

Guía de Seguridad de las TIC

CCN-STIC 599AB25

PERFILADO DE SEGURIDAD PARA WINDOWS 11 (CLIENTE MIEMBRO O CLIENTE INDEPENDIENTE)



SEPTIEMBRE 2026

Edita:



Pº de la Castellana 109, 28046 Madrid
© Autor y editor, 2026
(edición en línea)



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: 2026.09.07 15:09:58 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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



[Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.](#)

INDICE

1. INTRODUCCIÓN	6
2. OBJETO.....	7
3. ALCANCE	8
4. DESCRIPCIÓN DE USO DE ESTA GUÍA	9
5. PERFIL DE CUMPLIMIENTO TÉCNICO ESPECÍFICO CCN-STIC	13
6. OPCIÓN A. EQUIPO WINDOWS 11 MIEMBRO DE DOMINIO	14
6.1. ANEXO A. CONFIGURACIÓN BASE DE WINDOWS.....	14
6.1.1. CARACTERÍSTICAS DE WINDOWS.....	14
6.1.1.1. IMPACTO.....	14
6.1.2. PLANTILLAS ADMINISTRATIVAS.....	15
6.1.2.1. IMPACTO.....	15
6.1.3. APLICACIÓN DE MEDIDAS EN EQUIPOS FINALES	15
6.1.4. APLICACIÓN DE MEDIDAS DE SEGURIDAD BASE EN EL CONTROLADOR DE DOMINIO	21
6.2. ANEXO B. POLÍTICAS DE SEGURIDAD, AUDITORIA Y REGISTROS DE EVENTOS	30
6.2.1. IMPACTO	30
6.2.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD, AUDITORÍA Y REGISTROS.....	31
6.3. ANEXO C. GESTIÓN DE USUARIOS Y POLÍTICAS DE CUENTA Y CONTRASEÑA	32
6.3.1. SISTEMA DE NOMBRES.....	32
6.3.2. IMPACTO	32
6.3.3. APLICACIÓN DE MEDIDAS DE SEGURIDAD DE USUARIOS, CUENTAS Y CONTRASEÑAS.....	33
6.4. ANEXO D. SEGURIDAD DE RED Y FIREWALL DE WINDOWS DEFENDER.....	34
6.4.1. IMPACTO	34
6.4.2. APLICACIÓN DE SEGURIDAD DE RED.....	35
6.5. ANEXO E. MANEJO Y CONTROL DE DISPOSITIVOS.....	36
6.5.1. IMPACTO	36
6.5.2. APLICACIÓN DE SEGURIDAD SOBRE DISPOSITIVOS EXTRAÍBLES	37
6.6. ANEXO F. CONFIGURACIÓN DE BITLOCKER Y CRIPTOGRAFIA	38
6.6.1. IMPACTO	38
6.6.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD CRIPTOGRÁFICAS.....	39
6.7. ANEXO G. ACCESO MEDIANTE ESCRITORIO REMOTO	41
6.7.1. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN RDP.....	41

6.8.	ANEXO H. PROTECCIÓN FRENTE A CÓDIGO DAÑINO	43
6.8.1.	IMPACTO	43
6.8.2.	APLICACIÓN DE MEDIDAS DE SEGURIDAD	44
6.9.	ANEXO I. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD	46
6.9.1.	IMPACTO	46
6.9.2.	APLICACIÓN DE MEDIDAS DE SEGURIDAD	47
6.10.	CONFIGURACIONES MANUALES Y COMPROBACIONES.....	51
6.10.1.	GESTIÓN DE GPOS	51
6.10.2.	ADMINISTRACIÓN Y CONTROL DE NUEVOS DISPOSITIVOS EXTRAÍBLES	55
6.10.2.1.	INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES	55
6.10.2.2.	INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR	58
6.10.2.3.	ELIMINAR DISPOSITIVOS USB DADOS DE ALTA	66
6.10.3.	MODIFICACIÓN DEL MENSAJE DE INICIO DE SESIÓN	73
6.10.4.	COMPROBACIONES DE LAS MEDIDAS APLICADAS.....	76
7.	OPCIÓN B. EQUIPO WINDOWS 11 INDEPENDIENTE	78
7.1.	ANEXO A. CONFIGURACIÓN BASE DE WINDOWS.....	78
7.1.1.	CARACTERÍSTICAS DE WINDOWS.....	78
7.1.1.1.	IMPACTO.....	78
7.1.2.	PLANTILLAS ADMINISTRATIVAS.....	79
7.1.2.1.	IMPACTO.....	79
7.1.3.	APLICACIÓN DE MEDIDAS DE SEGURIDAD BASE.....	79
7.2.	ANEXO B. POLÍTICAS DE SEGURIDAD, AUDITORIA Y REGISTROS DE EVENTOS	86
7.2.1.	IMPACTO	86
7.2.2.	APLICACIÓN DE MEDIDAS DE SEGURIDAD, AUDITORÍA, REGISTROS Y SERVICIOS	87
7.3.	ANEXO C. GESTIÓN DE USUARIOS Y POLÍTICAS DE CUENTA Y CONTRASEÑA	88
7.3.1.	SISTEMA DE NOMBRES.....	88
7.3.2.	IMPACTO	88
7.3.3.	APLICACIÓN DE MEDIDAS DE SEGURIDAD DE USUARIOS, CUENTAS Y CONTRASEÑAS.....	89
7.4.	ANEXO D. SEGURIDAD DE RED Y FIREWALL DE WINDOWS DEFENDER.....	90
7.4.1.	IMPACTO	90
7.4.2.	APLICACIÓN DE SEGURIDAD DE RED.....	91

7.5. ANEXO E. MANEJO Y CONTROL DE DISPOSITIVOS.....	92
7.5.1. IMPACTO	92
7.5.2. APLICACIÓN DE SEGURIDAD SOBRE DISPOSITIVOS EXTRAÍBLES	92
7.6. ANEXO F. CONFIGURACIÓN DE BITLOCKER Y CRIPTOGRAFIA	94
7.6.1. IMPACTO	94
7.6.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD CRIPTOGRÁFICAS	95
7.7. ANEXO G. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD	96
7.7.1. IMPACTO	96
7.7.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD	97
7.8. ANEXO H. PROTECCIÓN FRENTE A CÓDIGO DAÑINO	98
7.8.1. IMPACTO	98
7.8.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD	98
7.9. CONFIGURACIONES MANUALES Y COMPROBACIONES.....	100
7.9.1. ADMINISTRACIÓN Y CONTROL DE NUEVOS DISPOSITIVOS EXTRAÍBLES	100
7.9.1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB POR PARTE DE ADMINISTRADORES	100
7.9.1.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR	102
7.9.1.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA	109
7.9.2. MODIFICACIÓN DEL MENSAJE DE INICIO DE SESIÓN	115
7.9.3. COMPROBACIONES DE LAS MEDIDAS APLICADAS.....	118

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 11.

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 11, alineándolas y clasificándolas en función de los requisitos definidos por las normativas aplicables.

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

3. ALCANCE

La guía se ha elaborado para proporcionar información específica sobre cómo implementar las distintas configuraciones según diferentes escenarios. En particular, se incluirá la configuración para asegurar **equipos basados en un sistema operativo “Microsoft Windows 11”**, instalados en español, bien actuando como **cliente miembro de un dominio** o bien como un **cliente independiente**.

El documento no se centrará en una edición y versión concreta del sistema operativo, como pueda ser Windows 11 23H2 o Windows 11 25H2, sino que será de utilidad para **cualquier edición y versión cliente de Windows 11** (siendo recomendable su aplicación desde la edición Windows 11 23H2 en adelante). Esto será posible siempre que estas configuraciones puedan ser de aplicación o bien cuando los aspectos técnicos del propio sistema operativo permitan la aplicación de las medidas definidas en el presente documento.

Nota: Para la elaboración del presente documento y la definición de medidas de seguridad se ha hecho uso del sistema operativo Windows 11 Pro, Versión 25H2.

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:

- 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.
- 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. A medida que el sistema operativo Windows Cliente disponga de nuevas configuraciones de seguridad de interés que cubran las medidas aplicables, se incluirá en dicho punto la explicación sobre dichas parametrizaciones. Esto tiene por objetivo cumplir lo indicado en el apartado anterior sobre la actualización en el tiempo según las nuevas amenazas y estado de arte tecnológico en ciberseguridad, así como nuevas configuraciones de seguridad proporcionadas por los productos.
- d) Aplicación de seguridad. Permitirá implantar y establecer las configuraciones de seguridad definidas y creadas para sistemas operativos Windows 11, cuando estos realicen las funciones de cliente miembro de un dominio o un cliente independiente.

4. DESCRIPCIÓN DE USO DE ESTA GUÍA

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

- a) Independiente de la aplicación de medidas asociadas a esta guía, debe cubrirse todo el espectro de necesidades recogidas bajo las indicaciones del ENS, así como el resto de normativa aplicable que pueda intervenir para la correcta adecuación de los sistemas de información TIC.
- b) Dada la necesidad anterior, previo a la aplicación de medidas descritas en el presente documento, y según se especifica en el ENS, se tendrá en consideración que el análisis y la gestión de los riesgos es uno de los puntos esenciales del proceso de seguridad. En este sentido deberá prestarse especial atención a los riesgos asociados a un sistema operativo Windows 11.
 - 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) 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.
- f) 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.
- g) 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
- 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:

- ENS
- 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.

		CALIFICACIÓN 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 el que, 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.

- a) Definido el perfil a implementar, en este paso se aplicarán las medidas de seguridad necesarias, adicionales y recomendadas según el perfil de seguridad seleccionado y las posibles normativas adicionales aplicables (Ley de Secretos Oficiales, normativa CCN-STIC-301, entre otras).
 - i. Si el equipo va a ser cliente miembro de un dominio, se debe proceder de la siguiente manera:
 - Revisar e implementar el apartado correspondiente a la aplicación de seguridad sobre un cliente miembro.
 - ii. Si el equipo es un cliente independiente, se debe proceder de la siguiente forma:

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

La presente guía, a su vez, recoge el conjunto de medidas técnicas de seguridad que pueden aplicarse a sistemas operativos Windows 11, 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 11, 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 11, 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.

6. OPCIÓN A. EQUIPO WINDOWS 11 MIEMBRO DE DOMINIO

6.1. 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.

El presente apartado contempla la aplicación de medidas de seguridad sobre equipos cliente miembros del dominio. **Se debe tener en cuenta que algunos anexos del script deben ejecutarse de forma local en los equipos miembro del dominio**, en concreto aquellos relacionados con **configuraciones locales** del sistema operativo.

Nota: Los scripts asociados al presente apartado **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.

6.1.1. CARACTERÍSTICAS DE WINDOWS

Nota: Este anexo debe ejecutarse de manera local sobre los equipos Windows 11 Miembro del entorno.

El presente anexo recoge las configuraciones iniciales necesarias para establecer una base segura en sistemas Windows 11. 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 desinstalación de aplicaciones aprovisionadas e 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 11.

6.1.1.1. IMPACTO

La desactivación de características y la desinstalación de aplicaciones aprovisionadas del sistema operativo que no son necesarias para el rol específico del cliente miembro de dominio 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, 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) Imposibilidad de que nuevas cuentas de usuario reciban determinadas aplicaciones aprovisionadas, al haber sido eliminadas de la imagen del sistema.
- d) Necesidad de revisión previa de los requisitos funcionales del sistema, de las aplicaciones desplegadas y de los perfiles de usuario existentes, 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.

6.1.2. PLANTILLAS ADMINISTRATIVAS

6.1.2.1. 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.

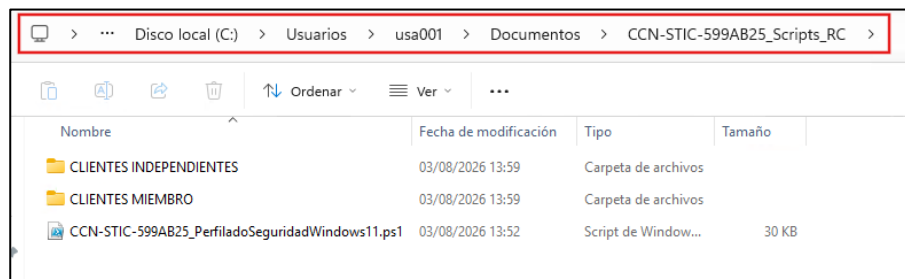
Nota: Se recomienda validar las plantillas en un entorno de pruebas antes de su despliegue en producción, y documentar cualquier excepción necesaria para garantizar la operatividad del sistema.

6.1.3. APLICACIÓN DE MEDIDAS EN EQUIPOS FINALES

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

3. Verifique que en su interior se encuentran los siguientes archivos:

- CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
- Directorio: CLIENTES INDEPENDIENTES.
- Directorio: CLIENTES MIEMBRO.

*Ilustración 1 - Ruta del script*

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

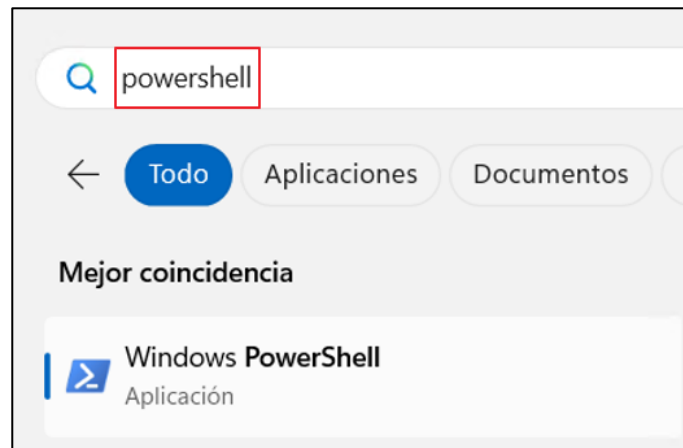


Ilustración 2 - Búsqueda de Powershell

A continuación, seleccione “Ejecutar como administrador”.

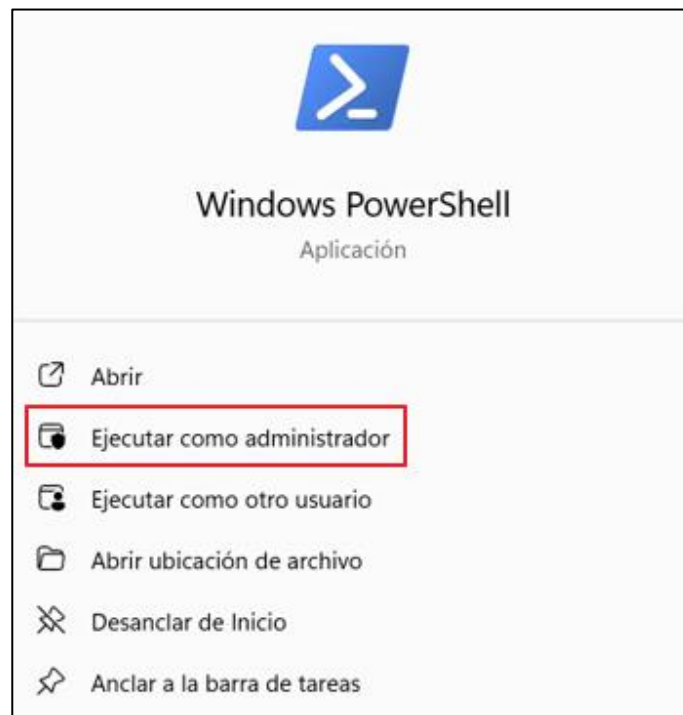
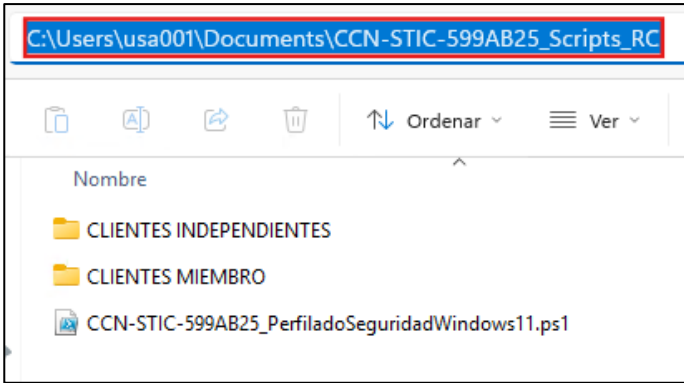


Ilustración 3 - Ejecución como administrador de PowerShell

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.

5.	En la consola de comandos de Powershell, ejecute la sentencia “Get-ExecutionPolicy”: <pre>PS C:\WINDOWS\system32> Get-ExecutionPolicy Restricted PS C:\WINDOWS\system32> _</pre> <i>Ilustración 4 - Ejecución de Get-ExecutionPolicy</i>
6.	Si el resultado muestra un valor diferente a “Unrestricted”, deberá ejecutar el siguiente comando para permitir la ejecución de scripts: “Set-ExecutionPolicy Unrestricted”. <pre>PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted</pre> Cambio de directiva de ejecución La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución? [S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): _ <i>Ilustración 5 - Ejecución de Set-ExecutionPolicy</i>
7.	A continuación, pulse la tecla “O” y posteriormente, la tecla “enter” para confirmar: <pre>PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted</pre> Cambio de directiva de ejecución La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución? [S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): O PS C:\WINDOWS\system32> _ <i>Ilustración 6 - Confirmación de cambio de directiva de ejecución</i>
8.	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”.  <i>Ilustración 7 - Copia de la ruta</i>
9.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada. <pre>PS C:\Windows\System32> cd C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC</pre> <i>Ilustración 8 - Acceso a la ruta desde PowerShell</i>

- 10.** Ejecute el comando “dir” para verificar la ubicación y el contenido.

```
PS C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC> dir

Directorio: C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC

Mode                LastWriteTime         Length Name
----                -
d-----          03/08/2026   13:59             CLIENTES INDEPENDIENTES
d-----          03/08/2026   13:59             CLIENTES MIEMBRO
d-----          03/08/2026   13:52          30612 CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
```

Ilustración 9 - Verificación de los archivos

- 11.** Ejecute el archivo “CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1” escribiendo “.” y pulsando la tecla tabulador hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.

```
CCN-STIC-599AB25_Scripts_RC> .\CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
```

Ilustración 10 - Ejecución del script de perfilado de seguridad de Windows 11

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

```

      ---ADVERTENCIA---
Este script incorpora modificaciones en el sistema orientadas a la aplicación de medidas de bastionado, conforme a los
perfiles de seguridad definidos por el Centro Criptológico Nacional (CCN). Para su correcta aplicación, es imprescindible
seguir las recomendaciones establecidas en la guía CCN-STIC-599AB25, comprendiendo los riesgos, impactos y acciones
asociadas que en ella se detallan.
      ---FIN ADVERTENCIA---
```

Ilustración 11 - Advertencia de uso

- 13.** El asistente detectará que el equipo es miembro de dominio y que el sistema utilizado es Windows 11.

```

Este equipo es miembro de un dominio y ejecuta Windows 11
Creando carpeta Scripts...
Carpeta preparada

Creando carpeta CLIENTES MIEMBRO...
Carpeta CLIENTES MIEMBRO preparada

ELIJA EL PERFIL DE CALIFICACION
Seleccione una opcion
[D] DIFUSION LIMITADA [I] INFORMACION CLASIFICADA [?] Ayuda (el valor predeterminado es "D"): _
```

Ilustración 12 - Detección del sistema utilizado

- 14.** A continuación, seleccione el perfil de calificación de la información que se desea aplicar. En este caso, “[D] Difusión Limitada”.

```

ELIJA EL PERFIL DE CALIFICACION
Seleccione una opcion
[D] DIFUSION LIMITADA [I] INFORMACION CLASIFICADA [?] Ayuda (el valor predeterminado es "D"): D
```

Ilustración 13 - Selección del perfil de calificación

15.

Se detectarán las características implementadas en el sistema y se solicitará confirmación para continuar con la desinstalación de las características aprovisionadas. Introduzca “S” y a continuación, pulse la tecla “Enter”.

```
Windows 11 miembro de dominio detectado.
Grado seleccionado: DIFUSION LIMITADA
Buscando Appx-Caract en:
C:\Scripts\CLIENTES MIEMBRO\DIFUSION LIMITADA\ANEXO A - CONFIGURACION BASE\CCN-STIC-599A25 - ANEXO A (Appx-Caract).ps1

Ejecutando Appx-Caract...
CARACTERISTICAS OPCIONALES HABILITADAS EN EL EQUIPO

Name                                DisplayName                                FeatureType                                State
----                                -
MediaPlayback                      MediaPlayback                            WindowsOptionalFeature                  Enabled
Microsoft-RemoteDesktopConnection Microsoft-RemoteDesktopConnection        WindowsOptionalFeature                  Enabled
MicrosoftWindowsPowerShellV2Root MicrosoftWindowsPowerShellV2Root        WindowsOptionalFeature                  Enabled
MSRDC-Infrastructure               MSRDC-Infrastructure                    WindowsOptionalFeature                  Enabled
NetFx4-AdvSrvs                     NetFx4-AdvSrvs                          WindowsOptionalFeature                  Enabled
Printing-Foundation-Features        Printing-Foundation-Features             WindowsOptionalFeature                  Enabled
Printing-Foundation-InternetPrinting-Client Printing-Foundation-InternetPrinting-Client WindowsOptionalFeature                  Enabled
Printing-PrintToPDFServices-Features Printing-PrintToPDFServices-Features      WindowsOptionalFeature                  Enabled
SearchEngine-Client-Package         SearchEngine-Client-Package              WindowsOptionalFeature                  Enabled
SmbDirect                          SmbDirect                               WindowsOptionalFeature                  Enabled
WCF-Services45                     WCF-Services45                          WindowsOptionalFeature                  Enabled
WCF-TCP-PortSharing45              WCF-TCP-PortSharing45                   WindowsOptionalFeature                  Enabled
Windows-Defender-Default-Definitions Windows-Defender-Default-Definitions      WindowsOptionalFeature                  Enabled
WindowsMediaPlayer                  WindowsMediaPlayer                        WindowsOptionalFeature                  Enabled
WorkFolders-Client                  WorkFolders-Client                       WindowsOptionalFeature                  Enabled

Se van a deshabilitar características opcionales del sistema y eliminar aplicaciones aprovisionadas/capacidades indicadas.
ADVERTENCIA: El script contempla las características mínimas necesarias y las mantiene.

ADVERTENCIA: El script contempla las aplicaciones mínimas necesarias y las mantiene

¿Desea continuar la deshabilitación de características opcionales y la eliminación de aplicaciones aprovisionadas?
Seleccione una opción:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): _
```

Ilustración 14 - Confirmación de eliminación de aplicaciones

16.

Transcurridos unos instantes, todas las características innecesarias se habrán eliminado completamente del sistema.

```
Deshabilitando característica: WindowsMediaPlayer
ADVERTENCIA: No se pudo deshabilitar la característica: WindowsMediaPlayer. Continuando...
Características opcionales deshabilitadas correctamente.
Puede consultar un registro de las características deshabilitadas en el fichero C:\Scripts\CCN-STIC-599A25_Caracteristicas Deshabilitadas.csv

Para completar los cambios se recomienda reiniciar el equipo.
```

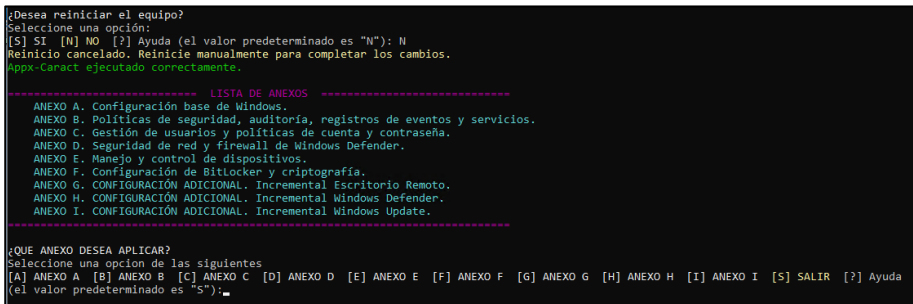
Ilustración 15 - Finalización de la ejecución

17.

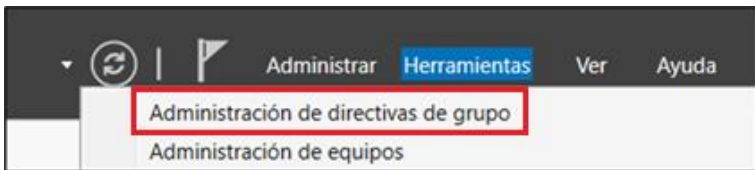
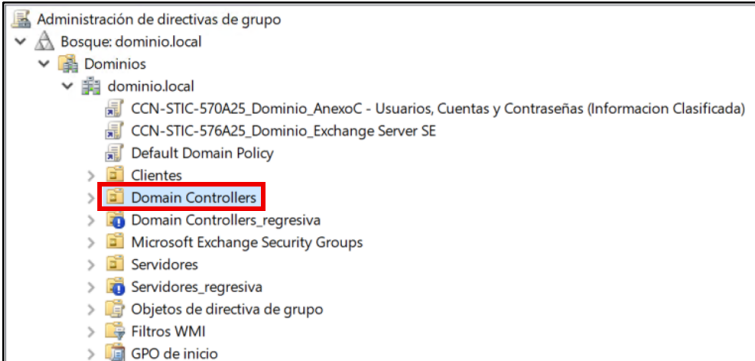
Pulse la tecla “S” si desea reiniciar el equipo tras la finalización de la ejecución. Si, por el contrario, desea reiniciar el sistema más adelante, pulse “N”.

```
Para completar los cambios se recomienda reiniciar el equipo.
¿Desea reiniciar el equipo?
Seleccione una opción:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): _
```

Ilustración 16 - Reiniciar el equipo

18.	En el caso de no reiniciar el equipo en el punto anterior, pulse la tecla “S” para finalizar la ejecución del script de fortificación y continuar con los siguientes anexos de esta guía. 
------------	---

6.1.4. APLICACIÓN DE MEDIDAS DE SEGURIDAD BASE EN EL CONTROLADOR DE DOMINIO

Paso	Descripción
19.	Inicie sesión en el servidor con rol Controlador de Dominio sobre el que se quiere comenzar el proceso de fortificación.
20.	En el “Administrador del servidor”, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.  <i>Ilustración 17 - Administración de directivas de grupo</i>
21.	Despliegue en el panel izquierdo hasta llegar a la OU “Domain Controllers”.  <i>Ilustración 18 - Acceso a la OU de Domain Controllers</i>

- 22.** Despliegue dicha Unidad Organizativa, haga clic derecho sobre el GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Información Clasificada)”, y seleccione “Editar”.

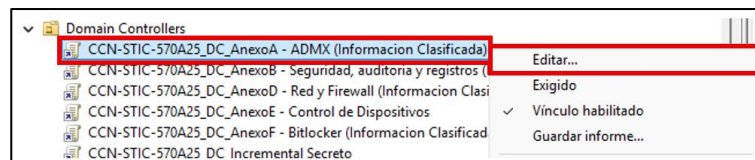


Ilustración 19 - Edición de GPO

- 23.** En el panel “Editor de administración de directivas de grupo”, despliegue la lista siguiendo la siguiente ruta: “Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell”. Haga clic sobre “Windows PowerShell” para consultar las políticas que aplica.

