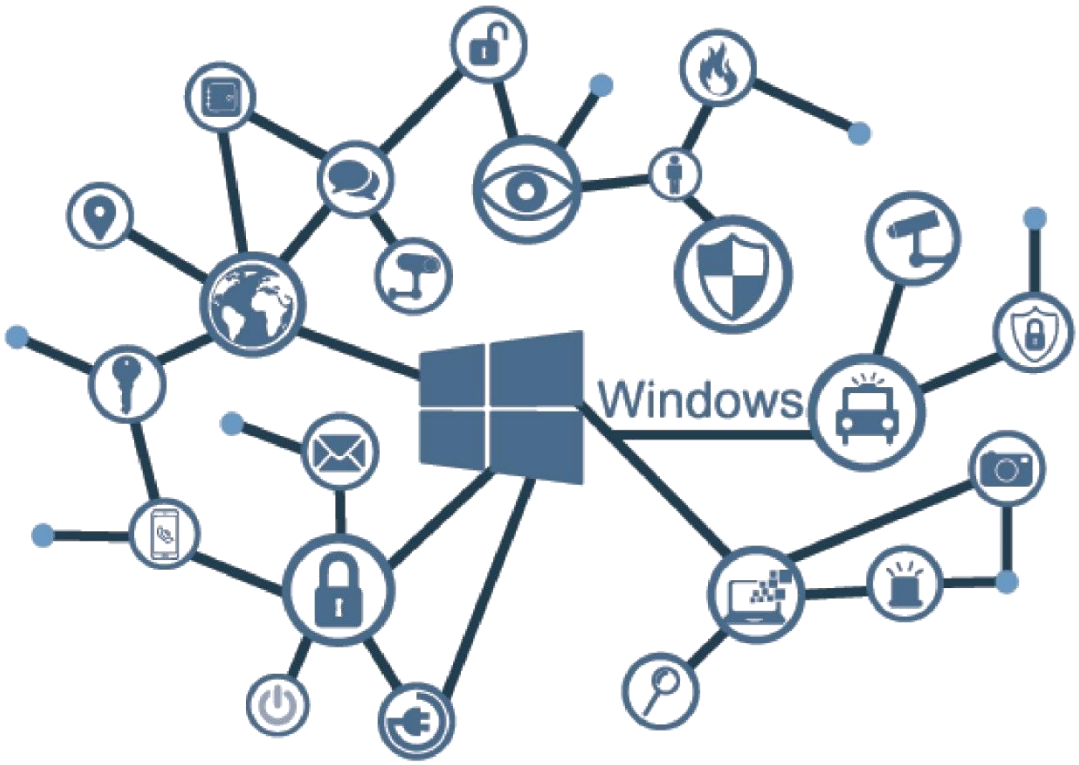
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 570A25

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



SEPTIEMBRE 2026

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

CCN centro criptológico nacional

Firmado digitalmente por CCN
Nombre de reconocimiento (DN): c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
Fecha: 2026.09.09 09:50:34 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO 083-26-273-6 (edición en línea)

Fecha de Edición: septiembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

INDICE

1. INTRODUCCIÓN

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

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

Por ejemplo, en el caso de un entorno para un servidor miembro de un dominio con Microsoft Windows Server 2025, en el que se instale Microsoft Exchange, deberán aplicarse las guías técnicas más recientes publicadas en el portal web del CCN-CERT:

a) Guía CCN-STIC-570A25 en el servidor miembro con Windows Server 2025.

b) Guía CCN-STIC sobre Internet Information Services (IIS), para la configuración segura del servicio web utilizado por Exchange.

c) Guía CCN-STIC sobre Microsoft Exchange, aplicable a los servidores que alojarán el servicio de Exchange.

Nota: Actualmente, las guías Microsoft publicadas en la serie **800** están orientadas a servicios en la **nube** adaptados al Esquema Nacional de Seguridad (ENS). Para el despliegue en infraestructura propia, las guías aplicables se encuentran en la serie **500**, que recoge la documentación más actualizada para estos escenarios.

2. OBJETO

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

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

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

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

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

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

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

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

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

3. ALCANCE

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

El documento no se centrará en una edición y versión concreta del sistema operativo, como pueda ser Windows Server 2025, sino que será de utilidad para **cualquier edición y versión de Windows Server** (siendo recomendable su aplicación desde la edición Windows Server 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 Server 2025 Standard.

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

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

Por otro lado, las configuraciones a implementar y definidas en el presente documento, según se ha indicado con anterioridad, se basan en las necesidades para **cubrir los aspectos técnicos definidos en el ENS en función de la clasificación 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.

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.

c) Nuevas medidas de seguridad. Se han incorporado nuevas medidas de seguridad basadas en el esquema de Active Directory de Windows Server 2025.

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

Dentro del presente documento, no se contempla un entorno basado en un sistema operativo Windows Server no unido a un dominio (Independiente).

4. DESCRIPCIÓN DE USO DE ESTA GUÍA

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   ii. No instalar otros sistemas operativos en el equipo.

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

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

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

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

h) Aplicación de medidas de seguridad. Para ayudar a las organizaciones a implementar las medidas de seguridad, se ha considerado la necesidad de crear tres (3) alcances de implementación o perfiles, basándose en la clasificación de la información manejada por los sistemas de información:

- ENS (Bajo / Medio / Alto).
- Difusión Limitada.
- Información Clasificada.

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:

- BAJO.
- MEDIO.
- ALTO
- DIFUSIÓN LIMITADA.
- INFORMACIÓN CLASIFICADA.

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 clasificación de la información y la categoría del sistema de información. A continuación, se define una tabla que recopila dicha información.

		CLASIFICACIÓN DE LA INFORMACIÓN/PERFIL		
		ENS	DIFUSIÓN LIMITADA	INFORMACIÓN CLASIFICADA
CATEGORÍA DEL SISTEMA DE INFORMACIÓN	BÁSICA	✓	✗	✗
	MEDIA	✓	✗	✗
	ALTA	✓	✗	✗
	DIFUSIÓN LIMITADA	✗	✓	✗
	CONFIDENCIAL RESERVADO SECRETO	✗	✗	✓

Tabla 1. Selección de perfil de medidas de seguridad

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

- Para los sistemas de información enmarcados dentro de la categoría baja, media o 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 Difusión Limitada, en todos los equipos se deberán implementar las medidas establecidas para el perfilado DIFUSIÓN LIMITADA, no pudiendo establecer configuraciones menos restrictivas en ningún otro equipo.

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

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

- Aplicación de los siguientes Anexos:

1. ANEXO A. Configuración base de Windows.
2. ANEXO B. Políticas de seguridad, auditoría y registros de eventos.
3. ANEXO C. Gestión de usuarios y políticas de cuenta y contraseña.
4. ANEXO D. Seguridad de red y firewall de Windows Defender.
5. ANEXO E. Manejo y control de dispositivos.
6. ANEXO F. Configuración de BitLocker y criptografía.
7. ANEXO G. Acceso mediante escritorio remoto.
8. ANEXO H. Acceso a auditorías mediante Nessus.

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

- Aplicación de los siguientes Anexos:

1. ANEXO A. Configuración base de Windows.
2. ANEXO E. Manejo y control de dispositivos.

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

La presente guía recoge el conjunto de medidas técnicas aplicables a sistemas operativos Windows Server, conforme a los requisitos establecidos por el Esquema Nacional de Seguridad (ENS). Estas medidas pueden aplicarse independientemente de la clasificación de la información o de la categoría del sistema de la información, y están orientadas a reforzar la seguridad del entorno mediante configuraciones concretas y verificables.

El conjunto de medidas técnicas constituye lo que se denomina Perfil de Cumplimiento Técnico Específico (PCTE) para sistemas Windows Server. Este perfil incluye controles técnicos que serán desarrollados en los apartados posteriores, donde se explicará su aplicación práctica, alcance y adaptación según el nivel de exigencia requerido por la categoría del sistema.

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

6. PERFIL DE CUMPLIMIENTO TÉCNICO ESPECÍFICO CCN-STIC

La presente guía, a su vez, recoge el conjunto de medidas técnicas de seguridad que pueden aplicarse a sistemas operativos Windows Server, conforme a los requisitos definidos en la guía de seguridad CCN-STIC-301.

El conjunto de controles constituye el Perfil de Cumplimiento Técnico Específico (PCTE) para sistemas Windows Server, ampliado respecto al perfil general para incluir consideraciones específicas en entornos que gestionan Información Clasificada. Este perfil técnico permite adaptar las configuraciones de seguridad al nivel de exigencia requerido, incorporando refuerzos adicionales cuando el entorno lo requiere.

En los siguientes apartados se desarrollarán los controles aplicables al sistema operativo Windows Server, explicando su implementación técnica y las consideraciones específicas para entornos clasificados o de uso oficial.

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

ANEXO A. CONFIGURACIÓN BASE DE WINDOWS

El presente y próximos anexos describen el paso a paso para establecer una **configuración de seguridad base** para cumplir con los requisitos técnicos aplicables establecidos según el perfilado **Difusión Limitada.** En el momento de selección de las configuraciones de seguridad deberá seleccionar aquella acorde a su perfilado (ENS, DIFUSIÓN LIMITADA, INFORMACIÓN CLASIFICADA) cuando así se indique.

La presente guía contempla la aplicación de medidas de seguridad sobre controlador de dominio y servidor miembro. **Se debe tener en cuenta que algunos anexos del script deben ejecutarse en los servidores miembro del dominio**, en concreto, los que hacen referencia a **configuraciones locales** del sistema.

Nota: Los scripts asociados a la presente guía, destinados tanto a la realización de copia de seguridad como a la aplicación de medidas de seguridad, **no deben ubicarse en la raíz del disco C**:. Esta práctica garantiza que la copia de todos los ficheros se realice de manera adecuada, evitando errores derivados de la falta de permisos en dicha ubicación.

Se aconseja ubicar los scripts en la carpeta **"Documentos"** del usuario administrador que será utilizado para la ejecución de los mismos, asegurando así la correcta accesibilidad y disponibilidad de permisos necesarios.

Dichas configuraciones afectan directamente al comportamiento del sistema operativo en cada servidor, independientemente de su rol dentro del dominio, y son esenciales para garantizar una postura de seguridad homogénea en todo el entorno.

ANEXO A.1. CONFIGURACIONES PREVIAS

Durante el proceso de fortificación de sistemas Windows Server, se introducen modificaciones que afectan directamente a la configuración base del sistema operativo. Dichas modificaciones, aunque necesarias para elevar el nivel de seguridad, pueden generar efectos no deseados en el entorno, como pérdida de ciertas funcionalidades, incompatibilidades con servicios existentes o degradación del rendimiento.

Con el objetivo de mitigar estos riesgos y facilitar las tareas de diagnóstico y recuperación ante posibles incidencias, la presente guía contiene un mecanismo automatizado de regresión del sistema base. Este mecanismo permite capturar y preservar el estado original de los elementos esenciales del sistema antes de aplicar cualquier medida de seguridad. De este modo, se garantiza la posibilidad de revertir los cambios y restaurar el entorno a un estado funcional previo, facilitando así el análisis de impacto y la resolución de problemas.

El proceso de regresión se realiza mediante un script que ejecuta de forma automatizada la copia de seguridad de los siguientes componentes clave:

a) **Características del sistema:** Se guarda un registro de las características que consta el sistema, pudiendo ser revertidas tras la aplicación de medidas de seguridad en caso de necesidad.

b) **Directivas de grupo (GPO):** Tanto locales como aplicadas, incluyendo configuraciones de seguridad.

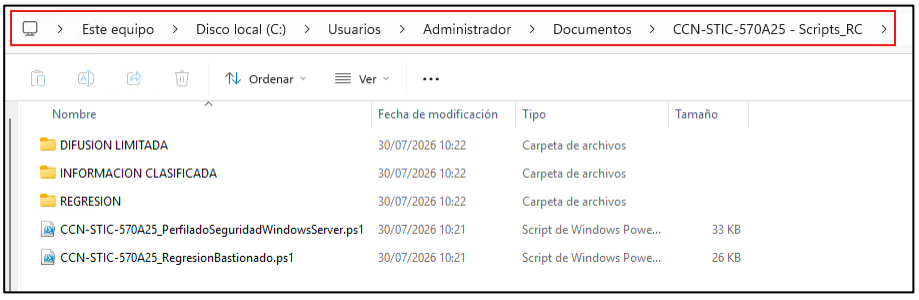
c) **Permisos:** Sobre archivos, carpetas y claves de registro que se modifican durante la fase de implementación de seguridad.

d) **Servicios:** Tipo de inicio y permisos de los servicios instalados.

Este enfoque permite mantener un control preciso sobre los cambios introducidos, reducir el riesgo operativo y mejorar la trazabilidad de las acciones realizadas durante el proceso de aplicación de seguridad sobre los equipos del Sistema. Además, proporciona una base sólida para el diagnóstico de errores en caso de que se detecten anomalías tras la aplicación de las medidas de seguridad.

Nota: Los procedimientos descritos a continuación son aplicables a cualquier sistema basado en Windows Server, en su versión 2025.

ANEXO A.1.1. COPIA DE SEGURIDAD

Paso	Descripción
1.	Inicie sesión en el servidor sobre el que quiere exportar la copia de seguridad regresiva. Debe iniciar sesión con una cuenta que se encuentre en el grupo Admins. del Dominio.
2.	Copie los ficheros y directorios que acompañan a esta guía, al directorio en la carpeta "Documentos" del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: – CCN-STIC-570A25_RegresionBastionado.ps1 – CCN-STIC-570A25_PerfiladoSeguridadWindowsServer.ps1 – Directorio: REGRESION. – Directorio: DIFUSION LIMITADA. – Directorio: INFORMACION CLASIFICADA.  *Ilustración 1 - Ruta de los scripts RC* **Nota:** Dado que en la presente guía se aplican las configuraciones correspondientes al grado de **Difusión Limitada**, únicamente se muestran los directorios de "DIFUSION LIMITADA" e "INFORMACION CLASIFICADA. En el caso de aplicar la configuración del grado **ENS**, se mostrarán los siguientes archivos: - CCN-STIC-570A25_RegresionBastionado.ps1 - CCN-STIC-570A25_PerfiladoSeguridadWindowsServer.ps1

