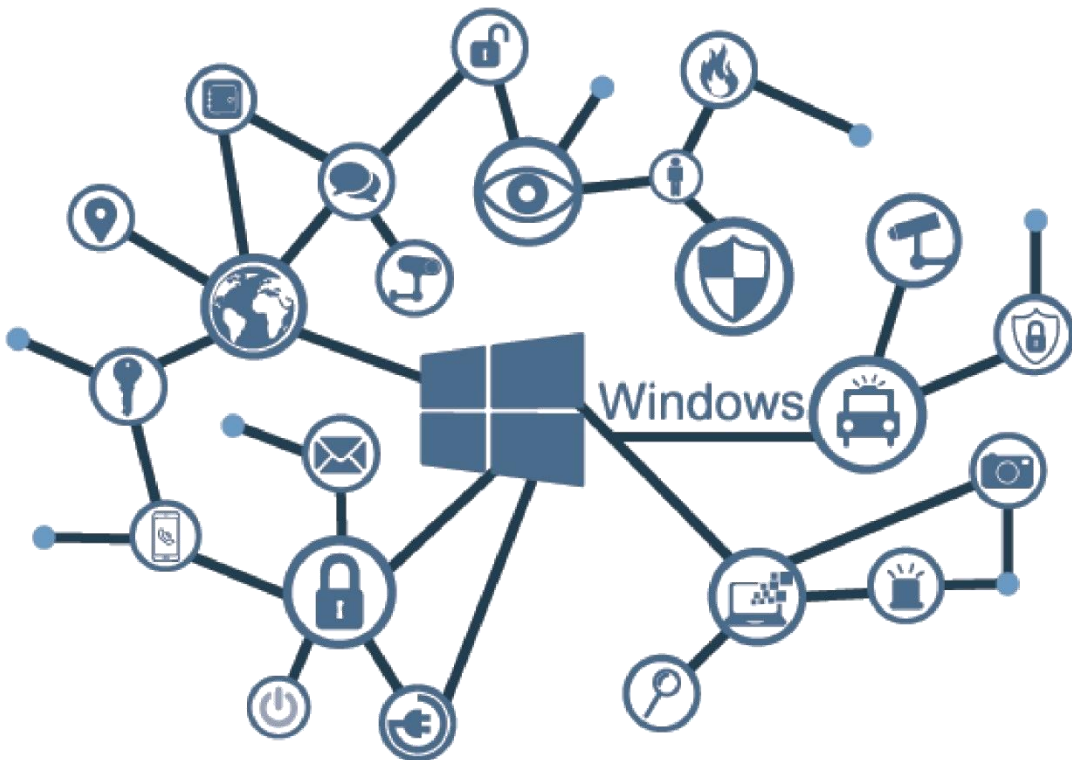


CCN-STIC 599B19

IMPLEMENTACIÓN DE SEGURIDAD SOBRE

MICROSOFT WINDOWS 10 (1809) (CLIENTE INDEPENDIENTE)



SEPTIEMBRE 2019



Edita:



© Centro Criptológico Nacional, 2019

NIPO: 083-19-242-8

Fecha de Edición: octubre de 2019

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

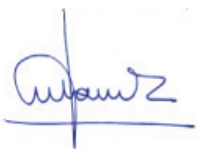
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

julio de 2019



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN EL ENS COMO CLIENTE INDEPENDIENTE	9
ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE MS WINDOWS 10 EN EL ENS	10
1. APLICACIÓN DE MEDIDAS EN MICROSOFT WINDOWS 10	10
1.1. MARCO OPERACIONAL	11
1.1.1. CONTROL DE ACCESO	11
1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN	11
1.1.1.2. OP. ACC. 2. REQUISITOS DE ACCESO	11
1.1.1.3. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS	12
1.1.1.4. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO.....	13
1.1.1.5. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN	14
1.1.1.6. OP. ACC. 6. ACCESO LOCAL	15
1.1.1.7. OP. ACC. 7. ACCESO REMOTO	15
1.1.2. EXPLOTACIÓN.....	16
1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD.....	16
1.1.2.2. OP. EXP. 4. MANTENIMIENTO	16
1.1.2.3. OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO.....	17
1.1.2.4. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS.....	18
1.1.2.5. OP. EXP. 10. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	18
1.2. MEDIDAS DE PROTECCIÓN.....	19
1.2.1. PROTECCIÓN DE LOS EQUIPOS.....	19
1.2.1.1. MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO	19
1.2.1.2. MP. EQ. 3. PROTECCIÓN DE LOS PORTÁTILES.....	19
1.2.2. PROTECCIÓN DE LAS COMUNICACIONES.....	20
1.2.2.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD	20
1.2.3. PROTECCIÓN DE LA INFORMACIÓN	21
1.2.3.1. MP. INFO. 3. CIFRADO	21
2. RESUMEN Y APLICACIÓN DE MEDIDAS EN MICROSOFT WINDOWS 10.....	21
ANEXO A.2. CATEGORÍA BÁSICA.....	24
ANEXO A.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS	24
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA BÁSICA.....	32
ANEXO A.3. CATEGORÍA MEDIA	66

ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS	66
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA MEDIA	78
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA.....	116
ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	116
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA	128
ANEXO A.4.3. IMPLEMENTACIÓN DE BITLOCKER PARA CIFRADO DE DISCO EN CLIENTES WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	166
ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	178
ANEXO A.5.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA	178
ANEXO A.5.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA WINDOWS 10 INDEPENDIENTE	186
1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 INDEPENDIENTES	186
ANEXO A.5.3. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	187
1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	188
2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	189
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	191
ANEXO B. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN REDES CLASIFICADAS COMO CLIENTE INDEPENDIENTE	198
ANEXO B.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 COMO CLIENTE INDEPENDIENTE.....	200
ANEXO B.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA	200
1. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10	201
2. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10	217
ANEXO B.1.2. LISTA DE COMPROBACIÓN PASO A PASO.....	244
ANEXO B.2. APLICACIÓN DE NIVELES DE CLASIFICACIÓN	340
ANEXO B.2.1. NIVEL DE CLASIFICACIÓN CONFIDENCIAL.....	340
ANEXO B.2.2. NIVEL DE CLASIFICACIÓN RESERVADO O SUPERIOR.....	343
ANEXO B.3. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	345
ANEXO B.3.1. CIFRADO DE DISCO CON BITLOCKER.....	345
1. ALCANCE	345
2. DESCRIPCIÓN DE USO DE ESTE ANEXO	346

3. REQUISITOS HARDWARE Y SOFTWARE.....	346
4. GUÍA PASO A PASO – BITLOCKER	347
5. LISTA DE COMPROBACIÓN – BITLOCKER	357
ANEXO B.3.2. USO DE DIFERENTES CONSOLAS DE ADMINISTRACIÓN TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19.....	359
ANEXO B.3.3. USO DE GRABADORA DE CD/DVD TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE	362
ANEXO B.3.4. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE	365
1. ADMINISTRAR DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES	365
1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB.....	366
1.2. DESINSTALACIÓN DE CONTROLADORES PARA IMPEDIR EL USO DE DISPOSITIVOS USB.....	373
2. ADMINISTRAR EL USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE EL IDENTIFICADOR DE DISPOSITIVO	375
2.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR.....	376
2.2. IMPEDIR EL USO DE DISPOSITIVOS USB.....	384
ANEXO B.3.5. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19	387
ANEXO B.3.6. CONFIGURACIÓN DE CLIENTE INDEPENDIENTE PARA PODER ACCEDER A UN RECURSO COMPARTIDO EN LA RED	392
ANEXO B.3.7. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	403
1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	403
2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	405
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	407
ANEXO C. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN EL ENS COMO CLIENTE INDEPENDIENTE	417
ANEXO C.1. CATEGORÍA BÁSICA.....	418
ANEXO C.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS	418
ANEXO C.1.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA BÁSICA.....	427
ANEXO C.2. CATEGORÍA MEDIA	462
ANEXO C.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS	462
ANEXO C.2.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA MEDIA	473
ANEXO C.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA.....	513

ANEXO C.3.1.	PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	513
ANEXO C.3.2.	LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA	526
ANEXO C.3.3.	IMPLEMENTACIÓN DE BITLOCKER PARA CIFRADO DE DISCO EN CLIENTES WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	564
ANEXO C.4.	TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	576
ANEXO C.4.1.	IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA	576
ANEXO C.4.2.	CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA WINDOWS 10 INDEPENDIENTE	584
1.	CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 INDEPENDIENTES	584
2.	CONFIGURACIÓN DE OPCIÓN DE MANTENIMIENTO PARA WINDOWS 10 INDEPENDIENTE ...	585
3.	DESINSTALACIÓN DE APPS (UWP) EN WINDOWS 10.....	587
3.1.	IDENTIFICACIÓN DE APPX INSTALADAS	587
3.2.	ELIMINACIÓN DE APPX PROVISIONADAS E INSTALADAS.....	588
4.	ACTIVACIÓN DE TIENDA DE WINDOWS PARA CLIENTES WINDOWS 10 INDEPENDIENTES.....	590
5.	ACTIVACIÓN DE MICROSOFT ONEDRIVE PARA CLIENTES WINDOWS 10 INDEPENDIENTES	592
ANEXO C.4.3.	PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	593
1.	DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	594
2.	DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	595
3.	RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	597
ANEXO D.	CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN REDES CLASIFICADAS COMO CLIENTE INDEPENDIENTE	605
ANEXO D.1.	IMPLEMENTACIÓN SEGURA DE WINDOWS 10 COMO CLIENTE INDEPENDIENTE.....	607
ANEXO D.1.1.	PASO A PASO DE IMPLEMENTACIÓN SEGURA	607
1.	INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10	608
2.	CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10	624
ANEXO D.1.2.	LISTA DE COMPROBACIÓN PASO A PASO	648
ANEXO D.2.	APLICACIÓN DE NIVELES DE CLASIFICACIÓN	743
ANEXO D.2.1.	NIVEL DE CLASIFICACIÓN CONFIDENCIAL.....	743
ANEXO D.2.2.	NIVEL DE CLASIFICACIÓN RESERVADO O SUPERIOR.....	746
ANEXO D.3.	TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	748
ANEXO D.3.1.	CIFRADO DE DISCO CON BITLOCKER.....	748
1.	ALCANCE	748
2.	DESCRIPCIÓN DE USO DE ESTE ANEXO	749

3. REQUISITOS HARDWARE Y SOFTWARE.....	749
4. GUÍA PASO A PASO – BITLOCKER	750
5. LISTA DE COMPROBACIÓN – BITLOCKER	760
ANEXO D.3.2. USO DE DIFERENTES CONSOLAS DE ADMINISTRACIÓN TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19.....	762
ANEXO D.3.3. USO DE GRABADORA DE CD/DVD TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE	765
ANEXO D.3.4. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE	768
1. ADMINISTRAR DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES	768
1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB.....	769
1.2. DESINSTALACIÓN DE CONTROLADORES PARA IMPEDIR EL USO DE DISPOSITIVOS USB.....	776
2. ADMINISTRAR EL USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE EL IDENTIFICADOR DE DISPOSITIVO	778
2.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR.....	779
2.2. IMPEDIR EL USO DE DISPOSITIVOS USB	787
ANEXO D.3.5. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19	790
ANEXO D.3.6. CONFIGURACIÓN DE CLIENTE INDEPENDIENTE PARA PODER ACCEDER A UN RECURSO COMPARTIDO EN LA RED	795
ANEXO D.3.7. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	806
1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	806
2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	808
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	810

ANEXO A. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN EL ENS COMO CLIENTE INDEPENDIENTE

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un puesto de trabajo con el sistema operativo Microsoft Windows 10 1809 en su versión Enterprise con opción de mantenimiento LTSC según criterios del ENS.

Debido a las características de los puestos de trabajo a los que van dirigidas las guías de aplicación del Esquema Nacional de Seguridad, se toma la determinación de establecer la versión Microsoft Windows 10 Enterprise o Pro con las opciones de mantenimiento Canal Semi-Anual o Canal Semi-Anual (Dirigido) como las más adecuadas para su implementación, aunque en este anexo se contempla el uso de la versión Enterprise con opción de mantenimiento LTSC. Esto se basa en los siguientes condicionantes:

- a) Estos equipos pueden estar conectados a Internet por lo cual determinadas funcionalidades como la tienda o Cortana, pueden ser utilizadas o no, en función de las necesidades de cada organización.
- b) El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.
- c) Las opciones de mantenimiento permiten garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con Microsoft Windows. No obstante, deben considerarse siempre las actualizaciones de seguridad como un elemento esencial para garantizar la seguridad de los puestos de trabajo en cualquier infraestructura.

Además de esta determinación existen varias configuraciones que son desactivadas durante la aplicación del “ANEXO A.5.2 CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA WINDOWS 10 INDEPENDIENTE” para garantizar la securización del sistema. Dichas características son:

- a) Sistema Experiencia de Usuario. Este componente se encuentra limitado por la aplicación de la presente guía.
- b) Sistema de telemetría. La configuración de telemetría de la organización deberá establecerse en función de las necesidades y acuerdos establecidos para la misma. En los pasos a paso existentes en los Anexos, se detallará el proceso para que pueda establecer el nivel de telemetría de los sistemas MS Windows 10 existentes en su organización.

Por otro lado, Internet Explorer 11 podrá ser securizado según los mecanismos definidos en la guía CCN-STIC-520 destinada a redes clasificadas, y siguiendo la aplicación de la misma. Las políticas y configuraciones de dicha guía deberán ser adaptadas en función de las necesidades para asegurar el equipo cliente Microsoft Windows 10.

De manera análoga a lo citado anteriormente, el sistema podrá ser securizado con MS Office 2016 según los mecanismos definidos en la guía CCN-STIC-585, y siguiendo la aplicación de la misma. Las políticas y configuraciones de dicha guía deberán ser adaptadas en función de las necesidades para asegurar el equipo cliente Microsoft Windows 10.

No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas, puedan ser modificadas para adaptarlas a sus necesidades operativas.

Se ha de tener en consideración que, en el caso del ENS, el sistema operativo Microsoft Windows 10 se asume instalado y por lo tanto no se dedica ningún apunte respecto a su proceso de instalación.

Nota: En este anexo se hace referencia a la nomenclatura de guía CCN-STIC-599B19. Esta nomenclatura corresponde a la aplicación de seguridad a través del presente anexo, y que se ha mantenido por compatibilidad con la versión anterior del documento.

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE MS WINDOWS 10 EN EL ENS

1. APLICACIÓN DE MEDIDAS EN MICROSOFT WINDOWS 10

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de clientes con Windows 10 y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande. En este último caso, por ejemplo, para la segregación de roles, se detallarán procedimientos y condiciones que deberá aplicar un operador de una organización para hacerlas efectivas.

Nota: Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará uso de la aplicación de medidas de seguridad descritas en el “ANEXO A.4 CATEGORÍA ALTA / DIFUSIÓN LIMITADA”.

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

- a) Aplicación de seguridad en clientes independientes, donde se realizará la ejecución de aplicaciones o el tratamiento de información sujetos al RD 3/2010 y se encontraran implementados con Windows 10.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para Windows 10, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema.

Esta guía por lo tanto no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean nativas al sistema operativo o las funcionalidades que el propio rol pueda aportar. Es factible en ello que se realicen referencias a soluciones de seguridad haciendo uso de antimalware para evitar el código dañino que como en el caso de MS Windows 10 vienen implementadas por el propio Sistema Operativo a través del software MS Windows Defender. No obstante, tal y como es lógico referenciar dicha implementación, y atendiendo a los requerimientos del ENS, requiere una administración centralizada que no aporta esta solución, cubriendo además solo uno de los aspectos requeridos por la medida de protección frente a código dañino.

Para un mejor entendimiento de las medidas éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a las categorías que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de las diferentes categorías de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso abarca todo el conjunto de acciones que bien preparatorias o ejecutivas orientadas a determinar qué o quién puede o no, acceder a un recurso del sistema, mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la comodidad de uso y la protección del sistema. De tal forma que la seguridad se irá incrementando en base a la categoría exigida. Así en la categoría básica se prima la comodidad y en las categorías altas se prima la protección.

1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN

Desde las categorías básicas debe especificarse mecanismos para garantizar la autenticidad y trazabilidad de las diferentes entidades. Esto se transforma generando una identificación singular para cada entidad: usuario, proceso o servicio. De esta manera siempre se podrá conocer quién recibe qué derechos y se puede saber qué ha hecho.

La identificación de usuario se traduce en la necesidad de crear cuentas únicas e inequívocas para cada usuario y servicio, a través de cuentas locales en los puestos de trabajo. Dichas cuentas deberán ser gestionadas de tal forma que deberán ser inhabilitadas cuando se dieran una serie de condicionantes:

- a) El usuario deja la organización.
- b) Cesa en la función para la cual se requería dicha cuenta.
- c) La persona que lo autorizó emite una orden en contra.

Debe tenerse en consideración que nunca deberán existir dos cuentas iguales de forma que estas no puedan confundirse o bien imputarse acciones a usuarios diferentes.

1.1.1.2. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde la categoría básica y atenderán a la necesidad que los recursos del sistema queden protegidos con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de los derechos de acceso suficientes.

Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad para la organización, a través de la persona responsable de dicha determinación y haciendo uso de las tecnologías necesarias.

Desde el punto de vista tecnológico, esta medida abarca un gran número de actividades, de tal forma que los puntos de control para restringir o conceder un acceso son abundantes. Acceder a un fichero o una carpeta o imprimir en un recurso, son acciones que pueden ser controladas y determinar para ello los permisos asignados.

La plantilla de seguridad recoge una serie de permisos que serán asignados con objeto de limitar las acciones por parte de usuarios y administradores. De esta forma y controlando los requisitos de acceso, se reducirán todos aquellos riesgos del uso habitual de administración de un puesto de trabajo.

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia. La siguiente dirección URL facilita la información que proporciona el fabricante sobre los controles y vigilancia de acceso para la familia Windows Server y Windows como sistema operativo cliente.

[https://msdn.microsoft.com/es-es/library/dn408189\(v=ws.11\).aspx](https://msdn.microsoft.com/es-es/library/dn408189(v=ws.11).aspx)

1.1.1.3. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS

Aplicable a partir de la categoría media, se considera un requerimiento importante para una organización la segregación de funciones en base a la actividad. De esta forma se establece cadenas de autorización y control enfocadas a evitar la existencia de una única persona autorizada y que ésta pueda abusar de sus derechos para cometer alguna acción ilícita.

Desde el punto de vista formal la segregación de funciones deberá realizarse al menos para las siguientes tareas:

- a) Desarrollo de operación.
- b) Configuración y mantenimiento del sistema de operación.
- c) Auditoría o supervisión de otra función.

Dichos procesos de segregación son factibles realizarlos a través de los propios mecanismos que proporciona Windows 10, así como las funcionalidades implicadas en la presente guía.

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura y puesta en marcha de la guía “CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2”. Aunque será mencionada a lo largo de la presente guía en relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en Windows Server 2008 R2 y Windows 7, a través del sistema de Suscripción de eventos con el que Microsoft dotó a Windows Server 2008 R2 y a Windows 7.

1.1.1.4. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Altamente vinculado al punto 1.1.1.2 OP. ACC. 2. REQUISITOS DE ACCESO, estas medidas requieren consolidación de los derechos de acceso, de tal forma que:

- a) Exista la aplicación del mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para poder cumplir las obligaciones.
- b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
- c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

Como ya se comentó previamente, Windows 10 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Adicionalmente y siguiendo uno de los principios fundamentales de mínimo privilegio posible, a través de la aplicación de la presente guía se activarán las condiciones de control de cuenta de usuario, aparecidas con Windows Vista y mejorada la experiencia de usuario y funcionalidad en Windows 10 y Windows Server 2012 R2, este componente debe entenderse como un mecanismo para impedir que el trabajo directo con usuarios con privilegios de administrador, repercuta negativamente en la seguridad, a acometer todas las acciones con el máximo privilegio cuando este no es siempre requerido.

Así en la navegación a Internet, acceso a recurso o tratamientos ofimáticos por citar algunos ejemplos frecuentes, un usuario no requiere del privilegio de administrador para desempeñarlo. Así y sin darse cuenta podría estar poniendo en grave riesgo la seguridad del sistema al tratar ficheros, ejecutables, componentes y otros, que descargados de Internet u otras fuentes de dudosa confianza con máximos privilegios.

El control de cuentas de usuarios (UAC) nace con la clara idea de hacer factible que un administrador sea consciente de cuando una acción requiere un privilegio. Así y en toda la sesión el usuario “administrador” se convierte en un mero usuario estándar salvo cuando el sistema requiere de forma consciente la necesidad de la elevación.

Puesto que las condiciones de funcionalidad de UAC, pueden establecerse desde la usabilidad hasta la máxima seguridad y atendiendo a los criterios marcados por el propio Esquema Nacional de Seguridad, las diferentes plantillas de seguridad que se generan para las diferentes categorías atenderán a estos criterios de criticidad. No obstante, y aunque se detallará más adelante, el operador puede conocer la funcionalidad del mecanismo de UAC a través de la información facilitada por el propio fabricante:

[http://technet.microsoft.com/es-es/library/cc731416\(v=ws.10\).aspx](http://technet.microsoft.com/es-es/library/cc731416(v=ws.10).aspx)

<https://docs.microsoft.com/es-es/windows-server/security/user-account-control/how-user-account-control-works>

De esta forma el principio de mínima exposición y menor privilegio se puede materializar de forma extensiva a los propios administradores de los servidores y servicios que gestiona la organización.

1.1.1.5. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Dentro de los procesos habituales en el manejo de los sistemas de la información, el correspondiente a la autenticación, corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema “quién eres”.

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes generalidades estos serán:

- a) Para la categoría básica se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, dispositivos físicos (en inglés “Tokens”), sistemas de biometría o certificados digitales entre otros.
- b) Para la categoría media se desaconseja el empleo de contraseñas o claves concertadas, siendo recomendable el uso de sistemas físicos (Tokens), biométricos o certificados digitales.
- c) Para la categoría alta, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige para ello el uso de dispositivos físicos o de biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-807 de criptología de empleo en el ENS.

Conforme a las necesidades establecidas por el Esquema Nacional de Seguridad se deberá tener también en consideración lo establecido en la guía CCN-STIC-804 para los mecanismos de autenticación y que se encuentra recogido en el punto 4.2.5.

La presente guía tiene en consideración los siguientes aspectos, para el desarrollo de plantillas de seguridad por categorías, enfocados en los procesos de autenticación:

- a) Gestión y definición de política de contraseñas.
- b) Gestión y definición de política para los bloqueos de cuenta.
- c) Implementación de algoritmos para el almacenamiento de contraseñas cifradas.
- d) Implementación de mecanismos para el bloqueo de cuentas de usuario y de servicio.
- e) Permisividad para el empleo de mecanismos de algoritmos y criptografía basados en biometría, certificados o tarjetas inteligentes.

Debe tenerse en consideración que Windows 10 basan la implementación de los sistemas de autenticación en el empleo de contraseñas o bien en el uso de Microsoft Passport como una mejora en los sistemas de autenticación. No obstante, los proveedores de credenciales con los que cuenta Windows 10 extienden los mecanismos de autenticación de Microsoft herederos de la antigua GINA (Graphic Identification and Autentication). Estos proveedores facultan la capacidad de introducir en los sistemas operativos, mecanismos de autenticación que se adapten a cualquiera de las necesidades que pueden existir ahora y en el futuro.

Windows 10 a través de proveedores criptográficos determinados tiene además la capacidad además de introducir la capacidad de autenticación multifactor, como puede ser el empleo de un sistema de biometría y otro de tarjeta inteligente. Windows Hello y especialmente Microsoft Passport cubren estas necesidades. Puede encontrar más información sobre Microsoft Passport en la siguiente dirección URL:

[https://technet.microsoft.com/es-es/library/mt589441\(v=vs.85\).aspx](https://technet.microsoft.com/es-es/library/mt589441(v=vs.85).aspx)

1.1.1.6. OP. ACC. 6. ACCESO LOCAL

Se considera acceso local aquel que se ha realizado desde los puestos dentro de las propias instalaciones que tiene la organización.

El Esquema Nacional de Seguridad, tiene en cuenta la aplicación de medidas diferentes atendiendo a la criticidad de servicios y sistemas. Así en función de la categoría de seguridad deberán aplicarse medidas para:

- a) En la categoría básica, se prevendrán ataques para evitar intentos de ataques reiterados contra los sistemas de autenticación. Adicionalmente la información proporcionada en caso de fallo en el acceso deberá ser mínima, siendo este hecho especialmente crítico en las aplicaciones web. También deberán registrarse los intentos satisfactorios y erróneos, así como la de informar a los usuarios de las obligaciones.
- b) En la categoría media será exigencia el proporcionar al usuario el detalle de la última vez que se ha autenticado.
- c) En la categoría alta deberán existir limitaciones para la fecha y hora en la que se accede. También se facilitará mediante identificación singular la renovación de la autenticación, no bastando el hecho de hacerlo en la sesión iniciada.

Windows 10 a través de la aplicación de políticas de grupo (GPO) permite establecer mecanismos para garantizar bloqueos de cuenta, proporcionar información al usuario, así como establecer medidas para garantizar un cambio seguro de las credenciales. Estas serán aplicadas de forma progresiva en función de la categoría de seguridad exigida.

Para los sistemas de auditoría como en el caso previo se remite al operador a la guía CCN-STIC-859 de gestión y consolidación de registros de seguridad. Allí se detallan los procesos tanto para habilitar los registros de auditoría que serán aplicados por políticas de seguridad, así como los procesos para recogerlos e interpretarlos.

1.1.1.7. OP. ACC. 7. ACCESO REMOTO

Las organizaciones deberán mantener las consideraciones de seguridad en cuanto al acceso remoto cuando éste se realice desde fuera de las propias instalaciones de la organización a través de redes de terceros. Estas organizaciones deberán garantizar la seguridad, tanto en el propio acceso en sí, como en el canal del acceso remoto.

Windows 10 faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación. Sin embargo, no todos los protocolos empleados históricamente por los productos de Microsoft se pueden considerar a día de hoy seguros. La presente guía tiene en consideración estos detalles y por lo tanto habilitará o deshabilitará en su defecto aquellos protocolos que son considerados seguros o no, incluido en ello los correspondientes a autenticaciones empleadas en redes locales o remotas.

1.1.2. EXPLOTACIÓN

Se incluyen en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define a través de ellas una serie de procesos tanto para el control, como para la gestión que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Los equipos antes de su entrada en producción, deberán configurarse de tal forma que:

- a) Se retiren cuentas y contraseñas estándar.
- b) Se aplicará la regla de mínima funcionalidad.

Se considera indispensable que el sistema no deberá proporcionar funcionalidades gratuitas. Solamente las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello se eliminarán o desactivarán mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias e incluso aquellas que sean inadecuadas para el fin que se persigue.

Para el cumplimiento de este sentido las diferentes plantillas de seguridad, se dotarán de las funcionalidades necesarias para deshabilitar y configurar todos aquellos servicios que, no siendo necesarios para ningún entorno operativo, pudieran constituir un riesgo de seguridad. Adicionalmente se protegerán los más importantes de tal forma que quedarán configurados a través de las políticas de grupo que correspondieran por categorías. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

Adicionalmente la guía configurará a través de objetos GPO o bien mostrará mecanismos de administración adicionales para configurar nuevos componentes de MS Windows con objeto de reducir la superficie de exposición, así como limitar la información remitida hacia Internet.

1.1.2.2. OP. EXP. 4. MANTENIMIENTO

Para mantener el equipamiento físico y lógico se deberán atender a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas. Se realizará un seguimiento continuo para garantizar la seguridad de los sistemas. Para ello deberá existir un procedimiento que permita analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

En este sentido la presente guía sigue los patrones establecidos por Microsoft como fabricante de Windows 10. Debe tenerse en consideración que este Sistema Operativo es un elemento en constante evolución, donde ante la aparición de un riesgo de seguridad deberá dotar de los mecanismos necesarios para paliar el problema. Para ellos Microsoft hace una constante difusión de actualizaciones de seguridad que deberá evaluar e implementar sobre los servidores, con objetos de mantener las garantías de seguridad necesarias.

Adicionalmente a las actualizaciones de seguridad, debe tomar en consideración que el Sistema Operativo Windows 10 inaugura una nueva metodología basada en la revisión continua del sistema. Dicha revisión incluye nuevas funcionalidades y características al sistema. Las opciones de mantenimiento reflejan los tiempos máximos que tendrá la organización para mantener actualizado el sistema. No debe confundir no obstante dichas actualizaciones de funcionalidad con las actualizaciones tradicionales de seguridad. Un sistema con la opción CBB, seguirá recibiendo las actualizaciones de seguridad dentro del ciclo natural de publicación de las mismas.

Para ello deberá diferenciar los siguientes tipos de actualizaciones:

- a) Feature updates.
- b) Quality updates.

Las actualizaciones de funcionalidad tienen una entrega más frecuente que en revisiones previas de Windows. Se estima 2 o 3 cada año en lugar de una cada 3 o 5 años como estaba sucediendo hasta ahora.

Las actualizaciones de calidad vienen a subsanar un problema que tenían muchas organizaciones. Las actualizaciones mensuales en versiones anteriores de Windows resultaban abrumadora debido a la gran cantidad de actualizaciones disponibles cada mes. Muchas organizaciones elegían selectivamente cuales aplicaban y cuáles no. Esto creó un sinnúmero de escenarios en los que las organizaciones implementan actualizaciones de seguridad esenciales, pero sólo un subconjunto de correcciones que no eran de seguridad.

En Windows 10, en lugar de recibir varias actualizaciones cada mes, verán una actualización mensual acumulativa que reemplaza la actualización del mes anterior. Ésta contendrá tanto la seguridad y como las correcciones no relacionadas con la seguridad.

Recuerde por lo tanto que deberá atender no solo a las especificaciones del fabricante en cuanto a las actualizaciones de seguridad, sino también a las actualizaciones que incluyen las mejoras de funcionalidad. También es importante atender a los cambios producidos a partir de octubre de 2016 cuando las actualizaciones de funcionalidad y de seguridad se agrupan en una única actualización mensual.

Nota: No es un objetivo de esta guía especificar los mecanismos o procedimientos necesarios para mantener los sistemas actualizados. Las plantillas de seguridad configuran las directivas adecuadas para que los sistemas operativos puedan ser actualizados empleando para ello el servicio de actualizaciones de Microsoft, existente en Windows 10.

1.1.2.3. OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La organización para puestos de trabajo deberá implementar una solución que proteja contra código dañino. Se considerarán como tal los virus, gusanos, troyanos, programas espías y en general cualquier tipo de aplicación considerada como código dañino.

Debe tomarse en consideración que, aunque Windows 10 tenga implementada de forma predeterminada la solución Windows Defender, ésta no cubre todo el espectro de protección frente a código dañino. Por ejemplo sin una solución de administración centralizada como la aportada por MS System Center 2012 Endpoint Protection o la de otros fabricantes no tendrá la visibilidad para hacer la gestión centralizada de la seguridad y gestión de incidencias demandadas por el Esquema Nacional de Seguridad.

Adicionalmente este producto en sí mismo no ofrece un mecanismo de protección con administración centralizada, objetivo fundamental de toda organización no solo para centralizar los procesos de despliegue y configuración de políticas de protección, sino de la centralización de los estados y reportes de detección y eliminación de código dañino que ofrezca un alcance completo en la detección y eliminación de código dañino, así como atender a las recomendaciones del fabricante para su mantenimiento.

1.1.2.4. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS

Aplicable en las categorías básica, media y alta de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

- a) Quién realiza la actividad, cuándo la realiza y sobre qué.
- b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.
- c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.
- d) La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.
- e) La categoría alta requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

Windows 10, implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que de forma predeterminada los datos son almacenados localmente. Existen no obstante mecanismos nativos para la suscripción y recolección de evento. Ya comentado previamente, la guía CCN-STIC-859 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoría desde múltiples sistemas, permitiendo establecer así mecanismos de correlación.

1.1.2.5. OP. EXP. 10. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

En las categorías media y alta se deberán implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:

- a) Determinar el período de retención de los registros.
- b) Asegurar la fecha y hora.
- c) Permitir el mantenimiento de los registros sin que estos puedan ser alterados o eliminados por personal no autorizado.
- d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

Nuevamente en la guía CCN-STIC-859 se articulan los mecanismos para garantizar la disponibilidad y retención de los registros, así como los procedimientos operativos para su salvaguarda.

1.2. MEDIDAS DE PROTECCIÓN

Este conjunto de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que se incluye una gran variedad de las mismas que son aplicables desde las más puramente procedimentales, a las puramente físicas o a las de aplicación técnica.

Solo estas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado son de aplicación sobre las funcionalidades del propio sistema operativo servidor. La mayor parte de ellas son de aplicación en la red o cuando un sistema tipo portátil sale de la organización, cuestión que no se considera de aplicación a un servidor que se considera ubicado en un entorno estable dentro del centro de procesamiento de datos (CPD) que tuviera la organización.

Se considera en este sentido que la organización ha dispuestos todos aquellos mecanismos de control físico necesarios, con objeto evitar el acceso a los equipos de escritorio existentes por parte de personal no autorizado.

1.2.1. PROTECCIÓN DE LOS EQUIPOS

Las medidas de protección de los equipos cubren todos aquellos mecanismos que son necesarios para garantizar tanto una configuración de seguridad válida para el sistema, así como para mantener la propia privacidad del trabajo desarrollado.

Dentro de las medidas se articulan la aplicación de mecanismos de índole tecnológica y otras de tipo física. Entre estas últimas, pueden localizarse las correspondientes a un puesto de trabajo despejado.

Aunque esta guía de seguridad se encuentra orientada a un sistema operativo de escritorio, se tiene en consideración aquellas medidas que, siendo establecidas para un puesto de trabajo, le son de completa aplicación, por ejemplo, la necesidad de realizar un bloqueo del puesto de trabajo.

1.2.1.1. MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO

Aplicable desde la categoría media se establece la necesidad de realizar un bloqueo de la cuenta toda vez que se haya producido una inactividad en el sistema tras un tiempo prudencial. Dicho tiempo prudencial deberá ser establecido por política de seguridad:

Adicionalmente a todos aquellos sistemas de categoría alta, deberán cancelarse las sesiones abiertas, cuando se supere un tiempo de actividad superior al anteriormente planteado.

Estos controles serán aplicables a Windows mediante la implementación de objetos de política de grupo local en el equipo.

1.2.1.2. MP. EQ. 3. PROTECCIÓN DE LOS PORTÁTILES

Los equipos que salgan fuera de las instalaciones donde opere la organización y por lo tanto no puedan beneficiarse de las medidas de protección física que éstas ofrezcan, deberán ser protegidos frente a riesgos de pérdida o robo.

Como condición general a partir de la categoría básica, los sistemas portátiles, deberán ser identificados e inventariados. Deberá asimismo de proporcionarse de un mecanismo de comunicación de incidencias frente a pérdidas o sustracciones de los mismos.

En dicho procedimiento deberán consignarse mecanismos para las bajas de cuentas, inclusive aquellas que permitan conexiones remotas desde el equipo perdido o sustraído. Para ello deberá asimismo consignarse un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el equipo se conecte a redes, en particular si el equipo se conecta a redes públicas.

Para aquellos sistemas portátiles que manejen información considerada como de categoría alta según las definiciones de la categoría del ENS, deberán disponerse de mecanismos de cifrado que permitan la confidencialidad de los datos almacenados.

Existen en el mercado numerosas soluciones que permiten el cumplimiento de esta medida recogida para categorías altas de información en el RD 3/2010. Windows 10 en sus versiones Enterprise y Pro permite el uso de la solución de BitLocker como mecanismos para garantizar la confidencialidad de los datos. La presente guía recoge los mecanismos para el cifrado de unidades con BitLocker en el ANEXO A.4.3.IMPLEMENTACIÓN DE BITLOCKER PARA CIFRADO DE DISCO EN CLIENTES WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS. Todo aquel operador que quiera realizar la implementación de BitLocker en Microsoft Windows 10 podrá consultar de forma adicional todos los detalles al respecto a través del siguiente enlace.

<https://technet.microsoft.com/en-us/itpro/windows/keep-secure/bitlocker-overview>

1.2.2. PROTECCIÓN DE LAS COMUNICACIONES

Los conjuntos de medidas orientadas a la protección de las comunicaciones tienen como objetivo la protección de la información en tránsito, así como dotar a los mecanismos para la detección y bloqueo de intrusos en una red.

1.2.2.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD

Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberá prevenirse ataques activos, garantizando que los mismos serán al menos detectados, permitiendo activarse los procedimientos que se hubieran previsto en el tratamiento frente a incidentes.

En aquellos sistemas que les sea de aplicación la categoría media, además de los mecanismos anteriores aplicables a la categoría básica, les será de aplicación la necesidad de implementar redes virtuales privadas cuando su comunicación se realice por redes fuera de la organización. Para ello se deberá tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

Para aquellos entornos con sistemas o información catalogados como de categoría alta, es recomendable el empleo de dispositivos hardware para el establecimiento y utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberá tener en consideración los productos que se encuentran certificados y acreditados.

A través de controles centralizados en plantillas de seguridad, se establecerán mecanismos que controlen el acceso y salida de información a los puestos de trabajo mediante el empleo del firewall en su modalidad avanzada. Aunque se tratará en extensión en un anexo de la presente guía, el operador podrá conocer todos los detalles de esta solución a través de la información que proporciona el fabricante:

[http://technet.microsoft.com/es-es/library/cc748991\(v=ws.10\).aspx](http://technet.microsoft.com/es-es/library/cc748991(v=ws.10).aspx)

Nota: Aunque se proporciona una configuración base del firewall de Windows con la presente guía, el administrador deberá aplicar y gestionar los perfiles y reglas del firewall acorde a las necesidades de su organización, prevaleciendo como regla primordial la mínima exposición hacia el exterior del equipo que se configura.

Además, se establecerán por políticas de grupo los controles relativos a la protección de la autenticación, habilitando solo aquellos protocolos que son válidos y seguros.

1.2.3. PROTECCIÓN DE LA INFORMACIÓN

Conjunto de procesos y medidas para un correcto uso y salvaguarda de los datos de carácter personal identificados en el sistema.

1.2.3.1. MP. INFO. 3. CIFRADO

Se debe asegurar la integridad de la información con una categoría alta de confidencialidad cifrada tanto durante su almacenamiento como durante su transmisión

Solo será visible en claro dicha información cuando se esté realizando uso de ella.

La presente guía establece mecanismos a través de BitLocker para garantizar el cifrado de los datos existentes en los sistemas.

Las políticas GPO asignables en la presente guía estable la implementación de los algoritmos más seguros posibles que garanticen la integridad y confidencialidad de los datos transmitidos dentro de la red de área local.

Deberá adicionalmente aplicar mecanismos que garanticen el cifrado de comunicaciones cuando acceda a servicios e información de la organización de forma remota cuando esté fuera de ella.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN MICROSOFT WINDOWS 10

A continuación, se establece un cuadro resumen con las diferentes medidas a aplicar, así como los mecanismos que se implementarán para su aplicación. Dichas implementaciones podrán provenir de la revisión de otras guías de seguridad de la serie CCN-STIC-500, o bien por la aplicación de políticas de seguridad a nivel local.

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de mecanismos articulados en la guía CCN-STIC-870A, adaptándolos a la organización.
OP. ACC. 1	Auditoría y supervisión de actividad	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de mecanismos articulados en la guía CCN-STIC-870A, adaptándolos a la organización.
OP. ACC. 4	Control de cuentas de usuario	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 5	Política de contraseñas	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 5	Protocolos de autenticación local	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 6	Bloqueo de cuentas	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. ACC. 7	Protocolos de autenticación en red	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Implementación de GPO a través de plantillas facilitadas en la presente guía. Configuraciones adicionales de seguridad descritas a través de la presente guía.
OP. EXP. 2	Protección de aplicaciones de sistema para garantizar el principio de mínima funcionalidad.	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 4	Mantenimiento del Sistema Operativo	Configuraciones adicionales descritas a través de la presente guía. Deberá implementar mecanismos en su organización para garantizar la actualización de los sistemas y aplicaciones.
OP. EXP. 6	Protección frente a código dañino	La organización deberá emplear una solución adicional a Windows Defender que proporciona Windows 10 por no cubrir este los mínimos exigidos por el ENS para la protección frente a código dañino.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica.

Control	Medida	Mecanismo de aplicación
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica.
MP. EQ. 2	Bloqueo de los puestos de trabajo	Implementación de GPO a través de plantillas facilitadas en la presente guía.
MP. EQ. 3	Protección de portátiles	Adicionalmente a otras soluciones existentes en el mercado Windows 10, en sus versiones Pro y Enterprise, proporciona mecanismos para garantizar la confidencialidad de los datos. La configuración de BitLocker puede realizarse a través de la implementación de GPO.
MP. COM. 3	Protección del sistema mediante implementación de firewall.	Implementación de GPO a través de plantillas facilitadas en la presente guía. Implementación de configuración de firewall avanzado a nivel local según ANEXO A.5.1 en la presente guía.
MP. COM. 3	Protección de la autenticación.	Implementación de GPO a través de plantillas facilitadas en la presente guía.
MP. SI. 2	Criptografía	Implementación de GPO a través de plantillas facilitadas en la presente guía.
MP. INFO. 3	Cifrado	Implementación de GPO a través de plantillas facilitadas en la presente guía.

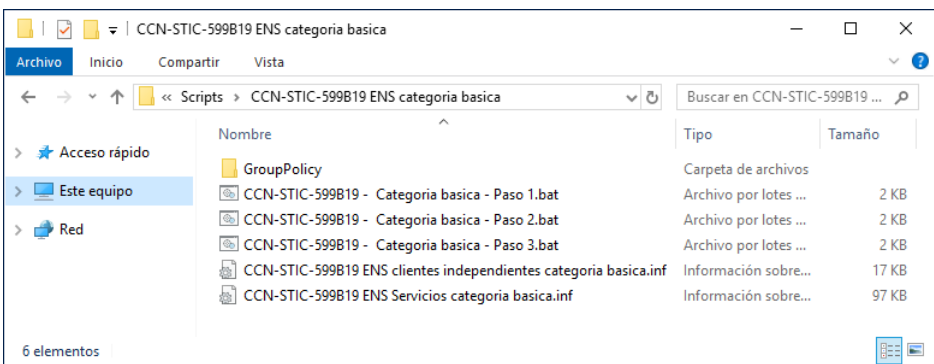
ANEXO A.2. CATEGORÍA BÁSICA

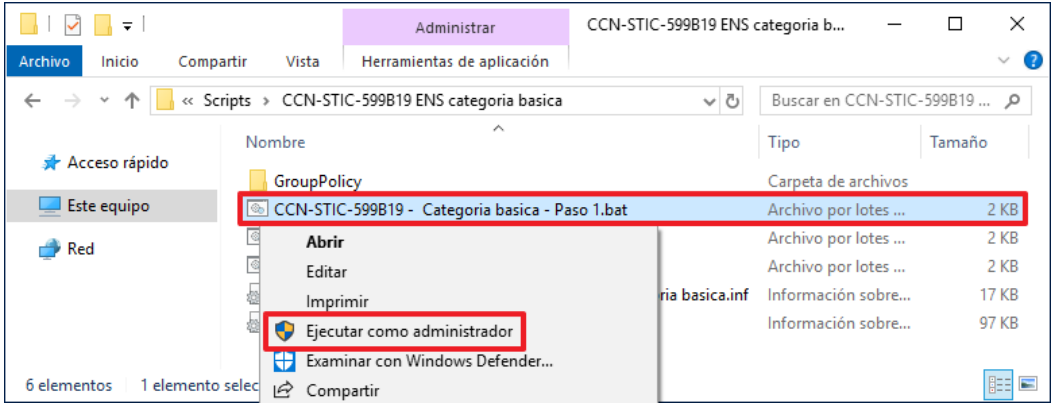
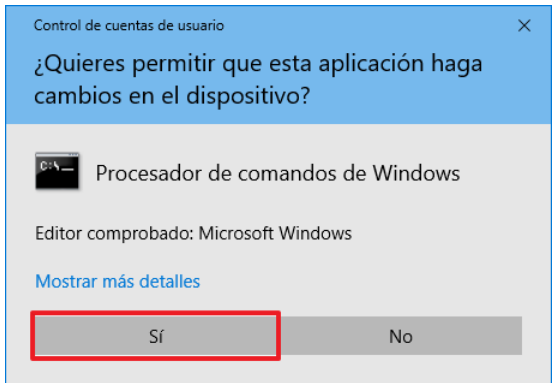
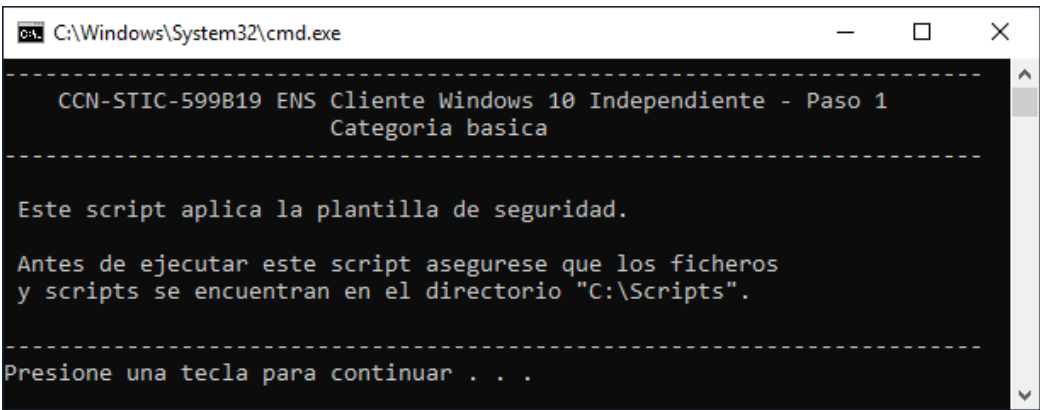
ANEXO A.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

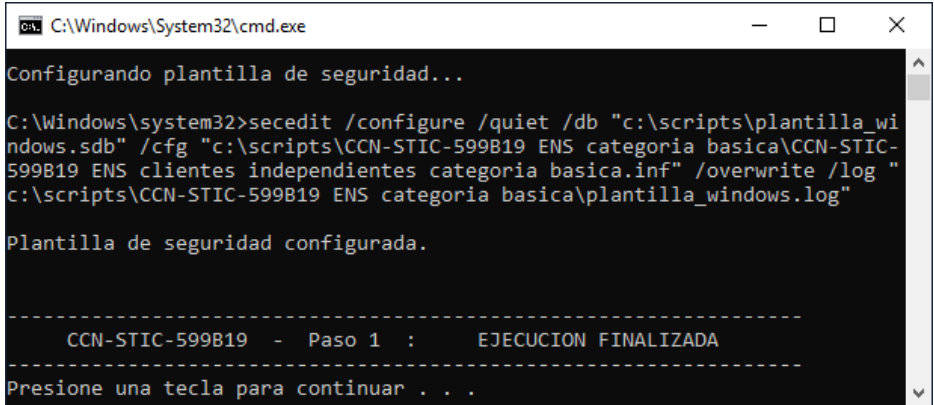
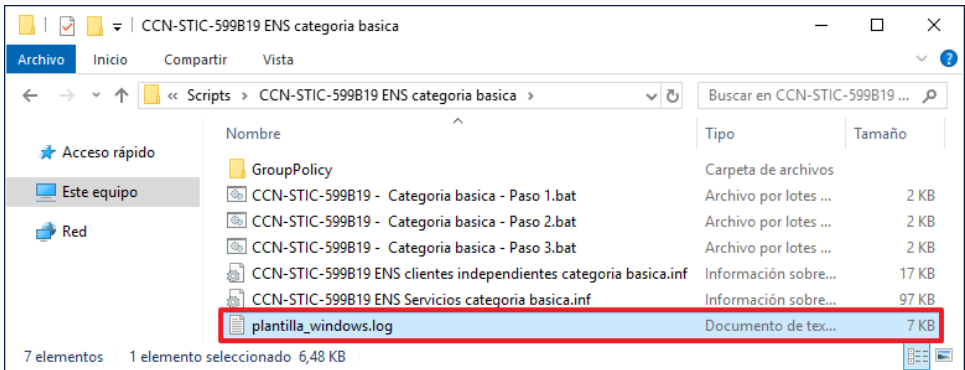
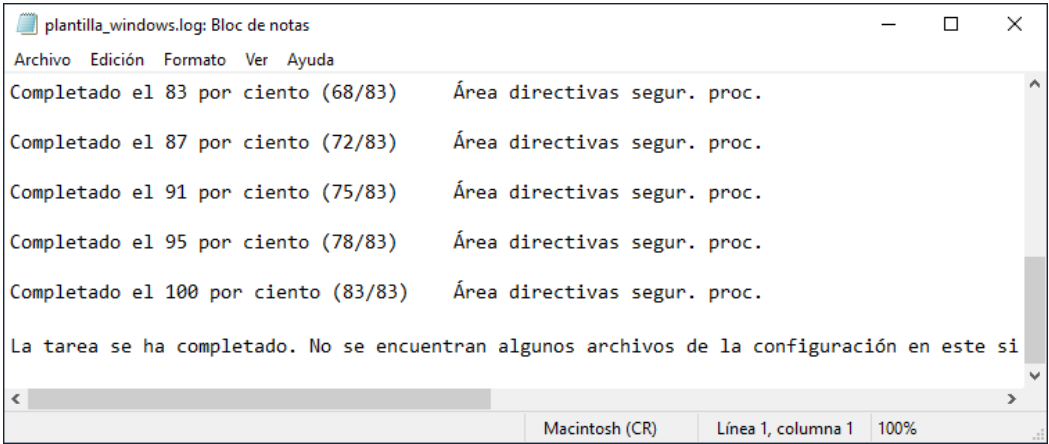
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes Windows 10 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

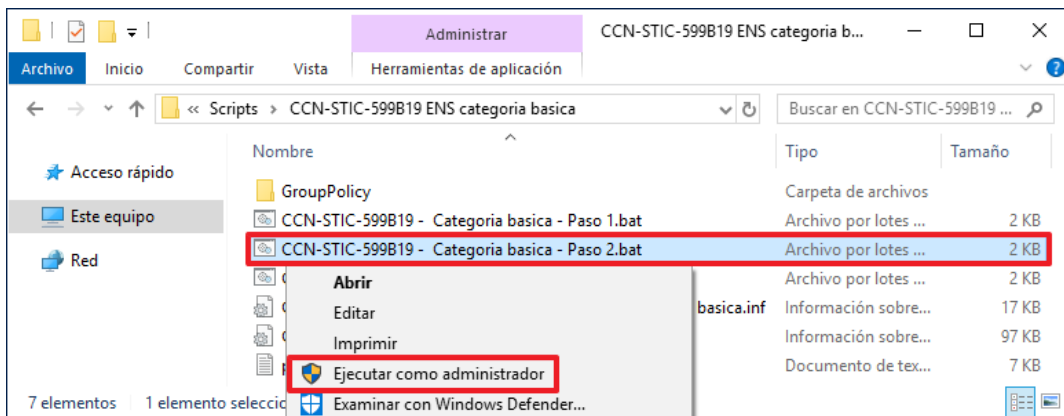
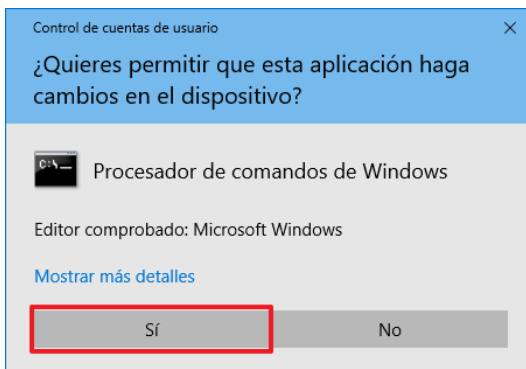
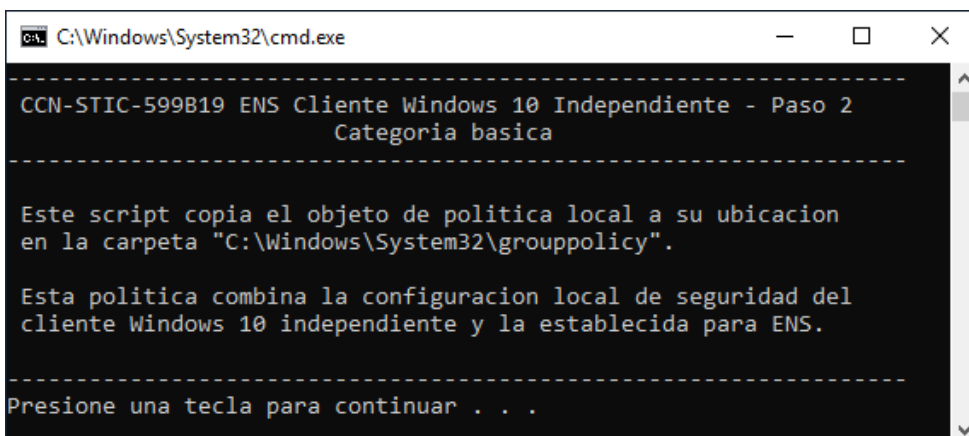
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Los pasos que se describen a continuación se realizarán en todos aquellos clientes Windows 10 Enterprise (versión 1809) con opción de mantenimiento LTSC, independientes a un dominio, que implementen servicios o información de categoría básica y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

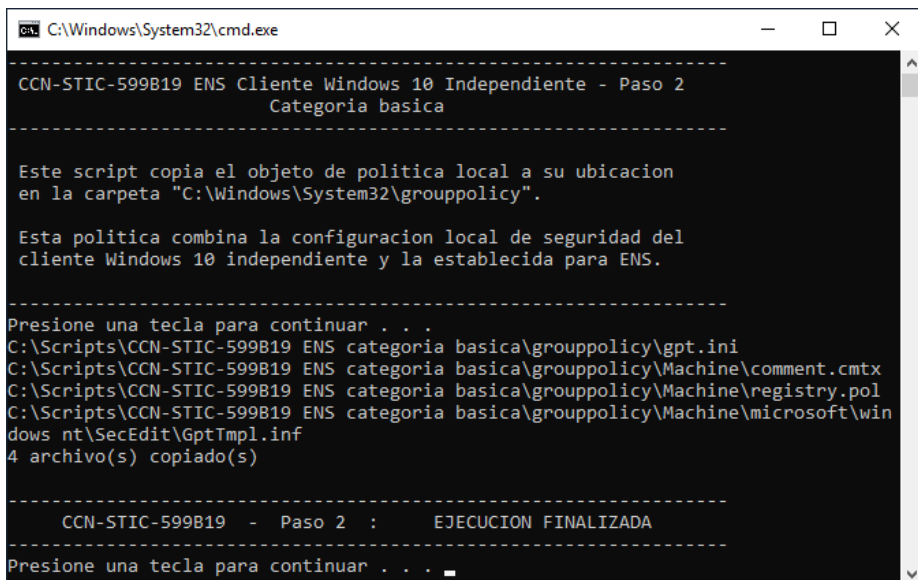
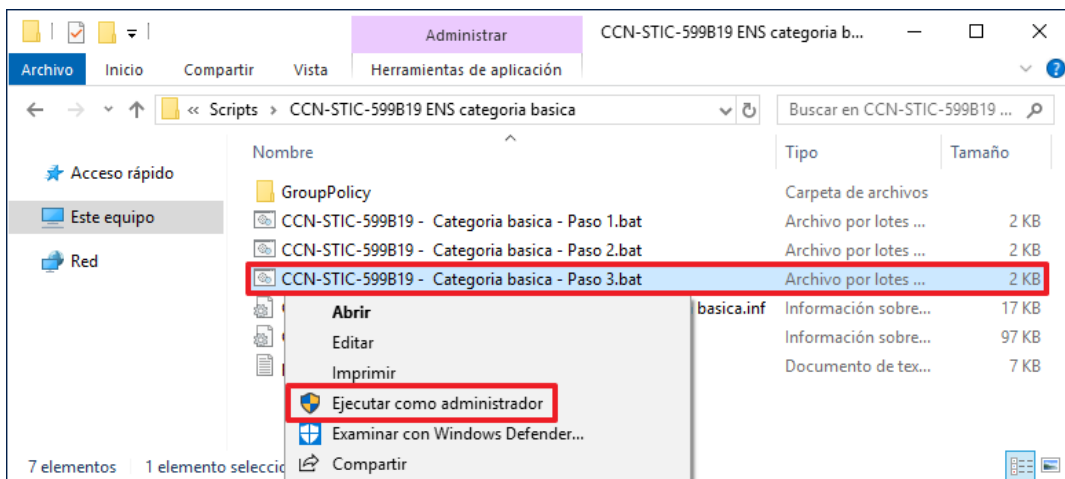
Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea administrador local.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en la ruta “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”.
5.	Abra la carpeta “CCN-STIC-599B19 ENS categoria basica” que encontrará en el directorio “C:\Scripts”.  Nota: Los scripts asumen que su ubicación es “C:\Scripts\CCN-STIC-599B19 ENS categoria basica”. De no ser así deberá modificar los scripts para que coincida con la ruta deseada.

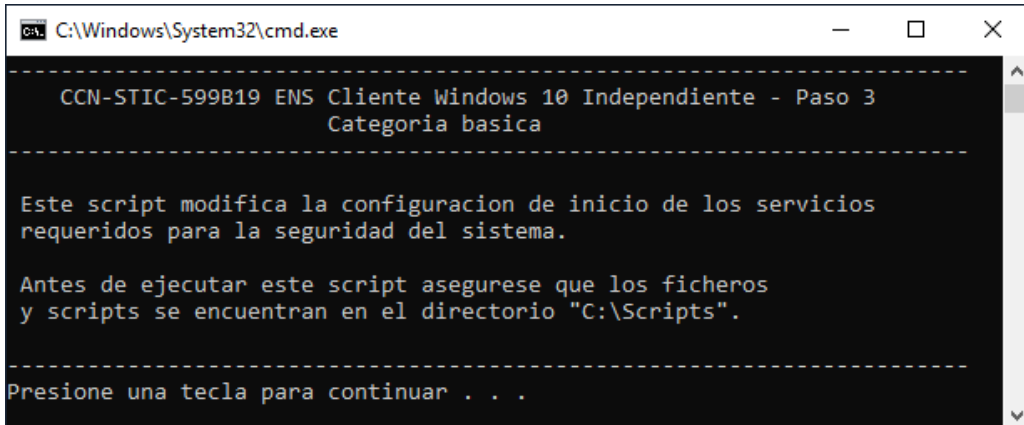
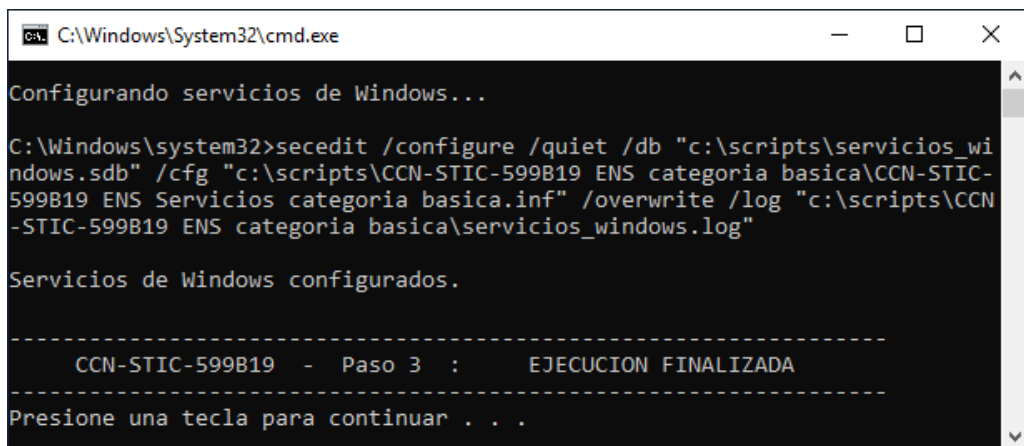
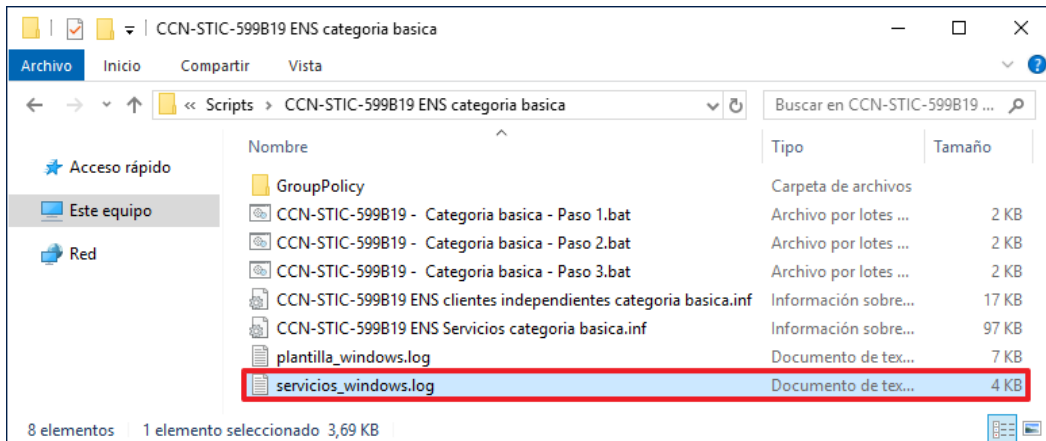
Paso	Descripción
6.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría básica – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”. 
7.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
8.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría básica del ENS. 

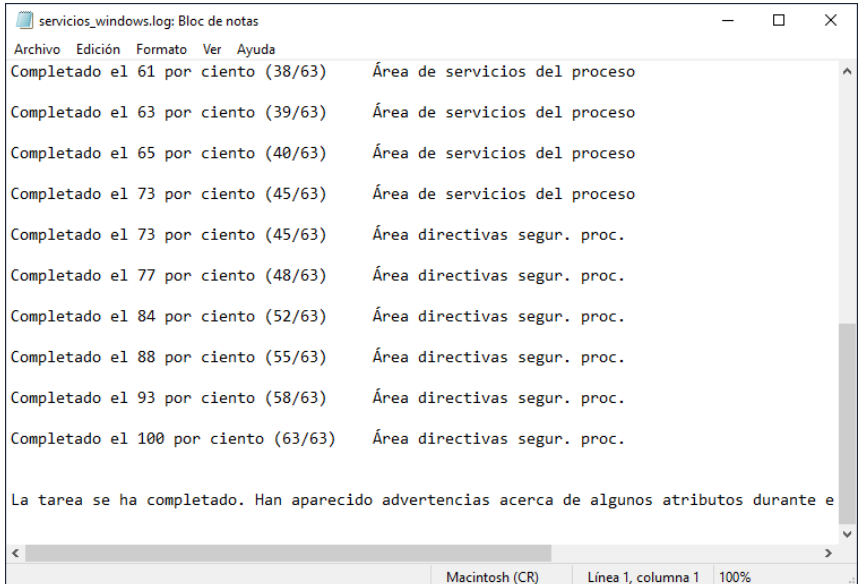
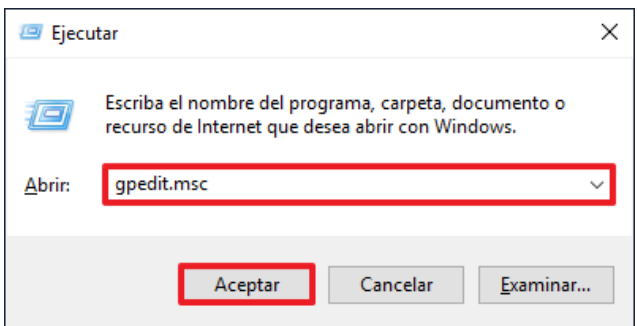
Paso	Descripción
9.	Una vez completado el proceso, deberá pulsar una tecla para continuar. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
10.	La ejecución del script genera un registro (log) en la carpeta "C:\Scripts\CCN-STIC-599B19 categoria basica" con el nombre "plantilla_windows.log". 
11.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el procedimiento desde el paso 6.

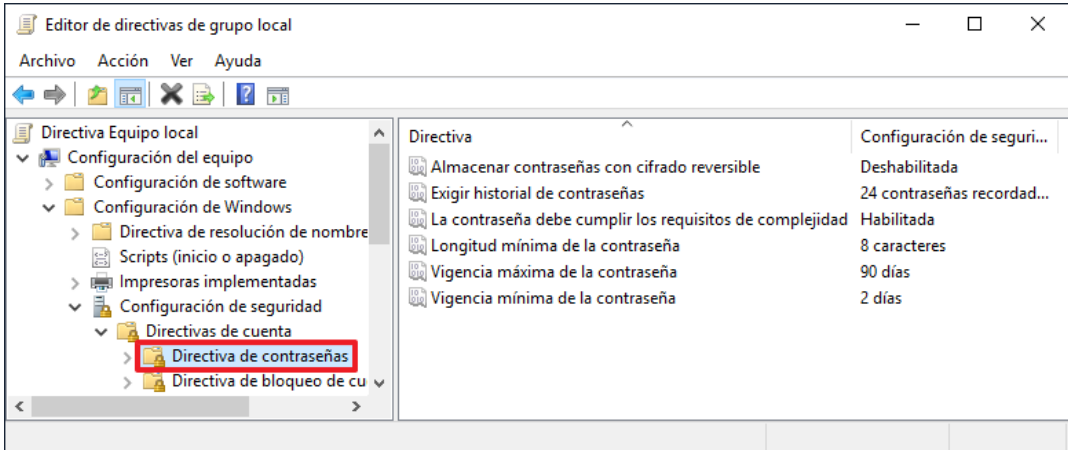
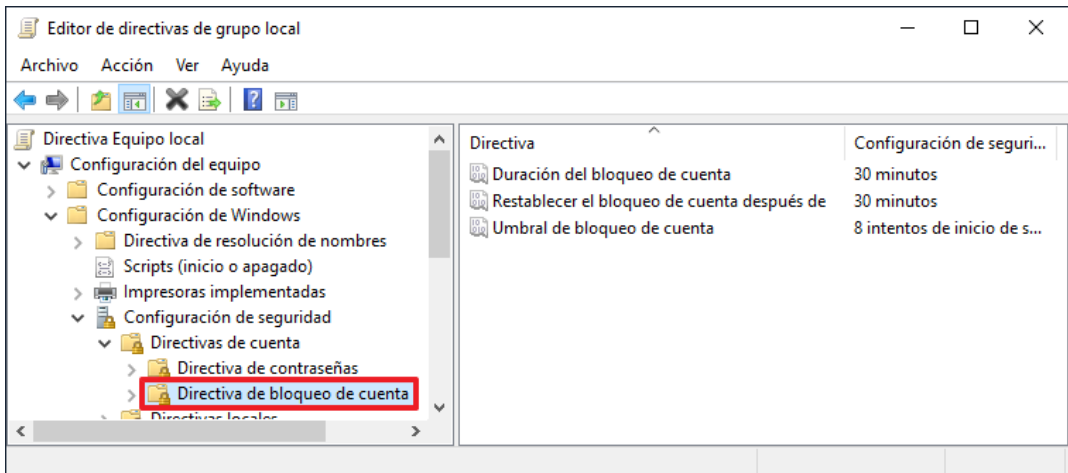
Paso	Descripción
12.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría básica – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”. 
13.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
14.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local. 



Paso	Descripción
15.	Completada la copia de los archivos, compruebe que no ha habido errores en la copia de los mismos. Debería obtener el mismo resultado que el mostrado en la siguiente imagen. Pulse una tecla para finalizar la ejecución del script.  Nota: En caso de haberse producido fallos, solúcelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.
16.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría básica – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”. 
17.	Pulse “S” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.

Paso	Descripción
18.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría básica del ENS. 
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 
20.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 ENS categoria basica” con el nombre de “servicios_windows.log”. 

Paso	Descripción
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados tal y como se muestra en la siguiente imagen.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el procedimiento desde el paso 16.
22.	Elimine la carpeta “C:\Scripts”.
23.	Es factible que su organización cuente con una política de contraseñas consolidada. La implementación de la política de categoría básica implementará una política específica para los clientes de categoría básica. Deberá evaluarla para determinar si esta configuración le es válida, o por el contrario deberá adaptarla a las condiciones de su organización.
24.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”. 
25.	Pulse “S” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.

Paso	Descripción
26.	Despliegue la política y sitúese en la siguiente ruta: “Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas” 
27.	Evalúe la política de contraseñas y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de credenciales es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
28.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que “Directiva de contraseñas”. 
29.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA BÁSICA

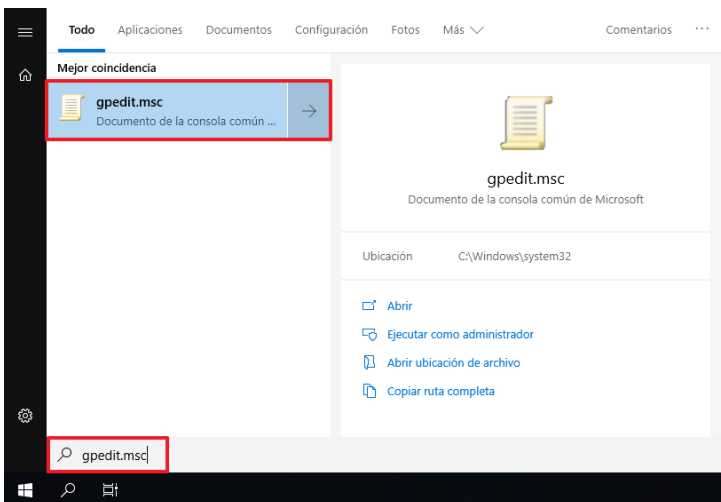
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO A.2.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS”.

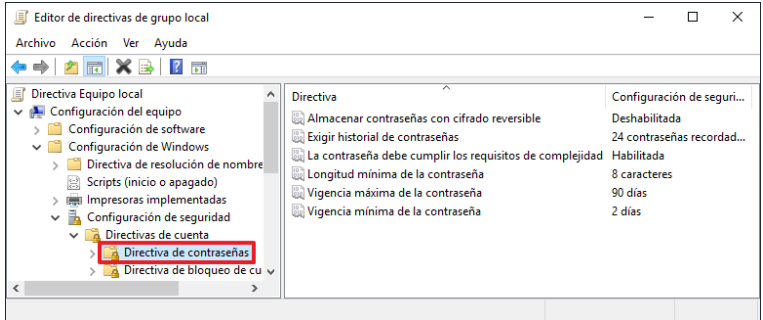
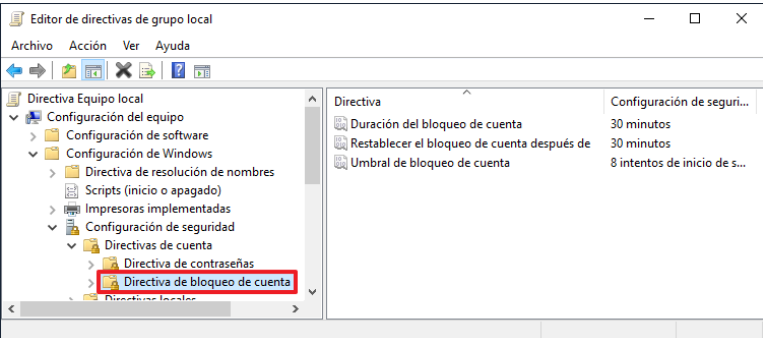
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes Windows 10 (versión 1809) Enterprise con opción de mantenimiento LTSC, independientes con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de administrador local.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario que es administrador local. Las consolas y herramientas que se utilizarán son las siguientes:

- Editor de objetos de directiva de grupo local (gpedit.msc).
- Editor de registro (regedit.exe).
- Visor de Eventos (eventvwr.exe).
- Servicios (services.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de administración local.
2. Inicie la aplicación de gestión de políticas locales.		Ejecute el “Editor de objetos de directiva de grupo local”. Para ello pulse “Inicio”, teclee “gpedit.msc” y pulse “Enter”. 