Configuración	Estado	Comentario
Activar registro de módulos	Habilitada	No
Activar el registro de bloque de script de PowerShell	Habilitada	No
Activar la ejecución de scripts	Habilitada	No
Activar la transcripción de PowerShell	Habilitada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Ilustración 20 - Modificación de la ejecución de scripts

- 24.** Haga doble clic sobre la política “Activar la ejecución de scripts”.

Configuración	Estado	Comentario
Activar registro de módulos	Habilitada	No
Activar el registro de bloque de script de PowerShell	Habilitada	No
Activar la ejecución de scripts	Habilitada	No
Activar la transcripción de PowerShell	Habilitada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Ilustración 21 - Activar la ejecución de scripts

- 25.** En el desplegable de la política, seleccione “Permitir todos los scripts”:

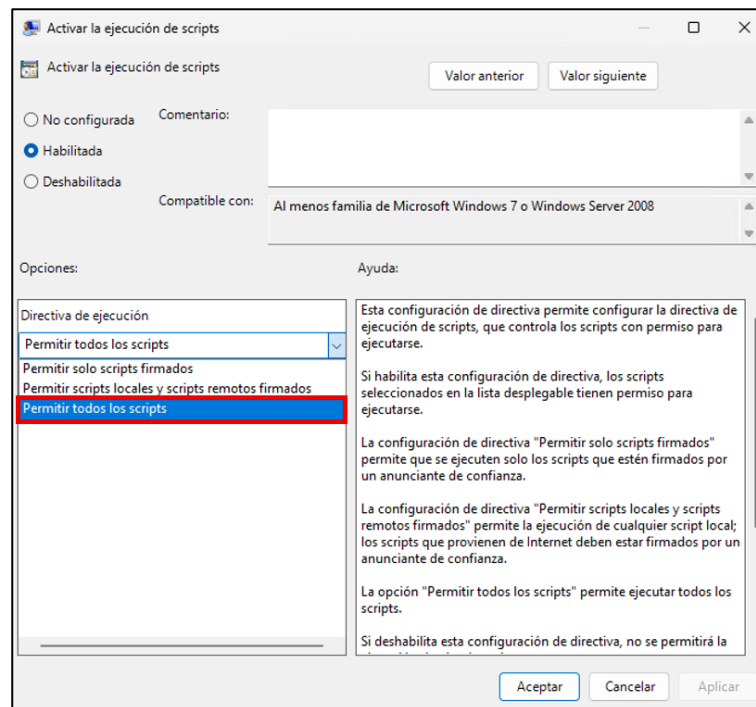


Ilustración 22 - Permitir todos los scripts

- 26.** A continuación, pulse en “Aplicar” y “Aceptar”

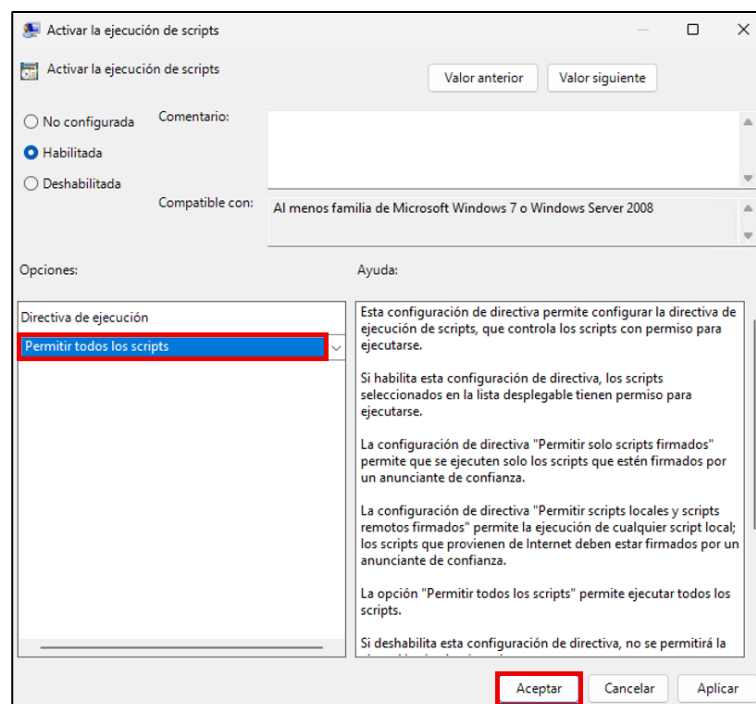
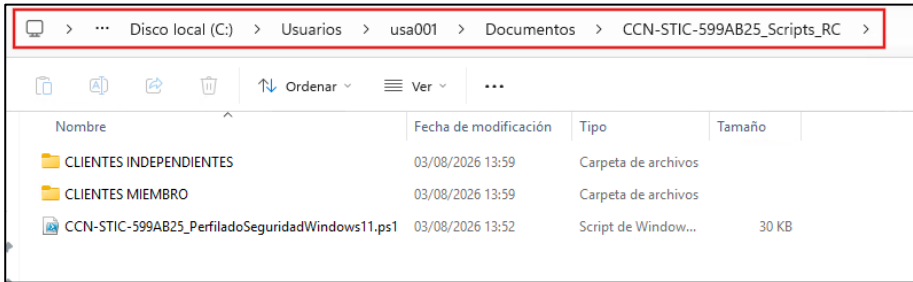


Ilustración 23 - Aplicación de los cambios

- 27.** Reinicie el controlador de dominio para que se aplique la configuración correctamente.

28.	A continuación, inicie de nuevo sesión en el controlador de dominio que está utilizando para la aplicación de las medidas de seguridad.
29.	Copie los ficheros y directorios que acompañan a esta guía, al directorio en la carpeta “Documentos” del usuario administrador. A continuación, descomprima la carpeta.
30.	Verifique que en su interior se encuentran los siguientes archivos: – CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1 – Directorio: CLIENTES INDEPENDIENTES. – Directorio: CLIENTES MIEMBRO.  <i>Ilustración 24 - Ruta de scripts</i>

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

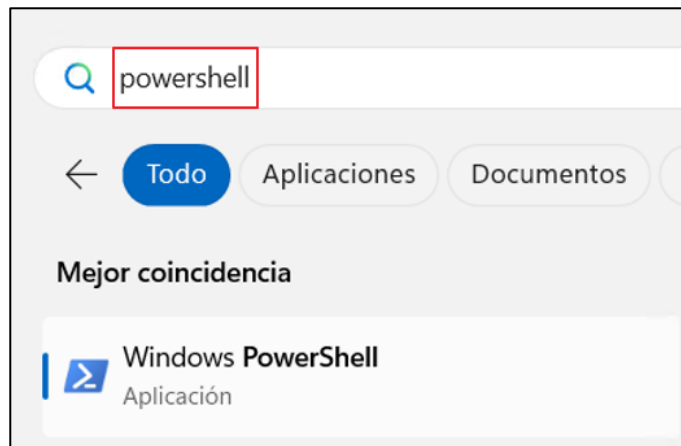


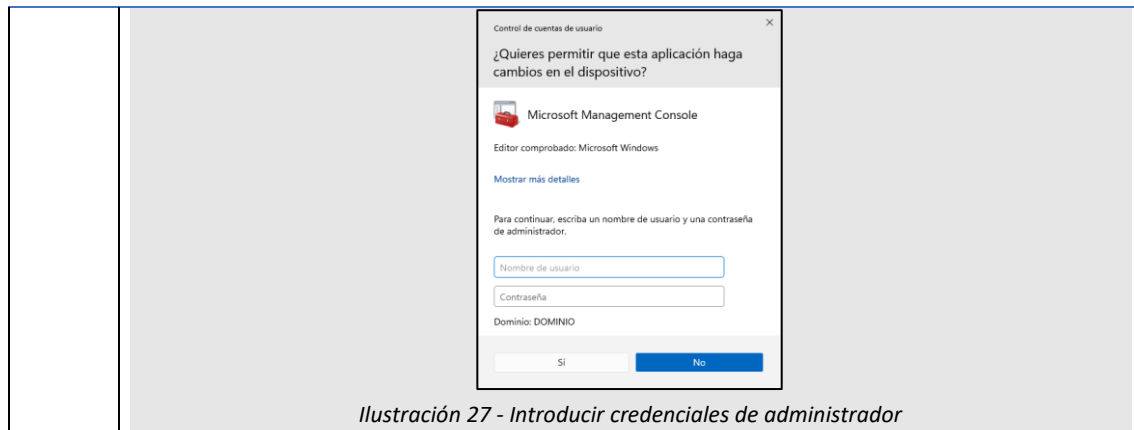
Ilustración 25 - Powershell

A continuación, seleccione “Ejecutar como administrador”.

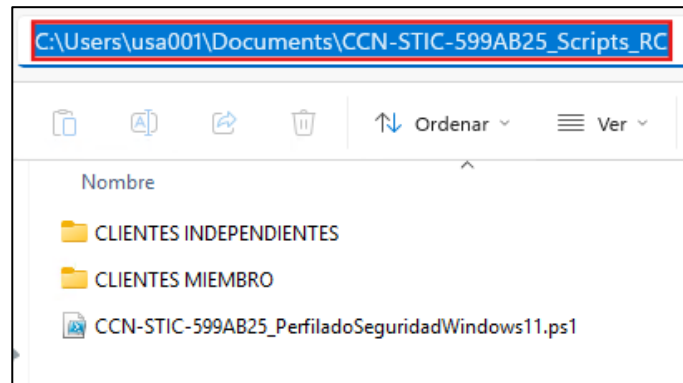


Ilustración 26 - Ejecución como administrador de PowerShell

Nota: Si el script no se ejecuta desde PowerShell en modo administrador, existe la posibilidad de que ocurran fallos durante el proceso de copia y/o que no se visualice la información de manera adecuada. Introduzca las credenciales de un usuario administrador si el control de cuentas de usuario lo solicita.



- 32.** 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”.



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

```
PS C:\Windows\System32> cd C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC
```

Ilustración 29 - Acceso a la ruta desde PowerShell

- 34.** Ejecute el comando “dir” para verificar la ubicación y el contenido.

```
PS C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC> dir

Directorio: C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC

Mode                LastWriteTime         Length Name
----                -
d-----          03/08/2026   13:59          CLIENTES INDEPENDIENTES
d-----          03/08/2026   13:59          CLIENTES MIEMBRO
-a-----          03/08/2026   13:52       30612 CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
```

Ilustración 30 - Verificación de los archivos

35.	Ejecute el archivo “CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1” escribiendo “.\” y pulsando la tecla tabulador hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución. <pre>CCN-STIC-599AB25_Scripts_RC> .\CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1</pre> <i>Ilustración 31 - Ejecución del script perfilado de seguridad</i>
36.	A continuación, se mostrará una advertencia de uso, continuando con el siguiente mensaje: <pre> ---ADVERTENCIA--- Este script incorpora modificaciones en el sistema orientadas a la aplicación de medidas de bastionado, conforme a los perfiles de seguridad definidos por el Centro Criptológico Nacional (CCN). Para su correcta aplicación, es imprescindible seguir las recomendaciones establecidas en la guía CCN-STIC-599AB25, comprendiendo los riesgos, impactos y acciones asociadas que en ella se detallan. ---FIN ADVERTENCIA---</pre> <i>Ilustración 32 - Advertencia de uso</i>
37.	Debe introducir el carácter “S” y pulsar la tecla “Enter”: <pre> ¿Desea aceptar los riesgos y continuar con el bastionado del sistema? Selecciona una opcion: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S</pre> <i>Ilustración 33 – Ejecución del script</i>
38.	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 Unidad Organizativa “Clientes 599A25”. Se podrá observar la siguiente salida: <pre> Comprobando Unidad Organizativa Clientes La Unidad Organizativa Clientes no existe. Creando Unidad Organizativa Clientes... Unidad Organizativa Clientes creada correctamente. Comprobando Unidad Organizativa Clientes 599A25 Creando Unidad Organizativa Clientes 599A25 dentro de Clientes Unidad Organizativa Clientes 599A25 creada correctamente.</pre> <i>Ilustración 34 - UO creada</i>

39. 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”.

```

ELIJA EL PERFIL DE CALIFICACION
Seleccione una opción
[D] DIFUSION LIMITADA [I] INFORMACION CLASIFICADA [?] Ayuda (el valor predeterminado es "D"): D

```

Ilustración 35 – Elegir grado

Nota: Dado que en la presente guía se aplican las configuraciones correspondientes al grado de **Difusión Limitada**, únicamente se muestran las opciones de “DIFUSION LIMITADA” e “INFORMACION CLASIFICADA. Si se aplicara la configuración correspondiente al grado **ENS**, se mostraría dicha opción.

Se copiarán automáticamente todos los archivos del grado correspondiente, junto a las configuraciones adicionales, a la carpeta de C:\Scripts\DIFUSION LIMITADA.

```

ELIJA EL PERFIL DE CALIFICACION
Seleccione una opción
[D] DIFUSION LIMITADA [I] INFORMACION CLASIFICADA [?] Ayuda (el valor predeterminado es "D"): D
Grado final seleccionado: DIFUSION LIMITADA

Preparando copia de archivos de bastionado...
Origen: C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC\CLIENTES MIEMBRO\DIFUSION LIMITADA
Destino: C:\Scripts\CLIENTES MIEMBRO

Copiando archivos de bastionado...
Copiando configuraciones adicionales...
Configuraciones adicionales copiadas.

Archivos copiados correctamente.

```

Ilustración 36 - Archivos copiados correctamente

40. Seguidamente, 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)”.

```

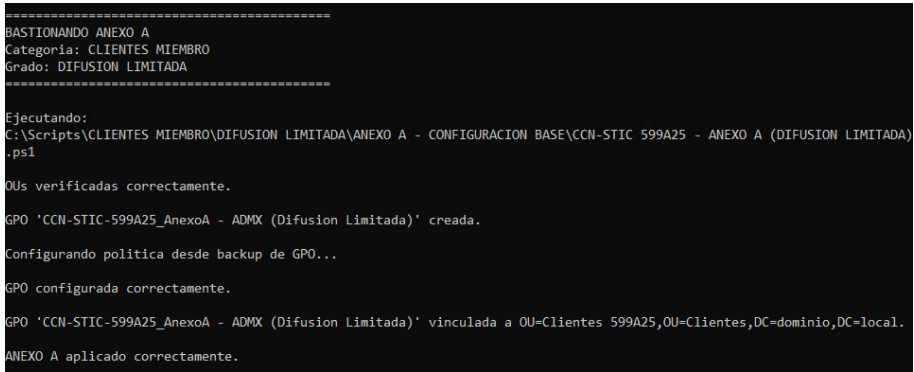
Archivos copiados correctamente.

===== LISTA DE ANEXOS =====
ANEXO A. Configuración base de Windows.
ANEXO B. Políticas de seguridad, auditoría, registros de eventos y servicios.
ANEXO C. Gestión de usuarios y políticas de cuenta y contraseña.
ANEXO D. Seguridad de red y firewall de Windows Defender.
ANEXO E. Manejo y control de dispositivos.
ANEXO F. Configuración de BitLocker y criptografía.
ANEXO G. CONFIGURACIÓN ADICIONAL. Incremental Windows Update.
ANEXO H. CONFIGURACIÓN ADICIONAL. Incremental Windows Defender.
=====

¿QUE ANEXO DESEA APLICAR?
Seleccione una opción de las siguientes
[A] ANEXO A [B] ANEXO B [C] ANEXO C [D] ANEXO D [E] ANEXO E [F] ANEXO F [G] ANEXO G [H] ANEXO H [S] SALIR
[?] Ayuda(el valor predeterminado es "S"): A

```

Ilustración 37 - Selección del anexo a aplicar

41.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 38 - Proceso de aplicación finalizado</i>
42.	No reinicie el controlador de dominio ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

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

6.2.1. 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 cliente miembro de dominio.

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.

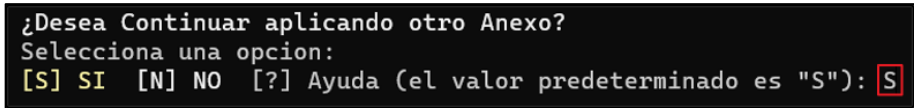
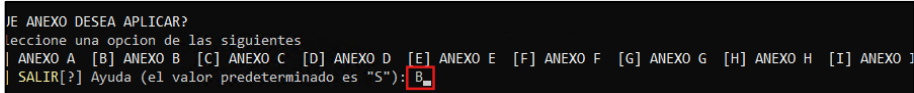
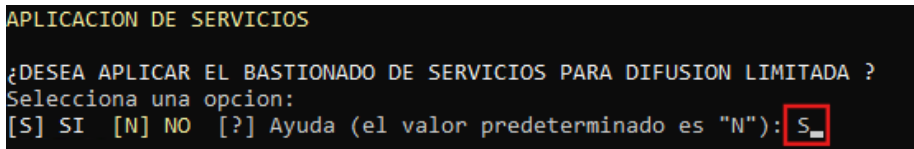
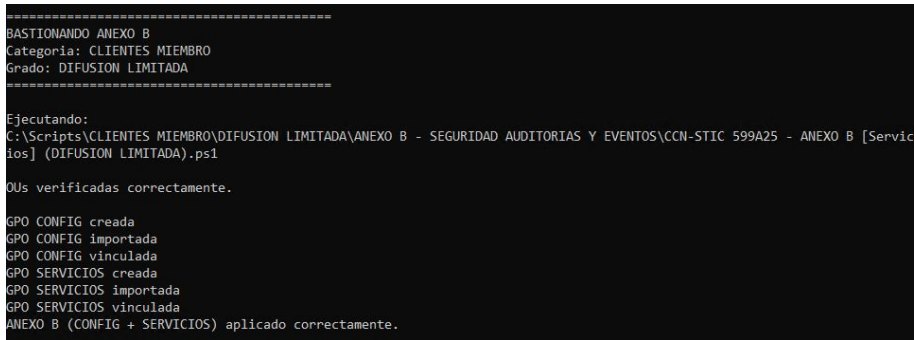
Nota: Se recomienda validar previamente las políticas en entornos de prueba y documentar excepciones necesarias para tareas operativas.

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.

6.2.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD, AUDITORÍA Y REGISTROS

Paso	Descripción
43.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 39 - Aplicación del siguiente anexo</i> Pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del presente Anexo.
44.	Introduzca el carácter “B” y pulse “Enter” para aplicar las políticas asociadas al presente anexo: “ANEXO B. Políticas de seguridad, auditoría, registro de eventos y servicios”.  <i>Ilustración 40 - Aplicación Anexo B</i>
45.	El script preguntará si desea aplicar el bastionado de servicios para el grado seleccionado. En el caso querer configurar los servicios, introduzca el carácter “S” y pulse “Enter”.  <i>Ilustración 41 - Aplicación de servicios</i>
46.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 42 - Proceso finalizado</i>
47.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

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

6.3.1. 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.

6.3.2. IMPACTO

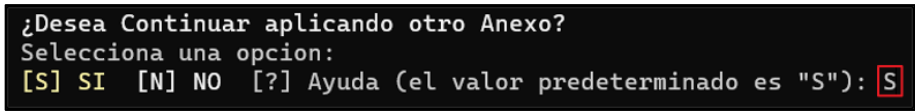
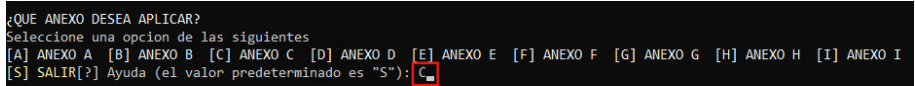
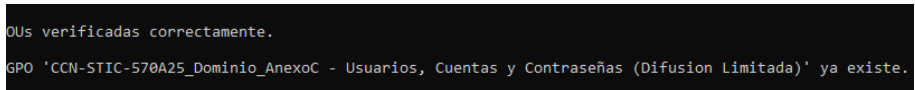
La aplicación de políticas restrictivas de cuenta y contraseña puede tener los siguientes efectos en el entorno:

- 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.

6.3.3. APLICACIÓN DE MEDIDAS DE SEGURIDAD DE USUARIOS, CUENTAS Y CONTRASEÑAS

Paso	Descripción
48.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 43 - Aplicación del siguiente anexo</i> Pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del presente Anexo.
49.	Introduzca el carácter “C” y pulse “Enter”.  <i>Ilustración 44 - Aplicación Anexo C</i> Observará el siguiente mensaje comentando que ya existe la GPO de dominio del presente Anexo.  <i>Ilustración 45 - Selección del siguiente anexo a aplicar</i>

6.4. 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 11 Miembro de dominio. 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.

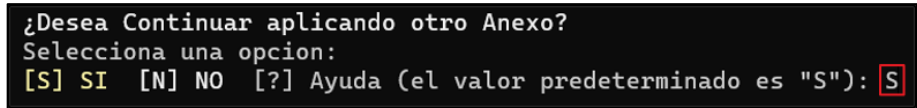
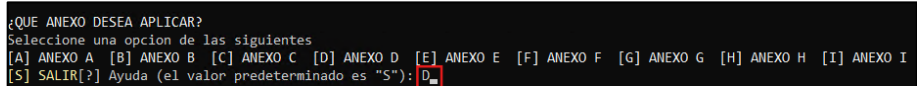
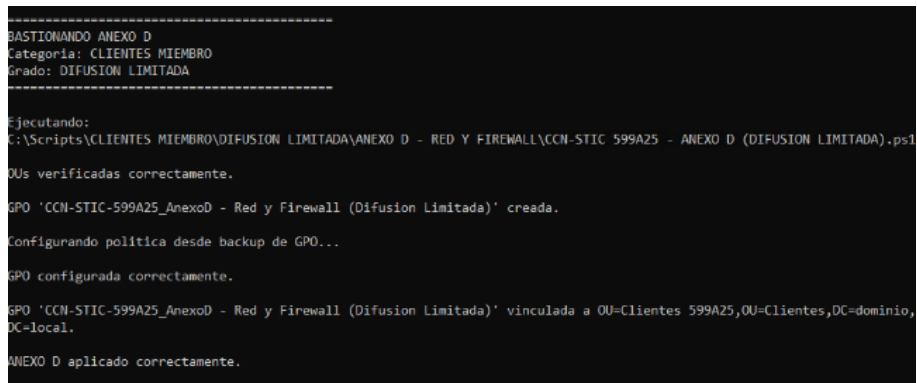
6.4.1. IMPACTO

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.

6.4.2. APLICACIÓN DE SEGURIDAD DE RED

Paso	Descripción
50.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 46 - Aplicación del siguiente anexo</i> Pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del presente Anexo. Nota: En caso de la existencia de una directiva correspondiente al “Anexo C” de las medidas de seguridad CCN-STIC-570, se podrá obviar este paso, ya que el script mostrará la selección del siguiente anexo sin interacción alguna.
51.	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”.  <i>Ilustración 47 - Selección del siguiente anexo a aplicar</i>
52.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 48 - Anexo D configurado</i>
53.	No reinicie el servidor ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

6.5. ANEXO E. MANEJO Y CONTROL DE DISPOSITIVOS

Nota: Para completar la configuración de este anexo, deberá ejecutar de manera manual los pasos descritos en la sección “7.9.1 ADMINISTRACIÓN Y CONTROL DE NUEVOS DISPOSITIVOS EXTRAÍBLES”.

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.

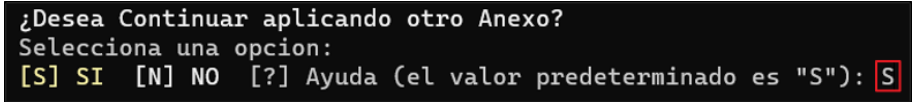
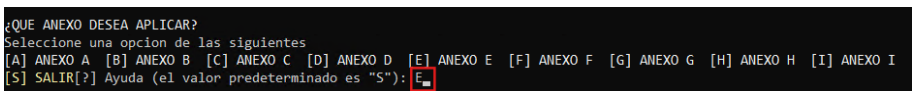
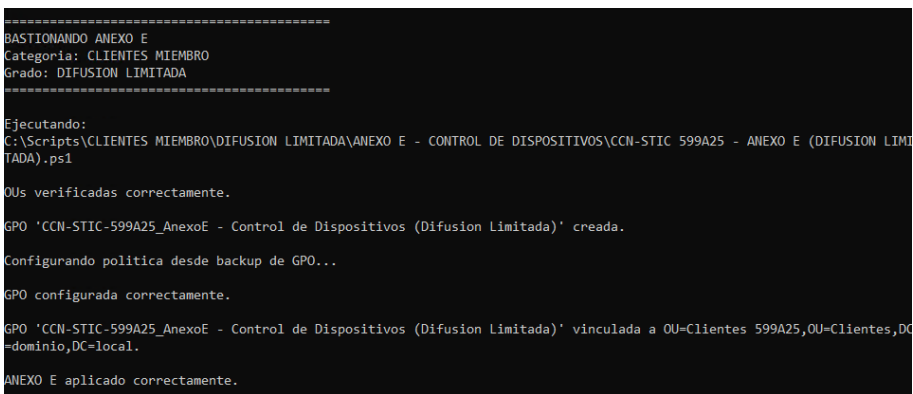
6.5.1. IMPACTO

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.

6.5.2. APLICACIÓN DE SEGURIDAD SOBRE DISPOSITIVOS EXTRAÍBLES

Paso	Descripción
54.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 49 - Aplicación del siguiente anexo</i> Pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del presente Anexo.
55.	Introduzca el carácter “E” y pulse “Enter” para aplicar las políticas asociadas al presente anexo: “ANEXO E. Manejo y control de dispositivos”.  <i>Ilustración 50 - Selección del siguiente anexo a aplicar</i>
56.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 51 - Anexo E configurado</i>
57.	No reinicie ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

6.6. 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 11. 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 las guías CCN-STIC y se adaptan a los requisitos de sistemas en distintos niveles de clasificación.

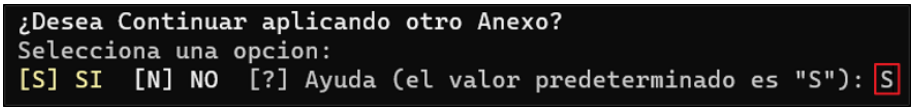
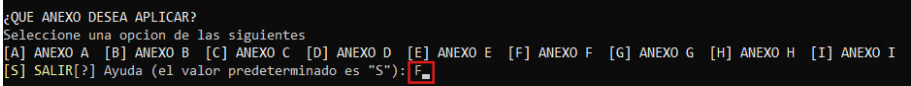
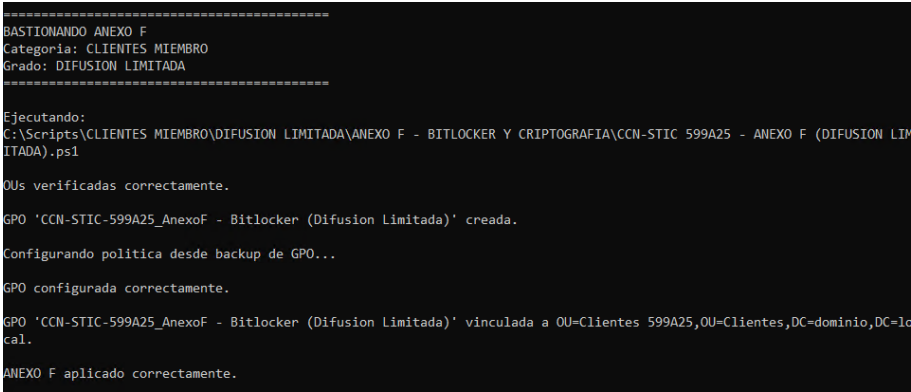
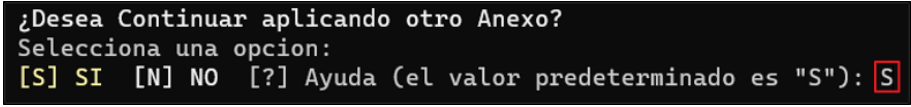
6.6.1. IMPACTO

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

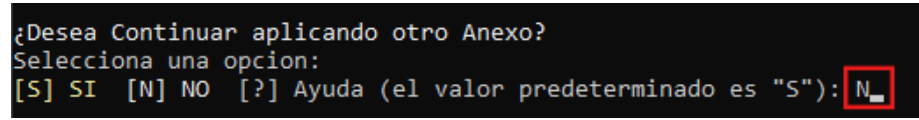
- a) Incremento en el tiempo de arranque y acceso a discos, especialmente en sistemas con hardware limitado o sin aceleración criptográfica.
- b) Incompatibilidad con herramientas de recuperación o mantenimiento si no se gestionan adecuadamente las claves de recuperación de BitLocker.
- c) Restricciones 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.

