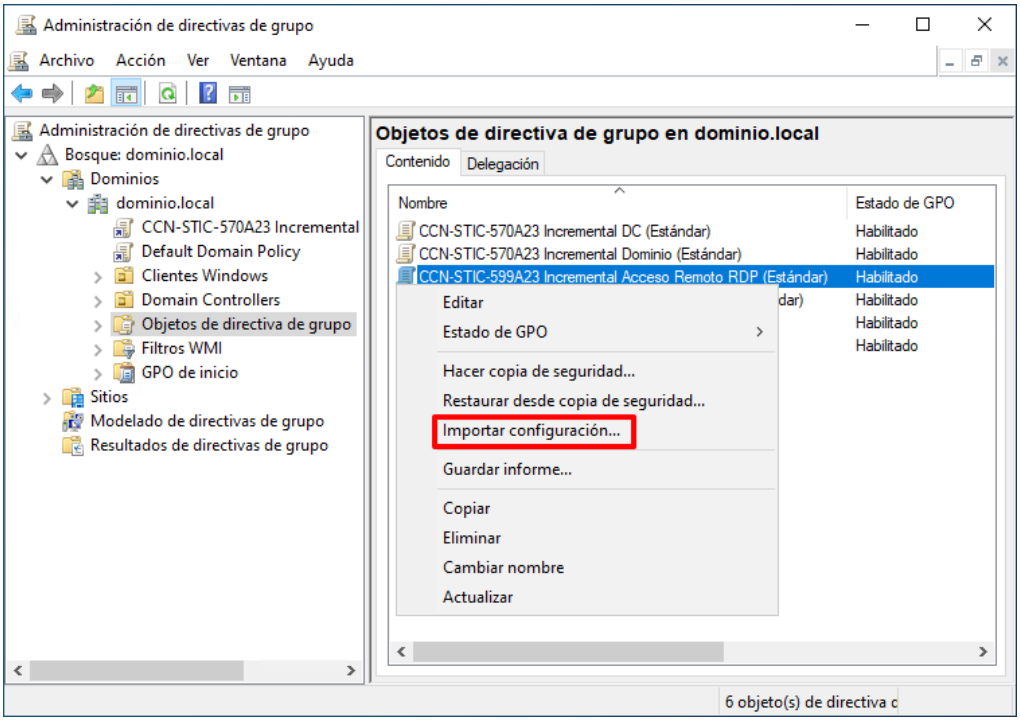
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

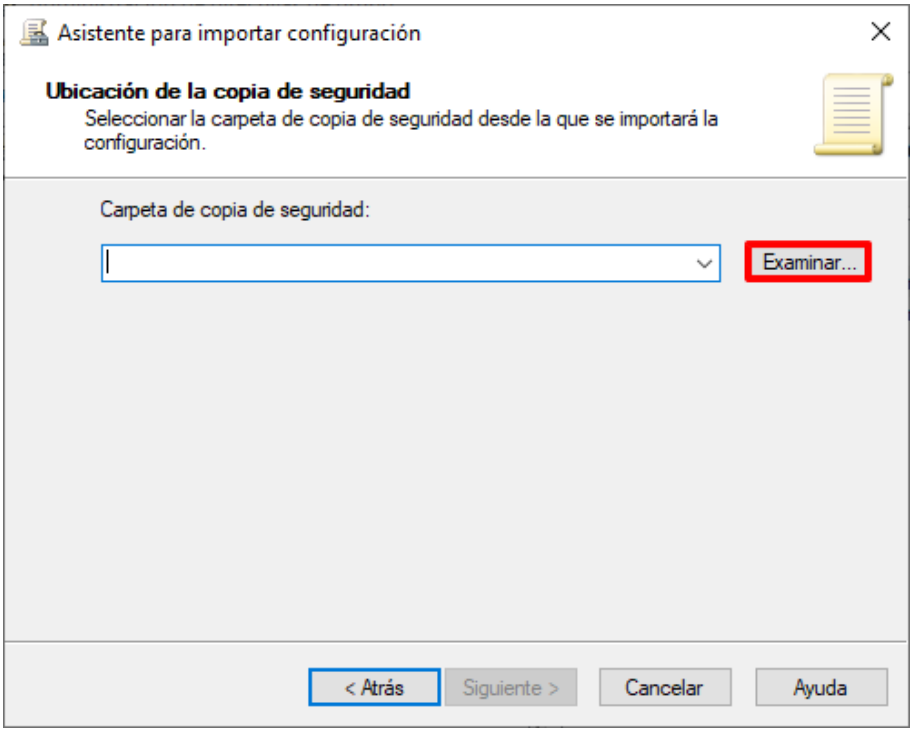
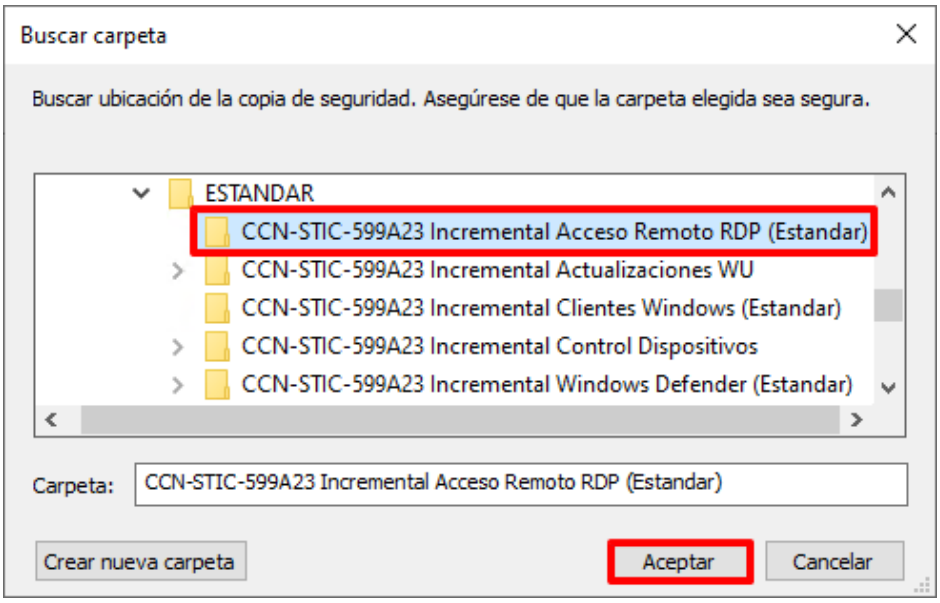
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

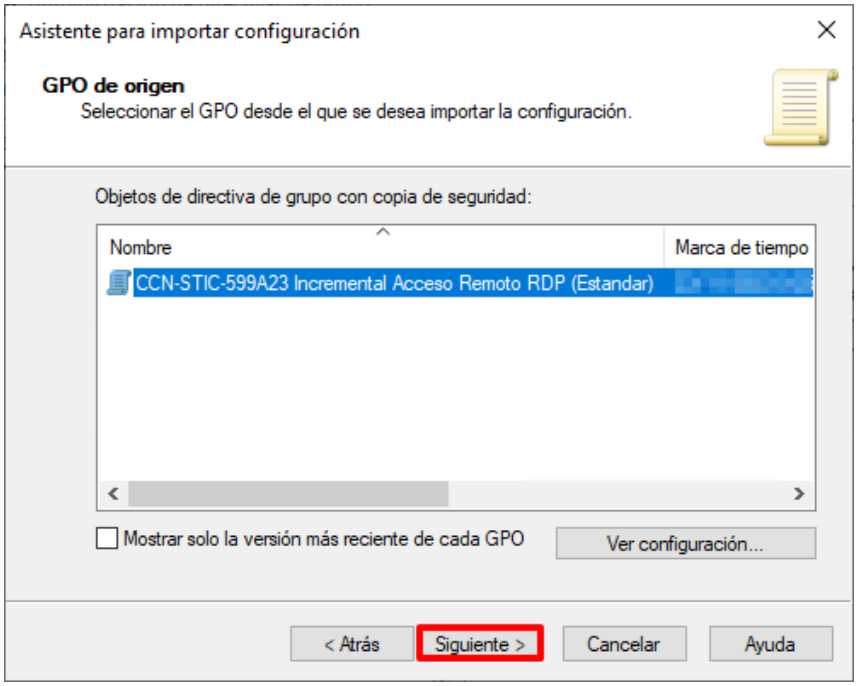
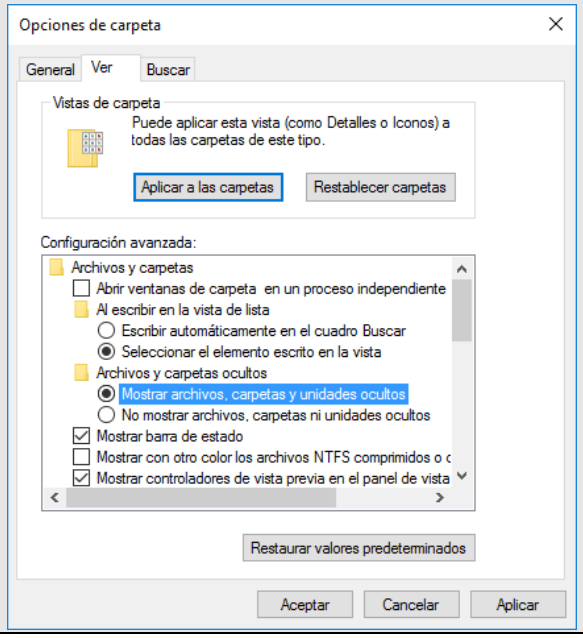
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

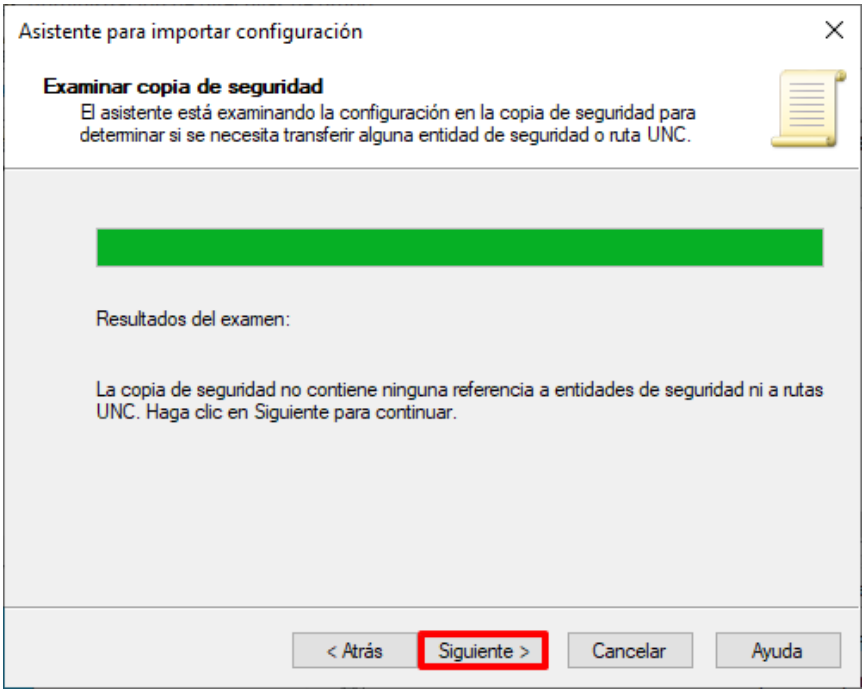
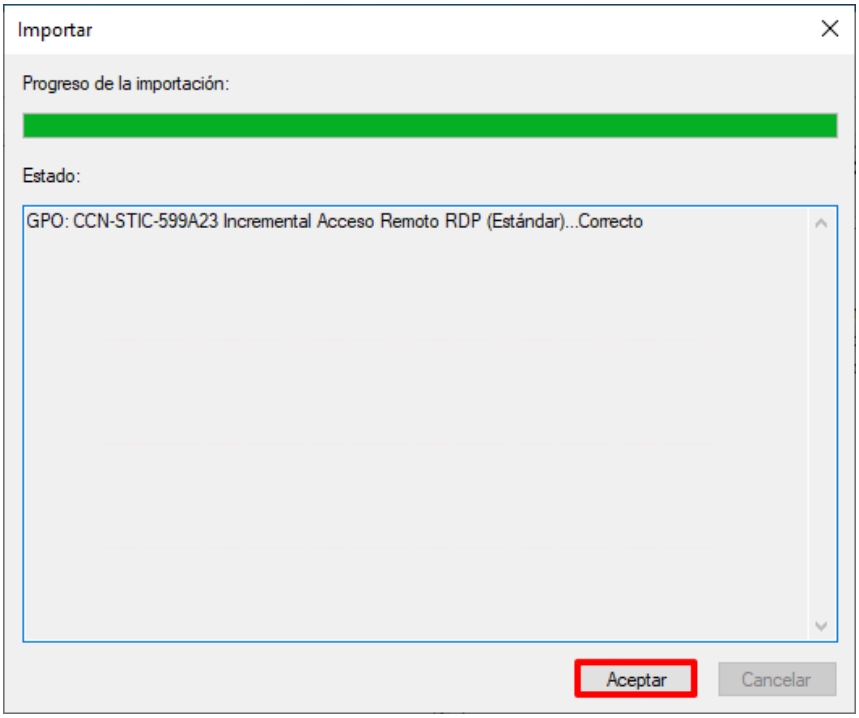
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

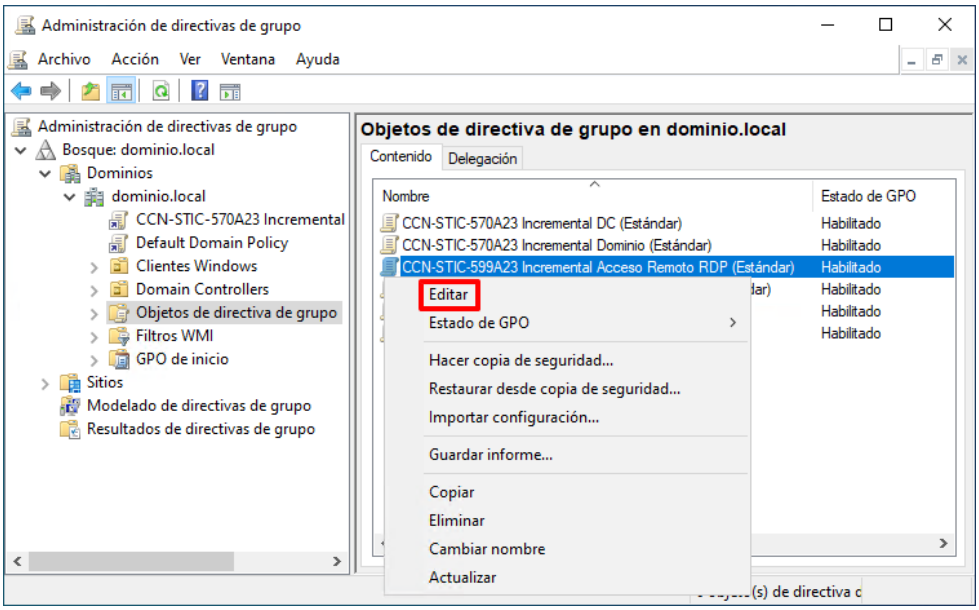
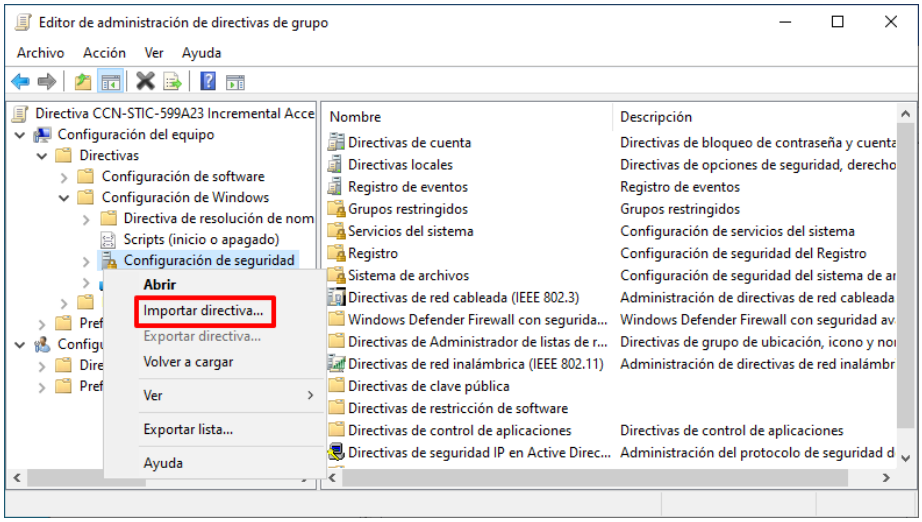
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])**" 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".

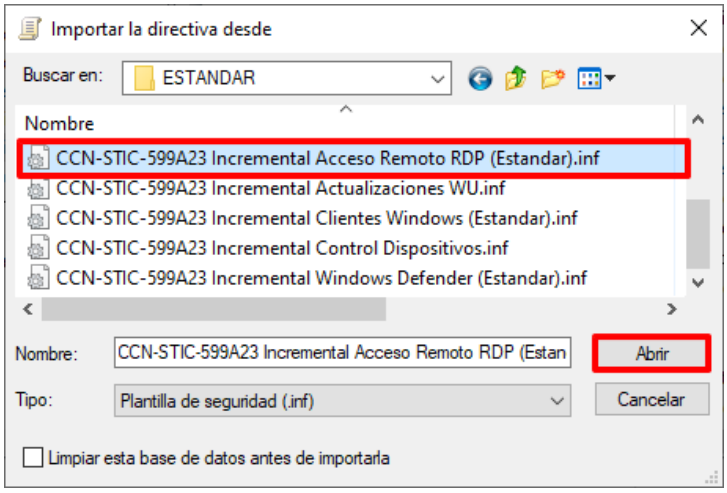
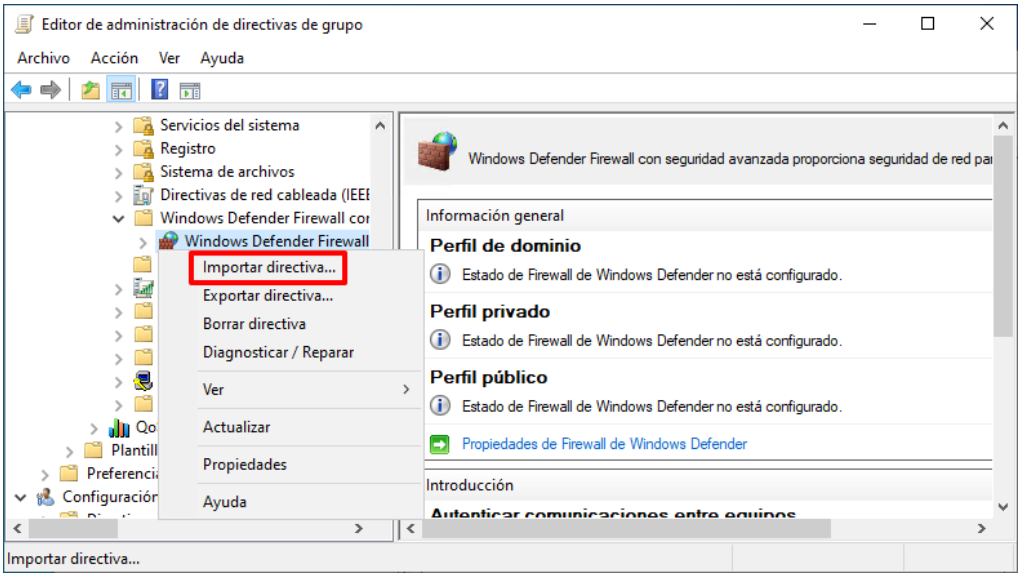
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

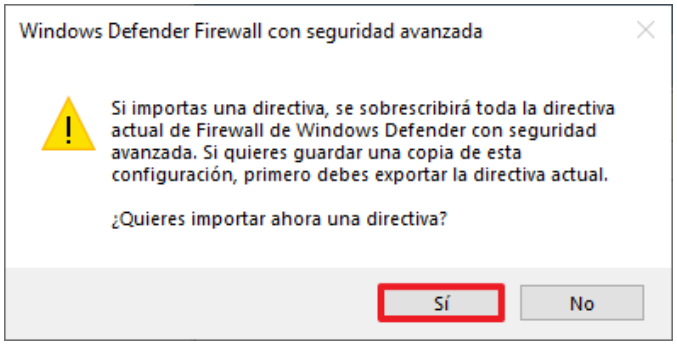
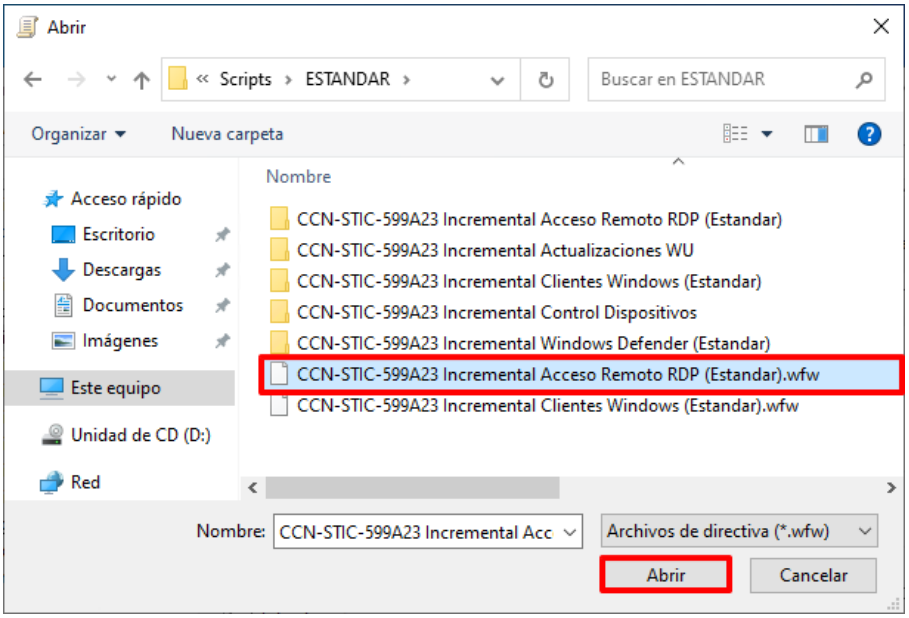
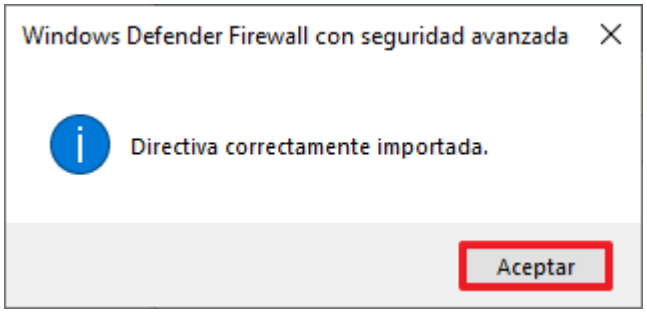
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.

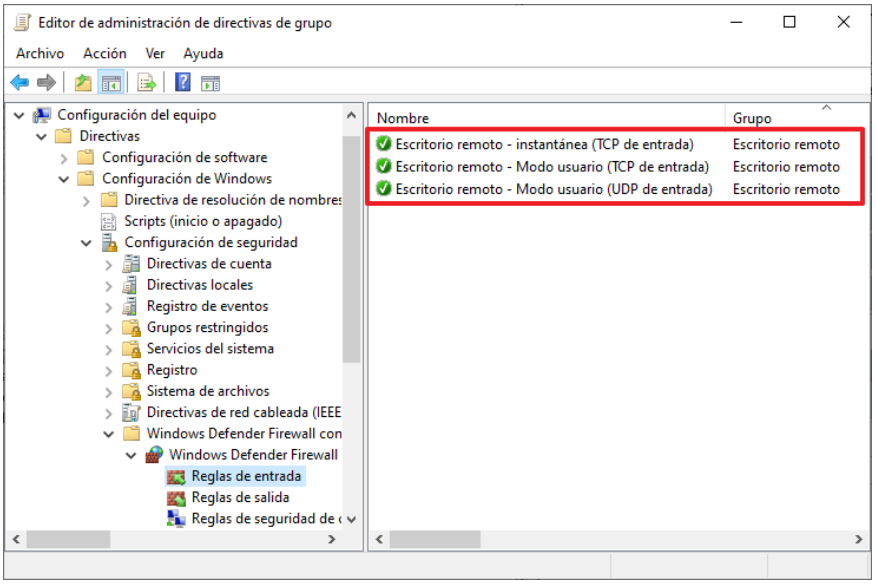
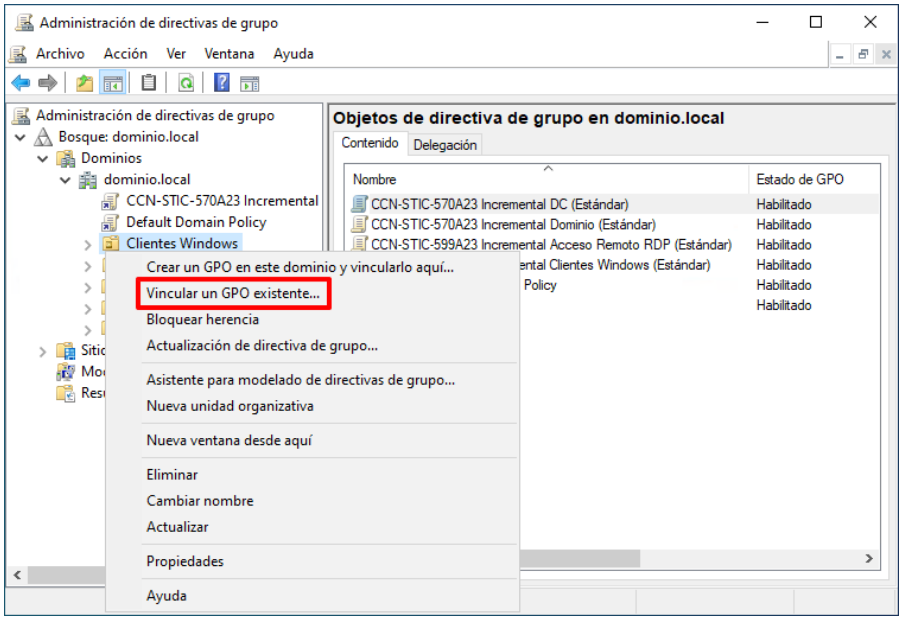
Paso	Descripción
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”.
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-599A23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política 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”. 

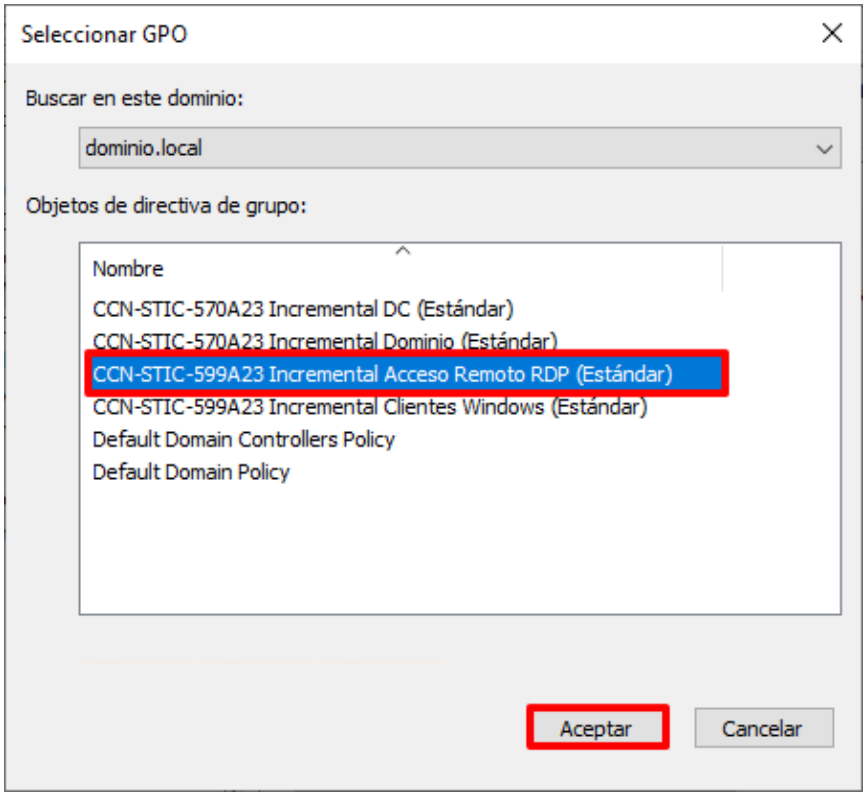
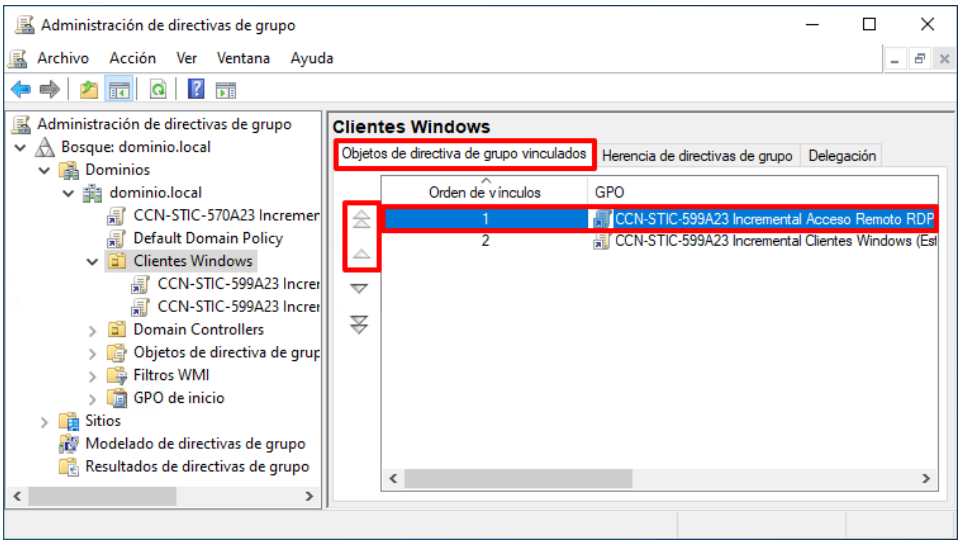
Paso	Descripción
14.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
15.	Para completar el asistente pulse sobre el botón “Finalizar”.
16.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-599A23 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-599A23 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-599A23 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".
21.	En la misma ventana del editor de administración de directivas de grupo, seleccione el siguiente nodo: "**Directiva CCN-STIC-599A23 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. 

Paso	Descripción
22.	Pulse “Sí” para continuar. 
23.	Seleccione el archivo de configuración “CCN-STIC-599A23 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 “Clientes Windows”, creada para tal fin.

Paso	Descripción
28.	A continuación, seleccione el objeto GPO "CCN-STIC-599A23 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.1.2.2 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.

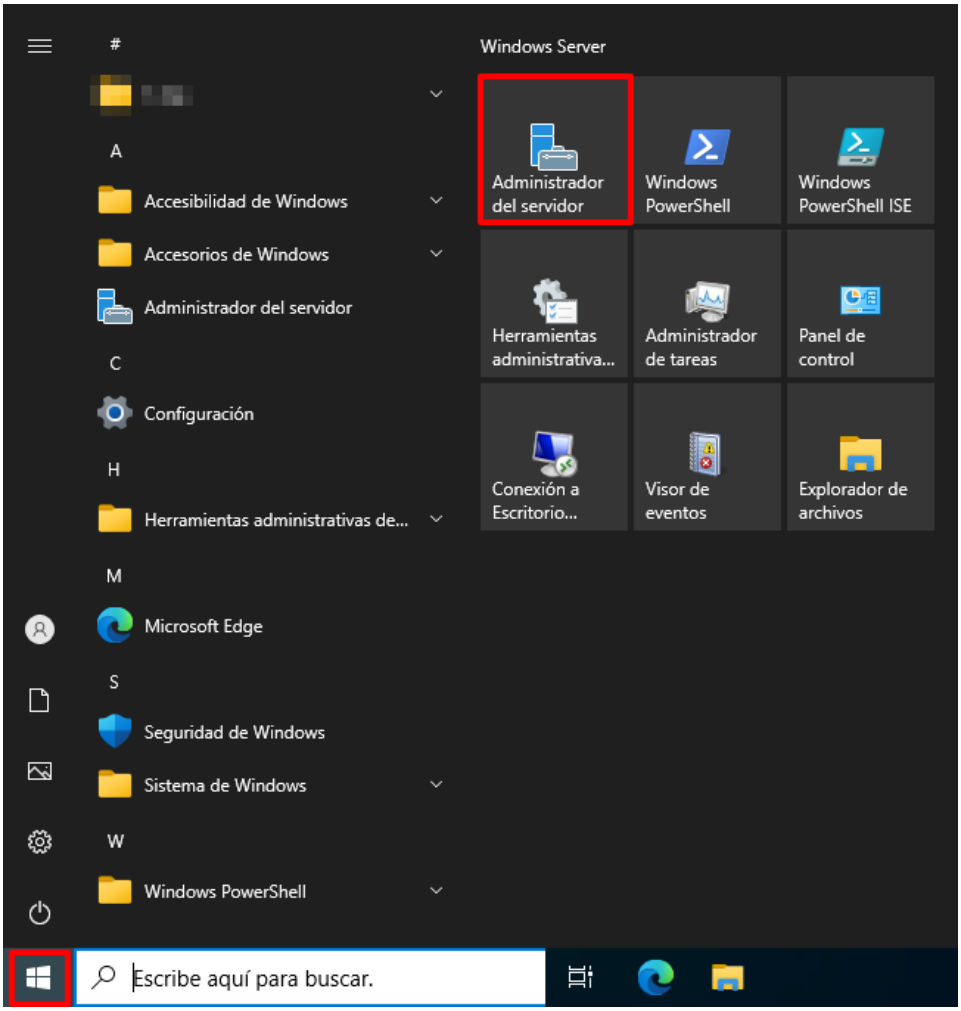
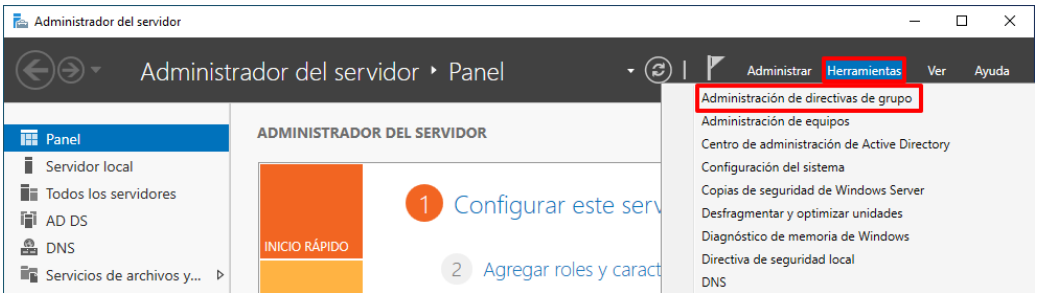
ANEXO A.2.2. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

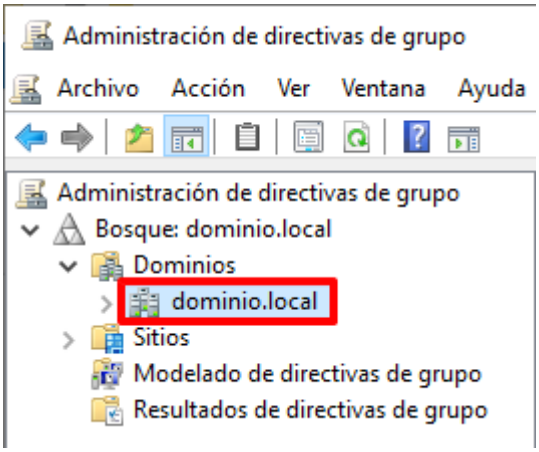
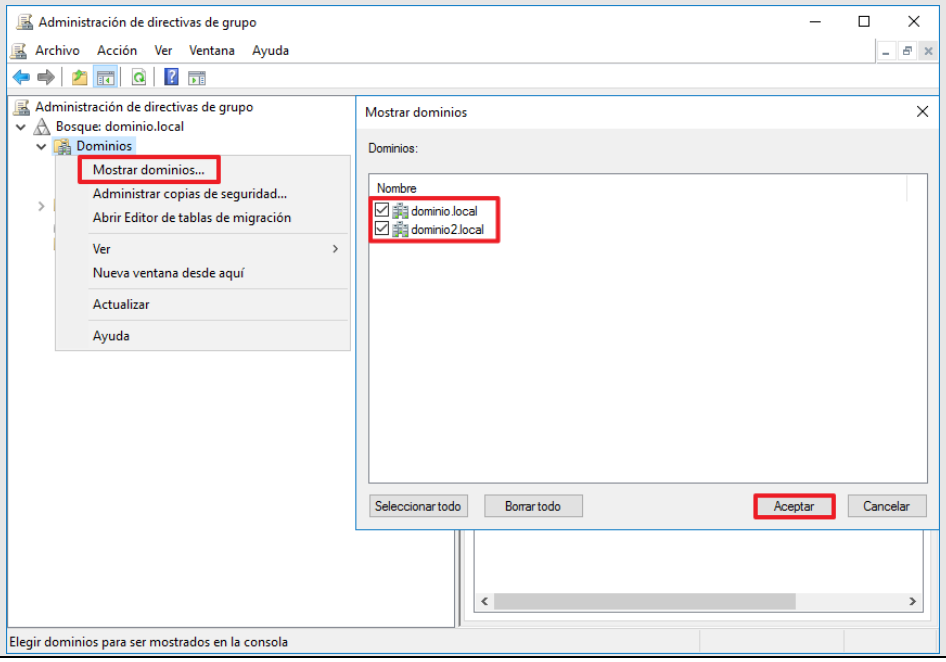
A través de la siguiente sección y su paso a paso, se definirán las acciones para dotar a los sistemas operativos Windows Cliente de un servicio de actualizaciones automáticas completamente configurado.

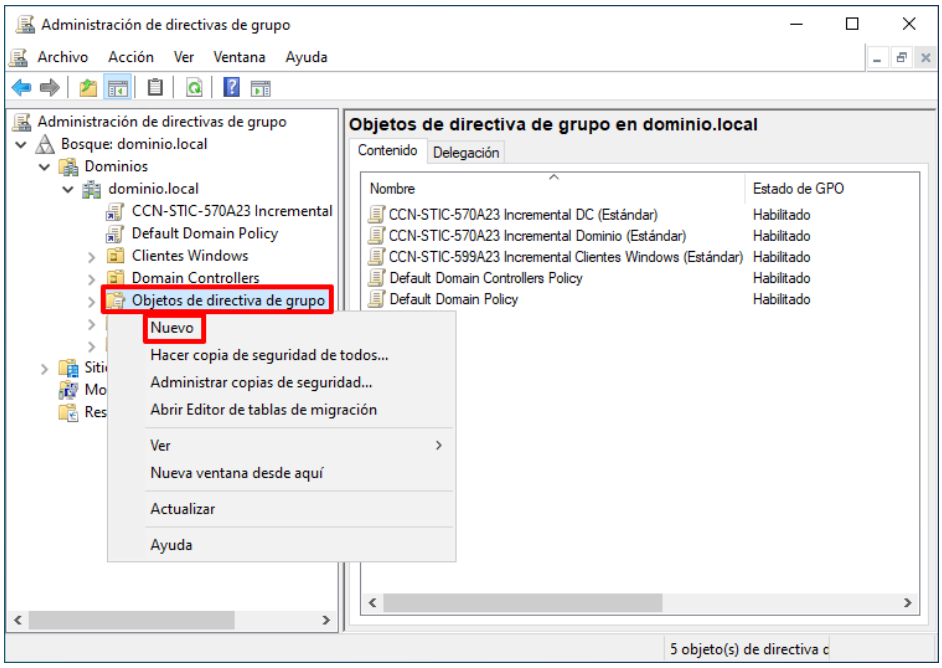
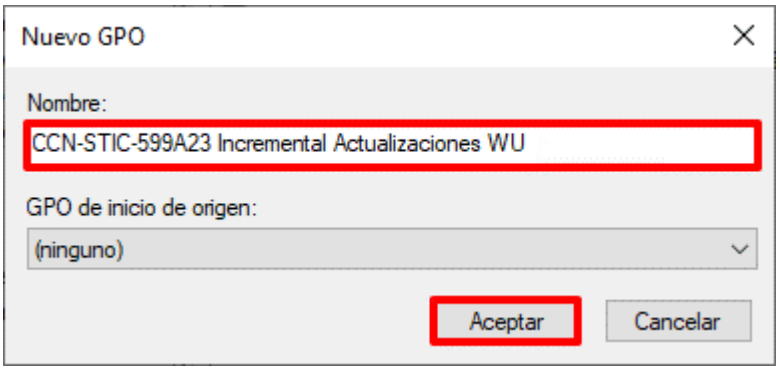
Nota: Si en su organización ya dispone de un producto o servicio para la actualización y mantenimiento del sistema operativo, como el servicio de WSUS, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

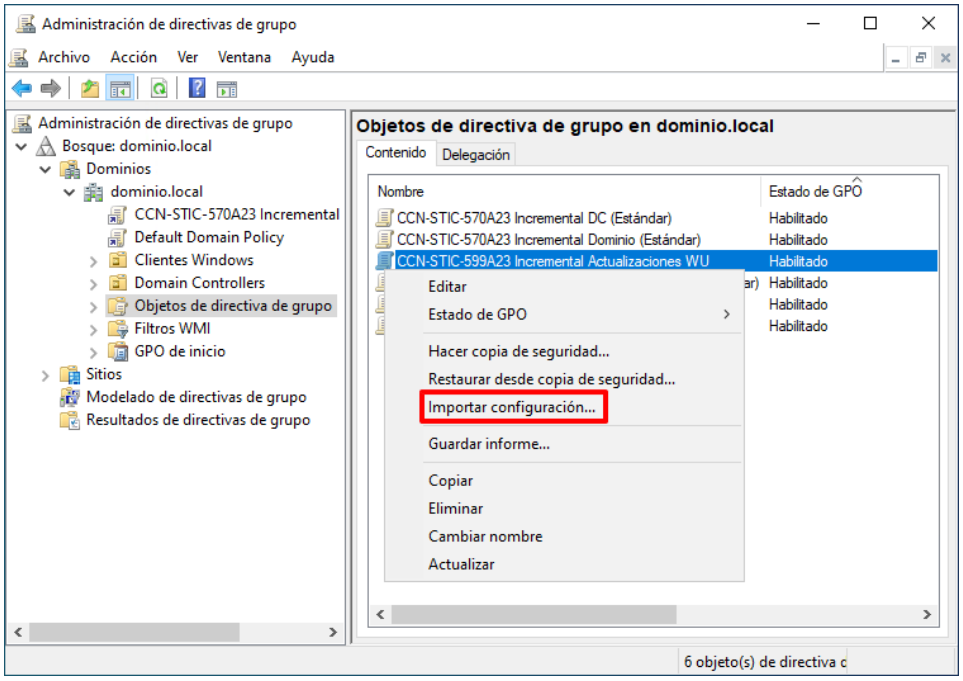
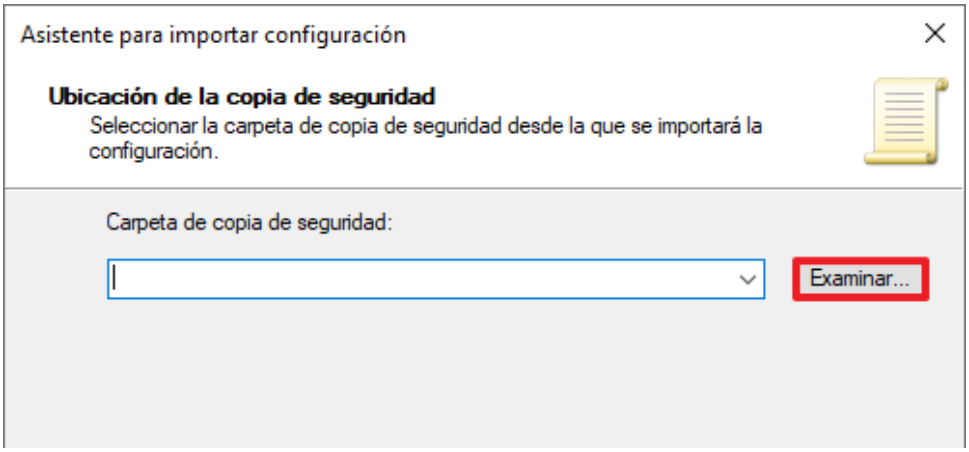
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

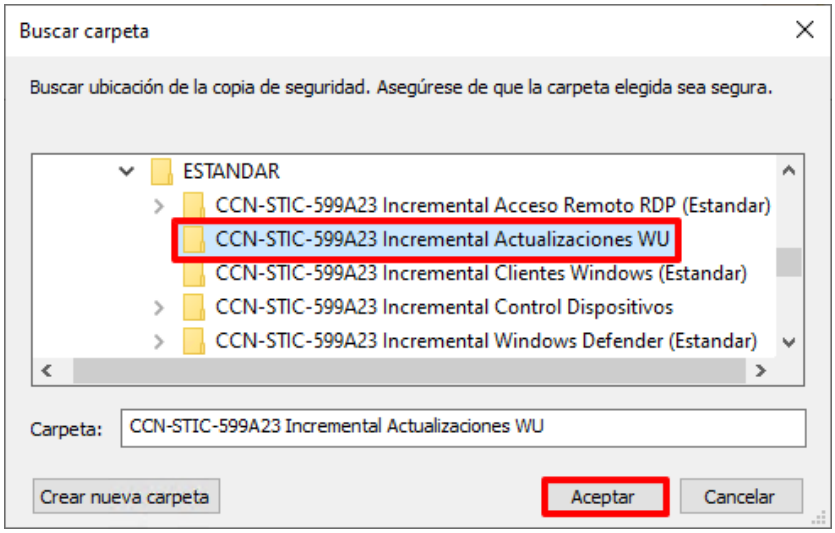
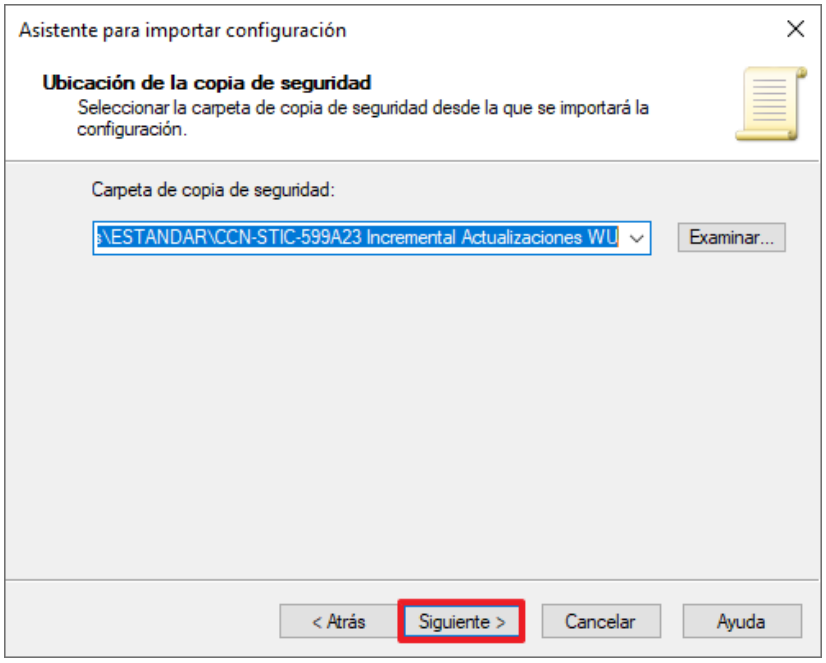
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

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”. 

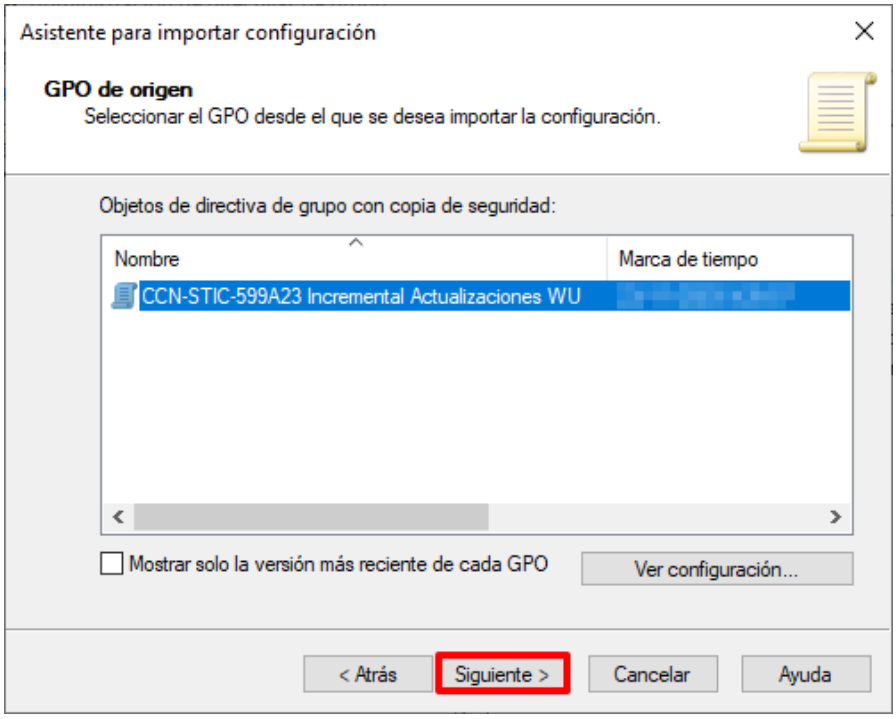
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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-599A23 Incremental Actualizaciones WU**" y pulse el botón "Aceptar". 

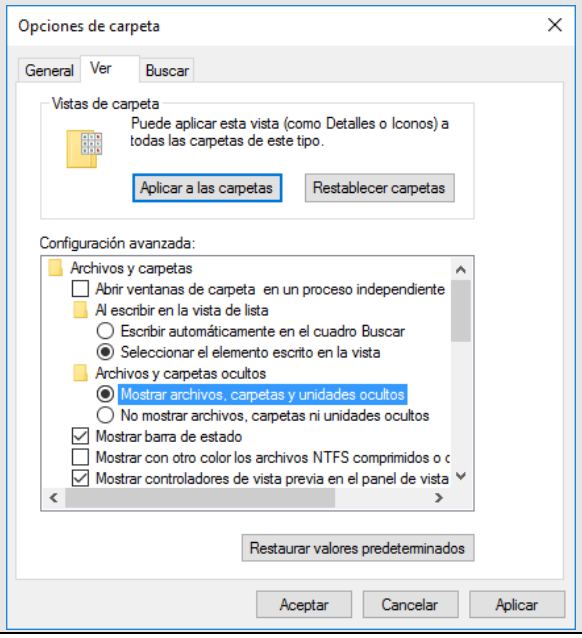
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

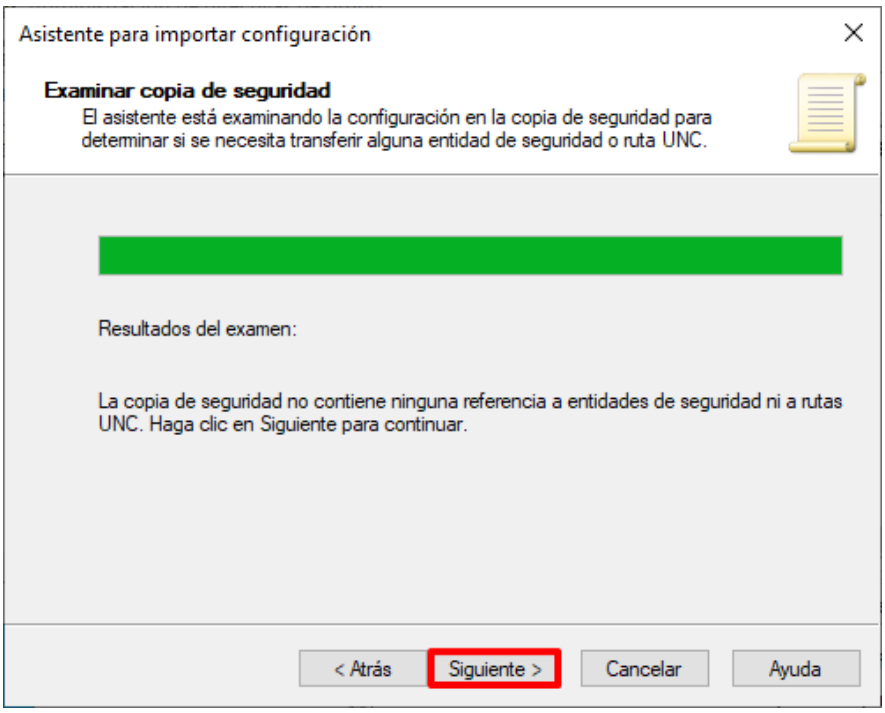
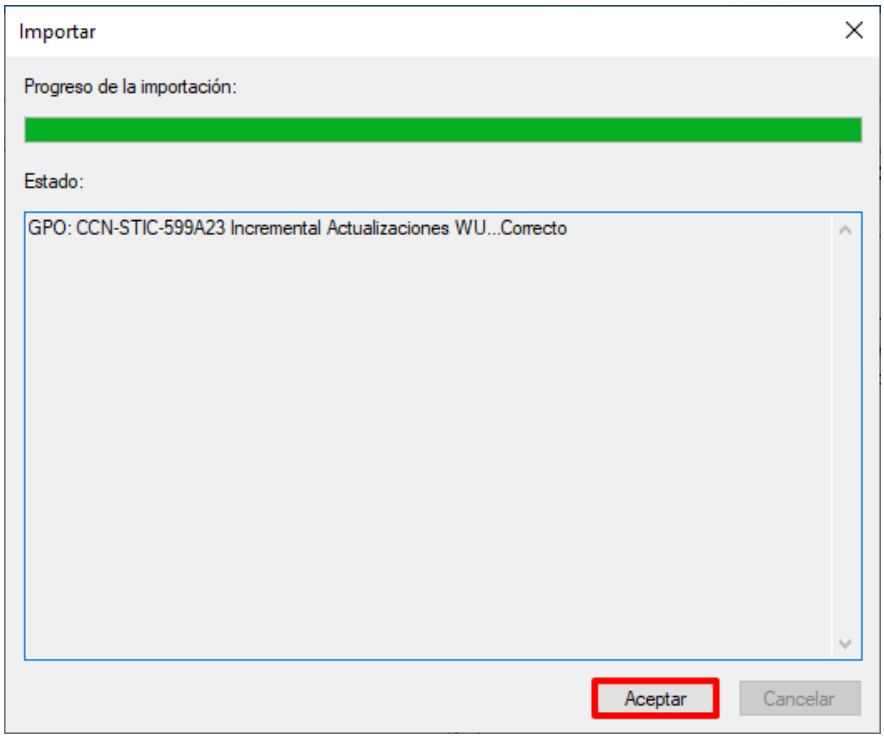
Paso	Descripción
11.	Seleccione la carpeta "CCN-STIC-599A23 Incremental Actualizaciones WU" situada en el directorio "C:\Scripts\[TIPO DE PERFILADO]" y pulse "Aceptar".  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
12.	Pulse "Siguiente >" en la sección "Ubicación de la copia de seguridad". 

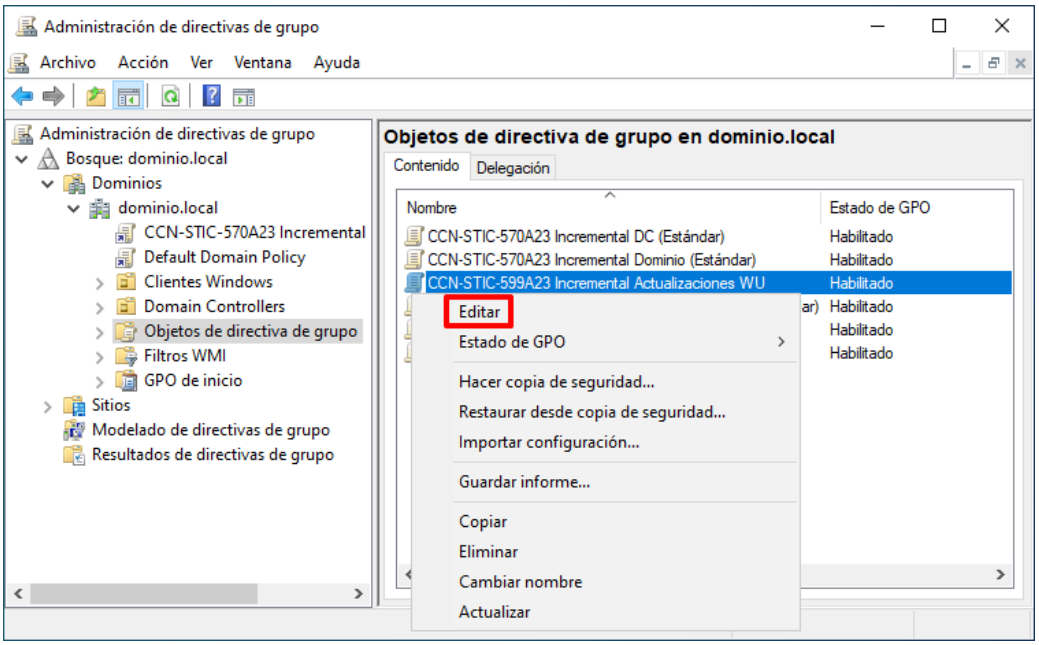
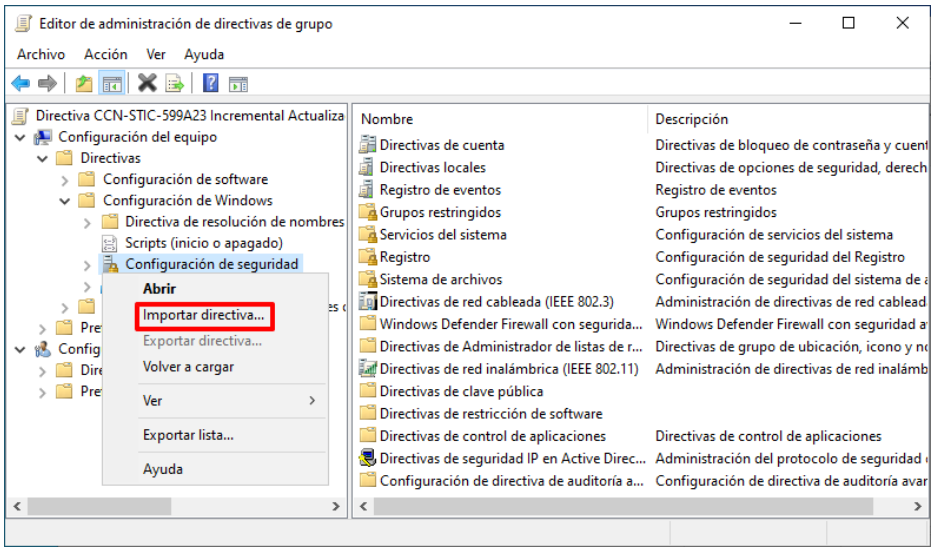
Paso	Descripción
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-599A23 Incremental Actualizaciones WU” y pulse “Siguiente >”.

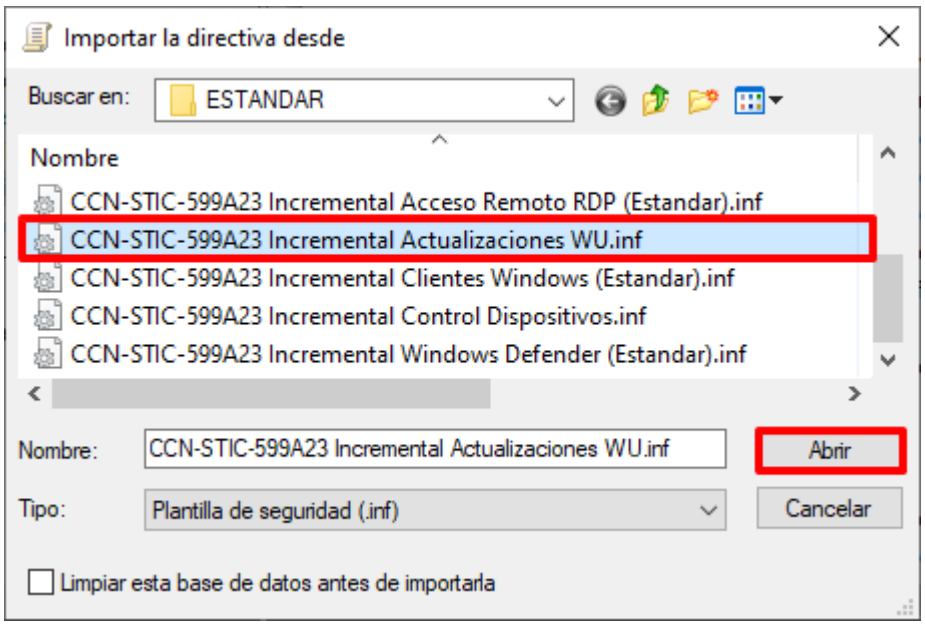
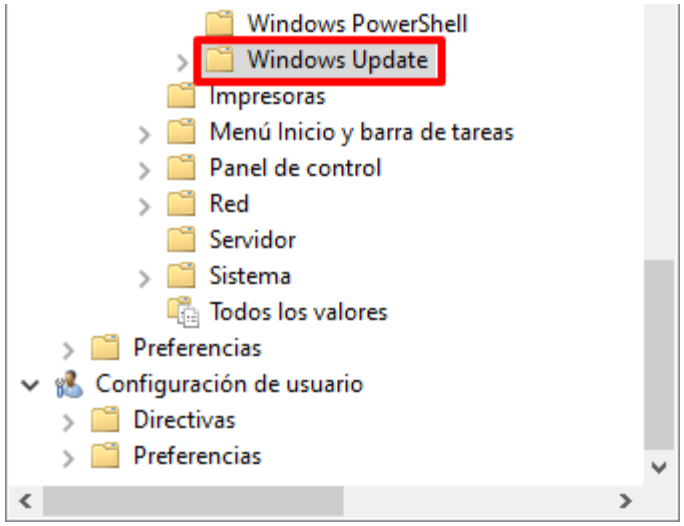


Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en las opciones de carpeta (“Vista → Opciones → Ver” en el menú superior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

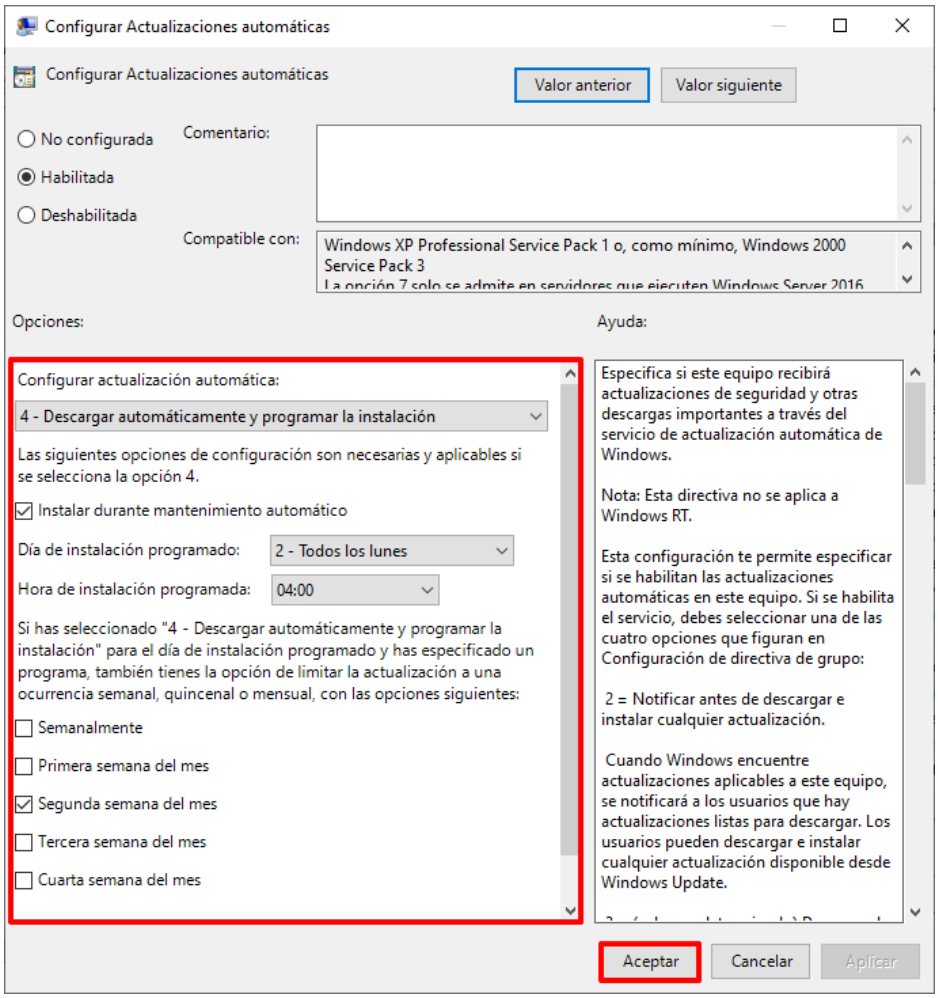


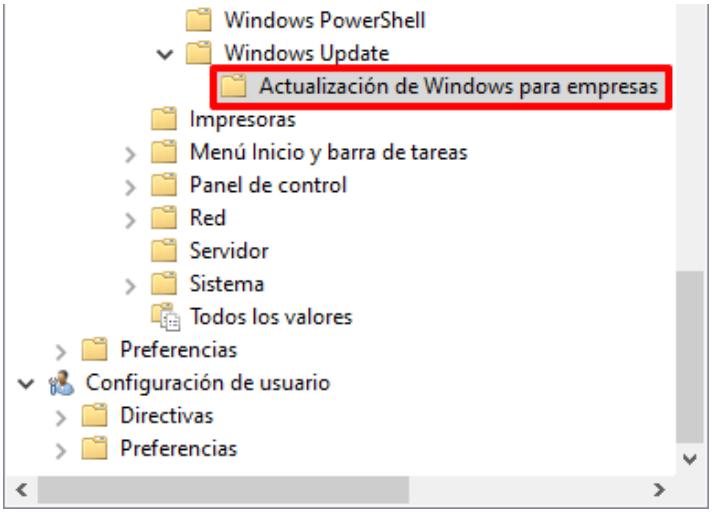
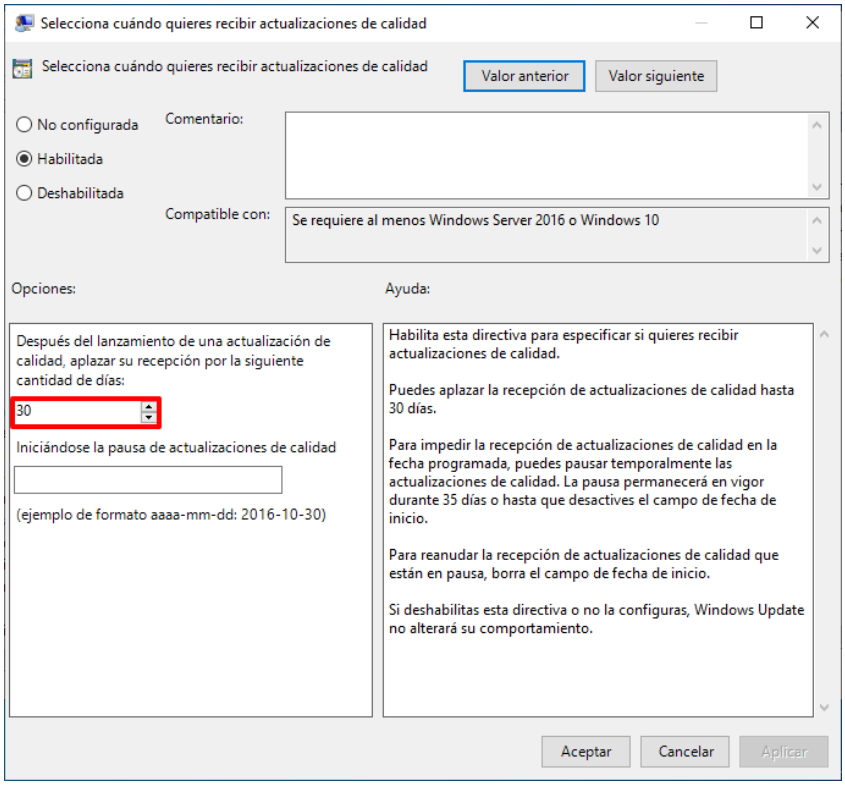
Paso	Descripción
14.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
15.	Para completar el asistente pulse sobre el botón “Finalizar”.
16.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

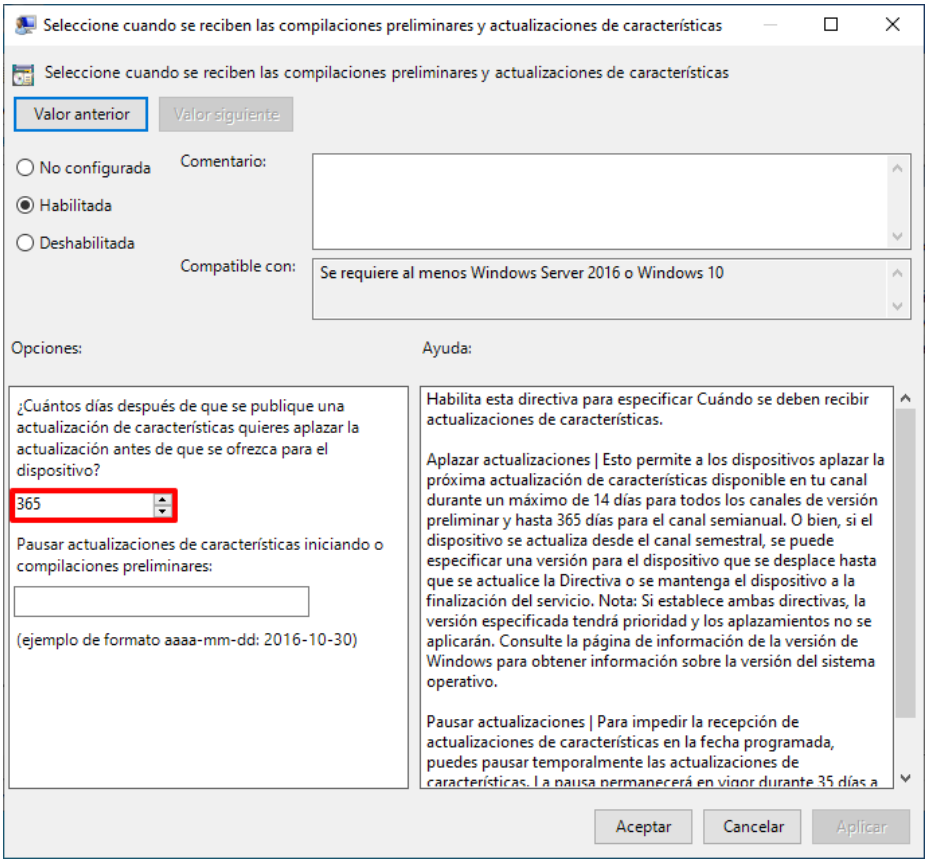
Paso	Descripción
17.	Seleccione de nuevo el objeto GPO "CCN-STIC-599A23 Incremental Actualizaciones WU" con el botón derecho y seleccione la opción "Editar" del menú contextual que aparecerá. 
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"CCN-STIC-599A23 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. 

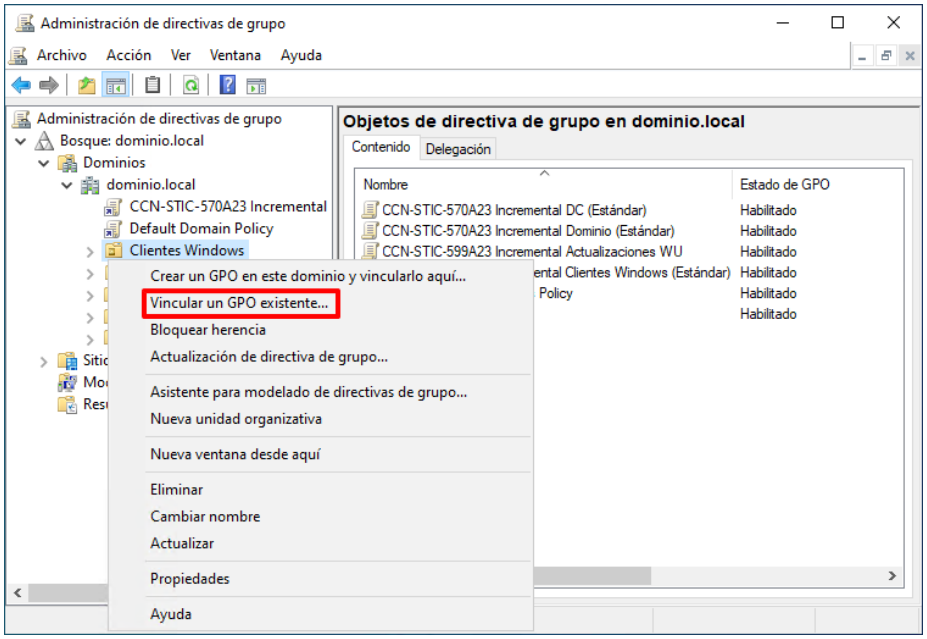
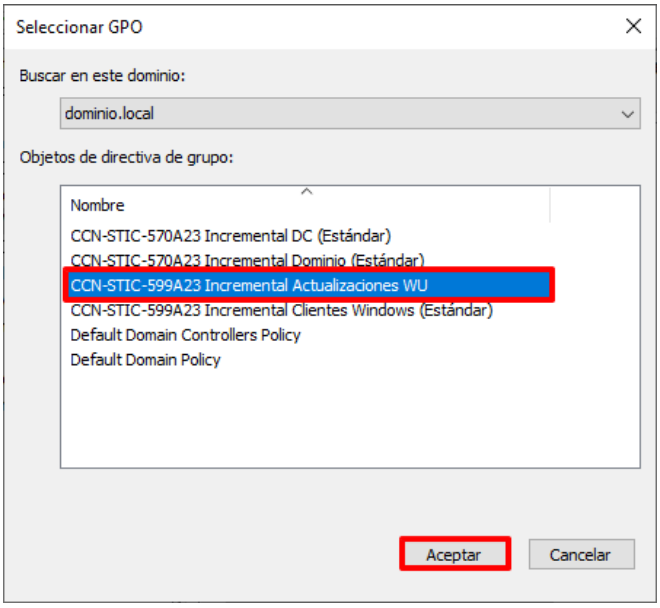
Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-599A23 Incremental Actualizaciones WU.inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** 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-599A23 Incremental Actualizaciones WU → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Windows Update"** 

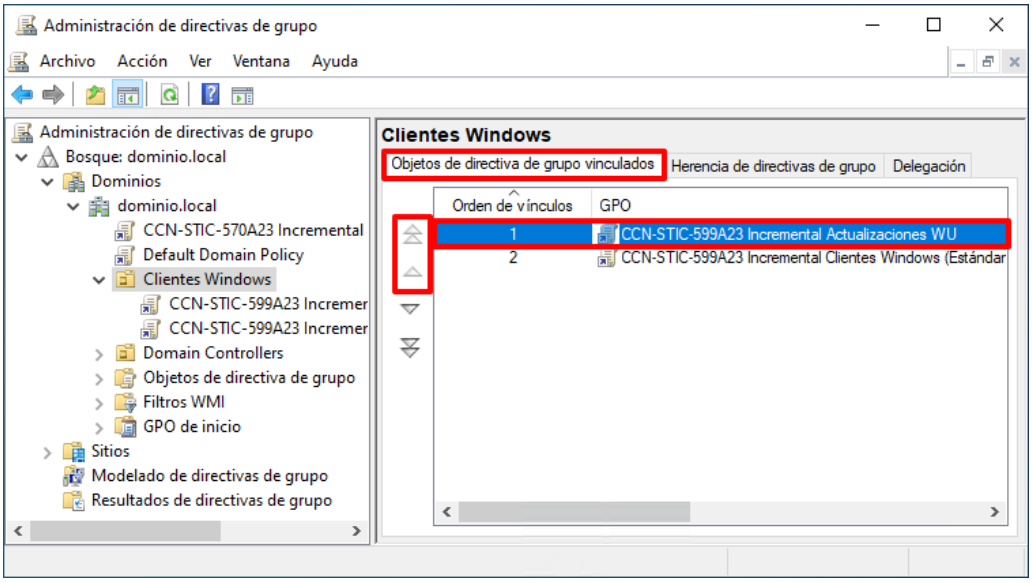
Paso	Descripción
22.	En el panel derecho identifique y haga doble clic sobre la directiva “Configurar Actualizaciones automáticas”. Evalúe y adapte la configuración ofrecida acorde a las necesidades de su organización.



Paso	Descripción
23.	A continuación, despliegue el nodo: **"CCN-STIC-599A23 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 “Clientes Windows”, creada para tal fin.
28.	A continuación, seleccione el objeto GPO “CCN-STIC-599A23 Incremental Actualizaciones WU” y pulse “Aceptar”. 

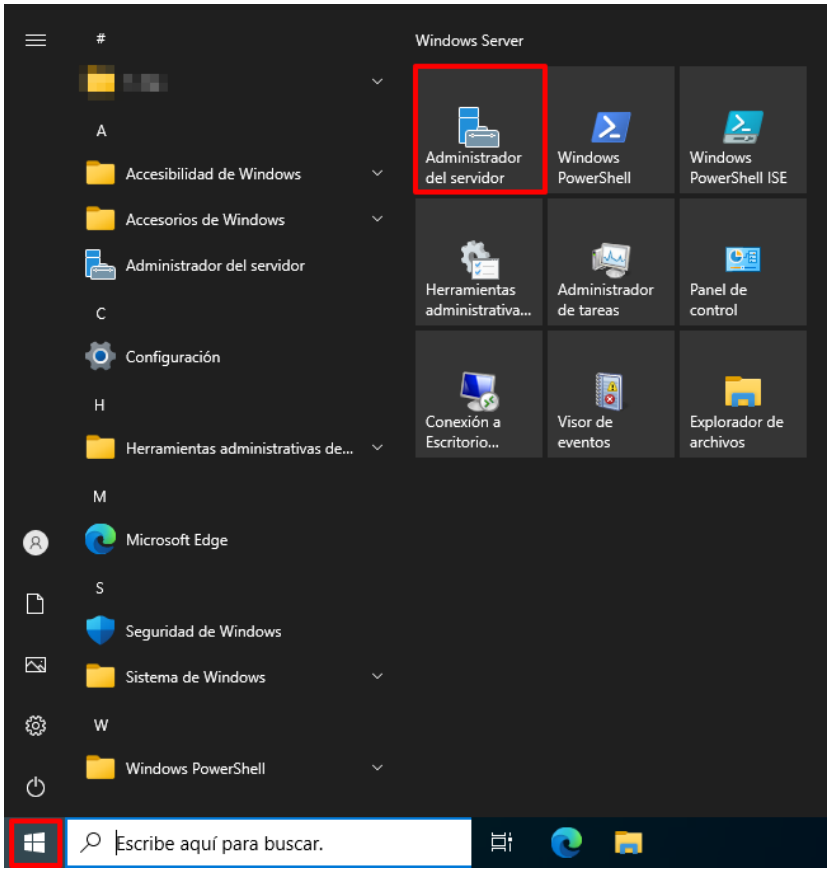
Paso	Descripción
29.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña “Objetos de directiva de grupo vinculados”, seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 
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.1.2.2 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.

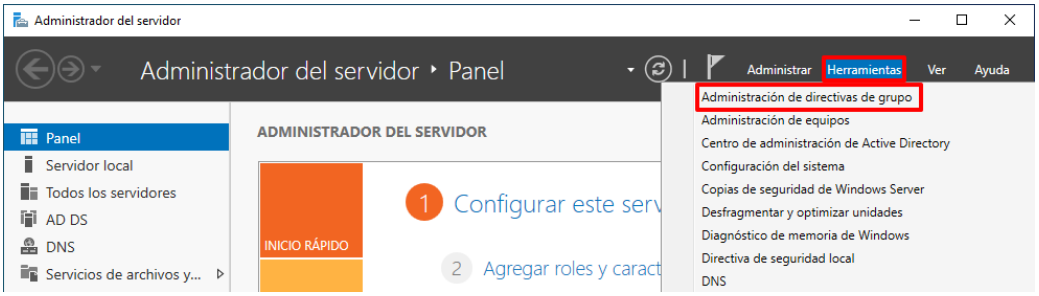
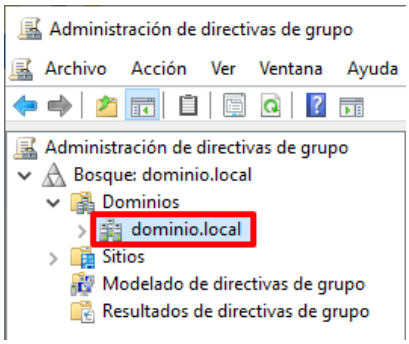
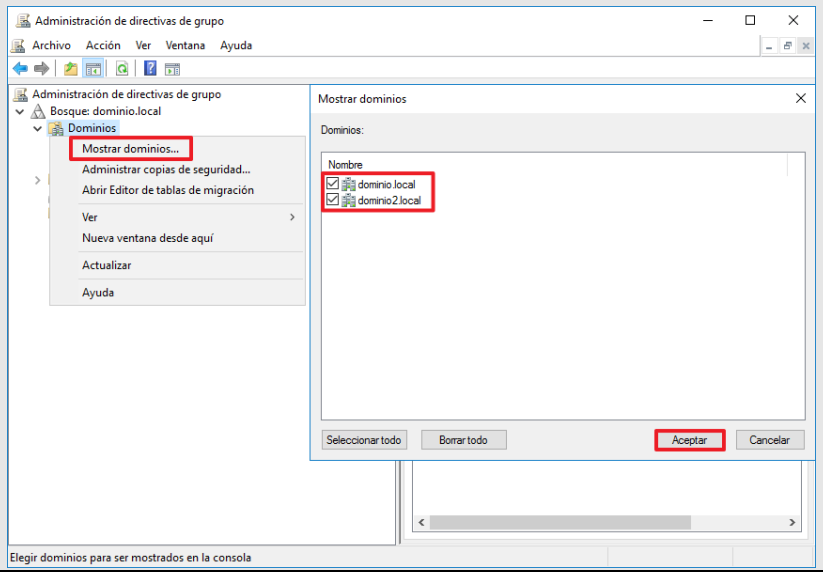
ANEXO A.2.3. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

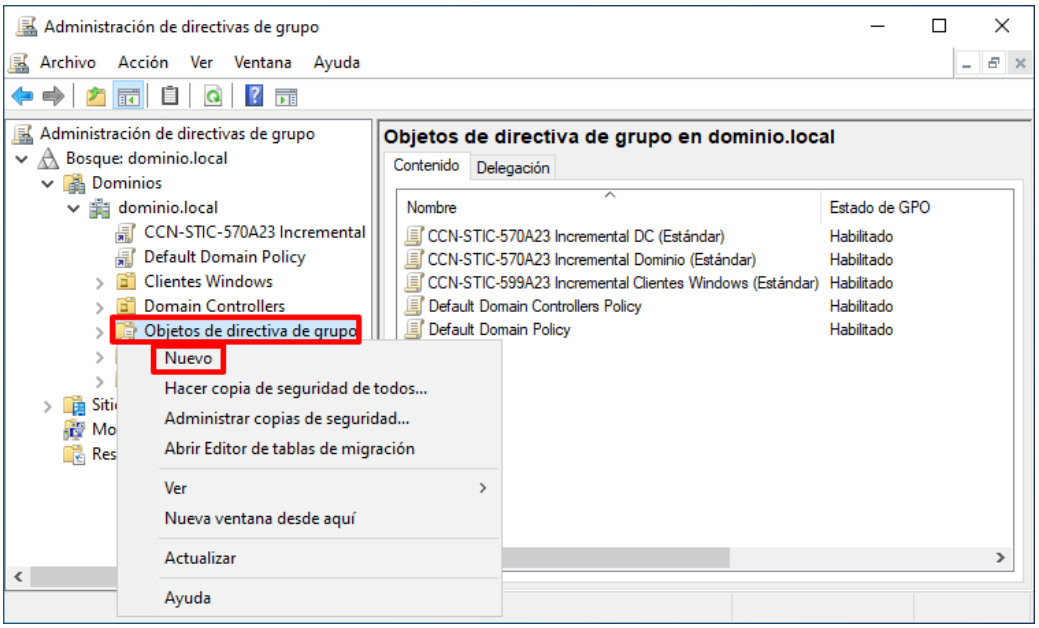
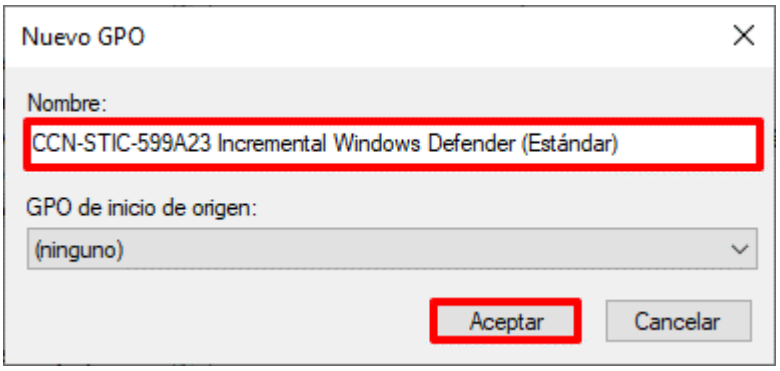
La sección y los pasos descritos a continuación, permiten establecer la configuración sobre el software frente a protección de código dañino incluido por defecto en los sistemas operativos Windows Cliente.

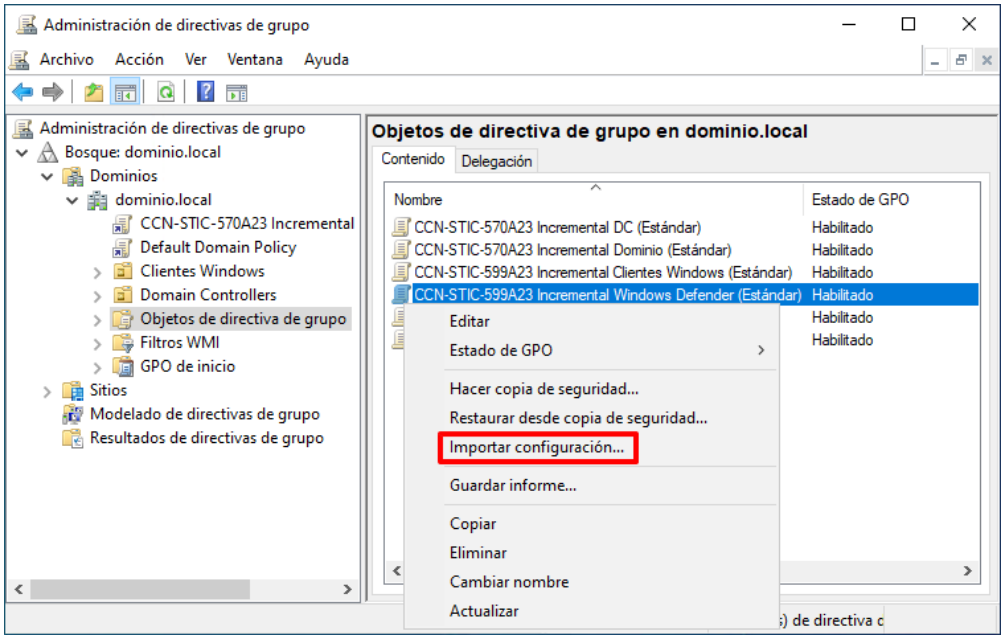
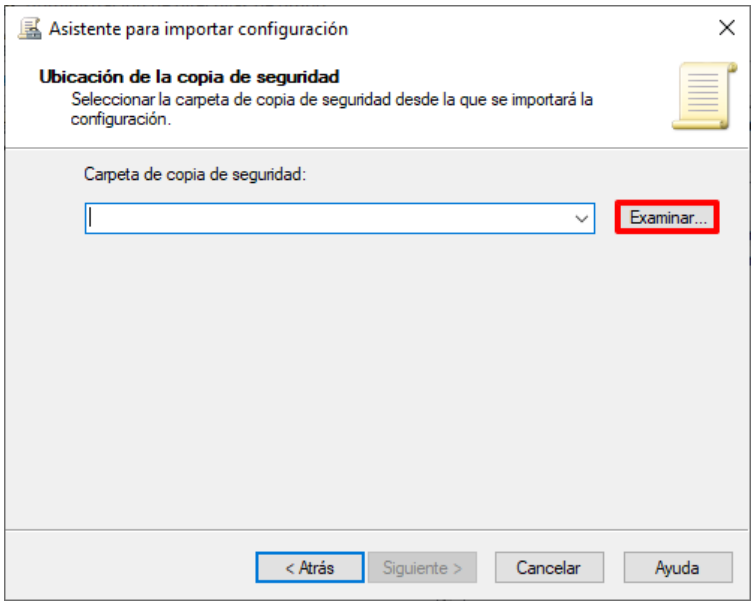
Nota: Si en su organización ya dispone de un producto o servicio frente a código dañino en el sistema operativo, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

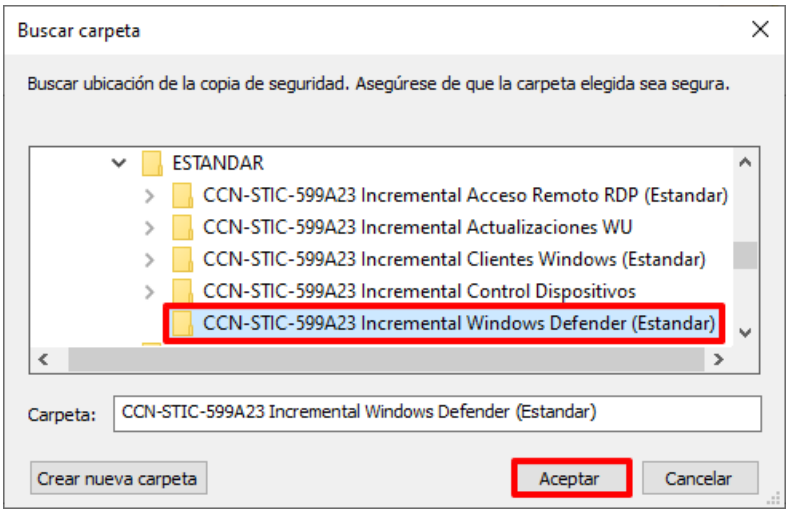
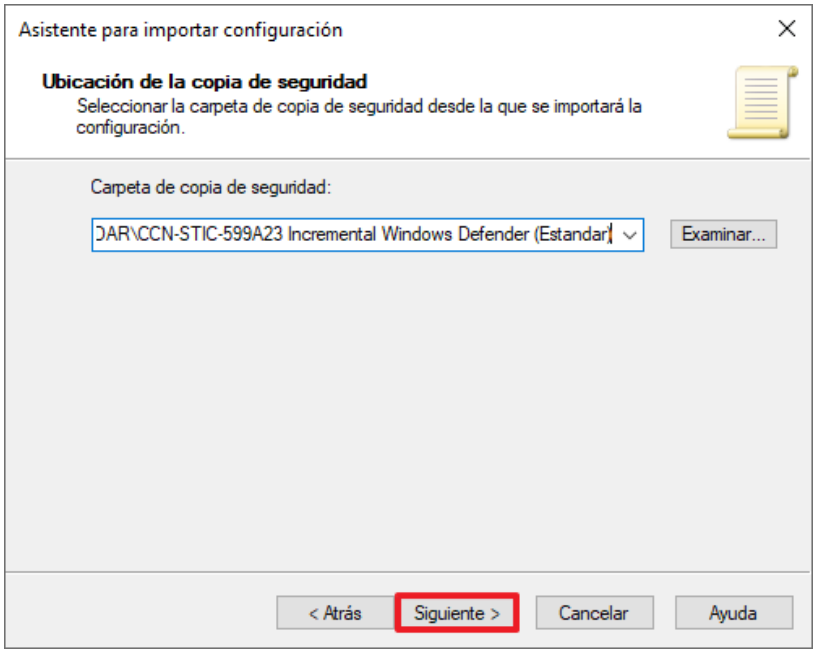
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

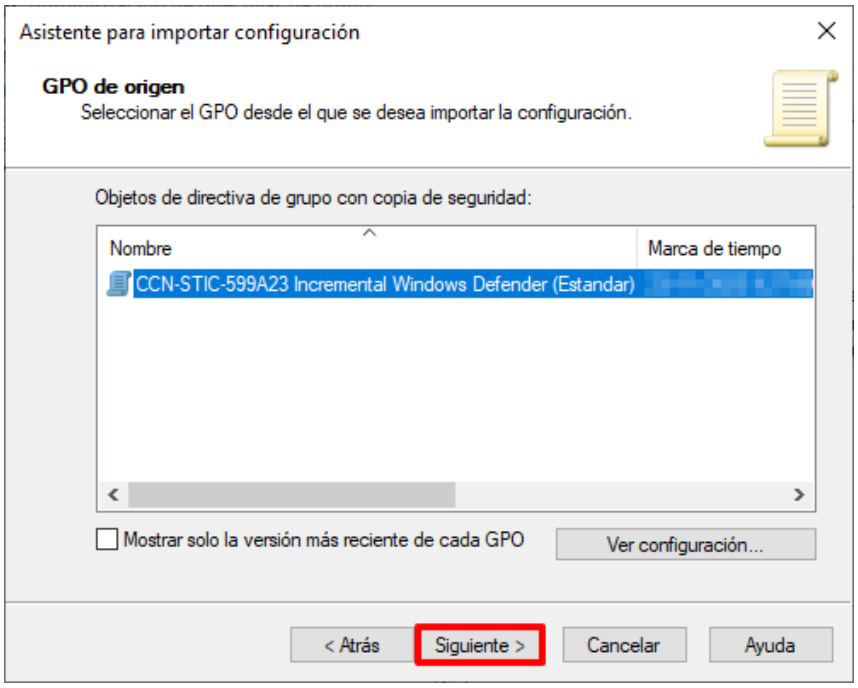
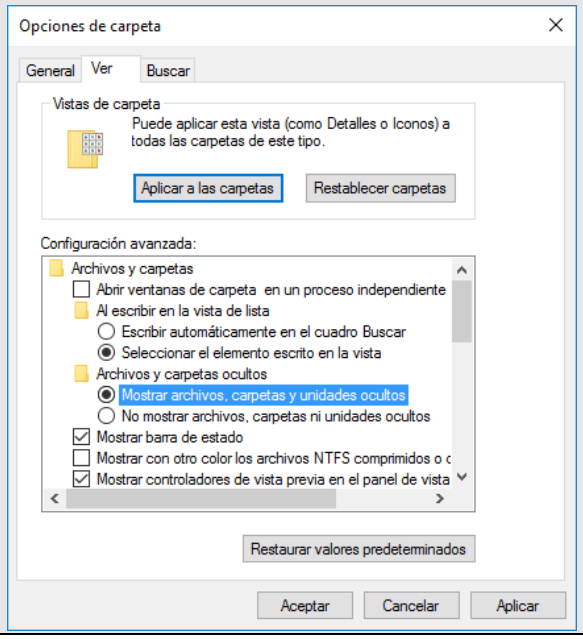
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **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".

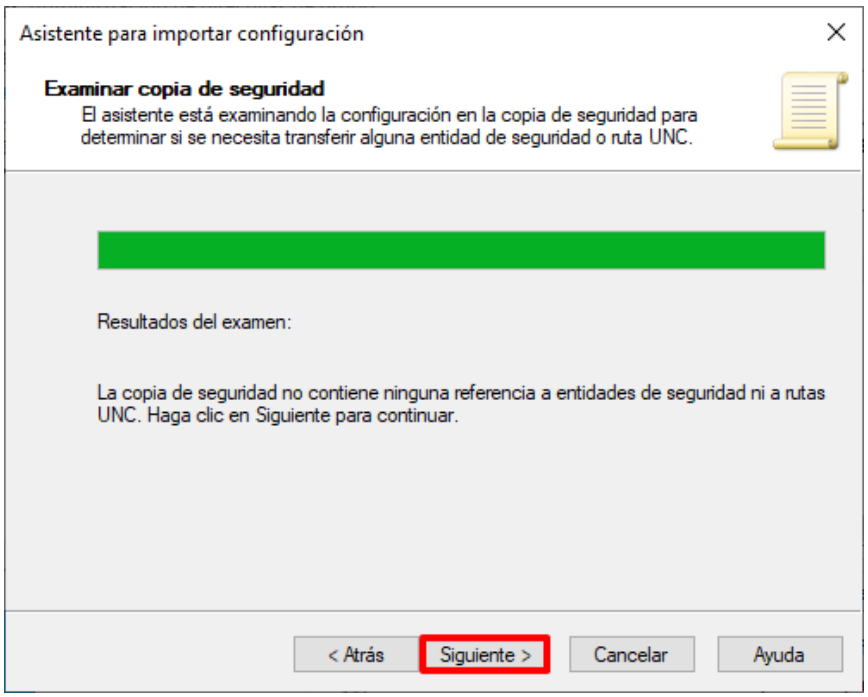
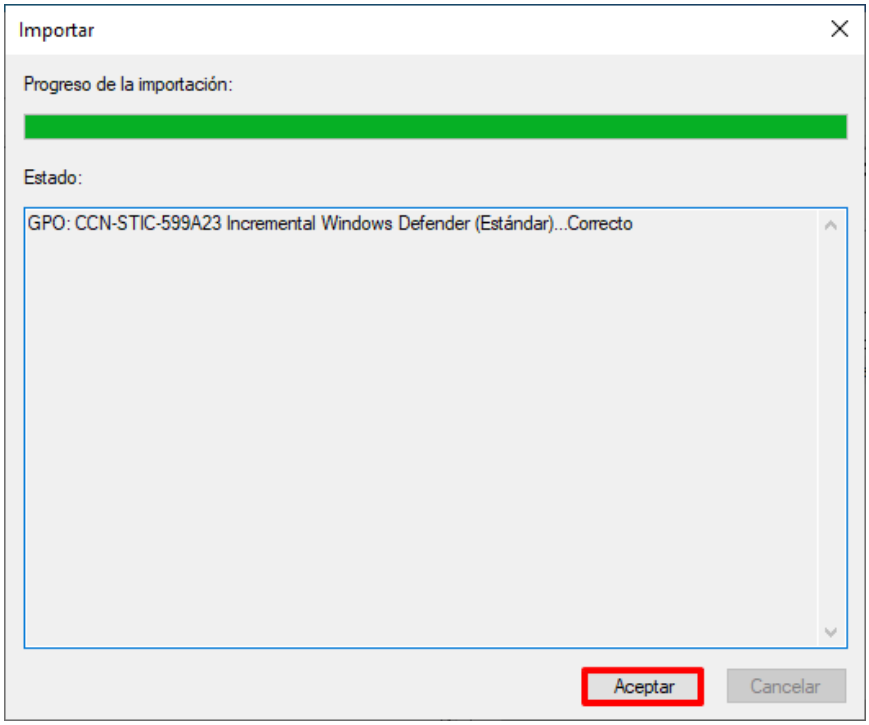
Paso	Descripción
3.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
4.	Una vez abierta la consola, seleccione: **“Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. Hasta que se indique lo contrario, 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. 

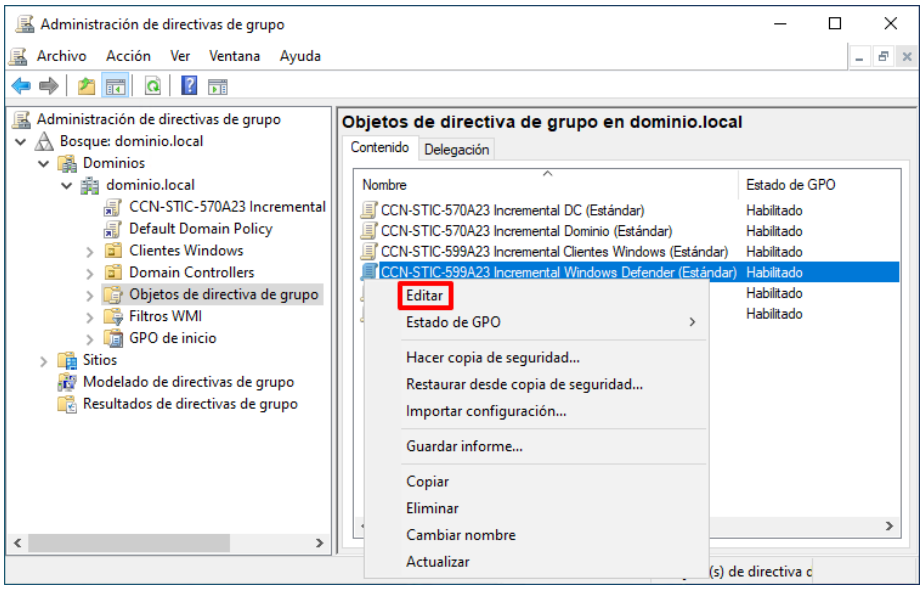
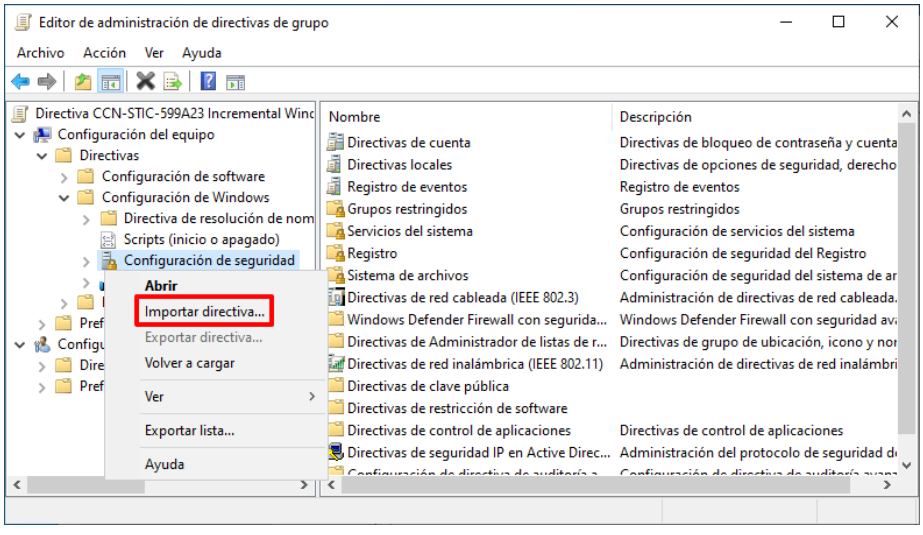
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO])**" y pulse el botón "Aceptar". 

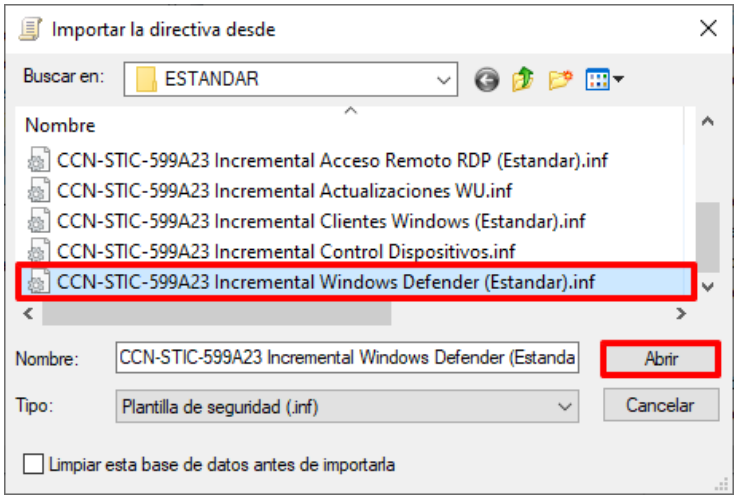
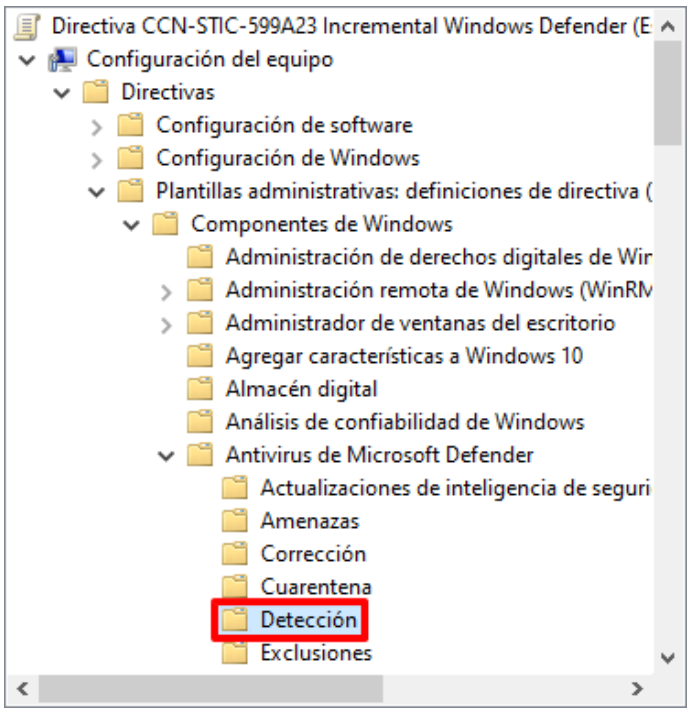
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

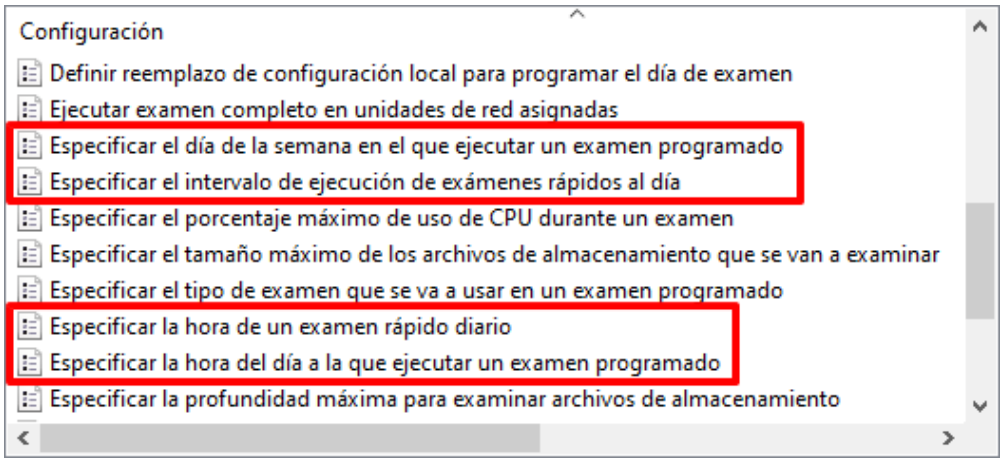
Paso	Descripción
11.	Seleccione la carpeta “CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO])” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración “Estándar”.
12.	Pulse “Siguiente >” en la sección “Ubicación de la copia de seguridad”. 

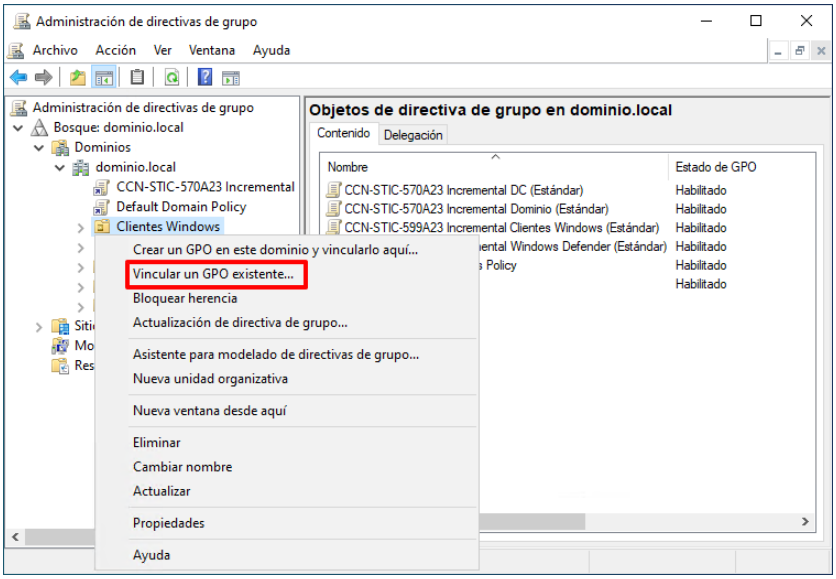
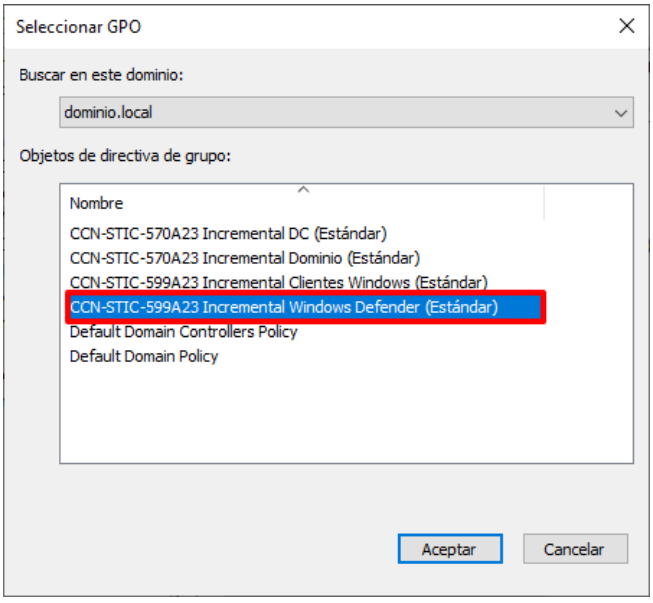
Paso	Descripción
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO])” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe 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”. 