Comprobación	OK/NOK	Cómo hacerlo																					
3. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas” Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. 																					
		<table> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> <tr> <td>Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr> <tr> <td>Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr> <tr> <td>Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr> <tr> <td>Longitud mínima de la contraseña</td><td>8 caracteres</td><td></td></tr> <tr> <td>Vigencia máxima de la contraseña</td><td>90 días</td><td></td></tr> <tr> <td>Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr> </table>	Directiva	Valor	OK/NOK	Almacenar contraseñas usando cifrado reversible	Deshabilitada		Exigir historial de contraseñas	24 contraseñas recordadas		Las contraseñas deben cumplir los requisitos de complejidad	Habilitada		Longitud mínima de la contraseña	8 caracteres		Vigencia máxima de la contraseña	90 días		Vigencia mínima de la contraseña	2 días	
Directiva	Valor	OK/NOK																					
Almacenar contraseñas usando cifrado reversible	Deshabilitada																						
Exigir historial de contraseñas	24 contraseñas recordadas																						
Las contraseñas deben cumplir los requisitos de complejidad	Habilitada																						
Longitud mínima de la contraseña	8 caracteres																						
Vigencia máxima de la contraseña	90 días																						
Vigencia mínima de la contraseña	2 días																						
4. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta” 																					

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Duración del bloqueo de cuenta		30 minutos	
	Restablecer recuentos de bloqueo de cuenta tras		30 minutos	
	Umbral de bloqueo de cuenta		8 intentos de inicio de sesión no válidos	
5. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”		
	Directiva		Valor	OK/NOK
	Auditar el acceso a objetos		Correcto, Erróneo	
	Auditar el acceso del servicio de directorio		Correcto, Erróneo	
	Auditar el cambio de directivas		Correcto, Erróneo	
	Auditar el uso de privilegios		Correcto, Erróneo	
	Auditar eventos de inicio de sesión		Correcto, Erróneo	
	Auditar eventos de inicio de sesión de cuenta		Correcto, Erróneo	
	Auditar eventos del sistema		Correcto, Erróneo	
	Auditar la administración de cuentas		Correcto, Erróneo	
6. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: “Directiva Equipo Local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”		
	Directiva		Valor	OK/NOK
	Actuar como parte del sistema operativo		(Definida, pero sin ningún valor)	
	Administrar registro de seguridad y auditoría		Administradores	
	Agregar estaciones de trabajo al dominio		(Definida, pero sin ningún valor)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red
		Apagar el sistema	Administradores, Usuarios
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL, Usuarios
		Aumentar prioridad de programación	Administradores
		Bloquear páginas en la memoria	(Definida, pero sin ningún valor)
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores
		Cargar y descargar controladores de dispositivo	Administradores
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)
		Crear objetos globales	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL
		Crear un archivo de paginación	Administradores
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)
		Crear vínculos simbólicos	Administradores
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados
		Denegar el inicio de sesión como servicio	Invitados
		Denegar el inicio de sesión como trabajo por lotes	Invitados
		Denegar el inicio de sesión local	Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red
		Generar perfiles de un solo proceso	Administradores

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Actuar como parte del sistema operativo	(Definida, pero sin ningún valor)
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtén un token de suplantación para otro usuario en la misma sesión	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Omitir comprobación de recorrido	SERVICIO LOCAL, Servicio de Red, Administradores, Usuarios Autenticados
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	(Definida, pero sin ningún valor)
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento de volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	(Definida, pero sin ningún valor)
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Tener acceso a este equipo desde la red	Administradores, Usuarios	
		Tomar posesión de archivos y otros objetos	Administradores	
		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
7. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.				
		Acceso a redes: canalizaciones con nombre accesibles anónimamente	(Definida, pero sin ningún valor)	
		Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
		Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Deshabilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, System\Microsoft\Windows NT\CurrentVersion
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	System\CurrentControlSet\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUser Configuration, Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada
		Apagado: borrar el archivo de paginación de la memoria virtual	Deshabilitada
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Deshabilitada
		Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Deshabilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Deshabilitada	
		Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada	
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitada
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de registro en diferentes ubicaciones por usuario	Habilitada
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, Firma y operaciones hash	Deshabilitada
		Cuentas: cambiar el nombre de cuenta de invitado	Invitado
		Cuentas: cambiar el nombre de la cuenta de administrador	Administrador
		Cuentas: estado de la cuenta de administrador	Deshabilitada
		Cuentas: estado de la cuenta de invitado	Deshabilitada
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Deshabilitada
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Habilitada
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		Inicio de sesión interactivo: mostrar información de usuario cuando bloquee la sesión	No mostrar la información del usuario
		Inicio de sesión interactivo: No mostrar último inicio de sesión	Habilitada
		Inicio de sesión interactivo: No requerir Ctrl + Alt + Supr	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	1 inicios de sesión
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada
		Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	Deshabilitada
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada
		Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada
		Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
		Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits	
		Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits	
		Servidor de red de Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	30 minutos	
8. Verifique la directiva de almacén digital en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitado	
9. Verifique la directiva de asistencia en línea en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	
10.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Contenido en la Nube”		
		Directiva	Valor	OK/NOK
		Desactivar experiencias del consumidor de Microsoft	Habilitada	
		No mostrar recomendaciones de Windows	Habilitada	
11.Verifique las directivas de contenido en Buscar en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	
12.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	

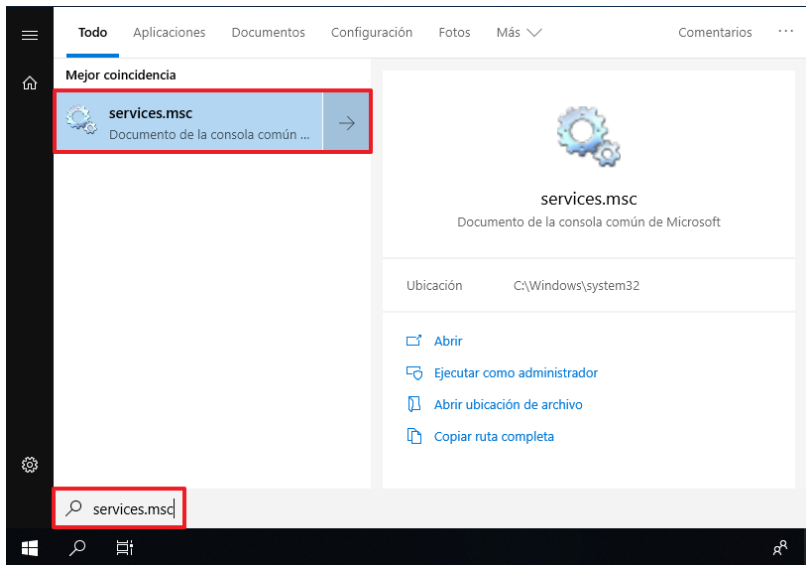
Comprobación	OK/NOK	Cómo hacerlo		
13.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		No enviar datos adicionales	Habilitado	
		Deshabilitar el informe de errores de Windows	Habilitado	
14.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		
		Directiva	Valor	OK/NOK
		Impedir la administración del filtro SmartScreen	Deshabilitado	
		Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	Habilitado	
		Activar Sitios sugeridos	Deshabilitado	
15.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Eliminar el historial de exploración”		
		Directiva	Valor	OK/NOK
		Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento.	Deshabilitado	
		Impedir que se elimine el historial de descarga	Deshabilitado	
		Impedir que se eliminen contraseñas	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir que se eliminen cookies	Deshabilitado	
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitado	
		Impedir que se eliminen los archivos temporales de Internet	Deshabilitado	
		Impedir que se eliminen los datos de filtrado InPrivate	Deshabilitado	
		Impedir que se eliminen los datos de formularios	Deshabilitado	
		Impedir que se eliminen los sitios web que el usuario visitó	Deshabilitado	
		Permitir que se elimine el historial de exploración al salir	Habilitado	
16.Verifique las directivas de OneDrive en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	
17.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas.	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
18.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”		
		Directiva	Valor	OK/NOK
		No volver a mostrar notificaciones de comentarios	Habilitado	
		Permitir telemetría	Habilitado	
19.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
20.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
21.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar scripting de ubicación		Habilitado	
	Desactivar sensores		Habilitado	
	Desactivar ubicación		Habilitado	
22.Verifique la directiva de Windows Update en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”			
	Directiva		Valor	OK/NOK
	Administrar preliminares		Habilitado (Deshabilitar preliminares)	
23.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Sistema → Perfiles de usuario”			
	Directiva		Valor	OK/NOK
	Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)		Habilitado (Siempre desactivado)	

Comprobación	OK/NOK	Cómo hacerlo		
24.Verifique el modo de configuración de los servicios del sistema.		Ejecute la herramienta de servicios. Para ello pulse “Inicio”, teclee “services.msc” y pulse “Enter”.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto, entre paréntesis) para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de escucha Net.Msmq	NetMsmqActivator	Automático	Configurado	
Adaptador de escucha Net.Pipe	NetPipeActivator	Automático	Configurado	
Adaptador de escucha Net.Tcp	NetTcpActivator	Automático	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administración de aplicaciones	AppMgmt	Manual	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Manual	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Automático	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de cuentas web	TokenBroker	Manual	Configurado		
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMgrSvc	Manual	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Automático	Configurado		
Agrupación de red del mismo nivel	p2psvc	Manual	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Manual	Configurado		
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Audio de Windows	Audiosrv	Automático	Configurado		
Autenticación natural	NaturalAuthentication	Manual	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Manual	Configurado		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		
CaptureService	CaptureService	Manual	Configurado		
Carpetas de trabajo	workfolderssvc	Manual	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente para NFS	NfsClnt	Automático	Configurado		
Cliente web	WebClient	Manual	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Automático	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Conexiones de red	Netman	Manual	Configurado		
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración automática de WLAN	WlanSvc	Manual	Configurado		
Configuración automática de WWAN	WwanSvc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado		
ConsentUX	ConsentUxUserSvc	Manual	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Control parental	WpcMonSvc	Deshabilitado	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado	
Copias de seguridad de Windows	SDRSVC	Manual	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado	
Desencadenadores de Message Queue Server	MSMQTriggers	Automático	Configurado	
Detección de hardware shell	ShellHWDetection	Automático	Configurado	
Detección SSDP	SSDPSRV	Manual	Configurado	
DevicePicker	DevicePickerUserSvc	Manual	Configurado	
DevicesFlow	DevicesFlowUserSvc	Manual	Configurado	
Diagnostic Execution Service	diagsvc	Manual	Configurado	
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado	
Disco virtual	vds	Manual	Configurado	
Dispositivo host de UPnP	upnphost	Manual	Configurado	
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado	
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Escucha de RIP	iprip	Automático	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	
Examinador de equipos	Browser	Manual	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado	
Fax	Fax	Manual	Configurado	
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Firewall de Windows	MpsSvc	Automático	Configurado		
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado		
Hora de Windows	W32Time	Manual	Configurado		
Host de proveedor de detección de función	fdPHost	Manual	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Manual	Configurado		
Host del servicio de diagnóstico	WdiServiceHost	Manual	Configurado		
Identidad de aplicación	AppIDSvc	Manual	Configurado		
Información de la aplicación	Appinfo	Manual	Configurado		
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado		
Inicio de sesión secundario	seclogon	Manual	Configurado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado		
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
LxssManager	LxssManager	Manual	Configurado		
Message Queue Server	MSMQ	Automático	Configurado		
MessagingService	MessagingService	Manual	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Automático	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	Configurado		
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Manual	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Manual	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Manual	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado		
Registrador de configuración de Windows Connect Now	wcncsvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Manual	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManager Svc	Manual	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático	Configurado		
Servicio AVCTP	BthAvctpSvc	Manual	Configurado		
Servicio biométrico de Windows	WbioSrv	Manual	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Automático	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado		
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado		
Servicio de administración de radio	RmSvc	Manual	Configurado		
Servicio de administración de web	WMSVC	Manual	Configurado		
Servicio de administración de Windows	WManSvc	Manual	Configurado		
Servicio de administración IIS	IISADMIN	Automático	Configurado		
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Manual	Configurado		
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asistente para perfil local	wlpassvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Automático	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de cliente de protección de host	HgClientService	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de datos espacial	SharedRealitySvc	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado	
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado		
Servicio de geolocalización	lfsvc	Manual	Configurado		
Servicio de historial de archivos	fhsvc	Manual	Configurado		
Servicio de host HV (Hyper-V)	HvHost	Manual	Configurado		
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado		
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado		
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de instalación de Microsoft Store	InstallService	Manual	Configurado		
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de mejora de visualización	DisplayEnhancementService	Manual	Configurado		
Servicio de monitor de infrarrojos	irmon	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		

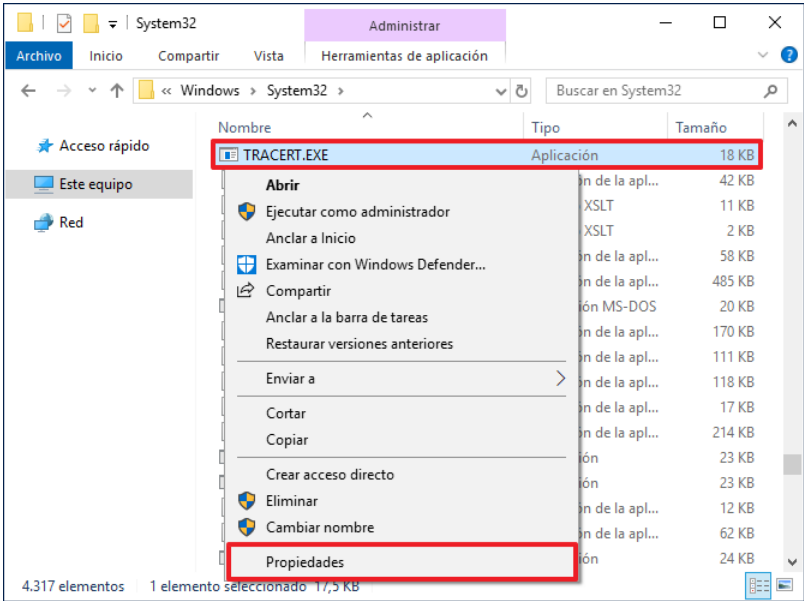
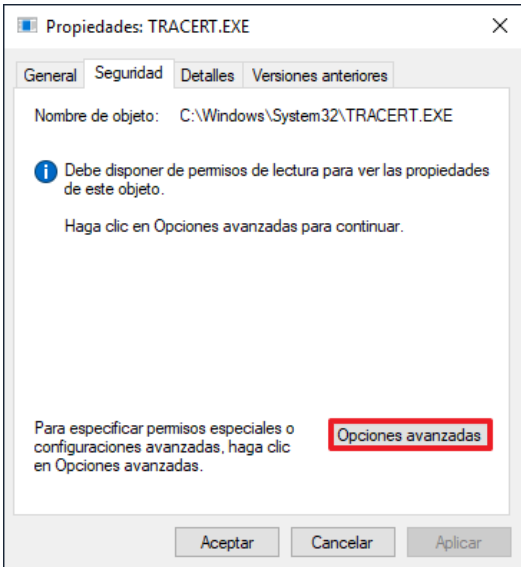
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Manual	Configurado		
Servicio de percepción de Windows	spectrum	Manual	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Manual	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado		
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Manual	Configurado		
Servicio de publicación World Wide Web	W3SVC	Automático	Configurado		
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Manual	Configurado		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		
Servicio de red de host	hns	Manual	Configurado		
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado		
Servicio de registro de W3C	w3logsvc	Manual	Configurado		
Servicio de reparación MultiPoint	WmsRepair	Automático	Configurado		
Servicio de repositorio de estado	StateRepository	Manual	Configurado		
Servicio de sensores	SensorService	Manual	Configurado		

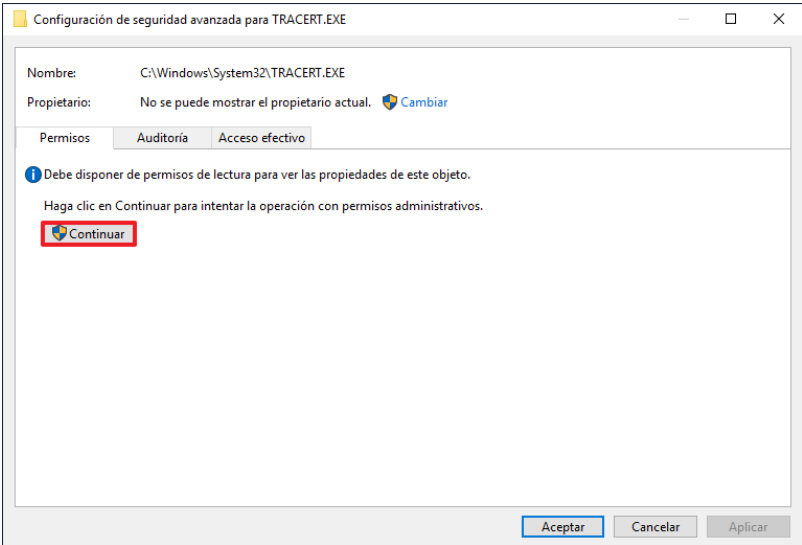
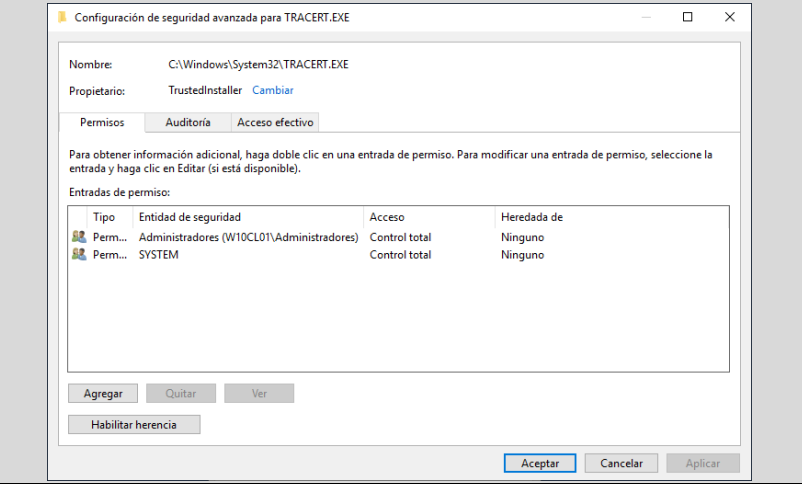
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado		
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Manual	Configurado		
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado		
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Automático	Configurado		
Servicio de uso compartido de datos	DsSvc	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Manual	Configurado		
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado		
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Automático	Configurado		
Servicio de usuario del portapapeles	cbdhsvc	Manual	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Manual	Configurado		
Servicio de Windows Defender	WinDefend	Automático	Configurado		
Servicio de Windows Insider	wisvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio FTP de Microsoft	ftpsvc	Automático	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio LPD	LPDSVC	Automático	Configurado	
Servicio MultiPoint	Wms	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado	
Servicio SNMP	SNMP	Deshabilitado	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	



Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado	
Servicio WAS (Windows Process Activation Service)	WAS	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servicios simples de TCP/IP	simptcp	Automático	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor de roles de DS	DsRoleSvc	Manual	Configurado	
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Automático	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Manual	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Automático	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
Uso de datos	DusmSvc	Automático	Configurado	
WalletService	WalletService	Manual	Configurado	
WarpJITSvc	WarpJITSvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Manual	Configurado	
Windows Search	WSearch	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Windows Update	wuauerv	Manual	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Manual	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	
25.Verifique los permisos asignados a ficheros y carpetas.		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione la opción "Propiedades". 		
		Nota: Deberá tener precaución para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". En la pestaña "Seguridad", seleccione "Opciones Avanzadas". 		

Comprobación	OK/NOK	Cómo hacerlo
		Es posible que deba pulsar sobre el botón “Continuar” para ver los permisos asignados.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. En la ventana resultante, compruebe los permisos asignados a cada carpeta o fichero. Nota: Tenga en consideración que es posible que algunos ficheros no se encuentren en el sistema debido a la configuración aplicada y según las necesidades que requiera su organización. 

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%Public%\		Administradores	Control total	
		System	Control total	
		Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\security		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control total	
%SystemRoot%\system32\raschap.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\rastls.dll		Administradores	Control total	
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

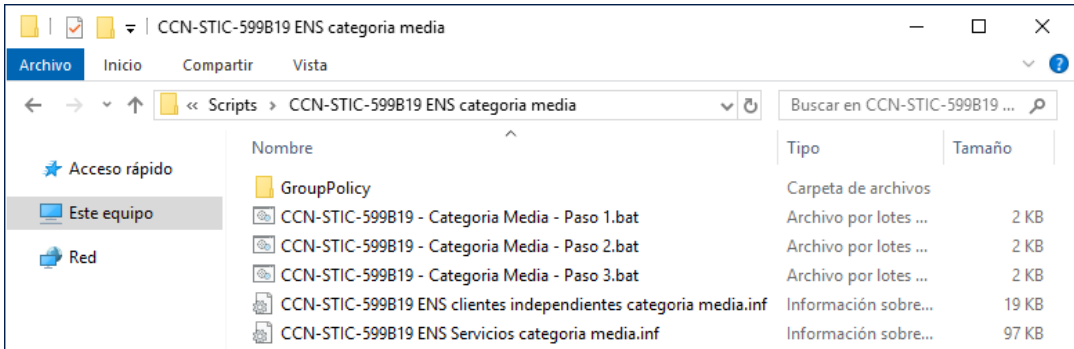
ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

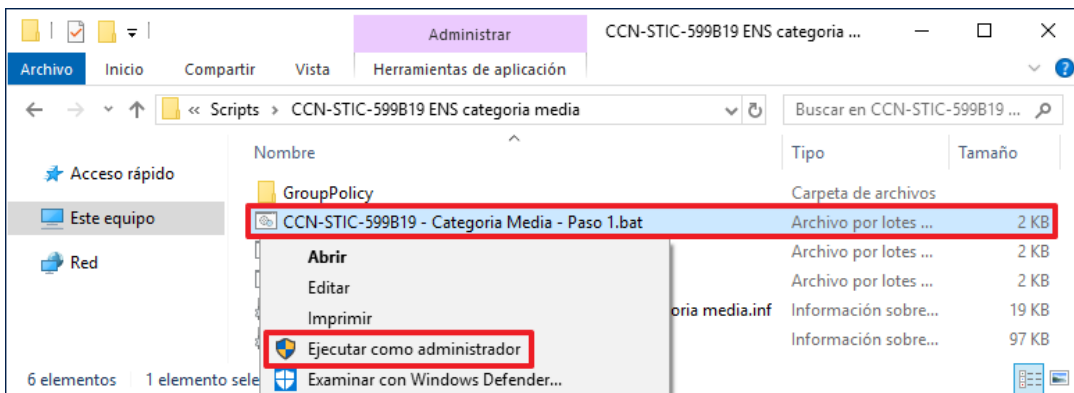
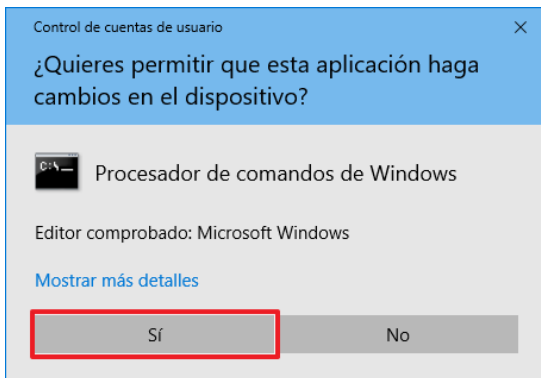
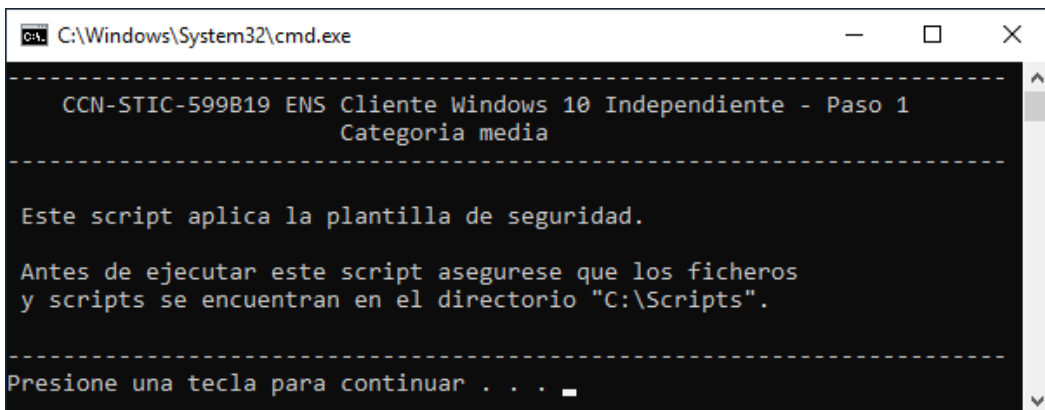
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes Windows 10 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

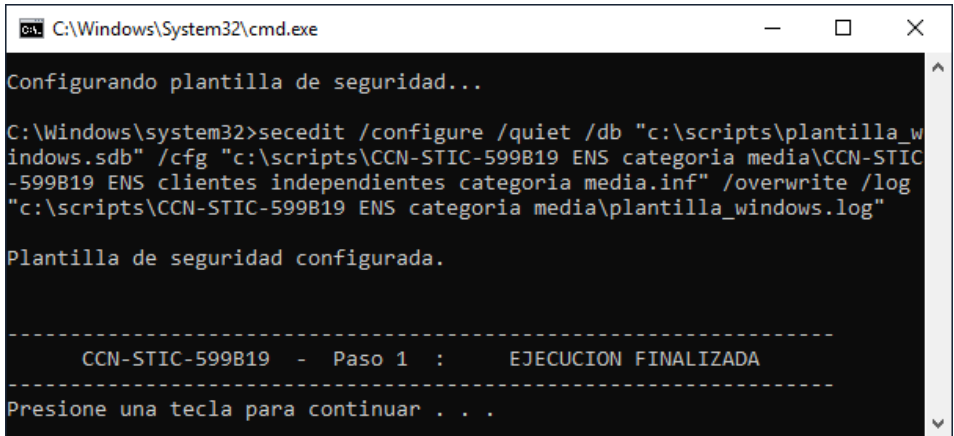
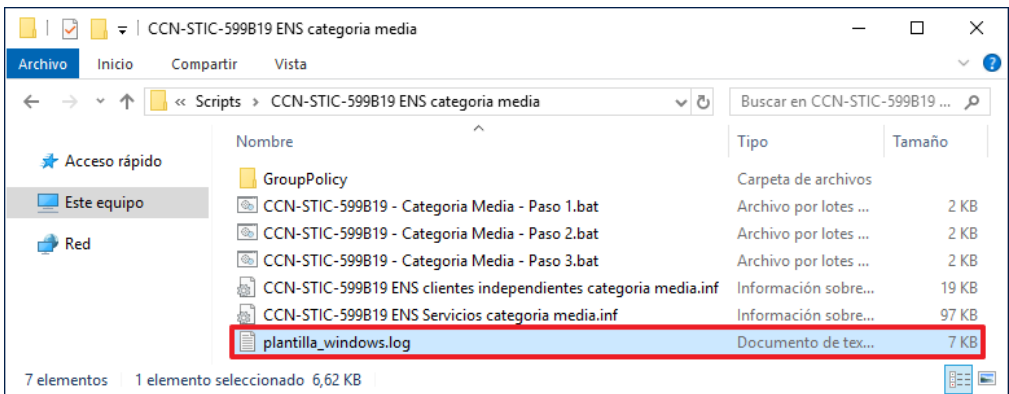
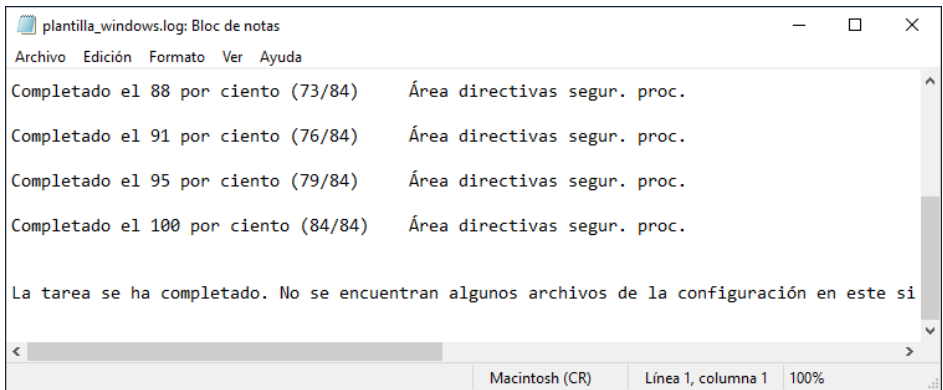
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Los pasos que se describen a continuación se realizarán en todos aquellos clientes Windows 10 Enterprise (versión 1809) con opción de mantenimiento LTSC, independientes a un dominio, que implementen servicios o información de categoría media y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

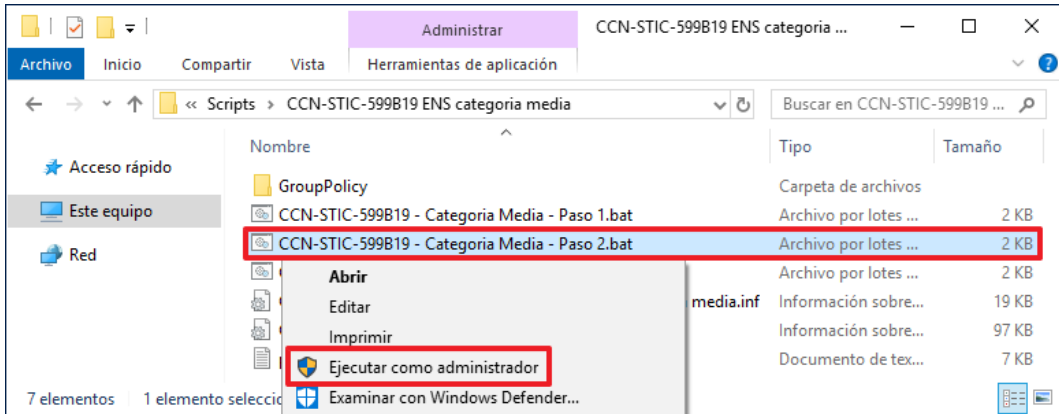
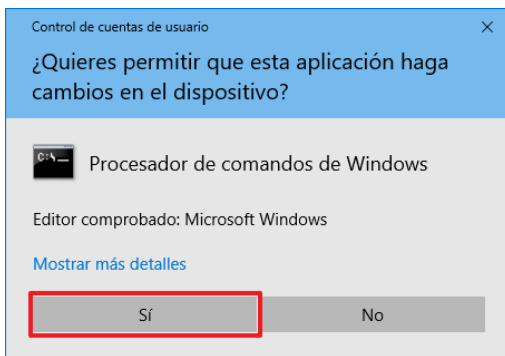
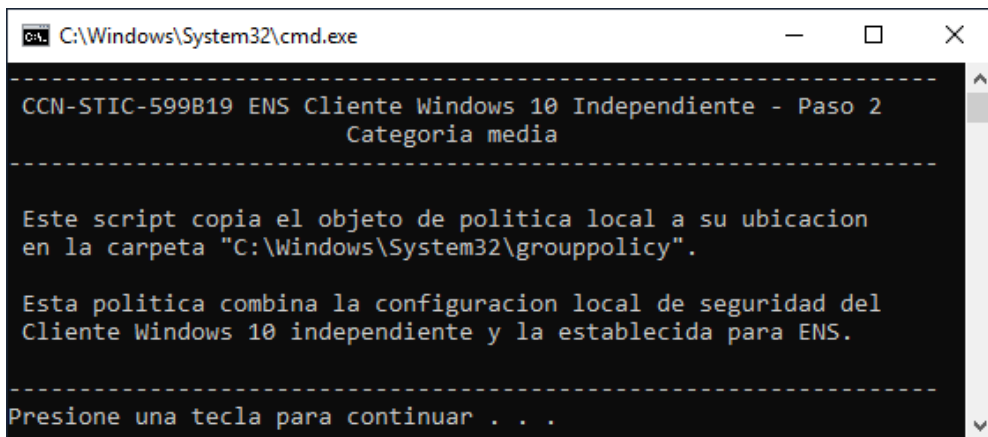
Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador local.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en la ruta “C:\Scripts”.
	Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”.
5.	Abra la carpeta “CCN-STIC-599B19 ENS categoria media” que encontrará en el directorio “C:\Scripts”.  Nota: Los scripts asumen que su ubicación es “C:\Scripts\CCN-STIC-599B19 ENS categoria media”. De no ser así deberá modificar los scripts para que coincidan con la ruta deseada.

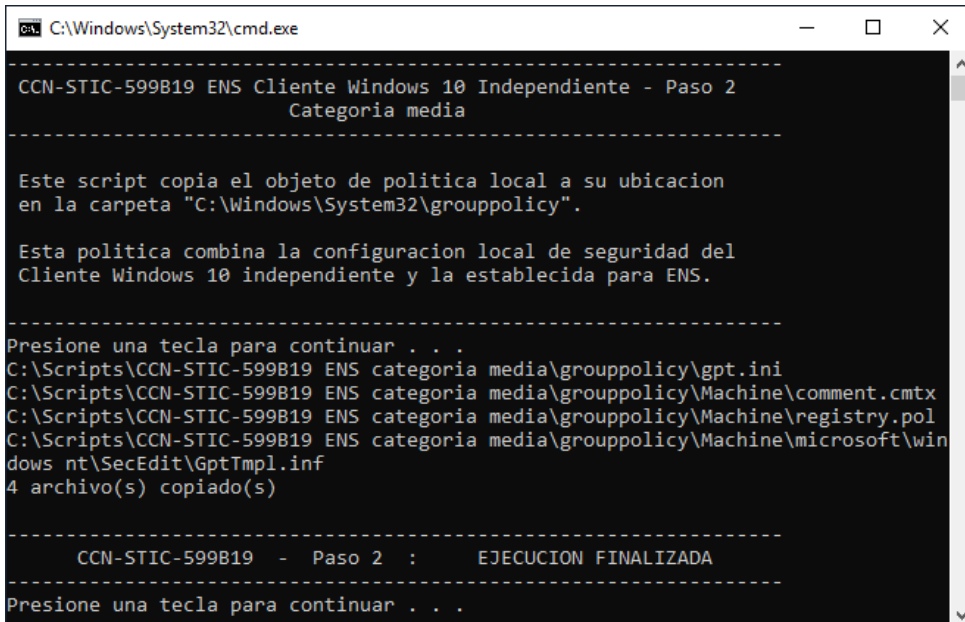
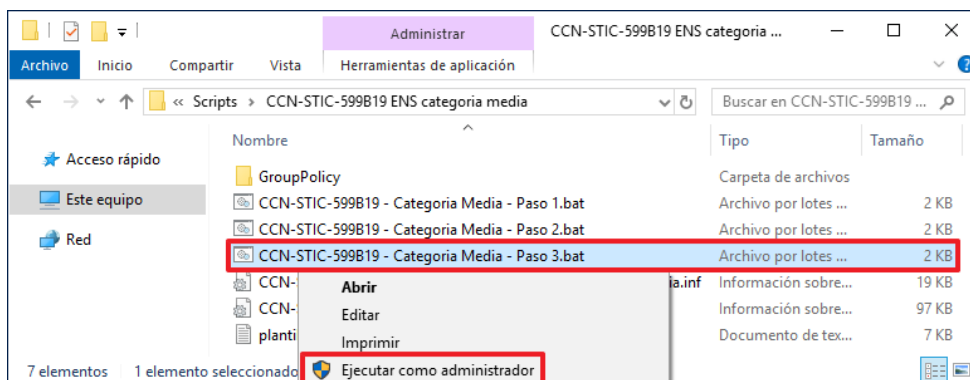


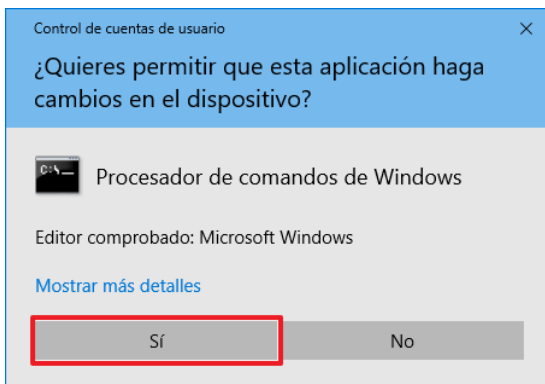
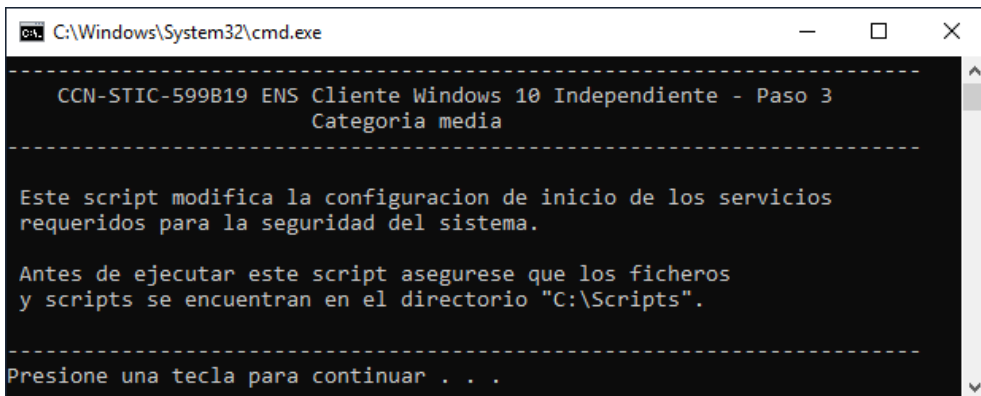
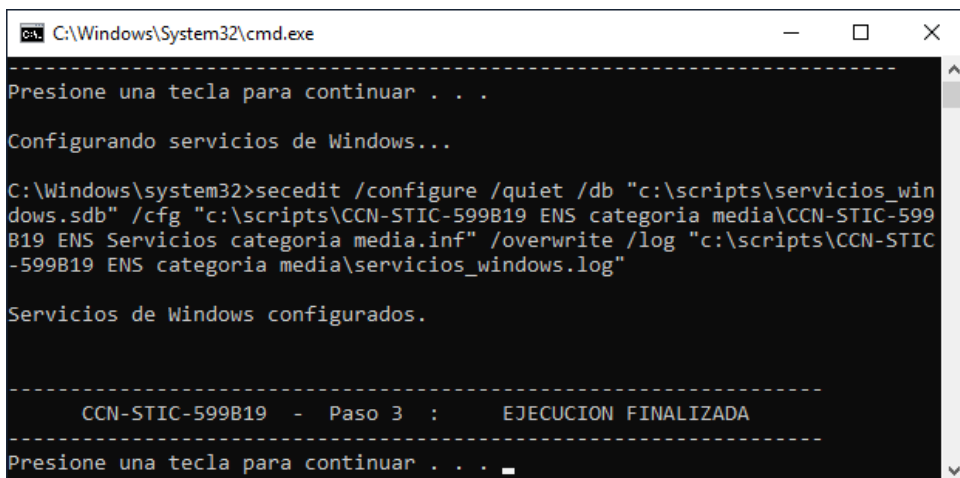
Paso	Descripción
6.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Media – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”. 
7.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
8.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría media del ENS. 

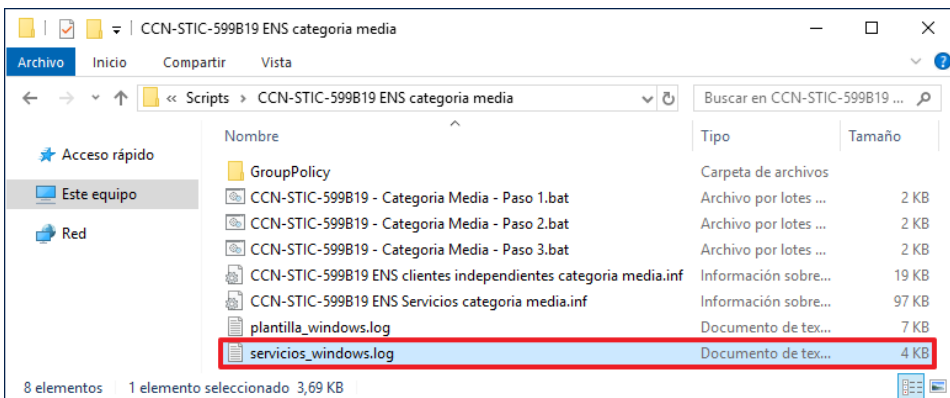
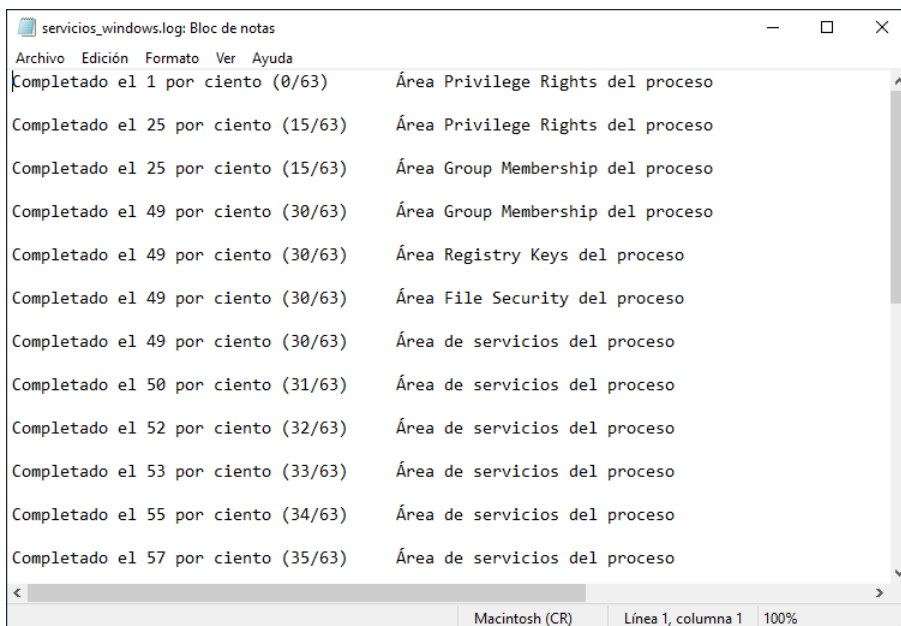
Paso	Descripción
9.	Una vez completado el proceso, deberá pulsar una tecla para continuar. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
10.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 categoria media” con el nombre “plantilla_windows.log”. 
11.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el procedimiento desde el paso 5.

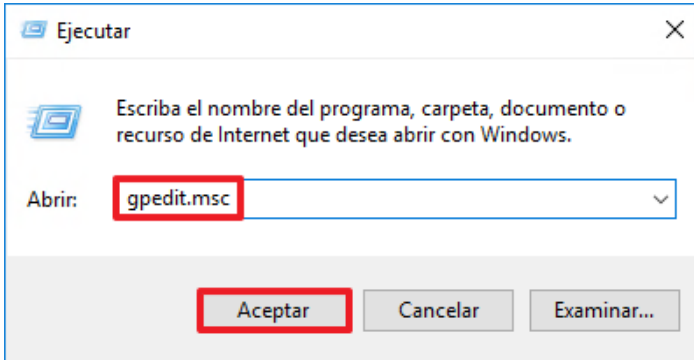
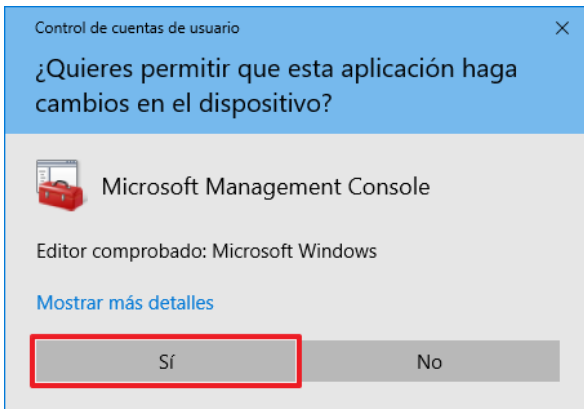
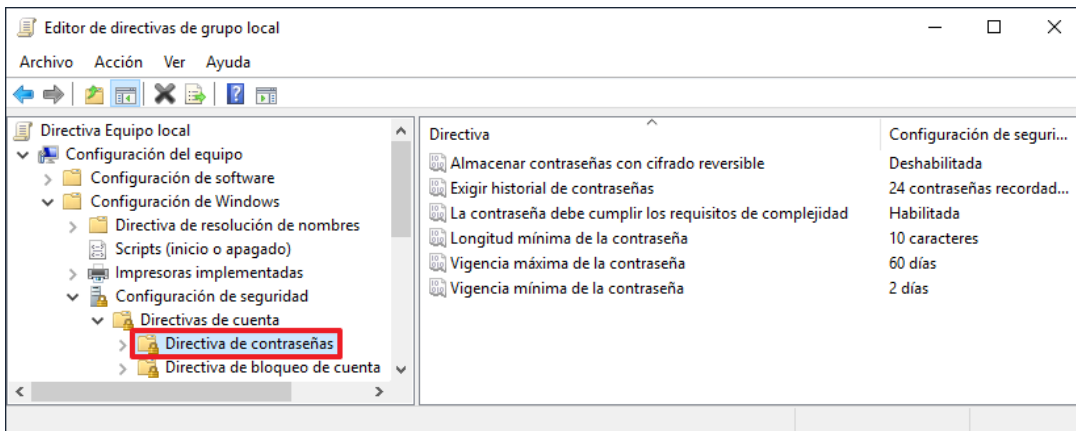


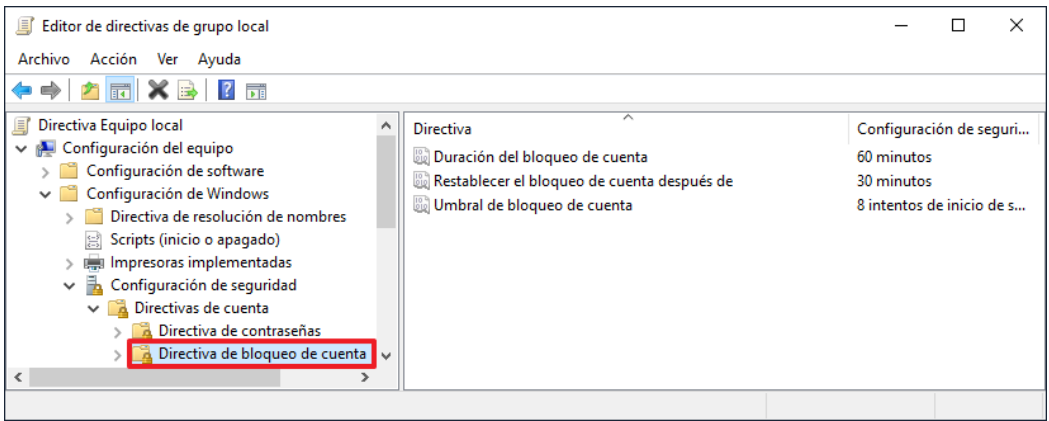
Paso	Descripción
12.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Media – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”. 
13.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
14.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local. 

Paso	Descripción
15.	Completada la copia de los archivos, compruebe que no ha habido errores en la copia de los mismos. Debería obtener el mismo resultado que el mostrado en la siguiente imagen. Pulse una tecla para finalizar la ejecución del script.  <pre> C:\Windows\System32\cmd.exe ----- CCN-STIC-599B19 ENS Cliente Windows 10 Independiente - Paso 2 Categoría media ----- Este script copia el objeto de politica local a su ubicacion en la carpeta "C:\Windows\System32\grouppolicy". Esta politica combina la configuracion local de seguridad del Cliente Windows 10 independiente y la establecida para ENS. ----- Presione una tecla para continuar . . . C:\Scripts\CCN-STIC-599B19 ENS categoria media\grouppolicy\gpt.ini C:\Scripts\CCN-STIC-599B19 ENS categoria media\grouppolicy\Machine\comment.cmtx C:\Scripts\CCN-STIC-599B19 ENS categoria media\grouppolicy\Machine\registry.pol C:\Scripts\CCN-STIC-599B19 ENS categoria media\grouppolicy\Machine\microsoft\win dows nt\SecEdit\GptTmpl.inf 4 archivo(s) copiado(s) ----- CCN-STIC-599B19 - Paso 2 : EJECUCION FINALIZADA ----- Presione una tecla para continuar . . . </pre> Nota: En caso de haberse producido fallos, soluciónelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.
16.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Media – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”. 

Paso	Descripción
17.	Pulse "Sí" cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
18.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría media del ENS. 
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 

Paso	Descripción
20.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 ENS categoria media” con el nombre de “servicios_windows.log”. 
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 16.
22.	Elimine la carpeta “C:\Scripts”.
23.	Es factible que su organización cuente con una política de contraseñas consolidada. La implementación de la política de categoría media implementará una política específica para los clientes de categoría media. Deberá evaluarla para determinar si esta configuración le es válida, o por el contrario debe adaptarla a las condiciones de su organización.

Paso	Descripción
24.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”. 
25.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
26.	Despliegue la política y sitúese en la siguiente ruta: “Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña” 

Paso	Descripción
27.	Evalúe la política de contraseñas y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de credenciales es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
28.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que “Directiva de contraseñas”. 
29.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.

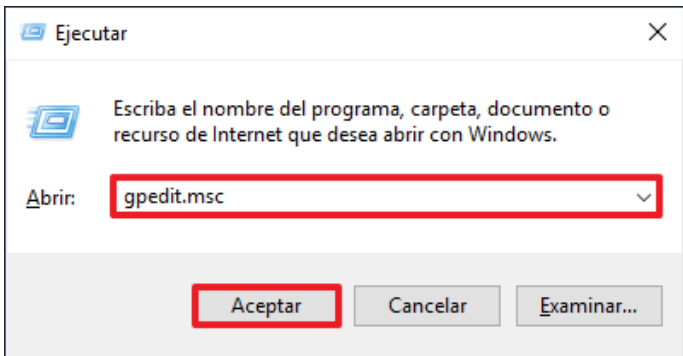
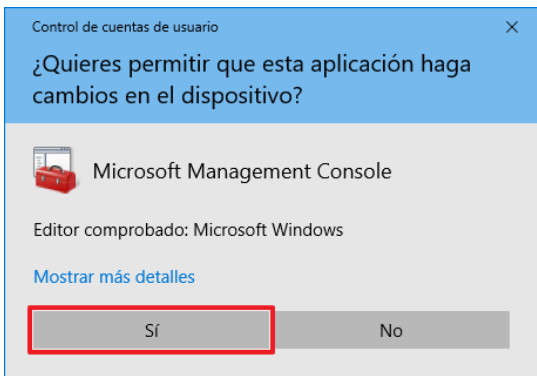
Hasta ahora han sido aplicados cambios, entre otros aspectos, sobre las directivas de contraseña y cuenta, aunque es importante señalar que existen más directivas interesantes a la hora de configurar el sistema.

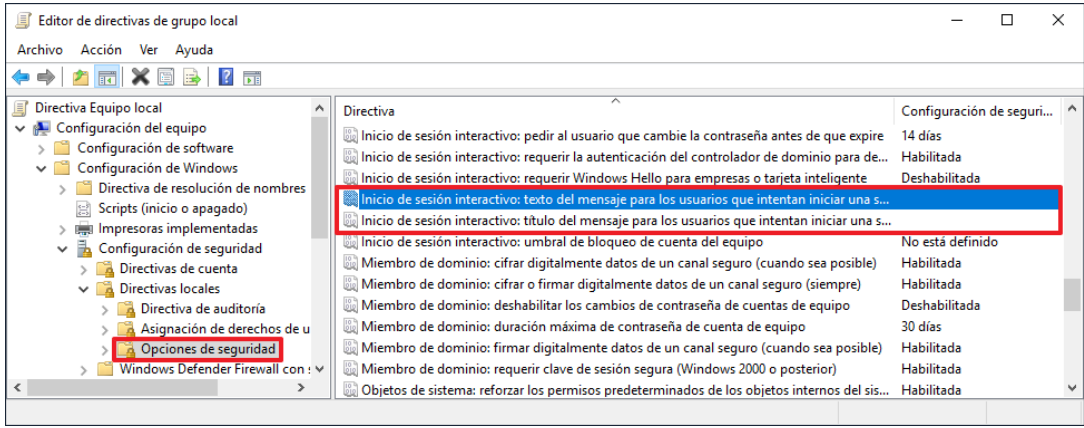
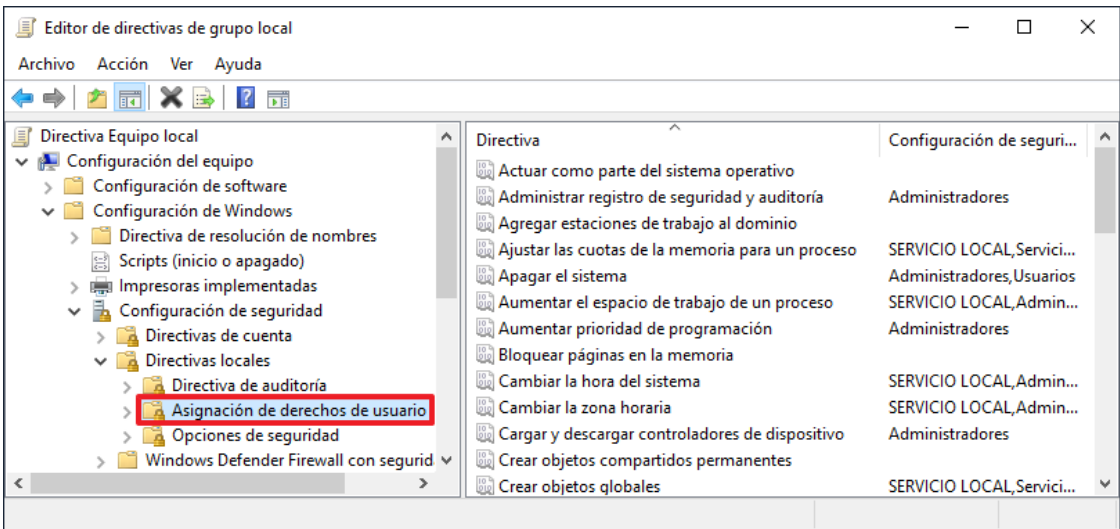
Uno de los aspectos que marca el ENS, desde su requisito de categoría media en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

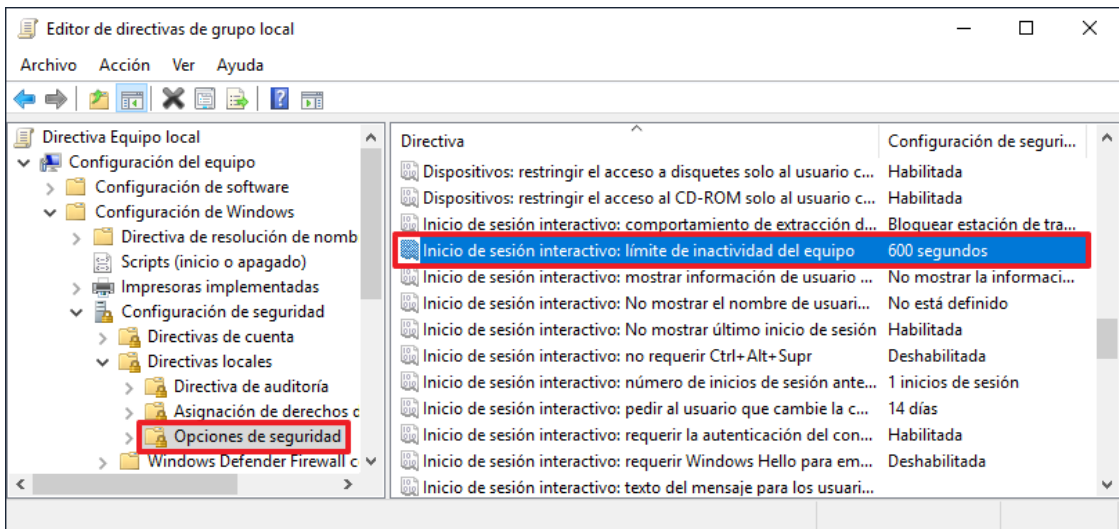
Los sistemas Windows presentan mecanismos para implementar mensajes que realizan advertencias al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

Si su organización no está haciendo uso de este mecanismo realice los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según queda estipulado en la política de seguridad de la organización.

Paso	Descripción
30.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
31.	Debe iniciar sesión con una cuenta que sea Administrador local.
32.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”. 
33.	Pulse “S” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
34.	Para informar de las obligaciones sitúese en la siguiente ruta: Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad

Paso	Descripción
35.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intenta iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intenta iniciar una sesión”. 
36.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
37.	Por último, la política de seguridad local especifica unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones sobre la configuración de política local.
38.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 
39.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.

Paso	Descripción
40.	Se establece a partir de la categoría media, según MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de la política local aplicable sobre equipo, puede establecerse la medida de protección que habilita el protector de pantalla y por lo tanto el bloqueo de la sesión. Nota: Si la organización presenta algún mecanismo para realizar el bloqueo del equipo ante inactividad no es necesario que aplique la siguiente configuración. No obstante, revise la configuración para adaptarse a la normativa vigente. Si la organización no tiene medidas dispuestas siga los siguientes pasos.
41.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad” Habilite y configure la siguiente directiva de seguridad: – Inicio de sesión interactivo: límite de inactividad del equipo. Establezca el valor en 600 segundos (10 minutos). 
42.	Cierre el editor de política de grupo local.
43.	Reinicie el puesto de trabajo.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA MEDIA

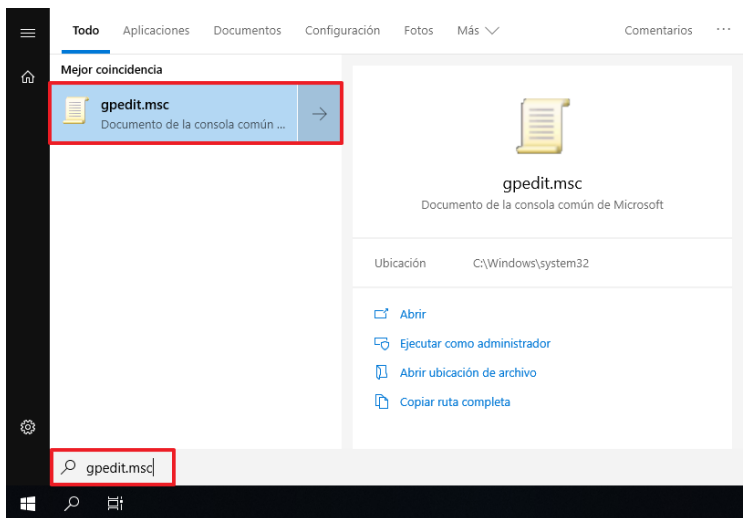
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO A.3.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS”.

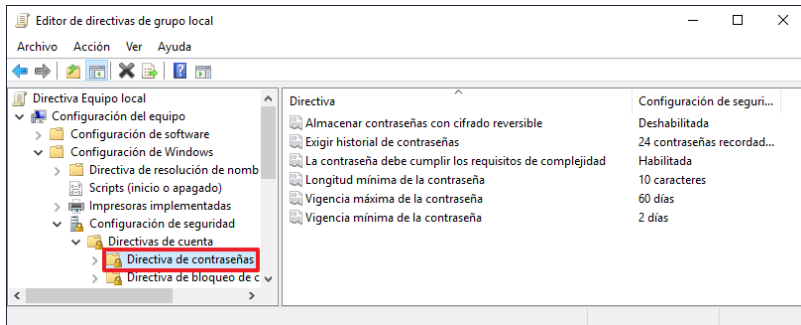
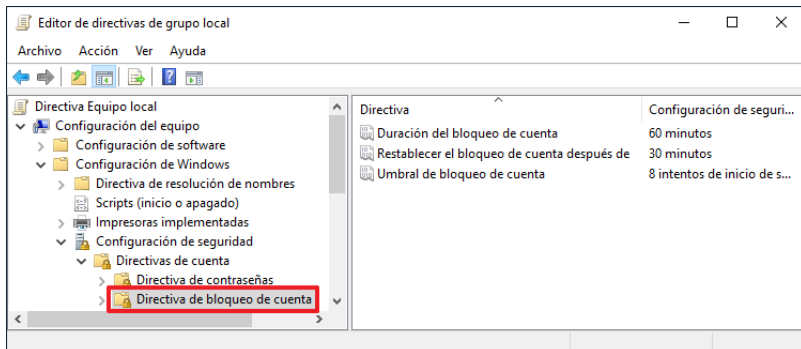
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes Windows 10 (versión 1809) Enterprise con opción de mantenimiento LTSC, independientes con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de administrador local.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario que es administrador local. Las consolas y herramientas que se utilizarán son las siguientes:

- Editor de objetos de directiva de grupo local (gpedit.msc).
- Editor de registro (regedit.exe).
- Visor de Eventos (eventvwr.exe).
- Servicios (services.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de administración local.
2. Inicie la aplicación de gestión de políticas locales.		Ejecute el “Editor de objetos de directiva de grupo local”. Para ello pulse “Inicio”, teclee “gpedit.msc” y pulse “Enter”. 

Comprobación	OK/NOK	Cómo hacerlo																					
3. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas” Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. 																					
		<table><tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Almacenar contraseñas usando cifrado reversible</td><td>Deshabilitada</td><td></td></tr><tr><td>Exigir historial de contraseñas</td><td>24 contraseñas recordadas</td><td></td></tr><tr><td>Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitada</td><td></td></tr><tr><td>Longitud mínima de la contraseña</td><td>10 caracteres</td><td></td></tr><tr><td>Vigencia máxima de la contraseña</td><td>60 días</td><td></td></tr><tr><td>Vigencia mínima de la contraseña</td><td>2 días</td><td></td></tr></table>	Directiva	Valor	OK/NOK	Almacenar contraseñas usando cifrado reversible	Deshabilitada		Exigir historial de contraseñas	24 contraseñas recordadas		Las contraseñas deben cumplir los requisitos de complejidad	Habilitada		Longitud mínima de la contraseña	10 caracteres		Vigencia máxima de la contraseña	60 días		Vigencia mínima de la contraseña	2 días	
	Directiva	Valor	OK/NOK																				
	Almacenar contraseñas usando cifrado reversible	Deshabilitada																					
	Exigir historial de contraseñas	24 contraseñas recordadas																					
	Las contraseñas deben cumplir los requisitos de complejidad	Habilitada																					
	Longitud mínima de la contraseña	10 caracteres																					
	Vigencia máxima de la contraseña	60 días																					
Vigencia mínima de la contraseña	2 días																						
4. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta” 																					
		<table><tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Duración del bloqueo de cuenta</td><td>60 minutos</td><td></td></tr><tr><td>Restablecer el bloqueo de cuenta después de</td><td>30 minutos</td><td></td></tr><tr><td>Umbral de bloqueo de cuenta</td><td>8 intentos de inicio de s...</td><td></td></tr></table>	Directiva	Valor	OK/NOK	Duración del bloqueo de cuenta	60 minutos		Restablecer el bloqueo de cuenta después de	30 minutos		Umbral de bloqueo de cuenta	8 intentos de inicio de s...										
	Directiva	Valor	OK/NOK																				
Duración del bloqueo de cuenta	60 minutos																						
Restablecer el bloqueo de cuenta después de	30 minutos																						
Umbral de bloqueo de cuenta	8 intentos de inicio de s...																						

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Restablecer el bloqueo de cuenta después de	30 minutos	
		Umbral de bloqueo de cuenta	8 intentos de inicio de sesión no válidos	
5. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”		
		Directiva	Valor	OK/NOK
		Auditar el acceso a objetos	Correcto, Erróneo	
		Auditar el acceso del servicio de directorio	Correcto, Erróneo	
		Auditar el cambio de directivas	Correcto, Erróneo	
		Auditar el uso de privilegios	Correcto, Erróneo	
		Auditar eventos de inicio de sesión	Correcto, Erróneo	
		Auditar eventos de inicio de sesión de cuenta	Correcto, Erróneo	
		Auditar eventos del sistema	Correcto, Erróneo	
		Auditar la administración de cuentas	Correcto, Erróneo	
6. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”		
		Directiva	Valor	OK/NOK
		Actuar como parte del sistema operativo	(Definida, pero sin ningún valor)	
		Administrar registro de seguridad y auditoría	Administradores	
		Agregar estaciones de trabajo al dominio	(Definida, pero sin ningún valor)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red
		Apagar el sistema	Administradores, Usuarios
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL, Usuarios
		Aumentar prioridad de programación	Administradores
		Bloquear páginas en la memoria	(Definida, pero sin ningún valor)
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores
		Cargar y descargar controladores de dispositivo	Administradores
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)
		Crear objetos globales	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL
		Crear un archivo de paginación	Administradores
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)
		Crear vínculos simbólicos	Administradores
		Denegar el acceso a este equipo desde la red	ANONYMOUS LOGON, Invitados
		Denegar el inicio de sesión como servicio	Invitados
		Denegar el inicio de sesión como trabajo por lotes	Invitados
		Denegar el inicio de sesión local	Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red
		Generar perfiles de un solo proceso	Administradores

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtén un token de suplantación para otro usuario en la misma sesión	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Omitir comprobación de recorrido	SERVICIO LOCAL, Servicio de Red, Administradores, Usuarios Autenticados
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	(Definida, pero sin ningún valor)
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento de volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	(Definida, pero sin ningún valor)
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Tener acceso a este equipo desde la red		Administradores, Usuarios	
	Tomar posesión de archivos y otros objetos		Administradores	
7. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
	Directiva		Valor	OK/NOK
	Acceso a redes: canalizaciones con nombre accesibles		(Definida, pero sin ningún valor)	
	Acceso a redes: modelo de seguridad y uso compartido para cuentas locales		Clásico: usuarios locales se autentican con credenciales propias	
	Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red		Deshabilitada	
	Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM		Habilitada	
	Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM		Habilitada	
	Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos		Deshabilitada	
	Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos		Habilitada	
	Acceso a redes: rutas del Registro accesibles remotamente		System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, System\Microsoft\Windows NT\CurrentVersion	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Acceso a redes: rutas y subrutinas del Registro accesibles remotamente	System\CurrentControlSet\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Deshabilitada
		Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Deshabilitada
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada
		Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitada
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de registro en diferentes ubicaciones por usuario	Habilitada
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, Firma y operaciones hash	Deshabilitada
		Cuentas: cambiar el nombre de cuenta de invitado	Invitado
		Cuentas: cambiar el nombre de la cuenta de administrador	Administrador
		Cuentas: estado de la cuenta de administrador	Deshabilitada
		Cuentas: estado de la cuenta de invitado	Deshabilitada
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Deshabilitada
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada
		Dispositivos: restringir el acceso a disquetes solo al usuario con sesión iniciada localmente	Habilitada
		Dispositivos: restringir el acceso al CD-ROM solo al usuario con sesión iniciada localmente	Habilitada
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		Inicio de sesión interactivo: mostrar información de usuario cuando bloquee la sesión	No mostrar la información del usuario
		Inicio de sesión interactivo: No mostrar último inicio de sesión	Habilitada
		Inicio de sesión interactivo: No requerir Ctrl + Alt + Supr	Deshabilitada
		Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	1 inicios de sesión
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	Deshabilitada
		Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión	(Definida, pero sin ningún valor)
		Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión	(Definida, pero sin ningún valor)
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada
		Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitada
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits
		Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits
		Servidor de red de Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos

Comprobación	OK/NOK	Cómo hacerlo		
8. Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media”		
		Directiva	Valor	OK/NOK
		Impedir el acceso a internet de Windows Media DRM	Habilitado	
9. Verifique la directiva de almacén digital en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitado	
10. Verifique la directiva de Antivirus en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitado	
11. Verifique la directiva de asistencia en línea en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
12.Verifique las directivas de biometría en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Habilitado	
		Permitir que los usuarios de dominio inicien sesión mediante biometría	Habilitado	
		Permitir que los usuarios inicien sesión mediante biometría	Habilitado	
13.Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		Permitir el uso de Cortana	Deshabilitado	
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	
14.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Contenido en la Nube”		
		Directiva	Valor	OK/NOK
		Desactivar experiencias del consumidor de Microsoft	Habilitada	
		No mostrar recomendaciones de Windows	Habilitada	
15.Verifique las directivas de reproducción automática en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Directivas de Reproducción automática”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Establece el comportamiento predeterminado para la ejecución automática	Habilitado (No ejecutar ningún comando de ejecución automática)	
		Desactivar reproducción automática	Habilitado (Todas las unidades)	
		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
16.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo local.		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
17.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo local.		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	
		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		
18.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Directiva	Valor	OK/NOK
		Activar sitios sugeridos	Deshabilitado	
		Impedir administración del filtro SmartScreen	Deshabilitado	
		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	Habilitado	
19.Verifique las directivas de autocompletar en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitado	
20.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Eliminar el historial de exploración”		
		Directiva	Valor	OK/NOK
		Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento.	Deshabilitado	
		Impedir que se elimine el historial de descarga	Deshabilitado	
		Impedir que se eliminen contraseñas	Deshabilitado	
		Impedir que se eliminen cookies	Deshabilitado	
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitado	
		Impedir que se eliminen los archivos temporales de Internet	Deshabilitado	
		Impedir que se eliminen los datos de filtrado InPrivate	Deshabilitado	
		Impedir que se eliminen los datos de formularios	Deshabilitado	
		Impedir que se eliminen los sitios web que el usuario visitó	Deshabilitado	
		Permitir que se elimine el historial de exploración al salir	Habilitado	

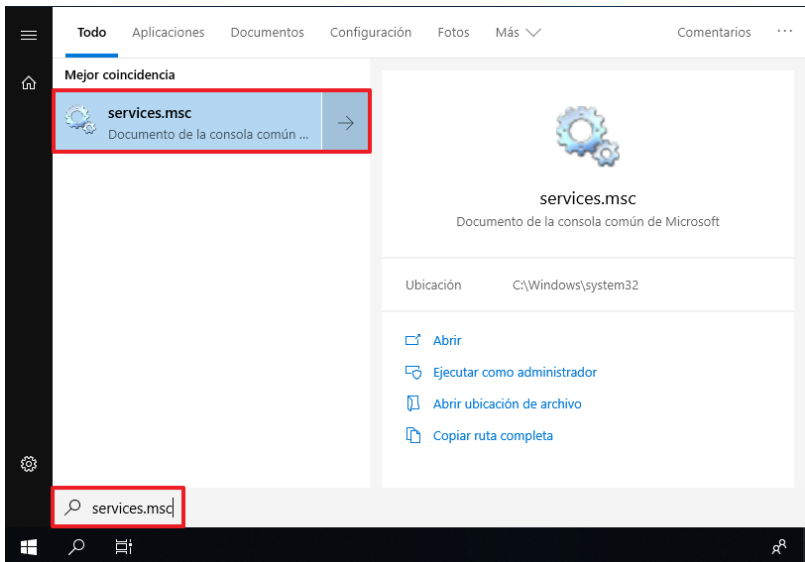
Comprobación	OK/NOK	Cómo hacerlo		
21.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → SmartScreen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
22.Verifique las directivas de OneDrive en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	
23.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK
		Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario	Habilitado	
		Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	Habilitado	
24.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitado (Solo HTTP (0))	

Comprobación	OK/NOK	Cómo hacerlo		
25.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas.	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows se ejecuten en el fondo		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados		Habilitado (Forzar denegación)	
26.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”			
	Directiva		Valor	OK/NOK
	No volver a mostrar notificaciones de comentarios		Habilitado	
	Permitir telemetría		Habilitado	
27.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”			
	Directiva		Valor	OK/NOK
	Permitir acceso a Shell remoto		Deshabilitado	
28.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”			
	Directiva		Valor	OK/NOK
	Configurar SmartScreen de Windows Defender		Habilitado (Advertir e impedir la omisión)	

Comprobación	OK/NOK	Cómo hacerlo		
29.Verifique la directiva de Tienda en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Store”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitado	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitado	
30.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitado	
		Desactivar sensores	Habilitado	
		Desactivar ubicación	Habilitado	
31.Verifique la directiva de Windows Update en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	
32.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
33.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Desactivar el acceso a Store	Habilitado	
		Desactivar el contenido “¿Sabías que...?” del Centro de ayuda y soporte técnico	Habilitado	
		Desactivar el informe de errores de Windows	Habilitado	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows	Habilitado	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger	Habilitado	
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitado	
		Desactivar la actualización de archivos de contenido del Asistente para búsqueda	Habilitado	
		Desactivar búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico	Habilitado	
		Desactivar la tarea de imágenes “Pedir copias fotográficas”	Habilitado	
		Desactivar los vínculos “Event.asp” del Visor de eventos	Habilitado	
		Desactivar uso compartido de datos de personalización de escritura a mano	Habilitado	
34.Verifique la directiva de Net Logon en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Net Logon”		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
35.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Perfiles de usuario”		
		Directiva	Valor	OK/NOK
		Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)	Habilitado	
		Desactivar el identificador de publicidad	Habilitado	
36.Verifique el modo de configuración de los servicios del sistema.		Ejecute la herramienta de servicios. Para ello pulse “Inicio”, teclee “services.msc” y pulse “Enter”.		
		 Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto, entre paréntesis) para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado		
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado		
Adaptador de escucha Net.Msmq	NetMsmqActivator	Automático	Configurado		
Adaptador de escucha Net.Pipe	NetPipeActivator	Automático	Configurado		
Adaptador de escucha Net.Tcp	NetTcpActivator	Automático	Configurado		
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado		
Administración de aplicaciones	AppMgmt	Manual	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Manual	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Automático	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de cuentas web	TokenBroker	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMgrSvc	Manual	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Automático	Configurado		
Agrupación de red del mismo nivel	p2psvc	Manual	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Asignador de detección de topologías de nivel de vínculo	ltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Audio de Windows	Audiosrv	Automático	Configurado		
Autenticación natural	NaturalAuthentication	Manual	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Manual	Configurado		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		
CaptureService	CaptureService	Manual	Configurado		
Carpetas de trabajo	workfoldersvc	Manual	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente para NFS	NfsClnt	Automático	Configurado		
Cliente web	WebClient	Manual	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Automático	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Conexiones de red	Netman	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración automática de WLAN	WlanSvc	Manual	Configurado		
Configuración automática de WWAN	WwanSvc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado		
ConsentUX	ConsentUxUserSvc	Manual	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Automático	Configurado		
Detección de hardware shell	ShellHWDetection	Automático	Configurado		
Detección SSDP	SSDPSRV	Manual	Configurado		
DevicePicker	DevicePickerUserSvc	Manual	Configurado		
DevicesFlow	DevicesFlowUserSvc	Manual	Configurado		
Diagnostic Execution Service	diagsvc	Manual	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Manual	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
Energía	Power	Automático	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado		
Escucha de RIP	iprip	Automático	Configurado		
Estación de trabajo	LanmanWorkstation	Automático	Configurado		
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado		
Examinador de equipos	Browser	Manual	Configurado		
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado		
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado		
Fax	Fax	Manual	Configurado		
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado		
Firewall de Windows	MpsSvc	Automático	Configurado		
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado		
Hora de Windows	W32Time	Manual	Configurado		
Host de proveedor de detección de función	fdPHost	Manual	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Manual	Configurado		
Host del servicio de diagnóstico	WdiServiceHost	Manual	Configurado		
Identidad de aplicación	AppIDSvc	Manual	Configurado		
Información de la aplicación	Appinfo	Manual	Configurado		
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado		
Inicio de sesión secundario	seclogon	Manual	Configurado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado		
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
LxssManager	LxssManager	Manual	Configurado		
Message Queue Server	MSMQ	Automático	Configurado		
MessagingService	MessagingService	Manual	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Manual	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	Configurado		
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Manual	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Manual	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado		
Registrador de configuración de Windows Connect Now	wcnscvc	Manual	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Manual	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Manual	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático	Configurado		
Servicio AVCTP	BthAvctpSvc	Manual	Configurado		
Servicio biométrico de Windows	WbioSrv	Manual	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Automático	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado		
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administración de web	WMSVC	Manual	Configurado	
Servicio de administración de Windows	WManSvc	Manual	Configurado	
Servicio de administración IIS	IISADMIN	Automático	Configurado	
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asistente para perfil local	wlpsvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Automático	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de cliente de protección de host	HgClientService	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de datos espacial	SharedRealitySvc	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	



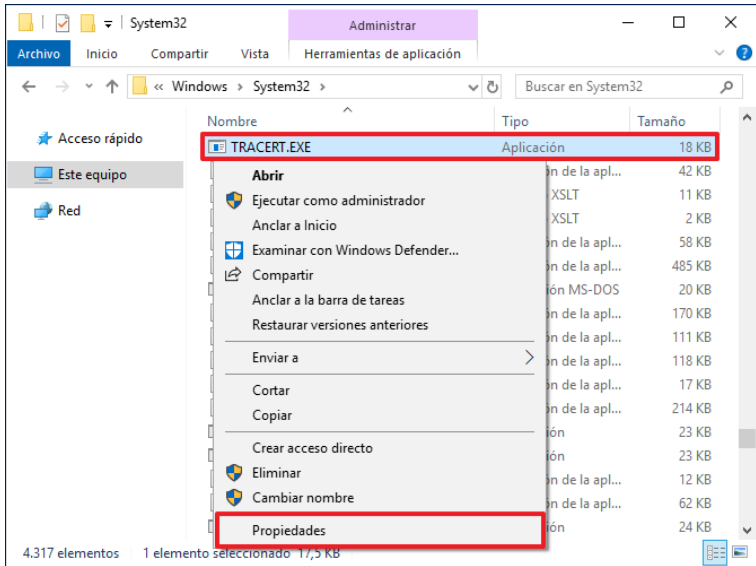
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado		
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado		
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado		
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado		
Servicio de geolocalización	lfsvc	Manual	Configurado		
Servicio de historial de archivos	fhsvc	Manual	Configurado		
Servicio de host HV (Hyper-V)	HvHost	Manual	Configurado		
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado		
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado		
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de instalación de Microsoft Store	InstallService	Manual	Configurado		
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		

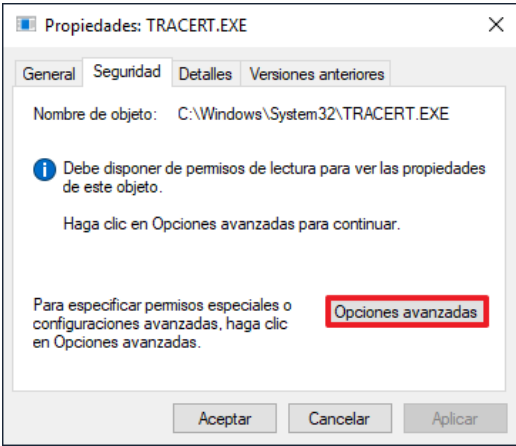
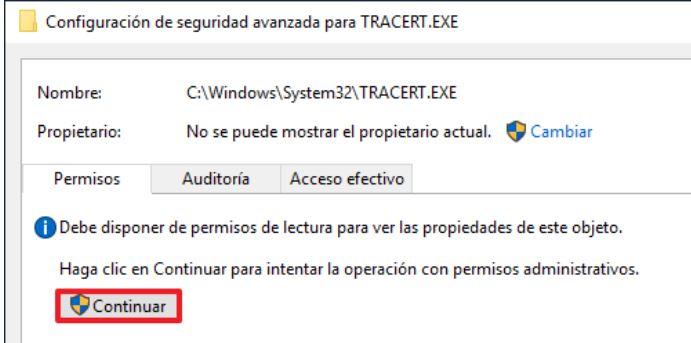
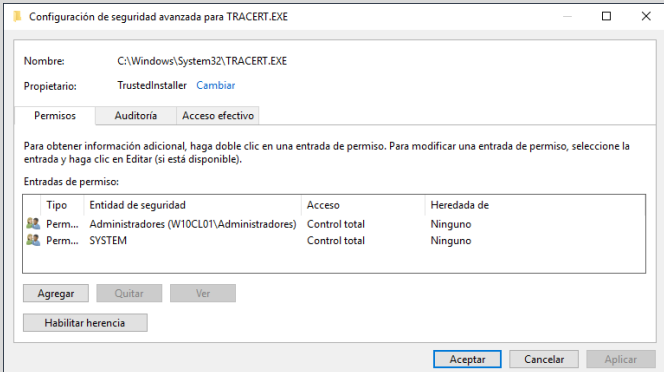
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de mejora de visualización	DisplayEnhancementService	Manual	Configurado		
Servicio de monitor de infrarrojos	irmon	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Manual	Configurado		
Servicio de percepción de Windows	spectrum	Manual	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Manual	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado		
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Manual	Configurado		
Servicio de publicación World Wide Web	W3SVC	Automático	Configurado		
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Manual	Configurado		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de red de host	hns	Manual	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado	
Servicio de registro de W3C	w3logsvc	Manual	Configurado	
Servicio de reparación MultiPoint	WmsRepair	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Manual	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Automático	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Manual	Configurado	
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado	
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Automático	Configurado	
Servicio de usuario del portapapeles	cbdhsvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de virtualización de red	nvagent	Manual	Configurado	
Servicio de Windows Defender	WinDefend	Manual	Configurado	
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio FTP de Microsoft	ftpsvc	Automático	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio LPD	LPDSVC	Automático	Configurado	
Servicio MultiPoint	Wms	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado		
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio telefónico	PhoneSvc	Manual	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Manual	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Manual	Configurado		
Servicios simples de TCP/IP	simptcp	Automático	Configurado		
Servidor	LanmanServer	Automático	Configurado		
Servidor de roles de DS	DsRoleSvc	Manual	Configurado		
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado		
Sincronizar host	OneSyncSvc	Automático	Configurado		
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado		
Sistema de eventos COM+	EventSystem	Automático	Configurado		
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado		
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado		
Superfetch	SysMain	Automático	Configurado		
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado		
Telefonía	TapiSrv	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Automático	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
Uso de datos	DusmSvc	Automático	Configurado	
WalletService	WalletService	Manual	Configurado	
WarpJITSvc	WarpJITSvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Manual	Configurado	
Windows Search	WSearch	Automático	Configurado	
Windows Update	wuauerv	Manual	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Manual	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	
37.Verifique los permisos asignados a ficheros y carpetas.		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione la opción "Propiedades".  Nota: Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".		