6.6.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD CRIPTOGRÁFICAS

Paso	Descripción
58.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 52 - Aplicación del siguiente anexo</i> Pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del presente Anexo.
59.	Introduzca el carácter “F” y pulse “Enter” para aplicar las políticas asociadas al presente anexo: “ANEXO F. Configuración de BitLocker y criptografía”.  <i>Ilustración 53 - Selección del siguiente anexo a aplicar</i>
60.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 54 - Anexo F configurado</i>
61.	Si desea continuar aplicando las configuraciones de seguridad adicionales no reinicie el cliente ni cierre la ventana de PowerShell y pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación de los Anexos.  <i>Ilustración 55 - Continuación de siguiente Anexo</i>

- 62.** Si sólo se desea configuración principal, pulse el carácter “N” y a continuación, la tecla “Enter”.



```
¿Desea Continuar aplicando otro Anexo?  
Selecciona una opcion:  
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): N
```

Ilustración 56 - Finalización del script

Nota: Si ya desea terminar con la configuración del script, prosiga al paso número **74**.

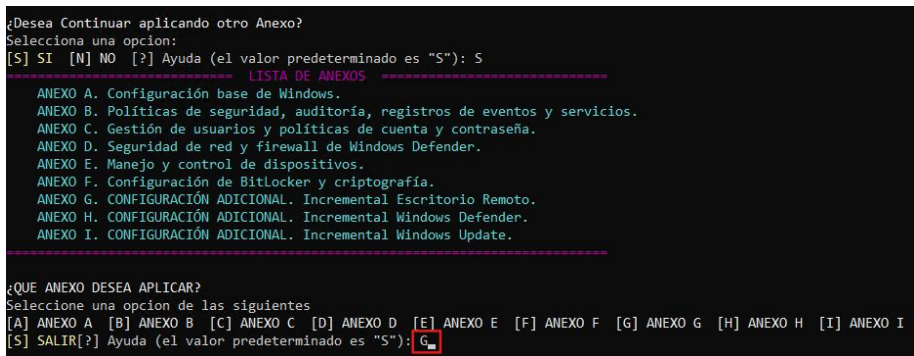
6.7. ANEXO G. ACCESO MEDIANTE ESCRITORIO REMOTO

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: Este 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”.

6.7.1. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN RDP

Paso	Descripción
63.	Mantenga la sesión iniciada en el servidor donde está aplicando la configuración de seguridad, y continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 57 - Aplicación del siguiente anexo</i> Pulse el carácter “G” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del ANEXO G Incremental Escritorio Remoto. Nota: Revise atentamente todas las configuraciones que aplica el presente Anexo.

64. Una vez finalizado el proceso, observará el siguiente mensaje:

```
=====
BASTIONANDO ANEXO - ESCRITORIO REMOTO
Categoría: CLIENTES MIEMBRO
Grado: DIFUSION LIMITADA
=====

Ejecutando:
C:\Scripts\CLIENTES MIEMBRO\CONFIGURACIONES ADICIONALES\ANEXO - ESCRITORIO REMOTO\CCN-STIC 599A25 - ANEXO ESCRITORIO REMOTO.ps1

OUs verificadas correctamente.

GPO 'CCN-STIC-599A25_Anexo Incremental - Escritorio Remoto' creada.

Configurando politica desde backup de GPO...

GPO configurada correctamente.

GPO 'CCN-STIC-599A25_Anexo Incremental - Escritorio Remoto' vinculada a OU=Clientes 599A25,OU=Clientes,DC=dominio,DC=local.

ANEXO ESCRITORIO REMOTO aplicado correctamente.
```

Ilustración 58 - Anexo G configurado

65. Si desea continuar aplicando las configuraciones de seguridad adicionales no reinicie el cliente ni cierre la ventana de PowerShell y pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación de los Anexos.

```
¿Desea Continuar aplicando otro Anexo?
Selecciona una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): S
```

Ilustración 59 - Configuración siguiente anexo

66. Si no desea ninguna otra configuración, pulse el carácter “N” y a continuación, la tecla “Enter”.

```
¿Desea Continuar aplicando otro Anexo?
Selecciona una opcion:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): N
```

Ilustración 60 - Finalización de script

6.8. ANEXO H. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

En esta sección se establecen las directivas necesarias para configurar y reforzar la protección frente a código dañino en los sistemas operativos Windows 11 Miembro de dominio, utilizando las capacidades integradas del software antimalware incluido por defecto. La configuración abarca la detección de aplicaciones potencialmente no deseadas, el uso de mecanismos heurísticos, la supervisión del comportamiento, el análisis de archivos, scripts, procesos y dispositivos extraíbles, así como la protección frente a accesos a sitios web peligrosos.

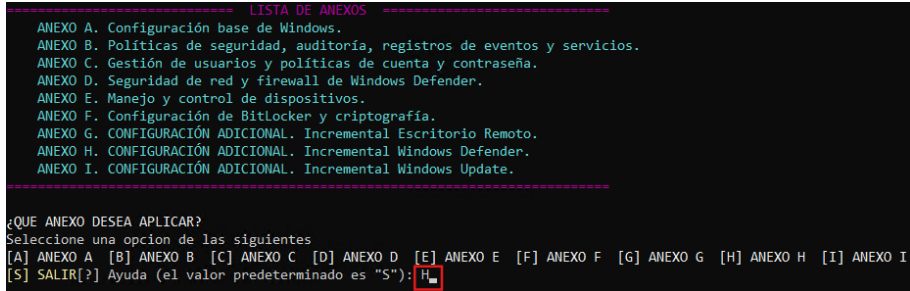
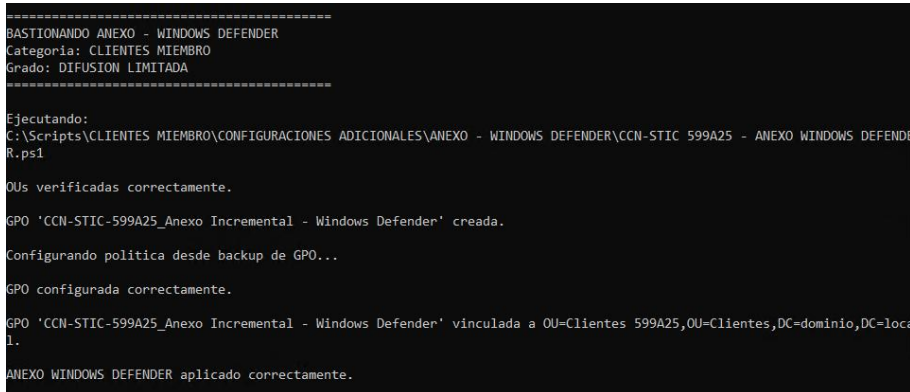
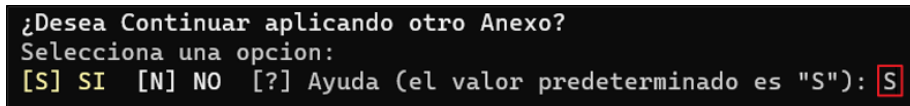
Nota: Si en su organización ya dispone de un producto o servicio frente a código dañino en el sistema operativo, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

6.8.1. IMPACTO

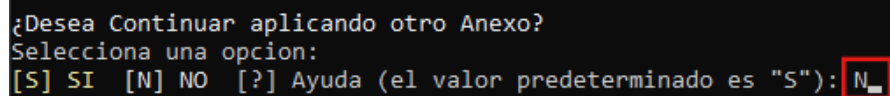
La configuración para la protección frente a código dañino puede impactar de la siguiente manera:

- a) Posibles bloqueos o restricciones de aplicaciones y acciones legítimas, como consecuencia de la detección de aplicaciones potencialmente no deseadas, el acceso controlado a carpetas o las políticas de protección de red y navegación.
- b) Incremento de incidencias relacionadas con falsos positivos, que pueden requerir análisis, ajustes de políticas o autorización explícita de aplicaciones, carpetas o procesos necesarios para la operativa.

6.8.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD

Paso	Descripción
67.	Mantenga la sesión iniciada en el equipo donde está aplicando la configuración de seguridad, y continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 61 - Aplicación del siguiente anexo</i> Pulse el carácter “H” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del ANEXO H Incremental Windows Defender. Nota: Revise atentamente todas las configuraciones que aplica el presente Anexo.
68.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 62 - Configuración Anexo H</i>
69.	Si desea continuar aplicando las configuraciones de seguridad adicionales no reinicie el cliente ni cierre la ventana de PowerShell y pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación de los Anexos.  <i>Ilustración 63 - Configuración de siguiente Anexo</i>

- 70.** Si no desea ninguna otra configuración, pulse el carácter “N” y a continuación, la tecla “Enter”.



```
¿Desea Continuar aplicando otro Anexo?  
Selecciona una opcion:  
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): N
```

Ilustración 64 - Finalización del script

6.9. ANEXO I. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

En el presente anexo se definen las acciones necesarias para dotar a los sistemas operativos Windows 11 Miembro de dominio de un servicio de actualizaciones automáticas centralizado y completamente configurado. Mediante la aplicación de directivas específicas de Windows Update, se controla el comportamiento de las actualizaciones automáticas, la recepción de actualizaciones de calidad, características y compilaciones preliminares, así como la instalación de actualizaciones recomendadas.

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

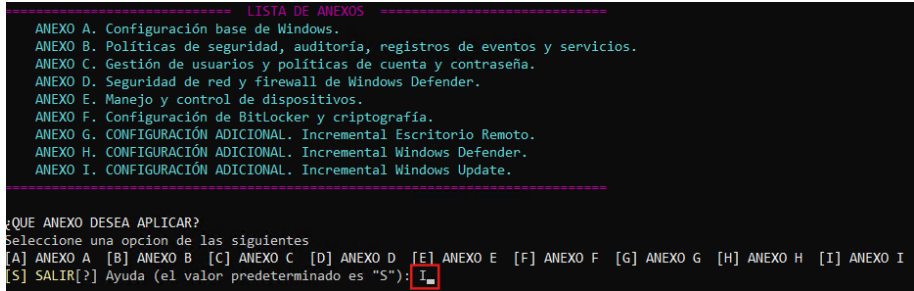
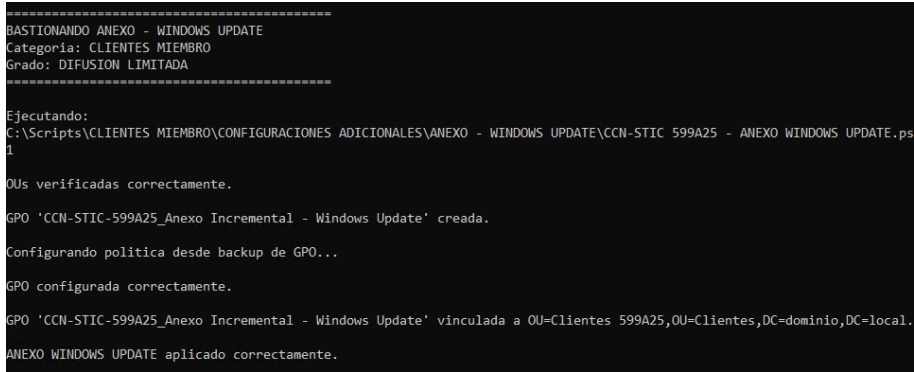
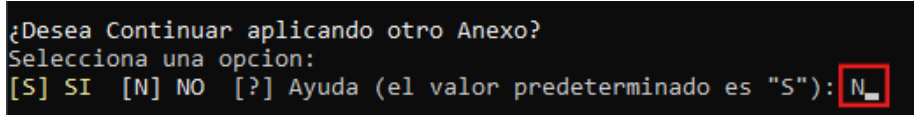
6.9.1. IMPACTO

La aplicación de este servicio puede tener los siguientes efectos en el entorno operativo:

- a) Instalación automática de actualizaciones en los equipos Windows cliente, reduciendo la exposición a vulnerabilidades, pero pudiendo introducir cambios en el sistema sin intervención directa del usuario.
- b) Reinicios necesarios tras determinadas actualizaciones, lo que puede interrumpir sesiones activas, tareas programadas o procesos en ejecución si no se han definido ventanas de mantenimiento adecuadas.
- c) Posibles incompatibilidades con aplicaciones, controladores o componentes corporativos, especialmente tras actualizaciones acumulativas, de características o de drivers.

Incremento puntual de incidencias operativas, derivadas de errores de instalación, equipos pendientes de reinicio, fallos de compatibilidad o usuarios afectados por cambios introducidos tras la actualización.

6.9.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD

Paso	Descripción
71.	Mantenga la sesión iniciada en el equipo donde está aplicando la configuración de seguridad, y continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 65 - Aplicación del siguiente anexo</i> Pulse el carácter “I” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del ANEXO I Incremental Windows Update. Nota: Revise atentamente todas las configuraciones que aplica el presente Anexo.
72.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 66 - Configuración Anexo I</i>
73.	Finalmente, pulse el carácter “N” y a continuación, la tecla “Enter”. Después de la realización de estas configuraciones, el dominio quedará preparado para administrar las configuraciones de seguridad.  <i>Ilustración 67 - Finalización del script</i>
74.	A continuación, restablezca la configuración de la ejecución de scripts en los servidores.

- 75.** En el “Administrador del servidor” del controlador de dominio, haga clic en “Herramientas” en la barra superior y seleccione “Administración de directivas de grupo”.

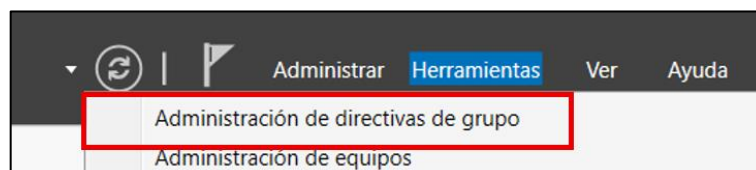


Ilustración 68 - Administración de directivas de grupo

- 76.** Despliegue el panel izquierdo hasta llegar a la OU “Domain Controllers”.

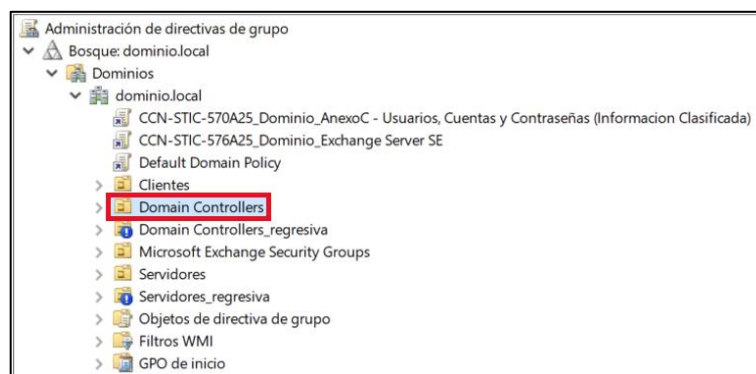


Ilustración 69 - Unidad organizativa de Domain Controllers

- 77.** Despliegue dicha OU, haga clic derecho sobre la GPO “CCN-STIC-570A25_DC_AnexoA – ADMX (Nivel de Clasificación)”, y seleccione “Editar”.

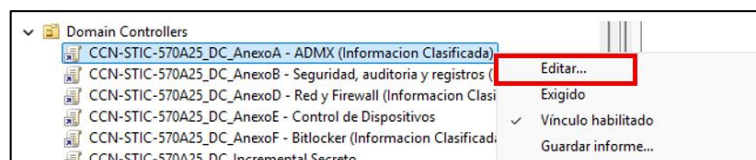


Ilustración 70 - Edición de directiva de grupo

- 78.** En el panel izquierdo, despliegue la lista siguiendo la siguiente ruta: “Configuración del Equipo > Plantillas administrativas > Componentes de Windows > Windows PowerShell”. Haga clic sobre “Windows PowerShell” para ver las políticas que aplica

Configuración	Estado	Comentario
Activar registro de módulos	Habilitada	No
Activar el registro de bloque de script de PowerShell	Habilitada	No
Activar la ejecución de scripts	Habilitada	No
Activar la transcripción de PowerShell	Habilitada	No
Establecer la ruta de acceso de origen de Update-Help	No configurada	No

Ilustración 71 - Modificación de la ejecución de scripts

- 79.** Haga doble clic sobre la política “Activar la ejecución de scripts”.

80. En el desplegable de la política, seleccione “Permitir solo scripts firmados”.

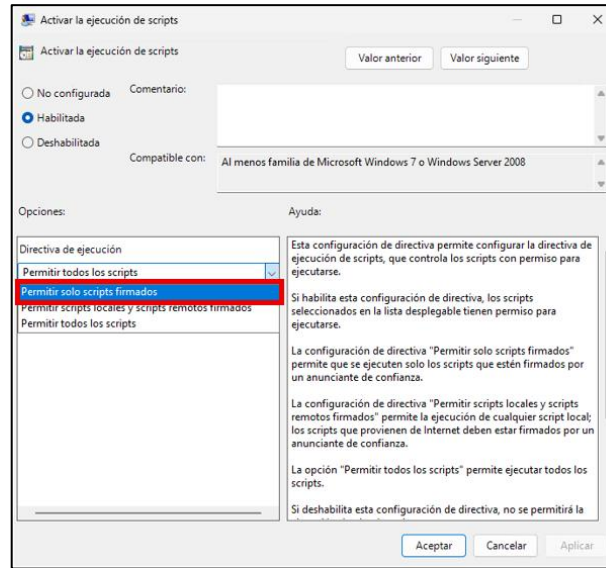


Ilustración 72 - Bloqueo de scripts no firmados

81. A continuación, pulse en “Aplicar” y “Aceptar”.

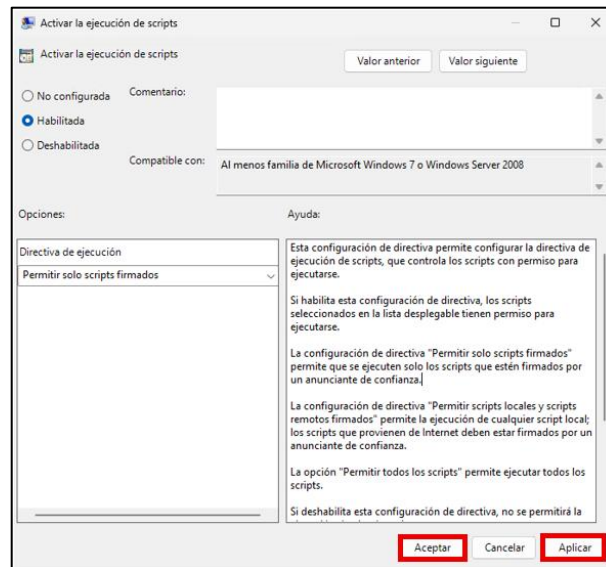
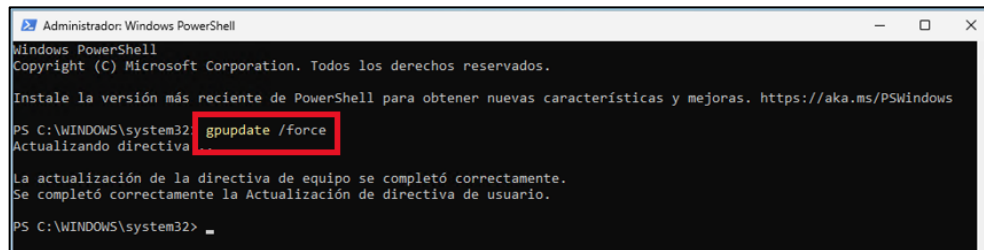


Ilustración 73 - Aplicación de la configuración

- 82.** A continuación, ejecute el comando “gpupdate /force” en el controlador de dominio y proceda a su reinicio.



```

Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\WINDOWS\system32> gpupdate /force
Actualizando directiva...
La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.
PS C:\WINDOWS\system32>
  
```

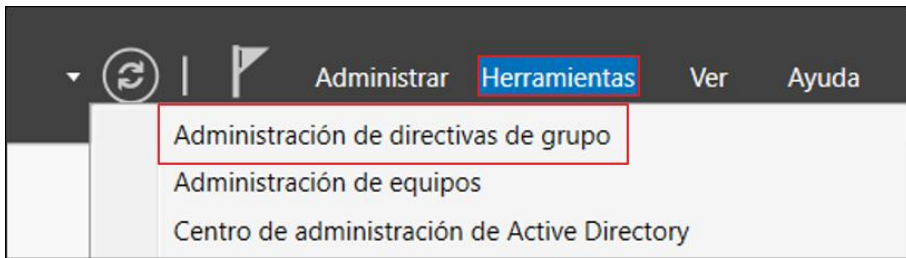
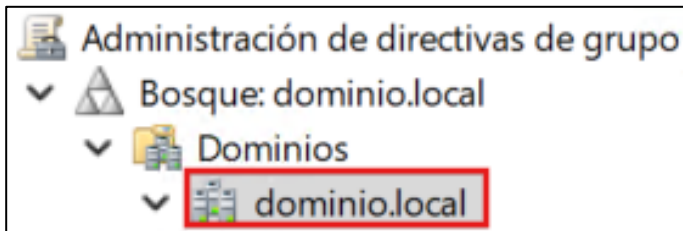
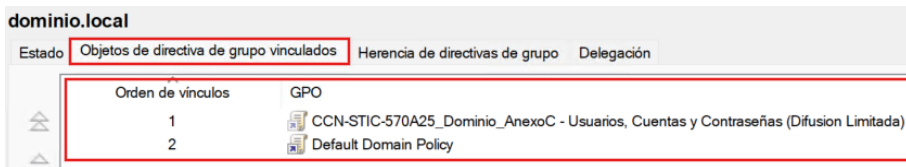
Ilustración 74 - Actualización de directivas

6.10. CONFIGURACIONES MANUALES Y COMPROBACIONES

6.10.1. 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 se confirmará la prioridad de las directivas importadas.
2.	Desde el “Administrador del servidor”, seleccione Herramientas > Administración de directivas de grupo.  <i>Ilustración 75 - Acceso a la administración de GPOs</i>
3.	Despliegue su dominio y seleccione la raíz, en el caso del ejemplo su nombre es “dominio.local”.  <i>Ilustración 76 - Selección del dominio</i>
4.	A continuación, a la derecha, seleccione “Objetos de directiva de grupo vinculados”. El orden de los vínculos debe ser el siguiente:  <i>Ilustración 77 - Orden de GPOs vinculados al dominio</i>

5. Seleccione nombre.dominio > Clientes > Clientes 599A25 con clic izquierdo.

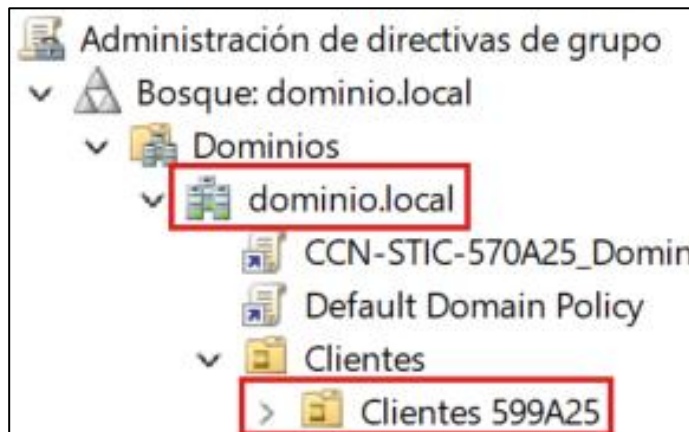


Ilustración 78 - Selección de la unidad organizativa de Clientes 599A25

6. A continuación, a la derecha, seleccione “Objetos de directiva de grupo vinculados”. El orden de los vínculos debe ser el siguiente:

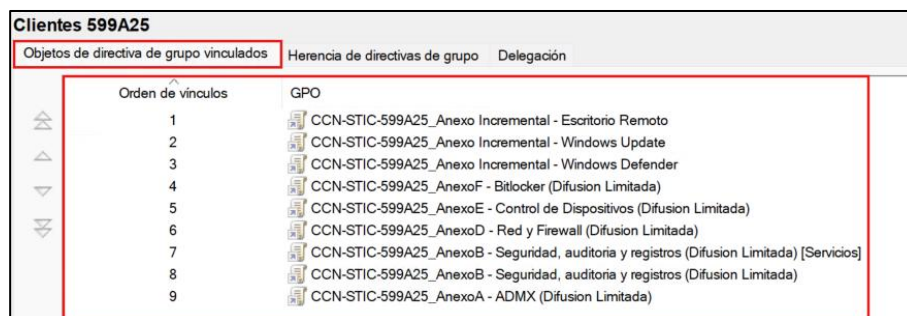


Ilustración 79 - Orden de GPOs vinculados a Clientes 599A25

7. 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”.

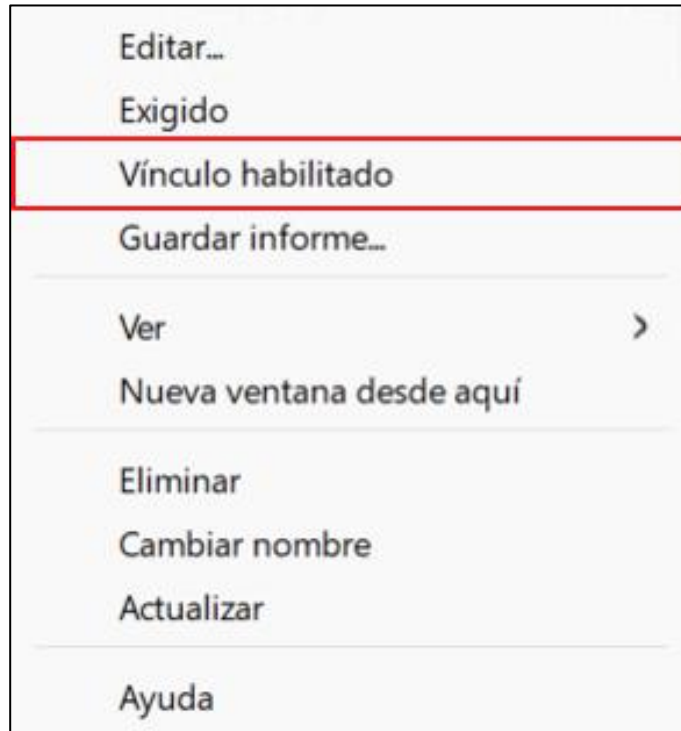


Ilustración 80 - Habilitación del vínculo de los GPOs

8. Una vez habilite todas las directivas de la unidad organizativa y la directiva correspondiente al “Anexo C” a nivel de dominio, deberá mover el equipo cliente a la OU correspondiente.