- Directorio: REGRESION.
- Directorio: ENS

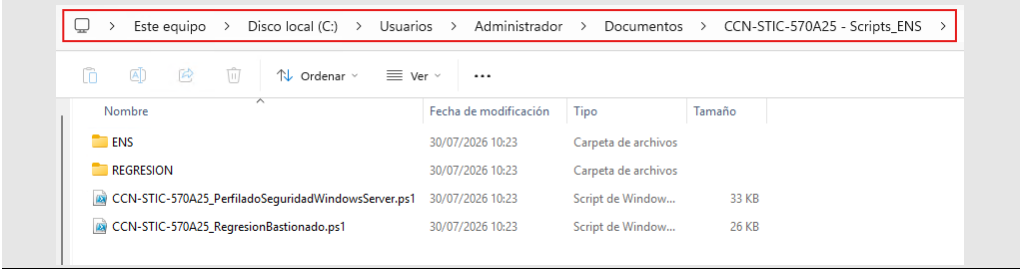


Ilustración 2 - Ruta de scripts ENS

3. Sobre la barra de búsqueda, escriba “PowerShell”.

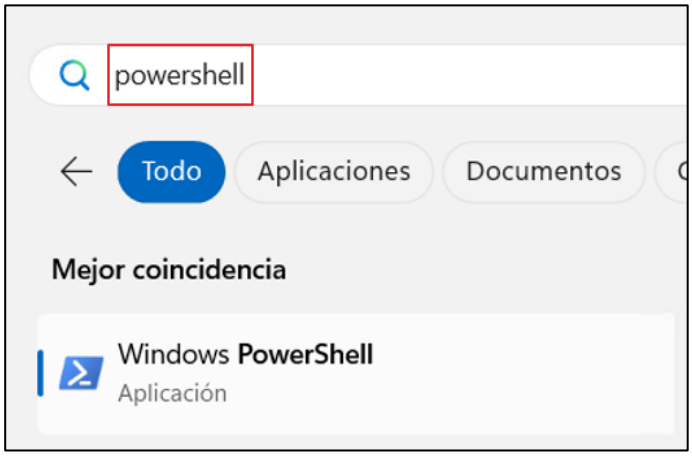
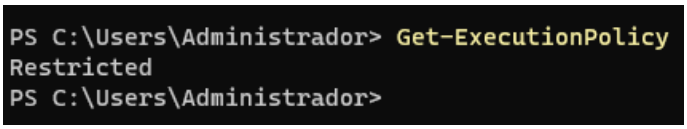
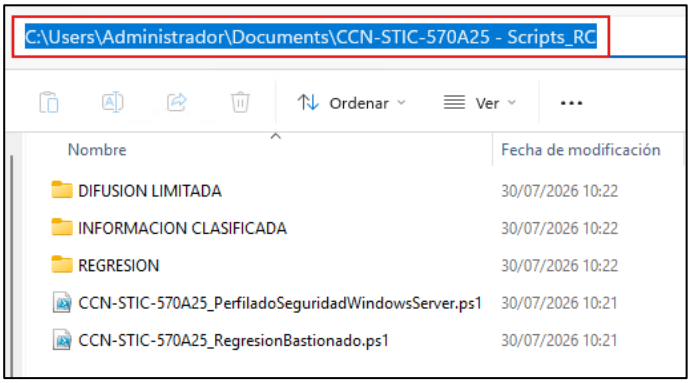


Ilustración 3 - Búsqueda de PowerShell para ejecución del script

4. A continuación, seleccione “Ejecutar como administrador”.

	Ilustración 4 - Ejecución como administrador de PowerShell **Nota:** Si el script no se ejecuta desde PowerShell, existe la posibilidad de que se produzcan errores durante el proceso de copia y/o que no se visualice la información de manera adecuada.
5.	En la consola de comandos de Powershell, ejecute la sentencia "Get-ExecutionPolicy":  *Ilustración 5 - Ejecución de Get-ExecutionPolicy*
6.	Si el resultado muestra un valor diferente a "Unrestricted", deberá ejecutar el siguiente comando para permitir la ejecución de scripts: "Set-ExecutionPolicy Unrestricted".  *Ilustración 6 - Ejecución Unrestricted*
7.	Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con "Ctrl + C".  *Ilustración 7 - Copia de la ruta*
8.	Desde la ventana de PowerShell, utilizando el comando "cd", acceda a la ruta recientemente copiada.  *Ilustración 8 - Acceso a la ruta desde PowerShell* **Nota:** Agregue las comillas simples (') entre la ruta como se aprecia en la imagen para que PowerShell pueda realizar la búsqueda correctamente.
9.	Ejecute el comando "dir" para verificar la ubicación y el contenido.

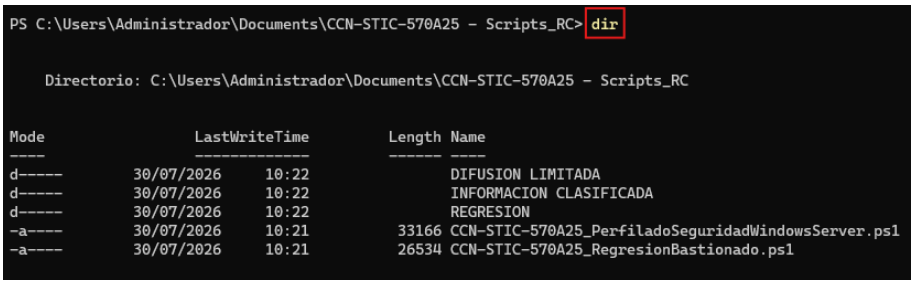


Ilustración 9 - Verificación de los archivos

10. Ejecute el archivo "CCN-STIC-570A25_RegresionBastionado.ps1" escribiendo ".\" y pulsando la tecla tabulador hasta ver el nombre del archivo autocompletado.

Pulse la tecla "Enter" para comenzar la ejecución.

Ilustración 10 - Ejecución del Script

11. A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:

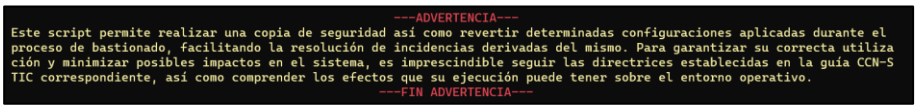


Ilustración 11 - Advertencia de uso

12. Si lo que se desea es realizar una exportación de la configuración, debe escribir "E" y pulsar la tecla "Enter".

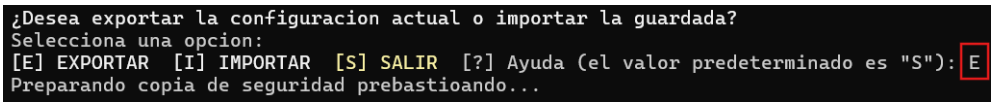


Ilustración 9 – Exportar configuración

13. Se le solicitará una segunda confirmación:

Ilustración 12 - Confirmación del script

Inmediatamente después de confirmar, comenzará la ejecución de la copia automatizada.

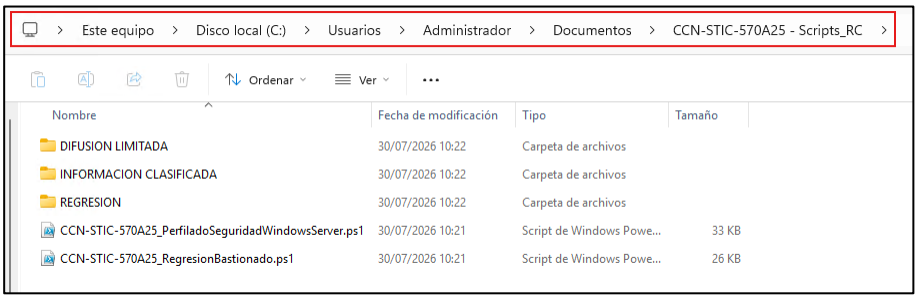
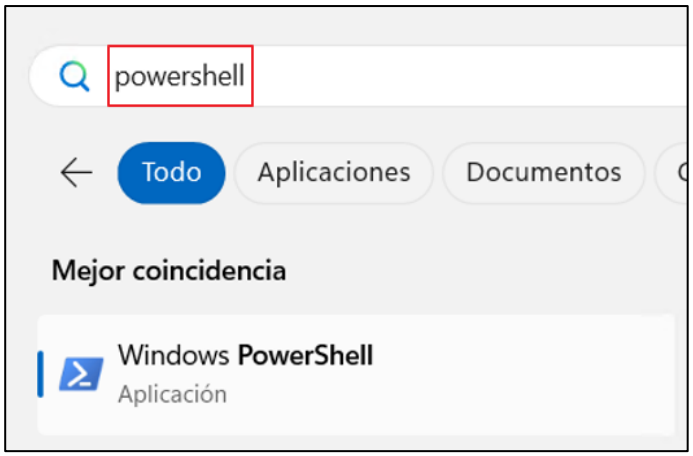
14.	Una vez finalizado el proceso de copia de archivos, se podrá observar el siguiente mensaje:
	`Creando carpeta Scripts...`
	`Carpeta preparada`
	`Copiando archivos de bastionado...`
	`Archivos copiados`
	Ilustración 13 - Copia de archivos completada

15.	Una vez finalizado el proceso de copia de los servicios:
	`Copiando servicios...`
	`Servicios copiados correctamente`
	Ilustración 14 - Copia de servicios completada

16.	Acceda a la ruta "C:\Scripts\REGRESION" mediante el explorador de archivos. Verifica que contiene los siguientes directorios: – CARACTERISTICAS – GPOS – PERMISOS – SERVICIOS  *Ilustración 15 - Ubicación de los archivos exportados*

ANEXO A.1.2. IMPORTADO DE COPIA DE SEGURIDAD

Paso	Descripción

1.	Inicie sesión en el servidor sobre el que quiere importar la copia de seguridad regresiva. Debe iniciar sesión con una cuenta que se encuentre en el grupo Admins. del Dominio.
2.	Copie los ficheros y directorios que acompañan a esta guía, al directorio en la carpeta "Documentos" del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: – CCN-STIC-570A25_RegresionBastionado.ps1 – CCN-STIC-570A25_PerfiladoSeguridadWindowsServer.ps1 – Directorio: REGRESION. – Directorio: DIFUSION LIMITADA. – Directorio: INFORMACION CLASIFICADA.  *Ilustración 16 - Ruta de los scripts*
3.	Sobre la barra de búsqueda, escriba "PowerShell".  *Ilustración 17 - Búsqueda de PowerShell para ejecución del script*

A continuación, seleccione “Ejecutar como administrador”.

Ilustración 18 - Ejecución como administrador de PowerShell

Nota: Si el script no se ejecuta desde PowerShell, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada.

4. Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con “Ctrl + C”.

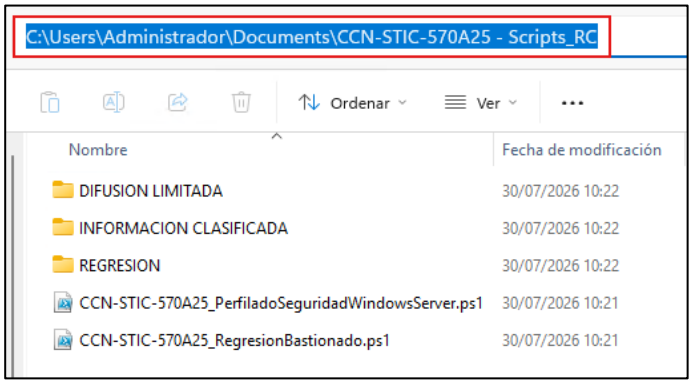
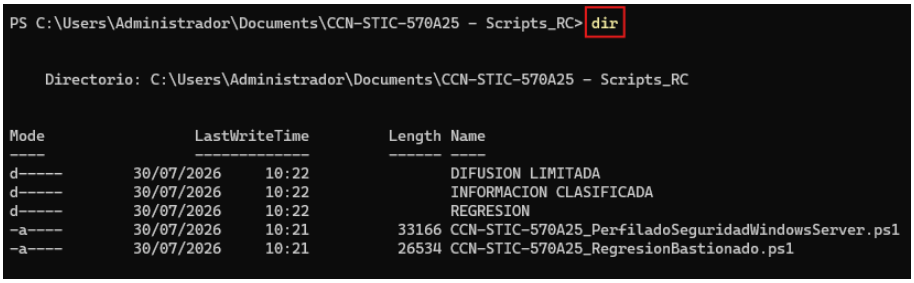
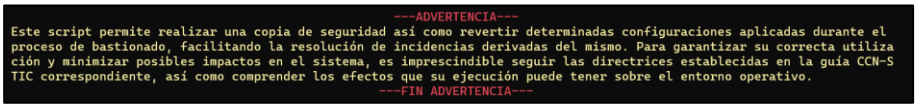
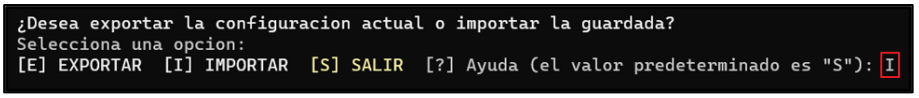


Ilustración 19 - Copia de la ruta

5. Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.

```
PS C:\Users\Administrador> cd 'C:\Users\Administrador\Documents\CCN-STIC-570A25 - Scripts_RC\'
```

Ilustración 20 - Acceso a la ruta desde PowerShell

6.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 21 - Verificación de los archivos*
7.	Ejecute el archivo “CCN-STIC-570A25_RegresionBastionado.ps1” escribiendo “.\” y pulsando la tecla tabulador hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 22 - Ejecución del script*
8.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 23 - Advertencia de uso*
9.	Si lo que se desea es importar una copia anteriormente realizada, se debe escribir “I” y pulsar la tecla “Enter”:  *Ilustración 24 - Pregunta inicial del script*
10.	Se le solicitará una segunda confirmación:  *Ilustración 25 - Confirmación del script*
11.	Inmediatamente después de confirmar, comenzará la importación de la copia automatizada. Una vez finalizado el proceso de copia, se podrá observar el siguiente mensaje:

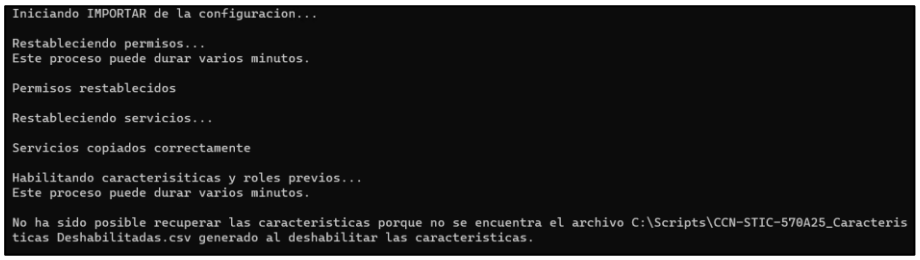


Ilustración 26 - Mensaje final del script

ANEXO A.2. CARACTERÍSTICAS DE WINDOWS

Nota: Este anexo debe ejecutarse de manera local sobre todos los Controladores de Dominio y Servidores Miembro del entorno.

El presente anexo recoge las configuraciones iniciales necesarias para establecer una base segura en sistemas Windows Server. Las medidas aquí descritas se centran en la gestión del sistema operativo y en la aplicación de directivas mediante plantillas administrativas (ADMX), con el objetivo de reducir la superficie de exposición y garantizar un entorno coherente con los principios normativos.

La configuración base constituye el primer paso del proceso de fortificación del Sistema y debe aplicarse antes de implementar políticas más específicas. Incluye la desactivación de funcionalidades innecesarias, la habilitación de componentes críticos para la seguridad y la definición de parámetros clave del sistema que afectan al comportamiento general del entorno.

Las recomendaciones incluidas en este anexo han sido alineadas conforme al resto de guías CCN-STIC para sistemas Windows Server.

ANEXO A.2.1. IMPACTO

La desactivación de características del sistema operativo que no son necesarias para el rol específico del servidor (controlador/es de dominio o servidor miembro) permite reducir la superficie de exposición y minimizar riesgos de seguridad. Sin embargo, esta acción puede tener los siguientes impactos:

a) Incompatibilidad con aplicaciones que dependan de características deshabilitadas (por ejemplo, .NET framework, servicios de impresión, IIS, XMP, etc.).

b) Pérdida de funcionalidad en tareas administrativas o de interoperabilidad si se eliminan componentes como SMBv1, Telnet o Escritorio Remoto (si no se gestiona adecuadamente).

c) Necesidad de revisión previa de los requisitos funcionales del sistema y de las aplicaciones desplegadas, para evitar interrupciones en el servicio.

Nota: Antes de aplicar esta configuración, se debe realizar un inventario de dependencias funcionales y validar que ninguna característica será deshabilitada sin una alternativa segura.