Comprobación	OK/NOK	Cómo hacerlo
		En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”.  Es posible que deba pulsar sobre el botón “Continuar” para ver los permisos asignados.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. En la ventana resultante, compruebe los permisos asignados a cada carpeta o fichero. Nota: Tenga en consideración que es posible que algunos ficheros no se encuentren en el sistema debido a la configuración aplicada y según las necesidades que requiera su organización. 

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%Public%\		Administradores	Control total	
		System	Control total	
		Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\security		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control total	
%SystemRoot%\system32\raschap.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\rastls.dll		Administradores	Control total	
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes Windows 10 con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría alta, deberá realizar las implementaciones según se referencian en el presente anexo.

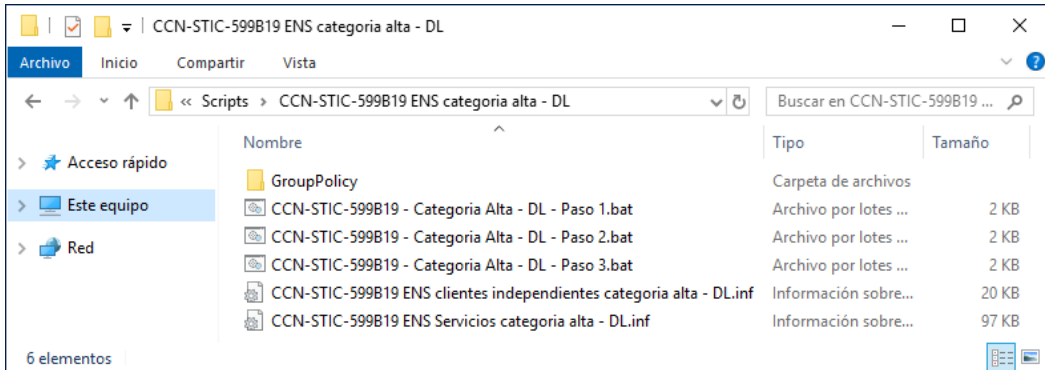
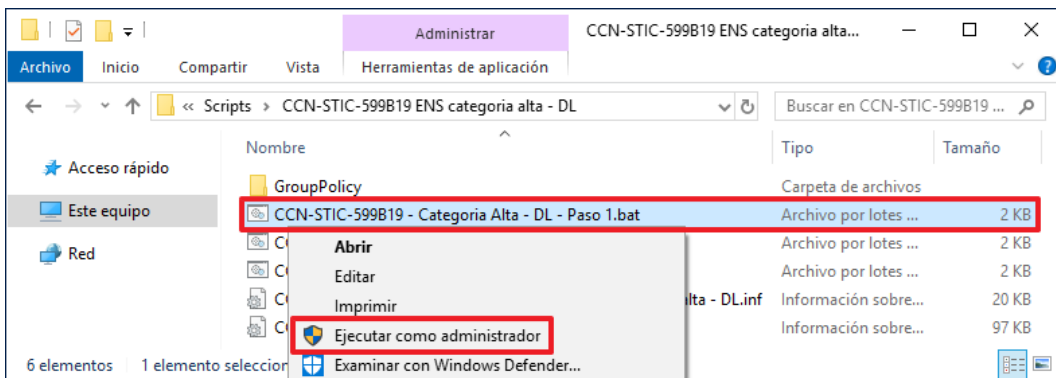
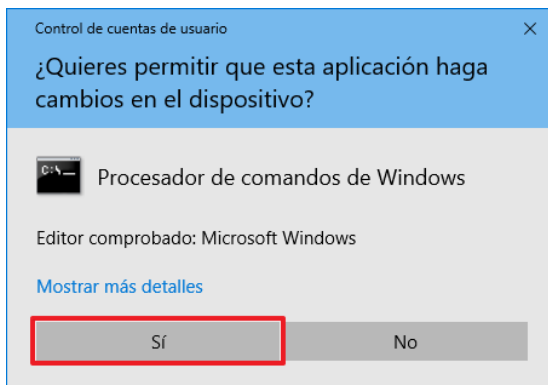
Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

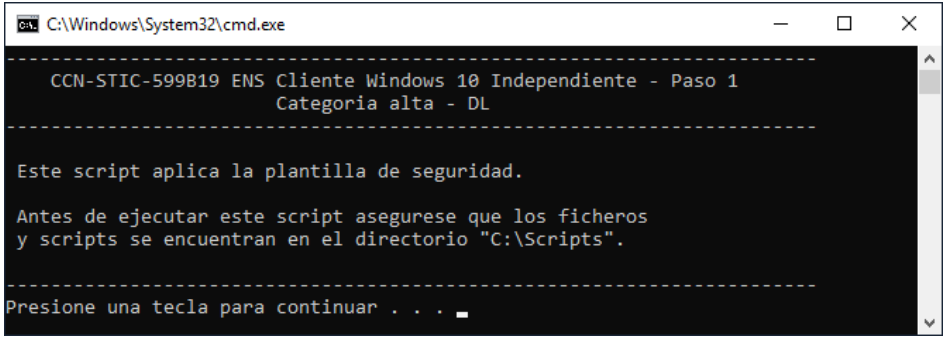
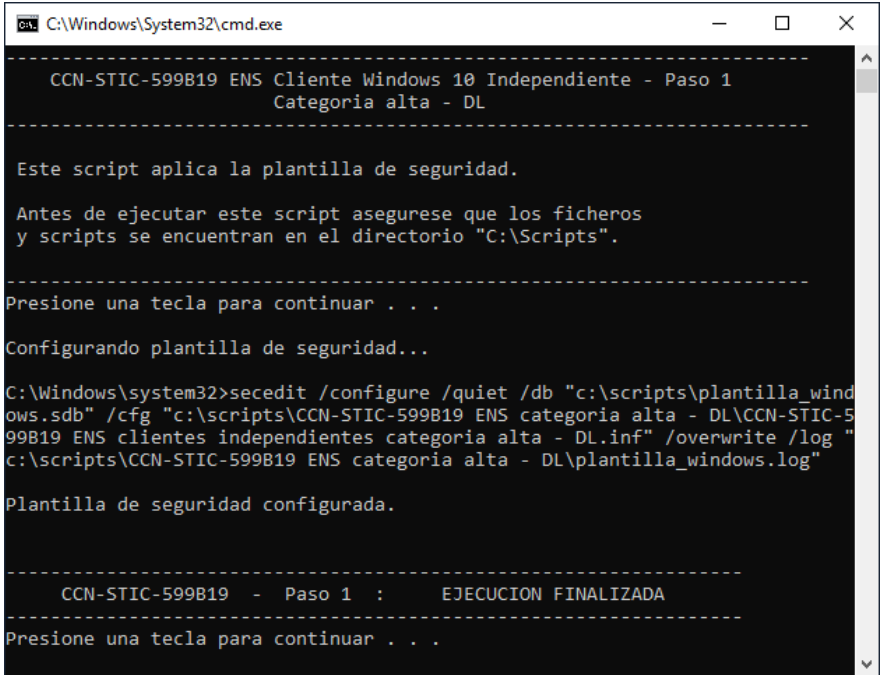
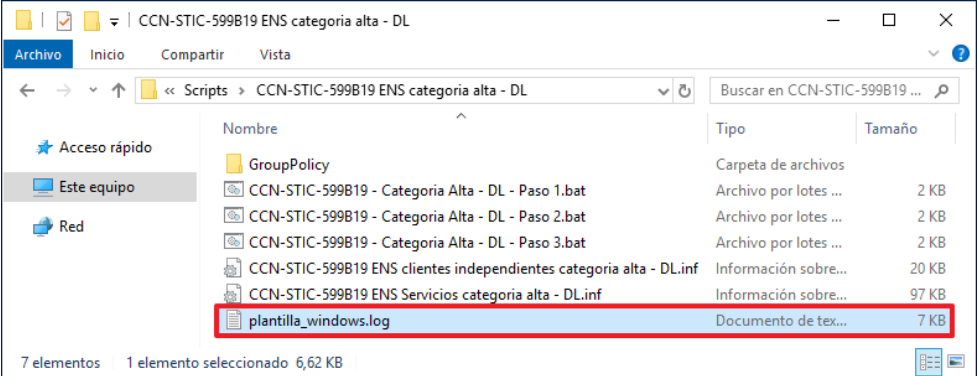
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará uso de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho caso.

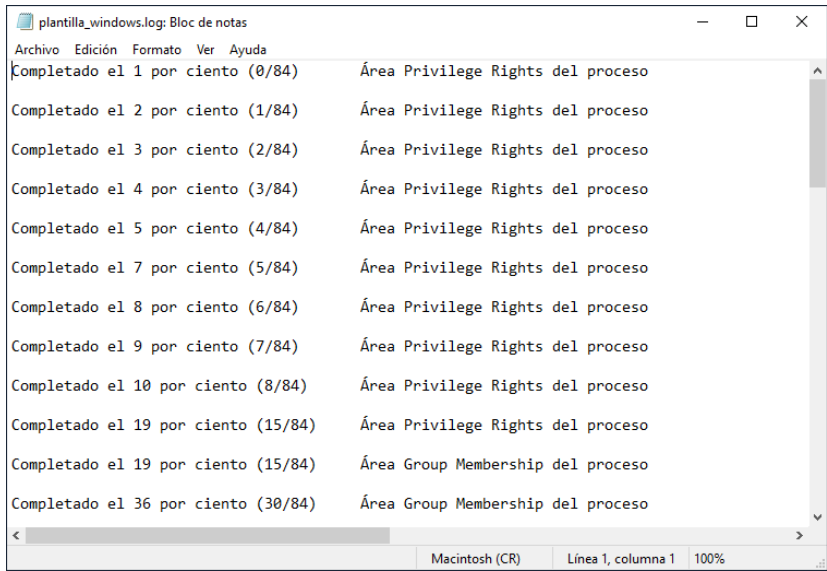
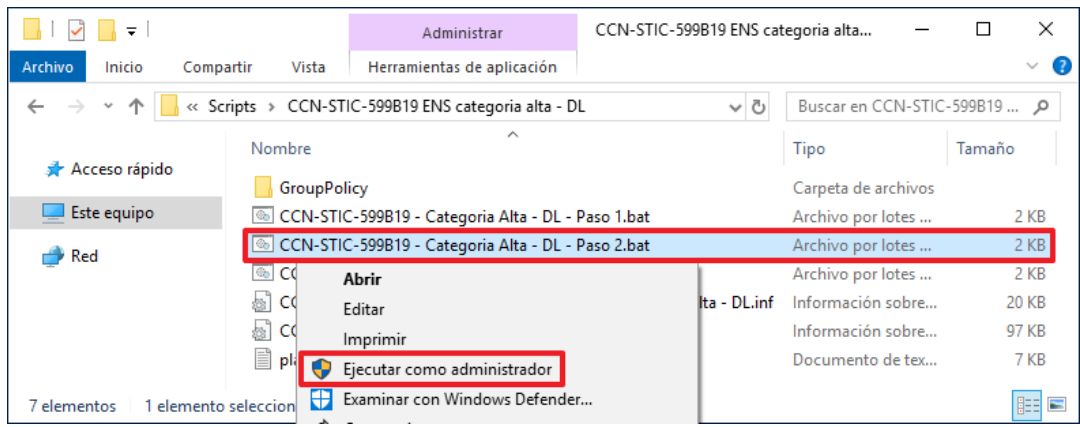
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

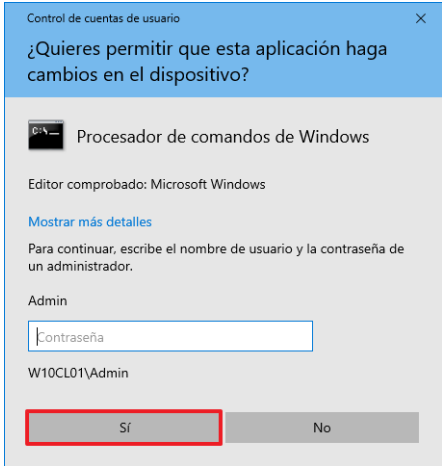
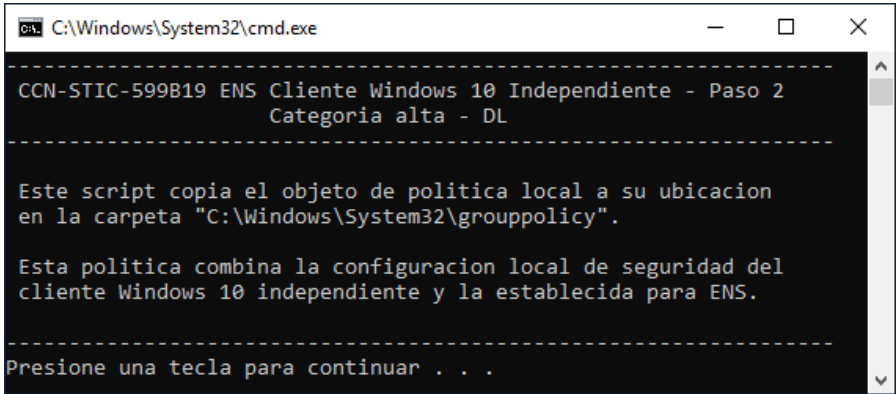
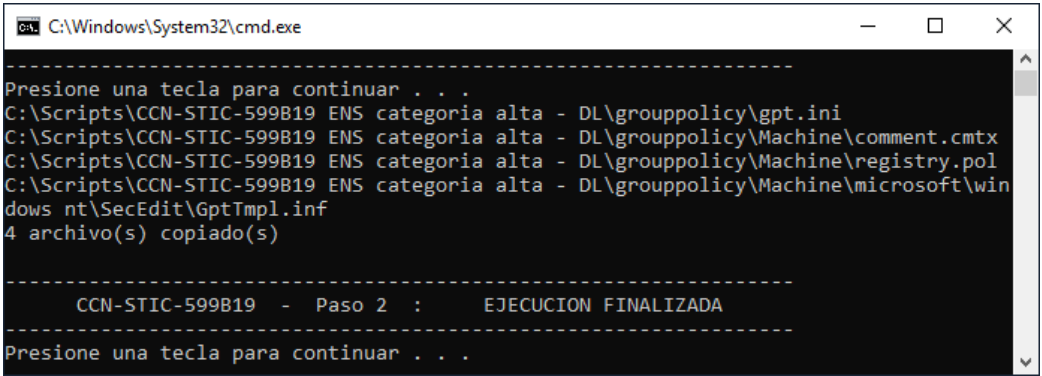
Los pasos que se describen a continuación se realizarán en todos aquellos clientes Windows 10 Enterprise (versión 1809) con opción de mantenimiento LTSC, independientes a un dominio, que implementen servicios o información de categoría alta y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad / Difusión Limitada.

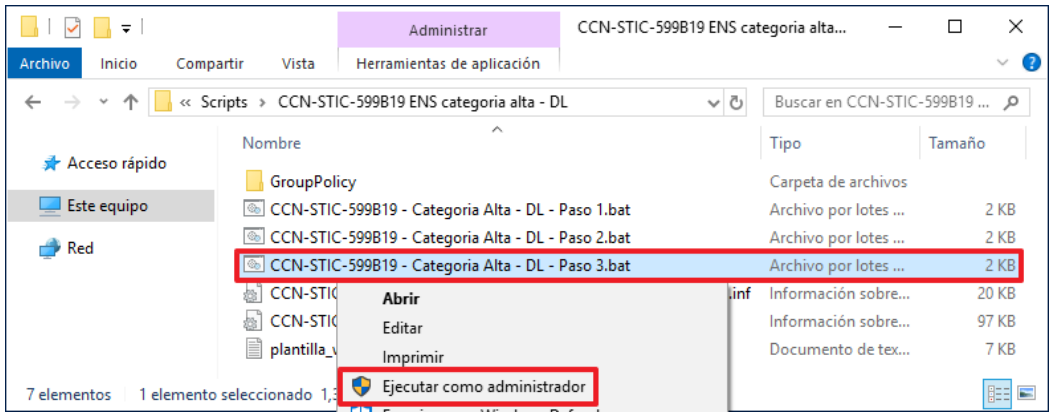
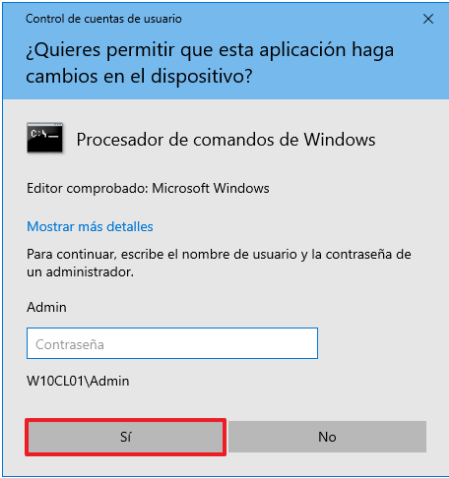
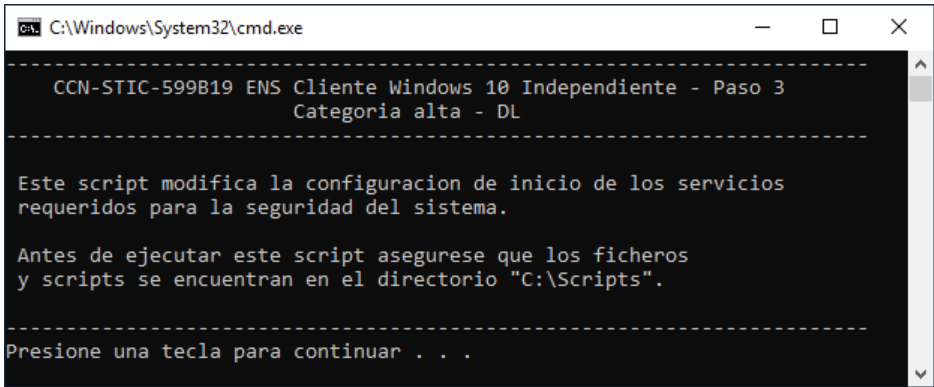
Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador local.
3.	Cree el directorio "Scripts" en la unidad "C:\".
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19".	

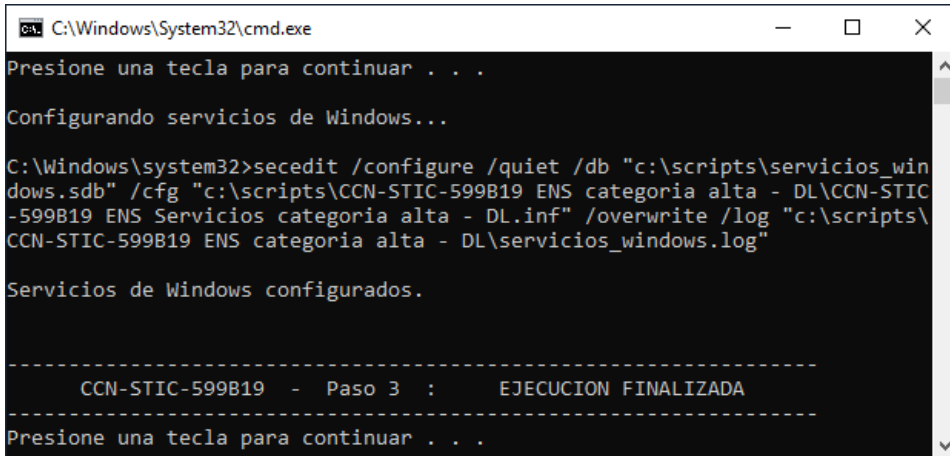
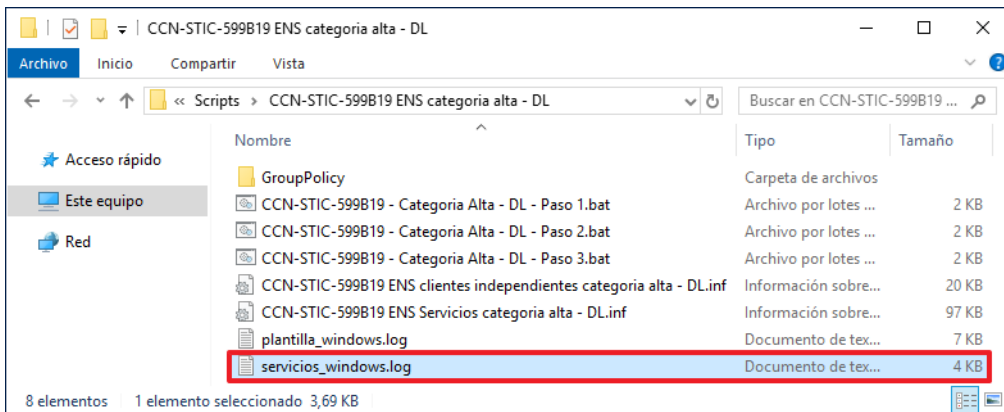
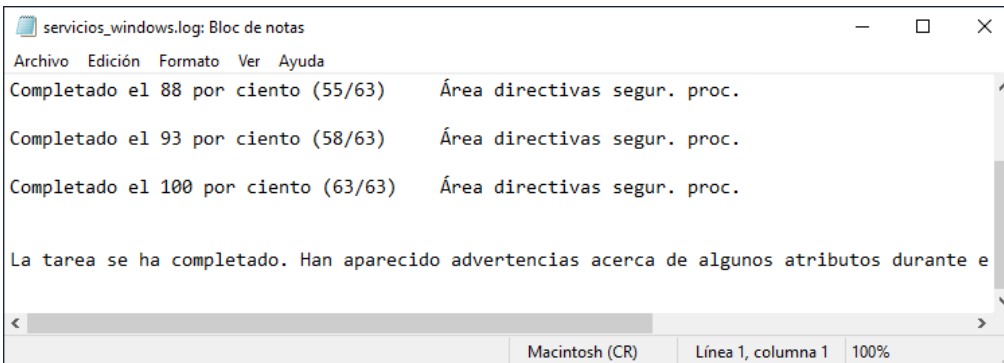
Paso	Descripción
5.	Abra la carpeta “CCN-STIC-599B19 ENS categoria alta” que encontrará en el directorio “C:\Scripts”.  Nota: Los scripts asumen que su ubicación es “C:\Scripts\CCN-STIC-599B19 ENS categoria alta - DL”. De no ser así deberá modificar los scripts para que coincidan con la ruta deseada.
6.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Alta - DL – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”. 
7.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 

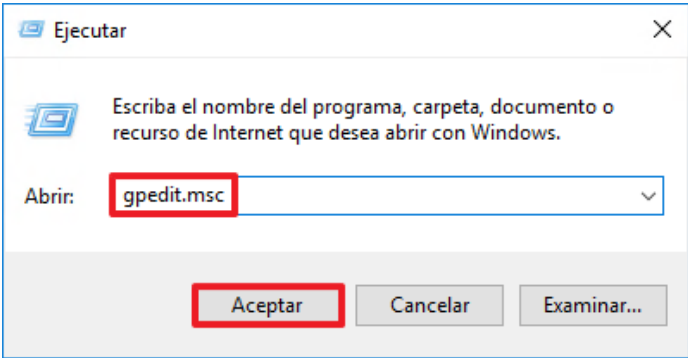
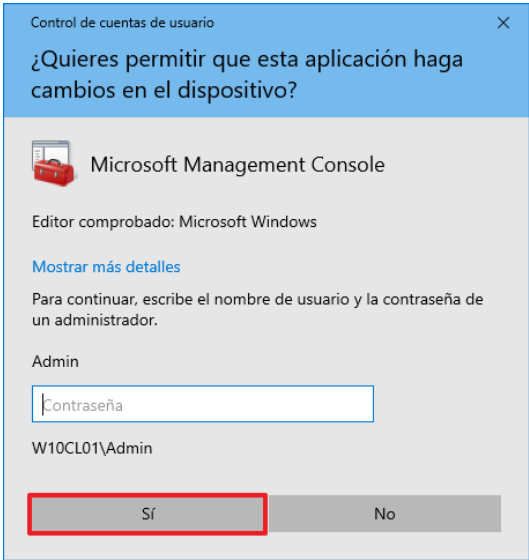
Paso	Descripción
8.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría alta del ENS / Difusión Limitada. 
9.	Una vez completado el proceso, deberá pulsar una tecla para continuar. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
10.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 categoria alta - DL” con el nombre de “plantilla_windows.log”. 

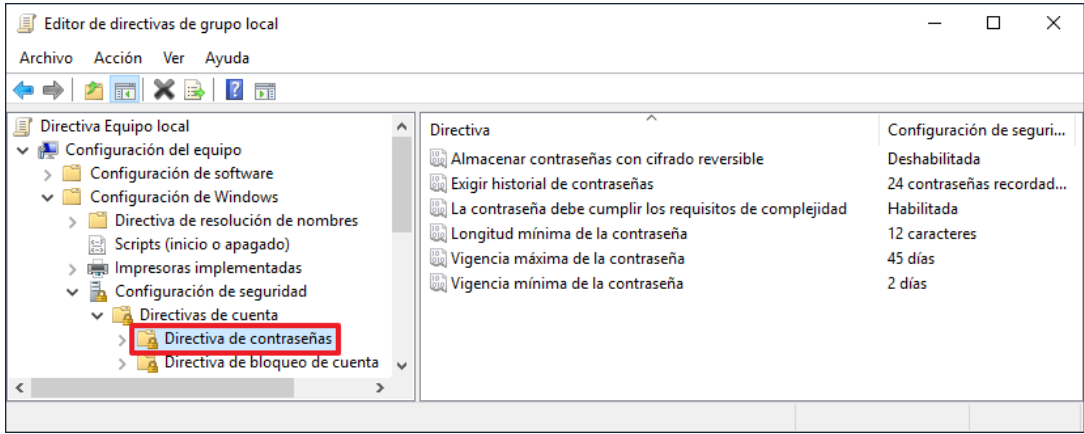
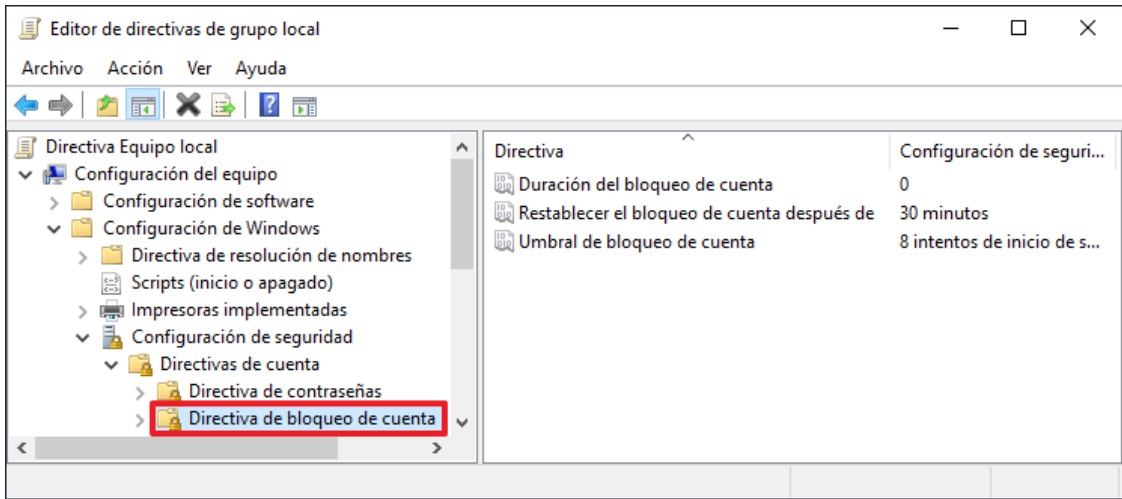
Paso	Descripción
11.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 5.
12.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Alta - DL – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.

Paso	Descripción
13.	Introduzca las credenciales y pulse el botón “Sí”. 
14.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local. 
15.	Completada la copia de los archivos, compruebe que no ha habido errores en la copia de los mismos. Debería obtener el mismo resultado que el mostrado en la siguiente imagen. Pulse una tecla para finalizar la ejecución del script.  Nota: En caso de haberse producido fallos, soluciónelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.

Paso	Descripción
16.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Alta - DL – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.
17.	Introduzca las credenciales y pulse el botón “Sí”. 
18.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría alta del ENS / Difusión Limitada. 

Paso	Descripción
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script.  <pre> C:\Windows\System32\cmd.exe Presione una tecla para continuar . . . Configurando servicios de Windows... C:\Windows\system32>secedit /configure /quiet /db "c:\scripts\servicios_windows.sdb" /cfg "c:\scripts\CCN-STIC-599B19 ENS categoria alta - DL\CCN-STIC-599B19 ENS Servicios categoria alta - DL.inf" /overwrite /log "c:\scripts\CCN-STIC-599B19 ENS categoria alta - DL\servicios_windows.log" Servicios de Windows configurados. ----- CCN-STIC-599B19 - Paso 3 : EJECUCION FINALIZADA ----- Presione una tecla para continuar . . . </pre>
20.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 ENS categoria alta - DL” con el nombre de “servicios_windows.log”. 
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 16.

Paso	Descripción
22.	Elimine la carpeta “C:\Scripts”
23.	Es factible que su organización cuente con una política de contraseñas consolidada. La implementación de la política de categoría alta implementará una política específica para los clientes de categoría alta. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.
24.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar la herramienta.
25.	Introduzca las credenciales y pulse el botón “Sí”. 

Paso	Descripción
26.	Despliegue la política y sitúese en la siguiente ruta: “Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña” 
27.	Evalúe la política de contraseñas y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de credenciales es menos rigurosa que la marcada en la configuración deseada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
28.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que “Directiva de contraseñas”. 
29.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración deseada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.

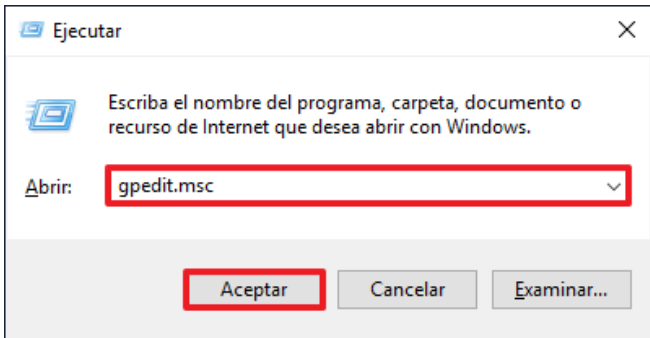
Hasta ahora han sido aplicados cambios, entre otros aspectos, sobre las directivas de contraseña y cuenta, aunque es importante señalar que existen más directivas interesantes a la hora de configurar el sistema.

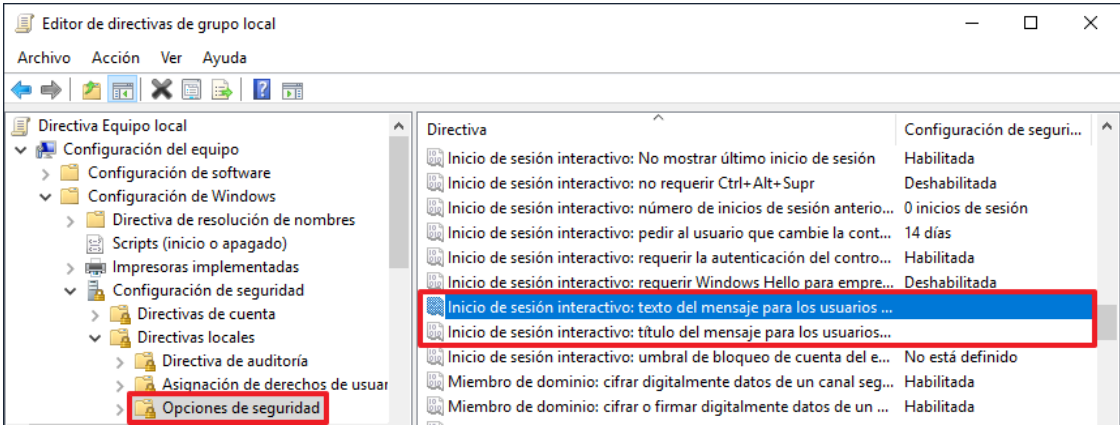
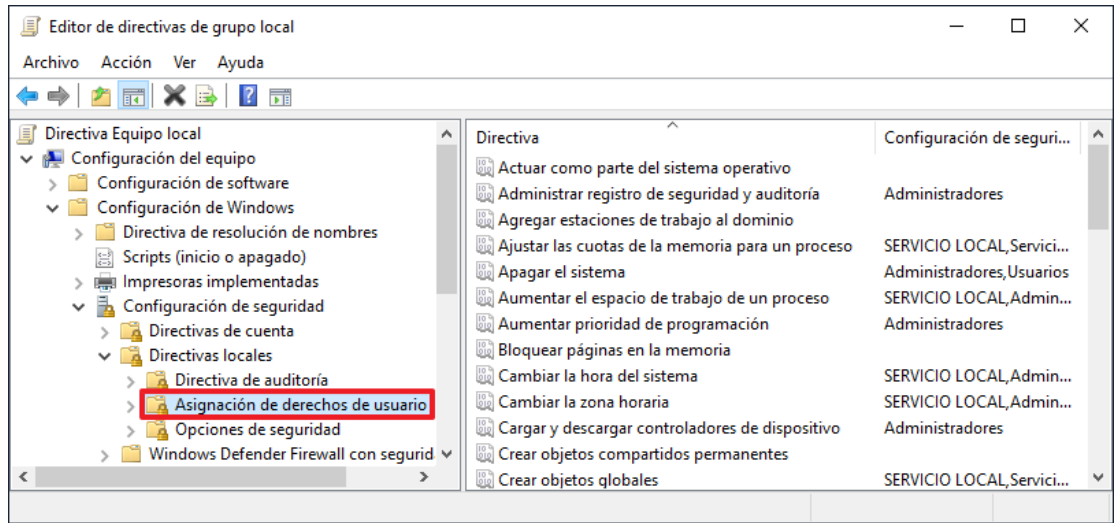
Uno de los aspectos que marca el ENS, desde su requisito de categoría alta en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

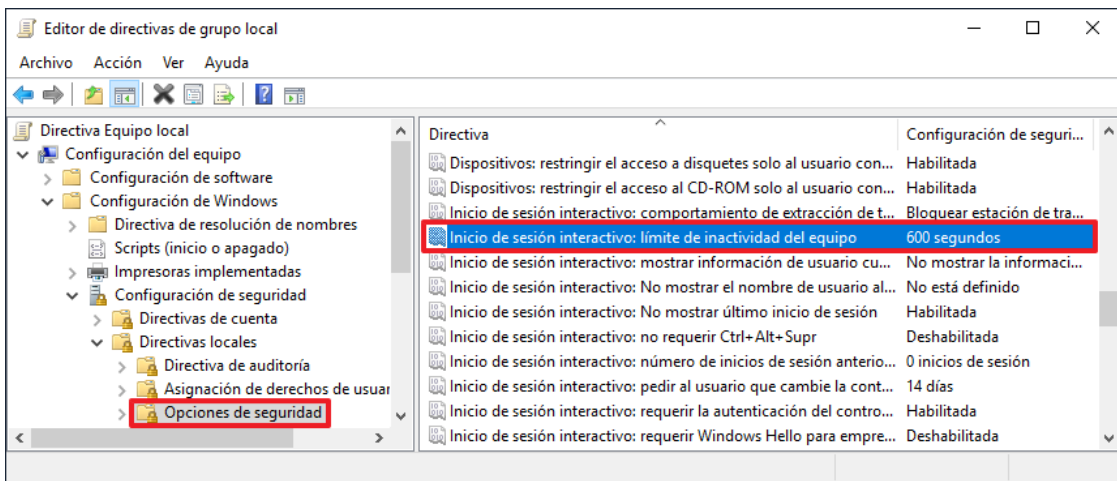
Los sistemas Windows presentan mecanismos para implementar mensajes que realizan advertencias al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

Si su organización no está haciendo uso de este mecanismo realice los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según queda estipulado en la política de seguridad de la organización.

Paso	Descripción
30.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
31.	Debe iniciar sesión con una cuenta que sea Administrador local.
32.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas "Windows + R", escriba "gpedit.msc" en la ventana emergente y pulse el botón "Aceptar".  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar la herramienta.
33.	Introduzca las credenciales y pulse el botón "Sí" .
34.	Para informar de las obligaciones sitúese en la siguiente ruta: "Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"

Paso	Descripción
35.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intenta iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intenta iniciar una sesión”. 
36.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
37.	Por último, la política de seguridad local especifica unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así deberá realizar las modificaciones sobre la configuración de política local.
38.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 

Paso	Descripción
39.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
40.	Se establece a partir de la categoría media, según MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de la política local aplicable sobre equipo, puede establecerse la medida de protección que habilita el protector de pantalla y por lo tanto el bloqueo de la sesión. Nota: Si la organización presenta algún mecanismo para realizar el bloqueo del equipo ante inactividad no es necesario que aplique la siguiente configuración. No obstante, revise la configuración para adaptarse a la normativa vigente. Si la organización no tiene medidas dispuestas siga los siguientes pasos.
41.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad” Habilite y configure la siguiente directiva de seguridad: – Inicio de sesión interactivo: límite de inactividad del equipo. Establezca el valor en 600 segundos (10 minutos). 
42.	Cierre el editor de política de grupo local.
43.	Reinicie el puesto de trabajo.

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

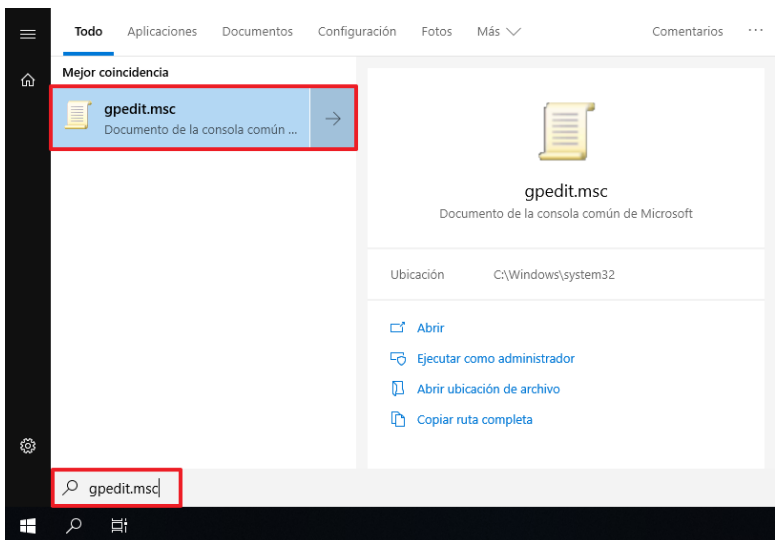
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO A.4.1.PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA”.

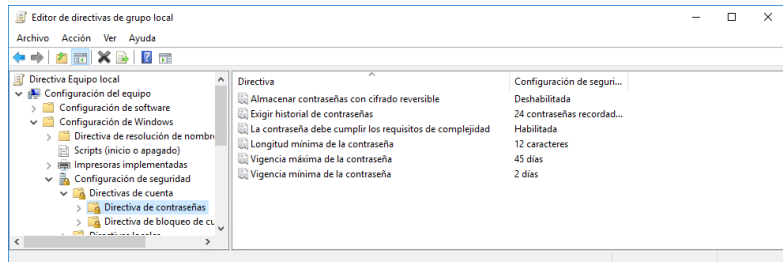
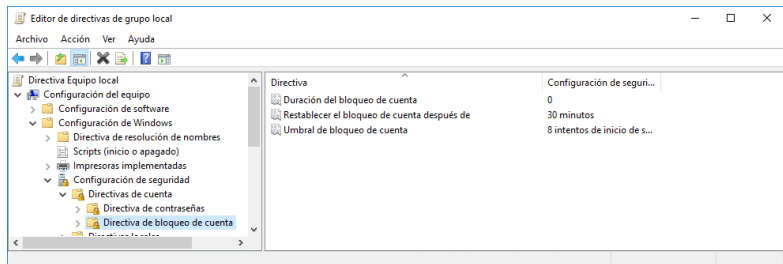
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes Windows 10 (versión 1809) Enterprise con opción de mantenimiento LTSC, independientes con implementación de seguridad de categoría alta del ENS/Difusión Limitada.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de administrador local.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario que es administrador local. Las consolas y herramientas que se utilizarán son las siguientes:

- Editor de objetos de directiva de grupo local (gpedit.msc)
- Editor de registro (regedit.exe)
- Visor de Eventos (eventvwr.exe)
- Servicios (services.msc)

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de administración local.
2. Inicie la aplicación de gestión de políticas locales.		Ejecute el “Editor de objetos de directiva de grupo local”. Para ello pulse “Inicio”, teclee “gpedit.msc” y pulse “Enter”. 

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas” Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. 
4. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta” 

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Umbral de bloqueo de cuenta	8 intentos de inicio de sesión no válidos	
5. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”		
		Directiva	Valor	OK/NOK
		Auditar el acceso a objetos	Correcto, Erróneo	
		Auditar el acceso del servicio de directorio	Correcto, Erróneo	
		Auditar el cambio de directivas	Correcto, Erróneo	
		Auditar el uso de privilegios	Correcto, Erróneo	
		Auditar eventos de inicio de sesión	Correcto, Erróneo	
		Auditar eventos de inicio de sesión de cuenta	Correcto, Erróneo	
		Auditar eventos del sistema	Correcto, Erróneo	
		Auditar la administración de cuentas	Correcto, Erróneo	
6. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”		
		Directiva	Valor	OK/NOK
		Actuar como parte del sistema operativo		
		Administrar registro de seguridad y auditoría	Administradores	
		Agregar estaciones de trabajo al dominio		
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Apagar el sistema	Administradores, Usuarios
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL, Usuarios
		Aumentar prioridad de programación	Administradores
		Bloquear páginas de la memoria	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores
		Cargar y descargar controladores de dispositivo	Administradores
		Crear objetos compartidos permanentes	
		Crear objetos globales	SERVICIO LOCAL, Servicio de red, Administradores, SERVICIO
		Crear un archivo de paginación	Administradores
		Crear un objeto símbolo (token)	
		Crear vínculos simbólicos	Administradores
		Denegar el acceso desde la red	ANONYMOUS LOGON, Invitados
		Denegar el inicio de sesión como servicio	Invitados
		Denegar el inicio de sesión como trabajo por lotes	Invitados
		Denegar el inicio de sesión local	Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red
		Generar perfiles de un solo proceso	Administradores
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	
		Hacer copias de seguridad de archivos y directorios	Administradores

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Iniciar sesión como proceso por lotes	
		Iniciar sesión como servicio	
		Modificar la etiqueta de un objeto	
		Modificar valores de entorno firmware	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	
		Obtén un token de suplantación para otro usuario de la misma sesión	Administradores
		Omitir comprobación de recorrido	SERVICIO LOCAL, Servicio de Red, Administradores, Usuarios Autenticados
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento de volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL
		Tener acceso a este equipo desde la red	Administradores, Usuarios
		Tomar posesión de archivos y otros objetos	Administradores
7. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Acceso a redes: canalizaciones con nombre accesibles anónimamente	
		Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias
		Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Habilitada
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Server Applications Software\Microsoft\WindowsNT\CurrentVersion

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	System\CurrentControlSet\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada	
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada	
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada	
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitada	
		Auditoría: auditar el acceso a objetos globales del sistema	Habilitada	
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Habilitada	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada
		Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Habilitada
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de registro en diferentes ubicaciones por usuario	Habilitada
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	Habilitada
		Cuentas: cambiar el nombre de cuenta de invitado	invitado
		Cuentas: cambiar el nombre de la cuenta de administrador	Administrador
		Cuentas: estado de la cuenta de administrador	Deshabilitada
		Cuentas: estado de la cuenta de invitado	Deshabilitada
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Deshabilitada
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada
		Dispositivos: restringir el acceso a disquetes solo al usuario con sesión iniciada localmente	Habilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Dispositivos: restringir el acceso al CD-ROM solo al usuario con sesión iniciada localmente	Habilitada
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		Inicio de sesión interactivo: mostrar información de usuario cuando bloquee la sesión	No mostrar la información del usuario
		Inicio de sesión interactivo: No mostrar último inicio de sesión	Habilitada
		Inicio de sesión interactivo: No requerir Ctrl + Alt + Supr	Deshabilitada
		Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	0 inicios de sesión
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada
		Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	Deshabilitada
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada
		Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada
		Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Habilitada
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits
		Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits
		Servidor de red de Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos	
8. Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Administración de derechos digitales de Windows”		
		Directiva	Valor	OK/NOK
		Impedir el acceso a internet de Windows Media DRM	Habilitada	
9. Verifique la directiva de almacén digital en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitada	
10. Verifique la directiva de Antivirus en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
11. Verifique la directiva de asistencia en línea en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitada	
12. Verifique las directivas de biometría en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Habilitada	
		Permitir que los usuarios de dominio inicien sesión mediante biometría	Habilitada	
		Permitir que los usuarios inicien sesión mediante biometría	Habilitada	
13. Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	
		Permitir el uso de Cortana	Deshabilitada	
14. Verifique las directivas de contenido en la nube en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Contenido en la Nube”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar experiencias del consumidor de Microsoft	Habilitada	
		No mostrar recomendaciones de Windows	Habilitada	
15. Verifique las directivas de reproducción automática en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar reproducción automática	Habilitada (Todas las unidades)	
		Establece el comportamiento predeterminado para la ejecución automática	Habilitada (No ejecutar ningún comando de ejecución automática)	
16. Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar Windows SmartScreen de Windows Defender	Habilitada (Advertir e impedir la omisión)	
17. Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitada	
		No enviar datos adicionales	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
18. Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		
		Directiva	Valor	OK/NOK
		Activar sitios sugeridos	Deshabilitada	
		Impedir la administración del filtro SmartScreen	Deshabilitada	
		Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	Habilitada	
19. Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de Internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitada	
20. Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Eliminar el historial de exploración”		
		Directiva	Valor	OK/NOK
		Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento.	Deshabilitada	
		Impedir que se elimine el historial de descarga	Deshabilitada	
		Impedir que se eliminen contraseñas	Deshabilitada	
		Impedir que se eliminen cookies	Deshabilitada	
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitada	

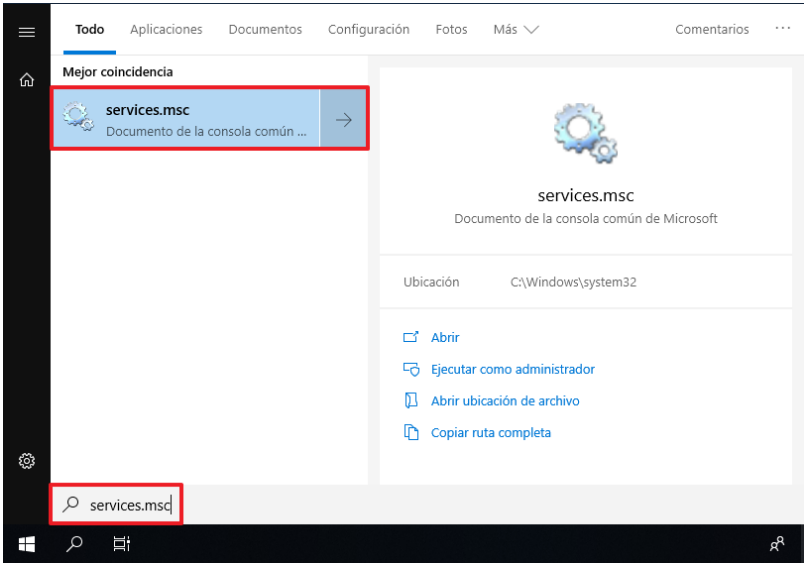
Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Impedir que se eliminen los archivos temporales de Internet		Deshabilitada	
	Impedir que se eliminen los datos de filtrado InPrivate		Deshabilitada	
	Impedir que se eliminen los datos de formularios		Deshabilitada	
	Impedir que se eliminen los sitios web que el usuario visitó		Deshabilitada	
	Permitir que se elimine el historial de exploración al salir		Habilitada	
21. Verifique las directivas de OneDrive en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → OneDrive”			
	Directiva		Valor	OK/NOK
	Impedir el uso de OneDrive para almacenar archivos.		Habilitada	
22. Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”			
	Directiva		Valor	OK/NOK
	Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario		Habilitada	
	Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario		Habilitada	
23. Verifique las directivas de optimización de entrega en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”			

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitada (Solo HTTP (0))	
24. Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitada (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitada (Forzar denegación)	
25. Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”		
		Directiva	Valor	OK/NOK
		No volver a mostrar notificaciones de comentarios	Habilitada	
		Permitir telemetría	Habilitada	
26. Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”		
		Directiva	Valor	OK/NOK
		Permitir acceso a Shell remoto	Deshabilitada	
27. Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitada (Advertir e impedir la omisión)	
28. Verifique la directiva de tienda en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitada	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitada	
29. Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
30. Verifique la directiva de Windows Update en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitada (Deshabilitar preliminares)	

Comprobación	OK/NOK	Cómo hacerlo		
31. Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		
	Directiva		Valor	OK/NOK
	Desactivar el aprendizaje automático		Habilitada	
32. Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
	Directiva		Valor	OK/NOK
	Desactivar el acceso a Store		Habilitada	
	Desactivar el contenido “¿Sabías que...?” del Centro de ayuda y soporte técnico		Habilitada	
	Desactivar el informe de errores de Windows		Habilitada	
	Desactivar el Programa para la mejora de la experiencia del usuario de Windows		Habilitada	
	Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger		Habilitada	
	Desactivar informe de errores de reconocimiento de escritura a mano		Habilitada	
	Desactivar la actualización de archivos de contenido del Asistente para búsqueda		Habilitada	
	Desactivar búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico		Habilitada	
	Desactivar la tarea de imágenes “Pedir copias fotográficas”		Habilitada	
	Desactivar los vínculos “Event.asp” del Visor de eventos		Habilitada	
	Desactivar uso compartido de datos de personalización de escritura a mano		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
33. Verifique la directiva de Net Logon en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Net Logon”		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada	
34. Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Perfiles de usuario”		
		Directiva	Valor	OK/NOK
		Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)	Habilitada	
		Desactivar el identificador de publicidad	Habilitada	
35. Verifique el modo de configuración de los servicios del sistema.		Ejecute la herramienta de servicios. Para ello pulse “Inicio”, teclee “services.msc” y pulse “Enter”. 		

Comprobación	OK/NOK	Cómo hacerlo		
		Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto, entre paréntesis) para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de escucha Net.Msmq	NetMsmqActivator	Automático	Configurado	
Adaptador de escucha Net.Pipe	NetPipeActivator	Automático	Configurado	
Adaptador de escucha Net.Tcp	NetTcpActivator	Automático	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado	
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado	
Administración remota de Windows (WS-Management)	WinRM	Manual	Configurado	
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administrador de conexiones de acceso remoto	RasMan	Automático	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado	
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado	
Administrador de credenciales	VaultSvc	Manual	Configurado	
Administrador de cuentas de seguridad	SamSs	Automático	Configurado	
Administrador de cuentas web	TokenBroker	Manual	Configurado	
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado	
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado	
Administrador de pagos y NFC/SE	SEMgrSvc	Manual	Configurado	
Administrador de sesión local	LSM	Automático	Configurado	
Administrador de usuarios	UserManager	Automático	Configurado	
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	
Agente de directiva IPsec	PolicyAgent	Manual	Configurado	
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado	
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Automático	Configurado		
Agrupación de red del mismo nivel	p2psvc	Manual	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Manual	Configurado		
Asignador de detección de topologías de nivel de vínculo	ltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Audio de Windows	Audiosrv	Automático	Configurado		
Autenticación natural	NaturalAuthentication	Manual	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Manual	Configurado		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		
CaptureService	CaptureService	Manual	Configurado		
Carpetas de trabajo	workfoldersvc	Manual	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente para NFS	NfsClnt	Automático	Configurado		
Cliente web	WebClient	Manual	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Automático	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Conexiones de red	Netman	Manual	Configurado		
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración automática de WLAN	WlanSvc	Manual	Configurado		
Configuración automática de WWAN	WwanSvc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado		
ConsentUX	ConsentUxUserSvc	Manual	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Automático	Configurado		
Detección de hardware shell	ShellHWDetection	Automático	Configurado		
Detección SSDP	SSDPSRV	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
DevicePicker	DevicePickerUserSvc	Manual	Configurado		
DevicesFlow	DevicesFlowUserSvc	Manual	Configurado		
Diagnostic Execution Service	diagsvc	Manual	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Manual	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
Energía	Power	Automático	Configurado		
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado		
Escucha de RIP	iprip	Automático	Configurado		
Estación de trabajo	LanmanWorkstation	Automático	Configurado		
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado		
Examinador de equipos	Browser	Manual	Configurado		
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado		
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado		
Fax	Fax	Manual	Configurado		
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado		
Firewall de Windows	MpsSvc	Automático	Configurado		
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado		
Hora de Windows	W32Time	Manual	Configurado		
Host de proveedor de detección de función	fdPHost	Manual	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Manual	Configurado		
Host del servicio de diagnóstico	WdiServiceHost	Manual	Configurado		
Identidad de aplicación	AppIDSvc	Manual	Configurado		
Información de la aplicación	Appinfo	Manual	Configurado		
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Inicio de sesión secundario	seclogon	Manual	Configurado		
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado		
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado		
Instantáneas de volumen	VSS	Manual	Configurado		
Instrumental de administración de Windows	Winmgmt	Automático	Configurado		
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
LxssManager	LxssManager	Manual	Configurado		
Message Queue Server	MSMQ	Automático	Configurado		
MessagingService	MessagingService	Manual	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Manual	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	Configurado		
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Manual	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Manual	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Manual	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado		
Registrador de configuración de Windows Connect Now	wcnscvc	Manual	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Manual	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Manual	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio AVCTP	BthAvctpSvc	Manual	Configurado	
Servicio biométrico de Windows	WbioSrv	Manual	Configurado	
Servicio Cifrado de unidad BitLocker	BDESVC	Automático	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administración de web	WMSVC	Manual	Configurado	
Servicio de administración de Windows	WManSvc	Manual	Configurado	
Servicio de administración IIS	IISADMIN	Automático	Configurado	
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asistente para perfil local	wlpasvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Automático	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdwn	Manual	Configurado	
Servicio de cliente de protección de host	HgClientService	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de datos espacial	SharedRealitySvc	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado	
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado	
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado	
Servicio de geolocalización	lfsvc	Manual	Configurado	
Servicio de historial de archivos	fhsvc	Manual	Configurado	
Servicio de host HV (Hyper-V)	HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de instalación de Microsoft Store	InstallService	Manual	Configurado		
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de mejora de visualización	DisplayEnhancementService	Manual	Configurado		
Servicio de monitor de infrarrojos	irmon	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Manual	Configurado		
Servicio de percepción de Windows	spectrum	Manual	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Manual	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		

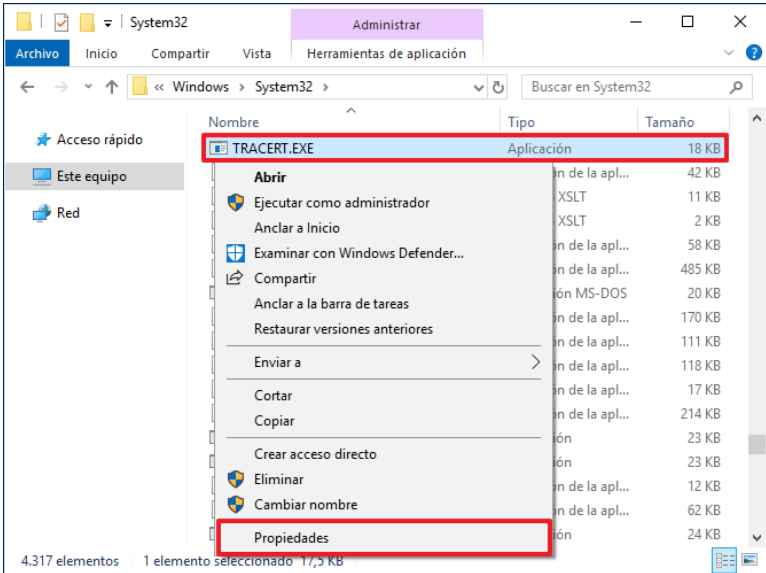
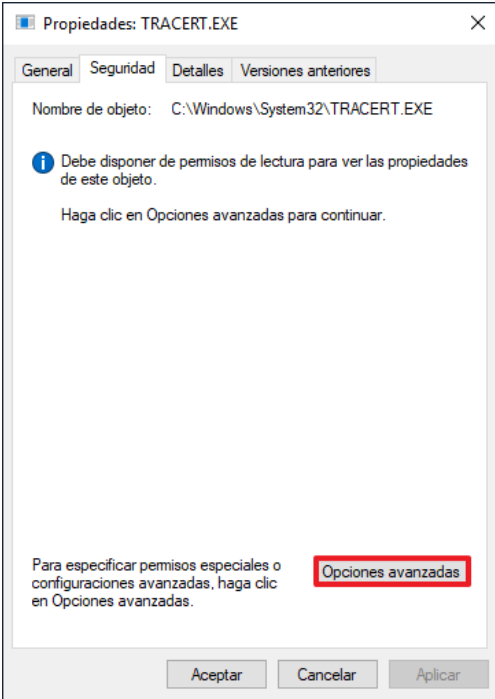
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado	
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Manual	Configurado	
Servicio de publicación World Wide Web	W3SVC	Automático	Configurado	
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado	
Servicio de registro de W3C	w3logsvc	Manual	Configurado	
Servicio de reparación MultiPoint	WmsRepair	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Manual	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Automático	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Manual	Configurado	

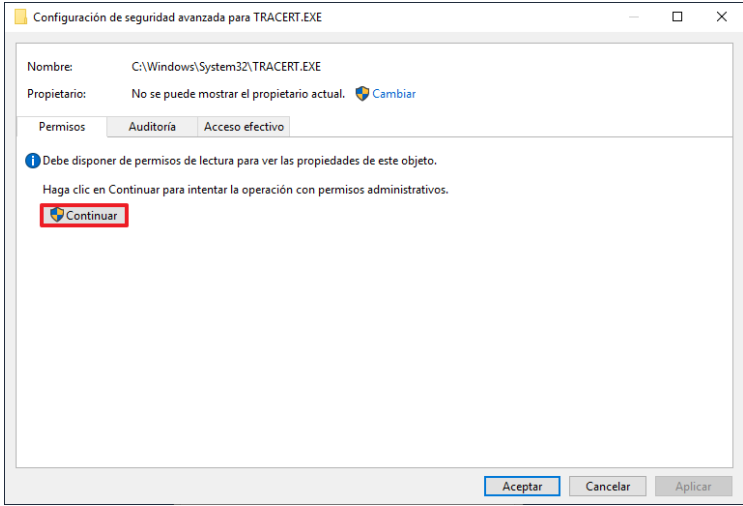
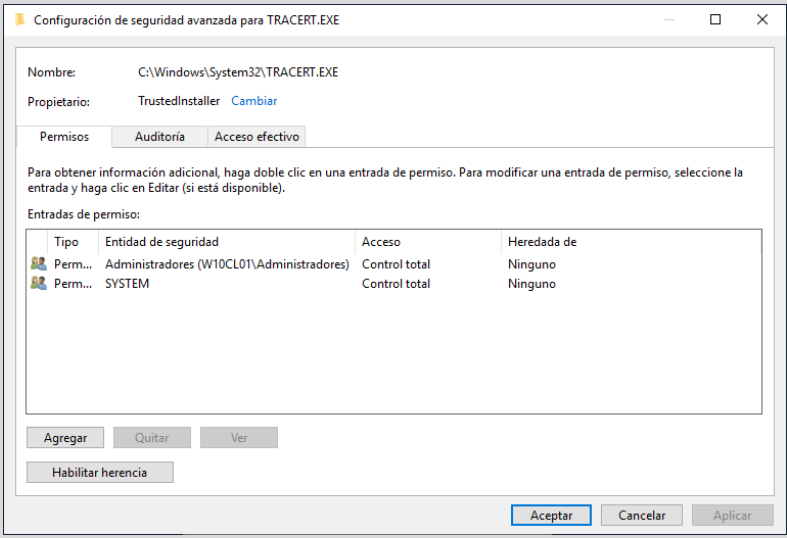
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado		
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Automático	Configurado		
Servicio de usuario del portapapeles	cbdhsvc	Manual	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Manual	Configurado		
Servicio de Windows Defender	WinDefend	Manual	Configurado		
Servicio de Windows Insider	wisvc	Manual	Configurado		
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado		
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado		
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Manual	Configurado		
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado		
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio FTP de Microsoft	ftpsvc	Automático	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio LPD	LPDSVC	Automático	Configurado		
Servicio MultiPoint	Wms	Automático	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado		
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standard.collector.service	Manual	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio telefónico	PhoneSvc	Manual	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Manual	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Manual	Configurado		
Servicios simples de TCP/IP	simptcp	Automático	Configurado		
Servidor	LanmanServer	Automático	Configurado		
Servidor de roles de DS	DsRoleSvc	Manual	Configurado		
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado		
Sincronizar host	OneSyncSvc	Automático	Configurado		
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado		
Sistema de eventos COM+	EventSystem	Automático	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado		
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado		
Superfetch	SysMain	Automático	Configurado		
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado		
Telefonía	TapiSrv	Manual	Configurado		
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado		
Temas	Themes	Automático	Configurado		
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado		
Uso de datos	DusmSvc	Automático	Configurado		
WalletService	WalletService	Manual	Configurado		
WarpJITSvc	WarpJITSvc	Manual	Configurado		
Windows Installer	msiserver	Manual	Configurado		
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Manual	Configurado		
Windows Search	WSearch	Automático	Configurado		
Windows Update	wuauserv	Manual	Configurado		
Windows Update Medic Service	WaaSMedicSvc	Manual	Configurado		
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo
36. Verifique los permisos asignados a ficheros y carpetas.		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione la opción “Propiedades”.  Nota: Deberá tener precaución para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”. 

Comprobación	OK/NOK	Cómo hacerlo
		Es posible que deba pulsar sobre el botón “Continuar” para ver los permisos asignados.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. En la ventana resultante, compruebe los permisos asignados a cada carpeta o fichero. Nota: Tenga en consideración que es posible que algunos ficheros no se encuentren en el sistema debido a la configuración aplicada y según las necesidades que requiera su organización. 

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%Public%\		Administradores	Control total	
		System	Control total	
		Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\security		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control total	
%SystemRoot%\system32\raschap.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\rastls.dll		Administradores	Control total	
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

ANEXO A.4.3. IMPLEMENTACIÓN DE BITLOCKER PARA CIFRADO DE DISCO EN CLIENTES WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

Tal y como se comentó en el punto “1.2.1.2. MP. EQ. 3. PROTECCIÓN DE LOS PORTÁTILES” sobre las medidas de protección de los portátiles en la categoría alta, es una necesidad de cumplimiento la implementación de medidas que garantizaran la confidencialidad de los datos almacenados. La implementación de BitLocker como mecanismo para el cifrado, permite garantizar el cumplimiento de esta medida.

Recuerde que no es una exigencia del ENS el que se haga implementación de BitLocker, puede hacer uso de otra solución que garantice la confidencialidad de los datos y que cumpla con los requerimientos de criptografía.

Este anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar la implementación de cifrado. Debe tomarse en consideración que el cifrado con BitLocker se basa en el uso de un sistema de cifrado basado en AES más CBC y un difusor denominado Elephant. No obstante, para poder acceder a la información cifrada es necesaria hacer uso de una clave de descifrado almacenada en una unidad flash USB o un PIN que libera la clave almacenada en el módulo de plataforma segura (TPM).

Se aconseja el uso de TPM como mecanismo para garantizar la funcionalidad de BitLocker. Aunque podría implementarse la unidad flash USB para almacenar la clave de descifrado, se desaconseja dicho mecanismo puesto que sería bastante habitual que el usuario ubicara dicha unidad en la misma ubicación donde transporta el portátil. Ante un eventual robo o pérdida del maletín, se estaría facilitando el mecanismo para acceder a la información cifrada.

Debe tener en cuenta que ante un potencial problema del módulo TPM podría necesitar acceder a la información cifrada sin la posibilidad de uso del mismo. BitLocker permite generar una clave de recuperación que almacenada de forma original en un dispositivo de memoria USB deberá almacenar posteriormente en algún lugar seguro.

Todas aquellas organizaciones que tengan acuerdo con Microsoft para cliente con Software Assurance tendrán a su disposición la solución MDOP (Microsoft Desktop Optimization Pack).

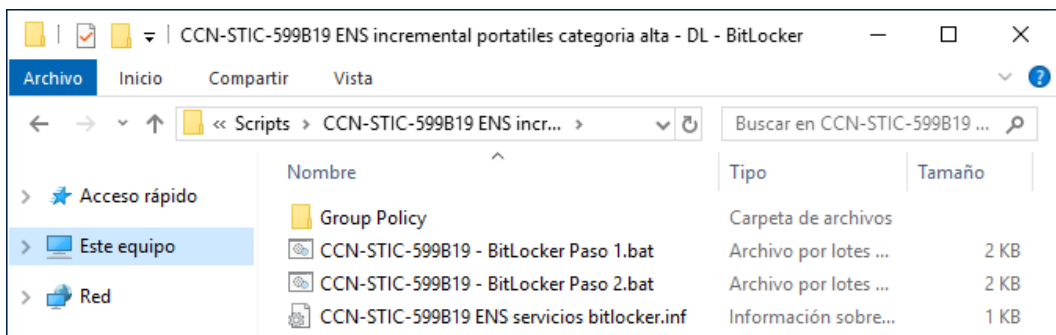
La implementación de BitLocker requiere de ciertos requisitos de tipo hardware y software:

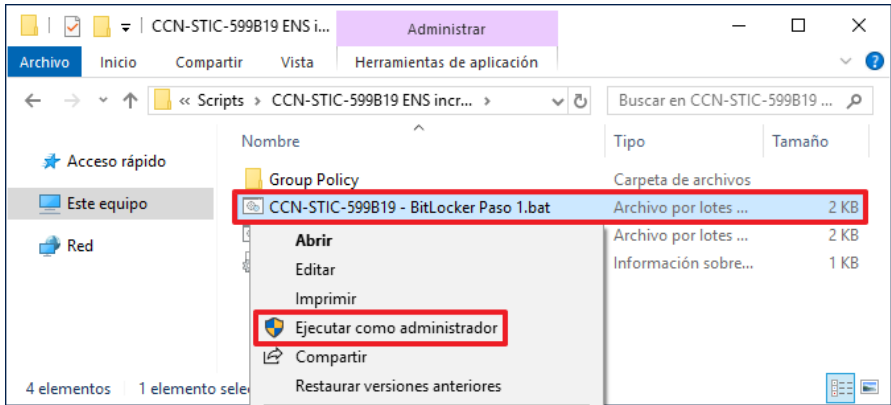
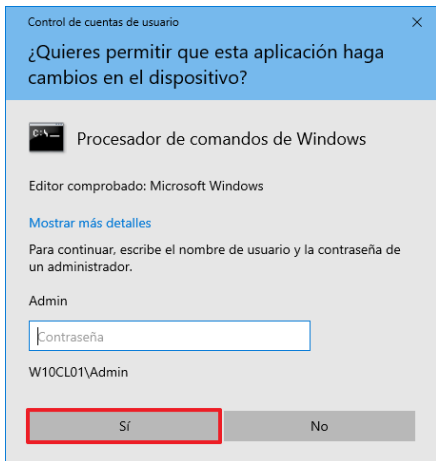
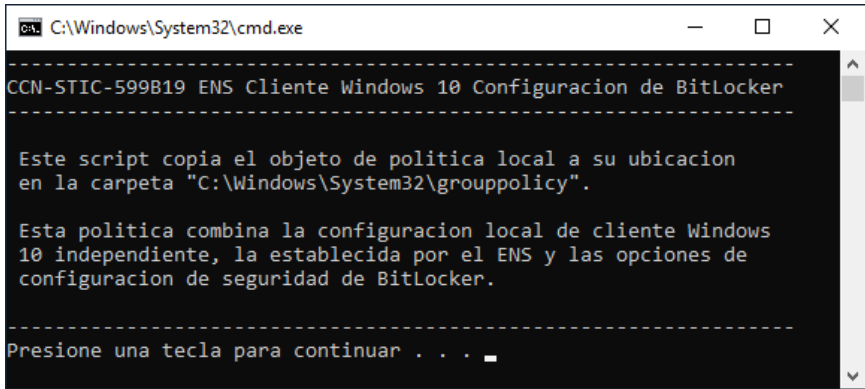
- a) Un equipo que cumpla los requisitos mínimos para Windows 10.
- b) Un chip TPM versión 1.2 o 2.0 activado. La activación de dicho chip se realiza a través del BIOS, siendo necesaria su implementación para garantizar su funcionalidad.
- c) BIOS compatible con TCG (Trusted Computing Group).
- d) Una partición de disco para la unidad del sistema, además de la partición que alberga el sistema operativo. En Windows 10, si cuenta con una sola partición de disco, BitLocker preparará automáticamente la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema que albergará los archivos del sistema que se necesitan para iniciar o recuperar el sistema operativo y que no se pueden cifrar. Esta unidad no tendrá una letra de unidad para evitar que se almacenen archivos de datos en esta unidad sin darse cuenta. Una vez que la unidad está preparada, debe reiniciarse el equipo.

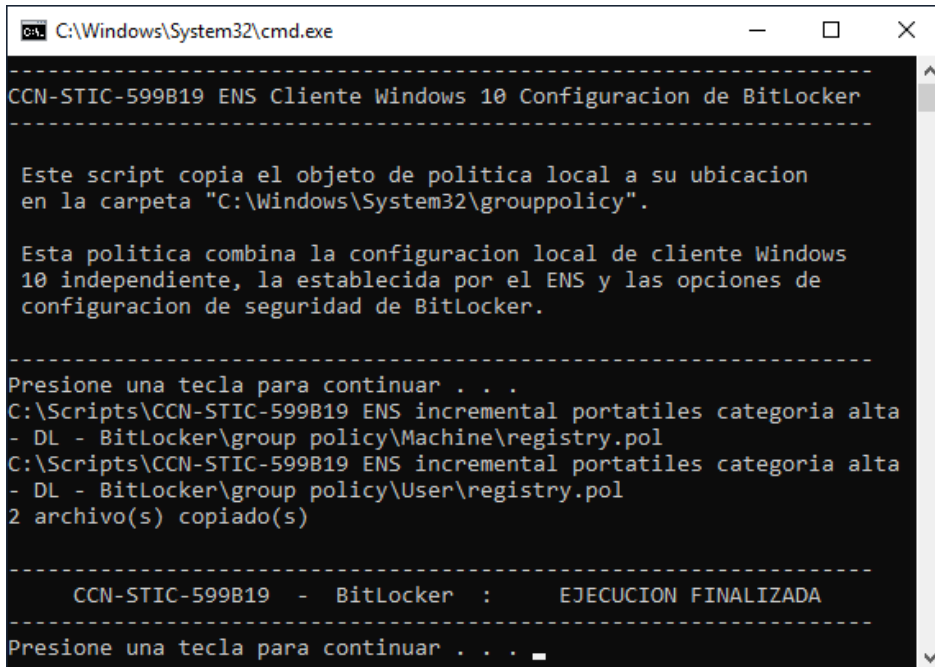
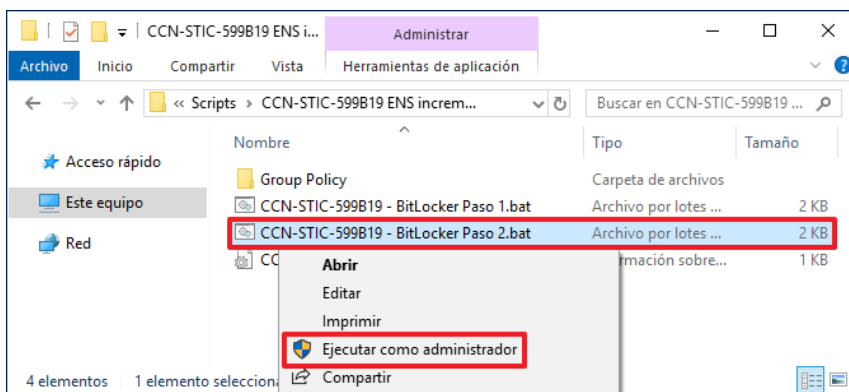
No obstante, si se ha realizado una instalación por defecto de Windows 10, el programa de instalación ya habrá creado, durante la instalación, las dos particiones de disco necesarias para activar BitLocker.

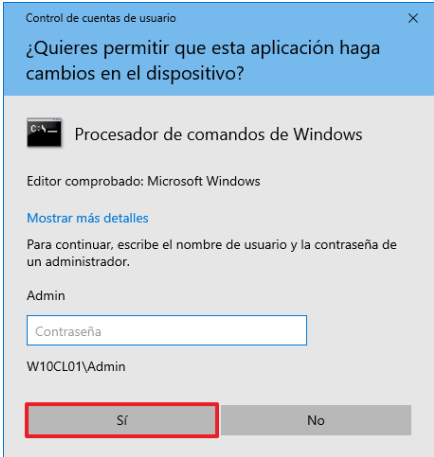
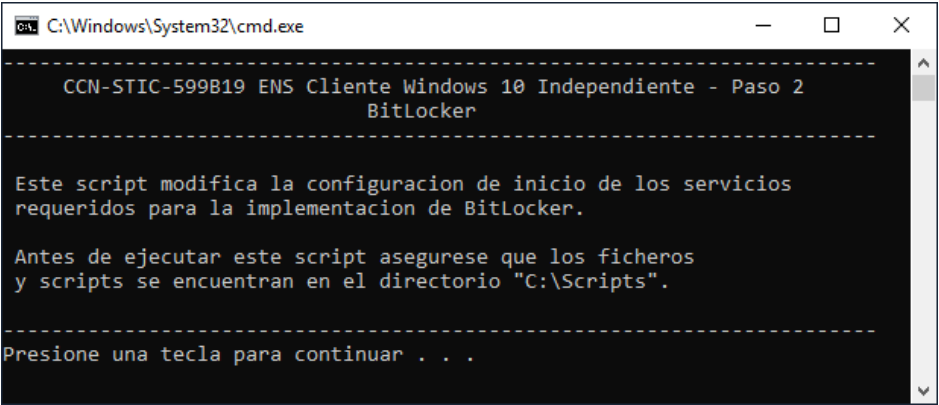
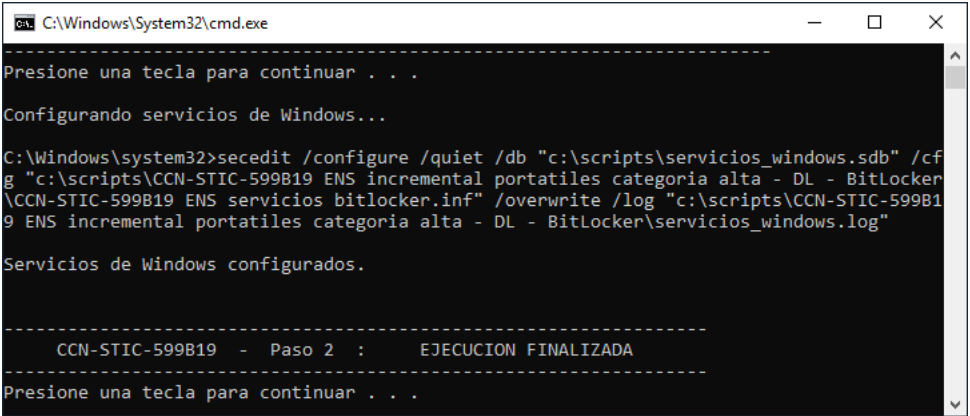
- a) Una unidad flash USB para almacenar claves de inicio y recuperación.
- b) Una configuración BIOS para iniciar primero desde el disco duro, no desde las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como la clave de recuperación), el BIOS debe admitir la lectura de unidades flash USB en el inicio.
- c) Opcionalmente, se puede disponer de una impresora conectada y configurada, para la impresión de las claves de recuperación. Alternativamente, se podrá tomar nota manualmente de las claves de recuperación.