9. De nuevo en el “Administrador del servidor” del controlador de dominio, haga clic en “Herramientas” en la barra superior, y seleccione “Usuarios y equipos de Active Directory”.



Ilustración 81 - Usuarios y equipos de Active Directory

- 10.** Arrastre hasta la unidad organizativa de “Clientes 599A25” los equipos donde desea aplicar la seguridad:

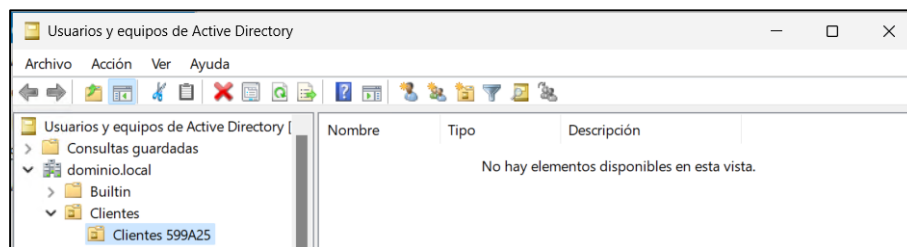


Ilustración 82 - Unidad organizativa Clientes 599A25

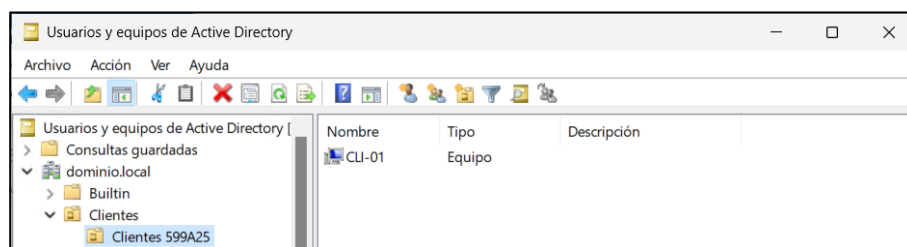


Ilustración 83 - Movimiento del objeto de máquina a la OU

Nota: Haga click sobre el botón “Sí” para confirmar el movimiento del objeto de directorio activo.

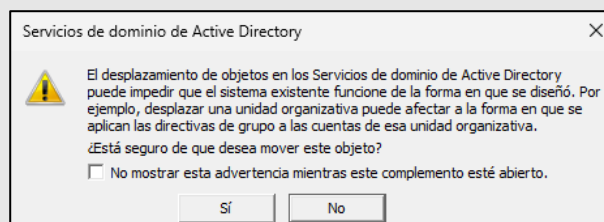


Ilustración 84 - Aceptar el desplazamiento de objetos

- 11.** Inicie sesión en el equipo que se acaba de reubicar.

12. Para una correcta aplicación, ejecute la Consola de Comandos del sistema en modo Administrador.

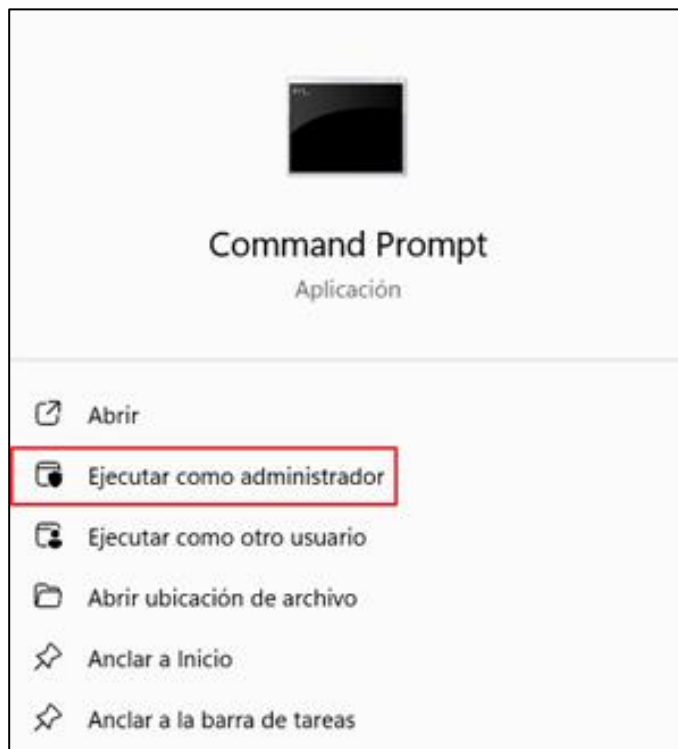


Ilustración 85 - Ejecución como administrador de CMD

13. Ejecute el comando `gpupdate /force`. Tras finalizar, observará el siguiente mensaje:

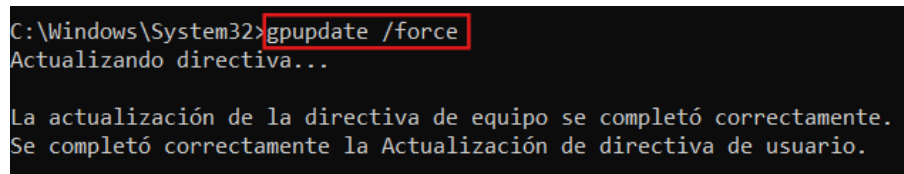
The image shows a Windows Command Prompt window with a black background and white text. The command prompt shows the path 'C:\Windows\System32>' followed by the command 'gpupdate /force', which is highlighted with a red rectangular box. Below the command, the text 'Actualizando directiva...' is displayed. Further down, the output message reads: 'La actualización de la directiva de equipo se completó correctamente. Se completó correctamente la Actualización de directiva de usuario.'

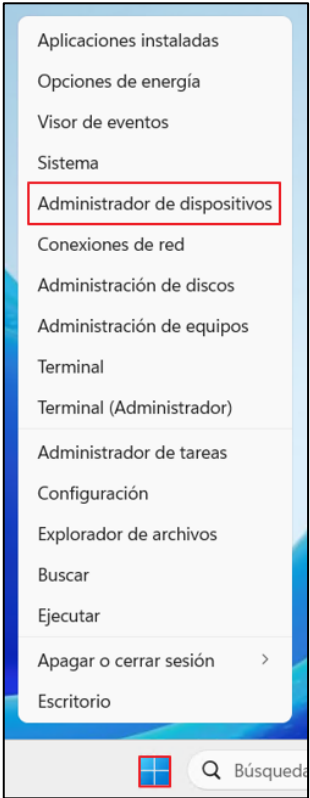
Ilustración 86 - Ejecución de `gpupdate /force`

Una vez completada la actualización de directivas de equipo y usuario, debe reiniciarse el equipo manualmente.

6.10.2. ADMINISTRACIÓN Y CONTROL DE NUEVOS DISPOSITIVOS EXTRAÍBLES

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

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

Paso	Descripción
1.	Inicie sesión en el cliente donde se pretende habilitar el uso de un dispositivo USB.
2.	Haga clic derecho sobre el botón de inicio, y sobre “Administrador de dispositivos”:  <i>Ilustración 87 - Ejecución del Administrador de dispositivos</i>

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”.

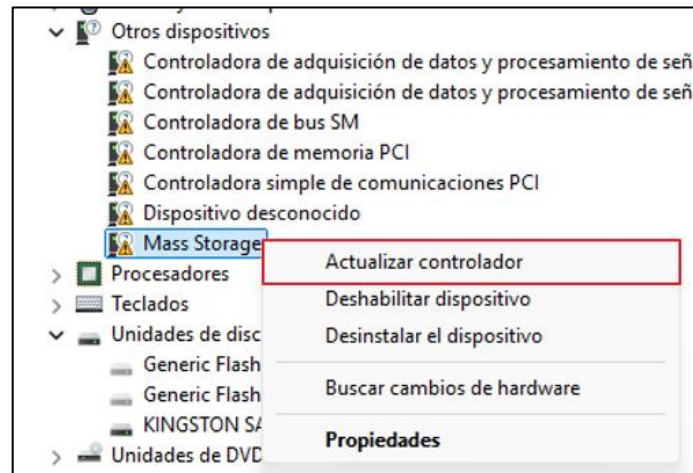


Ilustración 88 - Selección del dispositivo

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”.

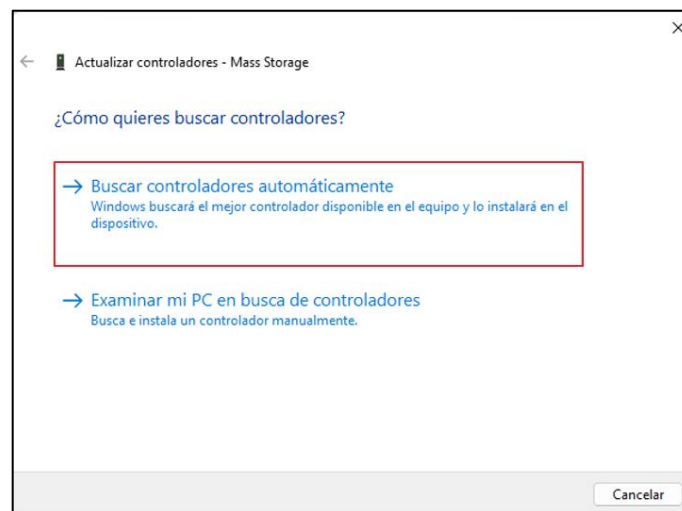


Ilustración 89 - Búsqueda automática de controladores

5. Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.

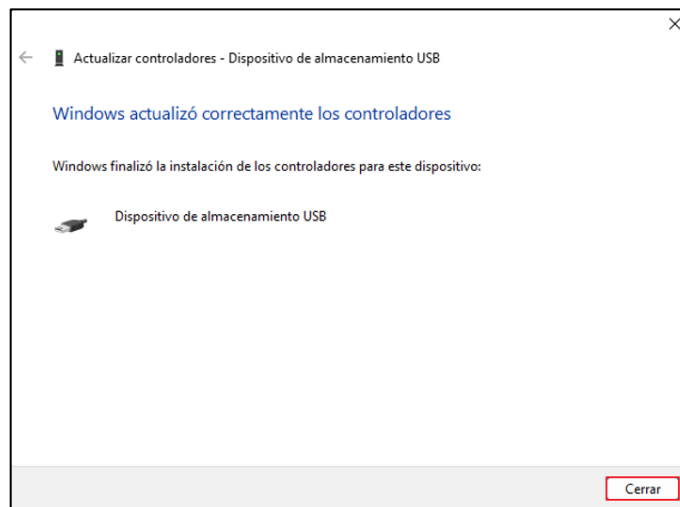


Ilustración 90 - Finalización de la actualización de controladores

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 91 - Unidad de disco nueva

6.10.2.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

Los pasos definidos a continuación deberán ser realizados tanto sobre el cliente 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”:

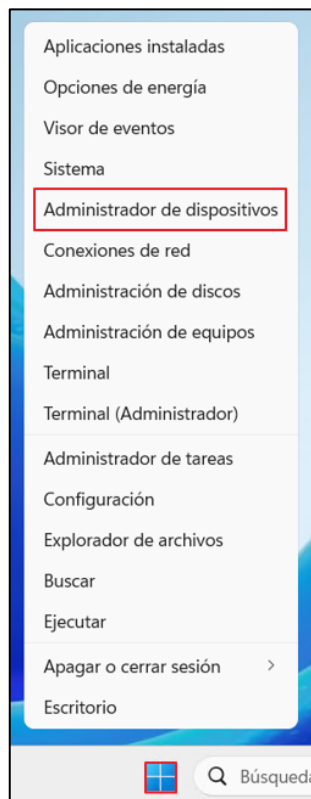


Ilustración 92 - Ejecución del Administrador de dispositivos

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”.

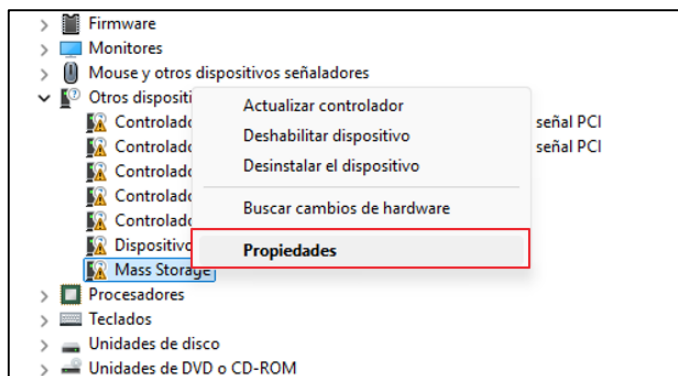


Ilustración 93 - Propiedades del dispositivo

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 anótelolo para poder utilizarlo más adelante.

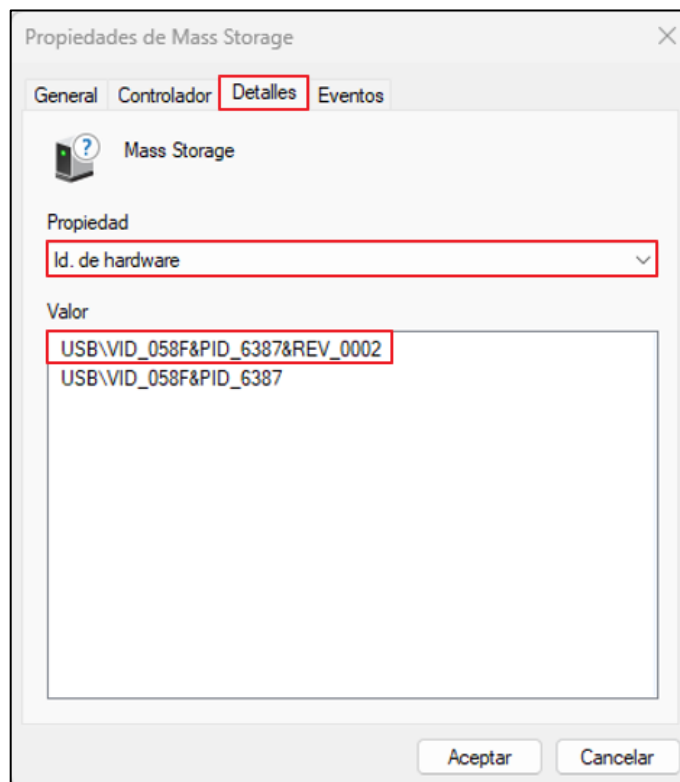


Ilustración 94 - Detalles del dispositivo

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.

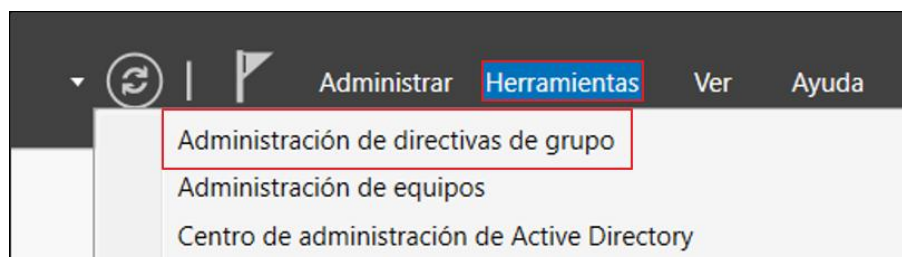


Ilustración 95 - Acceso a la administración de GPOs

6. Despliegue la raíz del dominio, y después despliegue “Objetos de directiva de grupo”.

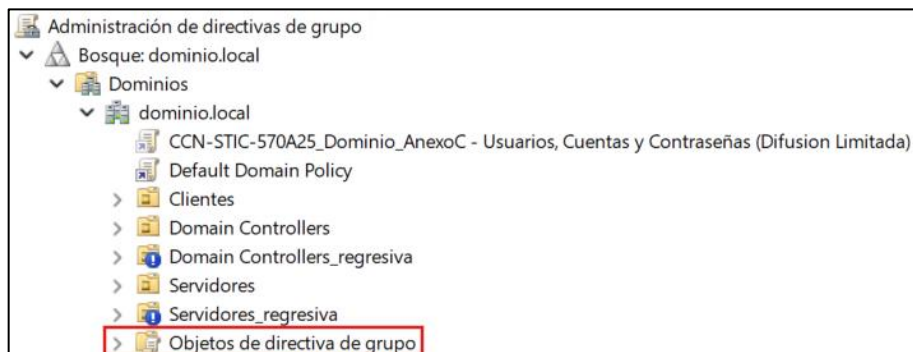


Ilustración 96 - Despliegue de los objetos de directiva de grupo

7. Haga clic derecho sobre el GPO “CCN-STIC-599A25_AnexoE – Control de dispositivos”, y seleccione la opción “Editar” en el menú contextual.

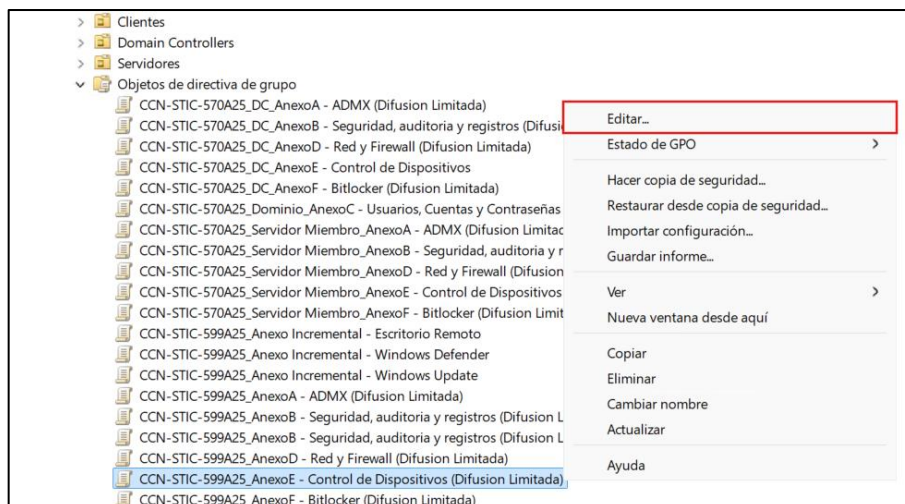


Ilustración 97 - Edición del GPO

8. Despliegue el nodo “Configuración del equipo > Plantillas administrativas > Sistema > Instalación de dispositivos > Restricciones de instalación de dispositivos”.

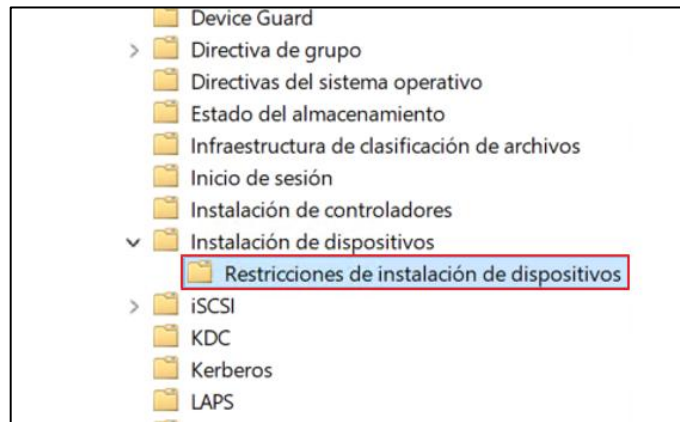


Ilustración 98 - Despliegue del nodo de restricciones de instalación de dispositivos

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”.

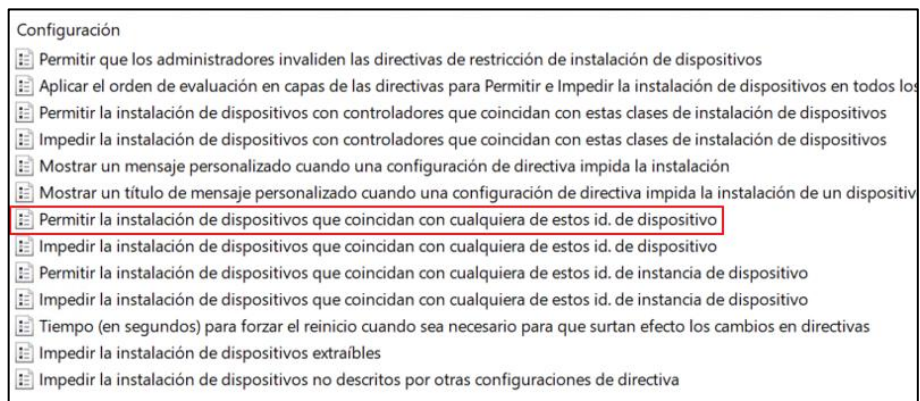


Ilustración 99 - Edición de la política

Hacer clic en “Mostrar...”:

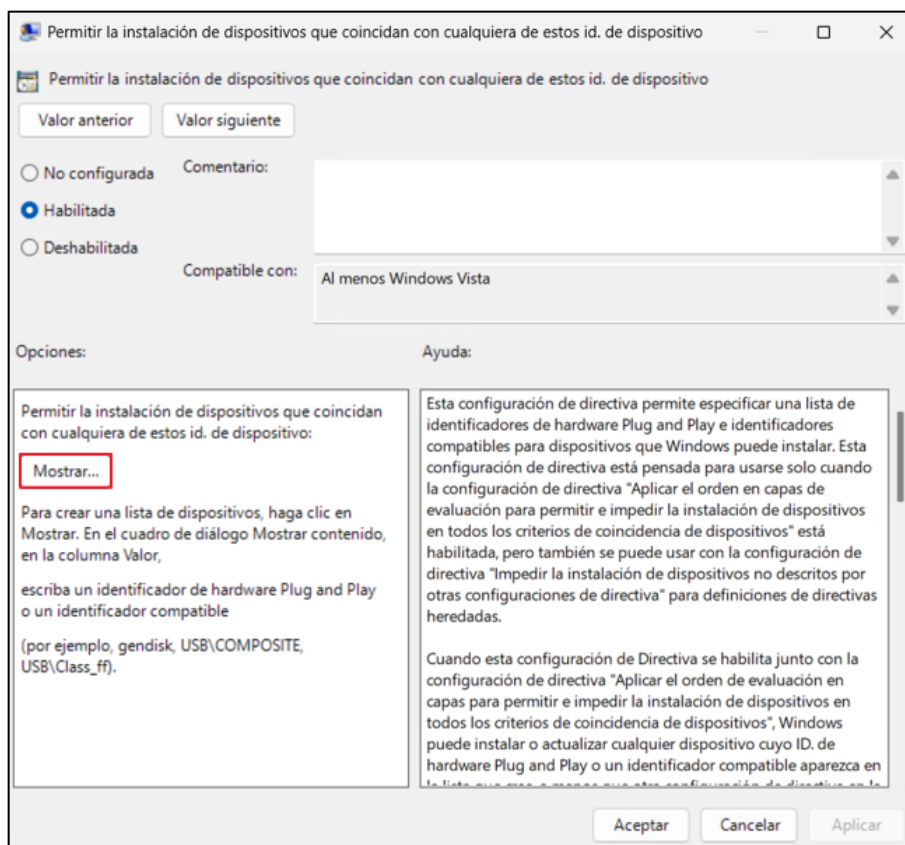


Ilustración 100 - Configuración de la política

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”.

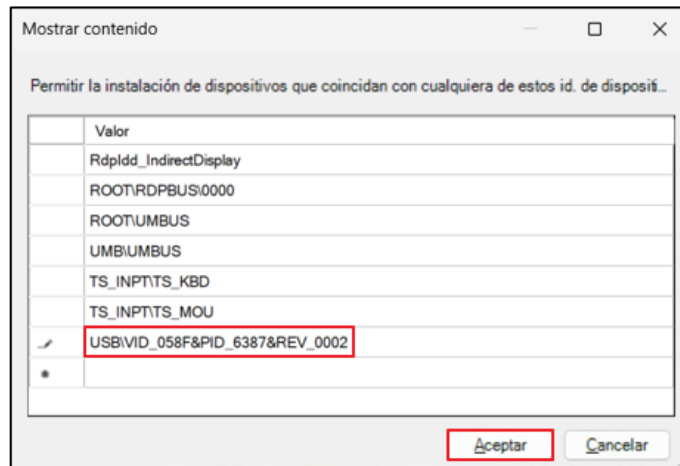


Ilustración 101 - Adición del id. de hardware del dispositivo

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”.

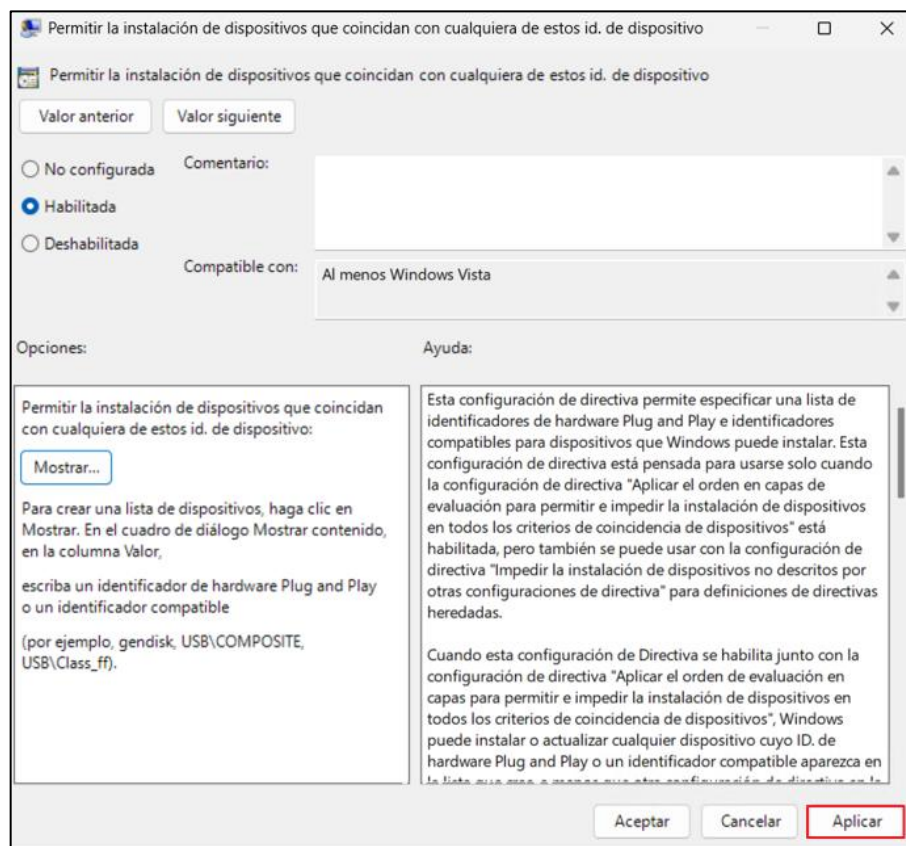


Ilustración 102 - Finalización de la configuración de la política

- 12.** Sin cerrar el “Editor de directivas de grupo local”, continúe con el siguiente paso.
- 13.** Inicie sesión en el cliente donde se pretende habilitar el uso de un dispositivo USB.

- 14.** Ejecute la Consola de Comandos del sistema en modo Administrador.