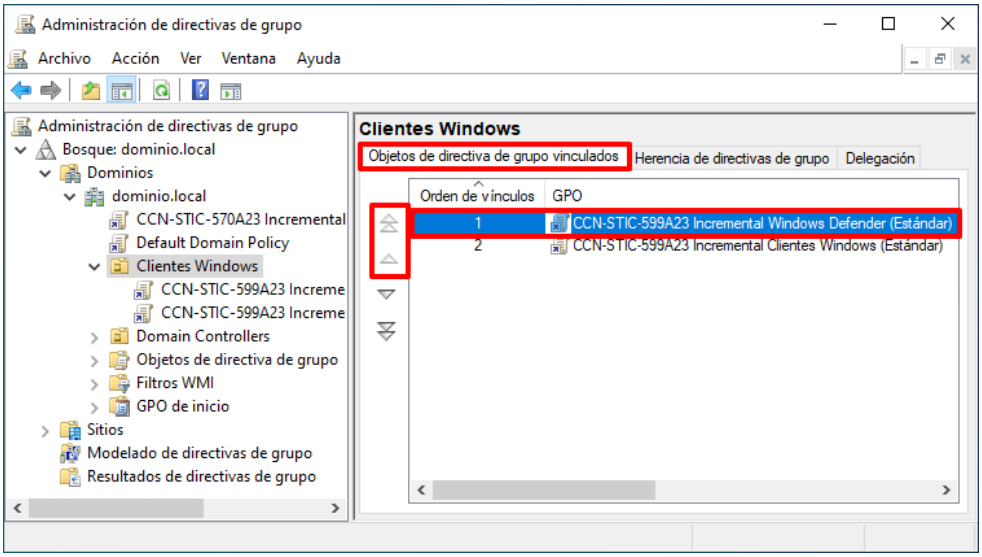
Paso	Descripción
14.	En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
15.	Para completar el asistente pulse sobre el botón “Finalizar”.
16.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores pulse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

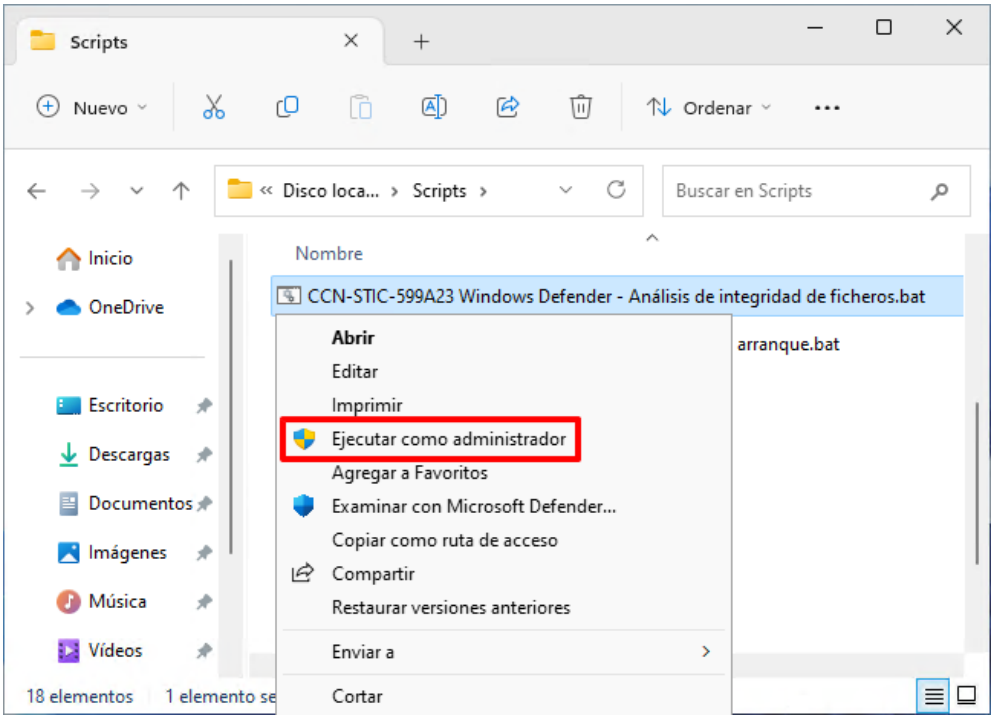
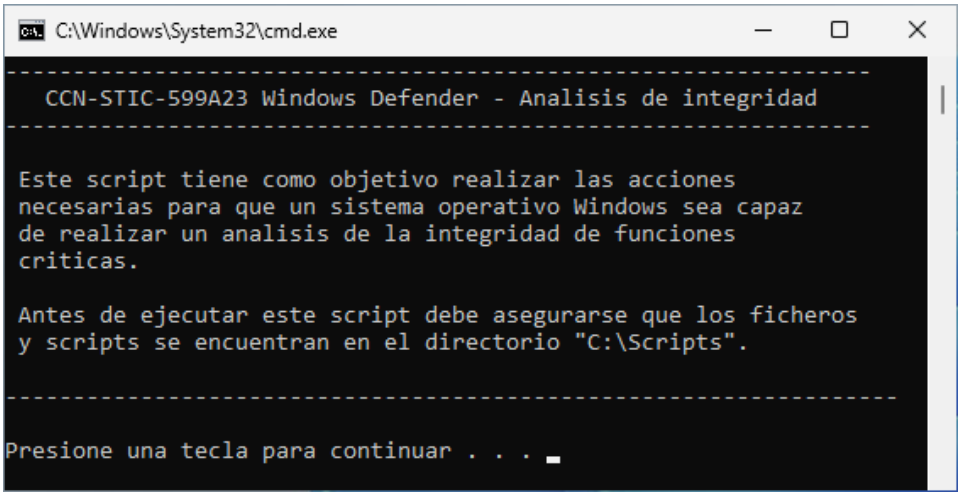
Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO])” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá.  **Nota:** Edite el objeto GPO acorde al perfil de seguridad que desea aplicar. En este ejemplo 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.
19.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“CCN-STIC-599A23 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. 

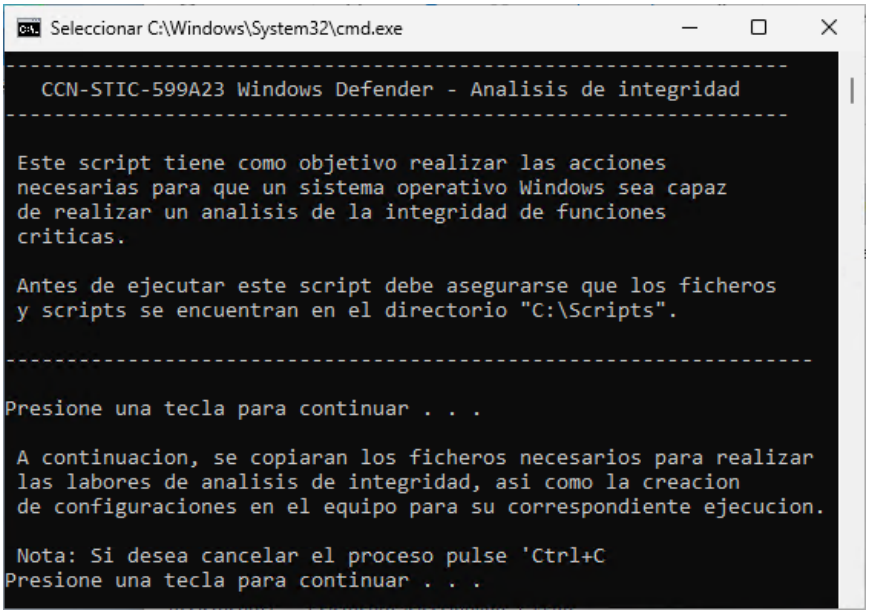
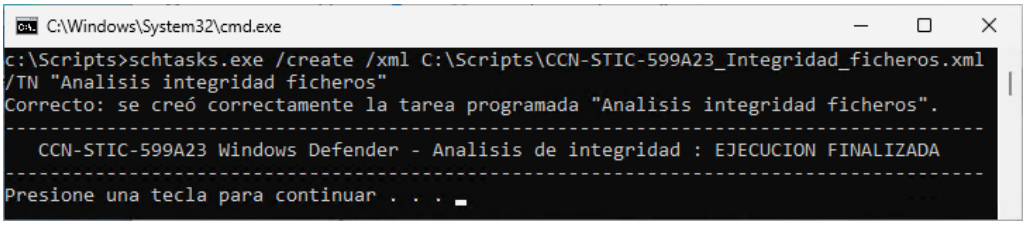
Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO]).inf". A continuación, pulse sobre el 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".
21.	A continuación, despliegue el nodo: **"CCN-STIC-599A23 Incremental Windows Defender ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Detección".** 

Paso	Descripción
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 
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”.

Paso	Descripción
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 “Clientes Windows”, creada para tal fin.
26.	A continuación, seleccione el objeto GPO “CCN-STIC-599A23 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”.

Paso	Descripción
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. 
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.1.2.2 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.

Paso	Descripción
29.	A continuación, diríjase al directorio "C:\Scripts" del cliente miembro del dominio, haga clic derecho sobre el fichero "CCN-STIC-599A23 Windows Defender – Análisis de integridad de ficheros.bat" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Identifique los clientes miembros del 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. 

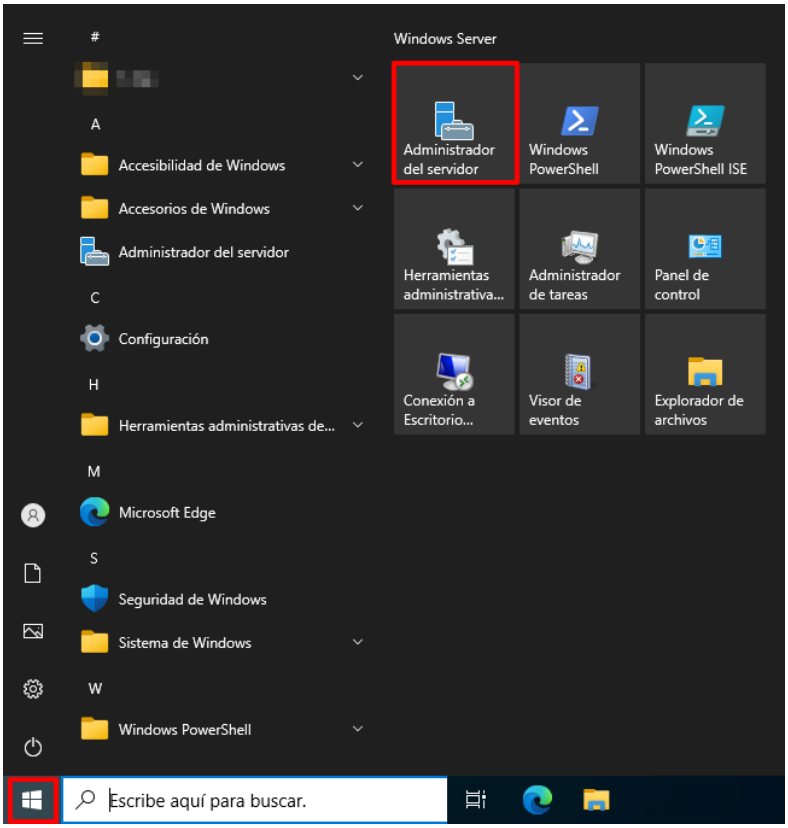
Paso	Descripción
31.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 
32.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
33.	Con esto habrá configurado el equipo para que se realice una comprobación de la integridad 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.

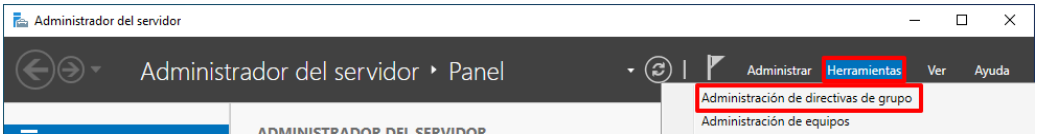
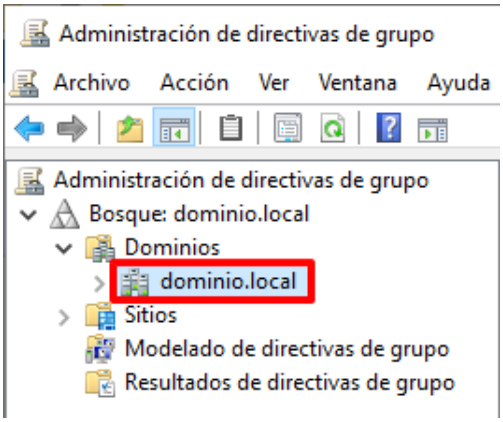
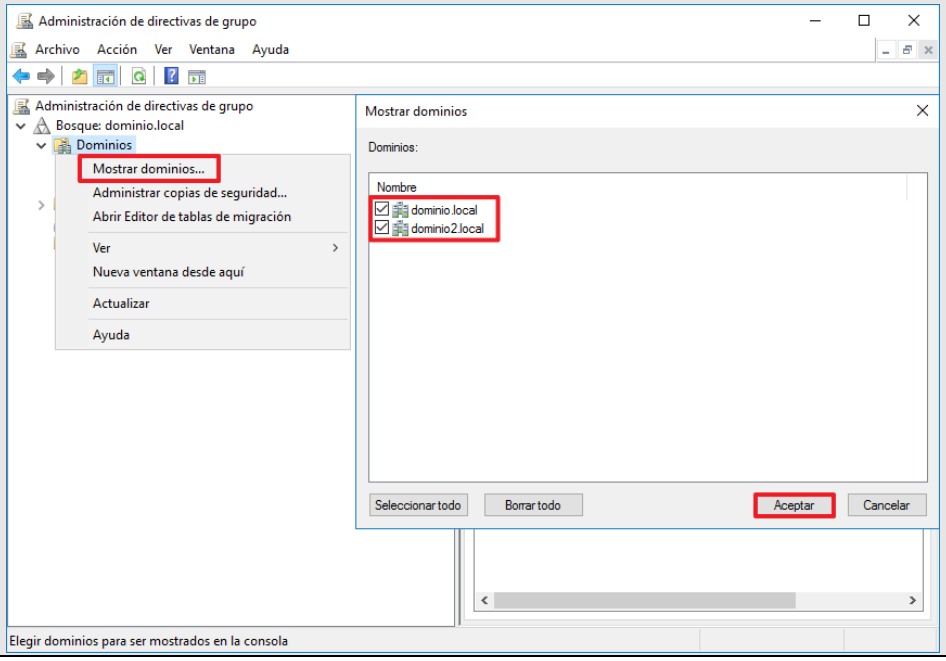
ANEXO A.2.3.1. PROTECCIÓN FRENTE A CÓDIGO DAÑINO (USO OFICIAL – MATERIAS CLASIFICADAS)

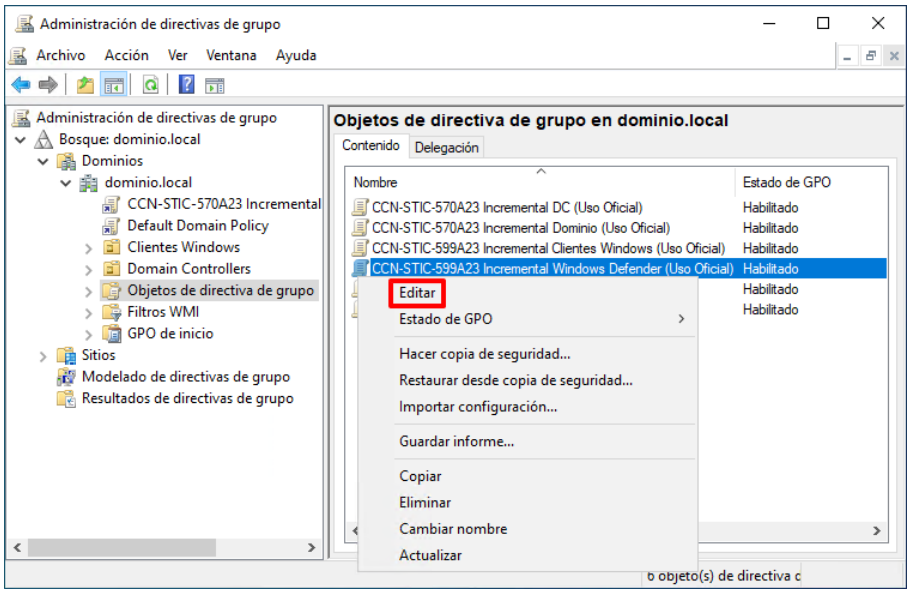
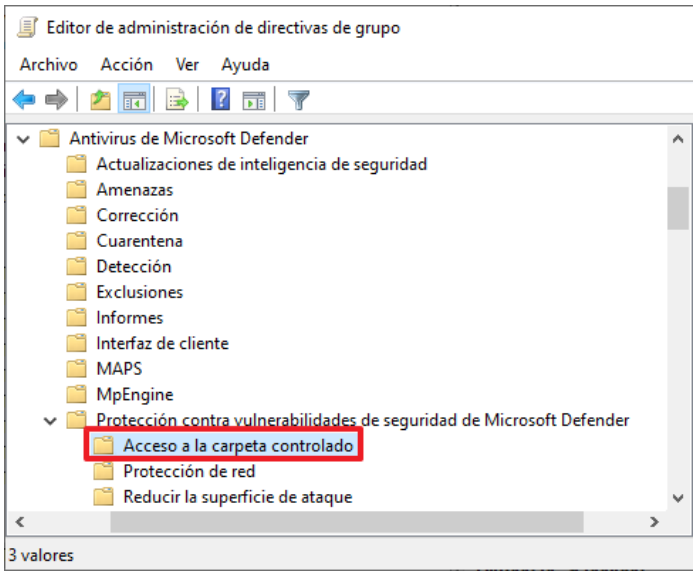
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

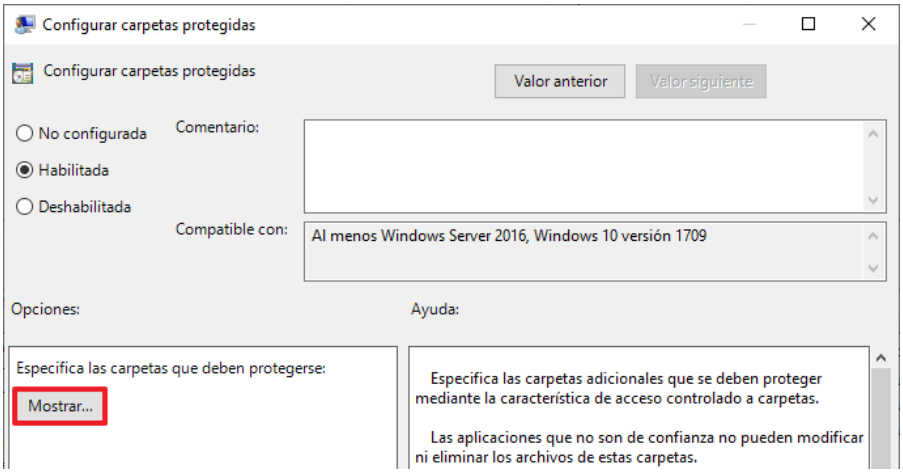
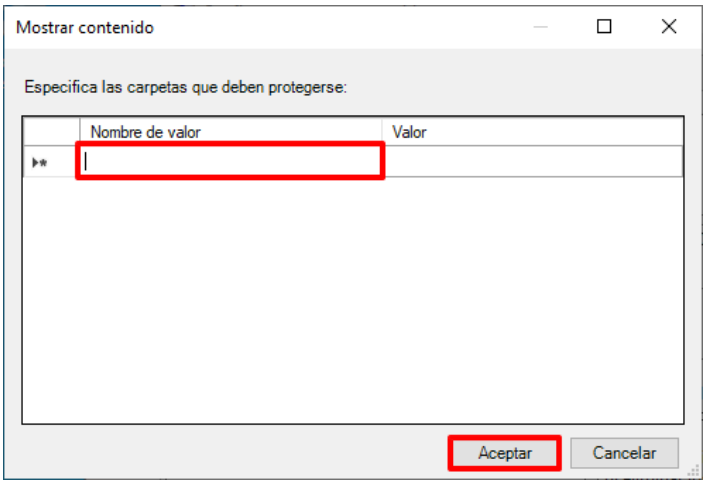
Las configuraciones definidas bajo el presente apartado tratan de impedir las modificaciones no autorizadas bajo directorios protegidos por el software contra código dañino, evitando de este modo la infección contra ramsonware.

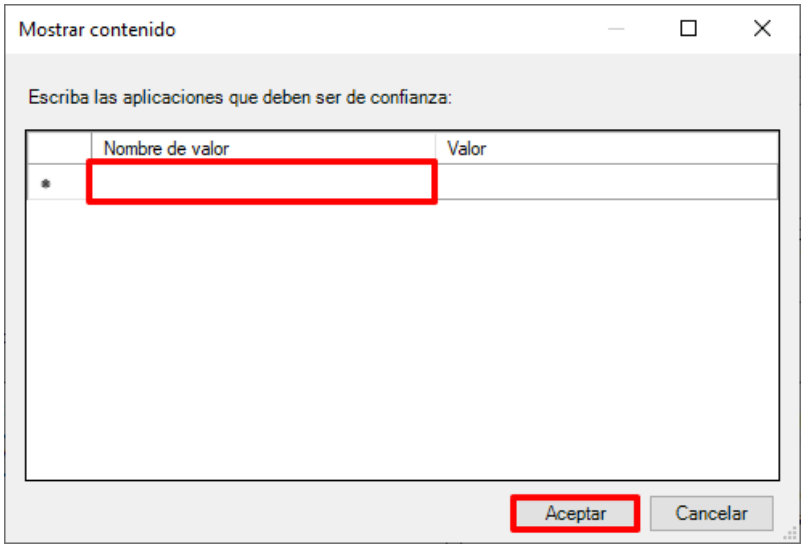
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

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-599A23 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.
40.	A continuación, despliegue el nodo: **“CCN-STIC-599A23 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…". 
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

Paso	Descripción
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…".
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 A.2.3.2. 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:

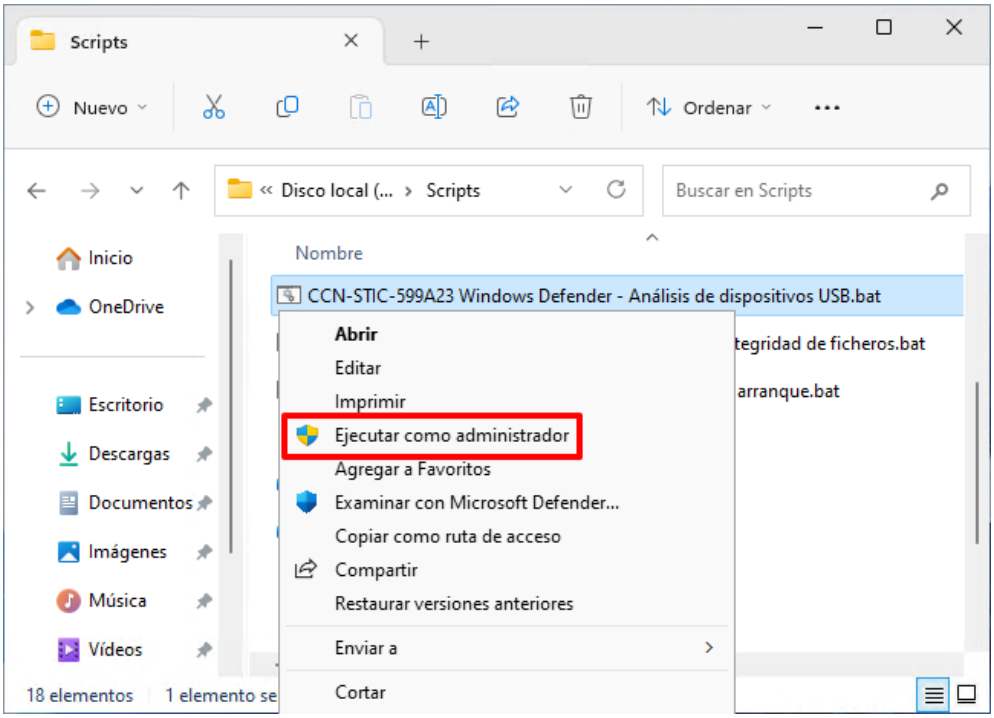
a) Análisis de dispositivos de almacenamiento extraíble cuando estos se conectan al equipo.

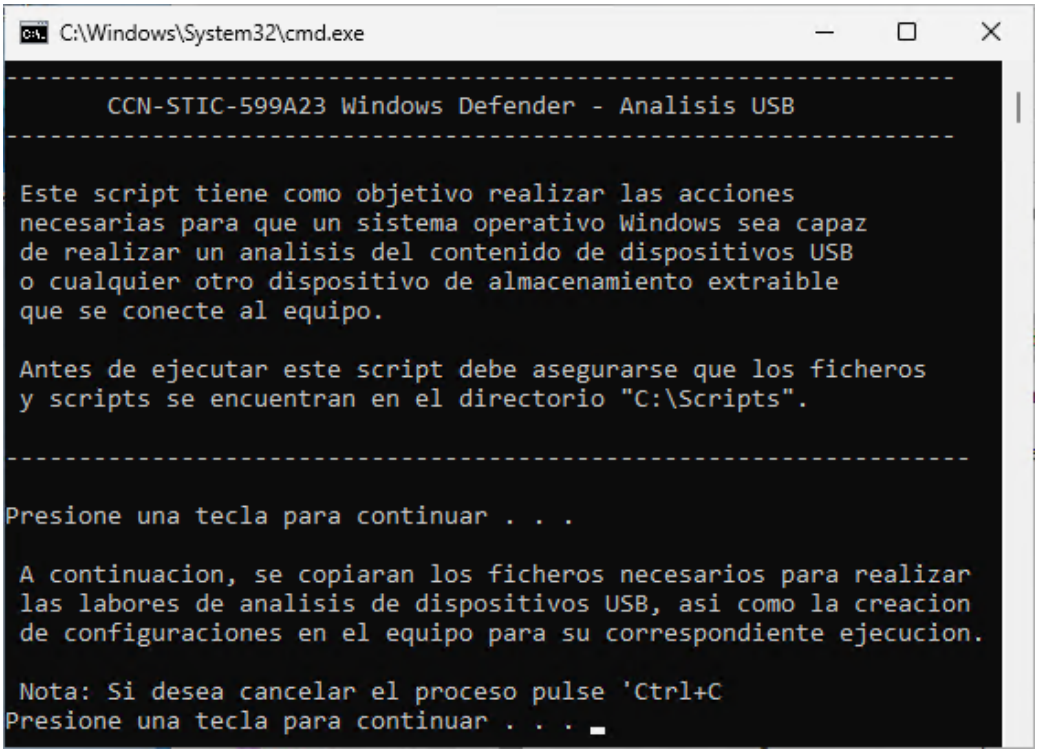
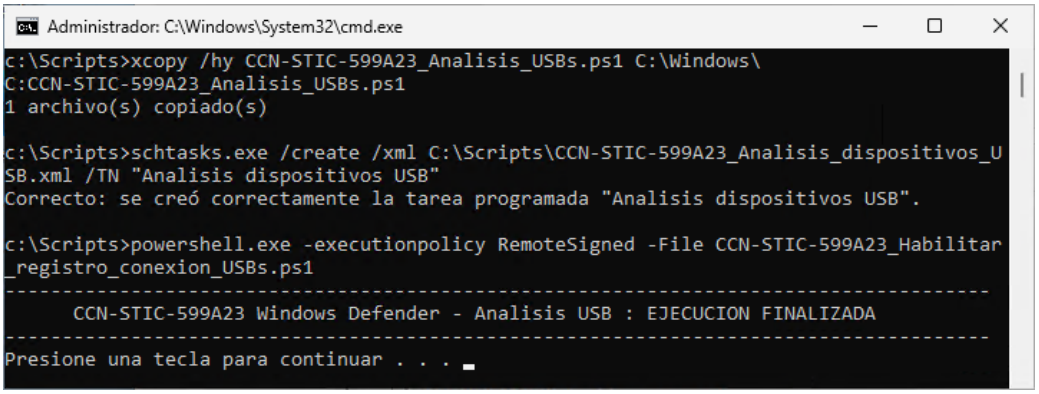
b) Análisis del sistema operativo en el arranque del sistema.

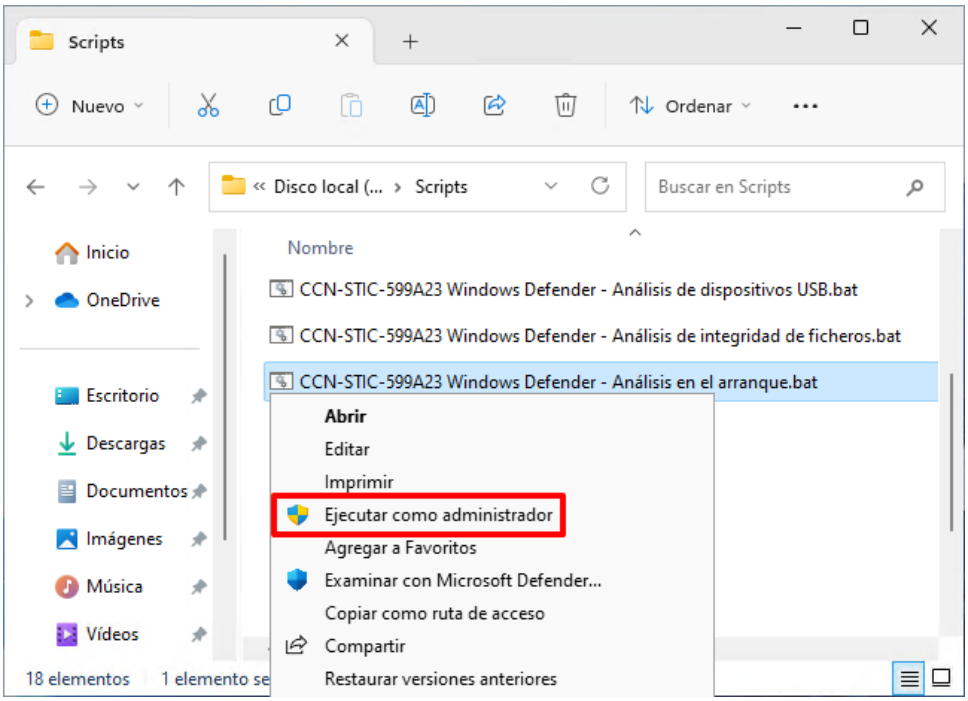
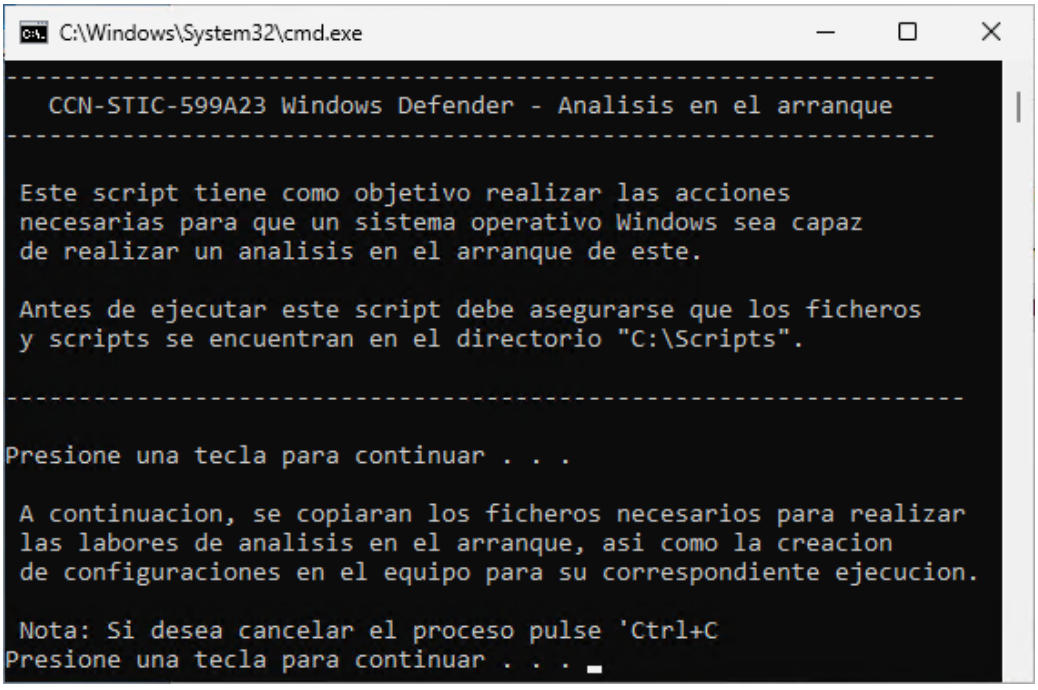
No se considera de aplicación las configuraciones del presente apartado si no se han aplicado el resto de configuraciones de esta herramienta según el punto "ANEXO A.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO".

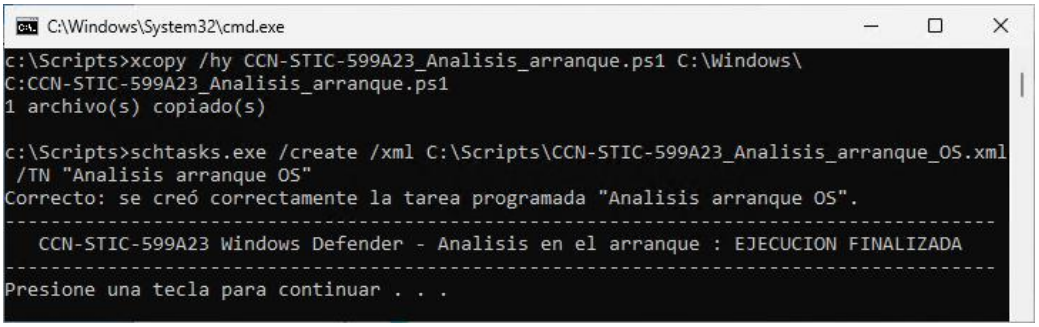
Tenga en consideración que estas configuraciones pueden afectar al rendimiento del sistema operativo.

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
46.	Inicie sesión en un cliente miembro perteneciente al dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
47.	Diríjase al directorio "C:\Scripts", haga clic derecho sobre el fichero "CCN-STIC-599A23 Windows Defender – Análisis de dispositivos USB.bat" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
48.	Pulse cualquier tecla para continuar.

Paso	Descripción
49.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 
50.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
51.	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
52.	De nuevo, en el directorio “C:\Scripts” haga clic derecho sobre el fichero “CCN-STIC-599A23 Windows Defender – Análisis en el arranque.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
53.	Pulse una tecla para continuar.
54.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 

Paso	Descripción
55.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
56.	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 A.2.4. PROTECCIÓN DE LA INTEGRIDAD Y LA AUTENTICIDAD

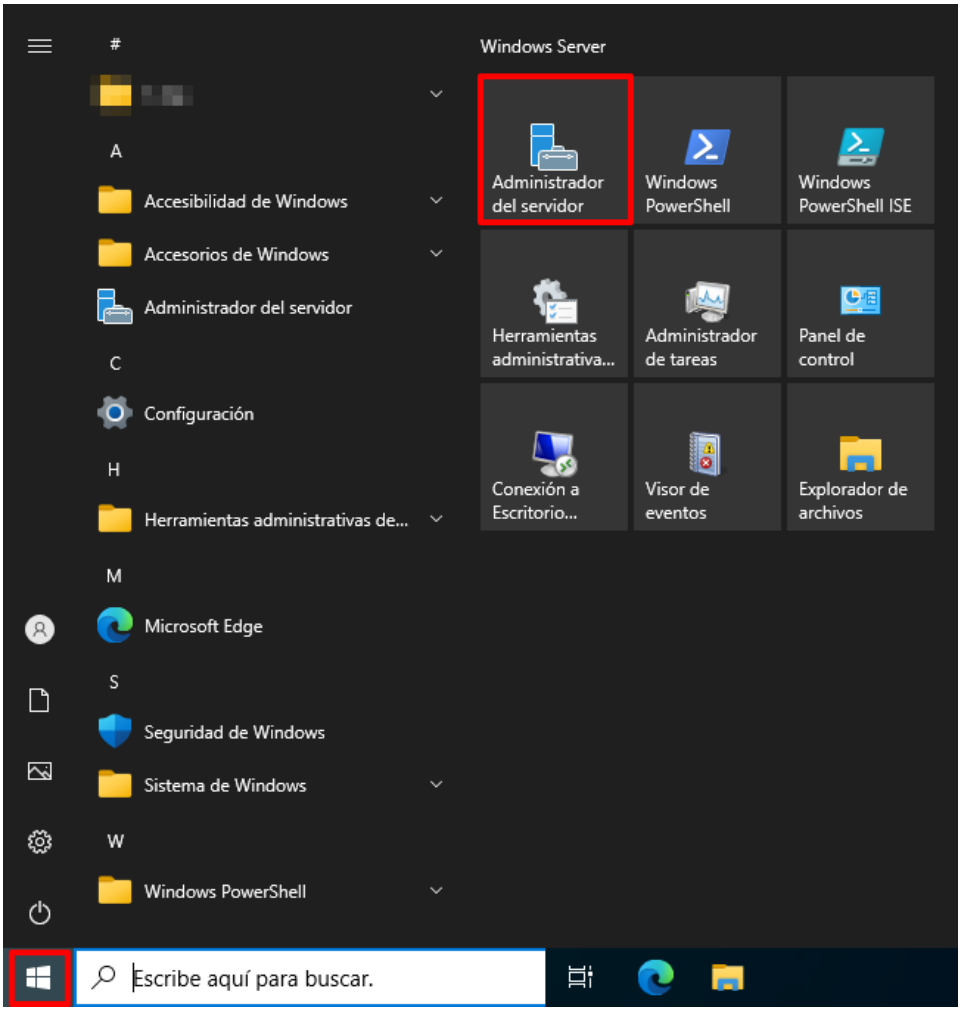
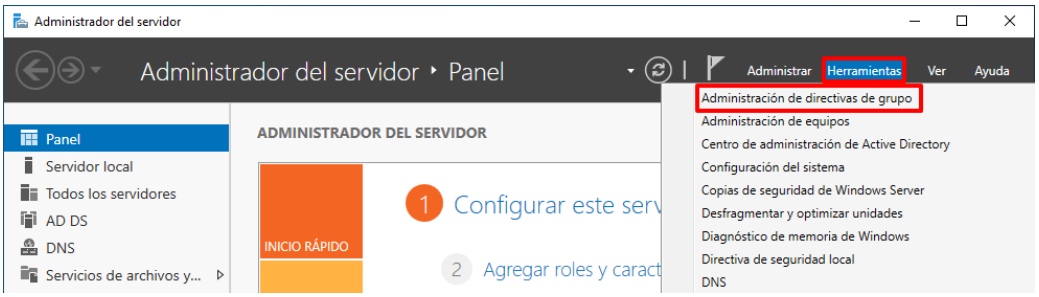
El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación del cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los equipos tipo Cliente Miembro.

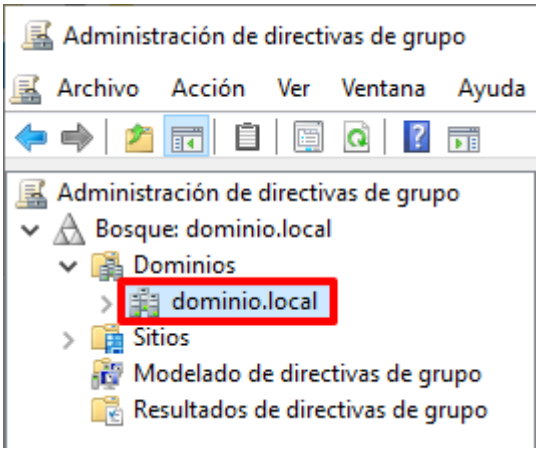
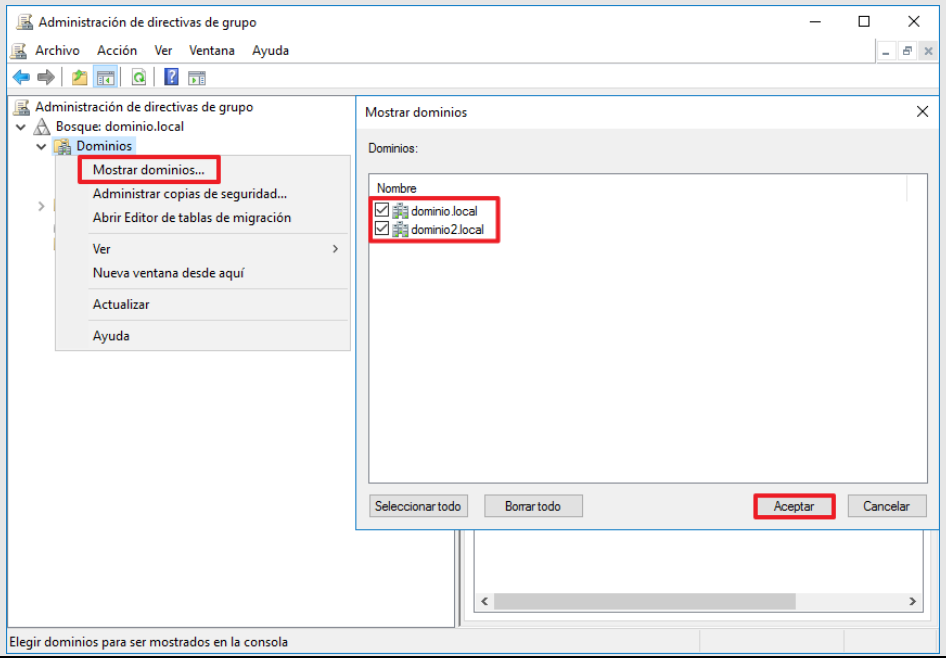
Debe tenerse en consideración que la implementación de un firewall de cliente dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que éste utilice de la infraestructura. No se tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, en un cliente que se utilice únicamente para usar Microsoft Office que un cliente utilizado para la compartición de unidades en red.

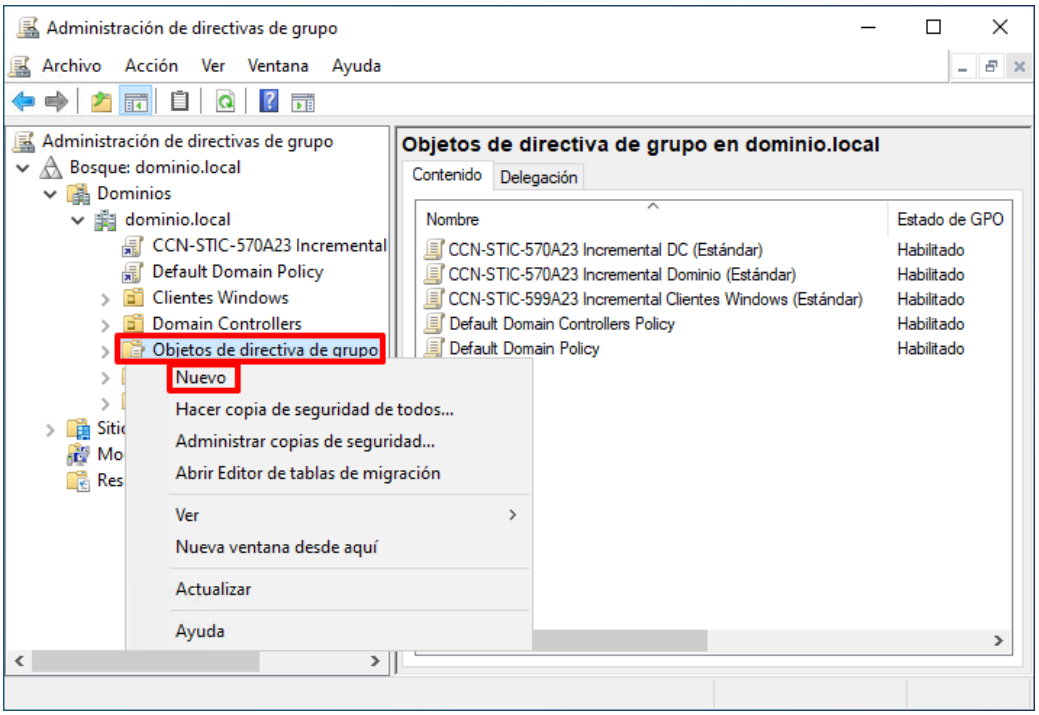
Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos para un conjunto de clientes miembro que necesitan que Configuration Manager pueda controlarlos remotamente, utilizando los puertos 135 y 2701.

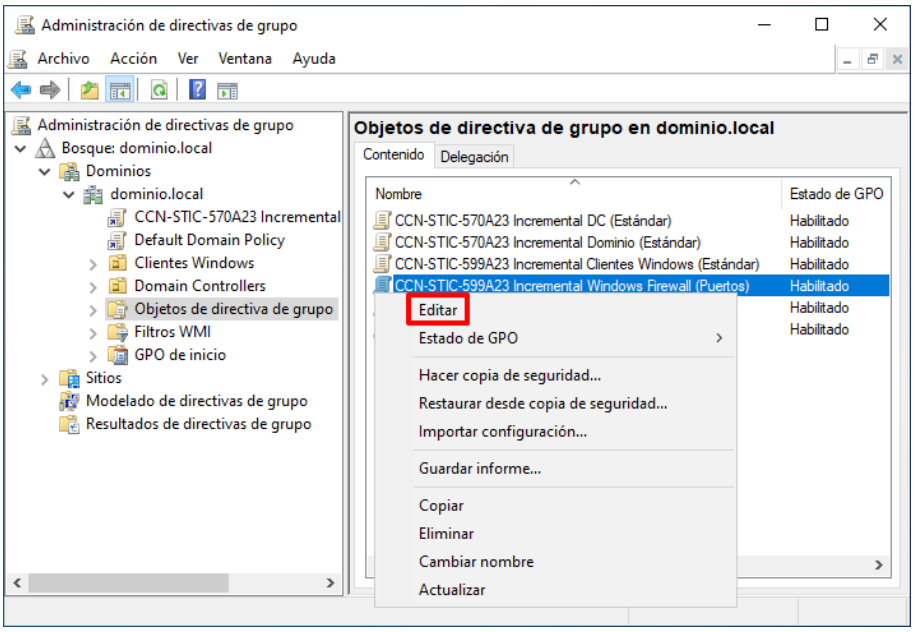
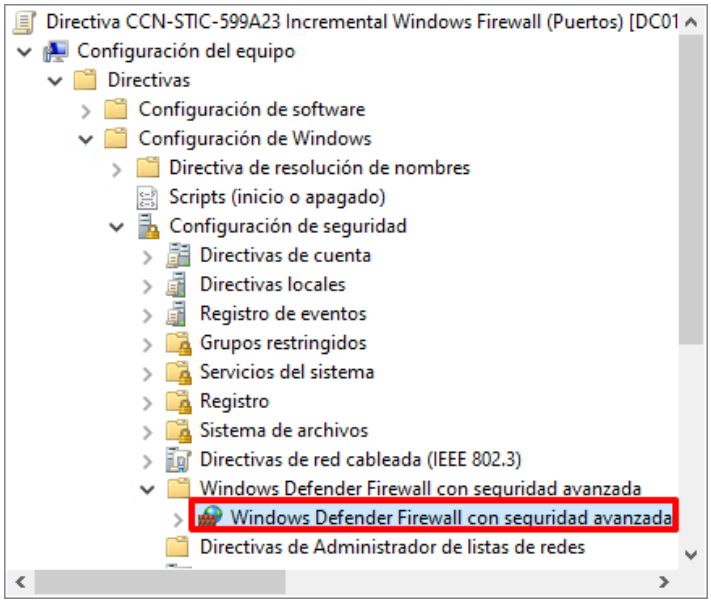
Por otro lado, si en su organización dispone de otro software que sustituya el firewall por defecto de Windows y este se encuentra habilitado y configurado podrá ignorar los siguientes pasos y continuar en el siguiente punto.

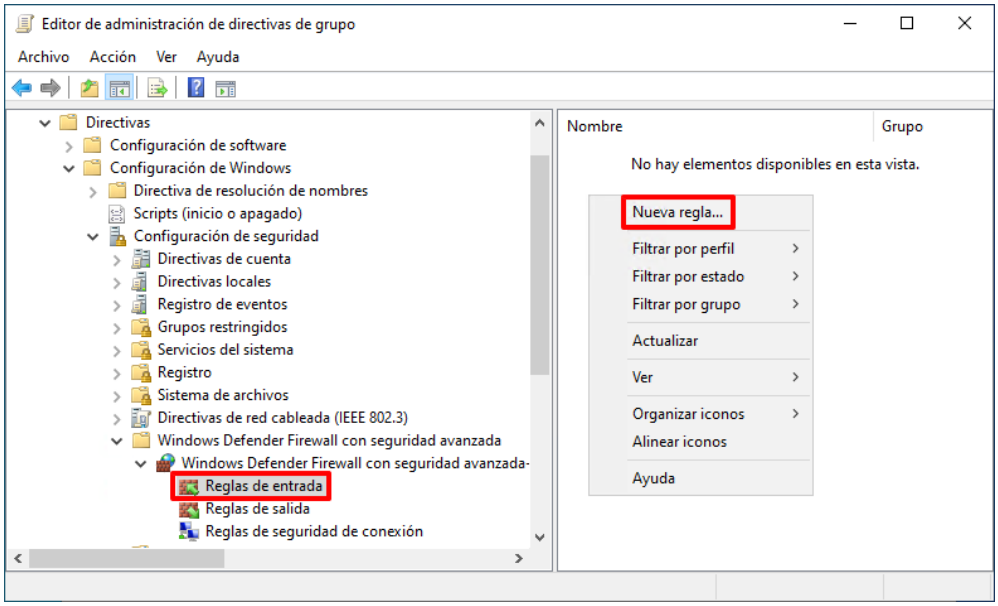
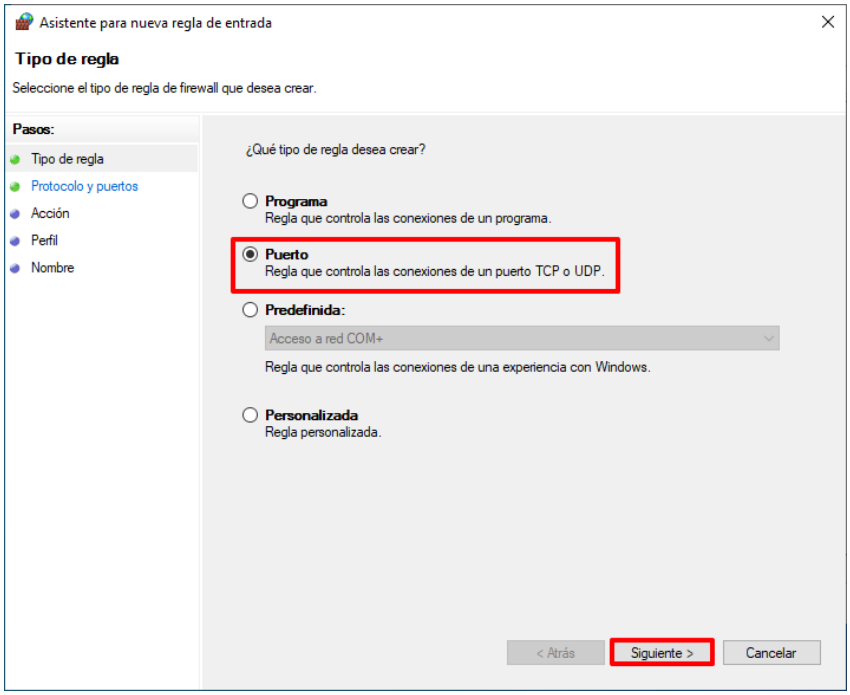
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

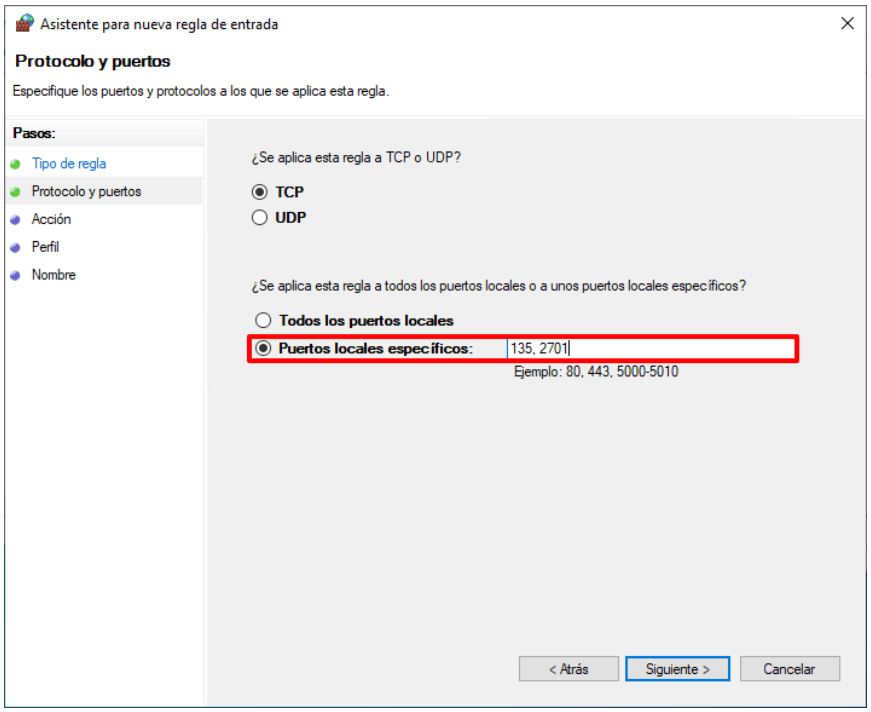
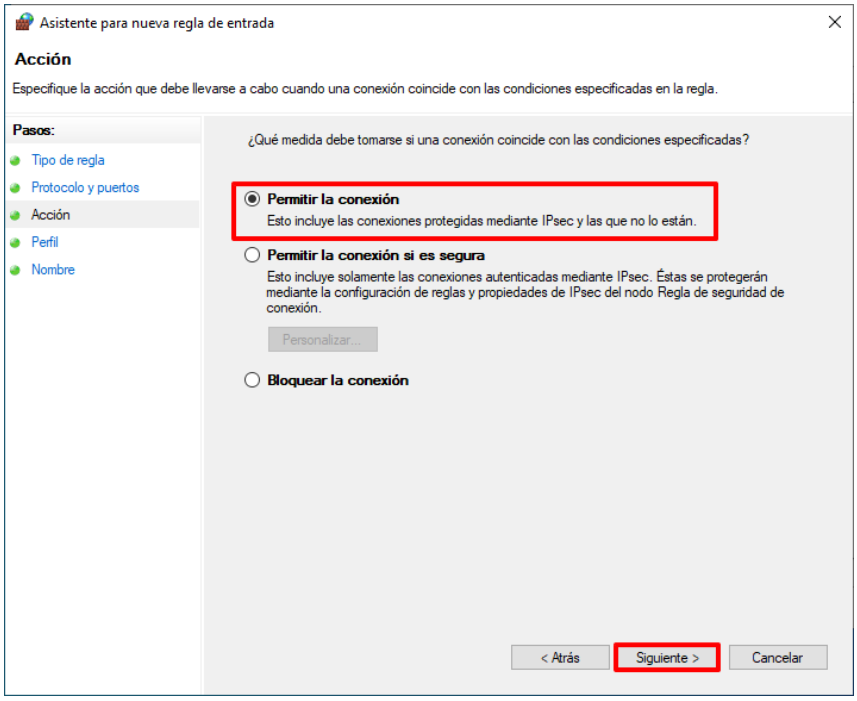
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

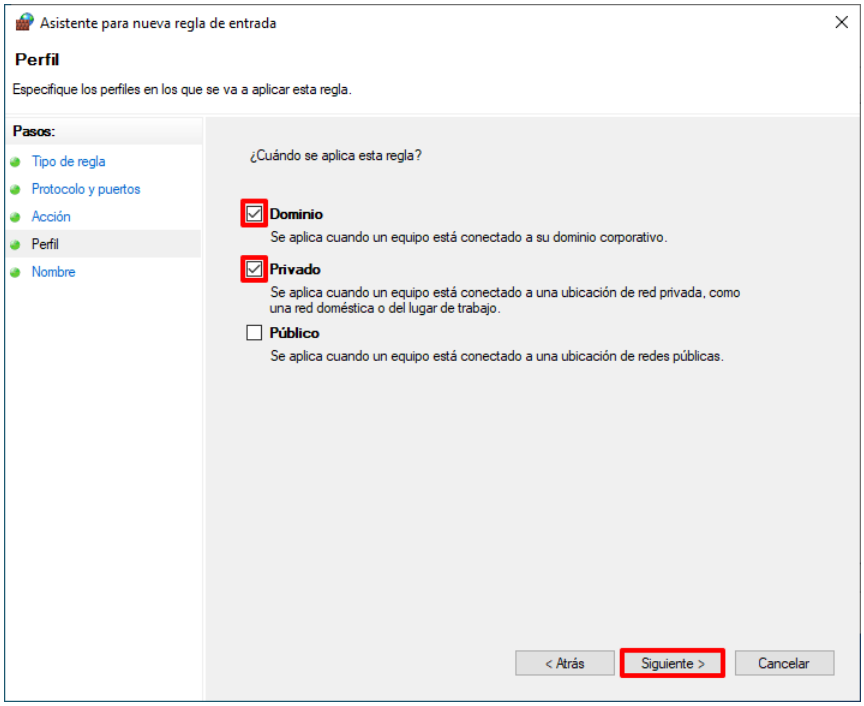
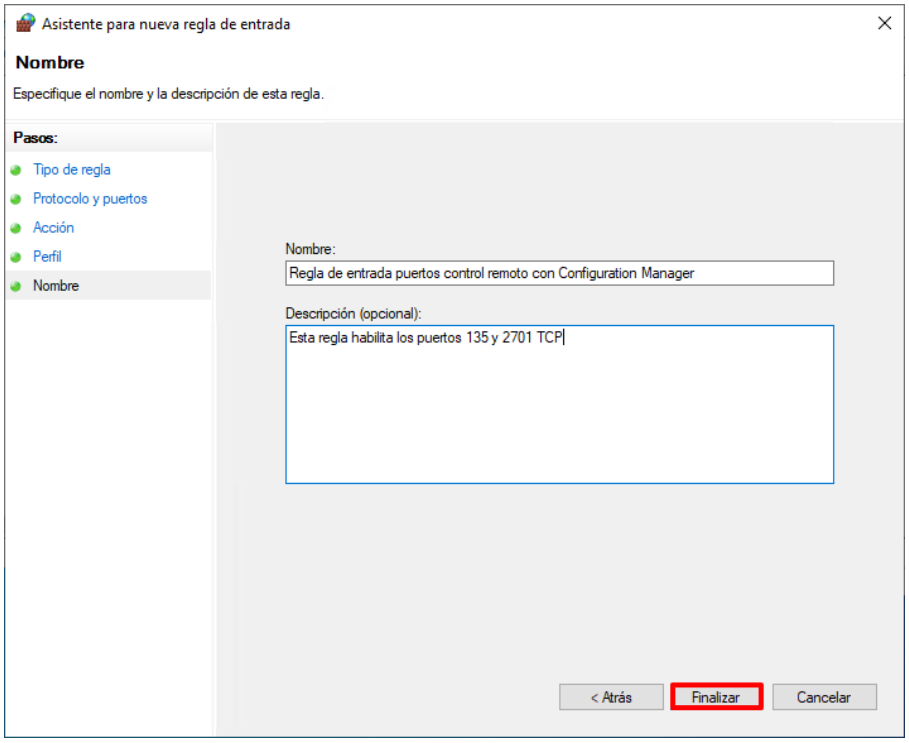
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

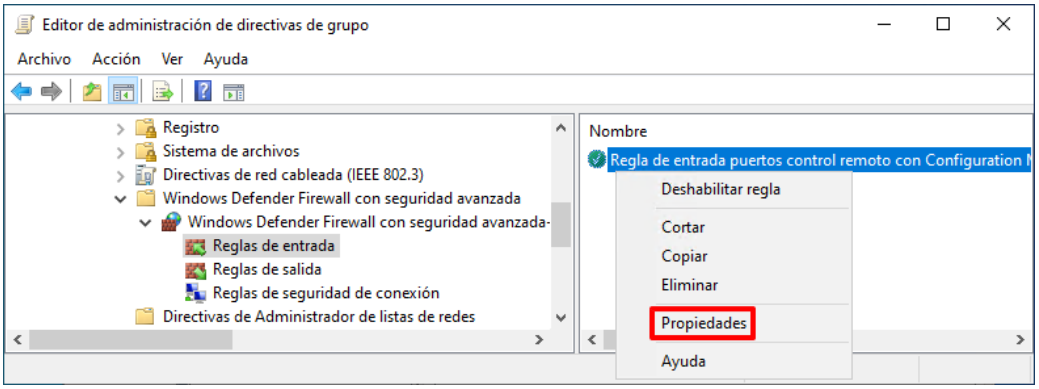
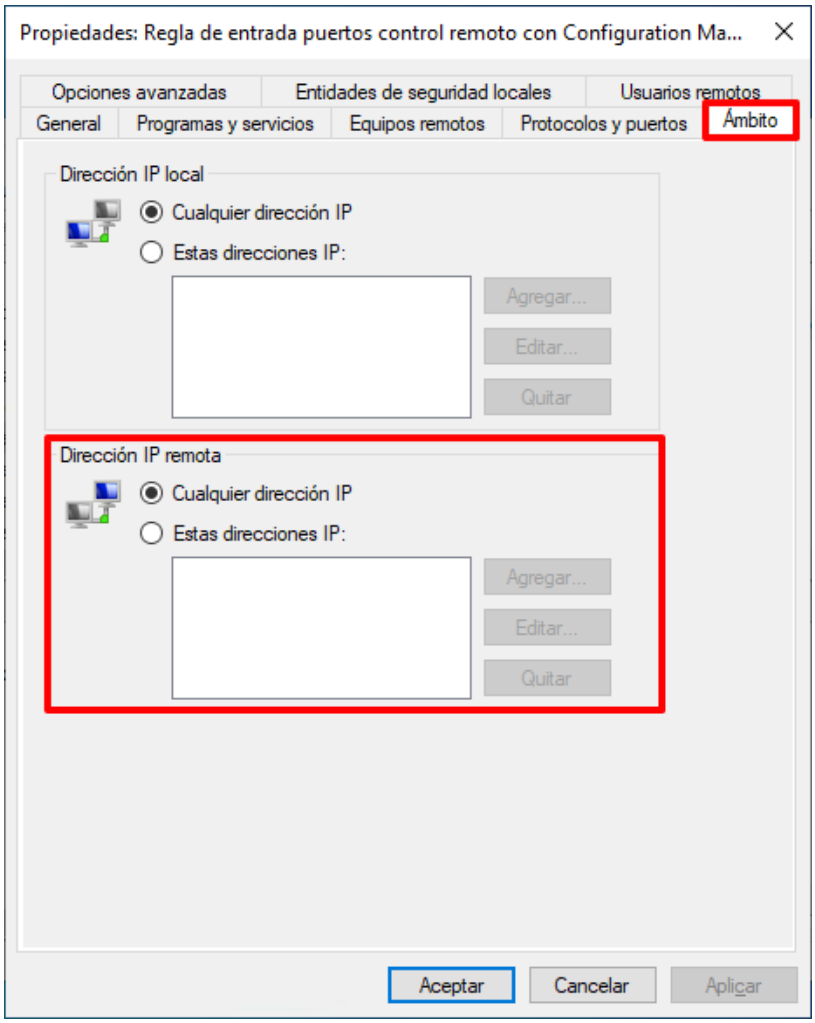
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental Windows Firewall (Puertos)**" y pulse el botón "Aceptar". 

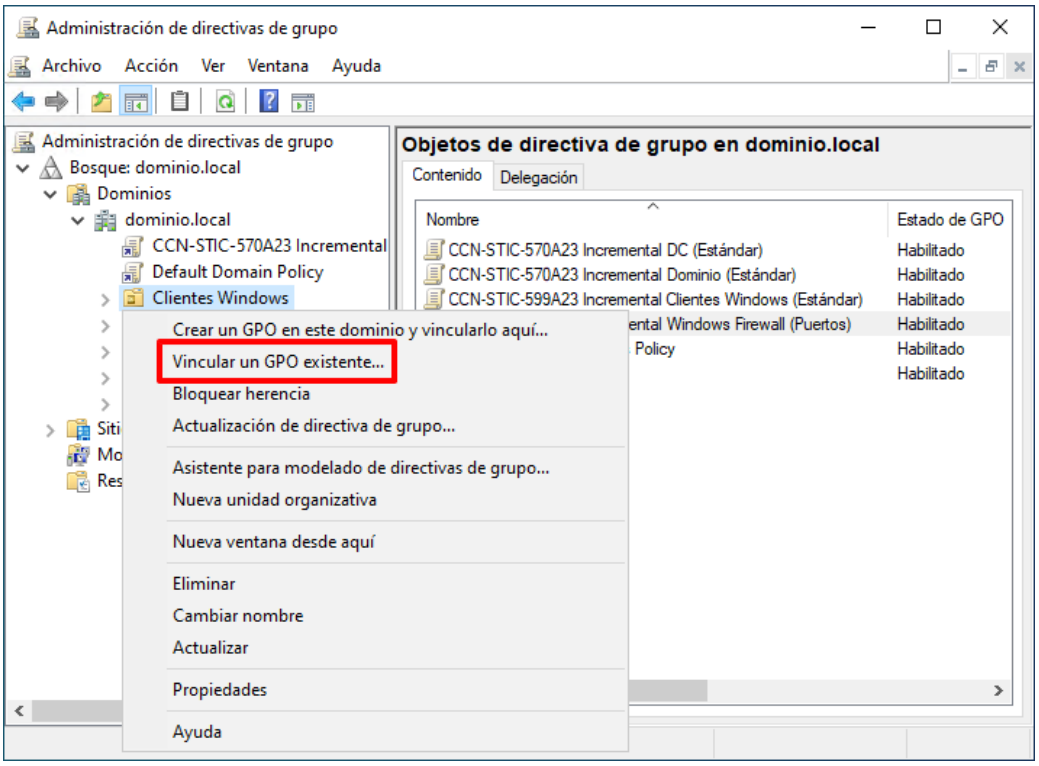
Paso	Descripción
7.	Seleccione de nuevo el objeto GPO “CCN-STIC-599A23 Incremental Windows Firewall (Puertos)” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá. 
8.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
9.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“CCN-STIC-599A23 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=...”**. 

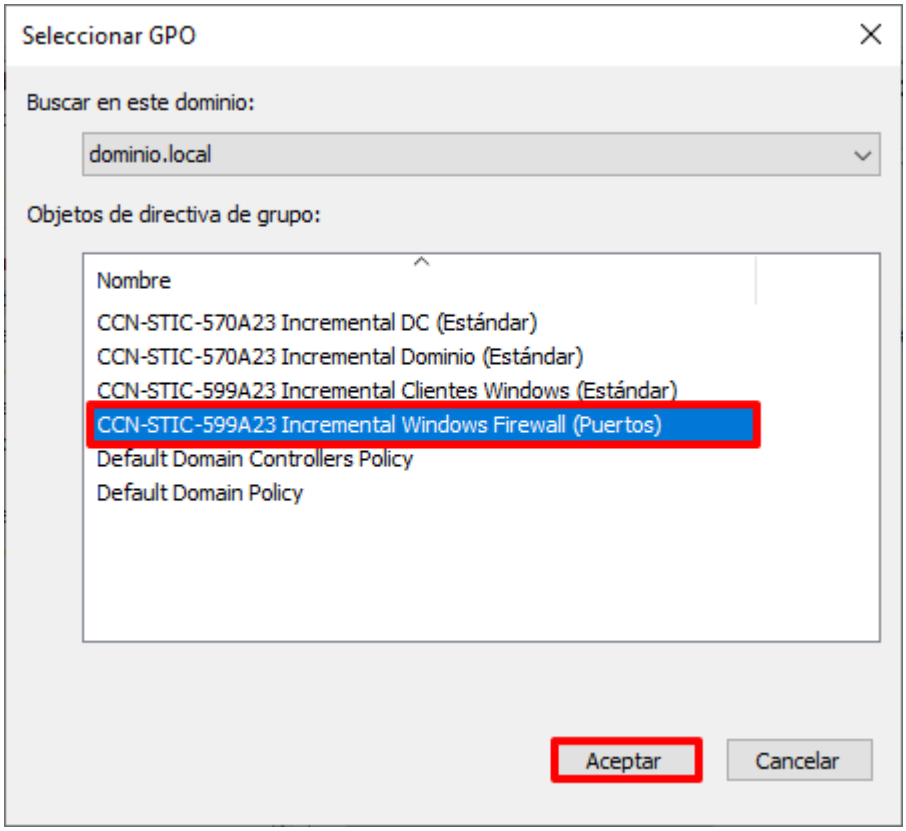
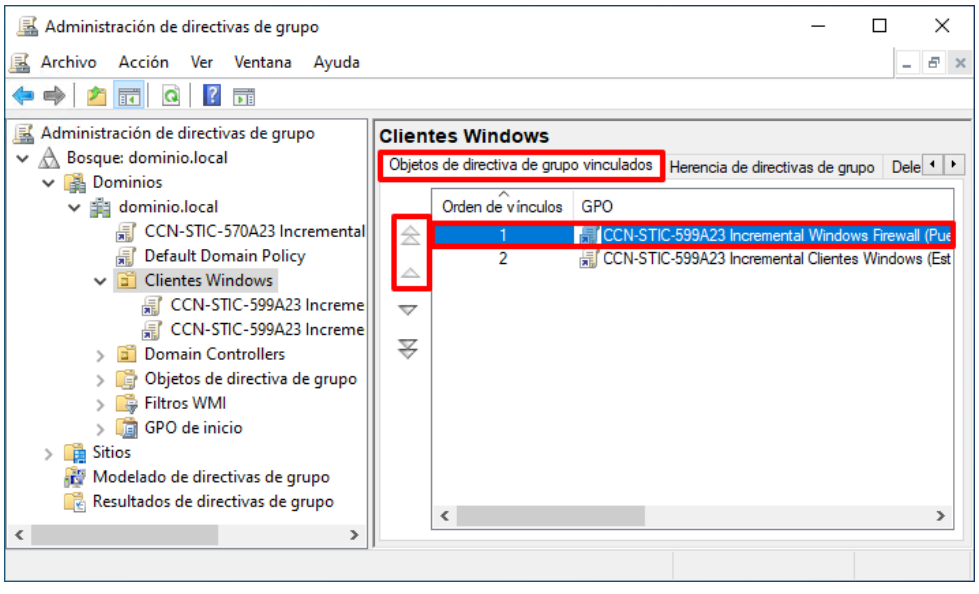
Paso	Descripción
10.	Despliegue el nodo “Windows Defender Firewall con seguridad avanzada y seleccione “Reglas de entrada”. A continuación, pulse sobre con el botón derecho sobre un espacio en blanco en el panel derecho de la consola y seleccione “Nueva regla…”. 
11.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 

Paso	Descripción
12.	En la opción de “Puertos locales específicos” introduzca “135, 2701”. Si los clientes miembro necesitan otros puertos para el correcto funcionamiento, debería introducir también dichos puertos. Pulse el botón “Siguiente >”.  **Nota:** Deberá tener en consideración el protocolo, siendo en este ejemplo TCP.
13.	En la pantalla de “Acción”, mantenga la configuración “Permitir la conexión” y pulse el botón “Siguiente >”. 

Paso	Descripción
14.	En la ventana “Perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 
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. 

Paso	Descripción
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”. 
17.	Podría, por ejemplo, limitarse las IP remotas o rangos de redes que podrían conectarse a los clientes miembro a través de los puertos 135 y 2701. De forma predeterminada, se admite cualquier IP, pero podría establecerse un límite a las mismas mediante la pestaña “Ámbito”. 

Paso	Descripción
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”.
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 “Clientes Windows”, creada para tal fin.

Paso	Descripción
21.	A continuación, seleccione el objeto GPO "CCN-STIC-599A23 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.1.2.2 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 A.2.5. 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:

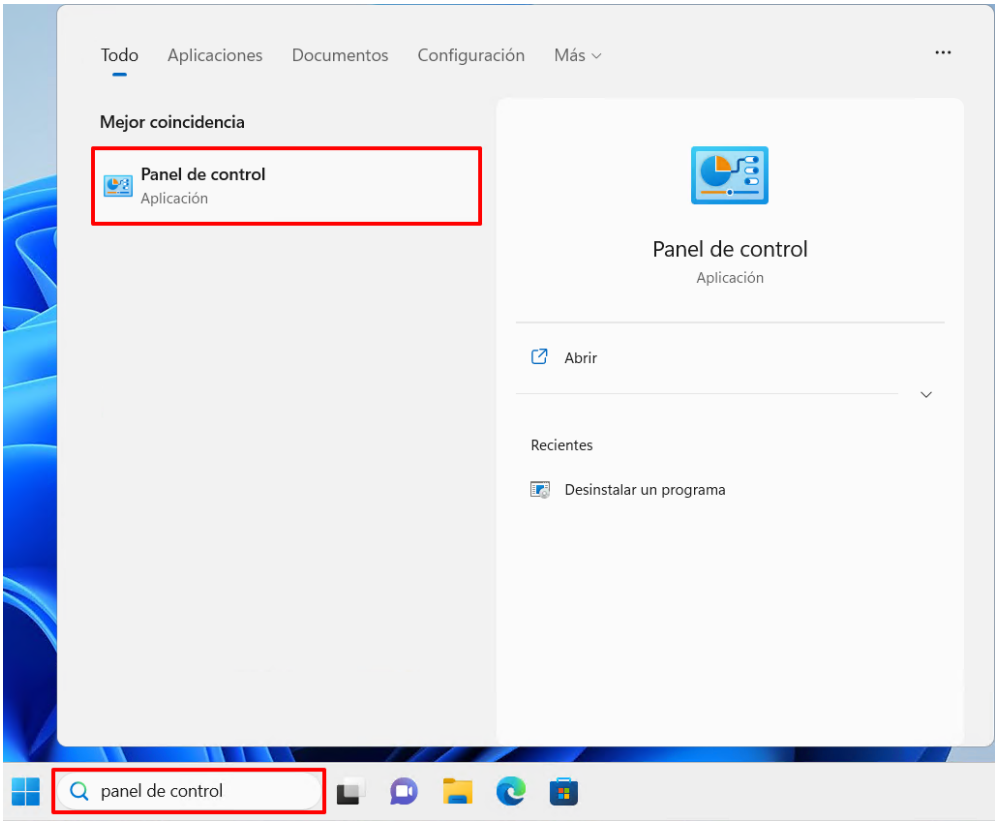
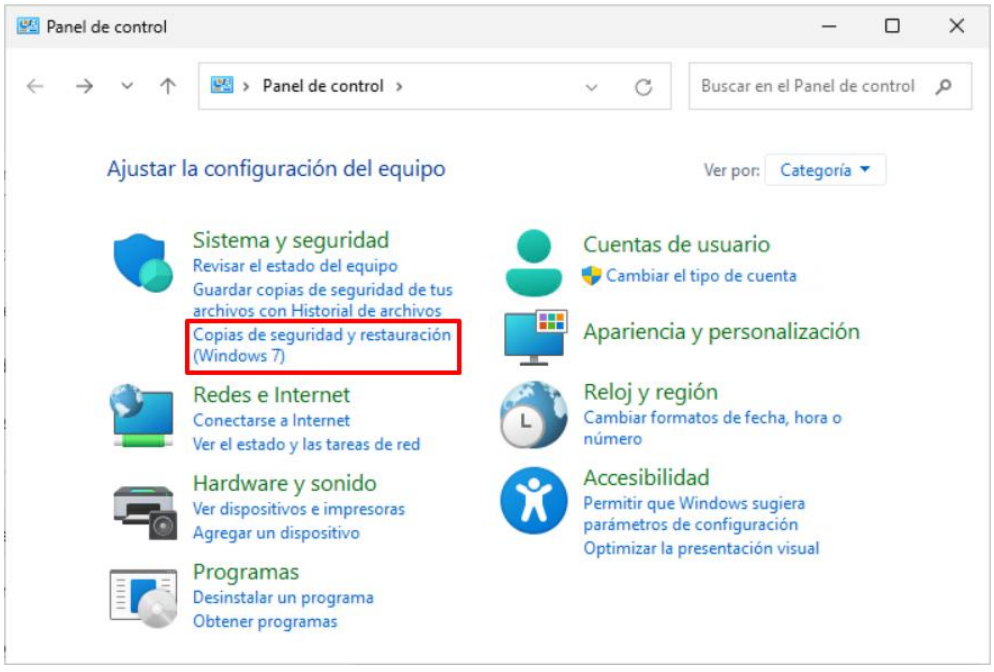
a) Deberá disponer de un espacio adicional donde alojar las copias realizadas.

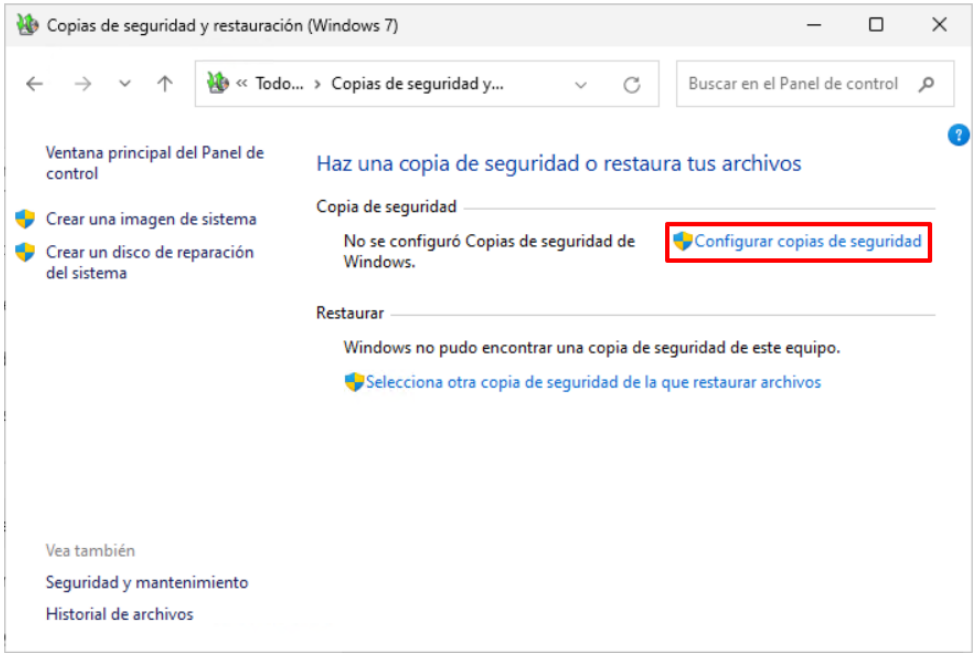
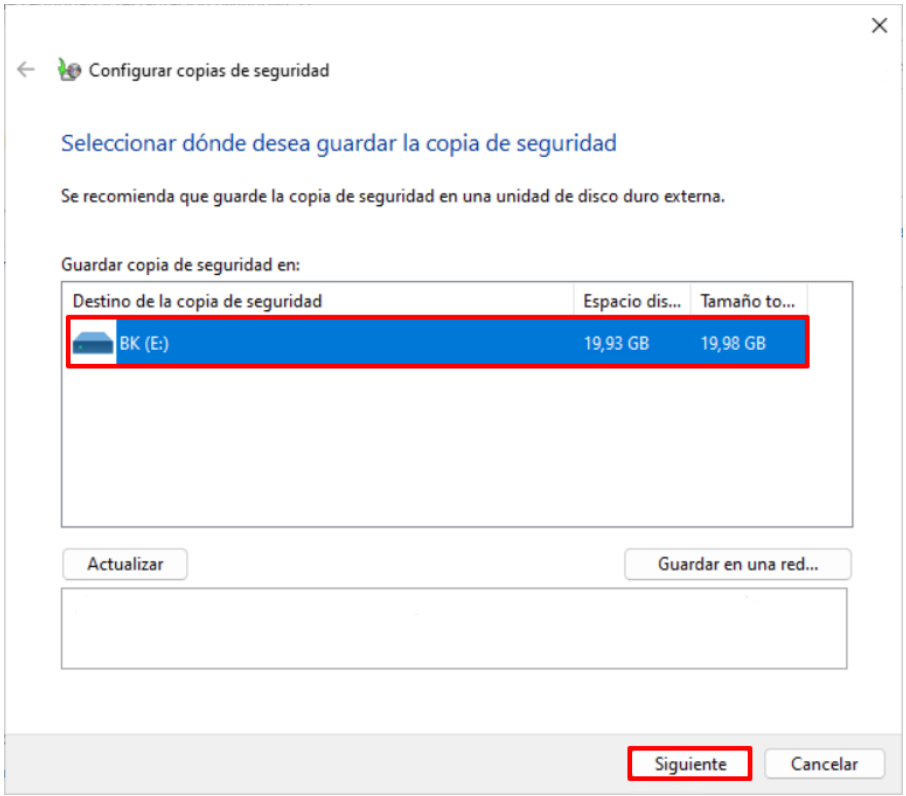
b) El uso de esta herramienta es de uso local por lo que no podrá utilizarse como mecanismo central de gestión de copias, aunque existe la posibilidad de programar dichas copias y alojarlas todas en una misma ubicación remota, de modo que estas se encuentren centralizadas.

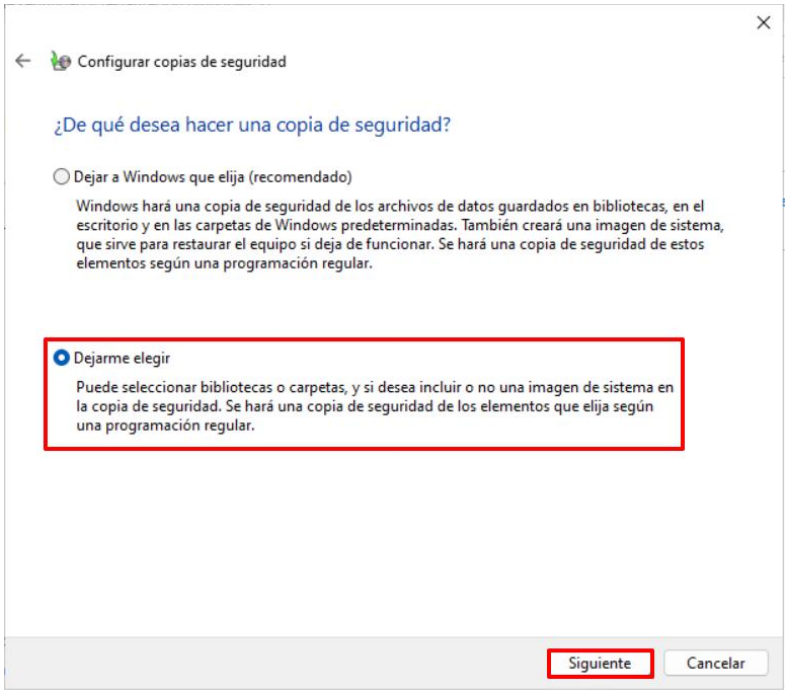
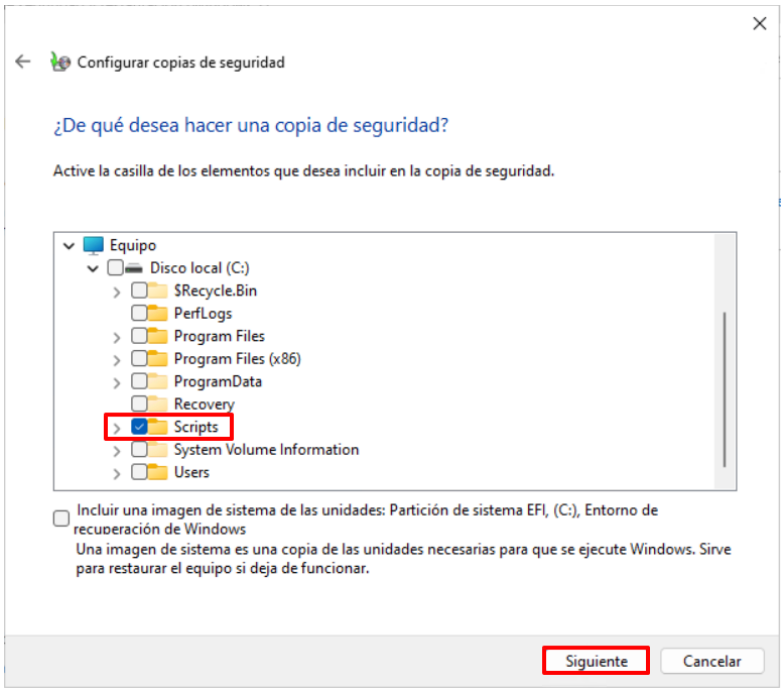
Nota: En este ejemplo se va a realizar una copia de seguridad puntual en el tiempo de una carpeta de datos alojada en un equipo de tipo Cliente Miembro.

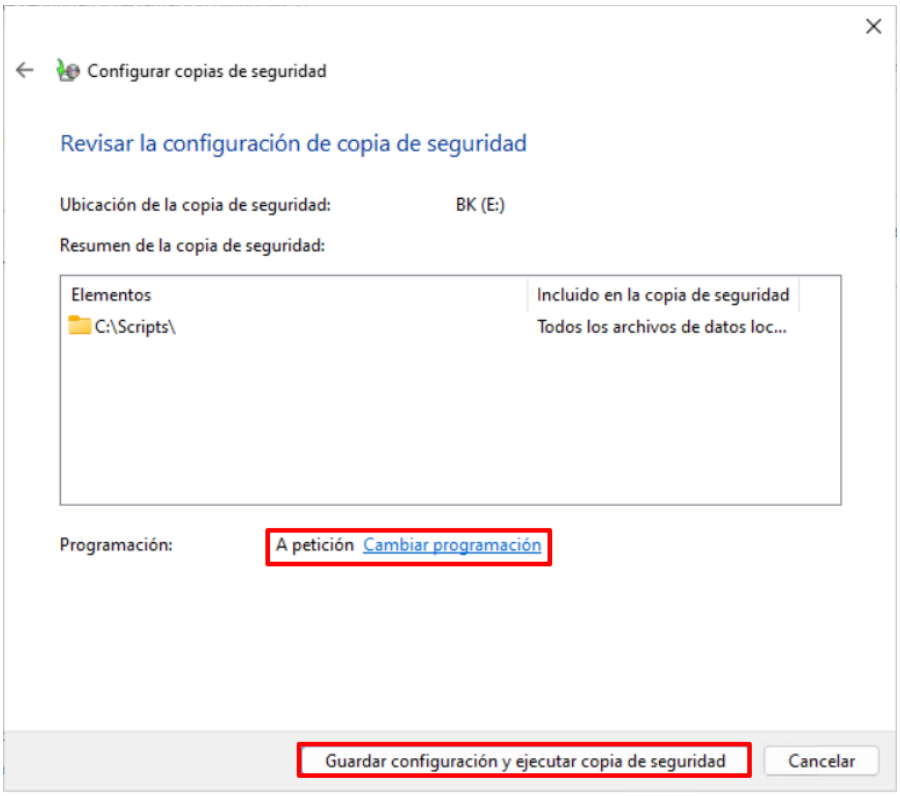
Se recomienda establecer una copia de seguridad programada con el objetivo de que esta se realice de una forma periódica acorde a las políticas de la organización, tomando en consideración su configuración (Completa, Incremental, etc.).

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

Paso	Descripción
2.	En el cuadro de búsqueda busque la aplicación “Panel de control” y una vez encontrada, haga clic sobre la misma. 
3.	En la parte superior izquierda del “Panel de control”, pulse sobre “Copias de seguridad y restauración (Windows 7)” en el apartado “Sistemas y seguridad”. 

Paso	Descripción
4.	En la nueva ventana haga clic sobre la opción “Configurar copias de seguridad”. 
5.	En la primera ventana del asistente seleccione la unidad local donde se va a alojar la copia de seguridad y pulse “Siguiente”.  **Nota:** Dependiendo de la configuración o ubicación donde se desea alojar la copia de seguridad deberá adaptar este paso.

Paso	Descripción
6.	En la siguiente ventana del asistente seleccione la opción “Dejarme elegir” y pulse “Siguiente” para continuar. 
7.	En la nueva ventana deberá seleccionar aquellos directorios y ficheros sobre los que desee realizar la copia de seguridad. Pulse “Siguiente” al finalizar.  **Nota:** Si la copia de seguridad no es del sistema al completo, como es el caso del ejemplo, deberá tener desmarcada la opción “Incluir una imagen de sistema de las unidades: Partición de sistema EFI, (C:), Entorno de recuperación de Windows”.

Paso	Descripción
8.	Establezca una programación para la copia de seguridad que se ajuste a las necesidades de la organización haciendo clic sobre “Cambiar programación”. Una vez establecida, pulse sobre “Guardar configuración y ejecutar copia de seguridad” para realizar la primera copia de seguridad y finalizar con el proceso.  **Nota:** En este caso se ha establecido una programación a petición, teniendo que ejecutar la copia de seguridad de forma manual.

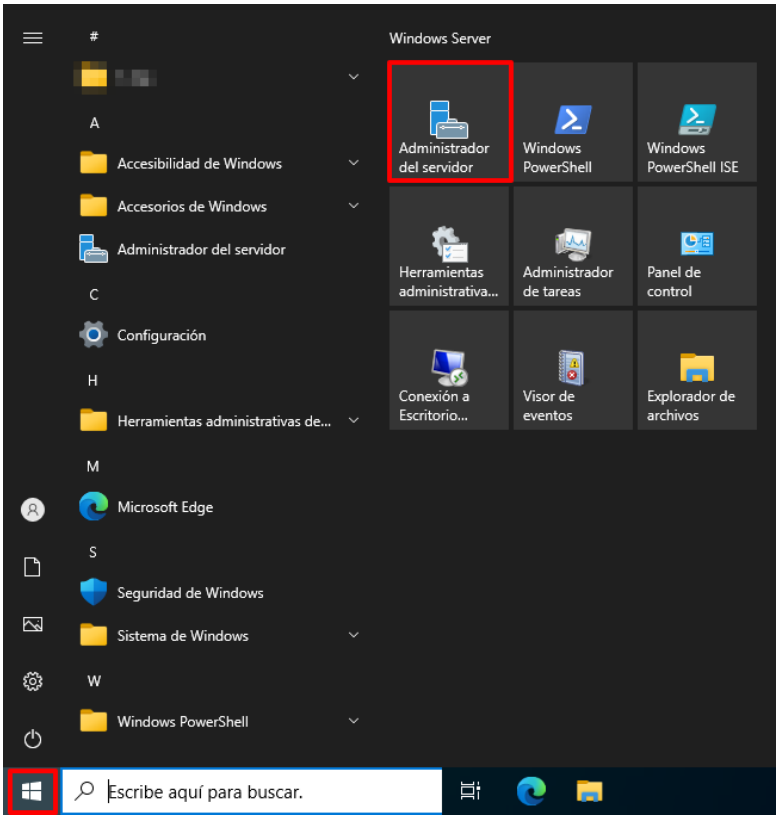
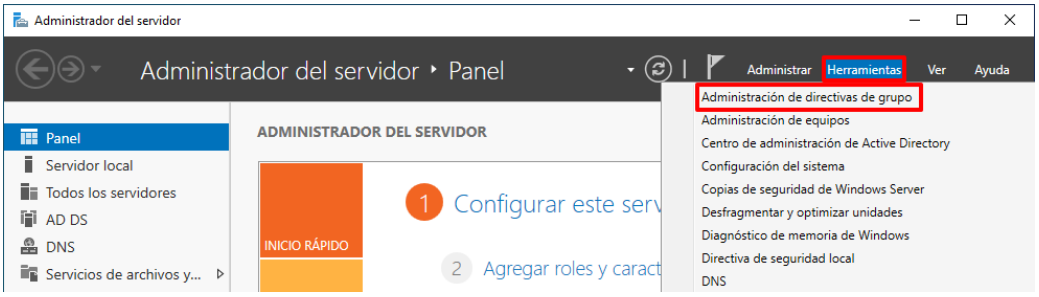
ANEXO A.2.6. PROTECCIÓN DE DISPOSITIVOS PORTÁTILES (USO OFICIAL – MATERIAS CLASIFICADAS)

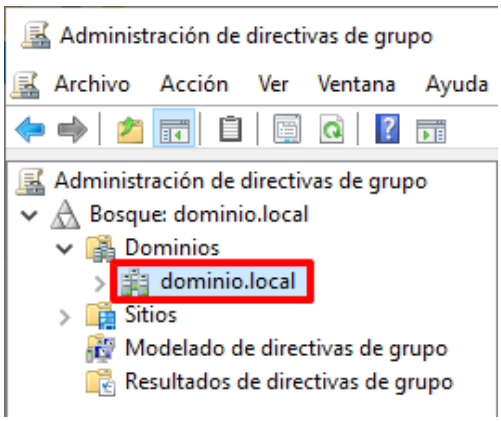
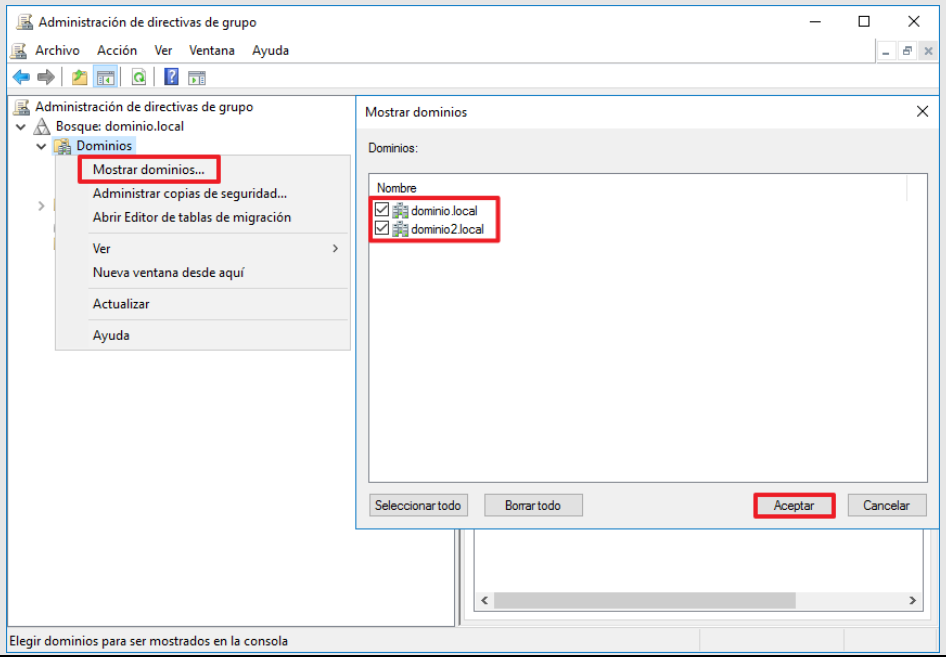
La presente sección tiene como objetivo la configuración y aplicación de directivas de modo que sea posible el cifrado de los sistemas operativos Windows Cliente, o de dispositivos portátiles, bajo el producto BitLocker.

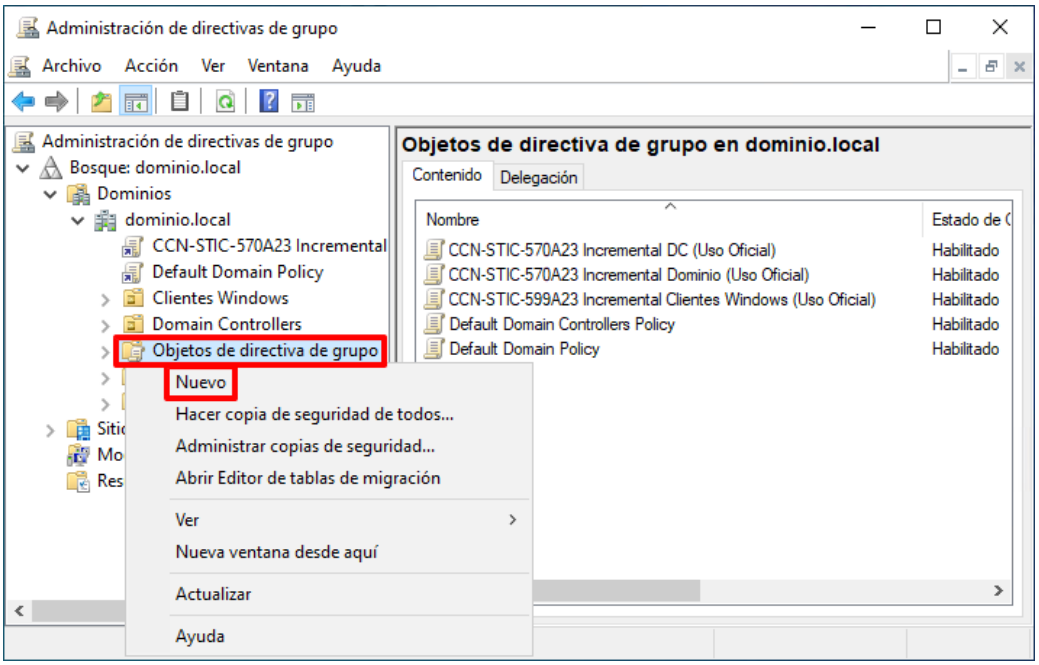
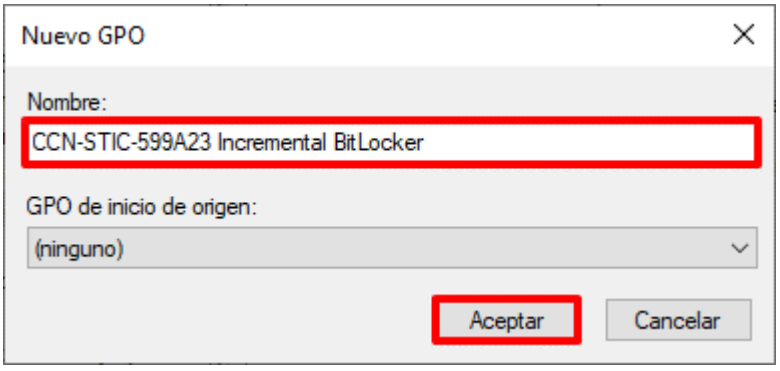
Nota: Si en su organización dispone de otro producto de cifrado, o bien su sistema operativo se encuentra implementado en un entorno protegido, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

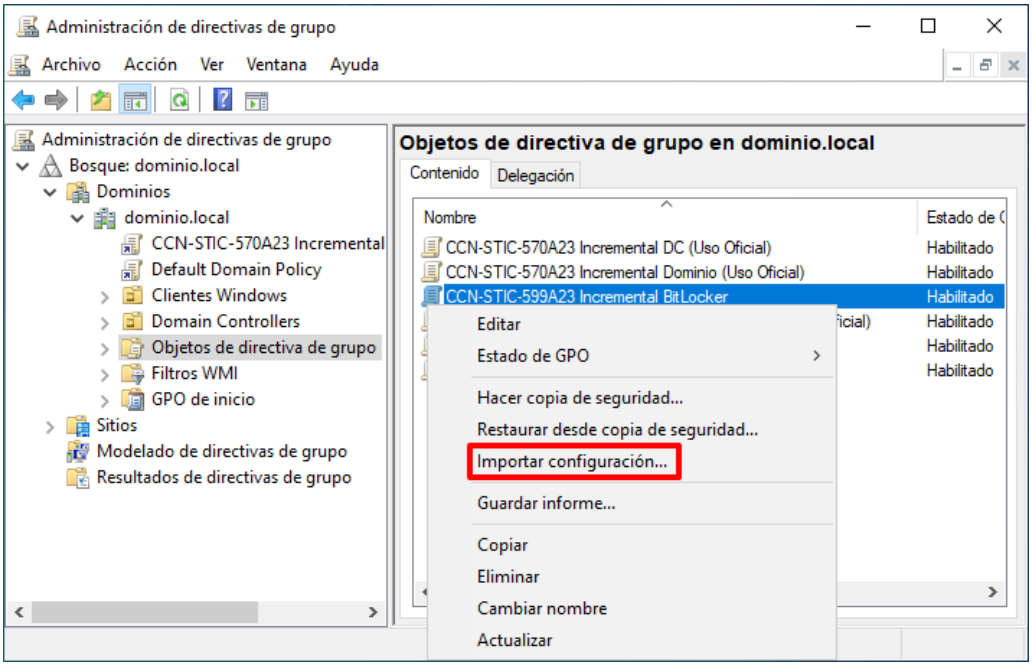
Se considera un entorno protegido, aquel entorno donde se disponga de un acceso controlado a salvo de hurtos y/o miradas indiscretas dentro de la organización.

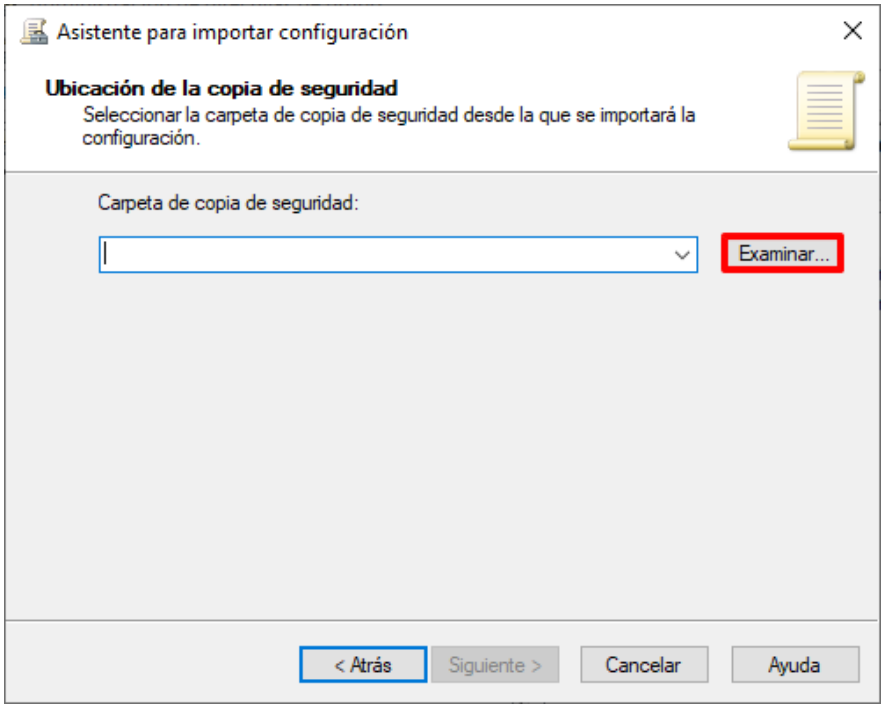
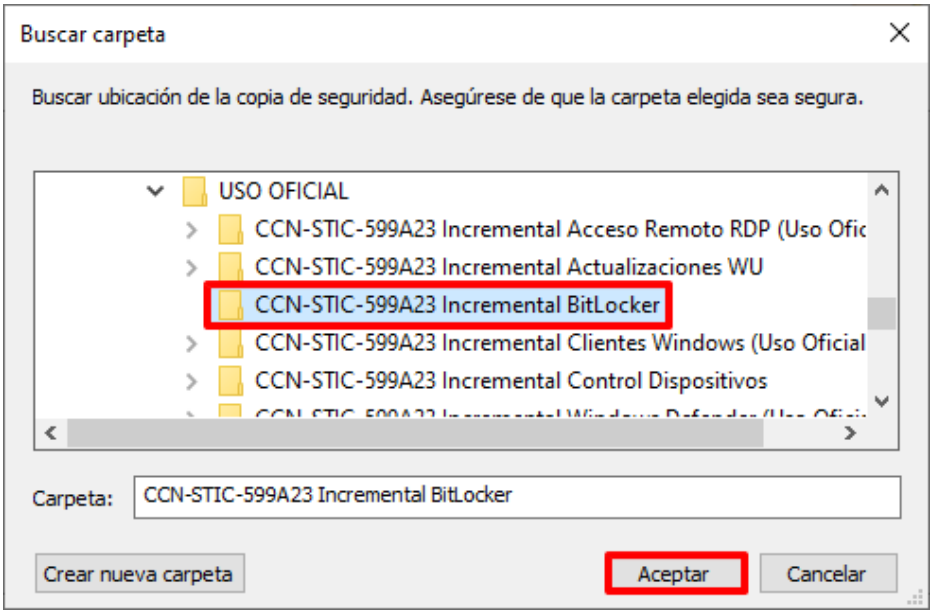
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Uso Oficial**. En el momento de **selección de las configuraciones** de seguridad deberá seleccionar aquella **acorde a su perfilado** (Uso Oficial o Materias Clasificadas).

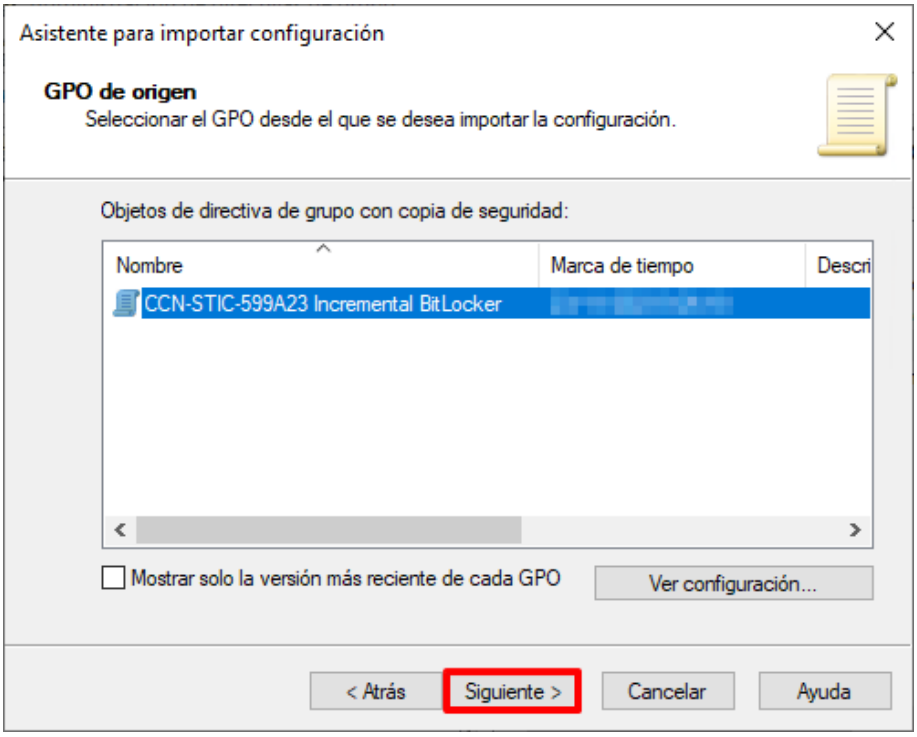
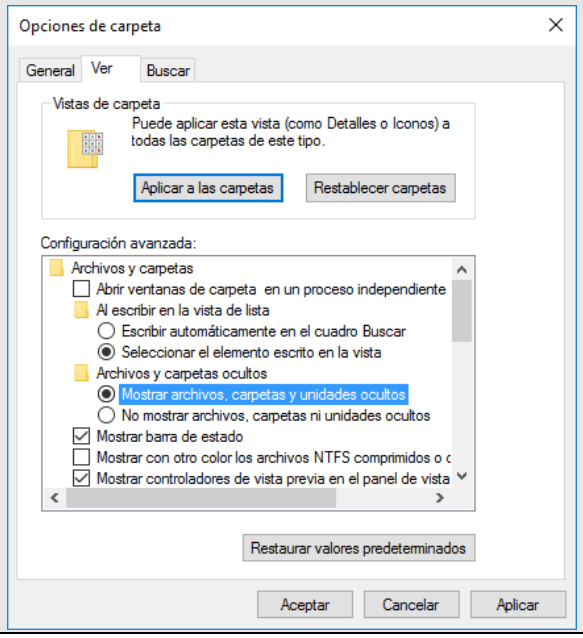
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **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". 

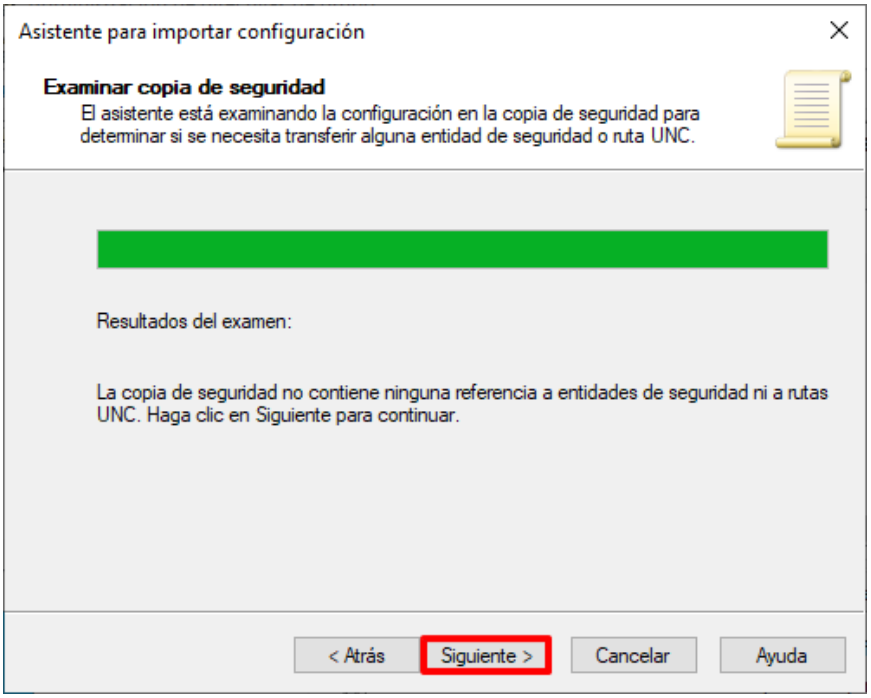
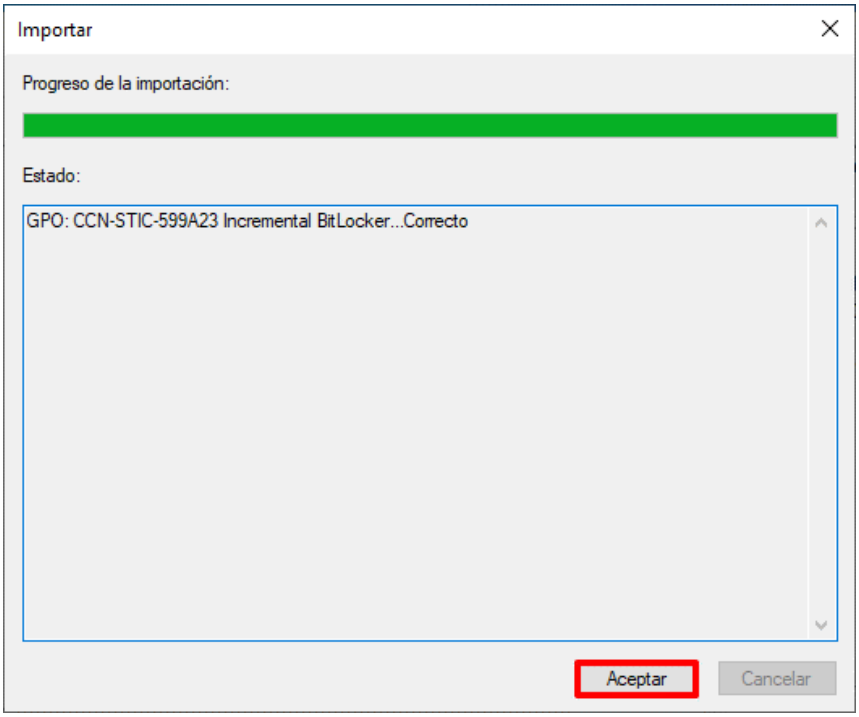
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

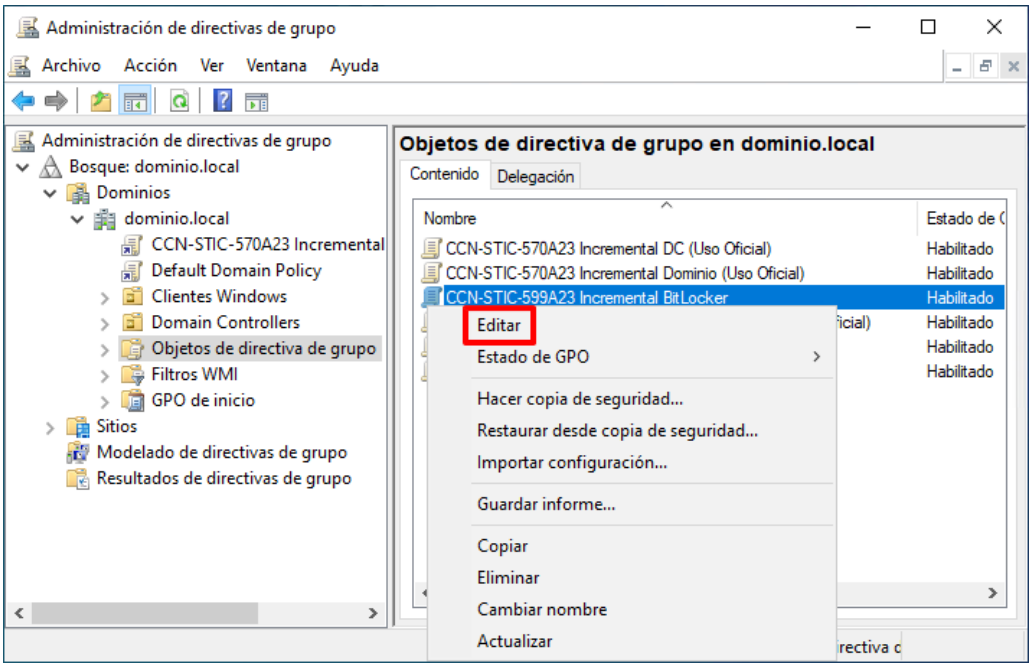
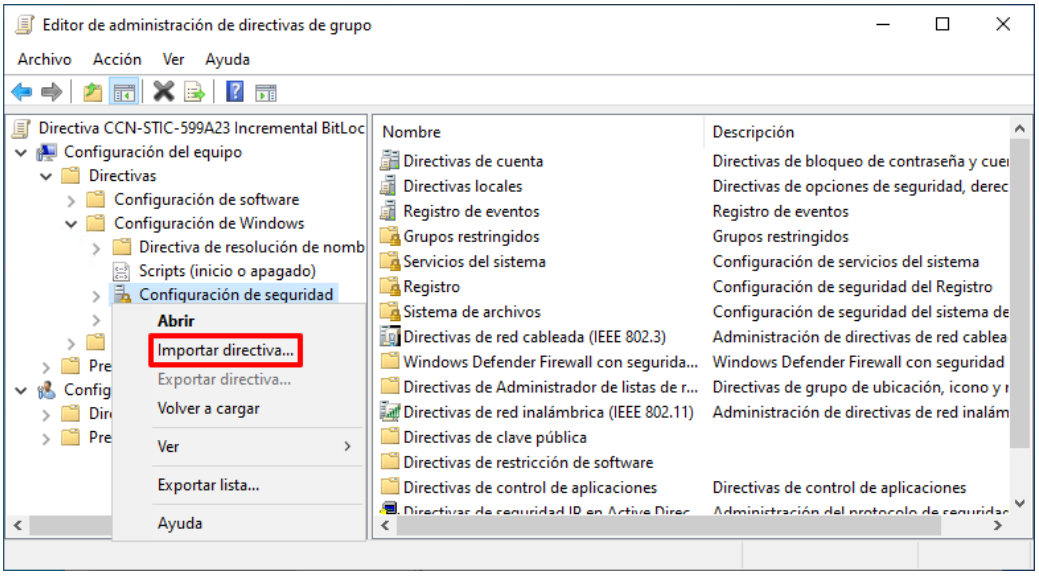
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental BitLocker**" y pulse el botón "Aceptar". 