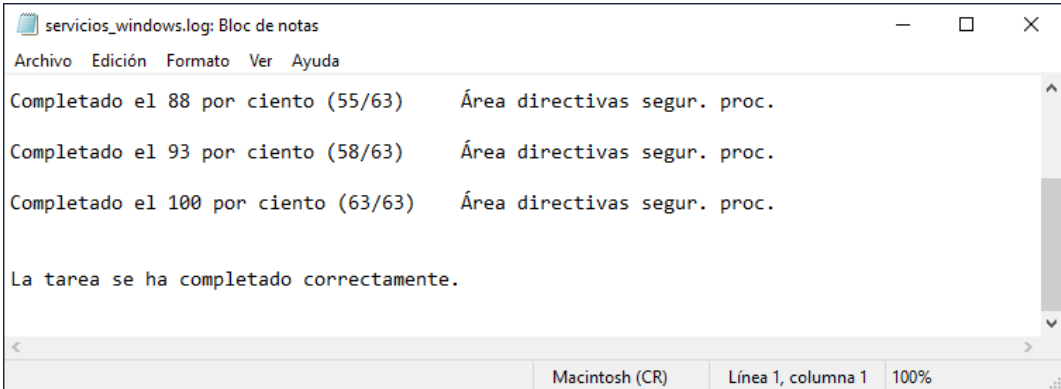
La implementación de BitLocker se basará en la aplicación de una política de seguridad aplicada sobre un grupo de equipos determinados. Para ello deberán seguirse los siguientes pasos.

Paso	Descripción
1.	Inicie sesión en el cliente con un usuario con privilegios de administrador
2.	Cree el directorio "Scripts" en la unidad C:\.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
	Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19".
4.	Abra la carpeta "CCN-STIC-599B19 ENS incremental portátiles categoria alta – DL - BitLocker" que encontrará en la carpeta "C:\Scripts" que ha copiado.  Nota: Los scripts asumen que su ubicación es "C:\Scripts\CCN-STIC-599B19 ENS incremental portátiles categoria alta – DL - BitLocker". De no ser así deberá modificar los scripts para que coincidan con la ruta deseada.

Paso	Descripción
5.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 BitLocker Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.
6.	Introduzca las credenciales y pulse el botón “Sí”. 
7.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local para el uso de BitLocker. 

Paso	Descripción
8.	Completada la copia de los archivos, pulse una tecla para finalizar la ejecución del script. Compruebe que no ha habido errores en la copia de los archivos. Debería obtener el mismo resultado que se muestra en la imagen siguiente.  <pre> C:\Windows\System32\cmd.exe ----- CCN-STIC-599B19 ENS Cliente Windows 10 Configuracion de BitLocker ----- Este script copia el objeto de politica local a su ubicacion en la carpeta "C:\Windows\System32\grouppolicy". Esta politica combina la configuracion local de cliente Windows 10 independiente, la establecida por el ENS y las opciones de configuracion de seguridad de BitLocker. ----- Presione una tecla para continuar . . . C:\Scripts\CCN-STIC-599B19 ENS incremental portatiles categoria alta - DL - BitLocker\group policy\Machine\registry.pol C:\Scripts\CCN-STIC-599B19 ENS incremental portatiles categoria alta - DL - BitLocker\group policy\User\registry.pol 2 archivo(s) copiado(s) ----- CCN-STIC-599B19 - BitLocker : EJECUCION FINALIZADA ----- Presione una tecla para continuar . . . </pre> Nota: En caso de haberse producido fallos, solúcelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.
9.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 BitLocker Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.

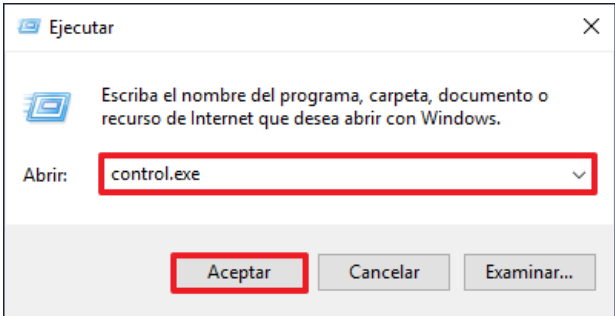
Paso	Descripción
10.	Introduzca las credenciales y pulse el botón “Sí”. 
11.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la implementación de BitLocker. 
12.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 
13.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 incremental portatiles categoria alta – DL - Bitlocker” con el nombre de “servicios_windows.log”.

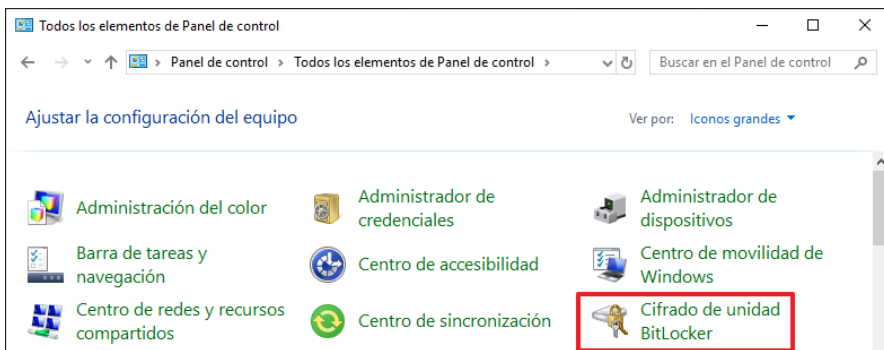
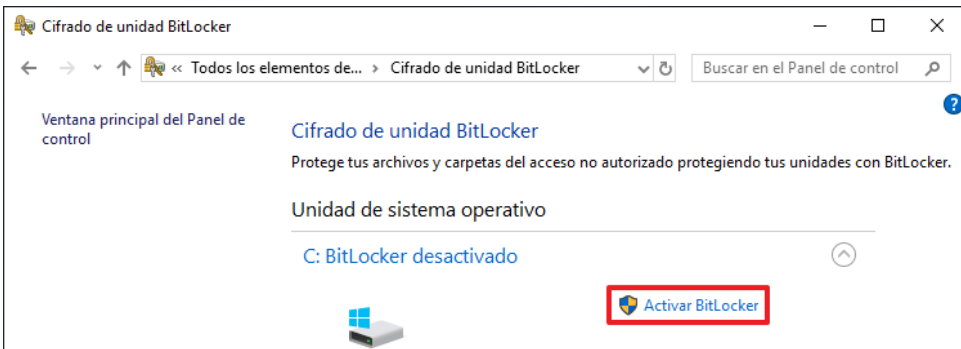
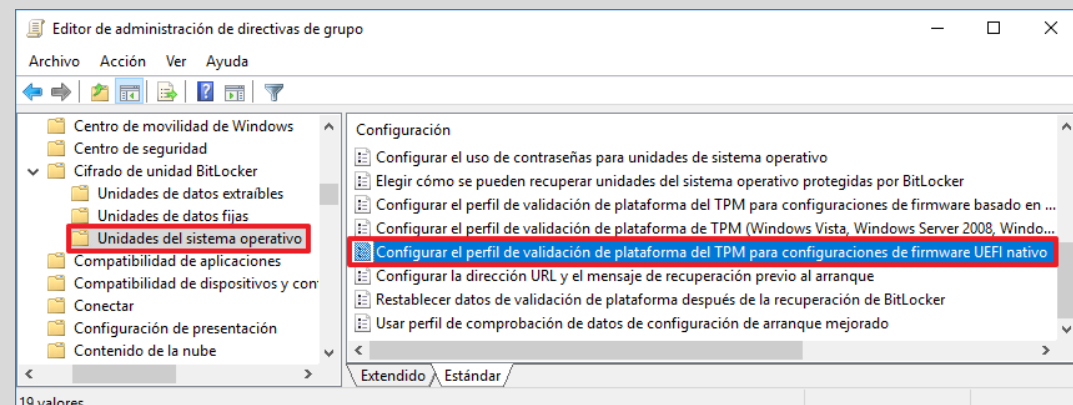
Paso	Descripción
14.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 4.
15.	Elimine la carpeta “C:\Scripts” y reinicie el puesto de trabajo.

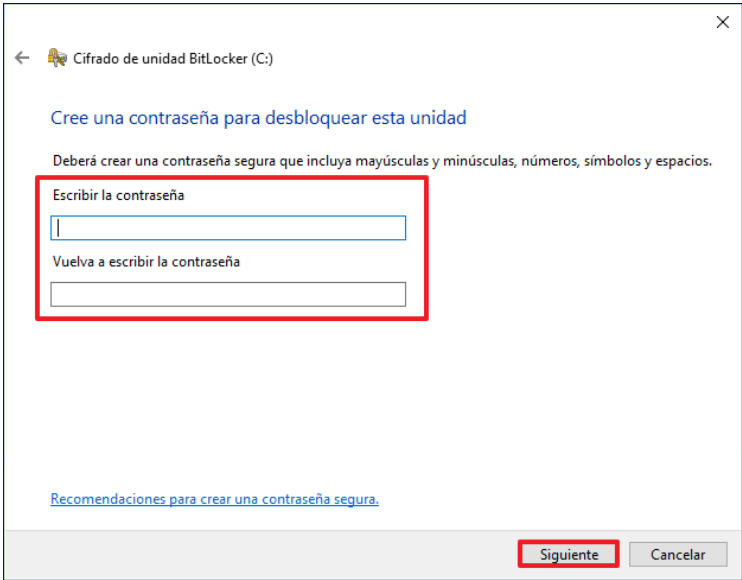
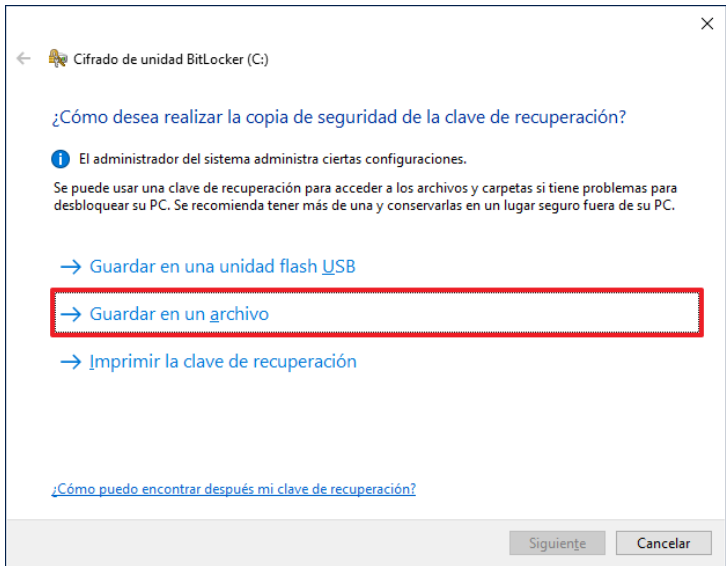
Si se cambia el TPM asociado al cifrado de unidad BitLocker o si alguien intenta iniciar el equipo desde un disco para evitar el sistema operativo, el equipo cambiará el modo de recuperación hasta que se suministre la clave de recuperación. Si se pierde la contraseña o PIN o bien hay un fallo, se puede entrar a través del modo de recuperación introduciendo la contraseña de recuperación.

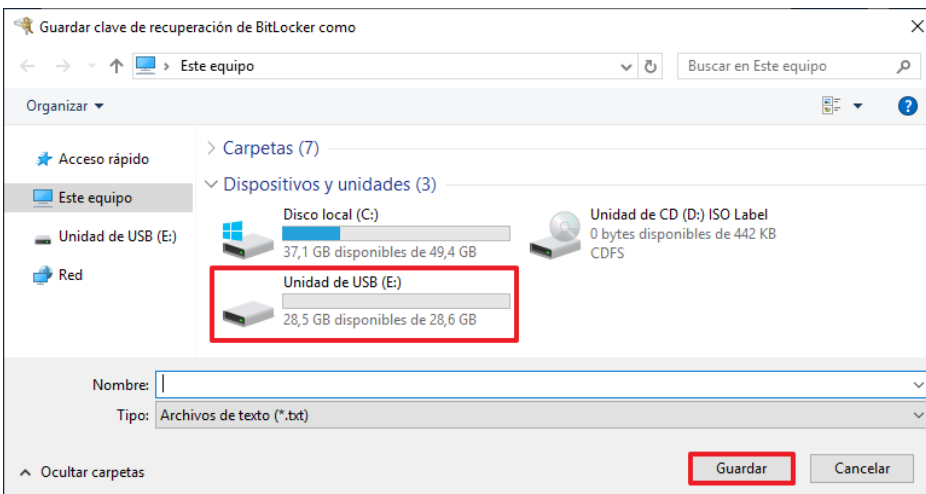
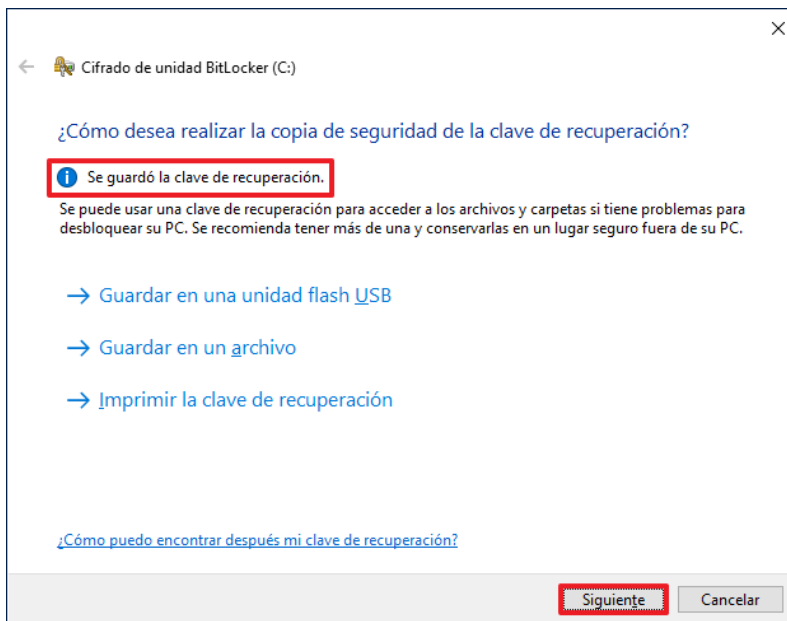
Los siguientes pasos describen el procedimiento para activar el cifrado de unidad BitLocker con contraseña.

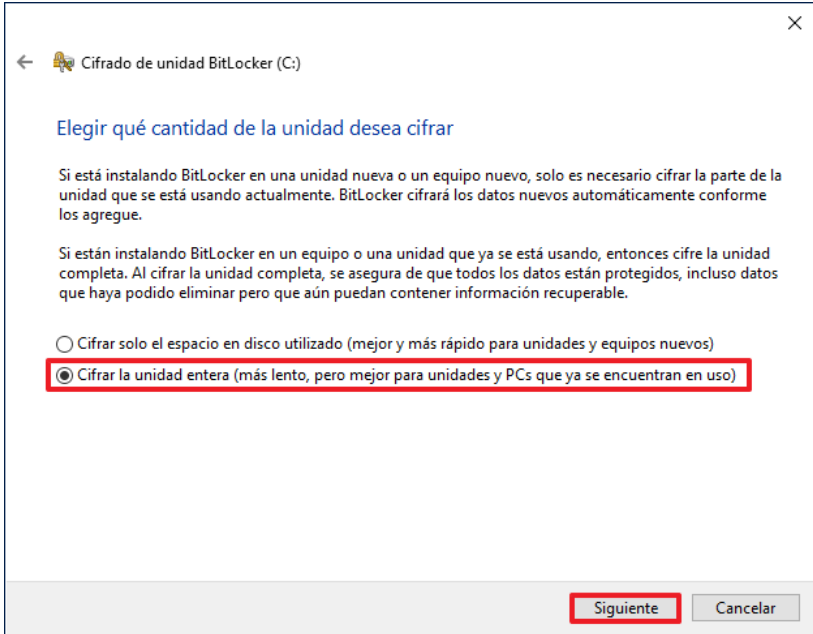
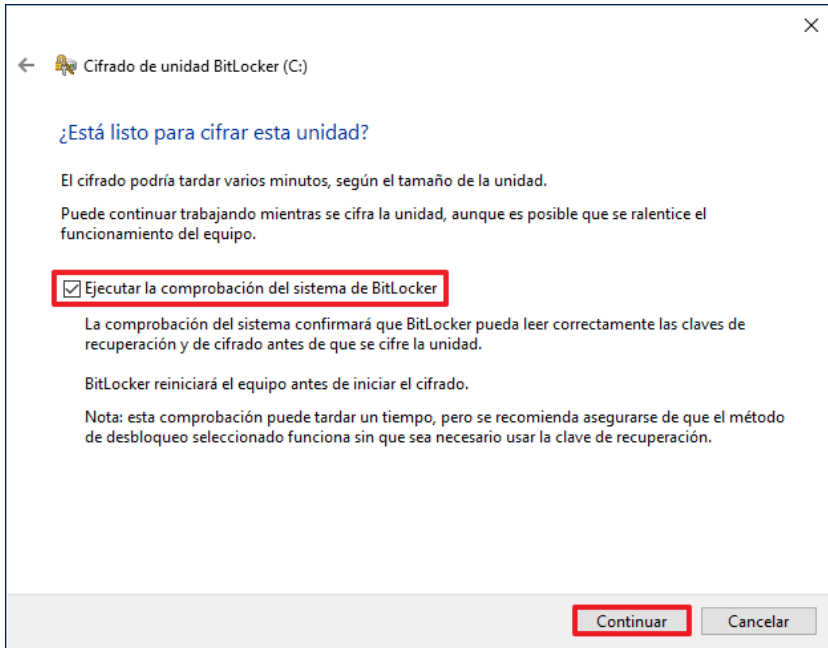
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números. Por tanto, se puede pensar en el PIN más como una "frase de paso" que como un "número".

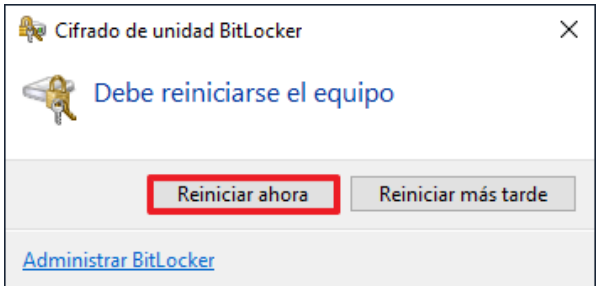
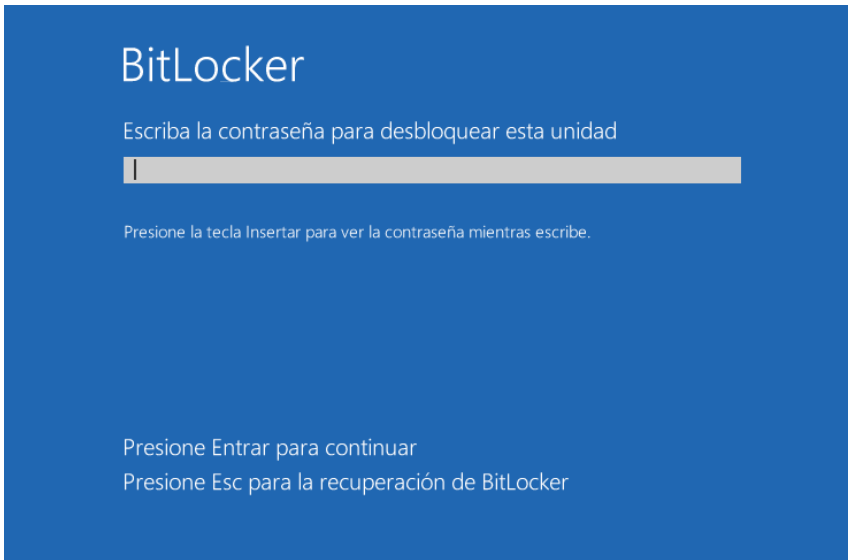
Paso	Descripción
16.	Inicie el “Panel de Control”. Para ello pulse la combinación de teclas “Windows + R”, escriba “control.exe” en la ventana emergente y pulse el botón “Aceptar”. 

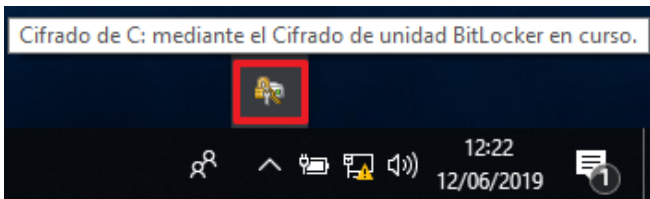
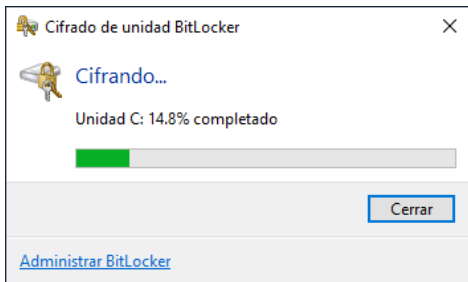
Paso	Descripción
17.	Seleccione dentro del “Panel de control” el apartado “Cifrado de unidad BitLocker”.  Nota: Tenga en cuenta la visualización del Panel de control. En la parte superior derecha podrá cambiar el modo en que se muestran los iconos. Ver por: Iconos grandes
18.	Pulse “Activar BitLocker”.  Nota: La configuración importada durante la aplicación de la guía establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si su equipo dispone de firmware UEFI nativo, deberá habilitar y configurar la directiva “Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo”. Para ello, con el editor de directivas de grupo (gpedit.msc) diríjase a la ruta “Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo” y habilite la directiva mencionada anteriormente. 

Paso	Descripción
19.	El sistema le solicitará elevación de privilegios. Introduzca credenciales de administrador en la ventana de "Control de cuentas de usuario". pulse "Sí" para continuar.
20.	Introduzca y confirme una contraseña de inicio y pulse "Siguiente".  Nota: Recuerde que puede utilizar entre 8 y 20 caracteres. A mayor longitud, mayor seguridad.
21.	Seleccione "Guardar en un archivo" para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
22.	Seleccione la ubicación de la unidad USB en la que guardará el archivo que contiene la clave y pulse el botón “Guardar”.  Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD. Debe tener en consideración que esta clave, durante el proceso no puede ser almacenado sobre la misma unidad que se está cifrando ni en otra unidad que este cifrada.
23.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

Paso	Descripción
24.	A continuación, elija la opción “Cifrar la unidad entera” y pulse “Siguiente”. 
25.	Marque la opción "Ejecutar la comprobación del sistema de BitLocker" y pulse el botón "Continuar". 

Paso	Descripción
26.	Reinicie el equipo para continuar con el proceso de cifrado de la unidad.  Nota: Si tras reiniciar el sistema aparece un mensaje como el mostrado a continuación pulse el botón “Cerrar” y repita los pasos 17 a 26, pero en este último paso pulse sobre la opción “Reiniciar más tarde” y reinicie el equipo manualmente mediante la ruta “Inicio → Iniciar/Apagar”. 
27.	Al reiniciar, el sistema le pedirá el PIN de cifrado de unidad BitLocker. Introduzca el PIN y pulse “Enter” para continuar. 

Paso	Descripción
28.	Una vez reiniciado el sistema, abra la sesión de nuevo con un usuario del grupo “Administradores”. El cifrado inicial de la unidad del sistema se realizará en segundo plano. Mientras dure este proceso es posible que el tiempo de respuesta del sistema se vea afectado por la intensa actividad del disco. Una vez finalizado el proceso de cifrado inicial, el cifrado y descifrado de los datos del disco será imperceptible por el usuario. Durante el proceso puede aparecer el siguiente mensaje informativo. Continúe con los siguientes pasos, aunque no haya finalizado este proceso de cifrado inicial del disco.: 
29.	Si marca con el ratón en él, o en el icono correspondiente del área de notificación, podrá visualizar la siguiente ventana mostrando el progreso de este cifrado inicial. 
30.	Desconecte la memoria USB que contiene la clave de recuperación del cifrado de BitLocker y guárdela en un lugar seguro, como una caja de seguridad. Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD.
31.	Una vez haya reiniciado el sistema, inicie sesión de nuevo con un usuario miembro del grupo “Administradores” y elimine la carpeta “C:\Scripts”. Nota: Todos los volúmenes NTFS del Sistema deberán ser cifrados con la utilidad BitLocker, una vez se haya cifrado totalmente el volumen del Sistema. Si se cambia el TPM asociado al cifrado de unidad BitLocker o si alguien intenta iniciar el equipo desde un disco para evitar el sistema operativo, el equipo cambiará al modo de recuperación hasta que se suministre la clave de recuperación. Si se pierde el PIN, se puede cambiar al modo de recuperación para iniciar el equipo e introducir la clave de recuperación. Para más información sobre el procedimiento de cifrado de unidad BitLocker, puede consultar el siguiente enlace: https://support.microsoft.com/es-es/help/4028713/windows-10-turn-on-device-encryption

ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO A.5.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA

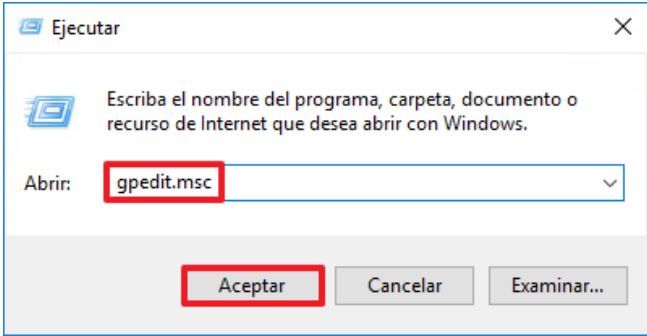
El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los clientes Windows 10 independientes. Este Anexo ha sido diseñado para atender al principio de mínima exposición que faculta a un sistema a reducir los riesgos minimizando los puntos de entrada al mismo.

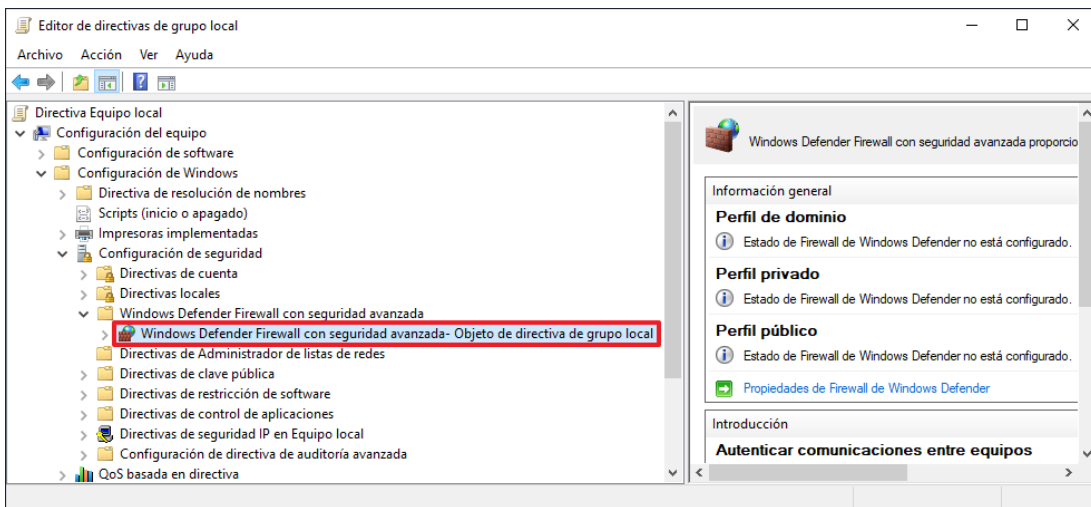
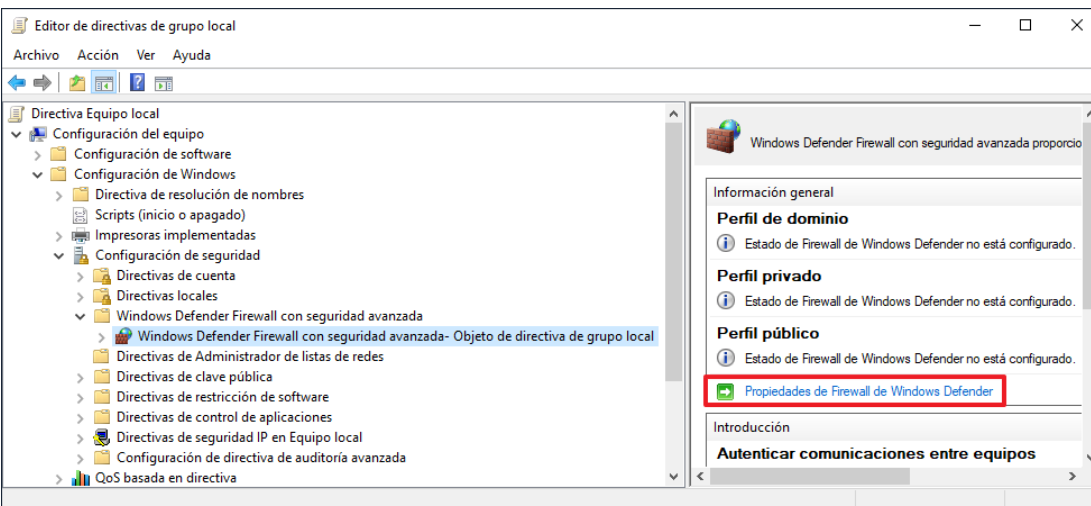
Debe tenerse en consideración que la implementación de un cortafuegos de cliente independiente dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que este ofrece a la infraestructura. No tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, un servidor que actúe para dar soporte a sitios web que un servidor que mantenga bases de datos. A partir de Windows Vista, Microsoft proporciona un servicio de cortafuegos con seguridad avanzada. Éste permite realizar el control tanto de lo que entra como de lo que sale y para las diferentes categorías de redes en la que puede estar un sistema: públicas, privadas o dominio.

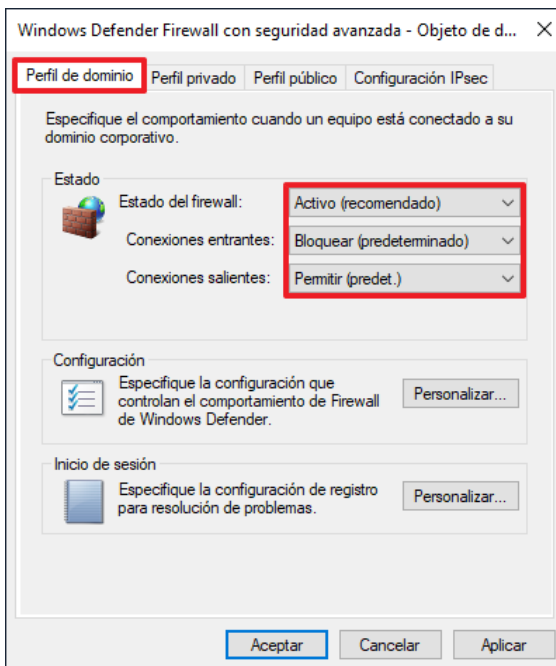
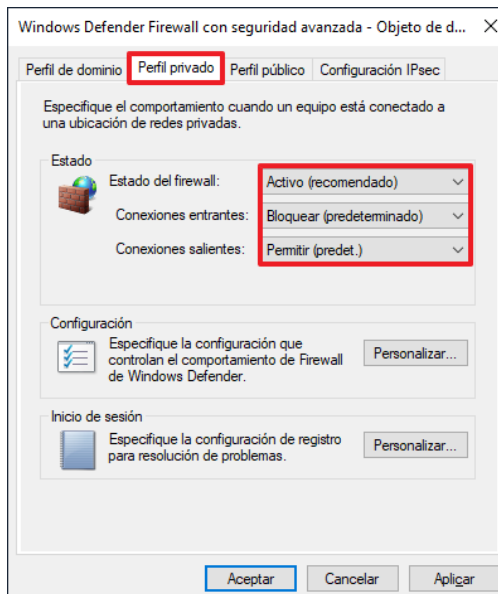
De forma predeterminada, el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local. No obstante, en un cliente independiente puede establecerse la configuración del mismo a través de la política local, de tal forma que, aunque se realizara una modificación del firewall, a través de la consola local o bien mediante una modificación directa por código dañino, a este le sería de aplicación la configuración establecida a través de la política local.

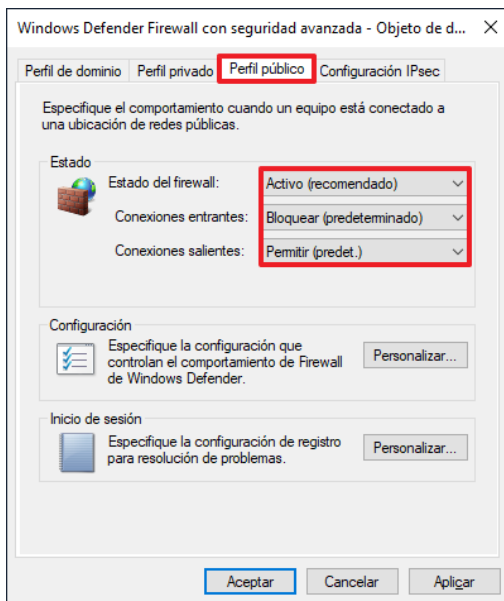
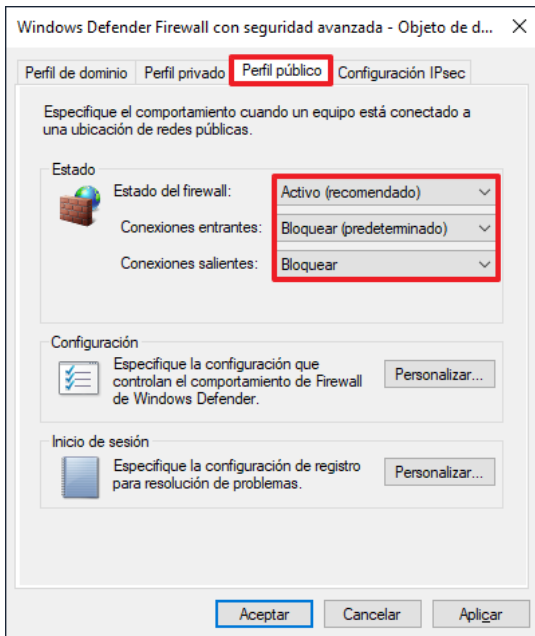
Teniendo en cuenta este hecho, a través de este Anexo se establecerá la configuración del cortafuegos mediante la aplicación de la política local. Como en los Anexos previos, los operadores deberán realizar pruebas en entornos de preproducción antes de realizar una implementación en el entorno de producción.

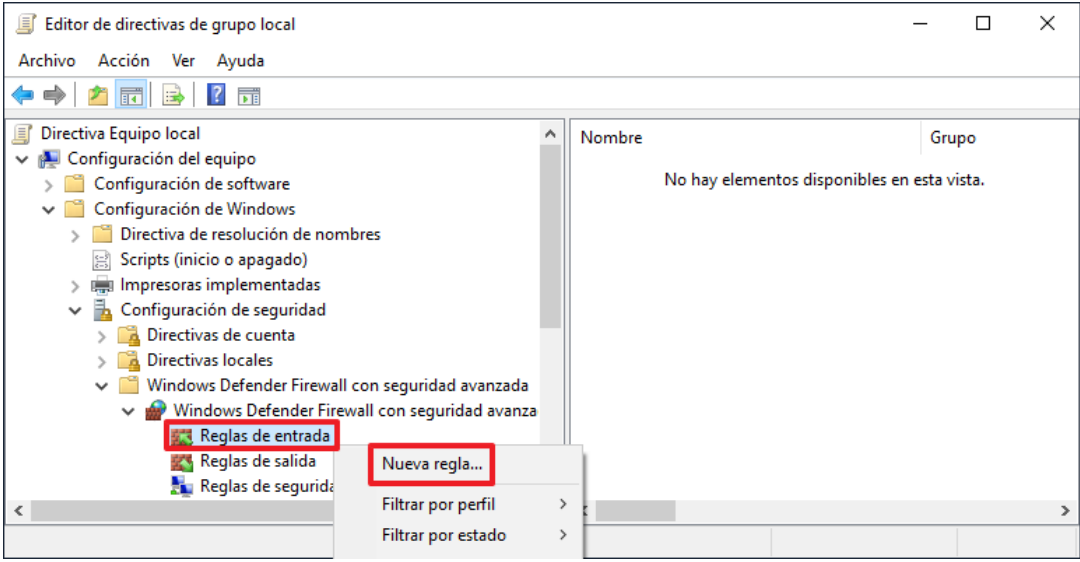
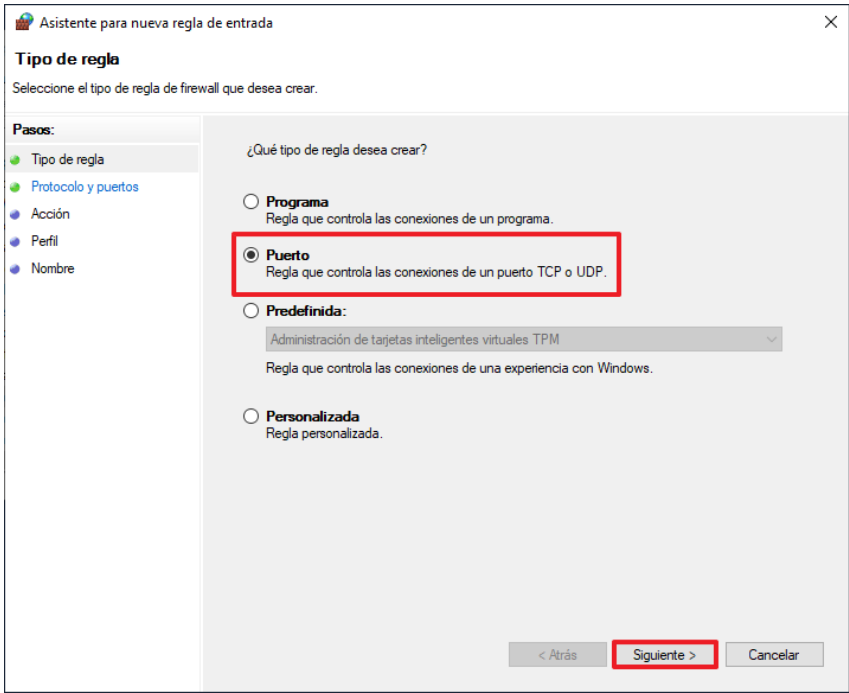
Nota: A modo de ejemplo, en este Anexo se va a mostrar cómo configurar la política local para la aplicación de seguridad de cortafuegos para permitir administración remota a través del puerto 3389.

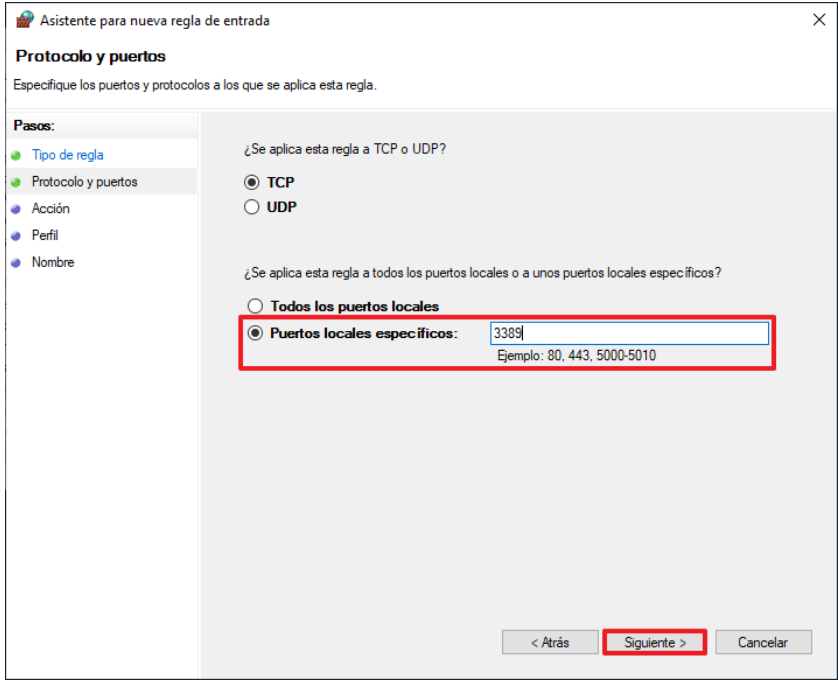
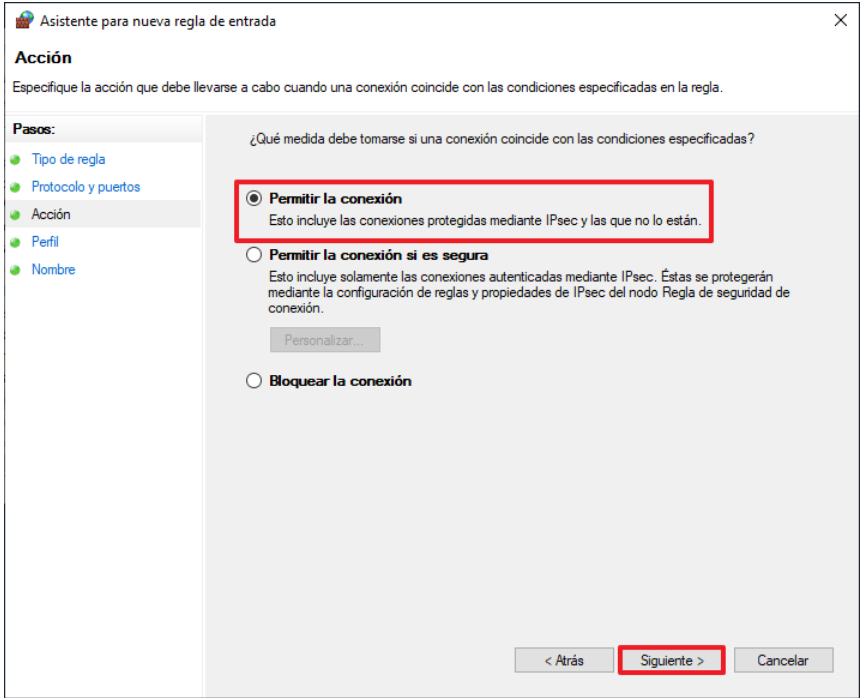
Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas "Windows + R", escriba "gpedit.msc" en la ventana emergente y pulse "Aceptar". 

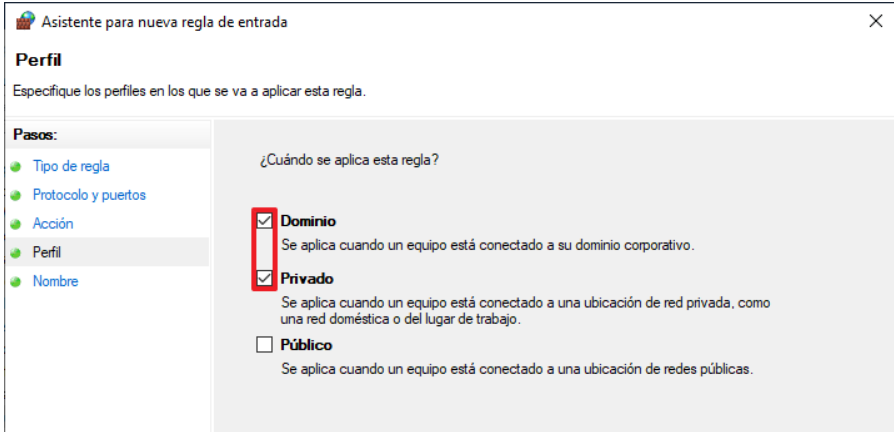
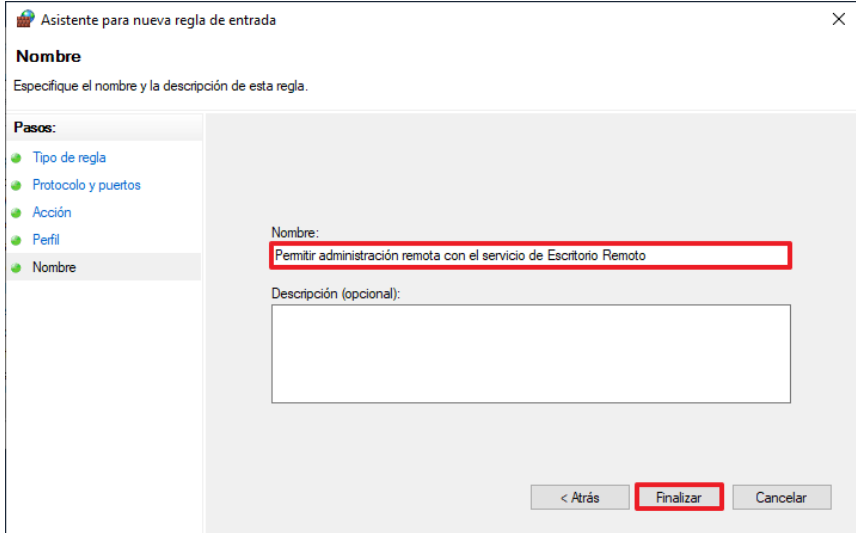
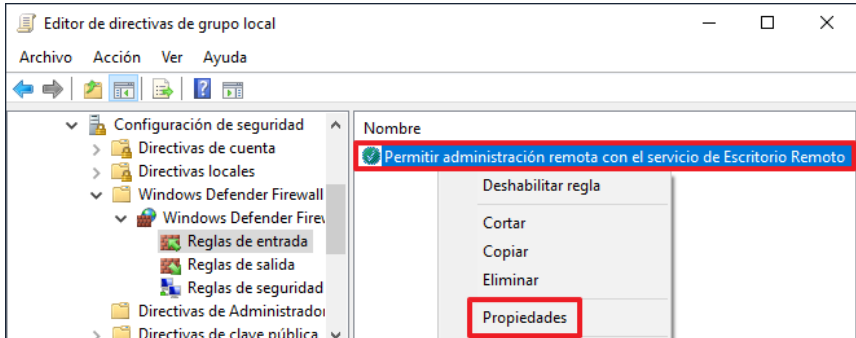
Paso	Descripción
3.	En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
4.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: “Directiva Equipo local → Configuración de equipo → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada- Objeto de directiva de grupo local” 
5.	Pulse sobre “Propiedades de Firewall de Windows” que aparecen en la configuración de “Información General”, existentes en el panel derecho. 

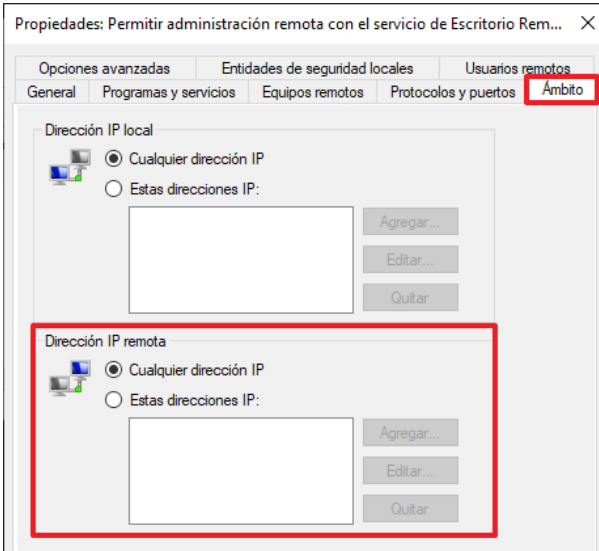
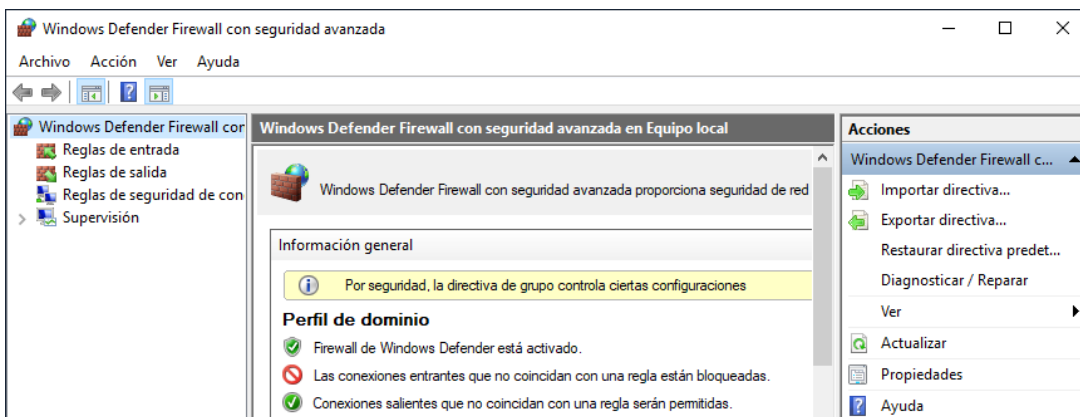
Paso	Descripción
6.	La primera de las pestañas “Perfil de dominio” configúrela como aparece en la siguiente imagen.  Nota: Debe tener en consideración que el presente cliente que está configurando es un cliente de tipo independiente y por lo tanto no formará parte de un dominio. No obstante, es adecuado establecer la configuración del dominio por si el cliente cambiara en algún momento su situación y este pasara a forma parte de un dominio.
7.	A continuación, vaya a la pestaña “Perfil privado” y configúrela tal y como aparece en la siguiente imagen. 

Paso	Descripción
8.	Vaya posteriormente a la pestaña “Perfil público” y establezca la configuración que aparece en la siguiente imagen.  Verifique que la configuración de la conexión de red con el que conecta el sistema a la red interna o a una DMZ, se encuentra en el perfil privado y no en perfil público.
9.	En el caso de que los clientes proporcionaran servicios de categoría alta, sería recomendable que el perfil público quedara configurado como aparece en la siguiente imagen. 
10.	Pulse el botón “Aceptar” para guardar los cambios introducidos en los diferentes perfiles.
11.	Despliegue el Firewall con seguridad avanzada y vaya al apartado “Reglas de entrada”.

Paso	Descripción
12.	Pulse con el botón derecho sobre “Reglas de entrada” y seleccione la opción “Nueva regla...”. 
13.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 

Paso	Descripción
14.	En el siguiente apartado seleccione la opción “Puertos locales específicos” e introduzca el puerto “3389”. Pulse el botón “Siguiente >”. 
15.	En el apartado “Acción”, mantenga la configuración y pulse el botón “Siguiente >”. 

Paso	Descripción
16.	En el apartado “Perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 
17.	Por último, asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”.  Nota: En el ejemplo se utiliza el nombre “Permitir administración remota con el servicio de Escritorio Remoto”.
18.	La nueva regla ya se encuentra creada. Puede editarla pulsando con el botón derecho del ratón sobre ella y seleccionando la opción “Propiedades”. 

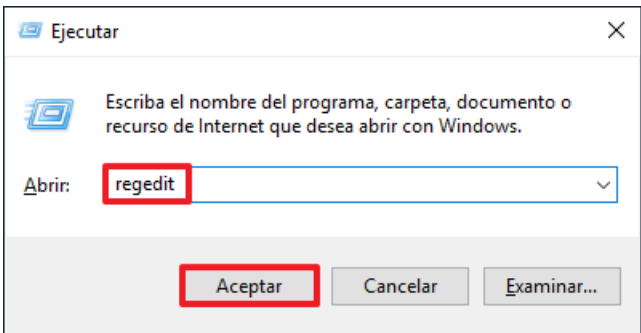
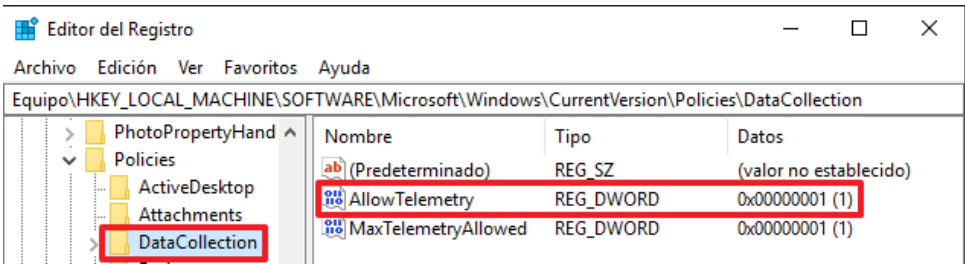
Paso	Descripción
19.	Podrían, por ejemplo, limitarse las IP remotas o rangos de redes que podrían conectarse a los puestos de trabajo a través del puerto 3389. De forma predeterminada se admite cualquier IP. 
20.	Cierre la política de seguridad local. La configuración se habrá aplicado en el puesto de trabajo y lo podrá comprobar ejecutando la configuración del Firewall. Para ello podrá ejecutar desde el menú "Ejecutar" (combinación de teclas "Windows + R") la aplicación "wf.msc".  Nota: La documentación existente en la web de Technet o MSDN de Microsoft le podrá servir de orientación para conocer los puertos que emplean los servicios y aplicaciones de productos Microsoft. La siguiente URL de soporte de Microsoft referencia los puertos habitualmente usados por los servicios de Windows. https://support.microsoft.com/es-es/help/832017/service-overview-and-network-port-requirements-for-windows

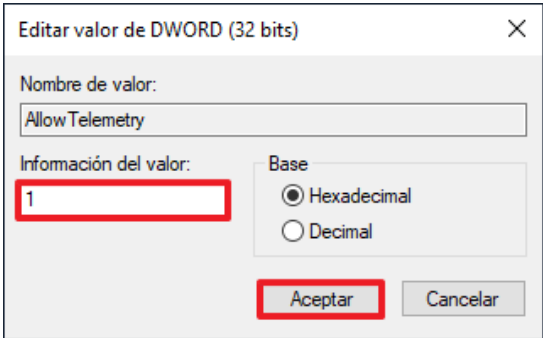
ANEXO A.5.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA WINDOWS 10 INDEPENDIENTE

1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 INDEPENDIENTES

Este anexo ha sido diseñado para ayudar a los operadores a configurar el servicio de telemetría acorde a las necesidades de conectividad de los puestos de trabajo en las administraciones. Dicha funcionalidad de telemetría opera tanto de forma interna generando registros internos de actividad, como remitiendo en determinadas condiciones el envío de información a Microsoft. En este punto se va a explicar cómo realizar cambios en los valores otorgados al componente de telemetría a través de la modificación de una clave de registro. Este valor viene definido tanto por la categoría de seguridad establecido por parte de la organización en sus sistemas, como por los acuerdos que pueda tener esta con Microsoft para el mantenimiento de sus equipos.

Debe tener en consideración que determinados componentes tales como Windows Defender ATP, podrían llegar a requerir al menos un nivel de telemetría de tipo básico (1).

Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie el registro de Windows. Para ello pulse la combinación de teclas “Windows + R”, escriba “regedit” en la ventana emergente y pulse el botón “Aceptar”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
3.	Se abrirá una consola, “Editor de registro” en la cual hay que desplegar el árbol de la izquierda de la pantalla hasta la siguiente clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection 

Paso	Descripción
4.	En panel de la derecha haga doble clic sobre “AllowTelemetry” y modifique el valor más adecuado acorde a las necesidades de su organización. Pulse “Aceptar” para finalizar.  Nota: Recuerde que en el caso de versiones MS Windows 10 Pro, el valor no podrá establecerse la telemetría en valor 0.
5.	Cierre la consola “Editor del Registro”.

ANEXO A.5.3. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN

Tras la aplicación de seguridad en el sistema, existirían todavía determinados vectores de ataque, que deberán ser corregidos con el fin de evitar la evasión de los sistemas de autorización del sistema operativo. La exploración de dichos vectores de ataque podría ocasionar una posible exfiltración de la información gestionada y almacenada en el sistema, así como una potencial manipulación del comportamiento del mismo.

Para evitar esta situación, dentro del marco de seguridad establecido, se disponen de cuatro soluciones que se relaciona a continuación, y que pueden aplicarse de forma independiente o en conjunción las unas con las otras. Con posterioridad se detallará los mecanismos de su aplicación dentro del presente anexo, con objeto de mejorar la seguridad global del sistema.

Nota: Antes de aplicar las soluciones que se indican a continuación, verifique la compatibilidad de las mismas con su organización, y tenga en consideración los riesgos asumidos por la aplicación de dichas medidas.

Se recomienda verificar la adecuación e idoneidad de la solución para la organización en un entorno de pruebas o “preproducción” de forma previa a su aplicación en un entorno real o de “producción”.

Las medidas a aplicar podrán ser:

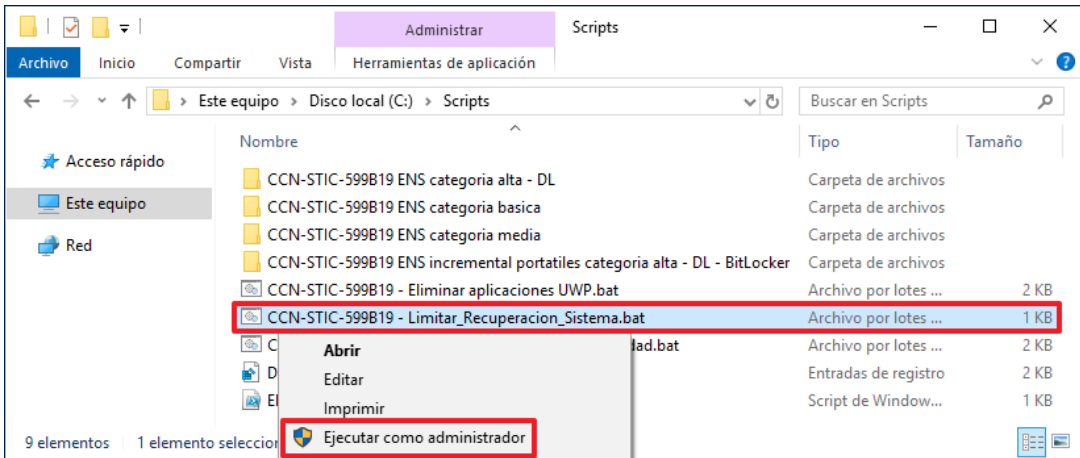
- Cifrado del sistema de archivos. Utilizar BitLocker u otro sistema de cifrado autorizado para evitar el acceso a la información almacenada y, por tanto, evitar su modificación ya que requiere de la introducción de un PIN o contraseña en el arranque del equipo, o en el momento de acceder a los datos. De las opciones presentadas, ésta es la más recomendada. El presente anexo no incorpora cómo aplicar el mecanismo de protección de BitLocker ya que ha sido convenientemente tratado en la presente guía.
- Deshabilitar la funcionalidad de restauración y/o recuperación del sistema a través de la utilidad “BCEDIT”.

- c) Deshabilitar las opciones de accesibilidad a través de claves de registro, evitando así que estas estén disponibles tanto si el usuario ha iniciado sesión como si no.
- d) Restaurar la integridad de los ficheros “C:\Windows\System32\sethc.exe” y “C:\Windows\System32\utilman.exe” al inicio del sistema.

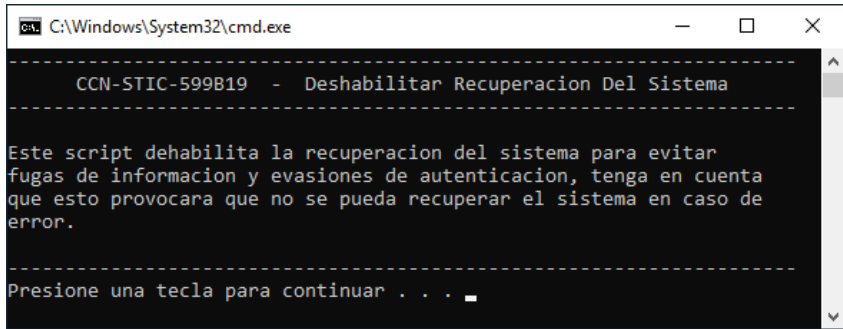
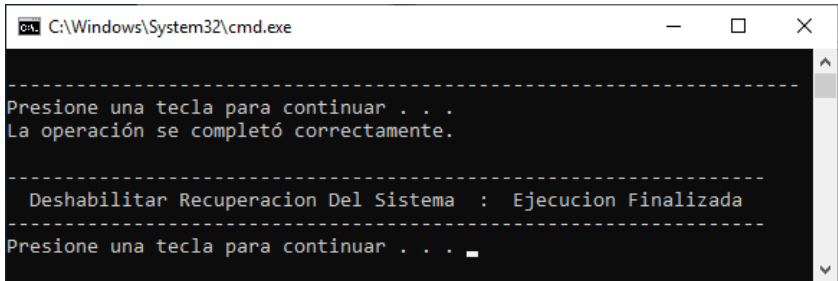
Atendiendo al RD 1494/2007, será necesario permitir el uso de esta funcionalidad de accesibilidad a aquellas personas que, por su discapacidad, requieran hacer uso de esta tecnología de accesibilidad. Se deberá tener en consideración los riesgos de seguridad que se asumen si se activan estas opciones, y se deberán implantar las medidas adecuadas para minimizar el grado de exposición del sistema en estos términos.

1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

A continuación, se indican los pasos a realizar para deshabilitar la funcionalidad de recuperación del sistema.

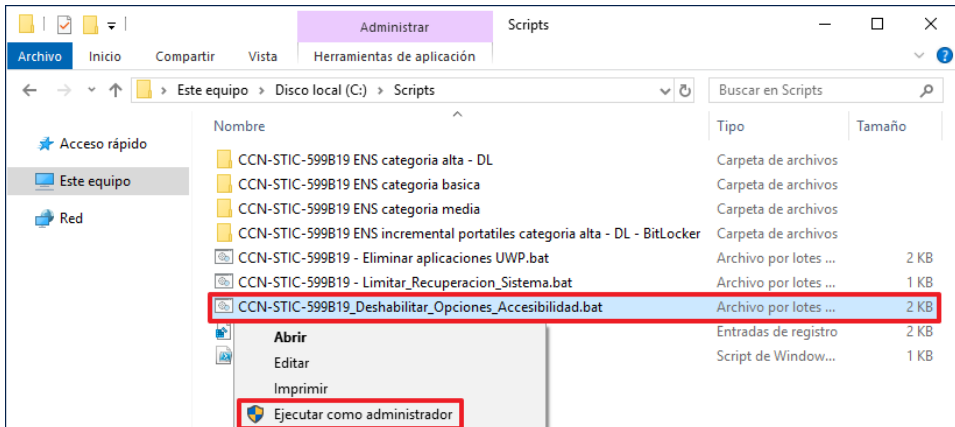
Paso	Descripción
30.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
31.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
32.	Localice el archivo “CCN-STIC-599B19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.

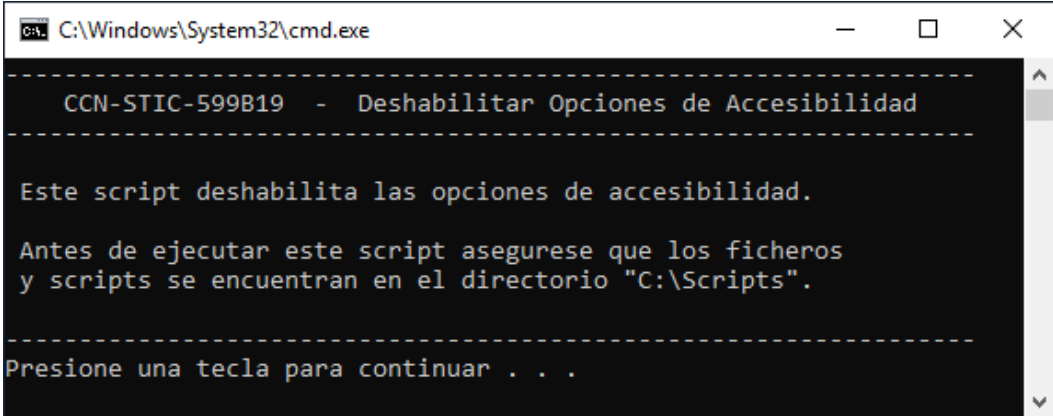
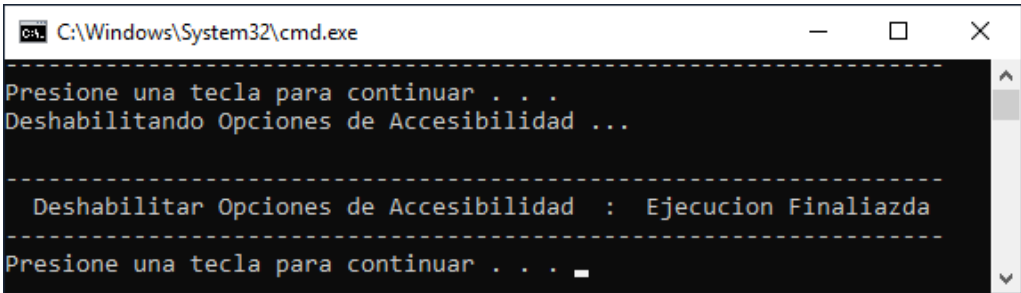
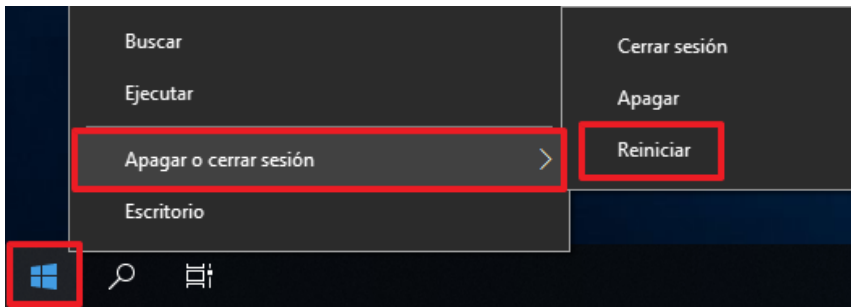


Paso	Descripción
33.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script limitará el uso de las opciones de recuperación del sistema. 
34.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana. 
35.	Elimine el directorio "C:\Scripts".

2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD

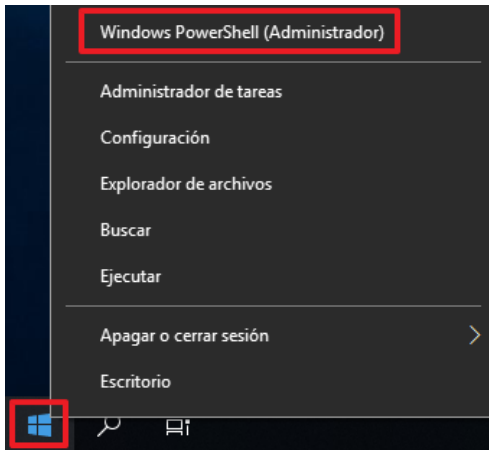
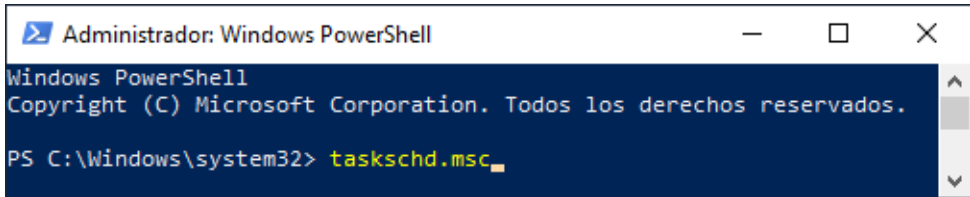
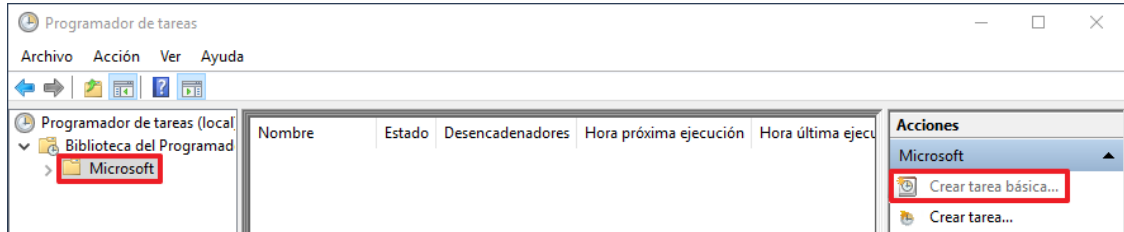
A continuación, se indican los pasos a realizar para deshabilitar las opciones de accesibilidad.

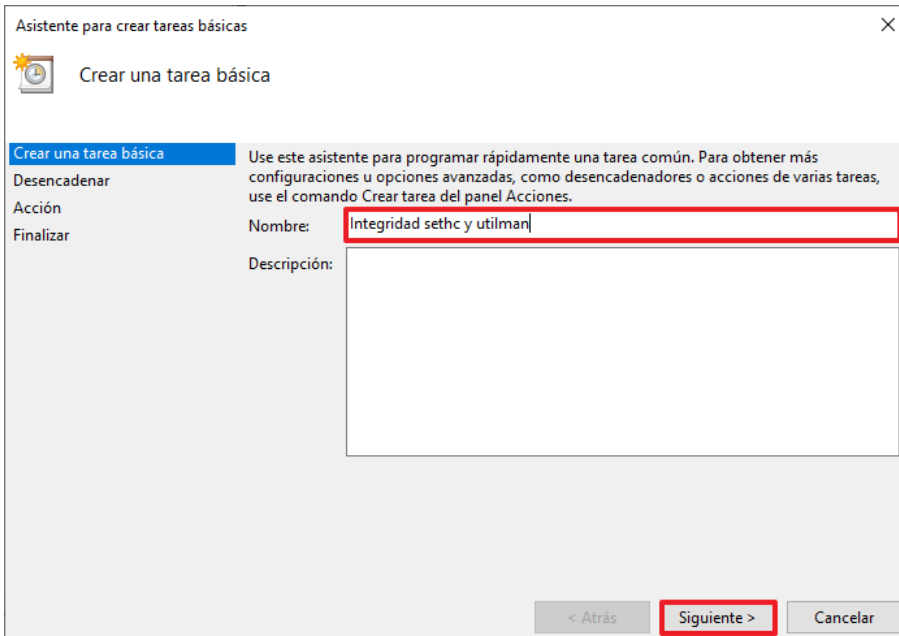
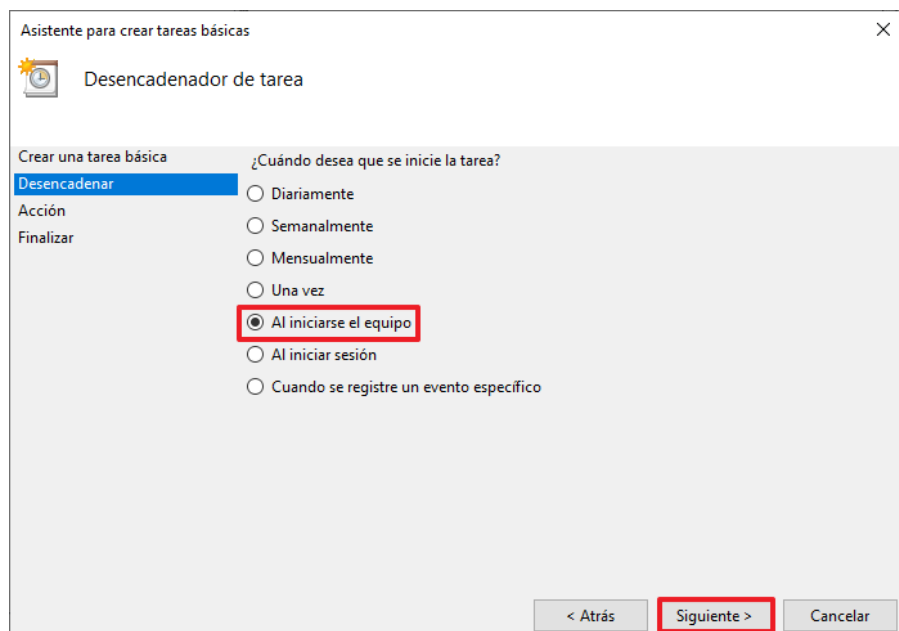
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio "C:\Scripts" y sitúese en dicho directorio.
3.	Localice el archivo "CCN-STIC-599B19 – Deshabilitar_Opciones_Accesibilidad.bat" haga clic derecho sobre este y seleccione la opción "Ejecutar como administrador". 

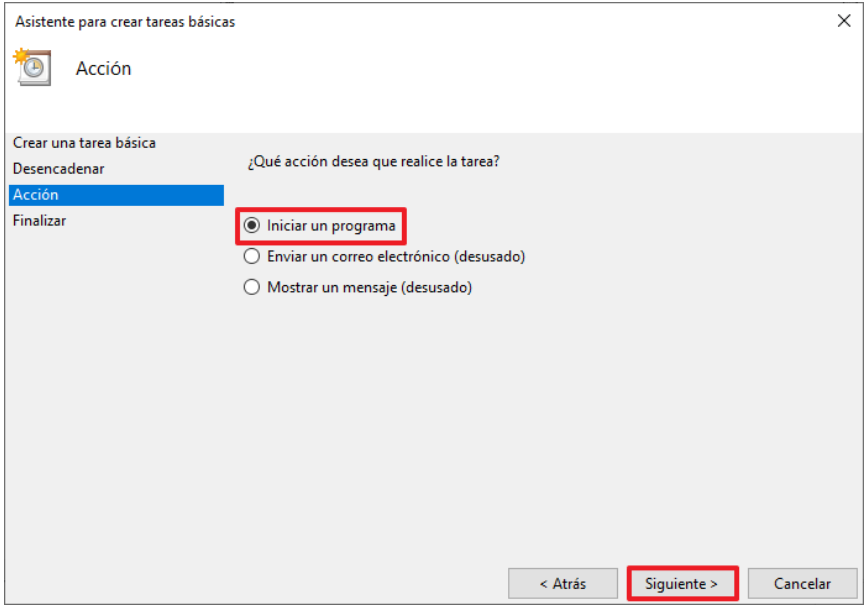
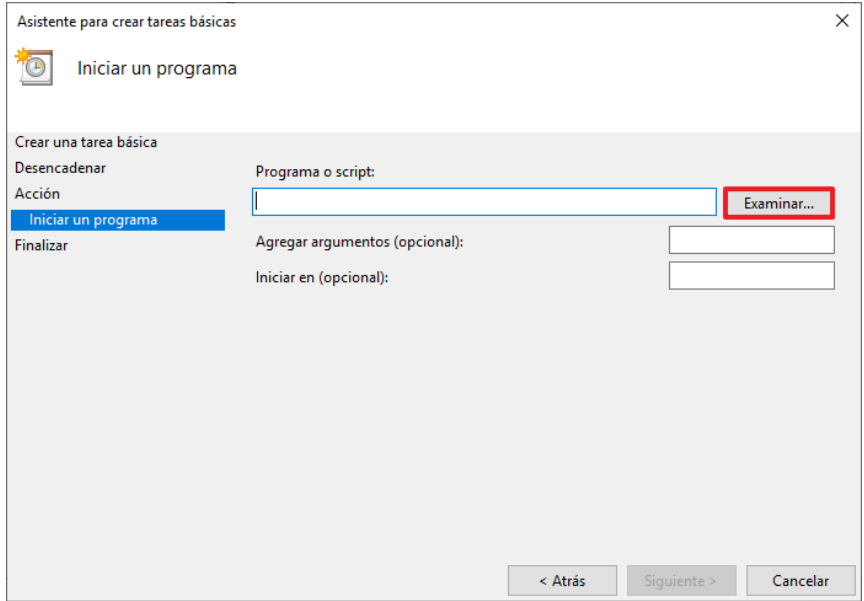
Paso	Descripción
4.	En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comando. 
7.	Por último, deberá reiniciar el sistema para que los cambios sean aplicados. Para ello haga clic derecho en el botón sobre “Inicio → Apagar o cerrar sesión → Reiniciar”. 
8.	Elimine el directorio “C:\Scripts”.