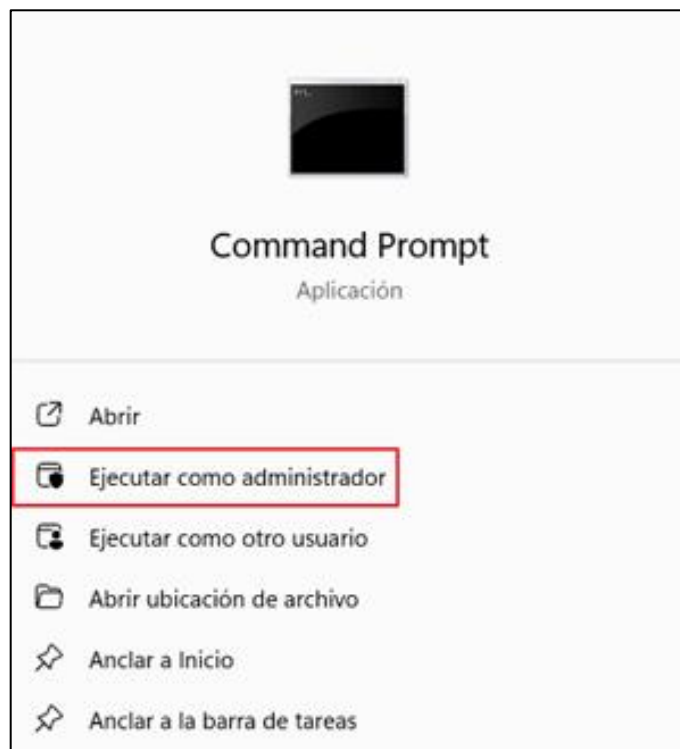


Ilustración 103 - Ejecución como administrador de CMD

- 15.** Ejecute el comando `gpupdate /force`. Tras finalizar, observará el siguiente mensaje:

```
C:\Windows\System32>gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.
```

Ilustración 104 - 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.

6.10.2.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

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

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

18. Haga clic derecho sobre el botón de inicio, y sobre “Administrador de dispositivos”:

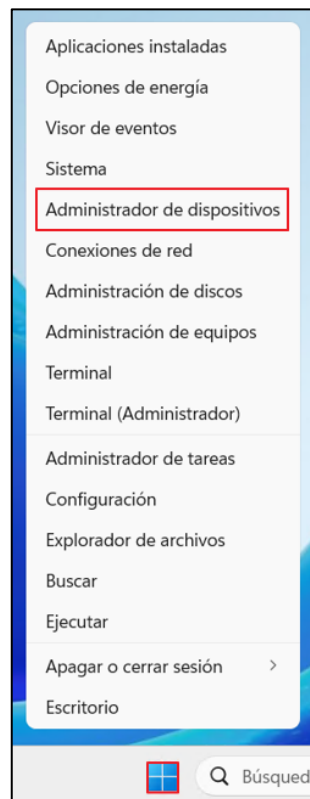


Ilustración 105 - Ejecución del Administrador de dispositivos

19. Seleccione la pestaña “Ver” y haga clic en la opción “Mostrar dispositivos ocultos”.

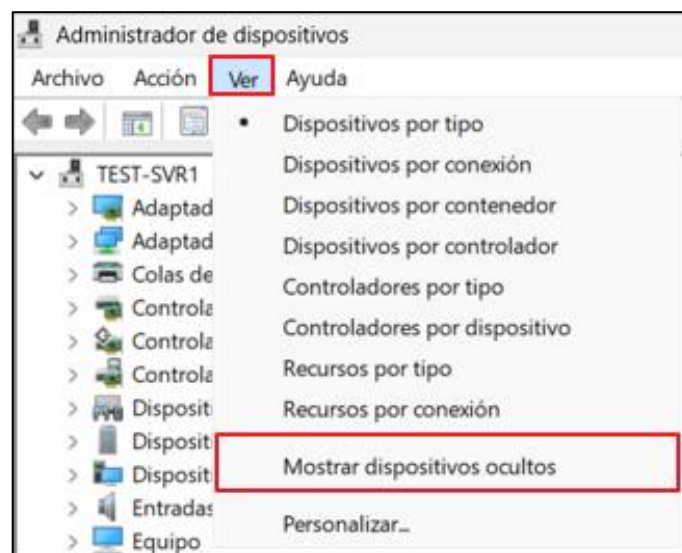


Ilustración 106 – Mostrar dispositivos ocultos

20. 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 107 - Desinstalación del dispositiv

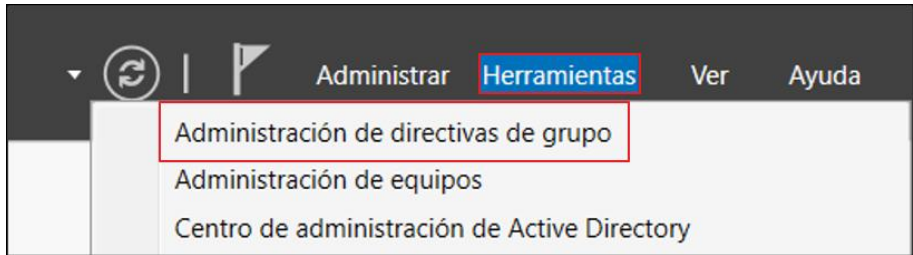
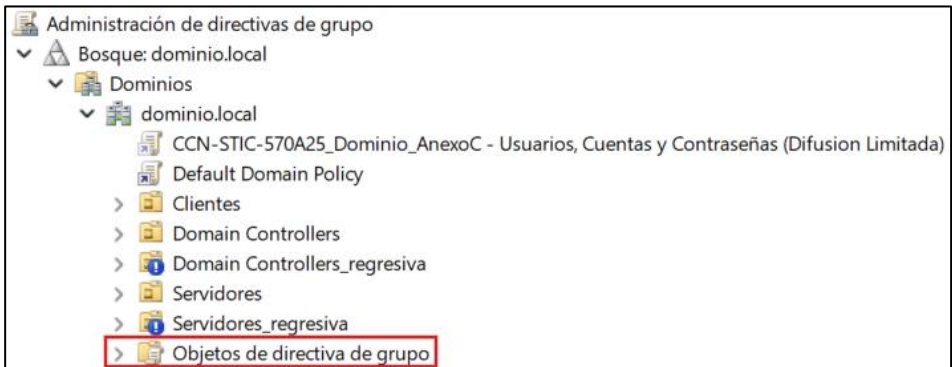
21. Haga clic sobre “Desinstalar” en la ventana emergente.



Ilustración 108 - Confirmación de la desinstalación

Nota: Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

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

Paso	Descripción
22.	Inicie sesión en un servidor con el rol de Controlador de Dominio del dominio en el que quiere configurarse el control de dispositivos.
23.	Desde el “Administrador del servidor”, seleccione Herramientas > Administración de directivas de grupo.  <i>Ilustración 109 - Acceso a la administración de GPOs</i>
24.	Despliegue la raíz del dominio, y después despliegue “Objetos de directiva de grupo”.  <i>Ilustración 110 - Despliegue de los objetos de directiva de grupo</i>

- 25.** Haga clic derecho sobre el GPO “CCN-STIC-599A25_AnexoE – Control de dispositivos”, y seleccione la opción “Editar” en el menú contextual.

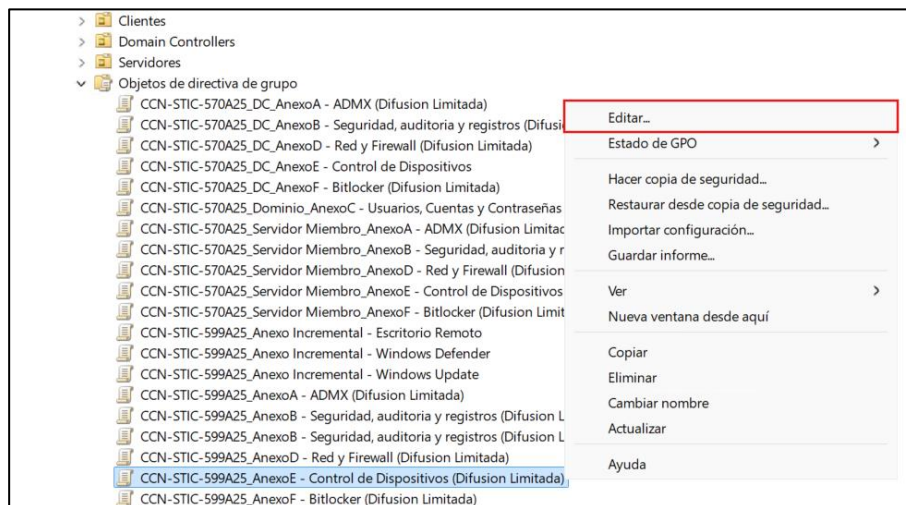


Ilustración 111 - Edición del GPO

- 26.** Despliegue el nodo “Configuración del equipo > Plantillas administrativas > Sistema > Instalación de dispositivos > Restricciones de instalación de dispositivos”.

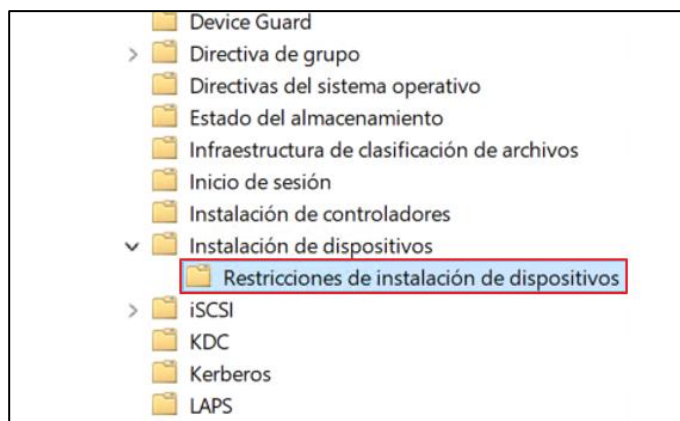


Ilustración 112 - Despliegue del nodo de restricciones de instalación de dispositivos

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

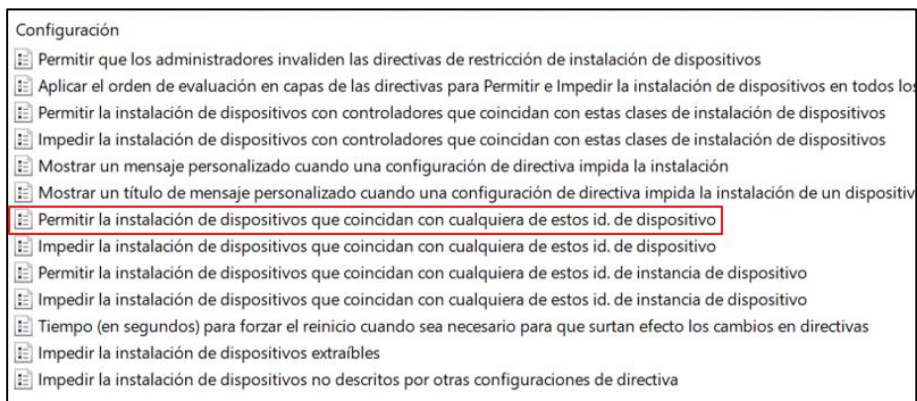


Ilustración 113 - Edición de la política

- 28.** Hacer clic en “Mostrar...”:

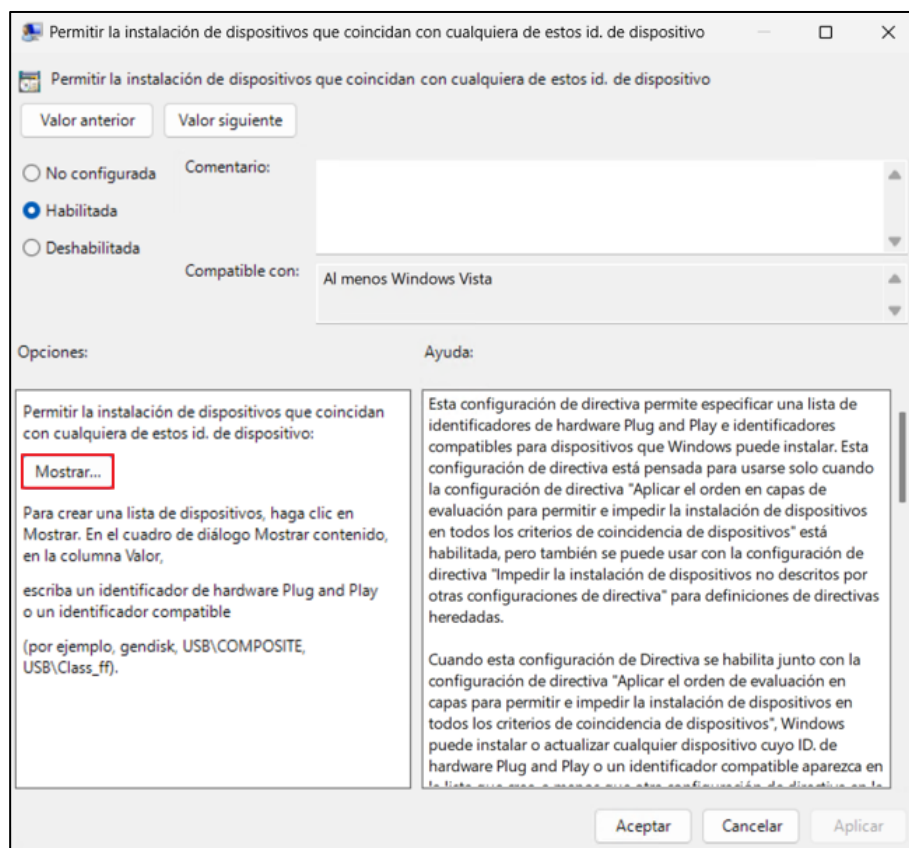


Ilustración 114 - Configuración de la política

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

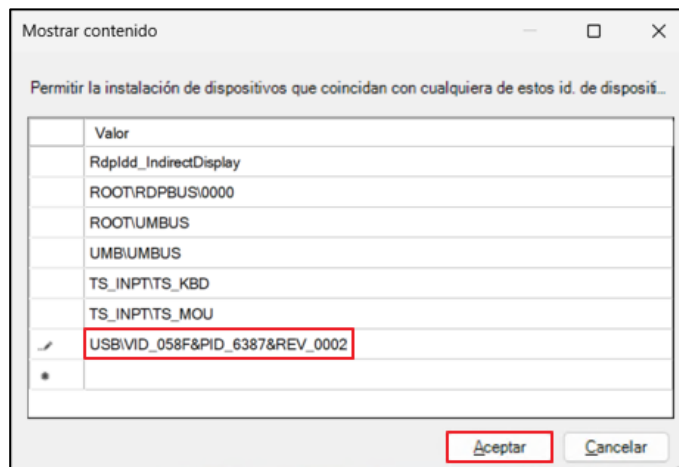


Ilustración 115 - Eliminación del id. de hardware del dispositivo

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

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

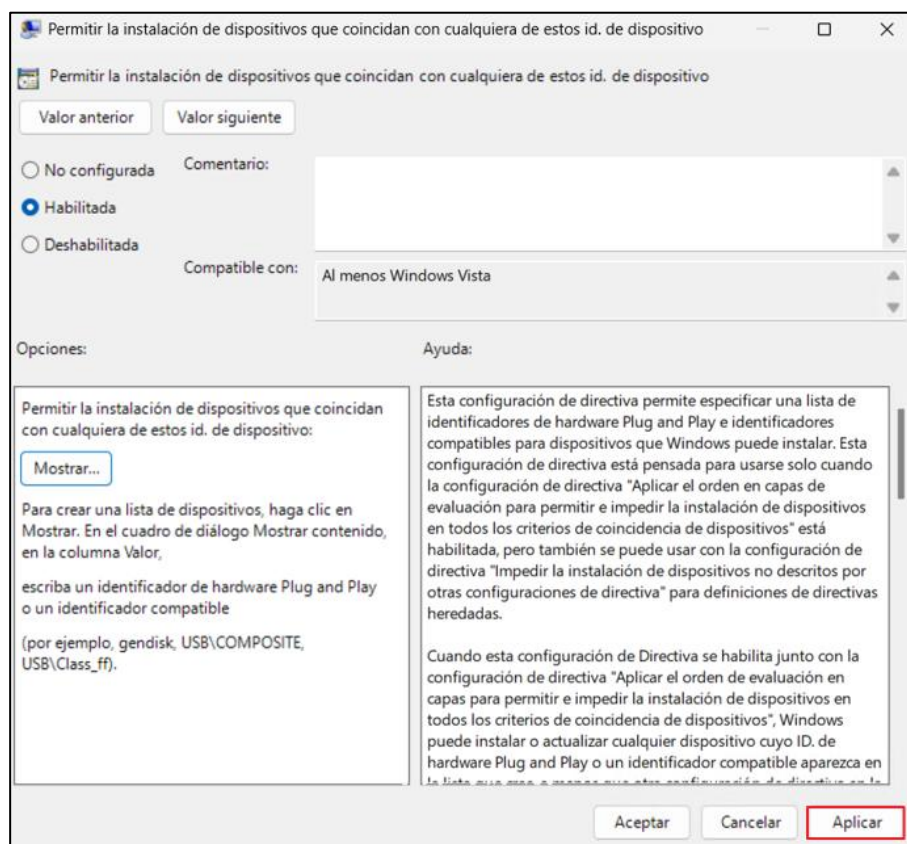
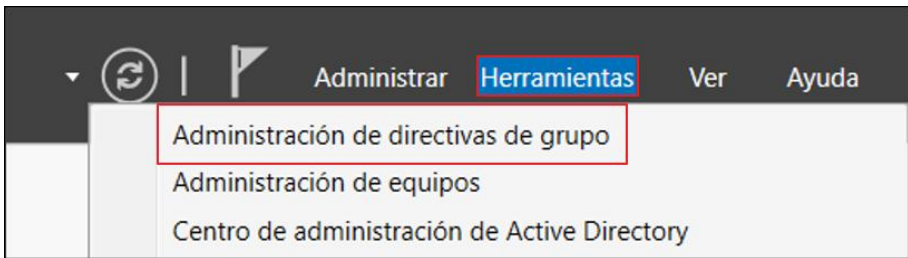
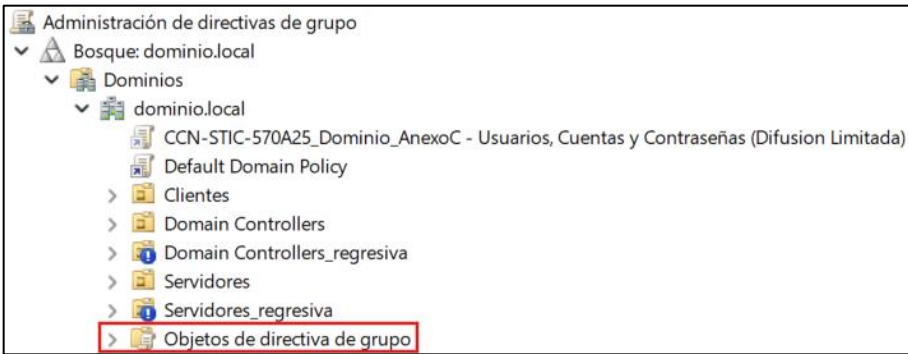


Ilustración 116 - Finalización de la configuración de la política

6.10.3. 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 los equipos cliente de Windows, 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
31.	Inicie sesión en un servidor con el rol de Controlador de Dominio del dominio en el que quiere configurarse el mensaje de inicio de sesión.
32.	Desde el “Administrador del servidor”, seleccione Herramientas > Administración de directivas de grupo.  <i>Ilustración 117 - Acceso a la administración de GPOs</i>
33.	Despliegue la raíz del dominio, y después despliegue “Objetos de directiva de grupo”.  <i>Ilustración 118 - Despliegue de los objetos de directiva de grupo</i>

- 34.** Haga clic derecho sobre el GPO “CCN-STIC-599A25_AnexoB – Seguridad, auditoría y registros (Difusión Limitada)”, y seleccione la opción “Editar” en el menú contextual.

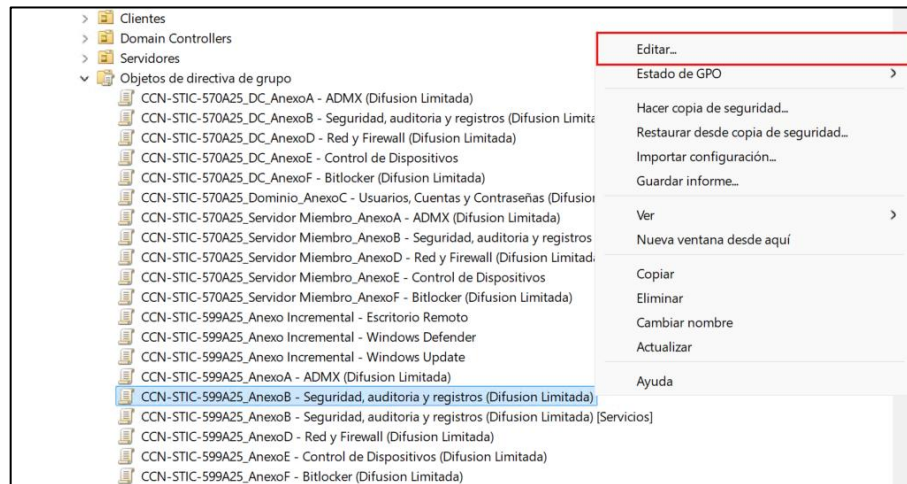


Ilustración 119 - Edición del GPO

- 35.** Despliegue el nodo “Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad”.

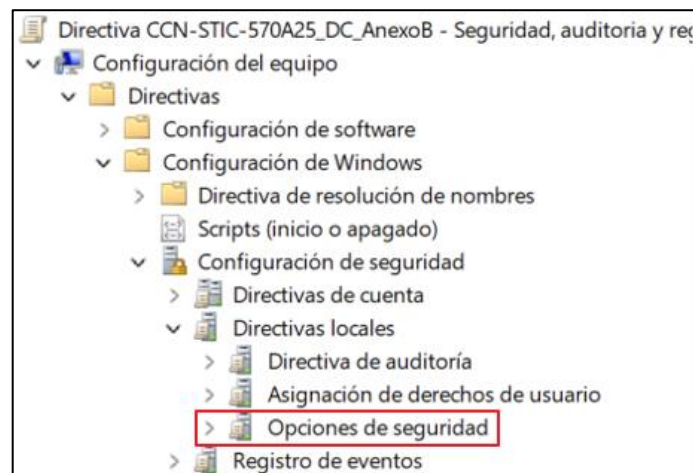


Ilustración 120 – Despliegue del nodo de opciones de seguridad

- 36.** 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.

Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear L...	Habilitada
Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	No está definido
Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión	Está usted accediendo a un equi...
Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión	AVISO IMPORTANTE DE SEGURID...
Inicio de sesión interactivo: umbral de bloqueo de cuenta del equipo	No está definido
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada

Ilustración 121 - GPOs de texto y título de mensaje

- 37.** Texto del mensaje:

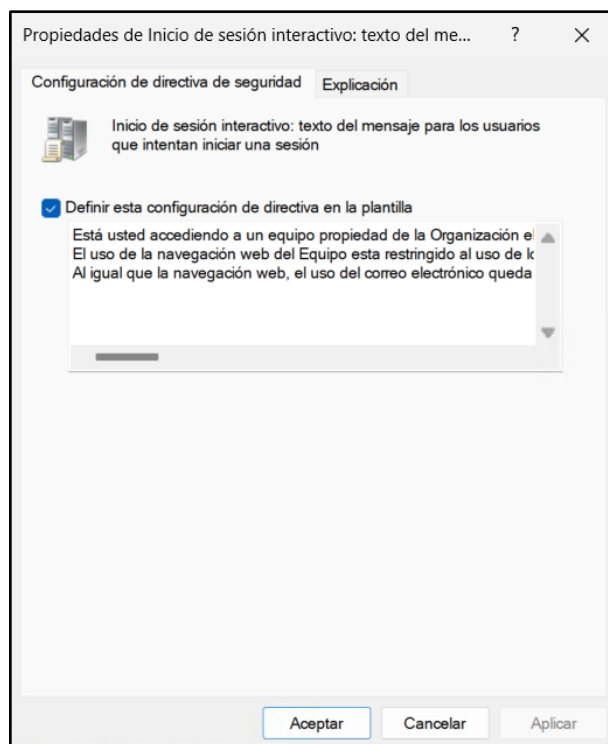
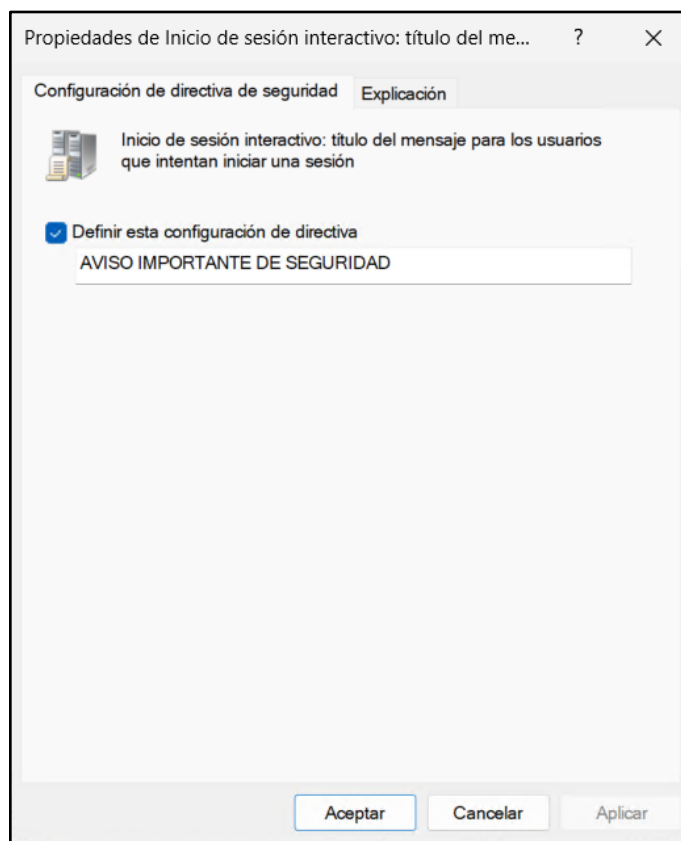
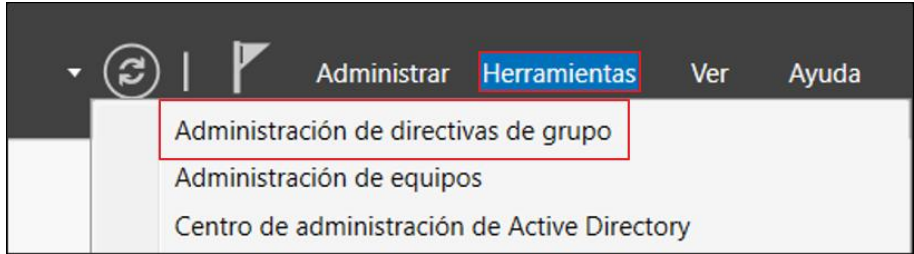
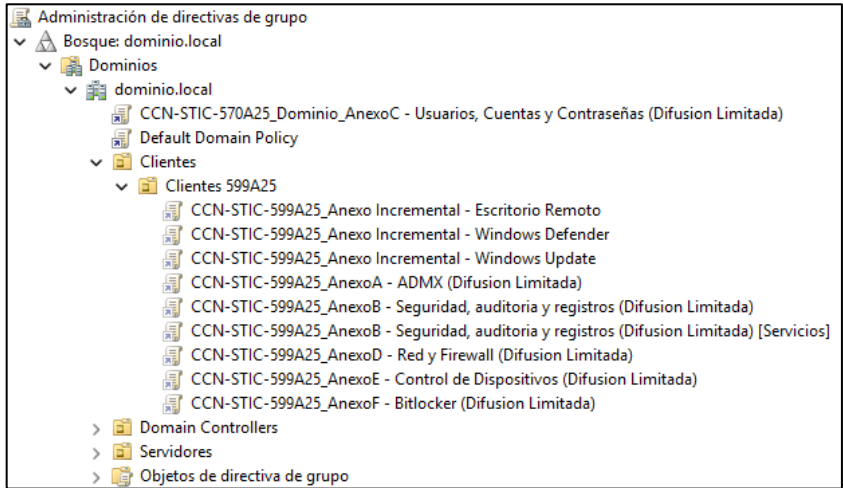


Ilustración 122 - Texto del mensaje

38. Título del mensaje:*Ilustración 123 - Título del mensaje***6.10.4. 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 la unidad organizativa (OU) correspondiente 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.  <i>Ilustración 124 - Acceso a la administración de GPOs</i>
3.	Despliegue la raíz del dominio, las GPO deben estar asociadas en base al siguiente esquema:  <i>Ilustración 125 - Listado completo de GPOs creadas</i> 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.