ANEXO A.3. PLANTILLAS ADMINISTRATIVAS

ANEXO A.3.1. IMPACTO

La aplicación de directivas mediante Plantillas Administrativas permite establecer configuraciones de seguridad homogéneas y forzadas en todo el entorno. No obstante, su aplicación puede generar los siguientes efectos:

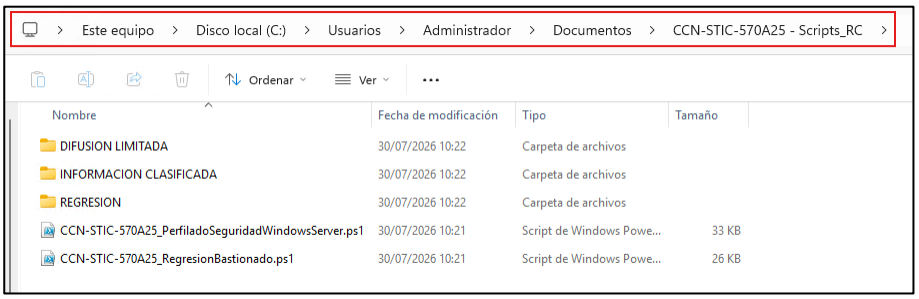
a) Restricciones en la experiencia de usuario (por ejemplo, bloqueo del acceso al Panel de Control, desactivación de notificaciones, limitación de ejecución de scripts o macros).

b) Incompatibilidades con software de terceros que requiera configuraciones específicas del sistema o del entorno de usuario.

c) Posibles conflictos con GPOs existentes en entornos con políticas heredadas o múltiples dominios.

Nota: Se recomienda validar las plantillas en un entorno de pruebas antes de su despliegue en producción, y documentar cualquier excepción necesaria para garantizar la operatividad del sistema.

ANEXO A.4. APLICACIÓN DE MEDIDAS DE SEGURIDAD BASE

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se quiere comenzar el proceso de fortificación.
2.	Copie los ficheros y directorios que acompañan a esta guía, al directorio en la carpeta “Documentos” del usuario administrador. A continuación, descomprima la carpeta. Verifique que en su interior se encuentran los siguientes archivos: – CCN-STIC-570A25_RegresionBastionado.ps1 – CCN-STIC-570A25_PerfiladoSeguridadWindowsServer.ps1 – Directorio: REGRESION. – Directorio: DIFUSION LIMITADA. – Directorio: INFORMACION CLASIFICADA.  *Ilustración 27 - Ruta de los scripts*

3. Sobre la barra de búsqueda, escriba “PowerShell”.

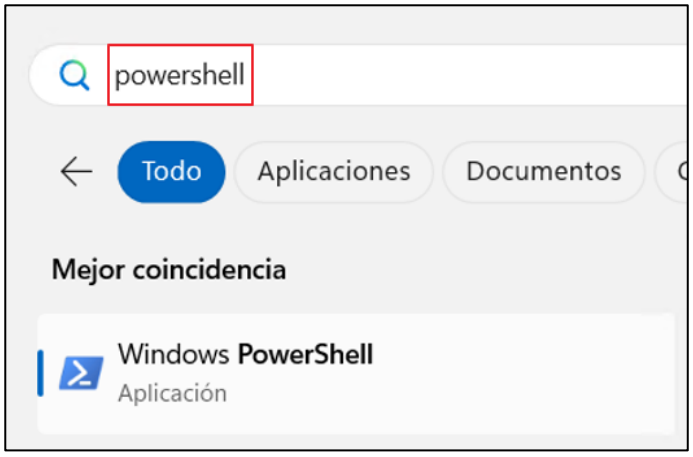
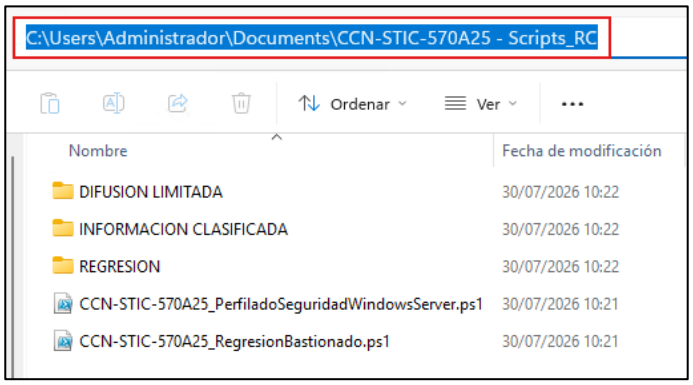
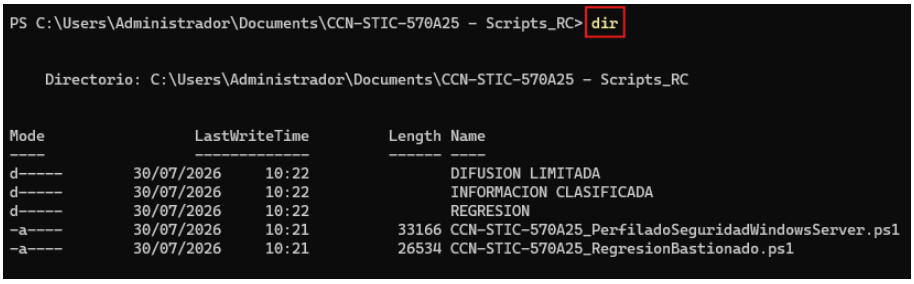


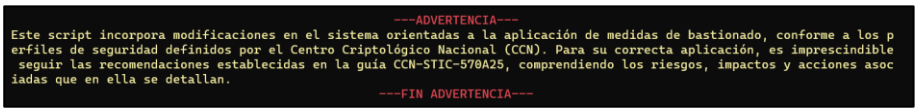
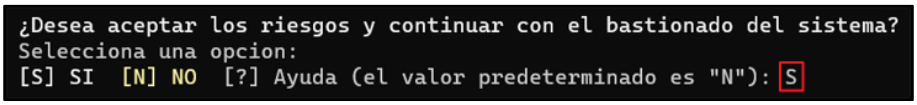
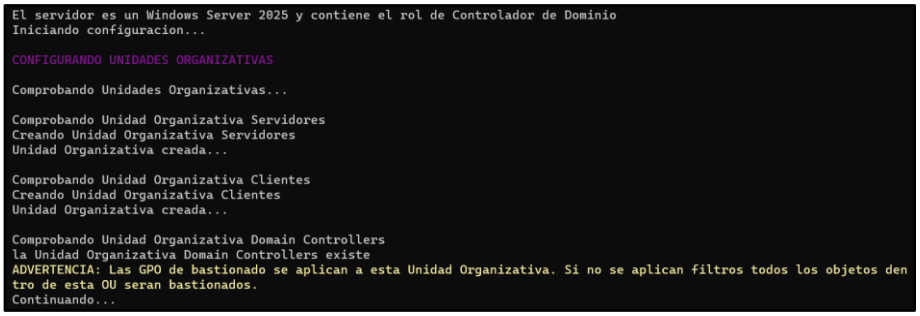
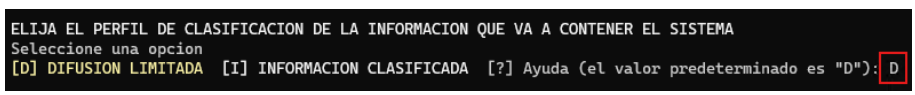
Ilustración 28 - Búsqueda de PowerShell para ejecución del script

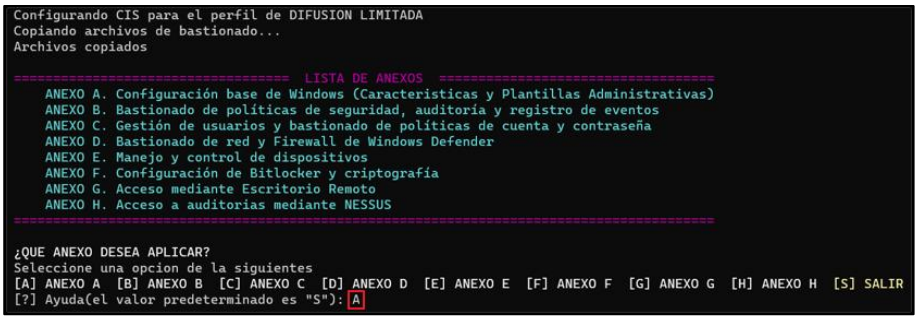
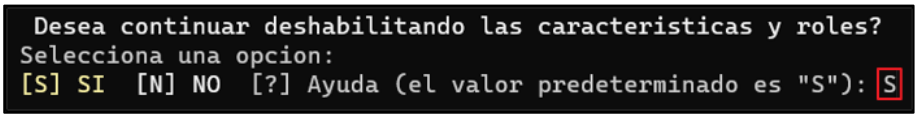
A continuación, seleccione “Ejecutar como administrador”.

Ilustración 29 - Ejecución como administrador de PowerShell

Nota: Si el script no se ejecuta desde PowerShell, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada.

4.	Desde el explorador de archivos, acceda al contenido de carpeta en la que ha copiado los scripts y copie la ruta en el portapapeles con “Ctrl + C”.  *Ilustración 30 - Copia de la ruta*
5.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada.  *Ilustración 31 - Acceso a la ruta desde PowerShell* **Nota:** Agregue las comillas simples (‘’) entre la ruta como se aprecia en la imagen para que PowerShell pueda realizar la búsqueda correctamente.
6.	Ejecute el comando “dir” para verificar la ubicación y el contenido.  *Ilustración 32 - Verificación de los archivos*
7.	Ejecute el archivo “CCN-STIC-570A25_PerfiladoSeguridadWindowsServer.ps1” escribiendo “.\” y pulsando la tecla tabulador hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.  *Ilustración 33 - Ejecución del script de regresión*

8.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje:  *Ilustración 34 - Advertencia de uso*
9.	Debe introducir el carácter “S” y pulsar la tecla “Enter”:  *Ilustración 35 – Ejecución del script*
10.	Automáticamente, el script detectará el sistema operativo host y verificará que se encuentre instalado el rol de “Controlador de Dominio”. Se crearán de manera automática las siguientes Unidades Organizativas: – Servidores. – Clientes. – Domain Controllers. Se podrá observar la siguiente salida:  *Ilustración 36 - Creación de las Unidades Organizativas* Nota: La Unidad Organizativa llamada “Domain Controllers” debe existir de manera predeterminada en el sistema si el controlador de dominio es nuevo o está recientemente promocionado. En caso de que no exista o se haya modificado anteriormente, será creada.
11.	A continuación, será necesario seleccionar el perfil de Clasificación de la Información que va a contener el sistema. En el ejemplo mostrado, se seleccionará “Difusión Limitada”.  *Ilustración 37 - Selección del perfil de clasificación de la información*

	Nota: Si usted ha seleccionado "Información Clasificada" el script le consultará si quiere aplicar la política incremental para grado "Secreto". No debe aplicarse si el grado de clasificación del sistema es "Confidencial" o "Reservado". Dicha GPO aplica una serie de configuraciones de seguridad adicionales referentes a los servicios del sistema.
12.	Una vez definido el perfil de Clasificación de la Información adecuado, introduzca el carácter "A" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO A. Configuración base de Windows (Características y Plantillas Administrativas)".  *Ilustración 38 - Selección del anexo a aplicar*
13.	El script solicitará confirmación para proceder con la inhabilitación de características del sistema. Introduzca el carácter "S" y pulse "Enter":  *Ilustración 39 - Eliminación de características y roles*
14.	Una vez finalizado el proceso, observará el siguiente mensaje:  *Ilustración 40 - Advertencia de reinicio* No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

ANEXO B. POLÍTICAS DE SEGURIDAD, AUDITORIA Y REGISTROS DE EVENTOS

ANEXO B.1.1. IMPACTO

Este anexo recoge las directivas necesarias para reforzar la seguridad del sistema mediante la configuración de políticas relacionadas con el control de acceso, la auditoría de eventos y el registro de actividad. Estas medidas permiten establecer un marco de trazabilidad y supervisión que facilita la detección de incidentes, el análisis forense y el cumplimiento de los requisitos del Esquema Nacional de Seguridad (ENS).

La correcta aplicación de estas políticas es esencial para garantizar la integridad del sistema, prevenir accesos no autorizados y mantener un registro fiable de las acciones realizadas por usuarios y procesos. Las configuraciones se adaptan a los roles de controlador de dominio y servidor miembro.

La aplicación de políticas de seguridad restrictivas puede generar los siguientes efectos:

a) Limitación de acciones administrativas al restringirse privilegios y reforzar los controles de acceso.

b) Bloqueo de cuentas por políticas de bloqueo tras intentos fallidos.

c) Incompatibilidad con software o scripts que requieran permisos elevados o configuraciones menos restrictivas.

Nota: Se recomienda validar previamente las políticas en entornos de prueba y documentar excepciones necesarias para tareas operativas.

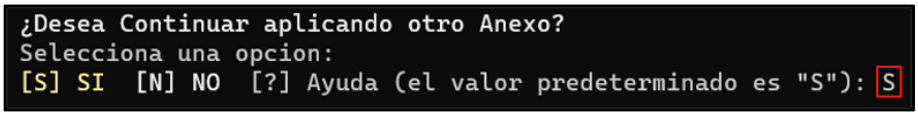
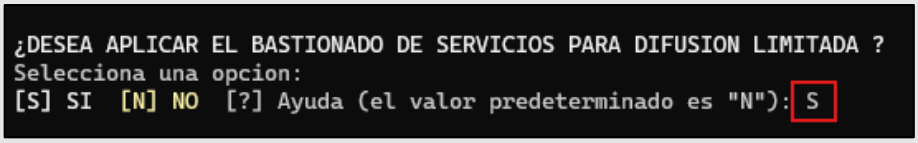
La activación de auditorías detalladas y el aumento del nivel de registro puede tener los siguientes impactos:

a) Incremento del volumen de logs, lo que puede afectar al rendimiento del sistema y al espacio en disco si no se gestiona adecuadamente.

b) Mayor carga en el sistema de monitorización, especialmente si se integran con SIEM o soluciones de correlación de eventos.

Nota: Es recomendable revisar de manera periódica los logs y eventos generados para evitar sobrecarga de información.

ANEXO B.1.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD, AUDITORÍA Y REGISTROS

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  *Ilustración 41 - Aplicación del siguiente anexo* Pulse el carácter "S" y a continuación, la tecla "Enter" para continuar con el proceso de fortificación del presente Anexo.
2.	Introduzca el carácter "B" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO B. Políticas de seguridad, auditoría y registro de eventos".  *Ilustración 42 - Selección del siguiente anexo a aplicar* **Nota:** El script preguntará si se desea la aplicación de seguridad de servicios para el grado indicado. Si lo desea, introduzca el carácter "S".  *Ilustración 43 - Configuración de servicios* Se creará y configurará la GPO "CCN-STIC-570A25_DC_AnexoB - Seguridad, auditoria y registros (Difusión Limitada)" de manera automática.
3.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

ANEXO C. GESTIÓN DE USUARIOS Y POLÍTICAS DE CUENTA Y CONTRASEÑA

El presente anexo recoge las directivas necesarias para reforzar la seguridad en la gestión de cuentas de usuario y contraseñas en sistemas Windows Server. Las medidas incluidas tienen como objetivo prevenir accesos no autorizados, reducir el riesgo de suplantación de identidad y garantizar el cumplimiento de los requisitos establecidos en la normativa.

La configuración de políticas de cuenta y contraseña se aplica de forma coherente en todo el entorno, tanto en controladores de dominio como en servidores miembros, y

contempla aspectos como la complejidad de las contraseñas, su caducidad, el historial, el bloqueo por intentos fallidos y la nomenclatura de cuentas.

ANEXO C.1.1. SISTEMA DE NOMBRES

Para garantizar la trazabilidad y evitar el uso de cuentas genéricas, se recomienda establecer un criterio uniforme para la creación de nombres de usuario. Este criterio puede ser:

a) Nominativo: Asociado directamente a una persona.

b) Único: Sin duplicidades en el dominio.

c) Reconocible: Fácil de identificar por el equipo técnico y de auditoría.