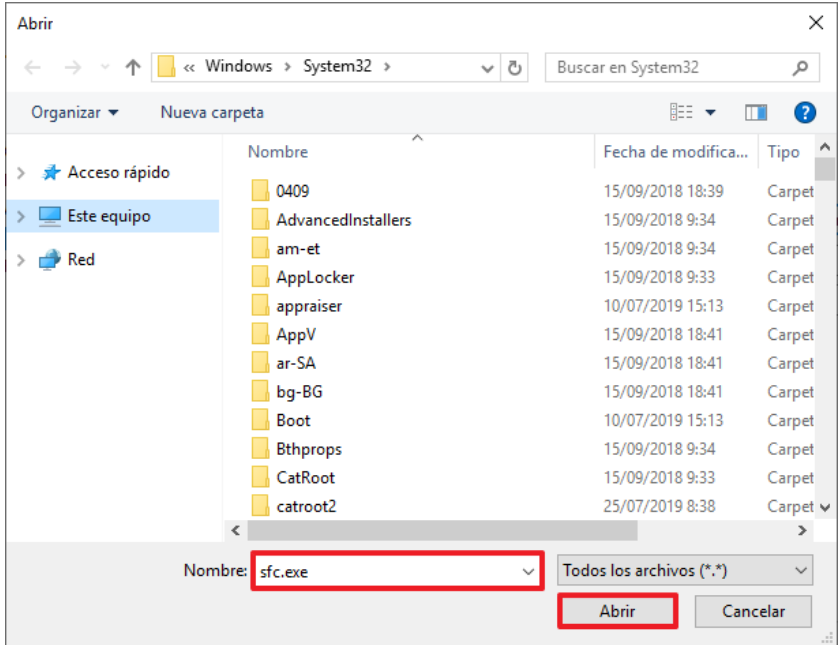
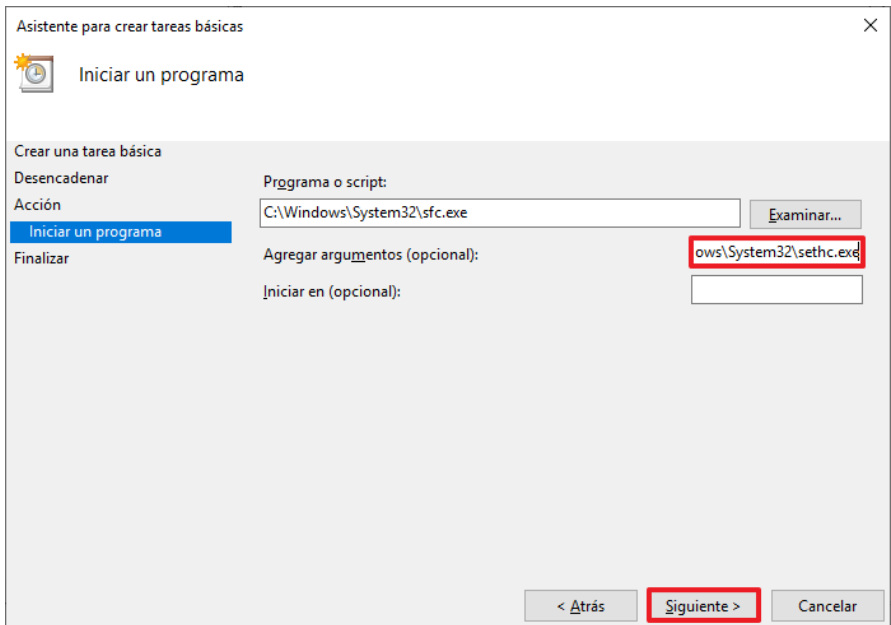
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

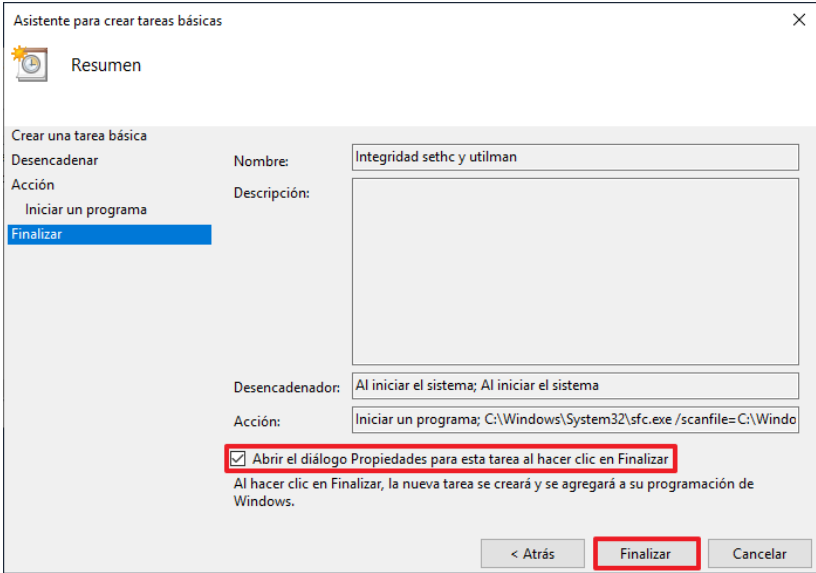
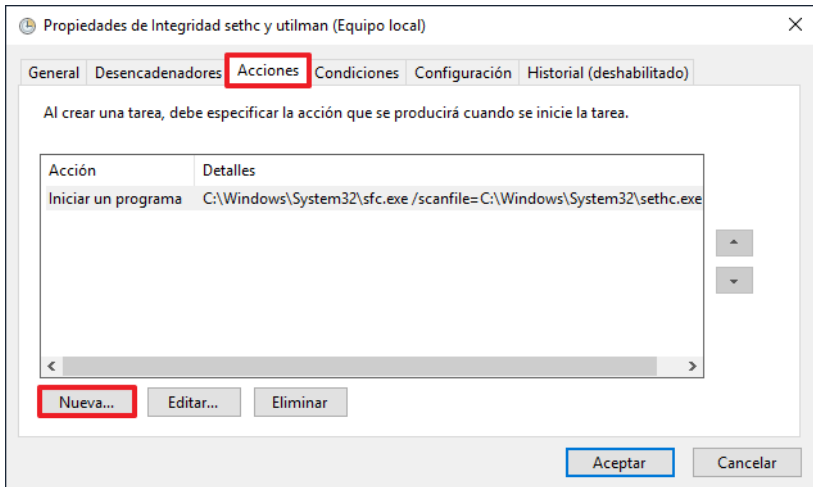
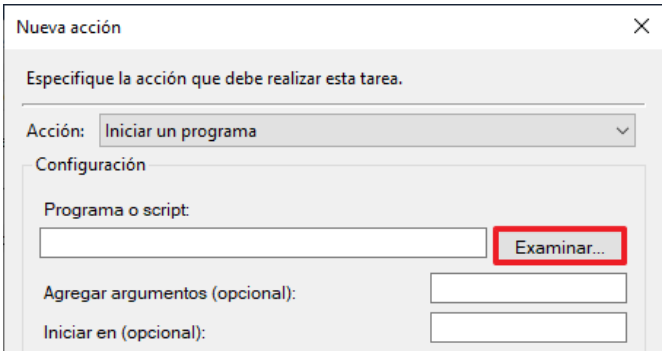
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

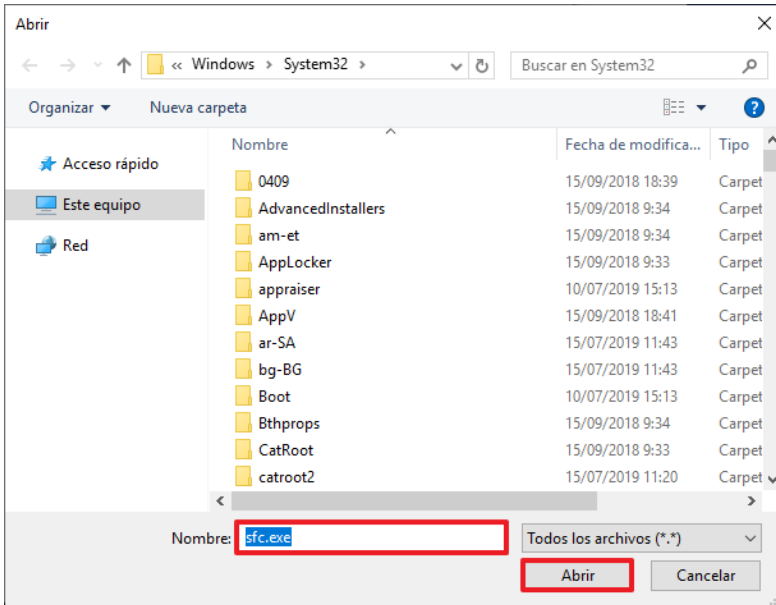
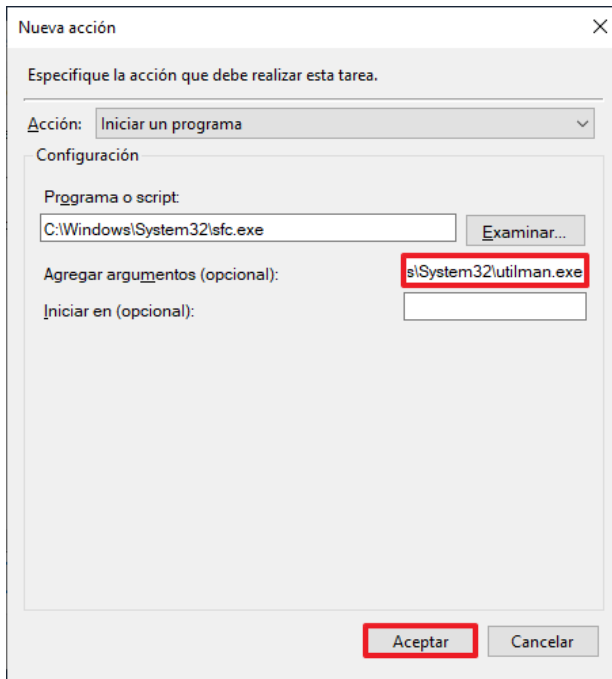
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador. Pulse con botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
2.	Ejecute el comando “taskschd.msc” en la misma consola de PowerShell para abrir el programador de tareas. 
3.	En el programador de tareas sitúese en la ruta “Biblioteca del Programador de tareas\Microsoft” y en el panel de “Acciones” situado en la parte derecha seleccione “Crear tarea básica”. 

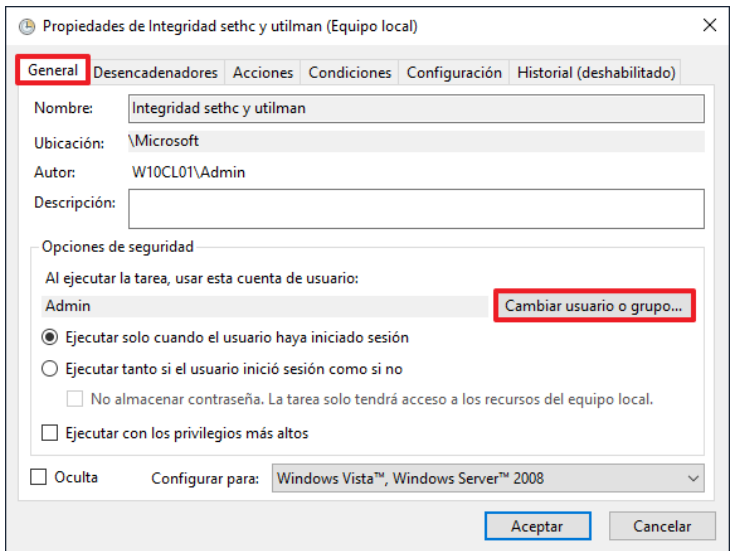
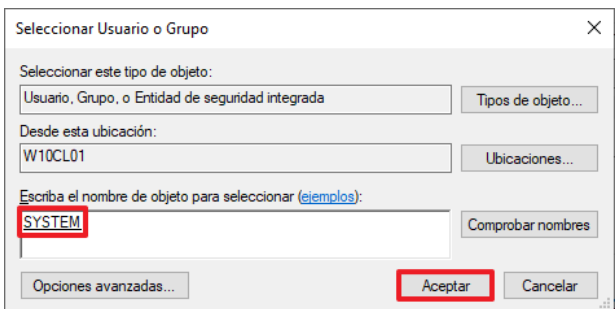
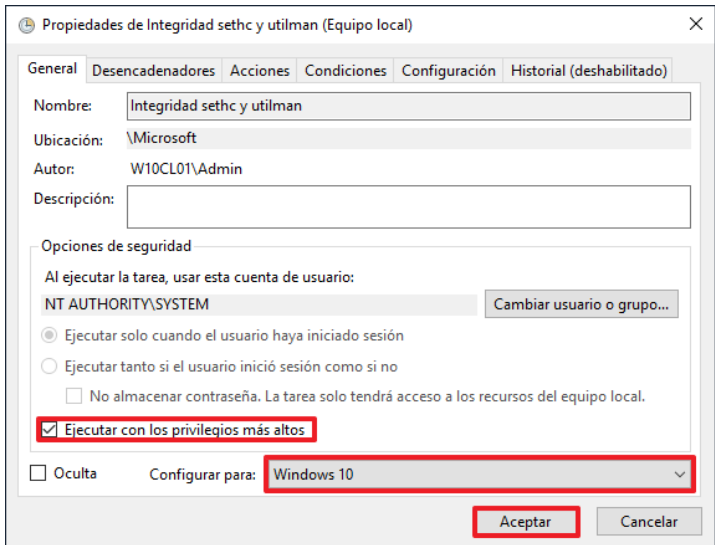
Paso	Descripción
4.	Se abrirá un asistente para la creación de la tarea programada. En la primera pestaña, indique el nombre de la tarea, en este caso “Integridad sethc y utilman” y pulse el botón “Siguiente >”. 
5.	En la ventana “Desencadenar” del asistente seleccione “Al iniciarse el equipo” y pulse sobre el botón “Siguiente >”. 

Paso	Descripción
6.	En la ventana “Acción” del asistente seleccione “Iniciar un programa” y haga clic sobre el botón “Siguiente >”. 
7.	Haga clic sobre el botón “Examinar” para indicar que programa se ejecutará. 

Paso	Descripción
8.	En la ventana emergente acceda a la ruta "C:\Windows\system32", escriba en el apartado "Nombre" "sfc.exe" y haga clic sobre el botón "Abrir". 
9.	En el apartado "Agregar argumentos (opcional)" escriba "/scanfile=C:\Windows\System32\sethc.exe" para indicarle al programa "sfc" que verifique la integridad del fichero "sethc.exe" situado en "C:\Windows\System32" y haga clic sobre el botón "Siguiente >". 

Paso	Descripción
10.	En la última ventana (Finalizar), marque la opción “Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar” y haga clic en “Finalizar”. 
11.	Al hacer clic en “Finalizar”, se abrirá el diálogo de propiedades de la tarea, sitúese en la pestaña de “Acciones” y haga clic en “Nueva...”. 
12.	Se abrirá una ventana con la nueva acción a indicar, pulse sobre el botón “Examinar...”. 

Paso	Descripción
13.	En la ventana emergente acceda a la ruta "C:\Windows\System32", escriba en el apartado "Nombre" "sfc.exe" y haga clic sobre el botón "Abrir". 
14.	En el apartado "Agregar argumentos (opcional)" escriba "/scanfile=C:\Windows\System32\utilman.exe" para indicarle al programa sfc que verifique la integridad del fichero utilman.exe situado en "C:\Windows\System32" y haga clic sobre el botón "Aceptar".  Nota: Si su sistema operativo es de 64 bits, repita el proceso del paso 15 al 18 con los ficheros "C:\Windows\SysWOW64\sethc.exe" y "C:\Windows\SysWOW64\utilman.exe".

Paso	Descripción
15.	A continuación, en la pestaña “General” del dialogo de propiedades de la tarea programada, haga clic en el botón “Cambiar usuario o grupo...”. 
16.	En la ventana emergente, introduzca el nombre “SYSTEM” y pulse aceptar. 
17.	Por último, marque la opción de “Ejecutar con los privilegios más altos”, establezca la opción “Windows 10” del desplegable “Configurar para:” y pulse en “Aceptar”. 
18.	Cierre el programador de tareas.

ANEXO B. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN REDES CLASIFICADAS COMO CLIENTE INDEPENDIENTE

Nota: Si no lo ha hecho ya, acuda a los puntos principales de esta guía establecidos en el documento principal de la guía. En estos puntos se indican el objeto, alcance y otra información que se debe tener en consideración como paso previo a la aplicación de este anexo.

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un puesto de trabajo con el sistema operativo Microsoft Windows 10 Enterprise LTSC (versión 1809) en un entorno aislado, es decir, no conectado a una red no segura, como es Internet.

Nota: Todas las referencias indicadas en este anexo hacen referencia a la guía codificada como “CCN-STIC-599B19” correspondiente con el ANEXO B enfocado a redes clasificadas.

Debido a las características de los puestos de trabajo a los que van dirigidas las guías de la serie 500, se recomienda establecer la versión Microsoft Windows 10 Enterprise 1809 con la opción de mantenimiento LTSC (versión contemplada en este anexo) como la más adecuada para su implementación. Esto se basa en los siguientes condicionantes:

- a) Estos equipos no estarán conectados a Internet por lo cual determinadas funcionalidades como la tienda o Cortana, que no son proporcionadas por la opción de mantenimiento LTSC, se consideran prescindibles.
- b) El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.
- c) La opción de mantenimiento a largo plazo permite garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con Microsoft Windows 10 y que, siendo críticas, no permitan, por sus características, cambios en funcionalidades habituales. No obstante, deben considerarse siempre las actualizaciones de seguridad como un elemento esencial para garantizar la seguridad de los puestos de trabajo en cualquier infraestructura, siendo aún más crítico en una red clasificada.

Pese a la recomendación anterior también está admitida la versión Windows 10 Pro/Enterprise sin opción de mantenimiento LTSC, en su versión 1809. Para la correcta implementación y adecuar dicha versión de Windows para un entorno de Redes Clasificadas, existen varias configuraciones y características que son desactivadas durante la presente guía para garantizar la securización del sistema. Dichas características son:

- a) Autenticación: Microsoft Passport y Windows Hello. Esta funcionalidad está inhabilitada con la aplicación del presente anexo.
- b) Sistema de telemetría. La configuración de telemetría se deshabilitará mediante la aplicación del presente anexo. Se inhabilitarán los servicios asociados a dicho componente.
- c) Tienda de Microsoft: La versión Enterprise con la opción de mantenimiento LTSC, utilizada para la realización de dicho anexo no posee esta herramienta, aunque es desactivada con la aplicación del presente anexo.
- d) Aplicaciones para la plataforma universal de Windows (UWP). Al igual que en el caso anterior las Appx o Modern App no existen con la opción de mantenimiento LTSC y en la versión Pro/Enterprise se limita por la aplicación de la presente guía.

- e) Sistema Experiencia de Usuario. Este componente se encuentra limitado por la aplicación de la presente guía.
- f) Microsoft Edge. Al igual que sucede con la Tienda no está disponible en la versión Enterprise con opción de mantenimiento LTSC y en la versión Pro/Enterprise se limita por la aplicación de la presente guía.
- g) Opciones de privacidad. El presente anexo tiene en consideración todos los aspectos e inhabilita el envío de información para cada uno de los elementos anteriormente citados. Tampoco permite la interacción de las aplicaciones con dichos componentes.
- h) Internet Explorer 11. Se le aplican los mecanismos de seguridad definidos en la guía CCN STIC 520.

A continuación, se describe la configuración específica de seguridad que va a ser aplicada sobre los puestos de trabajo en redes clasificadas.

Se ha de tener en consideración que la aplicación de esta guía se debe realizar en un sistema formateado (sin datos) siguiendo las indicaciones que se describen en este anexo.

A través del procedimiento indicado a continuación se establece la máxima seguridad posible teniendo en consideración la guía CCN-STIC-301 – Requisitos STIC. Si su sistema requiere de otra configuración menos restrictiva, y está autorizado para ello, consulte el apartado “ANEXO B.2 APLICACIÓN DE NIVELES DE CLASIFICACIÓN” para realizar los pasos adecuados.

ANEXO B.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 COMO CLIENTE INDEPENDIENTE

ANEXO B.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA

Este anexo ha sido diseñado para ayudar a los operadores a implementar las distintas configuraciones de seguridad. A continuación, se describe, paso a paso, como realizar la instalación y configuración de seguridad de un cliente Windows 10 Enterprise LTSC (versión 1809) independiente de un dominio.

Esta guía incorpora todos los ficheros y scripts necesarios para realizar la configuración segura de los equipos.

Antes de empezar deberán tenerse en cuenta las siguientes recomendaciones:

- a) Todos los discos y particiones deberán formatearse utilizando el sistema de archivos NTFS.

Por defecto el programa de instalación da a todos los sistemas de ficheros el formato NTFS, por lo que normalmente no será necesario indicarlo explícitamente.

A diferencia de lo que ocurría en Windows Vista, el programa de instalación de Windows 10 creará por defecto las particiones de disco necesarias para poder habilitar posteriormente el cifrado de disco BitLocker.

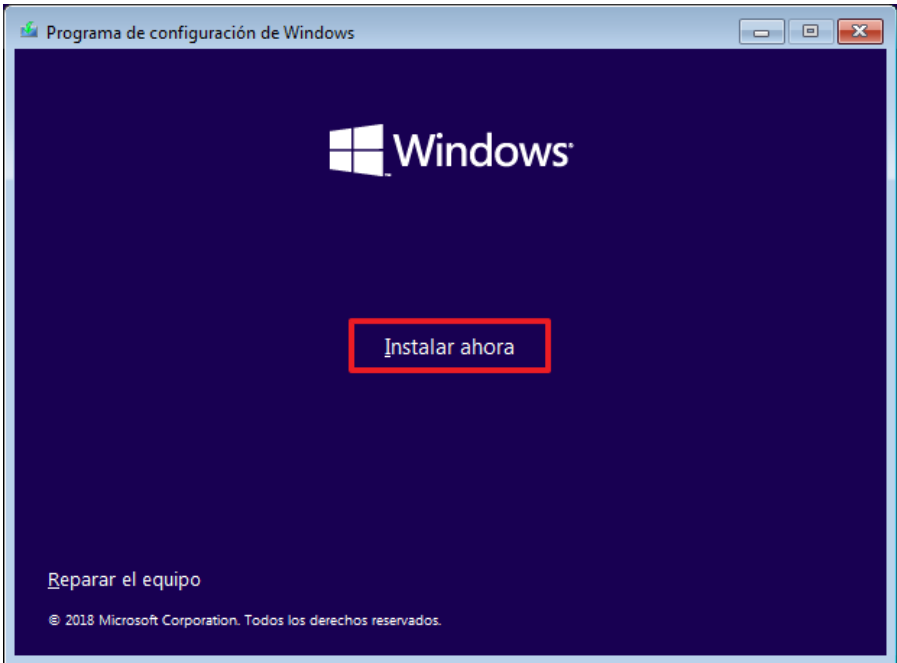
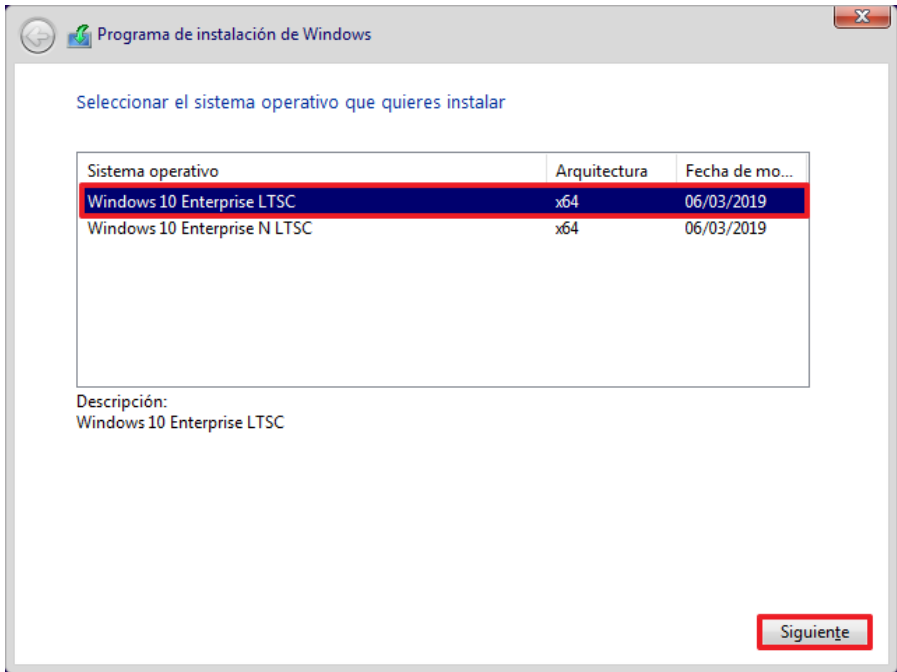
En el “ANEXO B.3.1 CIFRADO DE DISCO CON BITLOCKER” de la presente guía podrá consultar detalles sobre BitLocker y una guía paso a paso para poder aplicarlo en los equipos Windows 10 que requieran de su uso.

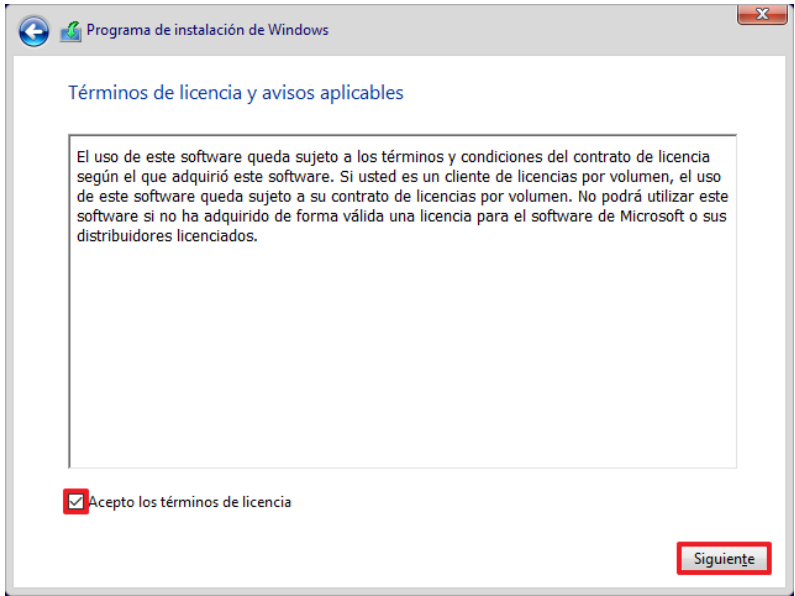
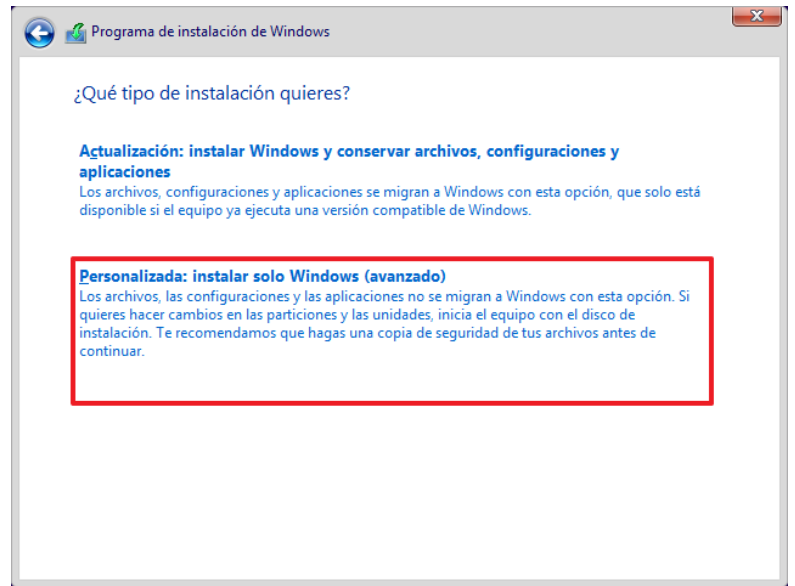
- b) Es importante separar datos, aplicaciones y sistema operativo en distintos dispositivos de almacenamiento, tanto para mejorar el rendimiento como para evitar ataques que se realizan navegando entre directorios. Para la seguridad de un equipo con sólo Windows 10 no se requiere la existencia de distintas particiones, pero se deberá tener en cuenta durante el proceso de instalación, ya que existen roles para los cuales se requiere que existan estas particiones diferenciadas.
- c) Si existen datos en el equipo antes del proceso de instalación, deberán eliminarse antes de comenzar el proceso.
- d) No deberán realizarse actualizaciones desde versiones previas, ya que de lo contrario no podrá garantizarse que los valores por defecto de los parámetros de seguridad se hayan aplicado.
- e) No utilizar discos o particiones que utilicen el sistema de archivos FAT.
- f) No instalar otros sistemas operativos en el equipo.
- g) Asignar una contraseña compleja a la cuenta de usuario que se crea durante el proceso de instalación.
- h) Una vez finalizada la instalación básica del sistema, asegurarse de que se instalan 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.
- i) Deberá realizarse la activación de Windows antes de comenzar el proceso de securización con el equipo conectado a una red segura.

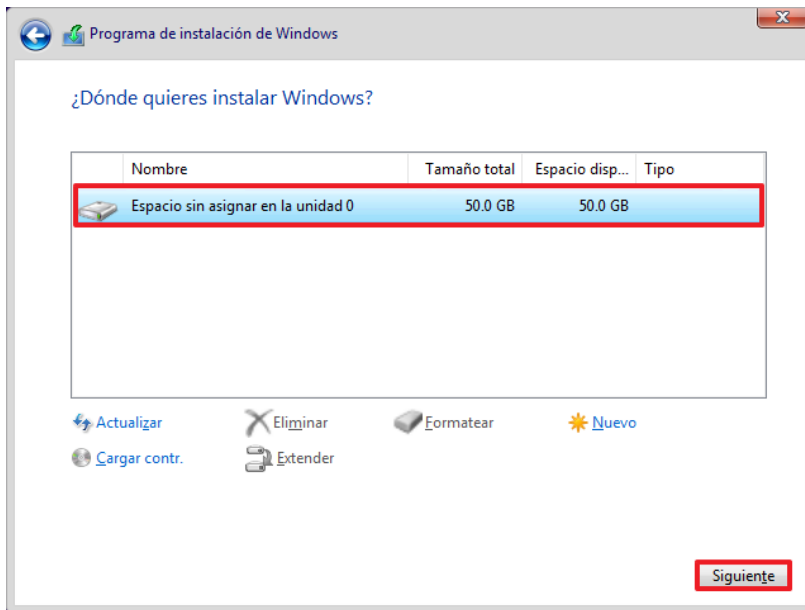
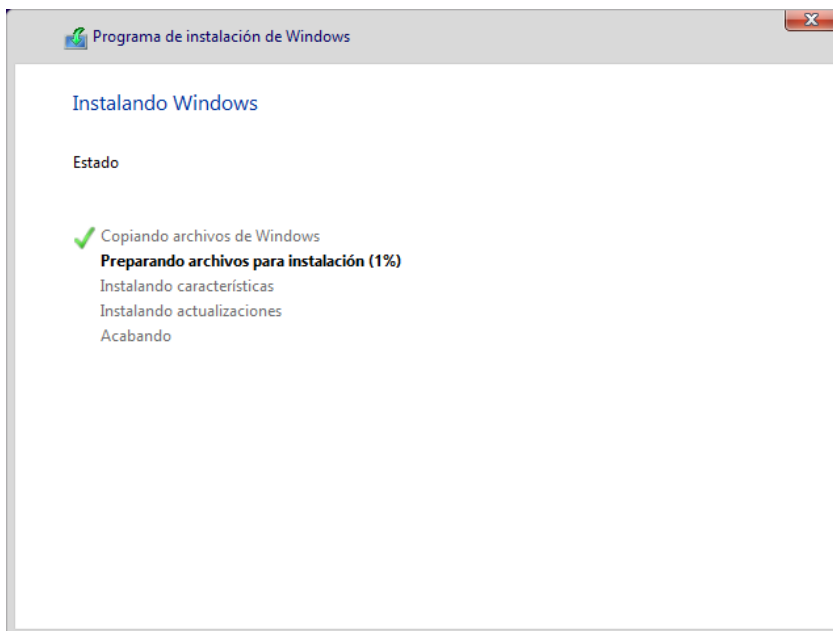
1. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10

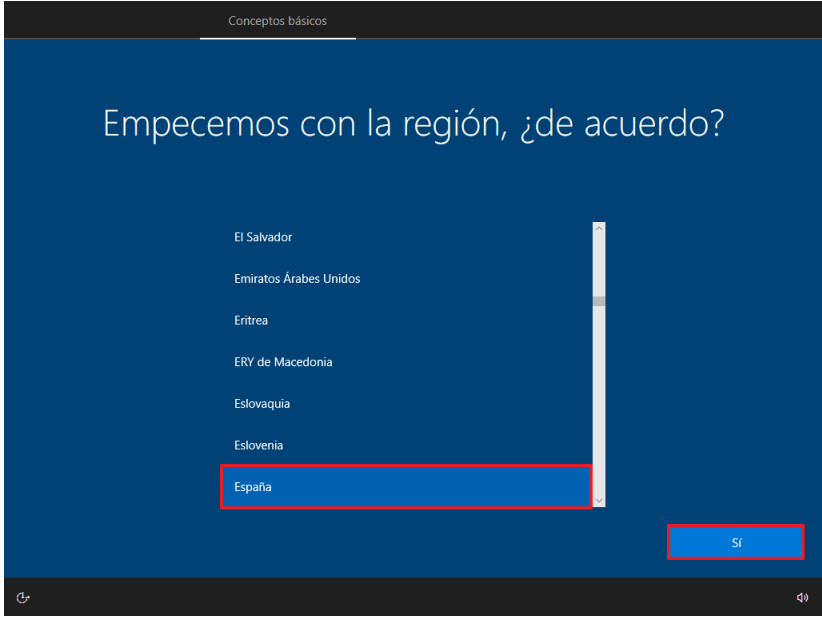
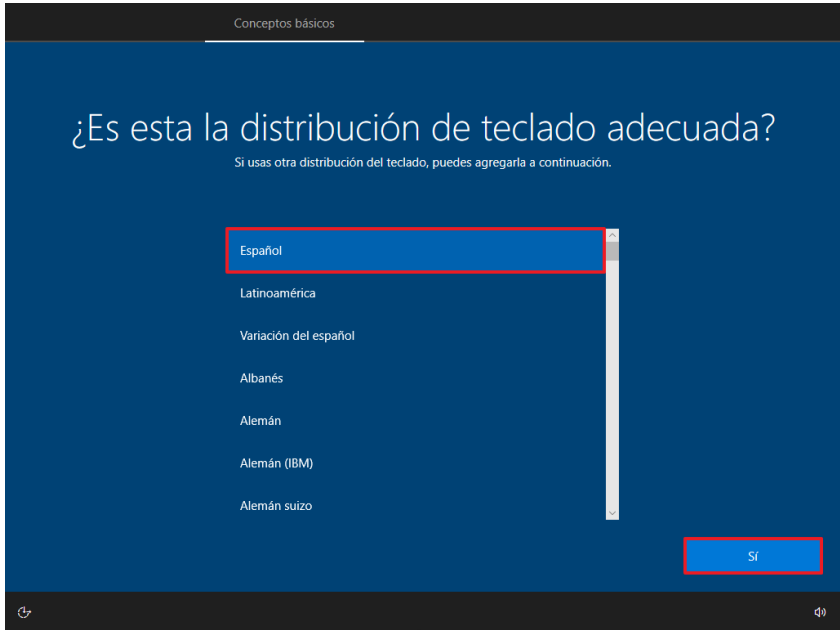
El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación. No se proporciona un fichero de respuestas automáticas, como se hacía en otras guías para versiones anteriores de Windows, esto se debe a que la instalación por defecto de Windows 10 habilita una serie de características opcionales, que serán fácilmente eliminadas a posteriori y antes del primer inicio del sistema. La eliminación de esta serie de características es parte del proceso de aplicación de esta guía.

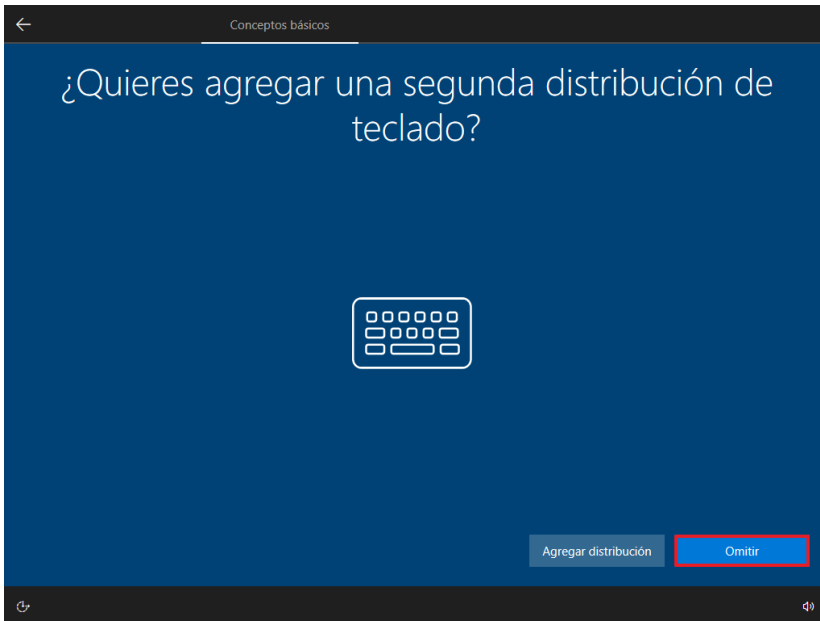
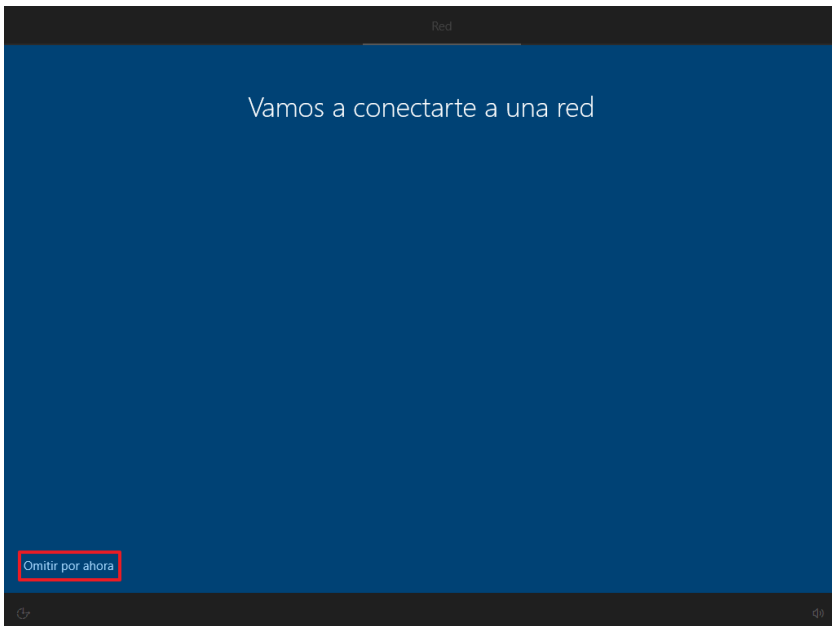
Paso	Descripción
1.	Introduzca el dispositivo USB o DVD de Windows 10 Enterprise LTSC y, si fuera necesario, reinicie la máquina para iniciar la instalación del sistema.
2.	Cuando aparezca el mensaje “Presionar una tecla para arrancar desde el DVD”, pulse una tecla. Si el equipo no se inicia desde DVD revise los parámetros de la BIOS.
3.	Cuando se le indique en pantalla, seleccione el idioma y la configuración de teclado (español). Pulse “Siguiente” para continuar. 

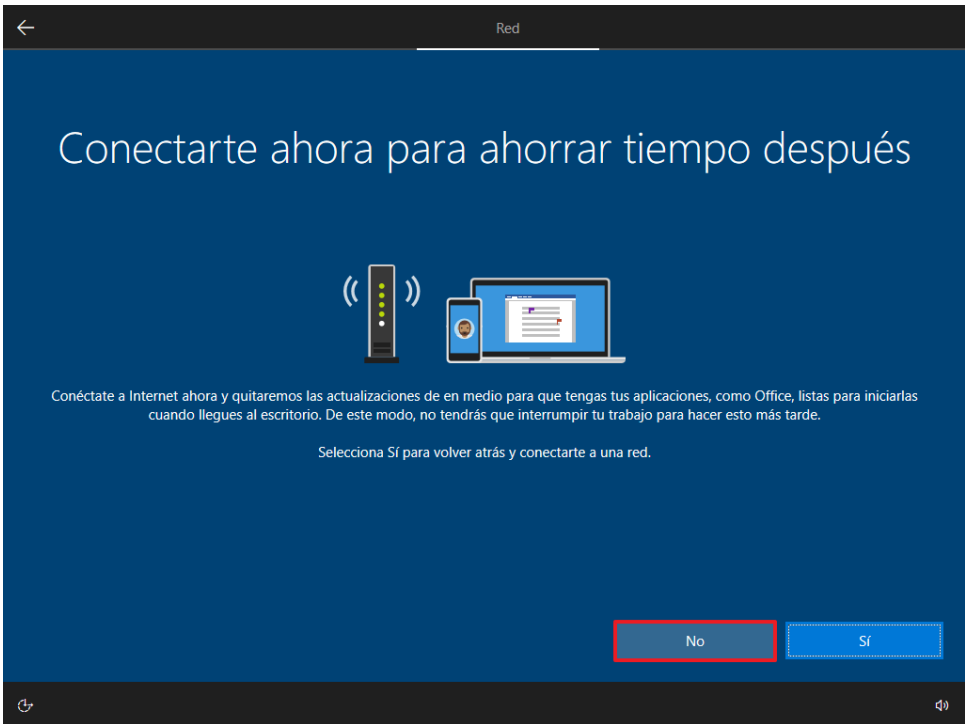
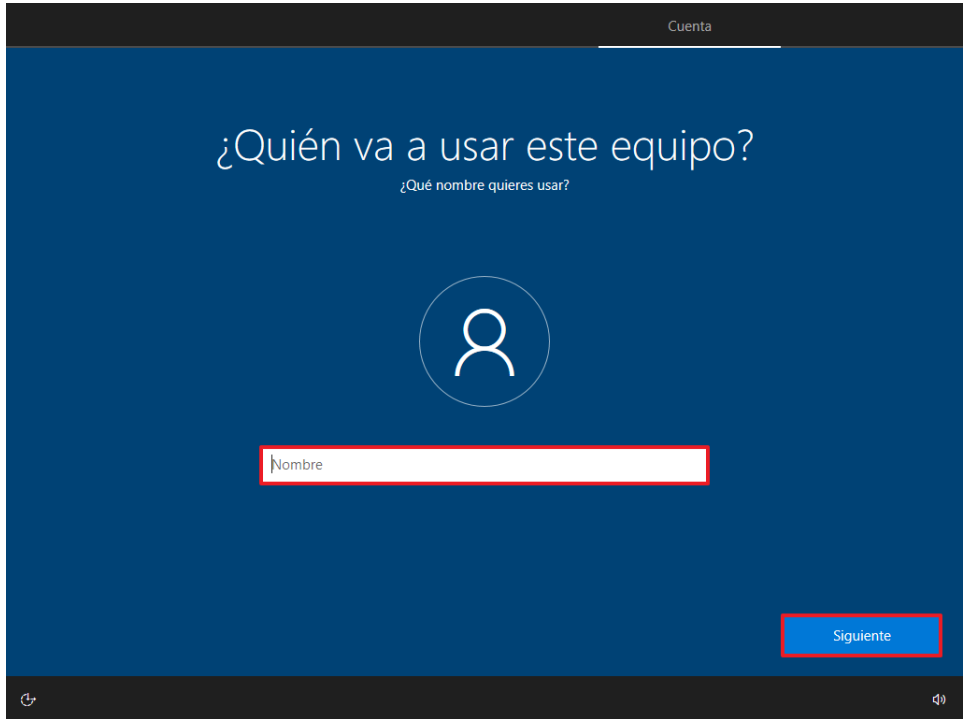
Paso	Descripción
4.	Pulse sobre “Instalar ahora”. 
5.	Seleccione la opción “Windows 10 Enterprise LTSC” y pulse “Siguiente”. 

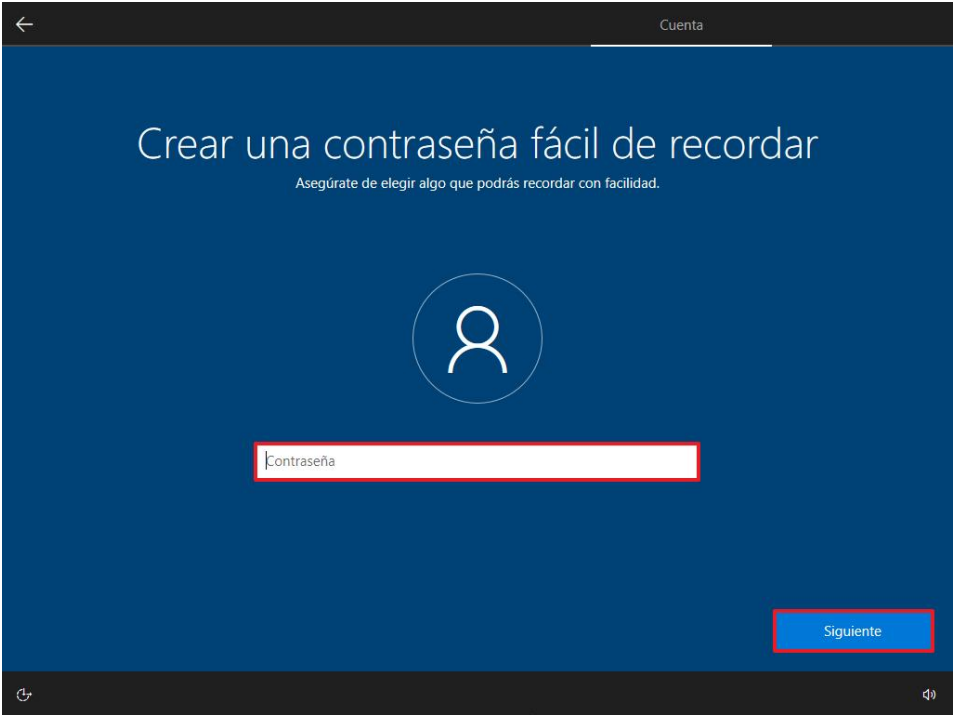
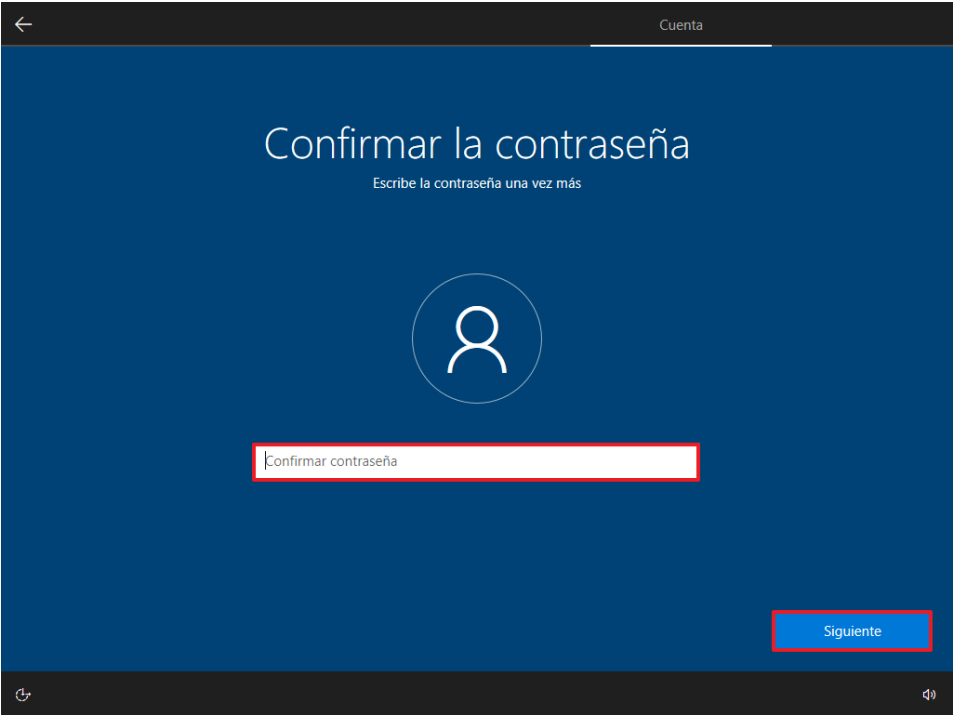
Paso	Descripción
6.	Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”. 
7.	Seleccione la opción tipo de instalación “Personalizada: instalar solo Windows (avanzado)”. 

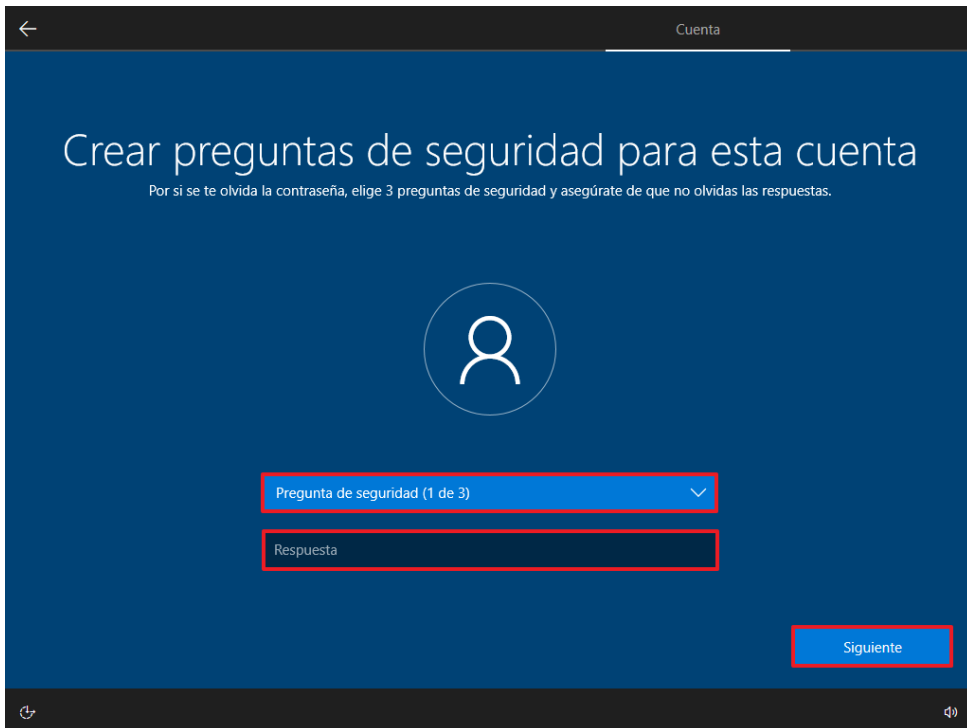
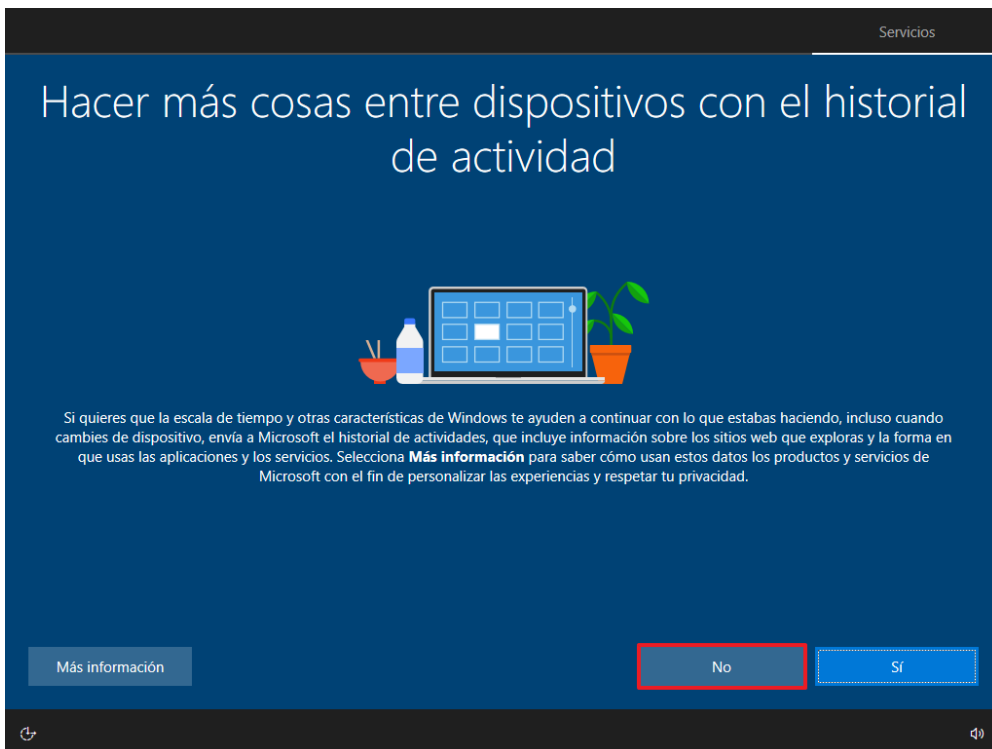
Paso	Descripción
8.	Seleccione el disco en el que se realizará la instalación y pulse “Siguiente”.  Nota: En caso de necesitar establecer particiones o formatear particiones o discos, es en este momento de la instalación en el que será necesario realizar dichos pasos. No es objeto de esta guía la explicación de los pasos a seguir para realizar este tipo de tareas, por tanto y si quiere realizar tareas de esta índole, puede consultar los pasos a seguir a través de este enlace: https://support.microsoft.com/es-es/help/15088/windows-10-create-installation-media#1TC=windows-10
9.	Comenzará la instalación en este momento. Este proceso durará varios minutos dependiendo de las prestaciones del dispositivo sobre el que se instale Windows 10 y, posiblemente, requerirá reiniciar en varias ocasiones. Espere a que aparezca la ventana “Conceptos básicos” y continúe con el siguiente paso. 

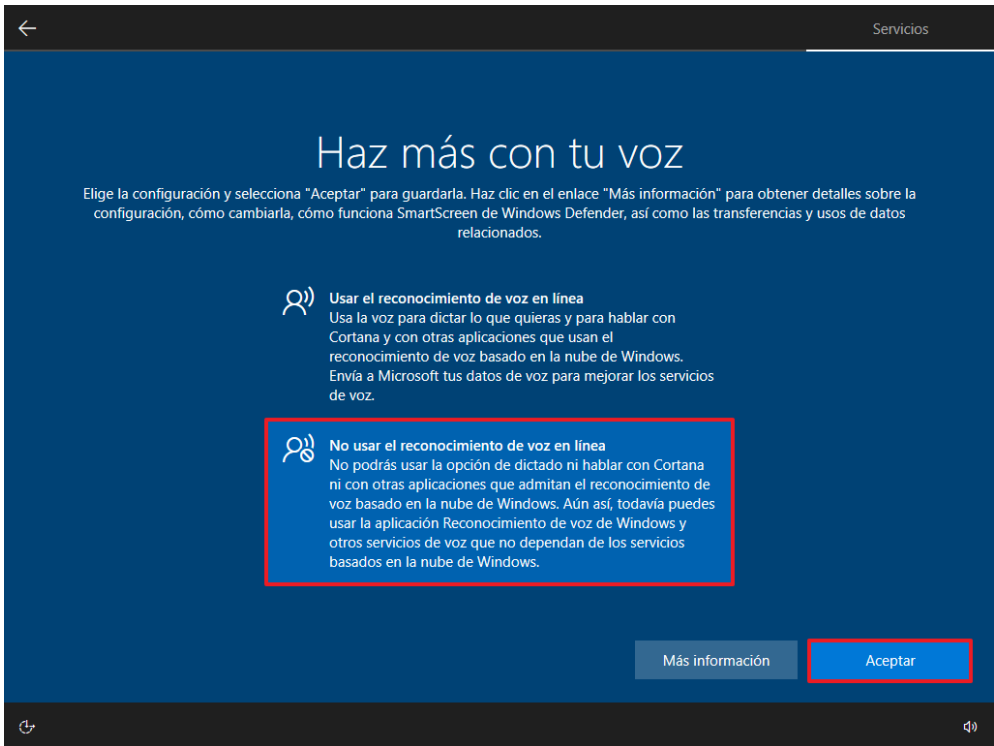
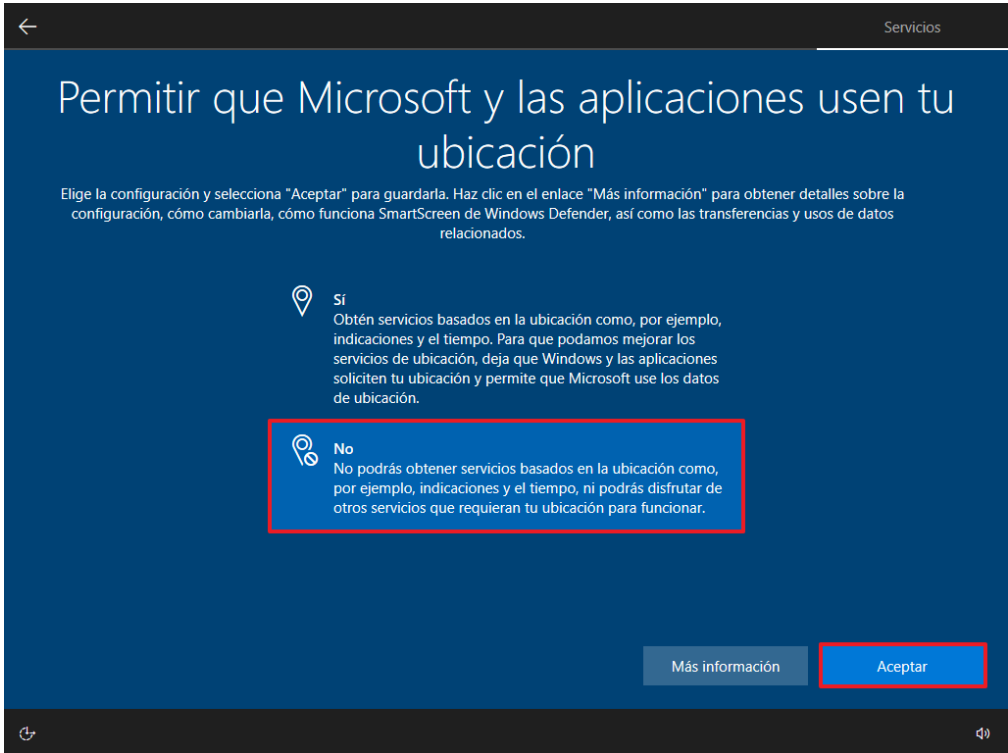
Paso	Descripción
10.	En la ventana “Conceptos básicos” seleccione la región “España” y pulse “Sí”. 
11.	Seleccione la distribución de teclado “Español” y pulse “Sí” para continuar. 

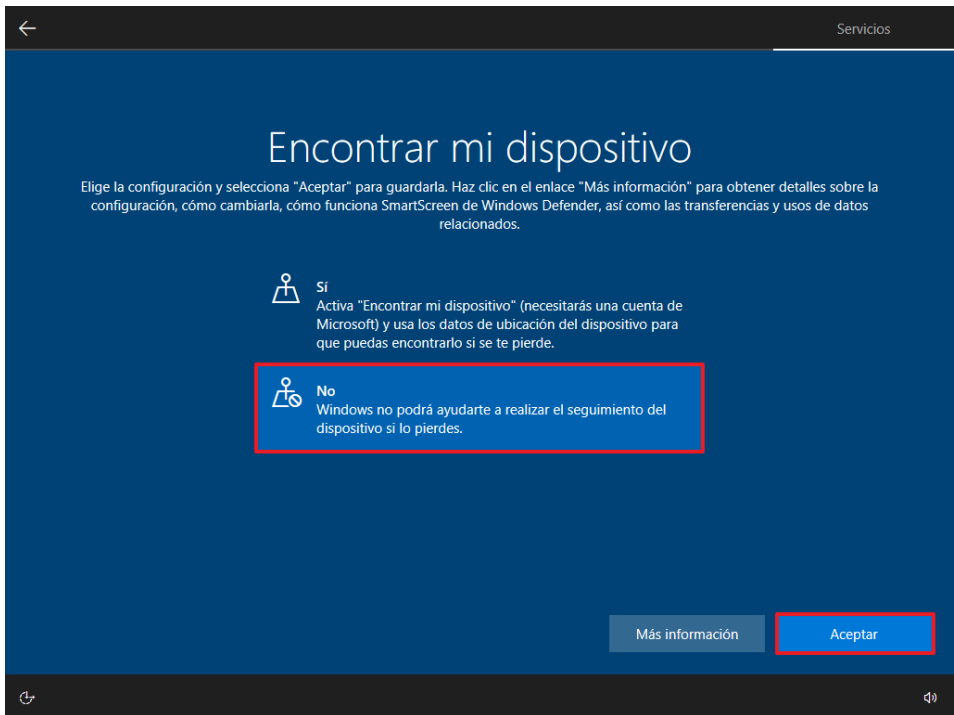
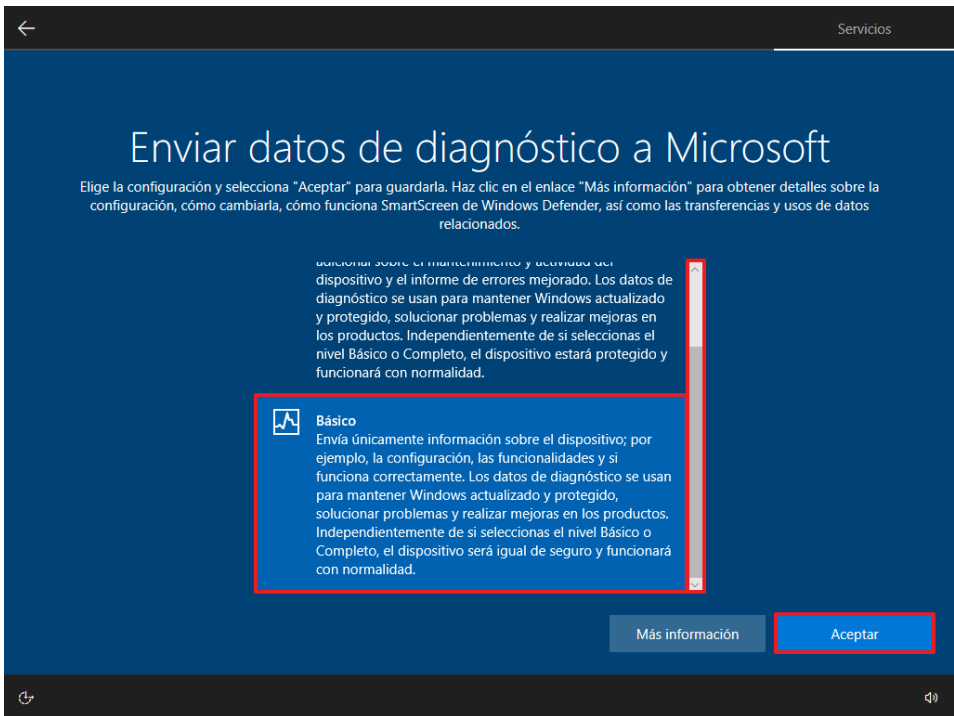
Paso	Descripción
12.	Pulse “Omitir” para no agregar una segunda distribución de teclado. 
13.	En el apartado de red seleccione la opción “Omitir por ahora”. 

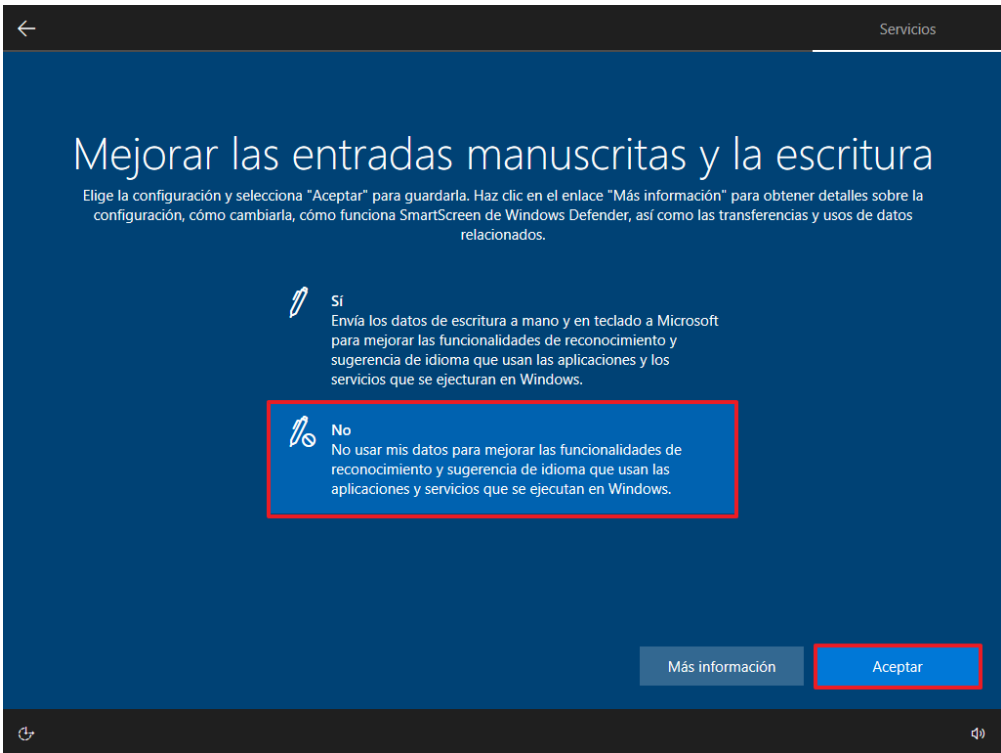
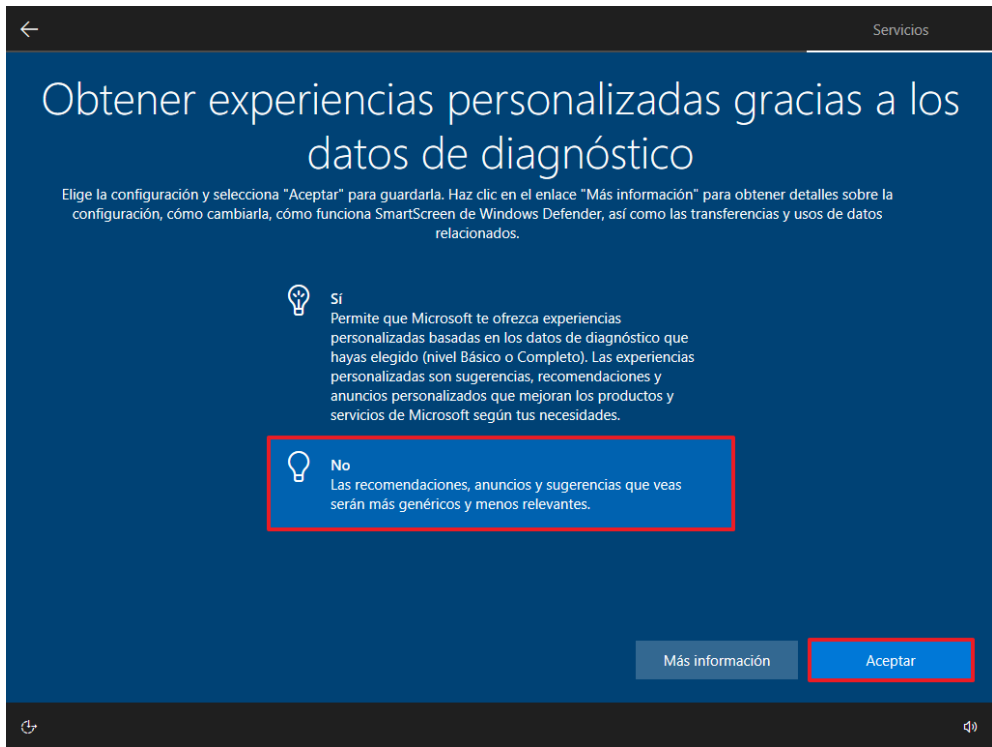
Paso	Descripción
14.	Pulse “No” para continuar. 
15.	En la ventana “Cuenta”, introduzca un nombre de usuario (por ejemplo "Admin") que se creará con permisos de administrador local. Pulse “Siguiente” para continuar.  Nota: Deberá elegir un nombre de usuario adecuado para su entorno. Los nombres aquí indicados sólo se proporcionan a modo de ejemplo.

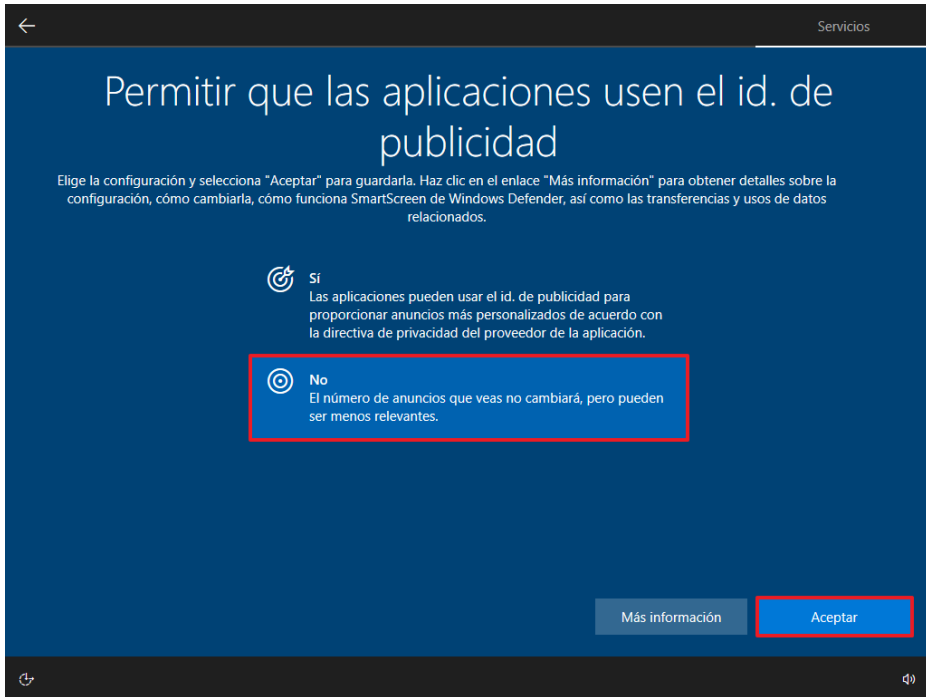
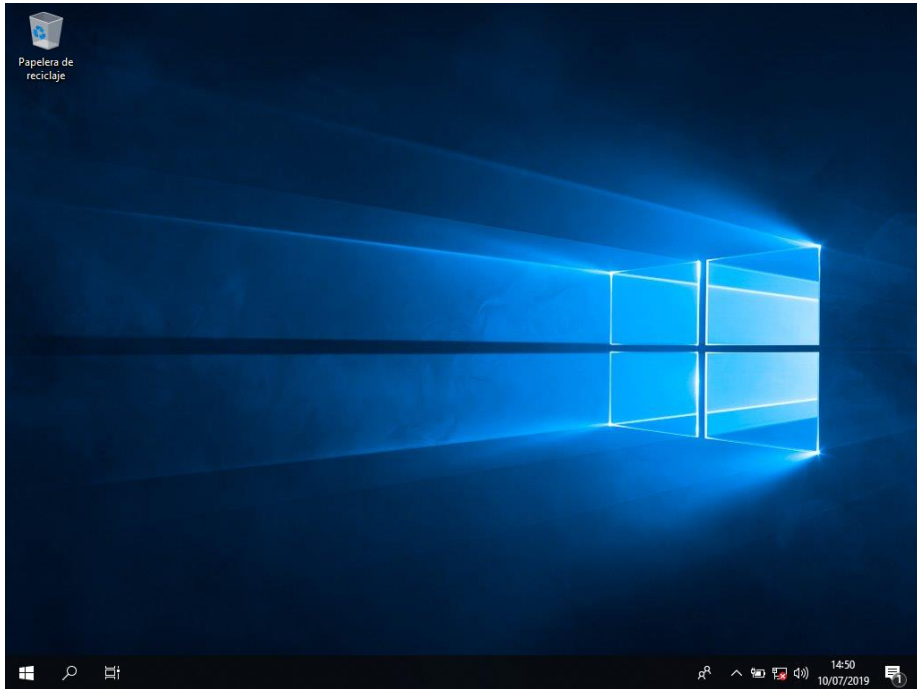
Paso	Descripción
16.	Introduzca una contraseña para el usuario administrador local y pulse “Siguiente”. 
17.	Introduzca nuevamente la contraseña y pulse “Siguiente”. 

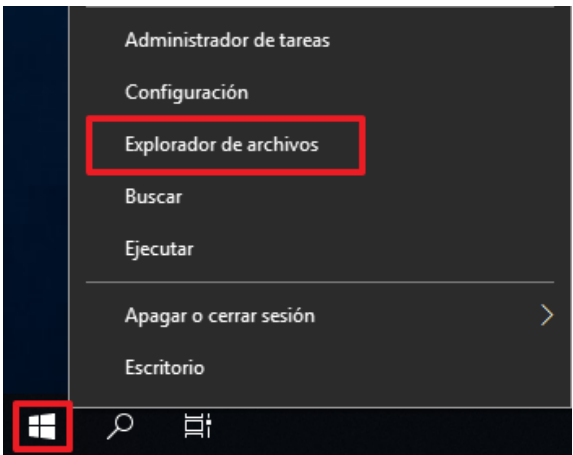
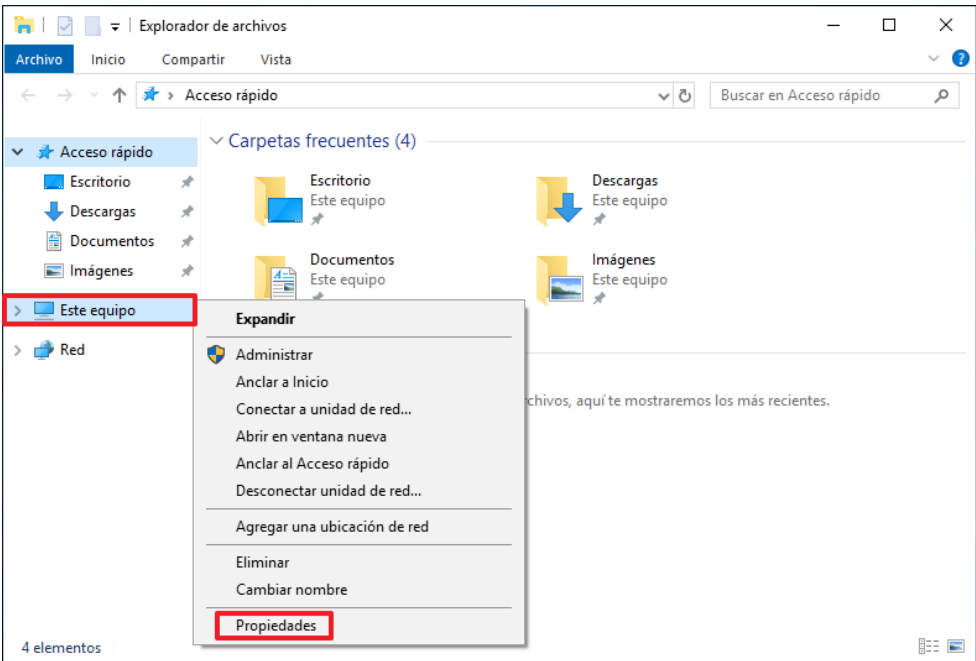
Paso	Descripción
18.	El instalador le solicitará tres preguntas de seguridad en caso de olvidar la contraseña. Seleccione las preguntas, respóndalas y pulse “Siguiente” para continuar.  Nota: Más adelante se establecerá el bloqueo de la cuenta en caso de introducir erróneamente la contraseña repetidas veces.
19.	Pulse “No” para desactivar el historial de actividad. 