7. OPCIÓN B. EQUIPO WINDOWS 11 INDEPENDIENTE

7.1. 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.

El presente apartado contempla la aplicación de medidas de seguridad sobre **equipos cliente independientes**.

Nota: Los scripts asociados al presente apartado, 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.

7.1.1. CARACTERÍSTICAS DE WINDOWS

El presente anexo recoge las configuraciones iniciales necesarias para establecer una base segura en sistemas Windows 11. 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 11.

7.1.1.1. IMPACTO

La desactivación de características del sistema operativo que no son necesarias para el rol específico del cliente independiente 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, 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) Imposibilidad de que nuevas cuentas de usuario reciban determinadas aplicaciones aprovisionadas, al haber sido eliminadas de la imagen del sistema.
- d) Necesidad de revisión previa de los requisitos funcionales del sistema, de las aplicaciones desplegadas y de los perfiles de usuario existentes, 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.

7.1.2. PLANTILLAS ADMINISTRATIVAS

7.1.2.1. 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.

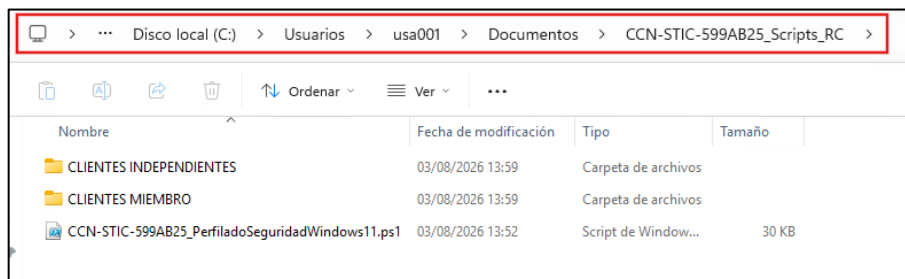
Nota: Se recomienda validar las plantillas en un entorno de pruebas antes de su despliegue en producción, y documentar cualquier excepción necesaria para garantizar la operatividad del sistema.

7.1.3. APLICACIÓN DE MEDIDAS DE SEGURIDAD BASE

Paso	Descripción
1.	Inicie sesión en un cliente independiente del entorno donde se va a aplicar seguridad. Debe iniciar sesión con una cuenta que sea Administrador.
2.	Copie los ficheros y directorios que acompañan a esta guía, al directorio en la carpeta "Documentos" del usuario administrador. A continuación, descomprima la carpeta.

3. Verifique que en su interior se encuentran los siguientes archivos:

- CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
- Directorio: CLIENTES INDEPENDIENTES.
- Directorio: CLIENTES MIEMBRO.

*Ilustración 126 - Ruta de script*

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

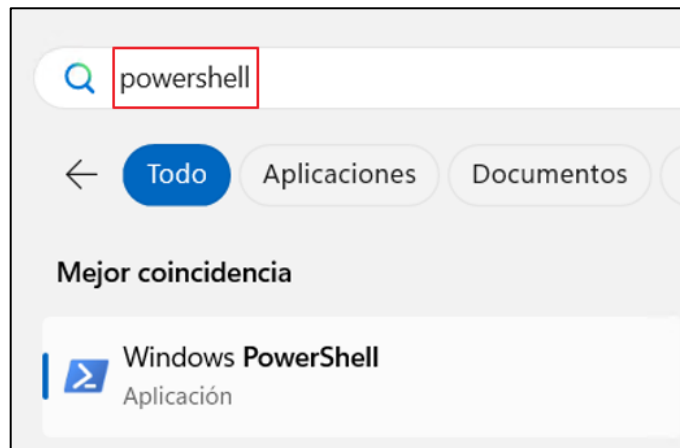


Ilustración 127 - Búsqueda de Powershell

A continuación, seleccione “Ejecutar como administrador”.

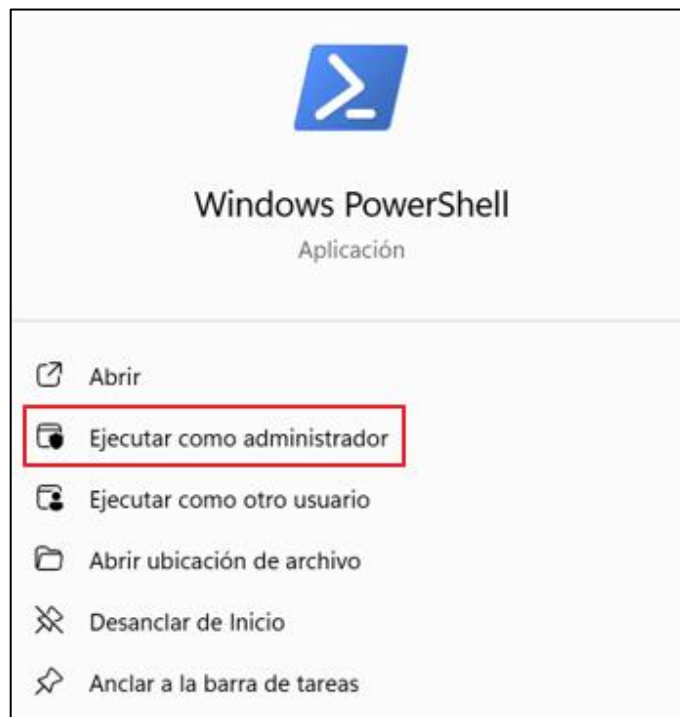
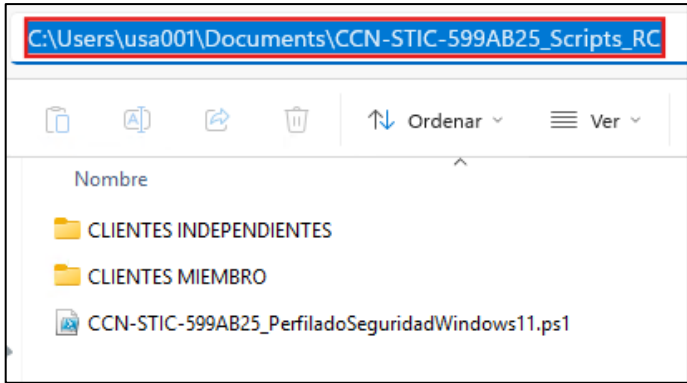


Ilustración 128 - Ejecución como administrador de PowerShell

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.

5.	En la consola de comandos de Powershell, ejecute la sentencia “Get-ExecutionPolicy”: <pre>PS C:\WINDOWS\system32> Get-ExecutionPolicy Restricted PS C:\WINDOWS\system32> _</pre> <i>Ilustración 129 - Ejecución de Get-ExecutionPolicy</i>
6.	Si el resultado muestra un valor diferente a “Unrestricted”, deberá ejecutar el siguiente comando para permitir la ejecución de scripts: “Set-ExecutionPolicy Unrestricted”. <pre>PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted Cambio de directiva de ejecución La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución? [S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): _</pre> <i>Ilustración 130 - Ejecución de Set-ExecutionPolicy</i>
7.	A continuación, pulse la tecla “O” y posteriormente, la tecla “enter” para confirmar: <pre>PS C:\WINDOWS\system32> Set-ExecutionPolicy Unrestricted Cambio de directiva de ejecución La directiva de ejecución te ayuda a protegerte de scripts en los que no confías. Si cambias dicha directiva, podrías exponerte a los riesgos de seguridad descritos en el tema de la Ayuda about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170. ¿Quieres cambiar la directiva de ejecución? [S] Sí [O] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda (el valor predeterminado es "N"): O PS C:\WINDOWS\system32> _</pre> <i>Ilustración 131 - Confirmación de cambio de directiva de ejecución</i>
8.	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”.  <i>Ilustración 132 - Copia de la ruta</i>
9.	Desde la ventana de PowerShell, utilizando el comando “cd”, acceda a la ruta recientemente copiada. <pre>PS C:\Windows\System32> cd C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC</pre> <i>Ilustración 133 - Acceso a la ruta desde PowerShell</i>

- 10.** Ejecute el comando “dir” para verificar la ubicación y el contenido.

```
PS C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC> dir

Directorio: C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC

Mode                LastWriteTime         Length Name
----                -
d-----         03/08/2026    13:59             CLIENTES INDEPENDIENTES
d-----         03/08/2026    13:59             CLIENTES MIEMBRO
d-----         03/08/2026    13:52    30612 CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
```

Ilustración 134 - Verificación de los archivos

- 11.** Ejecute el archivo “CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1” escribiendo “.\” y pulsando la tecla tabulador hasta ver el nombre del archivo autocompletado. Pulse la tecla “Enter” para comenzar la ejecución.

```
CCN-STIC-599AB25_Scripts_RC> .\CCN-STIC-599AB25_PerfiladoSeguridadWindows11.ps1
```

Ilustración 135 - Ejecución del script de perfilado de seguridad de Windows 11

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

```

--ADVERTENCIA--
Este script incorpora modificaciones en el sistema orientadas a la aplicación de medidas de bastionado, conforme a los
perfiles de seguridad definidos por el Centro Criptológico Nacional (CCN). Para su correcta aplicación, es imprescindible
seguir las recomendaciones establecidas en la guía CCN-STIC-599AB25, comprendiendo los riesgos, impactos y acciones
asociadas que en ella se detallan.
--FIN ADVERTENCIA--
```

Ilustración 136 - Advertencia de uso

- 13.** Debe introducir el carácter “S” y pulsar la tecla “Enter”:

```
{Desea aceptar los riesgos y continuar con el bastionado del sistema?
Selecciona una opción:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S
```

Ilustración 137 – Ejecución del script

- 14.** Automáticamente, el script detectará el sistema operativo y verificará que es un cliente independiente y Windows 11.

```
{Desea aceptar los riesgos y continuar con el bastionado del sistema?
Selecciona una opción:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S
Este equipo es un cliente independiente y ejecuta Windows 11
```

Ilustración 138 - Verificación de Windows 11

- 15.** 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”.

```
ELIJA EL PERFIL DE CALIFICACION
Seleccione una opcion
[D] DIFUSION LIMITADA [I] INFORMACION CLASIFICADA [?] Ayuda (el valor predeterminado es "D"): D
```

Ilustración 139 - Selección del perfil de clasificación de la información

Nota: Dado que en la presente guía se aplican las configuraciones correspondientes al grado de **Difusión Limitada**, únicamente se muestran las opciones de “DIFUSION LIMITADA” e “INFORMACION CLASIFICADA. Si se aplicara la configuración correspondiente al grado **ENS**, se mostraría dicha opción.

Se copiarán automáticamente todos los archivos del grado correspondiente, junto a las configuraciones adicionales, a la carpeta de C:\Scripts\DIFUSION LIMITADA.

```
ELIJA EL PERFIL DE CALIFICACION
Seleccione una opcion
[D] DIFUSION LIMITADA [I] INFORMACION CLASIFICADA [?] Ayuda (el valor predeterminado es "D"): D
Grado final seleccionado: DIFUSION LIMITADA

Preparando copia de archivos de bastionado...
Origen: C:\Users\usa001\Documents\CCN-STIC-599AB25_Scripts_RC\CLIENTES INDEPENDIENTES\DIFUSION LIMITADA
Destino: C:\Scripts\CLIENTES INDEPENDIENTES

Copiando archivos de bastionado...
Copiando configuraciones adicionales...
Configuraciones adicionales copiadas.

Archivos copiados correctamente.
```

Ilustración 140 - Archivos copiados a C:\Scripts

- 16.** Una vez identificado 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)”.

```
Archivos copiados correctamente.

===== LISTA DE ANEXOS =====
ANEXO A. Configuración base de Windows.
ANEXO B. Políticas de seguridad, auditoría, registros de eventos y servicios.
ANEXO C. Gestión de usuarios y políticas de cuenta y contraseña.
ANEXO D. Seguridad de red y firewall de Windows Defender.
ANEXO E. Manejo y control de dispositivos.
ANEXO F. Configuración de BitLocker y criptografía.
ANEXO G. CONFIGURACIÓN ADICIONAL. Incremental Windows Update.
ANEXO H. CONFIGURACIÓN ADICIONAL. Incremental Windows Defender.
=====

¿QUE ANEXO DESEA APLICAR?
Seleccione una opcion de las siguientes
[A] ANEXO A [B] ANEXO B [C] ANEXO C [D] ANEXO D [E] ANEXO E [F] ANEXO F [G] ANEXO G [H] ANEXO H [S] SALIR
[?] Ayuda(el valor predeterminado es "S"): A
```

Ilustración 141 - Selección del anexo a aplicar

- 17.** El script aplicará las plantillas administrativas y seguidamente, solicitará confirmación para proceder con la inhabilitación de características del sistema y la eliminación de aplicaciones aprovisionadas. Introduzca el carácter “S” y pulse “Enter”:

```
Se van a deshabilitar características opcionales del sistema y eliminar aplicaciones aprovisionadas/capacidades indicadas.

ADVERTENCIA: El script contempla las características mínimas necesarias y las mantiene.

ADVERTENCIA: El script contempla las aplicaciones mínimas necesarias y las mantiene

¿Desea continuar la deshabilitación de características opcionales y la eliminación de aplicaciones aprovisionadas?
Seleccione una opción:
[S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): S
```

Ilustración 142 - Inhabilitación de características y aplicaciones

Nota: Es posible que el proceso se “congele” la ventana del terminal, para continuar con el proceso, pulse la tecla “Enter”.

- 18.** Una vez finalizado el proceso, observará el siguiente mensaje:

```
Características opcionales deshabilitadas correctamente.
Puede consultar un registro de las características deshabilitadas en el fichero C:\Scripts\CCN-STIC-599A25_Características Deshabilitadas.csv
```

Ilustración 143 - Mensaje informativo

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

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

7.2.1. 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.

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.

7.2.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD, AUDITORÍA, REGISTROS Y SERVICIOS

Paso	Descripción
1.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje: <pre>¿Desea Continuar aplicando otro Anexo? Selecciona una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): S</pre> <i>Ilustración 144 - Aplicación del siguiente anexo</i> 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, registro de eventos y servicios". <pre>¿QUE ANEXO DESEA APLICAR? Seleccione una opción de las siguientes [A] ANEXO A [B] ANEXO B [C] ANEXO C [D] ANEXO D [E] ANEXO E [F] ANEXO F [G] ANEXO G [H] ANEXO H [S] SALIR [?] Ayuda(el valor predeterminado es "S"): B</pre> <i>Ilustración 145 - Selección del siguiente anexo a aplicar</i>
3.	El script preguntará si desea aplicar el bastionado de servicios para el grado seleccionado. En el caso querer configurar los servicios, introduzca el carácter "S" y pulse "Enter". <pre>APLICACION DE SERVICIOS ¿DESEA APLICAR EL BASTIONADO DE SERVICIOS PARA DIFUSION LIMITADA ? Selecciona una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "N"): S</pre> <i>Ilustración 146 - Aplicación de servicios</i>
4.	Una vez finalizado el proceso, observará el siguiente mensaje: <pre>===== BASTIONANDO ANEXO B Categoría: CLIENTES INDEPENDIENTES Grado: DIFUSION LIMITADA ===== Ejecutando: C:\Scripts\CLIENTES INDEPENDIENTES\DIFUSION LIMITADA\ANEXO B - SEGURIDAD AUDITORIAS Y EVENTOS\CCN-STIC-599B25 - ANEXO B [Servicios] (DIFUSION LIMITADA).ps1 ADVERTENCIA: seedit terminã con advertencias. Se continãa. Revisar log: C:\Scripts\CLIENTES INDEPENDIENTES\DIFUSION LIMITADA\CCN-STIC-599B25 - ANEXO B [Servicios] (DIFUSION LIMITADA).log ANEXO B aplicado correctamente y servicios configurados.</pre> <i>Ilustración 147 - Aplicación de Anexo B</i>
5.	No reinicie el equipo ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

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

7.3.1. 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 equipo.
- 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.

7.3.2. IMPACTO

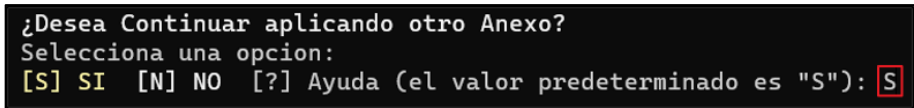
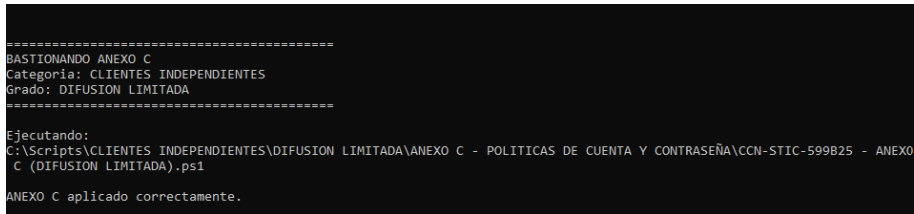
La aplicación de políticas restrictivas de cuenta y contraseña puede tener los siguientes efectos en el entorno:

- 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.

7.3.3. APLICACIÓN DE MEDIDAS DE SEGURIDAD DE USUARIOS, CUENTAS Y CONTRASEÑAS

Paso	Descripción
1.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 148 - Aplicación del siguiente anexo</i> 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”.  <i>Ilustración 149 - Selección del siguiente anexo a aplicar</i>
3.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 150 – Configuración de Anexo C</i>
4.	No reinicie el equipo ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

7.4. 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 11 Independientes. 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.

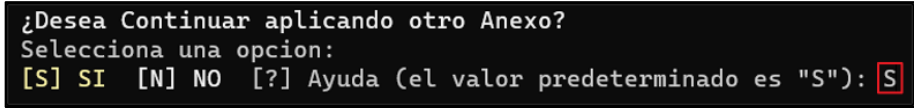
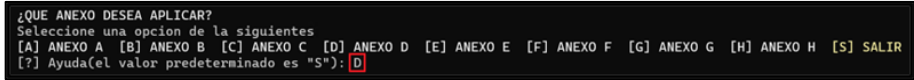
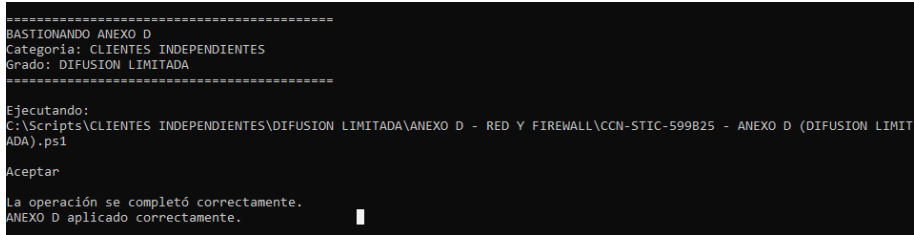
7.4.1. IMPACTO

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.

7.4.2. APLICACIÓN DE SEGURIDAD DE RED

Paso	Descripción
1.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 151 - Aplicación del siguiente anexo</i> 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”.  <i>Ilustración 152 - Selección del siguiente anexo a aplicar</i>
3.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 153 - Anexo D configurado</i>
4.	No reinicie el equipo ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

7.5. ANEXO E. MANEJO Y CONTROL DE DISPOSITIVOS

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.

7.5.1. IMPACTO

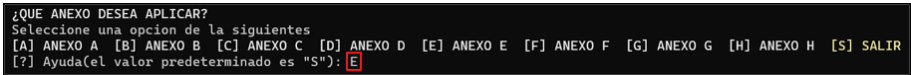
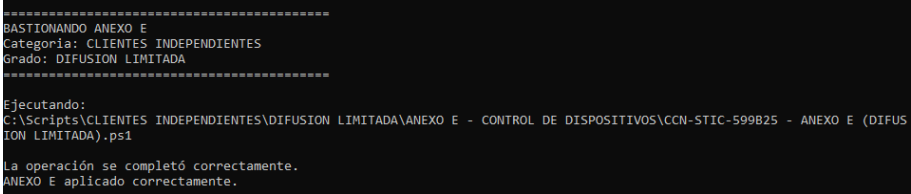
La aplicación de estas medidas puede tener los siguientes efectos en el entorno operativo:

- e) 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.
- f) Necesidad de mantener un inventario actualizado de dispositivos permitidos, incluyendo su ID de hardware, lo que implica una carga administrativa adicional.
- g) Incompatibilidad con procesos automatizados o herramientas de diagnóstico que dependan del uso de medios extraíbles.
- h) 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.

7.5.2. APLICACIÓN DE SEGURIDAD SOBRE DISPOSITIVOS EXTRAÍBLES

Paso	Descripción
1.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje: <pre>¿Desea Continuar aplicando otro Anexo? Selecciona una opción: [S] SI [N] NO [?] Ayuda (el valor predeterminado es "S"): S</pre> <i>Ilustración 154 - Aplicación del siguiente anexo</i> 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”.  <i>Ilustración 155 - Selección del siguiente anexo a aplicar</i>
3.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 156 - Anexo E configurado</i>
4.	No reinicie el equipo ni cierre la ventana de PowerShell, continúe con el siguiente Anexo.

7.6. 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 11. 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 las guías CCN-STIC y se adaptan a los requisitos de sistemas en distintos niveles de clasificación.

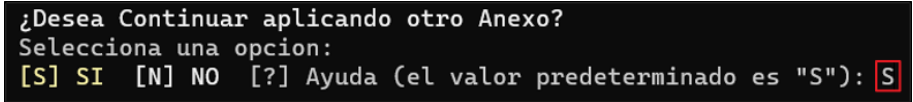
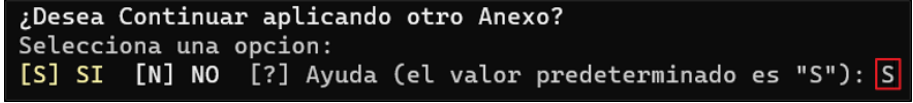
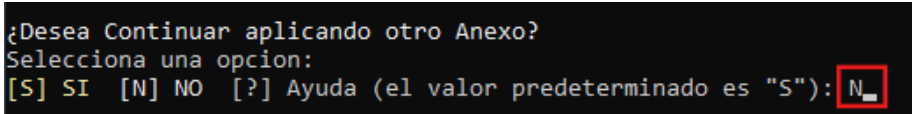
7.6.1. IMPACTO

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.

7.6.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD CRIPTOGRÁFICAS

Paso	Descripción
1.	Continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 157 - Aplicación del siguiente anexo</i> 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”.  <i>Ilustración 158 - Selección del siguiente anexo a aplicar</i>
3.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 159 - Anexo F configurado</i>
4.	Si desea continuar aplicando las configuraciones de seguridad adicionales no reinicie el equipo ni cierre la ventana de PowerShell y pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación de los Anexos.  <i>Ilustración 160 - Configuración de otro anexo</i>
5.	Si sólo se desea configuración principal, pulse el carácter “N” y a continuación, la tecla “Enter”. Seguidamente reinicie el equipo para que se aplique correctamente toda la configuración.  <i>Ilustración 161 - Finalización de script</i>

7.7. ANEXO G. MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

En el presente anexo se definen las acciones necesarias para dotar a los sistemas operativos Windows 11 Independientes de un servicio de actualizaciones automáticas centralizado y completamente configurado. Mediante la aplicación de directivas específicas de Windows Update, se controla el comportamiento de las actualizaciones automáticas, la recepción de actualizaciones de calidad, características y compilaciones preliminares, así como la instalación de actualizaciones recomendadas.

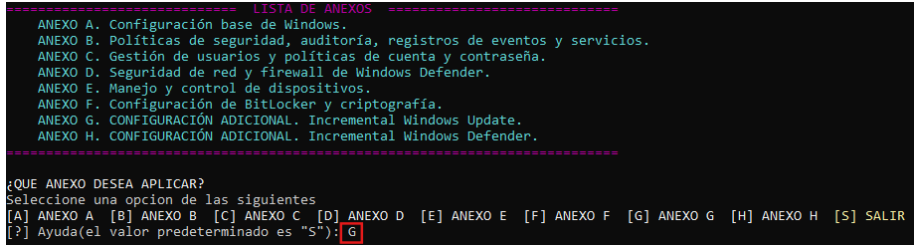
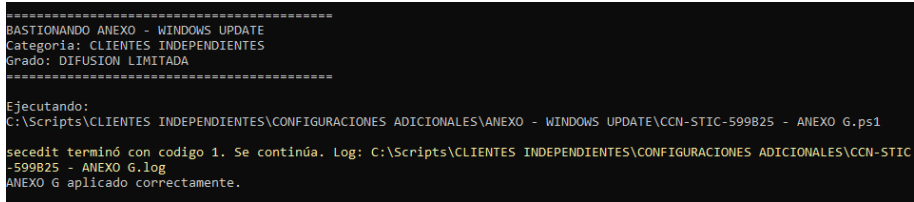
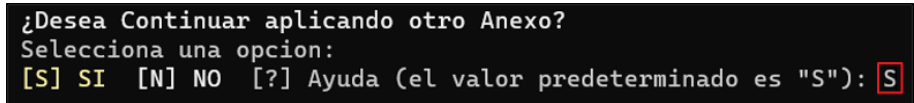
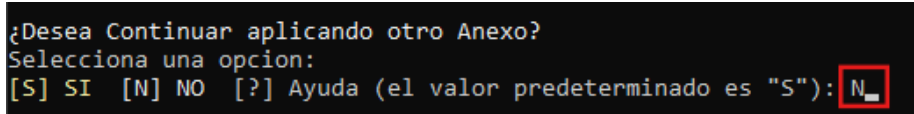
Nota: Si en su organización ya dispone de un producto o servicio para la actualización y mantenimiento del sistema operativo, como el servicio de WSUS, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

7.7.1. IMPACTO

La aplicación de este servicio puede tener los siguientes efectos en el entorno operativo:

- a) Instalación automática de actualizaciones en los equipos Windows cliente, reduciendo la exposición a vulnerabilidades, pero pudiendo introducir cambios en el sistema sin intervención directa del usuario.
- b) Reinicios necesarios tras determinadas actualizaciones, lo que puede interrumpir sesiones activas, tareas programadas o procesos en ejecución si no se han definido ventanas de mantenimiento adecuadas.
- c) Posibles incompatibilidades con aplicaciones, controladores o componentes corporativos, especialmente tras actualizaciones acumulativas, de características o de drivers.
- d) Incremento puntual de incidencias operativas, derivadas de errores de instalación, equipos pendientes de reinicio, fallos de compatibilidad o usuarios afectados por cambios introducidos tras la actualización.