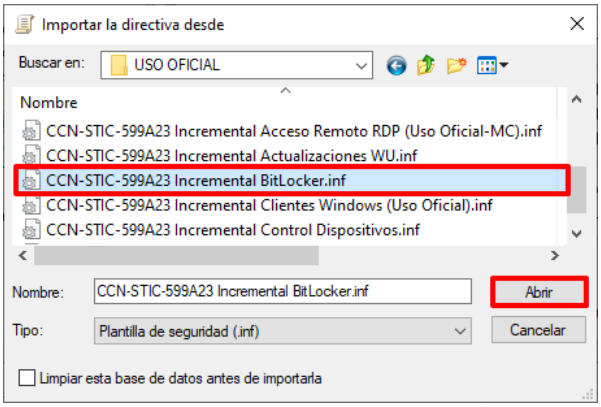
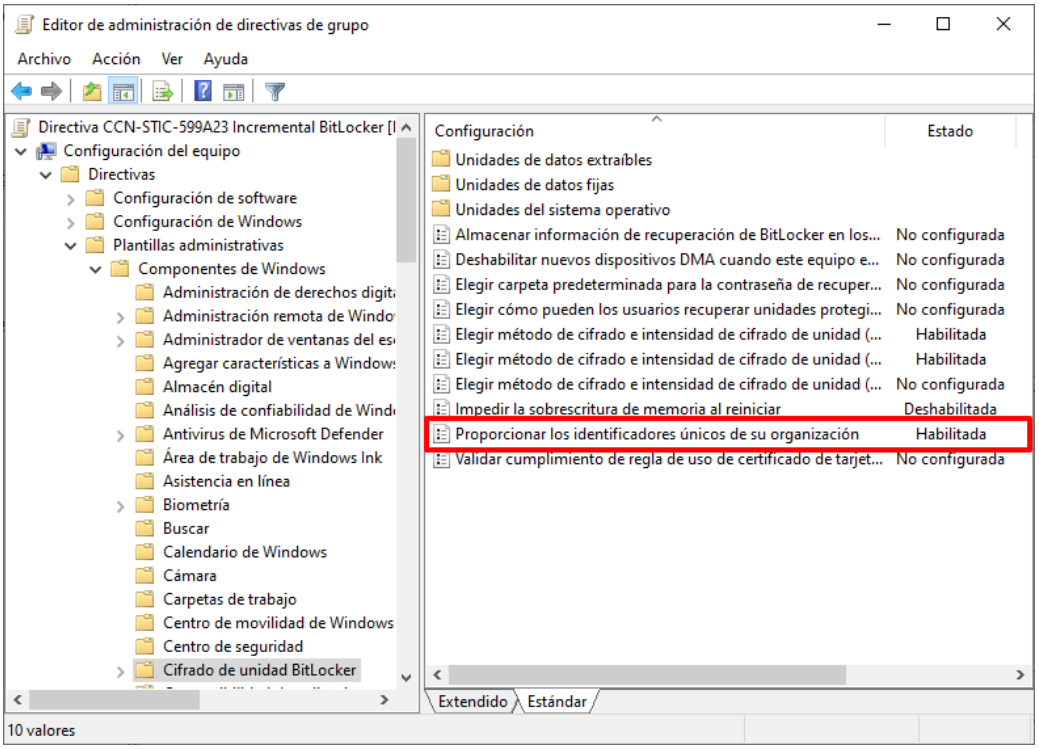
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

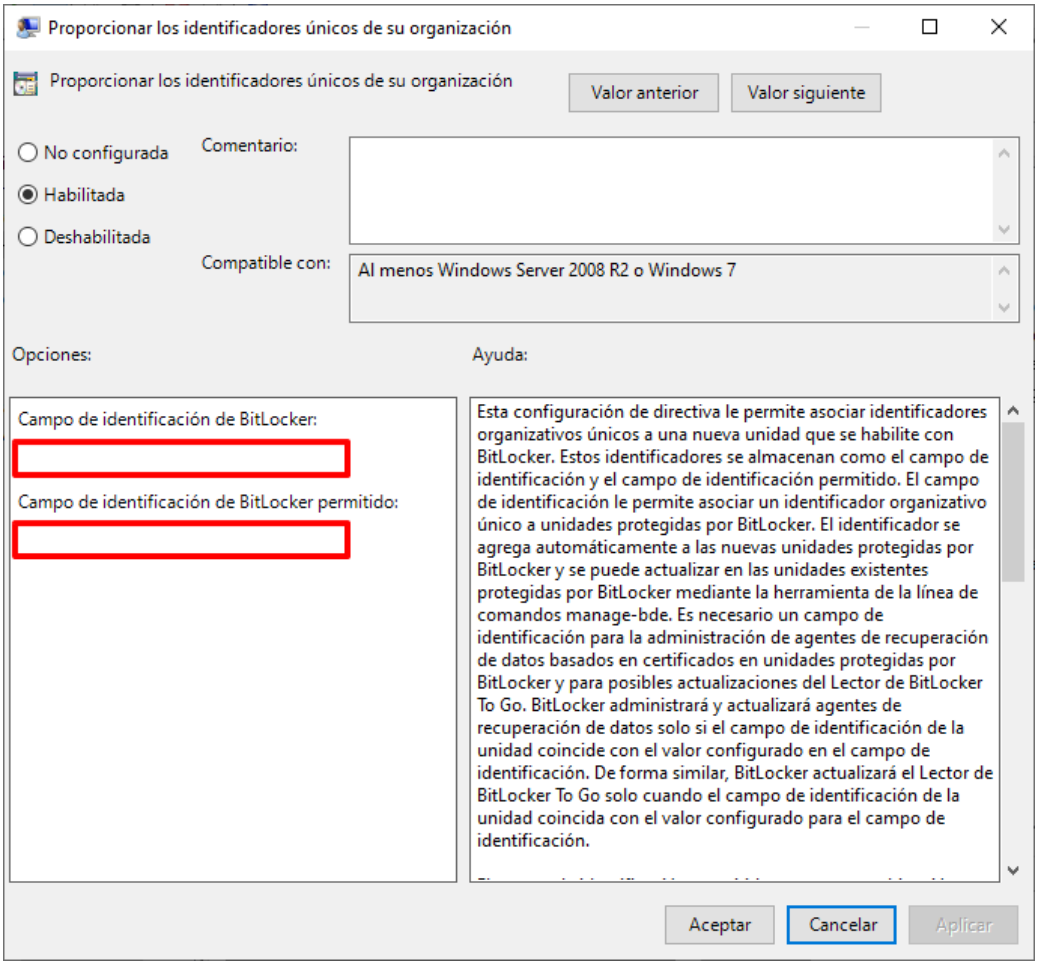
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-599A23 Incremental BitLocker” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Defina el nombre del objeto GPO acorde 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”.

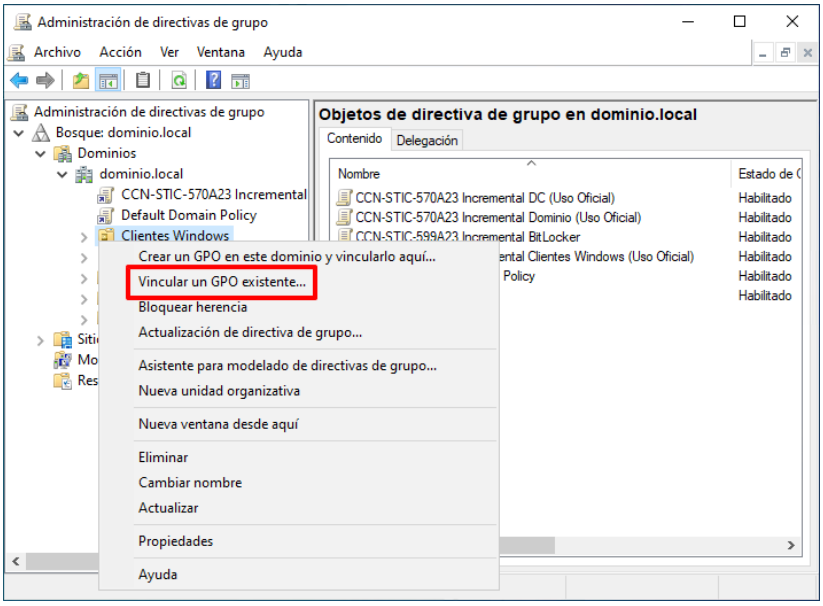
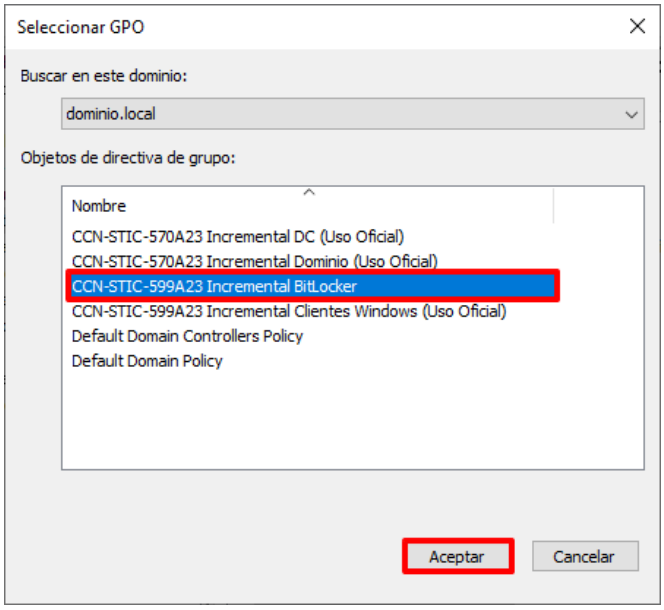
Paso	Descripción
13.	En la venta “GPO de origen” compruebe que aparece la política de seguridad “CCN-STIC-599A23 Incremental BitLocker” y pulse “Siguiente >”.  **Nota:** Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada 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. 

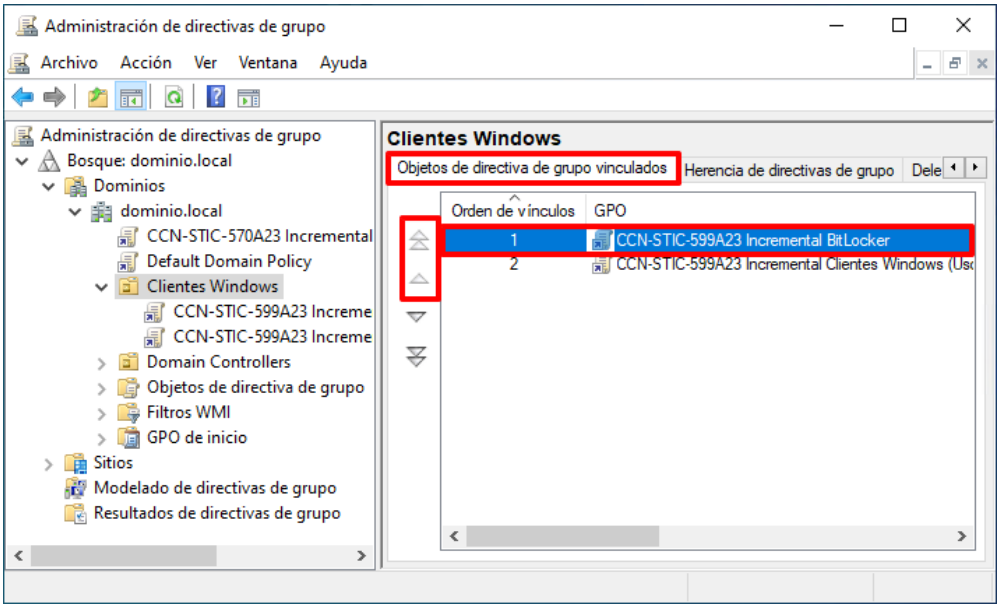
Paso	Descripción
17.	Seleccione de nuevo el objeto GPO “CCN-STIC-599A23 Incremental BitLocker” con el botón derecho y seleccione la opción “Editar” del menú contextual que aparecerá. 
18.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido del objeto GPO.
19.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“CCN-STIC-599A23 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-599A23 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.	De nuevo en la ventana del "Editor de administración de directivas de grupo", despliegue el nodo: "**CCN-STIC-599A23 Incremental BitLocker → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker**". Identifique en el panel derecho la directiva "**Proporcionar los identificadores únicos de su organización**" y haga doble clic sobre ella. 

Paso	Descripción
22.	En la nueva ventana emergente, establezca un identificador en el apartado "**Campo de identificación de BitLocker**" acorde a su organización. En el apartado contiguo "**Campo de identificación de BitLocker permitido**", deberá establecer el mismo identificador, pudiendo establecer identificadores adicionales separados por comas si así fuera necesario.  **Nota:** Cualquier dispositivo removible cifrado mediante BitLocker en los dispositivos con esta configuración aplicada tendrán establecido en el valor "Campo de identificación" el identificador configurado en la directiva. Cualquier dispositivo removible que dicho valor no lo tenga configurado, o su identificador no se encuentre establecido en el apartado "**Campo de identificación de BitLocker permitido**", solo podrá ser usado en **modo lectura**. Si un dispositivo removible ha sido cifrado en el equipo previamente a la aplicación de las directivas de seguridad tratadas en este punto, solo podrá ser utilizado en modo lectura tras la aplicación, pudiendo posteriormente **mediante línea de comandos** que el dispositivo tome el valor del campo de identificación y pueda ser **usado con normalidad**. En caso de que requiera deshabilitar la directiva "**Proporcionar los identificadores únicos de su organización**", o quiera información de cómo utilizar dispositivos removibles en modo escritura previamente cifrados a la aplicación de las directivas, consulte el apartado "**ANEXO A.4.7. CIFRADO DE UNIDAD DE BITLOCKER**".

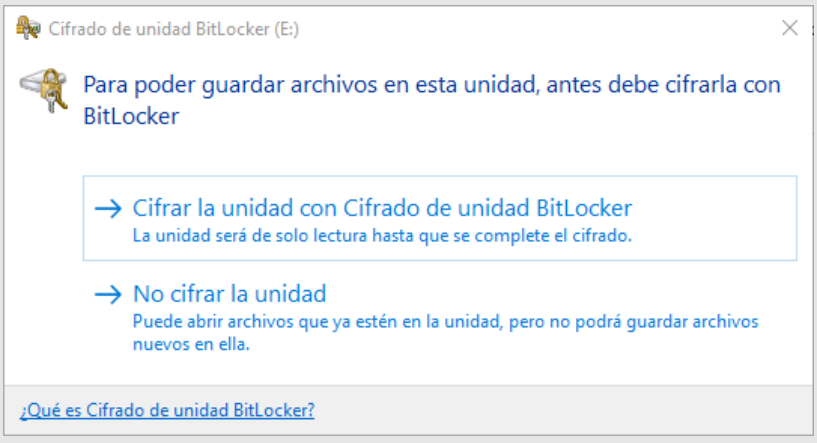
Paso	Descripción
23.	Cierre la ventana “Editor de administración de directivas de grupo”.
24.	Por último, identifique las unidades organizativas y objetos que requieran la configuración del servicio de actualizaciones y vincule el objeto GPO generado en apartados anteriores. Para ello, haga clic derecho 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 “Clientes Windows”, creada para tal fin.
25.	A continuación, seleccione el objeto GPO “CCN-STIC-599A23 Incremental BitLocker” y pulse “Aceptar”. 

Paso	Descripción
26.	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.



Nota: Si habilita esta configuración, todas las unidades de datos extraíbles que no estén protegidas con BitLocker **se montarán en modalidad solo lectura**. Si la unidad está protegida con BitLocker, con un identificador válido establecido, se montará con acceso de lectura y escritura.

Si hace uso de una unidad no protegida, podrá conectarla y cifrarla para permitir su uso en modo lectura y escritura. Al conectar el dispositivo removible por primera vez tras la aplicación de la citada configuración, **el módulo de BitLocker de Windows avisará de la necesidad de cifrado para permitir guardar ficheros**.



Si se requiere aplicar la configuración, pero evitar el funcionamiento indicado, consulte el apartado "**ANEXO A.4.7. CIFRADO DE UNIDAD DE BITLOCKER**".

Paso	Descripción
27.	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.1.2.2 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 A.2.7. 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 cliente miembro, independientemente de su función, 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).

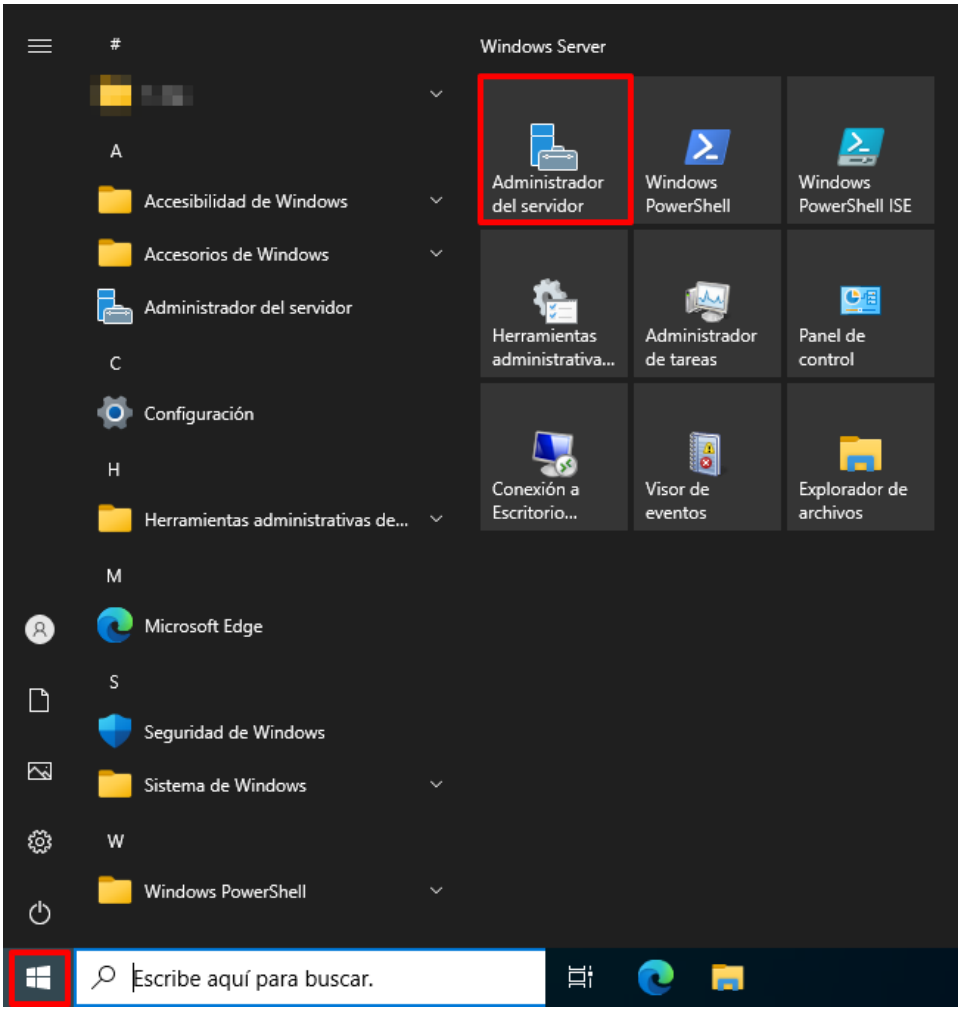
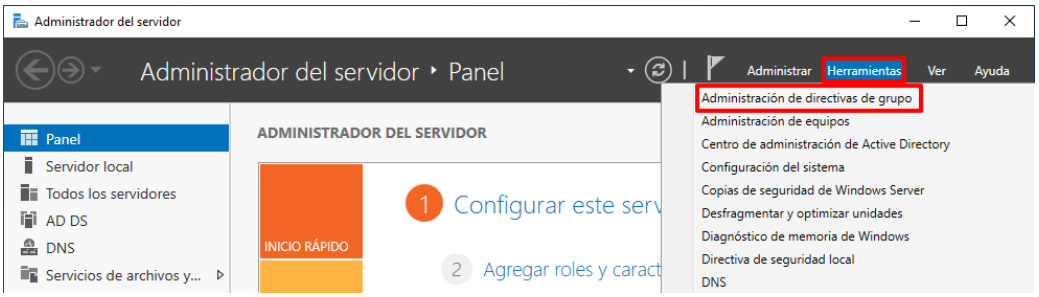
Realizadas las acciones descritas en el presente punto se presentarán dos formas de instalar controladores para el uso de dispositivos.

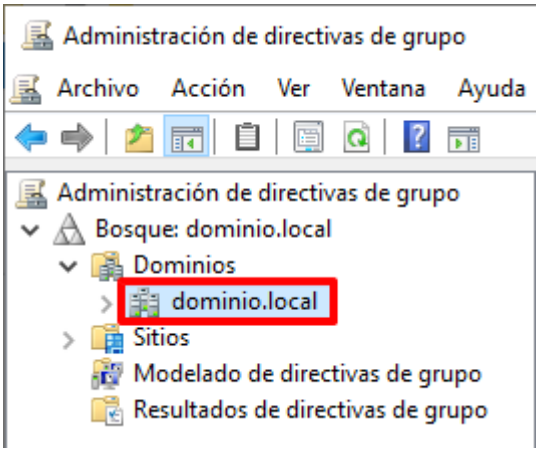
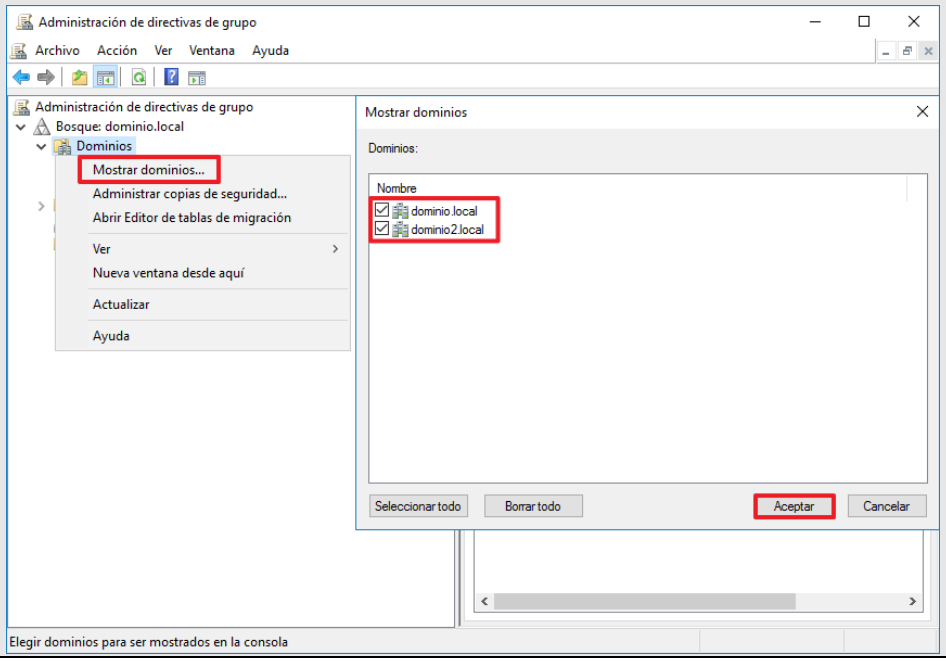
a) Actualización automática de controladores por parte de usuario con privilegios de administrador.

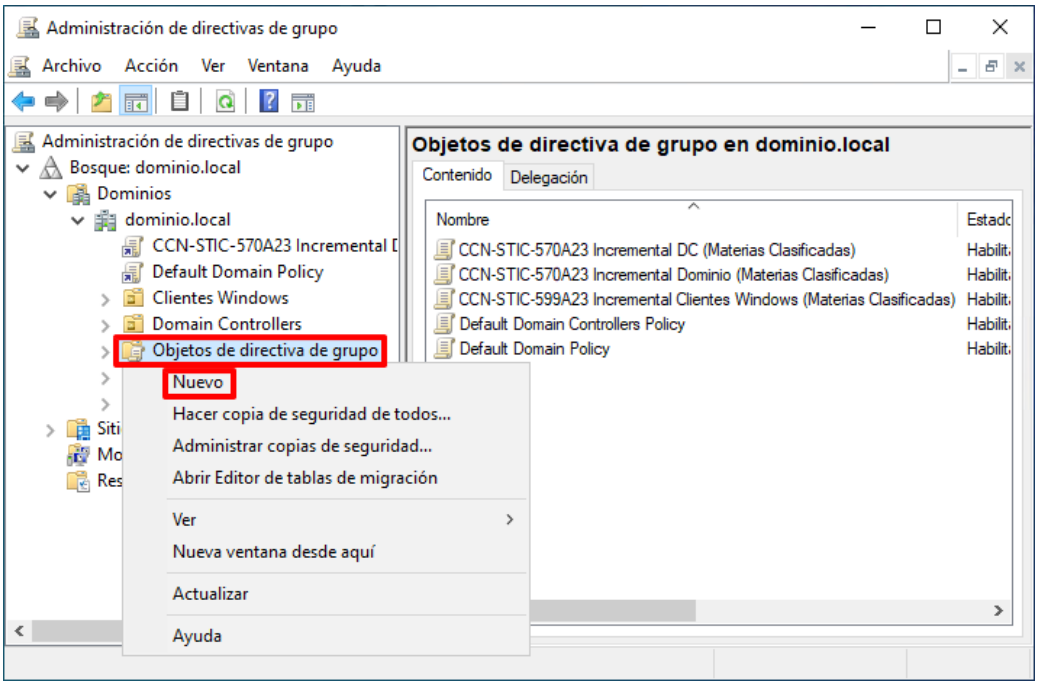
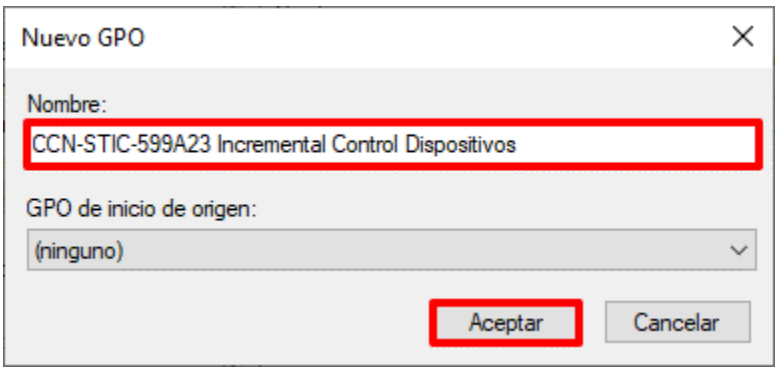
b) Alta de dispositivos por medio de identificadores únicos de los dispositivos.

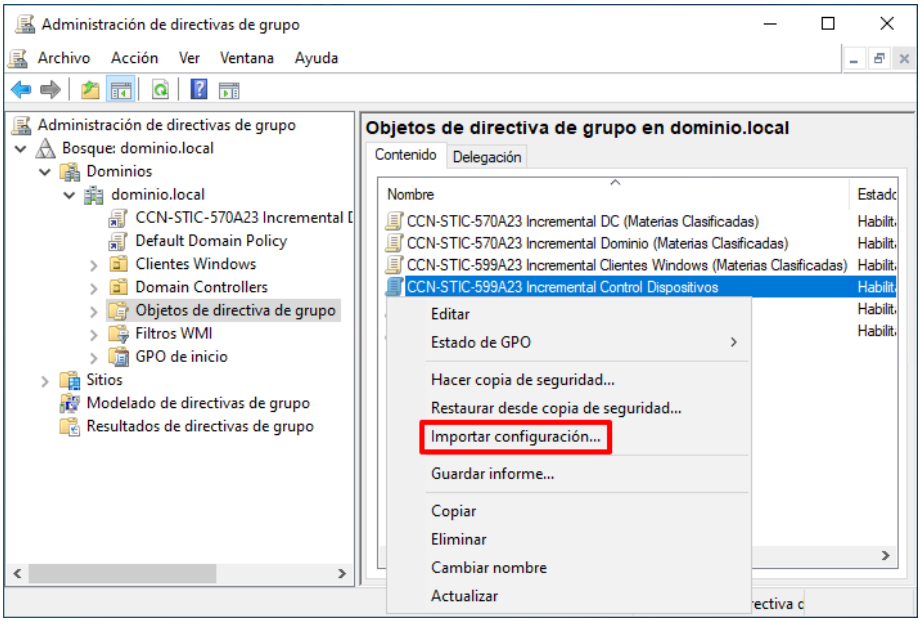
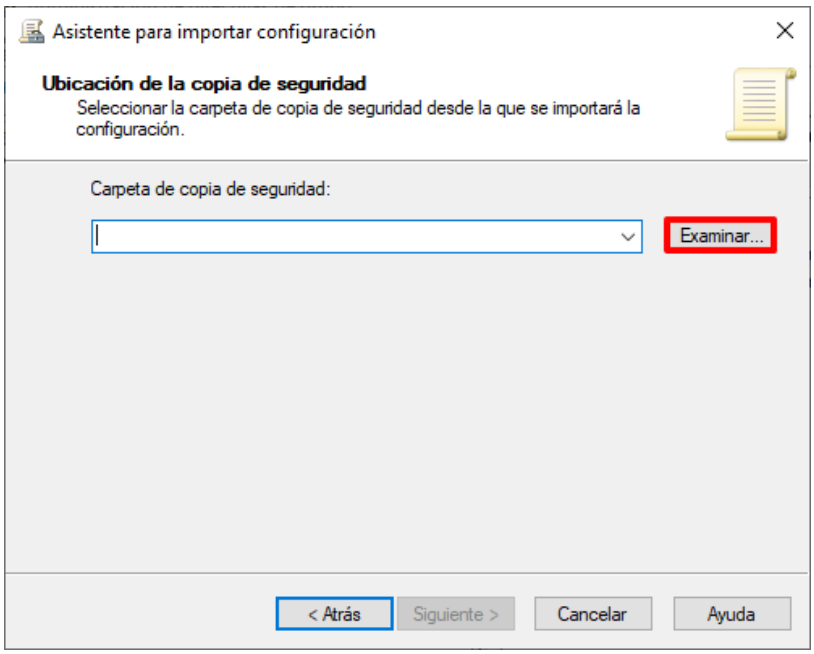
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Materias Clasificadas**, no siendo obligatorio en ningún otro perfilado.

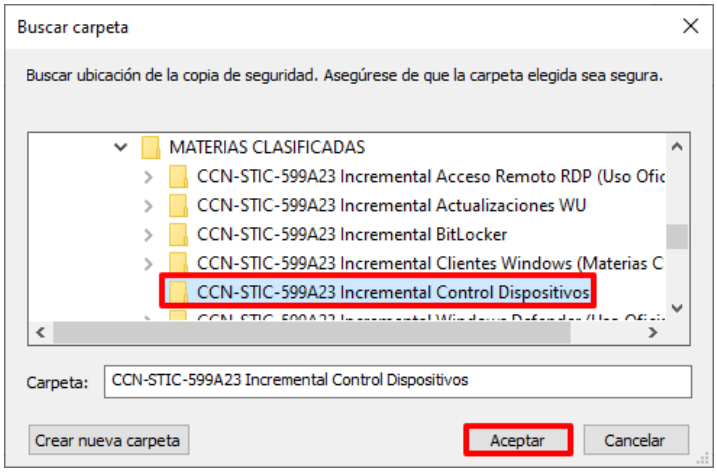
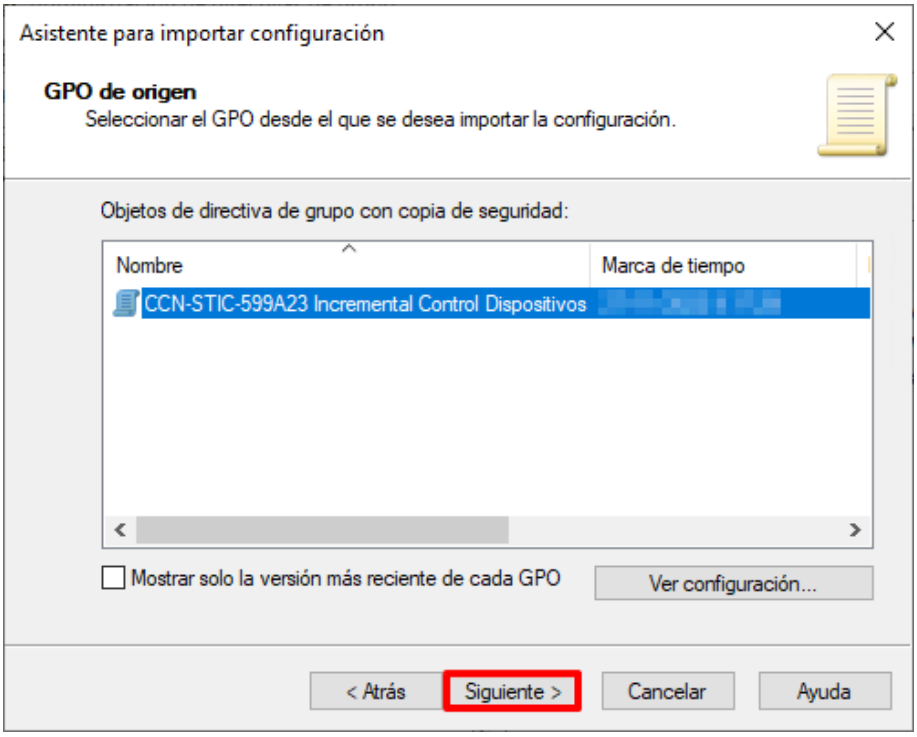
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

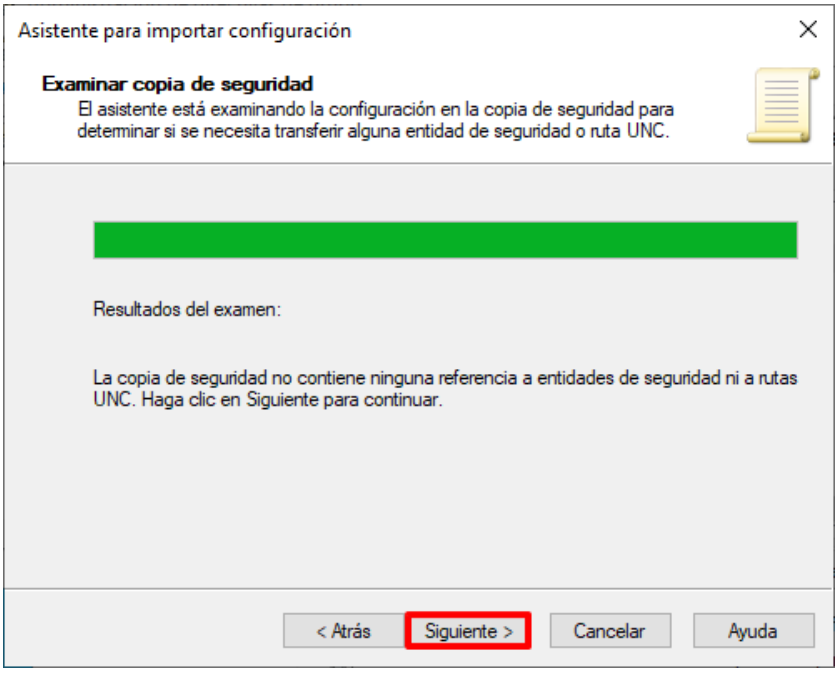
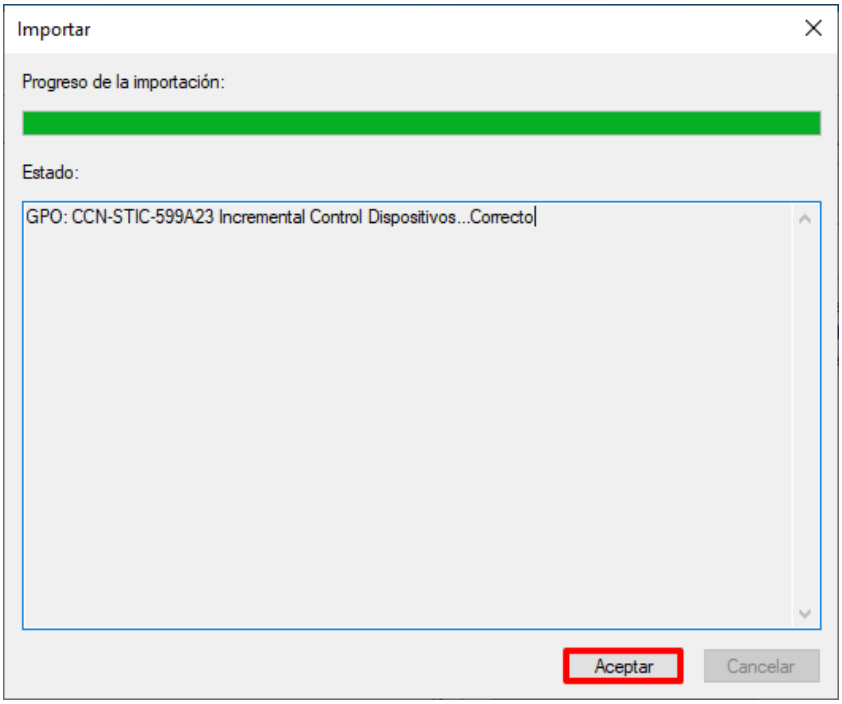
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

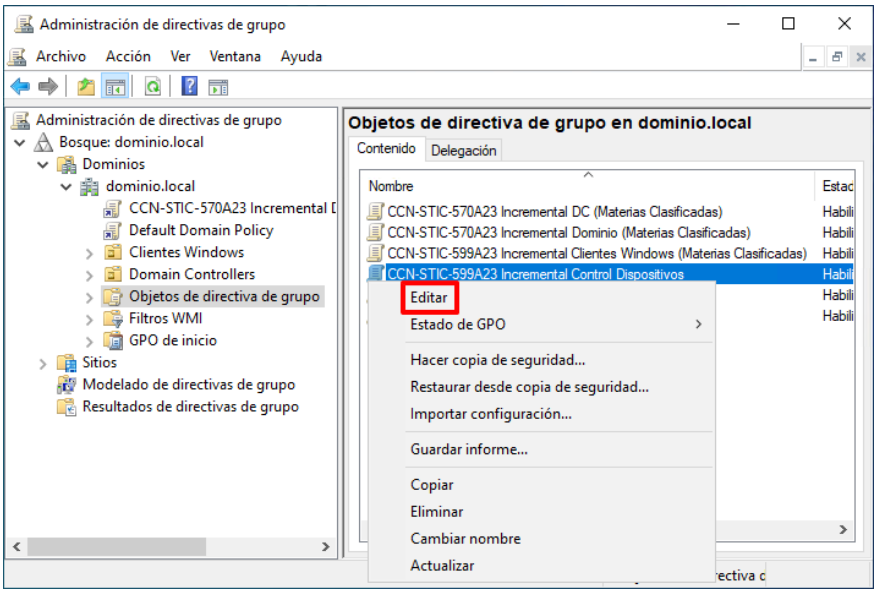
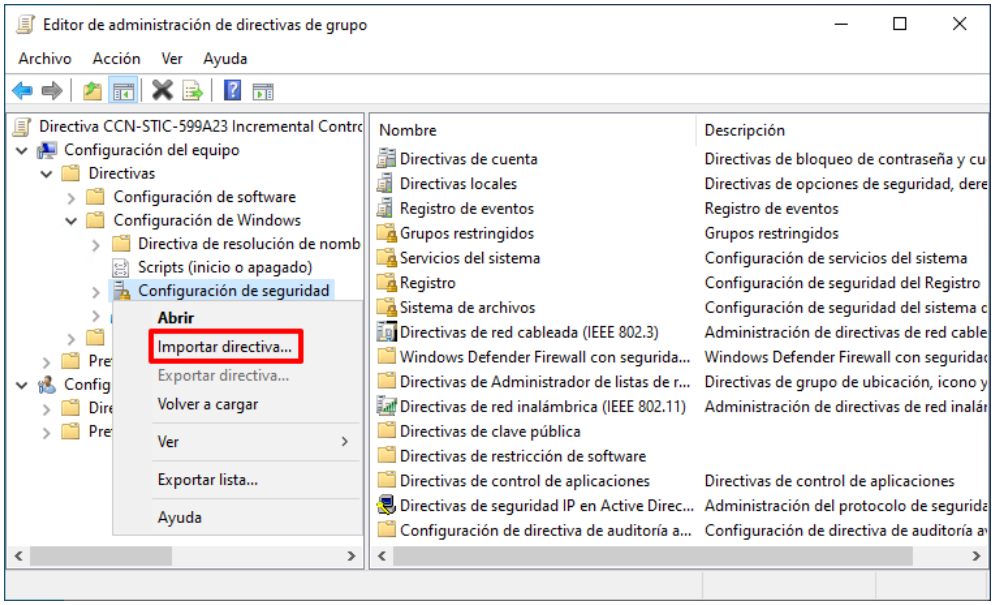
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

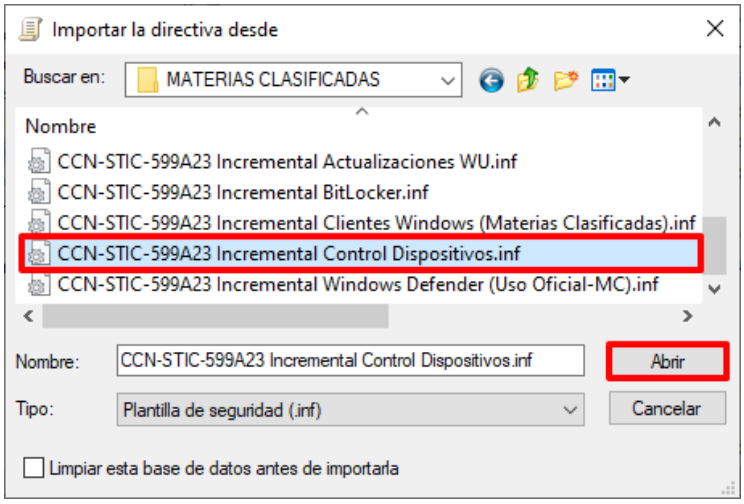
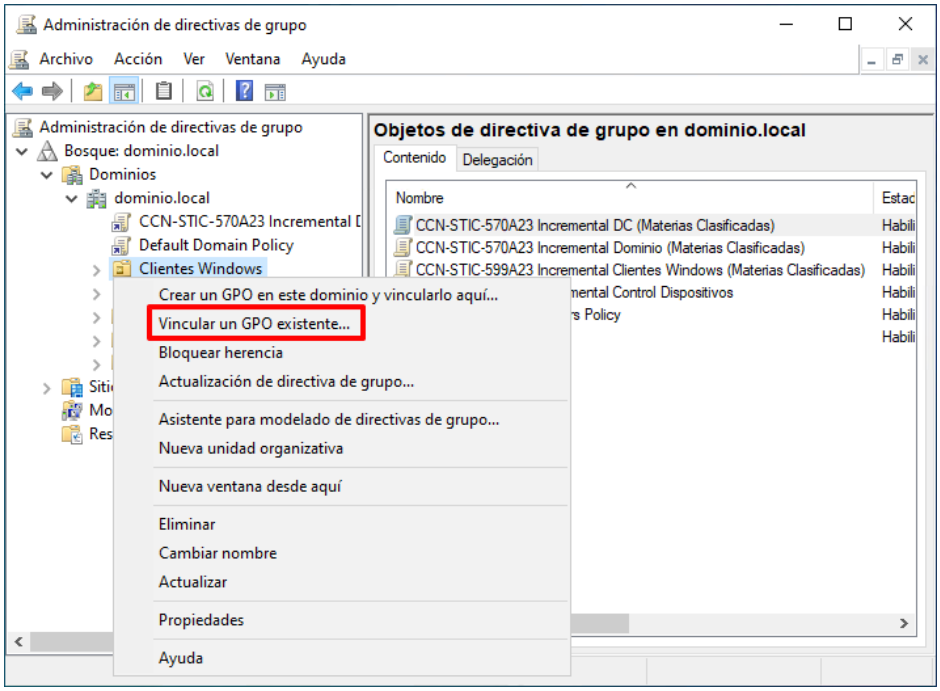
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental Control Dispositivos**" y pulse el botón "Aceptar". 

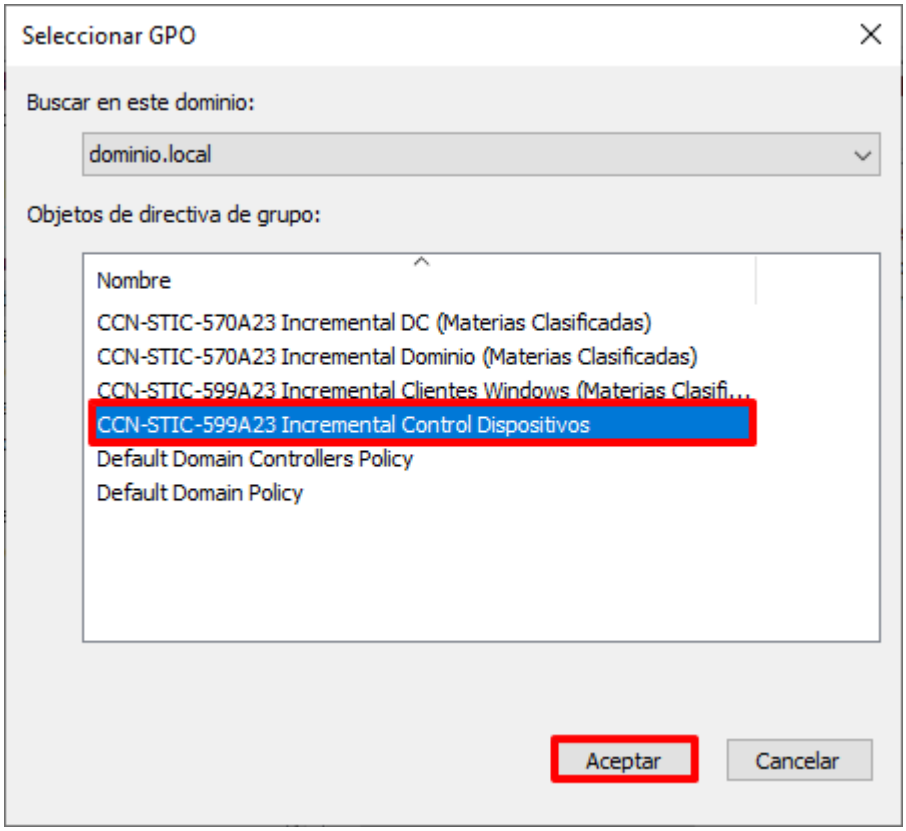
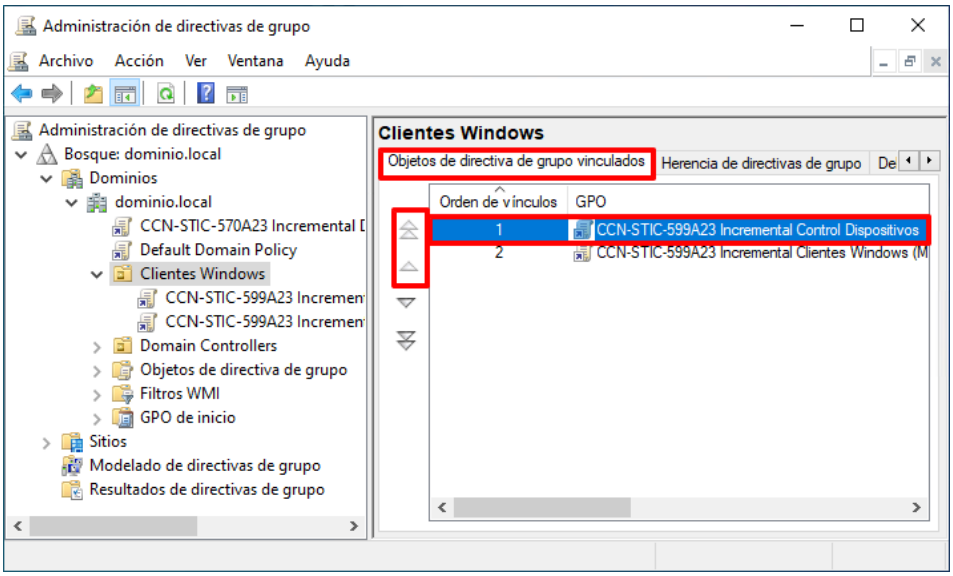
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

Paso	Descripción
11.	Seleccione la carpeta "CCN-STIC-599A23 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".
13.	En la venta "GPO de origen" compruebe que aparece la política de seguridad "CCN-STIC-599A23 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-599A23 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-599A23 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. 

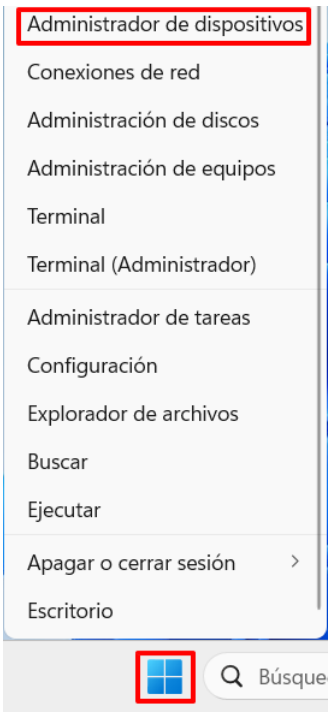
Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en “C:\Scripts\MATERIAS CLASIFICADAS” denominada “CCN-STIC-599A23 Incremental Control Dispositivos.inf”. A continuación, pulse sobre el botón “Abrir”. 
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 “Clientes Windows”, creada para tal fin.

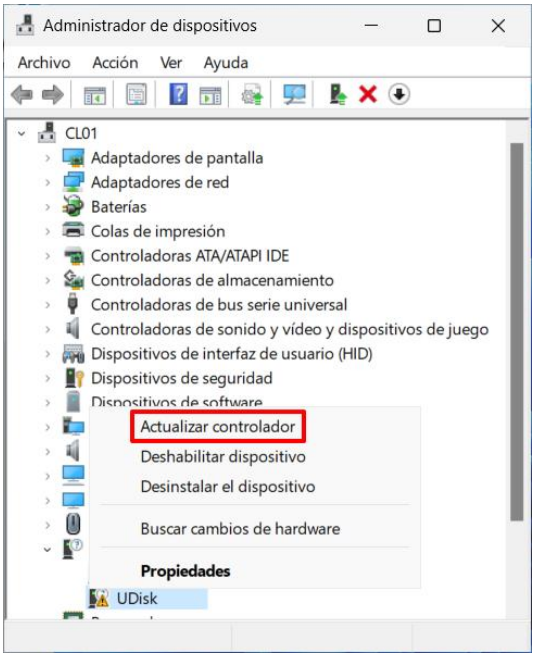
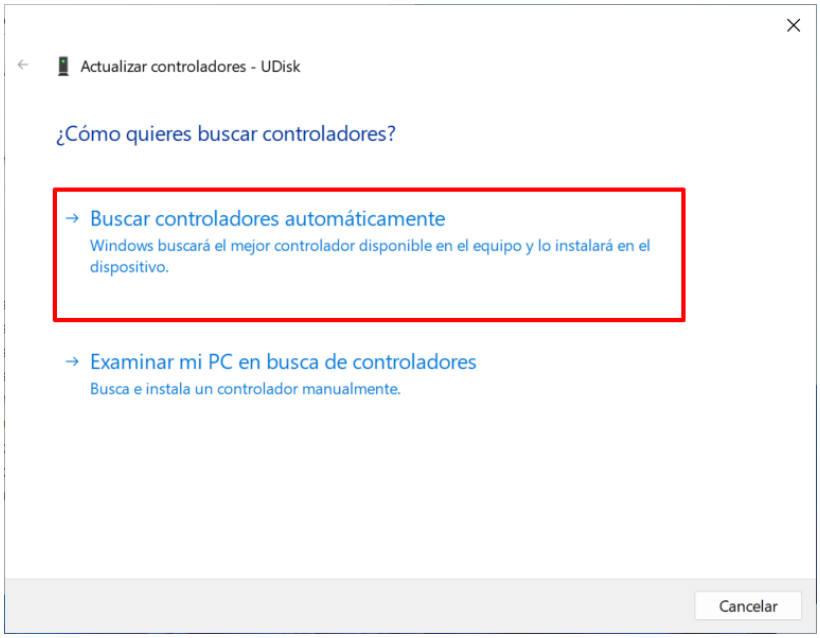
Paso	Descripción
22.	A continuación, seleccione el objeto GPO "CCN-STIC-599A23 Incremental Control Dispositivos" y pulse "Aceptar". 
23.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

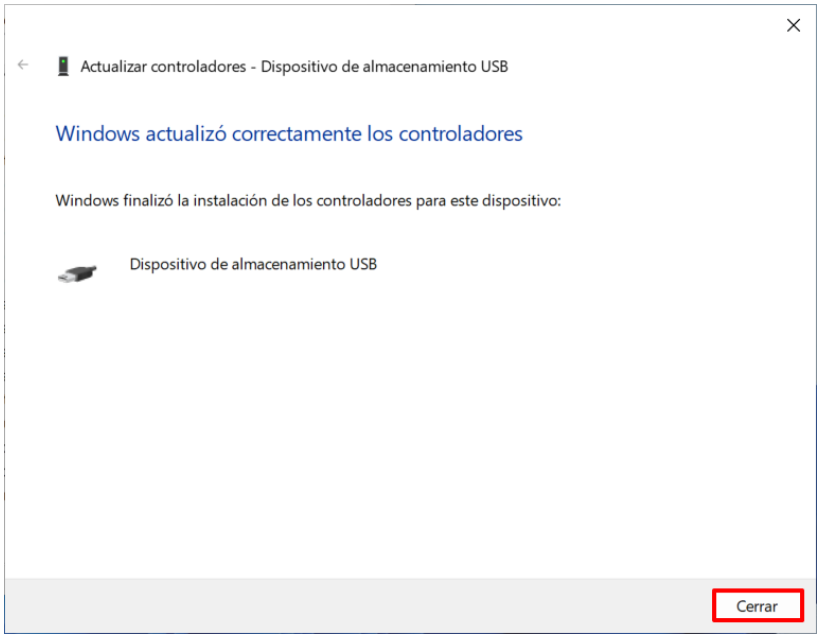
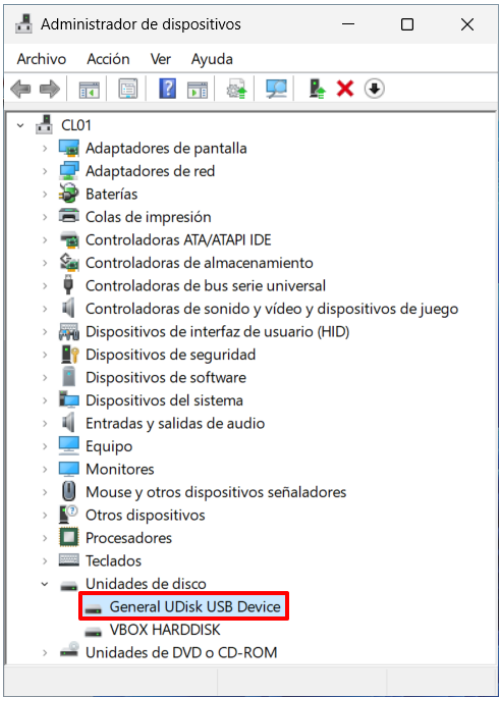
Paso	Descripción
24.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación 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.1.2.2 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 A.2.7.1. 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.

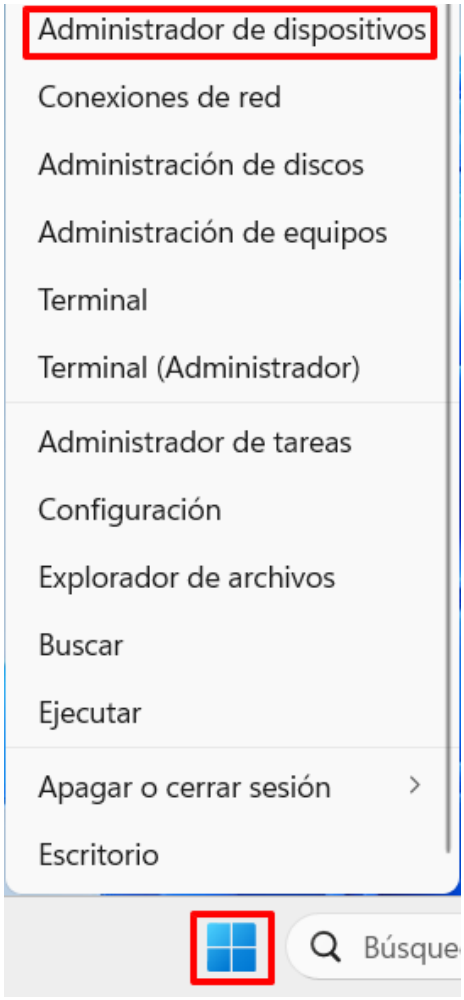
Paso	Descripción
25.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
26.	Haga clic derecho sobre el botón de "Inicio" y seleccione "Administrador de dispositivos". 

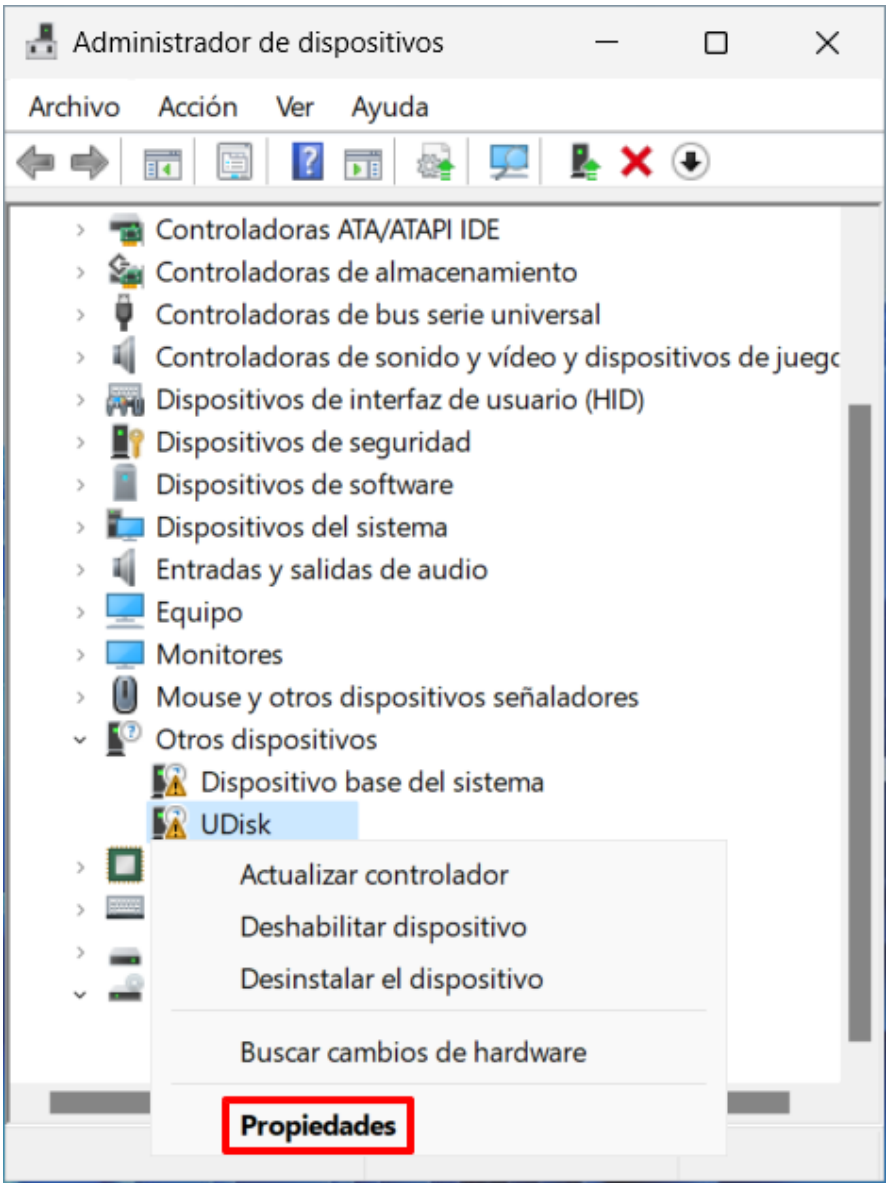
Paso	Descripción
27.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”.  **Nota:** Debido a la inexistencia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

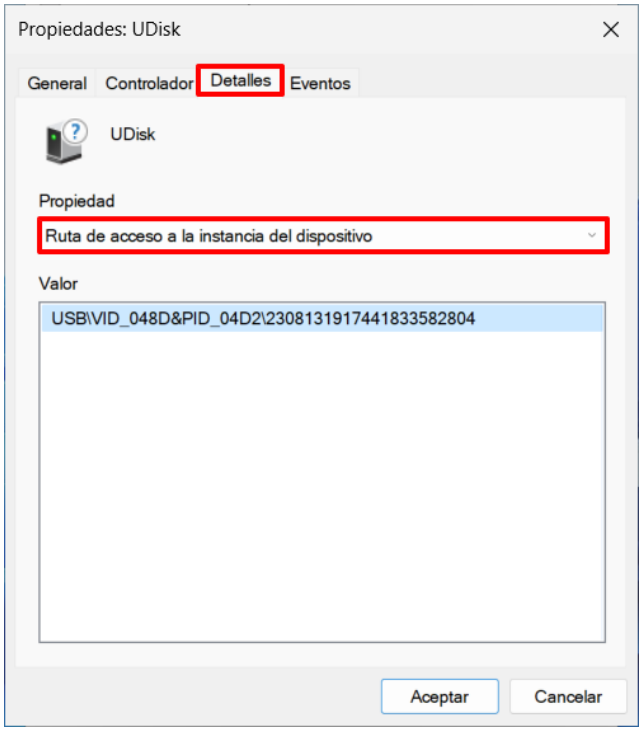
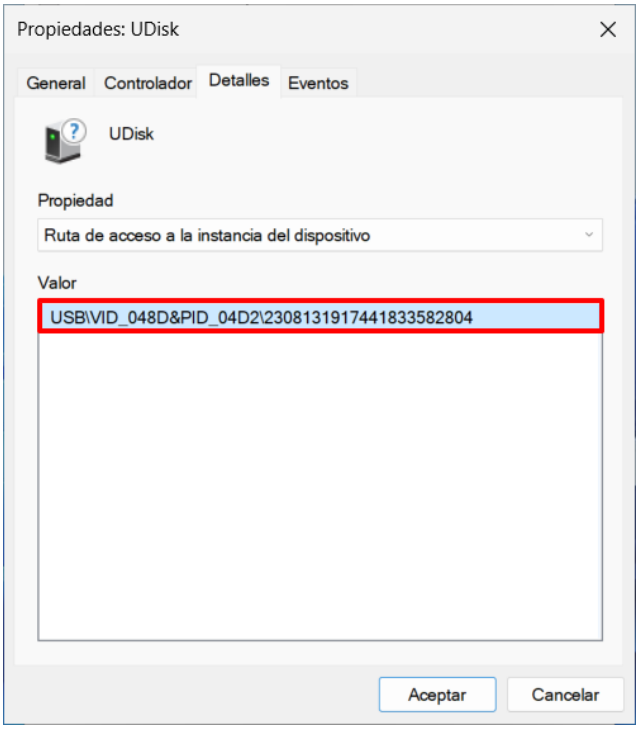
Paso	Descripción
29.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  **Nota:** No cierre el “Administrador de dispositivos” todavía.
30.	Ejecute los mismos pasos anteriores (pasos 27 a 29) hasta que el dispositivo aparezca 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. 

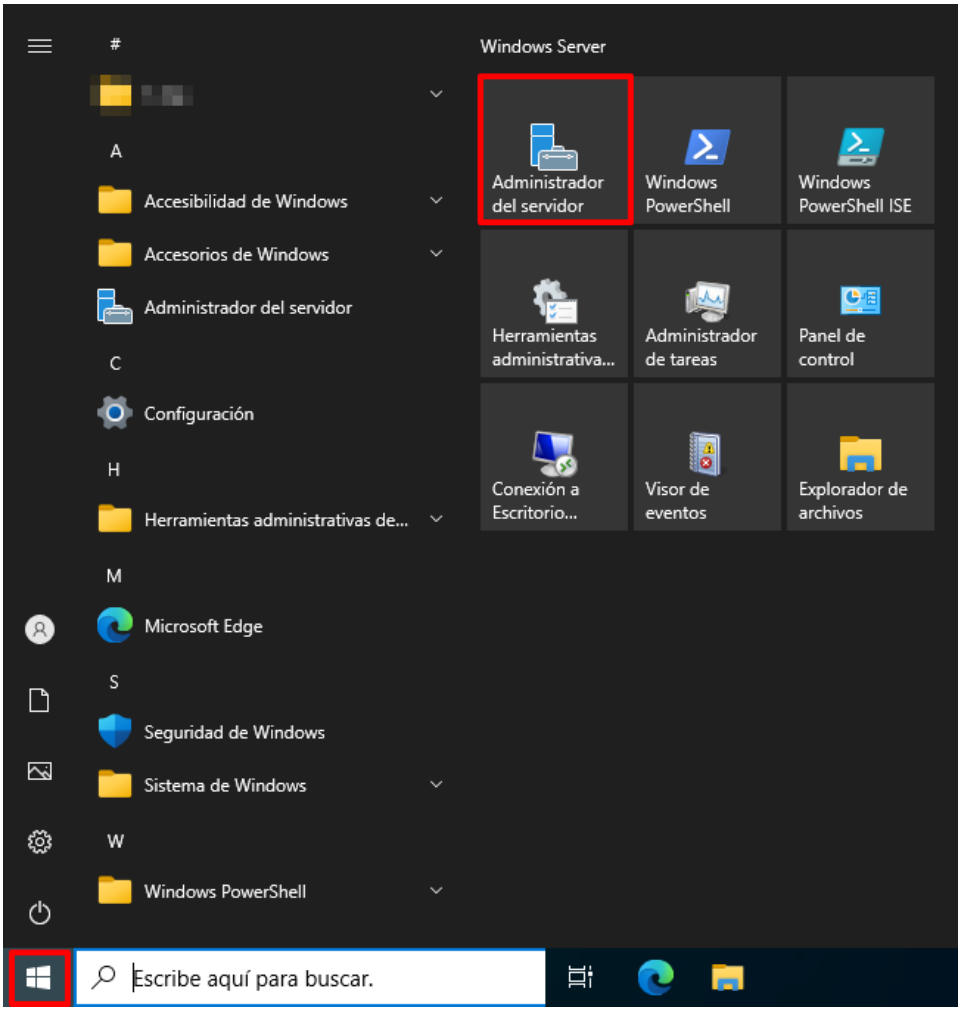
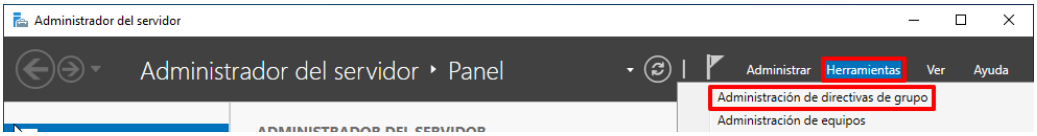
ANEXO A.2.7.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

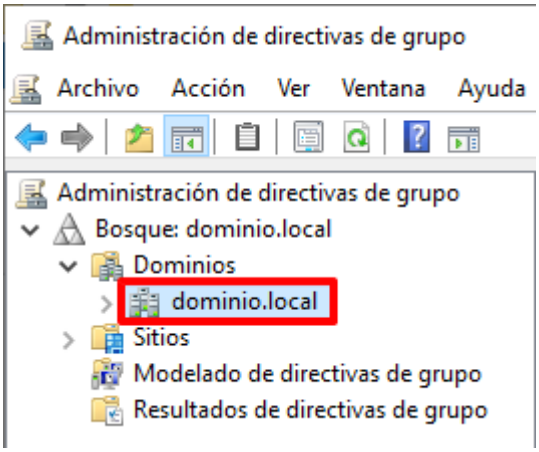
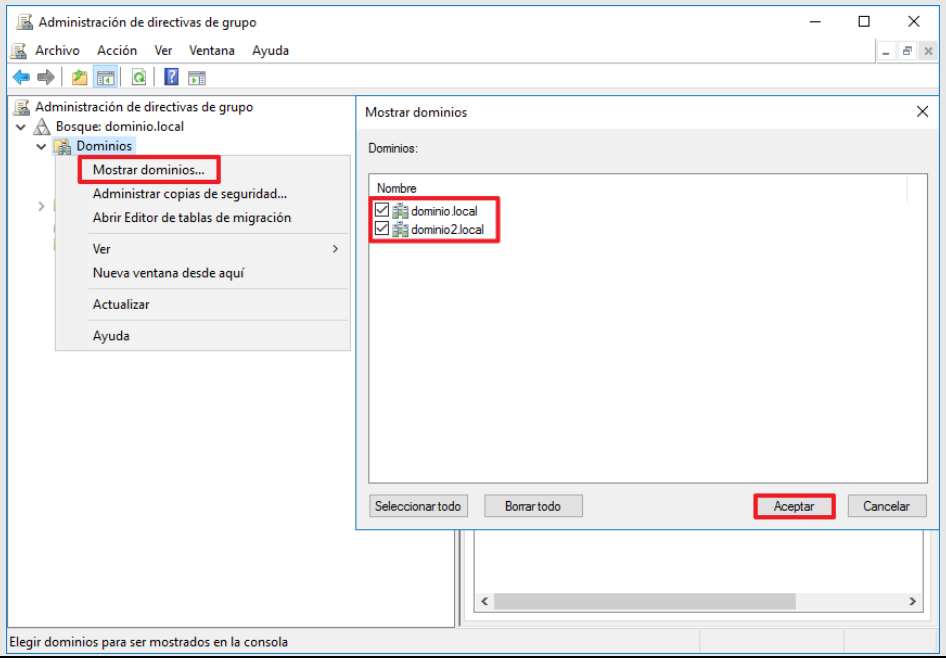
Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del dominio en el cual se está habilitando el uso de dispositivos USB y sobre un Controlador de Dominio perteneciente al dominio.

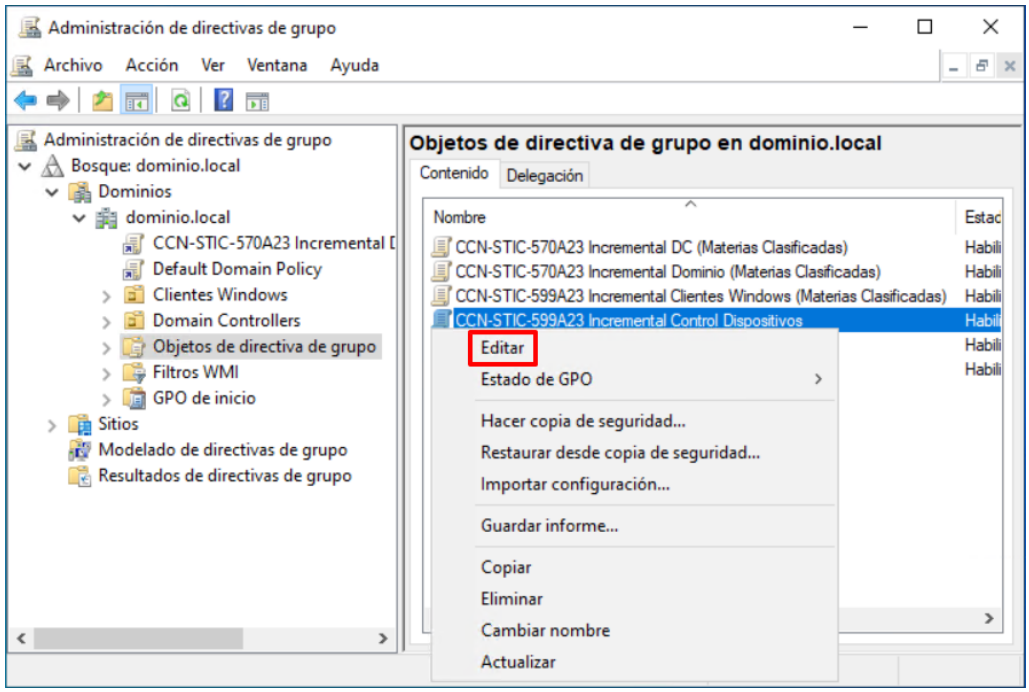
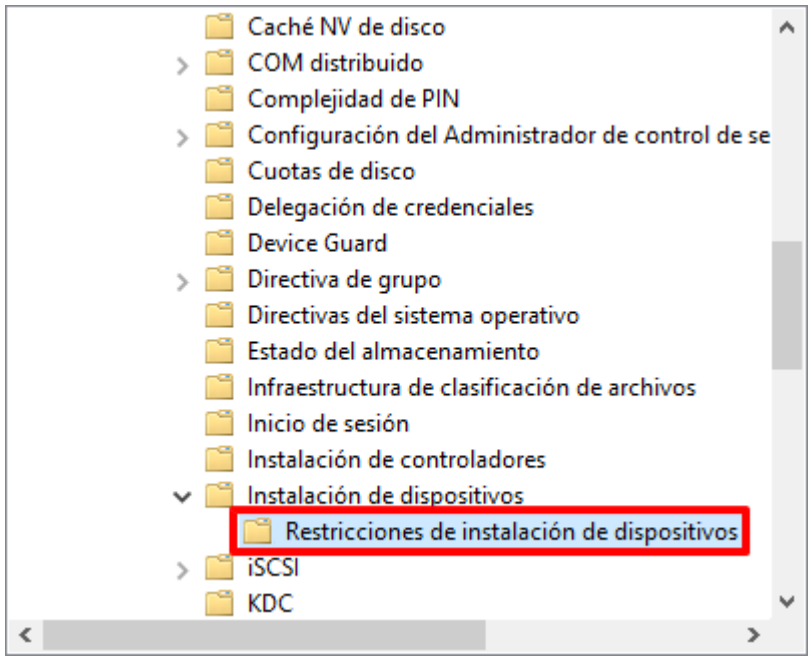
Paso	Descripción
31.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
32.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

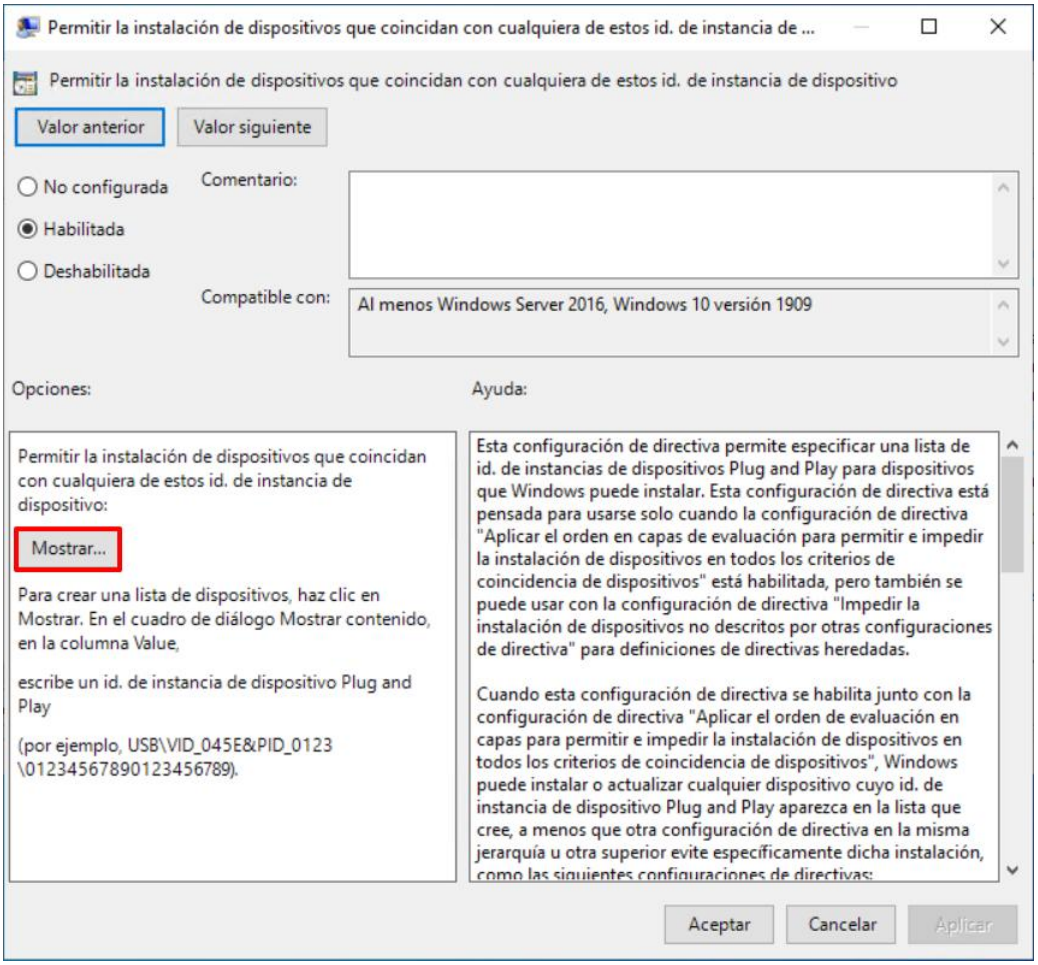
Paso	Descripción
33.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Propiedades”.  **Nota:** Debido a la inexistencia de controlador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

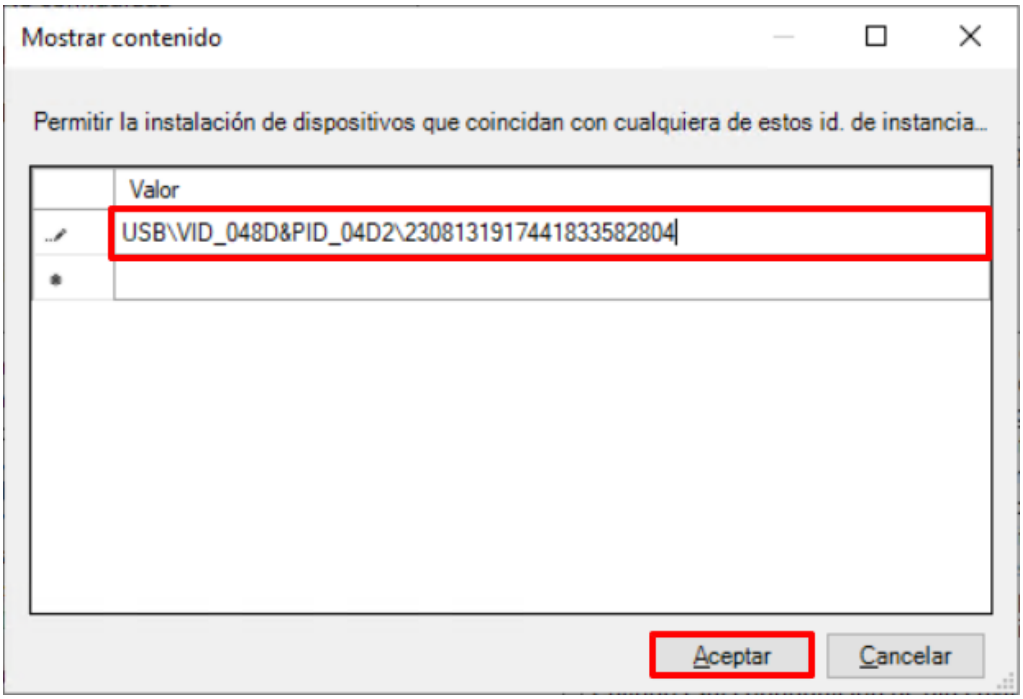
Paso	Descripción
34.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Ruta de acceso a la instancia del dispositivo”. 
35.	Seleccione el identificador y anótelo para poder introducirlo más adelante.  **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

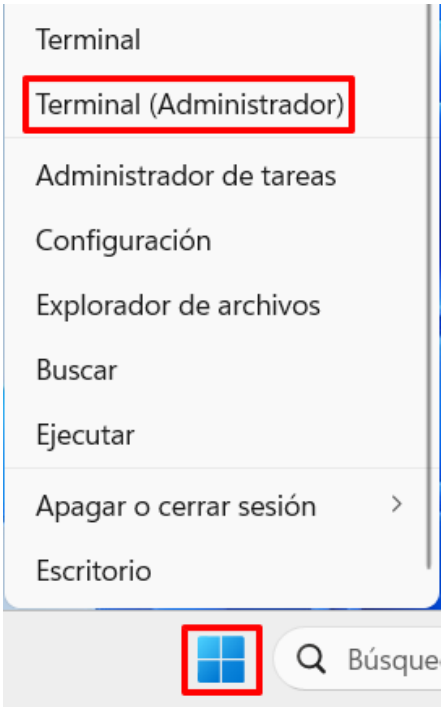
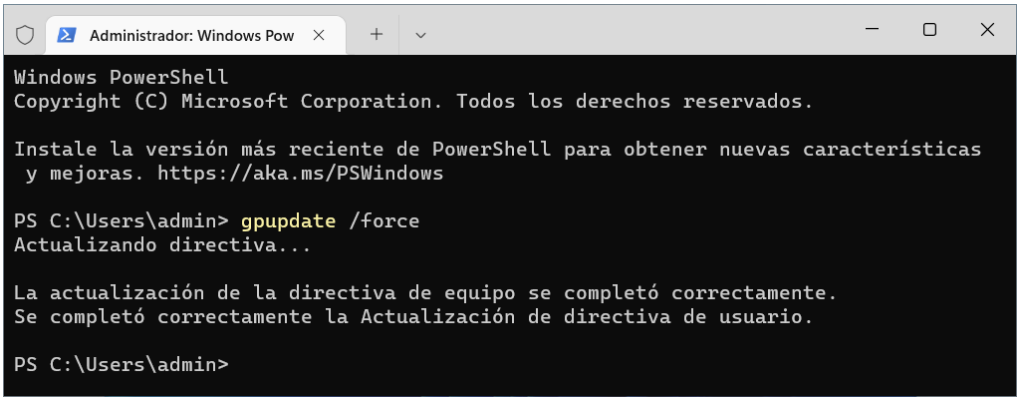
Paso	Descripción
36.	Inicie sesión en un servidor Controlado de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
37.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **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".
38.	En la parte superior derecha pulse sobre el botón "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

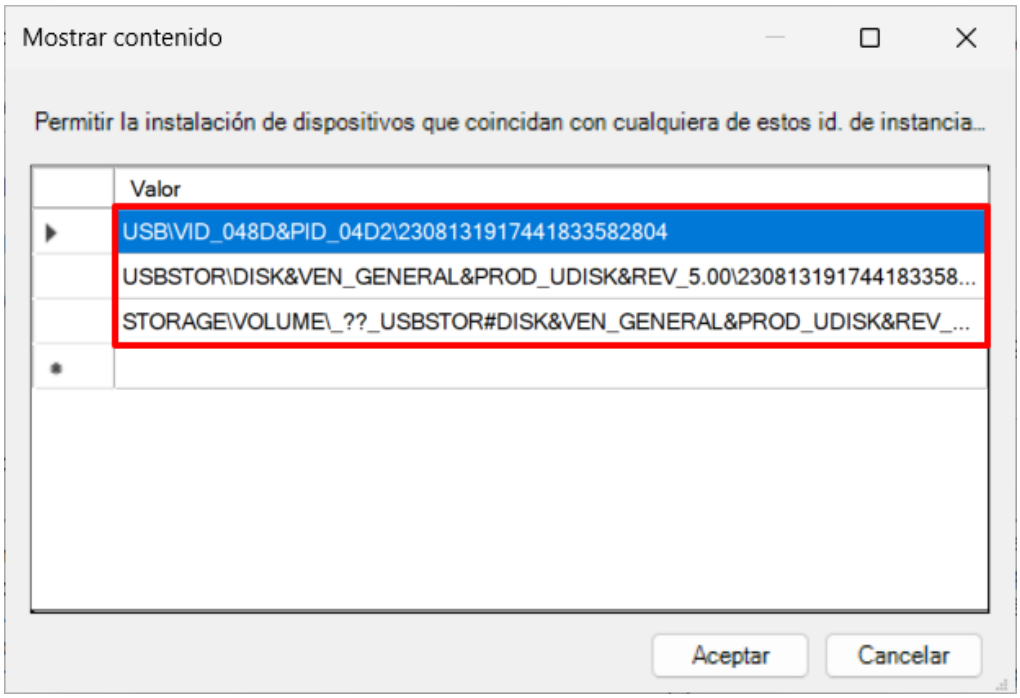
Paso	Descripción
39.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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
40.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-599A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
41.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

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

Paso	Descripción
43.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la línea en blanco para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Verifique el identificador introducido y pulse “Aceptar” para continuar. 
44.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo”.
45.	Sin cerrar el “Editor de directivas de grupo”, continue con el siguiente paso.

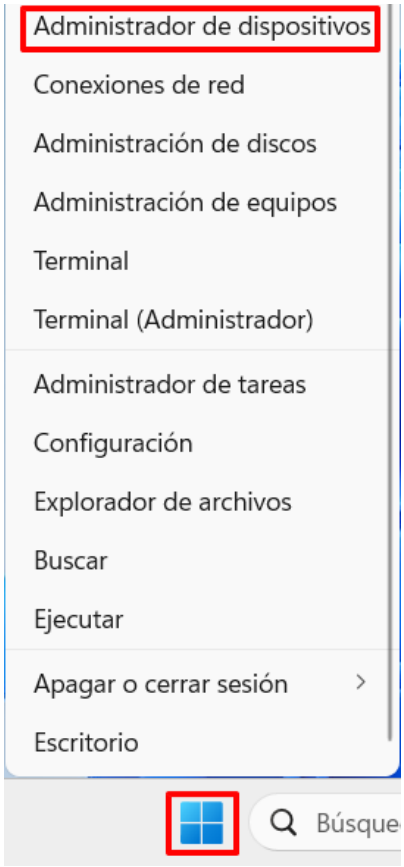
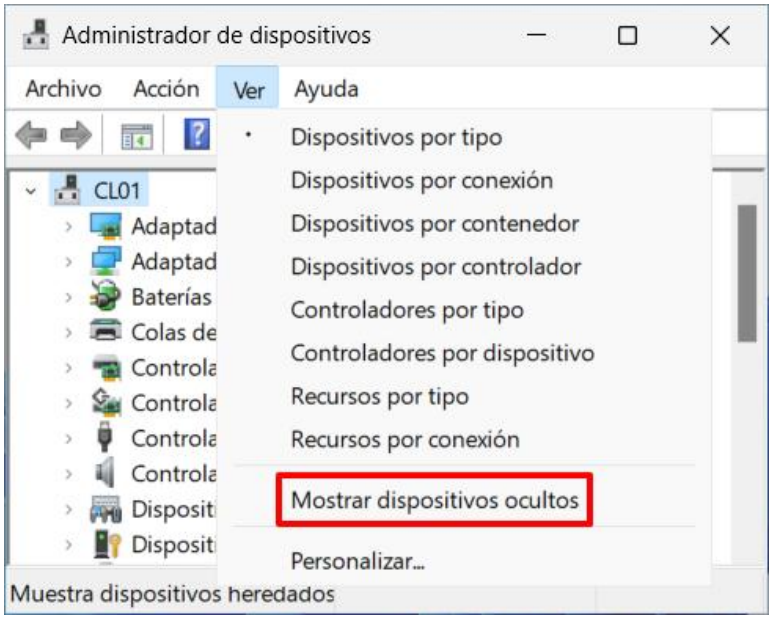
Paso	Descripción
46.	Sobre el equipo destino en el que se desea el uso de un dispositivo USB, haga clic derecho sobre el botón de “Inicio” y pulse sobre “Terminal (Administrador)”. 
47.	Ejecute el siguiente comando en la consola y espere a que finalice. > gpupdate /force 

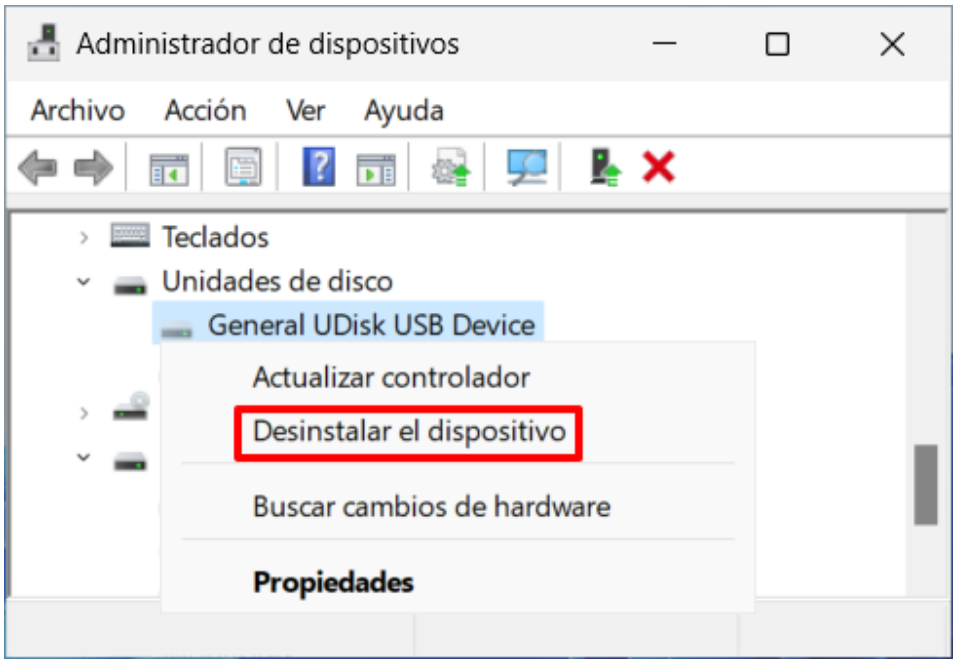
Paso	Descripción
48.	Ejecute de nuevo los pasos 33 a 47 con el objetivo de añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows. 

ANEXO A.2.7.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

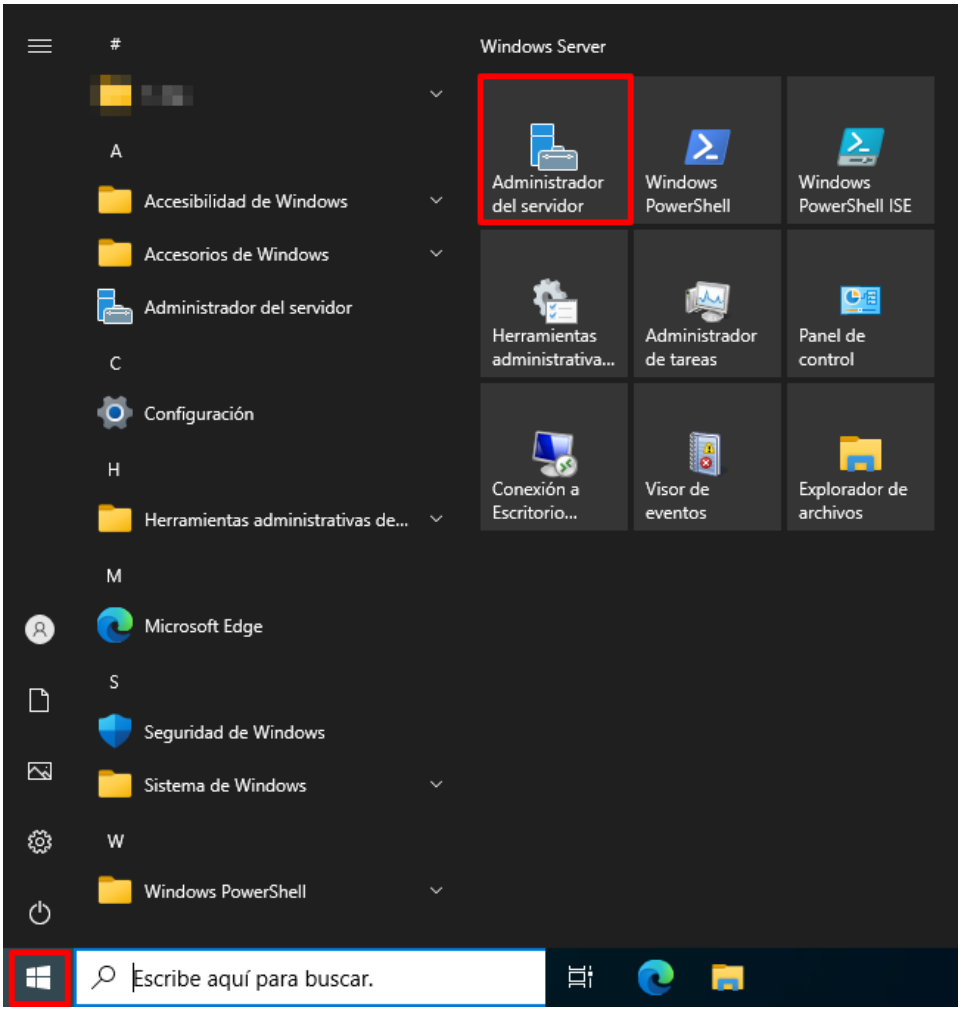
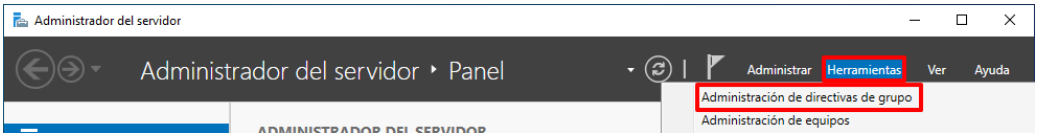
Tras la instalación del dispositivo y su posterior uso, es posible volver al estado anterior de bloqueo del uso de dispositivos USB dado de alta previamente. Para ello deberán seguir los siguientes pasos.

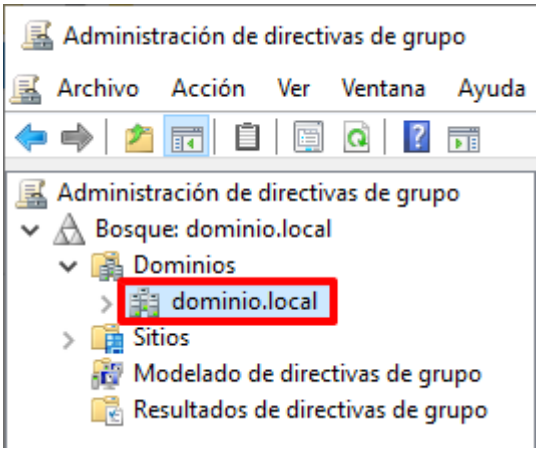
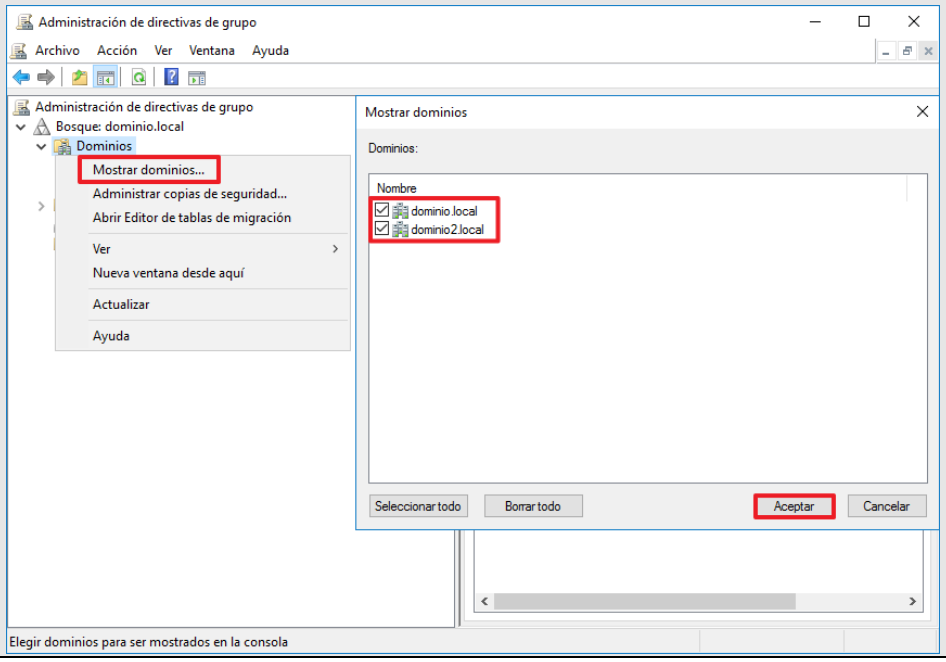
Paso	Descripción
49.	Inicie sesión en el equipo cliente donde pretende eliminar el uso de un dispositivo USB.

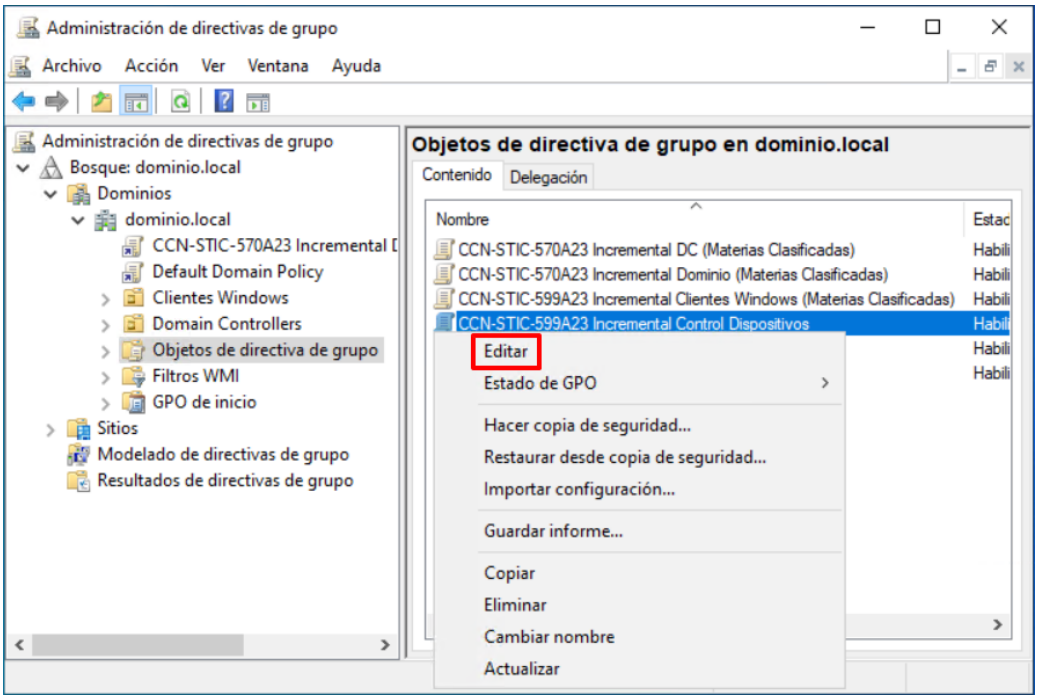
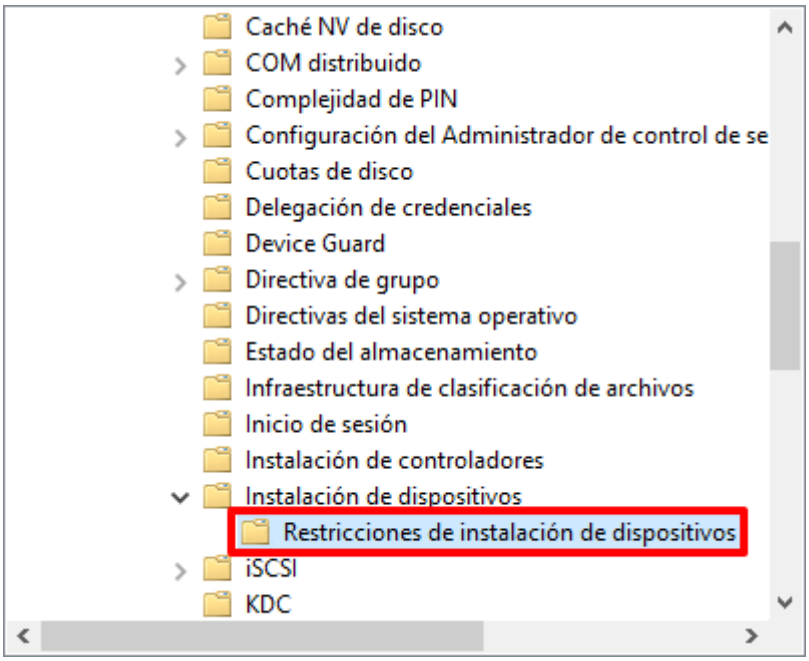
Paso	Descripción
50.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 
51.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

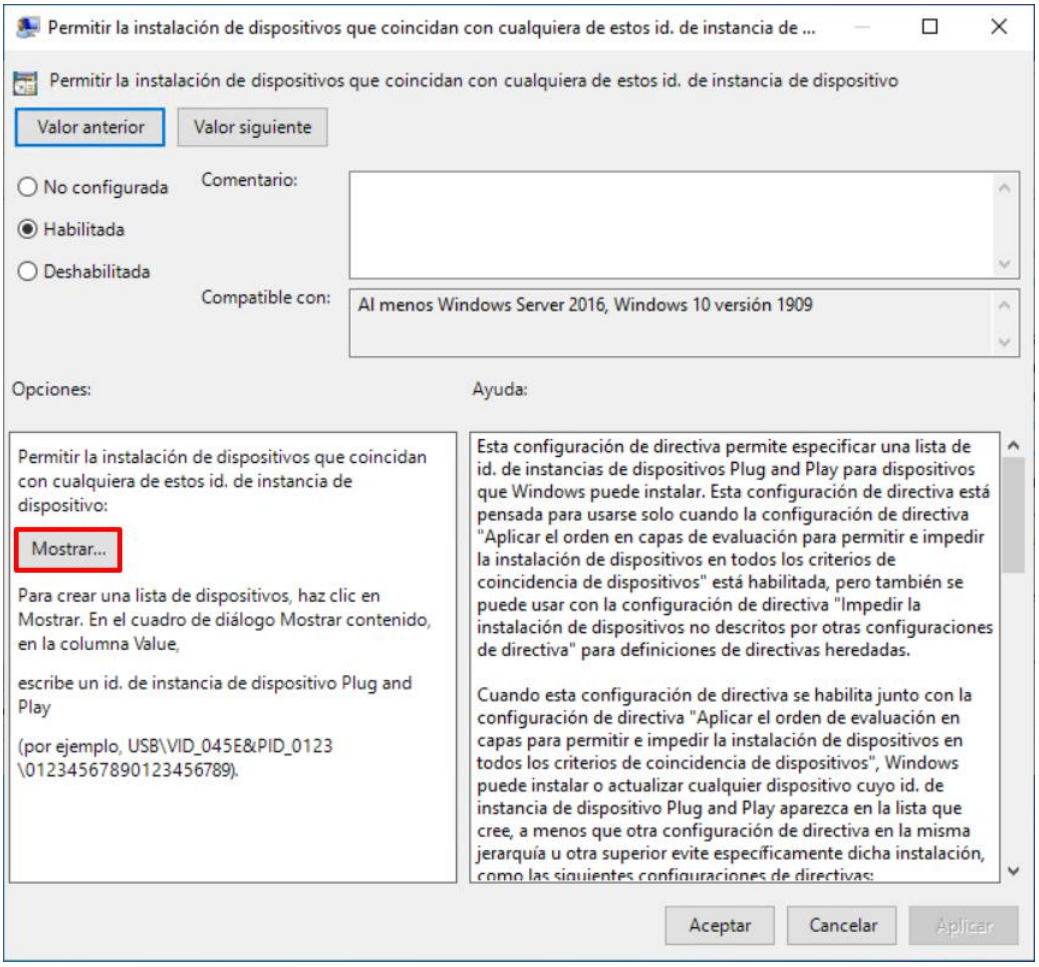
Paso	Descripción
52.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. A continuación, haga clic derecho sobre el mismo y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
53.	Pulse “Desinstalar” ante la advertencia 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.

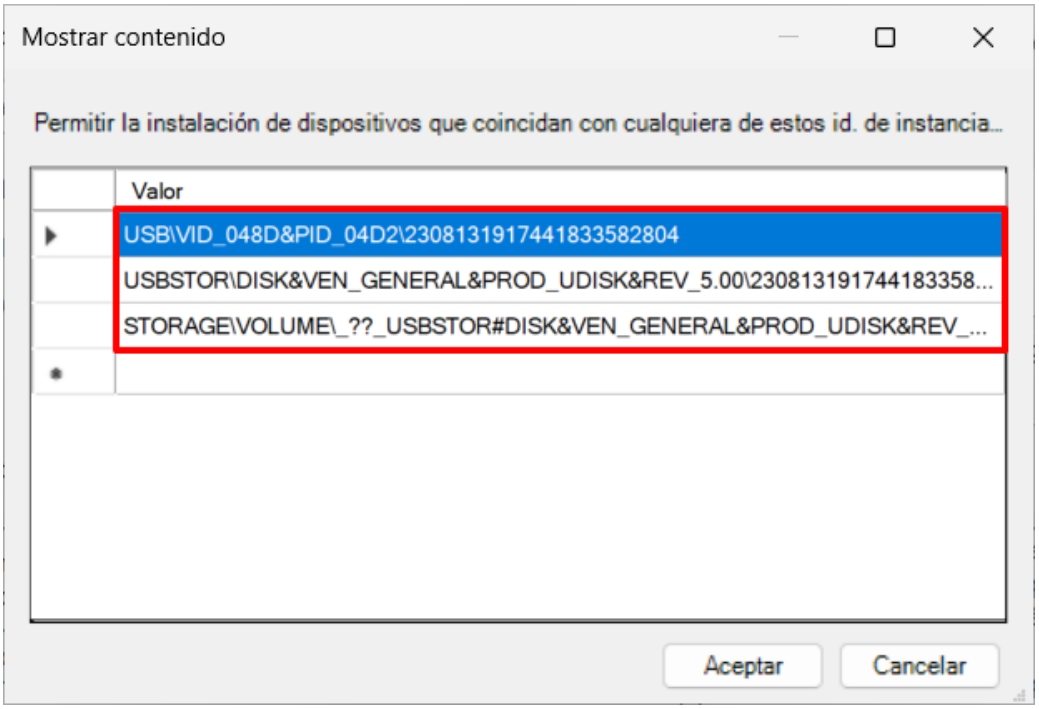
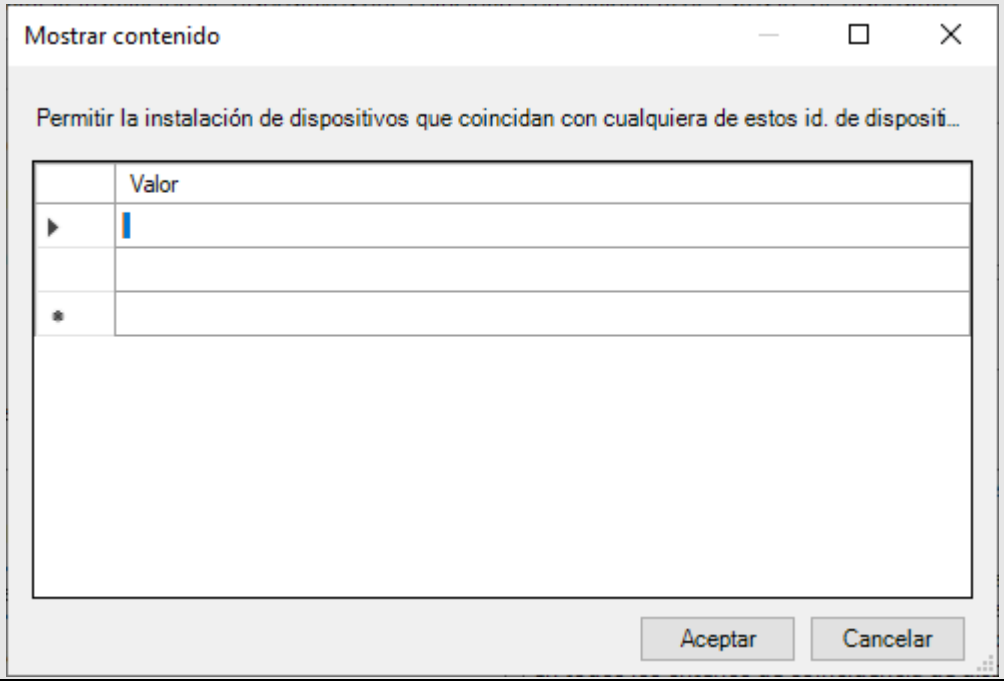
Los siguientes pasos solo serán necesarios en caso de haber hecho uso de la instalación mediante el uso de identificadores únicos de USB.

Paso	Descripción
54.	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.
55.	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".
56.	En la parte superior derecha pulse sobre el botón "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

Paso	Descripción
57.	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
58.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-599A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
59.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

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

Paso	Descripción
61.	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 A.3. CONFIGURACIONES DE MEJORA

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

ANEXO A.3.1. 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 cliente miembro, independientemente de su función, 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.

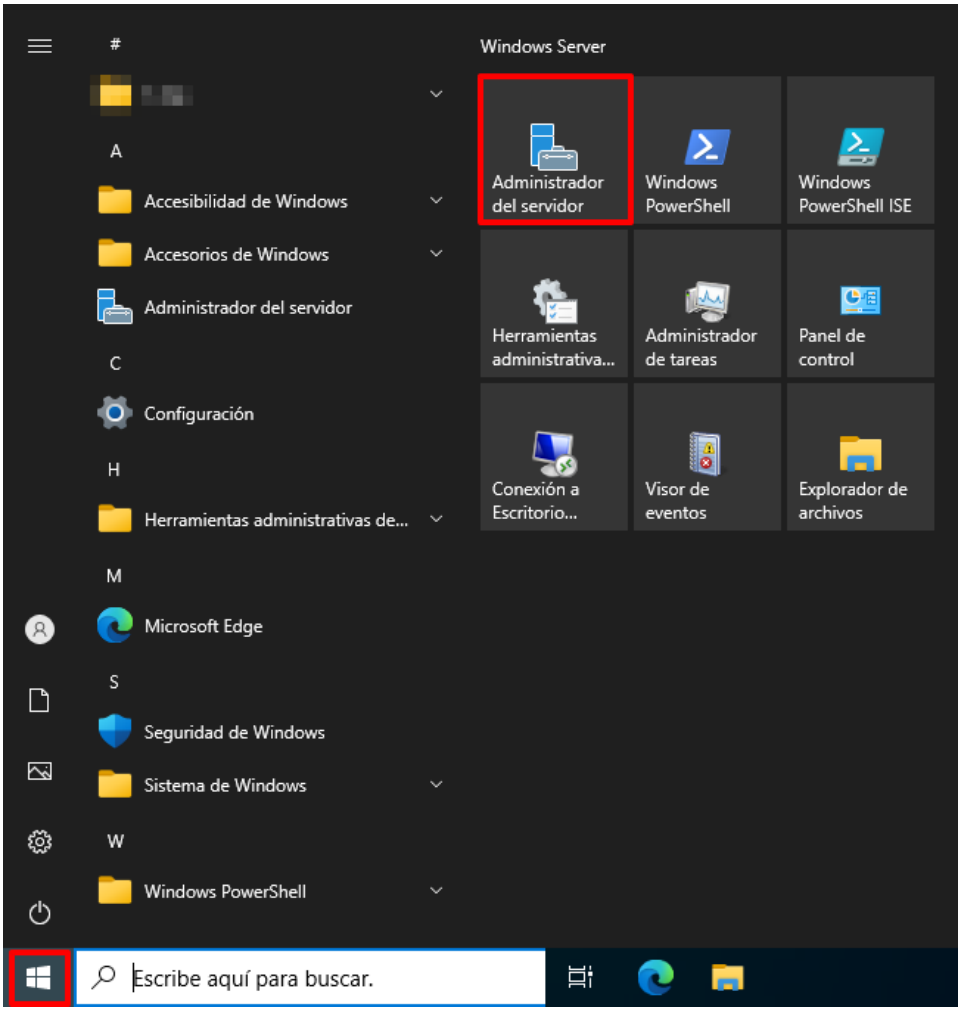
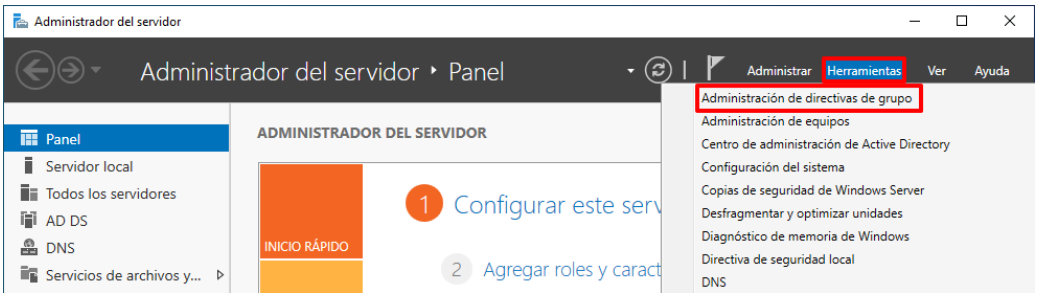
Realizadas las acciones descritas en el presente punto se presentarán dos formas de instalar controladores para el uso de dispositivos.