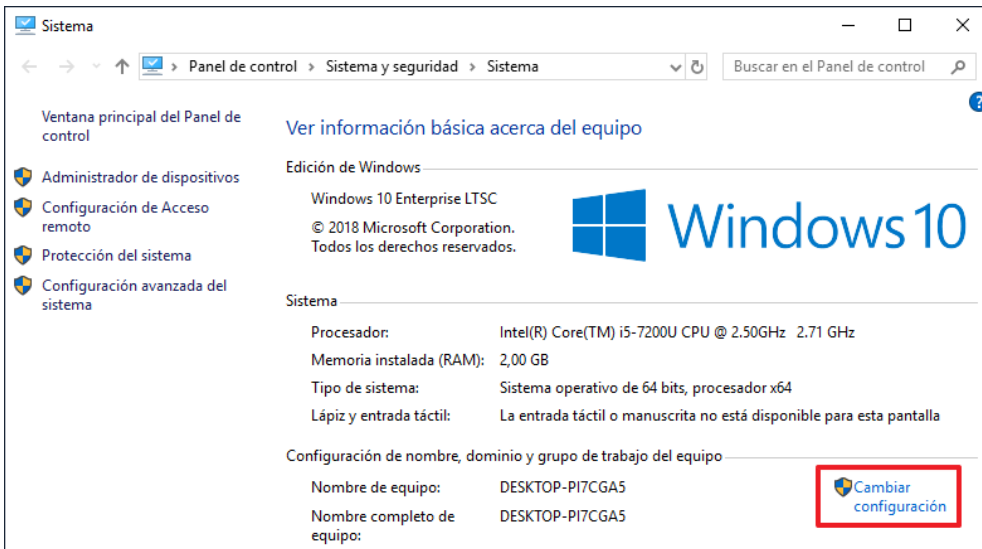
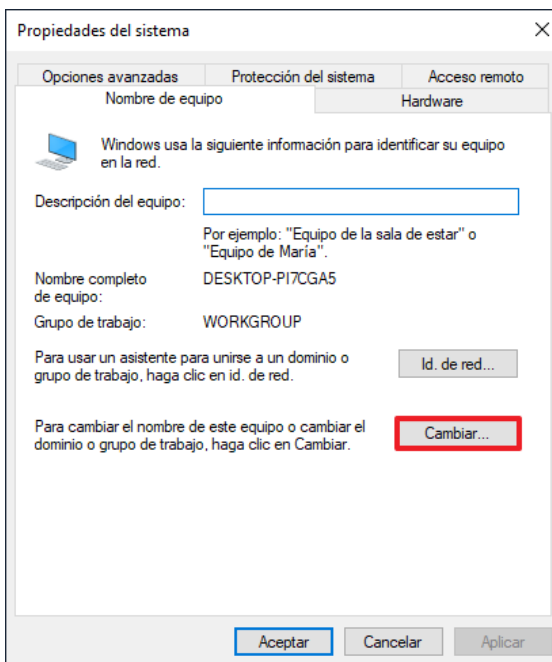
Paso	Descripción
20.	Seleccione “No” para no usar el reconocimiento de voz en línea y pulse “Aceptar”. 
21.	Seleccione “No” para impedir que las aplicaciones usen la ubicación y pulse “Aceptar”. 

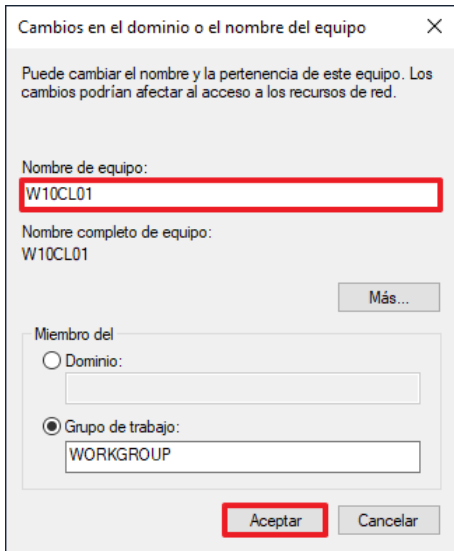
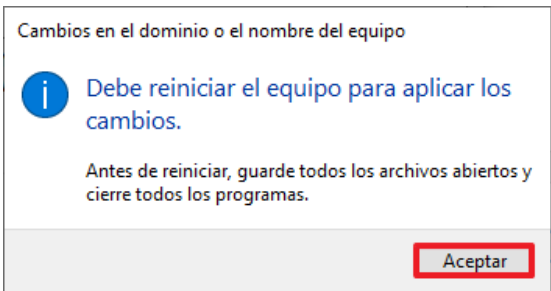
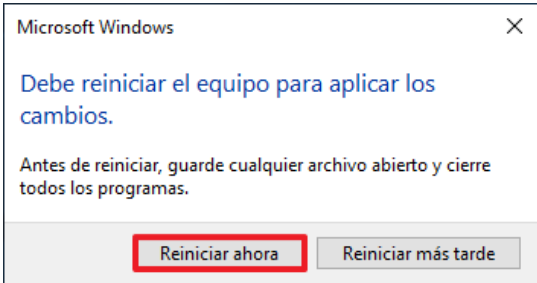
Paso	Descripción
22.	Seleccione “No” para desactivar la funcionalidad de “Encontrar mi dispositivo”. Pulse “Aceptar” para continuar. 
23.	Seleccione la opción “Básico” y pulse “Aceptar”.  Nota: Más adelante se impedirá toda comunicación con los servidores de Windows y se desactiva la telemetría.

Paso	Descripción
24.	Seleccione “No” y pulse “Aceptar”. 
25.	Seleccione “No” para no enviar datos de diagnóstico. Pulse “Aceptar” para continuar. 

Paso	Descripción
26.	Seleccione “No” para impedir que las aplicaciones usen el identificador de publicidad. Pulse “Aceptar” para continuar. 
27.	El sistema iniciará sesión tras unos momentos de preparación, con el usuario recién creado con las configuraciones especificadas, el cual pertenecerá al grupo “Administradores”, y finalmente se mostrará el escritorio. 

Paso	Descripción
28.	En la barra de tareas, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 
29.	En el “Explorador de archivos” pulse con el botón derecho del ratón sobre “Este equipo” y seleccione “Propiedades”. 

Paso	Descripción
30.	En la ventana “Sistema” localice el apartado “Configuración de nombre, dominio y grupo de trabajo del equipo” y pulse sobre “Cambiar configuración” 
31.	En “Propiedades del sistema”, seleccione la pestaña “Nombre de equipo”, pulse sobre “Cambiar”. 

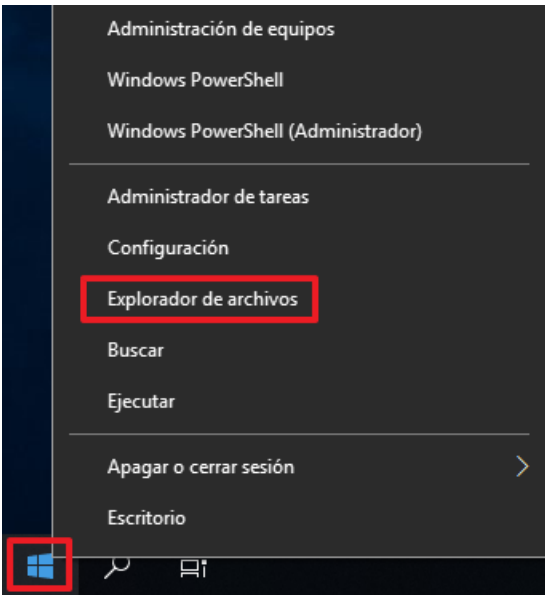
Paso	Descripción
32.	Establezca un nombre de equipo y pulse “Aceptar”.  Nota: En el ejemplo, el equipo se denomina “W10CL01”. Establezca el nombre más adecuado para su organización.
33.	El sistema deberá reiniciar para guardar los cambios. Pulse “Aceptar” en la ventana de “Cambios en el dominio o el nombre de equipo”. 
34.	Pulse sobre “Cerrar” en “Propiedades del sistema” y “Reiniciar ahora” para que se reinicie el equipo y hagan efecto los cambios. 

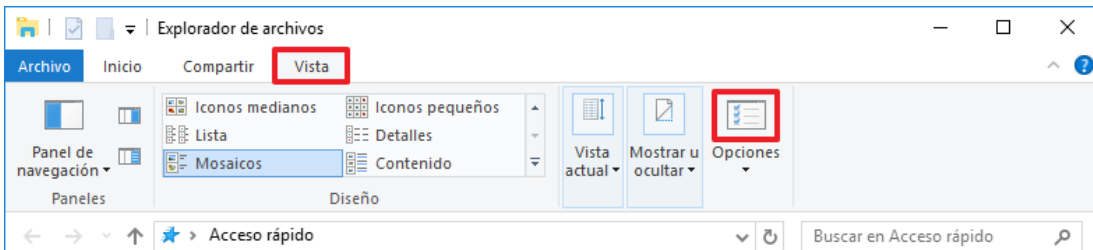
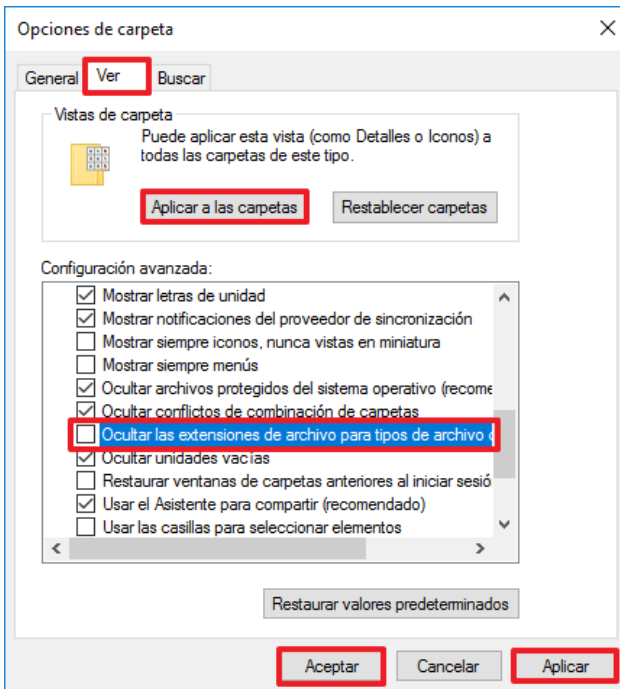
2. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10

A continuación, y una vez instalado el sistema operativo en el cliente Windows 10 independiente, se procederá a configurar el equipo.

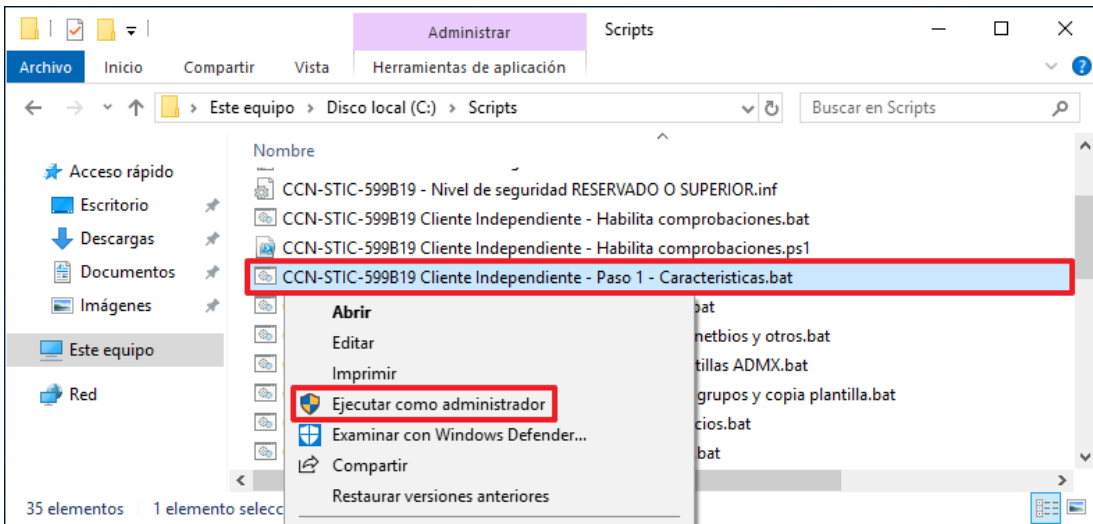
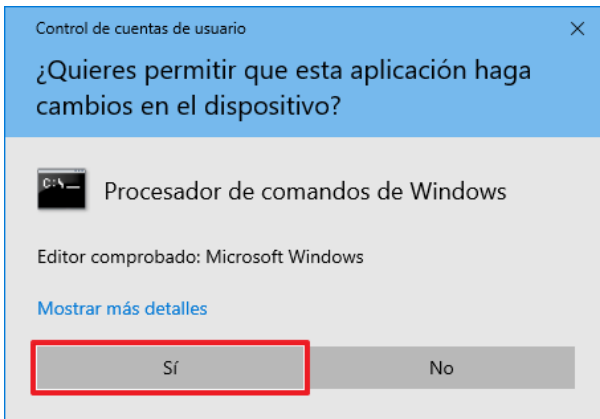
Nota: En este punto es conveniente recordar que, aunque en esta guía paso a paso no se dedica ningún apartado concreto a ello, será necesario instalar las actualizaciones de seguridad disponibles y realizar la activación de Windows en el equipo.

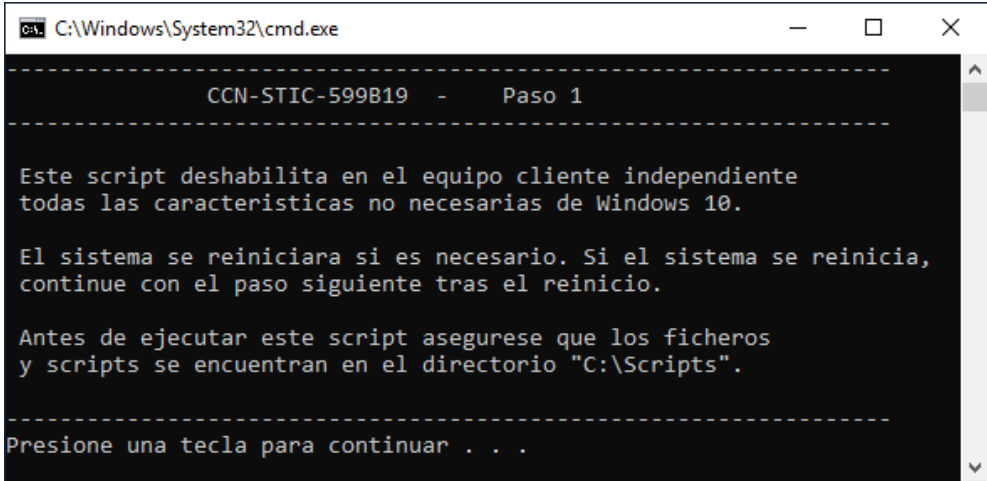
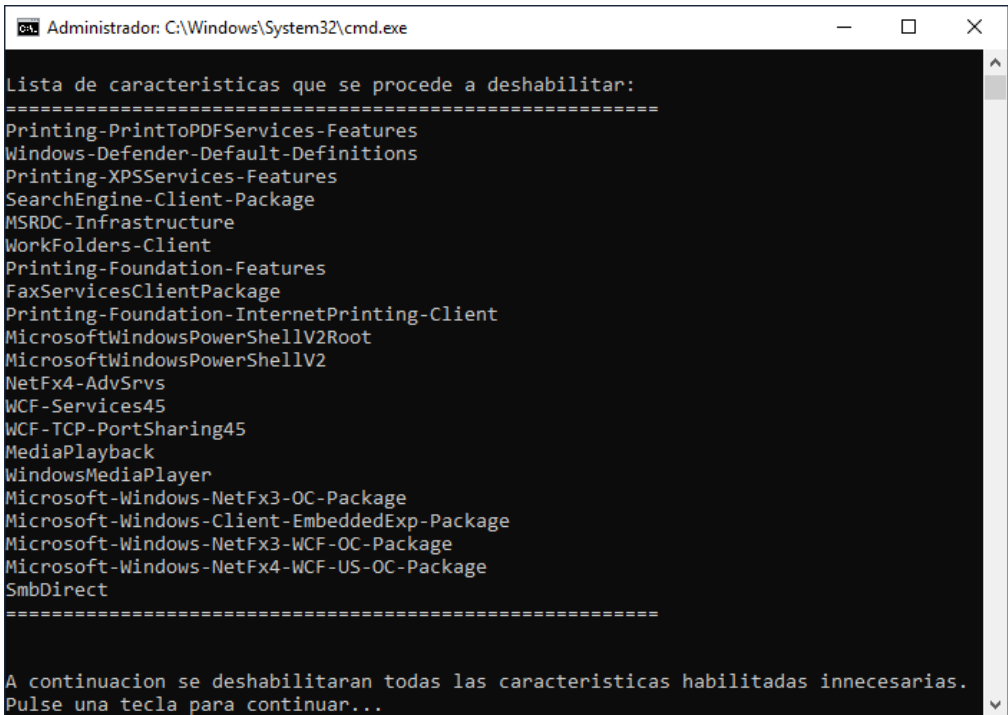
Los pasos que se describen a continuación contemplan el uso de Windows 10 en un equipo independiente. En este caso se incluirán los elementos de seguridad tanto para el sistema operativo como para Internet Explorer 11.

Paso	Descripción
35.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador.
36.	Cree el directorio "Scripts" en la unidad "C:\\"
37.	Copie los ficheros asociados a esta guía en el directorio "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19". Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación tendría que editar los scripts para reflejar la nueva ubicación.
38.	Configure el "Explorador de archivos" para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos" oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de "Inicio" con el botón derecho y seleccione "Explorador de archivos". 

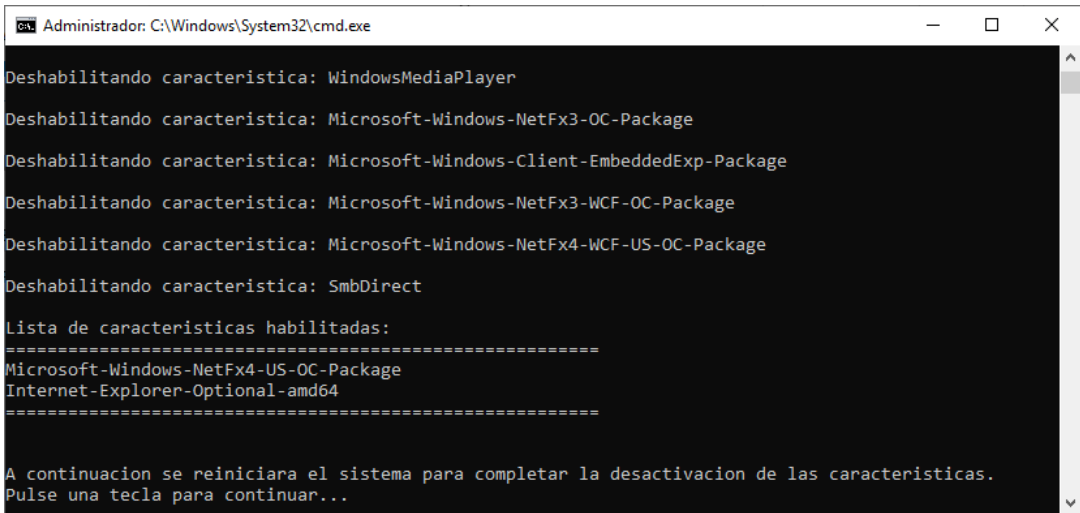
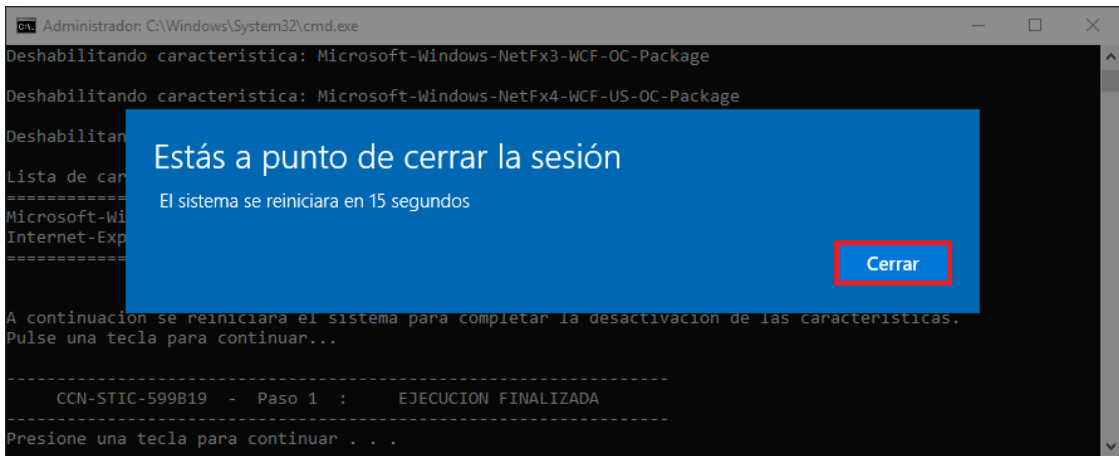
Paso	Descripción
39.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
40.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 

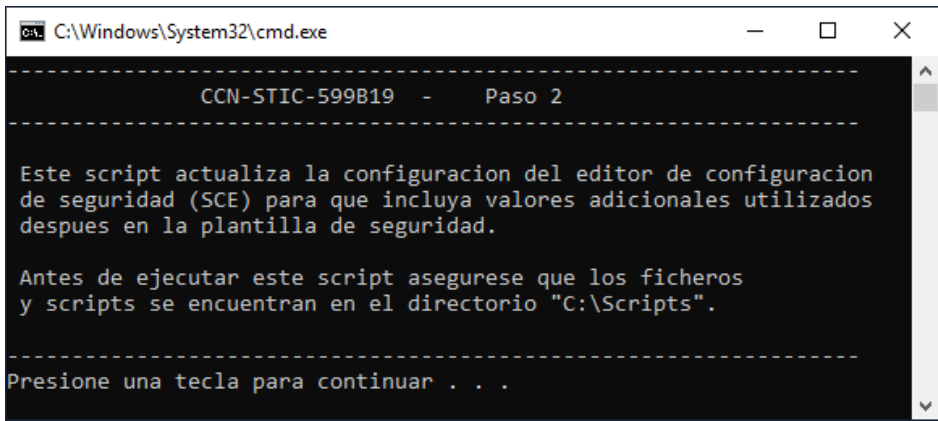
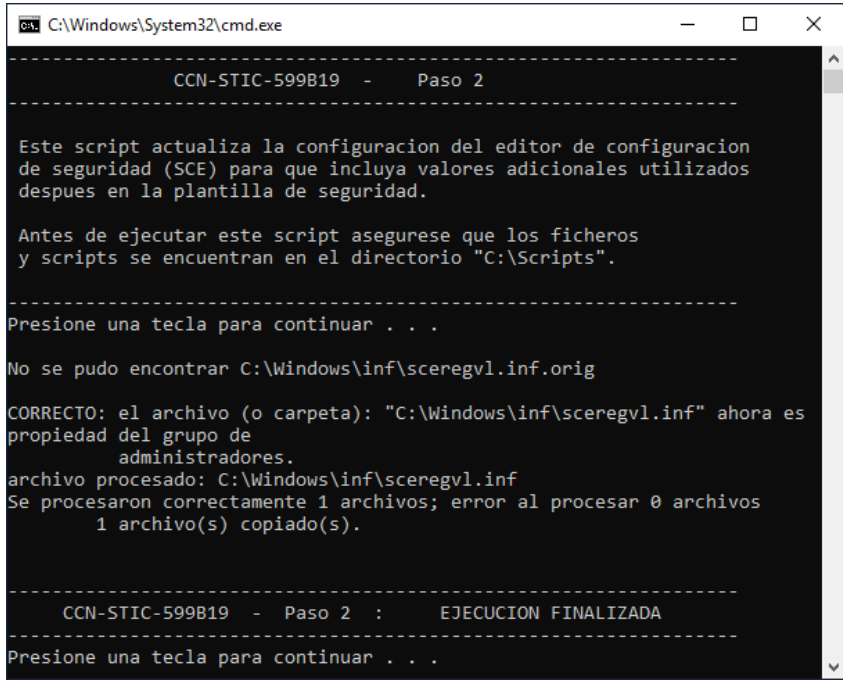
Paso	Descripción
41.	Compruebe que en el directorio "C:\Scripts" se encuentran al menos los siguientes directorios y ficheros: – Group Policy (Directorio) – PolicyDefinitions (Directorio) – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.ps1 – CCN-STIC-599B19 Cliente Independiente - Paso 1 - Caracteristicas.bat – CCN-STIC-599B19 Cliente Independiente - Paso 2 - SCE.bat – CCN-STIC-599B19 Cliente Independiente - Paso 3a - IPv6 netbios y otros - LTSC.bat – CCN-STIC-599B19 Cliente Independiente - Paso 3b - IPv6 netbios y otros - PRO.bat – CCN-STIC-599B19 Cliente Independiente - Paso 4 – Plantillas ADMX.bat – CCN-STIC-599B19 Cliente Independiente - Paso 5 – Crea grupos y copia plantilla.bat – CCN-STIC-599B19 Cliente Independiente - Paso 6 – Servicios.bat – CCN-STIC-599B19 Cliente Independiente - Paso 7 – GPO.bat – CCN-STIC-599B19 Cliente Independiente - Paso 8a – Deshabilita Appx - LTSC.bat – CCN-STIC-599B19 Cliente Independiente - Paso 8b – Deshabilita Appx - PRO.bat – CCN-STIC-599B19 Cliente Independiente - Paso 9 – Firewall.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10a - Aplica plantilla adicional CONFIDENCIAL.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat – CCN-STIC-599B19 Cliente Independiente - Paso 11 – Aplica plantilla y reinicia.bat – CCN-STIC-599B19 Cliente Independiente.inf – CCN-STIC-599B19 Cliente Independiente.wfw – CCN-STIC-599B19 Importar ADMX.ps1 – CCN-STIC-599B19 Servicios.inf – CCN-STIC-599B19_Deshabilita_NetBIOS_sobre_TCPIP.ps1 – CCN-STIC-599B19_Desinstala_Appx_LTSC.ps1 – CCN-STIC-599B19_Desinstala_Appx_Pro.ps1 – CCN-STIC-599B19_Desinstala_caracteristicas.ps1 – CCN-STIC-599B19_No_IPv6.reg – deshab_appx.reg – drwatson.reg – Plantillas de seguridad.msc – posix.reg – refusereset.reg – sceregl.inf – ssdp.reg – Start_Layout.xml

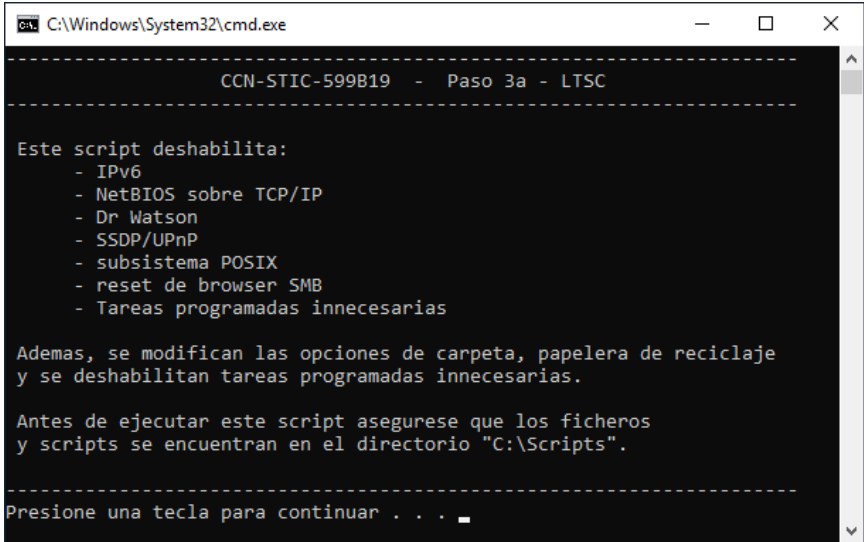
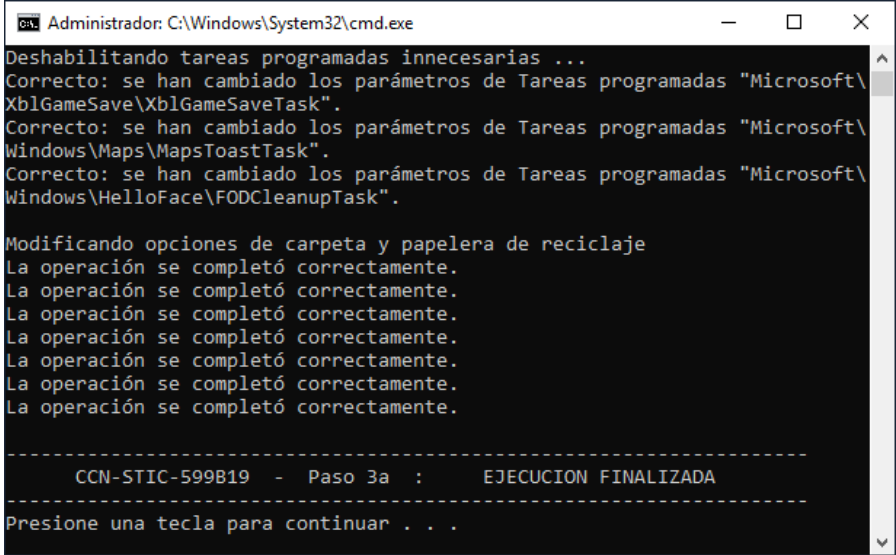
Paso	Descripción
42.	Ejecute con permisos de administrador el script "CCN-STIC-599B19 Cliente Independiente - Paso 1 - Caracteristicas.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario con permisos de administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
43.	Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

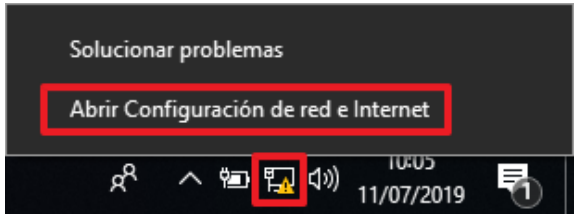
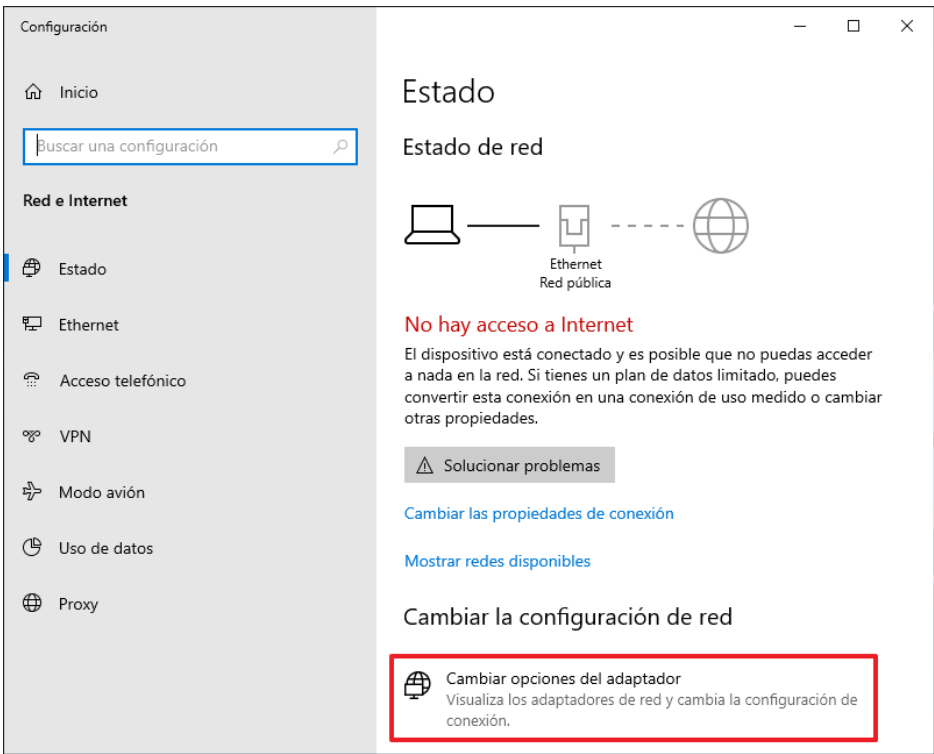
Paso	Descripción
44.	Este script deshabilitará todas las características opcionales que se encuentren habilitadas en el equipo. Pulse una tecla para continuar el proceso. 
45.	El sistema mostrará una lista de las características instaladas que no son necesarias y que deberán ser eliminadas. Pulse una tecla para continuar con el proceso de eliminación de las características.  Nota: Internet Explorer 11 se mantendrá instalada por ser la herramienta autorizada para la navegación. Como se ha indicado anteriormente, la aplicación de la presente guía incluirá también la seguridad de Internet Explorer 11 que aplica la guía CCN-STIC-520.

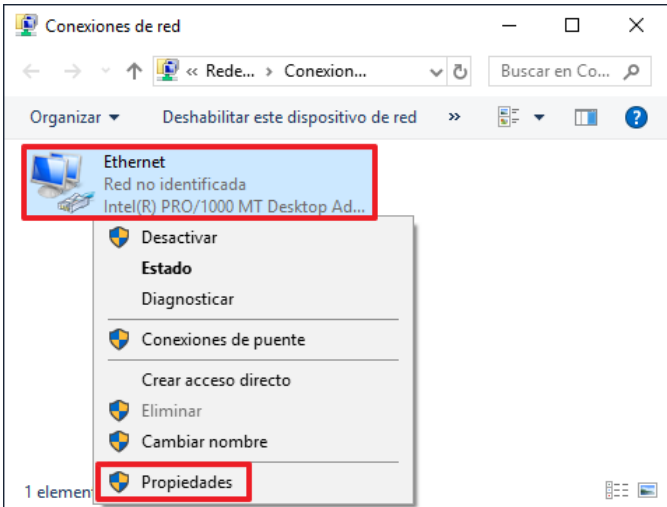
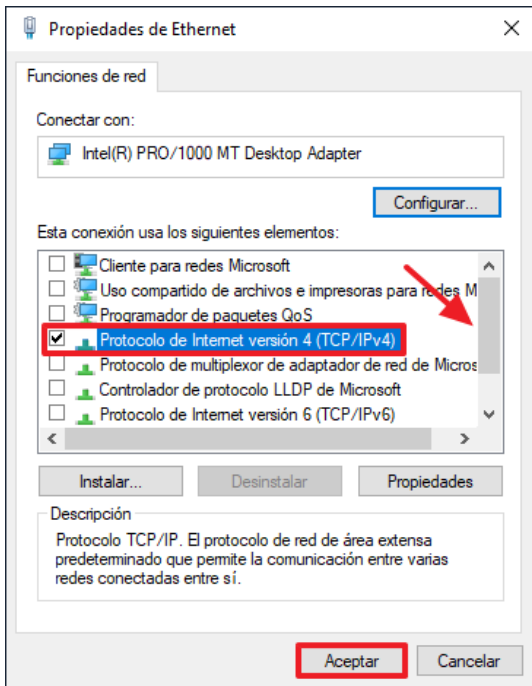


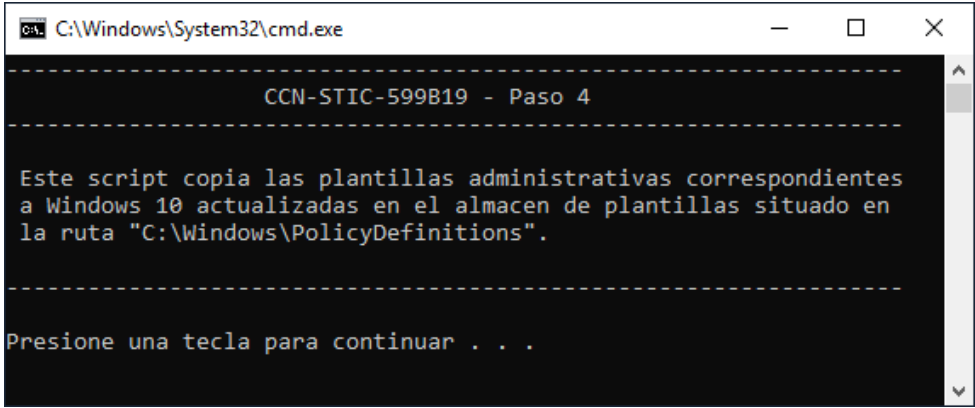
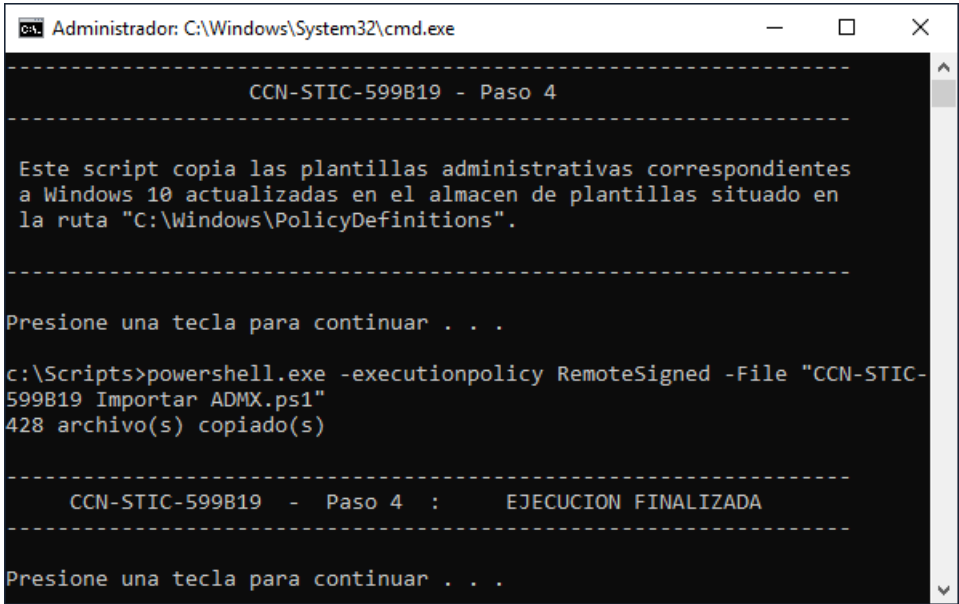
Paso	Descripción
46.	Una vez desinstaladas las características innecesarias compruebe que únicamente se mantienen instaladas las características “Internet-Explorer-Optional-amd64” y “Microsoft-Windows-NetFx4-US-OC-Package”, que son necesarias para la funcionalidad del cliente Windows 10.  Nota: Si apareciese el error “0x800f080c” durante la desinstalación se debe a un error con las dependencias de las características ya desinstaladas. Ignórelo y continúe con el siguiente paso.
47.	Será necesario que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. Al finalizar la ejecución, se reiniciará automáticamente el sistema. Pulse “Cerrar” en el mensaje de confirmación y cuando el sistema se inicie, continúe con el siguiente paso. 

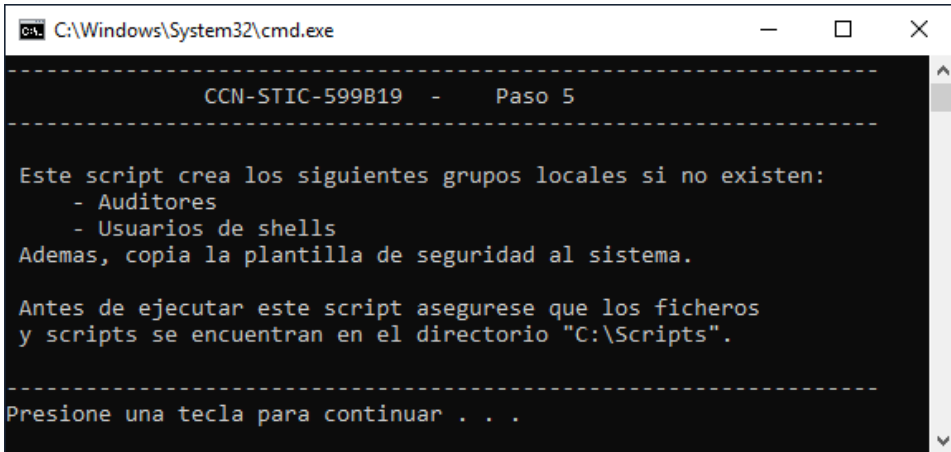
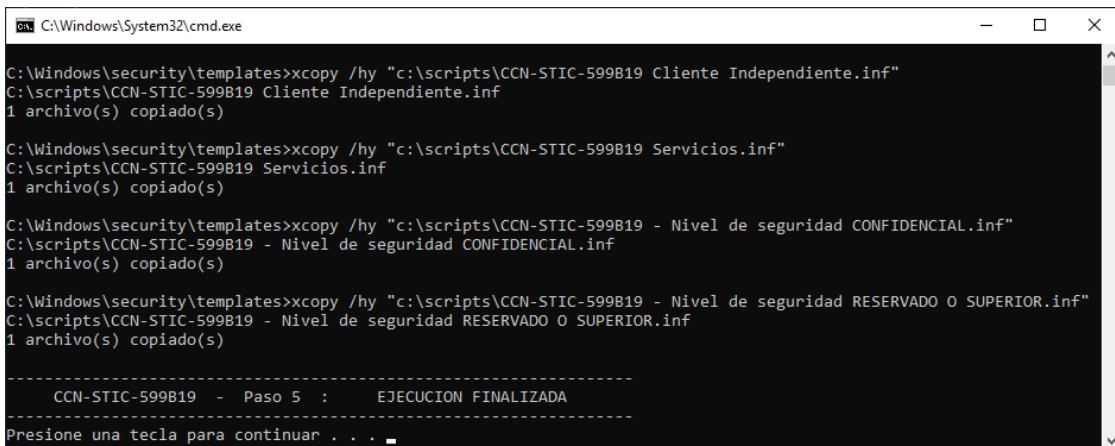
Paso	Descripción
48.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 2 - SCE.bat" situado en la carpeta "C:\Scripts" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: El sistema le solicitará elevación de privilegios.
49.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: Este script actualiza la configuración de SCE (editor de configuración de seguridad) para que incluya valores adicionales. Si aparece el aviso "No se pudo encontrar C:\Windows\inf\sceregl.inf.orig", este aviso se puede ignorar. Sólo se debe a que no se encontró una copia de seguridad anterior del fichero "sceregl.inf". No representa ningún problema y se puede continuar con el siguiente paso.

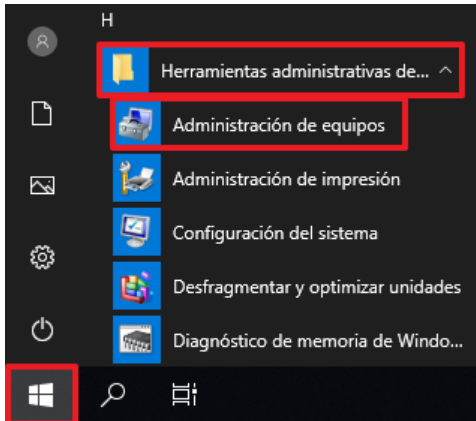
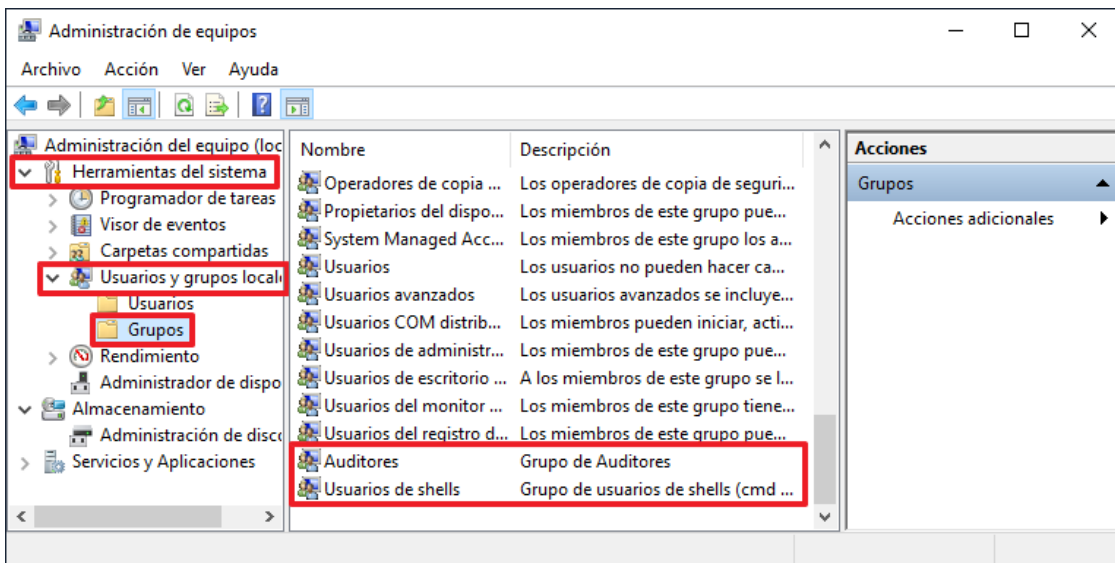
Paso	Descripción
50.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 3a – Ipv6 netbios y otros - LTSC.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: El sistema le solicitará elevación de privilegios.
51.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 

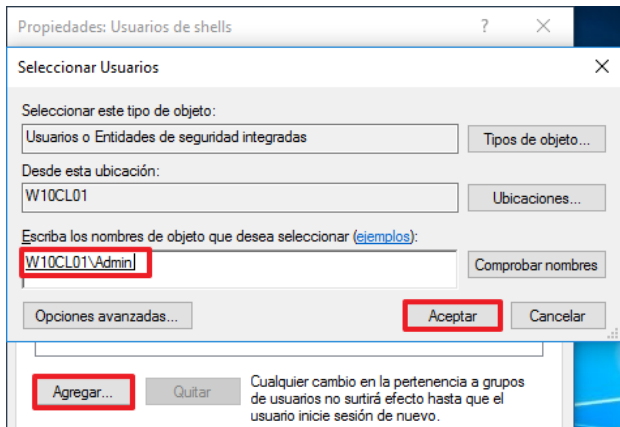
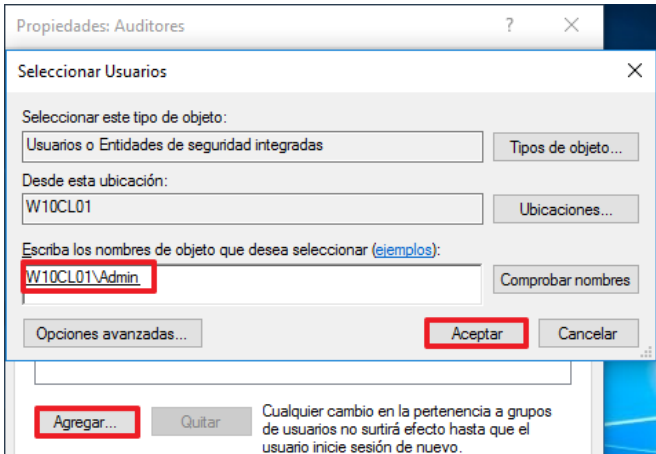
Paso	Descripción
52.	A continuación, en la barra de tareas, localice el icono de conexiones de red y pulsando con el botón derecho del ratón sobre él seleccione “Abrir Configuración de red e Internet”.  Nota: Los pasos que se describen a continuación deberá realizarlos únicamente si dispone de adaptador de red. Si no es el caso, continúe en el punto 57 del presente anexo.
53.	En el menú izquierdo del “Centro de redes y recursos compartidos” pulse sobre “Cambiar configuración del adaptador”. 

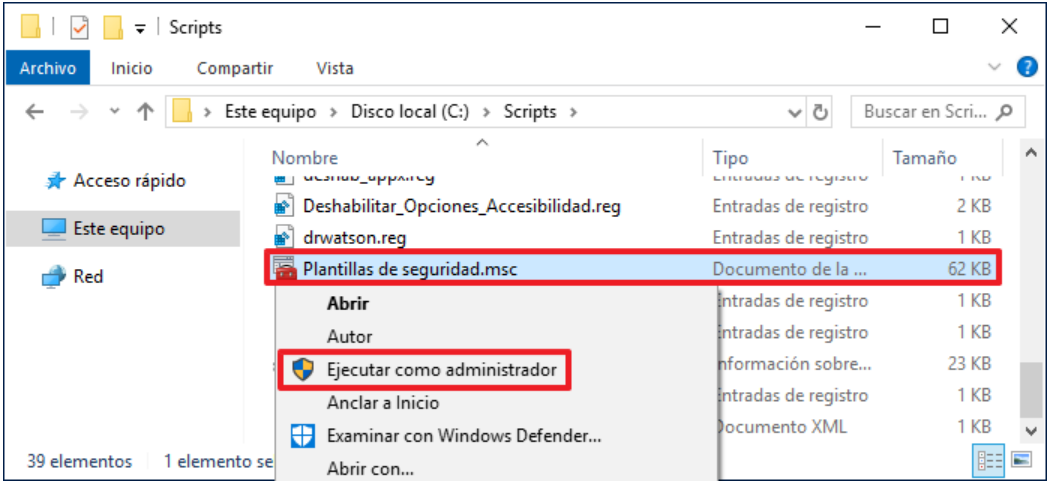
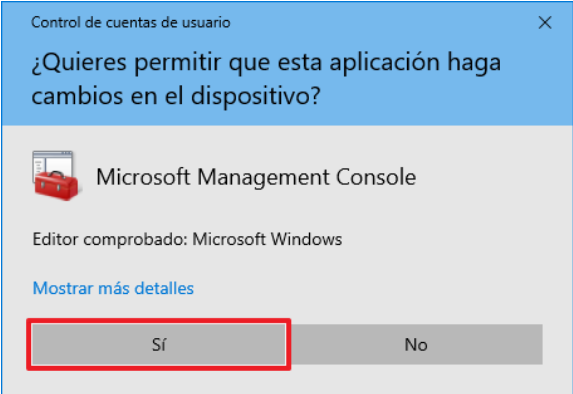
Paso	Descripción
54.	Pulse con el botón derecho sobre el adaptador de red y seleccione "Propiedades". 
55.	En la ventana "Propiedades de Ethernet" de las diferentes conexiones de red, desmarque si están marcados todos los elementos excepto "Protocolo de Internet versión 4 (TCP/IPv4)" como se muestra en la siguiente figura.  Nota: Recuerde hacer uso de la barra lateral para mostrar y deshabilitar todos los elementos.
56.	Pulse el botón "Aceptar", para cerrar la ventana guardando los cambios.

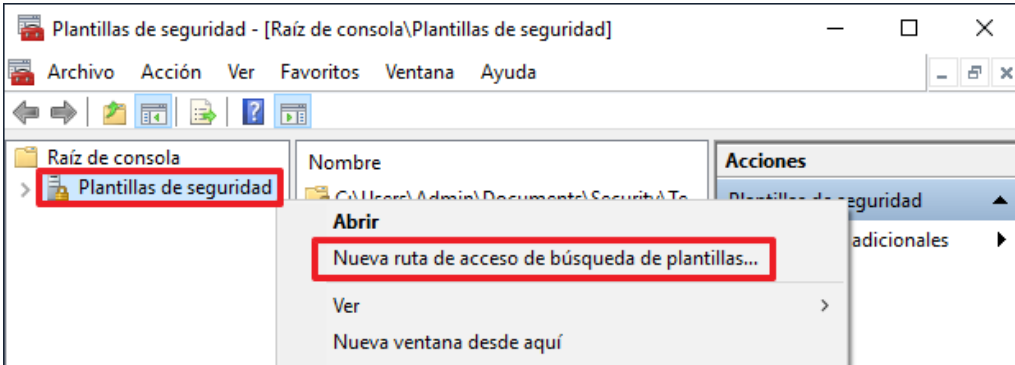
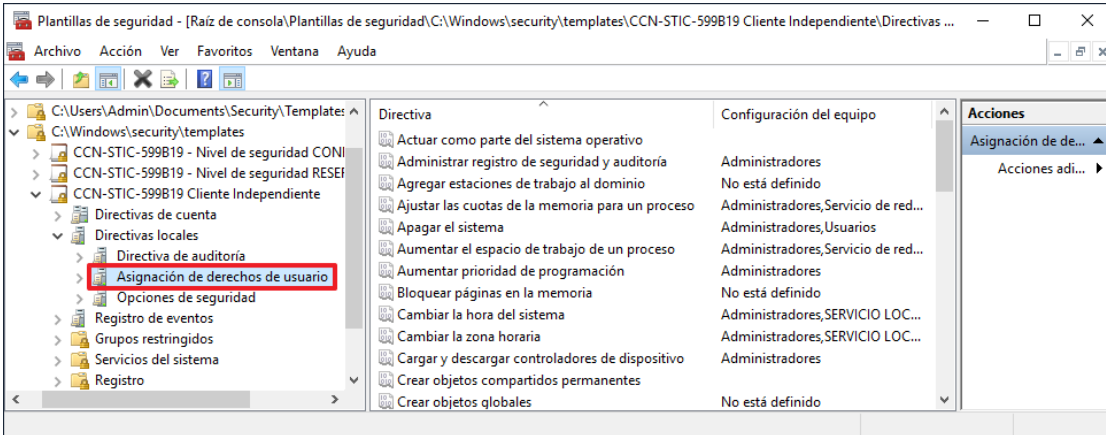
Paso	Descripción
57.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 4 – Plantillas ADMX.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: El sistema le solicitará elevación de privilegios.
58.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 

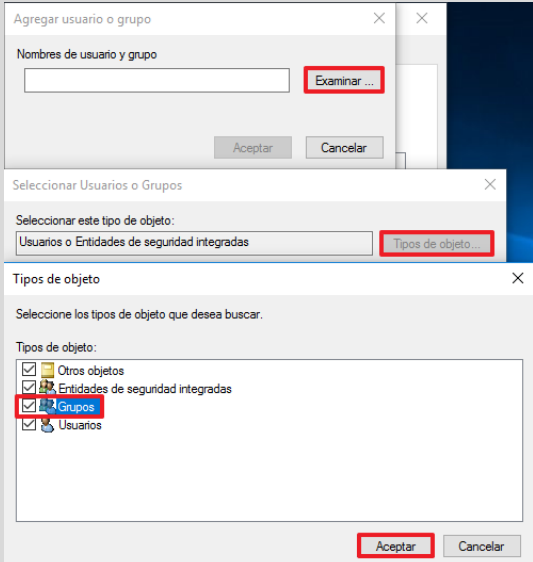
Paso	Descripción
59.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 5 – Crea grupos y copia plantilla.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script crea los grupos locales "Auditores" y "Usuarios de shells" y copia la plantilla de seguridad al sistema, bajo "C:\Windows\Security\Templates", para que pueda ser editada antes de su aplicación, tal y como se describe en los siguientes pasos.  Nota: Si el directorio principal de Windows no se encuentra en "C:\Windows", será necesario modificar el script para reflejar la ubicación correcta.
60.	Pulse una tecla de nuevo para cerrar la ventana de comandos. 

Paso	Descripción
61.	Incluya los usuarios adecuados de su organización en los grupos recién creados, "Auditores" y "Usuarios de shells". En el grupo "Usuarios de shells" deberá incluir al menos el usuario Administrador cuya identidad está utilizando para aplicar esta guía. Se recomienda incluir todos los miembros del grupo "Administradores". Para ello, ejecute la herramienta "Administración de equipos" haciendo clic sobre ella mediante la siguiente ruta: "Inicio → Herramientas administrativas de Windows → Administración de equipos"  Nota: Las plantillas de seguridad no pueden incluir a usuarios y grupos concretos de un dominio particular en los derechos de usuario ni en los permisos asignados a servicios o ficheros, puesto que éstos se incluyen mediante su SID que varía en cada instalación. Por ello, las plantillas de seguridad proporcionadas con estas guías no pueden aplicarse directamente y es necesario que se verifiquen y ajusten antes de su aplicación, para que presenten los valores adecuados.
62.	Una vez abierta la herramienta "Administrador de Equipos", expanda la siguiente rama: "Administración del equipo (local) → Herramientas del sistema → Usuarios y grupos locales → Grupos" 

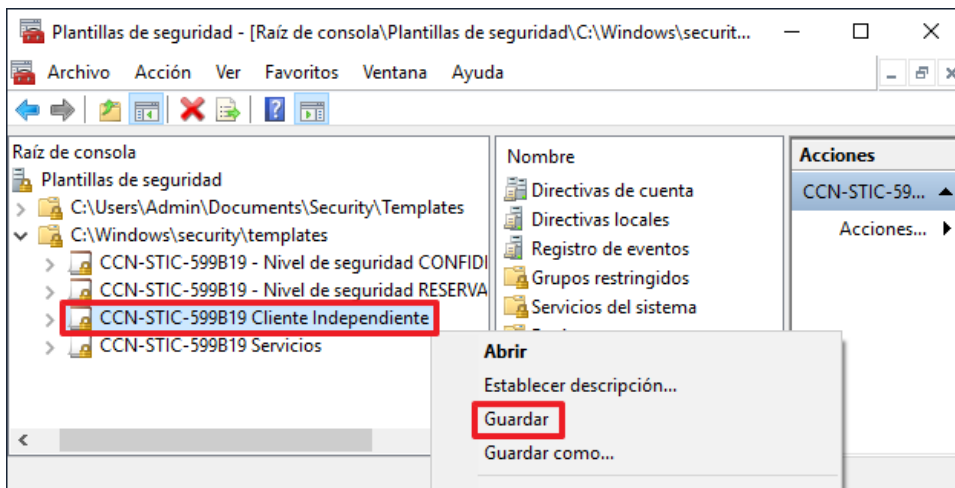
Paso	Descripción
63.	Haga doble clic en el grupo "Usuarios de shells" para mostrar sus propiedades y añada al menos como miembro al usuario administrador que está utilizando para aplicar esta guía. Para ello, pulse sobre el botón "Agregar..." y en la ventana "Seleccionar usuarios" escriba el nombre del usuario a añadir y pulse "Aceptar".  Adicionalmente y del mismo modo descrito, añada al grupo "Usuarios de shells" los demás usuarios que deban pertenecer a él, de acuerdo a las necesidades de su entorno. Los miembros del grupo "Usuarios de shells", y sólo ellos, tendrán permiso para ejecutar las shells del sistema, cmd.exe, powershell.exe y Powershell_ISE.exe. Pulse "Aceptar", de nuevo, para cerrar las propiedades del grupo "Usuarios de shells". Nota: La pertenencia a este grupo da a los usuarios permiso de ejecución sobre los archivos ejecutables (.exe) de ambas shells del sistema. Sin embargo, el acceso a cmd.exe estará restringido además por una directiva de plantillas administrativas, con lo que no podrá ser ejecutado, aunque el usuario pertenezca al grupo "Usuario de shells" mientras la directiva esté activa.
64.	Del mismo modo que en el paso anterior, haga doble clic en el grupo "Auditores" para mostrar sus propiedades y añada los usuarios que deban pertenecer a él de acuerdo a las necesidades de su entorno. Los miembros del grupo Auditores tendrán asignado el derecho "Administrar registro de seguridad y auditoría", lo que les permitirá especificar opciones de auditoría de acceso a objetos como archivos, objetos de Active Directory o claves del registro. 

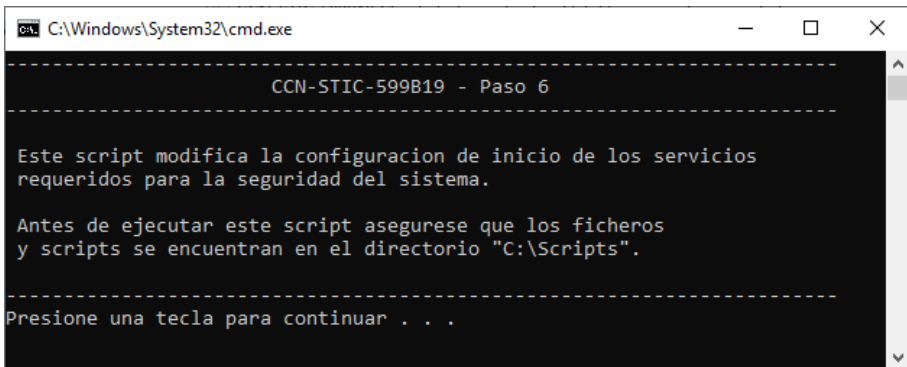
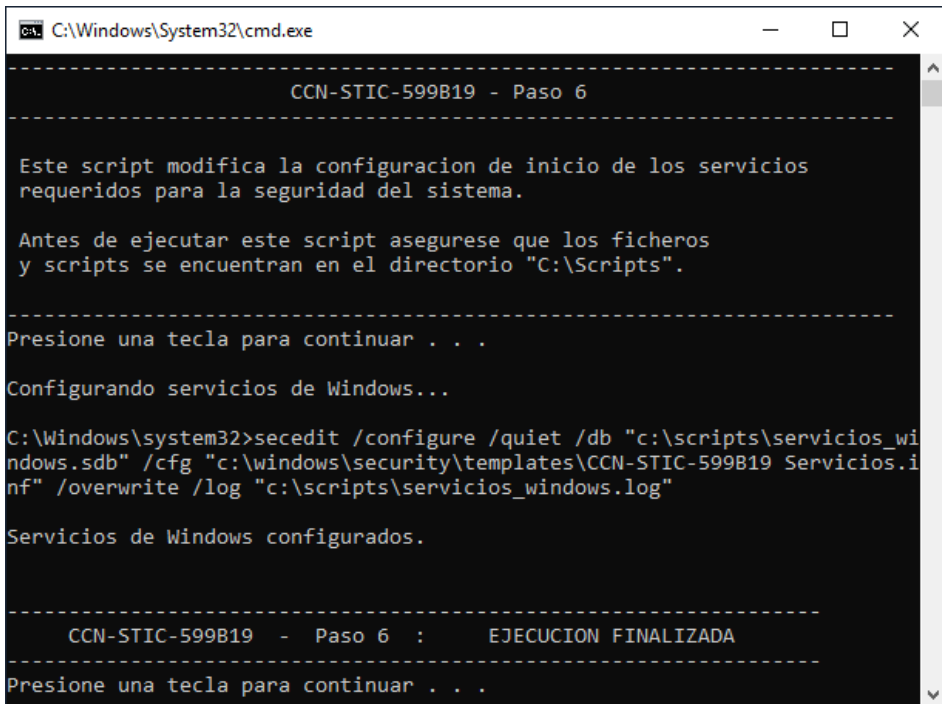
Paso	Descripción
65.	Utilizando el explorador de Windows, compruebe que el fichero "CCN-STIC-599B19 Cliente Independiente.inf" se encuentra en el directorio "C:\Windows\Security\Templates". Si no se encontrase allí, cópielo del directorio "C:\Scripts". Nota: Si el directorio principal de Windows no se encuentra en "C:\Windows", sustituya "C:\Windows" por la ubicación correspondiente.
66.	Edite la plantilla de seguridad "CCN-STIC-599B19 Cliente Independiente.inf" para incluir, en las reglas de asignación de derechos de usuario, los usuarios locales concretos del equipo que está asegurando. Para editar la plantilla ejecute con permisos de administrador (opción "Ejecutar como administrador" del menú contextual al marcarla con el botón derecho del ratón) la consola de administración "Plantillas de seguridad.msc" incluida en el directorio "C:\Scripts". 
67.	Pulse "Sí" cuando el control de cuentas de usuario le solicite elevación de privilegios. 

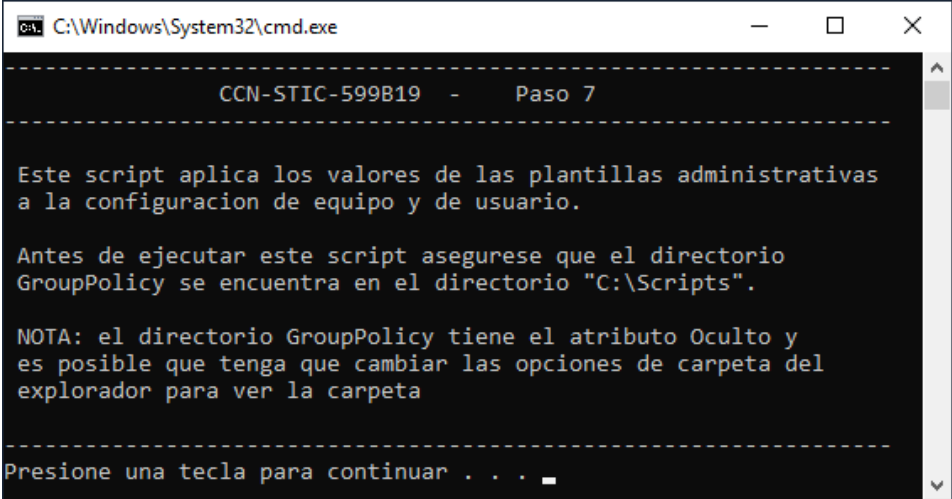
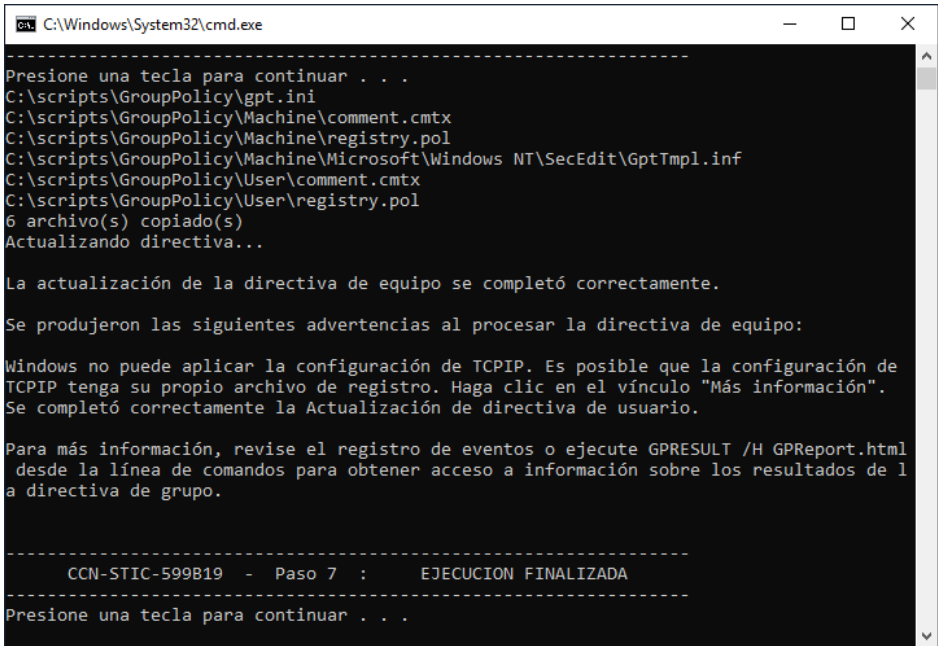
Paso	Descripción
68.	Para que el editor muestre las plantillas situadas en "C:\Windows\Security\Templates" será necesario marcar con el botón derecho el contenedor "Plantillas de seguridad", en la parte izquierda de la ventana, seleccionar la opción "Nueva ruta de acceso de búsqueda de plantillas..." en el menú contextual que aparecerá, y seleccionar entonces la ruta "Equipo\C:\Windows\Security\Templates". 
69.	Expanda entonces la plantilla "CCN-STIC-599B19 Cliente Independiente.inf" y, dentro de ella, seleccione el siguiente contenedor: "Directivas locales → Asignación de derechos de usuarios"  Haciendo doble clic en cada uno de los derechos de usuario correspondientes, deberá editar los derechos de usuario que se muestran a continuación. Estos derechos de usuario tendrán asignados algunos valores, pero deberán editarse para incluir los valores concretos de cuentas de usuarios locales del equipo. Para la edición de los derechos de usuario pulse sobre "Agregar Usuario o grupo..." y añada el usuario o grupo marcado en gris en la tabla que se muestra a continuación mediante el botón "Examinar..." y escribiendo el nombre del objeto correspondiente. Por último, pulse "Aceptar".

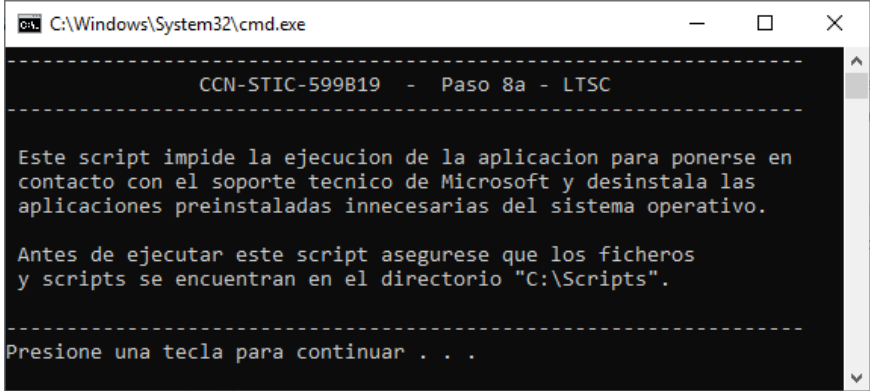
Paso	Descripción		
	Directiva	Valor	Descripción
	Administrar registro de seguridad y auditoría	Auditores, Administradores	Este privilegio permite que un usuario especifique opciones de auditoría de acceso a objetos para recursos individuales como archivos, objetos de Active Directory y claves de registro.
	Denegar el acceso a este equipo desde la red	Invitados, ANONYMOUS LOGON, Administrador	Este permiso determina a qué usuarios se les impide acceder a un ordenador desde la red
	Nota: Si no aparece el grupo Auditores en la lista disponible en el cuadro de diálogo "Seleccionar Usuarios o grupos", marque el botón "Tipos de objeto" y asegúrese de que la entidad "Grupos" está seleccionada, como se muestra en la siguiente figura. 		
70.	Continúe editando la plantilla de seguridad "CCN-STIC-599B19 Cliente Independiente.inf" para incluir, en esta ocasión en la sección "Sistema de archivos", los usuarios locales del equipo. Concretamente se deberán editar los permisos mediante la opción "Modificar seguridad..." y, al pulsar sobre "Agregar...", la operativa será similar a "Agregar grupo o usuario" del paso anterior, tal y como se muestra a continuación. Los permisos de los ficheros tendrán asignados algunos valores, pero deberán editarse para incluir los valores concretos de cuentas de usuarios locales. La tabla muestra el estado definitivo en el que deberán quedar configurados estos permisos, para lo cual deberá añadir las entradas correspondientes de los usuarios o grupos se muestran con fondo gris.		

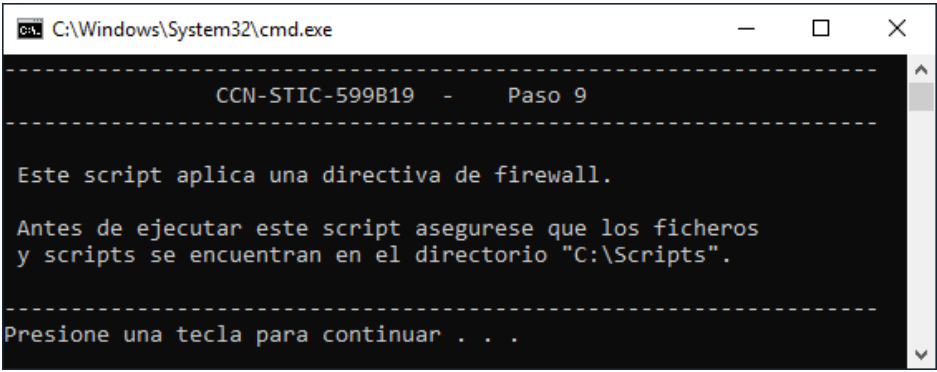
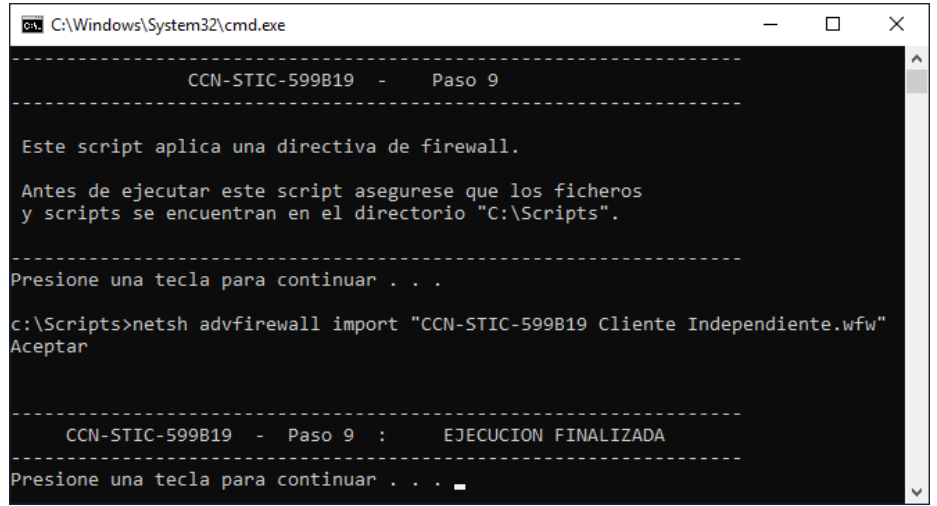
Paso	Descripción																		
	Una vez seleccionado el usuario o grupo recientemente añadido se podrán marcar los permisos correspondientes. Pulse “Aceptar” una vez añadidos todos los usuarios y/o grupos. Propiedades: %SystemRoot%\system32\cmd.exe Configuración de directiva de seguridad de plantillas  %SystemRoot%\system32\cmd.exe ☒ Configurar este archivo o carpeta ☒ Propagar permisos heredables a todas las subcarpetas y archivos ☐ Reemplazar los permisos existentes en archivos con permisos heredables ☐ No conceder permisos de reemplazo en este archivo o carpeta Modificar seguridad... Aceptar Seguridad para %SystemRoot%\system32\cmd.exe Seguridad Nombres de grupos o usuarios:  SYSTEM  Administradores (W10CL01\Administradores) Agregar... Quitar Permisos <table><thead><tr><th></th><th>Permitir</th><th>Denegar</th></tr></thead><tbody><tr><td>Control total</td><td>☐</td><td>☐</td></tr><tr><td>Modificar</td><td>☐</td><td>☐</td></tr><tr><td>Leer y ejecutar</td><td>☐</td><td>☐</td></tr><tr><td>Listar el contenido de la carpeta</td><td>☐</td><td>☐</td></tr><tr><td>Leer</td><td>☐</td><td>☐</td></tr></tbody></table> Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Aceptar Cancelar Aplicar		Permitir	Denegar	Control total	☐	☐	Modificar	☐	☐	Leer y ejecutar	☐	☐	Listar el contenido de la carpeta	☐	☐	Leer	☐	☐
	Permitir	Denegar																	
Control total	☐	☐																	
Modificar	☐	☐																	
Leer y ejecutar	☐	☐																	
Listar el contenido de la carpeta	☐	☐																	
Leer	☐	☐																	
Archivo o carpeta	Usuarios/Grupos	Permisos																	
%SystemRoot%\system32\cmd.exe	Administradores	Control Total																	
	SYSTEM	Control Total																	
	Usuarios de shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																	
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe	Administradores	Control Total																	
	SYSTEM	Control Total																	
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																	
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ISE.exe	Administradores	Control Total																	
	SYSTEM	Control Total																	
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																	
%SystemRoot%\SysWOW64\cmd.exe	Administradores	Control Total																	
	SYSTEM	Control Total																	
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																	

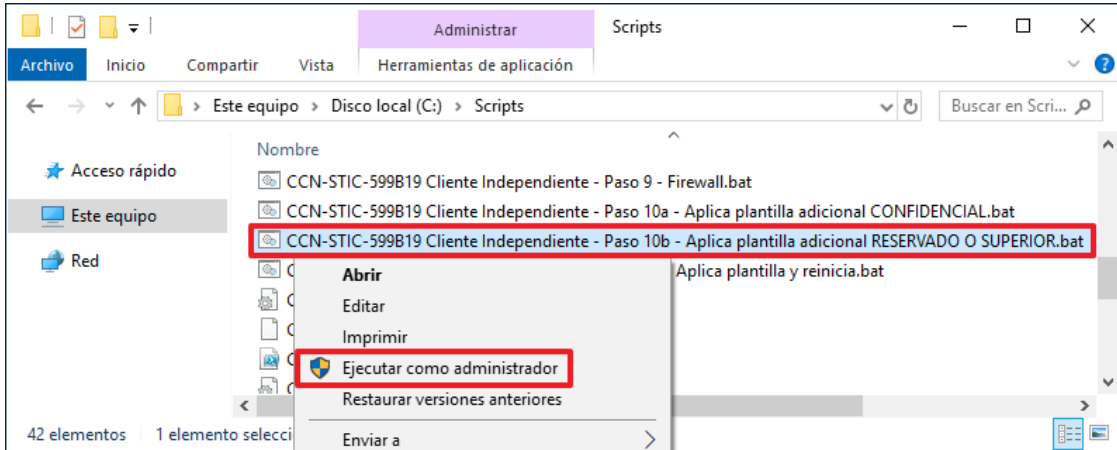
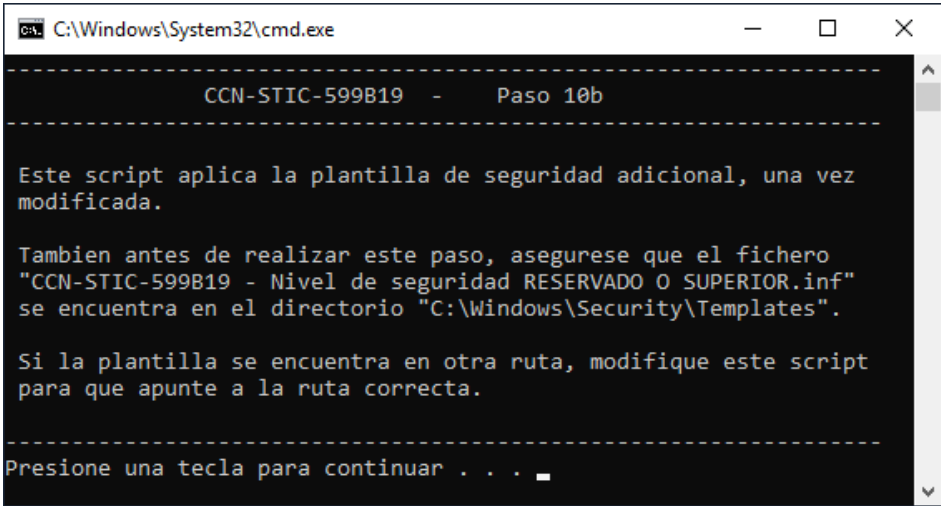
Paso	Descripción		
	Archivo o carpeta	Usuarios/Grupos	Permisos
	%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Administradores	Control Total
		SYSTEM	Control Total
		Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer
	%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell_ISE.exe	Administradores	Control Total
		SYSTEM	Control Total
		Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer
	Sin cerrar el editor de plantillas de seguridad, continúe con el siguiente paso.		
71.	Guarde la plantilla ("C:\Windows\Security\Templates\CCN-STIC-599B19 Cliente Independiente.inf") con las modificaciones realizadas. Para ello utilice la opción "Guardar" del menú contextual que aparece al marcar con el botón derecho del ratón el nombre de la plantilla, como se muestra en la figura.  Una vez salvados los cambios, cierre la consola de edición de plantillas. A la pregunta que aparecerá al cerrarla, "¿Guardar la configuración de la consola en Plantillas de seguridad.msc?", es indiferente que responda Sí o No. La plantilla en este punto habrá quedado lista para ser aplicada, cosa que hará en pasos posteriores.		