7.7.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD

Paso	Descripción
1.	Mantenga la sesión iniciada en el equipo donde está aplicando la configuración de seguridad, y continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 162 - Aplicación del siguiente anexo</i> Pulse el carácter “G” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del ANEXO G Incremental Windows Update. Nota: Revise atentamente todas las configuraciones que aplica el presente Anexo.
2.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 163 - Anexo G configurado</i>
3.	Si desea continuar aplicando las configuraciones de seguridad adicionales no reinicie el equipo ni cierre la ventana de PowerShell y pulse el carácter “S” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación de los Anexos.  <i>Ilustración 164 - Configuración de otro anexo</i>
4.	Si no desea ninguna otra configuración, pulse el carácter “N” y a continuación, la tecla “Enter”. Seguidamente reinicie el equipo para que se aplique correctamente toda la configuración.  <i>Ilustración 165 - Finalización de script</i>

7.8. ANEXO H. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

En esta sección se establecen las directivas necesarias para configurar y reforzar la protección frente a código dañino en los sistemas operativos Windows 11 Independiente, utilizando las capacidades integradas del software antimalware incluido por defecto. La configuración abarca la detección de aplicaciones potencialmente no deseadas, el uso de mecanismos heurísticos, la supervisión del comportamiento, el análisis de archivos, scripts, procesos y dispositivos extraíbles, así como la protección frente a accesos a sitios web peligrosos.

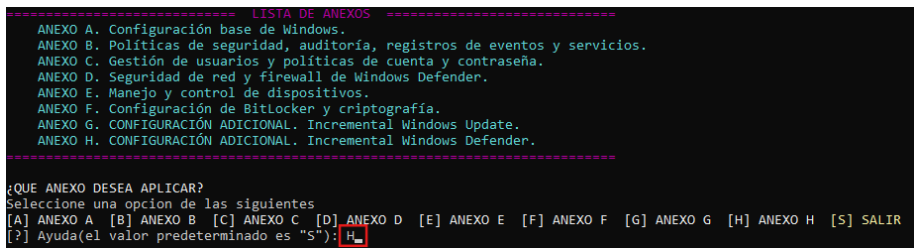
Nota: Si en su organización ya dispone de un producto o servicio frente a código dañino en el sistema operativo, puede ignorar el siguiente paso a paso y continuar en el siguiente punto.

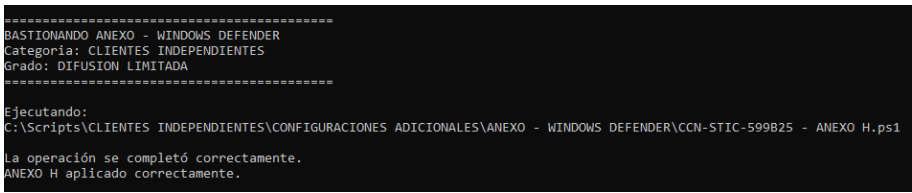
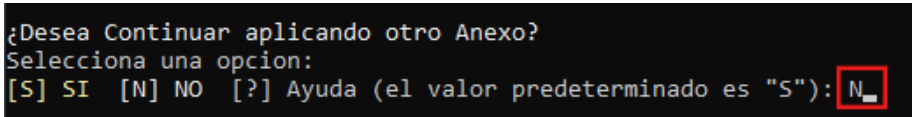
7.8.1. IMPACTO

La configuración para la protección frente a código dañino puede impactar de la siguiente manera:

- e) Posibles bloqueos o restricciones de aplicaciones y acciones legítimas, como consecuencia de la detección de aplicaciones potencialmente no deseadas, el acceso controlado a carpetas o las políticas de protección de red y navegación.
- f) Incremento de incidencias relacionadas con falsos positivos, que pueden requerir análisis, ajustes de políticas o autorización explícita de aplicaciones, carpetas o procesos necesarios para la operativa.

7.8.2. APLICACIÓN DE MEDIDAS DE SEGURIDAD

Paso	Descripción
1.	Mantenga la sesión iniciada en el equipo donde está aplicando la configuración de seguridad, y continuando con la configuración de seguridad, si ha seguido los pasos anteriores, debe observar el siguiente mensaje:  <i>Ilustración 166 - Aplicación del siguiente anexo</i> Pulse el carácter “H” y a continuación, la tecla “Enter” para continuar con el proceso de fortificación del ANEXO H Incremental Windows Defender. Nota: Revise atentamente todas las configuraciones que aplica el presente Anexo.

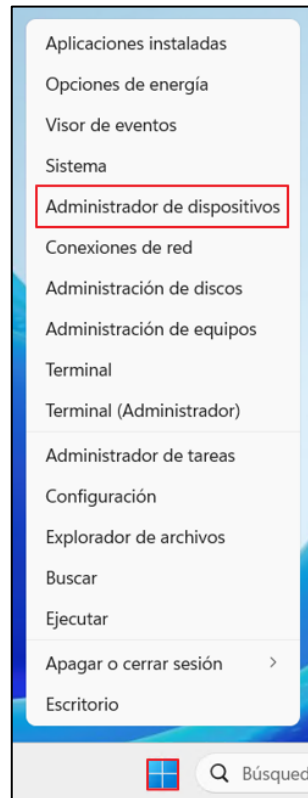
2.	Una vez finalizado el proceso, observará el siguiente mensaje:  <i>Ilustración 167 - Anexo H configurado</i>
3.	Finalmente, pulse el carácter “N” y a continuación, la tecla “Enter”. Seguidamente reinicie el equipo para que se aplique correctamente toda la configuración.  <i>Ilustración 168 - Finalización de script</i>

7.9. CONFIGURACIONES MANUALES Y COMPROBACIONES

7.9.1. ADMINISTRACIÓN Y CONTROL DE NUEVOS DISPOSITIVOS EXTRAÍBLES

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

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

Paso	Descripción
1.	Inicie sesión en el equipo donde se pretende habilitar el uso de un dispositivo USB con un usuario con privilegios de administración.
2.	Haga clic derecho sobre el botón de inicio, y sobre “Administrador de dispositivos”:  <i>Ilustración 169 - Ejecución del Administrador de dispositivos</i>

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”.

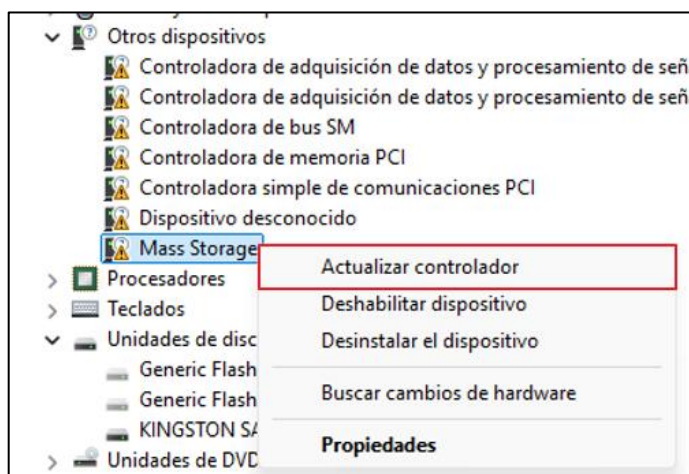


Ilustración 170 - Selección del dispositivo

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”.

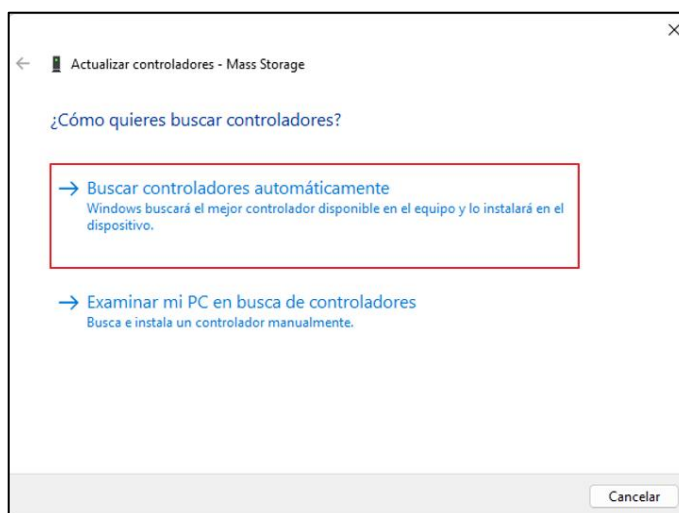


Ilustración 171 - Búsqueda automática de controladores

5. Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.

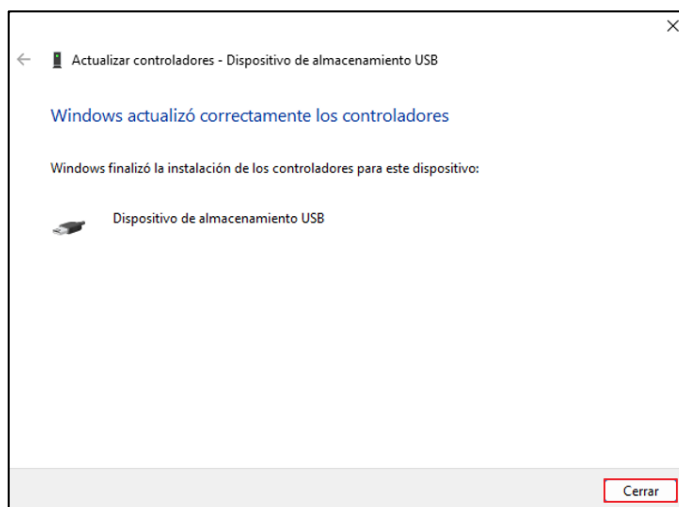


Ilustración 172 - Finalización de la actualización de controladores

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 173 - Unidad de disco nueva

7.9.1.2. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

Los pasos definidos a continuación deberán ser realizados en el equipo independiente en el cual se pretende habilitar el uso de dispositivos USB.

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

8. Haga clic derecho sobre el botón de inicio, y sobre “Administrador de dispositivos”:

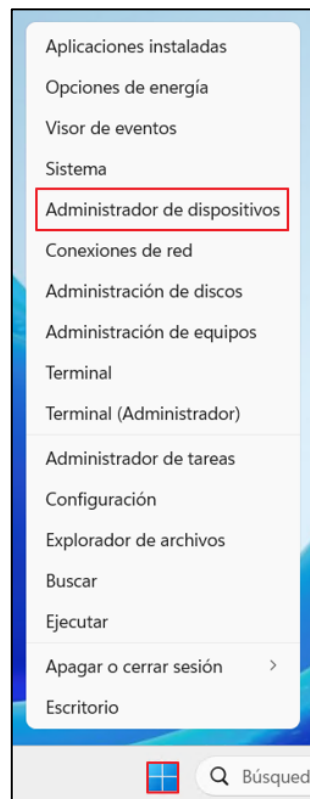


Ilustración 174 - Ejecución del Administrador de dispositivos

9. 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”.

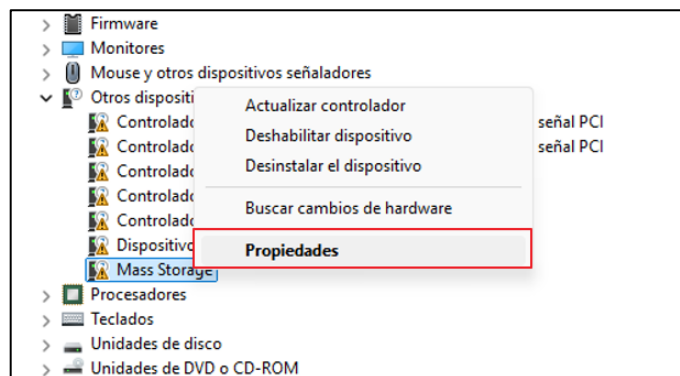


Ilustración 175 - Propiedades del dispositivo

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”.

10. Acceda a la pestaña “Detalles”. En el apartado “Propiedad”, seleccione “Id. de hardware”. Seleccione el identificador que se encuentra en primer lugar y anótelolo para poder utilizarlo más adelante.

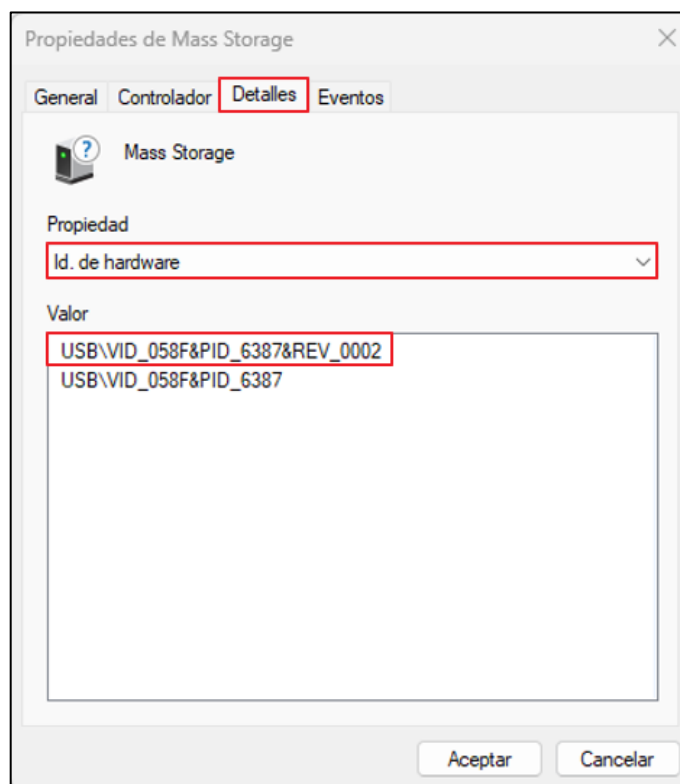


Ilustración 176 - Detalles del dispositivo

Nota: Independientemente del número de identificadores existentes, deberá seleccionar siempre aquel que se encuentre en primera posición.

11. Ejecute el Editor de directivas de grupo “gpedit.msc” en modo Administrador.

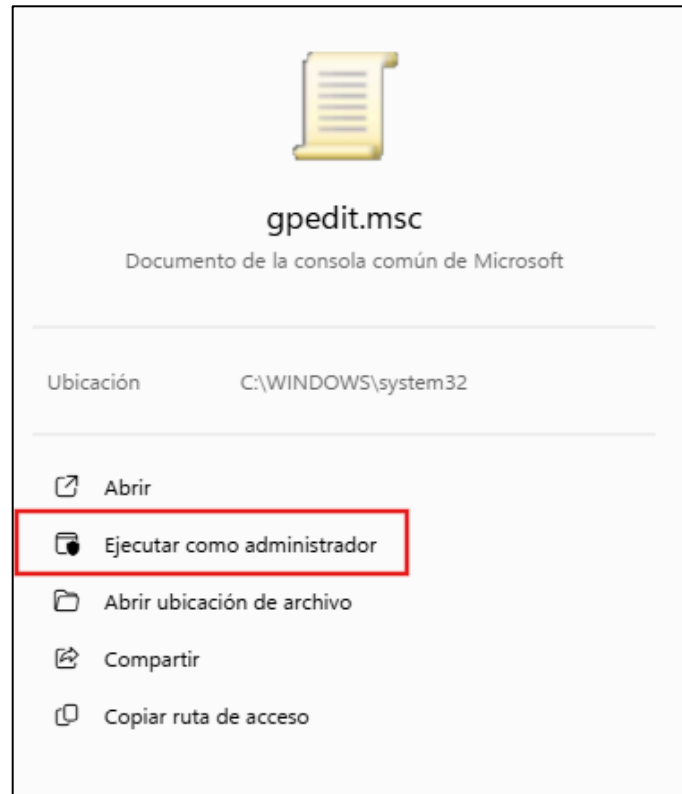


Ilustración 177 - Ejecución de Editor de directivas de grupo

12. Despliegue el nodo “Configuración del equipo > Plantillas administrativas > Sistema > Instalación de dispositivos > Restricciones de instalación de dispositivos”.

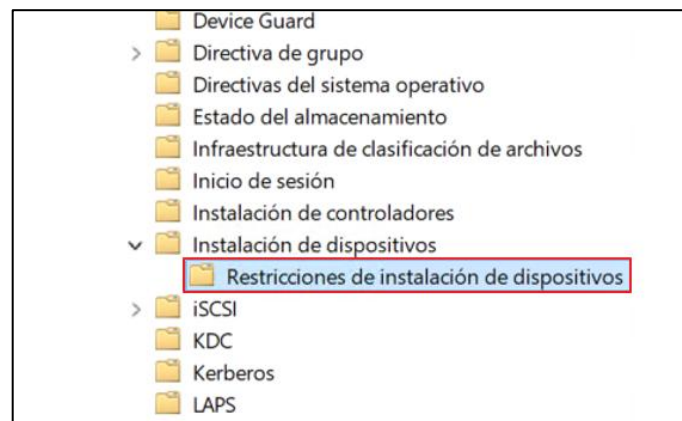


Ilustración 178 - Despliegue del nodo de restricciones de instalación de dispositivos

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

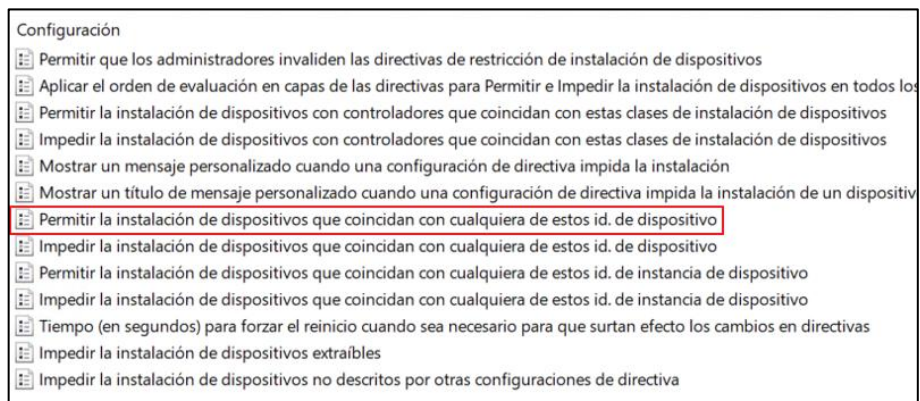


Ilustración 179 - Edición de la política

Hacer clic en “Mostrar...”:

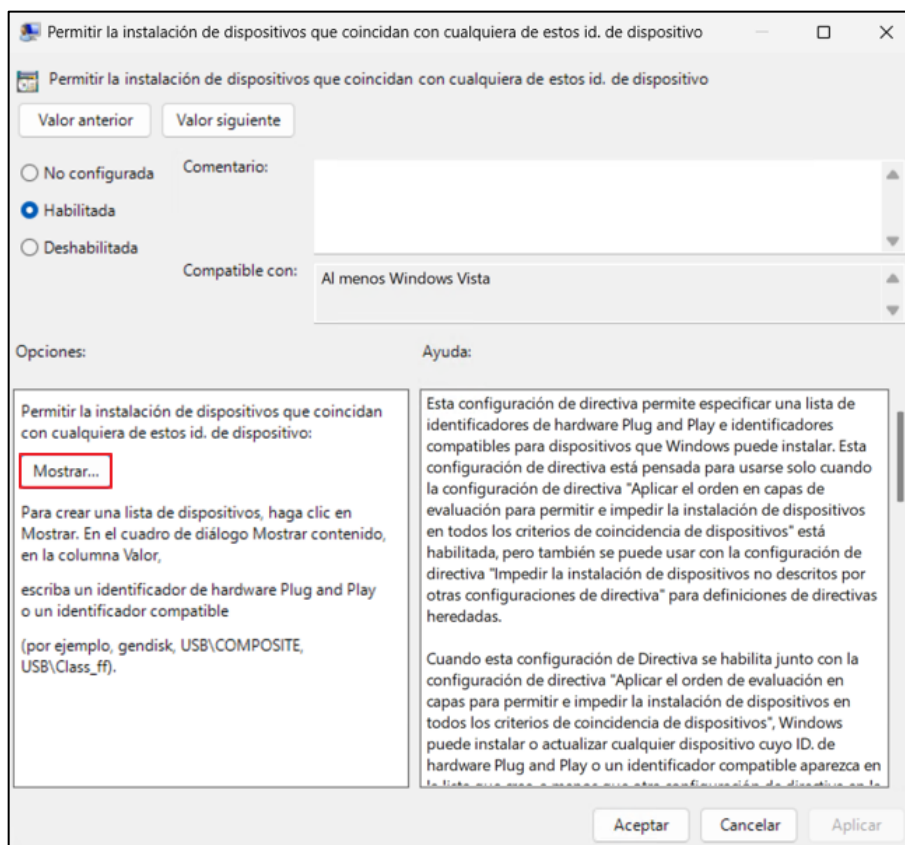


Ilustración 180 - Configuración de la política

- 14.** 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”.

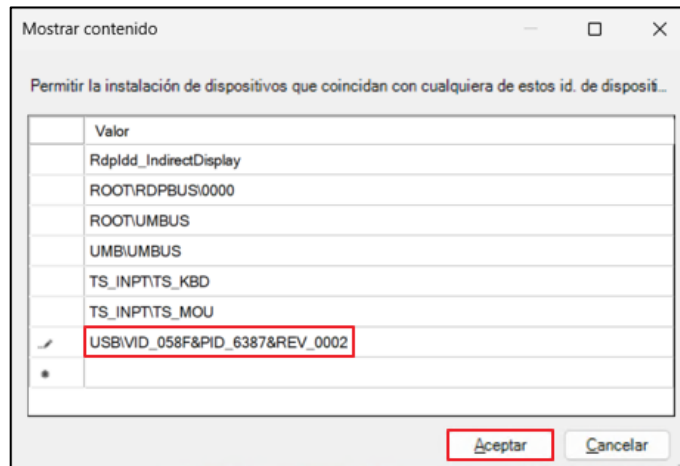


Ilustración 181 - Adición del id. de hardware del dispositivo

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

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

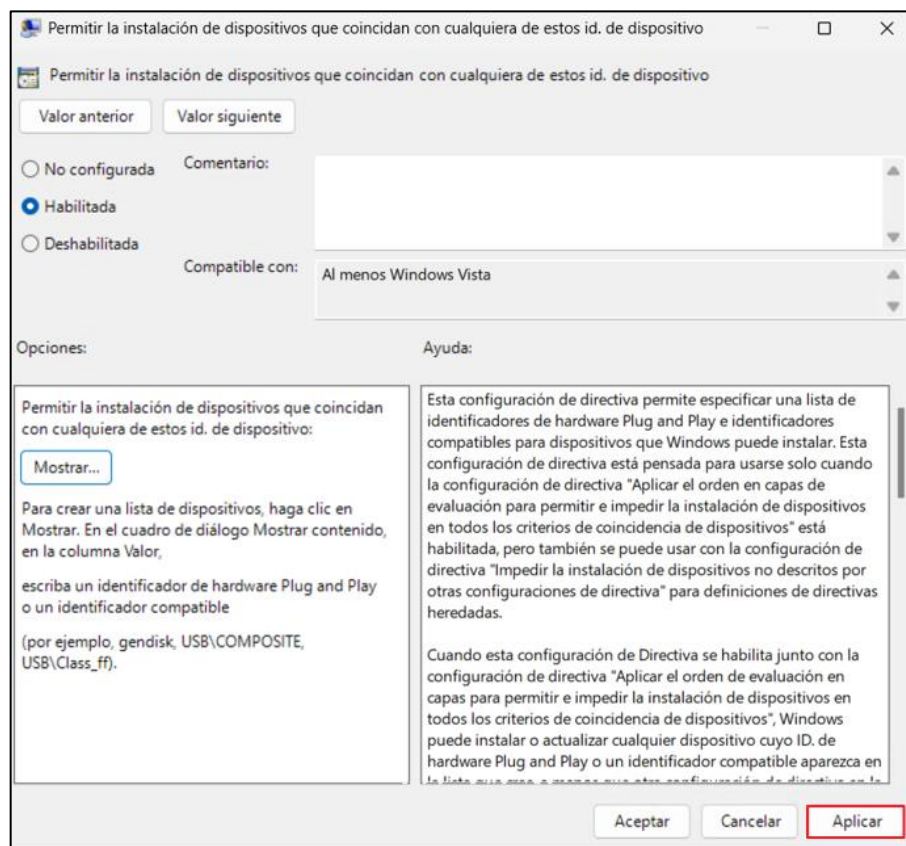


Ilustración 182 - Finalización de la configuración de la política

- 16.** Sin cerrar el “Editor de directivas de grupo local”, continúe con el siguiente paso.

17. Ejecute la Consola de Comandos del sistema en modo Administrador.

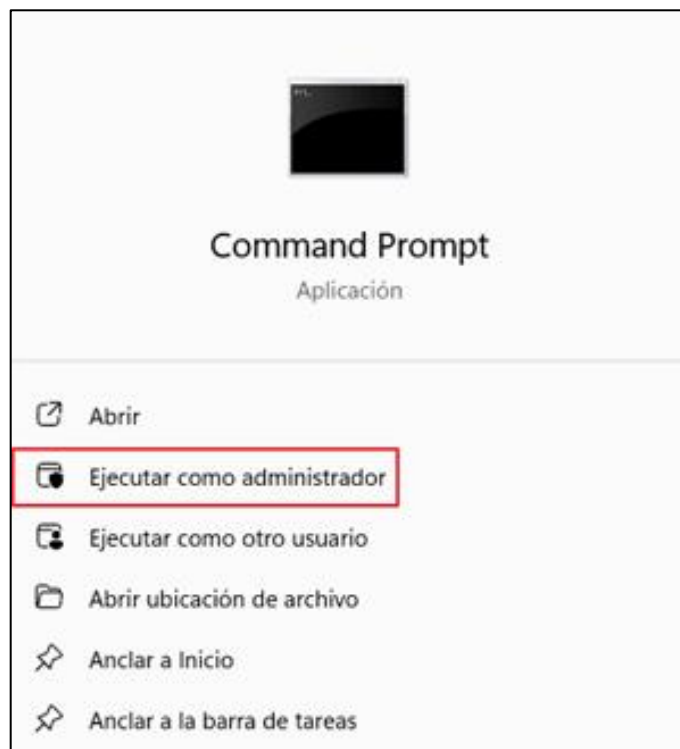


Ilustración 183 - Ejecución como administrador de CMD

18. Ejecute el comando `gpupdate /force`. Tras finalizar, observará el siguiente mensaje:

```
C:\Users\Administrador>gpupdate /force
Actualizando directiva...

La actualización de la directiva de equipo se completó correctamente.
Se completó correctamente la Actualización de directiva de usuario.
```

Ilustración 184 - Ejecución de `gpupdate /force`

19. 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.

7.9.1.3. ELIMINAR DISPOSITIVOS USB DADOS DE ALTA

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

Paso	Descripción
20.	Inicie sesión en el equipo cliente donde se pretende eliminar el uso de un dispositivo USB con un usuario con privilegios de administración.