A continuación, se describe el formato recomendado:

> [Inicial del nombre][Primer apellido][Segundo apellido][Número incremental si hay duplicados]

Siendo un ejemplo:

a) Juan Pérez García: jperezg

b) María López Vázquez: mlopezv

c) Carlos Ibáñez Cabello: cibanezc

Nota: En entornos con nombres comunes, se debe añadir un número incremental basado en dos dígitos (jperezg01, jperezg02) sustituible por un número identificador interno, como, por ejemplo, código de empleado.

El sistema descrito facilita la trazabilidad en auditorías, el control de privilegios y la gestión de accesos, especialmente en entornos clasificados o con requisitos de alta seguridad.

ANEXO C.1.2. IMPACTO

La aplicación de políticas restrictivas de cuenta y contraseña puede tener los siguientes efectos en el entorno:

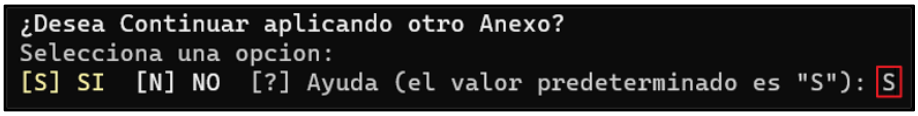
a) Incremento de incidencias de bloqueo de cuentas, especialmente en usuarios con hábitos inseguros o que reutilizan contraseñas.

b) Incompatibilidad con sistemas heredados o aplicaciones que no soportan requisitos de complejidad elevados.

c) Posible afectación de cuentas de servicio o automatismos, si no se gestionan adecuadamente las excepciones necesarias.

Nota: Antes de aplicar estas políticas, se debe realizar un análisis de impacto sobre usuarios, servicios y aplicaciones. Es recomendable establecer procedimientos de gestión de cuentas y contraseñas que contemplen excepciones controladas, así como mecanismos de recuperación seguros.

ANEXO C.1.3. APLICACIÓN DE MEDIDAS DE SEGURIDAD DE USUARIOS, CUENTAS Y CONTRASEÑAS

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  *Ilustración 44 - Aplicación del siguiente anexo* Pulse el carácter "S" y a continuación, la tecla "Enter" para continuar con el proceso de fortificación del presente Anexo.
2.	Introduzca el carácter "C" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO C. Gestión de usuarios y políticas de cuenta y contraseña".  *Ilustración 45 - Selección del siguiente anexo a aplicar* Se creará y configurará la GPO "CCN-STIC-570A25_Dominio_AnexoC - Usuarios, Cuentas y Contraseñas (Difusión Limitada)" de manera automática.
3.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

ANEXO D. SEGURIDAD DE RED Y FIREWALL DE WINDOWS DEFENDER

El presente anexo recoge las directivas necesarias para reforzar la seguridad de las comunicaciones y el control de tráfico en sistemas Windows Server, tanto en su rol de controlador de dominio como de servidor miembro. Las medidas incluidas se centran en la configuración de parámetros de red críticos y en la aplicación de reglas de firewall mediante Windows Defender, con el objetivo de limitar la exposición del sistema y controlar el flujo de datos de forma granular.

La configuración segura de red permite reducir el riesgo de ataques externos e internos, asegurando que solo los servicios estrictamente necesarios estén accesibles. Asimismo, el uso del firewall integrado facilita la segmentación del tráfico, la detección de comportamientos anómalos y la aplicación de políticas de seguridad adaptadas al entorno operativo.

ANEXO D.1.1. IMPACTO

La aplicación de medidas de seguridad sobre la red y el firewall puede tener los siguientes efectos:

a) Interrupción de servicios o comunicaciones si se bloquean puertos o protocolos requeridos por aplicaciones, servicios de directorio, monitorización o gestión remota.

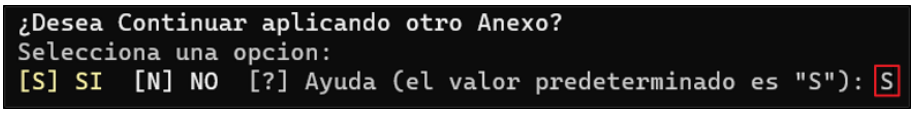
b) Pérdida de conectividad entre sistemas si no se contemplan excepciones necesarias en entornos distribuidos o con dependencias cruzadas.

c) Incompatibilidad con soluciones de terceros que requieran configuraciones específicas de red o reglas de acceso más permisivas.

d) Mayor complejidad en la gestión de incidencias, especialmente en entornos donde no se dispone de una documentación específica referente a puertos y protocolos de red autorizados.

Nota: Antes de aplicar estas configuraciones, se debe realizar un análisis de dependencias de red, identificar los servicios críticos y documentar las reglas necesarias para garantizar la operatividad. Es recomendable validar las reglas en entornos de prueba y establecer procedimientos de revisión periódica del firewall.

ANEXO D.1.2. APLICACIÓN DE SEGURIDAD DE RED

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  *Ilustración 46 - Aplicación del siguiente anexo* Pulse el carácter "S" y a continuación, la tecla "Enter" para continuar con el proceso de fortificación del presente Anexo.
2.	Introduzca el carácter "D" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO D. Seguridad de red y Firewall de Windows Defender".  *Ilustración 47 - Selección del siguiente anexo a aplicar* Se crearán y configurarán las siguientes GPO de manera automática: – CCN-STIC-570A25_DC_AnexoD - Red y Firewall (Difusión Limitada) – CCN-STIC-570A25_Servidor Miembro_AnexoD - Red y Firewall (Difusión Limitada)
3.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

ANEXO E. MANEJO Y CONTROL DE DISPOSITIVOS

Nota: Este anexo debe ejecutarse de manera local sobre todos los Controladores de Dominio y Servidores Miembro del entorno.

El presente anexo recoge las medidas de seguridad orientadas al control de dispositivos de almacenamiento que pueden conectarse físicamente al sistema, como unidades USB, discos duros externos, periféricos y otros medios extraíbles. El objetivo principal es prevenir la fuga de información, la introducción de código malicioso y el uso no autorizado de medios.

Las políticas aplicadas permiten restringir el uso de dispositivos no autorizados mediante el registro de sus identificadores únicos (ID de hardware), habilitando únicamente aquellos estrictamente necesarios para la operatividad del sistema. Esta estrategia garantiza un control granular sobre los medios que interactúan con el sistema.

ANEXO E.1.1. IMPACTO

La aplicación de estas medidas puede tener los siguientes efectos en el entorno operativo:

a) Bloqueo automático de dispositivos no registrados, lo que puede interrumpir tareas de transferencia de datos, mantenimiento o recuperación si no se han autorizado previamente los medios necesarios.

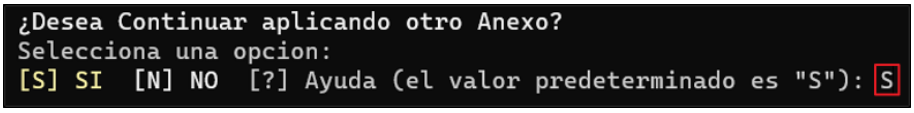
b) Necesidad de mantener un inventario actualizado de dispositivos permitidos, incluyendo su ID de hardware, lo que implica una carga administrativa adicional.

c) Incompatibilidad con procesos automatizados o herramientas de diagnóstico que dependan del uso de medios extraíbles.

d) Incremento de incidencias operativas, especialmente en entornos donde se utilizan dispositivos compartidos o rotativos sin una gestión centralizada.

Nota: Antes de aplicar estas políticas, se debe realizar un inventario de dispositivos utilizados en el entorno, establecer un procedimiento formal para el registro y autorización de medios, y definir excepciones controladas para tareas críticas. Es recomendable validar las configuraciones en entornos de prueba y documentar los dispositivos autorizados por rol o función.

ANEXO E.1.2. APLICACIÓN DE SEGURIDAD SOBRE DISPOSITIVOS EXTRAÍBLES

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  *Ilustración 48 - Aplicación del siguiente anexo* Pulse el carácter "S" y a continuación, la tecla "Enter" para continuar con el proceso de fortificación del presente Anexo.
2.	Introduzca el carácter "E" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO E. Manejo y control de dispositivos".  *Ilustración 49 - Selección del siguiente anexo a aplicar* Se crearán y configurarán las siguientes GPO de manera automática: – CCN-STIC-570A25_DC_AnexoE - Control de Dispositivos. – CCN-STIC-570A25_Servidor Miembro_AnexoE - Control de Dispositivos.
3.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

ANEXO E.1.3. CONFIGURACIONES MANUALES

ANEXO F. CONFIGURACIÓN DE BITLOCKER Y CRIPTOGRAFIA

El presente anexo recoge las directivas necesarias para aplicar mecanismos de protección de datos en reposo mediante el uso de BitLocker y la configuración de parámetros criptográficos en Sistemas Windows Server. Estas medidas son fundamentales para garantizar la confidencialidad de la información almacenada, especialmente en entornos clasificados o que manejan datos sensibles.

La configuración de BitLocker permite cifrar volúmenes completos del sistema, protegiendo los datos frente a accesos no autorizados, pérdida o robo de dispositivos. Asimismo, se establecen parámetros criptográficos que definen el uso de algoritmos seguros, el refuerzo de protocolos de comunicación y la desactivación de tecnologías obsoletas o vulnerables.

Las recomendaciones incluidas están alineadas con el resto de guías CCN-STIC y se adaptan a los requisitos de sistemas en distintos niveles de clasificación.

ANEXO F.1.1. IMPACTO

La aplicación de estas medidas puede tener los siguientes efectos en el entorno:

a) Incremento en el tiempo de arranque y acceso a discos, especialmente en sistemas con hardware limitado o sin aceleración criptográfica.

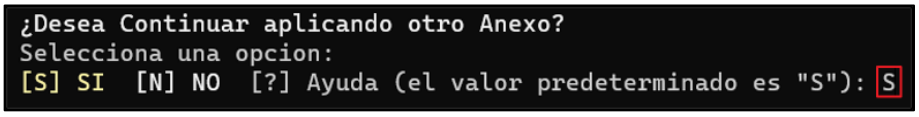
b) Incompatibilidad con herramientas de recuperación o mantenimiento si no se gestionan adecuadamente las claves de recuperación de BitLocker.

c) Restricciones en el uso de algoritmos no aprobados, lo que puede afectar a aplicaciones o servicios que dependan de configuraciones criptográficas específicas.

d) Necesidad de gestión centralizada de claves, para evitar pérdida de acceso de incidentes o rotación de personal.

Nota: Antes de aplicar estas configuraciones, se debe validar la compatibilidad del hardware con BitLocker, establecer un procedimiento seguro para la gestión de claves de recuperación, y revisar las dependencias criptográficas de las aplicaciones instaladas. Es recomendable realizar pruebas de rendimiento y funcionalidad en entornos controlados antes del despliegue en producción.

ANEXO F.1.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD CRIPTOGRÁFICAS

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  *Ilustración 50 - Aplicación del siguiente anexo* Pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del presente Anexo.
2.	Introduzca el carácter “F” y pulse “Enter” para aplicar las políticas asociadas al presente anexo: “ANEXO F. Configuración de Bitlocker y criptografía”.  *Ilustración 51 - Selección del siguiente anexo a aplicar* Se crearán y configurarán las siguientes GPO de manera automática: – CCN-STIC-570A25_DC_AnexoF - Bitlocker (Difusión Limitada). – CCN-STIC-570A25_Servidor Miembro_AnexoF - Bitlocker (Difusion Limitada).

3.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

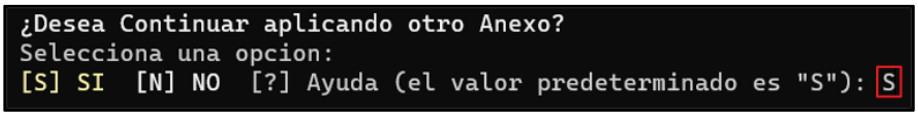
ANEXO G. ACCESO MEDIANTE ESCRITORIO REMOTO

El objetivo del presente anexo tiene como misión establecer las configuraciones necesarias sobre aquellos elementos a los que se les quiere permitir el acceso remoto por medio de Remote Desktop Protocol (RDP) de Microsoft Windows.

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: Éste Anexo solamente debe aplicarse en caso de necesidad explícita de la funcionalidad. En caso negativo, puede continuar con el siguiente Anexo, o bien, finalizar el script indicando que no quiere "Continuar con la aplicación de otro Anexo".

ANEXO G.1.1. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN RDP

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  *Ilustración 52 - Aplicación del siguiente anexo* Pulse el carácter "S" y a continuación, la tecla "Enter" para continuar con el proceso de fortificación del presente Anexo.
2.	Introduzca el carácter "G" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO G. Acceso mediante Escritorio Remoto".  *Ilustración 53 - Selección del siguiente anexo a aplicar* Se creará y configurará la "GPO CCN-STIC-570A25_Incremental RDP".
3.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

ANEXO H. ACCESO A AUDITORÍAS MEDIANTE NESSUS

El presente anexo recoge las configuraciones necesarias para permitir la ejecución de auditorías de seguridad mediante la herramienta Nessus, en modalidad de análisis de caja blanca. Este tipo de auditoría requiere acceso autenticado al sistema, lo que permite realizar una revisión más profunda de las vulnerabilidades presentes, incluyendo configuraciones internas, servicios activos y estado de parches.

La aplicación de estas configuraciones implica la creación de una cuenta técnica con privilegios controlados, así como la definición de políticas que permitan el acceso remoto seguro y la recopilación de información por parte del escáner.

Nota: Estas medidas deben aplicarse únicamente cuando sea estrictamente necesario, y solo si el sistema sobre el que se está aplicando seguridad lo permite y lo requiere.

Este tipo de auditoría está orientada a entornos dónde se necesita una validación exhaustiva de las medidas de seguridad aplicadas, y debe estar debidamente autorizado por el responsable de seguridad del sistema.

ANEXO H.1.1. IMPACTO

La configuración para permitir auditorías con Nessus puede tener los siguientes efectos:

a) Exposición temporal de credenciales técnicas, que deben ser gestionadas con medidas de protección adecuadas (uso de cuentas dedicadas, contraseñas robustas, caducidad controlada).

b) Incremento de la carga en el sistema durante la ejecución del escaneo, especialmente si se realiza en horarios de producción.

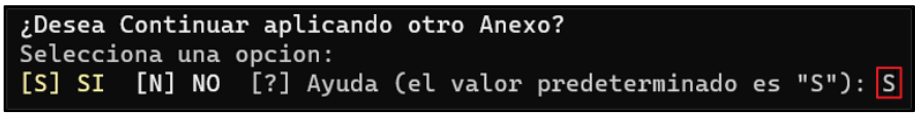
c) Posible detección de falsos positivos o alertas por comportamiento del escáner, que deben ser filtradas y analizadas correctamente.

d) Riesgo de acceso no autorizado si no se controla adecuadamente el uso de la cuenta técnica designada para este propósito.

Nota: Esta configuración debe aplicarse únicamente en sistemas dónde se haya autorizado expresamente la auditoría con Nessus. Se recomienda establecer una cuenta técnica con privilegios mínimos necesarios, limitar el acceso por IP, y revocar los permisos una vez finalizada la auditoría. Además, se debe documentar el alcance, duración y responsable de la ejecución del escaneo.