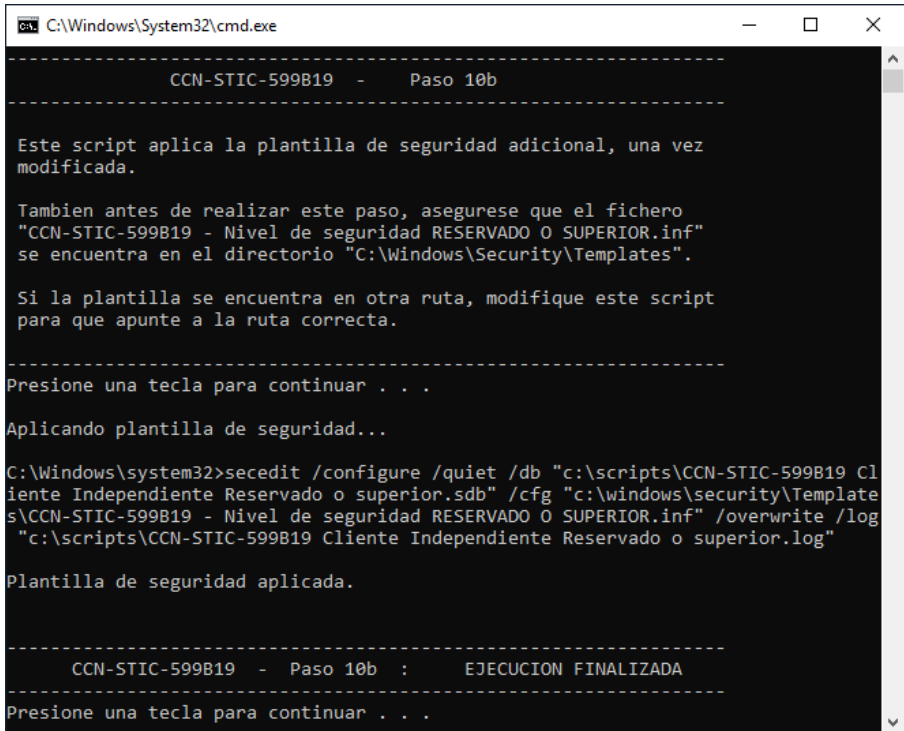
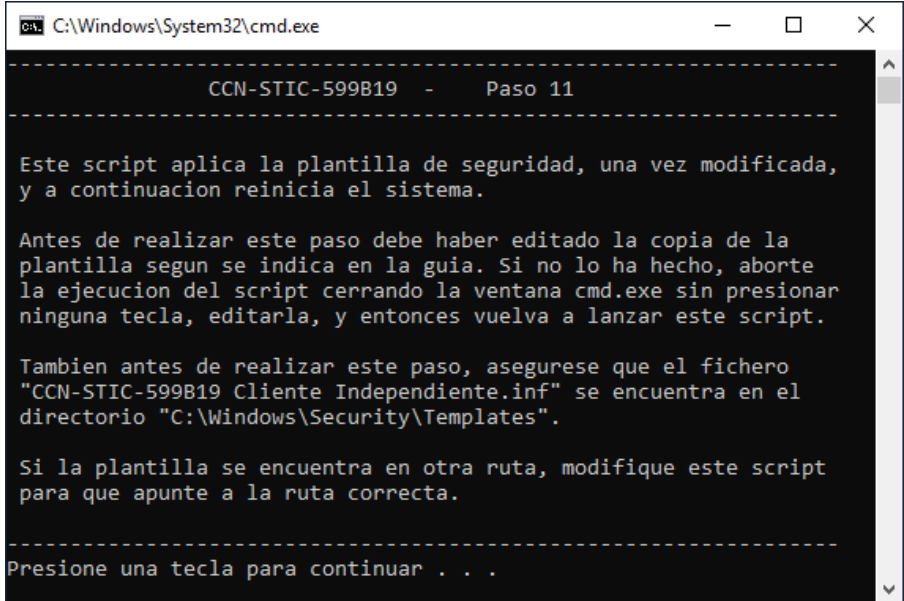
Paso	Descripción
72.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 6 – Servicios.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 
73.	Pulse una tecla de nuevo para cerrar la ventana de comandos.  Nota: Puede comprobar en la carpeta "C:\Scripts" que el proceso se ha realizado correctamente en el fichero de log denominado "servicios_windows.log".

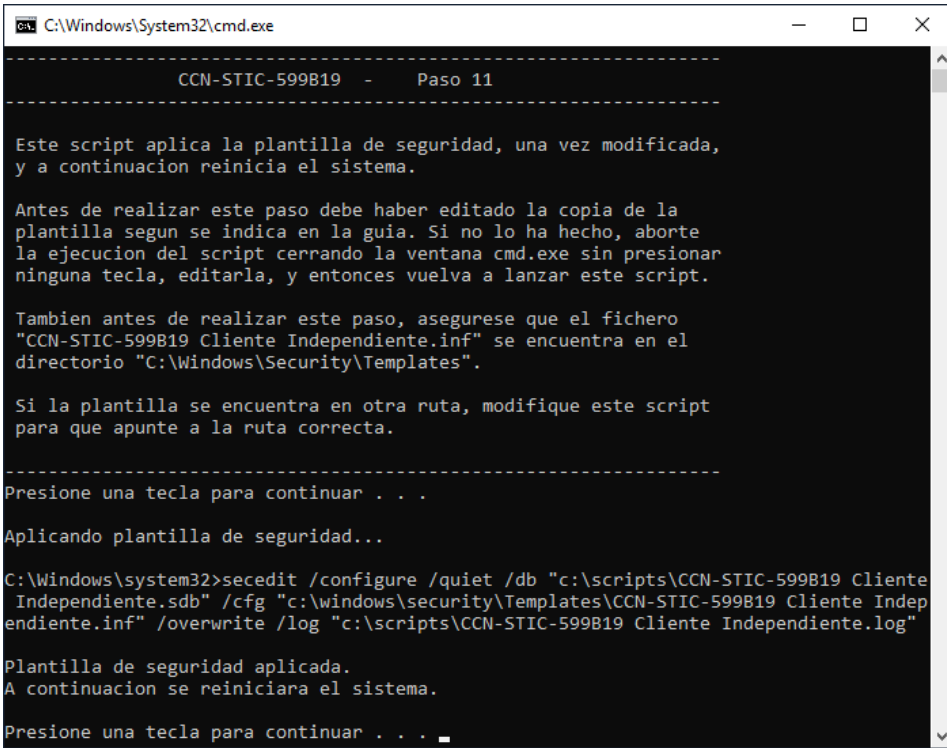
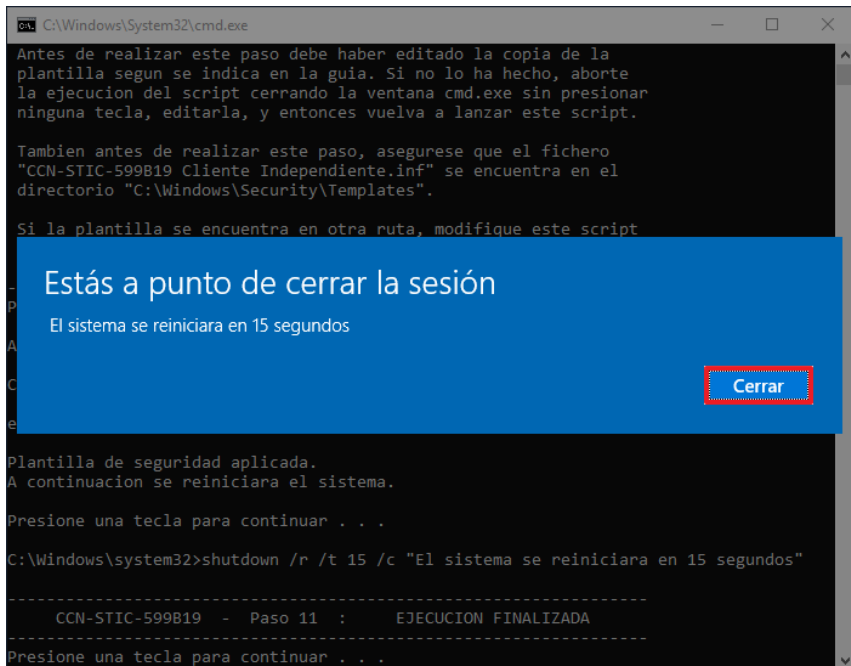
Paso	Descripción
74.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script " CCN-STIC-599B19 Cliente Independiente - Paso 7 – GPO.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script aplica los valores de las plantillas administrativas a la configuración de equipo y usuario, reemplazando la GPO local. 
75.	Pulse una tecla de nuevo para cerrar la ventana de comandos. 

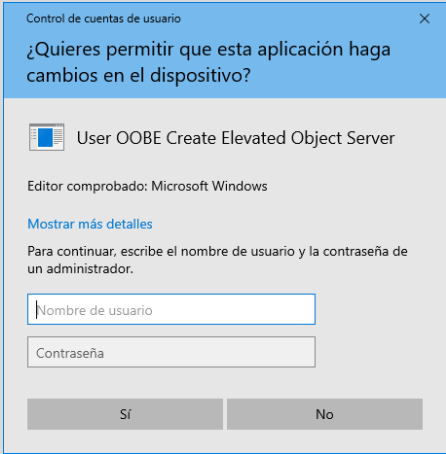
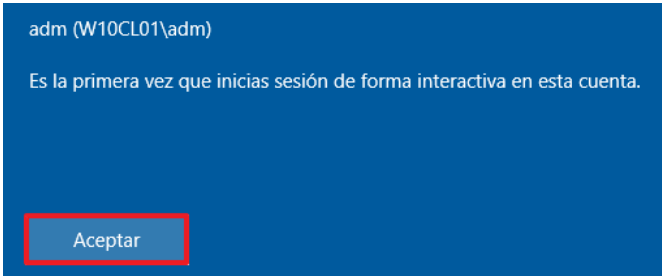
Paso	Descripción
76.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 8a – Deshabilita appx - LTSC.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilitará las AppX innecesarias y configurará la telemetría. 
77.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 

Paso	Descripción
78.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 9 – Firewall.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script aplicará la configuración del Firewall de Windows con Seguridad Avanzada. 
79.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 

Paso	Descripción
80.	Al igual que anteriormente, ejecute con permisos de administrador, opción “Ejecutar como administrador” el script denominado “CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat”.  Nota: Esta guía ha sido generada en función de la máxima seguridad. Debido a ello se realiza la ejecución de dicho script ya que aplica la máxima seguridad en el equipo. Si desea modificar esta configuración de máxima seguridad consulte el “ANEXO B.2 APLICACIÓN DE NIVELES DE CLASIFICACIÓN”. Consulte además la guía “CCN-STIC-301 Requisitos STIC” para más información.
81.	El control de cuentas le solicitará la elevación de privilegios. Pulse “Sí” para continuar.
82.	Pulse cualquier tecla para comenzar la ejecución del script. 

Paso	Descripción
83.	Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
84.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 11 – Aplica plantilla y reinicia.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Este script aplicará la configuración de seguridad, asegúrese de que el fichero "CCN-STIC-599B19 Cliente Independiente.inf" se encuentra en el contenedor correspondiente (C:\Windows\Security\Templates).

Paso	Descripción
85.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos.  Nota: Si lo desea, puede comprobar la correcta aplicación de este paso a través del fichero de log denominado “CCN-STIC-599B19 Cliente Independiente.log” que se encuentra en el directorio “C:\Scripts”. Es posible que aparezca una nota de advertencia que indica que ésta puede ser ignorada. Aunque aparezca dicha nota, la política ha sido aplicada correctamente.
86.	El equipo reiniciará con la configuración aplicada. 

Paso	Descripción
87.	Una vez reiniciado el sistema y habiendo aplicado la seguridad, pulse “Ctrl+Alt+Supr” para continuar con inicio de sesión. Al iniciar sesión aparecerá la leyenda “ES UN DELITO CONTINUAR SIN LA DEBIDA AUTORIZACIÓN. El sistema está restringido a los usuarios autorizados”. Pulse “Aceptar” para continuar y, en este momento podrá introducir las credenciales de inicio de sesión.  Nota: A la hora de crear nuevos usuarios, en el primer inicio de sesión, es posible que el sistema le solicite las credenciales de un usuario administrador para finalizar la configuración inicial. 
88.	Debido a que se trata del primer inicio de sesión tras la aplicación de seguridad en el sistema mostrara el siguiente mensaje, pulse “Aceptar” para continuar con el inicio de sesión.  Nota: En el mensaje de inicio de sesión aparecerá con el nombre de usuario que haya definido previamente.
89.	Elimine la carpeta “C: \Scripts”.

ANEXO B.1.2. LISTA DE COMPROBACIÓN PASO A PASO

Este apartado se ha diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad de la presente guía.

Se parte de la suposición de que en el equipo que se va a comprobar se ha instalado el sistema operativo Windows 10 Enterprise LTSC (versión 1809), que el equipo es un cliente independiente de un dominio y que en el equipo se ha aplicado la configuración expuesta en la presente guía.

La lista de comprobación deberá ejecutarse iniciando sesión en el equipo con un usuario con permisos de administrador local (miembro del grupo "Administradores"). La cuenta integrada de administrador no podrá usarse porque estará deshabilitada (ver directiva "Cuentas: estado de la cuenta de administrador" en las opciones de seguridad de la plantilla de seguridad).

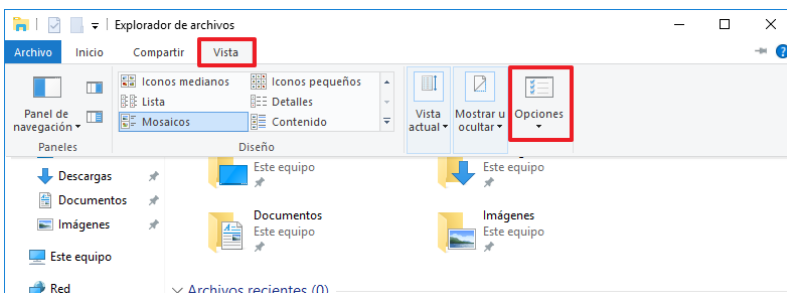
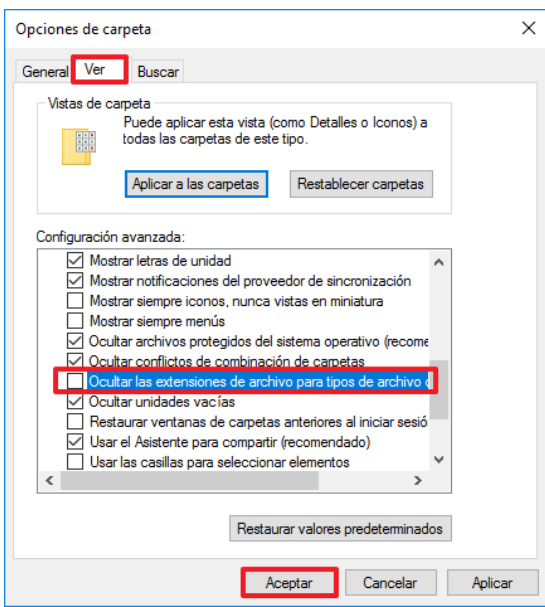
Para realizar algunas de las comprobaciones necesitará ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán son las siguientes:

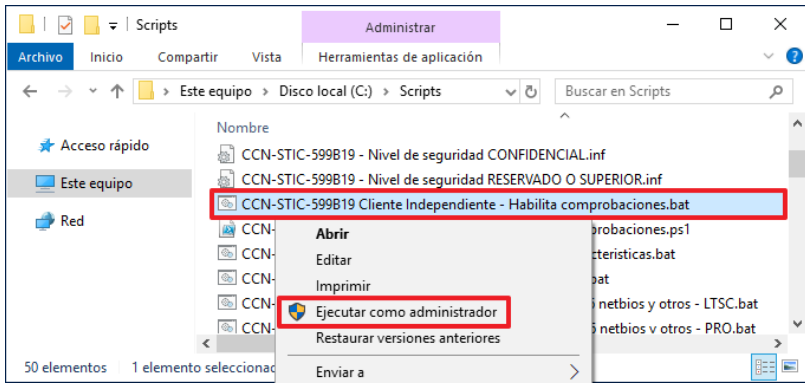
- a) Explorador de Windows (explorer.exe).
- b) Powershell (powershell.exe)
- c) Editor de objetos directiva de grupo (gpedit.msc).
- d) Varias consolas de administración accesibles desde el panel de control (control.exe)
- e) Consola de administración de Microsoft (mmc.exe)
- f) Editor del registro (regedit.exe)

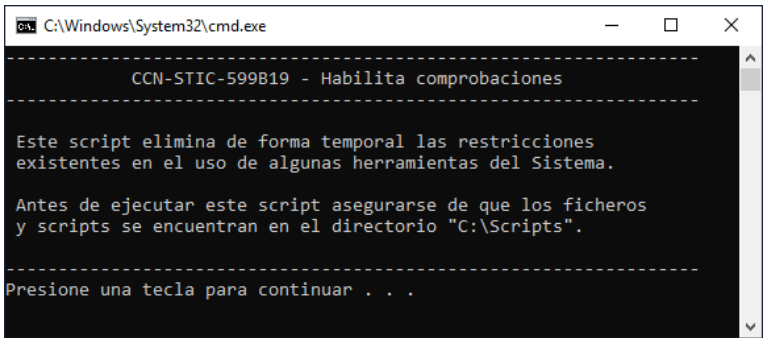
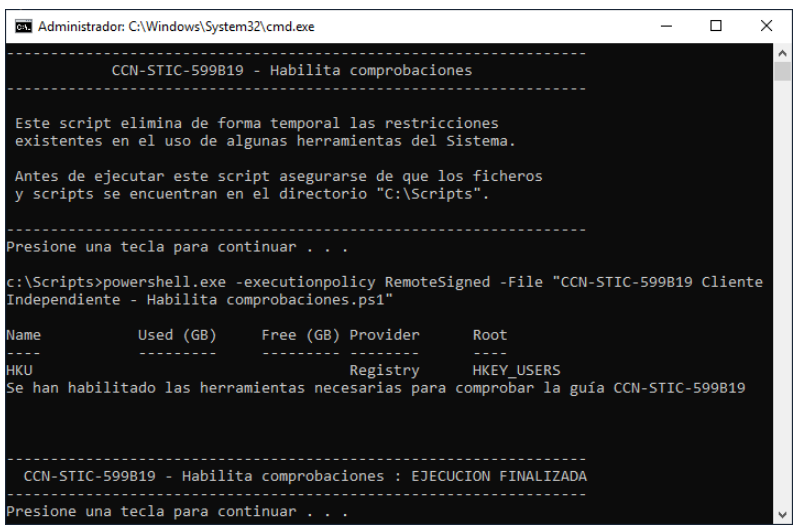
Siguiendo las recomendaciones de seguridad de esta guía, algunas de estas herramientas y consolas de administración estarán inicialmente deshabilitadas en el equipo cliente independiente. Para poder implementar la lista de comprobación será necesario habilitarlas temporalmente. Para ello se suministra junto con esta guía el script "CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat", que deberá ejecutar en uno de los primeros pasos a seguir en la implementación de esta lista de comprobación, tal y como se indica a continuación.

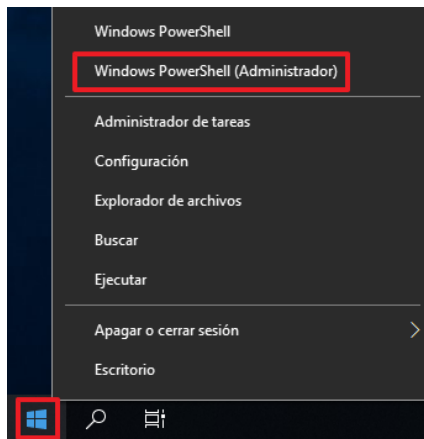
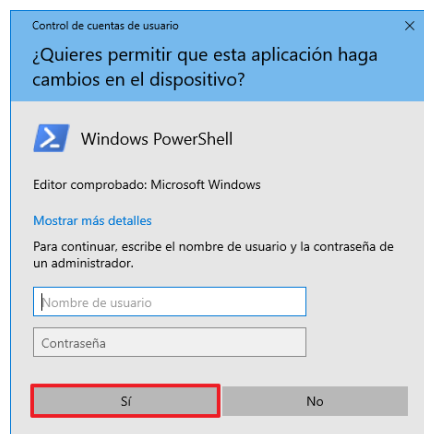
Nota: Tenga en consideración que durante la aplicación de la presente guía se está incluyendo la implementación de seguridad sobre Internet Explorer 11 por lo que será necesario además de verificar las comprobaciones que se indican en este anexo, verificar las comprobaciones de la guía "CCN-STIC-520 Internet Explorer 11".

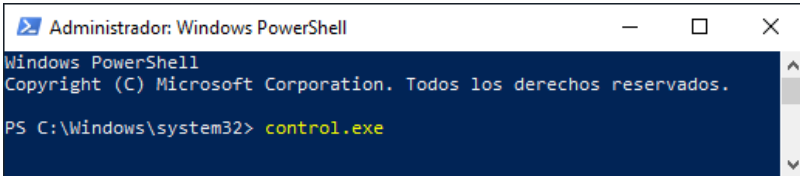
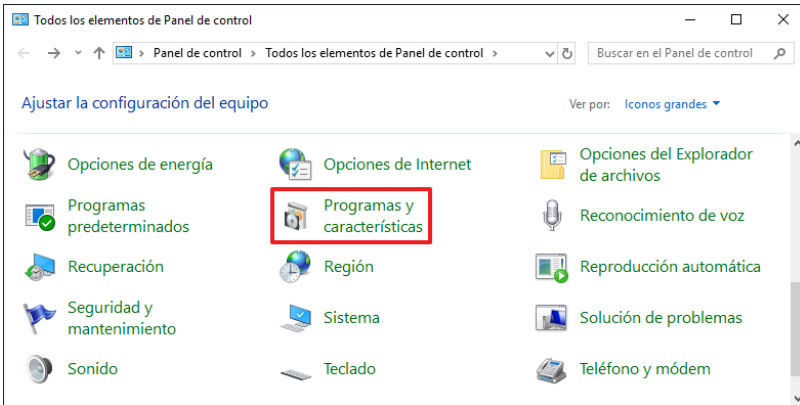
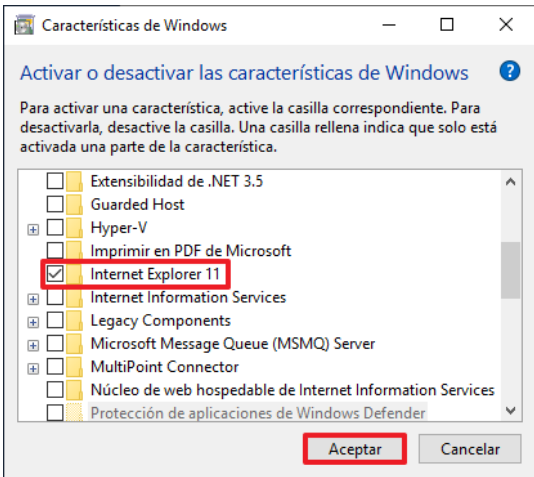
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión con privilegios de administración		Inicie sesión en el equipo que está comprobando con una cuenta de usuario que pertenezca al grupo local "Administradores" y al grupo local "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.

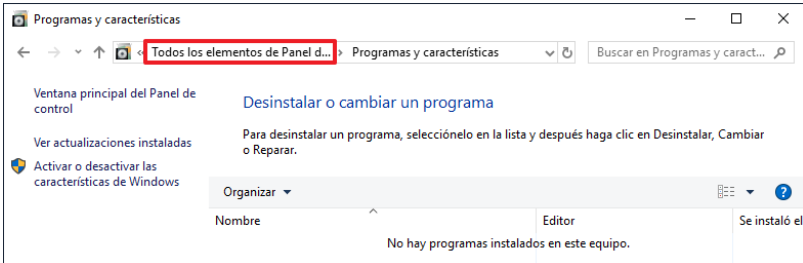
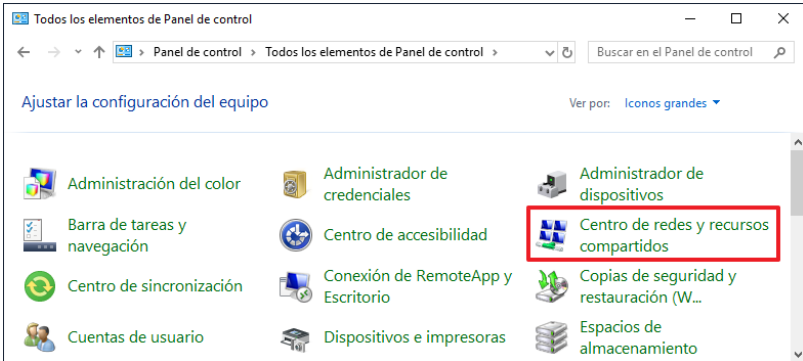
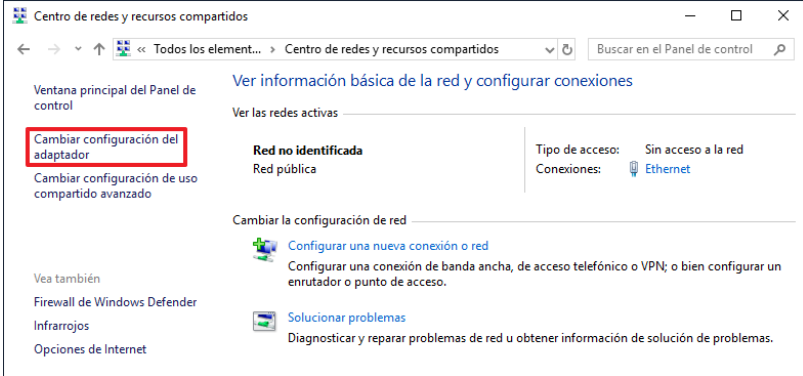
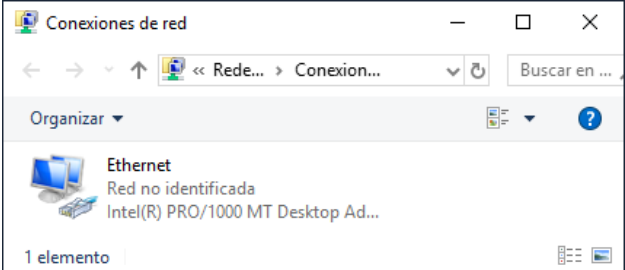
Comprobación	OK/NOK	Cómo hacerlo
2. Configure el Explorador de Windows para que muestre las extensiones de los archivos.		Por defecto Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” sí muestra las extensiones de los archivos. Para configurar “Explorador de Windows” de modo que muestre las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, por ejemplo, desde la siguiente ruta: "Inicio → Explorador de Windows" En el menú superior pulse sobre “Vista” y seleccione “Opciones”.  De la ventana que aparecerá denominada “Opciones de carpeta”, seleccione la pestaña “Ver” y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos” y pulse sobre “Aplicar a las carpetas”, como se muestra en la siguiente figura.  Responda pulsando “Sí” a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse “Aceptar” para cerrar la ventana “Opciones de carpeta”.

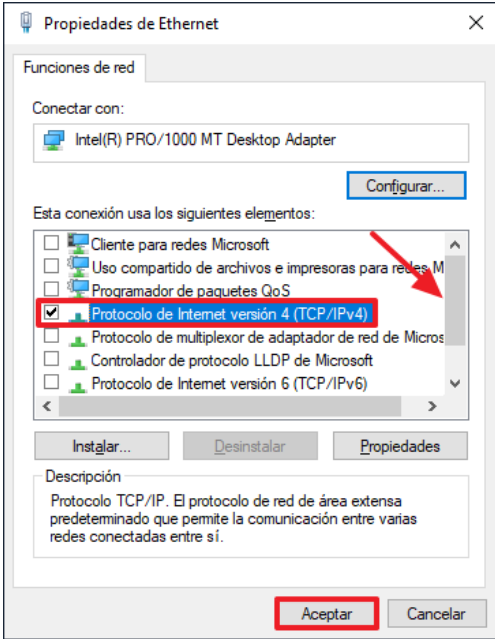
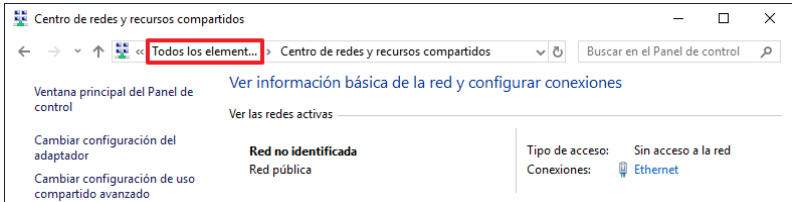
Comprobación	OK/NOK	Cómo hacerlo
3. Cree el directorio "C:\Scripts" y copie en él al menos los ficheros que se indican.		Cree el directorio "scripts" en la unidad "C:" ("C:\Scripts") en el sistema y copie en él al menos los siguientes dos scripts, los cuales están incluidos entre los ficheros que acompañan a esta guía: - CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.bat - CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.ps1 Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19".
4. Ejecute el script que habilita temporalmente las consolas de administración restringidas.		Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual, como se muestra en la siguiente figura. Nota: Aunque la sesión se haya iniciado con un usuario con permisos de administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.  Aparecerá la solicitud de credenciales el escritorio seguro, en el cual deberá introducir las credenciales de un usuario con permisos de administrador y pulse "Sí".

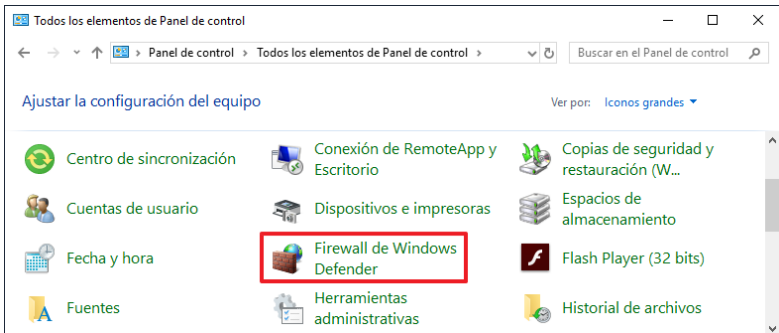
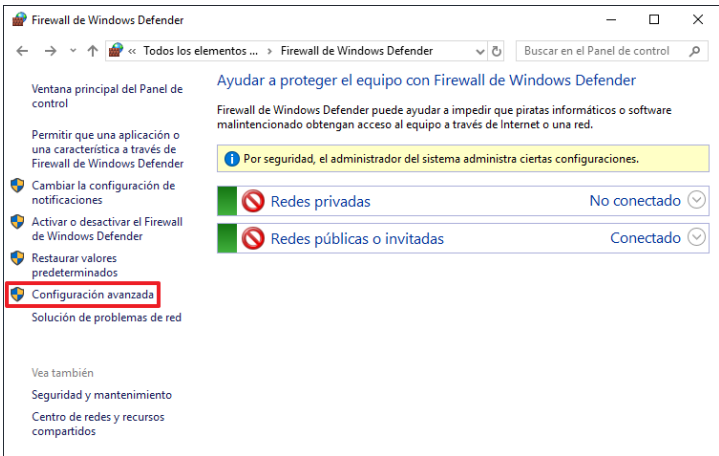
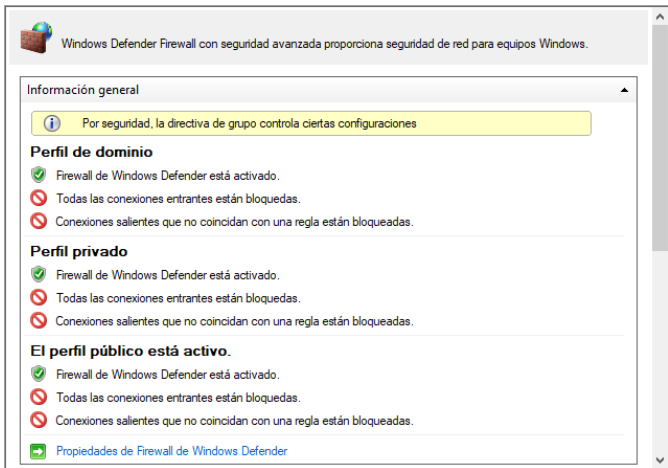
Comprobación	OK/NOK	Cómo hacerlo
5. Habilite temporalmente las consolas de administración restringidas.		Aparecerá una consola de comandos con la ejecución del script. Pulse una tecla para continuar:  Cuando termine la ejecución, pulse una tecla para cerrar la ventana de comandos:  Nota: La próxima vez que se reinicie el sistema o se vuelva a aplicar el objeto de directiva de grupo local las consolas y herramientas volverán a estar deshabilitadas. En caso de que aparezca algún mensaje de error puede ignorarlo y continuar con la comprobación. En caso de que, durante las comprobaciones que se realizarán en el presente anexo, no se pueda realizar alguno de los pasos, esto es debido a que el equipo cliente Windows 10 ha refrescado las políticas locales y, por tanto, se han deshabilitado las comprobaciones. Ante tal eventualidad deberá volver a ejecutar el script “CCN-STIC-599B19 Cliente Independiente- Habilita comprobaciones.bat” del mismo modo en que se describe en los pasos 4 y 5 del presente anexo.

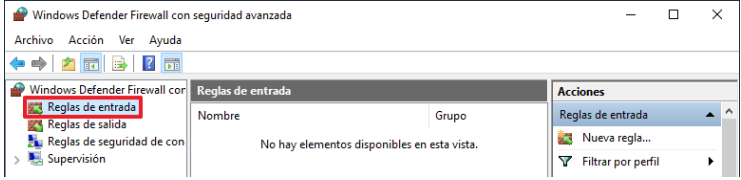
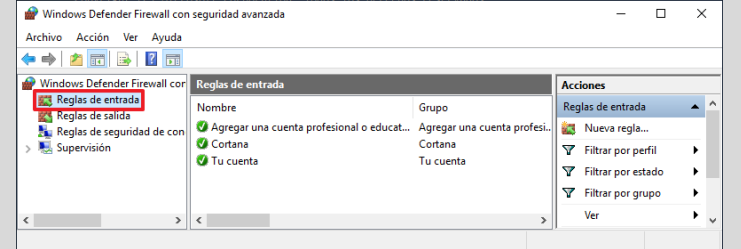
Comprobación	OK/NOK	Cómo hacerlo
6. Lance una ventana de Powershell con permisos de administrador, para lanzar desde ella en pasos posteriores comandos con permisos de administrador.		Haga clic con el botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”.  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.  Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.

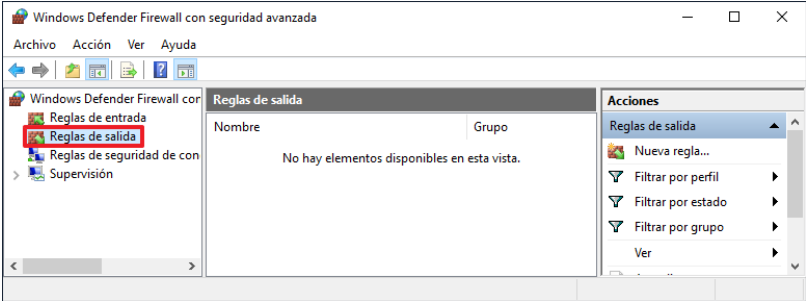
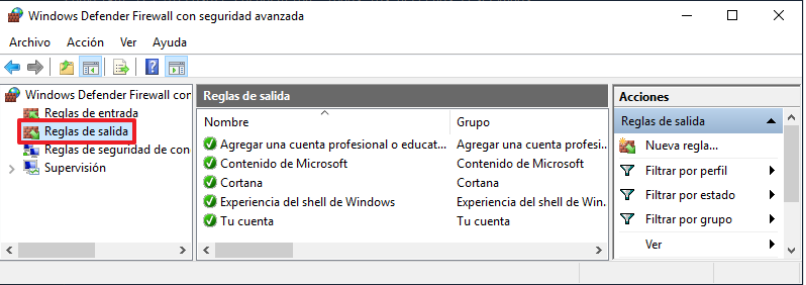
Comprobación	OK/NOK	Cómo hacerlo
7. Compruebe que no hay características opcionales de Windows habilitadas (a excepción de Internet Explorer 11 que deberá estar instalada).		Desde la ventana de Powershell con privilegios de administrador, teclee "control.exe" y pulse "Enter" para abrir el "Panel de Control":  Seleccione la opción "Programas y características":  Dentro de la ventana que aparecerá, seleccione la opción "Activar o desactivar las características de Windows". En la ventana de control de cuentas de usuario, introduzca de nuevo las credenciales de un usuario con permisos de administrador, para acceder a la ventana de Características de Windows:  Compruebe que ninguna característica, excepto Internet Explorer 11, tiene marcada la casilla de selección, lo cual indicaría que dicha característica estaría activa. Todas las características deben estar desactivadas. Una vez comprobado, pulse "Aceptar" para cerrar la ventana.

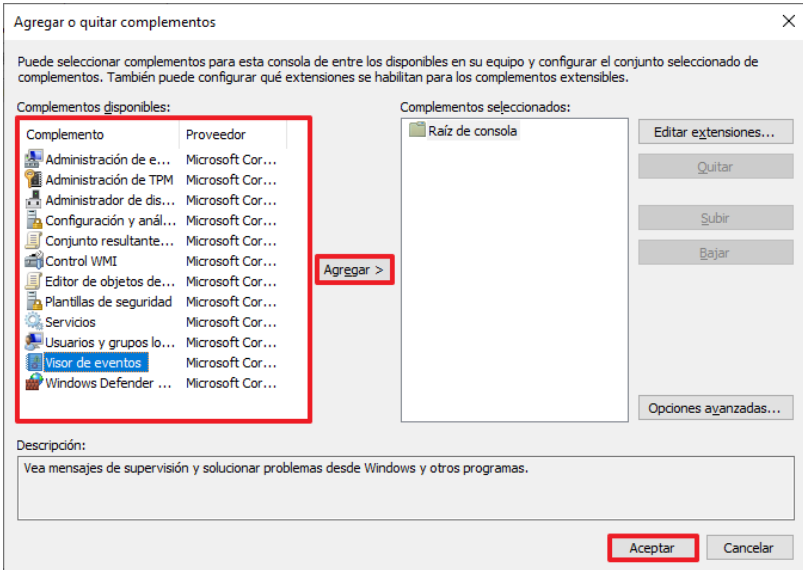
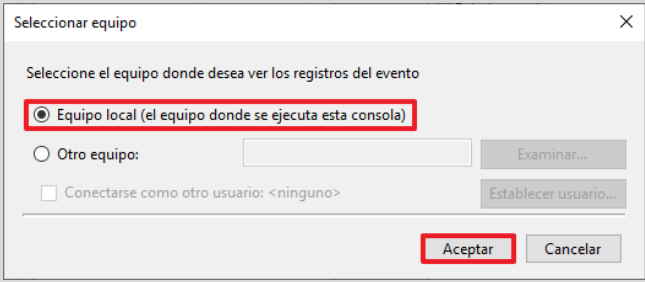
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique los protocolos enlazados a las tarjetas de red.		Vuelva a la pantalla principal del panel de control. Para ello, marque "Todos los elementos de Panel de control" en la barra de navegación superior de la ventana.  Seleccione ahora "Centro de redes y recursos compartidos":  Seleccione "Cambiar configuración del adaptador":  Aparecerá en la ventana del panel de control la lista de tarjetas de red del sistema:  Nota: Deberá realizar esta comprobación únicamente si dispone de tarjetas de red.

Comprobación	OK/NOK	Cómo hacerlo
		Para cada tarjeta de red, marque con el botón derecho del ratón el icono de la tarjeta y seleccione la opción "Propiedades" del menú contextual que aparecerá. Tras introducir las credenciales de un usuario con permisos de administrador de nuevo, aparecerá la ventana de propiedades del adaptador:  Compruebe que el único elemento seleccionado sea "Protocolo de Internet versión 4 (TCP/IPv4)", como se muestra en la figura anterior. Pulse el botón "Cancelar" para cerrar la ventana de propiedades de la interfaz de red. Nota: Recuerde repetir la comprobación para todas las tarjetas de red del equipo.
9. Verifique la aplicación de seguridad del Firewall de Windows con Seguridad Avanzada.		Vuelva a la pantalla principal del panel de control. Para ello, marque "Todos los elementos de Panel de control" en la barra de navegación superior de la ventana. 

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione “Firewall de Windows” en el “Panel de Control”.  Seleccione “Configuración avanzada”:  Introduzca las credenciales de un usuario con permisos de administrador en el “Control de Cuentas de Usuario” y, a continuación, aparecerá una ventana con la configuración del firewall de Windows con seguridad avanzada:  Compruebe que los valores coinciden con la tabla siguiente.

Comprobación	OK/NOK	Cómo hacerlo
	Parámetro	
	OK/NOK	
	Por seguridad, la directiva de grupo controla ciertas configuraciones	
	Perfil de dominio	Firewall de Windows está activado.
		Todas las conexiones entrantes están bloqueadas
		Conexiones salientes que no coincidan con una regla están bloqueadas
	Perfil privado	Firewall de Windows está activado.
		Todas las conexiones entrantes están bloqueadas
		Conexiones salientes que no coincidan con una regla están bloqueadas
	Perfil público	Firewall de Windows está activado.
		Todas las conexiones entrantes están bloqueadas
		Conexiones salientes que no coincidan con una regla están bloqueadas
10. Compruebe las reglas de entrada del firewall de Windows con seguridad avanzada.		En la ventana del Firewall de Windows con seguridad avanzada, seleccione el contenedor siguiente: “Firewall de Windows con seguridad avanzada → Reglas de entrada”  Compruebe que en la parte central de la ventana aparece el mensaje "No hay elementos disponibles en esta vista", como en el siguiente ejemplo. Esto significa que no hay ninguna regla de entrada configurada. Nota: Es posible que aparezcan reglas predeterminadas en el sistema. Esto es debido a que la ejecución del script “CCN-STIC-599B19 Cliente Independiente - Paso 9 - Firewall.bat” se realizó con un usuario distinto al que se está revisando este paso. Si es así, vuelva a lanzar dicho script con privilegios de administrador para eliminar las reglas predeterminadas que aparecen. 

Comprobación	OK/NOK	Cómo hacerlo
11.Compruebe las reglas de salida del firewall de Windows con seguridad avanzada.		En la ventana del Firewall de Windows con seguridad avanzada, seleccione el contenedor siguiente: “Firewall de Windows con seguridad avanzada → Reglas de salida”  Compruebe que en la parte central de la ventana aparece el mensaje "No hay elementos disponibles en esta vista", como en el siguiente ejemplo. Esto significa que no hay ninguna regla de entrada configurada. Nota: Es posible que aparezcan reglas predeterminadas en el sistema. Esto es debido a que la ejecución del script “CCN-STIC-599B19 Cliente Independiente - Paso 9 - Firewall.bat” se realizó con un usuario distinto al que se está revisando este paso. Si es así, vuelva a lanzar dicho script con privilegios de administrador para eliminar las reglas predeterminadas que aparecen. 

Comprobación	OK/NOK	Cómo hacerlo
12. Ejecute la herramienta "Consola de administración de Microsoft (mmc.exe)" para poder realizar las comprobaciones de los siguientes pasos.		Desde la ventana de PowerShell abierta anteriormente, ejecute "mmc.exe". A continuación, seleccione "Archivo → Agregar o quitar complemento..." y utilice esta combinación para agregar los "Complementos disponibles:", y que son requeridos en los siguientes pasos utilizando el botón, "Agregar >" y pulsando "Aceptar" para agregar el complemento.  Nota: Tenga en consideración que algunos de los elementos agregados tendrán que ser referidos al equipo local. 
13. Agregue el complemento a la consola.		Agregue el "Visor de eventos" (Equipo local) desde la ventana "Complementos disponibles" tal y como se explica en el paso 12.
14. Verifique la configuración del registro de eventos de Aplicación.		Pulse el botón derecho del ratón sobre el contenedor "Aplicación", que se encuentra en la ruta siguiente: "Visor de eventos (local) → Registros de Windows → Aplicación" Seleccione la opción "Propiedades" del menú contextual que aparecerá a su derecha y compruebe que los valores configurados coinciden con los siguientes:

Comprobación	OK/NOK	Cómo hacerlo		
		Parámetro	Valor	OK/NOK
		Tamaño máximo del registro (KB)	32768	
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)	
15.Verifique la configuración del registro de eventos de Seguridad.		Pulse el botón derecho del ratón sobre el contenedor "Seguridad", que se encuentra en la ruta siguiente: "Visor de eventos (local) → Registros de Windows → Seguridad" Seleccione la opción "Propiedades" del menú contextual que aparecerá y compruebe que los valores configurados coinciden con los siguientes:		
		Parámetro	Valor	OK/NOK
		Tamaño máximo del registro (KB)	163840	
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)	
16.Verifique la configuración del registro de eventos de Sistema.		Pulse el botón derecho del ratón sobre el contenedor "Sistema", que se encuentra en la ruta siguiente: "Visor de eventos (local) → Registros de Windows → Sistema" Seleccione la opción "Propiedades" del menú contextual que aparecerá y compruebe que los valores configurados coinciden con los siguientes:		
		Parámetro	Valor	OK/NOK
		Tamaño máximo del registro (KB)	32768	
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)	
17.Agregue el complemento a la consola.		Agregue la herramienta "Usuarios y grupos locales" (Equipo local) desde la ventana "Complementos disponibles" tal y como se explica en el paso 12.		
18.Verifique que los grupos "Usuarios avanzados" y "Usuarios de escritorio remoto" están vacíos.		Sitúese sobre el contenedor "Grupos", que se encuentra en la ruta siguiente: "Usuarios y grupos locales → Grupos" Compruebe que los siguientes grupos no tienen miembros, haciendo doble clic sobre ellos y observando la lista de miembros que aparecerá:		

Comprobación	OK/NOK	Cómo hacerlo																			
	Grupos		OK/NOK																		
	Usuarios avanzados																				
	Usuarios de escritorio remoto																				
19.Verifique que los grupos "Auditores" y "Usuarios de shells" están creados.		Sitúese sobre el contenedor “Grupos”, que se encuentra en la ruta siguiente: "Usuarios y grupos locales → Grupos" Compruebe que los siguientes grupos aparecen en la lista.																			
	Grupos		OK/NOK																		
	Auditores																				
	Usuarios de shells																				
20.Verifique el resto de los grupos.		Adicionalmente, haga doble clic en el resto de los grupos y compruebe que sus miembros corresponden con los usuarios adecuados para su entorno.																			
21.Verifique que se han renombrado los usuarios locales Administrador e Invitado.		Sitúese sobre el contenedor “Usuarios”, que se encuentra en la ruta siguiente: "Usuarios y grupos locales → Usuarios" Compruebe que aparecen los siguientes usuarios y que el icono lleva una flecha indicando que están deshabilitadas como en la siguiente figura.																			
	<table><tr><th>Nombre</th><th>Nombre com...</th><th>Descripción</th></tr><tr><td> aCdCmN599</td><td></td><td>Cuenta integrada para la administración del eq...</td></tr><tr><td> Admin</td><td></td><td></td></tr><tr><td> DefaultAccount</td><td></td><td>Cuenta de usuario administrada por el sistema.</td></tr><tr><td> IcNcVn599</td><td></td><td>Cuenta integrada para el acceso como invitado ...</td></tr><tr><td> WDAGUtilityAccount</td><td></td><td>Una cuenta de usuario que el sistema administr...</td></tr></table>			Nombre	Nombre com...	Descripción	 aCdCmN599		Cuenta integrada para la administración del eq...	 Admin			 DefaultAccount		Cuenta de usuario administrada por el sistema.	 IcNcVn599		Cuenta integrada para el acceso como invitado ...	 WDAGUtilityAccount		Una cuenta de usuario que el sistema administr...
	Nombre	Nombre com...	Descripción																		
	 aCdCmN599		Cuenta integrada para la administración del eq...																		
	 Admin																				
 DefaultAccount		Cuenta de usuario administrada por el sistema.																			
 IcNcVn599		Cuenta integrada para el acceso como invitado ...																			
 WDAGUtilityAccount		Una cuenta de usuario que el sistema administr...																			
Usuarios		OK/NOK																			
aCdCmN599																					
IcNcVn599																					

Comprobación	OK/NOK	Cómo hacerlo		
22.Verifique el tipo de inicio configurado para cada uno de los servicios del sistema.		Desde la ventana de PowerShell abierta anteriormente, ejecute "services.msc". A continuación, se abrirá la consola de “Servicios del sistema”. Compruebe que el tipo de inicio configurado para cada servicio coincide con el mostrado en la siguiente tabla: Nota: Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios, que no aparezca el servicio e incluso que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el equipo en el que esté realizando la comprobación, o el nombre corto, si no lo está. Lo importante es que el modo de inicio de los servicios que aparezcan tanto en la ventana de la consola de servicios como en esta tabla, coincida en ambos casos. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
ASP.NET State Service	aspnet_state	Deshabilitado	Configurado	
Acceso a datos de usuarios	UserDataSvc	Deshabilitado	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de escucha Net.Msmq	NetMsmqActivator	Deshabilitado	Configurado	
Adaptador de escucha Net.Pipe	NetPipeActivator	Deshabilitado	Configurado	
Adaptador de escucha Net.Tcp	NetTcpActivator	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administración de aplicaciones	AppMgmt	Deshabilitado	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Deshabilitado	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Deshabilitado	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Deshabilitado	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Deshabilitado	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Deshabilitado	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Deshabilitado	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de cuentas web	TokenBroker	Manual	Configurado		
Administrador de identidad de redes de mismo nivel	p2pimsvc	Deshabilitado	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMgrSvc	Deshabilitado	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Deshabilitado	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Deshabilitado	Configurado		
Agrupación de red del mismo nivel	p2psvc	Deshabilitado	Configurado		
Aislamiento de claves CNG	KeyIso	Deshabilitado	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Deshabilitado	Configurado		
Aplicación auxiliar IP	iphlpvc	Deshabilitado	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Deshabilitado	Configurado		
Archivos sin conexión	CscService	Deshabilitado	Configurado		
Asignador de detección de topologías de nivel de vínculo	ltdsvc	Deshabilitado	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
Audio de Windows	Audiosrv	Deshabilitado	Configurado		
Autenticación natural	NaturalAuthentication	Deshabilitado	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Deshabilitado	Configurado		
BranchCache	PeerDistSvc	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Deshabilitado	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CaptureService	CaptureService	Deshabilitado	Configurado		
Carpetas de trabajo	workfolderssvc	Deshabilitado	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Deshabilitado	Configurado		
Cliente para NFS	NfsClnt	Deshabilitado	Configurado		
Cliente web	WebClient	Deshabilitado	Configurado		
Cola de impresión	Spooler	Deshabilitado	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Deshabilitado	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexiones de red	Netman	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Configuración automática de WLAN	WlanSvc	Deshabilitado	Configurado		
Configuración automática de WWAN	WwanSvc	Deshabilitado	Configurado		
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Deshabilitado	Configurado		
ConsentUX	ConsentUxUserSvc	Deshabilitado	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Deshabilitado	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Coordinador de transacciones distribuidas	MSDTC	Deshabilitado	Configurado		
Copias de seguridad de Windows	SDRSVC	Deshabilitado	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Deshabilitado	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Deshabilitado	Configurado		
Detección SSDP	SSDPSRV	Deshabilitado	Configurado		
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado		
DevicePicker	DevicePickerUserSvc	Deshabilitado	Configurado		
DevicesFlow	DevicesFlowUserSvc	Deshabilitado	Configurado		
Diagnostic Execution Service	diagsvc	Deshabilitado	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Deshabilitado	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Deshabilitado	Configurado		
Energía	Power	Deshabilitado	Configurado		
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado		
Escucha de RIP	iprip	Deshabilitado	Configurado		
Estación de trabajo	LanmanWorkstation	Automático	Configurado		
Eventos de adquisición de imágenes estáticas	WiaRpc	Deshabilitado	Configurado		
Examinador de equipos	Browser	Deshabilitado	Configurado		
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado		
Extensiones y notificaciones de impresora	PrintNotify	Deshabilitado	Configurado		
Fax	Fax	Deshabilitado	Configurado		
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado		
Firewall de Windows	mpssvc	Automático	Configurado		
GraphicsPerfSvc	GraphicsPerfSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Hora de Windows	W32Time	Automático	Configurado	
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación	AppIDSvc	Deshabilitado	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)	AxInstSV	Deshabilitado	Configurado	
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado	
Instantáneas de volumen	VSS	Deshabilitado	Configurado	
Instrumental de administración de Windows	Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Deshabilitado	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Deshabilitado	Configurado	
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado	
LxssManager	LxssManager	Deshabilitado	Configurado	
Message Queue Server	MSMQ	Deshabilitado	Configurado	
MessagingService	MessagingService	Deshabilitado	Configurado	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado	
Microsoft Passport	NgcSvc	Deshabilitado	Configurado	
Modo incrustado	embeddedmode	Deshabilitado	Configurado	
Motor de filtrado de base	BFE	Automático	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado	
Net Logon	Netlogon	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Notificaciones del servicio de token de Windows	c2wts	Deshabilitado	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Automático	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Automático	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Deshabilitado	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Deshabilitado	Configurado		
Protección de software	spssvc	Automático	Configurado		
Protocolo de autenticación extensible	Eaphost	Deshabilitado	Configurado		
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Deshabilitado	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Deshabilitado	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Deshabilitado	Configurado		
Registrador de configuración de Windows Connect Now	wcnscvc	Deshabilitado	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Deshabilitado	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado		
Servicio AVCTP	BthAvctpSvc	Deshabilitado	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Deshabilitado	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Deshabilitado	Configurado		
Servicio FTP de Microsoft	ftpsvc	Deshabilitado	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Deshabilitado	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio LPD	LPDSVC	Deshabilitado	Configurado		
Servicio MultiPoint	Wms	Deshabilitado	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Deshabilitado	Configurado		
Servicio PushToInstall de Windows	PushToInstall	Deshabilitado	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Deshabilitado	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Deshabilitado	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio biométrico de Windows	WbioSrv	Deshabilitado	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Deshabilitado	Configurado		
Servicio de Windows Defender	WinDefend	Deshabilitado	Configurado		
Servicio de Windows Insider	wisvc	Deshabilitado	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado		
Servicio de administración IIS	IISADMIN	Deshabilitado	Configurado		
Servicio de administración de Windows	WManSvc	Deshabilitado	Configurado		
Servicio de administración de aplicaciones de empresa	EntAppSvc	Deshabilitado	Configurado		
Servicio de administración de radio	RmSvc	Deshabilitado	Configurado		
Servicio de administración de web	WMSVC	Deshabilitado	Configurado		
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Deshabilitado	Configurado		
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado		
Servicio de almacenamiento	StorSvc	Manual	Configurado		
Servicio de asistente para perfil local	wlpasvc	Deshabilitado	Configurado		
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado		
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de cierre de invitado de Hyper-V	vmicshuttdown	Deshabilitado	Configurado		
Servicio de cliente de protección de host	HgClientService	Deshabilitado	Configurado		
Servicio de compatibilidad con Bluetooth	bthserv	Deshabilitado	Configurado		
Servicio de configuración de red	NetSetupSvc	Manual	Configurado		
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Deshabilitado	Configurado		
Servicio de datos del sensor	SensorDataService	Deshabilitado	Configurado		
Servicio de datos espacial	SharedRealitySvc	Deshabilitado	Configurado		
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Deshabilitado	Configurado		
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado		
Servicio de dispositivo de interfaz humana	hidserv	Deshabilitado	Configurado		
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado		
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Deshabilitado	Configurado		
Servicio de experiencia de idioma	LxpSvc	Deshabilitado	Configurado		
Servicio de geolocalización	lfsvc	Deshabilitado	Configurado		
Servicio de historial de archivos	fhsvc	Deshabilitado	Configurado		
Servicio de host HV (Hyper-V)	HvHost	Deshabilitado	Configurado		

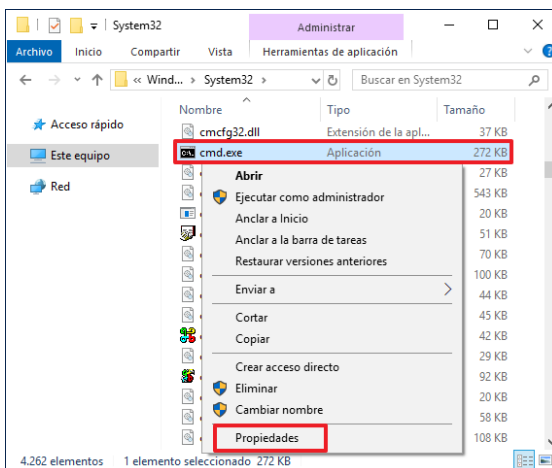
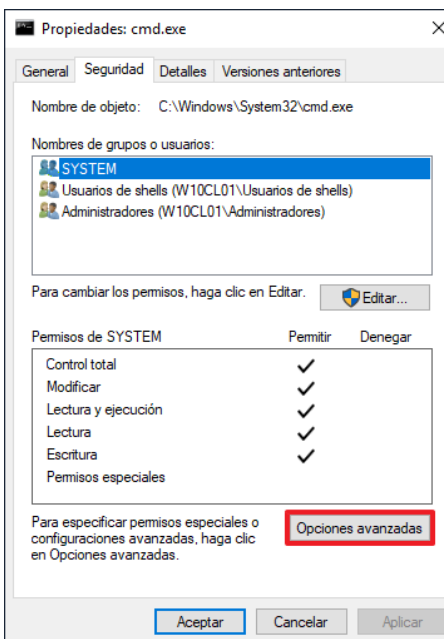
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado	
Servicio de instalación de Microsoft Store	InstallService	Deshabilitado	Configurado	
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Deshabilitado	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Deshabilitado	Configurado	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado	
Servicio de lista de redes	netprofm	Manual	Configurado	
Servicio de mejora de visualización	DisplayEnhancementService	Deshabilitado	Configurado	
Servicio de monitor de infrarrojos	irmon	Deshabilitado	Configurado	
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado	
Servicio de percepción de Windows	spectrum	Deshabilitado	Configurado	
Servicio de perfil de usuario	ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados	CDPSvc	Deshabilitado	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Deshabilitado	Configurado	
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Deshabilitado	Configurado	
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado	

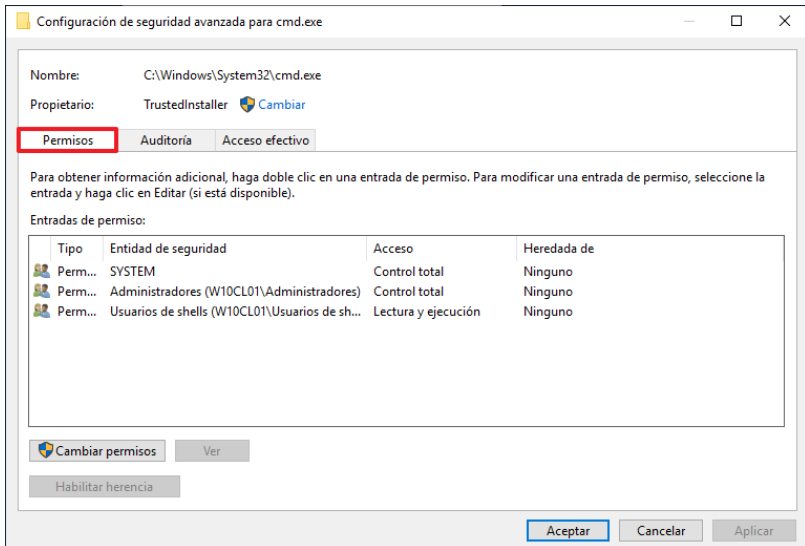
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de publicación World Wide Web	W3SVC	Deshabilitado	Configurado	
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Deshabilitado	Configurado	
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Deshabilitado	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Deshabilitado	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado	
Servicio de red de host	hns	Deshabilitado	Configurado	
Servicio de registro de W3C	w3logsvc	Deshabilitado	Configurado	
Servicio de reparación MultiPoint	WmsRepair	Deshabilitado	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Deshabilitado	Configurado	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Deshabilitado	Configurado	
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Deshabilitado	Configurado	
Servicio de supervisión de sensores	SensrSvc	Deshabilitado	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Deshabilitado	Configurado	
Servicio de uso compartido de datos	DsSvc	Deshabilitado	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Deshabilitado	Configurado		
Servicio de usuario del portapapeles	cbdhsvc	Deshabilitado	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Deshabilitado	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Deshabilitado	Configurado		
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado		
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Deshabilitado	Configurado		
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Deshabilitado	Configurado		
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado		
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Deshabilitado	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio telefónico	PhoneSvc	Deshabilitado	Configurado		
Servicios de Escritorio remoto	TermService	Deshabilitado	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios simples de TCP/IP	simptcp	Deshabilitado	Configurado		
Servidor	LanmanServer	Deshabilitado	Configurado		
Servidor de roles de DS	DsRoleSvc	Deshabilitado	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado		
Sincronizar host	OneSyncSvc	Deshabilitado	Configurado		
Sistema de cifrado de archivos (EFS)	EFS	Deshabilitado	Configurado		
Sistema de eventos COM+	EventSystem	Automático	Configurado		
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Deshabilitado	Configurado		
Superfetch	SysMain	Deshabilitado	Configurado		
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado		
Telefonía	TapiSrv	Deshabilitado	Configurado		
Telemetría y experiencias del usuario conectado	DiagTrack	Deshabilitado	Configurado		
Temas	Themes	Deshabilitado	Configurado		
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado		
Uso de datos	DusmSvc	Deshabilitado	Configurado		
WalletService	WalletService	Deshabilitado	Configurado		
WarpJITSvc	WarpJITSvc	Deshabilitado	Configurado		
Windows Installer	msiserver	Manual	Configurado		
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Deshabilitado	Configurado		
Windows Search	WSearch	Deshabilitado	Configurado		
Windows Update	wuauserv	Deshabilitado	Configurado		
Windows Update Medic Service	WaaSMedicSvc	Deshabilitado	Configurado		
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo
23.Verifique que se han asignado los permisos correctos en el sistema de archivos.		Desde la ventana de Powershell abierta anteriormente, ejecute "explorer.exe". A continuación, se abrirá el "Explorador de Windows". Localice cada fichero de los mostrados a continuación, siguiendo la ruta definida en la tabla, y seleccione propiedades con el botón derecho del ratón:  En la ventana de "Propiedades", seleccione la pestaña "Seguridad" y pulse sobre "Opciones Avanzadas".  Nota: En caso de que no aparezca la pestaña de seguridad, esto será debido a que las políticas administradas a través de la herramienta "Administración de directivas de grupo local" se han aplicado y, por tanto, se deberá volver a ejecutar el script "CCN-STIC-599B19 Cliente independiente – Habilita comprobaciones.bat".

Comprobación	OK/NOK	Cómo hacerlo	
		En la pestaña “Permisos” de la ventana “Configuración de <archivo a comprobar>”, aparecerán los permisos asignados al contenedor o fichero a comprobar.  Observe los permisos y compárelos con la siguiente tabla: Nota: Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados. Tenga en cuenta que tanto la cuenta Administrador como la cuenta Invitado estarán renombradas y, por tanto, aparecerán con su nuevo nombre. Es importante que no se modifiquen estos permisos, asegúrese de que al cerrar las ventanas de “Propiedades” y “Configuración de seguridad avanzada” pulsa sobre “Cancelar”.	
Archivo	Usuario	Permiso	OK/NOK
%Public%	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemDrive%\	Administradores	Control Total	
	CREATOR OWNER	Permisos especiales ¹	
	SYSTEM	Control Total	
	Usuarios	Lectura	

¹ Los permisos especiales que se establecerán para el creador de los objetos %SystemDrive% serán de Control Total pero aplicados a “Sólo subcarpetas y archivos” en lugar de aplicarlos a “Esta carpeta, subcarpeta y archivos”.

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemDrive%\Users\Default		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\regedit.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\Registration		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarioscmd	Leer y ejecutar	
%SystemRoot%\security		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\arp.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\at.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\azuresettingsyncprovider.dll		Administradores	Control Total	
%SystemRoot%\system32\bash.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\cacls.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\chatapis.dll		Administradores	Control Total	
%SystemRoot%\system32\chatapis.dll		Administradores	Control Total	
%SystemRoot%\system32\clip.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\cmd.exe		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\cscript.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\diagtrack.dll		Administradores	Control Total	
%SystemRoot%\system32\eshell.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\finger.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\ftp.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\gamepanel.exe		Administradores	Control Total	
		SYSTEM	Control Total	

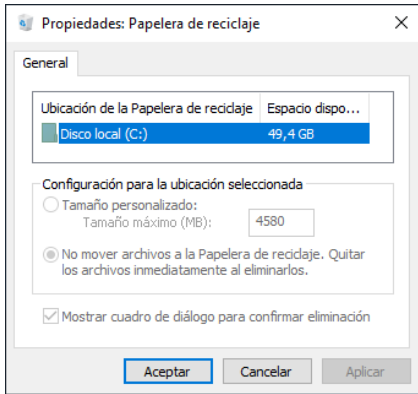
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\geolocation.dll		Administradores	Control Total	
%SystemRoot%\system32\hostname.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\ipconfig.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\iprip.dll		Administradores	Control Total	
%SystemRoot%\system32\nbtstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net1.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\netstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nfsadmin.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nslookup.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\phonecallhistoryapis.dll		Administradores	Control Total	
%SystemRoot%\system32\ping.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\privatecloudhnsplugin.dll		Administradores	Control Total	
%SystemRoot%\system32\ras		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control Total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control Total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control Total	
%SystemRoot%\system32\raschap.dll		Administradores	Control Total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control Total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control Total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control Total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control Total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control Total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control Total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control Total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control Total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control Total	
%SystemRoot%\system32\rastls.dll		Administradores	Control Total	
%SystemRoot%\system32\regedt32.exe		Administradores	Control Total	
		SYSTEM	Control Total	

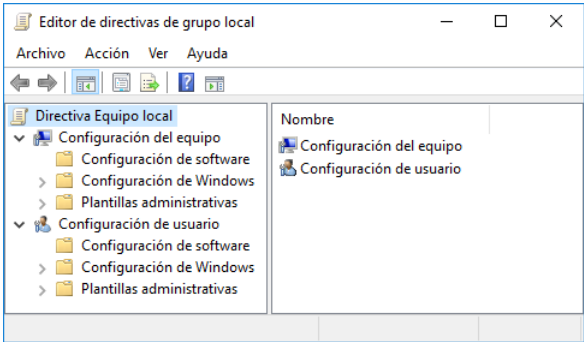


Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\regsvr32.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\route.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\runonce.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\secedit.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\telnet.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\tftp.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\tracert.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\uwfmgr.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\webcamui.dll	Administradores	Control Total	
%SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\wscript.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\xblgamesave.dll	Administradores	Control Total	
%SystemRoot%\system32\xcopy.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\arp.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\at.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\cacls.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\clip.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\cmd.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de shells	Lectura y ejecución, Lectura	

Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\cscript.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\finger.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\ftp.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\hostname.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\ipconfig.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\net.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\netstat.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\nslookup.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\ping.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\rasadhlp.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasautou.exe	Administradores	Control Total	
%SystemRoot%\syswow64\raschap.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasctnm.h	Administradores	Control Total	
%SystemRoot%\syswow64\rasctrs.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasdial.exe	Administradores	Control Total	
%SystemRoot%\syswow64\rasmontr.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasmxs.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasphone.exe	Administradores	Control Total	
%SystemRoot%\syswow64\rasppp.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasser.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rastapi.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rastls.dll	Administradores	Control Total	
%SystemRoot%\syswow64\regedt32.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\regsvr32.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\route.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\runonce.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\secedit.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\tracert.exe	Administradores	Control Total	
	SYSTEM	Control Total	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\PowerShell.exe		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\PowerShell_ISE.exe		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\syswow64\wscript.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\syswow64\xcopy.exe		Administradores	Control Total	
		SYSTEM	Control Total	
24. Compruebe los valores del registro configurados a través de los scripts de seguridad.		Desde la ventana de Powershell arrancada con anterioridad, ejecute "regedit.exe" para lanzar una ventana del editor del registro. Compruebe que las claves de registro indicadas en la siguiente tabla tienen los correspondientes valores mostrados en ella:		
		Clave	Valor	OK/NOK
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents\	ffffff	
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection\AllowTelemetry	00000001 (1)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MessagingService\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NgcCtnrSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NgcSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OneSyncSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PimIndexMaintenanceSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PrintWorkflowUserSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense\Start	00000004 (4)	

Comprobación	OK/NOK	Cómo hacerlo	
		Clave	Valor
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UnistoreSvc\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UserDataSvc\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WpnUserService\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EntAppSvc\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\LaunchTo	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsHistory	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsMenu	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClearRecentDocsOnExit	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecycleFiles	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ConfirmFileDelete	00000001 (1)
25.Verifique la configuración de la papelera de reciclaje.		Localice la papelera de reciclaje en el escritorio, márkela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá. Esto mostrará la siguiente ventana de propiedades de la papelera de reciclaje:  Compruebe que están seleccionadas las siguientes dos opciones:	

Comprobación	OK/NOK	Cómo hacerlo	
		Parámetro	OK/NOK
		No mover archivos a la Papelera de reciclaje. Quitar los archivos inmediatamente al eliminarlos.	
		Mostrar cuadro de diálogo para confirmar eliminación.	
26. Ejecute el editor de directiva de grupo local (gpedit.msc) para poder comprobar el contenido del GPO local en los próximos pasos.		Desde la ventana de Powershell arrancada anteriormente, ejecute "gpedit.msc". Esto abrirá una ventana del Editor de directivas de grupo local, como la mostrada en la siguiente figura.  En los siguientes pasos (identificados con el texto "GPO: ") verificará el contenido del objeto de directiva de grupo local (GPO). Hasta que se le indique, no deberá cerrar la ventana del Editor de directivas de grupo local, y deberá realizar las comprobaciones correspondientes dentro de ella, en las ubicaciones indicadas en cada caso.	
27. GPO: Compruebe la directiva de contraseñas.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas" Nota: Recuerde que estos datos pueden variar dependiendo del nivel de clasificación del que disponga el equipo. La guía asume la configuración de máxima seguridad.	
		Directiva	Valor
		Almacenar contraseñas con cifrado reversible	Deshabilitada
		Exigir historial de contraseñas	24 contraseñas recordadas
		La contraseña debe cumplir los requisitos de complejidad	Habilitada
		Longitud mínima de la contraseña	12 caracteres
		Vigencia máxima de la contraseña	90 días
		Vigencia mínima de la contraseña	2 días

Comprobación	OK/NOK	Cómo hacerlo		
28.GPO: Compruebe la directiva de bloqueo de cuenta.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de bloqueo de cuenta”		
		Nota: Recuerde que estos datos pueden variar dependiendo del nivel de clasificación del que disponga el equipo. La guía asume la configuración de máxima seguridad.		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	0	
		Restablecer el bloqueo de cuenta después de	30 minutos	
		Umbral de bloqueo de cuenta	3 intentos de inicio de sesión no válidos	
29.GPO: Compruebe la directiva de auditoría.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”		
		Directiva	Valor	OK/NOK
		Auditar el acceso a objetos	Correcto/Erróneo	
		Auditar el acceso al servicio de directorio	Correcto/Erróneo	
		Auditar el cambio de directivas	Correcto/Erróneo	
		Auditar el seguimiento de procesos	Sin auditoría	
		Auditar el uso de privilegios	Correcto/Erróneo	
		Auditar eventos de inicio de sesión	Correcto/Erróneo	
		Auditar eventos de inicio de sesión de cuenta	Correcto/Erróneo	
		Auditar eventos del sistema	Correcto/Erróneo	
		Auditar la administración de cuentas	Correcto/Erróneo	
30.GPO: Compruebe la asignación de derechos de usuario.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Actuar como parte del sistema operativo	(Definida, pero sin ningún valor)
		Administrar registro de seguridad y auditoría	Audidores, Administradores
		Agregar estaciones de trabajo al dominio	(Definida, pero sin ningún valor)
		Ajustar las cuotas de la memoria para un proceso	Administradores, Servicio de red, SERVICIO LOCAL
		Apagar el sistema	Administradores, Usuarios
		Aumentar el espacio de trabajo de un proceso	Administradores, Servicio de red, SERVICIO LOCAL
		Aumentar prioridad de programación	Administradores
		Cambiar la hora del sistema	Administradores, SERVICIO LOCAL
		Cambiar la zona horaria	Administradores, SERVICIO LOCAL
		Cargar y descargar controladores de dispositivo	Administradores
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)
		Crear objetos globales	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL
		Crear un archivo de paginación	Administradores
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)
		Crear vínculos simbólicos	Administradores
		Denegar el acceso a este equipo desde la red	Invitados, ANONYMOUS LOGON, aCdCmN599
		Denegar el inicio de sesión como servicio	Invitados ANONYMOUS LOGON
		Denegar el inicio de sesión como trabajo por lotes	Invitados ANONYMOUS LOGON

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Denegar el inicio de sesión local	Invitados ANONYMOUS LOGON
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	Servicio de red, SERVICIO LOCAL
		Generar perfiles de un solo proceso	Administradores
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Obtén un token de suplantación para otro usuario en la misma sesión	Administradores
		Omitir comprobación de recorrido	Administradores, Usuarios autenticados Servicio de red SERVICIO LOCAL
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	(Definida, pero sin ningún valor)
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento del volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	Servicio de red, SERVICIO LOCAL

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva		Valor
	Restaurar archivos y directorios		Administradores
	Sincronizar los datos del servicio de directorio		(Definida, pero sin ningún valor)
	Suplantar a un cliente tras la autenticación		Servicio Local, Servicio de red, Administradores
	Tener acceso a este equipo desde la red		Administradores, Usuarios
	Tomar posesión de archivos y otros objetos		Administradores
31.GPO: Compruebe las opciones de seguridad.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”	
Directiva		Valor	OK/NOK
Acceso a redes: canalizaciones con nombre accesibles anónimamente		(Definida, pero sin ningún valor)	
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales		Clásico: usuarios locales se autentican con credenciales propias	
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red		Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM		Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM		Habilitada	
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos		Deshabilitada	
Acceso a redes: recursos compartidos accesibles anónimamente		(Definida, pero sin ningún valor)	
Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Acceso a redes: rutas del Registro accesibles remotamente		System ² \CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\ServerApplications, Software\Microsoft\Windows NT\CurrentVersion	
Acceso a redes: rutas y subrutas del Registro accesibles remotamente		Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System ³ \CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	
Acceso de red: evitar que clientes con permiso realicen llamadas remotas a SAM		(Definida, pero sin ningún valor)	
Acceso de red: permitir traducción SID/nombre anónima		Deshabilitada	
Apagado: borrar el archivo de paginación de la memoria virtual		Habilitada	
Apagado: permitir apagar el sistema sin tener que iniciar sesión		Deshabilitada	
Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad		Habilitada	

² En este caso "System" hace referencia a HKEY_LOCAL_MACHINE\System, y "Software" a HKEY_LOCAL_MACHINE\Software.