21. Haga clic derecho sobre el botón de inicio, y sobre “Administrador de dispositivos”:

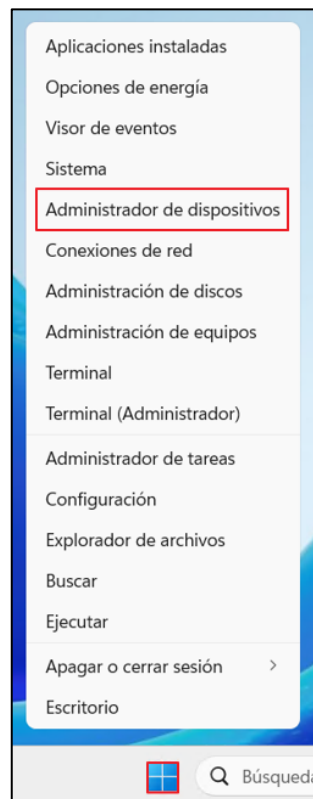


Ilustración 185 - Ejecución del Administrador de dispositivos

22. Seleccione la pestaña “Ver” y haga clic en la opción “Mostrar dispositivos ocultos”.

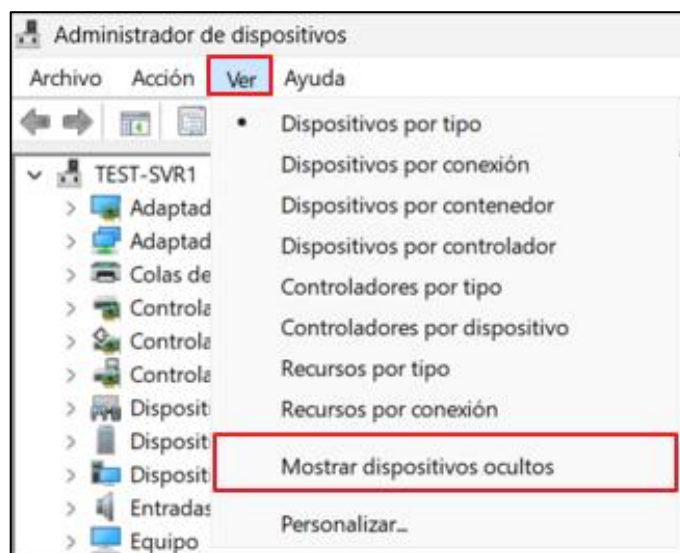


Ilustración 186 – Mostrar dispositivos ocultos

23. 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 187 - Desinstalación del dispositivo

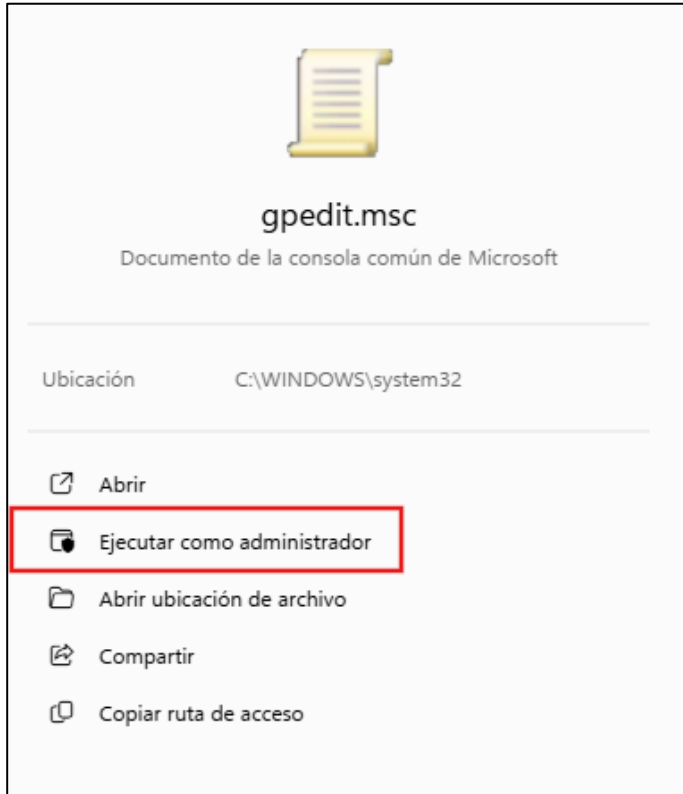
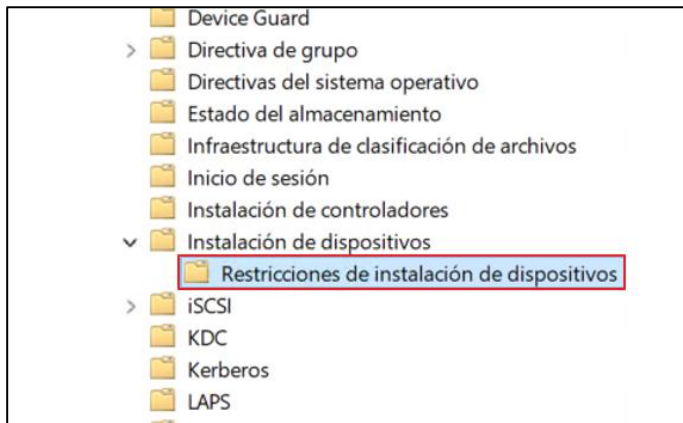
24. Haga clic sobre “Desinstalar” en la ventana emergente.



Ilustración 188 - Confirmación de la desinstalación

Nota: Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

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

Paso	Descripción
25.	Ejecute el Editor de directivas de grupo “gpedit.msc” en modo Administrador.  <i>Ilustración 189 - Ejecución de Editor de directivas de grupo</i>
26.	Despliegue el nodo “Configuración del equipo > Plantillas administrativas > Sistema > Instalación de dispositivos > Restricciones de instalación de dispositivos”.  <i>Ilustración 190 - Despliegue del nodo de restricciones de instalación de dispositivos</i>

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

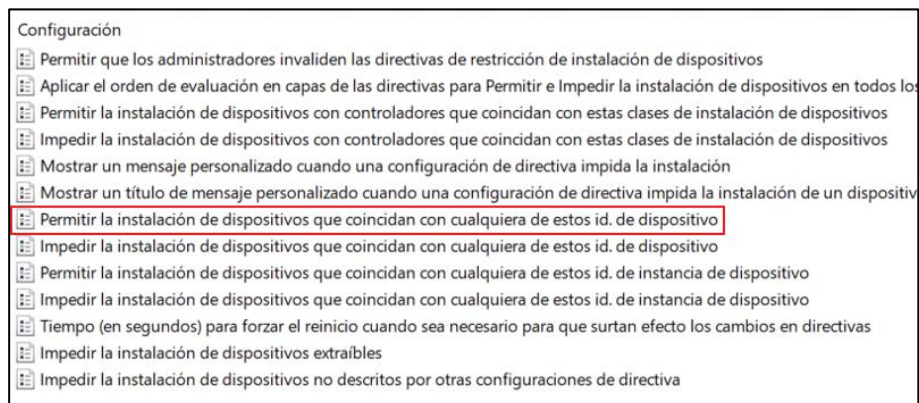


Ilustración 191 - Edición de la política

- 28.** Hacer clic en “Mostrar...”:

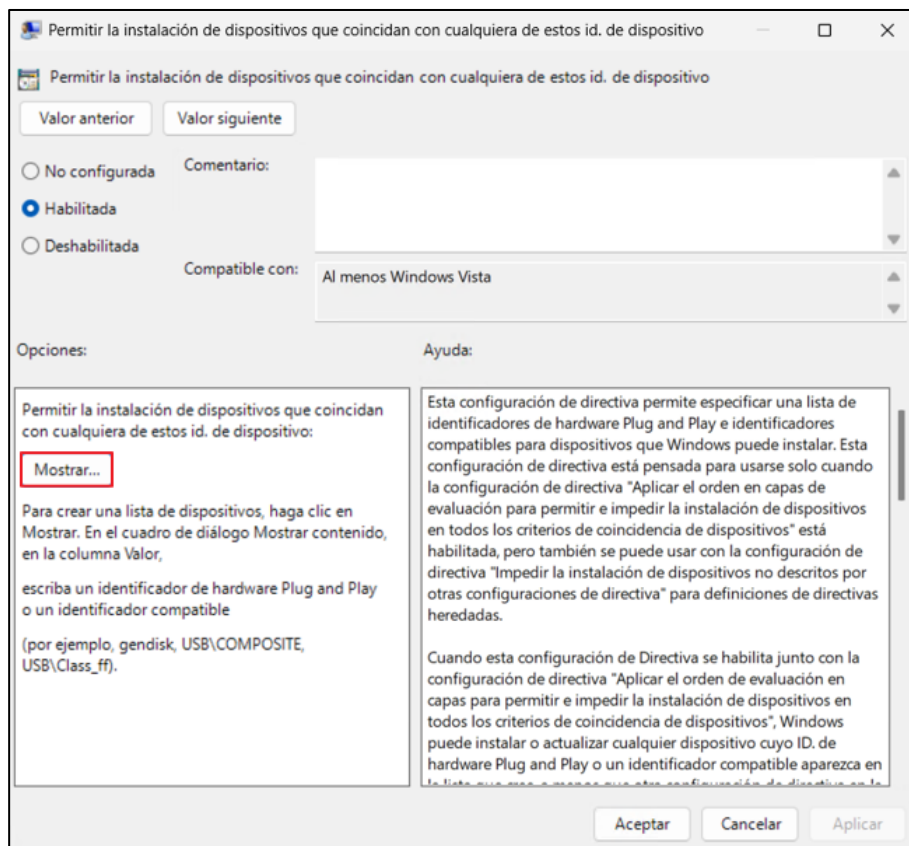


Ilustración 192 - Configuración de la política

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

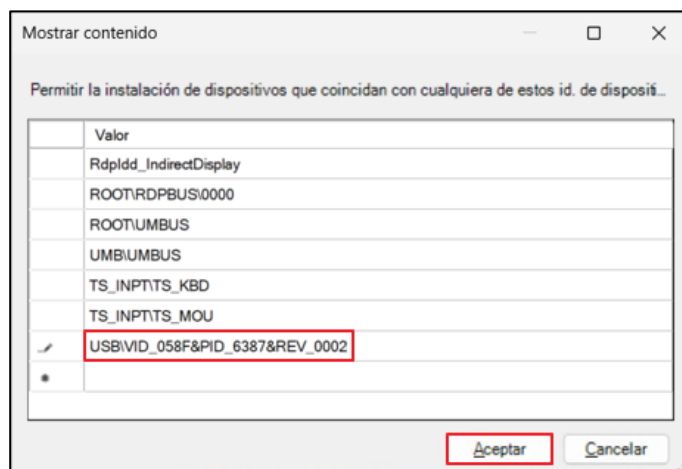


Ilustración 193 - Eliminación del id. de hardware del dispositivo

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

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

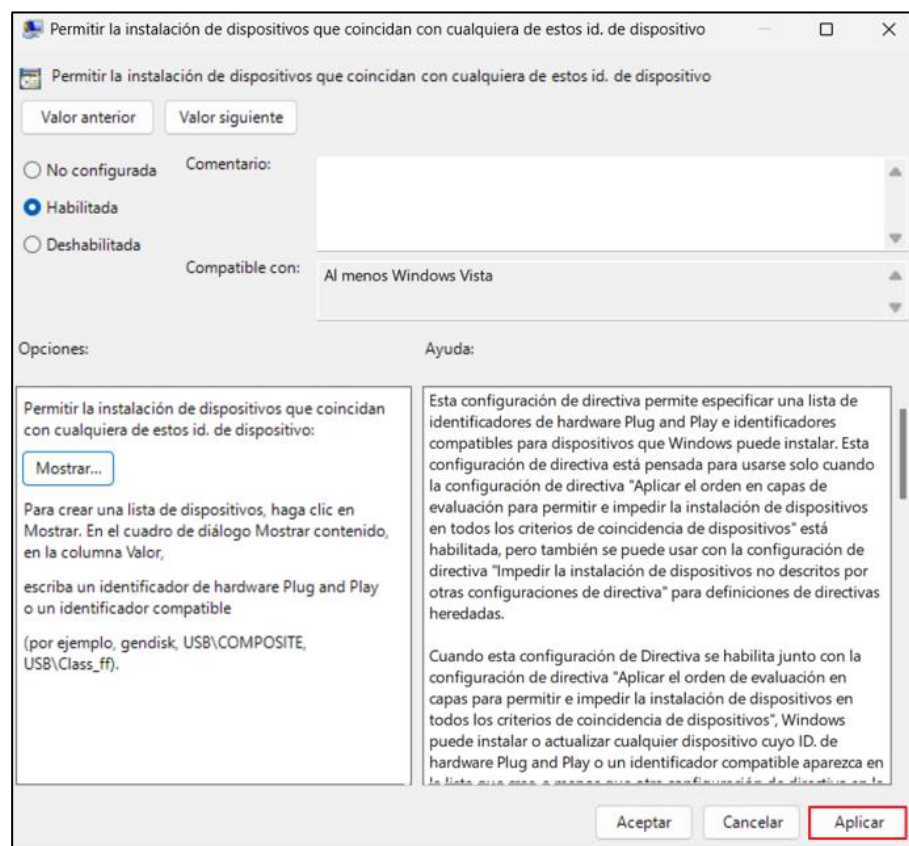
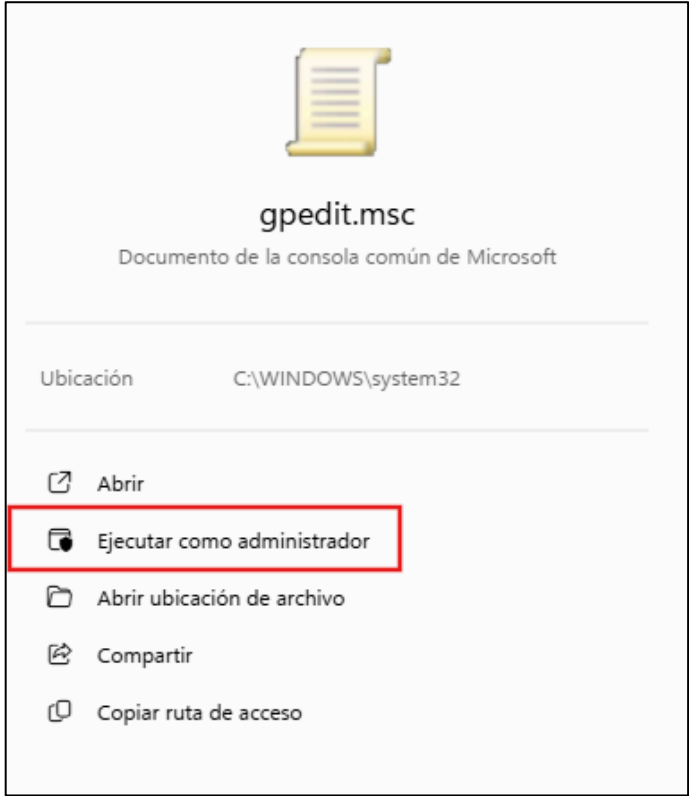
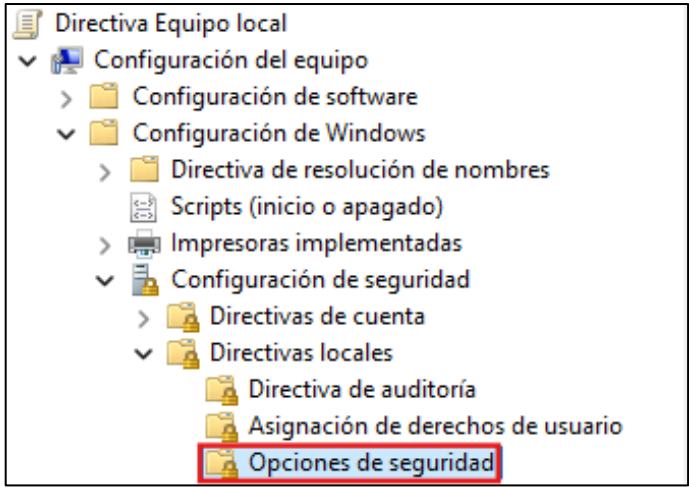


Ilustración 194 - Finalización de la configuración de la política

7.9.2. 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 11, 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 cliente independiente en el que quiere configurarse el mensaje de inicio de sesión.
2.	Ejecute el Editor de directivas de grupo “gpedit.msc” en modo Administrador.  <i>Ilustración 195 - Ejecución de Editor de directivas de grupo</i>
3.	Despliegue el nodo “Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad”.  <i>Ilustración 196 – Despliegue del nodo de opciones de seguridad</i>

4. 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.

Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear L...	Habilitada
Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	No está definido
Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión	Está usted accediendo a un equi...
Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión	AVISO IMPORTANTE DE SEGURID...
Inicio de sesión interactivo: umbral de bloqueo de cuenta del equipo	No está definido
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada

Ilustración 197 - GPOs de texto y título de mensaje

5. Texto del mensaje:

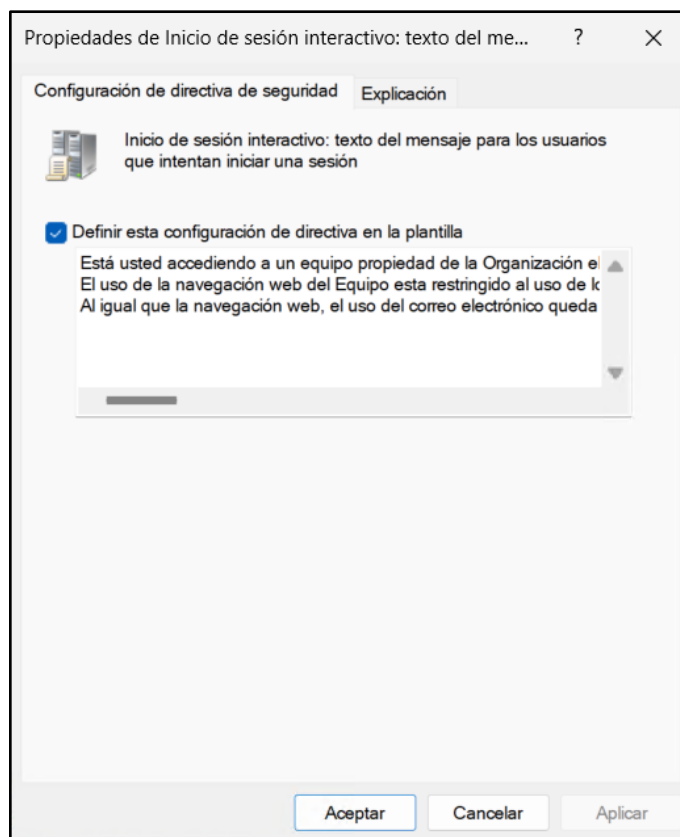
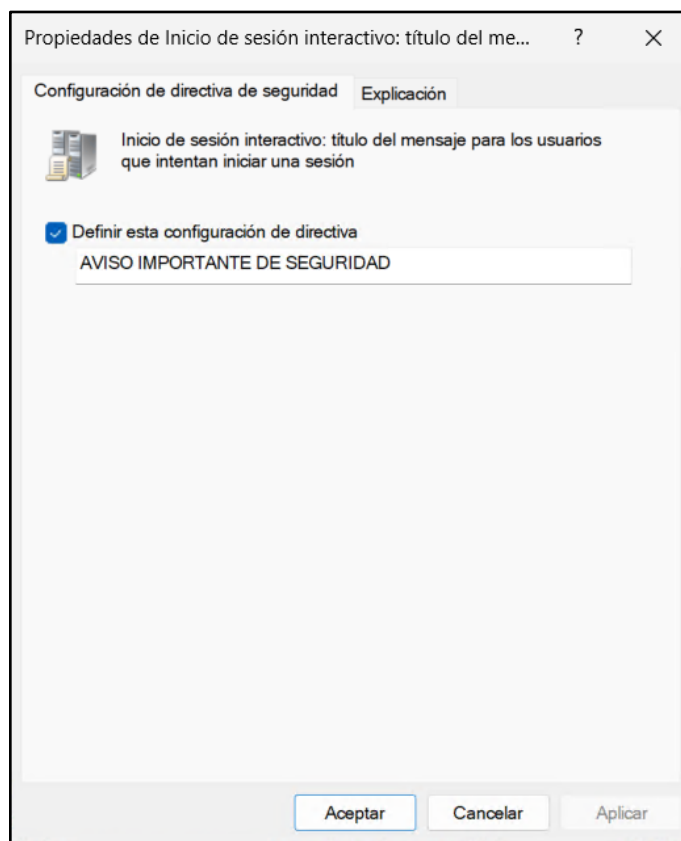
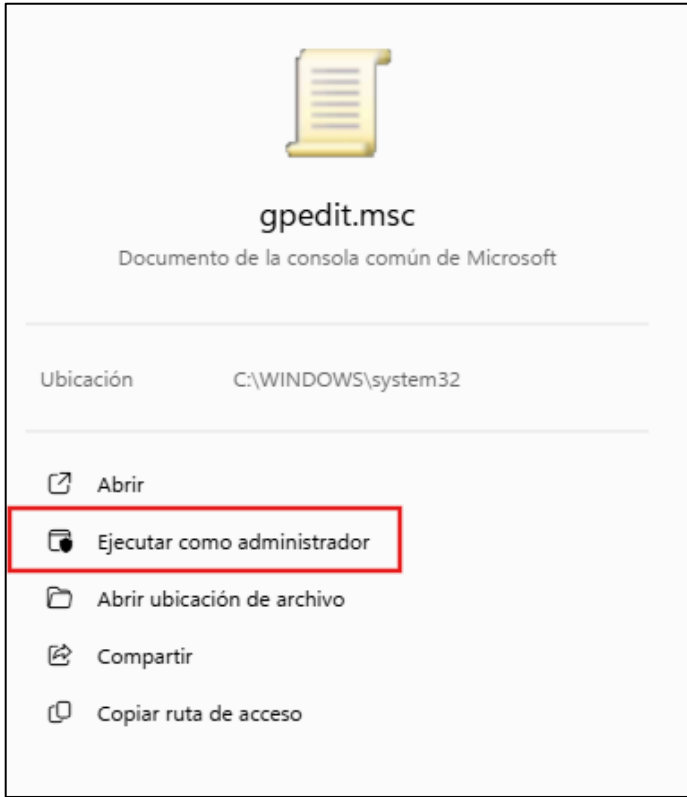
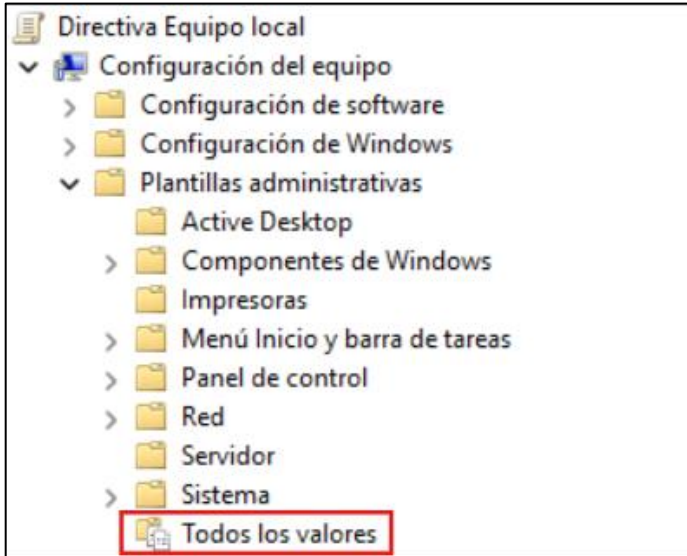


Ilustración 198 - Texto del mensaje

6. Título del mensaje:*Ilustración 199 - Título del mensaje***7.9.3. 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.

Para verificar que los principales anexos se han aplicado correctamente, se comprobará la existencia y aplicación de una directiva específica asociada a cada uno de ellos. La visualización de estas directivas permitirá confirmar que las configuraciones correspondientes han sido desplegadas en el sistema y que cada anexo ha sido procesado correctamente durante el procedimiento de configuración de seguridad.

Paso	Descripción
1.	Ejecute el Editor de directivas de grupo “gpedit.msc” en modo Administrador.  <i>Ilustración 200 - Ejecución de Editor de directivas de grupo</i>
2.	Para visualizar las plantillas administrativas del Anexo A aplicadas, despliegue el nodo “Configuración del equipo > Plantillas administrativas > Todos los valores”.  <i>Ilustración 201 - Ruta de Todos los valores</i>

3. Pulse en la columna de “Estado” para observar los valores configurados ordenados.

Configuración	Estado
 Permitir archivos de tema desde ubicaciones de red	No configurada
 Ocultar y deshabilitar todos los elementos del escritorio	No configurada
 Impedir el acceso a Internet de Windows Media DRM	No configurada
 Permitir autenticación básica	No configurada
 Permitir autenticación CredSSP	No configurada
 Permitir tráfico sin cifrar	No configurada
 No permitir autenticación implícita	No configurada
 No permitir autenticación Kerberos	No configurada

Ilustración 202 - Orden de las directivas

4. Si observa que existen políticas en estado “Habilitada” y “Deshabilitada” significa que se ha configurado correctamente el equipo.

Configuración	Estado
 Enumerar las cuentas de administración al realizar una elevación	Deshabilitada
 Iniciar sesión y bloquear el último usuario interactivo automáticamente después de un reinicio	Deshabilitada
 Mostrar animación de primer inicio de sesión	Deshabilitada
 Enumerar usuarios locales en equipos unidos al dominio	Deshabilitada
 Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada
 Configurar la función antisuplantación de identidad (spoofing) mejorada	Habilitada
 Permitir el uso de biometría	Habilitada
 Permitir que los usuarios inicien sesión mediante biometría	Habilitada
 Permitir que los usuarios de dominio inicien sesión mediante biometría	Habilitada
 Impedir que el equipo se una a un grupo en el hogar	Habilitada
 Impedir el uso de OneDrive para almacenar archivos	Habilitada
 Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	Habilitada
 Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario	Habilitada
 Evitar que el usuario muestre detalles de la cuenta al iniciar sesión	Habilitada
 No enumerar usuarios conectados en equipos unidos al dominio	Habilitada

Ilustración 203 - Visualización de directivas configuradas

Nota: Existen políticas de diferentes anexos que no se visualizan en el Editor de directivas de grupo. Esto es debido a que dichas directivas se han importado directamente al Editor de registro.

5. De igual forma, se analizarán las configuraciones de seguridad. Para ello, desplácese hasta “Configuración del equipo > Configuraciones de seguridad > Directivas de cuenta > Directiva de contraseñas”.

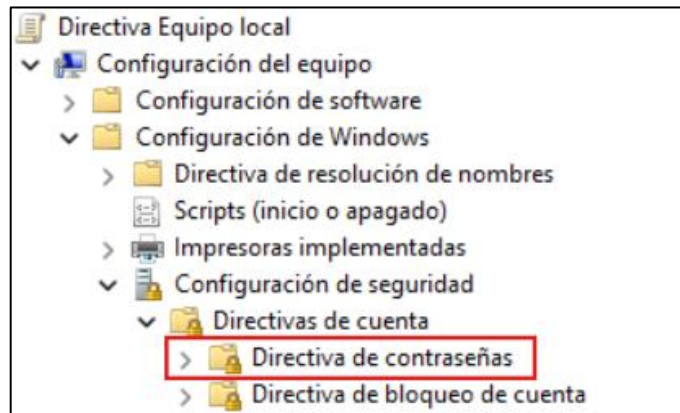


Ilustración 204 - Directivas de contraseñas

6. Se observa que las directivas se encuentran correctamente configuradas.

Directiva	Configuración de seguridad
 Almacenar contraseñas con cifrado reversible	Deshabilitada
 Auditoría de longitud mínima de contraseña	No está definido
 Exigir historial de contraseñas	24 contraseñas recordadas
 La contraseña debe cumplir los requisitos de complejidad	Habilitada
 Longitud mínima de la contraseña	10 caracteres
 Reducir los límites de longitud mínima de la contraseña	Habilitada
 Vigencia máxima de la contraseña	60 días
 Vigencia mínima de la contraseña	2 días

Ilustración 205 - Visualización de directivas de contraseñas