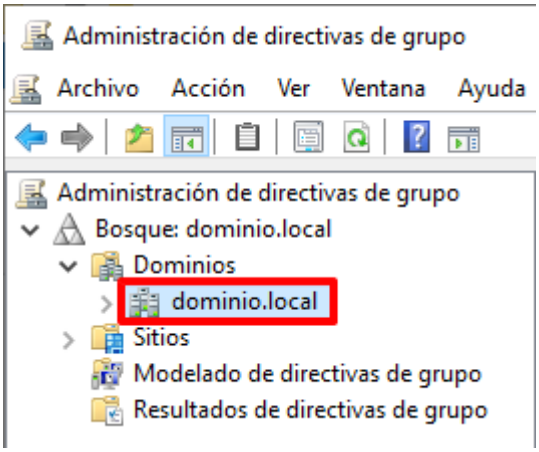
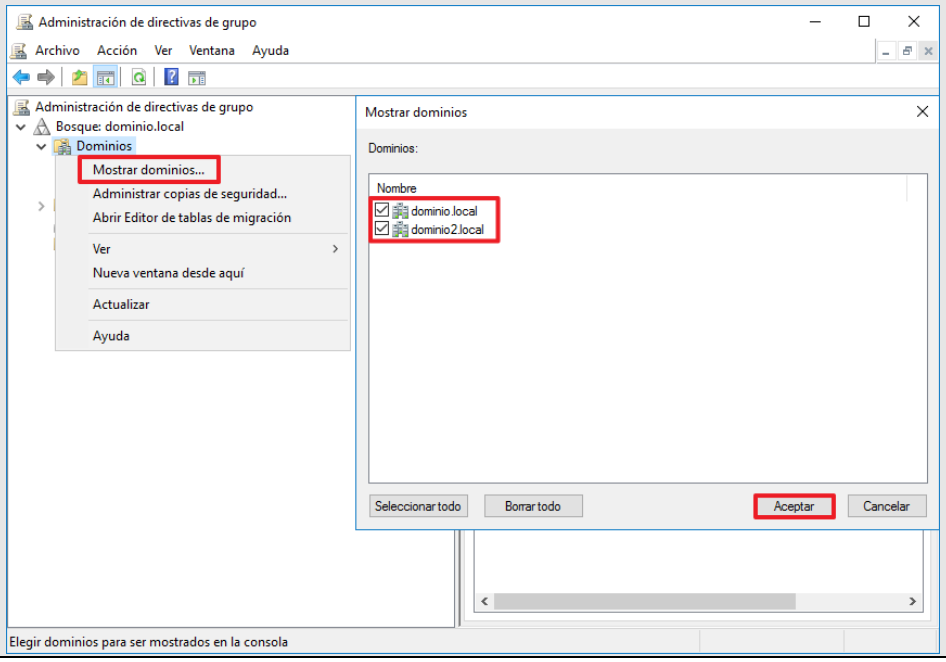
a) Actualización automática de controladores por parte de usuario con privilegios de administrador.

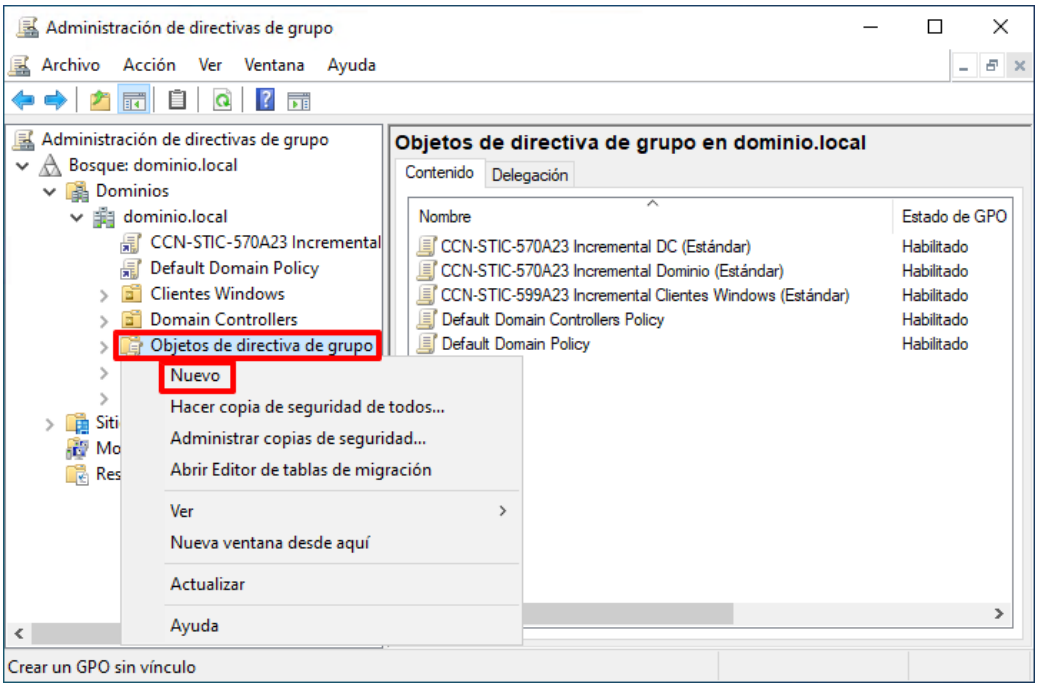
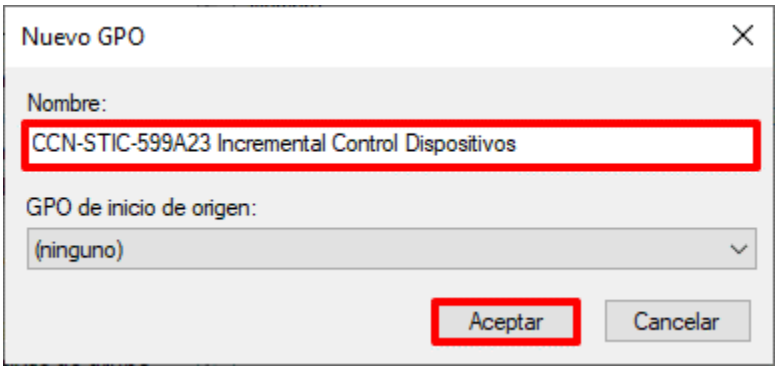
b) Alta de dispositivos por medio de identificadores únicos de los dispositivos.

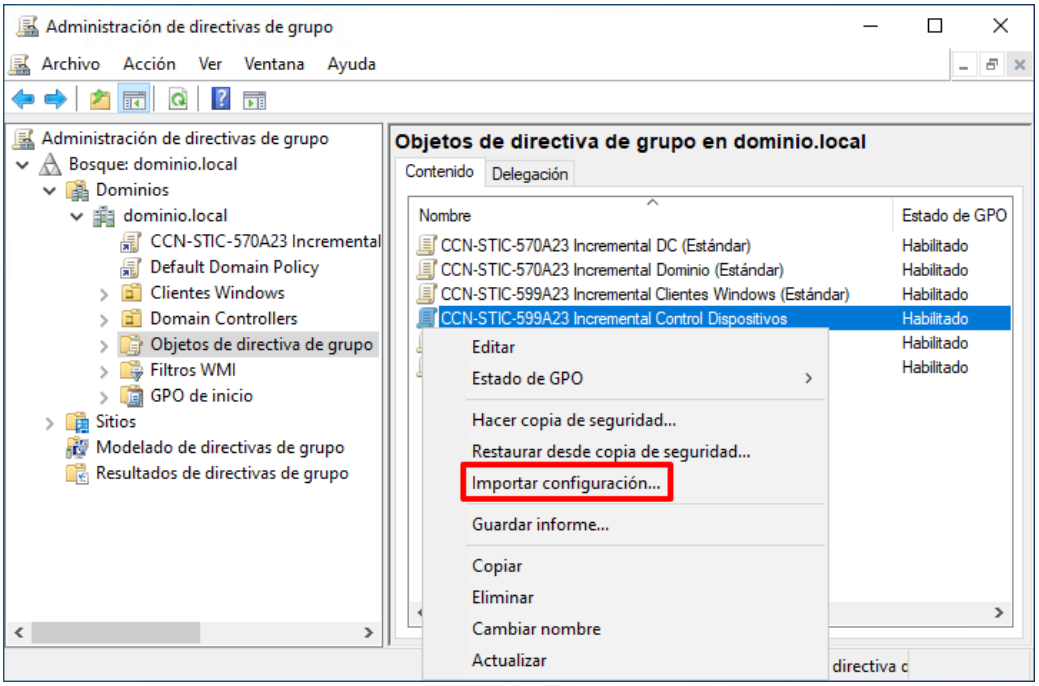
Nota: El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. A pesar de esto, las configuraciones y pasos descritos a continuación son válidos para el perfil "Uso Oficial" y obligatorio para el perfil "Materias Clasificadas", tal y como se expone en el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

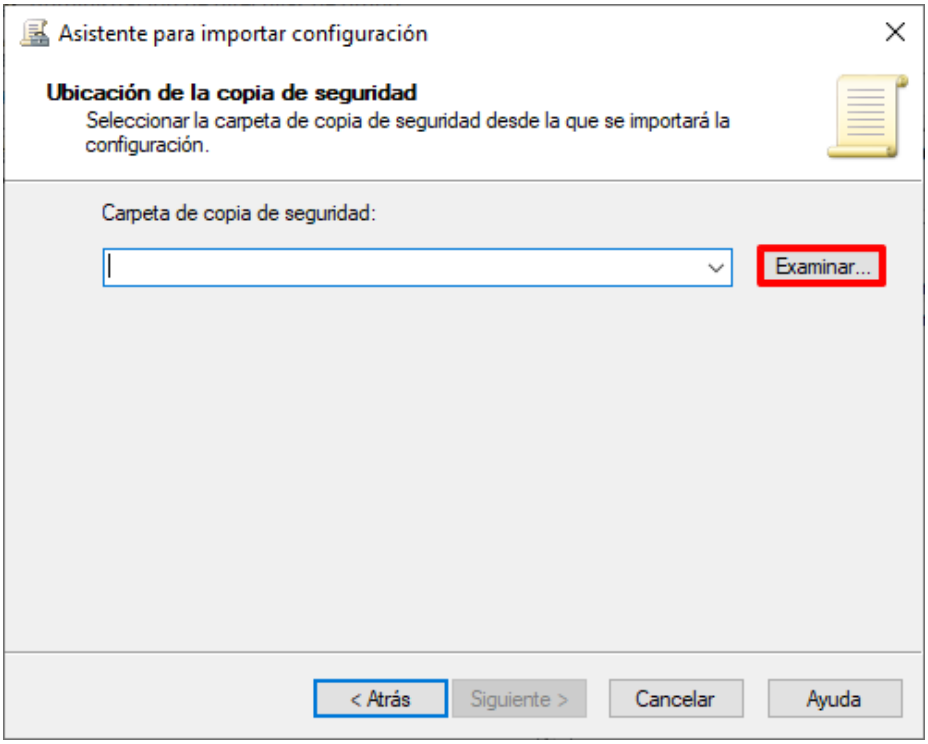
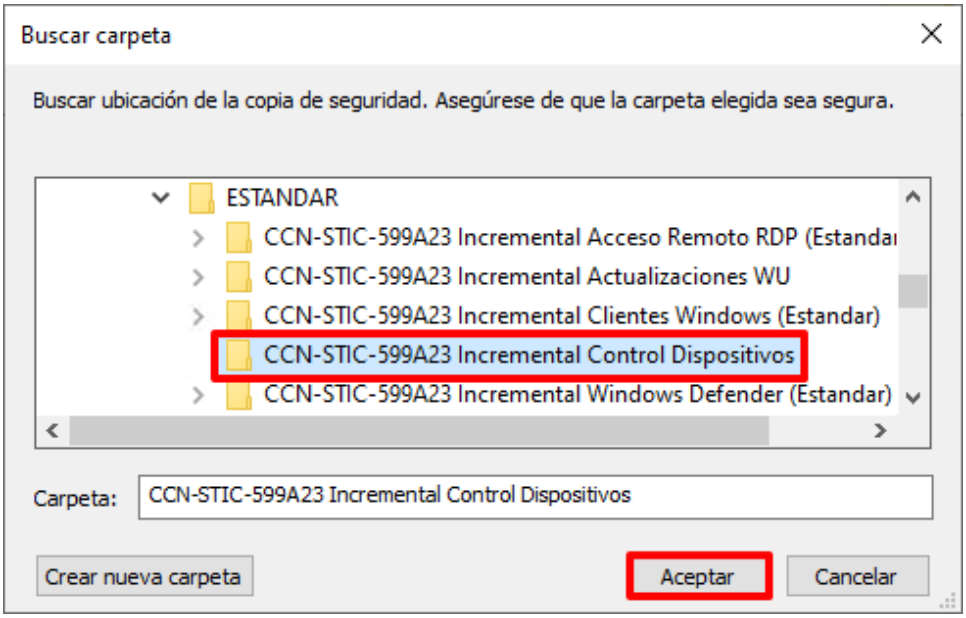
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

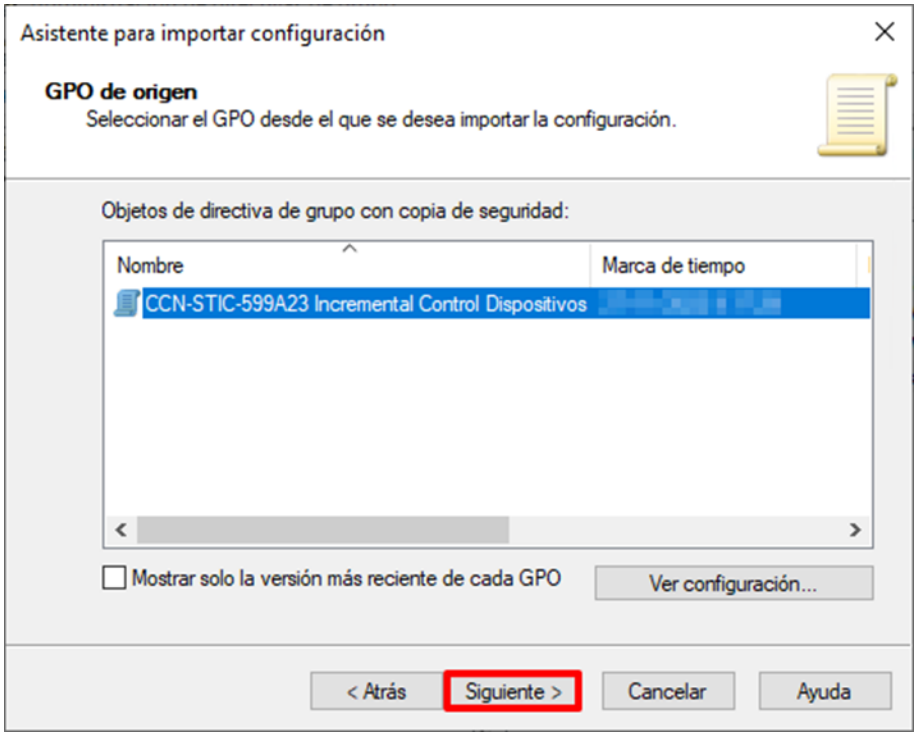
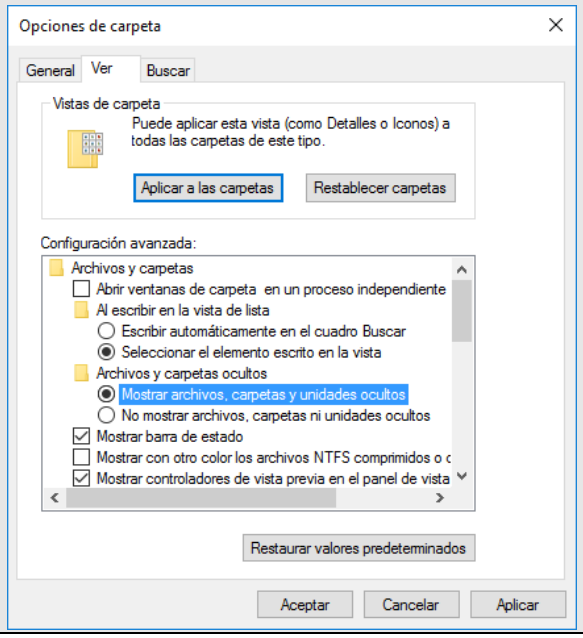
Paso	Descripción
2.	Ejecute el “Administrador del servidor”, haciendo clic sobre el botón de “Inicio” y seleccionando el icono correspondiente.  **Nota:** Si ha modificado o reubicado los accesos por defecto de Windows deberá hacer uso del buscador situado a la derecha del botón de “Inicio” para ejecutar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

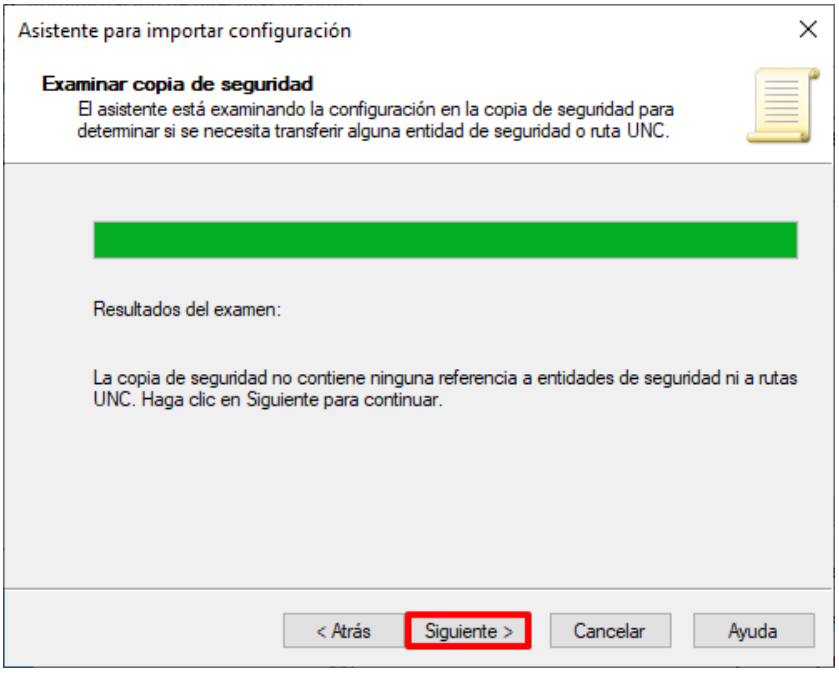
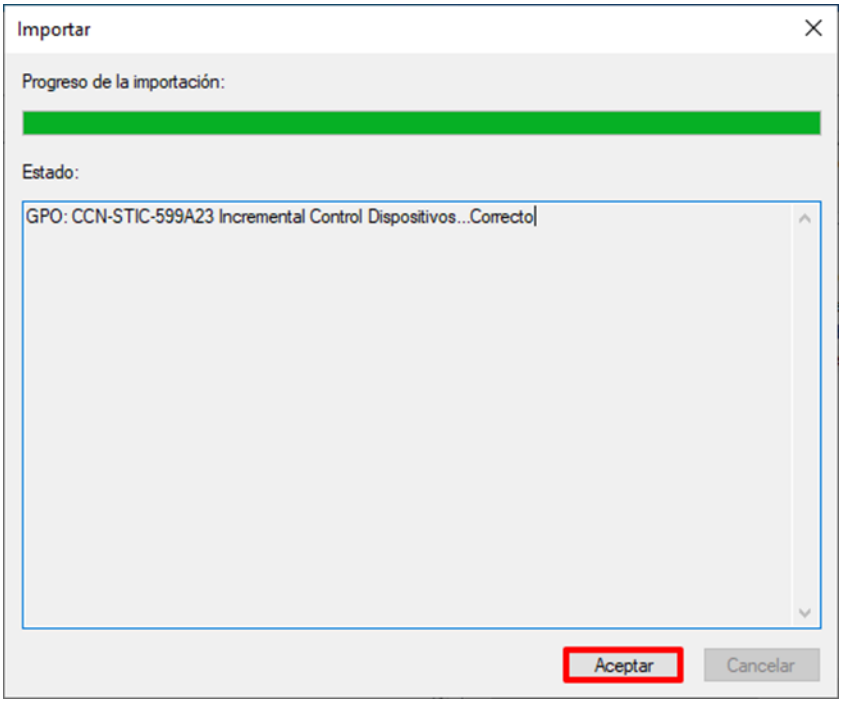
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

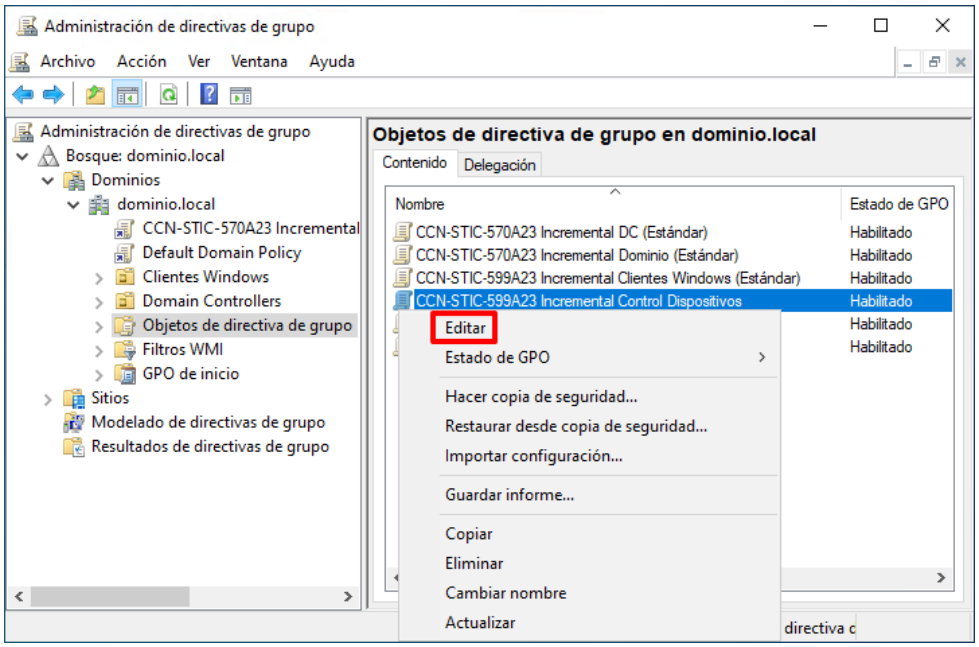
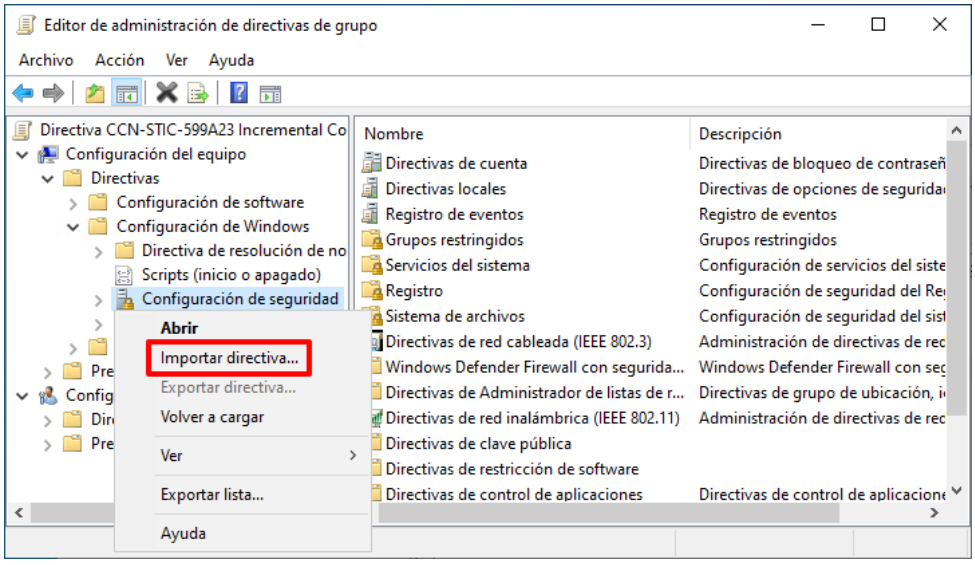
Paso	Descripción
5.	Seleccione el contenedor "Objetos de directiva de grupo", y pulsando con el botón derecho sobre él, seleccione la opción "Nuevo" del menú contextual que aparecerá. 
6.	Asigne el siguiente nombre al nuevo objeto GPO: "**CCN-STIC-599A23 Incremental Control Dispositivos**" y pulse el botón "Aceptar". 

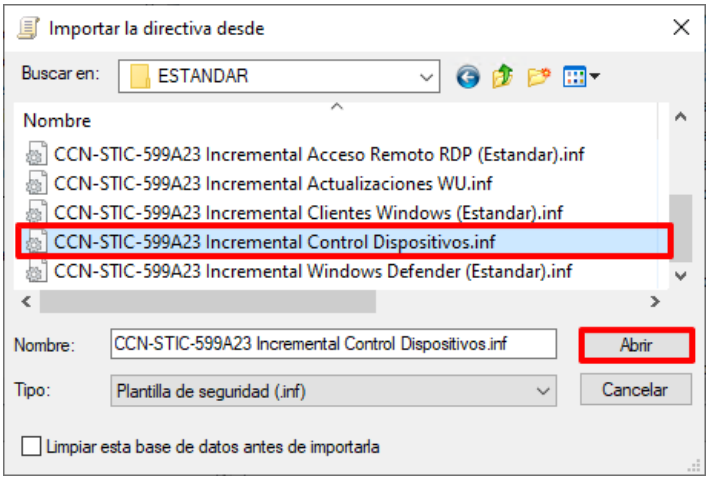
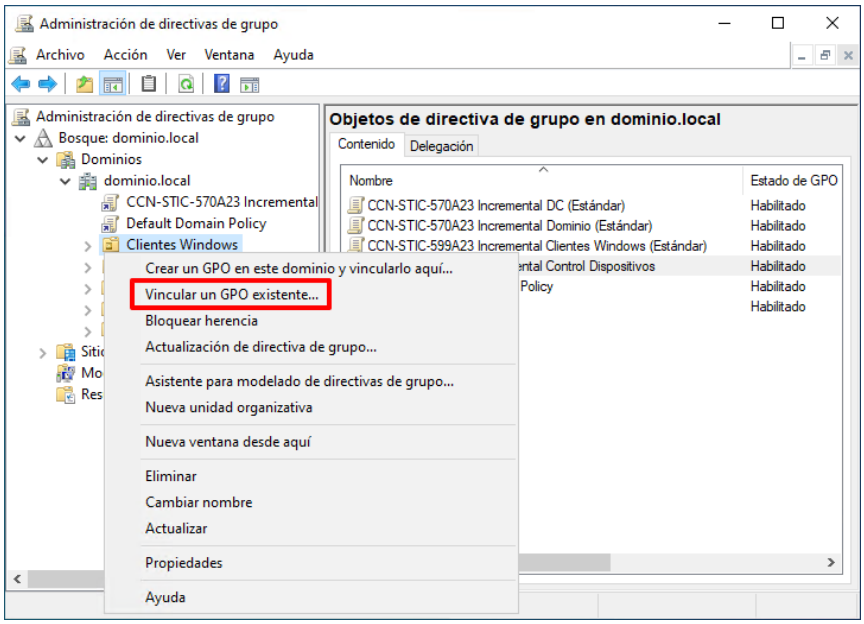
Paso	Descripción
7.	Seleccione con el botón derecho el objeto GPO recién creado y pulse sobre “Importar configuración…” del menú contextual que aparecerá. 
8.	En la primera ventana del “Asistente para importar configuración” pulse sobre “Siguiente >”.
9.	En la sección “Hacer copia de seguridad de GPO”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

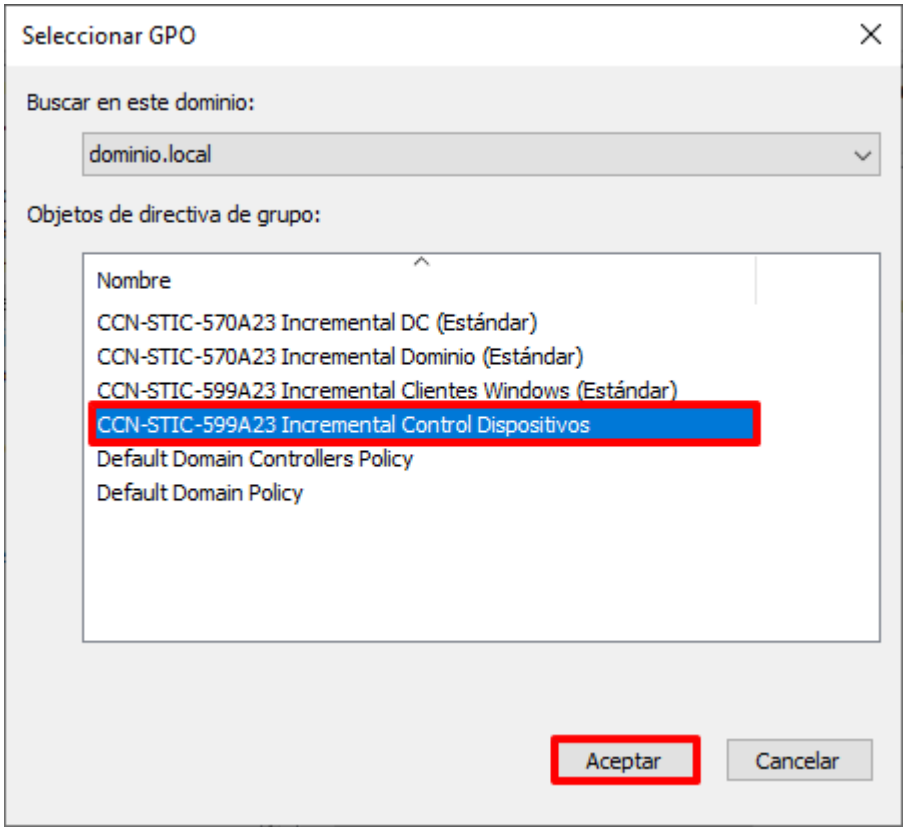
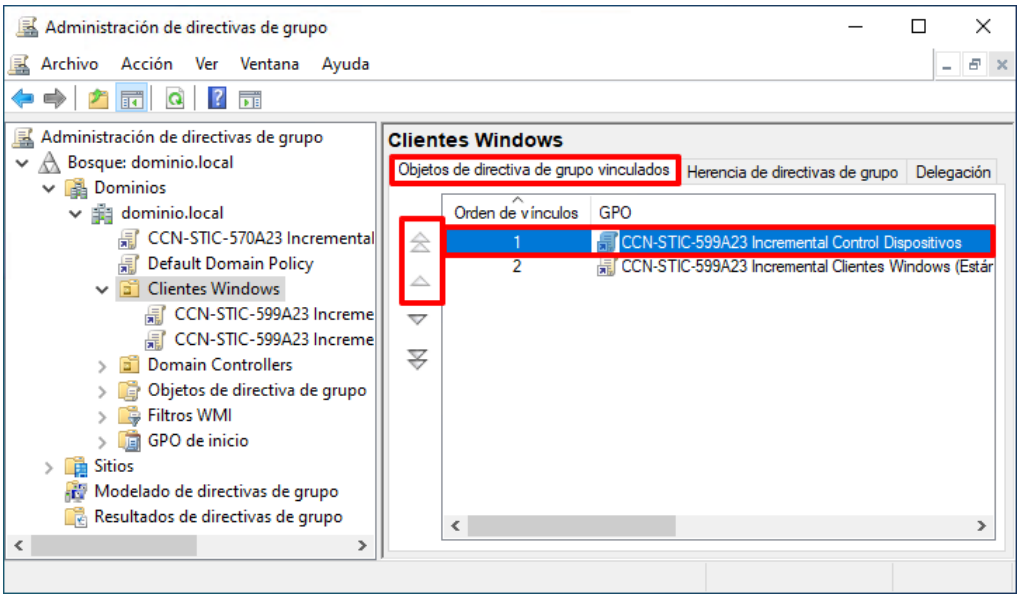
Paso	Descripción
10.	Pulse sobre el botón “Examinar…” en el apartado “Ubicación de la copia de seguridad”. 
11.	Seleccione la carpeta “CCN-STIC-599A23 Incremental Control Dispositivos” situada en el directorio “C:\Scripts\[TIPO DE PERFILADO]” y pulse “Aceptar”.  **Nota:** Seleccione el objeto GPO acorde 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-599A23 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-599A23 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-599A23 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. 

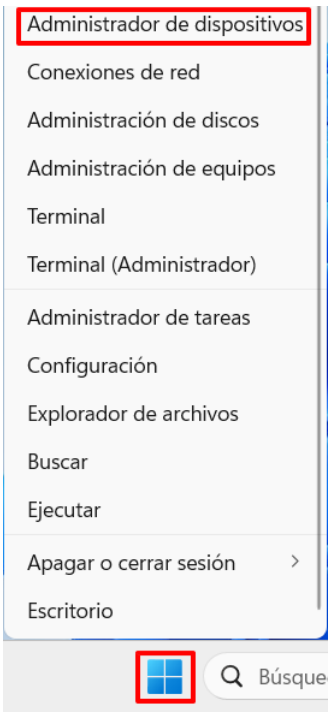
Paso	Descripción
20.	En el cuadro de diálogo que aparecerá, titulado "Importar la directiva desde", seleccione la configuración de seguridad ubicada en "C:\Scripts\[TIPO DE PERFILADO]" denominada "CCN-STIC-599A23 Incremental Control Dispositivos.inf". A continuación, pulse sobre el botón "Abrir".  **Nota:** 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 "Clientes Windows", creada para tal fin.

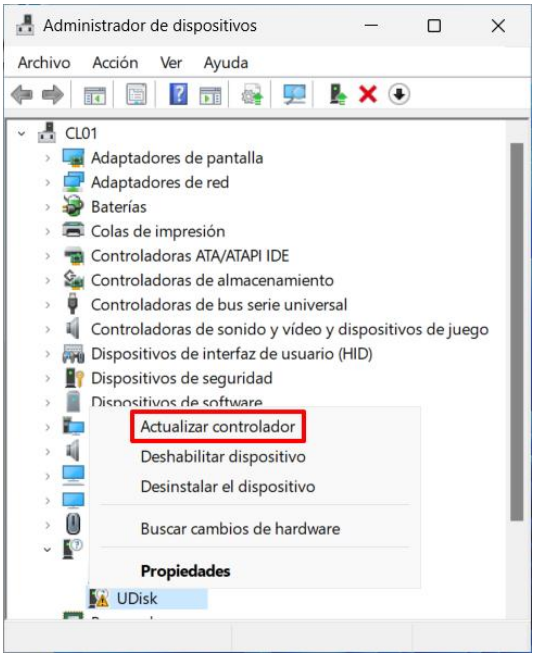
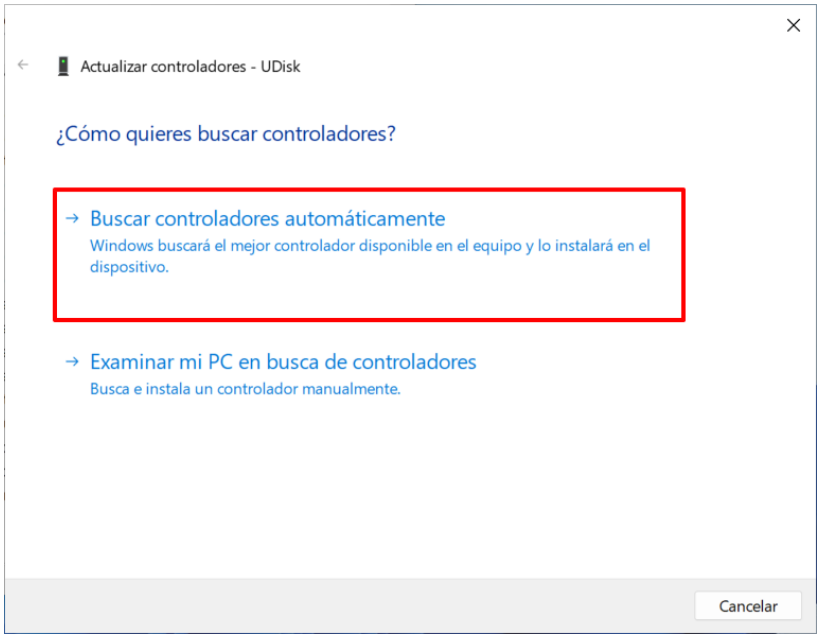
Paso	Descripción
22.	A continuación, seleccione el objeto GPO "CCN-STIC-599A23 Incremental Control Dispositivos" y pulse "Aceptar". 
23.	Seleccione la unidad organizativa sobre la que ha vinculado el objeto GPO y en el panel derecho, sobre la pestaña "Objetos de directiva de grupo vinculados", seleccione el objeto GPO recién vinculado y pulse sobre los botones para establecer el objeto GPO en el primer orden de vínculo. 

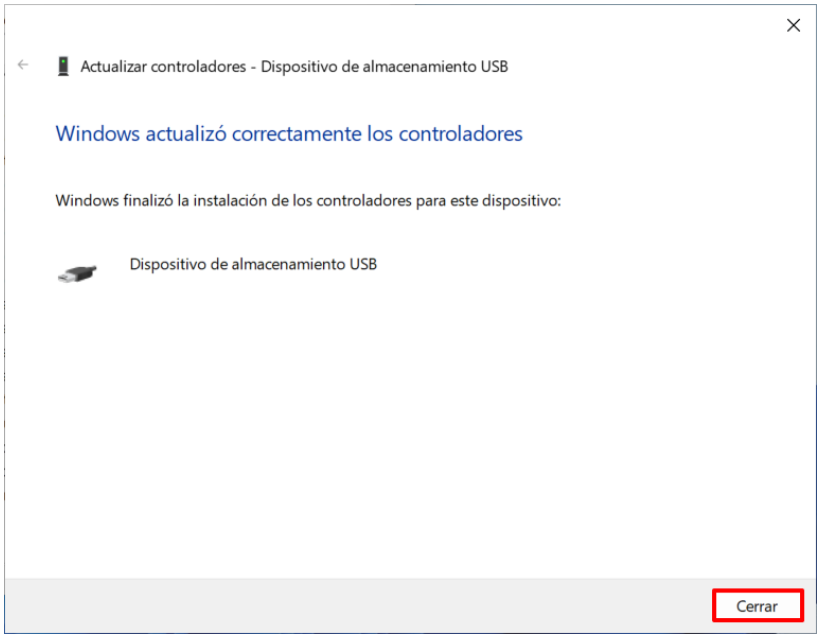
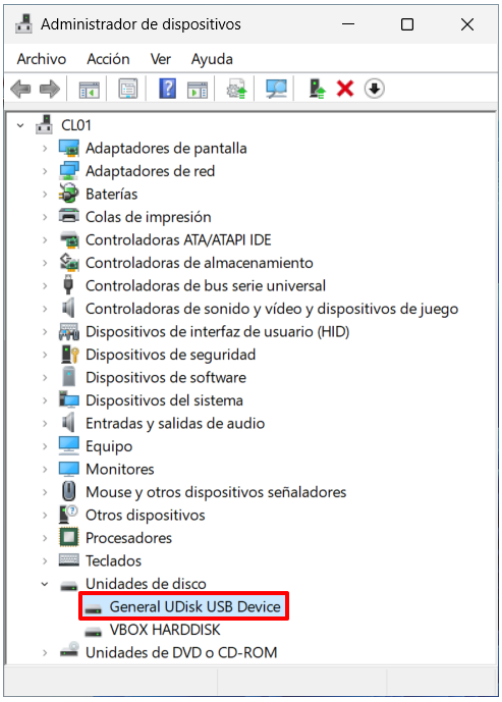
Paso	Descripción
24.	Tenga en consideración, que esto afectará a todos los equipos ubicados dentro de la unidad organizativa en la que se ha vinculado. Si no desea que la citada configuración afecte a todos los equipos dispone de varias alternativas entre las que se encuentran las siguientes: – Generación 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.1.2.2 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 A.3.1.1. 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.

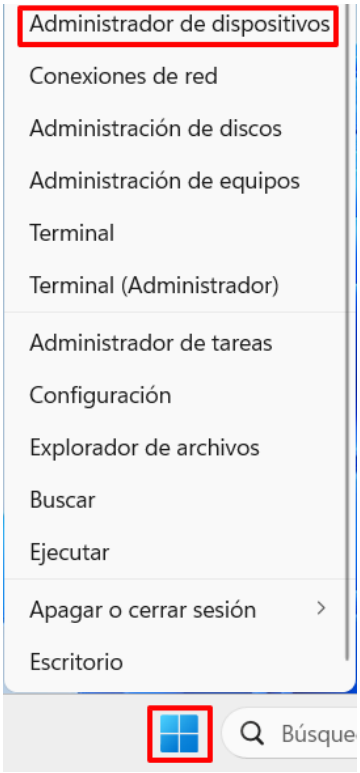
Paso	Descripción
25.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
26.	Haga clic derecho sobre el botón de "Inicio" y seleccione "Administrador de dispositivos". 

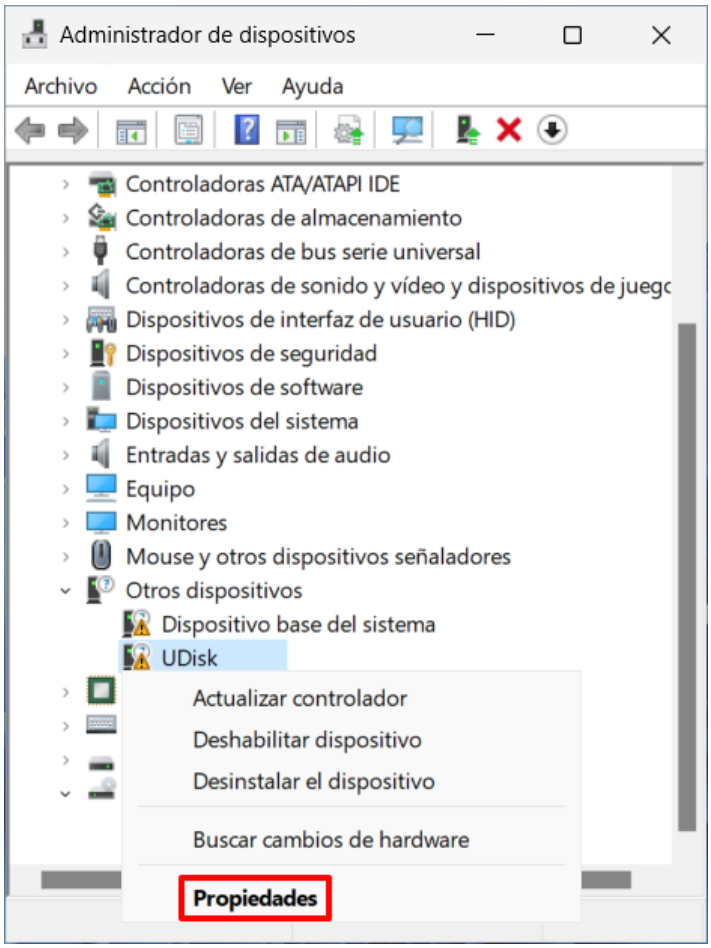
Paso	Descripción
27.	Despliegue en el "Administrador de dispositivos" el nodo "Otros dispositivos" y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual "Actualizar controlador".  **Nota:** Debido a la inexistencia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

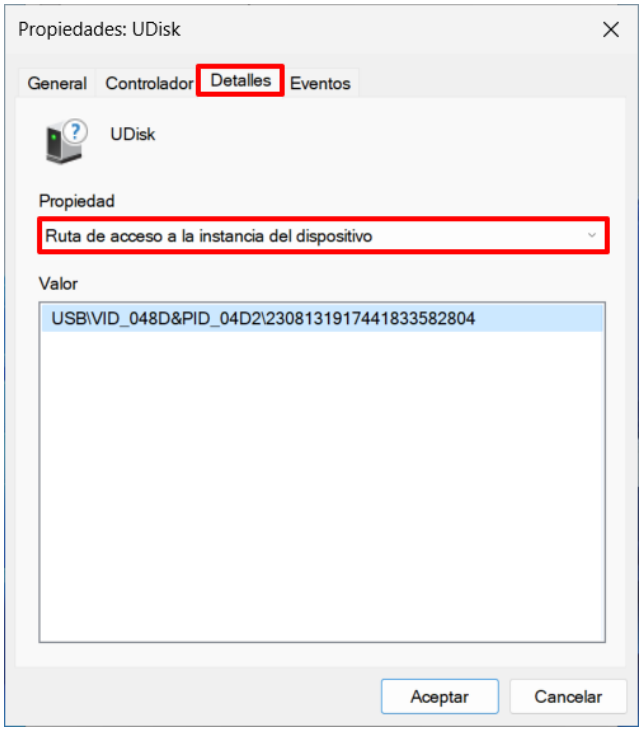
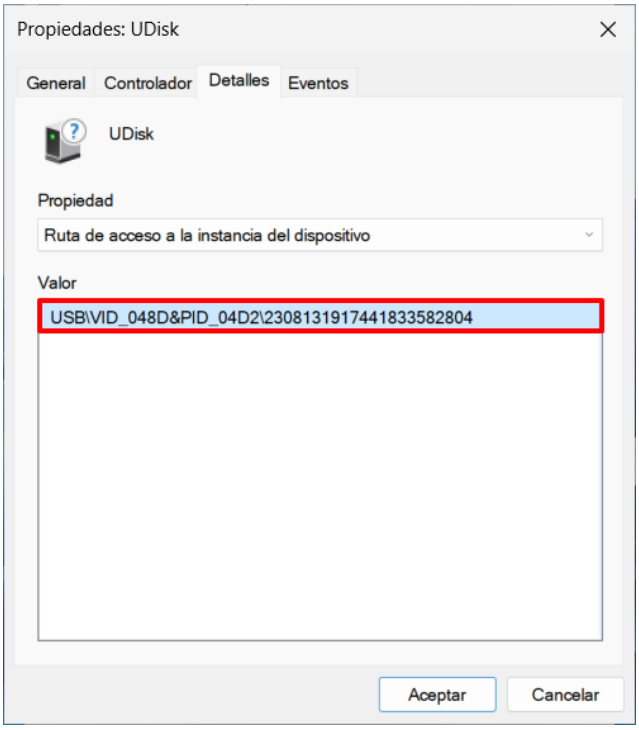
Paso	Descripción
29.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  **Nota:** No cierre el “Administrador de dispositivos” todavía.
30.	Ejecute los mismos pasos anteriores (pasos 27 a 29) hasta que el dispositivo aparezca 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. 

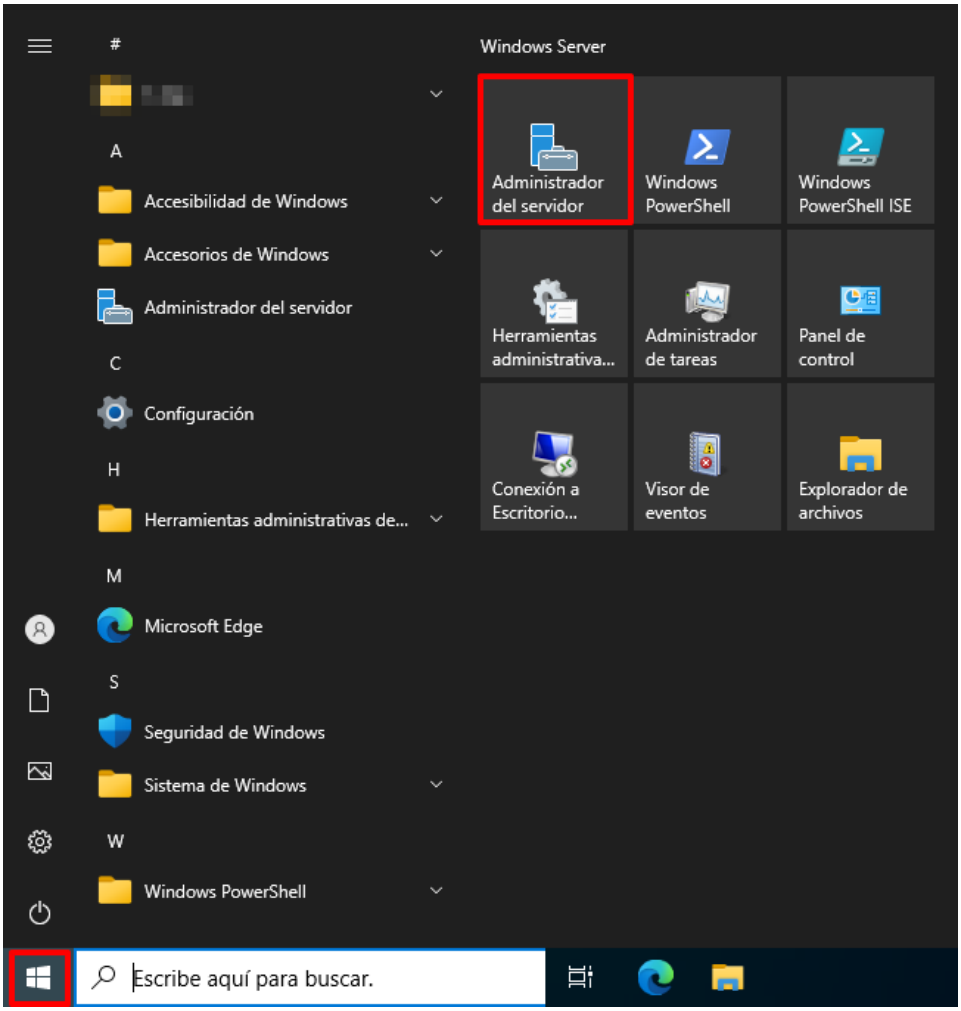
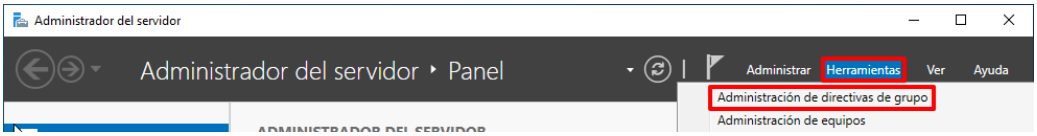
ANEXO A.3.1.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

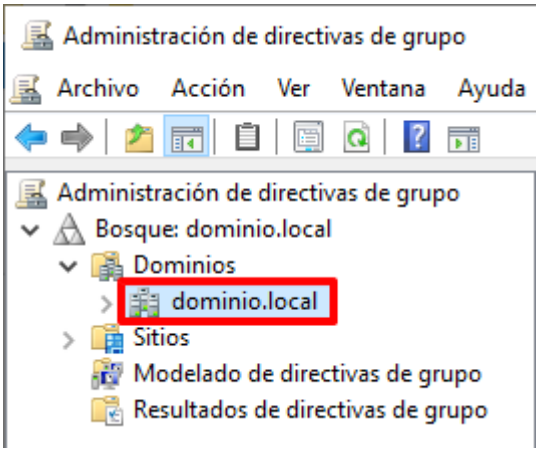
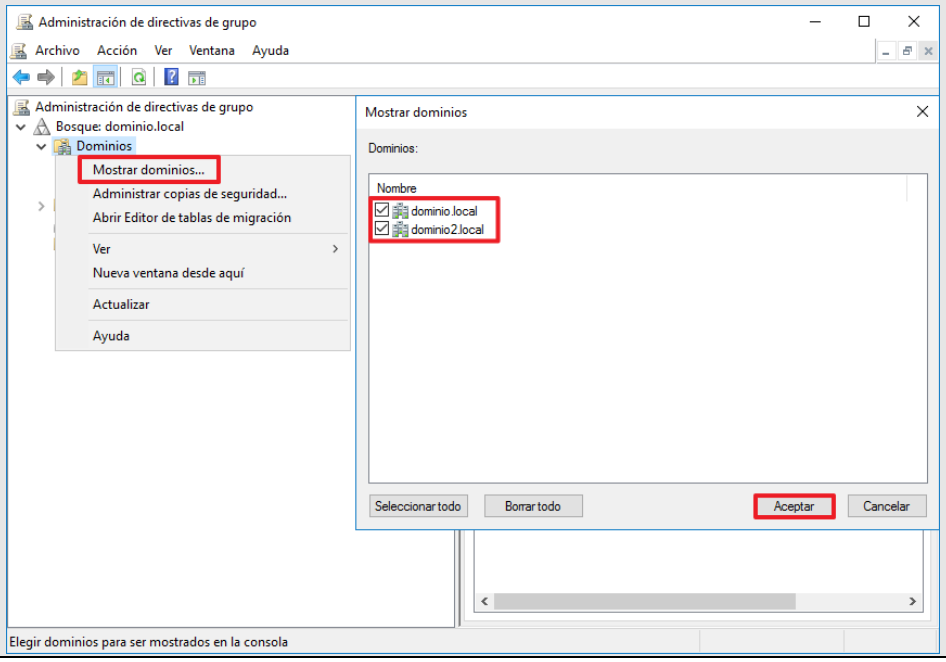
Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del dominio en el cual se está habilitando el uso de dispositivos USB y sobre un Controlador de Dominio perteneciente al dominio.

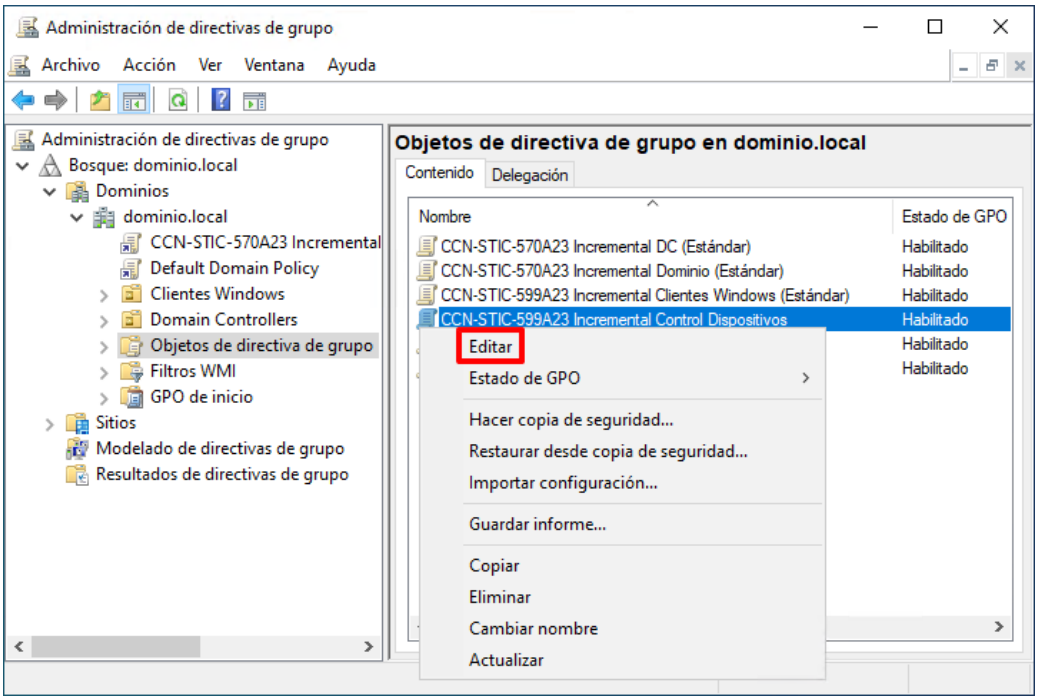
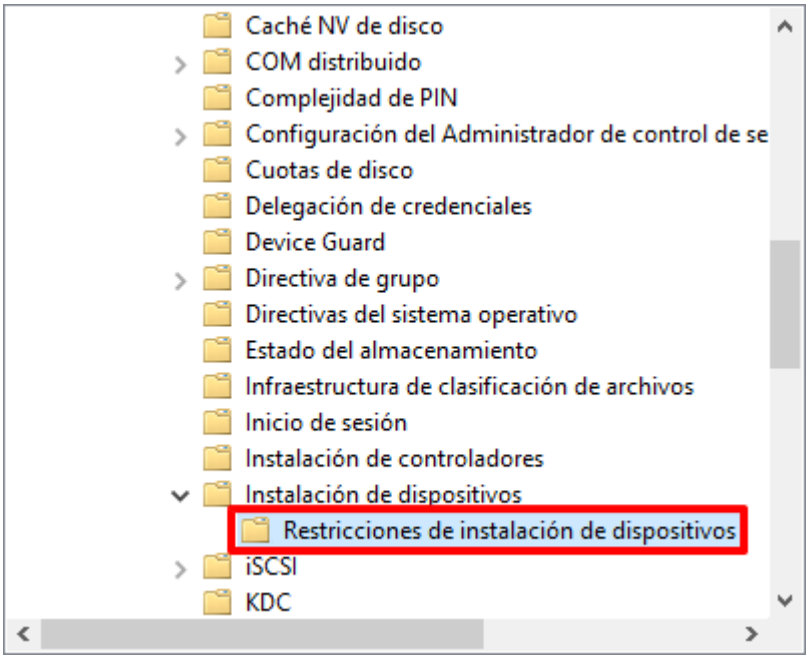
Paso	Descripción
31.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
32.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

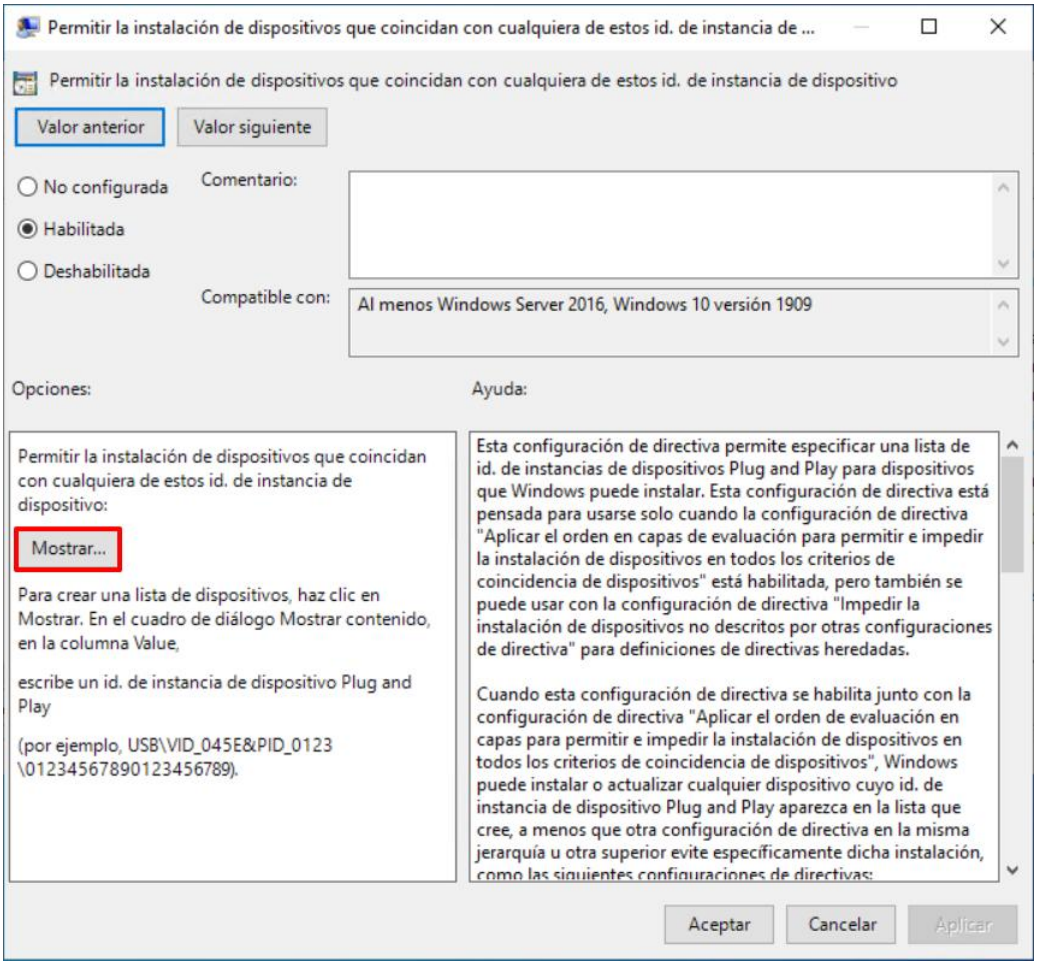
Paso	Descripción
33.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Propiedades”.  **Nota:** Debido a la inexistencia de controlador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

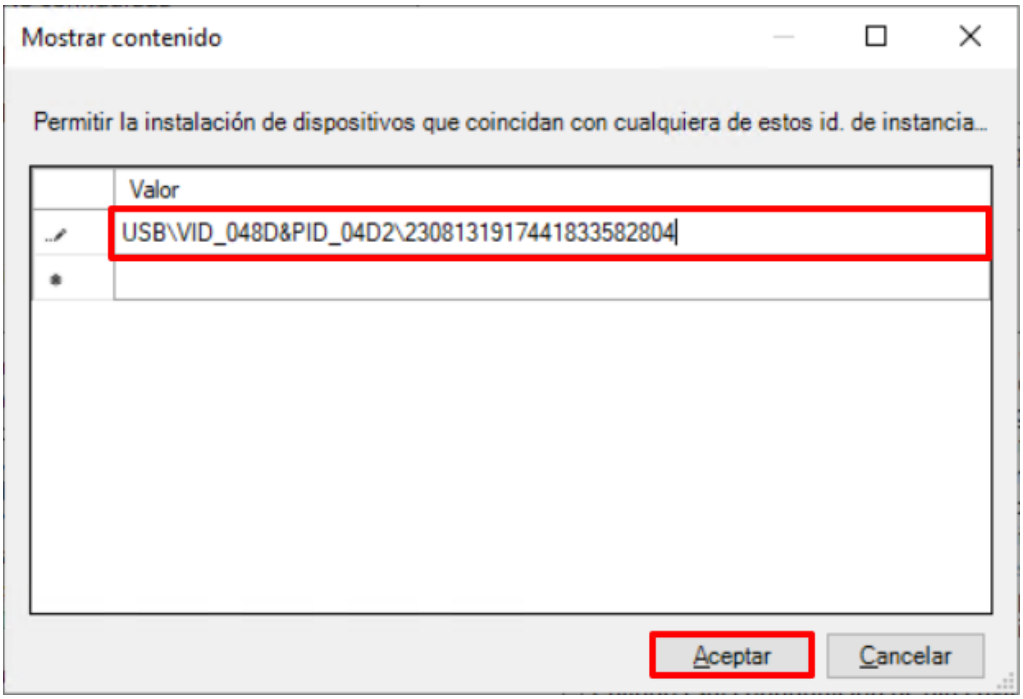
Paso	Descripción
34.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Ruta de acceso a la instancia del dispositivo”. 
35.	Seleccione el identificador y anótelo para poder introducirlo más adelante.  **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

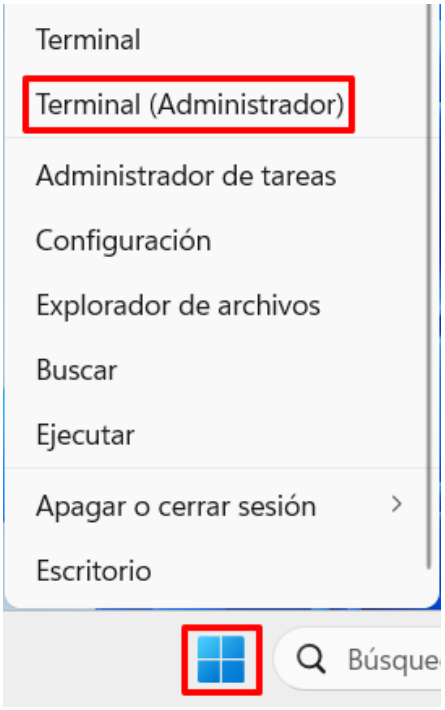
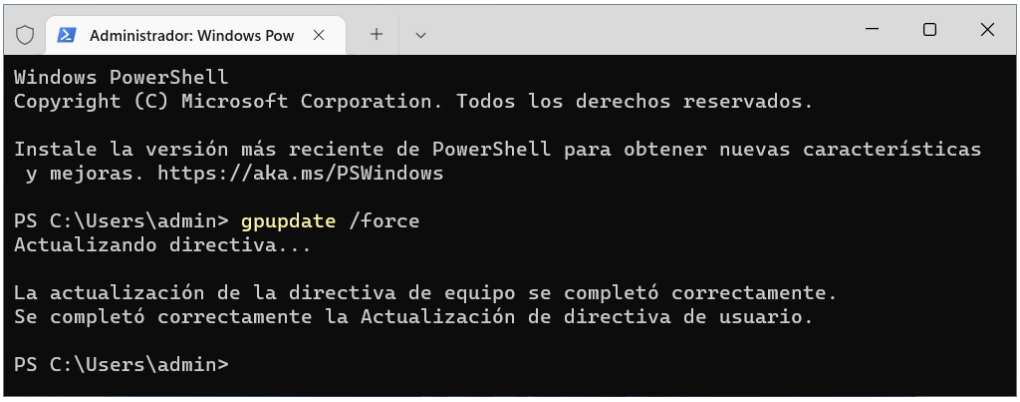
Paso	Descripción
36.	Inicie sesión en un servidor Controlado de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
37.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **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".
38.	En la parte superior derecha pulse sobre el botón "Herramientas" y a continuación seleccione "Administración de directivas de grupo". 

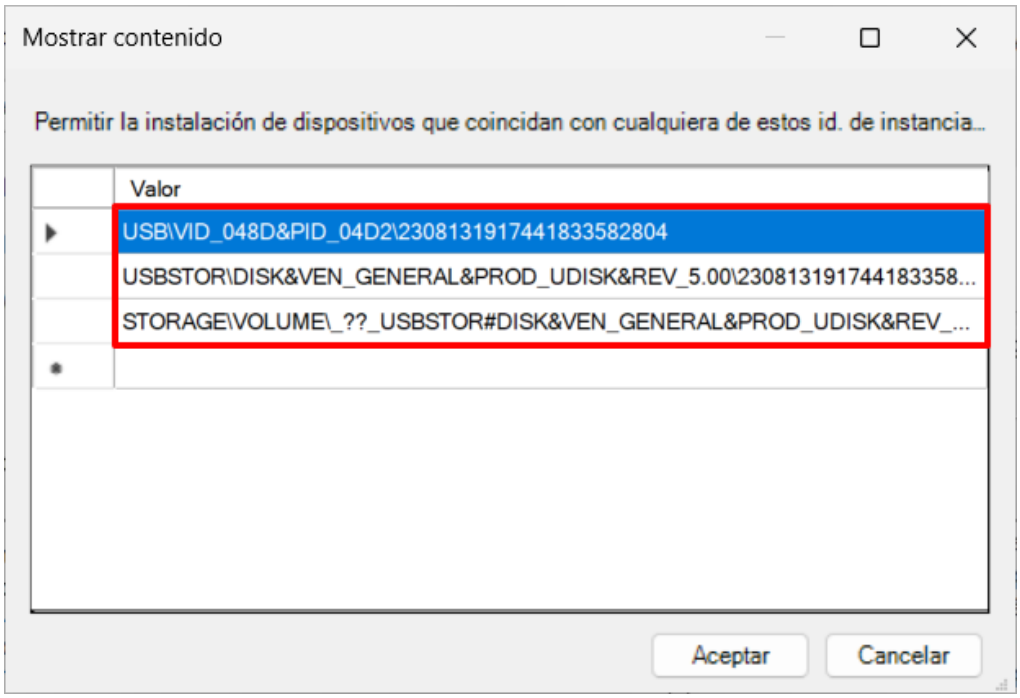
Paso	Descripción
39.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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
40.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-599A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
41.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

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

Paso	Descripción
43.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la línea en blanco para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Verifique el identificador introducido y pulse “Aceptar” para continuar. 
44.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo”.
45.	Sin cerrar el “Editor de directivas de grupo”, continue con el siguiente paso.

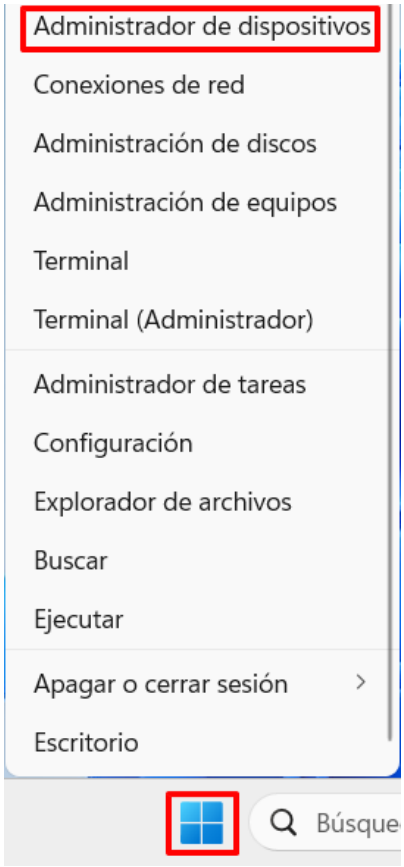
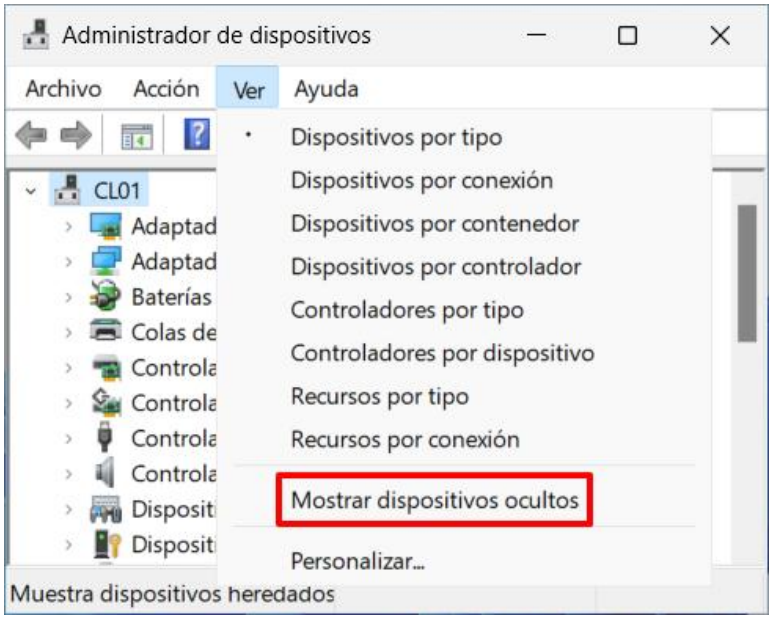
Paso	Descripción
46.	Sobre el equipo destino en el que se desea el uso de un dispositivo USB, haga clic derecho sobre el botón de “Inicio” y pulse sobre “Terminal (Administrador)”. 
47.	Ejecute el siguiente comando en la consola y espere a que finalice. > gpupdate /force 

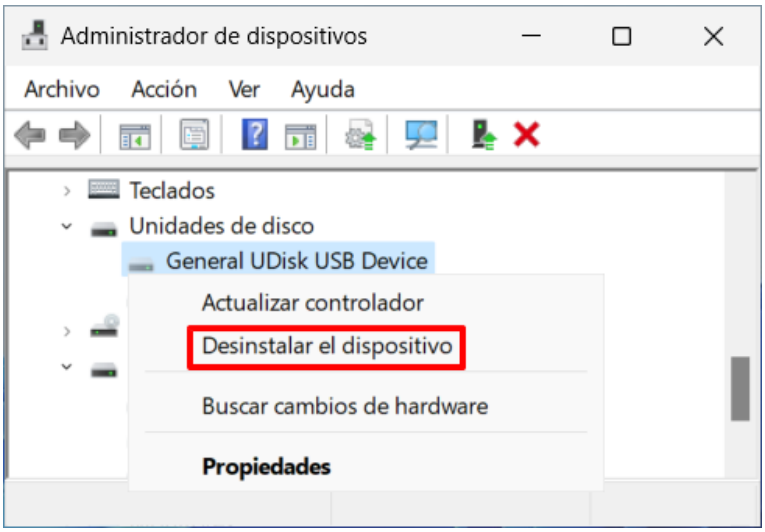
Paso	Descripción
48.	Ejecute de nuevo los pasos 33 a 47 con el objetivo de añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows. 

ANEXO A.3.1.3. 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.

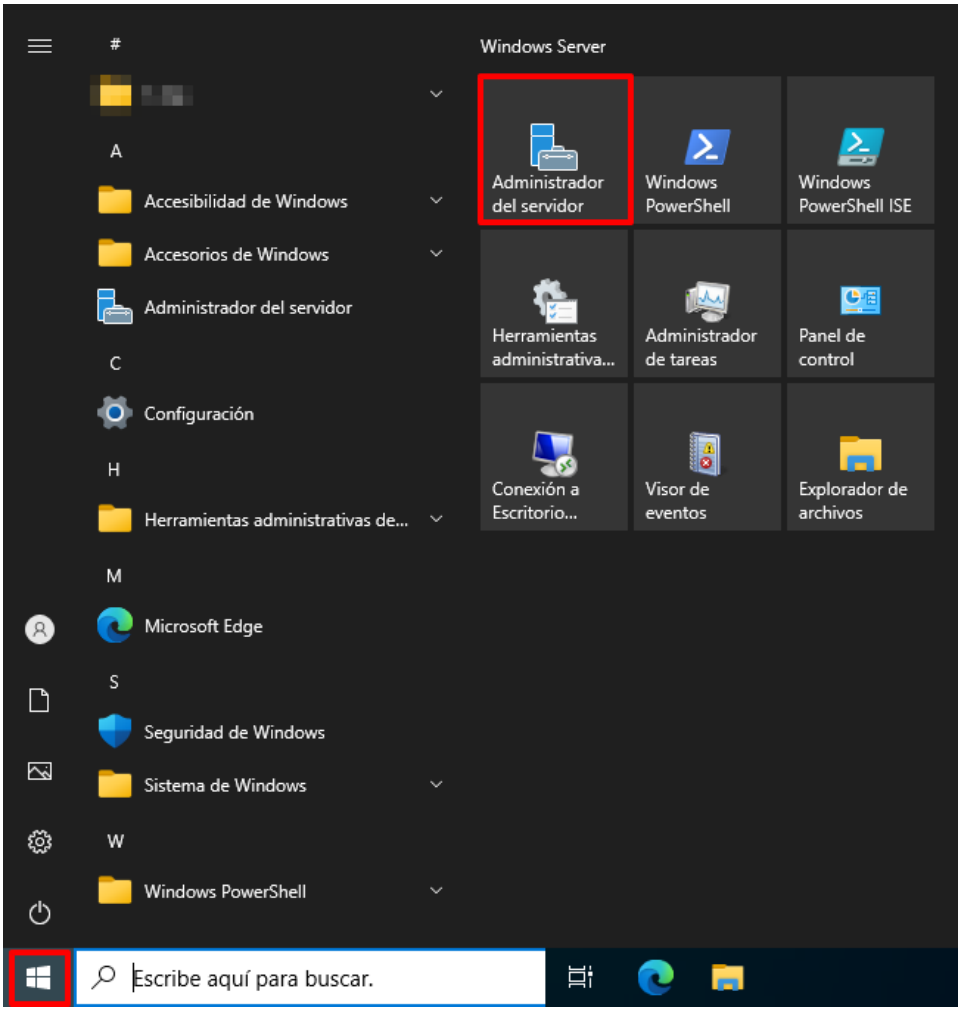
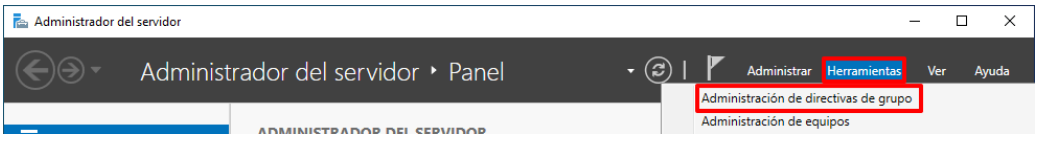
Paso	Descripción
49.	Inicie sesión en el equipo cliente donde pretende eliminar el uso de un dispositivo USB.

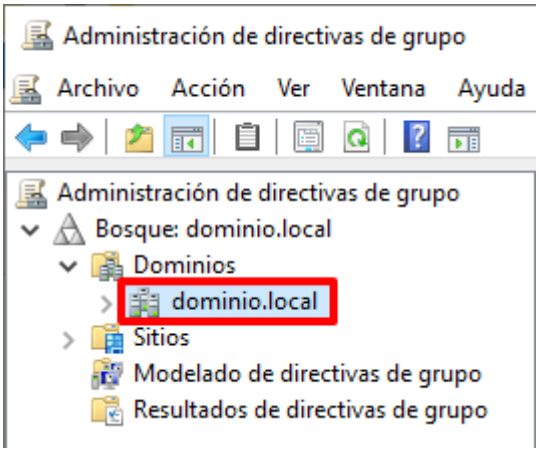
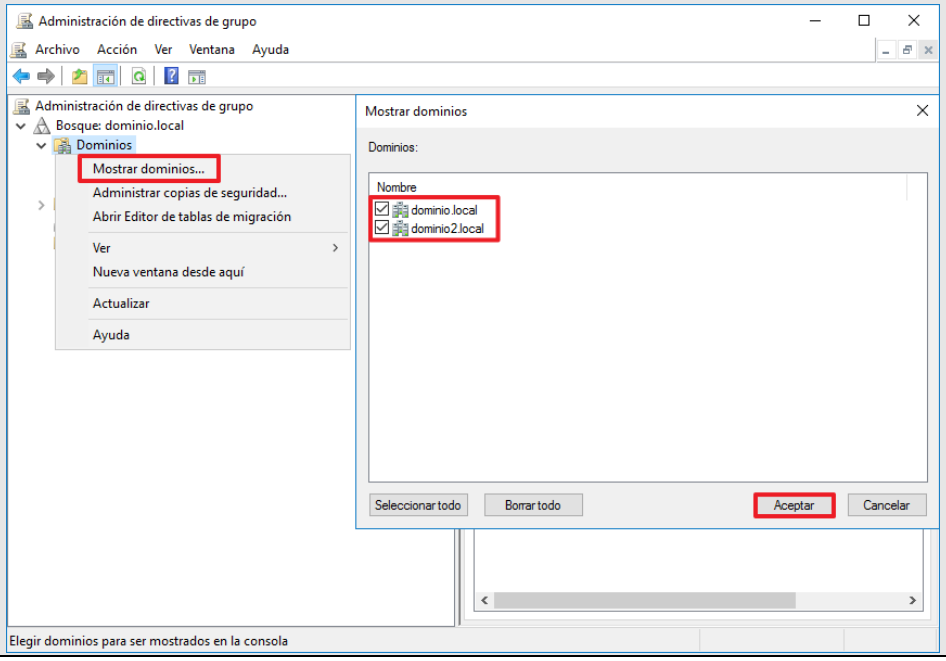
Paso	Descripción
50.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 
51.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

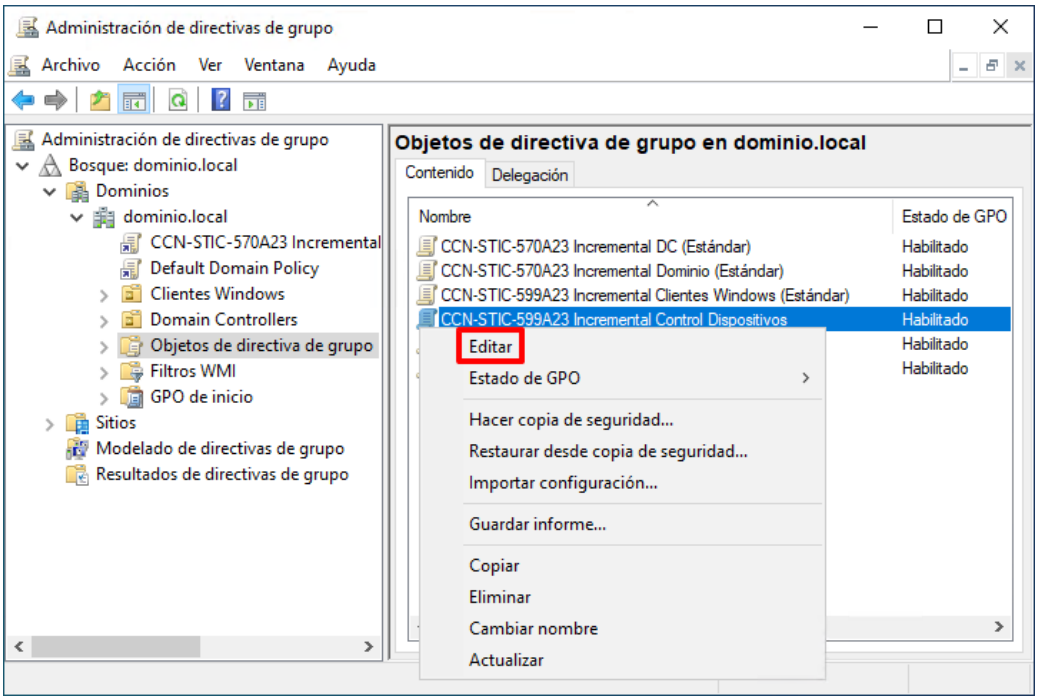
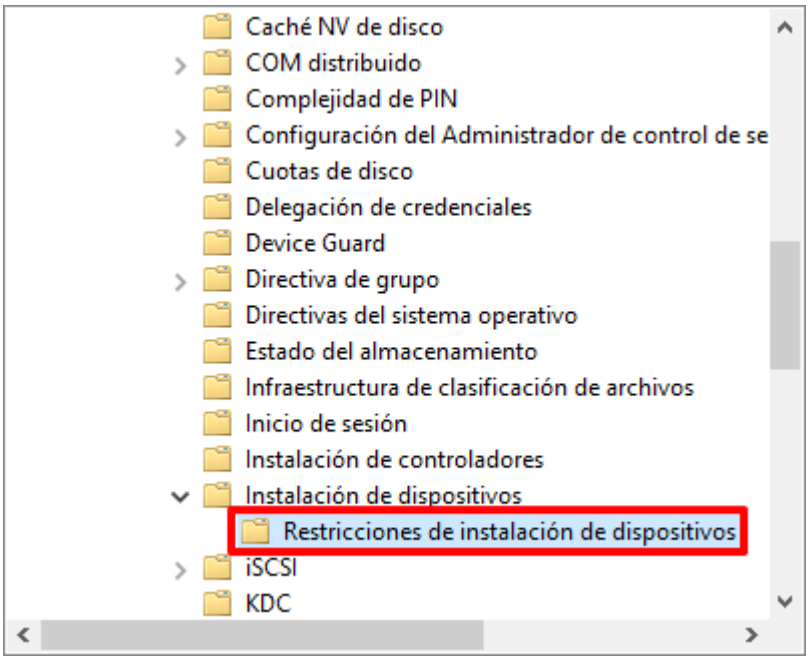
Paso	Descripción
52.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. A continuación, haga clic derecho sobre el mismo y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
53.	Pulse “Desinstalar” ante la advertencia 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.

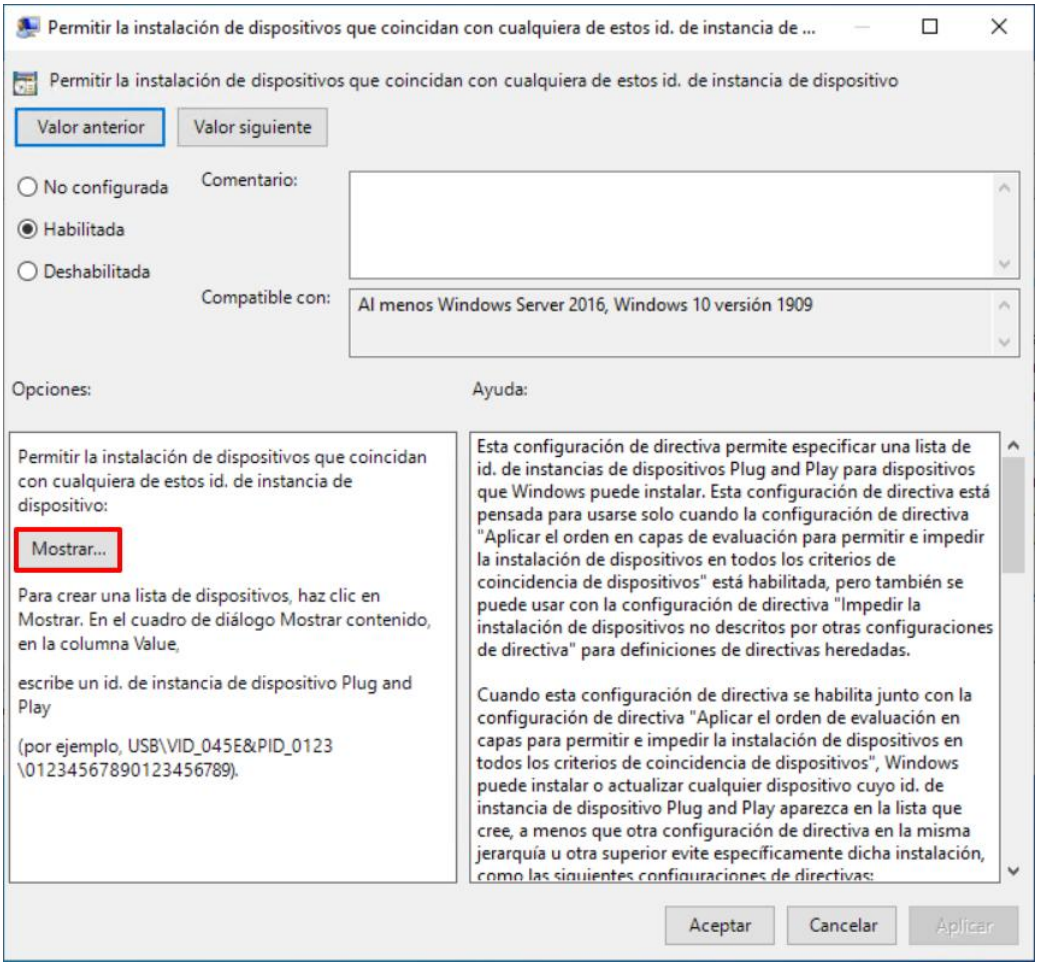
Los siguientes pasos solo serán necesarios en caso de haber hecho uso de la instalación mediante el uso de identificadores únicos de USB.

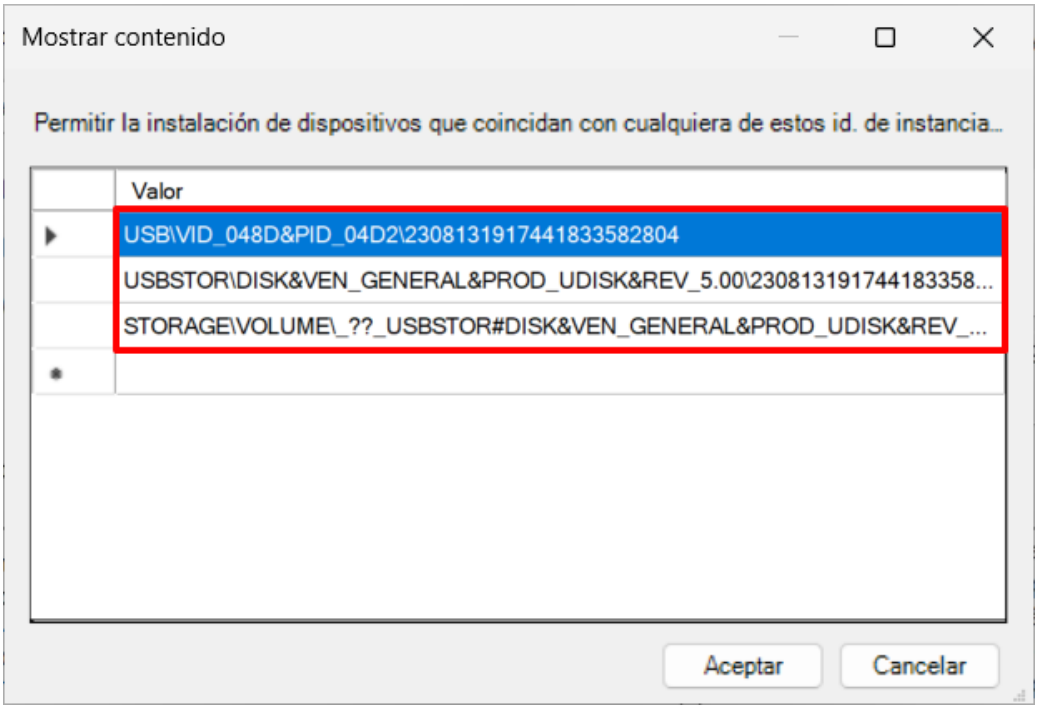
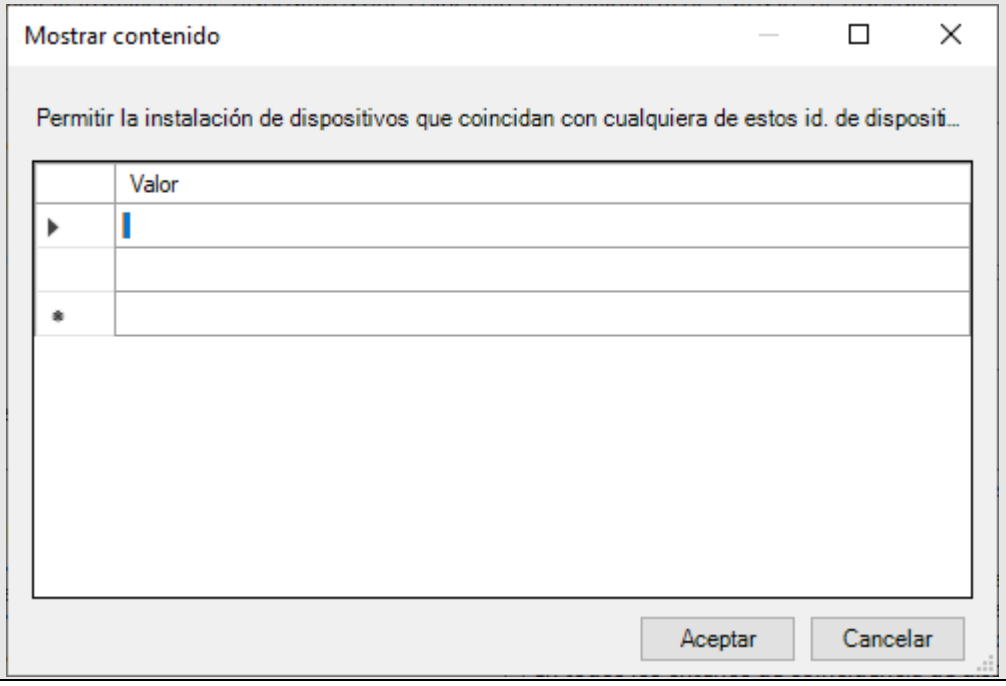
Paso	Descripción
54.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
55.	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”.
56.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 

Paso	Descripción
57.	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
58.	En el apartado “Objetos de directiva de grupo” seleccione con el botón derecho el objeto GPO “CCN-STIC-599A23 Incremental Control Dispositivos” y seleccione la opción del menú contextual “Editar”. 
59.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

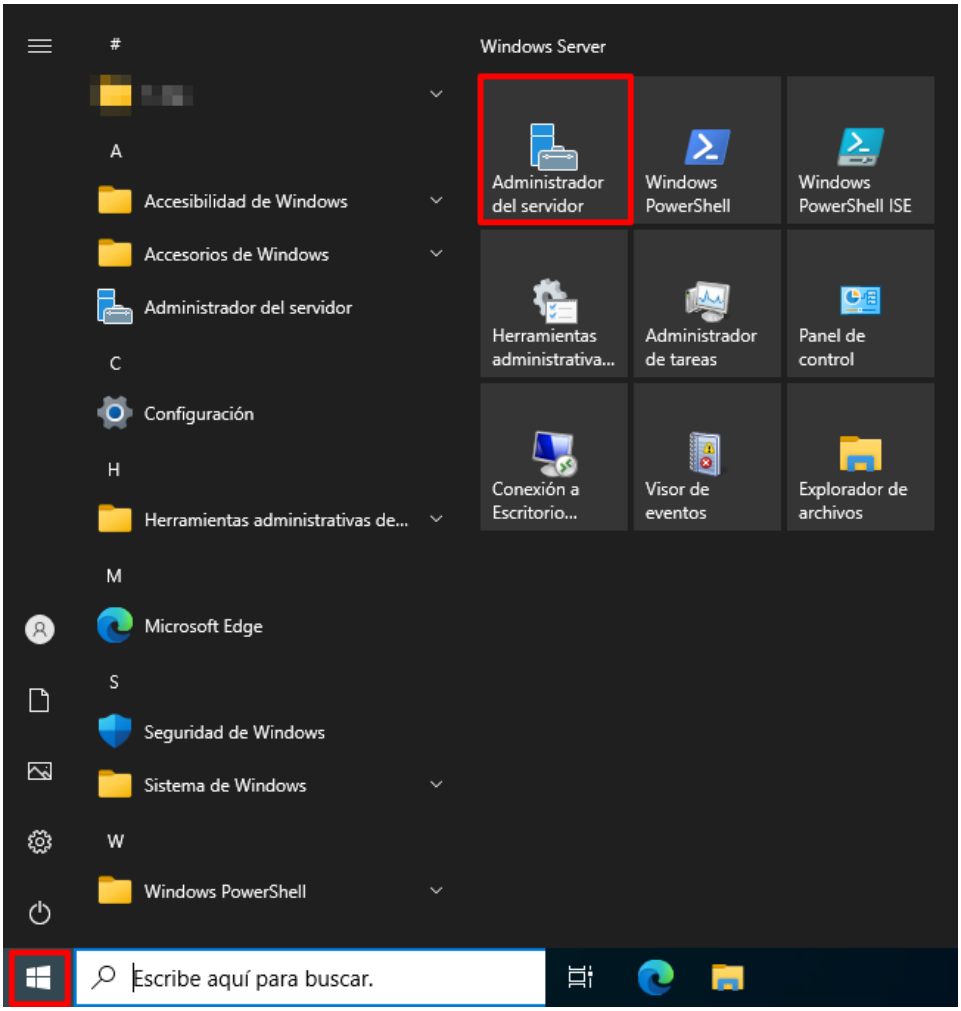
Paso	Descripción
60.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar…”. 

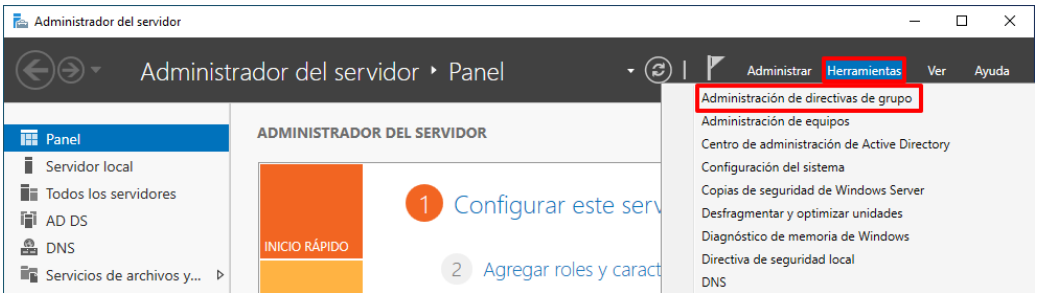
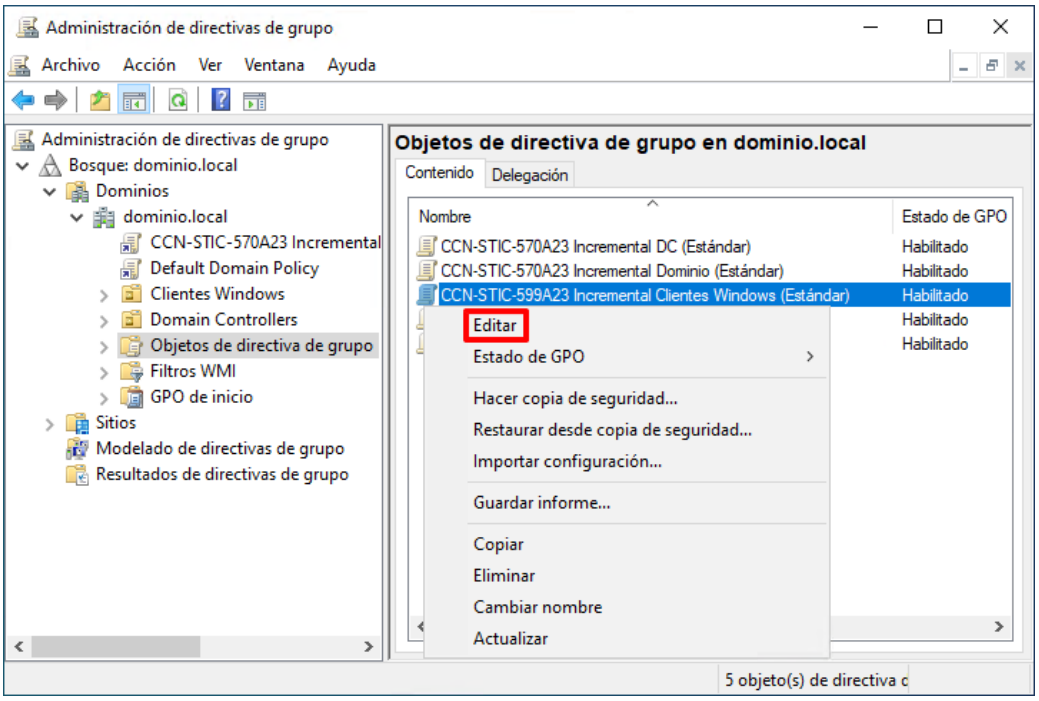
Paso	Descripción
61.	En la ventana emergente “Mostrar contenido” elimine los identificadores correspondientes a los dispositivos sobre los cuales ya no se desea su uso. Pulse “Aceptar” para continuar.  **Nota:** No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto 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. 

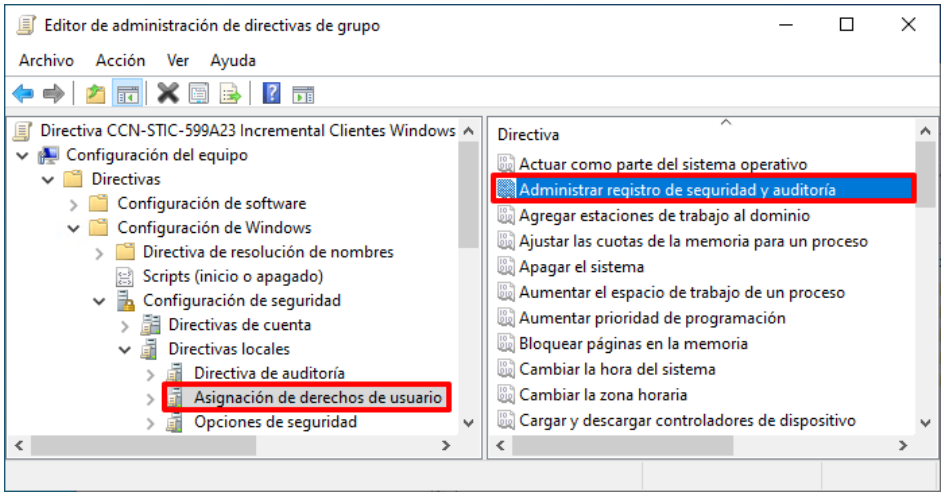
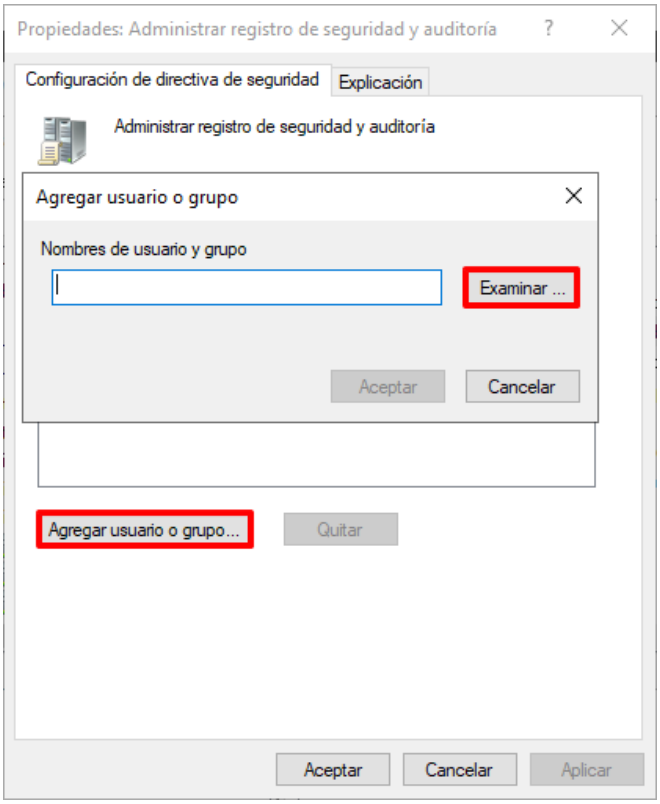
ANEXO A.3.2. SEGREGACIÓN DE FUNCIONES Y TAREAS (PRIVILEGIOS DE AUDITORÍA)

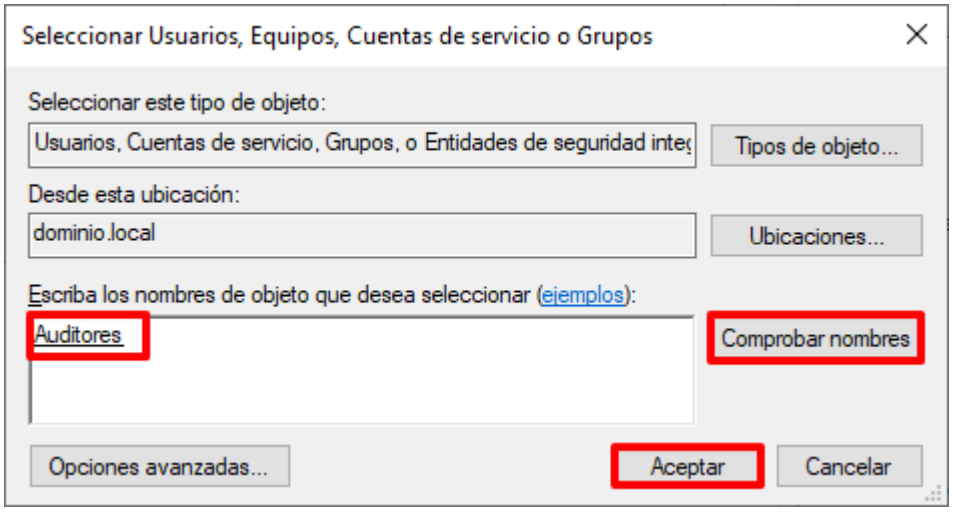
Los siguientes pasos definen las labores para permitir que solo aquellas cuentas deseadas sean capaces de generar auditorías en sistemas operativos Windows Cliente.

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-599A23 Incremental Clientes Windows ([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-599A23 Incremental Clientes Windows ([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”, siguiendo el documento codificado como “CCN-STIC-570A23”. En caso contrario puede ejecutar este script o bien crear el grupo de forma manual.

ANEXO A.3.3. 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 A.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO”. Las configuraciones definidas bajo el presente apartado son las siguientes:

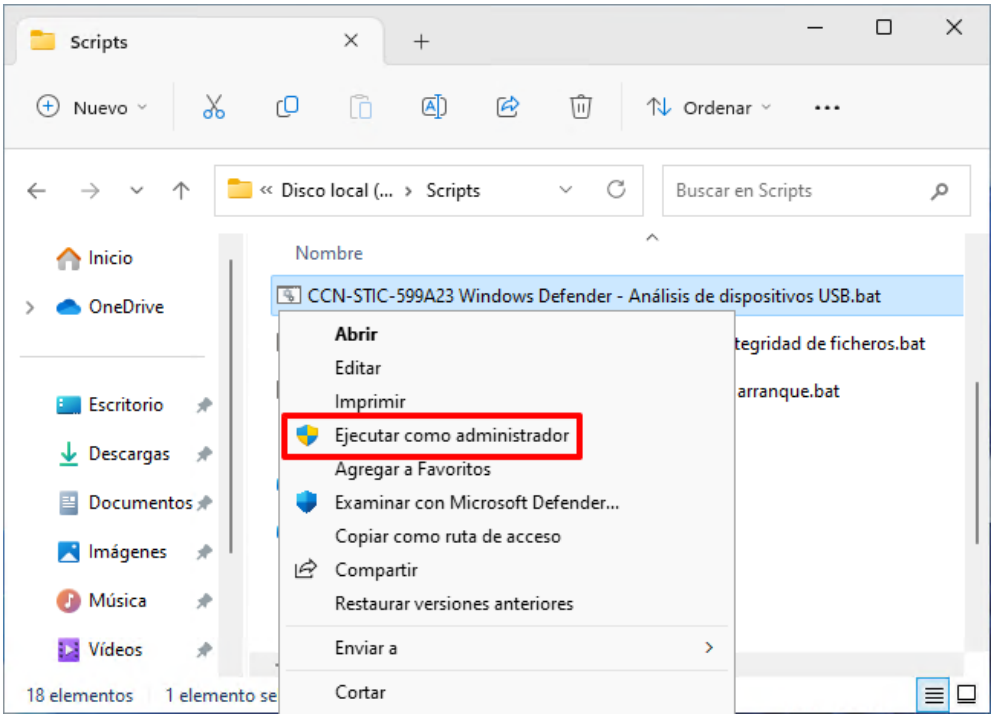
a) Análisis de dispositivos de almacenamiento extraíble cuando estos se conectan al equipo.

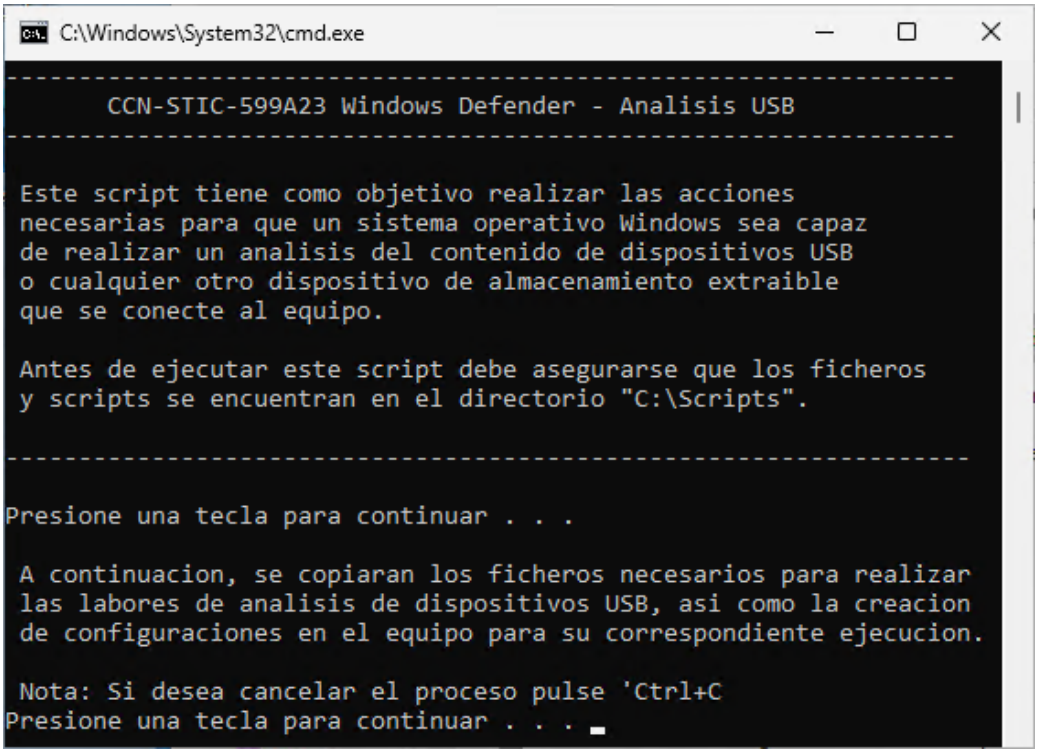
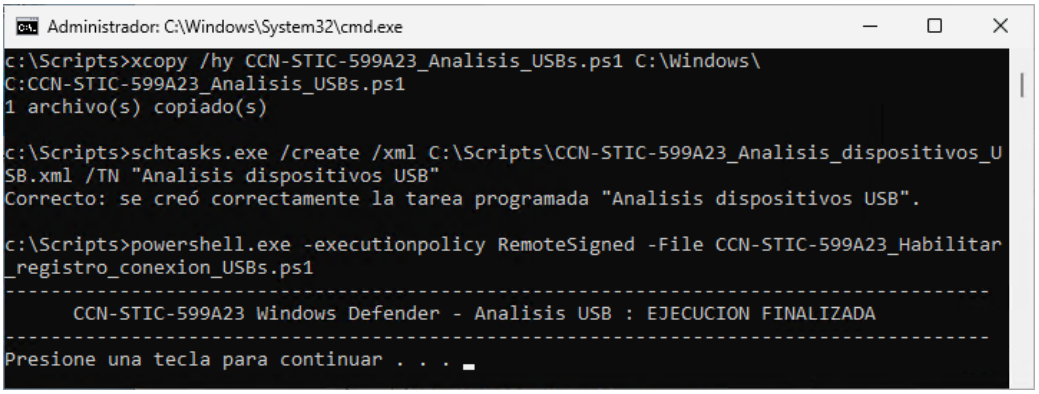
b) Análisis del sistema operativo en el arranque del sistema.

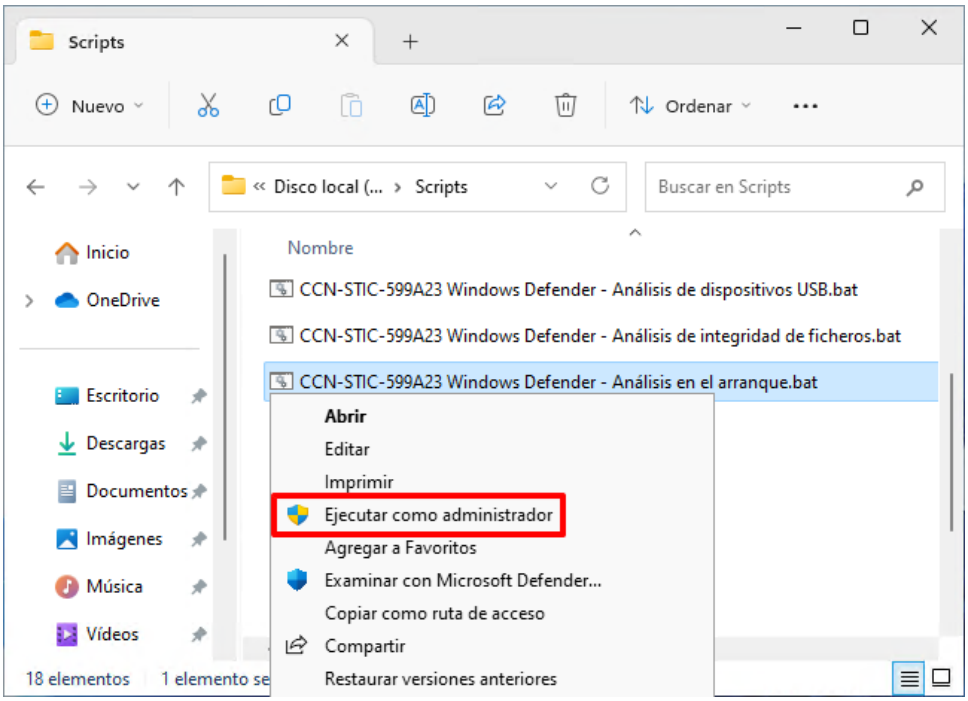
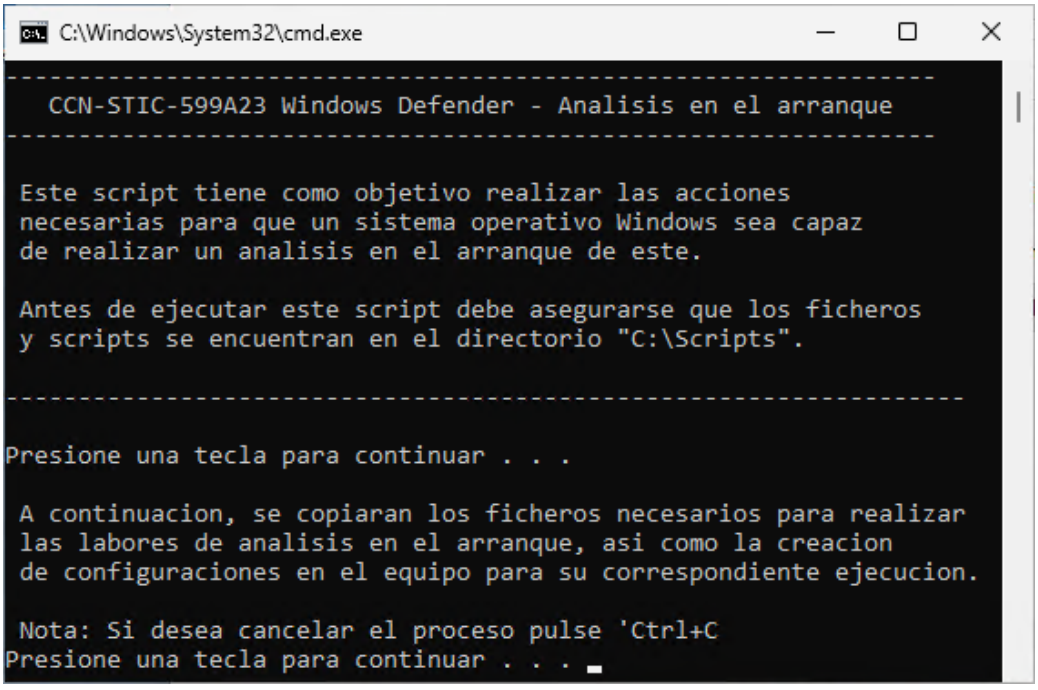
Nota: No se considera de aplicación las configuraciones del presente apartado si no se han aplicado el resto de configuraciones de esta herramienta según el punto indicado con anterioridad.