ANEXO H.1.2. APLICACIÓN DE LA POLÍTICA DE ACCESO DE AUDITORÍAS CON NESSUS

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se está aplicando seguridad. Si ha seguido los pasos anteriores, debe observar el siguiente mensaje:

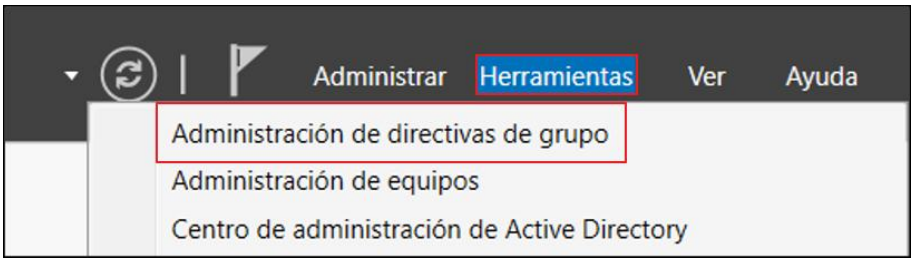
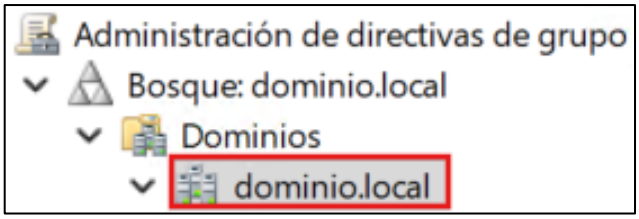
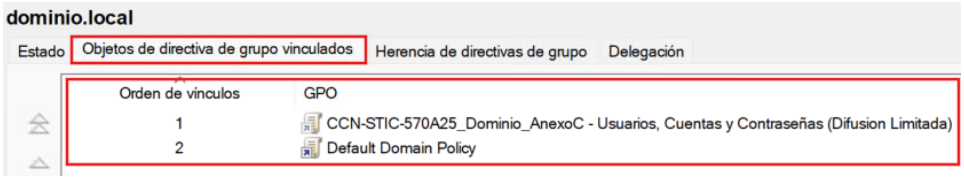
	 *Ilustración 54 - Aplicación del siguiente anexo* Pulse el carácter "S" y a continuación, la tecla "Enter" para continuar con el proceso de ejecución del presente Anexo.
2.	Introduzca el carácter "H" y pulse "Enter" para aplicar las políticas asociadas al presente anexo: "ANEXO H. Acceso a auditorias mediante NESSUS".  *Ilustración 55 - Selección del siguiente anexo a aplicar* Se creará y configurará la GPO "CCN-STIC-570A25_Incremental NESSUS".
3.	Cierre la ventana de PowerShell, continúe con el siguiente punto.

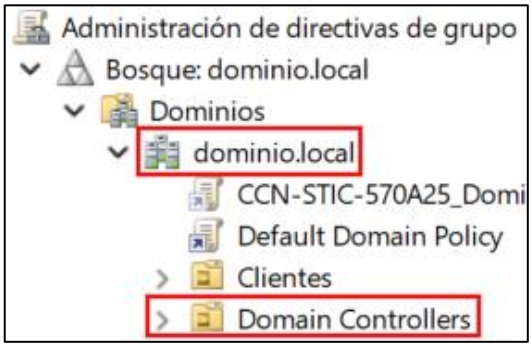
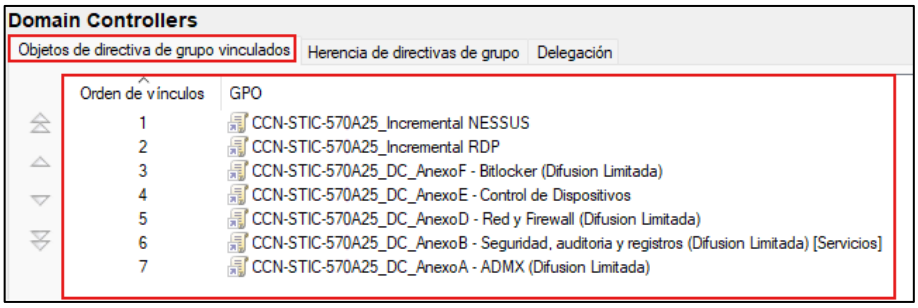
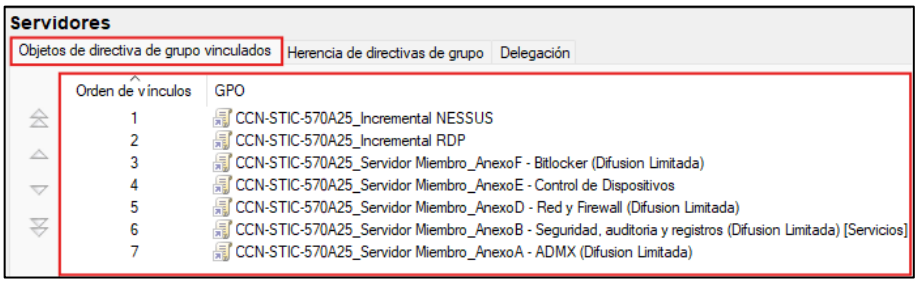
7. CONFIGURACIONES MANUALES Y COMPROBACIONES

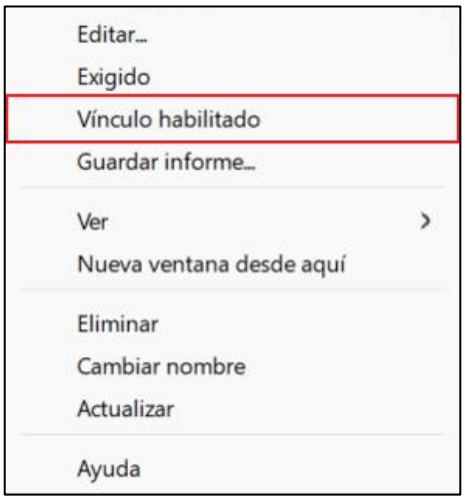
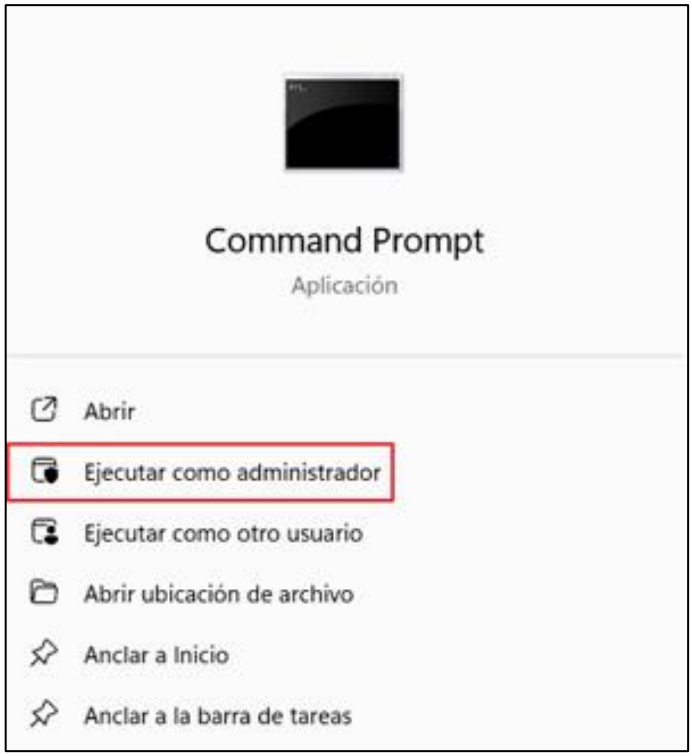
7.1. GESTIÓN DE GPOs

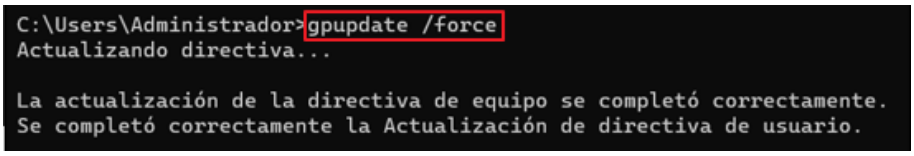
En el presente anexo se procederá a configurar el orden de aplicación de las políticas de seguridad mediante la sección “Objetivos de directiva de grupo vinculados” dentro de la consola de Administración de directivas de grupo (GPMC). Esta configuración permite establecer la prioridad de las GPOs en función de su relevancia y del rol del sistema al que estén asociadas.

Una vez definido el orden, se procederá a habilitar el vínculo de las GPOs, lo que permitirá que comiencen a aplicarse en el entorno de forma controlada.

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el dominio que quiere realizarse la modificación del mensaje de inicio de sesión.
2.	Desde el “Administrador del servidor”, seleccione Herramientas > Administración de directivas de grupo.  *Ilustración 56 - Acceso a la administración de GPOs*
3.	Despliegue su dominio y seleccione la raíz, en el caso del ejemplo su nombre es “dominio.local”.  *Ilustración 57 - Selección del dominio*
4.	A continuación, a la derecha, seleccione “Objetos de directiva de grupo vinculados”. El orden de los vínculos debe ser el siguiente:  *Ilustración 58 - Orden de GPOs vinculados al dominio*

5.	Seleccione nombre.dominio > Domain Controllers con clic izquierdo.  *Ilustración 59 - Selección de la unidad organizativa de Domain Controllers*
6.	A continuación, a la derecha, seleccione "Objetos de directiva de grupo vinculados". El orden de los vínculos debe ser el siguiente:  *Ilustración 60 - Orden de GPOs vinculados a Domain Controllers*
7.	Seleccione nombre.dominio > Servidores con clic izquierdo. A continuación, a la derecha, seleccione "Objetos de directiva de grupo vinculados". El orden de los vínculos debe ser el siguiente:  *Ilustración 61 - Orden de GPOs vinculados a Servidores*

8.	Por último, para que las políticas comiencen a aplicarse en el entorno, se debe habilitar el vínculo de cada una de ellas. Para ello, haga clic derecho sobre la GPO, y seleccione “Vínculo habilitado”.  *Ilustración 62 - Habilitación del vínculo de los GPOs*
9.	Para una correcta aplicación, ejecute la Consola de Comandos del sistema en modo Administrador.  *Ilustración 63 - Ejecución como administrador de CMD*

10.	Ejecute el comando gpupdate /force. Tras finalizar, observará el siguiente mensaje:  *Ilustración 64 - Ejecución de gpupdate /force* Una vez completada la actualización de directivas de equipo y usuario, debe reiniciarse el equipo manualmente.

7.2. MANEJO Y CONTROL DE DISPOSITIVOS

El presente apartado recoge las configuraciones manuales que se deben llevar a cabo para un correcto filtrado de los dispositivos conectados a los equipos de tipo servidor, independientemente de su rol, dentro de un dominio.

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.

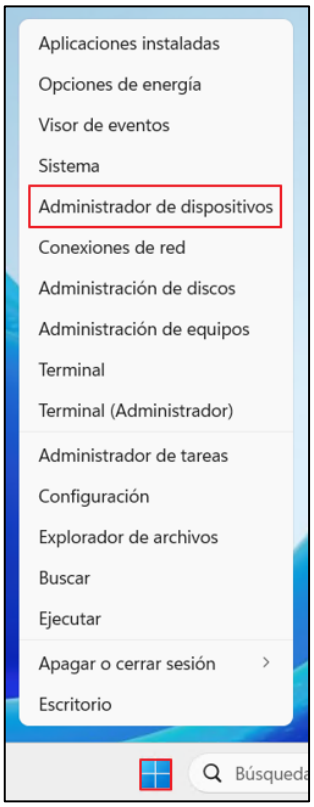
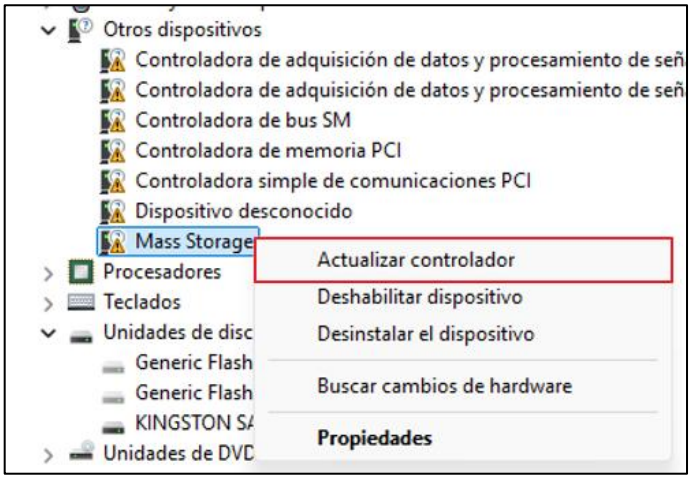
b) Alta de dispositivos por medio de identificadores únicos de los dispositivos.

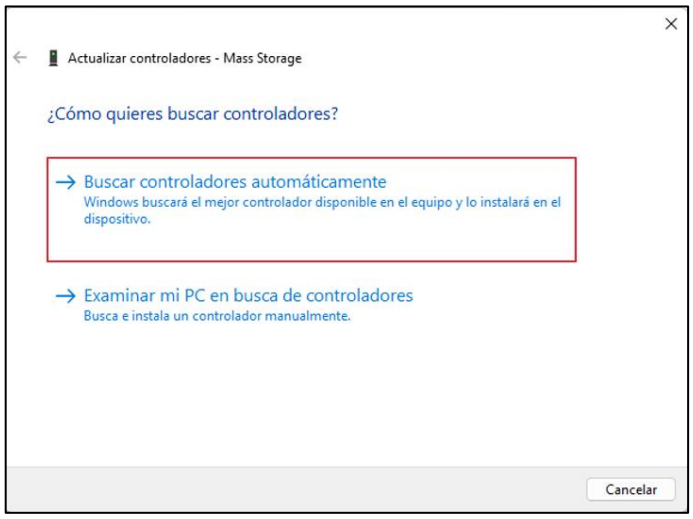
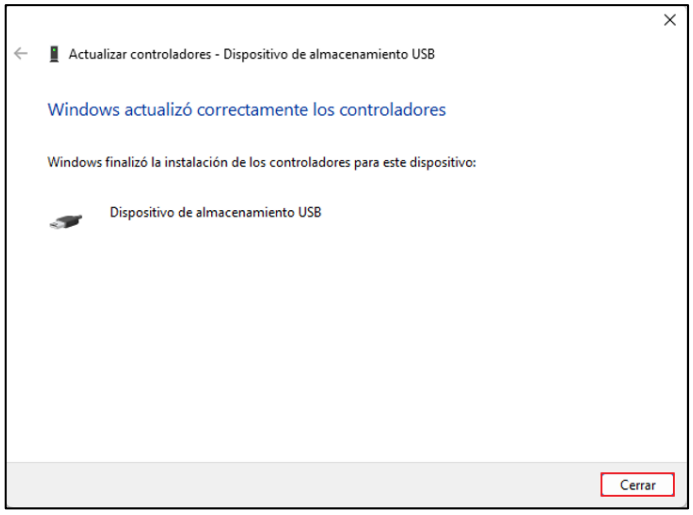
Nota: El presente paso a paso establece la **configuración de seguridad** para un **perfilado Difusión Limitada o Información Clasificada**, no siendo obligatorio en ningún otro perfilado.

7.2.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES

Los pasos definidos a continuación deberán ser realizados sobre el servidor del dominio afectado, en el cual se pretende habilitar el uso de dispositivos USB.

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

2.	Haga clic derecho sobre el botón de inicio, y sobre "Administrador de dispositivos":  *Ilustración 65 - Ejecución del Administrador de dispositivos*
3.	Despliegue 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".  *Ilustración 66 - Selección del dispositivo* **Nota:** Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de "Dispositivo desconocido".

4.	A continuación, se iniciará el asistente para instalar el software necesario. Seleccione la opción "Buscar software de controlador actualizado automáticamente".  *Ilustración 67 - Búsqueda automática de controladores*
5.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse "Cerrar" cuando haya finalizado.  *Ilustración 68 - Finalización de la actualización de controladores* **Nota:** No cierre el "Administrador de dispositivos" todavía.

6.	Ejecute los pasos 3 a 5 hasta que el dispositivo aparezca en “Unidades de disco” en caso de ser un dispositivo de almacenamiento.  *Ilustración 69 - Unidad de disco nueva*

7.2.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

Los pasos definidos a continuación deberán ser realizados tanto sobre el servidor del dominio en el cual se pretende habilitar el uso de dispositivos USB, como sobre el Controlador de Dominio perteneciente al mismo dominio.

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

2. Haga clic derecho sobre el botón de inicio, y sobre "Administrador de dispositivos":

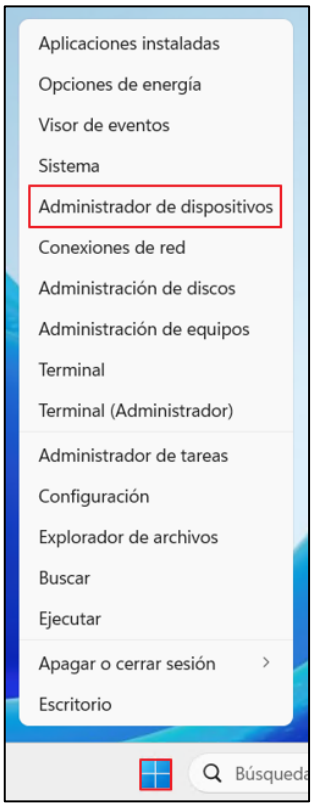


Ilustración 70 - Ejecución del Administrador de dispositivos

3. Despliegue 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".

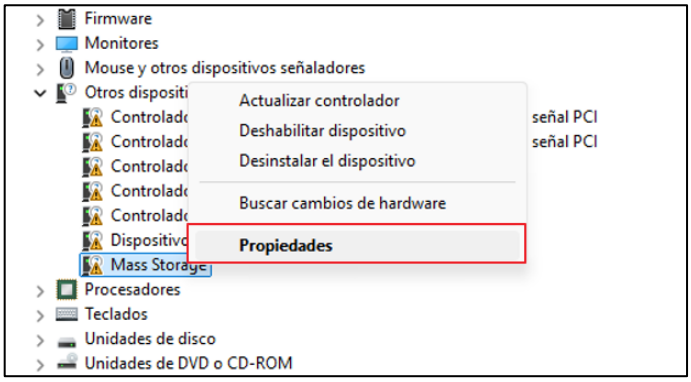
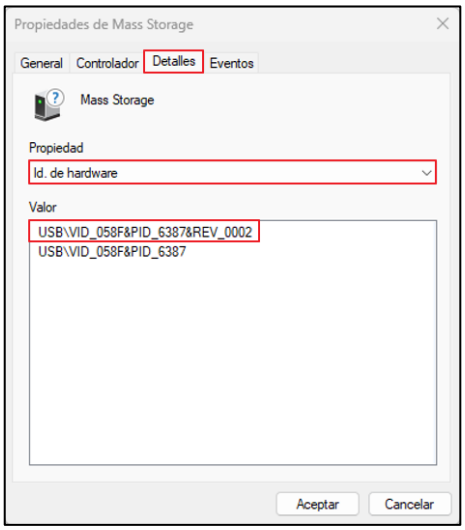
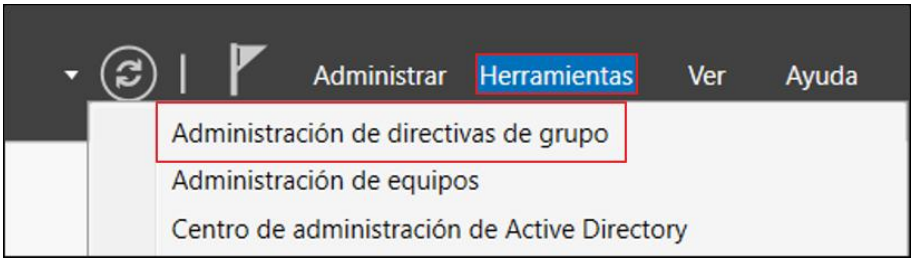
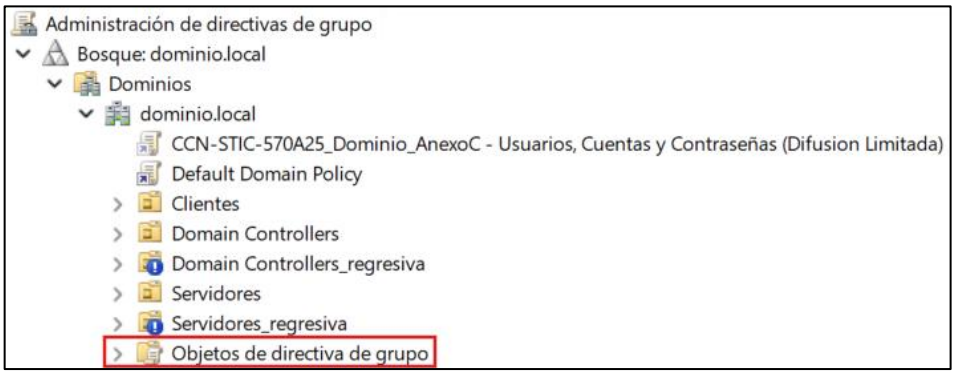
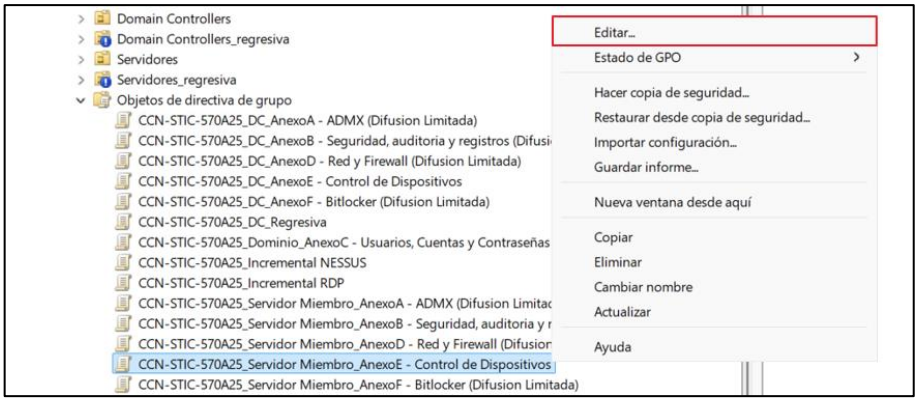
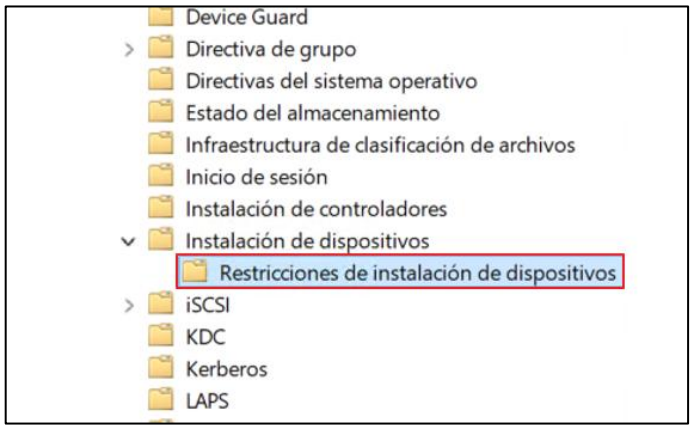
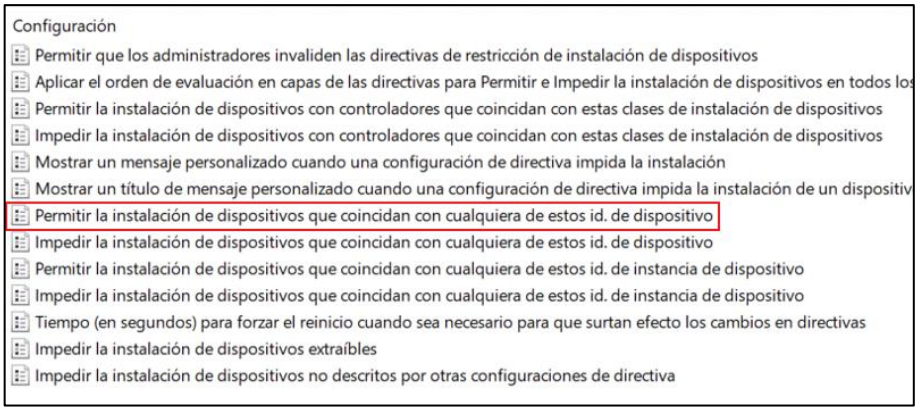


Ilustración 71 - Propiedades del dispositivo

Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y que le asigne el nombre de "Dispositivo desconocido".

4.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad”, seleccione “Id. de hardware”. Seleccione el identificador que se encuentra en primer lugar y anótelo para poder utilizarlo más adelante.  *Ilustración 72 - Detalles del dispositivo* **Nota:** Independientemente del número de identificadores existentes, deberá seleccionar siempre aquel que se encuentre en primera posición.
5.	Desde el “Administrador del servidor”, seleccione Herramientas > Administración de directivas de grupo.  *Ilustración 73 - Acceso a la administración de GPOs*

6.	Despliegue la raíz del dominio, y después despliegue “Objetos de directiva de grupo”.  *Ilustración 74 - Despliegue de los objetos de directiva de grupo*
7.	Haga clic derecho sobre el GPO “CCN-STIC-570A25_Servidor Miembro_AnexoE – Control de dispositivos”, y seleccione la opción “Editar” en el menú contextual.  *Ilustración 75 - Edición del GPO* **Nota:** Puede editar tanto los dispositivos USB permitidos de los servidores miembro del dominio (en el GPO indicado en el ejemplo) como los de Controladores de Dominio. Para el segundo caso, es necesario editar el GPO “CCN-STIC-570A25_DC_AnexoE – Control de Dispositivos”.

8.	Despliegue el nodo “Configuración del equipo > Plantillas administrativas > Sistema > Instalación de dispositivos > Restricciones de instalación de dispositivos”.  *Ilustración 76 - Despliegue del nodo de restricciones de instalación de dispositivos*
9.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.  *Ilustración 77 - Edición de la política*

Hacer clic en “Mostrar…”:

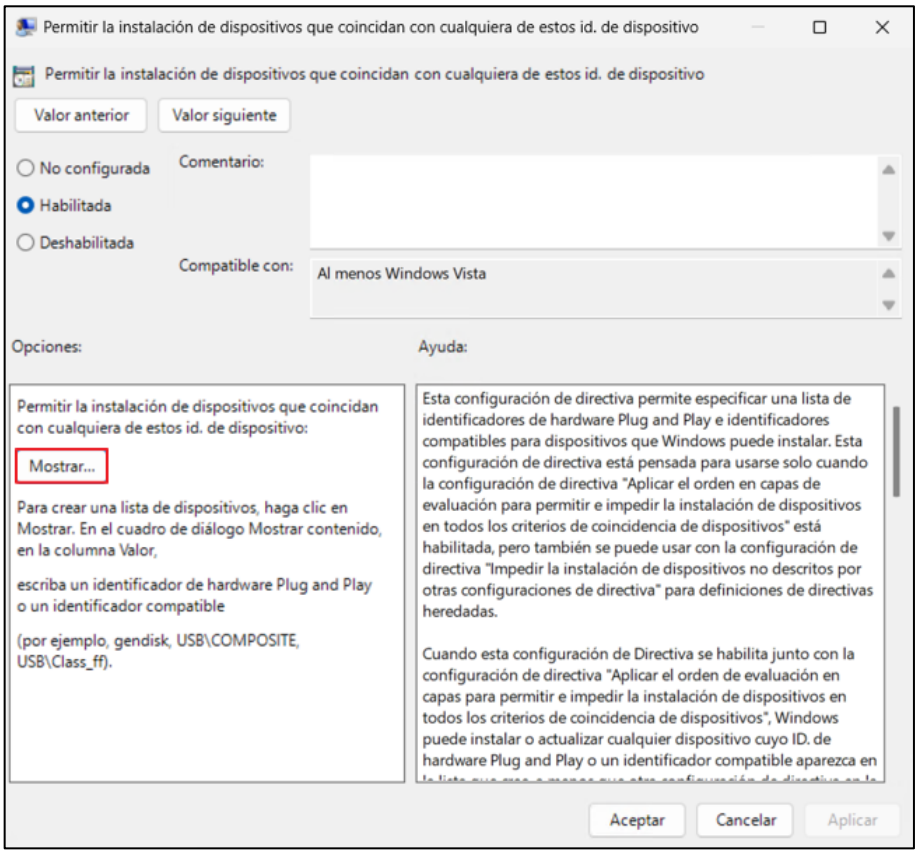


Ilustración 78 - Configuración de la política

10. En la ventana emergente, haga doble clic sobre la última línea para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado en pasos anteriores. Después, pulse “Aceptar”.

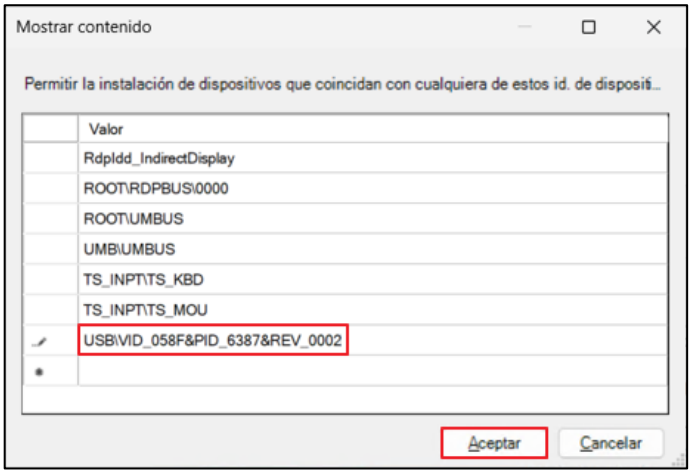
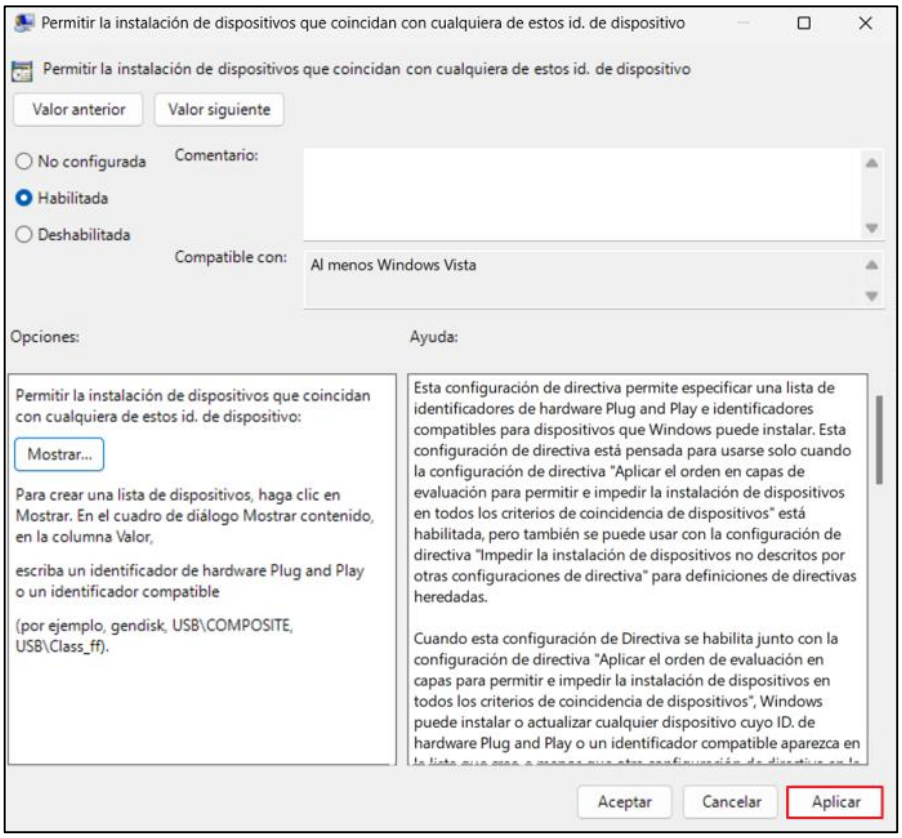
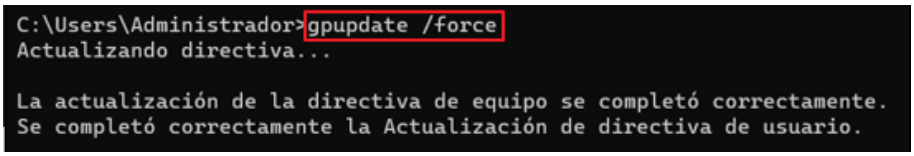


Ilustración 79 - Adición del id. de hardware del dispositivo

Nota: No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto funcionamiento del sistema.