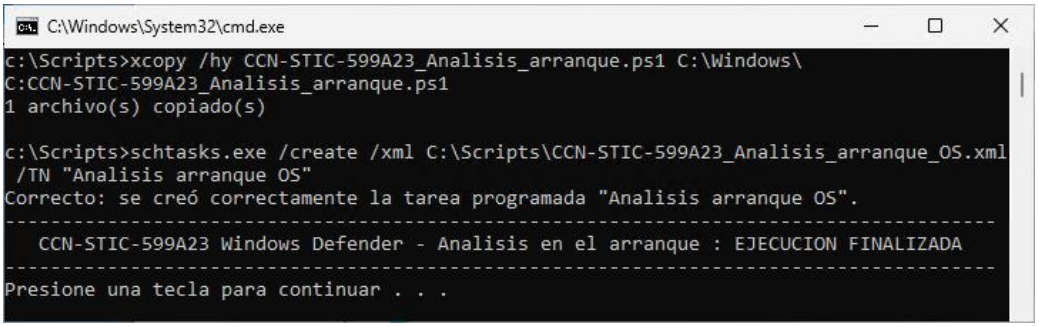
Deberá decidir si implementar toda o parte de la configuración según se expone en el presente paso a paso.

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

Paso	Descripción
1.	Inicie sesión en un cliente miembro 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-599A23 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-599A23 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.

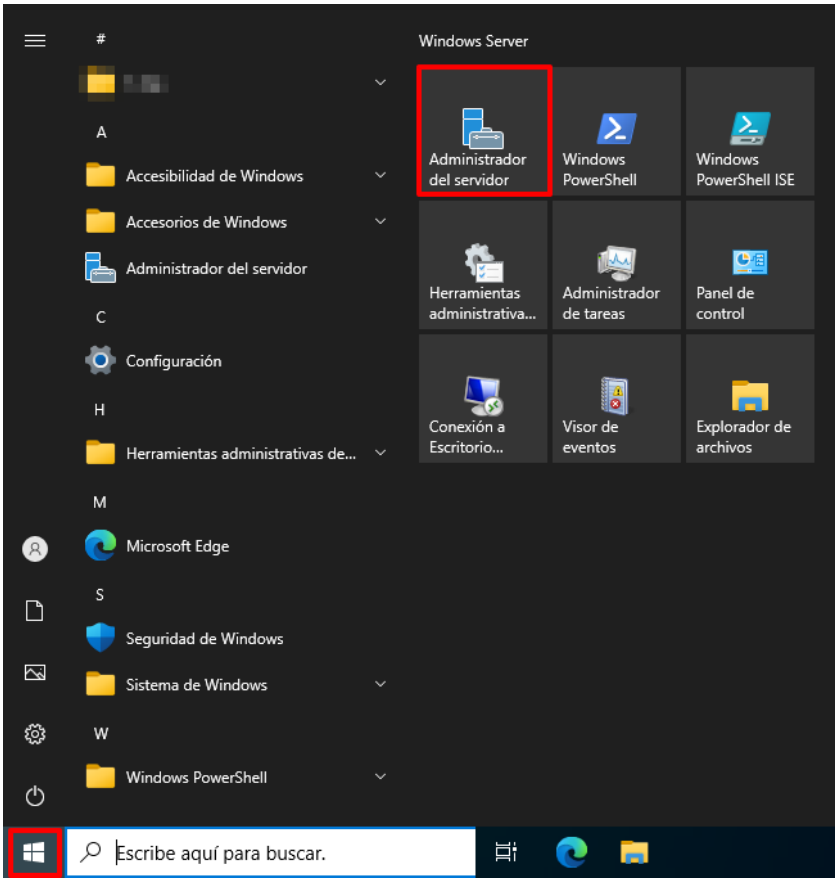
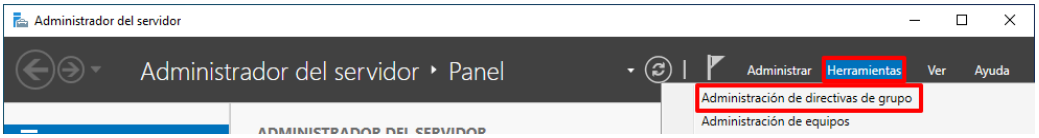
ANEXO A.4. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

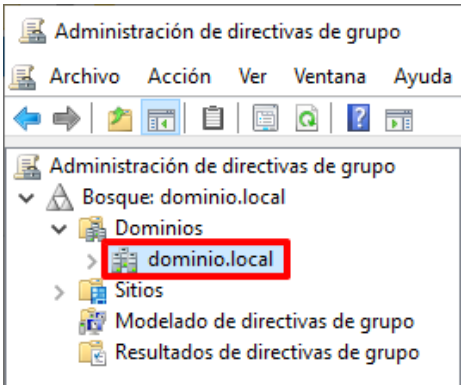
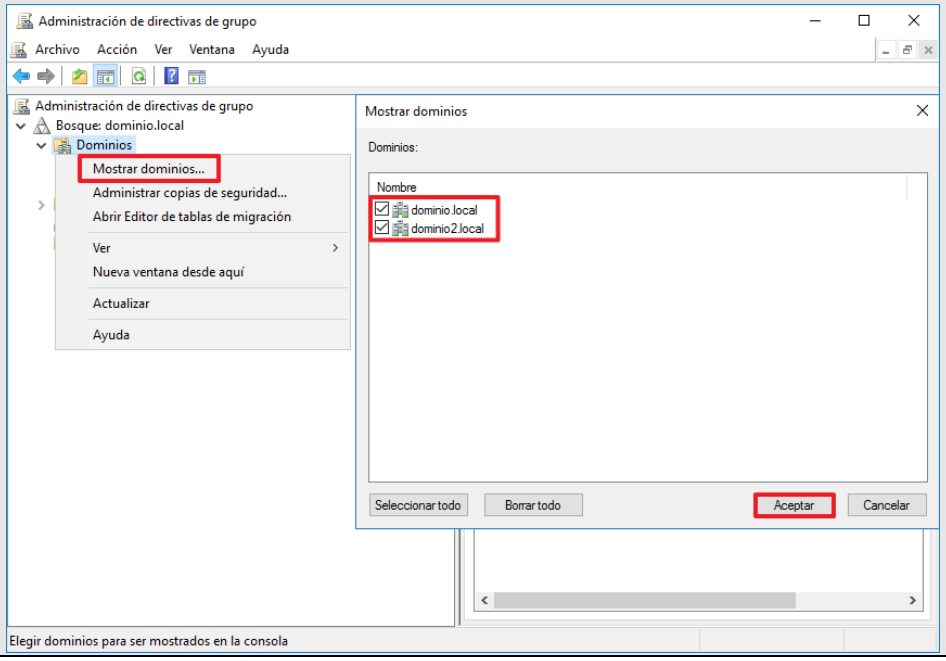
ANEXO A.4.1. INFORMACIÓN DE OBLIGACIONES

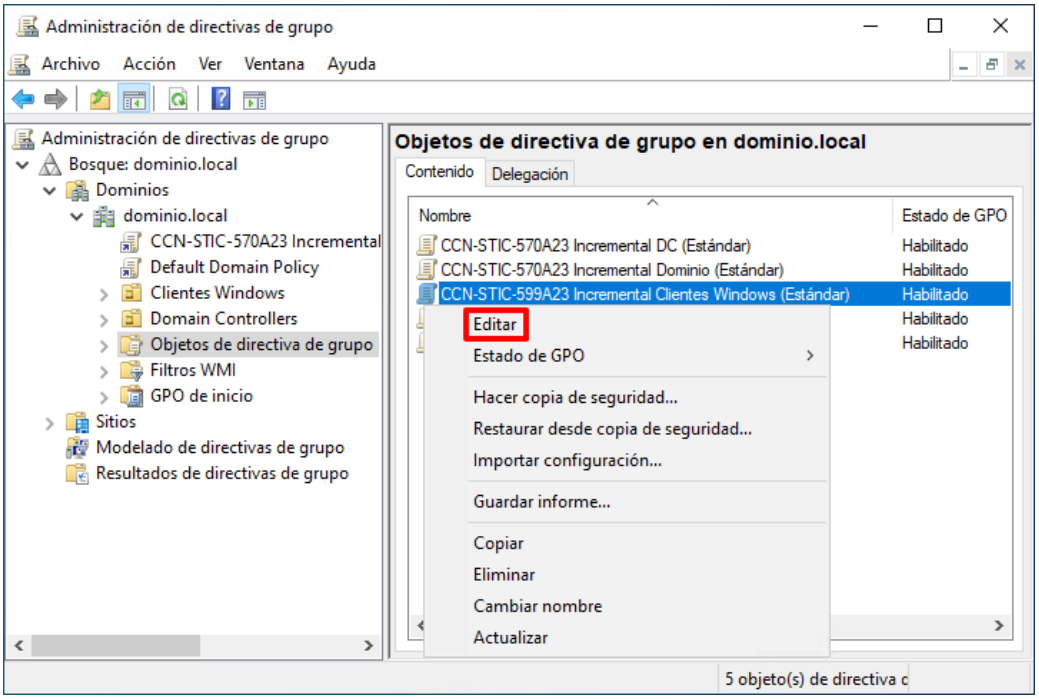
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a los mecanismos de autenticación, es necesario informar al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso al sistema.

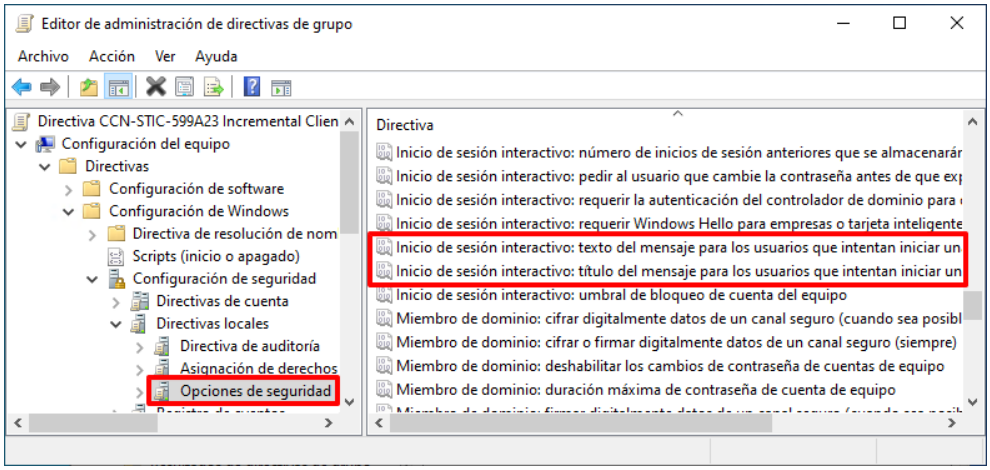
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a modificar y/o adaptar la configuración establecida en los apartados anteriores del presente documento.

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.

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. 
5.	Dentro del nodo "Objetos de directiva de grupo" identifique el siguiente objeto GPO para adecuar los parámetros información sobre derechos y obligaciones de los usuarios de la organización: – CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos parámetros.

Paso	Descripción
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-599A23 Incremental Clientes Windows (Estándar)".
7.	En la ventana del "Editor de administración de directivas de grupo" despliegue el nodo: **"Directiva CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**.

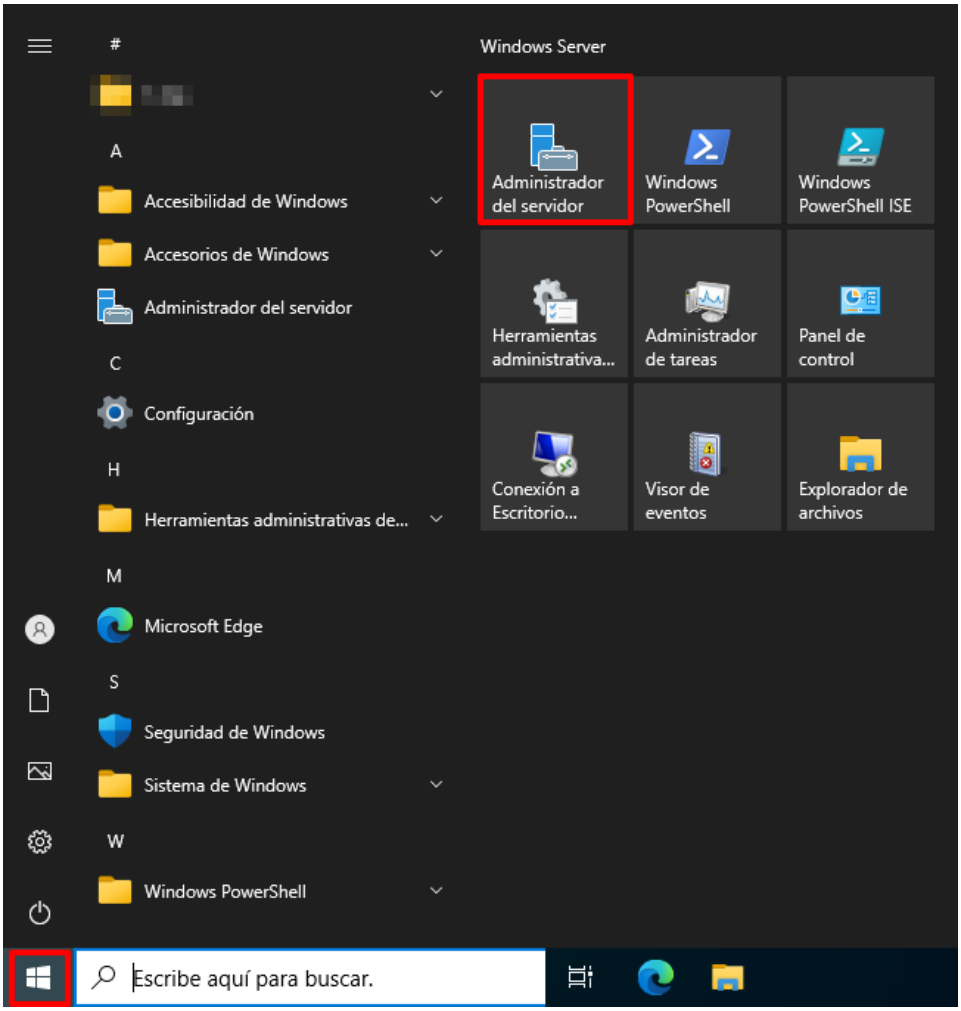
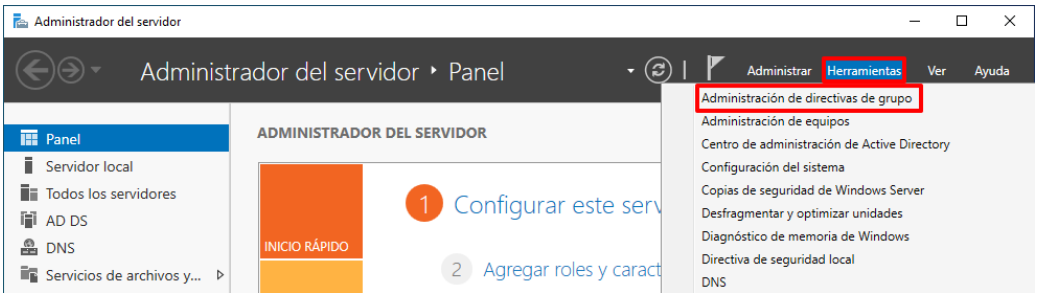
Paso	Descripción
8.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión – Inicio de sesión interactivo: título del mensaje para los usuarios que intentan inicia una sesión 
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.

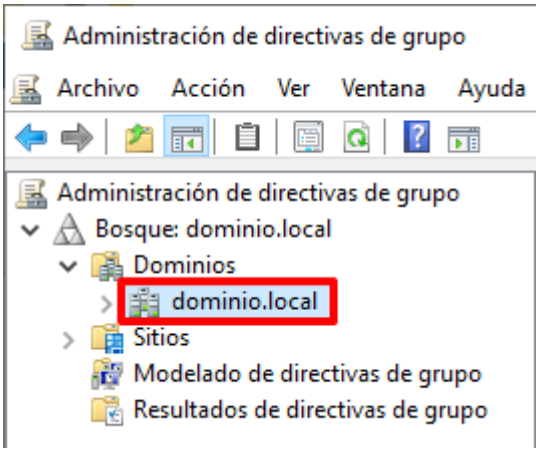
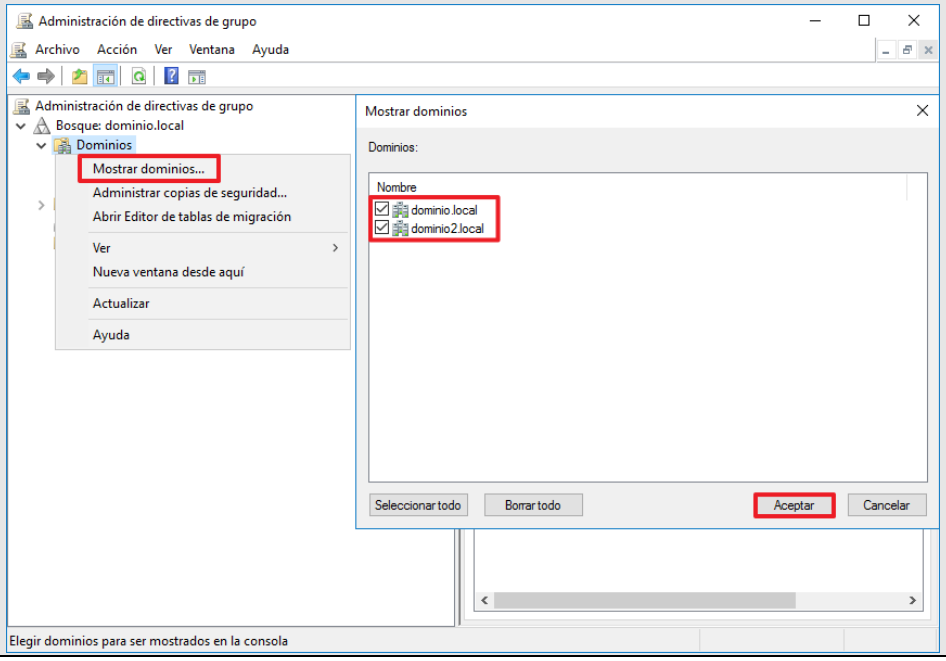
ANEXO A.4.2. RETENCIÓN DE REGISTROS DE ACTIVIDAD

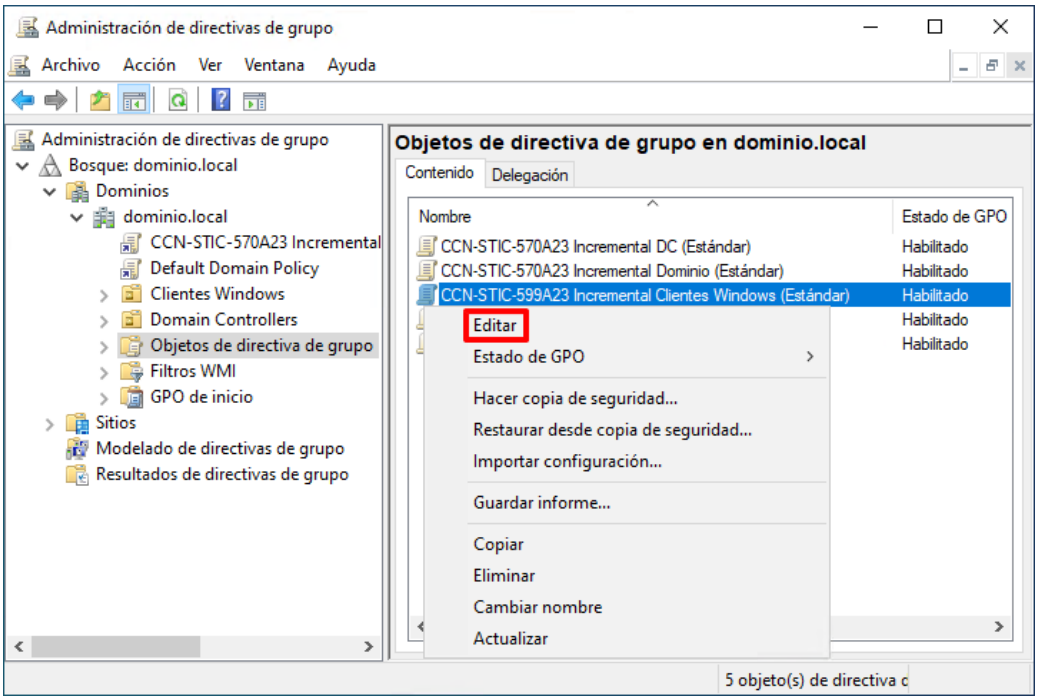
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a los registros de actividad y conforme a lo descrito en su refuerzo número tres (3), es necesario realizar una retención de los eventos auditados antes de que estos sean eliminados.

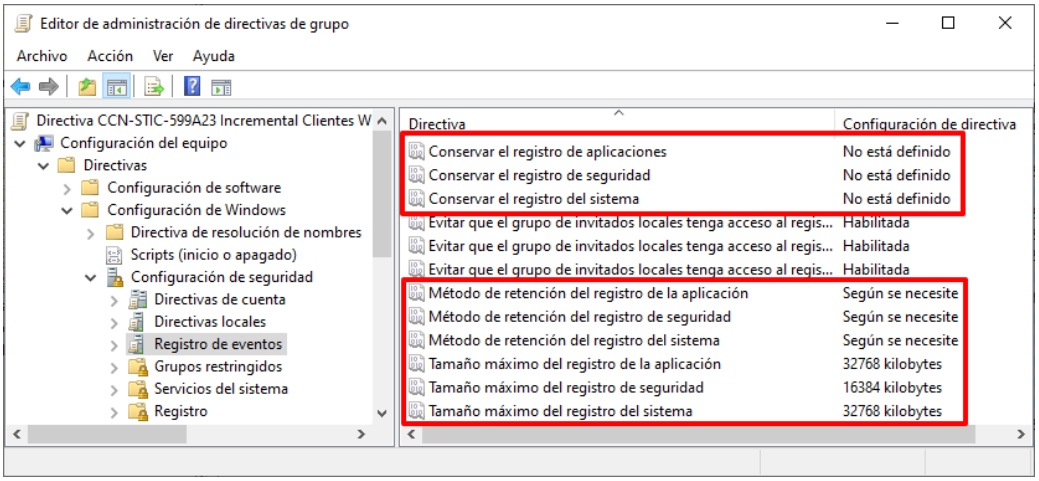
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a modificar y/o adaptar la configuración establecida en los apartados anteriores del presente documento.

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. 

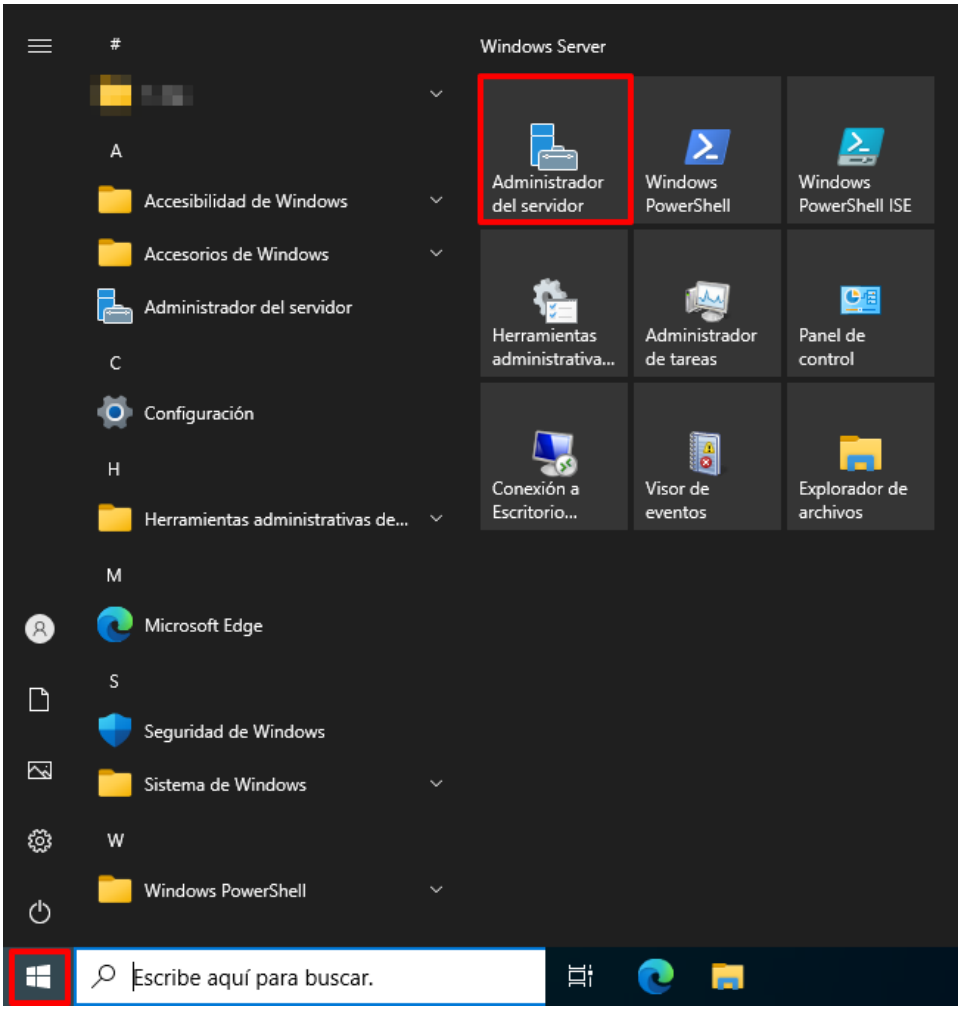
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de retención: – CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos 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-599A23 Incremental Clientes Windows (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”**.

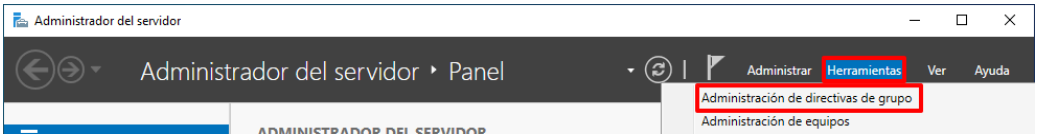
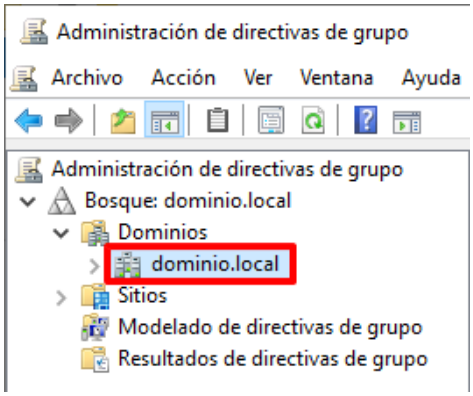
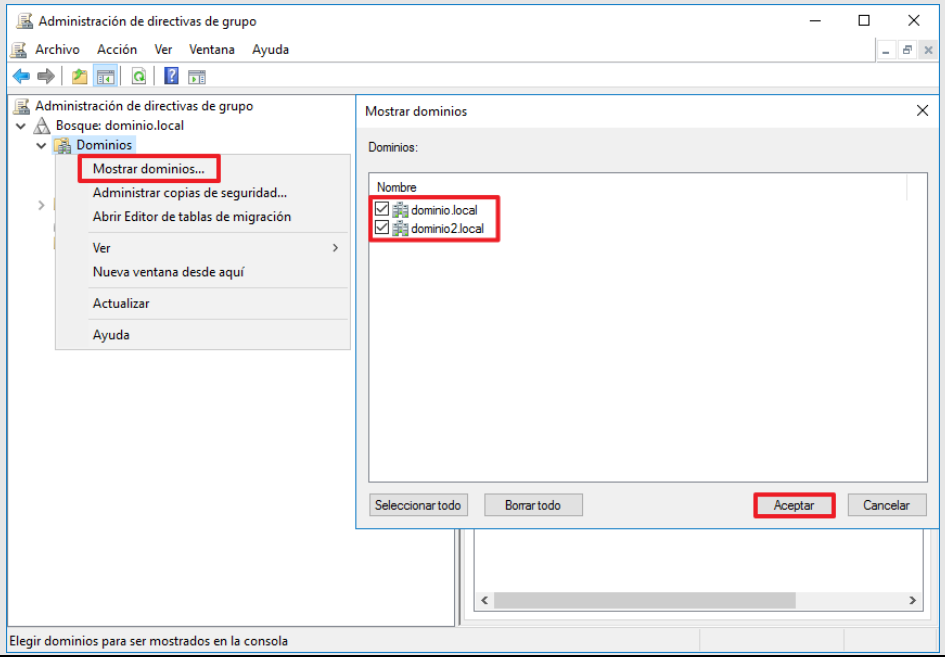
Paso	Descripción
8.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Conservar el registro de aplicaciones – Conservar el registro de seguridad – Conservar el registro del sistema – Método de retención del registro de la aplicación – Método de retención del registro 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 no asegura que se conserven todos los eventos, siendo necesario realizar una rotación manual de los registros para evitar la pérdida de los mismos. En el caso de que se requiera establecer una conservación de los registros por días, pudiendo configurar como máximo un (1) año, 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 a la retención de los registros debido a la sobreescritura de los eventos. **Nota:** Si no se dimensiona de forma correcta el tamaño de los registros, pueden darse errores debido al llenado de los mismos, como el bloqueo de inicio de sesión por parte de los usuarios sin privilegios. Por ello, es necesario comprobar previamente el funcionamiento de las directivas a implementar, para no realizar un bloqueo a los usuarios en sus puestos de trabajo.

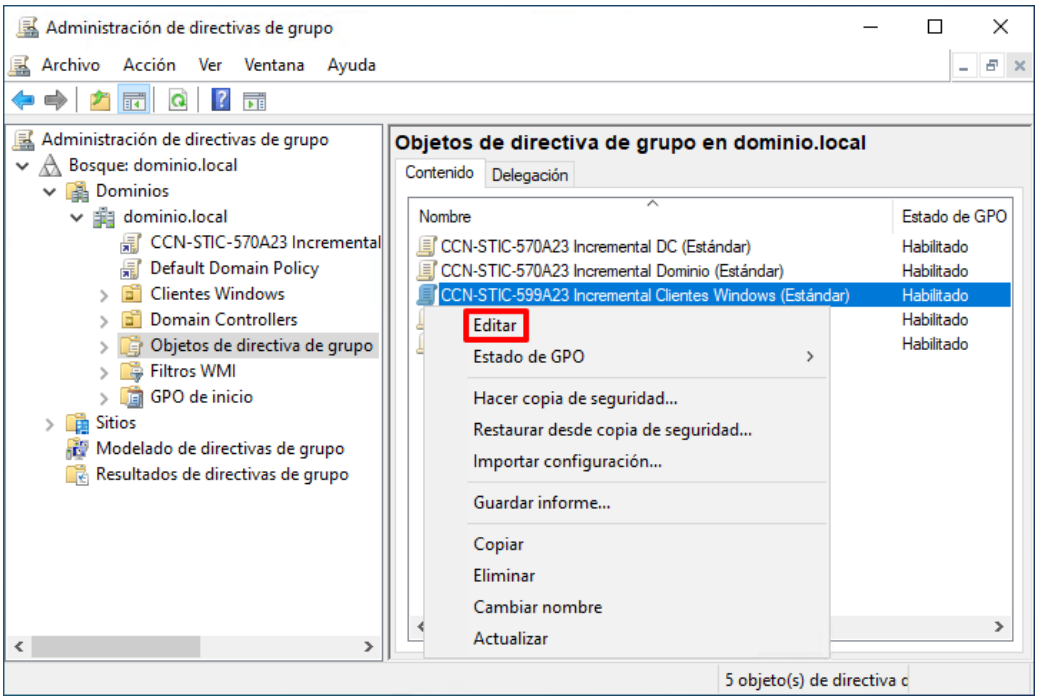
ANEXO A.4.3. PRIVILEGIOS

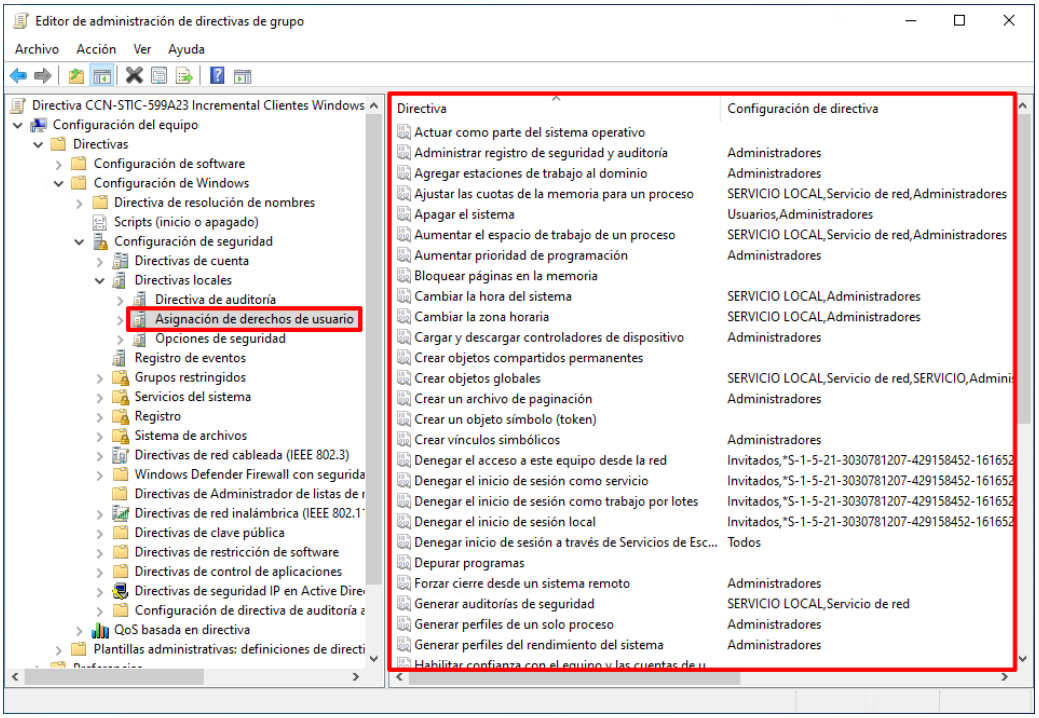
Dados los requisitos del ENS, tal y como se expone en la medida dedicada a la identificación y el acceso a los sistemas de información, es necesario establecer los privilegios adecuados en función de las necesidades.

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. 

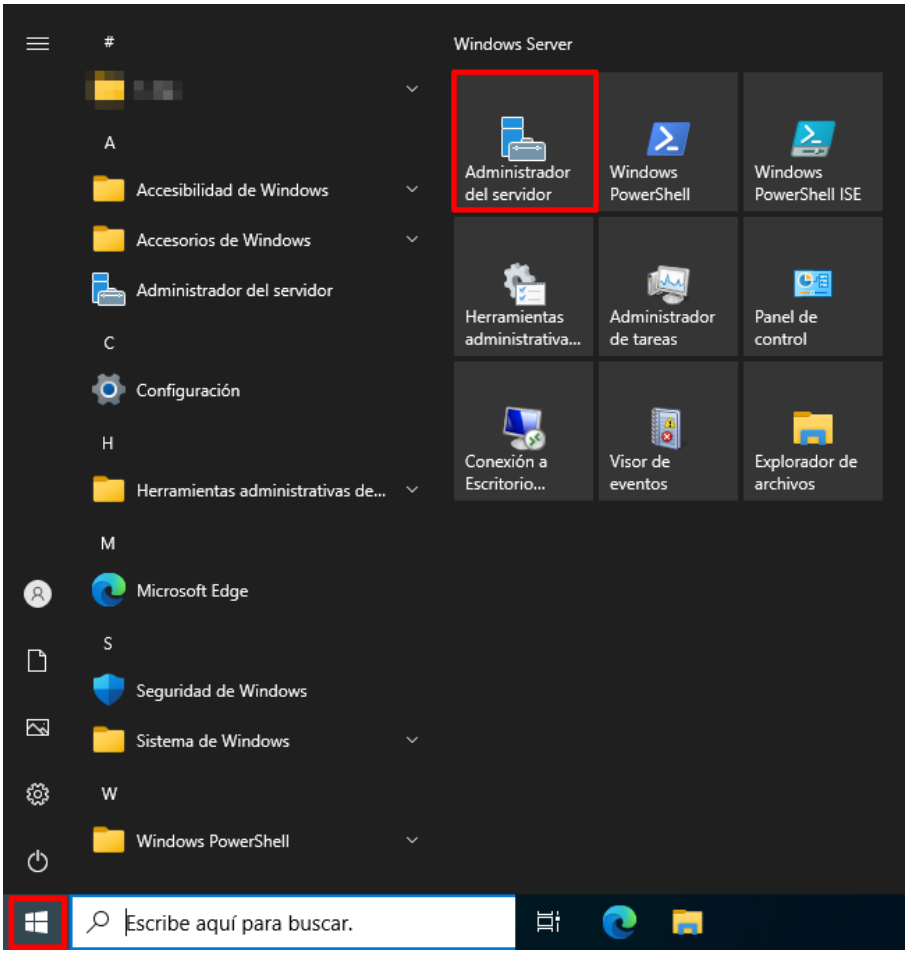
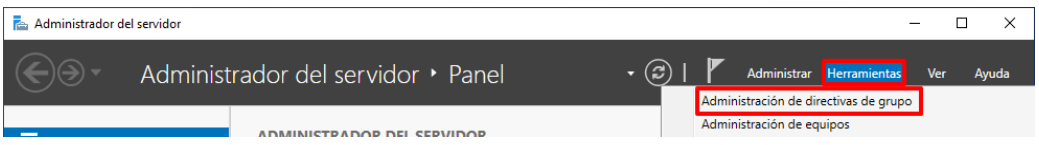
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de privilegios: – CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte estos 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-599A23 Incremental Clientes Windows (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”**.

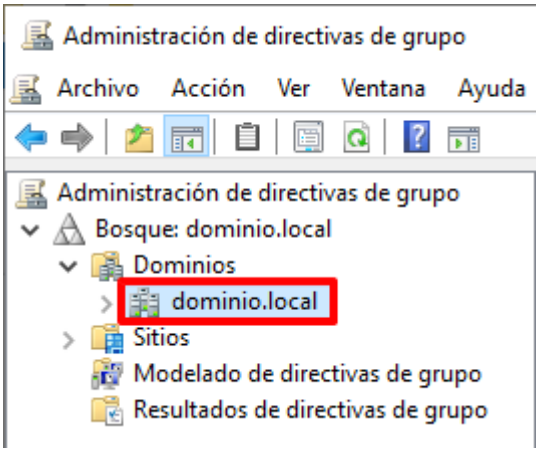
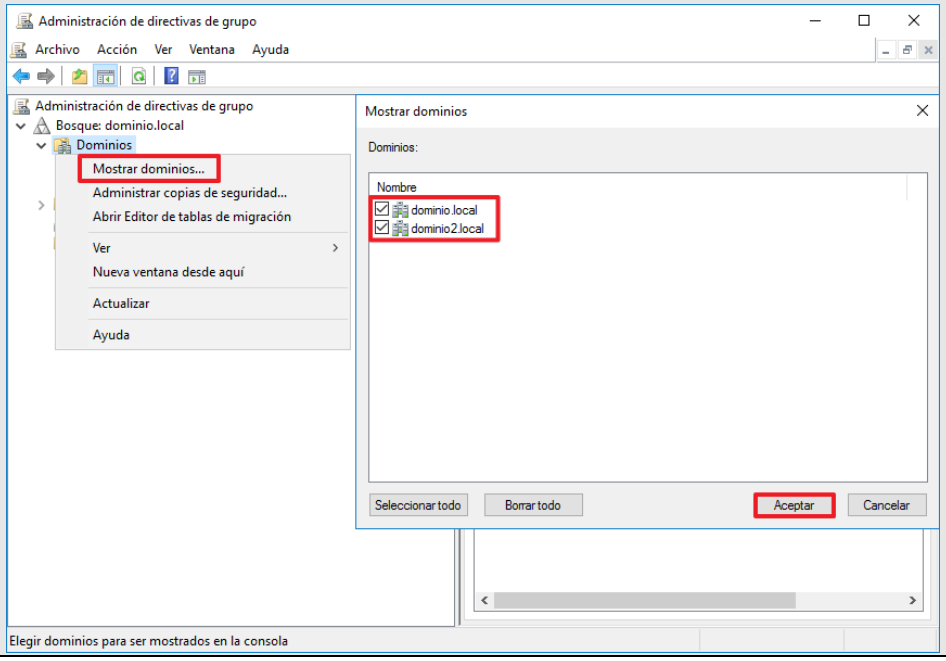
Paso	Descripción
8.	En el panel derecho evalúe todas las directivas de privilegios y edítelas a continuación. Tenga especial consideración con las siguientes directivas orientadas a los tipos de inicio de sesión, sobre todo cuando se realicen procesos automatizados en los sistemas de información o en los clientes 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  **Nota:** La configuración establecida trata de restringir todo lo posible los privilegios de los usuarios, pero manteniendo la usabilidad dentro de los sistemas.

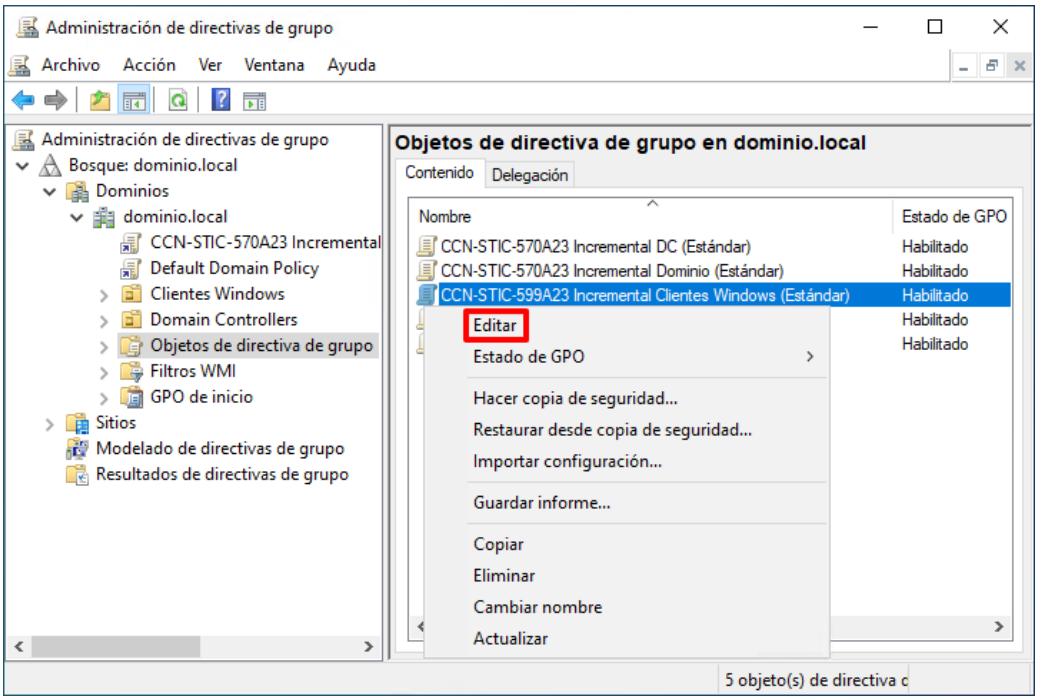
ANEXO A.4.4. BLOQUEO DE SESIÓN ANTE INACTIVIDAD

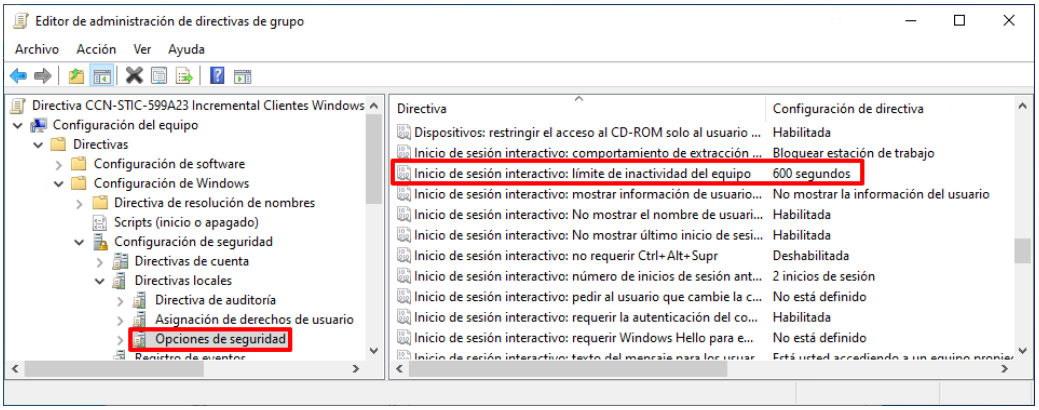
Dados los requisitos del ENS, tal y como se expone en la medida dedicada al bloqueo de puesto de trabajo, es necesario que este quede bloqueado pasado un tiempo prudencial de modo que requiera una nueva autenticación del usuario para el uso del mismo.

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. 

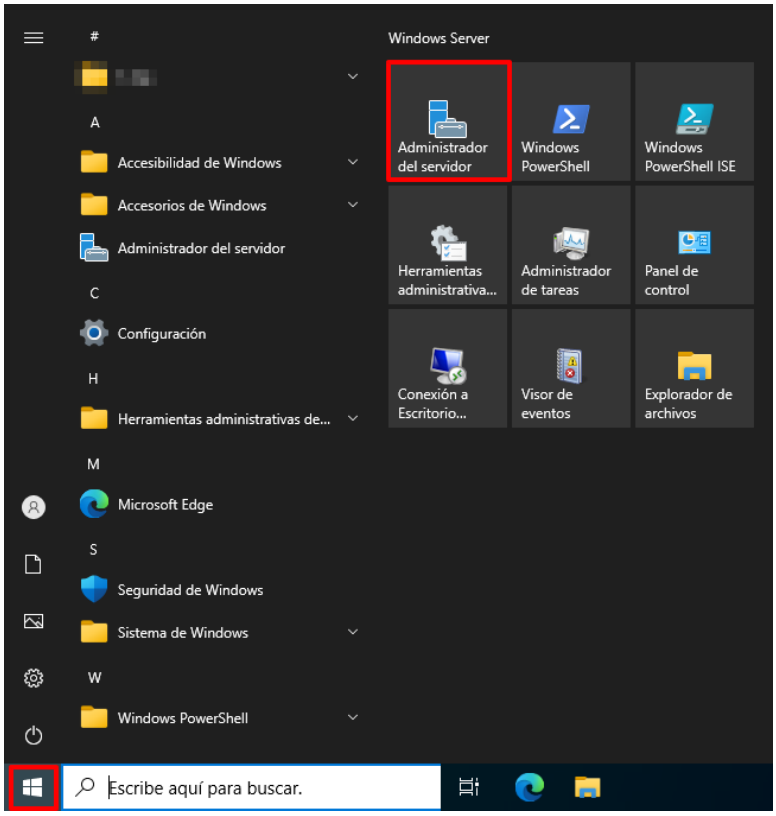
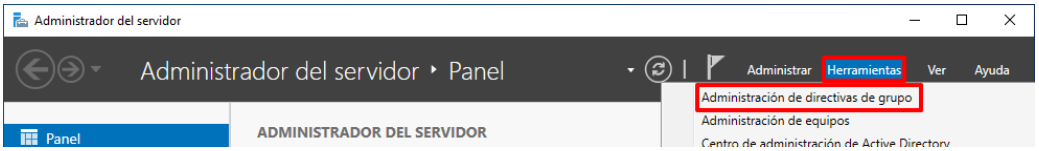
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de bloqueo de puesto de trabajo: – CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique 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-599A23 Incremental Clientes Windows (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.

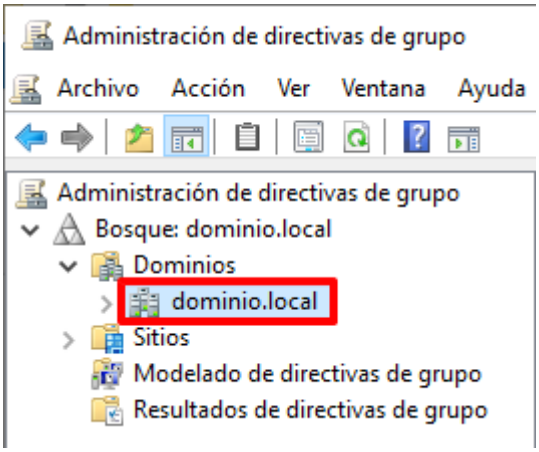
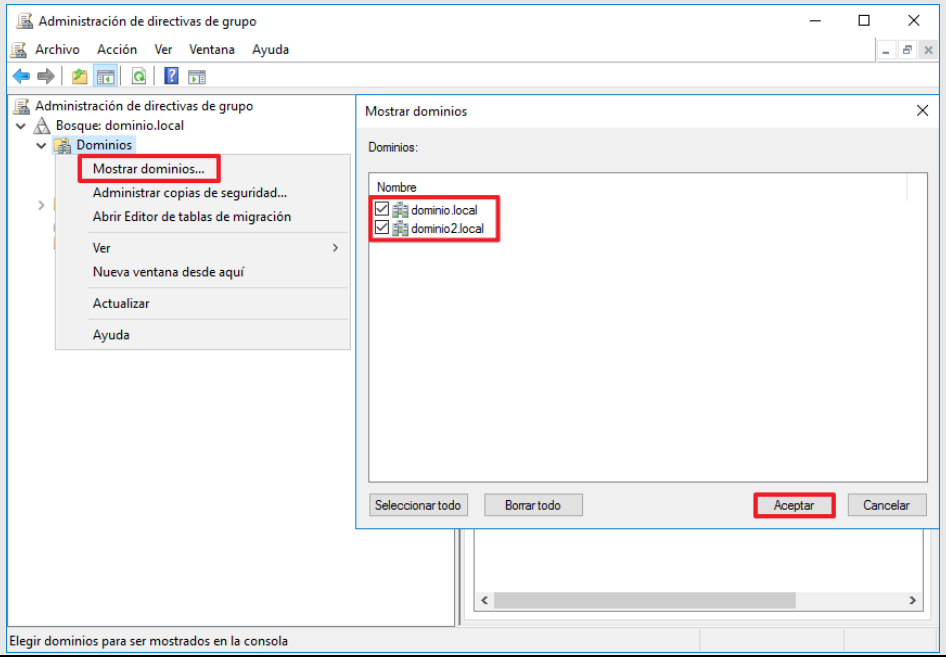
Paso	Descripción
8.	En el panel derecho identifique la siguiente directiva y edítela a continuación: – Inicio de sesión interactivo: límite de inactividad del equipo  **Nota:** La configuración establecida expone un tiempo prudencial el cual puede ser adaptado en función de la política de la organización.

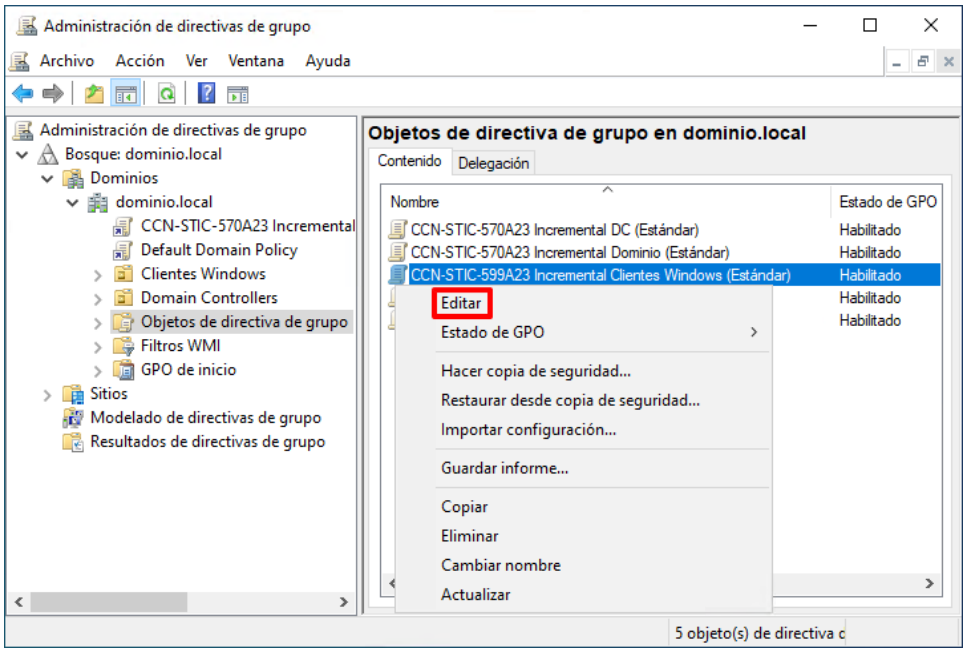
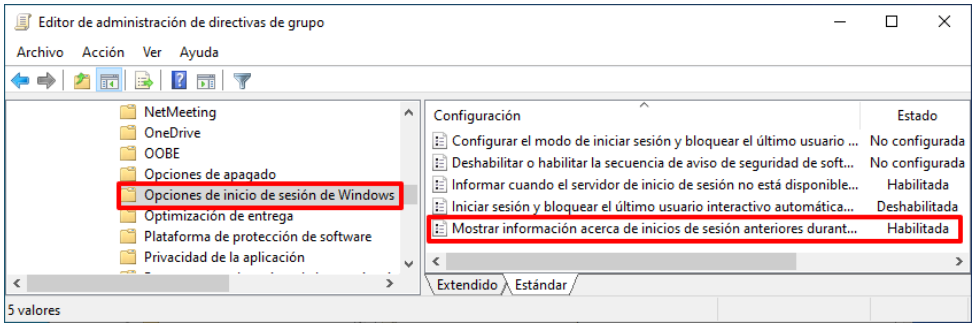
ANEXO A.4.5. MOSTRAR INICIOS DE SESIÓN ANTERIORES

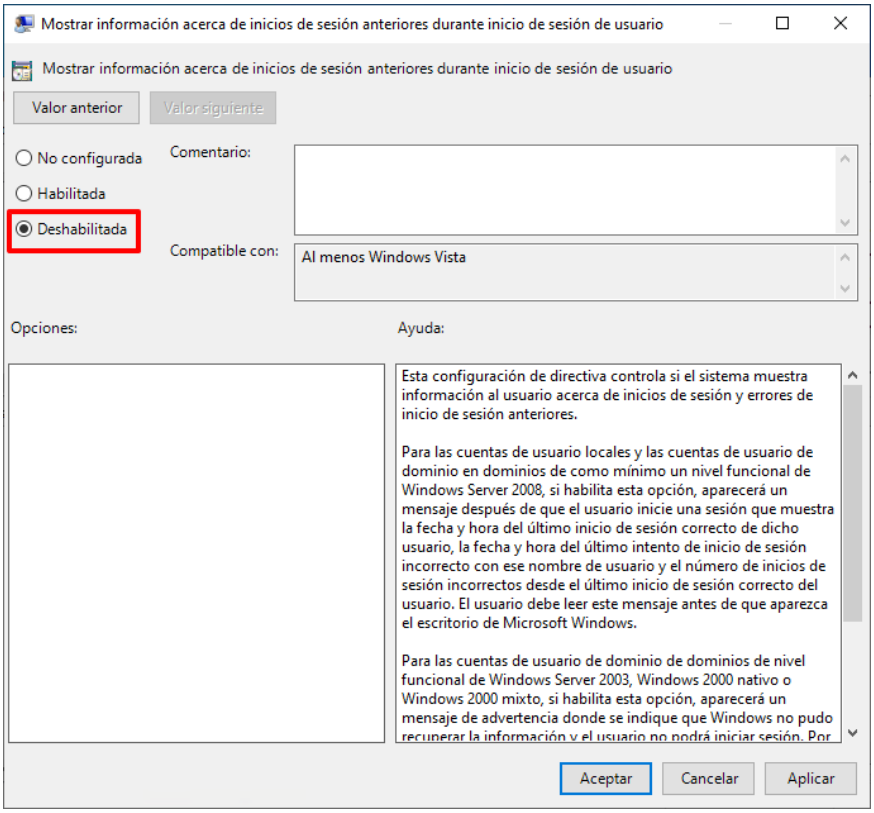
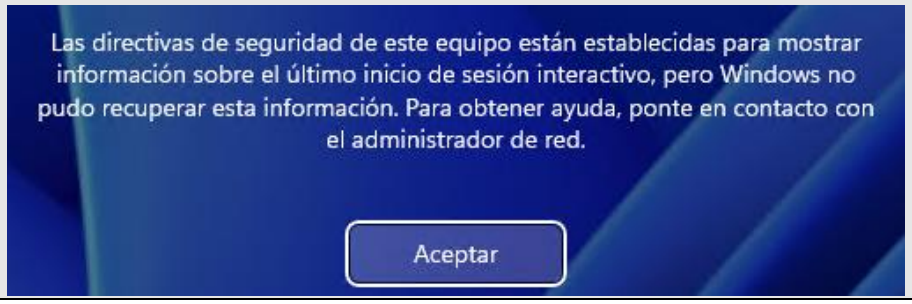
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a adaptar la configuración establecida sobre los equipos de tipo Clientes Miembro, modificando la directiva de inicio de sesión que mal configurada impide el inicio de los usuarios en los equipos cliente del sistema.

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 el siguiente objeto GPO para adecuar los parámetros de opciones de seguridad: – CCN-STIC-599A23 Incremental Clientes Windows ([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-599A23 Incremental Clientes Windows (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”**.
8.	En el panel derecho identifique la directiva “Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario”. 

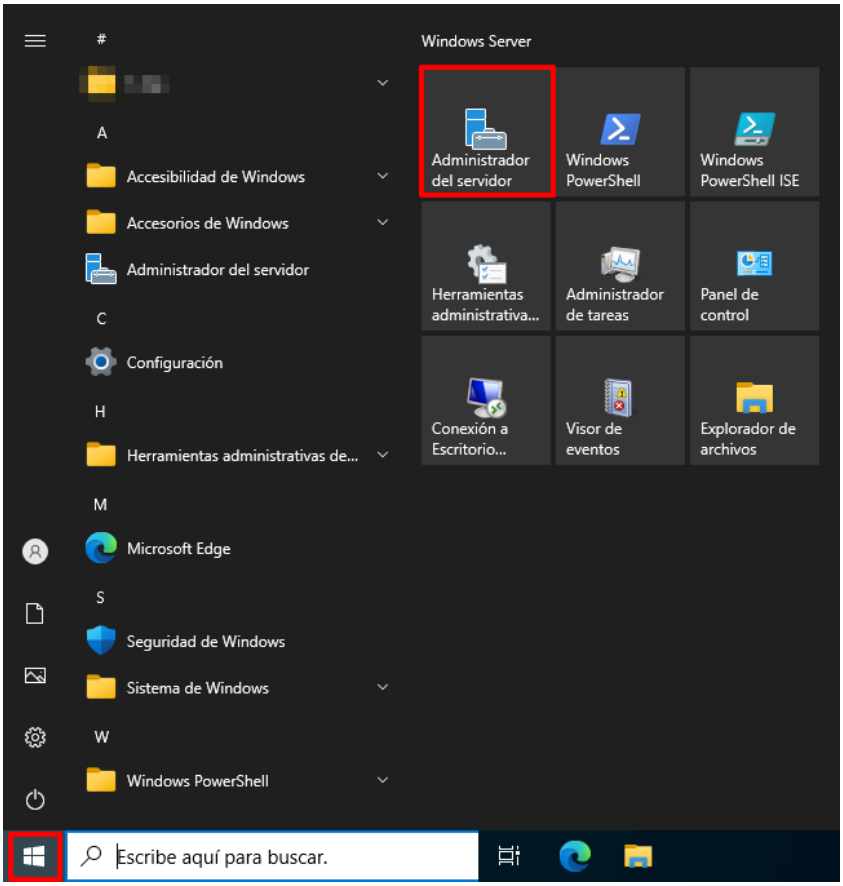
Paso	Descripción
9.	Cuando la presente directiva se encuentra configurada de forma desigual en los equipos de tipo Controlador de Dominio y los Clientes Miembro, puede generar errores en el inicio de sesión a los usuarios en los equipos cliente. Para evitar este tipo de comportamiento, deberá habilitar la directiva indicada en todos los Controladores de Dominio del sistema. Si por necesidades de la organización es necesario mantener la directiva deshabilitada en los Controladores de Dominio, edite la directiva indicada en el paso anterior y establezca su configuración en “Deshabilitada”, aplicando así a los equipos cliente.  **Nota:** Tenga en consideración que al configurar de forma desigual la presente directiva, tal como se ha indicado en el anterior ejemplo, el usuario observará el siguiente error. 

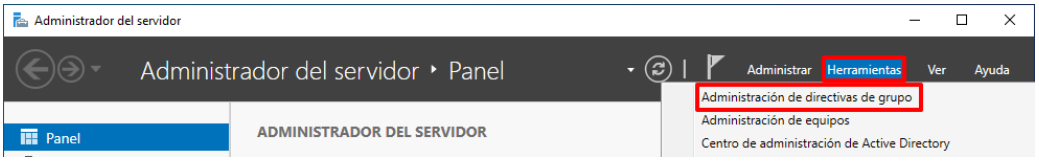
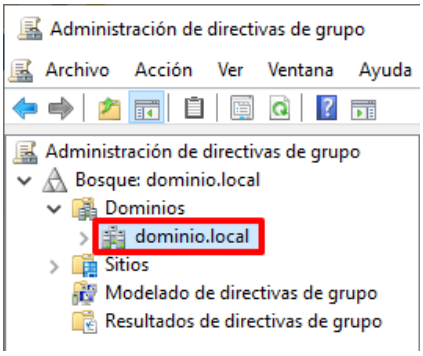
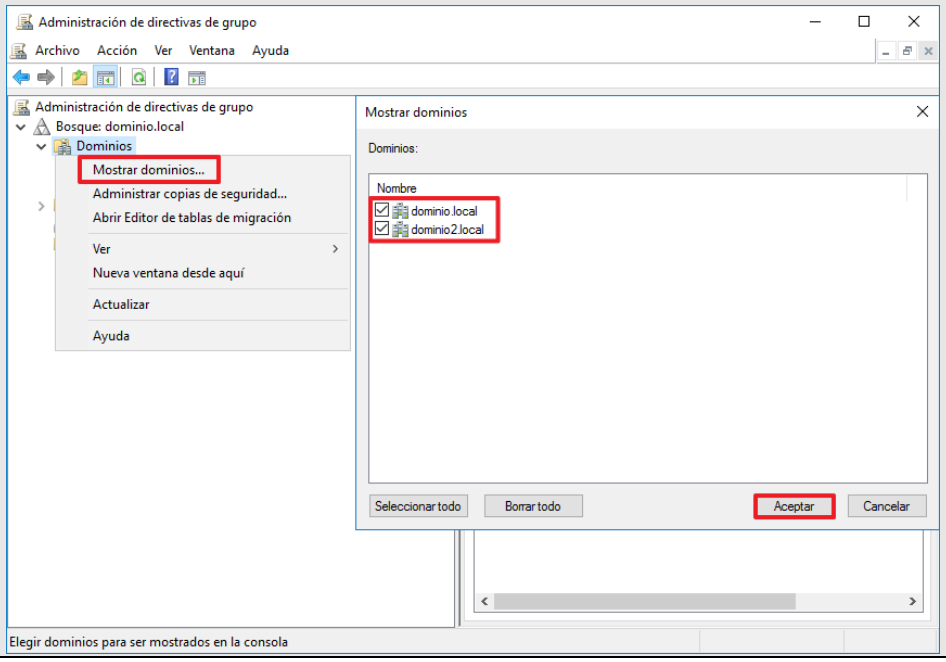
ANEXO A.4.6. OPCIONES DE SEGURIDAD

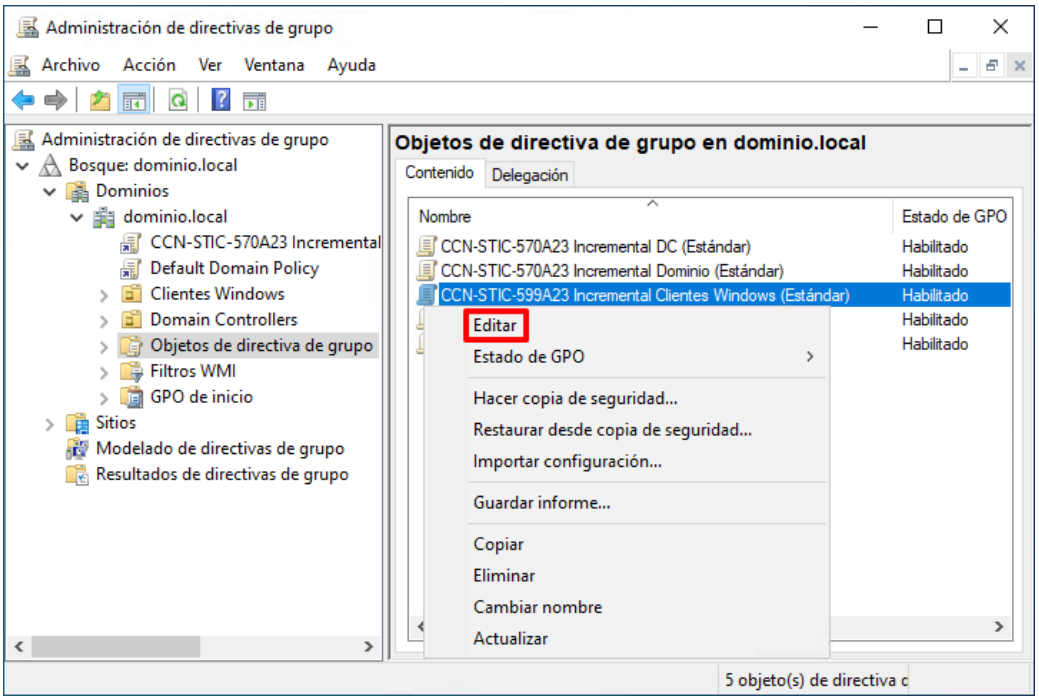
La sección y los pasos descritos a continuación, permiten establecer las modificaciones y/o adaptaciones de la configuración establecida en los apartados anteriores del presente documento.

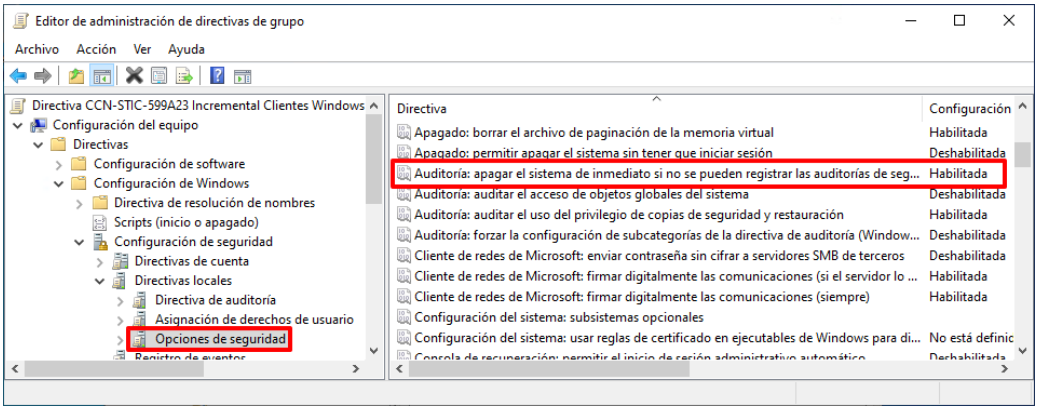
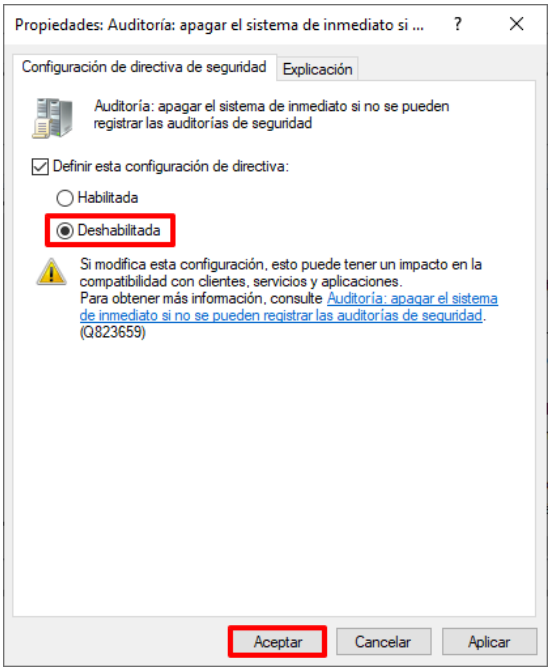
ANEXO A.4.6.1. REGISTRO DE LAS AUDITORÍAS DE SEGURIDAD

El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a adaptar la configuración establecida sobre los equipos de tipo Clientes Miembro, modificando la directiva de auditoría que puede provocar el apagado inesperado de los equipos del sistema.

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

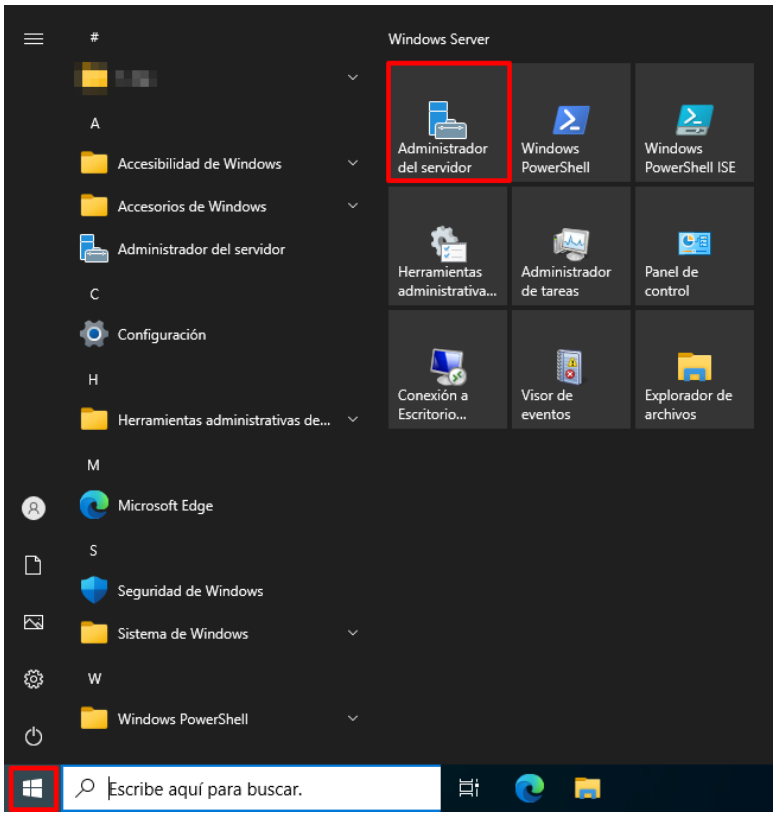
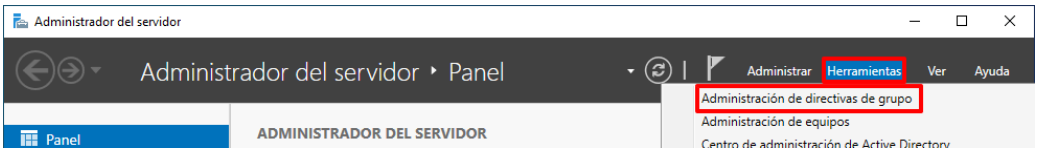
Paso	Descripción
3.	En la parte superior derecha pulse sobre el botón “Herramientas” y a continuación seleccione “Administración de directivas de grupo”. 
4.	Una vez abierta la consola, seleccione: **“Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. Hasta que se indique lo contrario,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

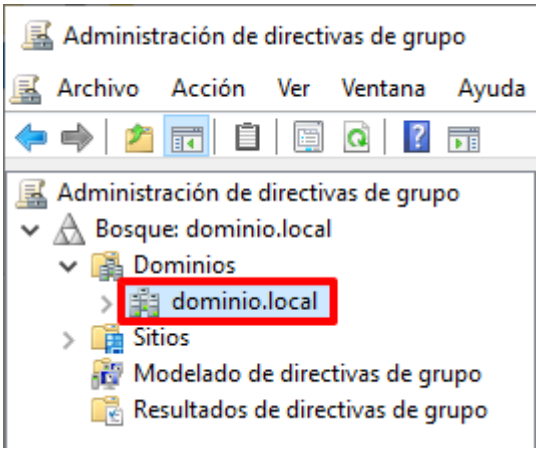
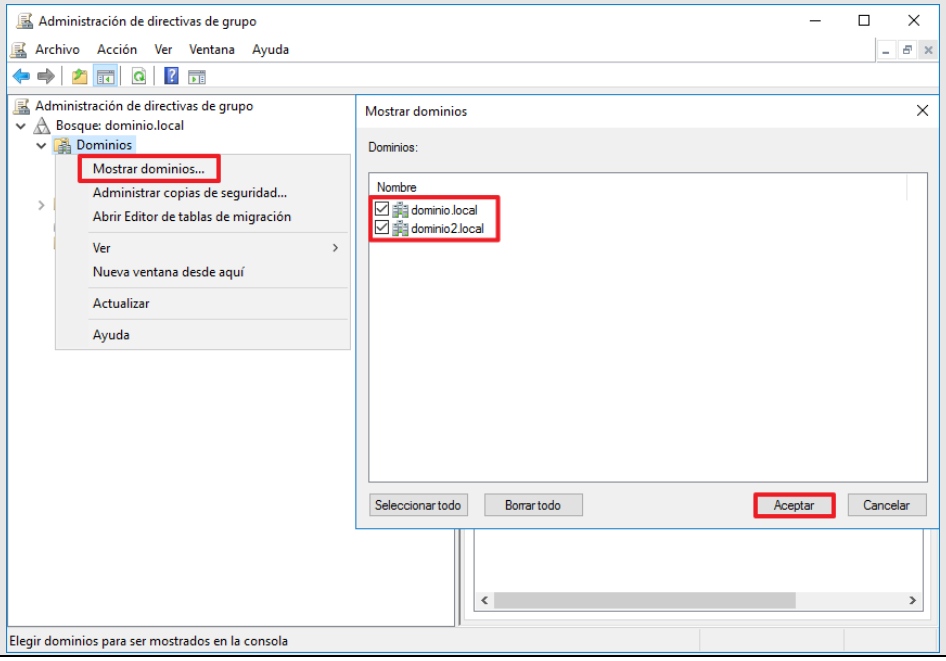
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de opciones de seguridad: – CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte 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-599A23 Incremental Clientes Windows (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.

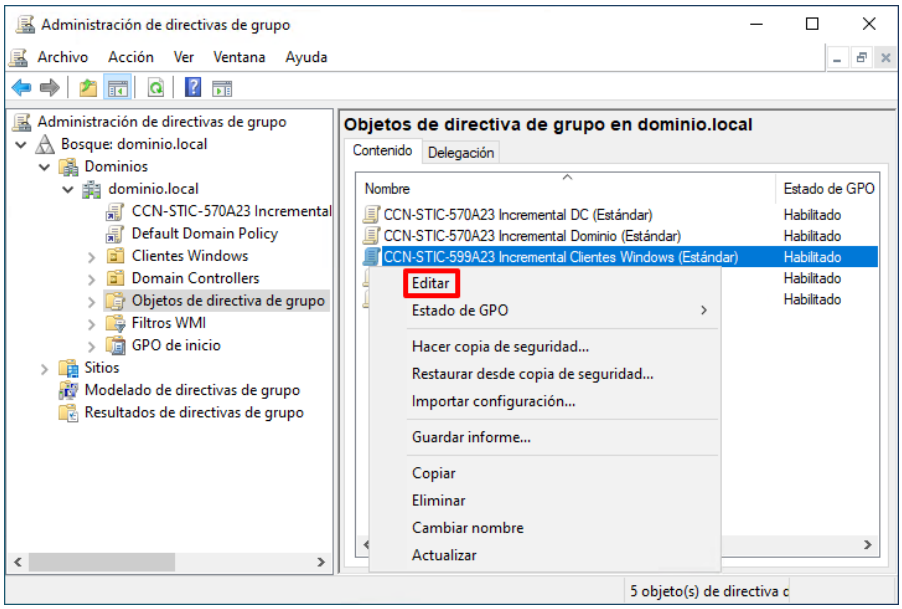
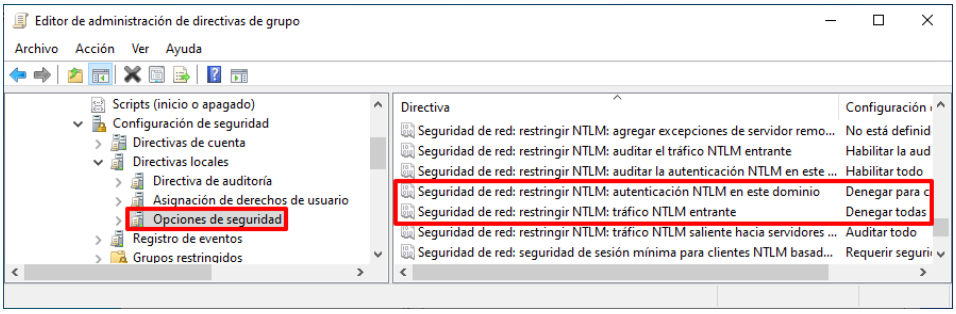
Paso	Descripción
8.	En el panel derecho identifique la directiva “Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad”. 
9.	Cuando los recursos hardware en los sistemas TIC son aprovisionados de una forma muy limitada, pueden producirse situaciones en las que 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.

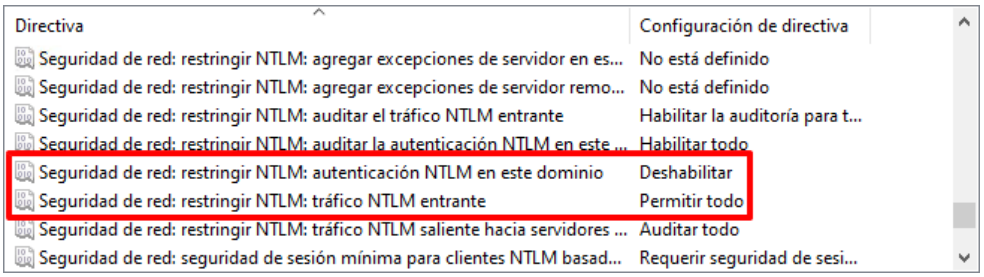
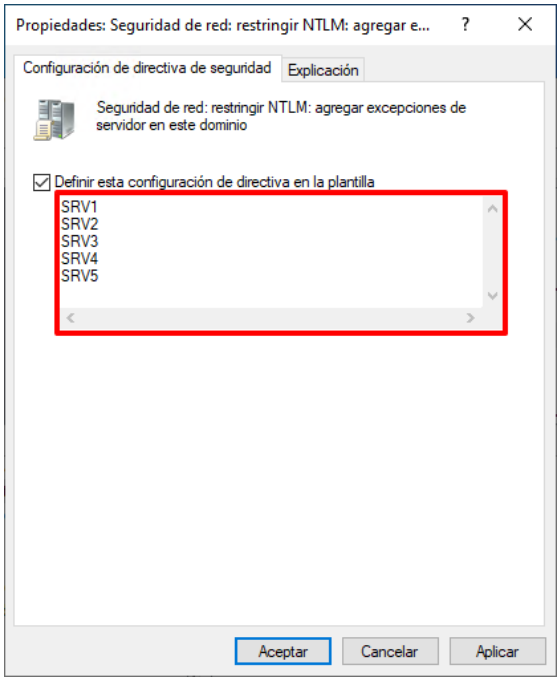
ANEXO A.4.6.2. HABILITAR NTLM

El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a adaptar la configuración establecida sobre los equipos de tipo Clientes Miembro, modificando las directivas que impiden la comunicación NTLM con los diferentes servicios que puede proporcionar el sistema.

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". 

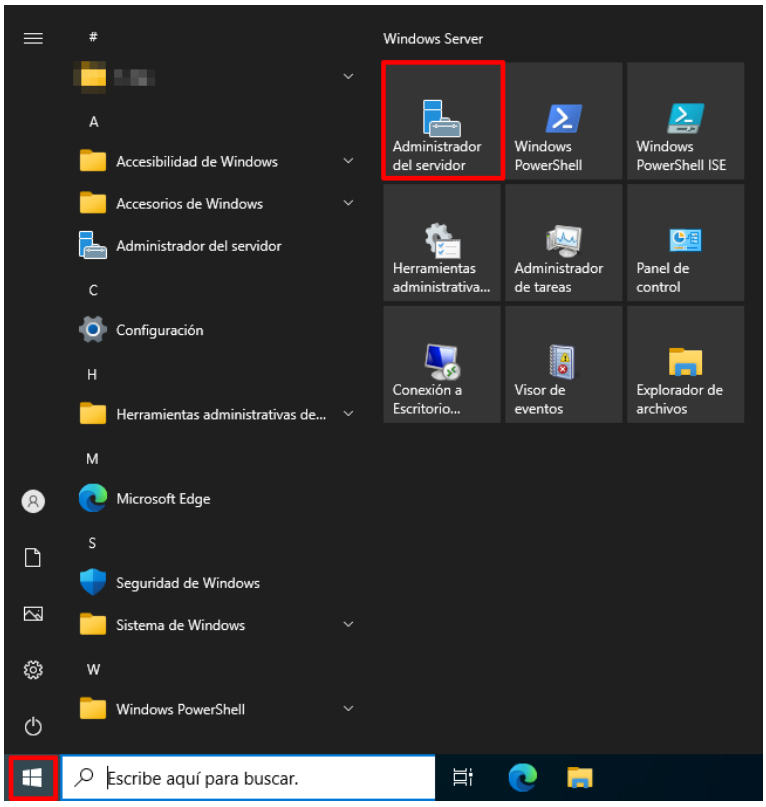
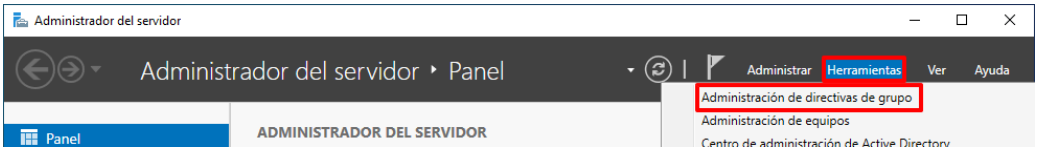
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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. 

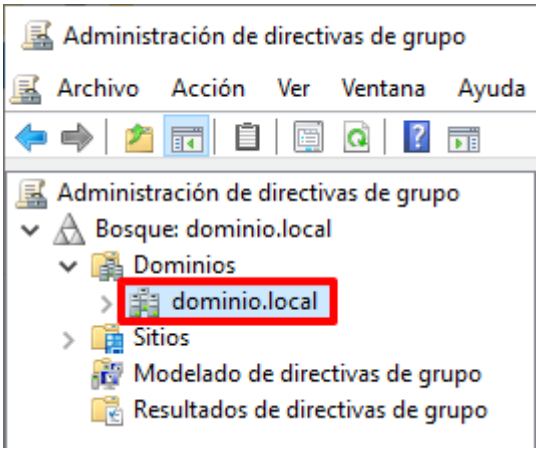
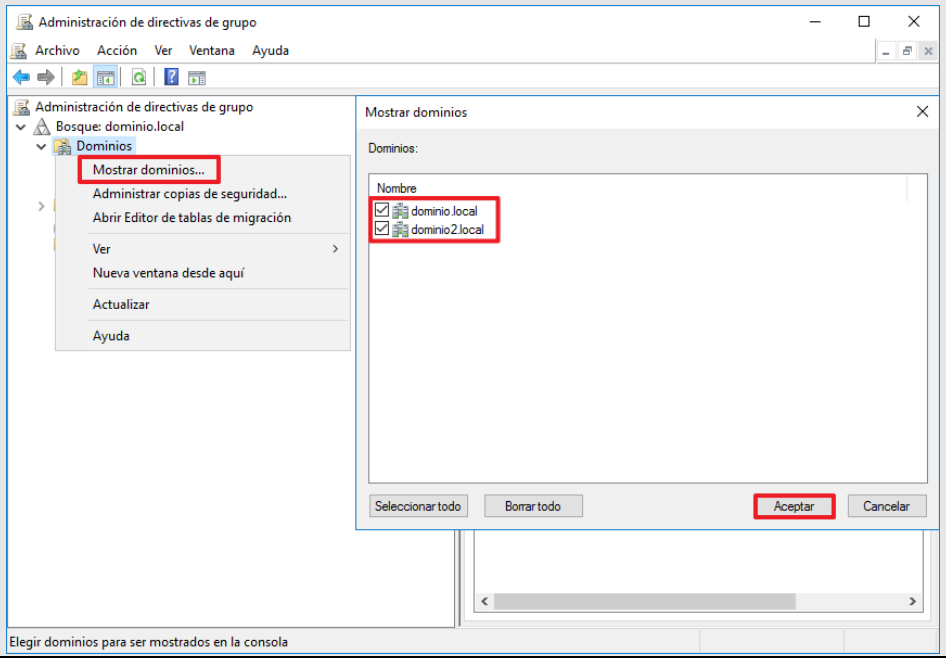
Paso	Descripción
5.	Dentro del nodo “Objetos de directiva de grupo” identifique el siguiente objeto GPO para adecuar los parámetros de opciones de seguridad: – CCN-STIC-599A23 Incremental Clientes Windows ([TIPO DE PERFILADO]) **Nota:** Si lo desea pueden generar un nuevo objeto GPO que modifique o adapte 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-599A23 Incremental Clientes Windows (Estándar)”.
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental Clientes Windows ([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: – Seguridad de red: restringir NTLM: autenticación NTLM en este dominio – Seguridad de red: restringir NTLM: tráfico NTLM entrante 

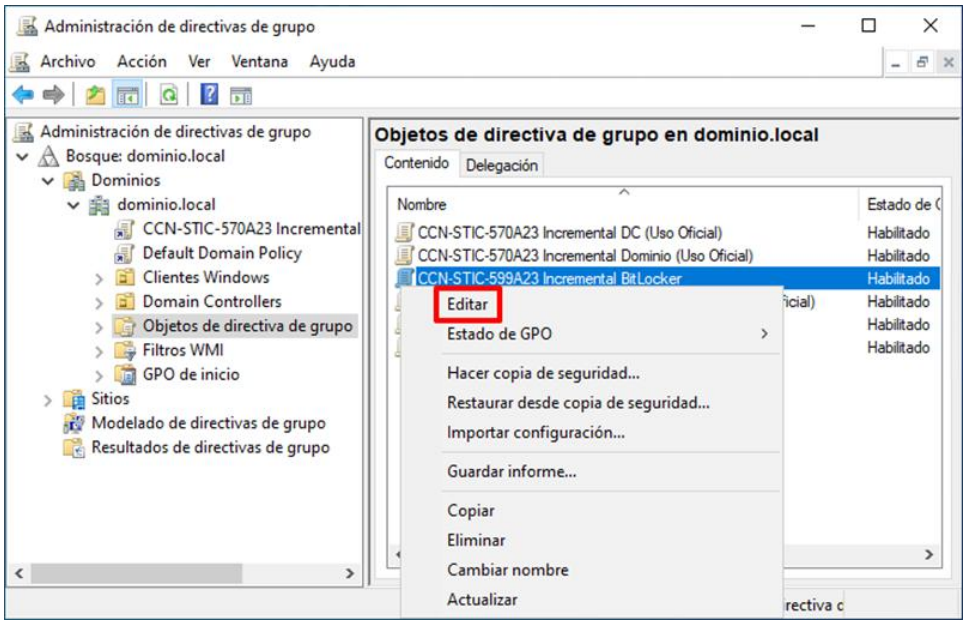
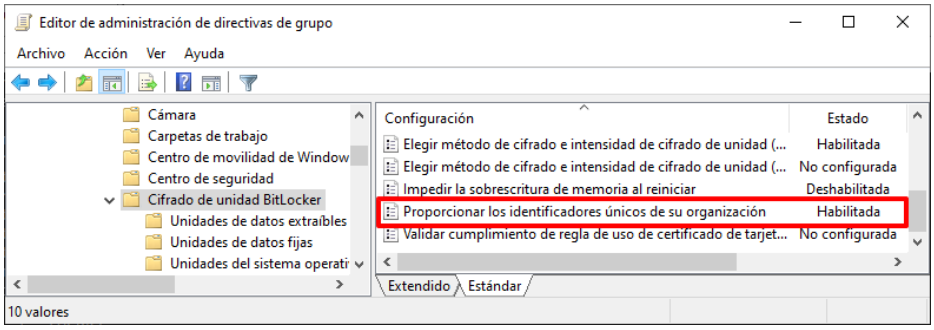
Paso	Descripción
9.	Cuando las presentes directivas se encuentran configuradas denegando la comunicación NTLM, se pueden generar errores a la hora de utilizar por parte de los clientes algunos de los servicios que ofrecen los servidores del dominio. Para habilitar NTLM y evitar estas casuísticas en caso de que la organización lo requiera, deberá configurar las directivas indicadas de la siguiente manera: – Seguridad de red: restringir NTLM: autenticación NTLM en este dominio: Deshabilitar – Seguridad de red: restringir NTLM: tráfico NTLM entrante: Permitir todo  **Nota:** Tenga en consideración que puede ser necesario aplicar la configuración de este apartado a todo el dominio dependiendo del servicio ofrecido por la organización.
10.	Con el fin de mantener la seguridad de la infraestructura, si se conocen los servidores de los cuales los clientes van a consumir sus servicios, se puede obviar la modificación realizada en pasos anteriores y establecer una lista de excepción de servidores para NTLM en la directiva “Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio”.  **Nota:** Tenga en consideración que puede ser necesario aplicar la configuración de este apartado a todo el dominio dependiendo del servicio ofrecido por la organización.

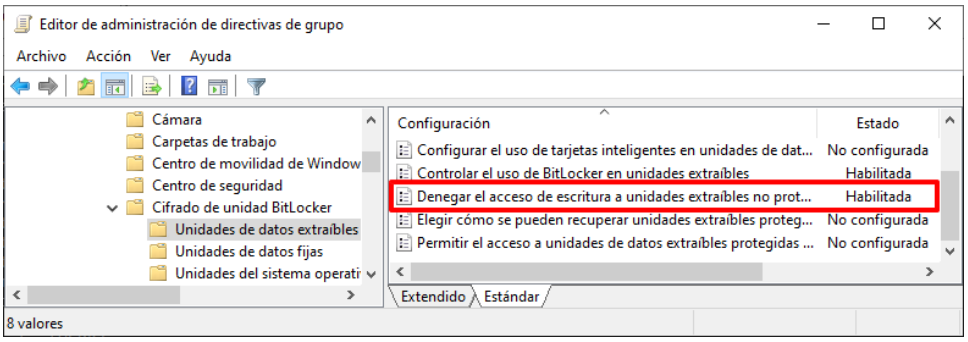
ANEXO A.4.7. CIFRADO DE UNIDAD DE BITLOCKER

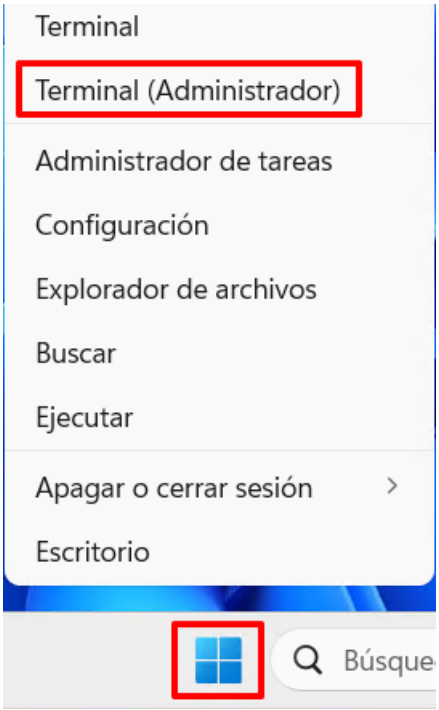
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad correspondientes a la protección de dispositivos portátiles mediante BitLocker, adaptando las configuraciones establecidas sobre los equipos de tipo Clientes Miembro, modificando las directivas que afectan a los dispositivos removibles y su uso dependiendo del cifrado.

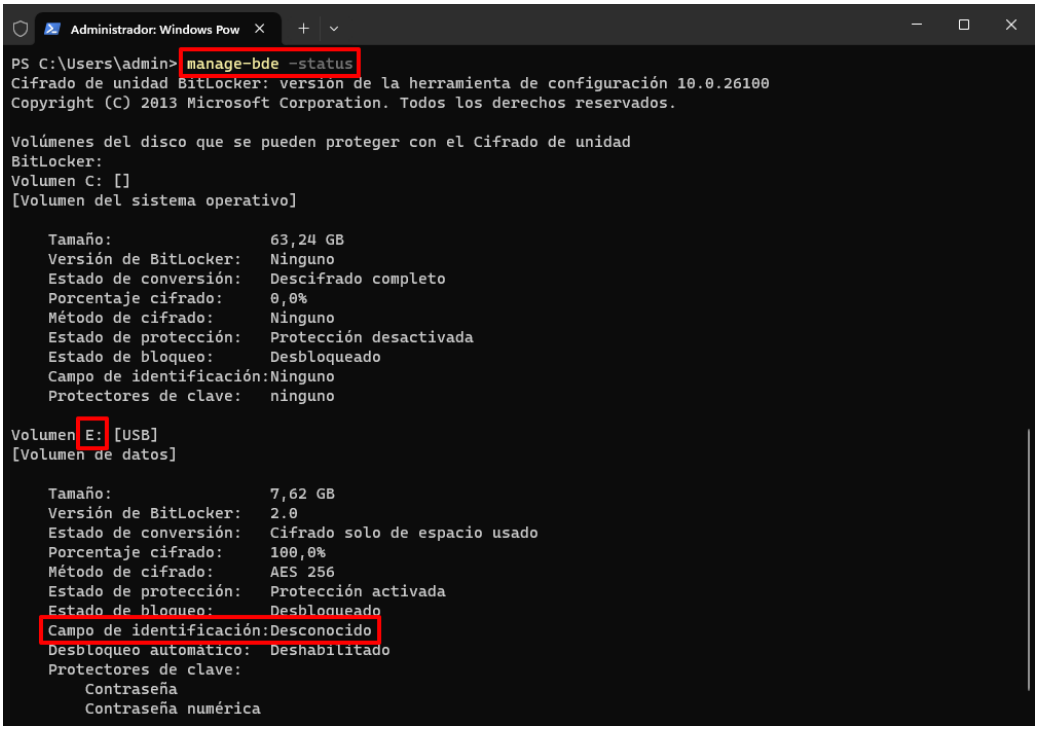
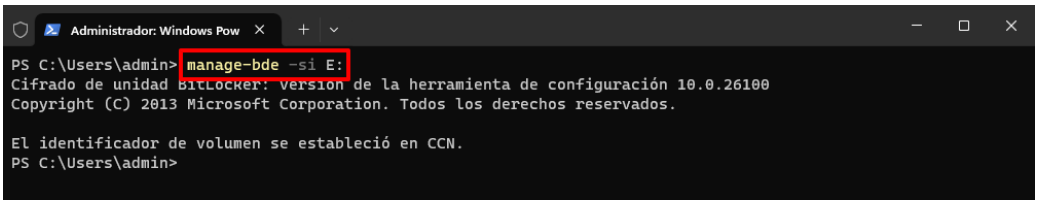
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Ejecute el "Administrador del servidor", haciendo clic sobre el botón de "Inicio" y seleccionando el icono correspondiente.  **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". 

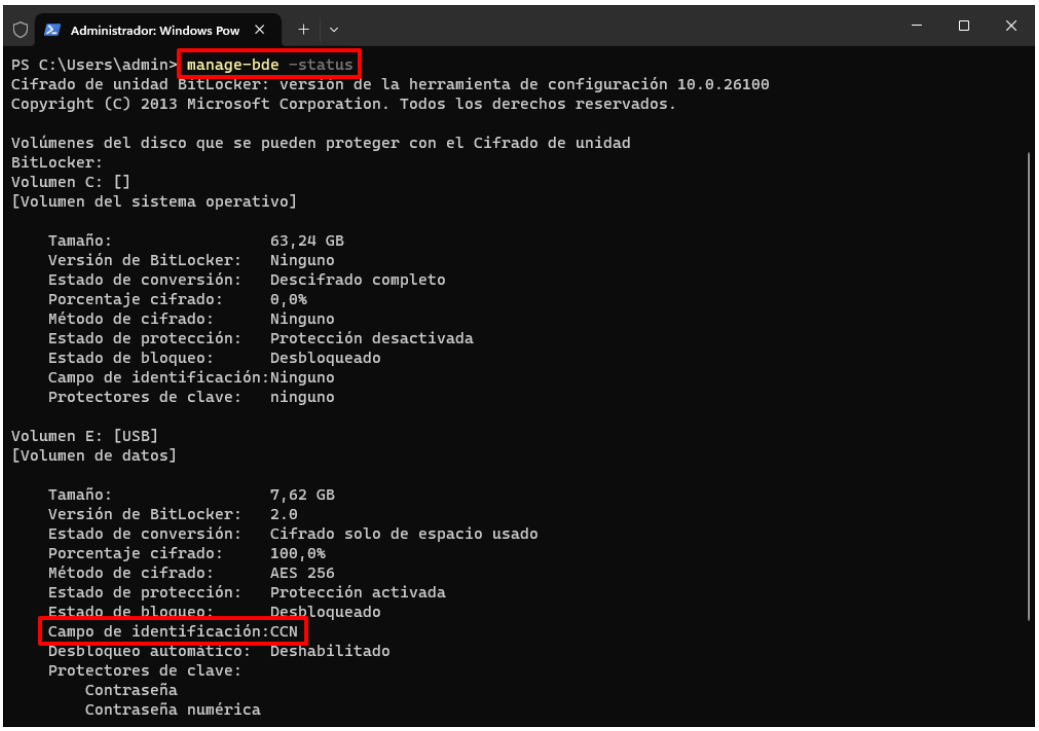
Paso	Descripción
4.	Una vez abierta la consola, seleccione: **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).  **Nota:** 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 opciones de seguridad: – CCN-STIC-599A23 Incremental BitLocker **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”. 
7.	En la ventana del “Editor de administración de directivas de grupo” despliegue el nodo: **“Directiva CCN-STIC-599A23 Incremental BitLocker→ Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker”**. Identifique en el panel derecho la directiva “**Proporcionar los identificadores únicos de su organización**”. 

Paso	Descripción
8.	De forma adicional, despliegue el nodo: **"Directiva CCN-STIC-599A23 Incremental BitLocker→ Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades datos extraíbles"**. Identifique en el panel derecho la directiva "**Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker**". 
9.	Con ambas directivas identificadas, a continuación, se describirán los diferentes casos posibles dependiendo de las necesidades de su organización: – Los dispositivos removibles solo se podrán utilizar en modo escritura si han sido **cifrados en el propio sistema utilizando identificadores para su filtrado** por organización, es decir, mantener la configuración establecida por la presente guía, en cuyo caso no se deberá hacer nada más que seguir el paso a paso correspondiente. – Los dispositivos removibles solo podrán ser utilizados en modo escritura si han sido **cifrados en cualquier equipo o sistema**, incluyendo uno ajeno a la organización. En este caso deberá establecer como "**Deshabilitada**" la directiva "**Proporcionar los identificadores únicos de su organización**", además de modificar la directiva "**Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker**", desmarcando la opción "**No permitir el acceso de escritura a dispositivos configurados en otra organización**" dentro de la directiva. – Los dispositivos removibles podrán ser utilizados en modo escritura **incluso si no se encuentran cifrados**. En este caso, deberá establecer como "**Deshabilitada**" tanto la directiva "**Proporcionar los identificadores únicos de su organización**", como "**Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker**".
10.	En el supuesto de que para su organización vaya a utilizar la configuración por defecto de la presente guía, es decir, que solo se podrán utilizar en modo escritura si han sido **cifrados en el propio sistema utilizando identificadores para su filtrado** por organización, pueden existir dispositivos removibles que **ya se encuentren cifrados** mediante BitLocker **previamente a la configuración** de seguridad. Para poder incluir el identificador configurado al dispositivo removible previamente cifrado, deberá establecerlo mediante comandos.

Paso	Descripción
11.	Inicie sesión en un cliente miembro del dominio donde se hayan aplicado las directivas de seguridad relativas a BitLocker. Debe iniciar sesión con una cuenta que sea Administrador del Dominio. **Nota:** Es necesario que el equipo donde se inicia sesión cuente con el objeto GPO que contenga las directivas de BitLocker configuradas, en especial la directiva "Proporcionar los identificadores únicos de su organización", en caso contrario, el paso a paso no funcionará correctamente tal como está contemplado.
12.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 

Paso	Descripción
13.	Conecte y descifre el dispositivo removible en el equipo. En la consola de PowerShell ejecute el siguiente comando para conocer aquellos discos o volúmenes presentes en el equipo.
	> manage-bde -status
	
	Nota: También podrá observar como el dispositivo removible muestra el "Campo de identificación" como desconocido, debido al cifrado del dispositivo sin la directiva "Proporcionar los identificadores únicos de su organización" configurada.
14.	Ejecute el siguiente comando para configurar el identificador previamente establecido en la directiva de BitLocker.
	> manage-bde -si [LETRA DE UNIDAD:]
	
	Nota: En este ejemplo se hace uso de la letra de unidad E:.

Paso	Descripción
15.	En la consola de PowerShell ejecute el siguiente comando para comprobar que el identificador establecido se ha configurado correctamente. > manage-bde -status  **Nota:** En este ejemplo se ha establecido el identificador como “CCN”.
16.	Realice estos pasos por cada dispositivo removible a configurar con el identificador establecido en la directiva “Proporcionar los identificadores únicos de su organización”, de esta manera no tendrá que descifrar cada dispositivo y volver a cifrarlo tras la aplicación de las directivas de seguridad.

ANEXO B. CONFIGURACIÓN SEGURA DE CLIENTES WINDOWS INDEPENDIENTES

ANEXO B.1. PASO A PASO DE CONFIGURACIÓN BASE DE SEGURIDAD SOBRE CLIENTES INDEPENDIENTES

En el presente anexo, se incluye una línea base de seguridad para el aseguramiento de los equipos clientes independientes, 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 la 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 independiente, tomando en este sentido los siguientes elementos:

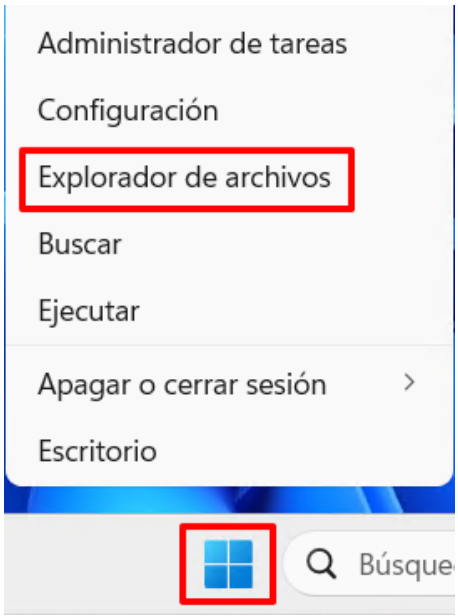
a) Clientes Independientes: Aplicable a aquellos equipos que utilicen cualquier tipo de servicio de forma independiente, se definirán medidas de seguridad mediante directivas de grupo local y se ejecutarán acciones manuales y automatizadas para finalizar las labores de configuración segura.

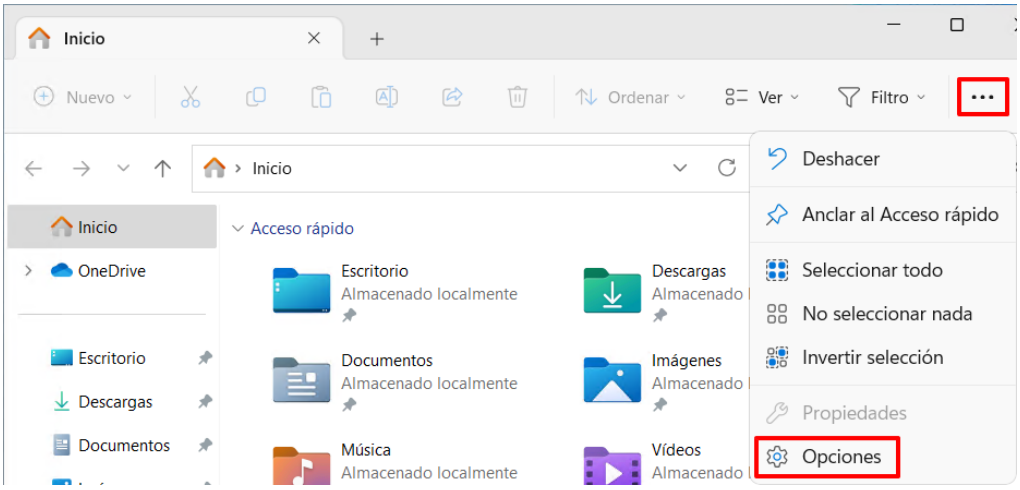
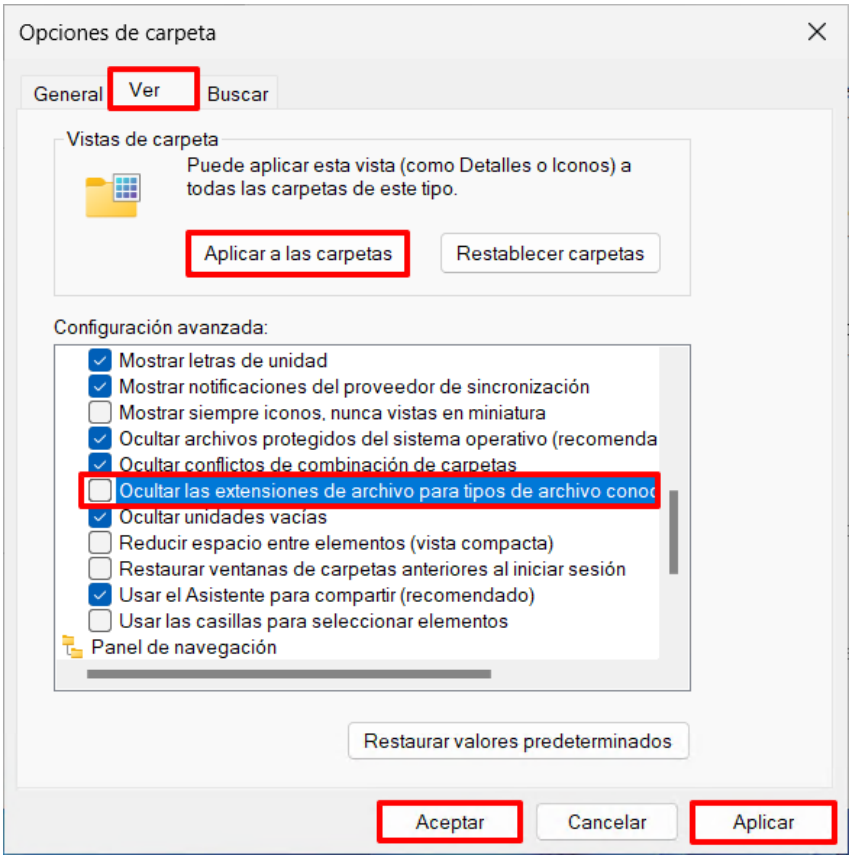
b) Configuraciones individuales: Es necesario indicar que ciertas medidas de seguridad no pueden ser aplicadas por medio de configuraciones exactas a nivel de Windows. Esto es debido a que deben ser personalizadas por cada organización o adaptadas a esta. Por ello, se han dedicado apartados específicos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

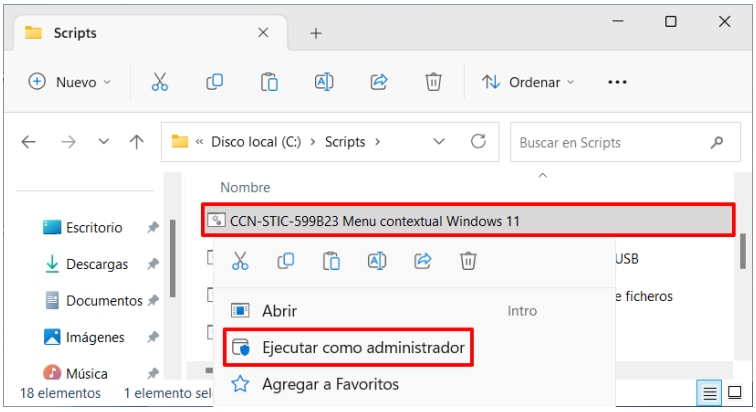
ANEXO B.1.1. PREPARACIÓN DEL EQUIPO

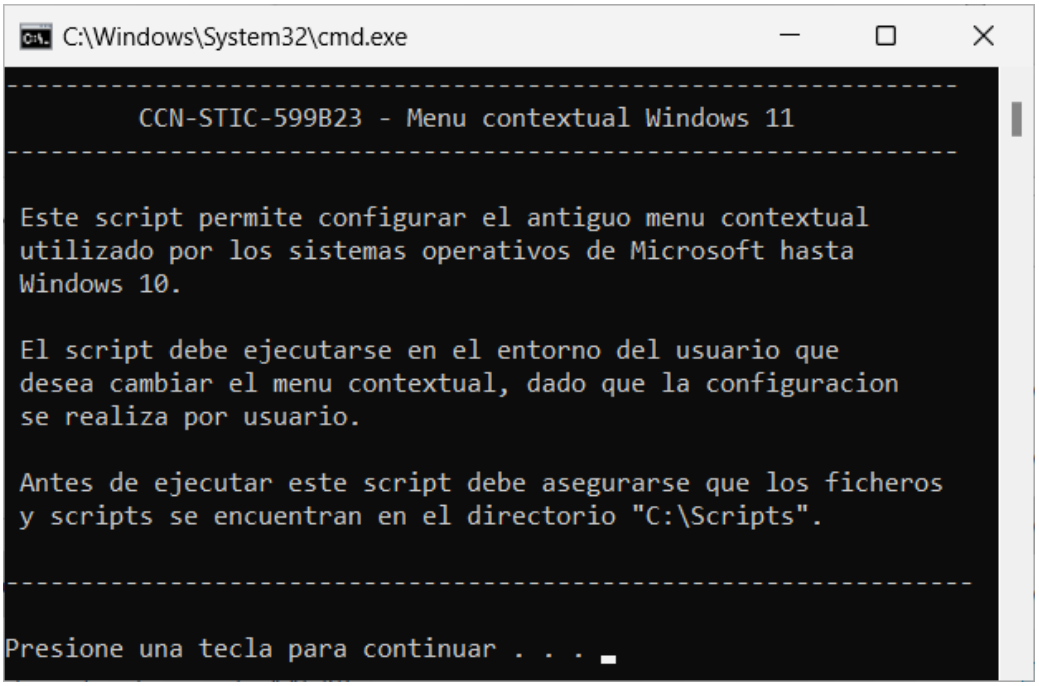
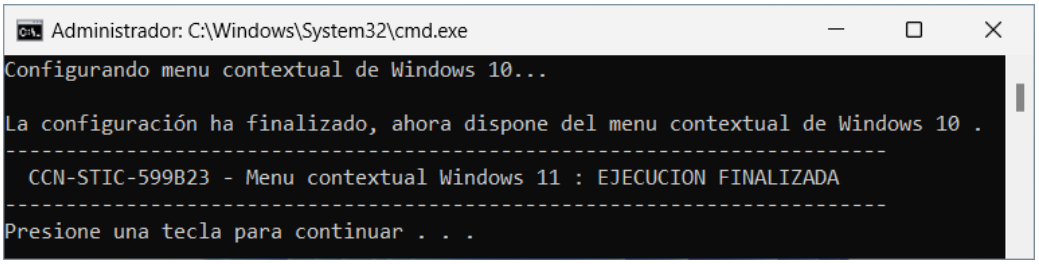
Los pasos que se describen a continuación se realizarán en un Cliente Independiente donde se realizará la implementación de las medidas de seguridad mediante directivas de grupo local. Solo es necesario realizar este procedimiento una (1) vez por Cliente Independiente a configurar.

Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
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-599AB23\CLIENTES INDEPENDIENTES”.
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 “…” del menú superior y seleccione el icono de “Opciones”. 
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 

Paso	Descripción
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del cliente independiente: – ESTANDAR/USO OFICIAL/MATERIAS CLASIFICADAS • Configuraciones Adicionales [Directorio] • CCN-STIC-599B23 Cliente Independiente – Acceso Remoto RDP ([TIPO DE PERFILADO]).bat • CCN-STIC-599B23 Cliente Independiente – Actualizaciones WU.bat • CCN-STIC-599B23 Cliente Independiente – BitLocker.bat (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) • CCN-STIC-599B23 Cliente Independiente – Control Dispositivos.bat • CCN-STIC-599B23 Cliente Independiente – Windows Defender ([TIPO DE PERFILADO]).bat • CCN-STIC-599B23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).inf • CCN-STIC-599B23 Incremental Acceso Remoto RDP ([TIPO DE PERFILADO]).wfw • CCN-STIC-599B23 Incremental Actualizaciones WU.inf • CCN-STIC-599B23 Incremental BitLocker.inf (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) • CCN-STIC-599B23 Incremental Control Dispositivos.inf • CCN-STIC-599B23 Incremental Windows Defender ([TIPO DE PERFILADO]).inf • CCN-STIC-599B23_Acceso_Remoto_RDP_([TIPO DE PERFILADO]).reg • CCN-STIC-599B23_Actualizaciones_WU.reg • CCN-STIC-599B23_BitLocker.reg (Solo disponible en USO OFICIAL o MATERIAS CLASIFICADAS) • CCN-STIC-599B23_Control_Dispositivos.reg • CCN-STIC-599B23_Windows_Defender_([TIPO DE PERFILADO]).reg • GroupPolicy [Directorio] • CCN-STIC-599B23 Cliente Independiente – Paso 1 – Servicios.bat • CCN-STIC-599B23 Cliente Independiente – Paso 2 – GPO.bat • CCN-STIC-599B23 Cliente Independiente – Paso 3 – Firewall.bat • CCN-STIC-599B23 Cliente Independiente – Paso 4 – Aplica plantilla y reinicia.bat • CCN-STIC-599B23 Incremental Clientes Independientes ([TIPO DE PERFILADO]).inf

Paso	Descripción
	• CCN-STIC-499B23 Incremental Clientes Independientes ([TIPO DE PERFILADO]).wfw • CCN-STIC-599B23 Incremental Servicios ([TIPO DE PERFILADO]).inf – CCN-STIC-599B23 Cliente Independiente – Desinstalar características.bat – CCN-STIC-599B23 Cliente Independiente – Eliminar aplicaciones aprovisionadas.bat – CCN-STIC-599B23 Cliente Independiente – Segregación de roles.bat – CCN-STIC-599B23 Menu contextual Windows 11.bat – CCN-STIC-599B23 Windows Defender - Análisis de dispositivos USB.bat – CCN-STIC-599B23 Windows Defender - Análisis de integridad de ficheros.bat – CCN-STIC-599B23 Windows Defender - Análisis en el arranque.bat – CCN-STIC-599B23_Analisis_arranque.ps1 – CCN-STIC-599B23_Analisis_arranque_OS.xml – CCN-STIC-599B23_Analisis_dispositivos_USB.xml – CCN-STIC-599B23_Analisis_USBs.ps1 – CCN-STIC-599B23_Antiguo_menu_contextual.ps1 – CCN-STIC-599B23_Desinstala_caracteristicas.ps1 – CCN-STIC-599B23_Eliminar_aplicaciones_aprovisionadas.ps1 – CCN-STIC-599B23_Habilitar_registro_conexion_USBs.ps1 – CCN-STIC-599B23_Integridad_ficheros.xml
8.	A continuación, diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-599B23 Menu contextual Windows 11.bat” y seleccione la opción del menú contextual “Ejecutar como Administrador”.  **Nota:** El presente script solamente es necesario ejecutarlo en el caso de que el sistema operativo del cliente independiente se corresponda con la versión Windows 11. Si su sistema operativo es Windows 10, o si quiere mantener el uso del nuevo menú contextual incluido en Windows 11, continúe en el siguiente apartado apartado. Tenga en consideración que para la elaboración del presente documento se ha ejecutado el script indicado y en los ejemplos se mostrará el antiguo menú contextual.

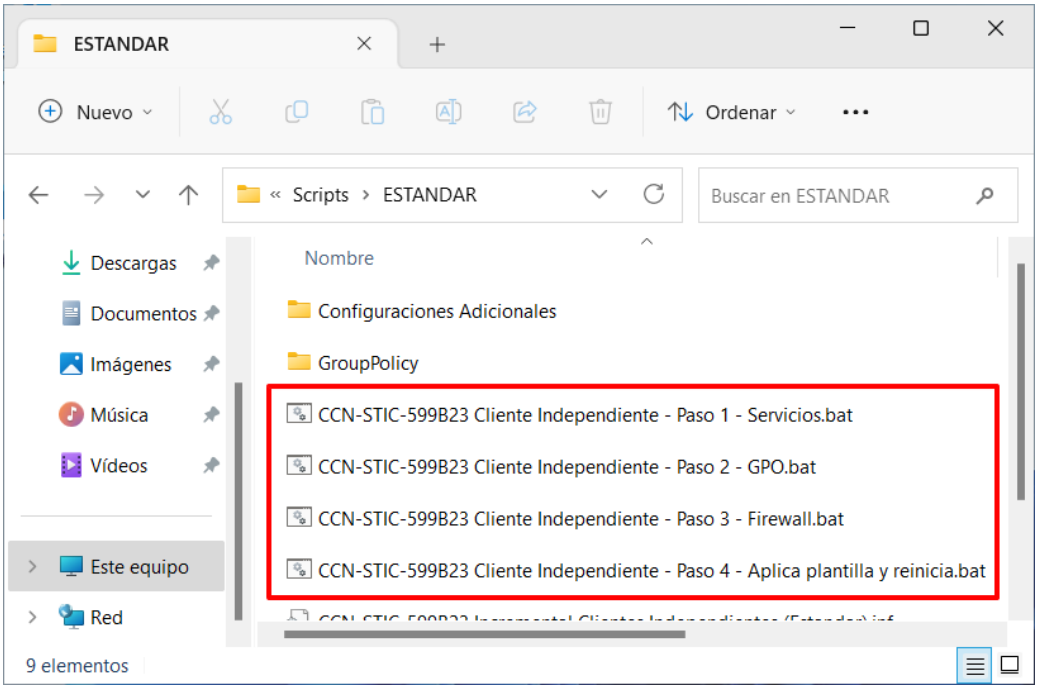
Paso	Descripción
9.	A continuación, se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar. 
10.	Espere a que finalice la ejecución y pulse una tecla para finalizar.  **Nota:** Durante la ejecución del script se reiniciará la interfaz gráfica del sistema.

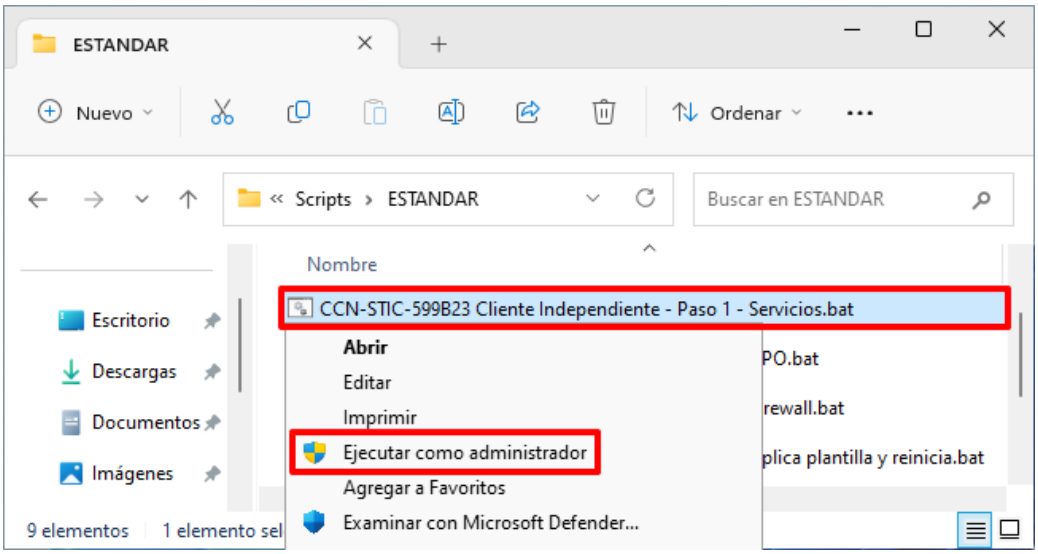
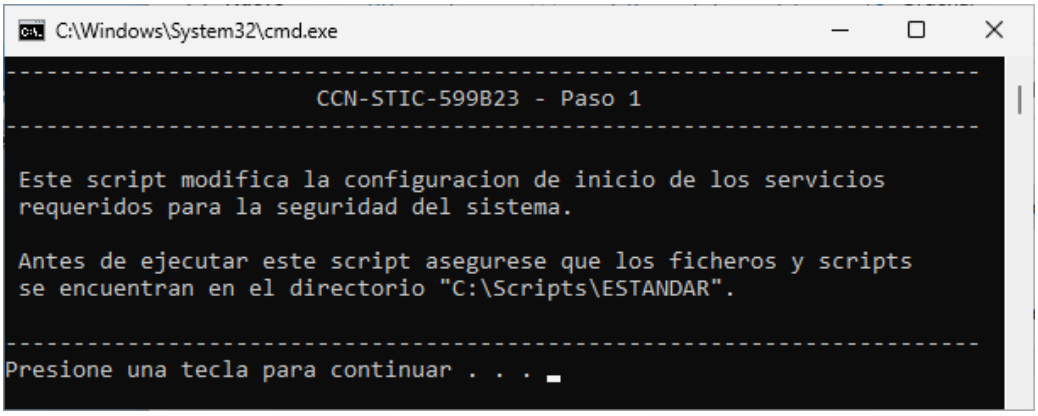
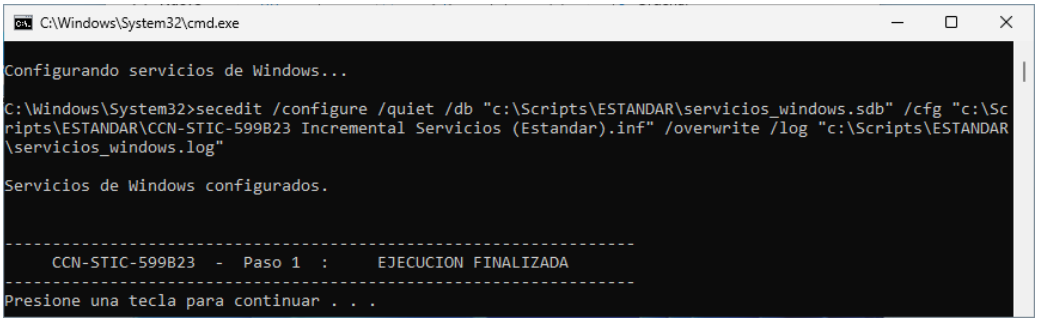
ANEXO B.1.2. CONFIGURACIÓN DE SEGURIDAD EN CLIENTES INDEPENDIENTES

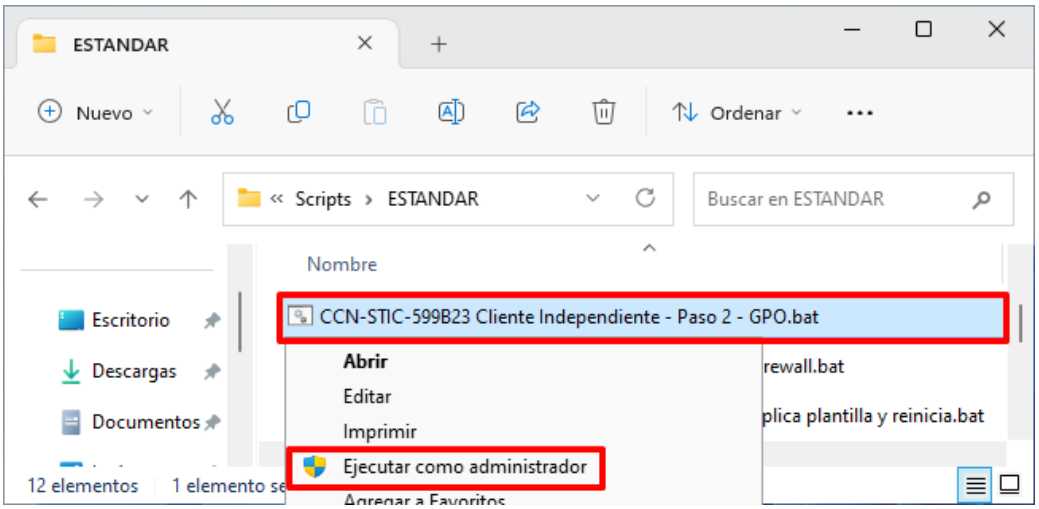
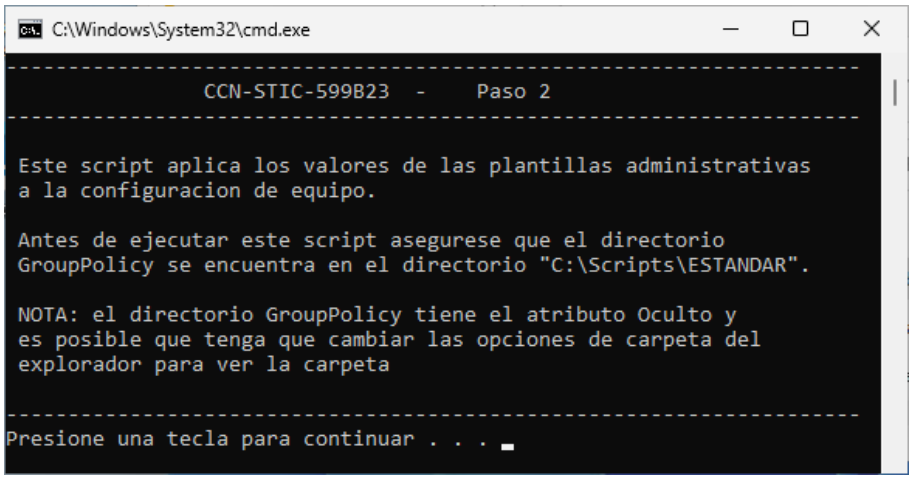
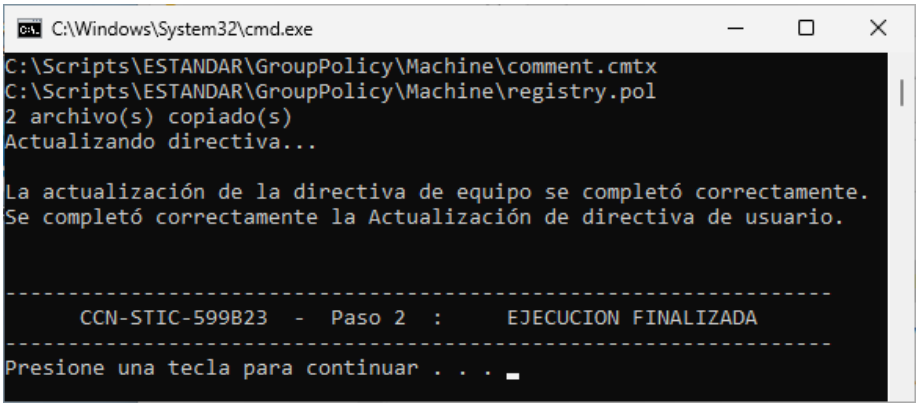
Una vez realizada la preparación de la configuración de seguridad necesaria a implementar, será necesaria su aplicación sobre el equipo correspondiente, así como la ejecución de labores adicionales para cubrir todos los aspectos necesarios de seguridad.

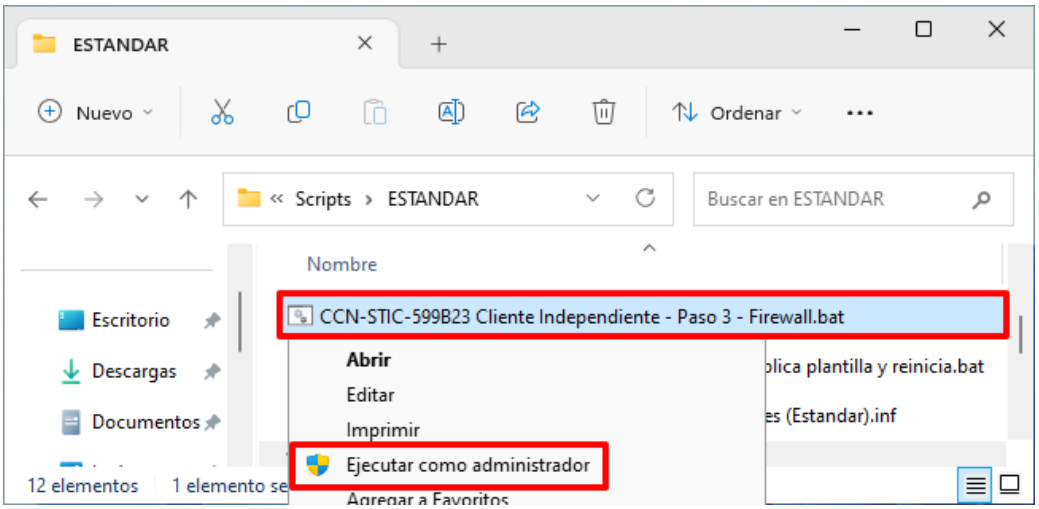
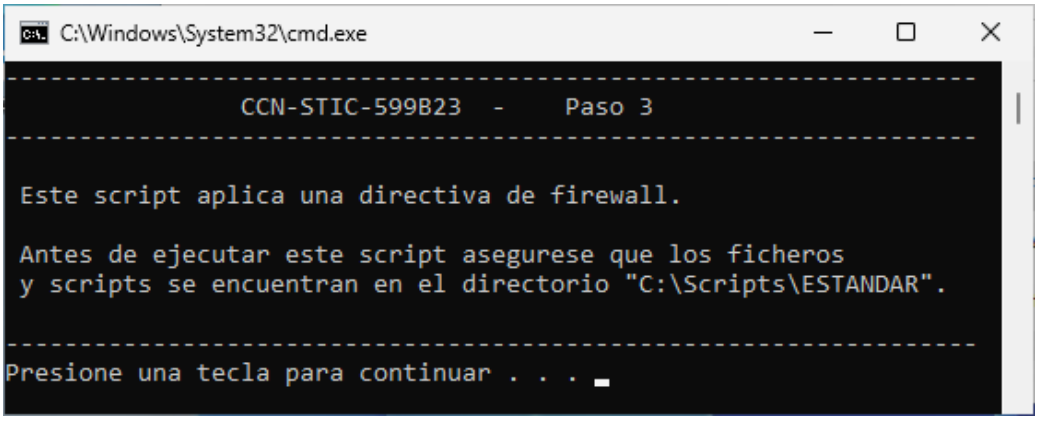
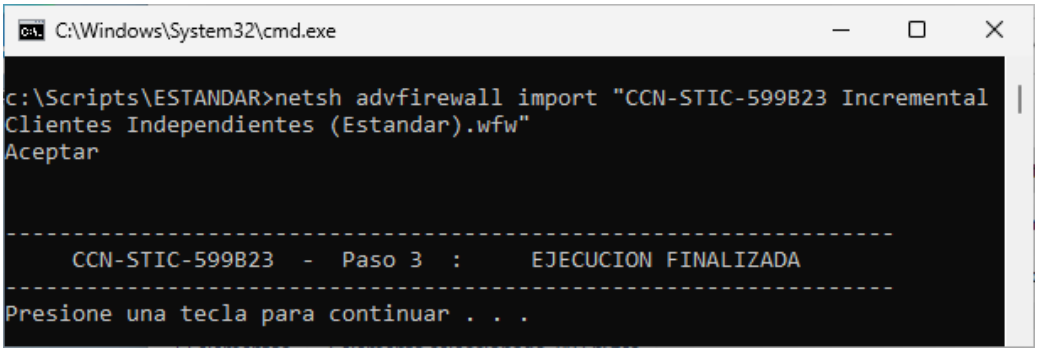
ANEXO B.1.2.1. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD

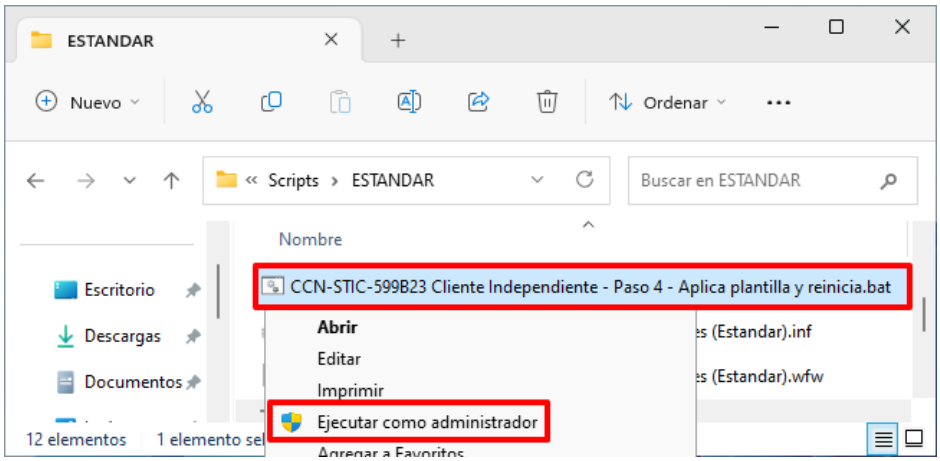
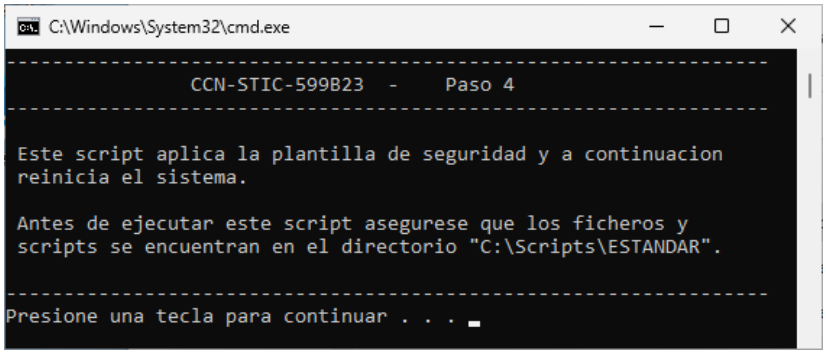
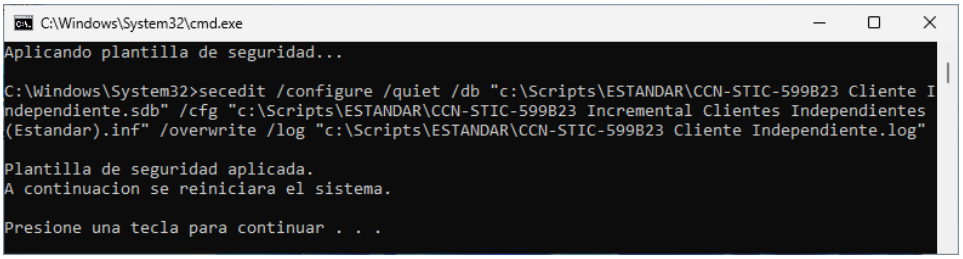
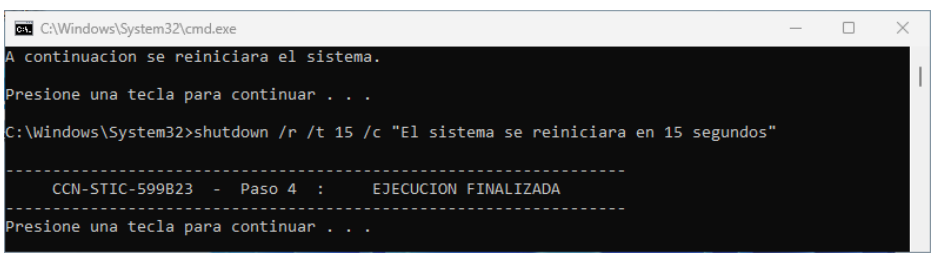
A continuación, se definen los pasos a seguir para la adecuada aplicación de las políticas de seguridad importadas en el punto anterior para aplicar la configuración de seguridad sobre el equipo independiente. Solo es necesario realizar este procedimiento una (1) vez por Cliente Independiente a configurar.

Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]**" y ubique los siguientes scripts: • CCN-STIC-599B23 Cliente Independiente – Paso 1 – Servicios.bat • CCN-STIC-599B23 Cliente Independiente – Paso 2 – GPO.bat • CCN-STIC-599B23 Cliente Independiente – Paso 3 – Firewall.bat • CCN-STIC-599B23 Cliente Independiente – Paso 4 – Aplica plantilla y reinicia.bat  **Nota:** Seleccione el directorio acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

Paso	Descripción
3.	A continuación, haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Paso 1 - Servicios.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
4.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración de inicio de los servicios. 
5.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

Paso	Descripción
6.	Después, haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Paso 2 - GPO.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
7.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la aplicación de las plantillas administrativas. 
8.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

Paso	Descripción
9.	Posteriormente, haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Paso 3 - Firewall.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
10.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la aplicación de la directiva de firewall. 
11.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

Paso	Descripción
12.	Por último, haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Paso 4 – Aplica plantilla y reinicia.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
13.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la aplicación de la plantilla de seguridad. 
14.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 
15.	Tras esto, se le avisará de que el sistema se reiniciará en 15 segundos. 

ANEXO B.1.2.2. CONFIGURACIÓN DE SEGURIDAD

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

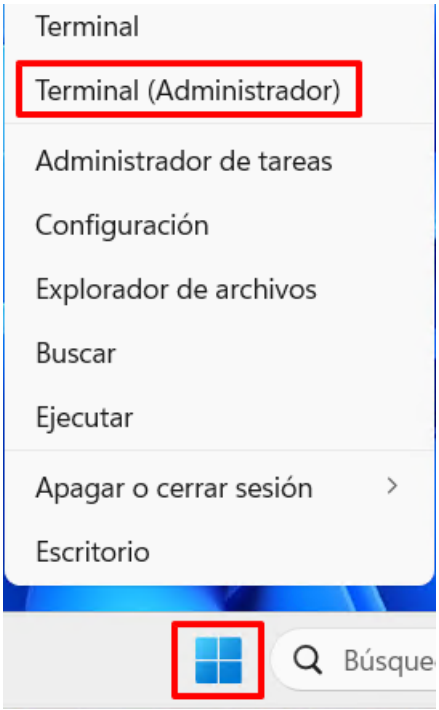
Para lograr el objetivo anterior se describen dos alternativas:

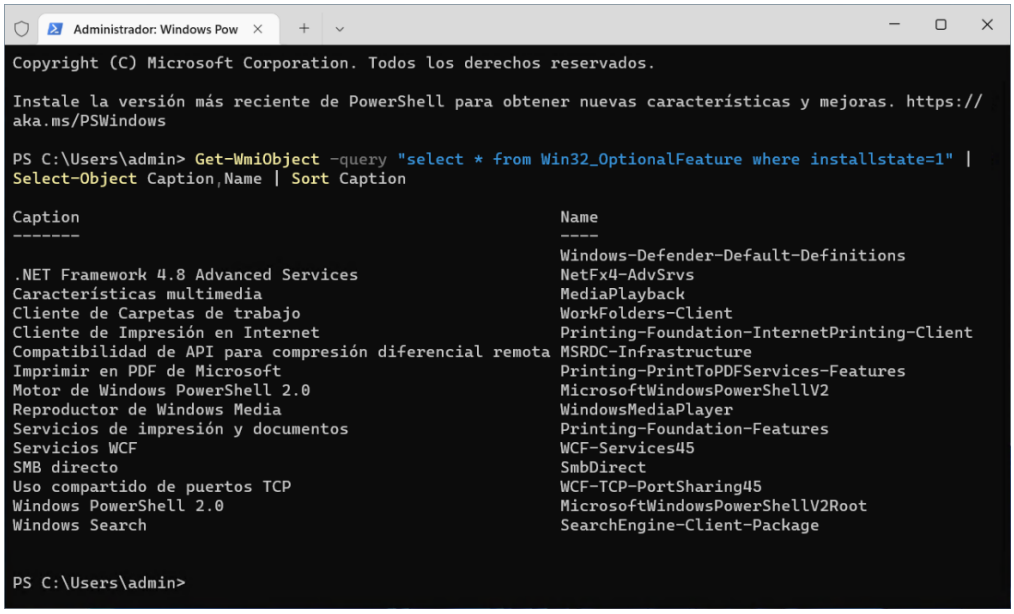
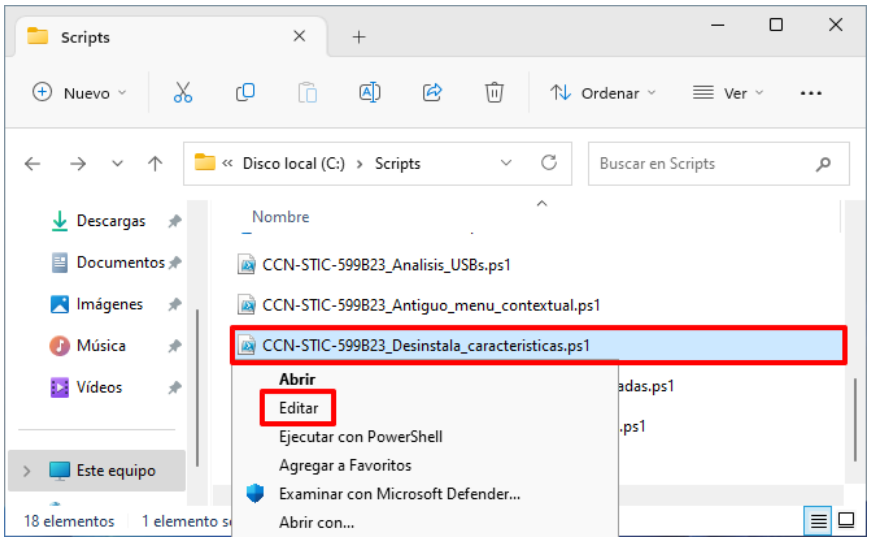
a) Por un lado, se facilitarán varios scripts que permitan desinstalar aquellas características y aplicaciones aprovisionadas consideradas no necesarias dentro de un equipo de tipo Cliente Independiente.

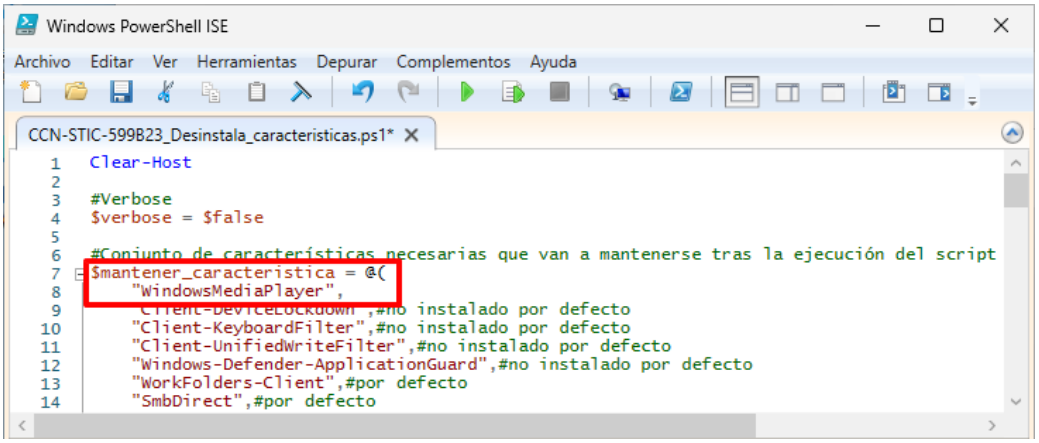
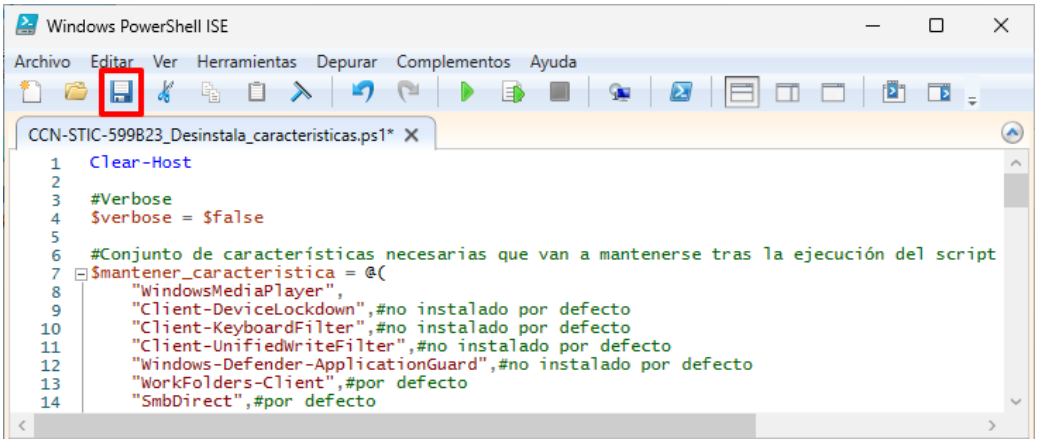
b) Por otra parte, se facilitará un paso a paso con información sobre como desinstalar características de forma gráfica y manual.

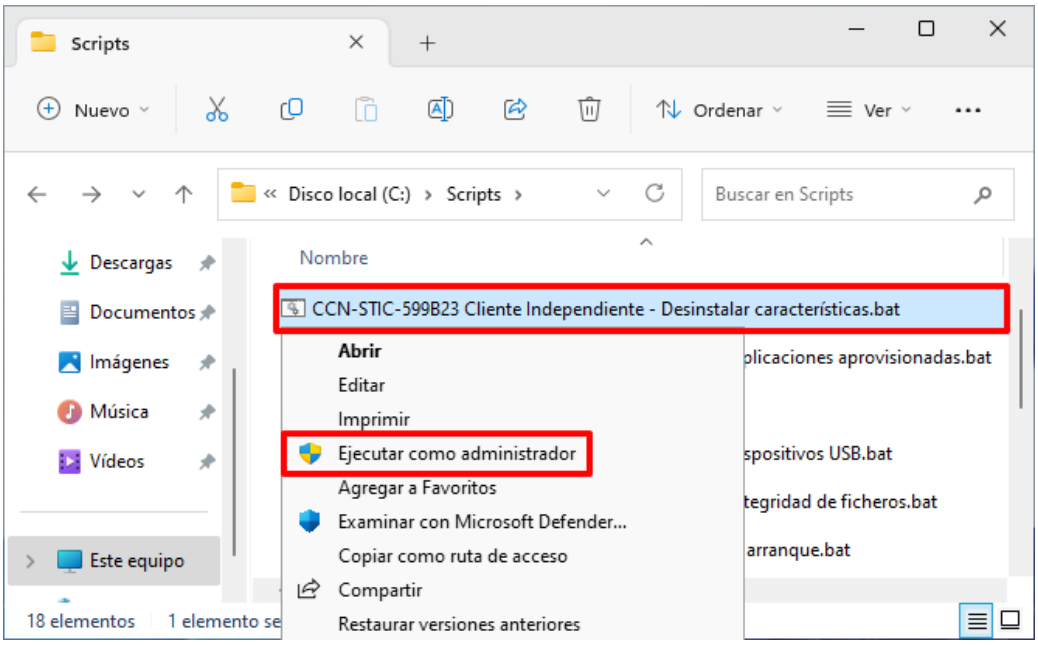
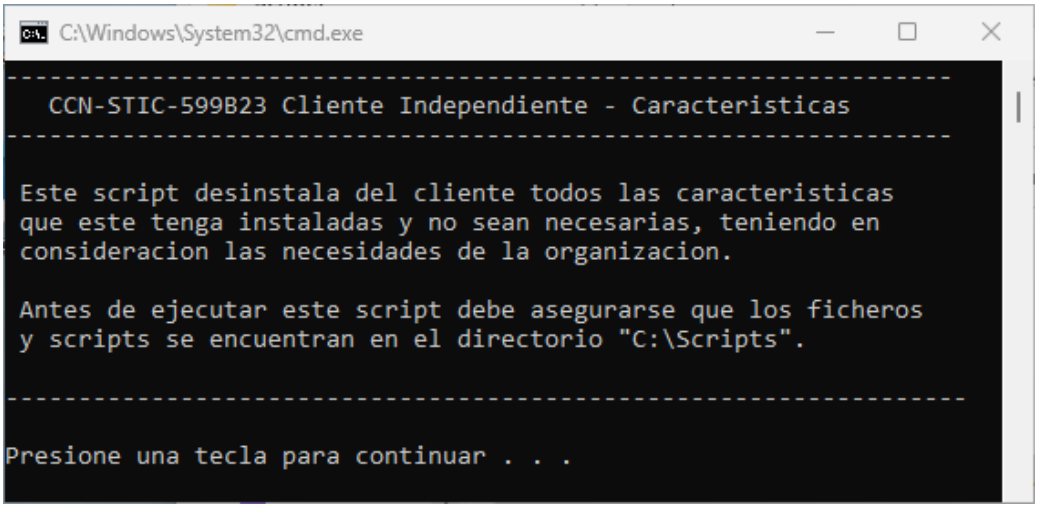
A continuación, se describen los pasos para realizar una desinstalación de características, mediante los scripts correspondientes, implementadas en un equipo de tipo Cliente Independiente. Solo es necesario realizar este procedimiento una (1) vez por Cliente Independiente a configurar.

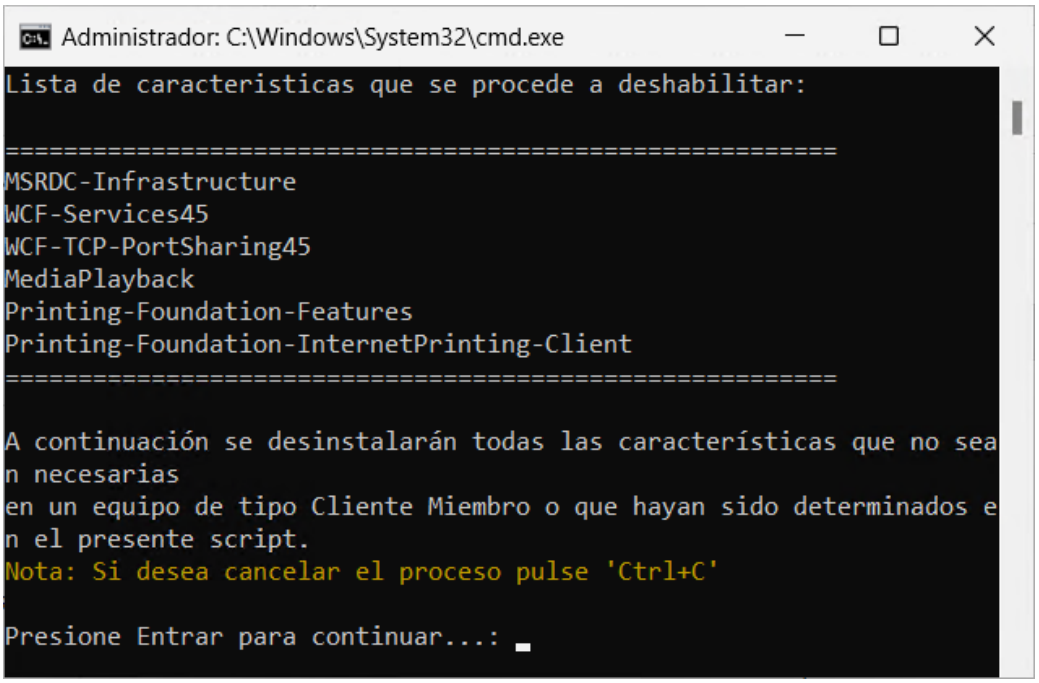
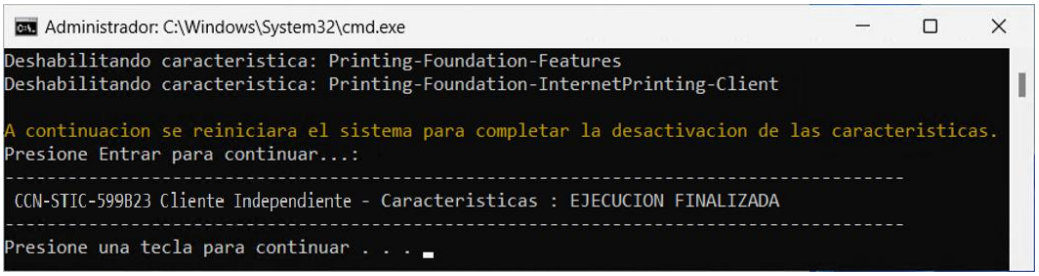
Nota: Si desea solo ejecutar esta acción de forma manual, vaya al "Paso 28" de este apartado.

Paso	Descripción
16.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
17.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 

Paso	Descripción
18.	En la consola de PowerShell ejecute el siguiente comando para conocer aquellas características instaladas en el equipo.
	> Get-WmiObject -query "select * from Win32_OptionalFeature where installstate= 1" | Select-Object Caption,Name | Sort Caption
	
	Nota: Puede redirigir la salida del comando a un fichero si lo desea con el objetivo de evaluar mejor la información mostrada.
19.	A continuación, **EVALÚE** y **DETERMINE** aquellas características **QUE NO SON NECESARIAS ELIMINAR** y anótelas. Deberá anotar los elementos ubicados en la columna “Name”.
20.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “CCN-STIC-599B23_Desinstala_caracteristicas.ps1” y seleccione la opción del menú contextual “Editar”. Con ello se abrirá una ventana de Windows PowerShell ISE.
	

Paso	Descripción
21.	Dentro de la ventana de PowerShell ISE, al inicio del script identifique la línea donde se indica "$mantener_caracteristica". Dentro de la citada línea deberá incluir aquellas características anotadas en pasos anteriores, sin modificar las características que ya vienen incluidas en el script por defecto. Deberá **incluir los nombres entre comillas ("") y separados por comas**.  **Nota:** En este ejemplo se ha incluido la característica "WindowsMediaPlayer". Tenga en consideración que ya existen otras características que ya han sido determinadas como necesarias y no se desinstalarán.
22.	Cuando haya finalizado pulse sobre el botón "Guardar" en la parte superior izquierda y cierre el editor. 

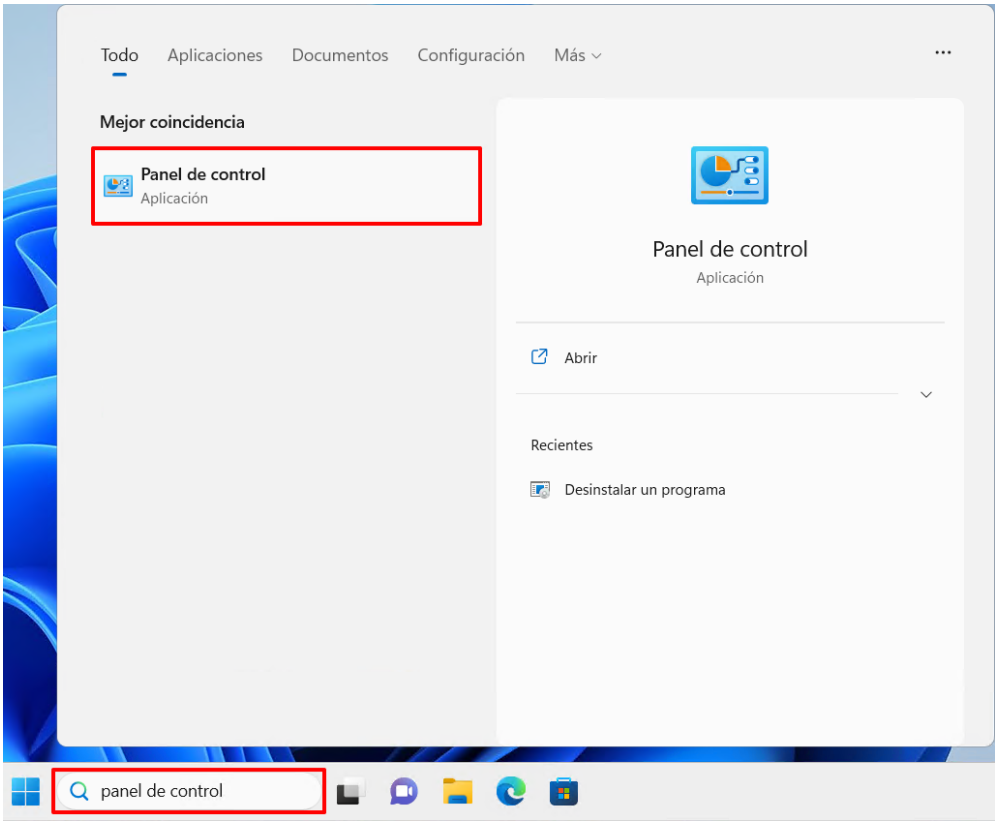
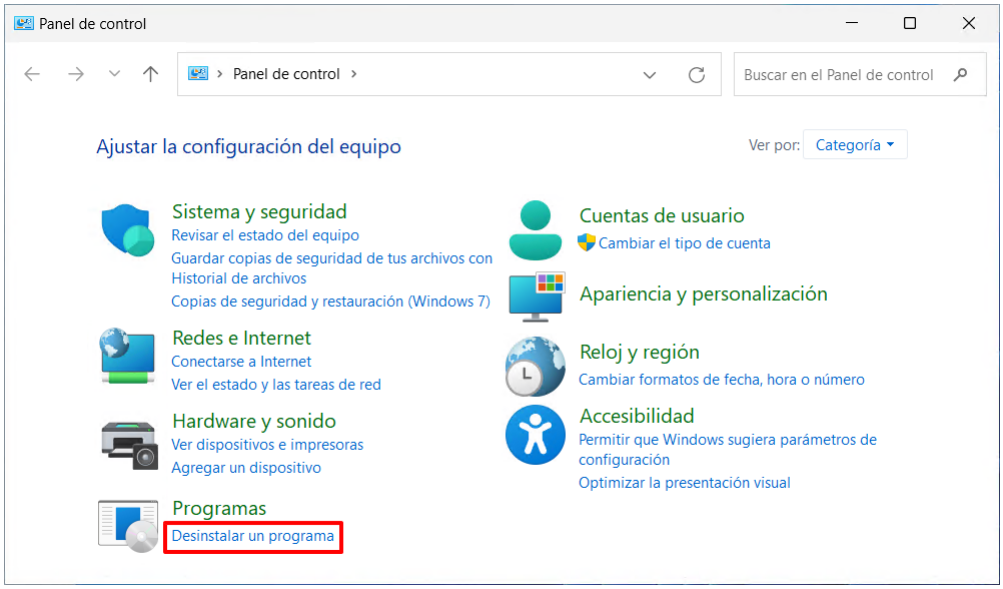
Paso	Descripción
23.	Diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “**CCN-STIC-599B23 Cliente Independiente – Desinstalar características.bat**” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
24.	Pulse cualquier tecla para continuar. 

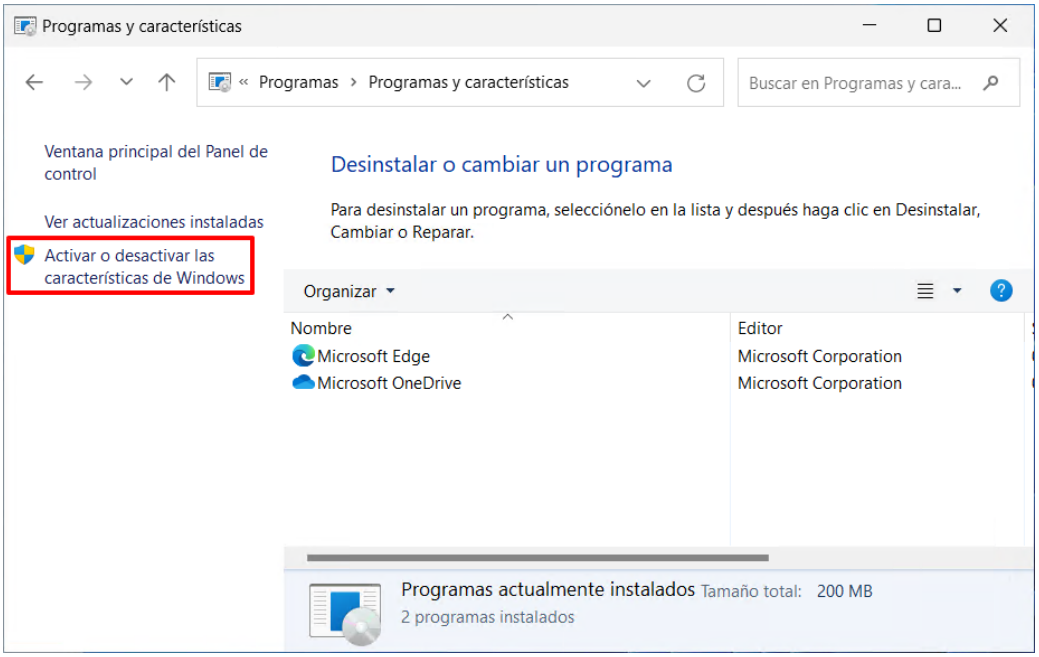
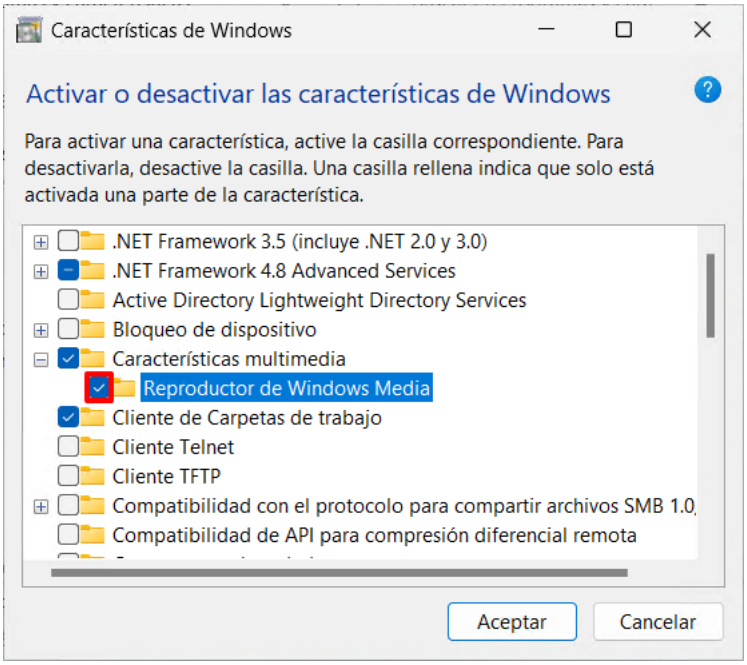
Paso	Descripción
25.	A continuación, se recopilará y mostrarán las características instaladas en el equipo. Deberá pulsar la tecla "Enter" para continuar y dar comienzo a la desinstalación de las características no necesarias. 
26.	El equipo se reiniciará a continuación para asegurar la adecuada desinstalación de características. Pulse de nuevo la tecla "Enter" para aceptar dicho reinicio, posteriormente pulse cualquier tecla para finalizar la ejecución del script. 
27.	Con esto se habrá finalizado la eliminación de características no necesarias en un equipo de tipo Cliente Independiente.

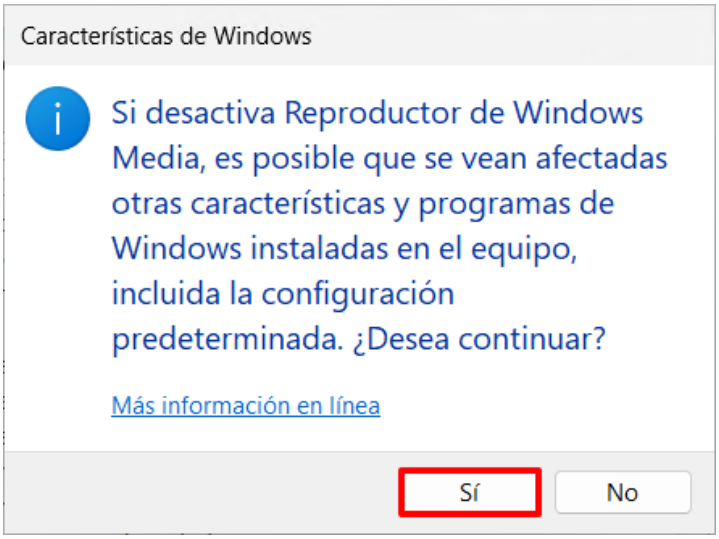
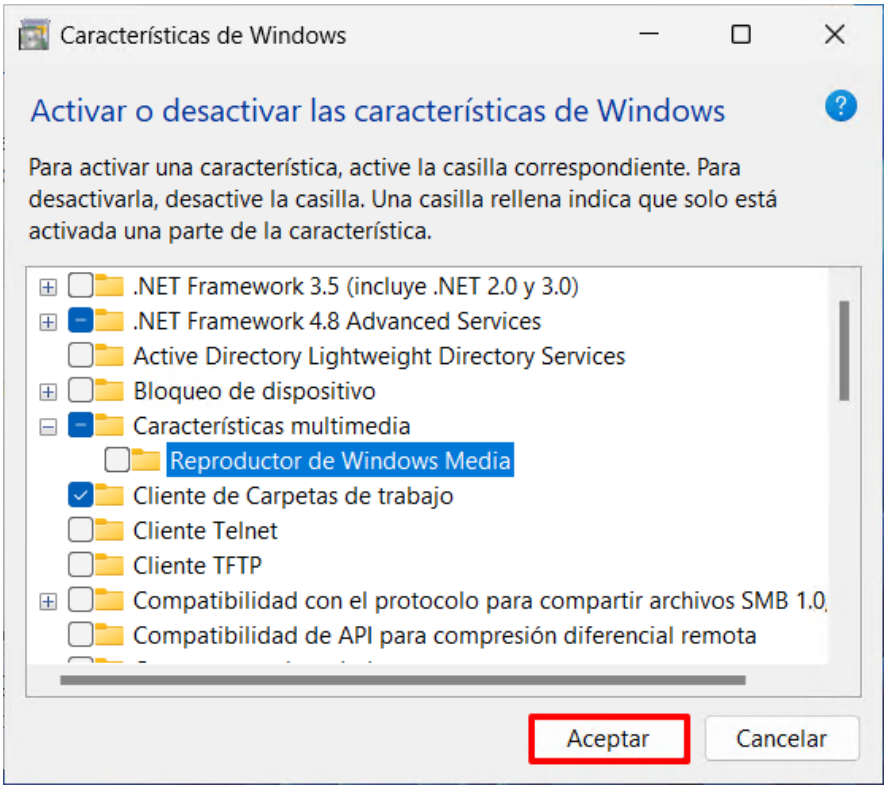
A continuación, se describen los pasos para realizar una desinstalación manual de características implementadas en un equipo de tipo Cliente Independiente.

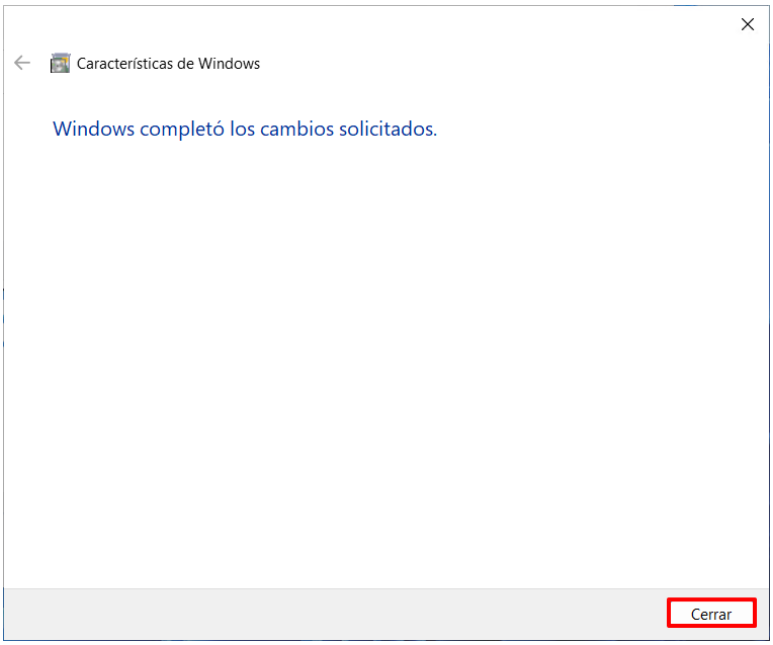
Nota: Para este ejemplo se desinstalará el Reproductor de Windows Media.

Paso	Descripción
28.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

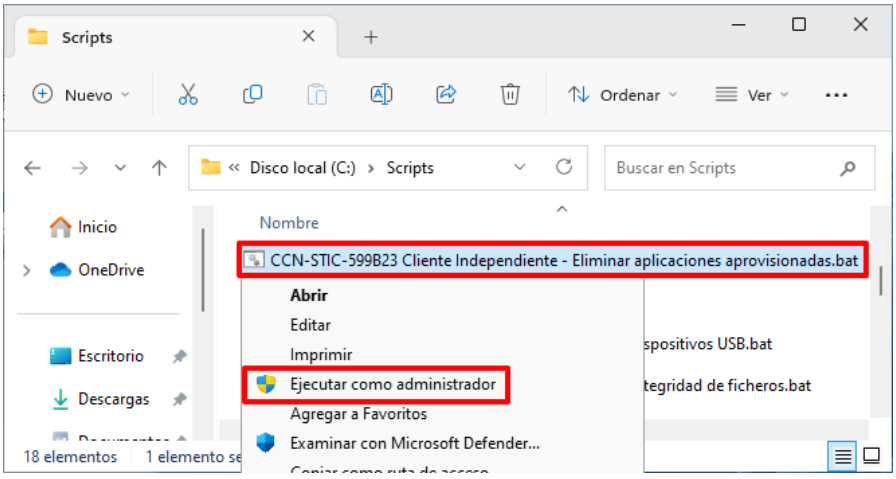
Paso	Descripción
29.	En el cuadro de búsqueda busque la aplicación “Panel de control” y una vez encontrada, haga clic sobre la misma. 
30.	En la parte inferior izquierda del “Panel de control”, pulse sobre “Desinstalar un programa” en el apartado “Programas”. 

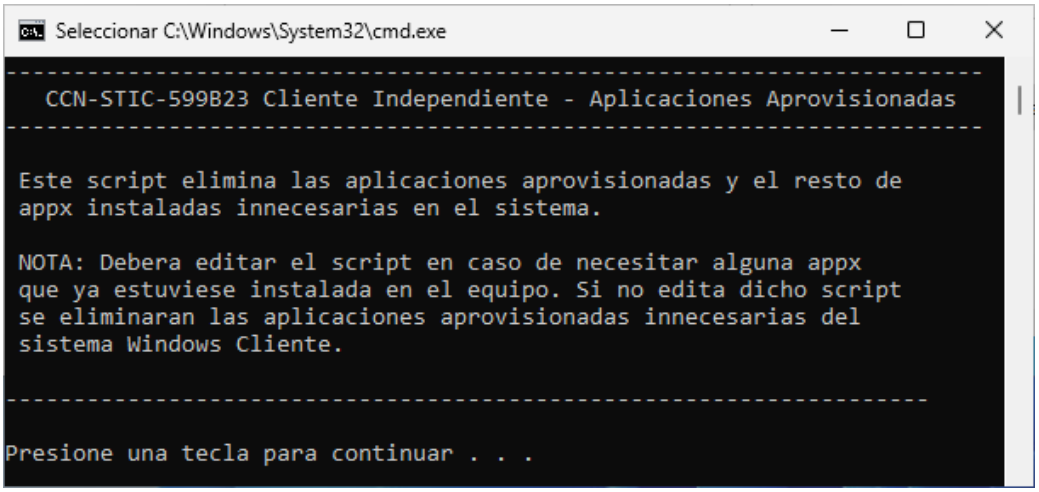
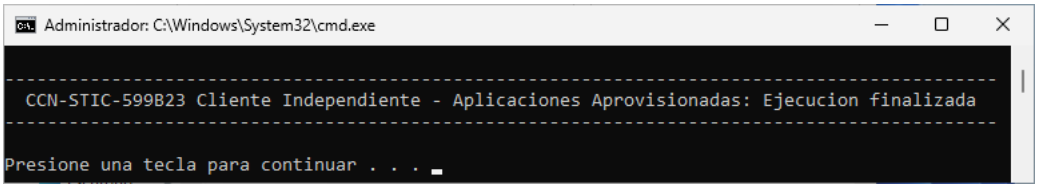
Paso	Descripción
31.	A continuación, seleccione la opción “Activar o desactivar las características de Windows” del menú ubicado en la parte izquierda de la ventana. 
32.	En la nueva ventana emergente, “Activar o desactivar las características de Windows”, identifique aquellas que no son necesarias y desmárquelas.  **Nota:** En este ejemplo se desinstala la característica “Reproductor de Windows Media”.

Paso	Descripción
33.	Pulse “Sí” ante el mensaje de advertencia. 
34.	Pulse sobre el botón “Aceptar” para continuar con la desinstalación. 

Paso	Descripción
35.	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. 

A continuación, se describen los pasos para realizar una desinstalación de las aplicaciones aprovisionadas implementadas en un Cliente Independiente.

Paso	Descripción
36.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
37.	A continuación, diríjase al directorio “C:\Scripts”, haga clic derecho sobre el fichero “**CCN-STIC-599B23 Cliente Independiente – Eliminar aplicaciones aprovisionadas.bat**” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 

Paso	Descripción
38.	Pulse cualquier tecla para comenzar con el proceso de desinstalación de aplicaciones aprovisionadas del sistema. 
39.	Espere a que finalice la ejecución y pulse una tecla para finalizar.  **Nota:** En caso de que el sistema muestre errores puede ignorarlos y continuar.

ANEXO B.2. 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.

Nota: Las configuraciones implementadas referentes a las Plantillas Administrativas del equipo se aplican mediante claves de registro, motivo por el cual al utilizar el Editor de directivas de grupo local no se podrán visualizar las directivas implementadas en la ejecución de los scripts.

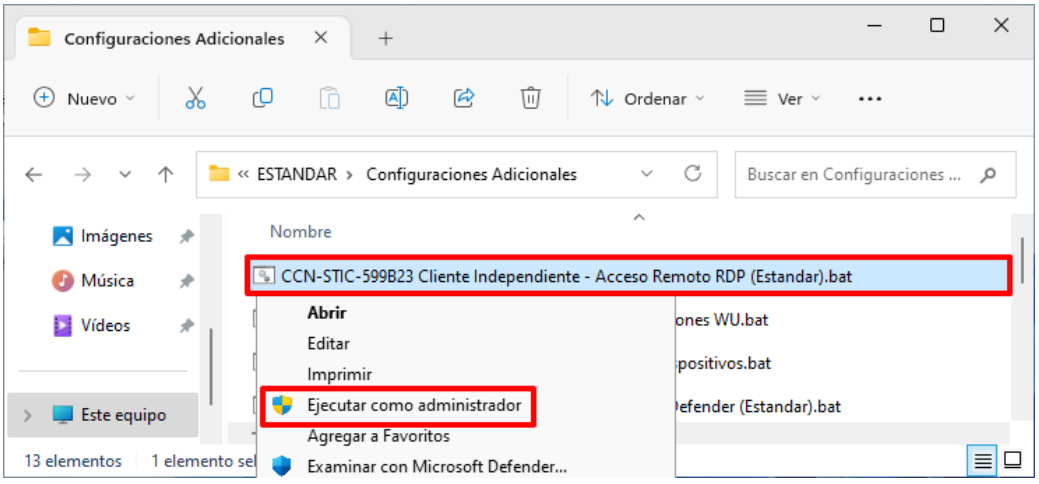
ANEXO B.2.1. ACCESO REMOTO

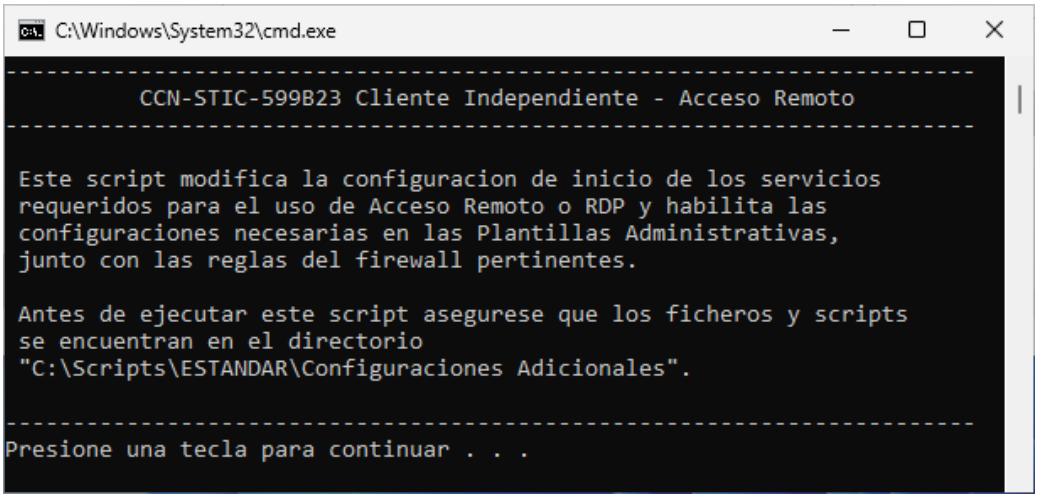
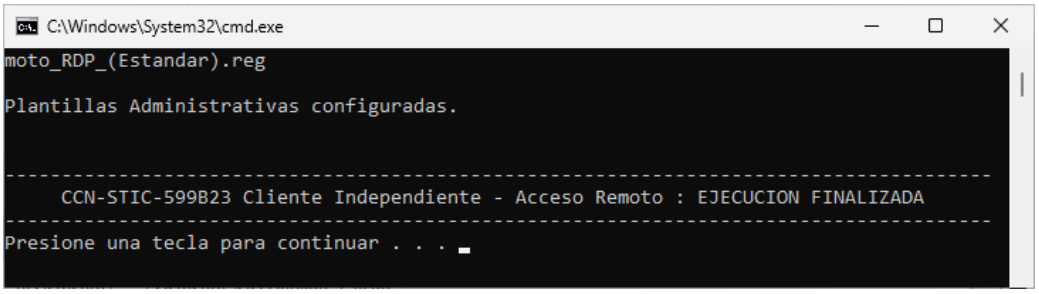
El objetivo del siguiente apartado tiene como misión establecer las configuraciones adecuadas sobre aquellos elementos a los que se les esté permitido el acceso remoto por medio de los elementos nativos de Windows. En este caso se hace referencia a Remote Desktop Connection (RDP).

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 del directorio** donde se ubican las configuraciones de seguridad, deberá seleccionar aquel **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]\Configuraciones Adicionales**", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Acceso Remoto RDP ([TIPO DE PERFILADO]).bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Seleccione el directorio acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

Paso	Descripción
3.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración de Acceso Remoto. 
4.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

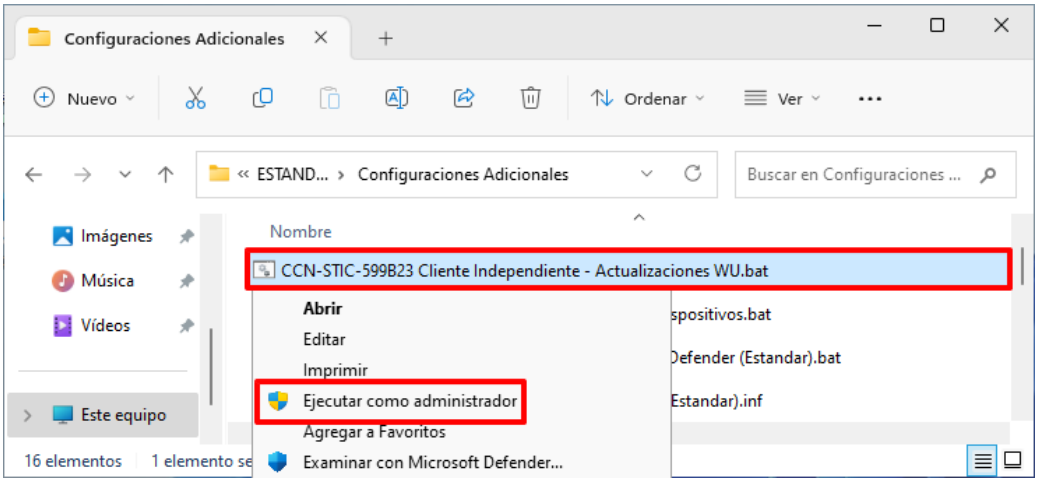
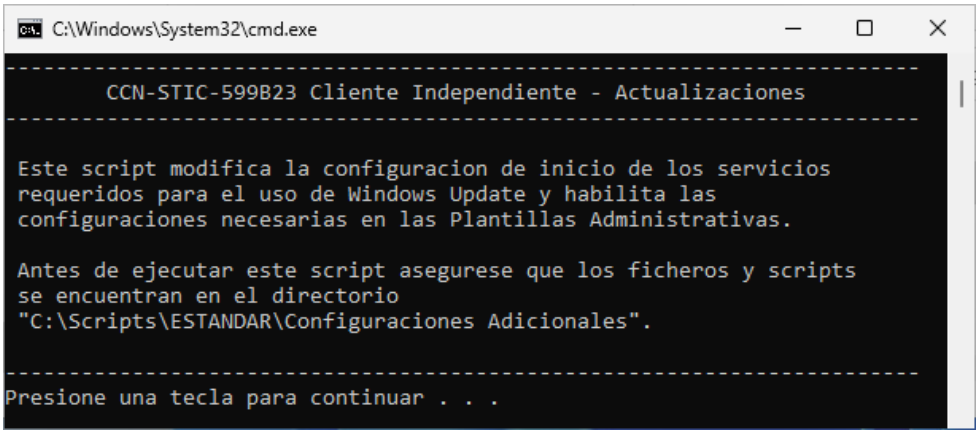
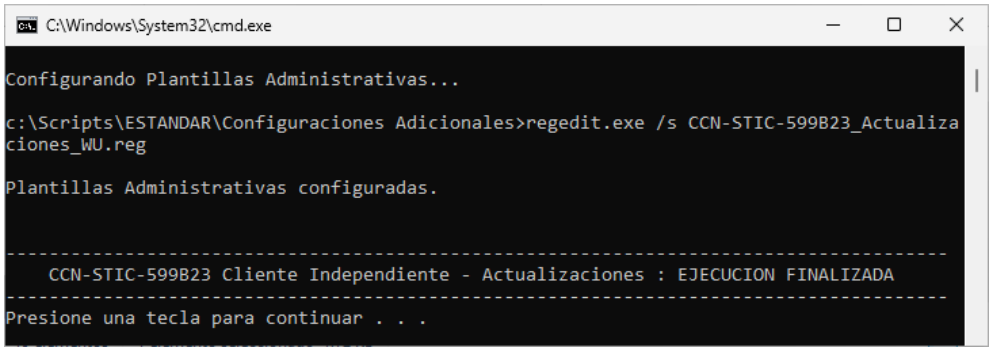
ANEXO B.2.2. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

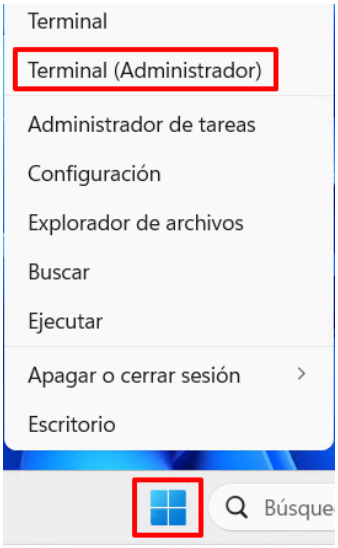
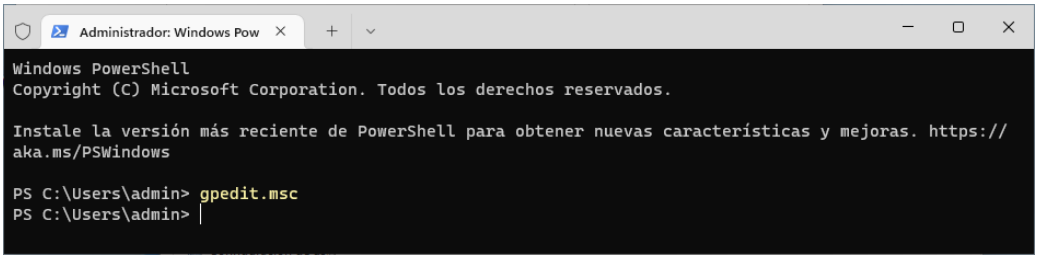
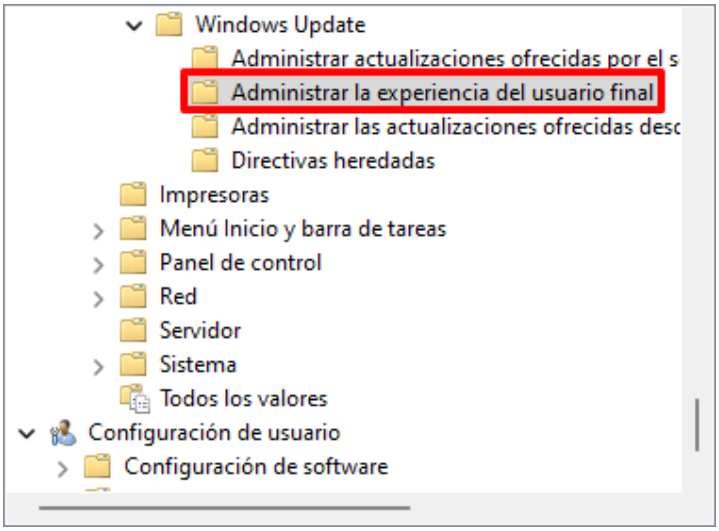
A través de la siguiente sección y su paso a paso, se definirán las acciones para dotar a los sistemas operativos Windows Cliente de un servicio de actualizaciones automáticas completamente configurado.

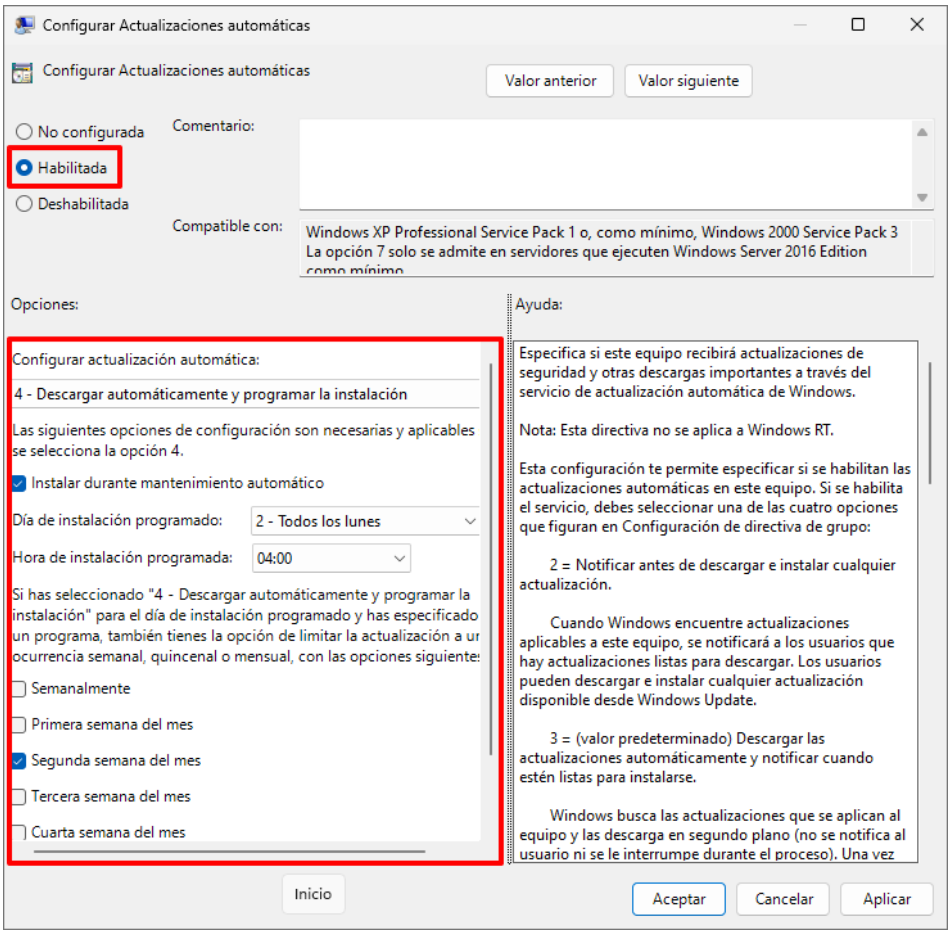
Nota: Si en su organización ya dispone de un producto o servicio para la actualización y mantenimiento del sistema operativo, como el servicio de WSUS, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

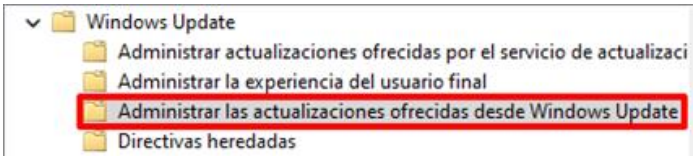
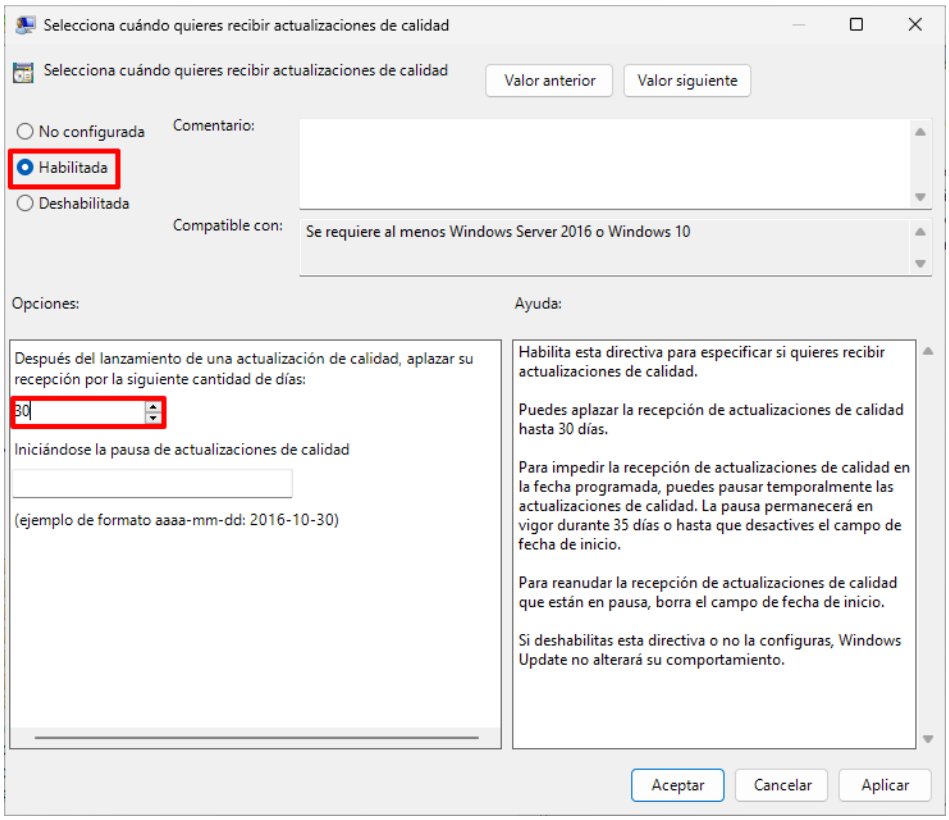
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección del directorio** donde se ubican las configuraciones de seguridad, deberá seleccionar aquel **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

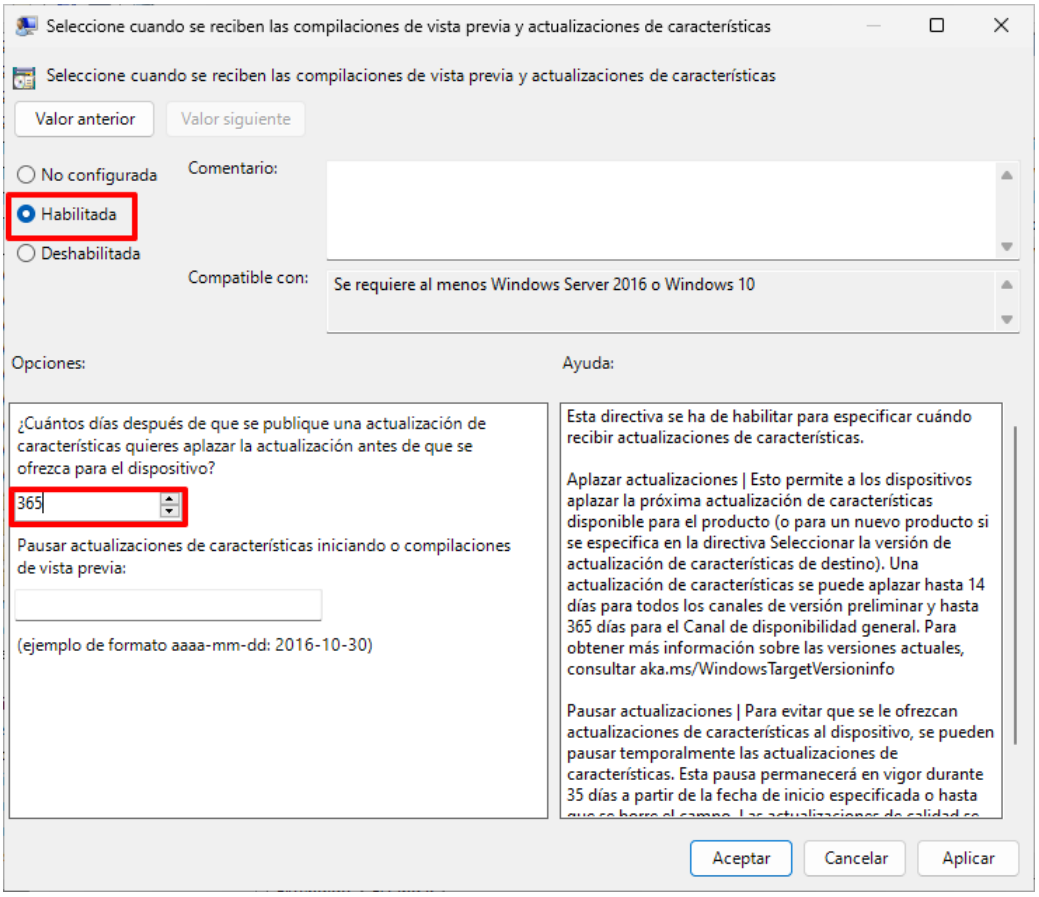
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

Paso	Descripción
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]\Configuraciones Adicionales**", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Actualizaciones WU.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Seleccione el directorio acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
3.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración de actualizaciones mediante Windows Update. 
4.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

Paso	Descripción
5.	Posteriormente, haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
6.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
7.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Windows Update → Administrar la experiencia del usuario final"** 

Paso	Descripción
8.	En el panel derecho identifique y haga doble clic sobre la directiva "**Configurar Actualizaciones automáticas**". Pulse sobre "Habilitada" y evalúe y adapte la configuración acorde a las necesidades de su organización.  **Nota:** Al configurarse la presente directiva mediante claves de registro, esta no se muestra con los valores configurados en el Editor de directivas de grupo local. Las medidas configuradas mediante los ficheros de configuración son las siguientes: - Configurar actualización automática: 4- Descargar automáticamente y programar la instalación - Instalar durante mantenimiento automático - Día de instalación programado: 2 - Todos los lunes - Hora de instalación programada: 4:00 - Segunda semana del mes - Instalar actualizaciones de otros productos de Microsoft Si existe la necesidad por parte de la organización en establecer otros valores, deberá seguir el proceso defino en el presente punto, habilitando y configurando la directiva. En caso contrario, puede seguir en el siguiente paso.

Paso	Descripción
9.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Windows Update → Administrar las actualizaciones ofrecidas desde Windows Update".** 
10.	En el panel derecho haga doble clic sobre la directiva: **"Selecciona cuándo quieres recibir actualizaciones de calidad"**. Pulse sobre "Habilitada" y edite el número de días acorde a las necesidades de su organización.  **Nota:** Al configurarse la presente directiva mediante claves de registro, esta no se muestra con los valores configurados en el Editor de directivas de grupo local. Las medidas configuradas mediante los ficheros de configuración son las siguientes: - Después del lanzamiento de una actualización de calidad, aplazar su recepción por la siguiente cantidad de días: 30 Si existe la necesidad por parte de la organización en establecer otros valores, deberá seguir el proceso defino en el presente punto, habilitando y configurando la directiva. En caso contrario, puede seguir en el siguiente paso. 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.

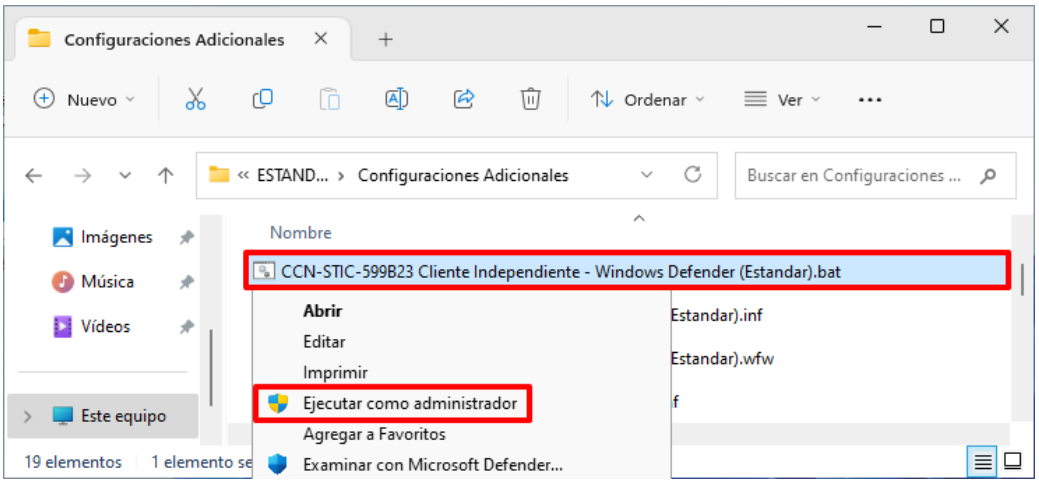
Paso	Descripción
11.	De forma análoga a lo realizado en los pasos anteriores, haga doble clic sobre la directiva **"Seleccione cuando se reciben las compilaciones de vista previa y actualizaciones de características"**. Pulse sobre "Habilitada" y edite el número de días acorde a las necesidades de su organización.  **Nota:** Al configurarse la presente directiva mediante claves de registro, esta no se muestra con los valores configurados en el Editor de directivas de grupo local. Las medidas configuradas mediante los ficheros de configuración son las siguientes: - ¿Cuántos días después de que se publique una actualización de características quieres aplazar la actualización antes de que se ofrezca para el dispositivo?: 365 Si existe la necesidad por parte de la organización en establecer otros valores, deberá seguir el proceso defino en el presente punto, habilitando y configurando la directiva. En caso contrario, puede seguir en el siguiente paso. 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.
12.	Cierre la ventana "Editor de directivas de grupo local".

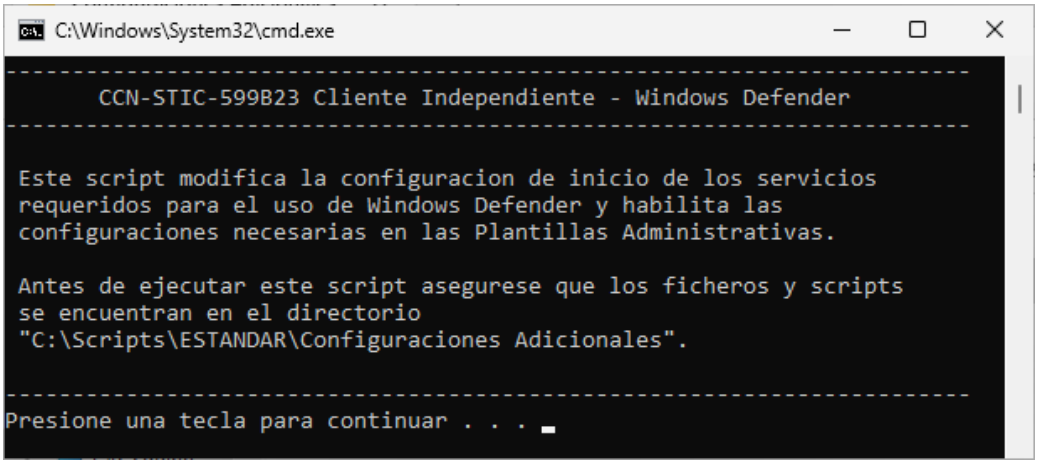
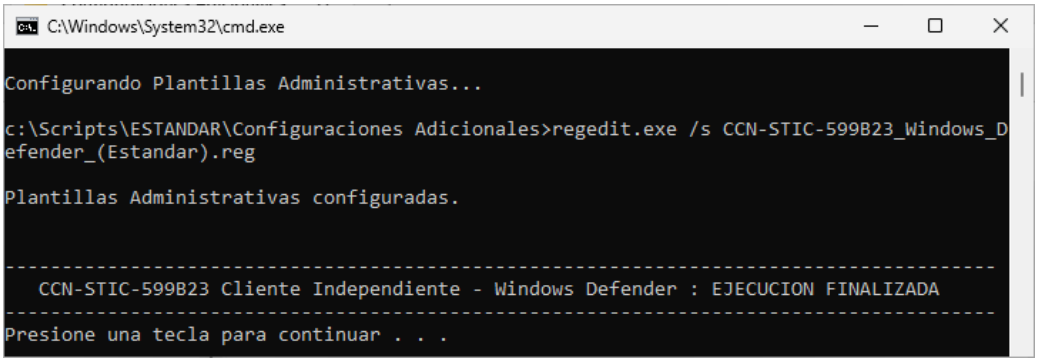
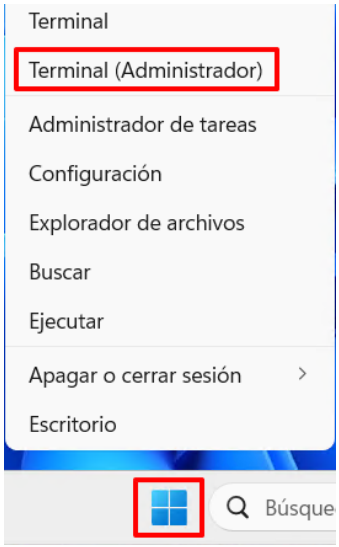
ANEXO B.2.3. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

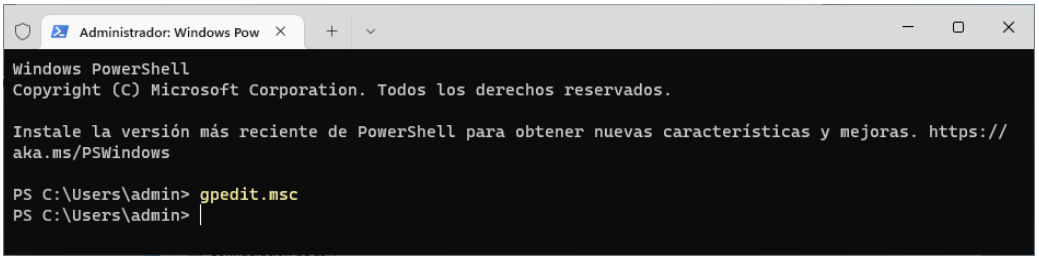
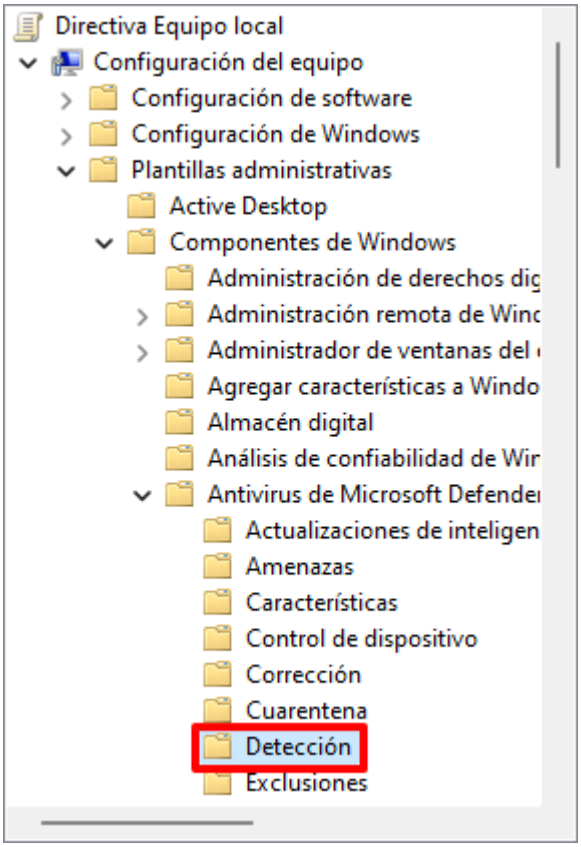
La sección y los pasos descritos a continuación, permiten establecer la configuración sobre el software frente a protección de código dañino incluido por defecto en los sistemas operativos Windows Cliente.

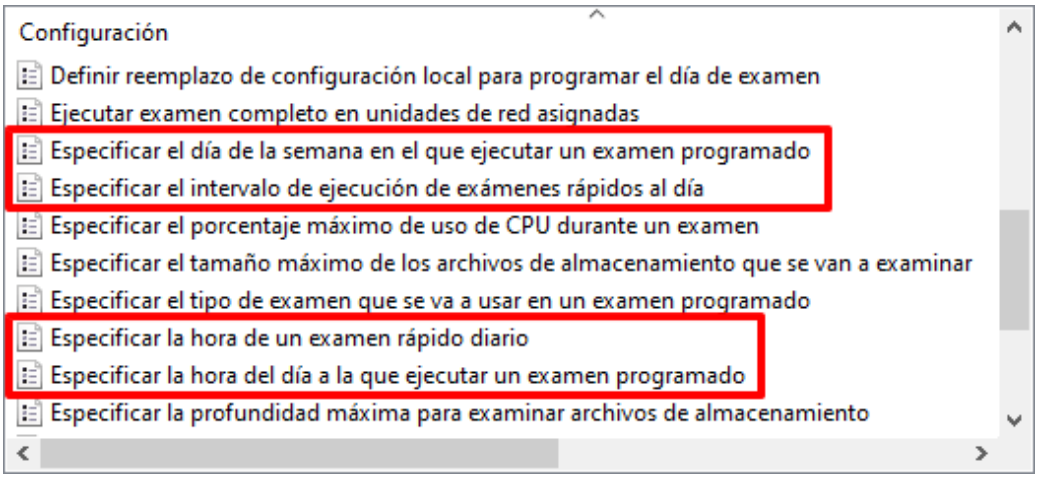
Nota: Si en su organización ya dispone de un producto o servicio frente a código dañino en el sistema operativo, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

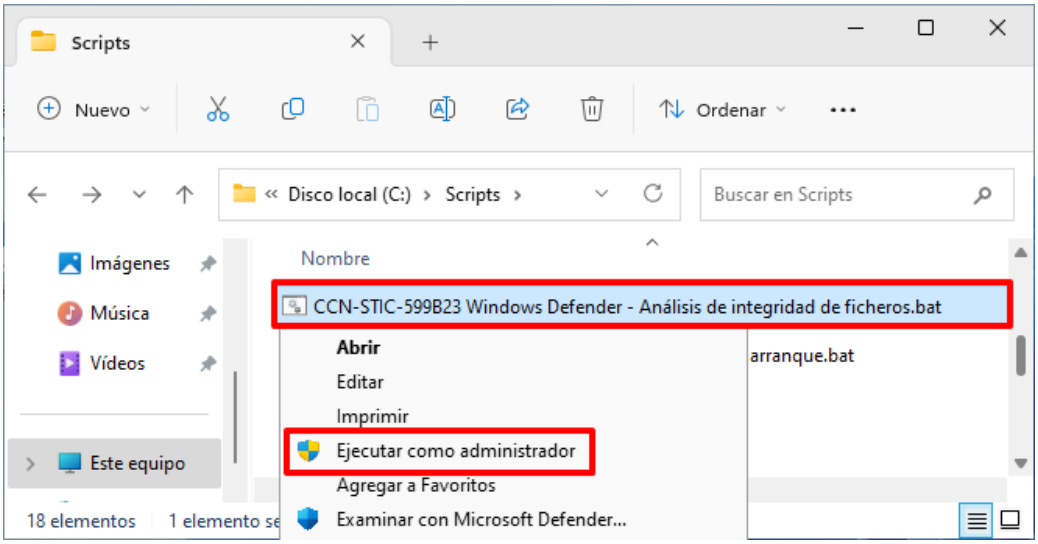
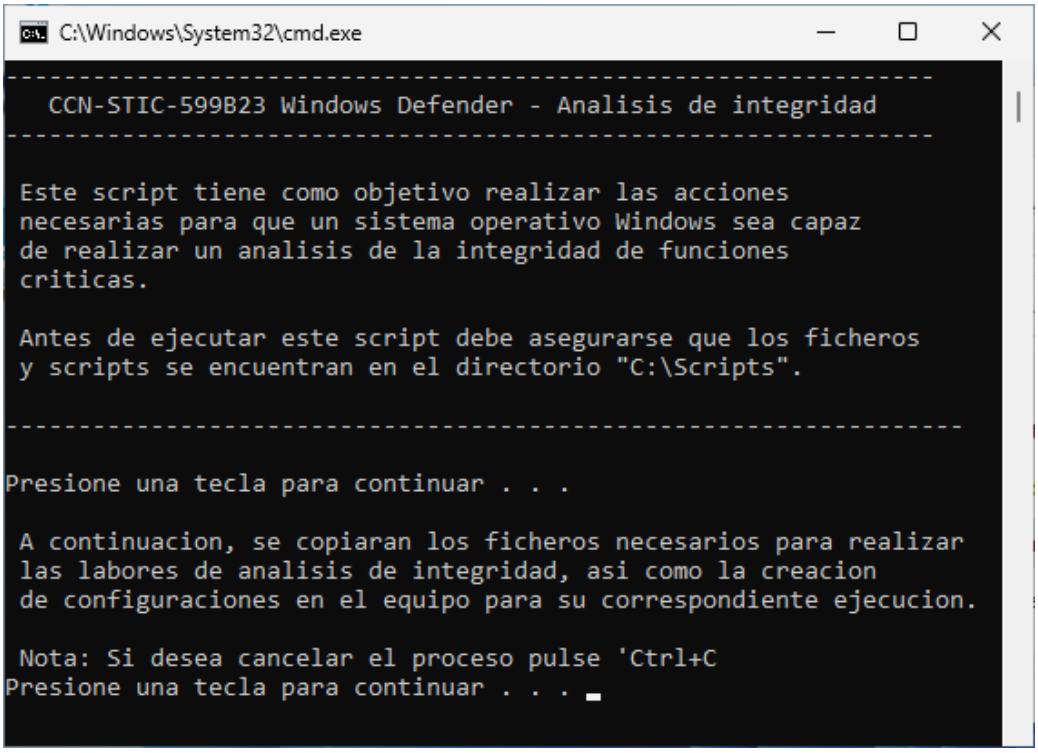
El **presente paso a paso** establece la **configuración de seguridad** para un **perfilado Estándar**. En el momento de **selección del directorio** donde se ubican las configuraciones de seguridad, deberá seleccionar aquel **acorde a su perfilado** (Estándar, Uso Oficial o Materias Clasificadas).

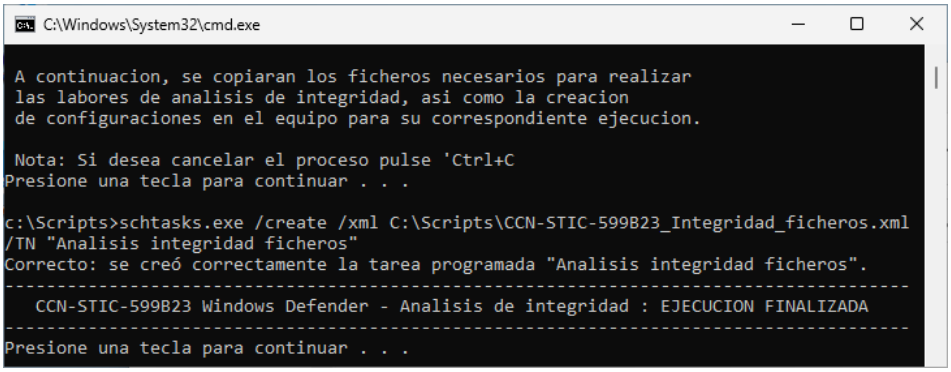
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]\Configuraciones Adicionales**", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Windows Defender ([TIPO DE PERFILADO]).bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Seleccione el directorio acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".

Paso	Descripción
3.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración del antivirus Windows Defender. 
4.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 
5.	Posteriormente, haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 

Paso	Descripción
6.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
7.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Detección"** 

Paso	Descripción
8.	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  **Nota:** Al configurarse las presentes directivas mediante claves de registro, estas no se muestran con los valores configurados en el Editor de directivas de grupo local. Las medidas configuradas mediante los ficheros de configuración son las siguientes: - 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]) Si existe la necesidad por parte de la organización en establecer otros valores, deberá habilitar y configurar las directivas. En caso contrario, puede seguir en el siguiente paso.
9.	Cierre la ventana “Editor de directivas de grupo local”.

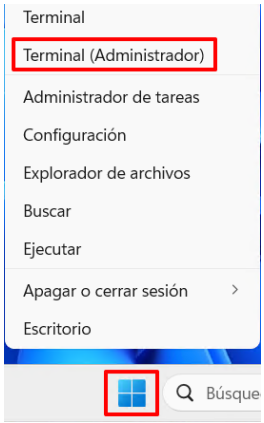
Paso	Descripción
10.	A continuación, diríjase al directorio “C:\Scripts”, y haga clic derecho sobre el fichero “**CCN-STIC-599B23 Windows Defender – Análisis de integridad de ficheros.bat**” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
11.	Pulse una tecla para continuar.
12.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 

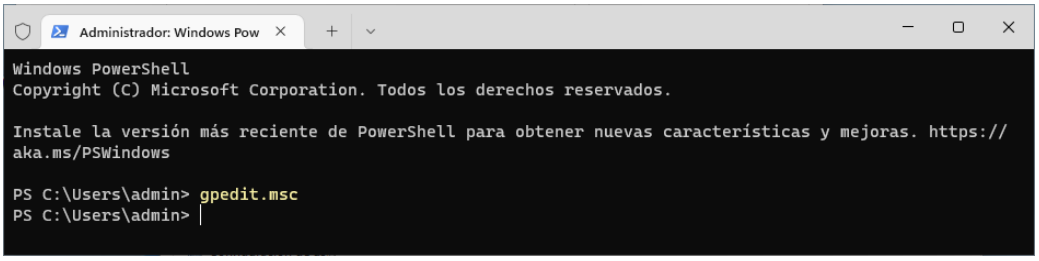
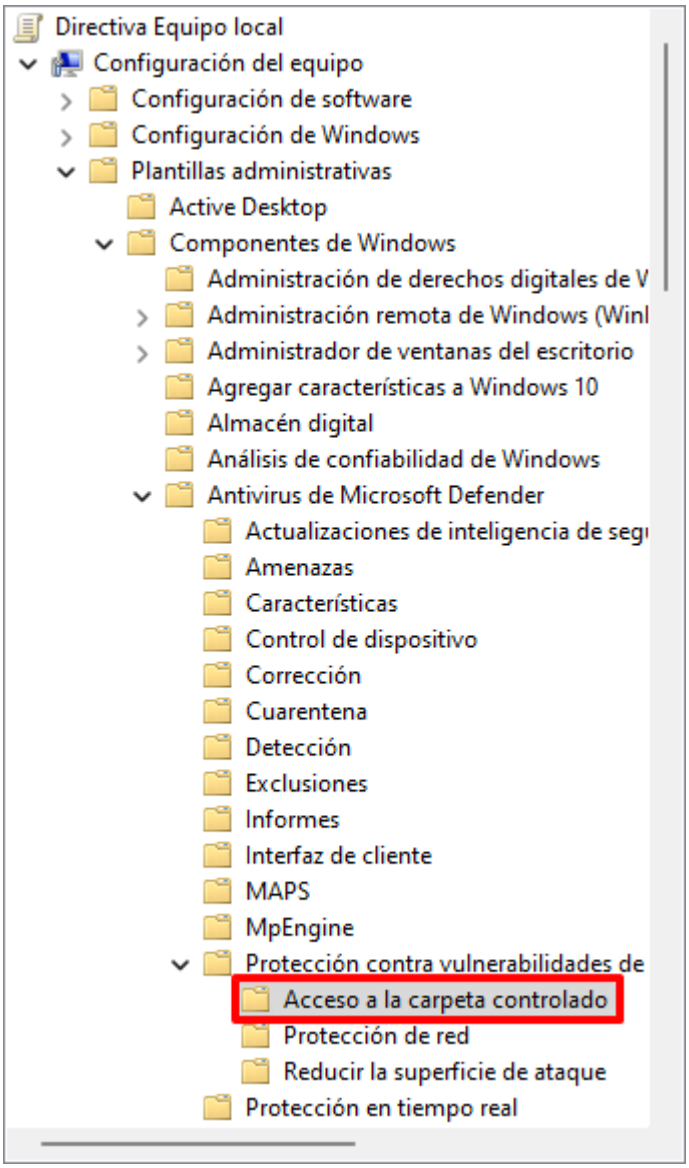
Paso	Descripción
13.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
14.	Con esto habrá configurado el equipo para que se realice una comprobación de la integridad de ficheros esenciales del sistema operativo. **Nota:** Podrá editar la tarea programa generada con el objetivo de incluir cualquier fichero que desee analizar y comprobar.

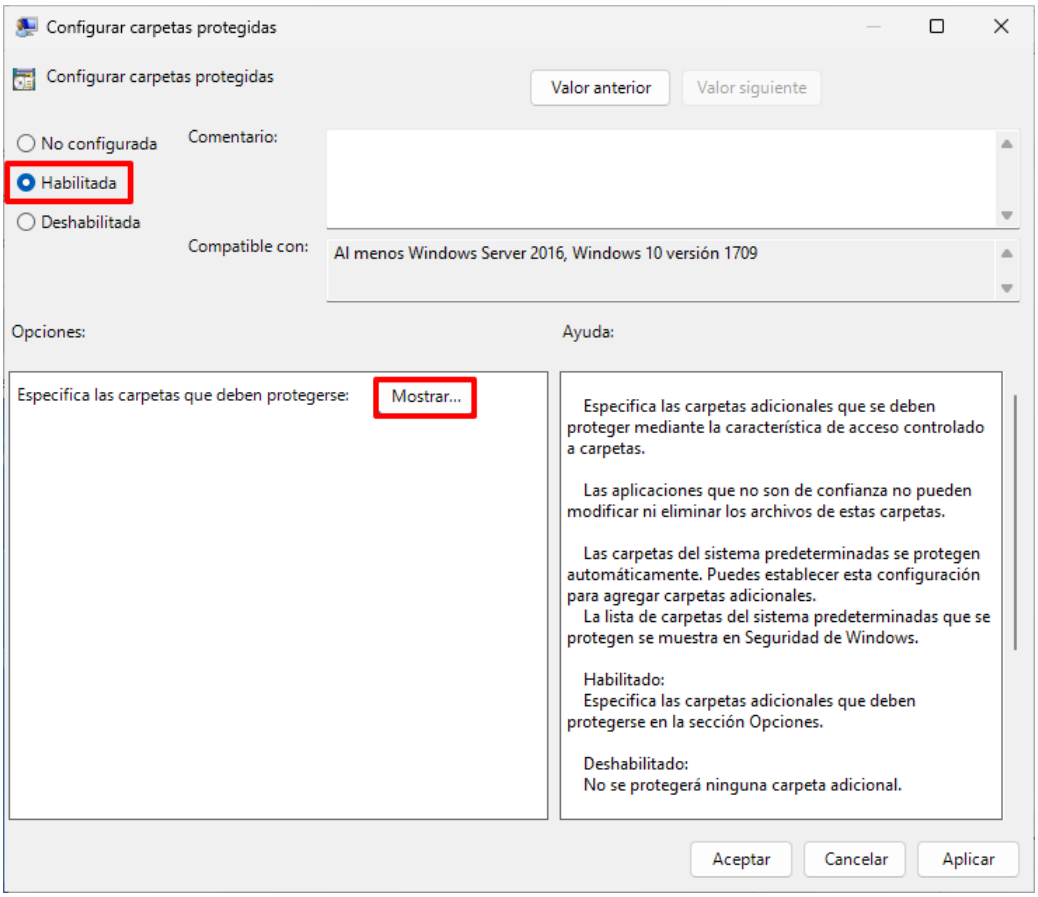
ANEXO B.2.3.1. PROTECCIÓN FRENTE A CÓDIGO DAÑINO (USO OFICIAL – MATERIAS CLASIFICADAS)

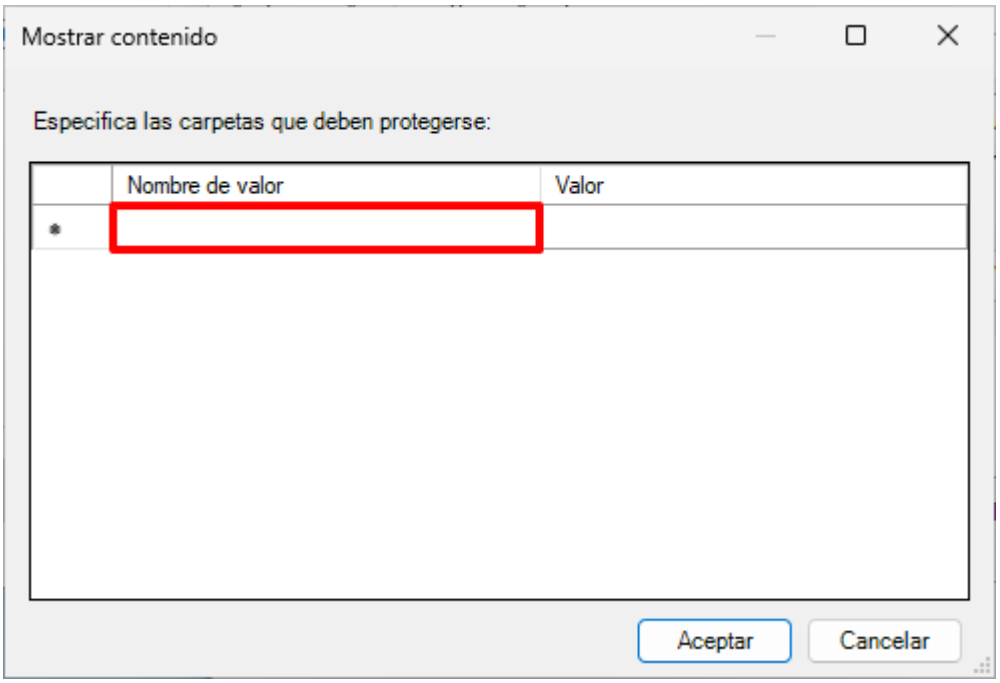
El presente apartado amplia las configuraciones necesarias aplicables con el objetivo de cumplir los requisitos en el caso de los perfiles USO OFICIAL o MATERIAS CLASIFICADAS.