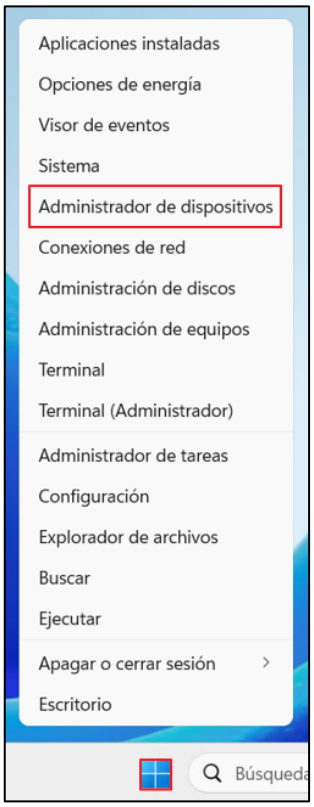
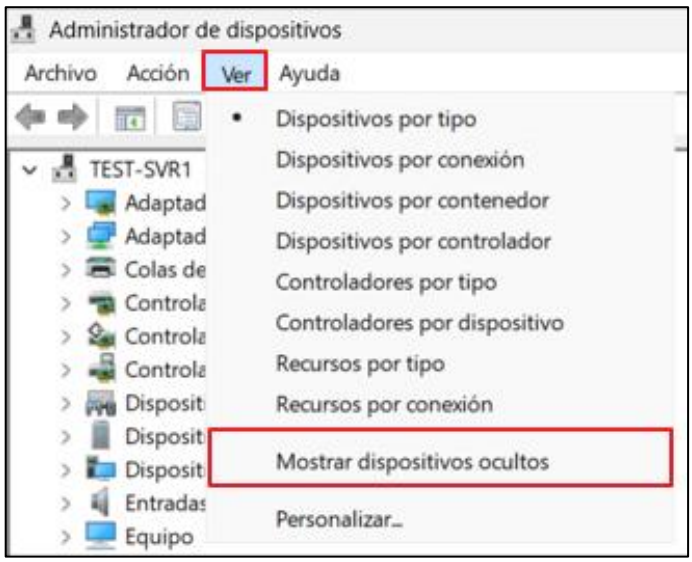
11.	Haga clic en “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.  *Ilustración 80 - Finalización de la configuración de la política*
12.	Sin cerrar el “Editor de directivas de grupo local”, continue con el siguiente paso.
13.	Inicie sesión en el servidor donde se pretende habilitar el uso de un dispositivo USB.

14.	Ejecute la Consola de Comandos del sistema en modo Administrador.  *Ilustración 81 - Ejecución como administrador de CMD*
15.	Ejecute el comando gpupdate /force. Tras finalizar, observará el siguiente mensaje:  *Ilustración 82 - Ejecución de gpupdate /force*
16.	Ejecute de nuevo los pasos 3 a 16 para añadir todos los identificadores necesarios hasta que el dispositivo sea reconocido por el explorador de ficheros de Windows en caso de ser un dispositivo de almacenamiento.

7.2.3. ELMINAR DISPOSITIVOS USB DADOS DE ALTA

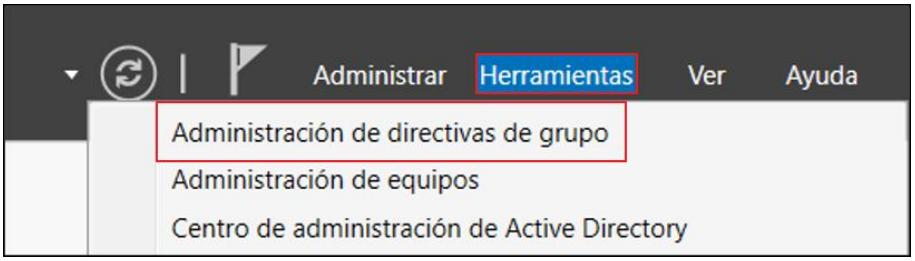
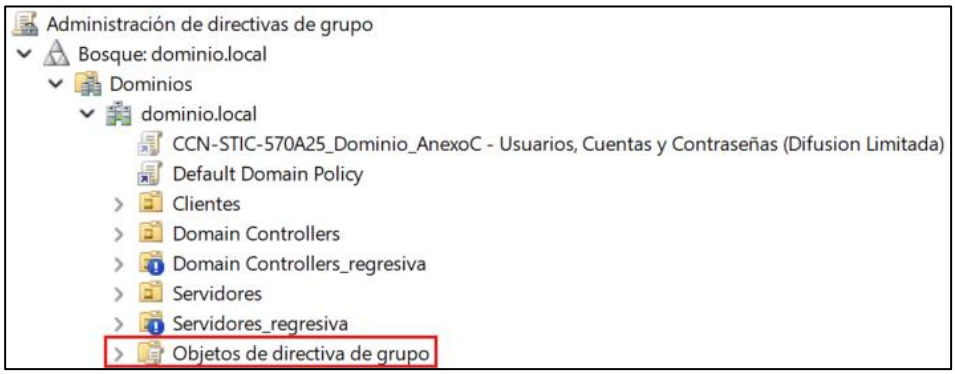
Tras la instalación del dispositivo y su posterior uso, es posible volver al estado anterior de bloqueo del uso de dispositivos USB previo. Para ello, se deberán seguir los siguientes pasos:

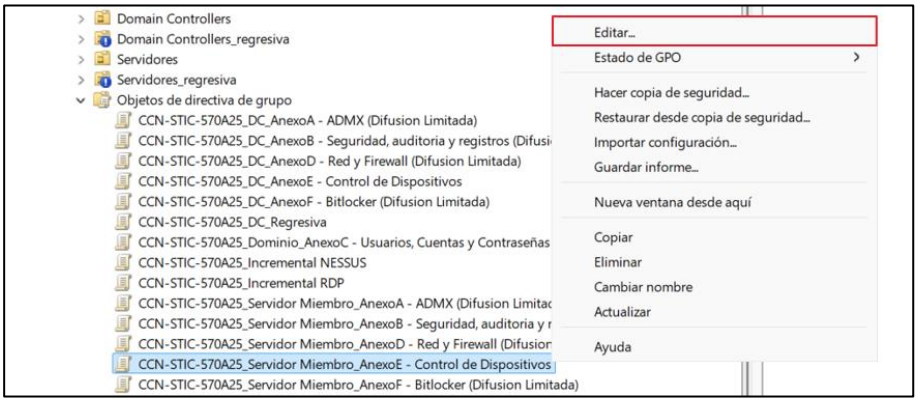
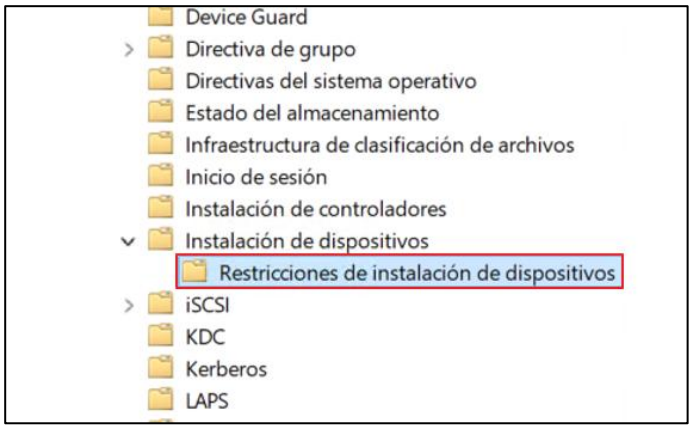
Paso	Descripción
1.	Inicie sesión en el servidor donde se pretende eliminar el uso de un dispositivo USB.

2.	Haga clic derecho sobre el botón de inicio, y sobre "Administrador de dispositivos":  *Ilustración 83 - Ejecución del Administrador de dispositivos*
3.	Seleccione la pestaña "Ver" y haga clic en la opción "Mostrar dispositivos ocultos".  *Ilustración 84 – Mostrar dispositivos ocultos*

4.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB cuyos controladores desea desinstalar. A continuación, haga clic derecho sobre el mismo y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”.  *Ilustración 85 - Desinstalación del dispositiv*
5.	Haga clic sobre “Desinstalar” en la ventana emergente.  *Ilustración 86 - Confirmación de la desinstalación* **Nota:** Una vez confirmada la desinstalación, el dispositivo USB n podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

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

Paso	Descripción
1.	Inicie sesión en un servidor con el rol de Controlador de Dominio del dominio en el que quiere configurarse el control de dispositivos.
2.	Desde el "Administrador del servidor", seleccione Herramientas > Administración de directivas de grupo.  *Ilustración 87 - Acceso a la administración de GPOs*
3.	Despliegue la raíz del dominio, y después despliegue "Objetos de directiva de grupo".  *Ilustración 88 - Despliegue de los objetos de directiva de grupo*

4.	Haga clic derecho sobre el GPO "CCN-STIC-570A25_Servidor Miembro_AnexoE – Control de dispositivos", y seleccione la opción "Editar" en el menú contextual.  *Ilustración 89 - Edición del GPO*
5.	Despliegue el nodo "Configuración del equipo > Plantillas administrativas > Sistema > Instalación de dispositivos > Restricciones de instalación de dispositivos".  *Ilustración 90 - Despliegue del nodo de restricciones de instalación de dispositivos*

6.	En el panel derecho, haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.

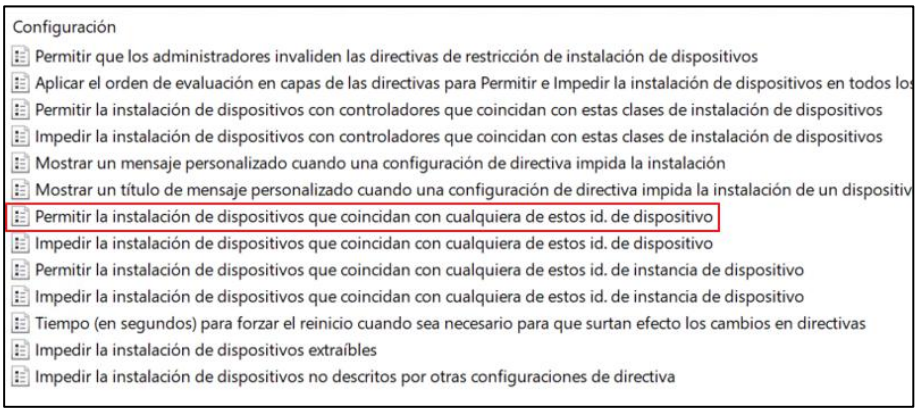


Ilustración 91 - Edición de la política

7.	Hacer clic en “Mostrar…”:

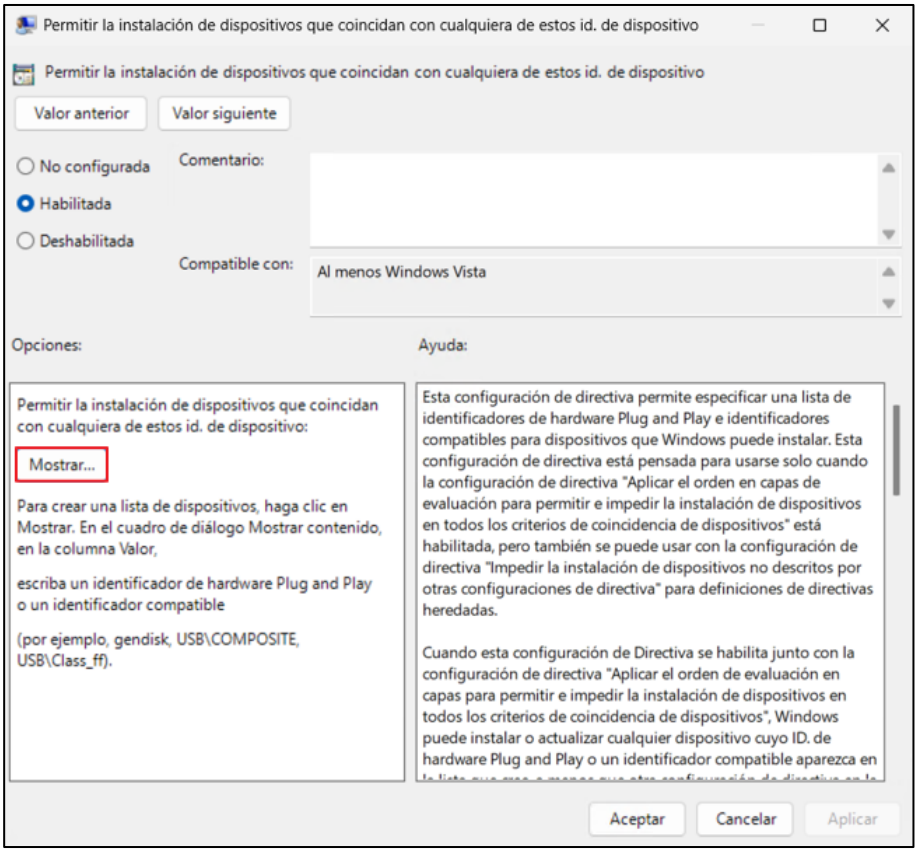


Ilustración 92 - Configuración de la política

8. En la ventana emergente, elimine los identificadores correspondientes a los dispositivos cuyo uso ya no es requerido. Después, pulse “Aceptar”.

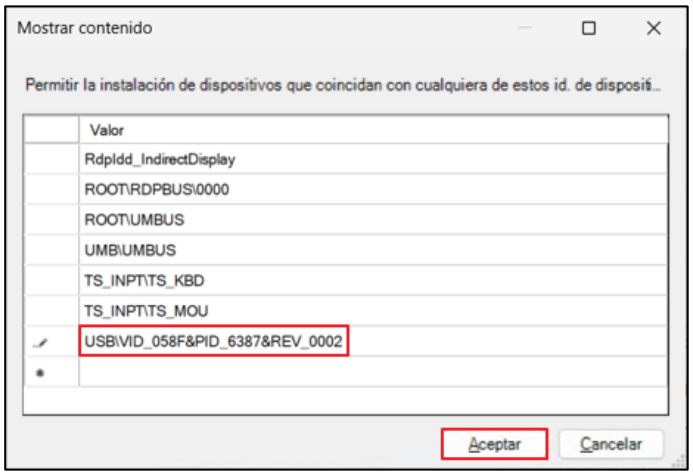


Ilustración 93 - Eliminación del id. de hardware del dispositivo

Nota: No modifique ni elimine los identificadores ya establecidos en la directiva para el correcto funcionamiento del sistema.