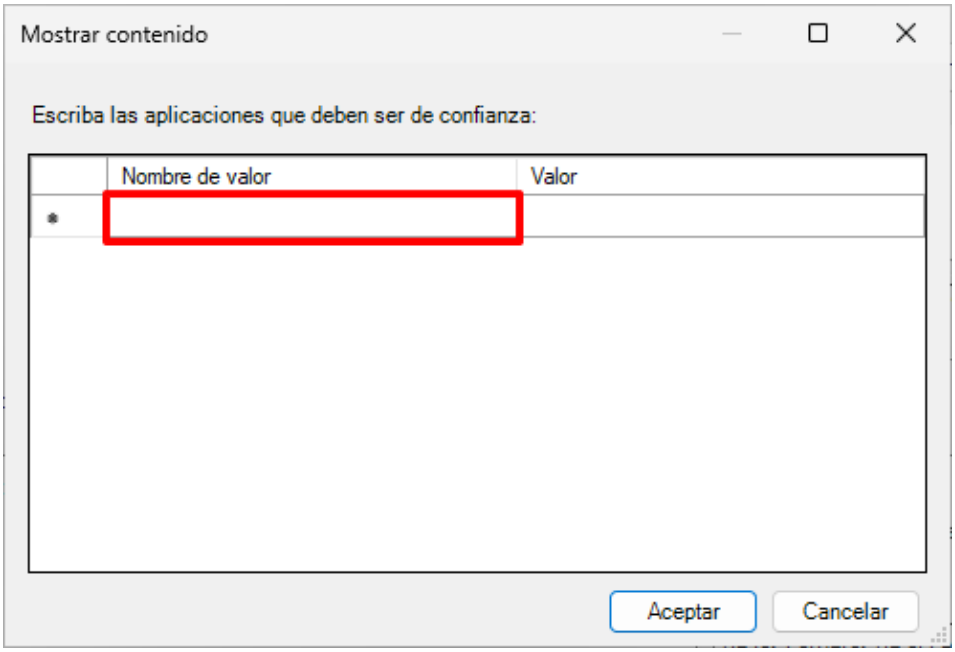
Las configuraciones definidas bajo el presente apartado tratan de impedir las modificaciones no autorizadas bajo directorios protegidos por el software contra código dañino, evitando de este modo la infección contra ransomware.

Paso	Descripción
15.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
16.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 

Paso	Descripción
17.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
18.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Componentes de Windows → Antivirus de Microsoft Defender → Protección contra vulnerabilidades de seguridad de Microsoft Defender → Acceso a la carpeta controlado"** 

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

Paso	Descripción
20.	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
21.	De forma análoga a lo realizado en los pasos anteriores, haga doble clic sobre la directiva **“Configurar aplicaciones permitidas”** y a continuación pulse sobre “Habilitada” y posteriormente sobre el botón “Mostrar…”.

Paso	Descripción
22.	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.
23.	Cierre la ventana “Editor de directivas de grupo local”.

ANEXO B.2.3.2. 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:

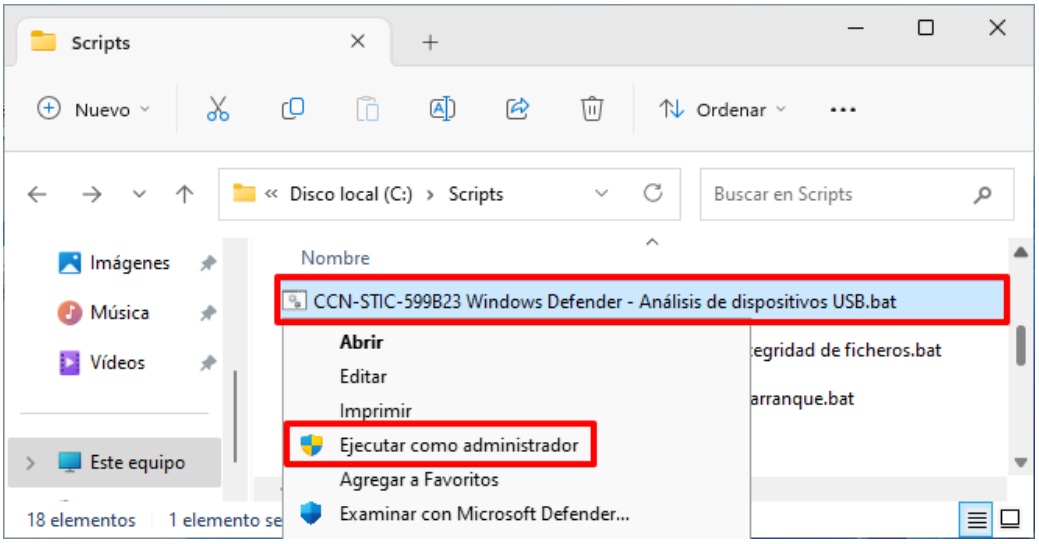
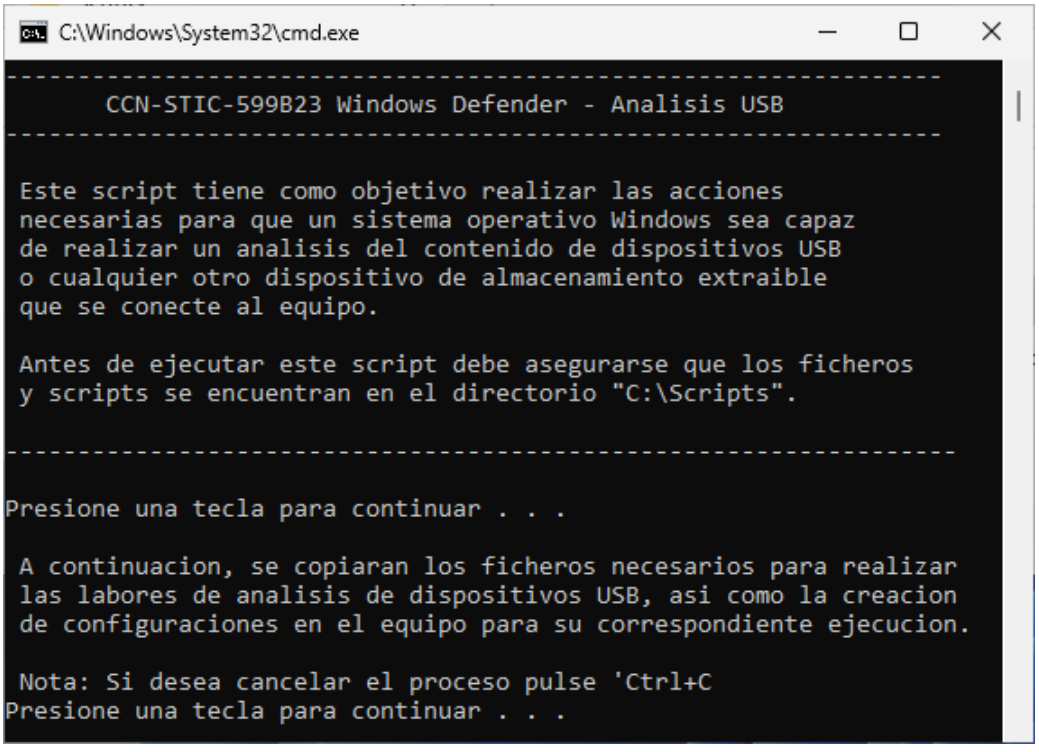
a) Análisis de dispositivos de almacenamiento extraíble cuando estos se conectan al equipo.

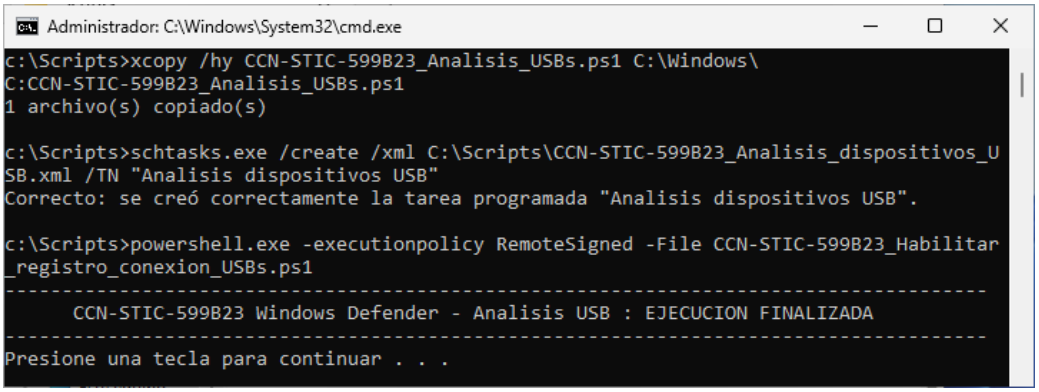
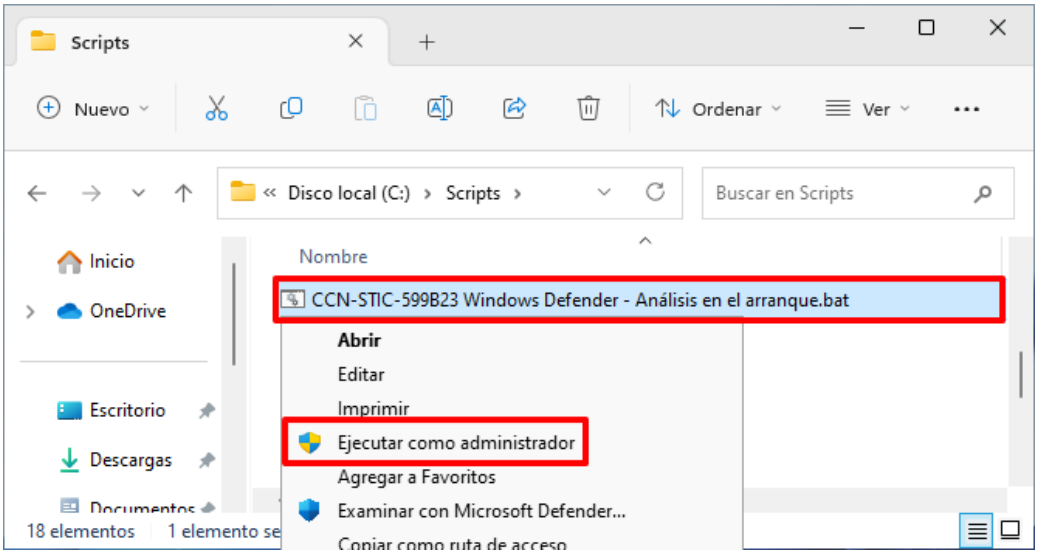
b) Análisis del sistema operativo en el arranque del sistema.

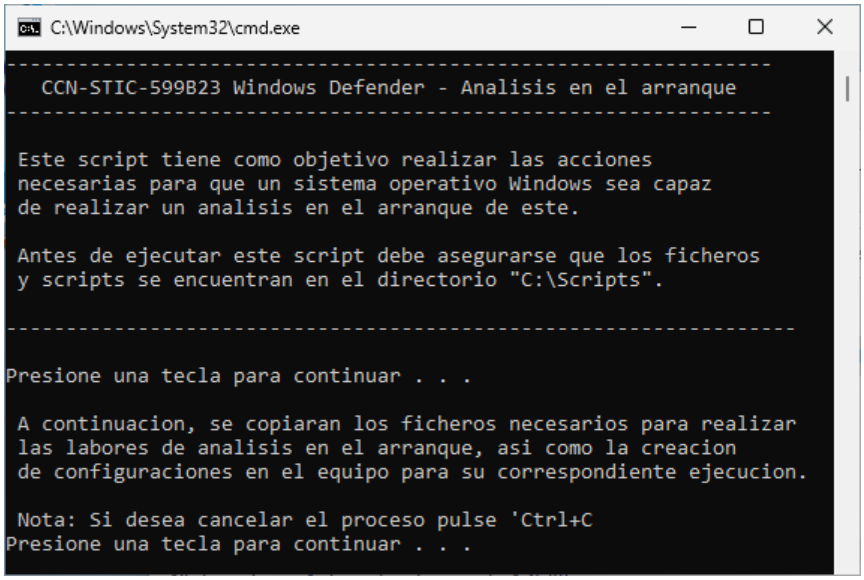
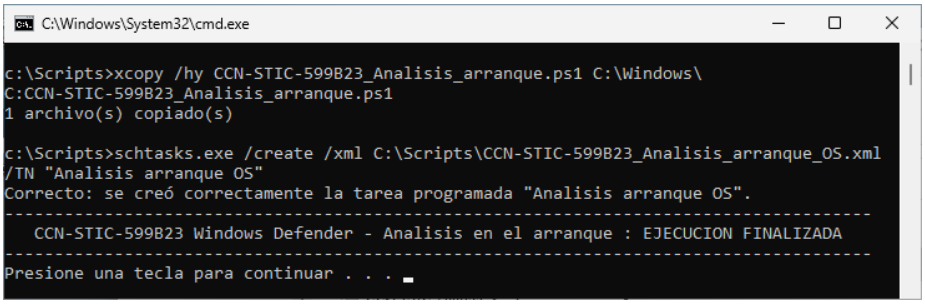
No se considera de aplicación las configuraciones del presente apartado si no se han aplicado el resto de configuraciones de esta herramienta según el punto “ANEXO A.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO”.

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
24.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
25.	Diríjase al directorio “C:\Scripts”, y haga clic derecho sobre el fichero “**CCN-STIC-599B23 Windows Defender – Análisis de dispositivos USB.bat**” y seleccione la opción del menú contextual “Ejecutar como Administrador”. 
26.	Pulse una tecla para continuar.
27.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 

Paso	Descripción
28.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
29.	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.
30.	De nuevo, en el directorio "**C:\Scripts" haga clic derecho sobre el fichero "CCN-STIC-599B23 Windows Defender – Análisis en el arranque.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
31.	Pulse una tecla para continuar.

Paso	Descripción
32.	A continuación, se le informará de las acciones que realizará el script. Pulse de nuevo una tecla para continuar. 
33.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
34.	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.

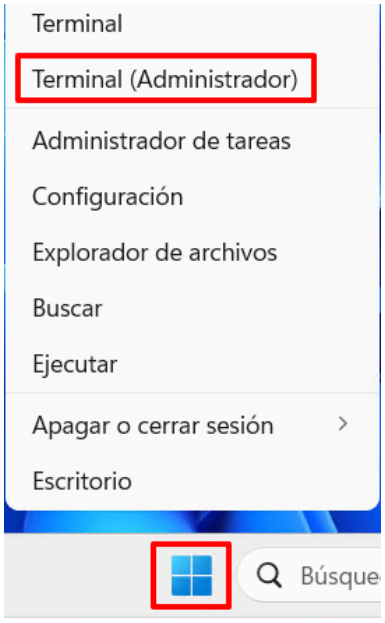
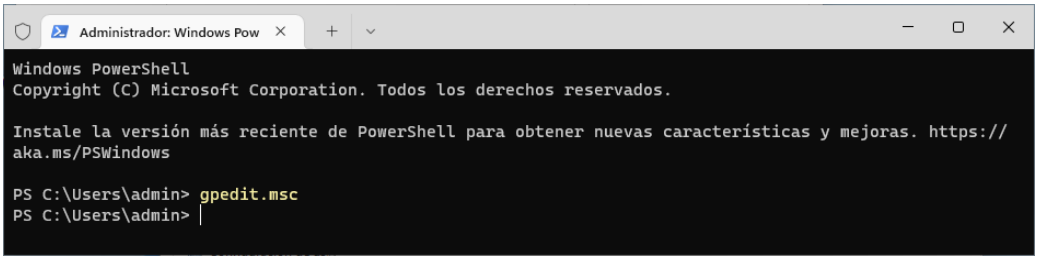
ANEXO B.2.4. PROTECCIÓN DE LA INTEGRIDAD Y LA AUTENTICIDAD

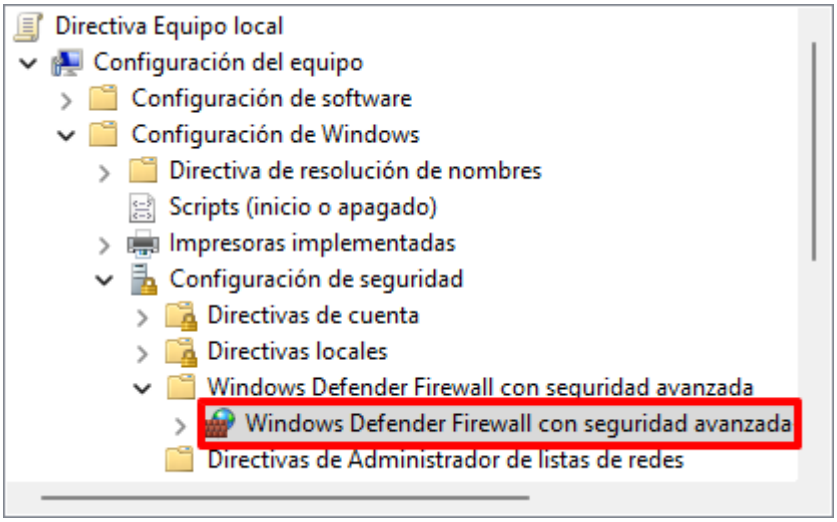
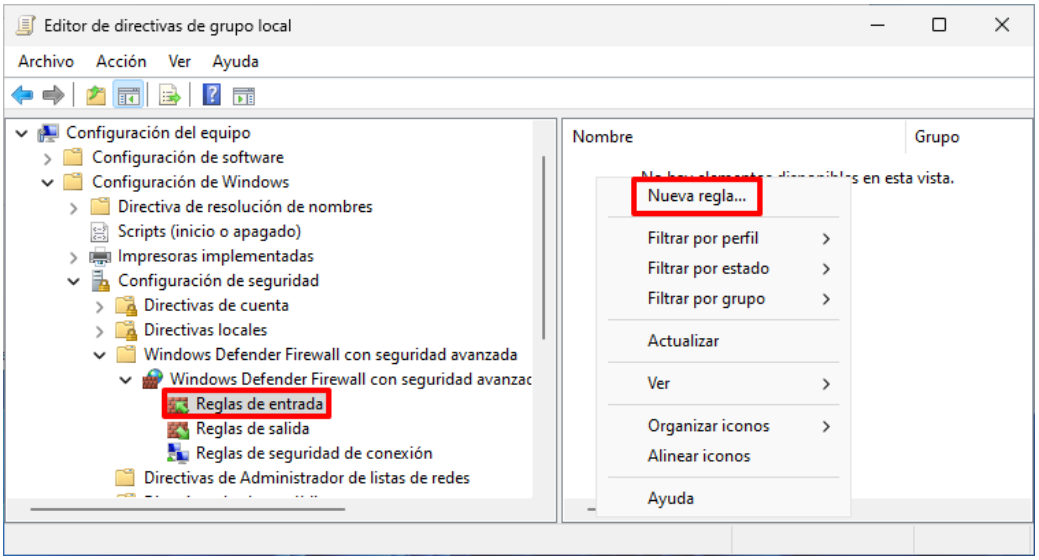
El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación del cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los equipos tipo Cliente Independiente.

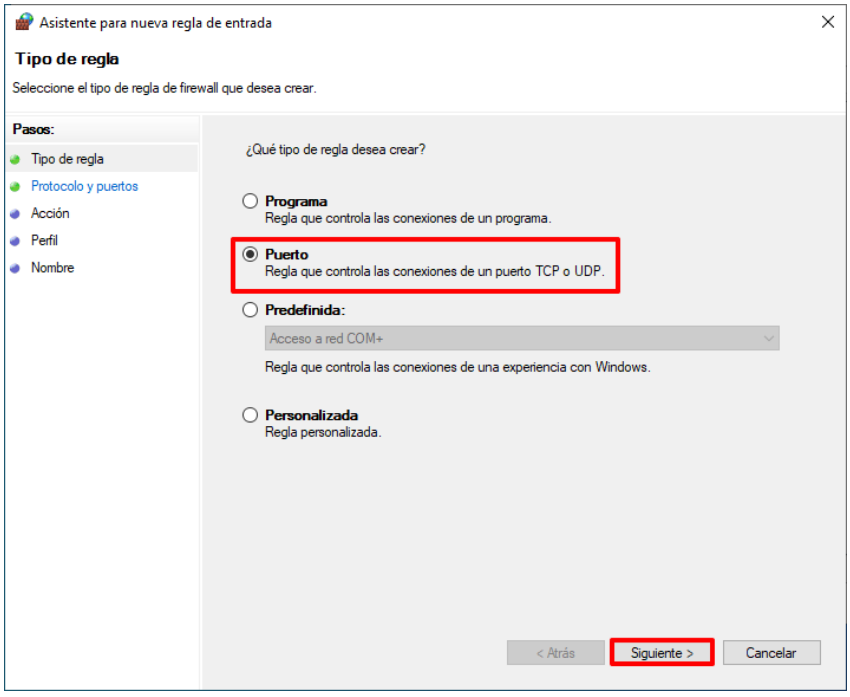
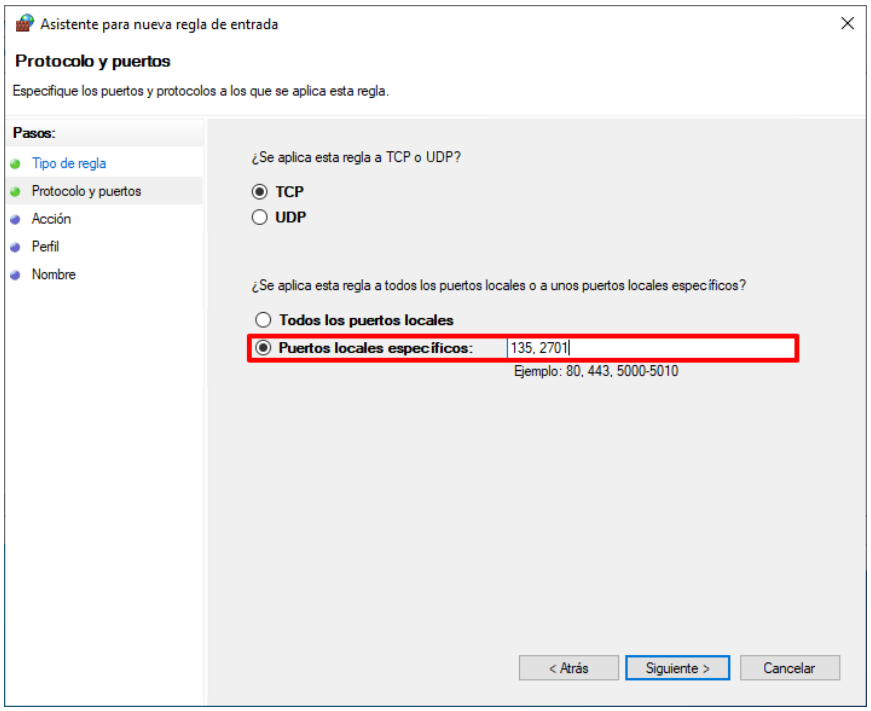
Debe tenerse en consideración que la implementación de un firewall de cliente dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que éste utilice dl entorno. No se tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, en un cliente que se utilice únicamente para usar Microsoft Office que un cliente utilizado para la compartición de unidades en red.

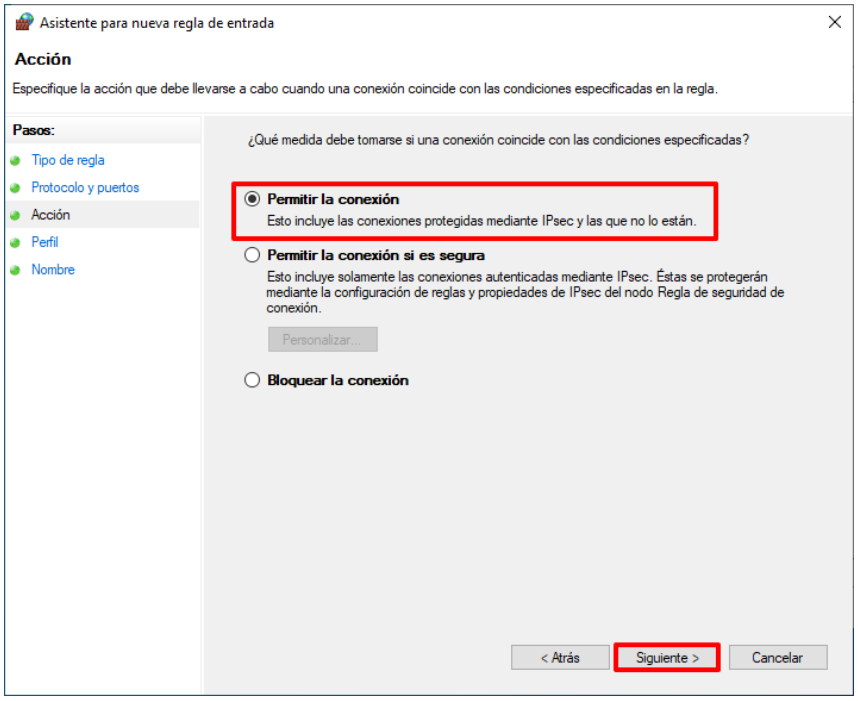
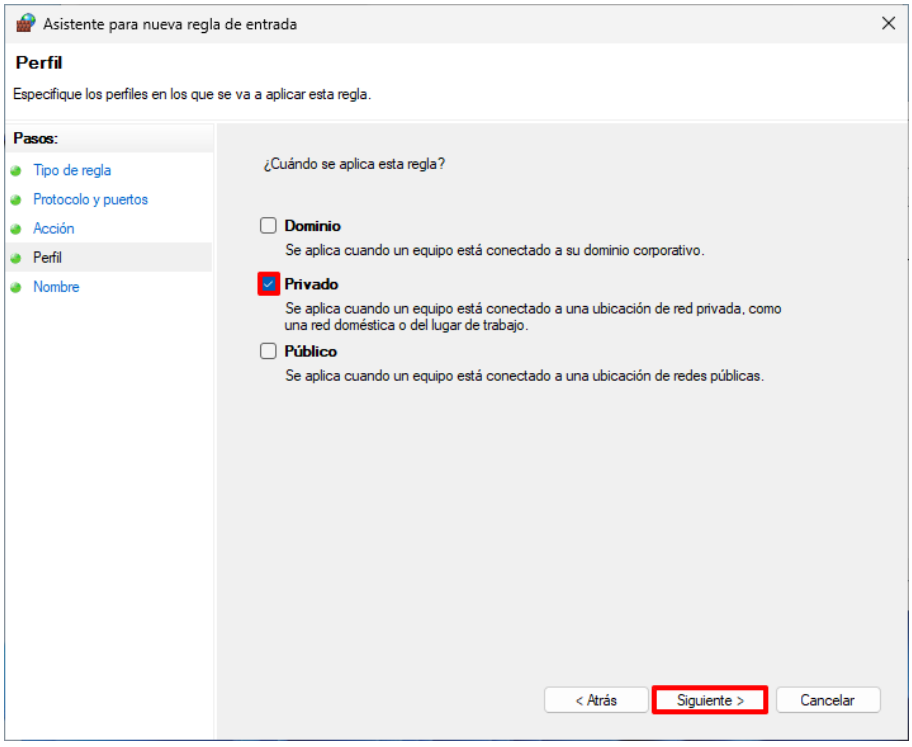
Nota: En el presente ejemplo se va a crear una regla de entrada para la configuración del cortafuegos para un cliente independiente que necesita que Configuration Manager pueda controlarlo remotamente, utilizando los puertos 135 y 2701.

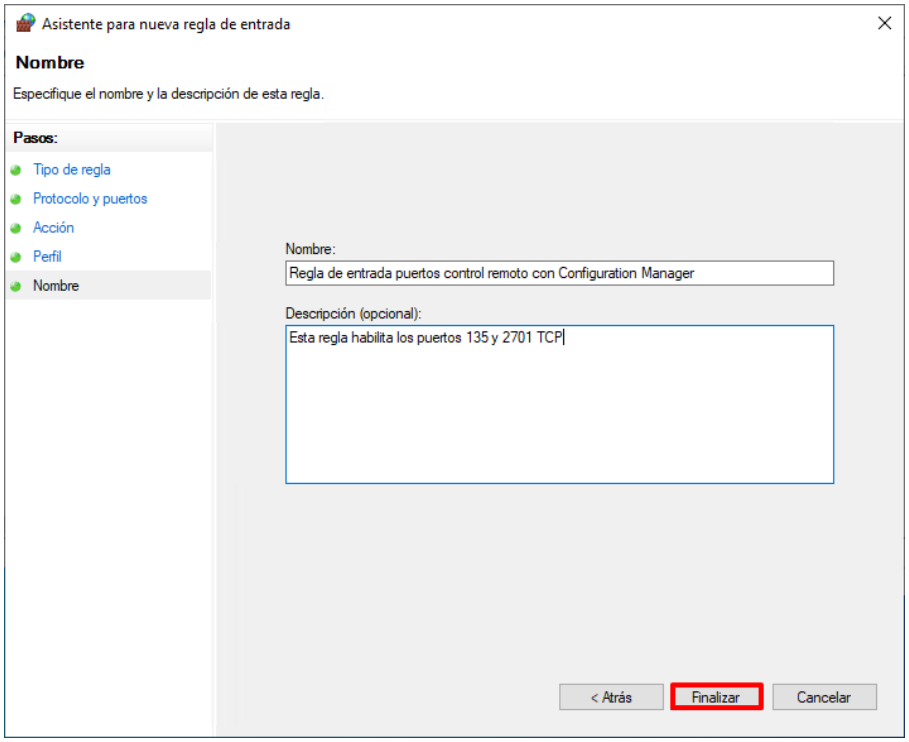
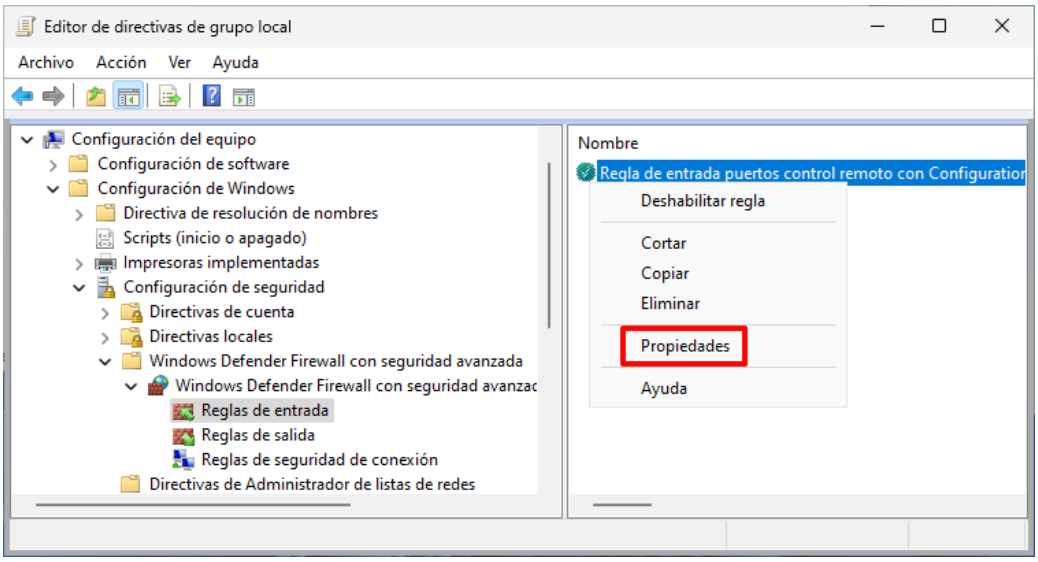
Por otro lado, si en su organización dispone de otro software que sustituya el firewall por defecto de Windows y este se encuentra habilitado y configurado podrá ignorar los siguientes pasos y continuar en el siguiente punto.

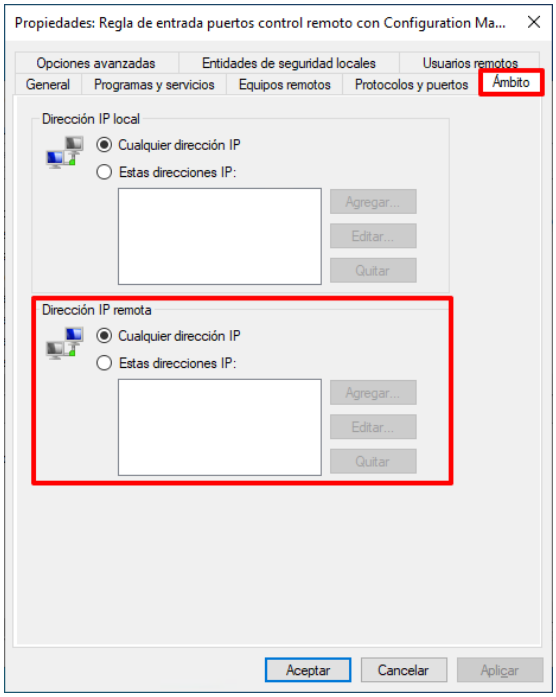
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
3.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 

Paso	Descripción
4.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada – Objeto de directiva de grupo local"** 
5.	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
6.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 
7.	En la opción de “Puertos locales específicos” introduzca “135, 2701”. Si los clientes miembro necesitan otros puertos para el correcto funcionamiento, debería introducir también dichos puertos. Pulse el botón “Siguiente >”.  **Nota:** Deberá tener en consideración el protocolo, siendo en este ejemplo TCP.

Paso	Descripción
8.	En la pantalla de “Acción”, mantenga la configuración “Permitir la conexión” y pulse el botón “Siguiente >”. 
9.	En la ventana “Perfil”, deje marcado el perfil “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 

Paso	Descripción
10.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”. Puede asignar una descripción si lo desea. 
11.	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
12.	Podría, por ejemplo, limitarse las IP remotas o rangos de redes que podrían conectarse al cliente independiente a través de los puertos 135 y 2701. De forma predeterminada, se admite cualquier IP, pero podría establecerse un límite a las mismas mediante la pestaña “Ámbito”. 
13.	Podrá repetir los pasos anteriores en caso de necesidad de habilitar otros puertos de conexión.
14.	Cierre la ventana “Editor de directivas de grupo local”.

ANEXO B.2.5. 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.

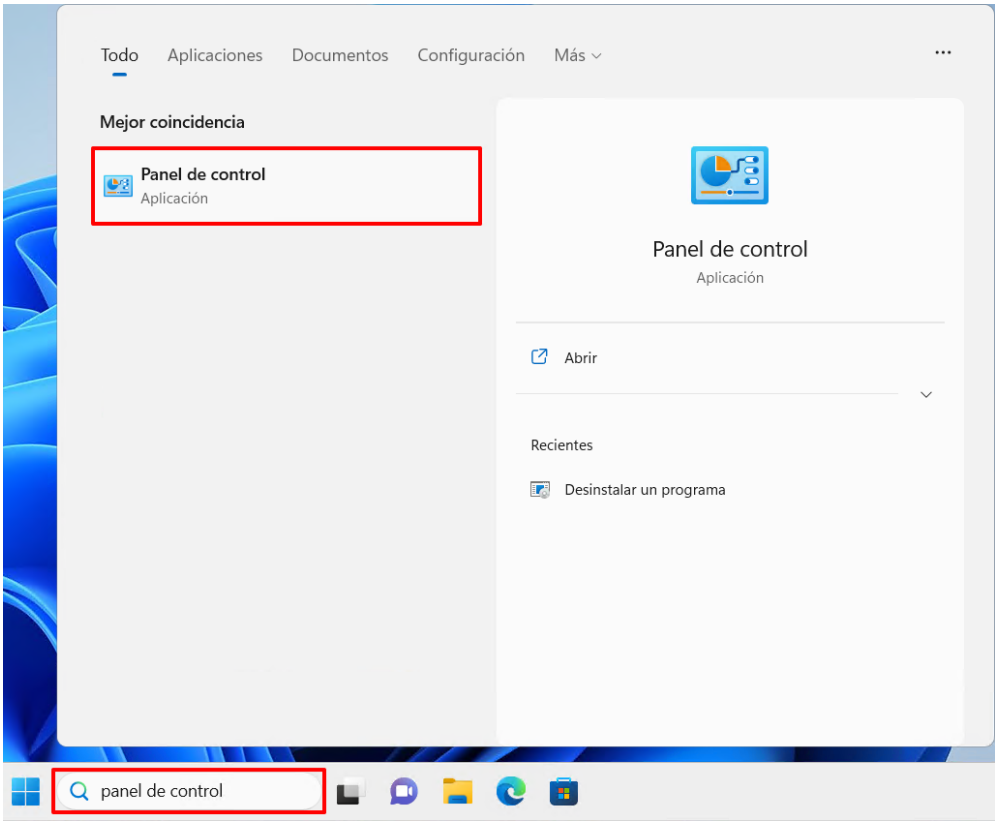
Antes de continuar tenga en consideración los siguientes aspectos:

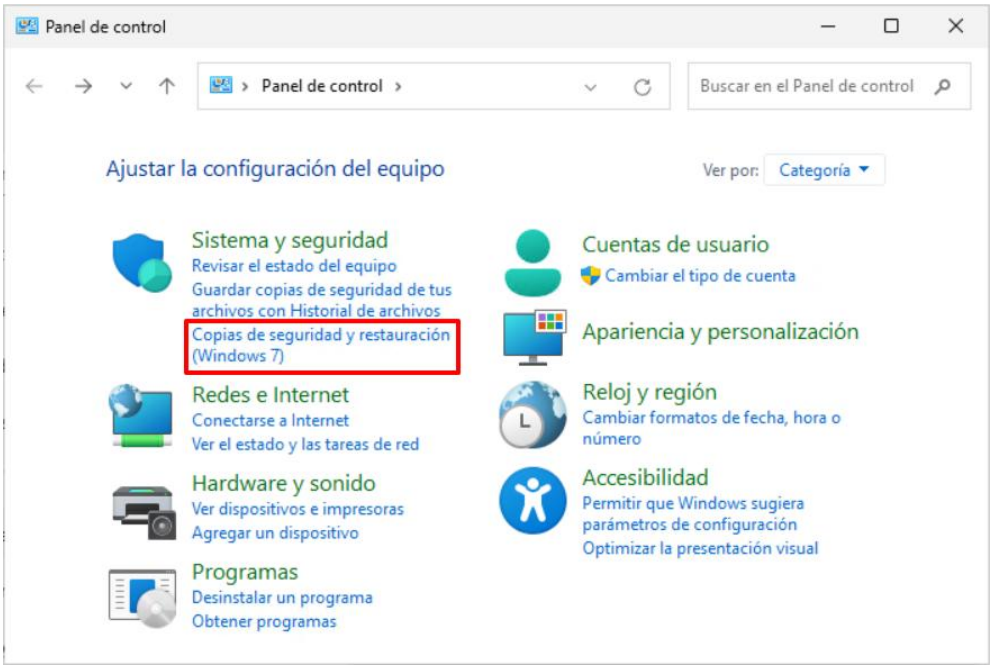
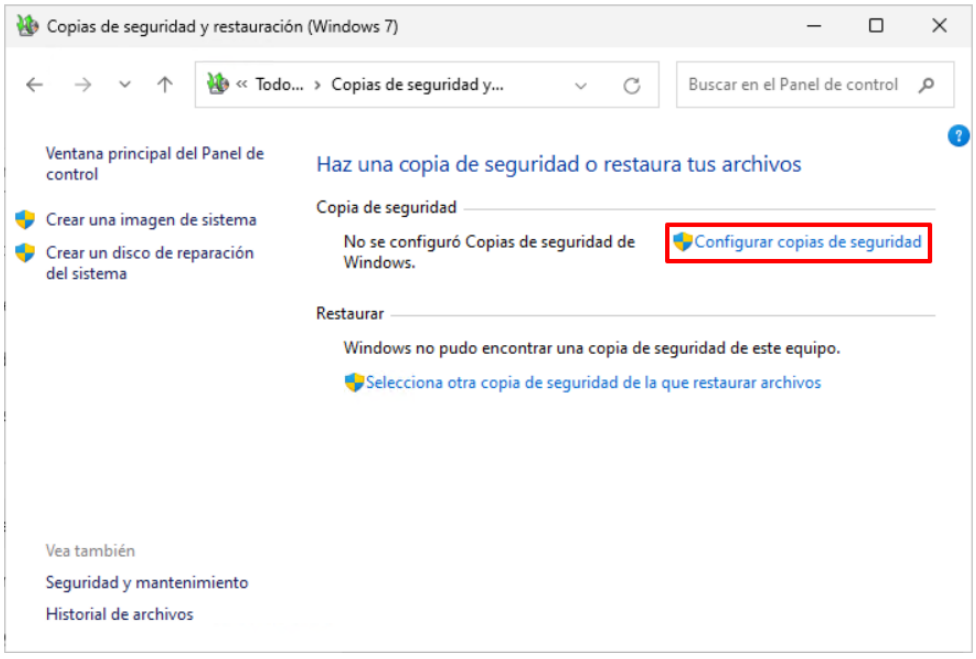
a) Deberá disponer de un espacio adicional donde alojar las copias realizadas.

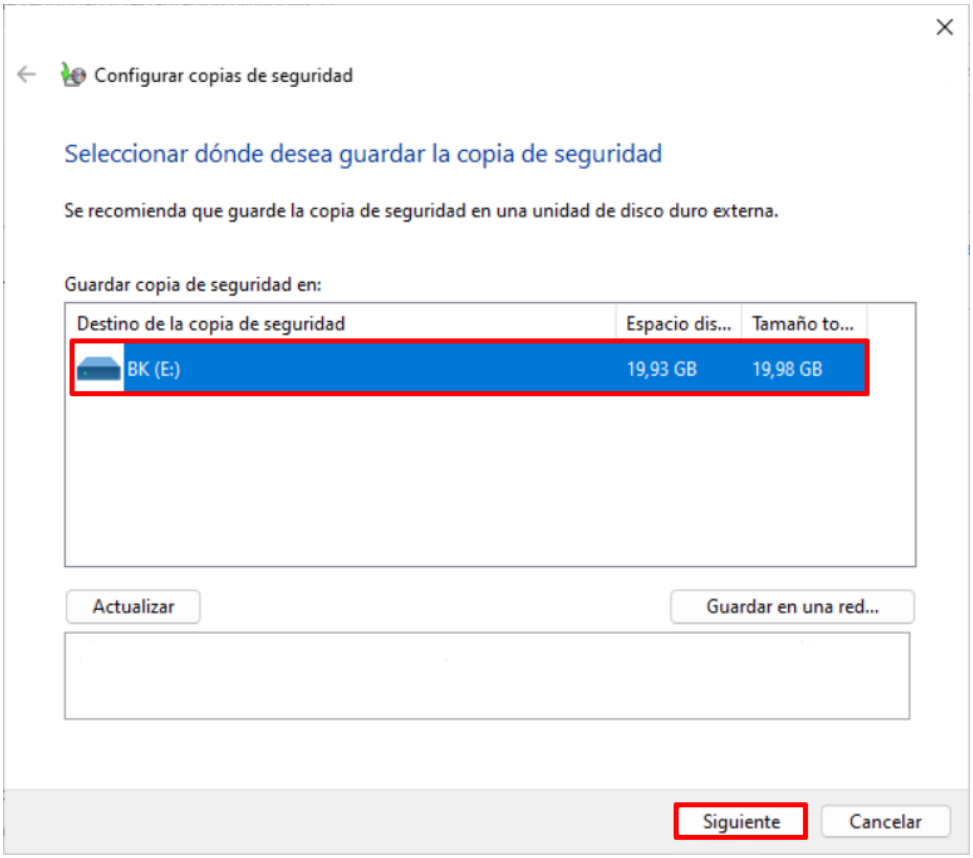
b) El uso de esta herramienta es de uso local por lo que no podrá utilizarse como mecanismo central de gestión de copias, aunque existe la posibilidad de programar dichas copias y alojarlas todas en una misma ubicación remota, de modo que estas se encuentren centralizadas.

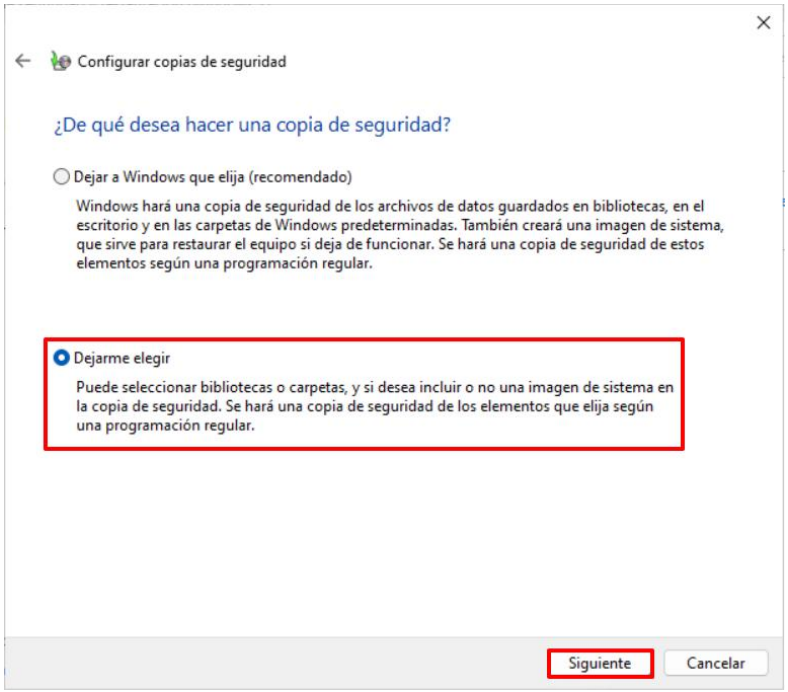
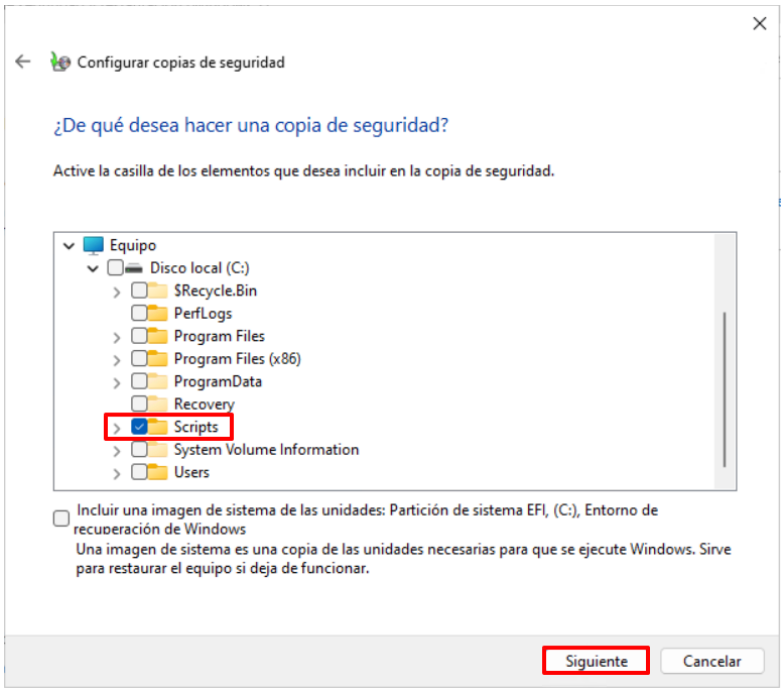
Nota: En este ejemplo se va a realizar una copia de seguridad puntual en el tiempo de una carpeta de datos alojada en un equipo de tipo Cliente Independiente.

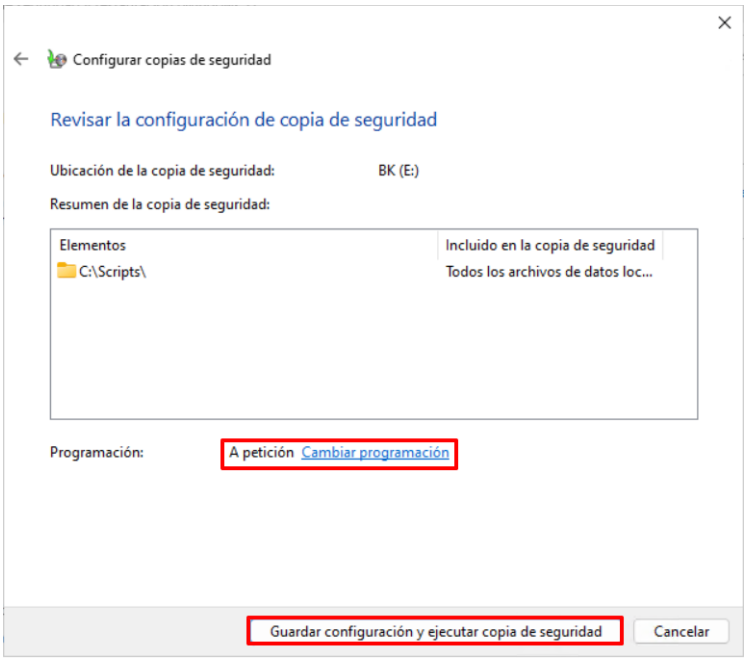
Se recomienda establecer una copia de seguridad programada con el objetivo de que esta se realice de una forma periódica acorde a las políticas de la organización, tomando en consideración su configuración (Completa, Incremental, etc.).

Paso	Descripción
1.	Inicie sesión en el equipo donde desea realizar la copia de seguridad. Debe iniciar sesión con una cuenta que sea Administrado.
2.	En el cuadro de búsqueda busque la aplicación “Panel de control” y una vez encontrada, haga clic sobre la misma. 

Paso	Descripción
3.	En la parte superior izquierda del “Panel de control”, pulse sobre “Copias de seguridad y restauración (Windows 7)” en el apartado “Sistemas y seguridad”. 
4.	En la nueva ventana haga clic sobre la opción “Configurar copias de seguridad”. 

Paso	Descripción
5.	En la primera ventana del asistente seleccione la unidad local donde se va a alojar la copia de seguridad y pulse “Siguiente”.  **Nota:** Dependiendo de la configuración o ubicación donde se desea alojar la copia de seguridad deberá adaptar este paso.

Paso	Descripción
6.	En la siguiente ventana del asistente seleccione la opción “Dejarme elegir” y pulse “Siguiente” para continuar. 
7.	En la nueva ventana deberá seleccionar aquellos directorios y ficheros sobre los que desee realizar la copia de seguridad. Pulse “Siguiente” al finalizar.  **Nota:** Si la copia de seguridad no es del sistema al completo, como es el caso del ejemplo, deberá tener desmarcada la opción “Incluir una imagen de sistema de las unidades: Partición de sistema EFI, (C:), Entorno de recuperación de Windows”.

Paso	Descripción
8.	Establezca una programación para la copia de seguridad que se ajuste a las necesidades de la organización haciendo clic sobre “Cambiar programación”. Una vez establecida, pulse sobre “Guardar configuración y ejecutar copia de seguridad” para realizar la primera copia de seguridad y finalizar con el proceso.  **Nota:** En este caso se ha establecido una programación a petición, teniendo que ejecutar la copia de seguridad de forma manual.

ANEXO B.2.6. PROTECCIÓN DE DISPOSITIVOS PORTÁTILES (USO OFICIAL – MATERIAS CLASIFICADAS)

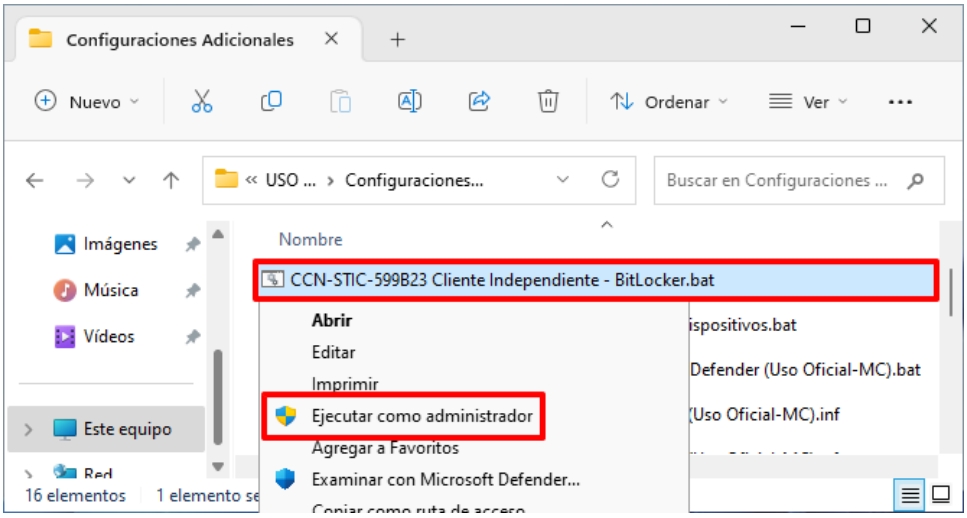
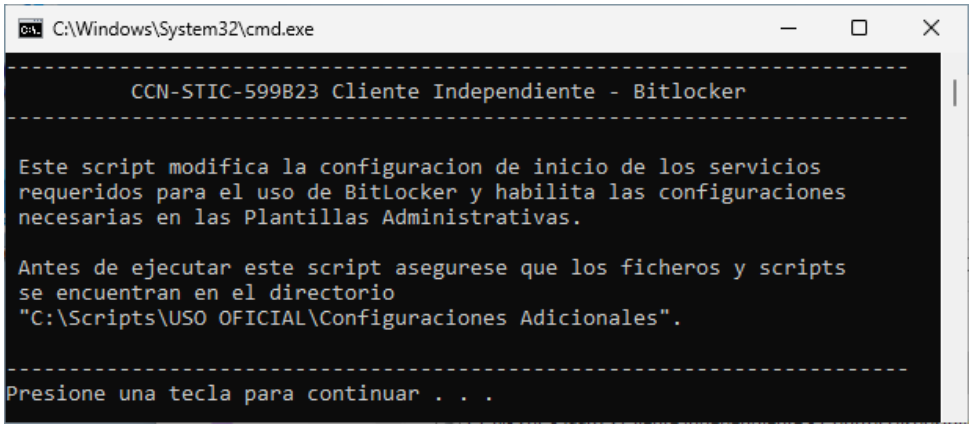
La presente sección tiene como objetivo la configuración y aplicación de directivas de modo que sea posible el cifrado de los sistemas operativos Windows Cliente, o de dispositivos portátiles, bajo el producto BitLocker.

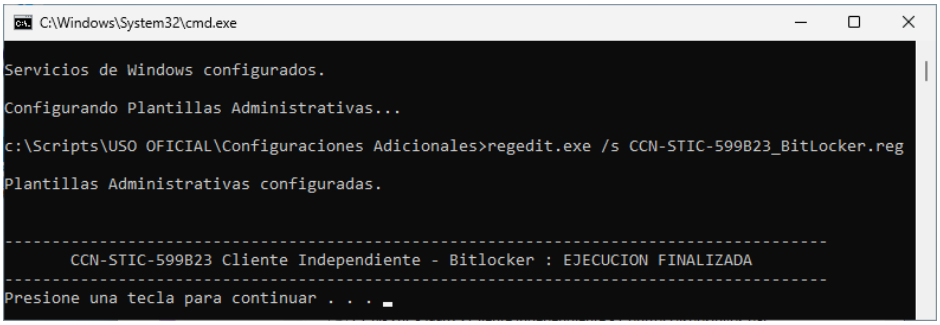
Nota: Si en su organización dispone de otro producto de cifrado, o bien su sistema operativo se encuentra implementado en un entorno protegido, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

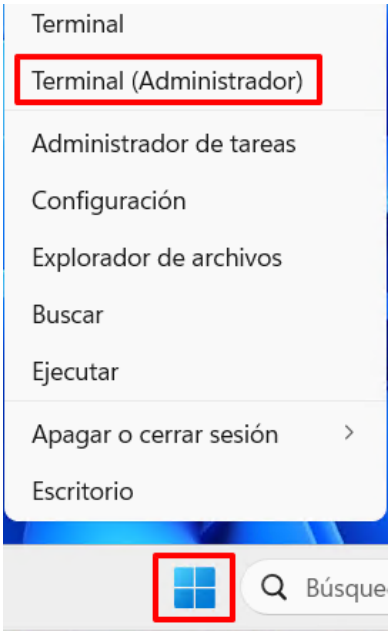
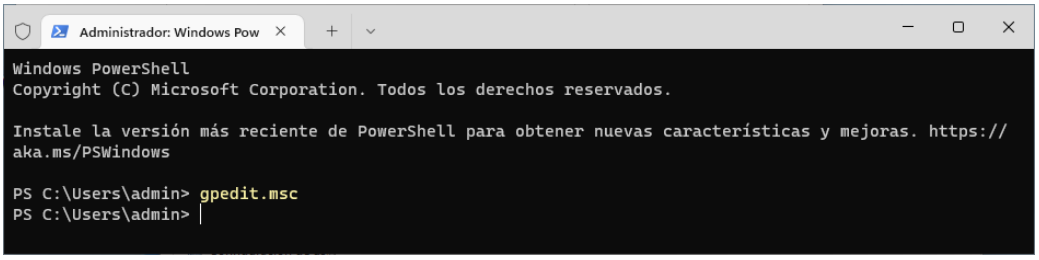
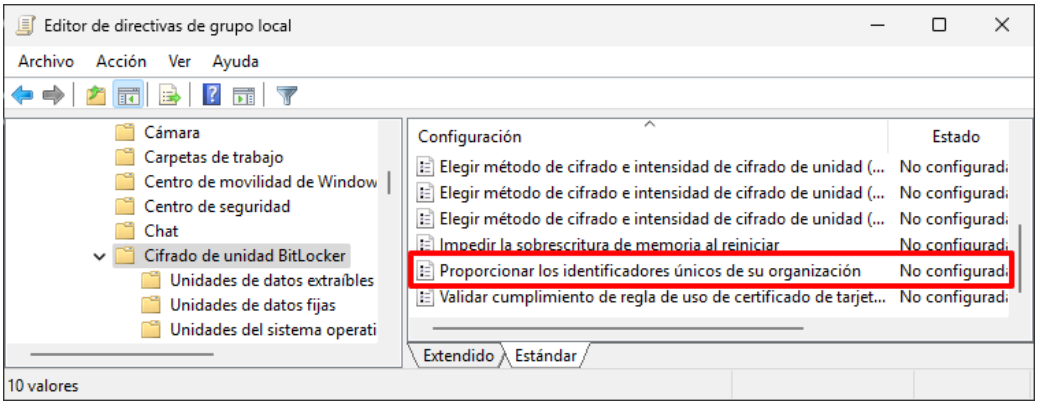
Se considera un entorno protegido, aquel entorno donde se disponga de un acceso controlado a salvo de hurtos y/o miradas indiscretas dentro de la organización.

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

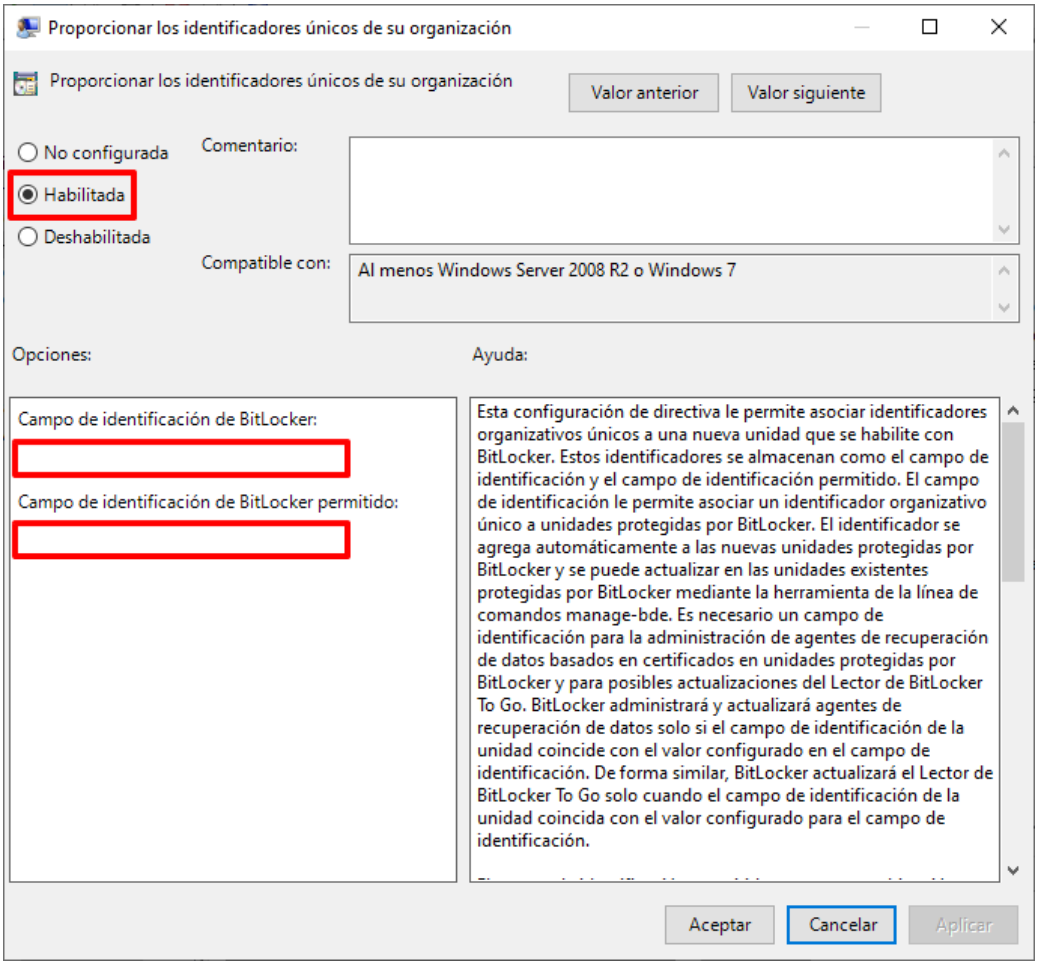
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

Paso	Descripción
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]\Configuraciones Adicionales**", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – BitLocker.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Seleccione el directorio acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Uso oficial".
3.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración de la herramienta de cifrado BitLocker. 

Paso	Descripción
4.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar.  **Nota:** Si habilita esta configuración, todas las unidades de datos extraíbles que no estén protegidas con BitLocker **se montarán en modalidad solo lectura**. Si la unidad está protegida con BitLocker, con un identificador válido establecido, se montará con acceso de lectura y escritura. Si hace uso de una unidad no protegida, podrá conectarla y cifrarla para permitir su uso en modo lectura y escritura. Al conectar el dispositivo removible por primera vez tras la aplicación de la citada configuración, **el módulo de BitLocker de Windows avisará de la necesidad de cifrado para permitir guardar ficheros**.  Si se requiere aplicar la configuración, pero evitar el funcionamiento indicado, consulte el apartado "**ANEXO B.4.5. CIFRADO DE UNIDAD DE BITLOCKER**".

Paso	Descripción
5.	Posteriormente, haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
6.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
7.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker"**. Identifique en el panel derecho la directiva "**Proporcionar los identificadores únicos de su organización**" y haga doble clic sobre ella. 

8. En la nueva ventana emergente, configure la directiva como "**Habilitada**" y establezca un identificador en el apartado "**Campo de identificación de BitLocker**" acorde a su organización. En el apartado contiguo "**Campo de identificación de BitLocker permitido**", deberá establecer el mismo identificador, pudiendo establecer identificadores adicionales separados por comas si así fuera necesario.



Nota: Cualquier dispositivo removible cifrado mediante BitLocker en los dispositivos con esta configuración aplicada tendrán establecido en el valor "Campo de identificación" el identificador configurado en la directiva.

Cualquier dispositivo removible que dicho valor no lo tenga configurado, o su identificador no se encuentre establecido en el apartado "**Campo de identificación de BitLocker permitido**", solo podrá ser usado en **modo lectura**. Si un dispositivo removible ha sido cifrado en el equipo previamente a la aplicación de las directivas de seguridad tratadas en este punto, solo podrá ser utilizado en modo lectura tras la aplicación, pudiendo posteriormente **mediante línea de comandos** que el dispositivo tome el valor del campo de identificación y pueda ser **usado con normalidad**.

En caso de que requiera deshabilitar la directiva "**Proporcionar los identificadores únicos de su organización**", o quiera información de cómo utilizar dispositivos removibles en modo escritura previamente cifrados a la aplicación de las directivas, consulte el apartado "**ANEXO B.4.5. CIFRADO DE UNIDAD DE BITLOCKER**".

ANEXO B.2.7. 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 cliente independiente, independientemente de su función, dentro de un entorno.

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.

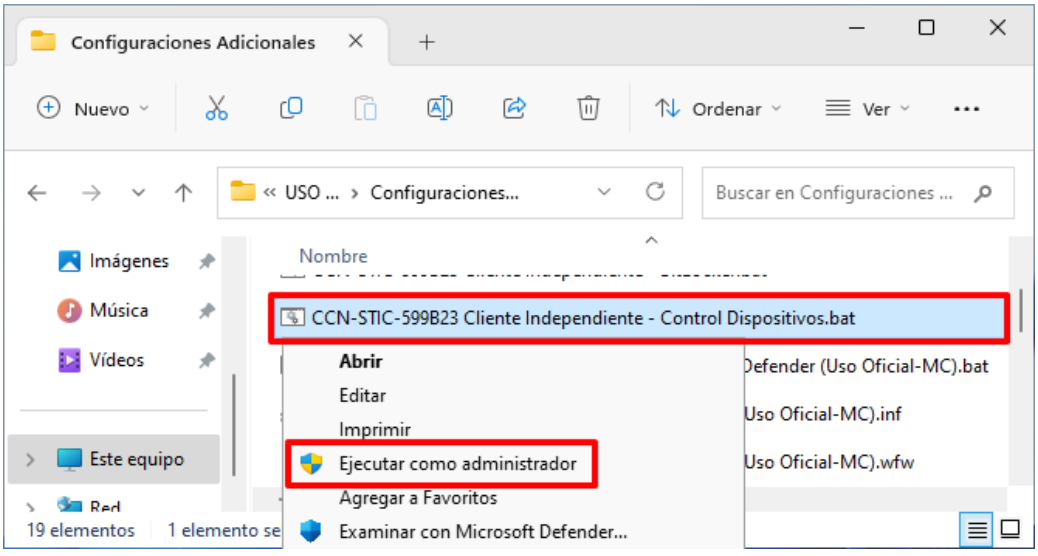
Se debe tener en consideración que tras la aplicación de los siguientes puntos se limitará la instalación de cualquier tipo de dispositivo, no solo dispositivos USB si no cualquier otro elemento como disco duro, tarjeta de red, etc., que haga uso de controladores (drivers).

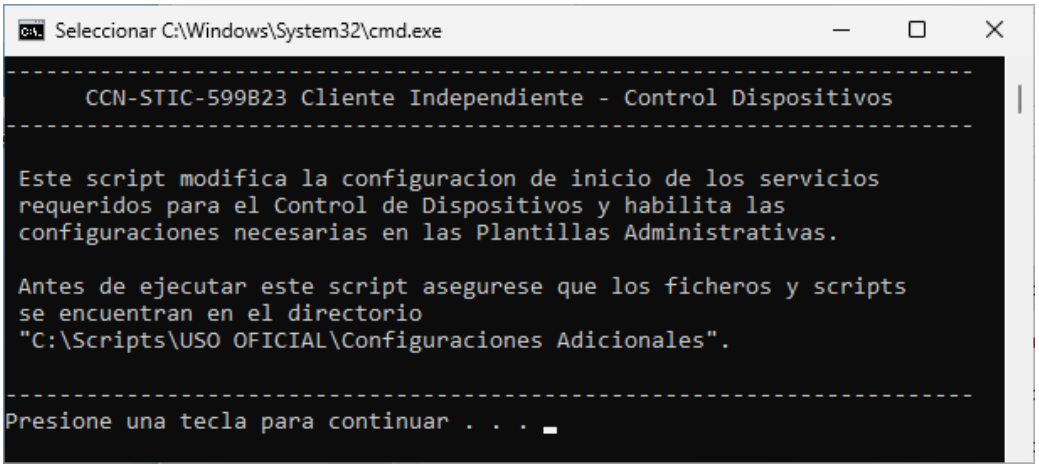
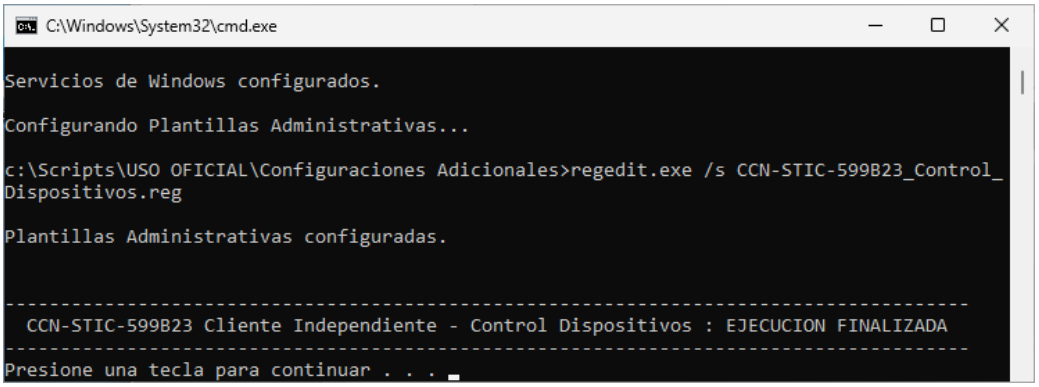
Realizadas las acciones descritas en el presente punto se presentarán dos formas de instalar controladores para el uso de dispositivos.

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.

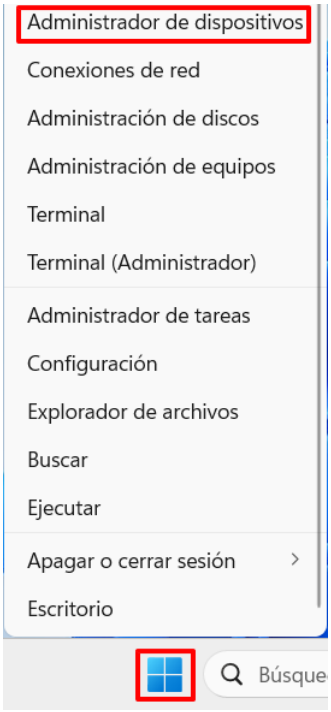
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]\Configuraciones Adicionales**", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Control Dispositivos.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 

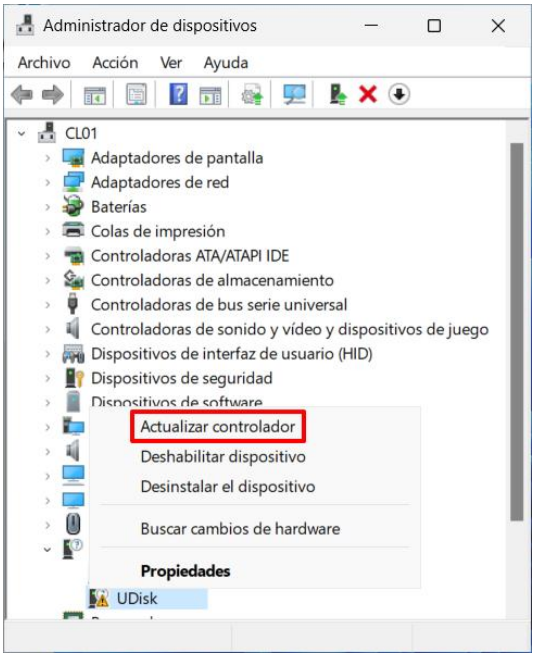
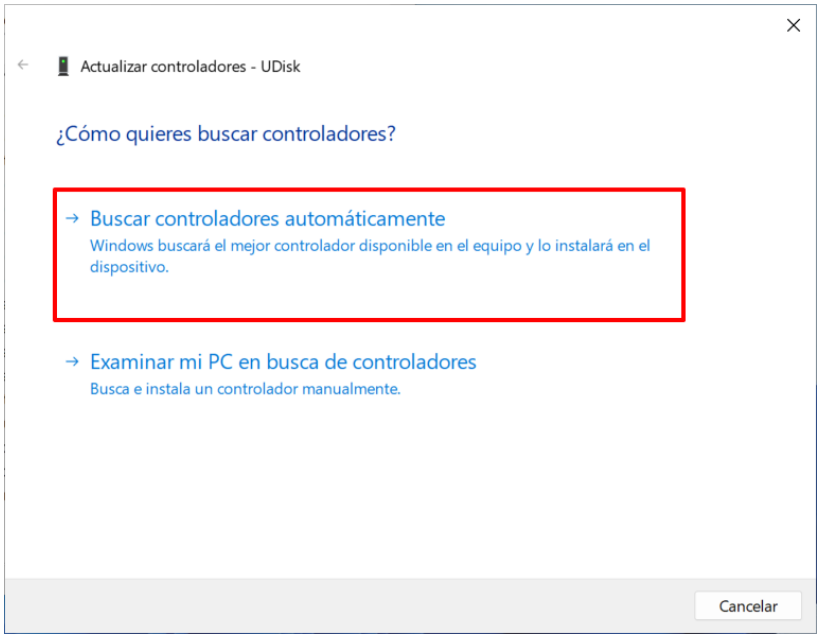
Paso	Descripción
3.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración para el control de dispositivos. 
4.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

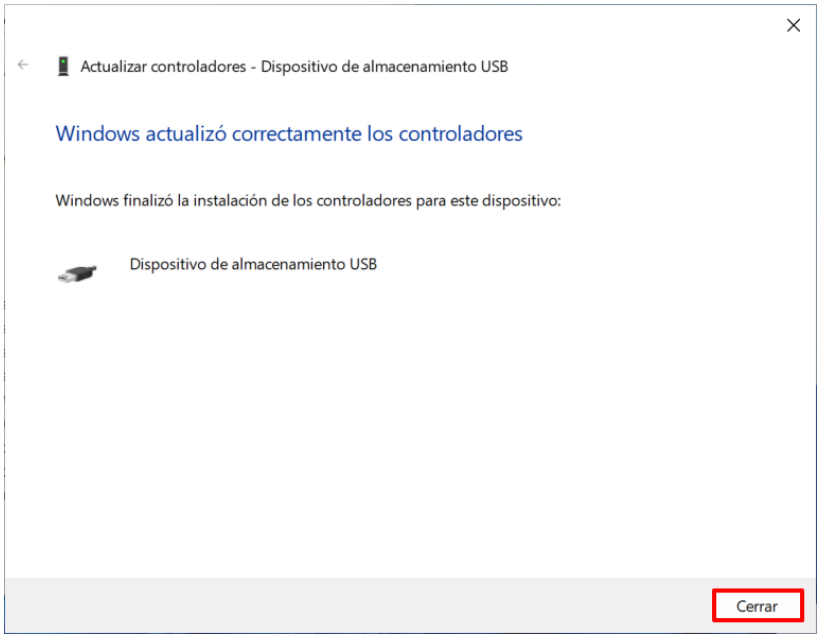
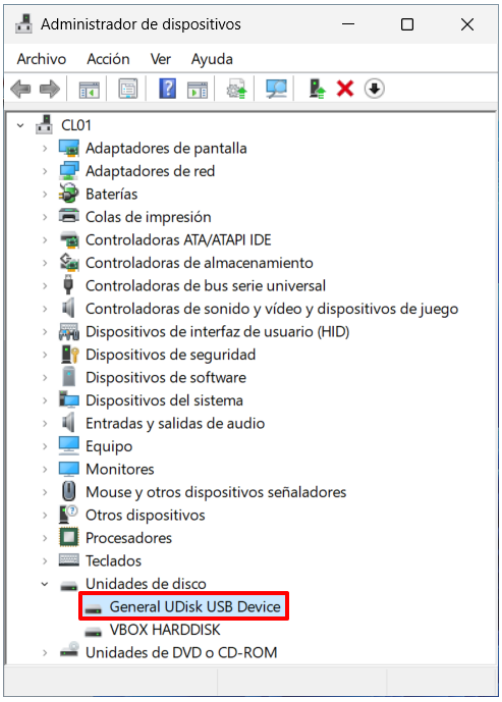
ANEXO B.2.7.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES

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

Paso	Descripción
5.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.

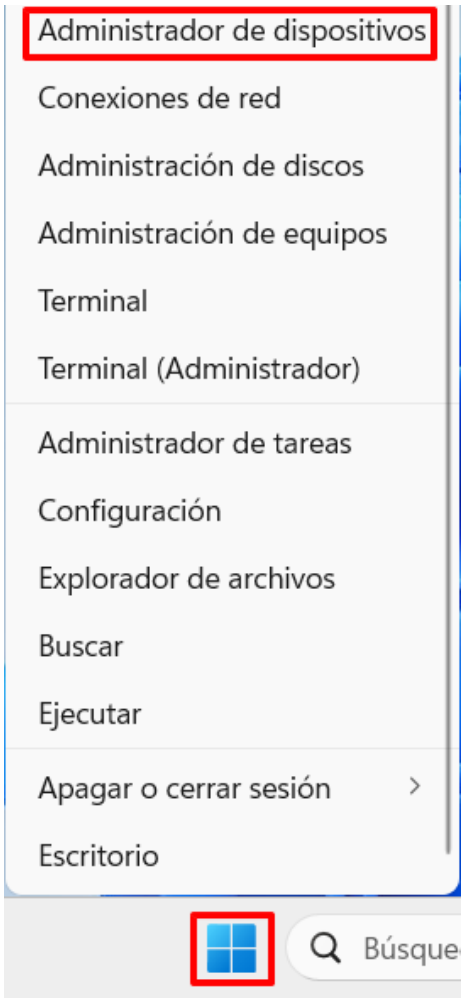
Paso	Descripción
6.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

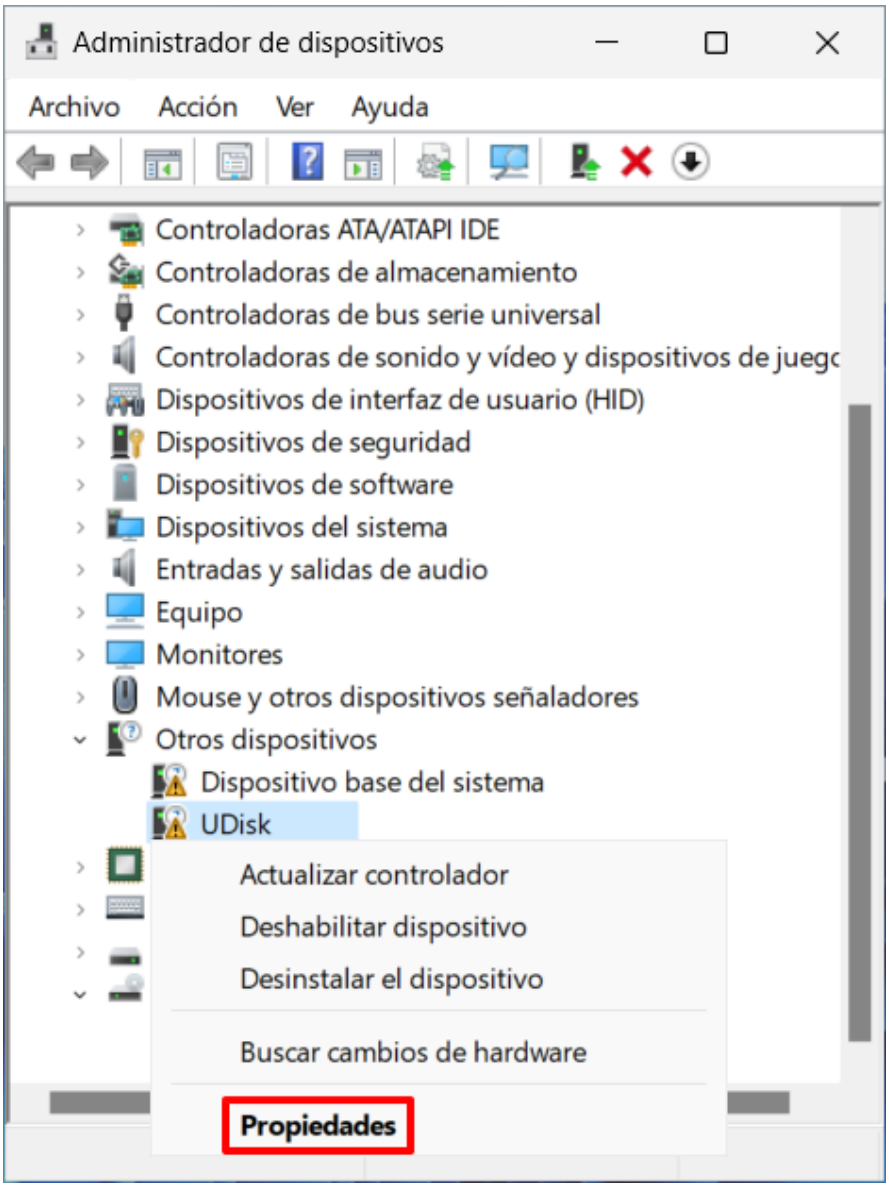
Paso	Descripción
7.	Despliegue en el "Administrador de dispositivos" el nodo "Otros dispositivos" y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual "Actualizar controlador".  **Nota:** Debido a la inexistencia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

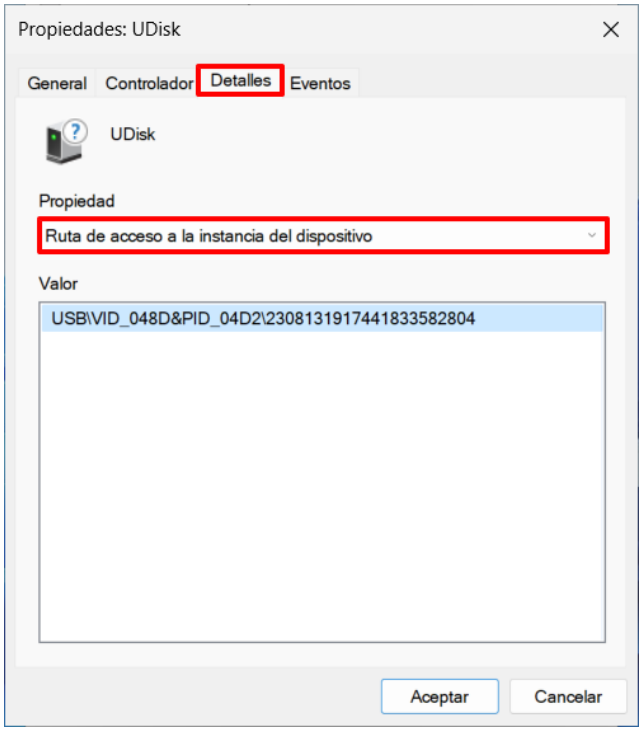
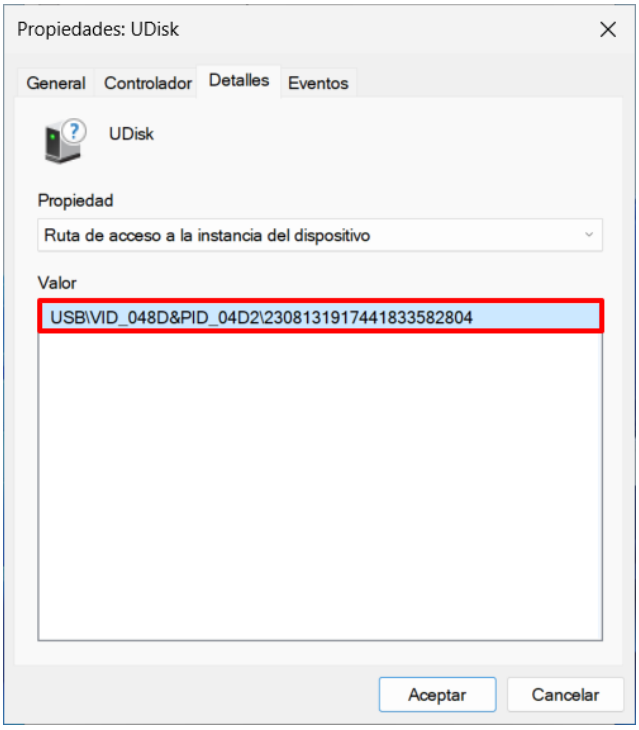
Paso	Descripción
9.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  **Nota:** No cierre el “Administrador de dispositivos” todavía.
10.	Ejecute los mismos pasos anteriores (pasos 7 a 9) hasta que el dispositivo aparezca en 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. 

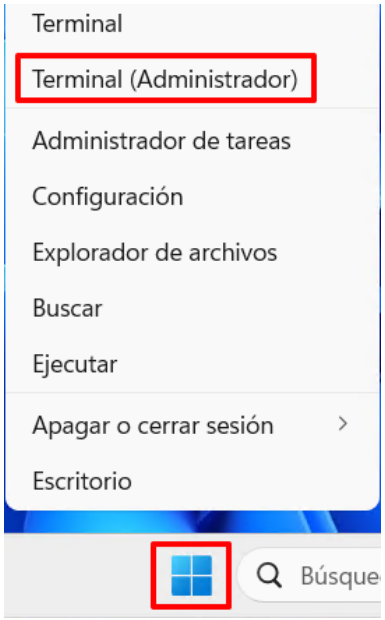
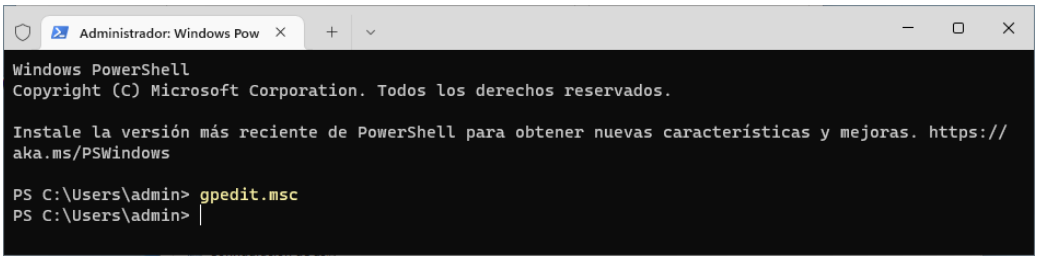
ANEXO B.2.7.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

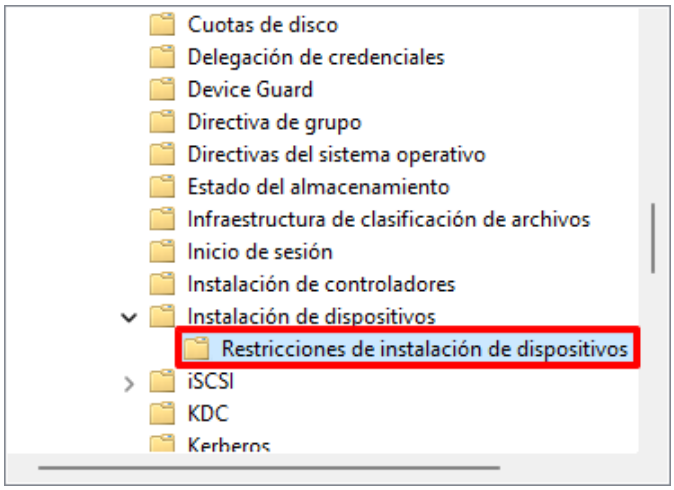
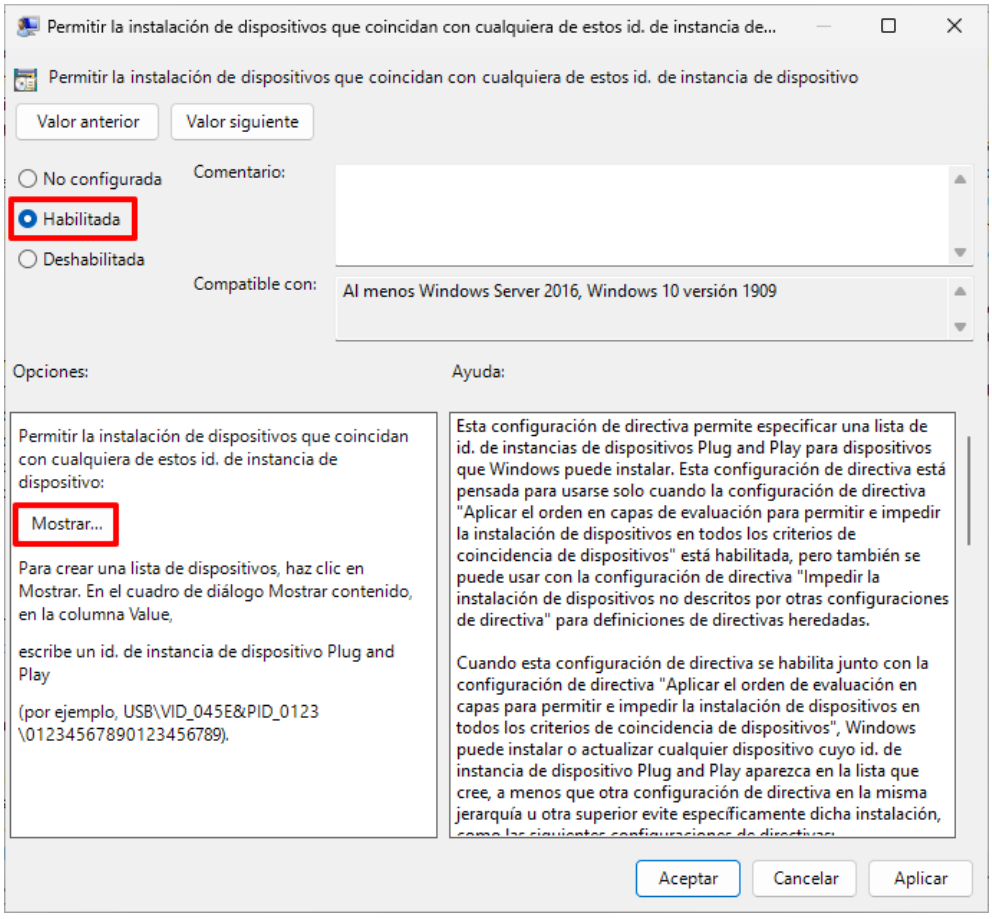
Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del entorno en el cual se está habilitando el uso de dispositivos USB.

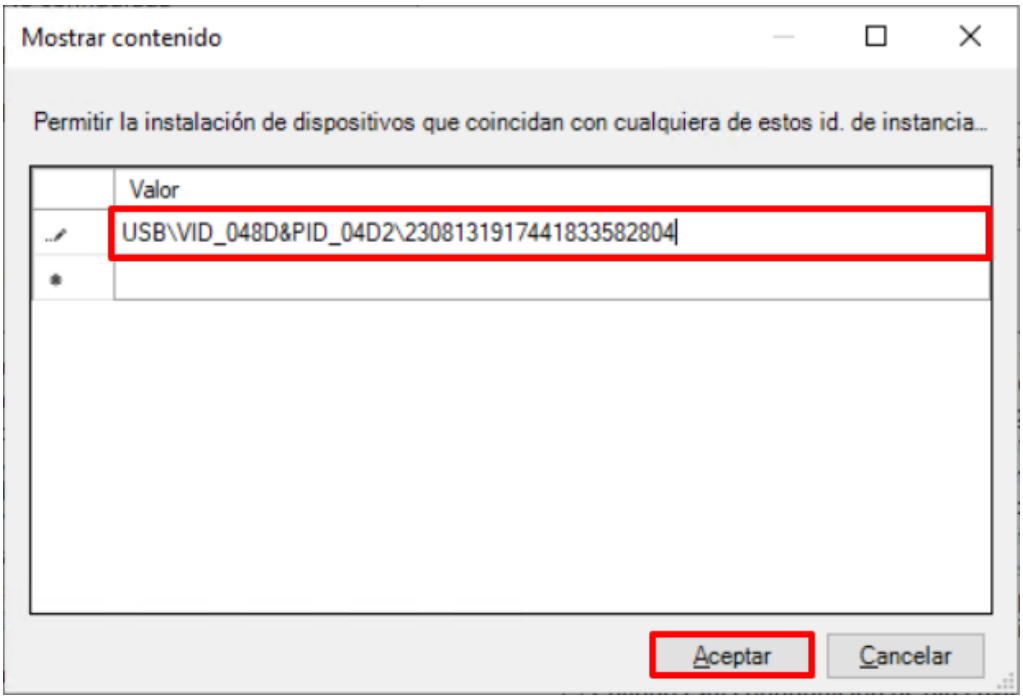
Paso	Descripción
11.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
12.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

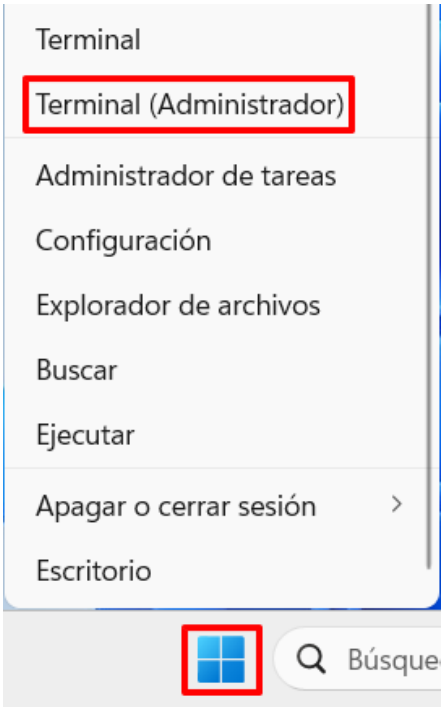
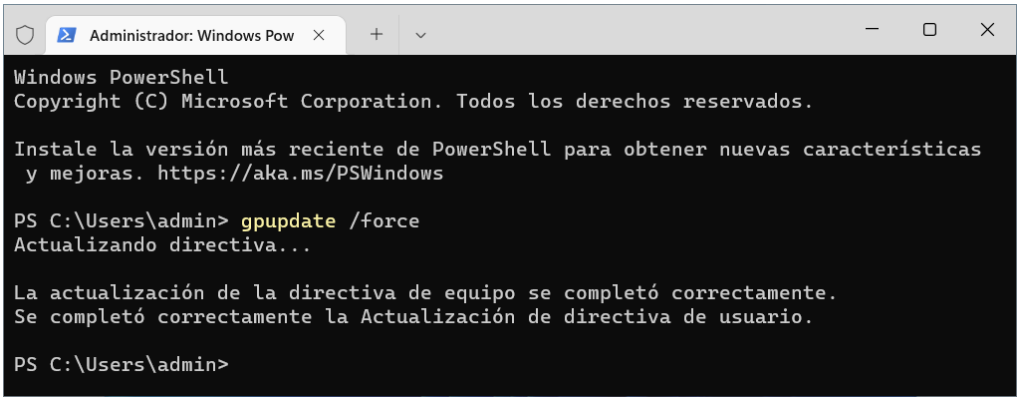
Paso	Descripción
13.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Propiedades”.  **Nota:** Debido a la inexistencia de controlador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

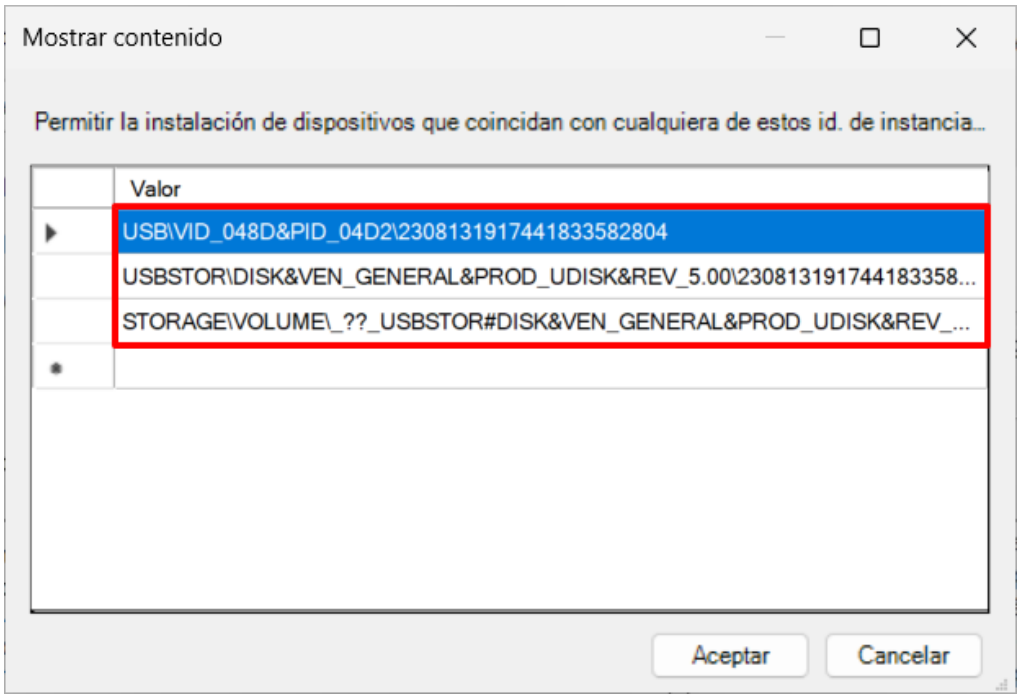
Paso	Descripción
14.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Ruta de acceso a la instancia del dispositivo”. 
15.	Seleccione el identificador y anótelo para poder introducirlo más adelante.  **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

Paso	Descripción
16.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
17.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 

Paso	Descripción
18.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos"** 
19.	En el panel derecho, haga doble clic sobre la directiva "**Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo**". Pulse sobre "Habilitada" y pulse el botón Mostrar…". 

Paso	Descripción
20.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la línea en blanco para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Verifique el identificador introducido y pulse “Aceptar” para continuar. 
21.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo”.
22.	Sin cerrar el “Editor de directivas de grupo local”, continue con el siguiente paso.

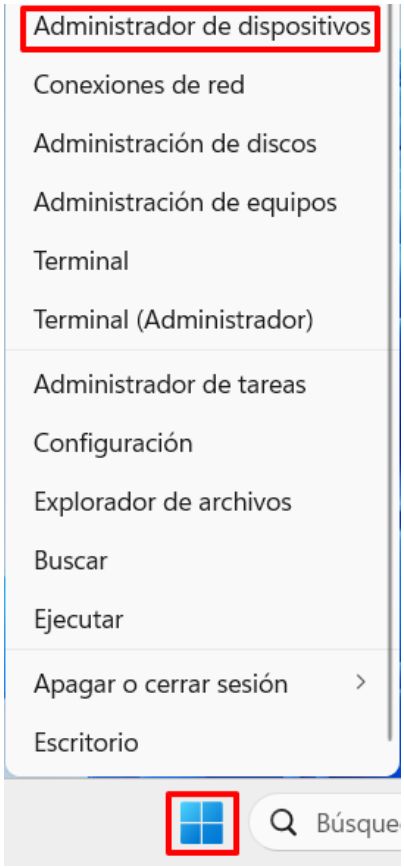
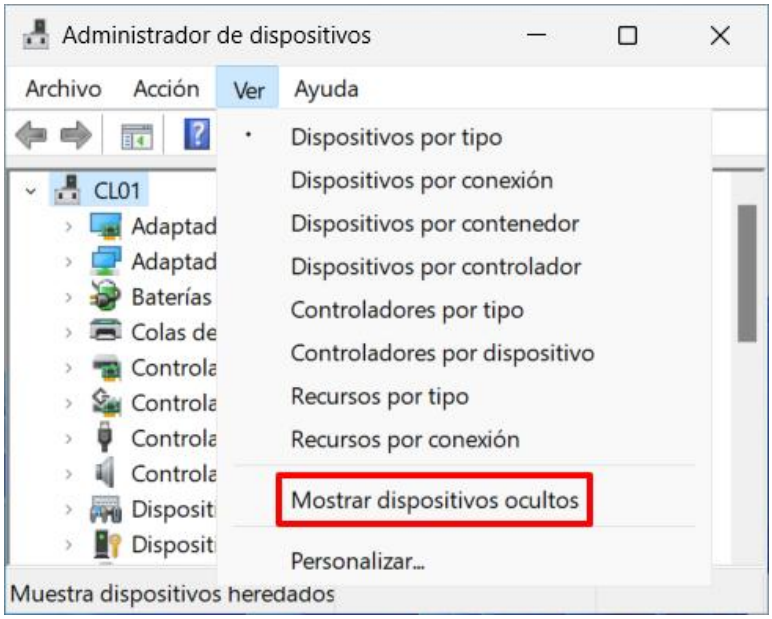
Paso	Descripción
23.	Sobre el equipo en el que se desea el uso de un dispositivo USB, haga clic derecho sobre el botón de “Inicio” y pulse sobre “Terminal (Administrador)”. 
24.	Ejecute el siguiente comando en la consola y espere a que finalice. > gpupdate /force 

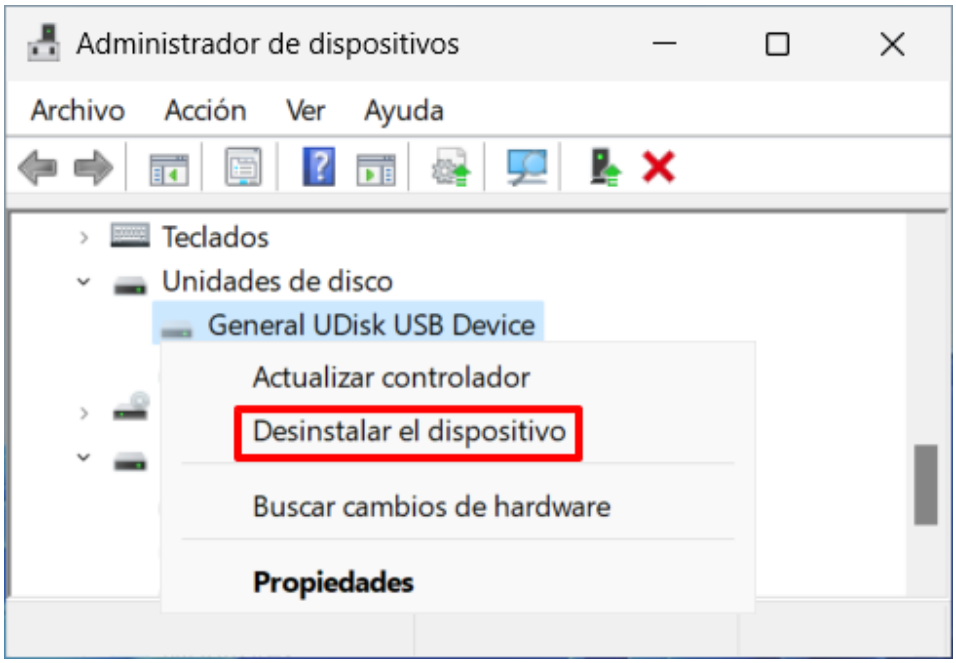
Paso	Descripción
25.	Ejecute de nuevo los pasos 13 a 24 con el objetivo de añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows. 

ANEXO B.2.7.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

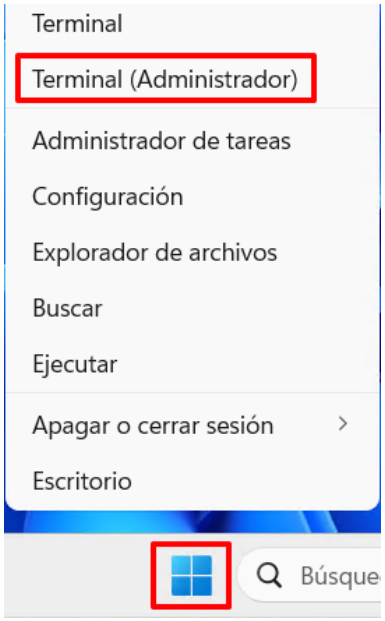
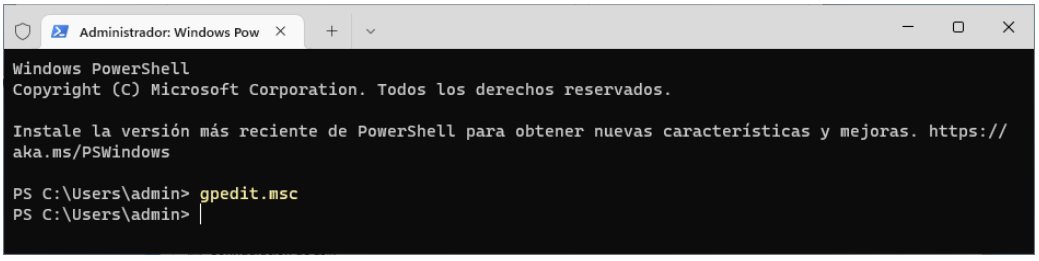
Tras la instalación del dispositivo y su posterior uso, es posible volver al estado anterior de bloqueo del uso de dispositivos USB dado de alta previamente. Para ello deberán seguir los siguientes pasos.

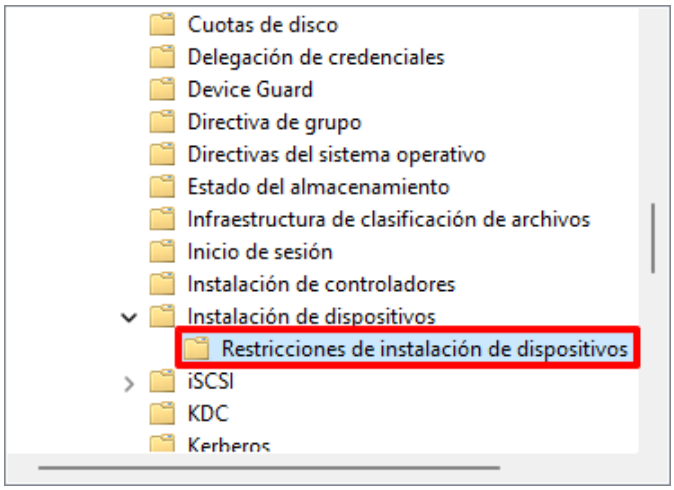
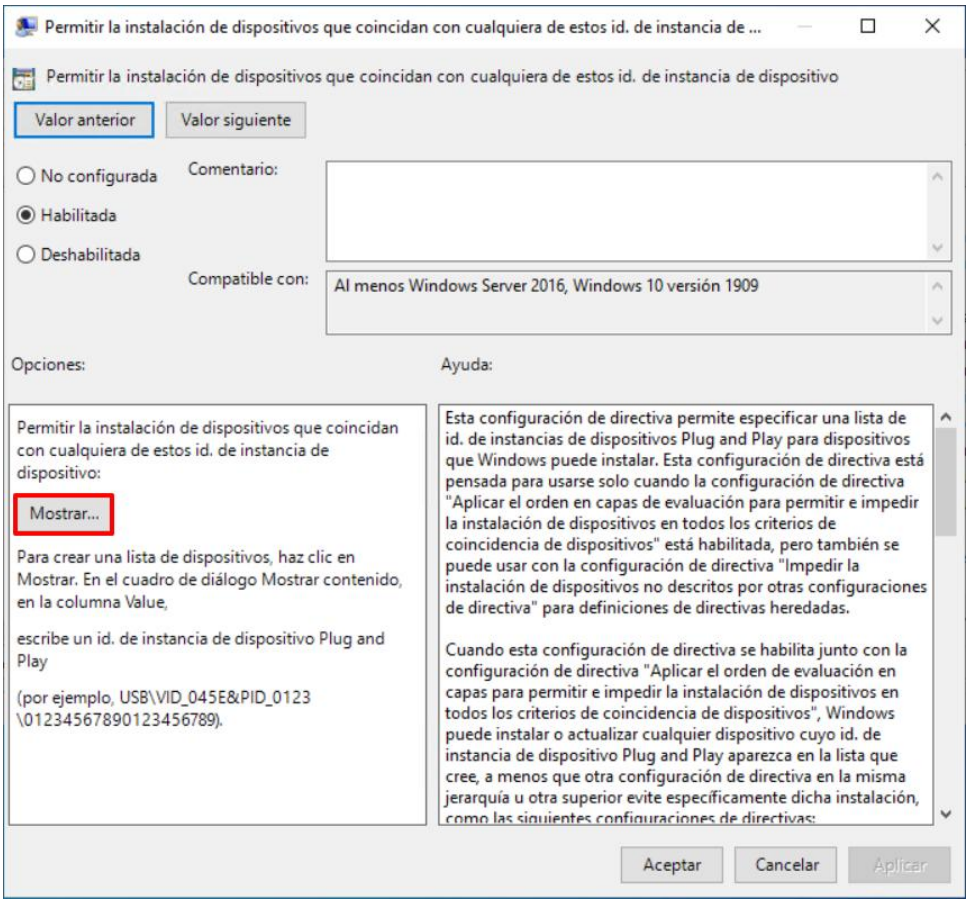
Paso	Descripción
26.	Inicie sesión en el equipo cliente donde pretende eliminar el uso de un dispositivo USB.

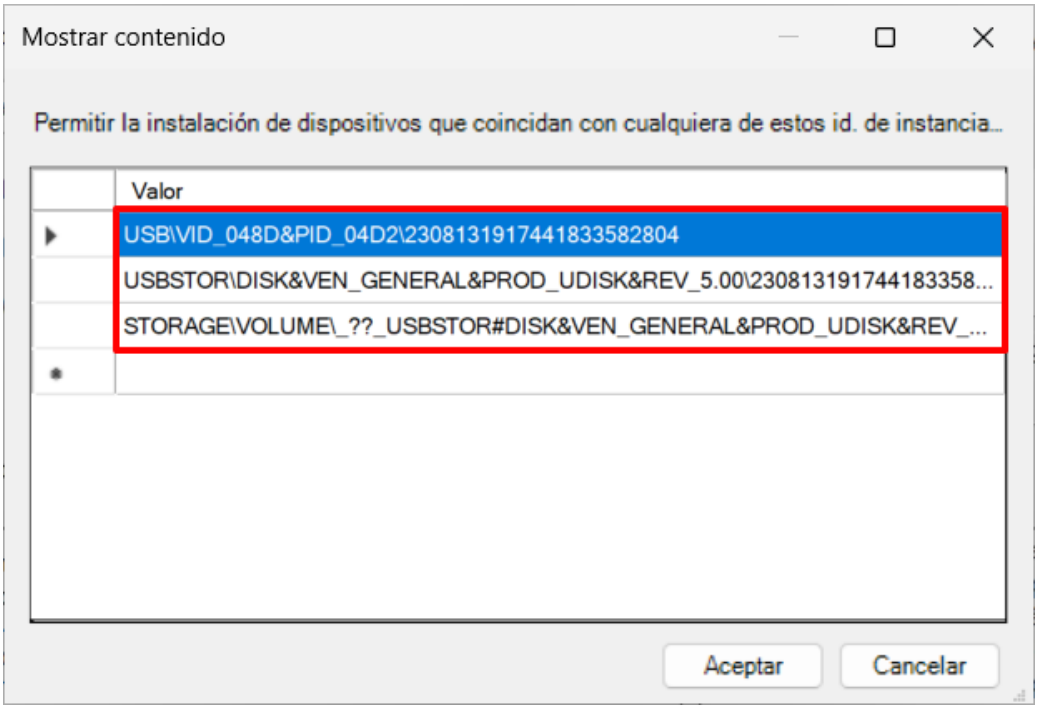
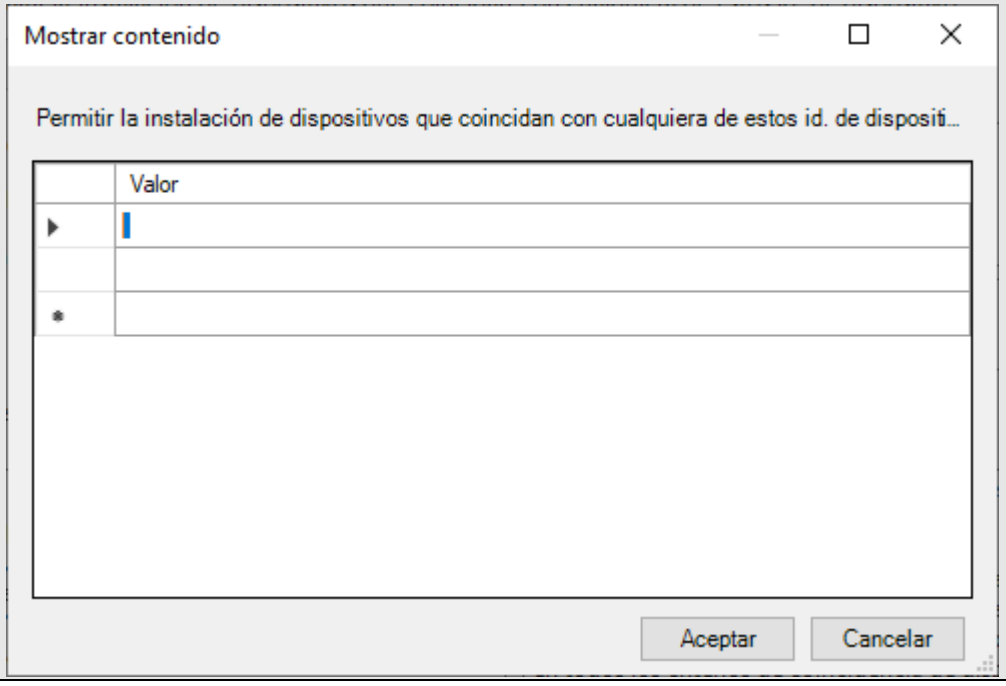
Paso	Descripción
27.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 
28.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

Paso	Descripción
29.	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”. 
30.	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
31.	Inicie sesión en el equipo cliente donde pretende eliminar el uso de un dispositivo USB.
32.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
33.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 

Paso	Descripción
34.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos"** 
35.	En el panel derecho, haga doble clic sobre la directiva "**Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo**", la cual debe estar configurada como "Habilitada" y dentro de ella pulse el botón Mostrar…". 