9. Haga clic en “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.

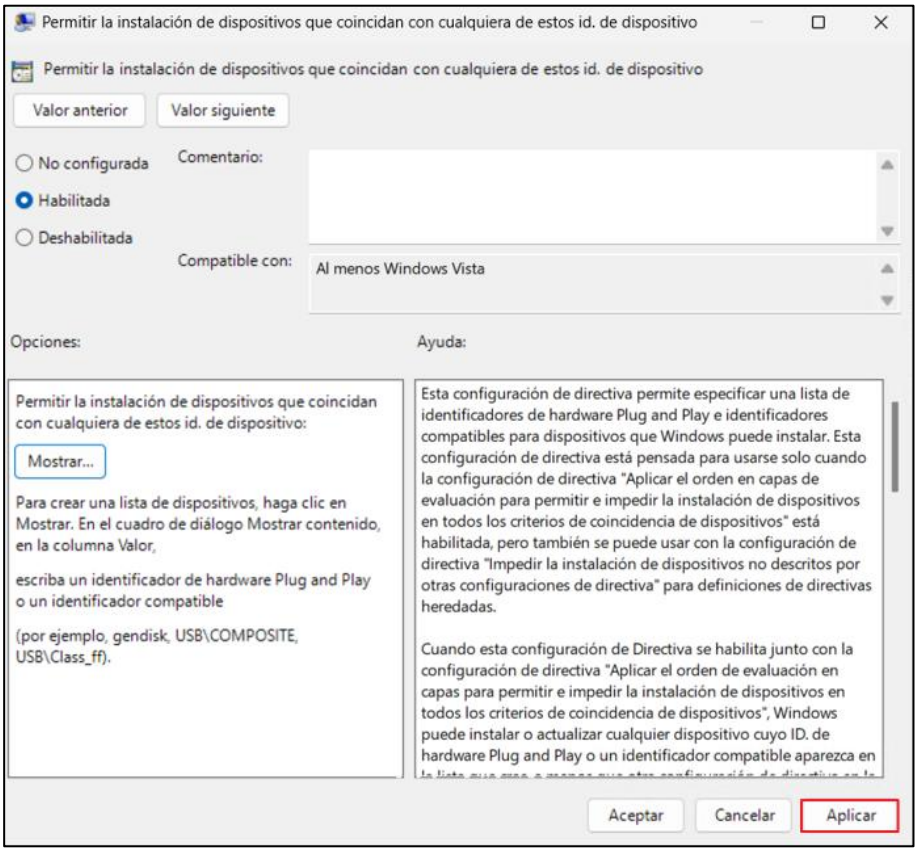
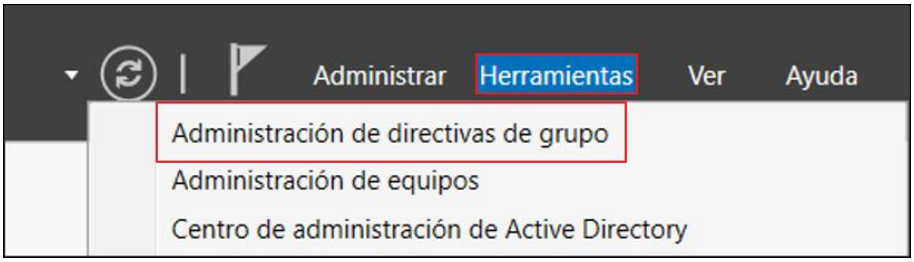
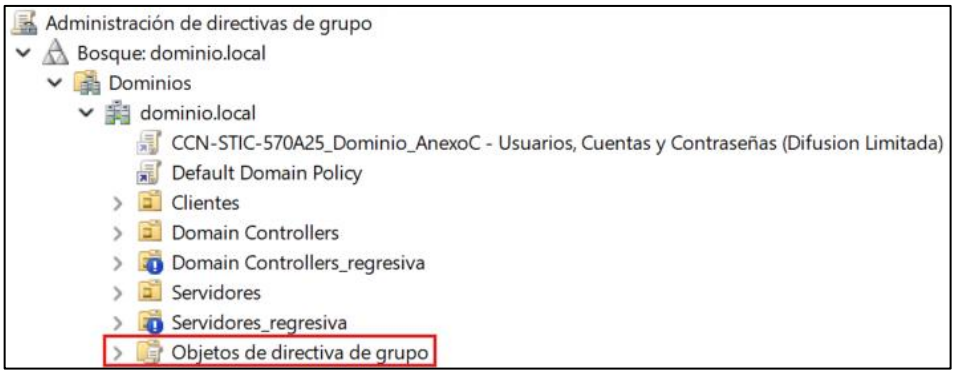


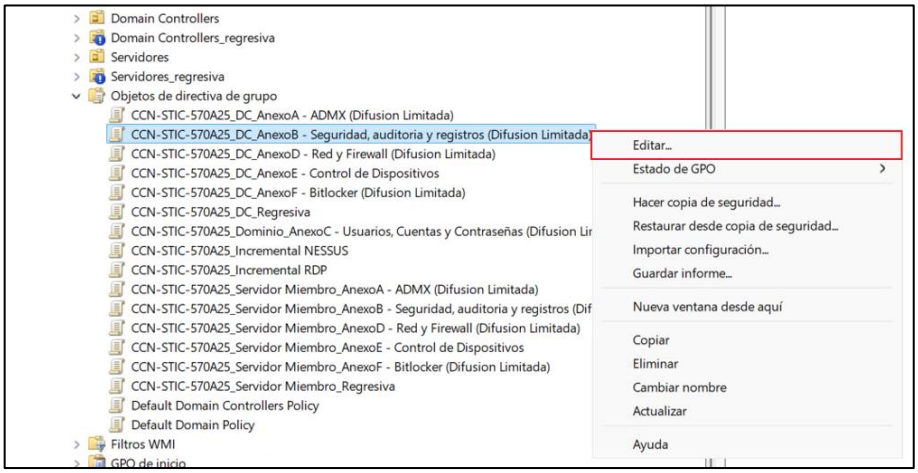
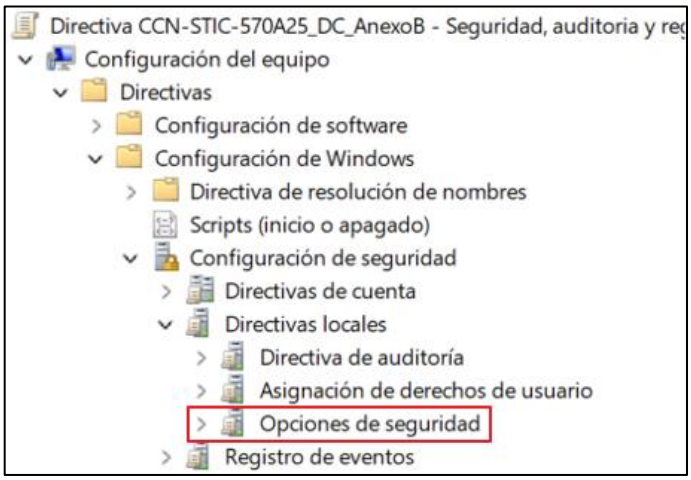
Ilustración 94 - Finalización de la configuración de la política

7.3. MODIFICACIÓN DEL MENSAJE DE INICIO DE SESIÓN

Este apartado recoge la necesidad de modificar el mensaje de inicio de sesión y acceso al sistema configurado por defecto durante el proceso de aplicación de medidas de seguridad en Windows Server, con el fin de adaptarlo a la política de seguridad de la organización. Esta modificación debe reflejar de forma clara el grado de clasificación del sistema (por ejemplo, Difusión Limitada, Confidencial, Reservado o Secreto) y el nombre oficial de la entidad responsable del sistema, conforme a los requisitos normativos pertinentes.

El mensaje de inicio de sesión tiene como objetivo informar al usuario de los derechos y obligaciones derivados del uso del sistema, así como advertir de las acciones que no están permitidas en el equipo. Así mismo, se deja constancia de que el sistema se encuentra monitorizado y cualquier acción es registrada y auditada.. Esta medida contribuye a reforzar el control de acceso y la concienciación del usuario sobre el entorno en el que opera.

Paso	Descripción
1.	Inicie sesión en un servidor con el rol de Controlador de Dominio del dominio en el que quiere configurarse el control de dispositivos.
2.	Desde el "Administrador del servidor", seleccione Herramientas > Administración de directivas de grupo.  *Ilustración 95 - Acceso a la administración de GPOs*
3.	Despliegue la raíz del dominio, y después despliegue "Objetos de directiva de grupo".  *Ilustración 96 - Despliegue de los objetos de directiva de grupo*

4.	Haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoB – Seguridad, auditoría y registros (Difusión Limitada)”, y seleccione la opción “Editar” en el menú contextual.  *Ilustración 97 - Edición del GPO* **Nota:** Puede editar el mensaje de inicio de sesión de los Controladores de Dominio (en el GPO indicado en el ejemplo) así como el de los servidores miembro del dominio. Para el segundo caso, es necesario editar el GPO “CCN-STIC-570A25_Servidor Miembro_AnexoB – Seguridad, auditoría y registros (Difusión Limitada)”.
5.	Despliegue el nodo “Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad”.  *Ilustración 98 – Despliegue del nodo de opciones de seguridad*
6.	Edite las políticas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión”. Para editarlas, haga doble clic sobre cada una de ellas.

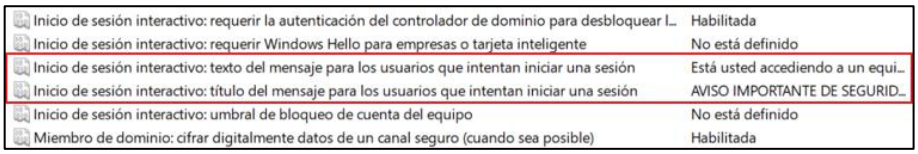


Ilustración 99 - GPOs de texto y título de mensaje

7. Texto del mensaje:

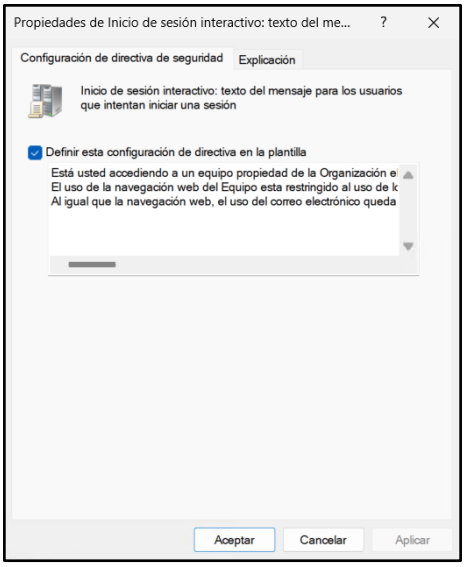


Ilustración 100 - Texto del mensaje

8. Título del mensaje:

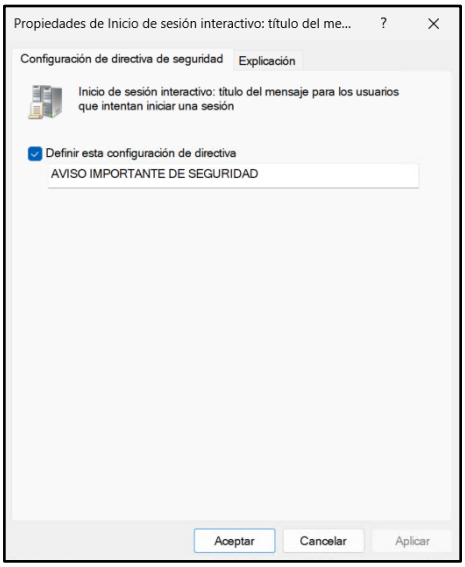
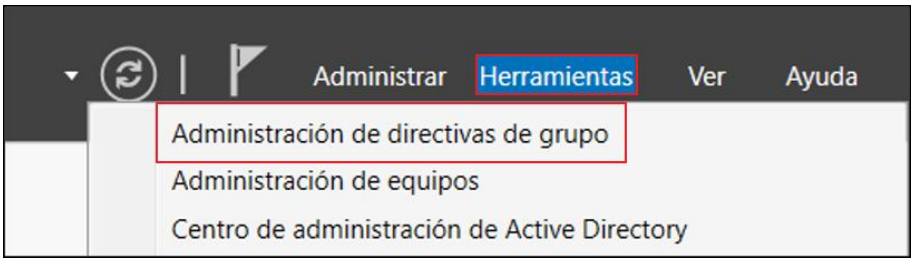
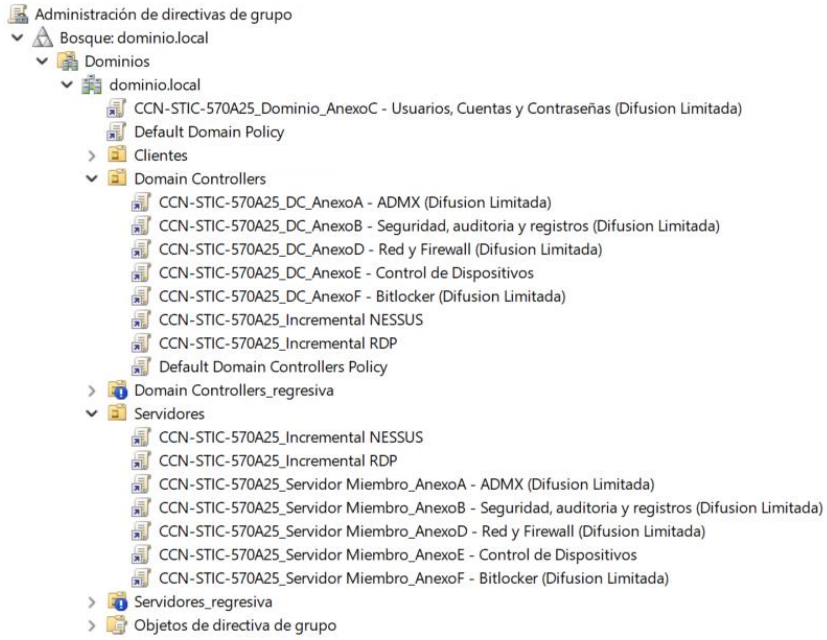


Ilustración 101 - Título del mensaje

7.4. COMPROBACIONES DE LAS MEDIDAS APLICADAS

El presente anexo describe el procedimiento para verificar que las políticas de seguridad definidas en los distintos anexos de esta guía han sido correctamente aplicadas y sus correspondientes políticas importadas y asignadas a las unidades organizativas (OUs) correspondientes dentro del entorno de Active Directory.

Paso	Descripción
1.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el dominio que se ha aplicado seguridad.
2.	Desde el "Administrador del servidor", seleccione Herramientas > Administración de directivas de grupo.  *Ilustración 102 - Acceso a la administración de GPOs*
3.	Despliegue la raíz del dominio, las GPO deben estar asociadas en base al siguiente esquema:  *Ilustración 103 - Listado completo de GPOs creadas* El grado de clasificación y los Anexos que se visualicen, deben ser los aplicados durante el proceso de fortificación del entorno.

Si no visualiza los anexos y/o falta alguno que haya sido ejecutado, se debe reiniciar el proceso aplicando exclusivamente los anexos que no se encuentran aplicados.

Nota: Todas las directivas de grupo se encuentran con el vínculo deshabilitado por defecto, como medida preventiva para evitar la aplicación automática antes de su validación final. La habilitación de estos vínculos se realizará en un anexo posterior de esta guía, una vez completadas las comprobaciones técnicas y funcionales necesarias.

PUBLICACIONES DE DEFENSA

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