Paso	Descripción
36.	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 B.3. CONFIGURACIONES DE MEJORA

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

ANEXO B.3.1. 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 cliente independiente, independientemente de su función, dentro de un entorno.

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.

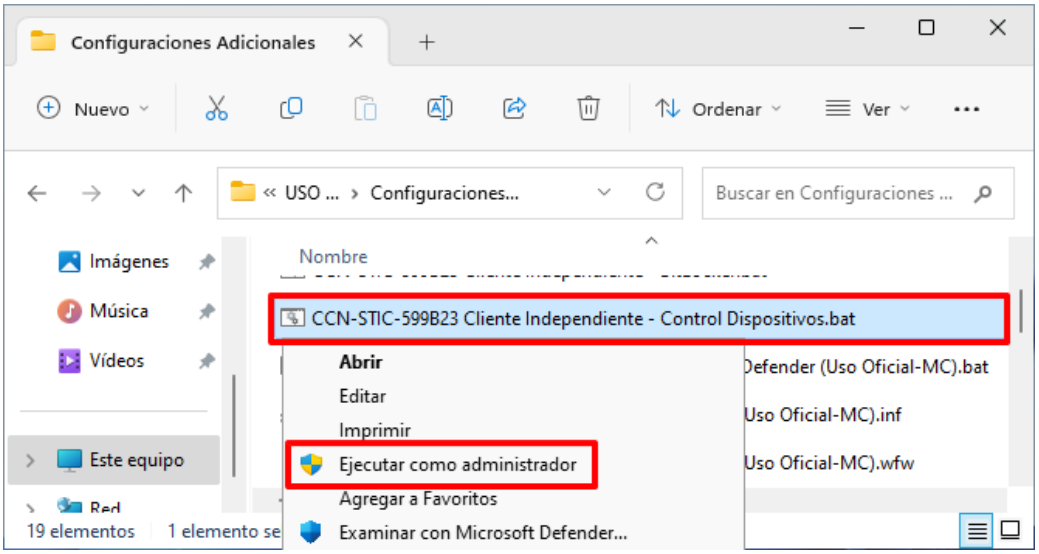
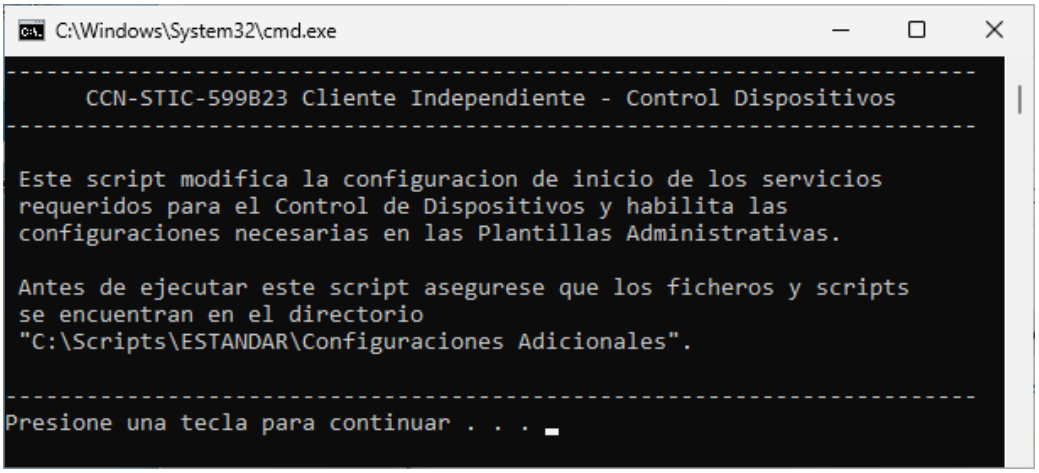
Realizadas las acciones descritas en el presente punto se presentarán dos formas de instalar controladores para el uso de dispositivos.

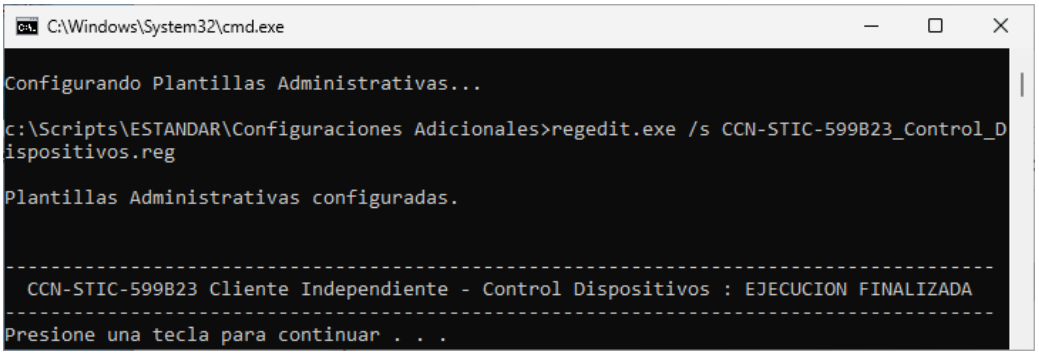
a) Actualización automática de controladores por parte de usuario con privilegios de administrador.

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.

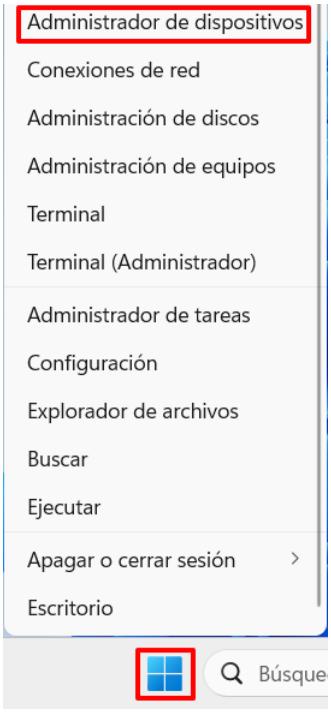
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

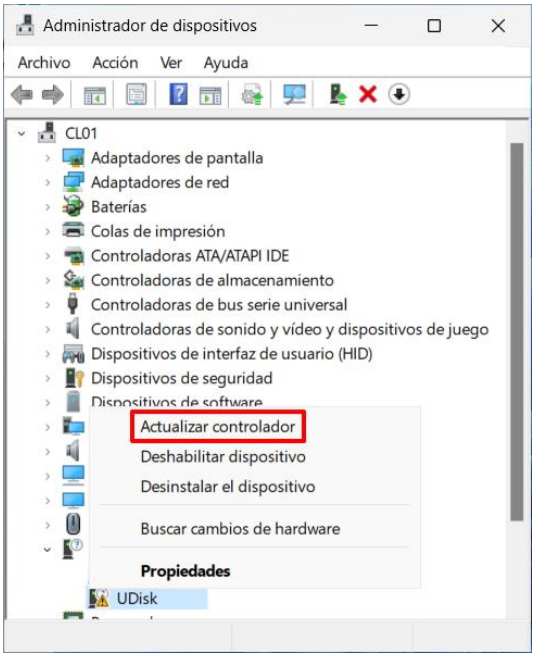
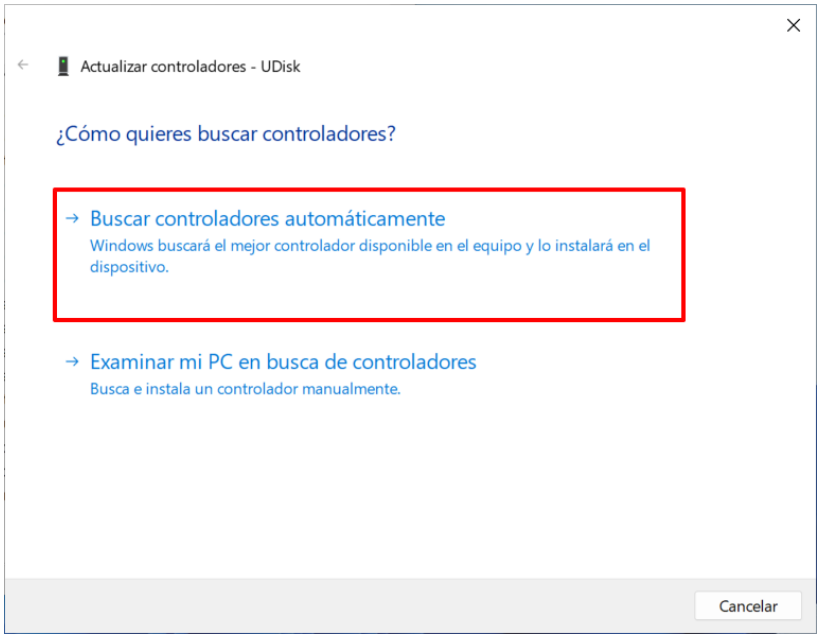
Paso	Descripción
2.	Diríjase al directorio "**C:\Scripts\[TIPO DE PERFILADO]\Configuraciones Adicionales**", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Control Dispositivos.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador".  **Nota:** Seleccione el directorio acorde al perfil de seguridad que desea aplicar. En este ejemplo se hace uso del perfil de configuración "Estándar".
3.	Se le informará de las acciones que realizará el script. Pulse cualquier tecla para continuar con la configuración para el control de dispositivos. 

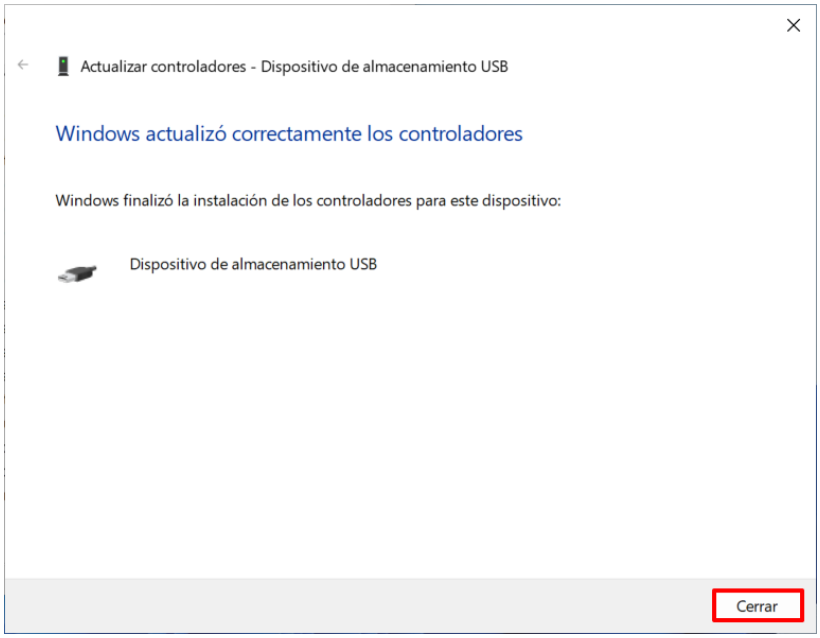
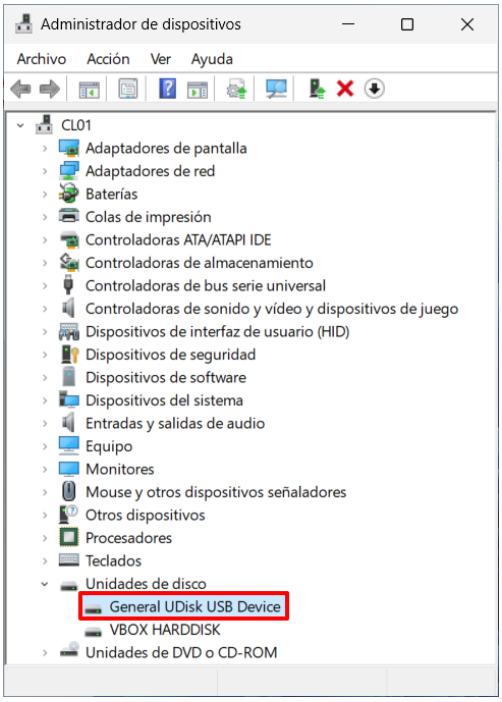
Paso	Descripción
4.	Espere a que finalice la ejecución y pulse de nuevo una tecla para finalizar. 

ANEXO B.3.1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES

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

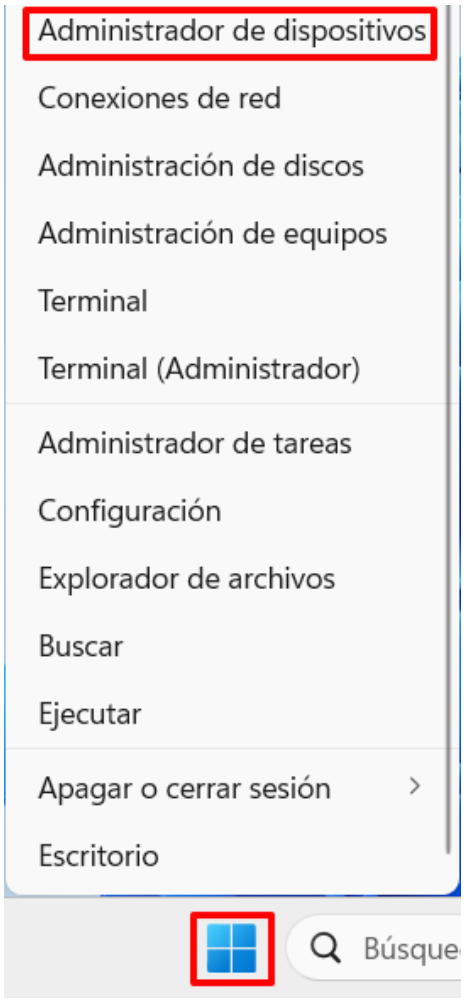
Paso	Descripción
5.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
6.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

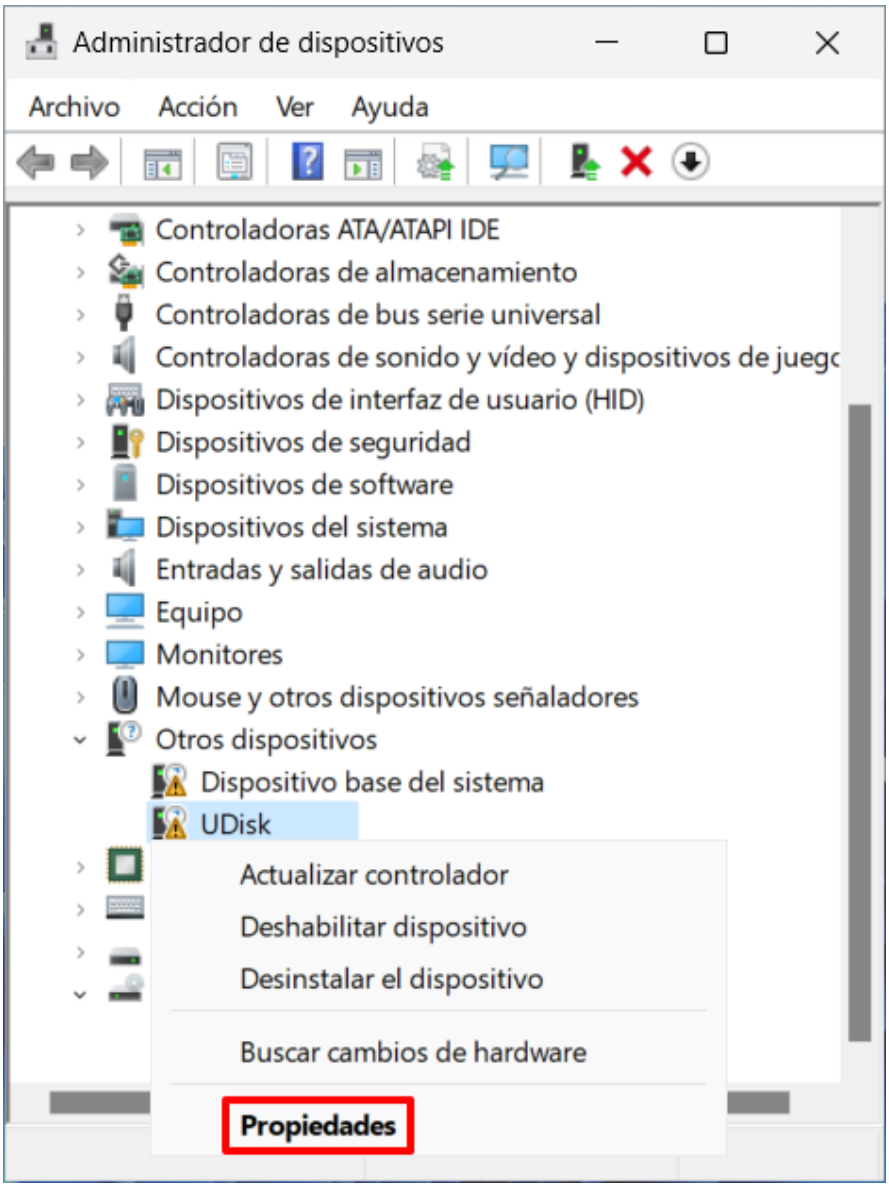
Paso	Descripción
7.	Despliegue en el "Administrador de dispositivos" el nodo "Otros dispositivos" y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual "Actualizar controlador".  **Nota:** Debido a la inexistencia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

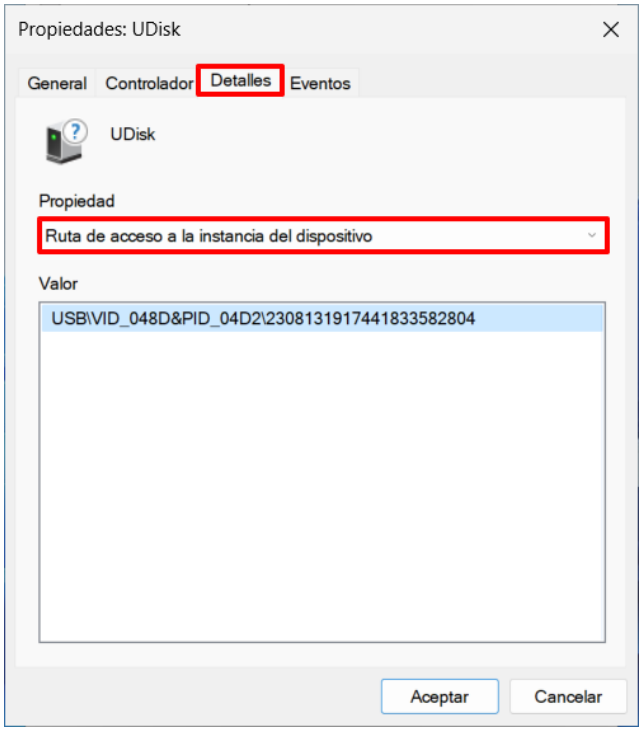
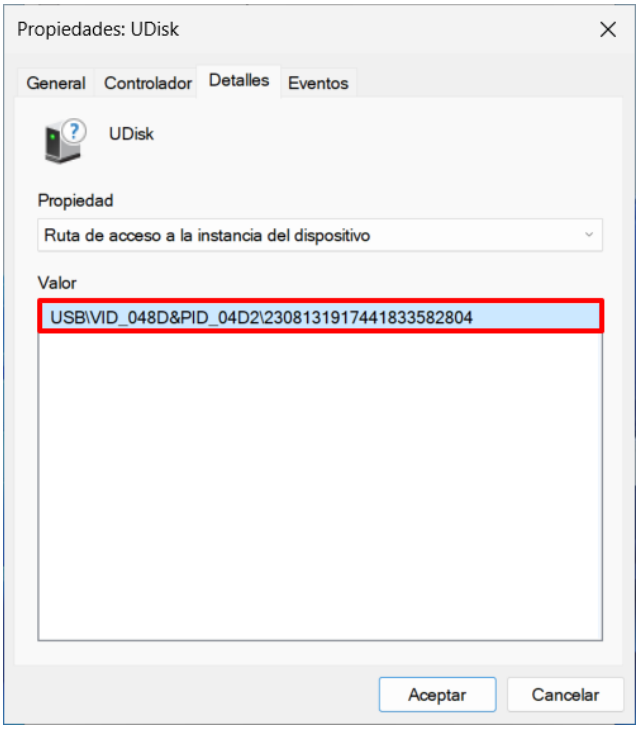
Paso	Descripción
9.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  **Nota:** No cierre el “Administrador de dispositivos” todavía.
10.	Ejecute los mismos pasos anteriores (pasos 7 a 9) hasta que el dispositivo aparezca en 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. 

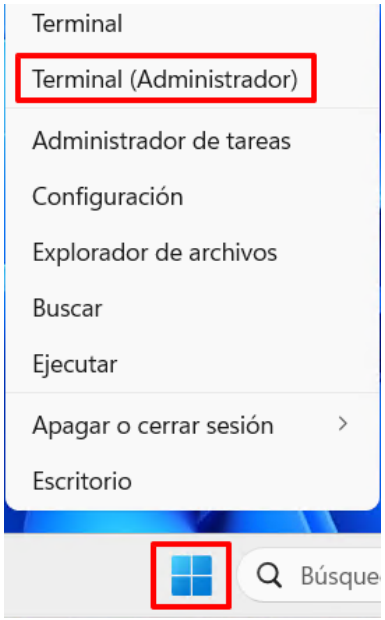
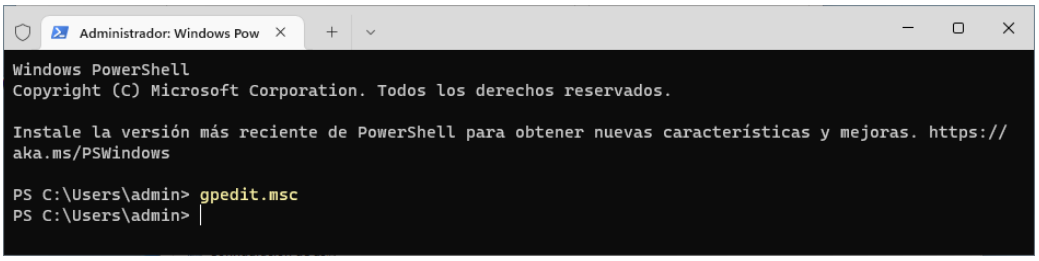
ANEXO B.3.1.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

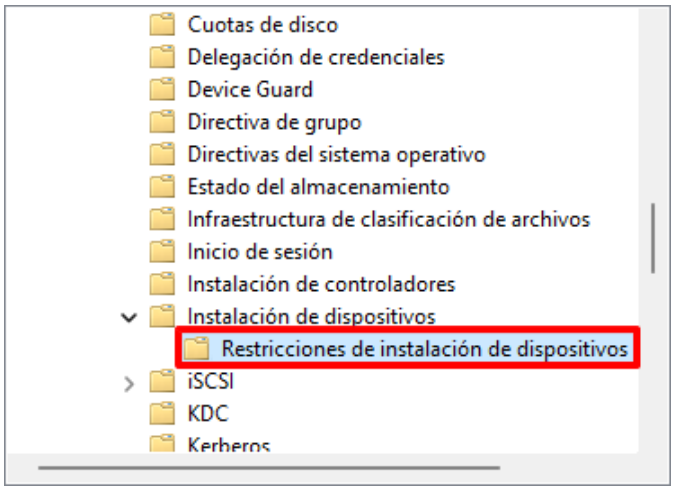
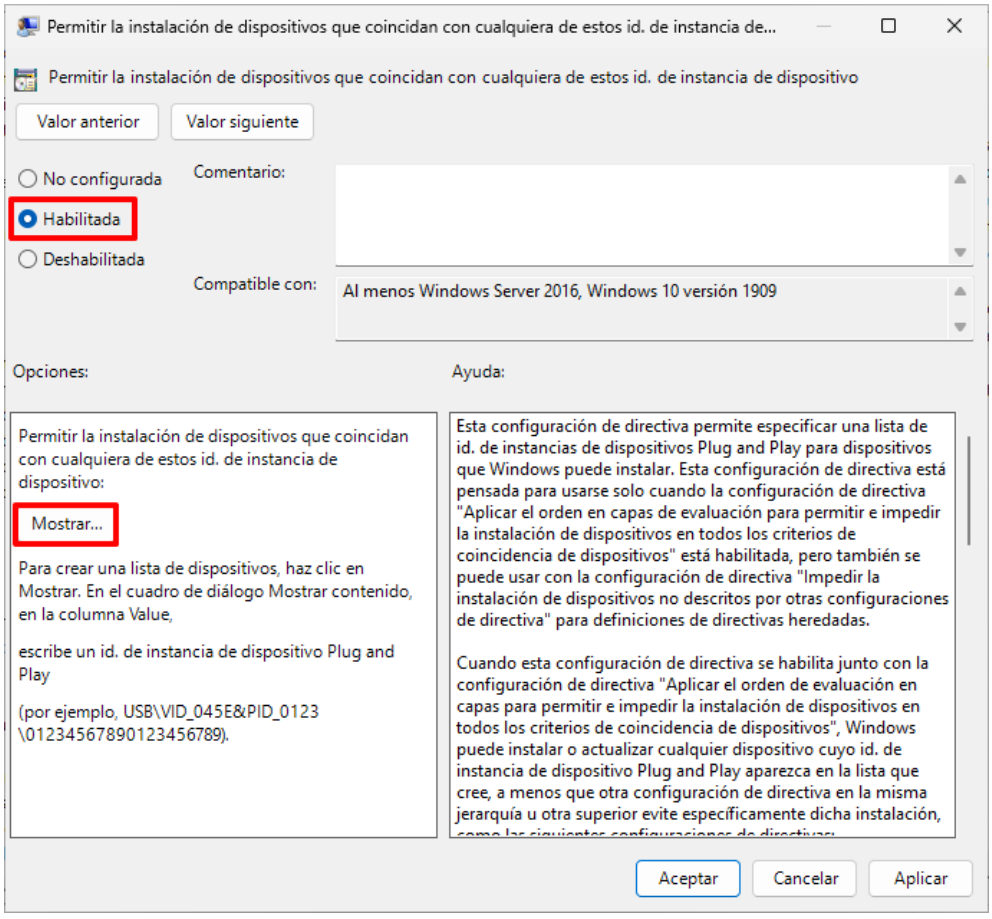
Los pasos definidos a continuación deberá realizarlos sobre el equipo afectado del entorno en el cual se está habilitando el uso de dispositivos USB.

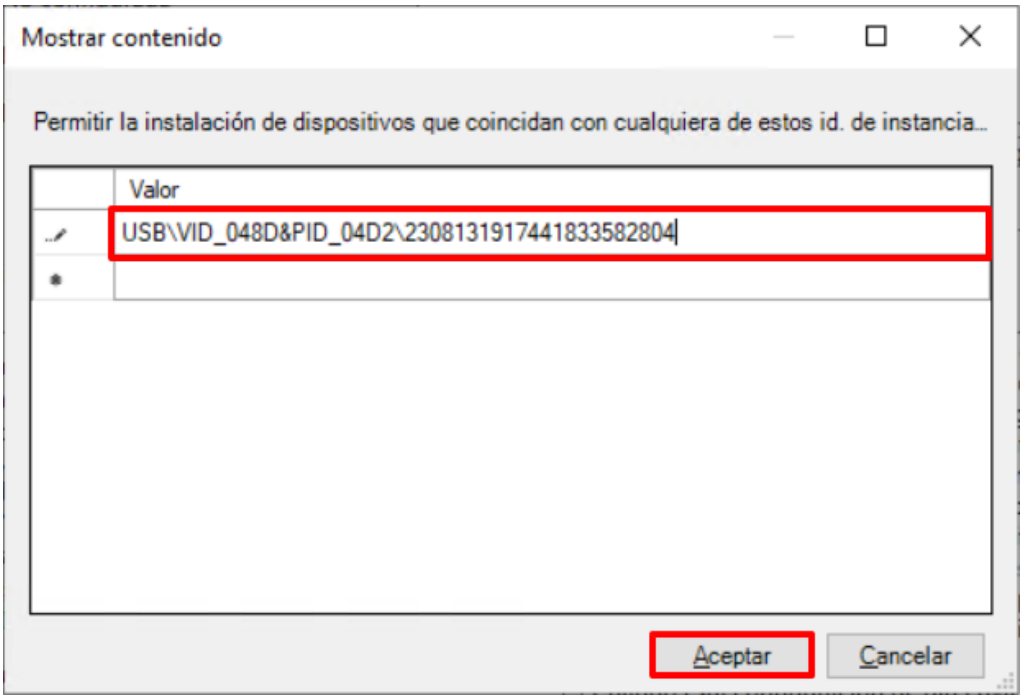
Paso	Descripción
11.	Inicie sesión en el equipo cliente donde pretende habilitar el uso de un dispositivo USB.
12.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 

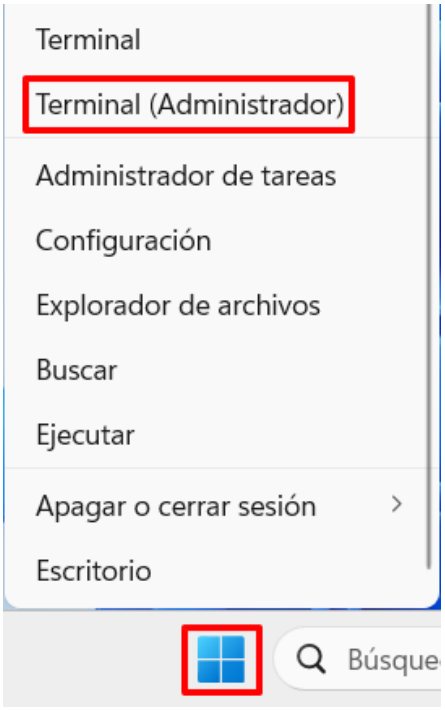
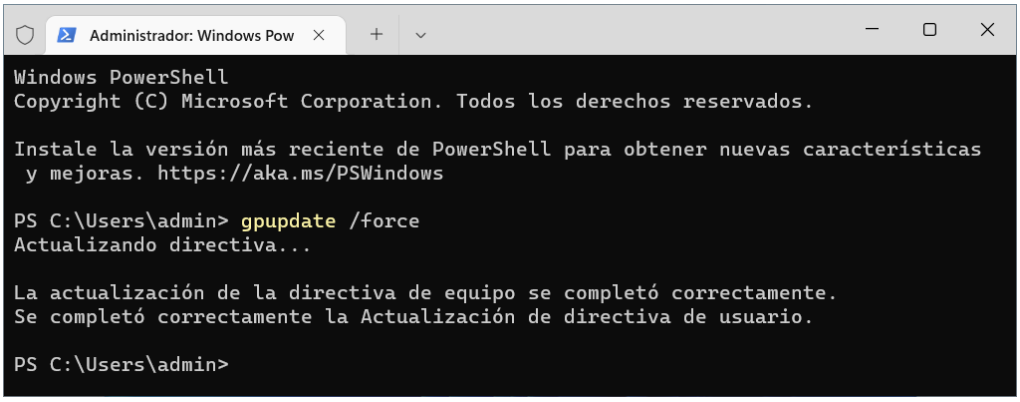
Paso	Descripción
13.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar. Haga clic derecho sobre el dispositivo y seleccione la opción del menú contextual “Propiedades”.  **Nota:** Debido a la inexistencia de controlador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

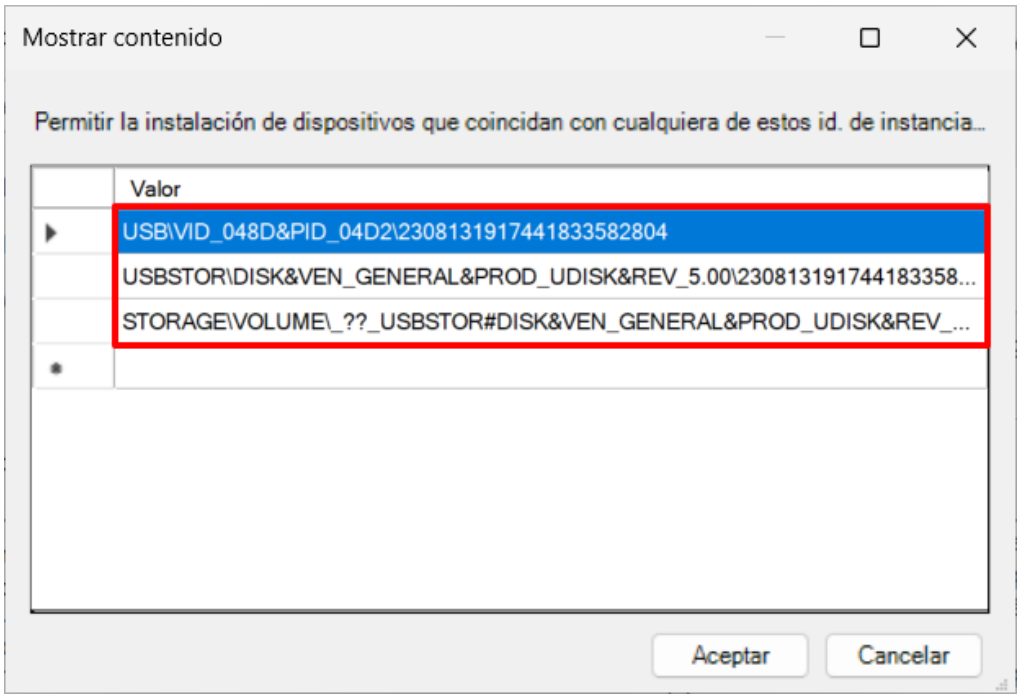
Paso	Descripción
14.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Ruta de acceso a la instancia del dispositivo”. 
15.	Seleccione el identificador y anótelo para poder introducirlo más adelante.  **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

Paso	Descripción
16.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
17.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 

Paso	Descripción
18.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos"** 
19.	En el panel derecho, haga doble clic sobre la directiva "**Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo**". Pulse sobre "Habilitada" y pulse el botón Mostrar…". 

Paso	Descripción
20.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la línea en blanco para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Verifique el identificador introducido y pulse “Aceptar” para continuar. 
21.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo”.
22.	Sin cerrar el “Editor de directivas de grupo local”, continue con el siguiente paso.

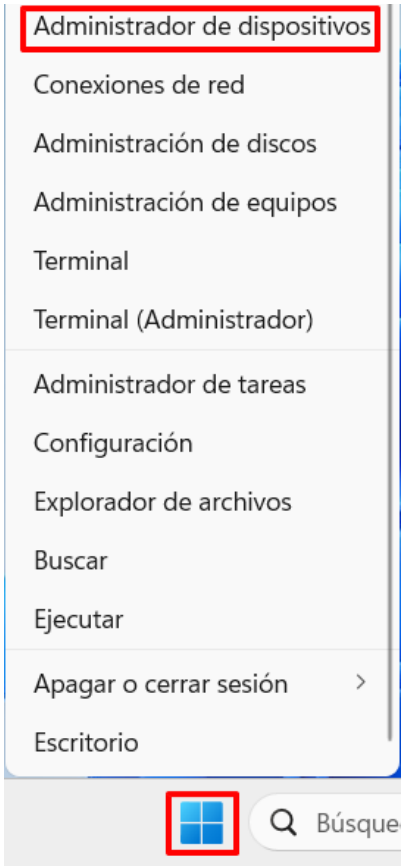
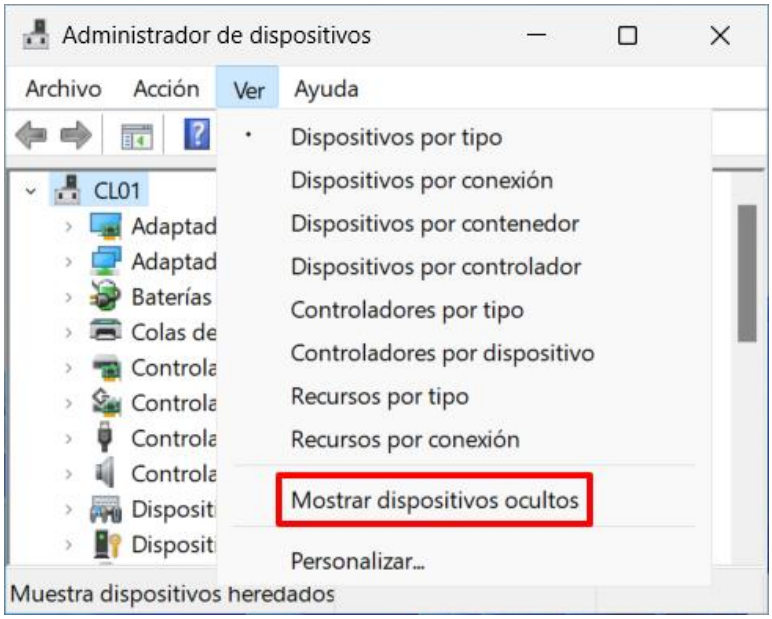
Paso	Descripción
23.	Sobre el equipo en el que se desea el uso de un dispositivo USB, haga clic derecho sobre el botón de “Inicio” y pulse sobre “Terminal (Administrador)”. 
24.	Ejecute el siguiente comando en la consola y espere a que finalice. > gpupdate /force 

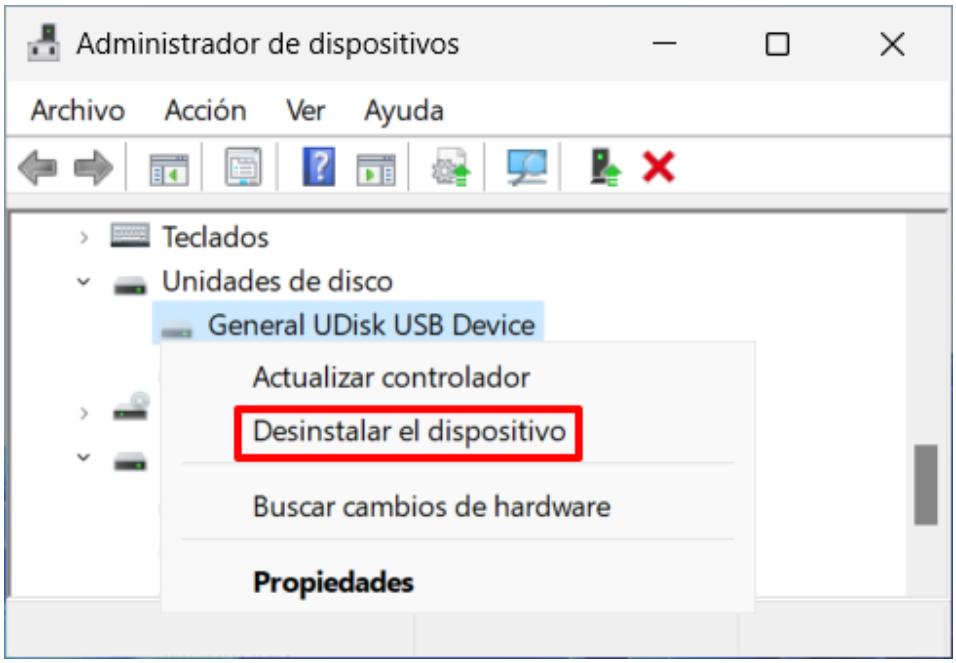
Paso	Descripción
25.	Ejecute de nuevo los pasos 13 a 24 con el objetivo de añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows. 

ANEXO B.3.1.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

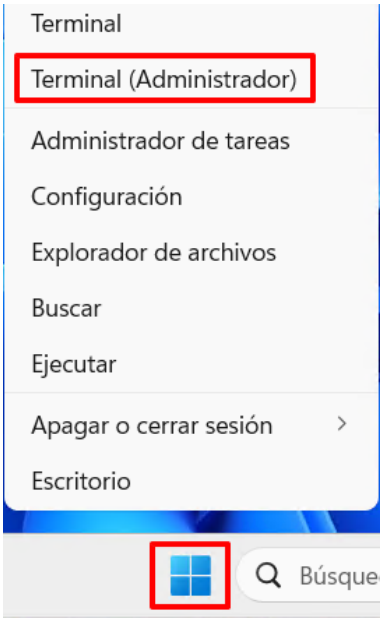
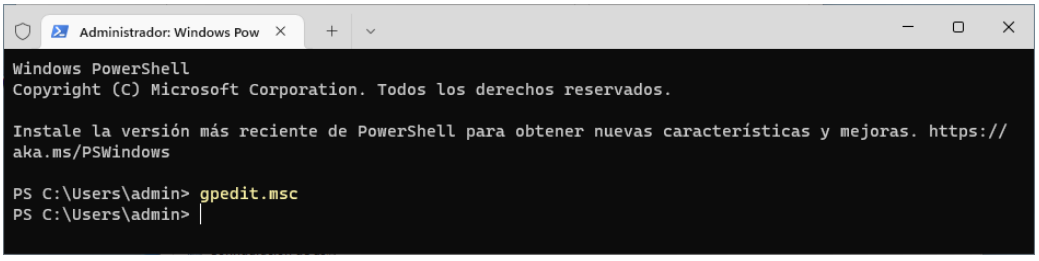
Tras la instalación del dispositivo y su posterior uso, es posible volver al estado anterior de bloqueo del uso de dispositivos USB dado de alta previamente. Para ello deberán seguir los siguientes pasos.

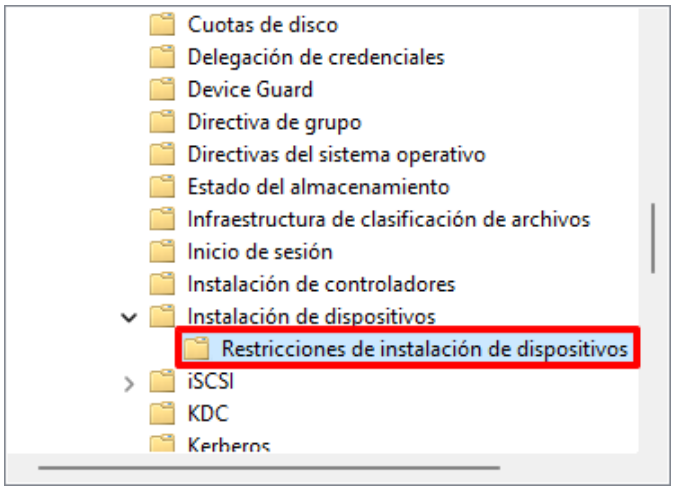
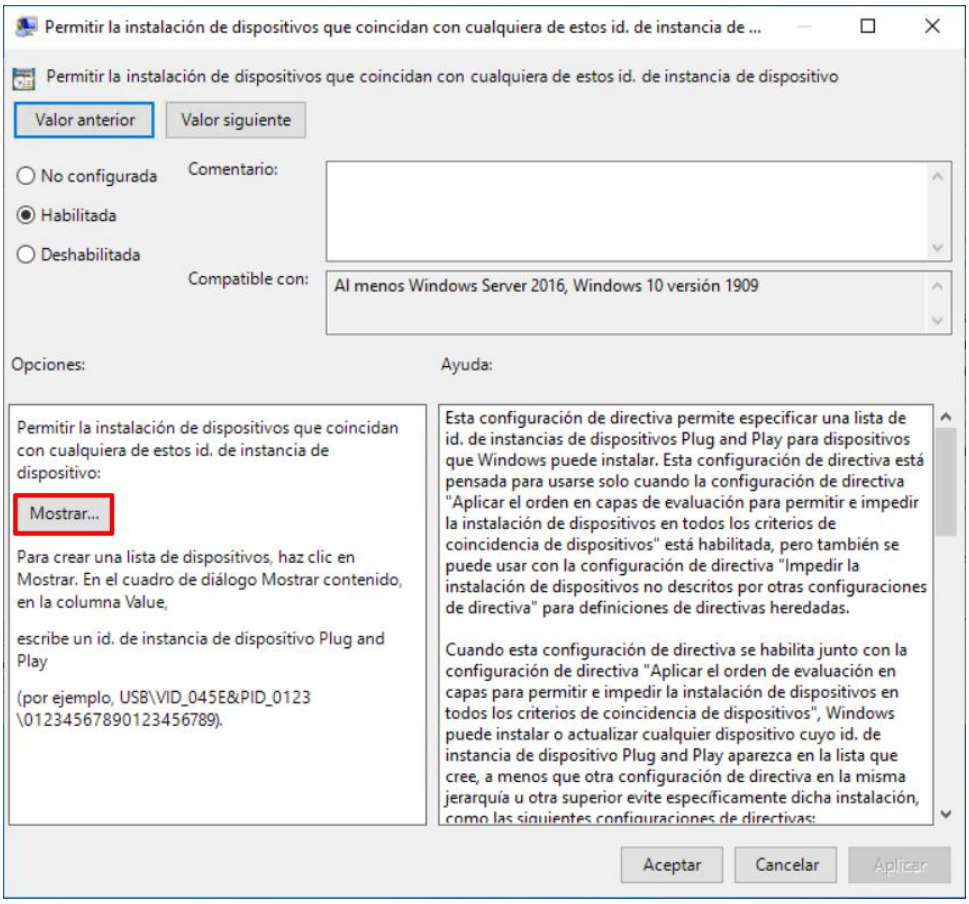
Paso	Descripción
26.	Inicie sesión en el equipo cliente donde pretende eliminar el uso de un dispositivo USB.

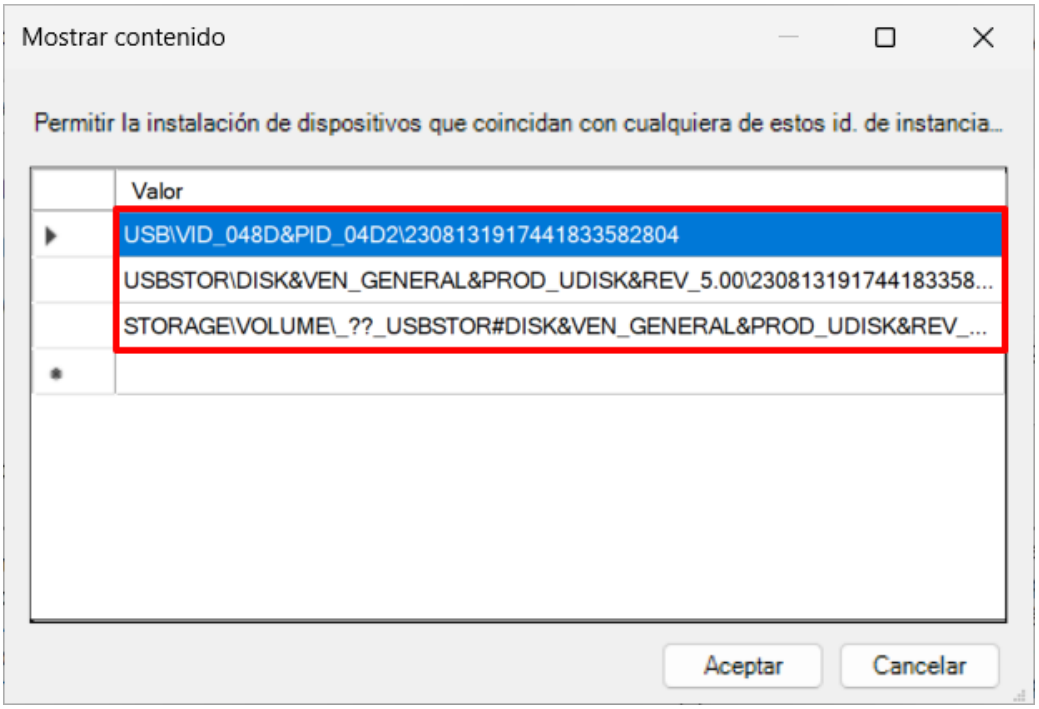
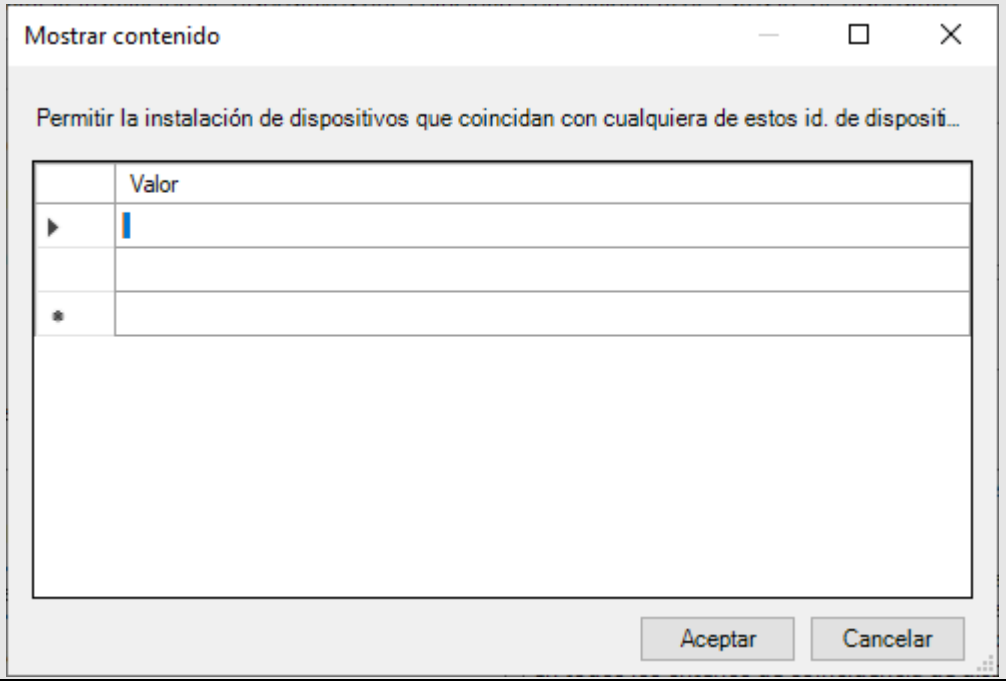
Paso	Descripción
27.	Haga clic derecho sobre el botón de “Inicio” y seleccione “Administrador de dispositivos”. 
28.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

Paso	Descripción
29.	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”. 
30.	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
31.	Inicie sesión en el equipo cliente donde pretende eliminar el uso de un dispositivo USB.
32.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
33.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 

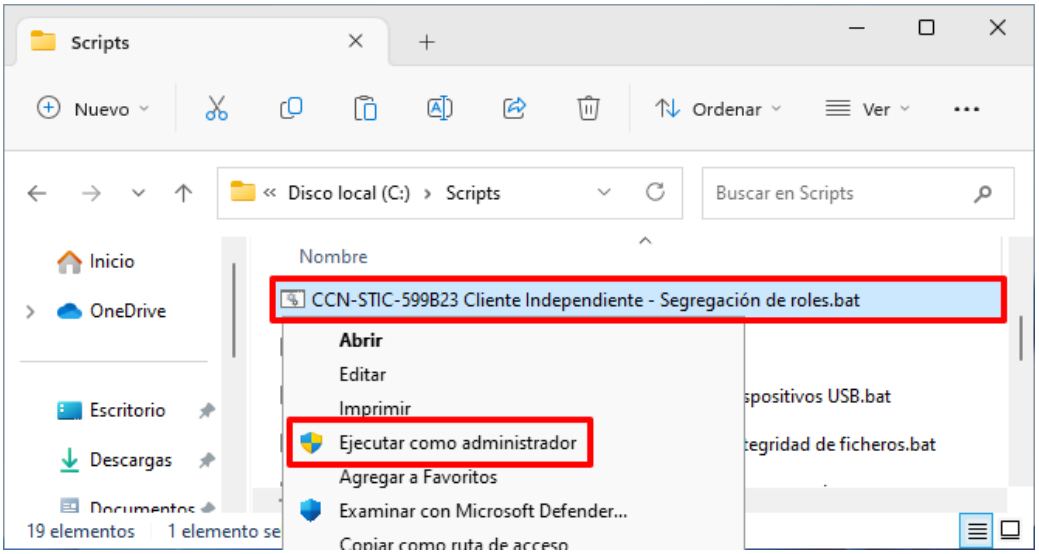
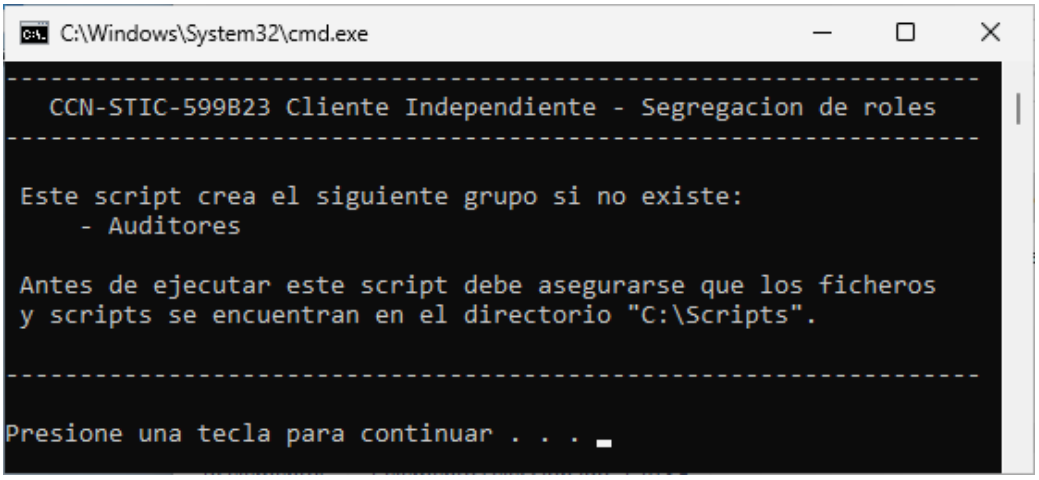
Paso	Descripción
34.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos"** 
35.	En el panel derecho, haga doble clic sobre la directiva "**Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de instancia de dispositivo**", la cual debe estar configurada como "Habilitada" y dentro de ella pulse el botón Mostrar…". 

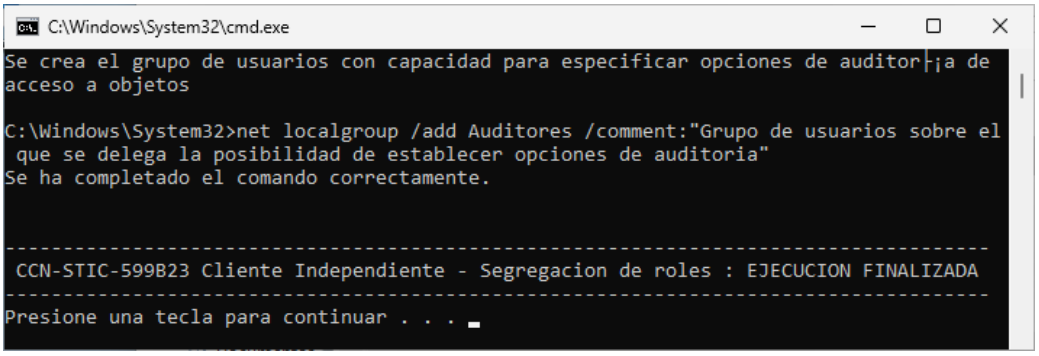
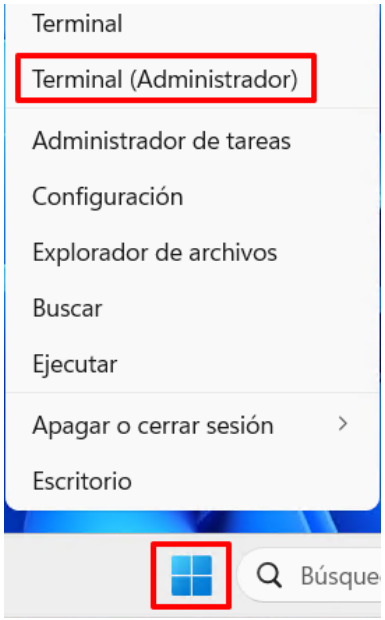
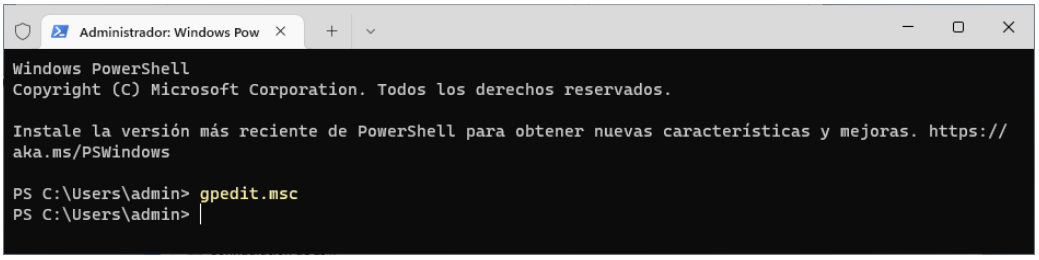
Paso	Descripción
36.	En la ventana emergente “Mostrar contenido” elimine los identificadores correspondientes a los dispositivos sobre los cuales ya no se desea su uso. Pulse “Aceptar” para continuar.  **Nota:** No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto 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. 

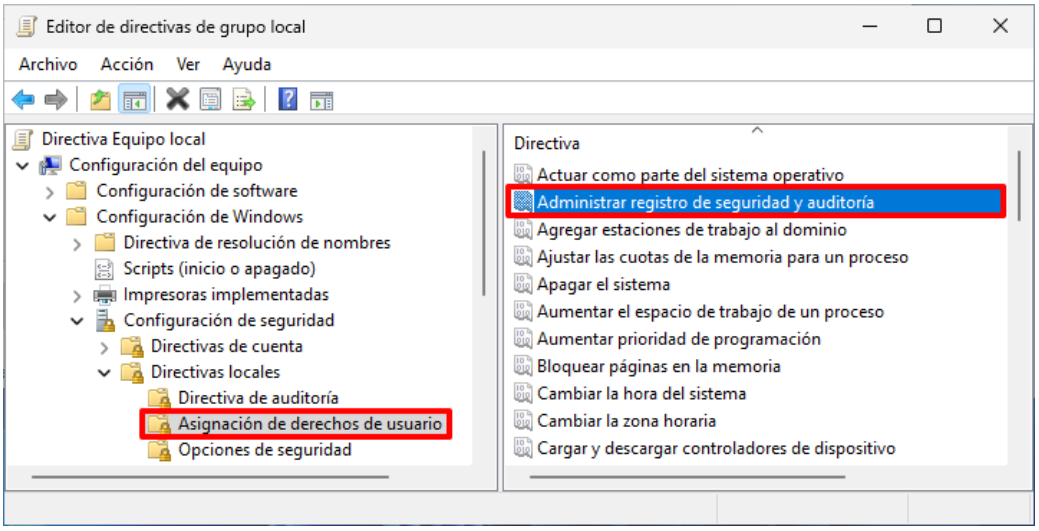
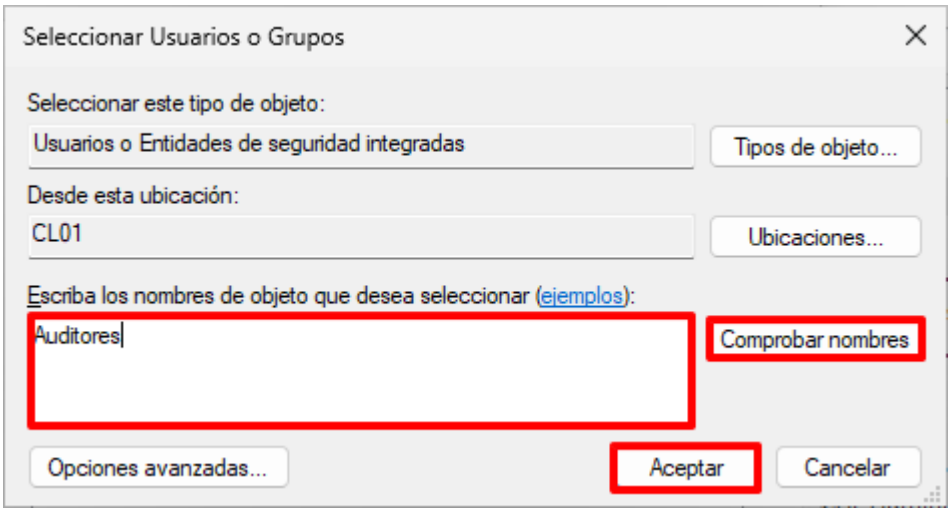
ANEXO B.3.2. SEGREGACIÓN DE FUNCIONES Y TAREAS (PRIVILEGIOS DE AUDITORÍA)

Los siguientes pasos definen las labores para permitir que solo aquellas cuentas deseadas sean capaces de generar auditorías en sistemas operativos Windows Cliente.

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 cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Diríjase al directorio "C:\Scripts", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Cliente Independiente – Segregación de roles.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
3.	A continuación, se le informará de las acciones que realizará el script. Pulse una tecla para continuar. 

Paso	Descripción
4.	Espere a que finalice la ejecución y pulse una tecla para finalizar. 
5.	Posteriormente, haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
6.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 

Paso	Descripción
7.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → 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"**. 
8.	En la ventana emergente, pulse sobre "Agregar usuario o grupo…". A continuación, introduzca el nombre del grupo "Auditores", haga uso del botón "Comprobar nombres" para completar la información y pulse "Aceptar". 

ANEXO B.3.3. 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.2.3 PROTECCIÓN FRENTE A CÓDIGO DAÑINO". Las configuraciones definidas bajo el presente apartado son las siguientes:

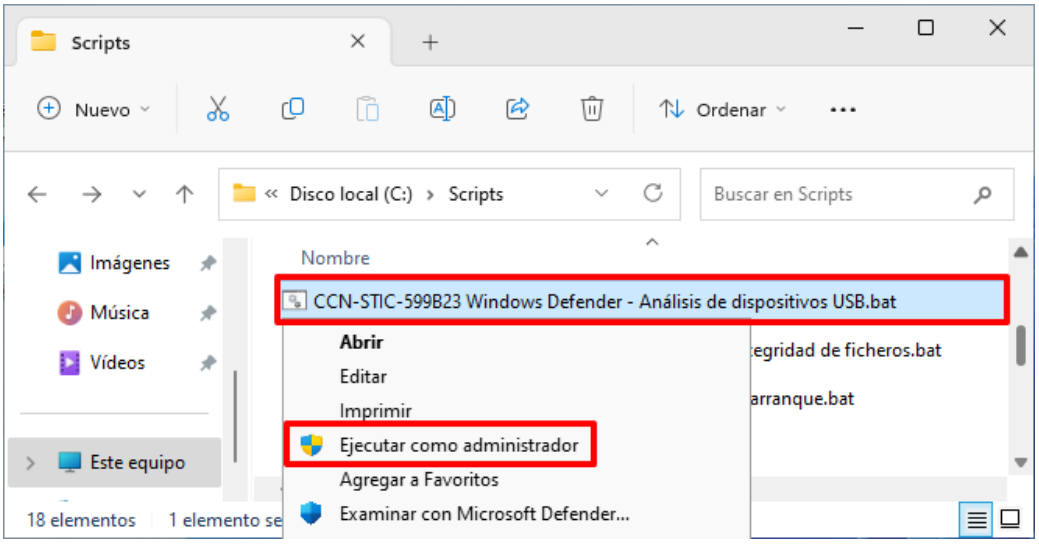
a) Análisis de dispositivos de almacenamiento extraíble cuando estos se conectan al equipo.

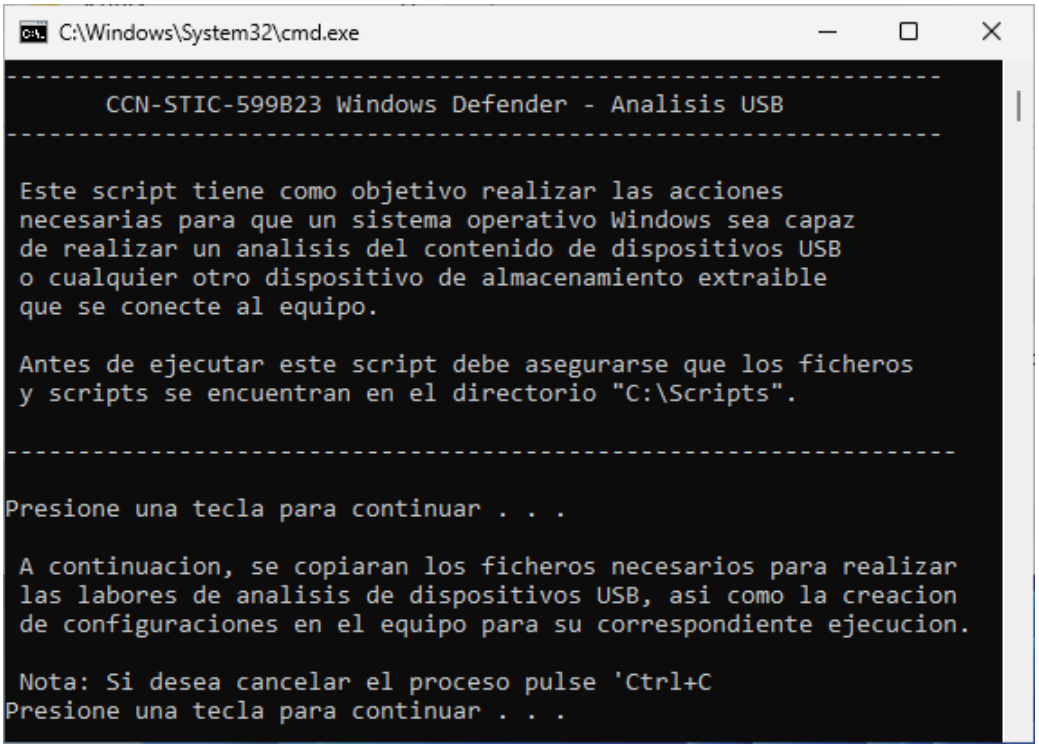
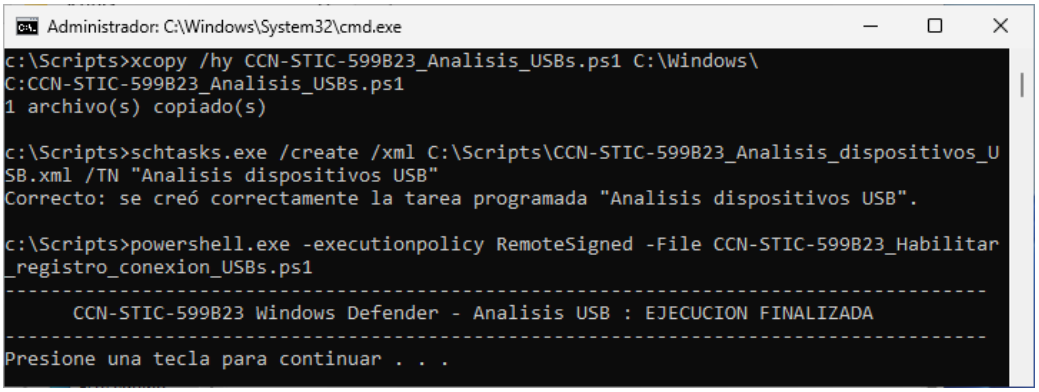
b) Análisis del sistema operativo en el arranque del sistema.

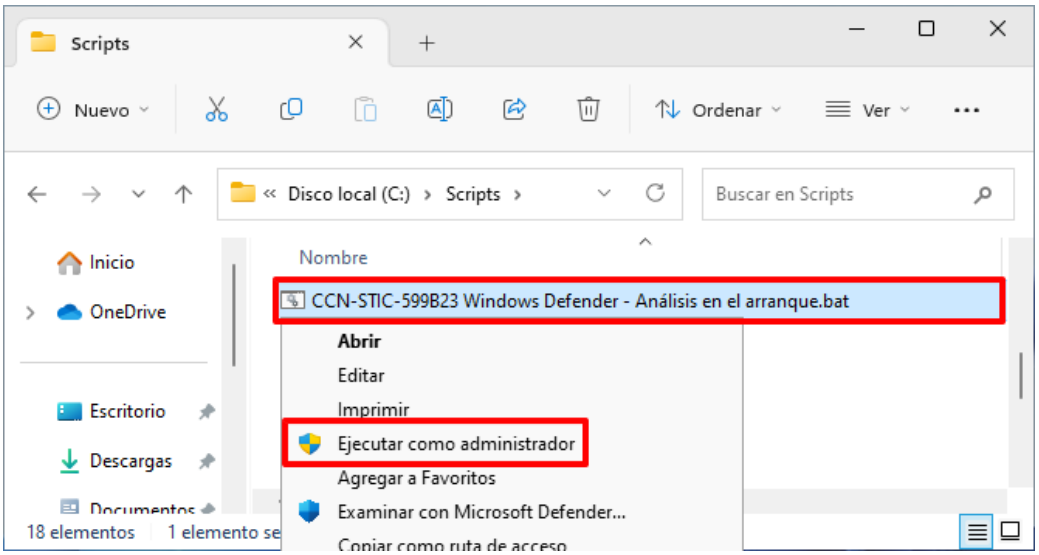
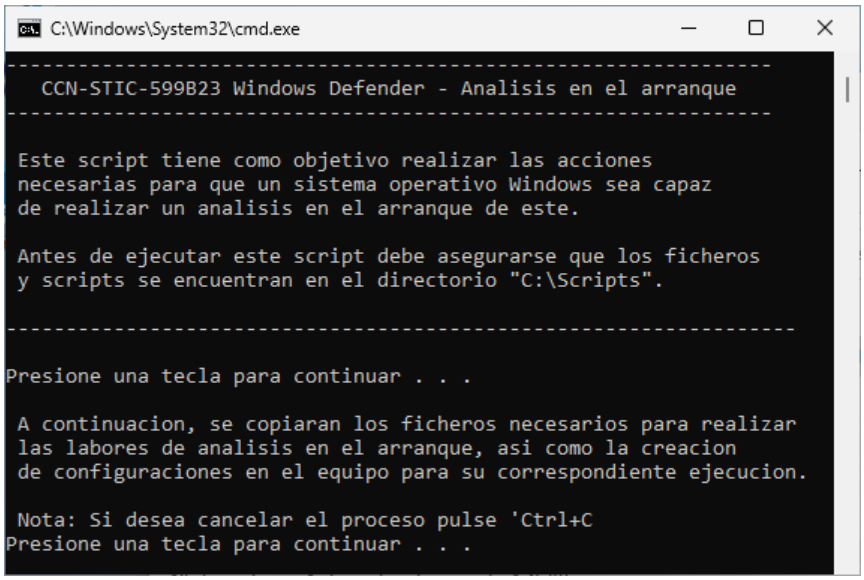
Nota: No se considera de aplicación las configuraciones del presente apartado si no se han aplicado el resto de configuraciones de esta herramienta según el punto indicado con anterioridad.

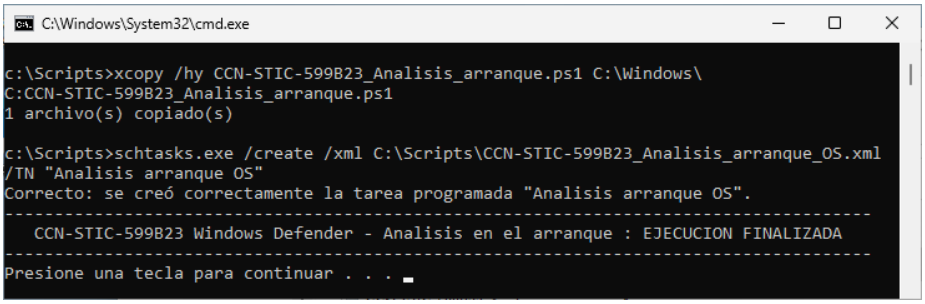
Deberá decidir si implementar toda o parte de la configuración según se expone en el presente paso a paso.

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

Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Diríjase al directorio "C:\Scripts", y haga clic derecho sobre el fichero "**CCN-STIC-599B23 Windows Defender – Análisis de dispositivos USB.bat**" y seleccione la opción del menú contextual "Ejecutar como Administrador". 
3.	Pulse una 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-599B23 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.

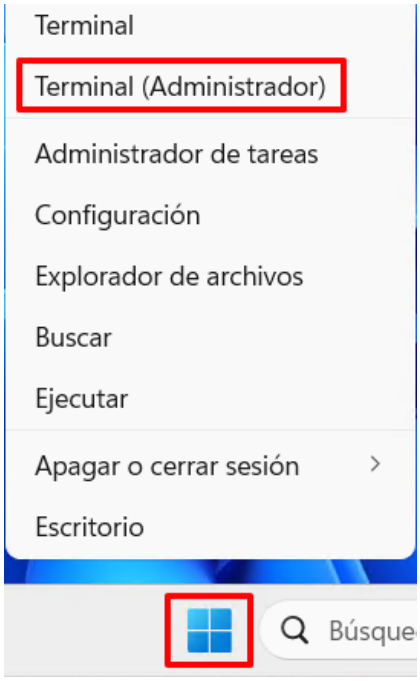
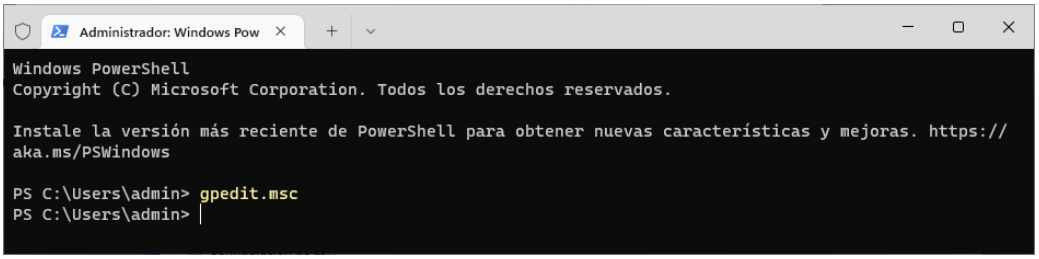
ANEXO B.4. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

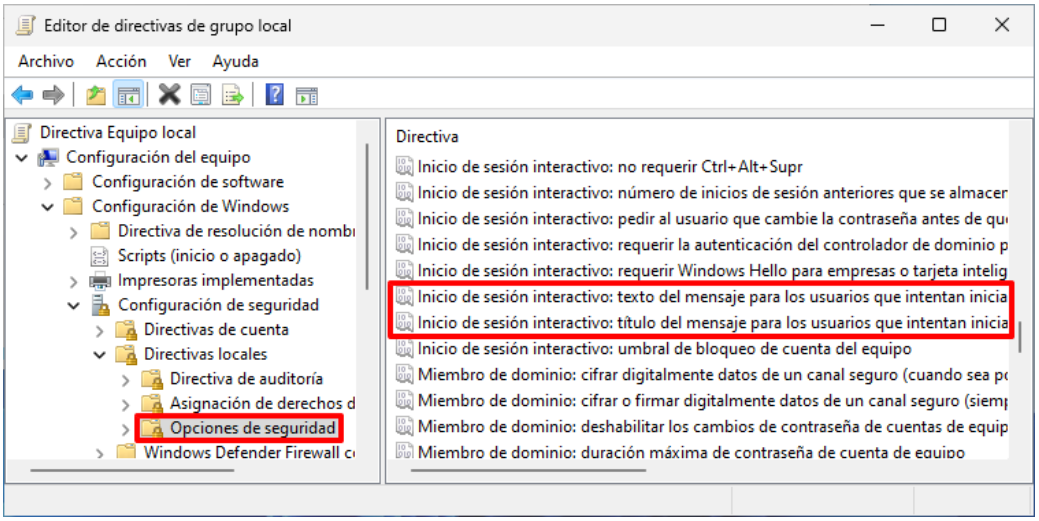
ANEXO B.4.1. INFORMACION DE OBLIGACIONES

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 cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

Paso	Descripción
2.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
3.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 
4.	A continuación, despliegue el nodo: **“Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”**.

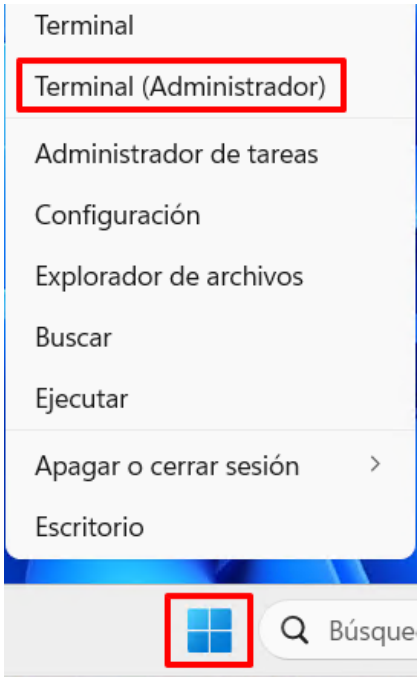
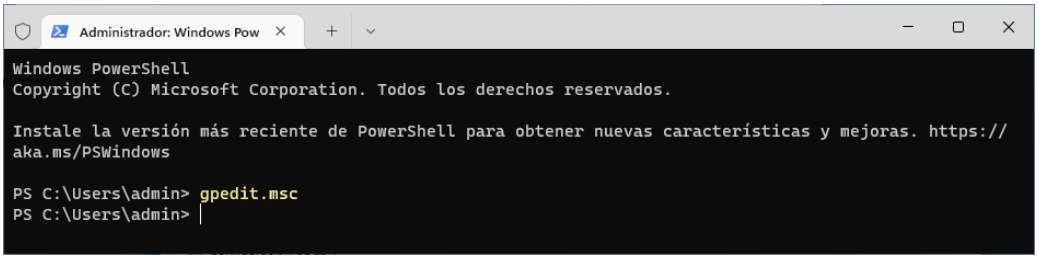
Paso	Descripción
5.	En el panel derecho identifique las siguientes directivas y edítelas a continuación: – Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión – Inicio de sesión interactivo: título del mensaje para los usuarios que intentan inicia una sesión 
6.	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.

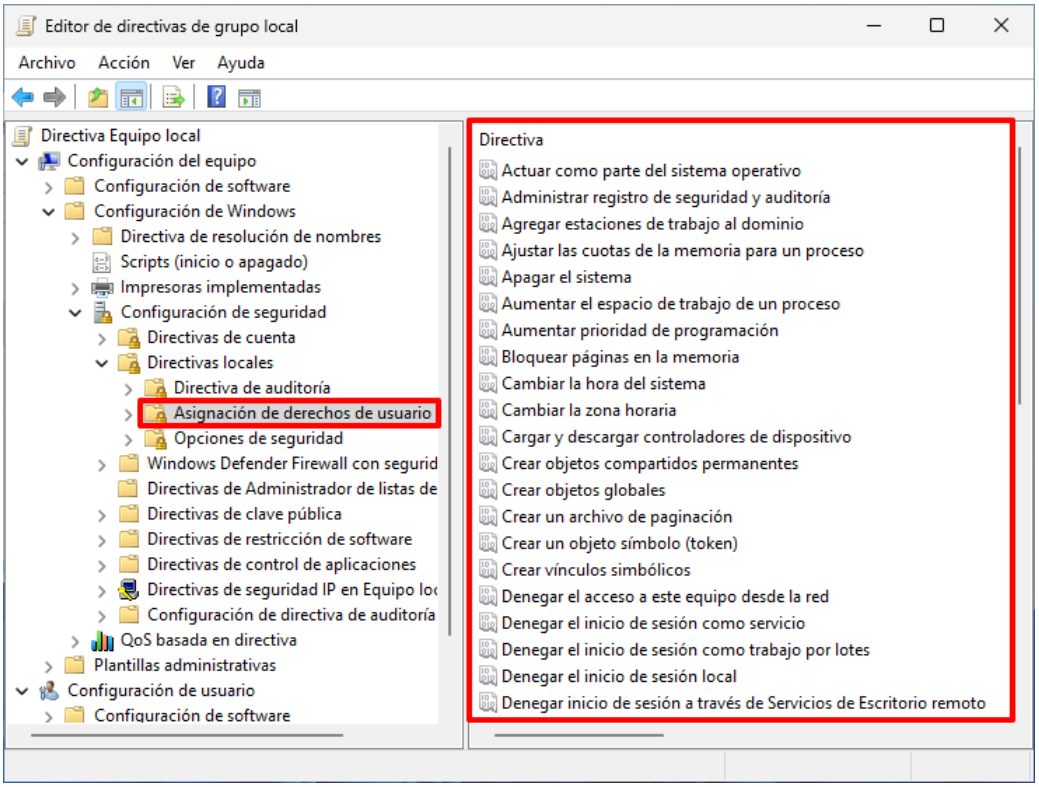
ANEXO B.4.2. PRIVILEGIOS

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 cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

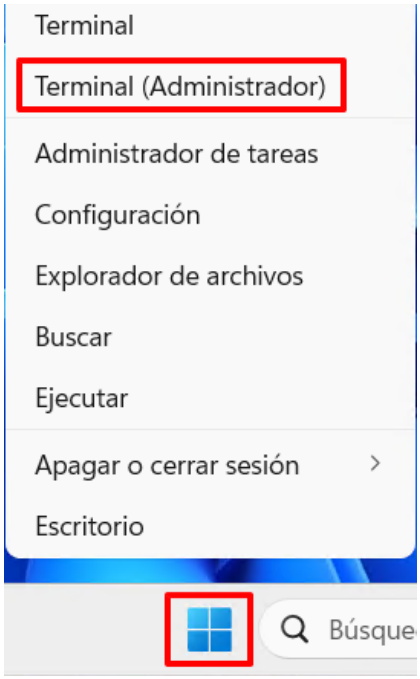
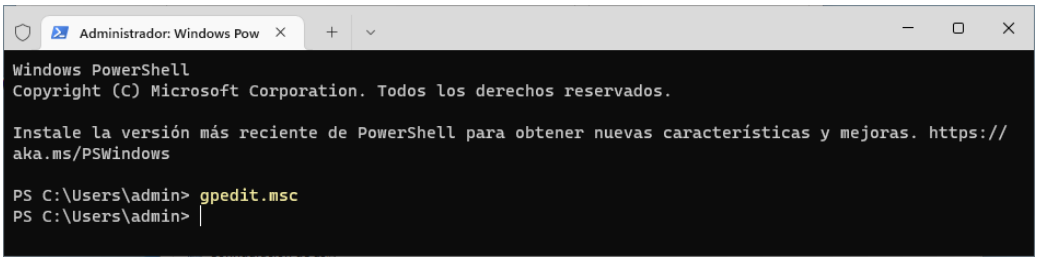
Paso	Descripción
2.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
3.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
4.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"**.

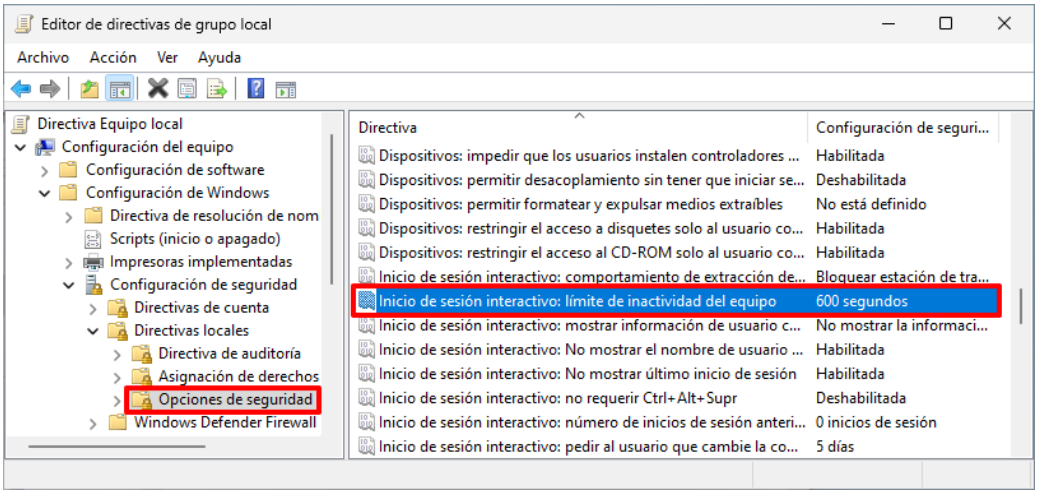
Paso	Descripción
5.	En el panel derecho evalúe todas las directivas de privilegios y edítelas a continuación. Tenga especial consideración con las siguientes directivas orientadas a los tipos de inicio de sesión, sobre todo cuando se realicen procesos automatizados en los sistemas de información o en los clientes independientes. – 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  **Nota:** La configuración establecida trata de restringir todo lo posible los privilegios de los usuarios, pero manteniendo la usabilidad dentro de los sistemas.

ANEXO B.4.3. 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 cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
3.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
4.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**.

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

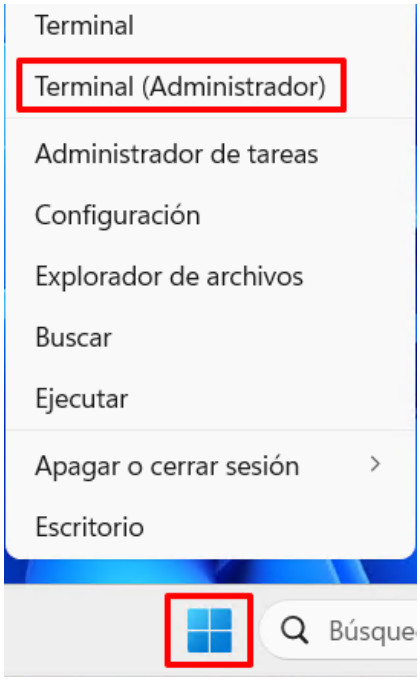
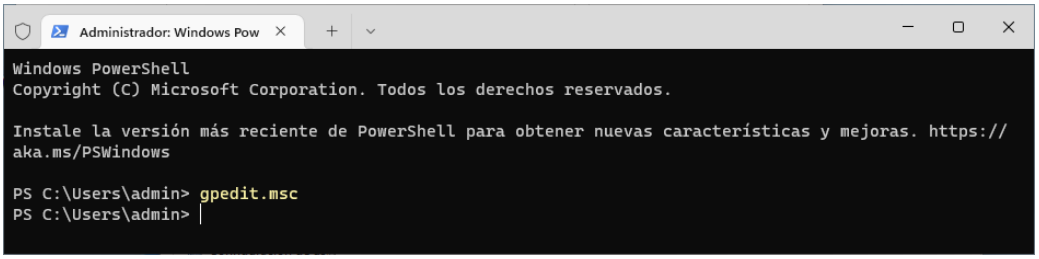
ANEXO B.4.4. OPCIONES DE SEGURIDAD

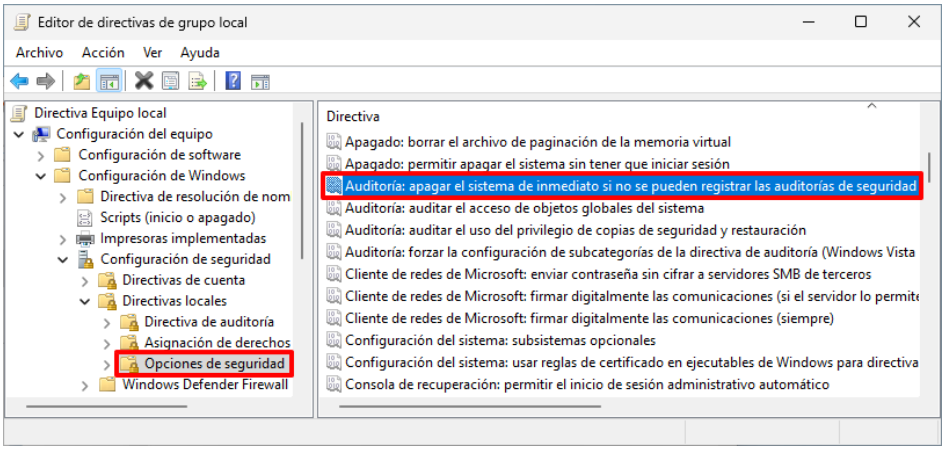
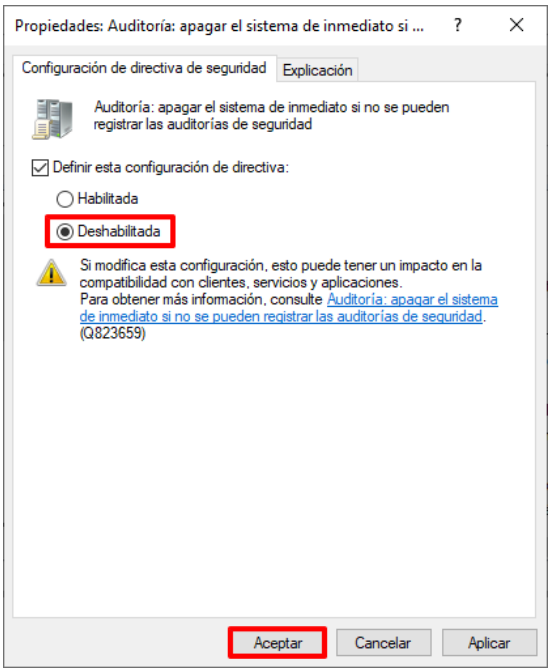
La sección y los pasos descritos a continuación, permiten establecer las modificaciones y/o adaptaciones de la configuración establecida en los apartados anteriores del presente documento.

ANEXO B.4.4.1. REGISTRO DE LAS AUDITORÍAS DE SEGURIDAD

El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a adaptar la configuración establecida sobre los equipos de tipo Clientes Independiente, modificando la directiva de auditoría que puede provocar el apagado inesperado de los equipos del sistema.

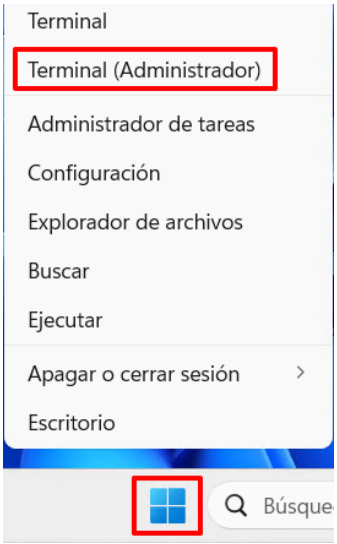
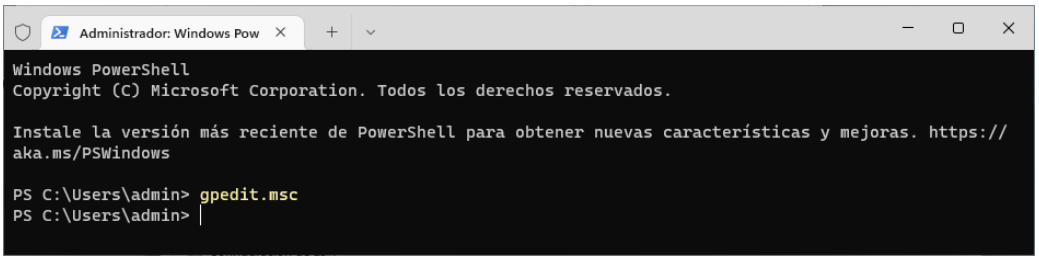
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

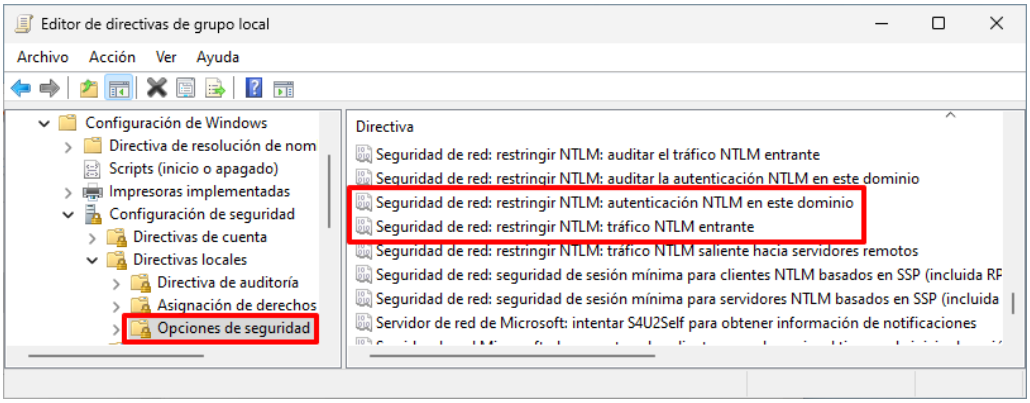
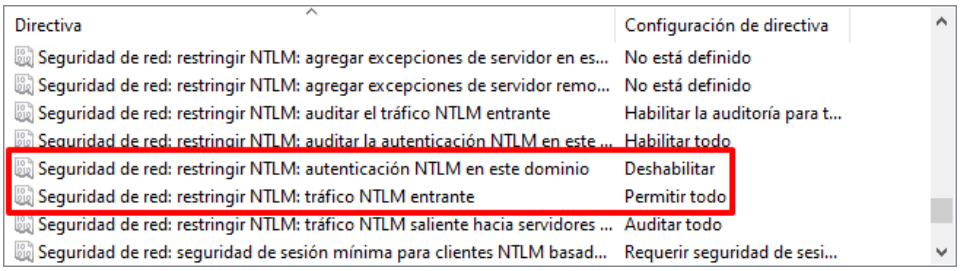
Paso	Descripción
2.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
3.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
4.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**.

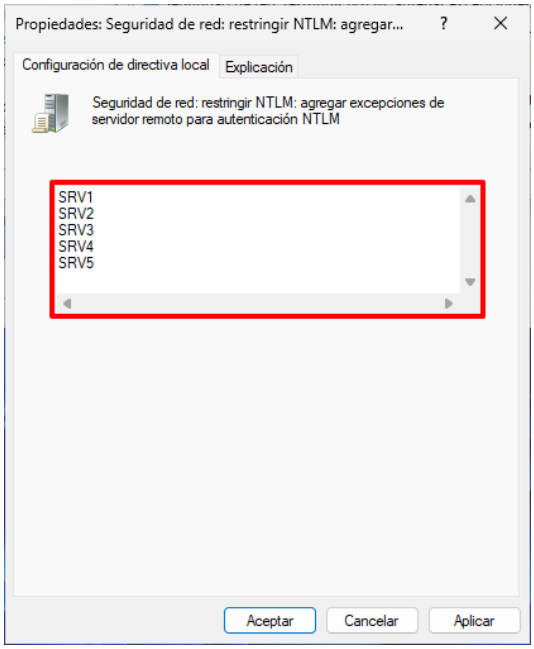
Paso	Descripción
5.	En el panel derecho identifique la directiva “Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad”. 
6.	Cuando los recursos hardware en los sistemas TIC son aprovisionados de una forma muy limitada, pueden producirse situaciones en las que 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.

ANEXO B.4.4.2. HABILITAR NTLM

El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad a adaptar la configuración establecida sobre los equipos de tipo Clientes Independiente, modificando las directivas que impiden la comunicación NTLM con los diferentes servicios que puede proporcionar el entorno.

Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Haga clic derecho sobre el botón "Inicio" y pulse sobre "Terminal (Administrador)". 
3.	En la consola de PowerShell ejecute el comando "**gpedit.msc**" para abrir el Editor de directivas de grupo local. 
4.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"**.

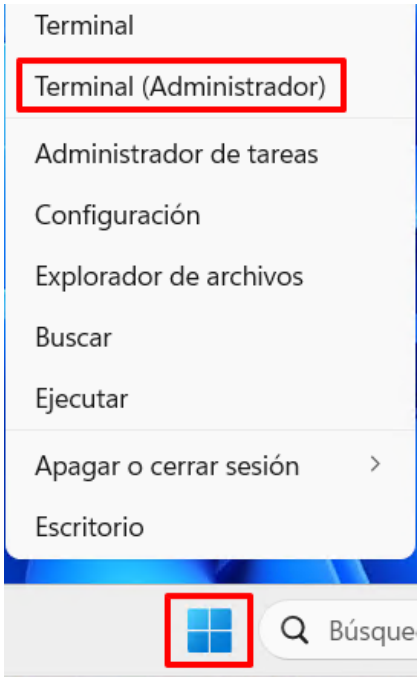
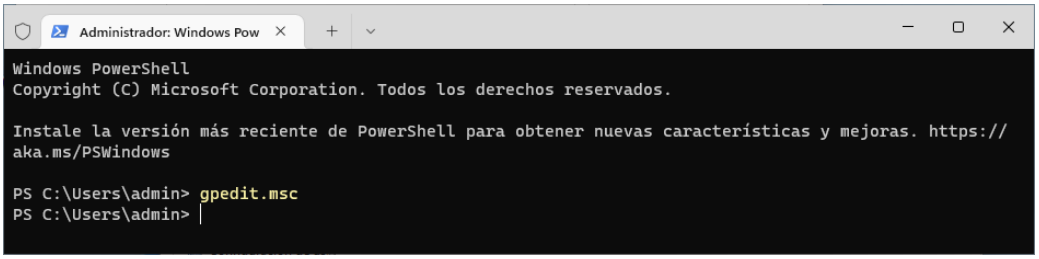
Paso	Descripción
5.	En el panel derecho identifique las siguientes directivas: – Seguridad de red: restringir NTLM: autenticación NTLM en este dominio – Seguridad de red: restringir NTLM: tráfico NTLM entrante 
6.	Cuando las presentes directivas se encuentran configuradas denegando la comunicación NTLM, se pueden generar errores a la hora de utilizar por parte de los clientes algunos de los servicios que ofrece el entorno. Para habilitar NTLM y evitar estas casuísticas en caso de que la organización lo requiera, deberá configurar las directivas indicadas de la siguiente manera: – Seguridad de red: restringir NTLM: autenticación NTLM en este dominio: Deshabilitar – Seguridad de red: restringir NTLM: tráfico NTLM entrante: Permitir todo  **Nota:** Tenga en consideración que puede ser necesario aplicar la configuración de este apartado a todo el entorno dependiendo del servicio ofrecido por la organización.

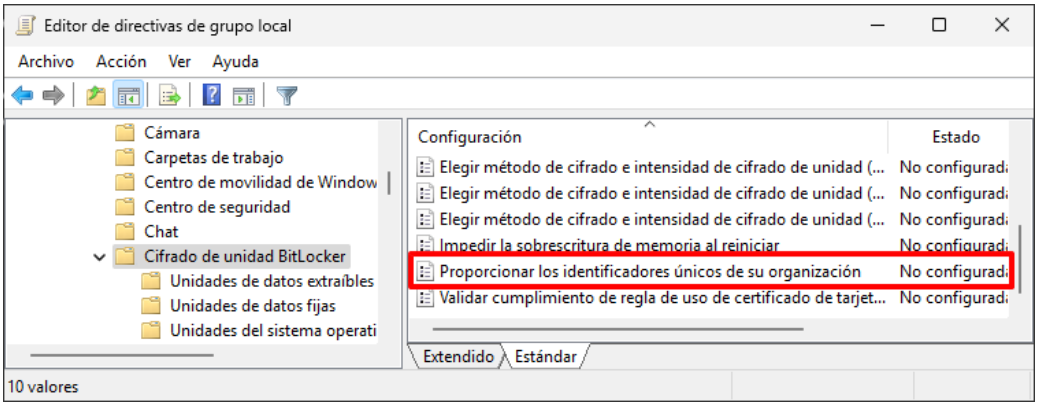
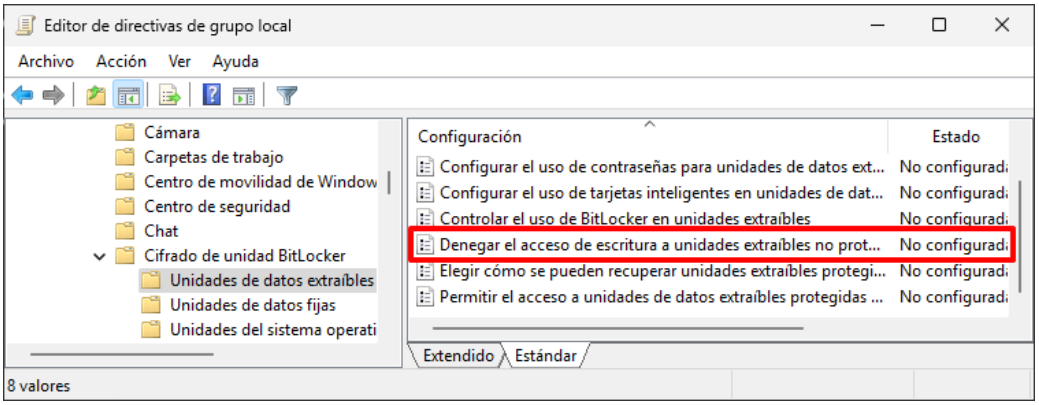
Paso	Descripción
7.	Con el fin de mantener la seguridad de la infraestructura, si se conocen los servidores de los cuales los clientes van a consumir sus servicios, se puede obviar la modificación realizada en pasos anteriores y establecer una lista de excepción de servidores para NTLM en la directiva "Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM".  **Nota:** Tenga en consideración que puede ser necesario aplicar la configuración de este apartado a todo el entorno dependiendo del servicio ofrecido por la organización.

ANEXO B.4.5. CIFRADO DE UNIDAD DE BITLOCKER

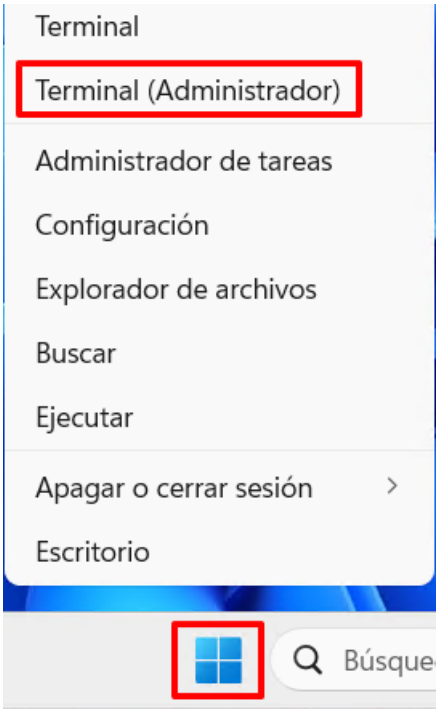
El presente apartado tiene como objetivo ayudar al personal que ha implementado las medidas de seguridad correspondientes a la protección de dispositivos portátiles mediante BitLocker, adaptando las configuraciones establecidas sobre los equipos de tipo Clientes Independientes, modificando las directivas que afectan a los dispositivos removibles y su uso dependiendo del cifrado.

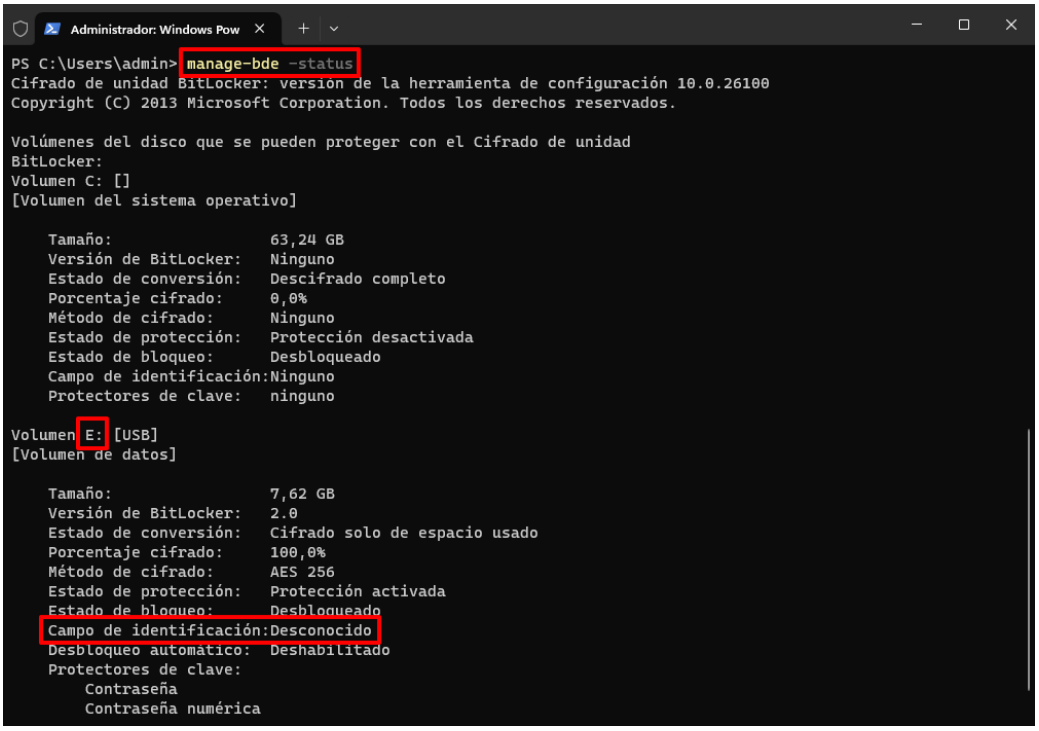
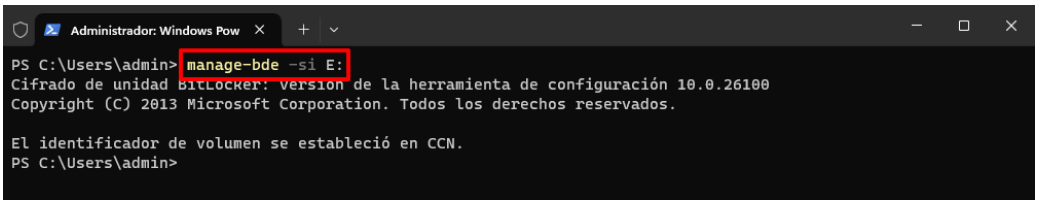
Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.

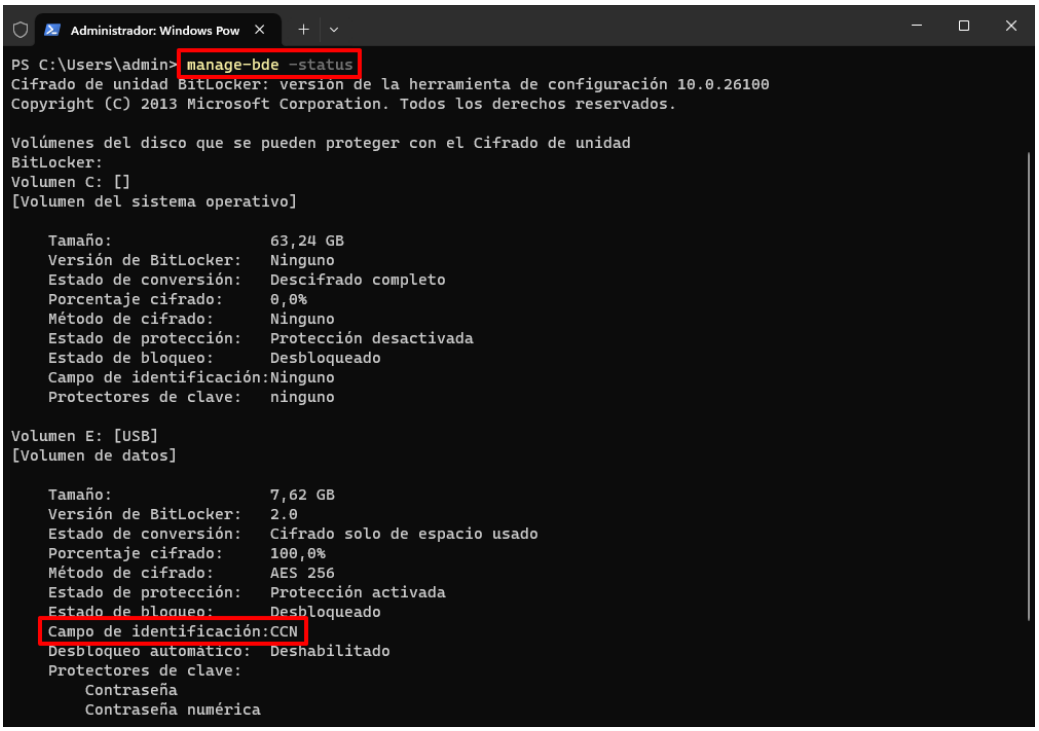
Paso	Descripción
2.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 
3.	En la consola de PowerShell ejecute el comando “**gpedit.msc**” para abrir el Editor de directivas de grupo local. 

Paso	Descripción
4.	A continuación, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker"**. Identifique en el panel derecho la directiva "**Proporcionar los identificadores únicos de su organización**". 
5.	De forma adicional, despliegue el nodo: **"Directiva Equipo local → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades datos extraíbles"**. Identifique en el panel derecho la directiva "**Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker**". 

Paso	Descripción
6.	Con ambas directivas identificadas, a continuación, se describirán los diferentes casos posibles dependiendo de las necesidades de su organización: – Los dispositivos removibles solo se podrán utilizar en modo escritura si han sido **cifrados en el propio equipo utilizando identificadores para su filtrado** por organización, es decir, mantener la configuración establecida por la presente guía, en cuyo caso no se deberá hacer nada más que seguir el paso a paso correspondiente. – Los dispositivos removibles solo podrán ser utilizados en modo escritura si han sido **cifrados en cualquier equipo o sistema**, incluyendo uno ajeno a la organización. En este caso deberá establecer como "**Deshabilitada**" la directiva "**Proporcionar los identificadores únicos de su organización**", además de modificar la directiva "**Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker**", estableciéndola en "**Habilitada**" y desmarcando la opción "**No permitir el acceso de escritura a dispositivos configurados en otra organización**" dentro de la directiva. – Los dispositivos removibles podrán ser utilizados en modo escritura **incluso si no se encuentran cifrados**. En este caso, deberá establecer como "**Deshabilitada**" tanto la directiva "**Proporcionar los identificadores únicos de su organización**", como "**Denegar el acceso de escritura a unidades extraíbles no protegidas por BitLocker**".
7.	En el supuesto de que para su organización vaya a utilizar la configuración por defecto de la presente guía, es decir, que solo se podrán utilizar en modo escritura si han sido **cifrados en el propio equipo utilizando identificadores para su filtrado** por organización, pueden existir dispositivos removibles que **ya se encuentren cifrados** mediante BitLocker **previamente a la configuración** de seguridad. Para poder incluir el identificador configurado al dispositivo removible previamente cifrado, deberá establecerlo mediante comandos.
8.	Inicie sesión en un cliente independiente donde se hayan aplicado las directivas de seguridad relativas a BitLocker. Debe iniciar sesión con una cuenta que sea Administrador. **Nota:** Es necesario que el equipo donde se inicia sesión cuente con las directivas de BitLocker configuradas, en especial la directiva "Proporcionar los identificadores únicos de su organización", en caso contrario, el paso a paso no funcionará correctamente tal como está contemplado.

Paso	Descripción
9.	Haga clic derecho sobre el botón “Inicio” y pulse sobre “Terminal (Administrador)”. 

Paso	Descripción
10.	Conecte y descifre el dispositivo removible en el equipo. En la consola de PowerShell ejecute el siguiente comando para conocer aquellos discos o volúmenes presentes en el equipo. > manage-bde -status  **Nota:** También podrá observar como el dispositivo removible muestra el "Campo de identificación" como desconocido, debido al cifrado del dispositivo sin la directiva "Proporcionar los identificadores únicos de su organización" configurada.
11.	Ejecute el siguiente comando para configurar el identificador previamente establecido en la directiva de BitLocker. > manage-bde -si [LETRA DE UNIDAD:]  **Nota:** En este ejemplo se hace uso de la letra de unidad E:.

Paso	Descripción
12.	En la consola de PowerShell ejecute el siguiente comando para comprobar que el identificador establecido se ha configurado correctamente. > manage-bde -status  **Nota:** En este ejemplo se ha establecido el identificador como “CCN”.
13.	Realice estos pasos por cada dispositivo removible a configurar con el identificador establecido en la directiva “Proporcionar los identificadores únicos de su organización”, de esta manera no tendrá que descifrar cada dispositivo y volver a cifrarlo tras la aplicación de las directivas de seguridad.

PUBLICACIONES DE DEFENSA

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