³ En este caso "System" hace referencia a HKEY_LOCAL_MACHINE\System, y "Software" a HKEY_LOCAL_MACHINE\Software.



Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Auditoría: auditar el acceso de objetos globales del sistema		Deshabilitada	
Auditoría: auditar el uso del privilegio de copias de seguridad y restauración.		Deshabilitada	
Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior) para invalidar la configuración de la categoría de directiva de auditoría		Deshabilitada	
CCN: (DisableIPSourceRouting) Nivel de protección de enrutamiento de origen IP		2 = Protección alta, el enrutamiento en origen está completamente deshabilitado	
CCN: (DynamicBacklogGrowthDelta) Número de conexiones a crear cuando se necesiten conexiones adicionales para aplicaciones Winsock		10	
CCN: (EnableDeadGWDetect) Permitir detección automática de puertas de enlace de red inactivas		Deshabilitada	
CCN: (EnableDynamicBacklog) Habilitar el registro de envíos dinámico para aplicaciones Winsock		Habilitada	
CCN: (EnableICMPRedirect) Permitir redireccionamientos ICMP que prevalezcan sobre rutas generadas con OSPF		Deshabilitada	
CCN: (EnablePMTUDiscovery) Permitir detección automática de tamaño de MTU		Deshabilitada	
CCN: (KeepAliveTime) Frecuencia en milisegundos de envío de paquetes de mantenimiento de conexión.		300000 o 5 minutos (recomendado)	
CCN: (MaximumDynamicBacklog) Máximo número de conexiones <<cuasi-libres>> para aplicaciones Winsock		20000 (recomendado)	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
CCN: (MinimumDynamicBacklog) Mínimo número de conexiones libres para aplicaciones Winsock		20	
CCN: (NoDriveTypeAutoRun) Desactivar Autoejecutar para todas las unidades		255, Deshabilitar Autoejecutar para todas las unidades	
CCN: (NoNameReleaseOnDemand) Permitir al equipo ignorar las solicitudes de publicación de nombres NetBIOS excepto de los servidores WINS		Habilitada	
CCN: (NtfsDisable8dot3NameCreation) Permitir al ordenador detener la generación de nombres de archivo de estilo 8.3		Habilitada	
CCN: (PerformRouterDiscovery) Permitir que IRDP detecte y configure direcciones de puerta de enlace predeterminadas		Deshabilitada	
CCN: (SafeDllSearchMode) Activar el modo de búsqueda seguro de DLLs (recomendado)		Habilitada	
CCN: (ScreenSaverGracePeriod) El tiempo en segundos antes de que expire el periodo de gracia del protector de pantalla (0 recomendado)		0	
CCN: (SynAttackProtect) Nivel de protección frente a ataques SYN		1 = El tiempo de espera de la conexión se consume antes si se detecta un ataque SYN	
CCN: (TcpMaxConnectResponseRetransmissions) Retransmisiones SYN-ACK cuando no se reconoce una solicitud de conexión		2 = Las conexiones medio abiertas o con 3 y 6 segundos de tiempo de espera se cierran después de 21 segundos	
CCN: (TcpMaxDataRetransmissions) Número de retransmisiones de datos no reconocidos		3	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
CCN: (TCPMaxPortsExhausted) Número de solicitudes de conexión necesarias para iniciar la protección contra ataques SYN		5	
CCN: (WarningLevel) Umbral de porcentaje para el registro de eventos de seguridad en el cual el sistema generará una advertencia		90%	
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros		Deshabilitada	
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)		Habilitada	
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)		Habilitada	
Configuración del sistema: subsistemas opcionales		(Definida, pero sin ningún valor)	
Configuración de sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software		Deshabilitada	
Consola de recuperación: permitir el inicio de sesión administrativo automático		Deshabilitada	
Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas		Deshabilitada	
Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación		Habilitada	
Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador		Pedir credenciales en el escritorio seguro	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar		Pedir credenciales en el escritorio seguro	
Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación		Habilitada	
Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador		Habilitada	
Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras		Habilitada	
Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados		Deshabilitada	
Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador		Habilitada	
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro		Deshabilitada	
Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario		Habilitada	
Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo		Deshabilitada	
Controlador de dominio: permitir a los operadores de servidor programar tareas		Deshabilitada	
Controlador de dominio: requisitos de firma de servidor LDAP		Requerir firma	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo		El usuario debe escribir una contraseña cada vez que use una clave.	
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash		Deshabilitada	
Cuentas: bloquear cuentas Microsoft		Los usuarios no pueden agregar cuentas Microsoft ni iniciar sesión	
Cuentas: cambiar el nombre de cuenta de invitado		lcNcVn599	
Cuentas: cambiar el nombre de la cuenta de administrador		aCdCmN599	
Cuentas: estado de la cuenta de administrador		Deshabilitada	
Cuentas: estado de la cuenta de invitado		Deshabilitada	
Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola		Habilitada	
DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)		O:BAG:BAD:(A;;CCDCLC;;;AU) Equivale a: Usuarios autenticados: Permitir Acceso local y Acceso remoto	
DCOM: restricciones de inicio de equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)		O:BAG:BAD:(A;;CCDCLCSWRP;;;BA)(A;;CCDCSW;;;AU) Equivale a: Administradores: Permitir Ejecución local, Ejecucion remota, Activacion local y Activacion remota Usuarios autenticados: Permitir Ejecución local, Ejecucion remota, Activacion local y Activacion remota	
Dispositivos: impedir que los usuarios instalen controladores de impresora		Habilitada	
Dispositivos: permitir desacoplamiento sin tener que iniciar sesión		Deshabilitada	
Dispositivos: permitir formatear y expulsar medios extraíbles		Administradores	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente		Habilitada	
Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente		Habilitada	
Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente		Bloquear estación de trabajo	
Inicio de sesión interactivo: límite de inactividad del equipo		300 segundos (En el caso de estar aplicado el nivel de seguridad RESERVADO O SUPERIOR) 900 segundos (En el caso de estar aplicado el nivel de seguridad CONFIDENCIAL)	
Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión		No mostrar la información del usuario	
Inicio de sesión interactivo: no mostrar el último nombre de usuario		Habilitada	
Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr		Deshabilitada	
Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)		0 inicios de sesión	
Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire		14 días	
Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo		Habilitada	
Inicio de sesión interactivo: requerir tarjeta inteligente		Deshabilitada	
Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión		Este sistema está restringido a los usuarios autorizados.	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión		ES UN DELITO CONTINUAR SIN LA DEBIDA AUTORIZACIÓN	
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)		Habilitada	
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)		Habilitada	
Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo		Deshabilitada	
Miembro de dominio: duración máxima de contraseña de cuenta de equipo		30 días	
Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)		Habilitada	
Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)		Habilitada	
Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)		Habilitada	
Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows		Habilitada	
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión		Habilitada	
Seguridad de red: nivel de autenticación de LAN Manager		Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM	
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña		Habilitada	
Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem		Deshabilitada	
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet		Deshabilitada	
Seguridad de red: requisitos de firma de cliente LDAP		Negociar firma	
Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio		(Definida, pero sin ningún valor)	
Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM		(Definida, pero sin ningún valor)	
Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante		Habilitar la auditoría para todas las cuentas.	
Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio		Habilitar todo	
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio		Denegar todo	
Seguridad de red: restringir NTLM: tráfico NTLM entrante		Permitir todo	
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos		Permitir todo	
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)		Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)		Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión		Habilitada	



Comprobación	OK/NOK	Cómo hacerlo		
Directiva		Valor		OK/NOK
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)		Habilitada		
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)		Habilitada		
Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor		Requerido del cliente		
Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión		15 minutos		
32.GPO: Compruebe los valores de Administración de derechos digitales de Windows Media.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media"		
		Directiva	Valor	OK/NOK
		Impedir el acceso a Internet de Windows Media DRM	Habilitada	
33.GPO: Compruebe los valores de Cliente WinRM.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas administrativas → Componentes de Windows → Administración remota de Windows (WinRM) → Cliente WinRM"		
		Directiva	Valor	OK/NOK
		Hosts de confianza	Habilitada (Vacio)	
		Permitir tráfico sin cifrar	Deshabilitada	
34.GPO: Compruebe los valores de Servicio WinRM.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas administrativas → Componentes de Windows → Administración remota de Windows (WinRM) → Servicio WinRM"		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Activar escucha HTTP de compatibilidad		Deshabilitada	
	Activar escucha HTTPS de compatibilidad		Deshabilitada	
	No permitir que WinRM almacene credenciales de RunAs		Habilitada	
	Permitir la administración de servidores remotos a través de WinRM		Deshabilitada	
	Permitir tráfico sin cifrar		Deshabilitada	
35.GPO: Compruebe los valores de para Agregar características a Windows 10.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10”			
	Directiva		Valor	OK/NOK
	Impedir que el asistente se ejecute		Habilitada	
36.GPO: Compruebe los valores del almacén digital.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Almacén digital”			
	Directiva		Valor	OK/NOK
	No permitir que se ejecute el Almacén digital		Habilitada	
37.GPO: Compruebe los valores de análisis de confiabilidad.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Análisis de confiabilidad de Windows”			
	Directiva		Valor	OK/NOK
	Configurar proveedores de WMI de confiabilidad		Habilitada	
38.GPO: Compruebe los valores de Windows Defender.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Antivirus de Windows Defender”			
	Directiva		Valor	OK/NOK
	Desactivar Antivirus Windows Defender		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
39.GPO: Compruebe los valores de Windows Ink.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Área de trabajo de Windows Ink”		
		Directiva	Valor	OK/NOK
		Permitir el Área de trabajo de Windows Ink	Deshabilitada	
		Permitir las aplicaciones sugeridas en el Área de trabajo de Windows Ink	Deshabilitada	
40.GPO: Compruebe los valores de asistencia en línea.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitada	
41.GPO: Compruebe los valores de biometría.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Deshabilitada	
42.Verifique los valores de búsqueda de la directiva.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		Deshabilitar la interrupción del indizador	Deshabilitada	
		Impedir la adición automática de carpetas compartidas al índice de Windows Search	Habilitada	
		No buscar en Internet o mostrar resultados de internet en Search	Habilitada	
		Permitir búsqueda en la nube	Deshabilitada	
		Permitir el uso de Cortana	Deshabilitada	
		Permitir el uso de la ubicación para las búsquedas y Cortana	Deshabilitada	
		Permitir usar Cortana sobre la pantalla de bloqueo	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir que los clientes soliciten el índice de forma remota	Habilitada	
43.GPO: Compruebe los valores de la cámara.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Cámara”		
		Directiva	Valor	OK/NOK
		Permitir el uso de la cámara	Deshabilitada	
44.GPO: Compruebe los valores del centro de movilidad de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows”		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	
45.GPO: Compruebe los valores del centro de seguridad.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Centro de seguridad”		
		Directiva	Valor	OK/NOK
		Activar el Centro de seguridad (solo equipos de dominio)	Deshabilitada	
46.GPO: Compruebe los valores de cifrado de unidad BitLocker.		En la misma ventana de Conjunto resultante de directivas, compruebe los valores de directiva de grupo indicados en las siguientes tablas y en la ubicación siguiente: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de unidad BitLocker”		
		Directiva	Valor	OK/NOK
		Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y posteriores)	Habilitada SO: XTS-AES de 256 bits Fijas: XTS-AES de 256 bits Extraíbles: AES-CBC de 256 bits	
		Impedir la sobreescritura de memoria al reiniciar	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
47.GPO: Compruebe los valores de cifrado de unidad BitLocker en unidades de datos extraíbles.		En la misma ventana de Conjunto resultante de directivas, compruebe los valores de directiva de grupo indicados en las siguientes tablas y en la ubicación siguiente: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades de datos extraíbles”		
		Directiva	Valor	OK/NOK
		Controlar el uso de BitLocker en unidades extraíbles	Deshabilitada	
48.GPO: Compruebe los valores de cifrado de unidad BitLocker en unidades de sistema operativo.		En la misma ventana de Conjunto resultante de directivas, compruebe los valores de directiva de grupo indicados en las siguientes tablas y en la ubicación siguiente: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades del sistema operativo”		
		Directiva	Valor	OK/NOK
		Configurar longitud mínima de PIN para el inicio	Habilitada, 8	
		Configurar perfil de validación de plataforma del TPM para configuraciones de firmware basado en BIOS	Habilitada, 0,2,4,5,7,8,9,10 y 11	
		Permitir los PIN mejorados para el inicio	Habilitada	
		Requerir autenticación adicional al iniciar	Habilitada – Requerir PIN de inicio con TPM (No permitir TPM) – Configurar PIN de inicio del TPM (Requerir PIN de inicio con TPM) – Configurar clave de inicio del TPM (No permitir clave de inicio con TPM) – Configurar la clave de inicio y el PIN del TPM (No permitir clave y PIN de inicio con TPM)	

Comprobación	OK/NOK	Cómo hacerlo		
49.GPO: Compruebe los valores de compatibilidad de aplicaciones.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Compatibilidad de aplicaciones”		
		Directiva	Valor	OK/NOK
		Desactivar el Asistente para la compatibilidad de programas	Habilitada	
		Desactivar el motor de compatibilidad de aplicaciones	Habilitada	
		Desactivar el motor de compatibilidad de SwitchBack	Habilitada	
		Desactivar el recopilador de inventario	Habilitada	
		Desactivar la grabación de acciones	Habilitada	
		Desactivar la telemetría de aplicaciones	Habilitada	
		Impedir el acceso a aplicaciones de 16 bits	Habilitada	
		Quitar página de propiedades de compatibilidad de programas	Habilitada	
50.GPO: Compruebe los valores de configuración de Conectar.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Conectar”		
		Directiva	Valor	OK/NOK
		No permitir que se proyecte nada en este PC	Habilitada	
		Solicitar PIN para emparejar dispositivos	Habilitada	
51.GPO: Compruebe los valores de configuración de presentación.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Configuración de presentación”		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
52.GPO: Compruebe los valores de contenido de la nube.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Contenido de la nube”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar experiencias del consumidor de Microsoft	Habilitada	
		No mostrar sugerencias de Windows	Habilitada	
53.GPO: Compruebe los valores de reproducción automática.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Directivas de reproducción automática” Nota: Para comprobar las opciones deberá pulsar doble clic sobre cada directiva.		
		Directiva	Valor	OK/NOK
		Desactivar Reproducción automática	Habilitada, (Todas las unidades)	
		Deshabilitar Reproducción automática para dispositivos que no son de volumen	Habilitada	
		Establece el comportamiento predeterminado para la ejecución automática	Habilitada, (No ejecutar ningún comando de ejecución automática)	
		Evitar que reproducción automática recuerde las elecciones del usuario	Habilitada	
54.GPO: Compruebe los valores del Explorador de archivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Explorador de Archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitada	
		Desactivar la prevención de ejecución de datos para el Explorador	Deshabilitada	
		Desactivar modo protegido de protocolo de shell	Deshabilitada	
		Desactivar terminación del montón al resultar dañado	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
55.GPO: Compruebe los valores de las versiones anteriores del Explorador de archivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Explorador de Archivos → Versiones anteriores”		
		Directiva	Valor	OK/NOK
		Impedir la restauración de versiones anteriores remotas	Habilitada	
		Ocultar lista de versiones anteriores para archivos remotos	Habilitada	
56.GPO: Compruebe los valores del Explorador de juegos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Explorador de juegos”		
		Directiva	Valor	OK/NOK
		Desactivar el seguimiento del último juego en la carpeta Juegos	Habilitada	
		Desactivar la actualización de juegos	Habilitada	
		Desactivar la descarga de información sobre juegos	Habilitada	
57.GPO: Compruebe los valores de las Fuentes RSS.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Fuentes RSS”		
		Directiva	Valor	OK/NOK
		Activar autenticación básica de la fuente a través de HTTP	Deshabilitada	
		Desactivar sincronización en segundo plano para fuentes y Web Slices	Habilitada	
		Impedir acceso a lista de fuentes	Habilitada	
		Impedir descarga de caracteres enmarcados	Habilitada	
		Impedir detección automática de fuentes y Web Slices	Habilitada	
		Impedir suscripción o eliminación de una fuente o Web Slice	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
58.Verifique los valores de la grabación y difusión de juegos de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Grabación y difusión de juegos de Windows”		
		Directiva	Valor	OK/NOK
		Habilita o deshabilita la grabación y difusión de juegos de Windows	Deshabilitada	
59.GPO: Verifique los valores de la grabadora de sonidos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute la grabadora de sonidos	Habilitada	
60.GPO: Verifique los valores del grupo en el hogar.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Grupo en el hogar”		
		Directiva	Valor	OK/NOK
		Impedir que el equipo se una a un grupo en el hogar	Habilitada	
61.GPO: Verifique los valores de Implementación de paquetes.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Implementación de paquetes de la aplicación”		
		Directiva	Valor	OK/NOK
		Deshabilitar la instalación de aplicaciones para Windows en volúmenes que no sean del sistema	Habilitada	
		Impedir que los datos de aplicaciones de los usuarios se almacenen en volúmenes que no sean del sistema	Habilitada	
		Permitir que una aplicaciones para Windows comparta datos de aplicaciones entre los usuarios	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
62.GPO: Verifique los valores del informe de errores de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el Informe de errores de Windows	Habilitada	
		No enviar datos adicionales	Habilitada	
63.GPO: Verifique los valores de la interfaz de usuario de credenciales.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Interfaz de usuario de credenciales”		
		Directiva	Valor	OK/NOK
		Enumerar las cuentas de administración al realizar una elevación	Deshabilitada	
		No mostrar el botón revelar contraseña	Habilitado	
64.GPO: Verifique los valores de Mapas.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Mapas”		
		Directiva	Valor	OK/NOK
		Desactivar el tráfico de red no solicitado en la página de configuración de Mapas sin conexión	Habilitada	
		Desactivar la descarga automática y la actualización de datos de mapa	Habilitada	
65.GPO: Verifique los valores de MDM.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → MDM”		
		Directiva	Valor	OK/NOK
		Deshabilitar la inscripción de MDM	Habilitada	
66.Verifique los valores de Mensajería.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Mensajería”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir la sincronización en la nube del servicio de mensajería	Deshabilitada	
67.GPO: Verifique los valores de NetMeeting.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → NetMeeting”		
		Directiva	Valor	OK/NOK
		Deshabilitar uso compartido de escritorio remoto	Habilitada	
68.GPO: Verifique los valores de las opciones de One Drive.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → One Drive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos	Habilitada	
69.GPO: Verifique los valores de las opciones de inicio de sesión de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar o habilitar la secuencia de aviso de seguridad de software	Habilitada (Ninguno)	
		Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario	Deshabilitada	
		Iniciar sesión automáticamente con el último usuario interactivo después de un reinicio iniciado por el sistema	Deshabilitada	
		Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	Habilitada	
70.GPO: Verifique los valores de la plataforma de protección de software.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Plataforma de protección de software”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Controlar la reactivación de dispositivos comerciales	Habilitada	
		Desactivar validación AVS en línea del cliente KMS	Habilitada	
71.GPO: Verifique los valores de Privacidad de aplicación.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Privacidad de la aplicación” Nota: Para comprobar las opciones deberá pulsar doble clic sobre cada directiva.		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows se sincronicen con dispositivos	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitada (Force Deny)	

Comprobación	OK/NOK	Cómo hacerlo		
72.GPO: Verifique los valores del programa para la mejora de la experiencia del usuario.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Programa para la mejora de la experiencia del usuario de Windows”		
		Directiva	Valor	OK/NOK
		Permitir la redirección corporativa de las cargas para la mejora de la experiencia del usuario	Deshabilitada	
73.GPO: Verifique los valores de Recopilación de datos y versiones preliminares.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos y versiones preliminares”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Alternar control de usuario sobre compilaciones de Insider	Deshabilitada	
		No volver a mostrar notificaciones de comentarios	Habilitada	
		Permitir Telemetría	Habilitada (0: Seguridad [solo empresas])	
74.GPO: Verifique los valores del cliente de conexión a escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Cliente de conexión a escritorio remoto”		
		Directiva	Valor	OK/NOK
		Configurar la autenticación del servidor para el cliente	Habilitada (No conectarse si hay errores de autenticación)	
		No permitir que se guarden las contraseñas	Habilitada	
		Permitir archivos .rdp de publicadores desconocidos	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
75.GPO: Verifique los valores de las conexiones de Host de sesión de Escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Conexiones”		
		Directiva	Valor	OK/NOK
		Permitir que los usuarios se conecten de forma remota mediante Servicios de Escritorio remoto	Deshabilitada	
76.GPO: Verifique los valores de la redirección de dispositivos o recursos de Host de sesión de Escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Redirección de dispositivo o recurso”		
		Directiva	Valor	OK/NOK
		No permitir redirección de unidad	Habilitada	
77.GPO: Verifique los valores de la seguridad de Host de sesión de Escritorio.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Seguridad”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Establecer el nivel de cifrado de conexión de cliente	Habilitada (Nivel alto)	
		Requerir comunicación RPC segura	Habilitada	
		Requerir la autenticación del usuario para las conexiones remotas mediante Autenticación a nivel de red	Habilitada	
		Solicitar la contraseña siempre al conectar	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
78.GPO: Verifique los valores del Shell remoto de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Shell Remoto de Windows”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Especificar número máximo de shells remoto por usuario	Habilitada, (MaxShellsPerUser: 1)	
		MaxConcurrentUsers	Habilitada (MaxConcurrentUsers: 1)	
		Permitir acceso a shell remoto	Deshabilitada	
79.GPO: Verifique los valores de Sincronizar la configuración.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Sincronizar la configuración”		
		Directiva	Valor	OK/NOK
		No sincronizar	Habilitada, (Permitir a los usuarios activar la sincronización: Deshabilitado))	
80.GPO: Verifique los valores de Accesorios.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Tablet PC → Accesorios”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute Windows Journal	Desabilitada	
81.GPO: Verifique los valores de tarjeta inteligente.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Tarjeta inteligente”		
		Directiva	Valor	OK/NOK
		Activar servicio Plug and Play de tarjeta inteligente	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
82.GPO: Verifique los valores de la tienda.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitada	
		Deshabilitar todas las aplicaciones de Microsoft Store	Deshabilitada	
83.GPO: Verifique los valores de ubicación y sensores.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
84.GPO: Verifique los valores del servicio de localización de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Servicio de localización de Windows”		
		Directiva	Valor	OK/NOK
		Desactivar el Servicio de localización de Windows	Habilitada	
85.GPO: Verifique los valores de virtualización de la experiencia del usuario de Microsoft.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Virtualización de la experiencia del usuario de Microsoft”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Configuración de sincronización de Windows		Deshabilitada	
	No sincronizar aplicaciones de Windows		Habilitada	
	Sincronizar aplicaciones de Windows que no aparecen en la lista		Deshabilitada	
	Sincronizar configuración en conexiones de uso medido		Deshabilitada	
	Sincronizar configuración en conexiones de uso medido incluso si son móviles		Deshabilitada	
	Usar User Experience Virtualization (UE-V)		Deshabilitada	
86.GPO: Verifique los valores de Windows Hello.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Hello para empresas”		
	Directiva		Valor	OK/NOK
	Usa Windows Hello para empresas		Deshabilitada	
	Usar biometría		Deshabilitada	
87.GPO: Verifique los valores de Windows Installer.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Installer”		
	Directiva		Valor	OK/NOK
	Impedir advertencias de seguridad de Internet Explorer para Scripts de Windows Installer		Deshabilitada	
	Impedir que los usuarios usen Windows Installer para instalar actualizaciones		Habilitada	
	Instalar siempre con privilegios elevados		Deshabilitada	
	Permitir a los usuarios aplicar revisiones a productos con privilegios elevados		Deshabilitada	
	Permitir a los usuarios buscar el origen cuando tienen privilegios elevados		Deshabilitada	
	Permitir a los usuarios usar el origen de medios cuando tienen privilegios elevados		Deshabilitada	
	Permitir el control del usuario sobre las instalaciones		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Prohibir a los usuarios que no son administradores la aplicación de actualizaciones firmadas por los proveedores	Habilitada	
88.GPO: Verifique los valores de Windows Messenger.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Messenger”		
		Directiva	Valor	OK/NOK
		No ejecutar automáticamente Windows Messenger al inicio	Habilitada	
		No permitir que se ejecute Windows Messenger	Habilitada	
89.GPO: Verifique los valores de Windows Update.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Update”		
		Directiva	Valor	OK/NOK
		Configurar Actualizaciones automáticas	Deshabilitada	
90.GPO: Verifique los valores de Impresoras.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Impresoras”		
		Directiva	Valor	OK/NOK
		Ejecutar controladores de impresión en procesos aislados	Habilitado	
		Permitir que se publiquen impresoras	Deshabilitado	
91.Verifique los valores de Notificaciones.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Menú inicio y barra de tareas → Notificaciones”		
		Directiva	Valor	OK/NOK
		Desactivar el uso de la red para notificaciones	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
92.Verifique los valores del Panel de control.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Panel de control"		
		Directiva	Valor	OK/NOK
		Permitir recomendaciones en línea	Deshabilitada	
93.GPO: Verifique los valores de Configuración regional e idioma.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma"		
		Directiva	Valor	OK/NOK
		Permitir que los usuarios habiliten servicios de reconocimiento de voz en línea	Deshabilitada	
94.GPO: Verifique los valores de Personalización de escritura a mano.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano"		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitada	
95.Verifique los valores de Personalización.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Panel de control → Personalización"		
		Directiva	Valor	OK/NOK
		Evitar la activación de la cámara de la pantalla de bloqueo	Habilitada	
96.Verifique los valores del administrador de conexiones de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Administrador de conexiones de Windows"		
		Directiva	Valor	OK/NOK
		Prohibir la conexión a redes de banda ancha móvil de proveedores móviles	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
97.GPO: Verifique los valores de archivos sin conexión.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Archivos sin conexión”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Especificar archivos sin conexión asignados de forma administrativa	Deshabilitada	
		Permitir o denegar el uso de la característica Archivos sin conexión	Deshabilitada	
		Quitar el comando “Disponible sin conexión”	Habilitada	
98.GPO: Verifique los valores de BranchCache.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → BranchCache”		
		Directiva	Valor	OK/NOK
		Activar BranchCache	Deshabilitada	
99.GPO: Verifique los valores del perfil de firewall de dominio.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Conexiones de Red → Firewall de Windows Defender → Perfil de dominio”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Firewall de Windows Defender: No permitir excepciones	Habilitada	
		Firewall de Windows Defender: No permitir notificaciones	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Firewall de Windows Defender: No permitir respuesta de unidifusión a peticiones de difusión o multidifusión	Deshabilitada	
		Firewall de Windows Defender: Permitir registro	Habilitada (Registro de paquetes perdidos – Deshabilitado) (Registro de conexiones correctas – Deshabilitado) (Ruta y nombre de archivos de registro: %systemroot%\system32\Log Files\Firewall\pfirewall.log) (Límite de tamaño: 4096 KB)	
		Firewall de Windows Defender: Proteger todas las conexiones de red	Habilitada	
100.GPO: Verifique los valores del perfil de firewall estándar.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Conexiones de Red → Firewall de Windows Defender → Perfil estándar”		
		Directiva	Valor	OK/NOK
		Firewall de Windows Defender: No permitir excepciones	Habilitada	
		Firewall de Windows Defender: No permitir notificaciones	Habilitada	
		Firewall de Windows Defender: No permitir respuesta de unidifusión a peticiones de difusión o multidifusión	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Firewall de Windows Defender: Permitir registro	Habilitada (Registro de paquetes perdidos – Deshabilitado) (Registro de conexiones correctas – Deshabilitado) (Ruta y nombre de archivos de registro: %systemroot%\system32\Log Files\Firewall\pfirewall.log) (Límite de tamaño: 4096 KB)	
		Firewall de Windows Defender: Proteger todas las conexiones de red	Habilitada	
101.GPO: Verifique los valores de las tecnologías de transición a IPv6.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Configuración de TCPIP → Tecnologías de transición IPv6”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Estado de 6to4	Habilitada (Estado Deshabilitado)	
		Estado de IP-HTTPS	Habilitada URL: ""(espacio en blanco), (Estado Deshabilitado)	
		Estado de ISATAP	Habilitada (Estado Deshabilitado)	
		Estado de Teredo	Habilitada (Estado Deshabilitado)	
102.GPO: Verifique los valores de la detección de topologías a nivel de vínculo.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Detección de topologías de nivel de vínculo”		
		Directiva	Valor	OK/NOK
		Activar controlador de E/S de asignador (LLTDIO)	Deshabilitada	
		Activar controlador de respuesta (RSPNDR)	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
103.GPO: Verifique los valores de la estación de trabajo Lanman.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Estación de trabajo Lanman”		
		Directiva	Valor	OK/NOK
		Habilitar inicios de sesión de invitado no seguros	Deshabilitada	
104.GPO: Verifique los valores de Fuentes.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Fuentes”		
		Directiva	Valor	OK/NOK
		Habilitar Proveedores de fuentes	Deshabilitada	
105.GPO: Verifique los valores de Proyección inalámbrica.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Proyección inalámbrica”		
		Directiva	Valor	OK/NOK
		Requerir emparejamiento de PIN	Habilitada	
106.GPO: Verifique los valores de Configuración WLAN.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Servicio WLAN → Configuración WLAN”		
		Directiva	Valor	OK/NOK
		Permite que Windows se conecte automáticamente a puntos de acceso abiertos sugeridos, redes compartidas por los contactos y puntos de acceso que ofrezcan servicios de pago	Habilitada	



Comprobación	OK/NOK	Cómo hacerlo		
107.Verifique los valores de Acceso a datos móviles de la directiva "CCN-STIC-599B19 Windows 10 - Equipos".		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servicio WWAN → Acceso a datos móviles"		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows tiene acceso a los datos móviles	Habilitada (Forzar denegación)	
108.Verifique los valores de Configuración de la interfaz de usuario de WWAN.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servicio WWAN → Configuración de la interfaz de usuario de WWAN"		
		Directiva	Valor	OK/NOK
		Establecer la visibilidad de interfaz de usuario de acceso de red de telefonía móvil por aplicación	Habilitada (Ocultar)	
109.GPO: Verifique los valores de los servicios de redes de igual a igual de Microsoft.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servicios de redes de igual a igual de Microsoft"		
		Directiva	Valor	OK/NOK
		Desactivar los Servicios de redes de igual a igual de Microsoft	Habilitada	
110.GPO: Verifique los valores del servidor Lanman.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servidor Lanman"		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		



Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Publicación de hash para BranchCache	Habilitada (No permitir la publicación de hash en ninguna carpeta compartida)	
111.GPO: Verifique los valores de Windows Connect Now.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Windows Connect Now”		
		Directiva	Valor	OK/NOK
		Prohibir el acceso de los asistentes de Windows Connect Now	Habilitada	
112.GPO: Verifique los valores de Acceso de almacenamiento extraíble.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Acceso de almacenamiento extraíble”		
		Directiva	Valor	OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitada	
113.GPO: Verifique los valores de la administración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Restringir comunicaciones de Internet	Habilitada	
114.GPO: Verifique los valores de la configuración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Desactivar al Asistente para la conexión a Internet si la conexión de direcciones URL hace referencia a Microsoft.com	Habilitada
		Desactivar descargas de Internet de los asistentes para la publicación en Web y pedidos en línea	Habilitada
		Desactivar el acceso a Store	Habilitada
		Desactivar el acceso a todas las características de Windows Update	Habilitada
		Desactivar el contenido "¿Sabía que...?" del Centro de ayuda y soporte técnico	Habilitada
		Desactivar el informe de errores de Windows	Habilitada
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows	Habilitada
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger	Habilitada
		Desactivar el registro si la conexión de direcciones URL hace referencia a Microsoft.com	Habilitada
		Desactivar el servicio de asociaciones de archivo de Internet	Habilitada
		Desactivar impresión a través de HTTP	Habilitada
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitada
		Desactivar la actualización automática de certificados raíz	Habilitada
		Desactivar la actualización de archivos de contenido del Asistente para búsqueda	Habilitada
		Desactivar la búsqueda de controladores de dispositivos en Windows Update	Habilitada
		Desactivar la búsqueda en Microsoft Knowledge Base del Centro de Ayuda y soporte técnico	Habilitada
		Desactivar la descarga de controladores de impresión a través de HTTP	Habilitada
		Desactivar la tarea "Publicar en Web" para archivos y carpetas	Habilitada
		Desactivar la tarea de imágenes "Pedir copias fotográficas"	Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar los vínculos "Events.asp" del Visor de eventos		Habilitada	
	Desactivar pruebas activas del Indicador de estado de conectividad de la red de Windows		Habilitada	
	Desactivar uso compartido de datos de personalización de escritura a mano		Habilitada	
115.GPO: Verifique los valores de App-V.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Sistema → App-V"			
	Directiva		Valor	OK/NOK
	Habilitar el cliente de App-V		Deshabilitada	
116.GPO: Verifique los valores de asistencia remota.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Sistema → Asistencia Remota"			
	Directiva		Valor	OK/NOK
	Configurar la asistencia remota solicitada		Deshabilitada	
	Configurar Ofrecer Asistencia remota		Deshabilitada	
117.GPO: Verifique los valores de directiva de grupo.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Sistema → Directiva de grupo"			
	Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.			
	Directiva		Valor	OK/NOK
	Configurar el procesamiento de directivas de mantenimiento de Internet Explorer		Habilitada (Procesar incluso si los objetos de directiva de grupo no han cambiado)	
	Configurar el procesamiento de directivas de seguridad		Habilitada (Procesar incluso si los objetos de directiva de grupo no han cambiado)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar el procesamiento de directivas del Registro	Habilitada (Procesar incluso si los objetos de directiva de grupo no han cambiado)	
		Continuar experiencias en este dispositivo	Deshabilitado	
118.Verifique los valores de directiva del sistema operativo.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Directiva del sistema operativo”		
		Directiva	Valor	OK/NOK
		Permitir historial del Portapapeles	Deshabilitada	
		Permitir la sincronización del portapapeles entre dispositivos	Deshabilitada	
		Habilita la fuente de actividades	Deshabilitada	
		Permitir la publicación de las actividades del usuario	Deshabilitada	
		Permitir la carga de actividades del usuario	Deshabilitada	
119.GPO: Verifique los valores de inicio de sesión.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Inicio de sesión”		
		Directiva	Valor	OK/NOK
		Desactivar inicio de sesión con contraseña de imagen	Habilitada	
		Desactivar las notificaciones de aplicaciones en la pantalla de bloqueo	Habilitada	
		Evitar que el usuario muestre detalles de la cuenta al iniciar sesión	Habilitada	
		Mostrar animación de primer inicio de sesión	Deshabilitada	
		No mostrar la interfaz de usuario de selección de red	Habilitada	
		No procesar la lista de ejecución heredada	Habilitada	
		No procesar la lista de una sola ejecución	Habilitada	
		Ocultar puntos de entrada para el Cambio rápido de usuario	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
120.GPO: Verifique los valores de instalación de dispositivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Instalación de dispositivos”		
		Directiva	Valor	OK/NOK
		Permitir acceso remoto a la interfaz Plug and Play	Deshabilitada	
121.GPO: Verifique los valores de restricciones de instalación de dispositivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Impedir la instalación de dispositivos no descritos por otras configuraciones de directiva	Habilitada	
		Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. De dispositivo	Habilitada (Crear lista de id - espacio en blanco para crear lista)	
		Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos	Deshabilitada	
122.GPO: Verifique los valores de la llamada a procedimiento remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Llamada a procedimiento remoto”		
		Directiva	Valor	OK/NOK
		Habilitar la Autenticación de clientes del Asignador de extremos de RPC	Habilitada	
		Restricciones para clientes de RPC no autenticados	Habilitada (Autenticado)	



Comprobación	OK/NOK	Cómo hacerlo		
123.Verifique los valores de Net Logon.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Net Logon”		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada	
124.GPO: Verifique los valores de Perfiles de usuario.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Perfiles de Usuario”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Administración del usuario del uso compartido del nombre de usuario, imagen de cuenta e información del dominio con aplicaciones (que no sean aplicaciones de escritorio)	Habilitada (Siempre desactivado)	
125.Verifique los valores de Servicios de configuración regional.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Servicios de configuración regional”		
		Directiva	Valor	OK/NOK
		Denegar el cambio de ubicación geográfica	Habilitada	
126.Verifique los valores de Herramienta de diagnóstico.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Solución de problemas y diagnósticos → Herramienta de diagnóstico para soporte técnico de Microsoft”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Herramienta de diagnóstico para soporte técnico de Microsoft: activar la comunicación interactiva de la herramienta MSDT con el proveedor de soporte técnico		Deshabilitada	
	Herramienta de diagnóstico para soporte técnico de Microsoft: configurar nivel de ejecución		Deshabilitada	
	Herramienta de diagnóstico para soporte técnico de Microsoft: restringir descarga de herramientas		Deshabilitada	
127.GPO: Verifique los valores de Carpetas compartidas.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Carpetas compartidas”			
	Directiva		Valor	OK/NOK
	Permitir publicación de carpetas compartidas		Deshabilitada	
	Permitir publicación de raíces DFS		Deshabilitada	
128.GPO: Verifique los valores del administrador de datos adjuntos.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Administrador de datos adjuntos”			
	Directiva		Valor	OK/NOK
	Confiar en la lógica de datos adjuntos de archivos		Habilitada, Examinar controlador y tipo de archivo	
	Nivel de riesgo predeterminado de los datos adjuntos de archivo		Habilitada, Alto riesgo	
	No conservar la información de zona en los datos adjuntos de archivo		Deshabilitada	
	Notificar a los programas antivirus cuando se abren datos adjuntos		Habilitada	
	Ocultar mecanismos para eliminar la información de zona		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
129.Verifique los valores para Agregar características .		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10”		
		Directiva	Valor	OK/NOK
		Impedir que el asistente se ejecute	Habilitada	
130.GPO: Verifique los valores del almacén digital.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el Almacén digital	Habilitada	
131.GPO: Verifique los valores del centro de movilidad de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows”		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	
132.GPO: Verifique los valores de la compatibilidad de aplicaciones.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Compatibilidad de aplicaciones”		
		Directiva	Valor	OK/NOK
		Desactivar el Asistente para la compatibilidad de programas	Habilitada	
133.GPO: Verifique los valores de la configuración de presentación.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Configuración de presentación”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
134.Verifique los valores de la configuración de nube.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Contenido de la nube”		
		Directiva	Valor	OK/NOK
		Configurar Contenido destacado de Windows en la pantalla de bloqueo	Deshabilitada	
		Desactivar todas las ventanas de Contenido destacado de Windows	Habilitada	
		No sugerir contenido de terceros en el contenido destacado de Windows	Habilitada	
135.GPO: Verifique los valores de las directivas de reproducción.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar Reproducción automática	Habilitada, Todas las unidades	
		Deshabilitar Reproducción automática para dispositivos que no son de volumen	Habilitada	
		Establece el comportamiento predeterminado para ejecución automática	Habilitada, No ejecutar ningún comando de ejecución automática	
		Evitar que Reproducción automática recuerde las elecciones del usuario	Habilitada	
136.GPO: Verifique los valores del explorador de archivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Archivos”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar el almacenamiento en caché de imágenes en miniatura		Habilitada	
	Desactivar la presentación de miniaturas y mostrar sólo iconos		Habilitada	
	Desactivar la presentación de miniaturas y mostrar sólo iconos en las carpetas de red		Habilitada	
	Desactivar modo protegido de protocolo de shell		Deshabilitada	
	Desactivar todas las características de bibliotecas de Windows que dependan de datos de archivos indizados		Habilitada	
	Mostrar el dialogo de confirmación al eliminar archivos		Habilitada	
	No mover los archivos eliminados a la papelera de reciclaje		Habilitada	
	Quitar la pestaña seguridad		Habilitada	
	Quitar las características de grabación de CD		Habilitada	
137.Verifique los valores de diálogo común para abrir archivos.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de archivos → Diálogo común para abrir archivos”			
	Directiva		Valor	OK/NOK
	Ocultar la lista desplegable de archivos recientes		Habilitada	
138.GPO: Verifique los valores del panel de marcos del explorador.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Archivos → Panel de marcos del explorador”			
	Directiva		Valor	OK/NOK
	Desactivar el panel de vista previa		Habilitada	
139.GPO: Verifique los valores de las versiones anteriores del explorador de Windows.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Windows → Versiones anteriores”			

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir la restauración de versiones anteriores remotas	Habilitada	
		Ocultar lista de versiones anteriores para archivos remotos	Habilitada	
140.GPO: Verifique los valores de las fuentes RSS.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Fuentes RSS”		
		Directiva	Valor	OK/NOK
		Activar autenticación básica de la fuente a través de HTTP	Deshabilitada	
		Desactivar sincronización en segundo plano para fuentes y Web Slices	Habilitada	
		Impedir acceso a lista de fuentes	Habilitada	
		Impedir descarga de caracteres enmarcados	Habilitada	
		Impedir detección automática de fuentes y Web Slices	Habilitada	
		Impedir suscripción o eliminación de una fuente o Web Slice	Habilitada	
141.GPO: Verifique los valores de la grabadora de sonidos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute la grabadora de sonidos	Habilitada	
142.GPO: Verifique los valores del informe de errores de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el Informe de errores de Windows	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
143.Verifique los valores de la interfaz de credenciales.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Interfaz de usuario de credenciales”		
		Directiva	Valor	OK/NOK
		No mostrar el botón revelar contraseña	Habilitada	
144.GPO: Verifique los valores de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console”		
		Directiva	Valor	OK/NOK
		Restringir a los usuarios a la lista de complementos con permisos explícitos	Habilitada	
		Restringir al usuario la entrada al modo de autor	Habilitada	
145.GPO: Verifique los valores de los complementos restringidos o permitidos de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Complementos restringidos o permitidos”		
		Directiva	Valor	OK/NOK
		Administración de almacenamiento extraíble	Deshabilitado	
		Administración de directivas de seguridad IP	Habilitado	
		Administración de discos	Habilitado	
		Administración de equipos	Habilitado	
		Administración de TPM	Deshabilitado	
		Administrador de clúster de conmutación por error	Deshabilitado	
		Administrador de dispositivos	Habilitado	
		Administrador del servidor	Deshabilitado	
		Autoridad de registro de mantenimiento (HRA)	Deshabilitado	
		Carpetas compartidas	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Certificados	Deshabilitado
		Configuración de .Net Framework	Habilitado
		Configuración de Servicios de Escritorio remoto	Habilitado
		Configuración del cliente de NAP	Deshabilitado
		Configuración y análisis de seguridad	Habilitado
		Control ActiveX	Deshabilitado
		Control de admisión QoS	Deshabilitado
		Control WMI	Deshabilitado
		Desfragmentador de discos	Deshabilitado
		Dominios y confianza de Active Directory	Deshabilitado
		Edición de ADSI	Deshabilitado
		Enrutamiento y acceso remoto	Habilitado
		Entidad de certificación	Deshabilitado
		Escritorios remotos	Deshabilitado
		Extensiones de servidor de FrontPage	Deshabilitado
		Firewall de Windows con seguridad avanzada	Habilitado
		Información del sistema	Deshabilitado
		Internet Information Services	Deshabilitado
		Monitor de seguridad IP	Deshabilitado
		Monitor inalámbrico	Deshabilitado
		PKI de empresa	Deshabilitado
		Plantillas de certificado	Deshabilitado
		Plantillas de seguridad	Habilitado
		Registros y alertas de rendimiento	Deshabilitado
		Servicio de Fax	Habilitado
		Servicio de respuesta en línea	Deshabilitado
		Servicios	Habilitado
		Servicios de componente	Deshabilitado
		Servicios de Index Server	Deshabilitado
		Servidor de directivas de redes (NPS)	Deshabilitado
		Sistema de archivos distribuido	Deshabilitado
		Sitios y servicios de Active Directory	Deshabilitado
		Telefonía	Habilitado
		Usuarios y equipos de Active Directory	Deshabilitado
		Usuarios y grupos locales	Habilitado
		Vínculo a la dirección web	Deshabilitado
		Visor de eventos (Windows Vista)	Habilitado
		Visor de eventos	Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
146.GPO: Verifique los valores de directiva de grupo de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Complementos restringidos o permitidos → Directiva de grupo”		
		Directiva	Valor	OK/NOK
		Administración de directivas de grupo	Habilitada	
		Editor de objetos de directiva de grupo	Habilitada	
		Conjunto resultante de directivas	Habilitada	
147.GPO: Verifique los valores de las extensiones de complemento de directivas de grupo de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Complementos restringidos o permitidos → Directiva de grupo → Extensiones de complemento de directivas de grupo”		
		Directiva	Valor	OK/NOK
		Configuración de Seguridad	Habilitada	
		Firewall de Windows con seguridad avanzada	Habilitada	
		Plantillas Administrativas (equipos)	Habilitada	
		Plantillas Administrativas (usuarios)	Habilitada	
148.GPO: Verifique los valores de NetMeeting.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Deshabilitar chat		Habilitada	
	Deshabilitar Pizarra		Habilitada	
	Deshabilitar Pizarra de NetMeeting 2.x		Habilitada	
	Deshabilitar servicios de directorio		Habilitada	
	Impedir el envío de archivos		Habilitada	
	Impedir la aceptación automática de llamadas		Habilitada	
	Impedir la adición de servidores de directorio		Habilitada	
	Impedir la modificación del método de realización de llamada		Habilitada	
	Impedir la recepción de archivos		Habilitada	
	Impedir ver el directorio web		Habilitada	
	Audio y video\Deshabilitar audio		Habilitada	
	Audio y video\Deshabilitar audio de dúplex completo		Habilitada	
	Audio y video\Impedir el envío de vídeo		Habilitada	
	Audio y video\Impedir la recepción de vídeo		Habilitada	
149.GPO: Verifique los valores de audio y video de NetMeeting.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting → Audio y vídeo”			
	Directiva		Valor	OK/NOK
	Deshabilitar audio		Habilitada	
	Deshabilitar audio de dúplex completo		Habilitada	
	Impedir el envío de vídeo		Habilitada	
	Impedir la recepción de vídeo		Habilitada	
150.GPO: Verifique los valores de compartir aplicaciones a través de NetMeeting.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting → Compartir aplicaciones”			

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Deshabilitar el uso compartido de aplicaciones		Habilitada	
	Impedir el control		Habilitada	
	Impedir el uso compartido		Habilitada	
	Impedir el uso compartido de las ventanas del Explorador		Habilitada	
	Impedir el uso compartido de símbolos del sistema		Habilitada	
	Impedir el uso compartido del escritorio		Habilitada	
151.GPO: Verifique los valores de la página de opciones de NetMeeting.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting → Página de opciones”			
	Directiva		Valor	OK/NOK
	Deshabilitar el botón Llamada avanzada		Habilitada	
	Ocultar la página General		Habilitada	
	Ocultar la página Seguridad		Habilitada	
152.GPO: Verifique los valores del cliente de conexión a escritorio remoto.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Servicios de escritorio remoto → Cliente de conexión a Escritorio remoto”			
	Directiva		Valor	OK/NOK
	No permitir que se guarden las contraseñas		Habilitada	
153.Verifique los valores de Accesorios.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Tablet PC → Accesorios”			
	Directiva		Valor	OK/NOK
	No permitir que se ejecute Windows Journal		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
154.Verifique los valores de Tienda.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitada	
		Desactivar la oferta para actualizar a la versión de Windows más reciente	Habilitada	
155.GPO: Verifique los valores de ubicación y sensores.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Ubicación y sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
156.GPO: Verifique los valores de uso compartido de red.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Uso compartido de red”		
		Directiva	Valor	OK/NOK
		Impedir que los usuarios compartan archivos dentro de su perfil	Habilitada	
157.GPO: Verifique los valores de virtualización de la experiencia del usuario de Microsoft.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas Administrativas → Componentes de Windows → Virtualización de la experiencia del usuario de Microsoft”		
		Directiva	Valor	OK/NOK
		Configuración de sincronización de Windows	Deshabilitada	
		No sincronizar aplicaciones de Windows	Habilitada	
		Sincronizar configuración en conexiones de uso medido	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Sincronizar configuración en conexiones de uso medido incluso si son móviles	Deshabilitada	
		Usar User Experience Virtualization (UE-V)	Deshabilitada	
158.GPO: Verifique los valores de Windows Messenger.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Windows Messenger”		
		Directiva	Valor	OK/NOK
		No ejecutar automáticamente Windows Messenger al inicio	Habilitada	
		No permitir que se ejecute Windows Messenger	Habilitada	
159.GPO: Verifique los valores de Windows Update.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Windows Update”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Quitar el acceso a todas las características de Windows Update	Habilitada, (0 – No mostrar ninguna notificación)	
160.GPO: Verifique los valores del menú Inicio y barra de tareas.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Menú Inicio y barra de tareas”		
		Directiva	Valor	OK/NOK
		Borrar historial de los documentos abiertos recientemente al salir	Habilitada	
		Borrar lista de programas recientes para nuevos usuarios	Habilitada	
		No guardar historial de documentos abiertos recientemente.	Habilitada	
		Quitar vínculos y accesos a Windows Update	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
161.GPO: Verifique los valores del Panel de Control.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Panel de Control”		
		Directiva	Valor	OK/NOK
		Abrir siempre Todos los elementos del Panel de control al abrir el Panel de control	Habilitada	
162.GPO: Verifique los valores de las impresoras.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Panel de Control → Impresoras”		
		Directiva	Valor	OK/NOK
		Impedir la adición de impresoras	Habilitada	
		Impedir la eliminación de impresoras	Habilitada	
163.Verifique los valores de personalización.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Panel de Control → Programas”		
		Directiva	Valor	OK/NOK
		Ocultar "Características de Windows"	Deshabilitada	
164.GPO: Verifique los valores de archivos sin conexión a la red.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Red → Archivos sin conexión”		
		Directiva	Valor	OK/NOK
		Especificar Archivos sin conexión asignados de forma administrativa	Deshabilitada	
		Quitar el comando “Disponible sin conexión”	Habilitada	
		Quitar el comando “Trabajar sin conexión”	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
165.Verifique los valores de Windows Connect Now.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Red → Windows Connect Now”		
		Directiva	Valor	OK/NOK
		Prohibir el acceso a los asistentes de Windows Connect Now	Habilitada	
166.GPO: Verifique los valores de sistema.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema”		
		Directiva	Valor	OK/NOK
		Descargar componentes COM que faltan	Deshabilitada	
		Impedir el acceso a herramientas de edición del Registro	Habilitada, No (¿Desea deshabilitar la ejecución sin notificación de regedit?)	
		Impedir el acceso al símbolo del sistema	Habilitada, No (¿Desea desactivar también el procesamiento de scripts del símbolo del sistema?)	
167.GPO: Verifique los valores de acceso de almacenamiento extraíble.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble”		
		Directiva	Valor	OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
168.GPO: Verifique los valores de administración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Administración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Restringir comunicación de Internet	Habilitada	
169.GPO: Verifique los valores de configuración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Desactivar clasificaciones de la ayuda	Habilitada	
		Desactivar descargas de Internet de los asistentes para la publicación en Web y pedidos en línea	Habilitada	
		Desactivar el programa de mejora de la Ayuda	Habilitada	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger	Habilitada	
		Desactivar impresión a través de HTTP	Habilitada	
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitada	
		Desactivar la descarga de controladores de impresión a través de HTTP	Habilitada	
		Desactivar la tarea “Publicar en Web” para archivos y carpetas	Habilitada	
		Desactivar la tarea de imágenes "Pedir copias fotográficas"	Habilitada	
		Desactivar uso compartido de datos de personalización de escritura a mano	Habilitada	
		Desactivar Windows Online	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
170.GPO: Verifique los valores de Ctrl+Alt+Supr.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Opciones de Ctrl+Alt+Supr”		
		Directiva	Valor	OK/NOK
		Quitar Administrador de tareas	Habilitada	
171.Verifique los valores de Servicios de configuración regional.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Sistema → Servicios de configuración regional”		
		Directiva	Valor	OK/NOK
		Denegar el cambio de ubicación geográfica	Habilitada	
172.Realice la comprobación de los valores de Internet Explorer 11.		Compruebe los valores de la lista de comprobación de la guía “CCN-STIC-520 Internet Explorer 11” para verificar la correcta configuración de dicho componente.		
173.Borre “C:\Scripts”.		Borre el directorio “C:\Scripts” con todo su contenido.		
174.Reinicie el equipo.		Reinicie el equipo que está comprobando. De esta manera volverán a aplicarse las restricciones sobre las consolas de administración y el equipo quedará en el mismo estado en el que estaba antes de realizar la lista de comprobación.		

ANEXO B.2. APLICACIÓN DE NIVELES DE CLASIFICACIÓN

Este Anexo define el procedimiento a seguir para realizar una configuración específica para el sistema operativo Microsoft Windows 10 (versión 1809) Enterprise LTSC en función del nivel de clasificación asignado al equipo según la normativa legal vigente que regula el uso de la información clasificada en equipos informáticos. Los niveles de clasificación disponibles para su aplicación a través de esta guía son los siguientes:

- a) CONFIDENCIAL.
- b) RESERVADO O SUPERIOR.

Antes de proceder a realizar la configuración, deberá conocer el nivel de clasificación del equipo que está securizando con el objeto de aplicar la configuración de seguridad adecuada.

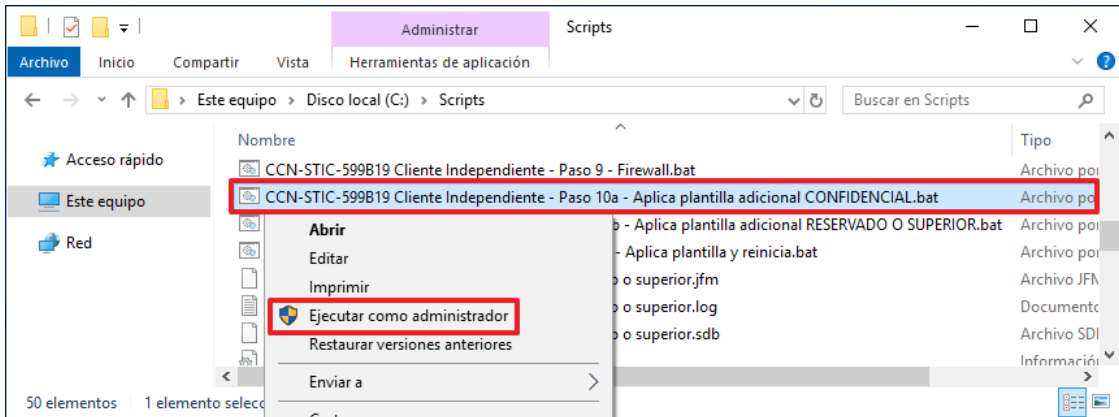
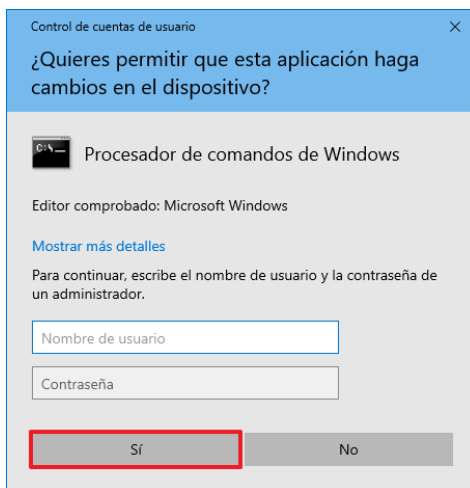
Nota: Si el nivel de clasificación del equipo no se encuentra en el listado de opciones indicadas, deberá establecer la configuración equivalente o superior.

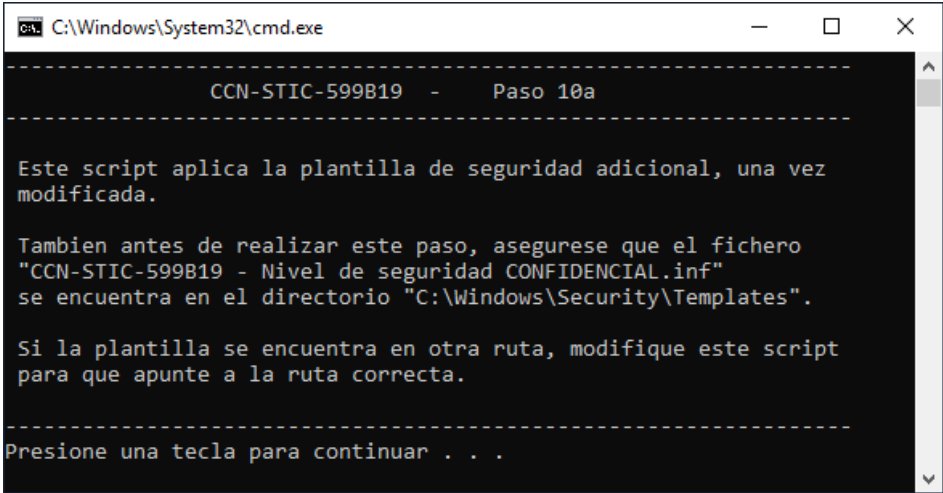
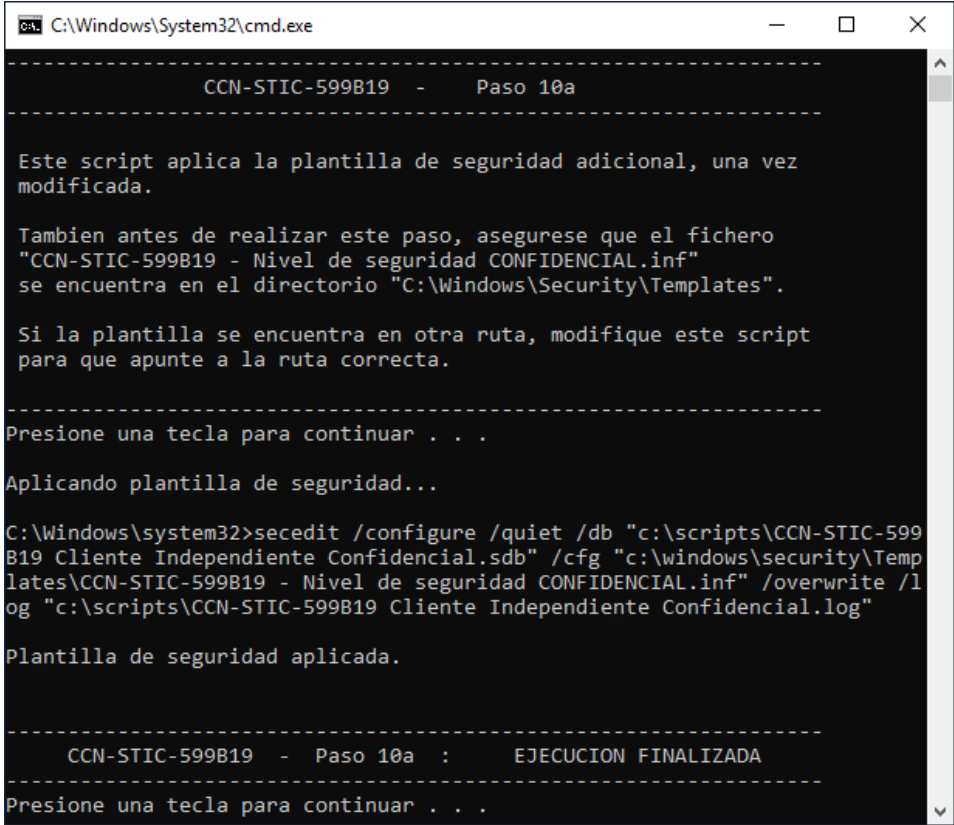
Los siguientes pasos permiten aplicar la configuración del nivel de clasificación correspondiente.

ANEXO B.2.1. NIVEL DE CLASIFICACIÓN CONFIDENCIAL

Los siguientes pasos establecen el procedimiento para establecer la configuración para un entorno de nivel de clasificación "CONFIDENCIAL".

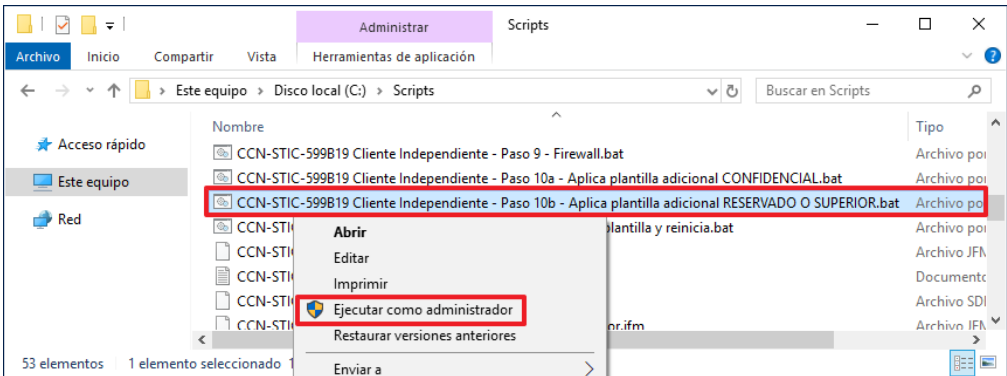
Paso	Descripción
1.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador.
2.	Copie los ficheros que acompañan a esta guía en el directorio "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19". Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Se le solicitará elevación de privilegios para realizar la operación.
3.	Localice en el directorio "C:\Scripts" los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf – CCN-STIC-599B19 Cliente Independiente - Paso 10a - Aplica plantilla adicional CONFIDENCIAL.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat

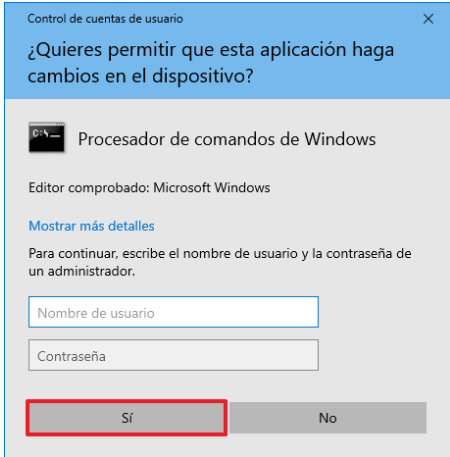
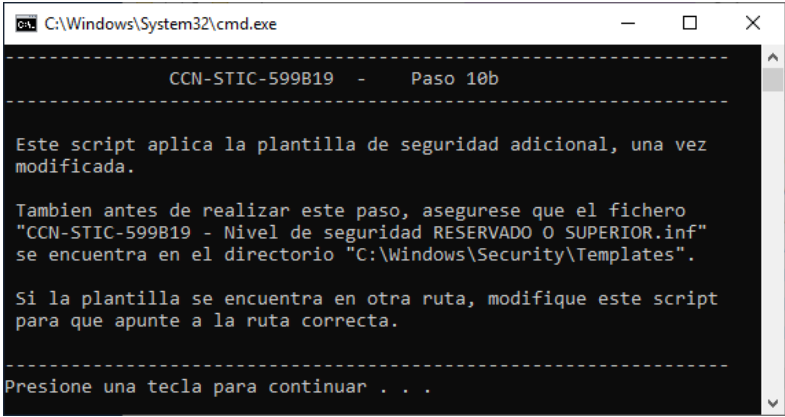
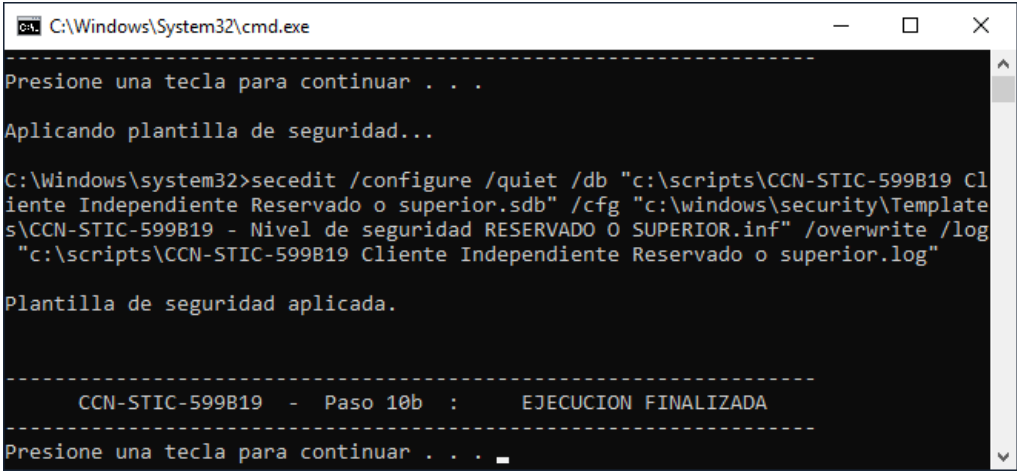
Paso	Descripción
4.	Asegúrese que en el directorio “C:\Windows\Security\Templates” están copiados al menos los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf En caso de no estar cópielos desde el directorio “C:\Scripts”. Nota: Estos ficheros deben estar en la ubicación correcta ya que durante la aplicación de la guía se copian de manera automática. En caso contrario cópielos manualmente.
5.	Acceda al directorio “C:\Scripts” y ejecute con permisos de administrador, opción “Ejecutar como administrador” el fichero “CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional CONFIDENCIAL.bat”. 
6.	El control de cuentas de usuarios le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local del equipo y pulse “Sí”. 

Paso	Descripción
7.	Se lanzará el script. Pulse cualquier tecla para comenzar la ejecución del script. 
8.	Espera a que finalice y pulse de nuevo una tecla para finalizar la ejecución. 
9.	A partir de este momento habrá quedado configurado el equipo con un nivel de clasificación "CONFIDENCIAL".
10.	Borre la carpeta "C:\Scripts" de su sistema.

ANEXO B.2.2. NIVEL DE CLASIFICACIÓN RESERVADO O SUPERIOR

Los siguientes pasos establecen el procedimiento para establecer la configuración para un entorno de nivel de clasificación “RESERVADO O SUPERIOR”.

Paso	Descripción
1.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Se le solicitará elevación de privilegios para realizar la operación.
3.	Localice en el directorio “C:\Scripts” los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf – CCN-STIC-599B19 Cliente Independiente - Paso 10a - Aplica plantilla adicional CONFIDENCIAL.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat
4.	Asegúrese que en el directorio “C:\Windows\Security\Templates” están copiados al menos los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf En caso de no estar cópielos desde el directorio “C:\Scripts”. Nota: Estos ficheros deben estar en la ubicación correcta ya que durante la aplicación de la guía se copian de manera automática. En caso contrario cópielos manualmente.
5.	Acceda al directorio “C:\Scripts” y ejecute con permisos de administrador, opción “Ejecutar como administrador” el fichero “CCN-STIC-599B19 Cliente Independiente - Paso 10c - Aplica plantilla adicional RESERVADO O SUPERIOR.bat”. 

Paso	Descripción
6.	El control de cuentas de usuarios le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local del equipo y pulse “Sí”. 
7.	Se lanzará el script. Pulse cualquier tecla para comenzar la ejecución del script. 
8.	Espere a que finalice y pulse de nuevo una tecla para finalizar la ejecución. 
9.	A partir de este momento habrá quedado configurado el equipo con un nivel de clasificación “RESERVADO O SUPERIOR”.
10.	Borre la carpeta “C:\Scripts” de su sistema.

ANEXO B.3. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO B.3.1. CIFRADO DE DISCO CON BITLOCKER

Este anexo se ha diseñado para ayudar a los operadores a implementar la configuración del cifrado de disco con BitLocker en un equipo cliente Windows 10 (versión 1809) Enterprise LTSC, independiente de un dominio.

BitLocker contribuye a la protección de datos en equipos cliente proporcionando el cifrado completo de un volumen de disco y la comprobación de la integridad de los componentes básicos durante el arranque del sistema. También ofrece la opción de bloquear el proceso normal de arranque hasta que el usuario proporcione un número de identificación personal (PIN, Personal Identification Number) o inserte una unidad flash USB con las claves de descifrado correctas.

Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números. Por tanto, se puede pensar en el PIN más como una "frase de paso" que como un "número".

El nivel de protección óptimo se obtiene cuando el equipo dispone de un Módulo de plataforma segura (TPM, del inglés Trusted Platform Module, Windows 10 soporta este módulo desde su versión 1.2 en adelante) para proteger los datos del usuario y reducir las posibilidades de manipulación del equipo cliente con Windows 10 cuando el sistema está desconectado.

Para más información sobre el procedimiento de cifrado de unidad BitLocker, puede consultar los siguientes enlaces:

[http://technet.microsoft.com/es-es/library/dd835565\(Ws.10\).aspx](http://technet.microsoft.com/es-es/library/dd835565(Ws.10).aspx)

<https://blogs.msdn.microsoft.com/mvpawardprogram/2016/01/12/securing-windows-10-with-bitlocker-drive-encryption/>

1. ALCANCE

Este anexo se ha elaborado para proporcionar información sobre cómo implementar la configuración del cifrado de disco con BitLocker sobre la unidad del sistema operativo, en el escenario con modo de autenticación en la secuencia de arranque mediante Módulo de plataforma segura (TPM 1.2) y número de identificación personal (PIN). Aunque existen otros escenarios de configuración del cifrado de disco con BitLocker, como por ejemplo sin uso de TPM, o cifrado de otras unidades lógicas, fijas o extraíbles, estos escenarios no se contemplan para el uso de esta guía.

Las copias de seguridad de la clave de BitLocker se realizarán sobre un dispositivo de memoria USB que posteriormente se almacenará en algún lugar seguro, como una caja de seguridad. Del mismo modo, aunque existen otros escenarios de almacenamiento de claves, como por ejemplo en Active Directory, éstos no se contemplan para el uso de esta guía.

El uso del dispositivo TPM a partir de la versión 1607 es controlado por el sistema operativo de modo que no es necesaria la administración del mismo. Para más información acerca de este echo consulte el siguiente enlace:

<https://docs.microsoft.com/es-es/windows/security/hardware-protection/tpm/change-the-tpm-owner-password>

2. DESCRIPCIÓN DE USO DE ESTE ANEXO

El contenido de este anexo se aplica a equipos independientes de un dominio, con sistema operativo Windows 10 (versión 1809) Enterprise LTSC, a los cuales, tras realizar una instalación por defecto, les ha sido aplicada la presente guía.

Para la implementación del cifrado de unidad BitLocker debe tenerse en cuenta que existen requisitos a cumplir adicionales a la instalación del sistema operativo y es necesario comprobarlos antes de comenzar a aplicar este anexo.

El hardware sobre el que se ha verificado el cifrado de unidad BitLocker tiene las siguientes características:

- a) Lenovo ThinkPad 13:
 - i. Intel Core i5 7200U 2.50GHz.
 - ii. SSD 250 GB.
 - iii. 8 GB de RAM.

3. REQUISITOS HARDWARE Y SOFTWARE

La implementación del cifrado de unidad BitLocker tiene los siguientes requisitos de hardware y software:

- a) Un equipo que cumpla los requisitos mínimos para Windows 10 Enterprise LTSC.
- b) Un chip TPM, versión 1.2 o superior, activado.
- c) BIOS compatible con TCG (Trusted Computing Group).
- d) Una partición de disco para la unidad del sistema, además de la partición que contiene el sistema operativo. En Windows 10, si cuenta con una sola partición de disco, BitLocker preparará automáticamente la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema que albergará los archivos del sistema que se necesitan para iniciar o recuperar el sistema operativo y que no se pueden cifrar. Esta unidad no tendrá una letra de unidad para evitar que se almacenen archivos de datos en esta unidad por error. Una vez que la unidad está preparada, debe reiniciarse el equipo.

No obstante, si se ha realizado una instalación por defecto de Windows 10, el programa de instalación ya habrá creado, durante la instalación, las dos particiones de disco necesarias para activar BitLocker.

- e) Una unidad flash USB para almacenar claves de inicio y recuperación.
- f) Una configuración BIOS para iniciar primero desde el disco duro, y no desde las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como una clave de inicio o de recuperación), la BIOS debe admitir la lectura de unidades flash USB en el inicio.

- g) Opcionalmente, se puede disponer de una impresora conectada y configurada, para la impresión de las claves de recuperación. Alternativamente, se podrá tomar nota manualmente de las claves de recuperación.

Nota: Tenga en cuenta que el acceso a las impresoras puede estar deshabilitado, debido a la aplicación de la configuración de seguridad implementada. Recuerde que antes de realizar este paso a paso necesitará de una unidad para almacenar las claves necesarias por lo que deberá aplicar la configuración para utilizar el dispositivo de almacenamiento descrito en el “ANEXO B.3.4 DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE”.

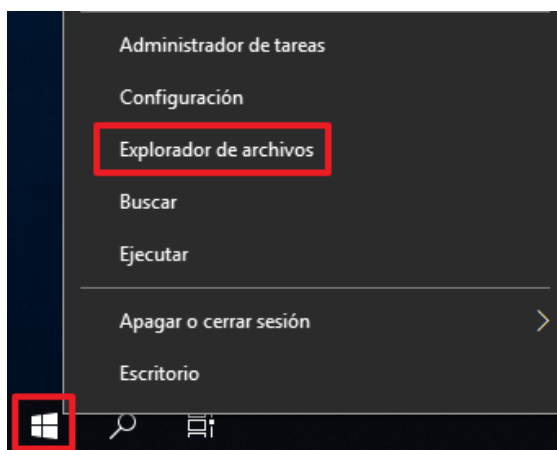
4. GUÍA PASO A PASO – BITLOCKER

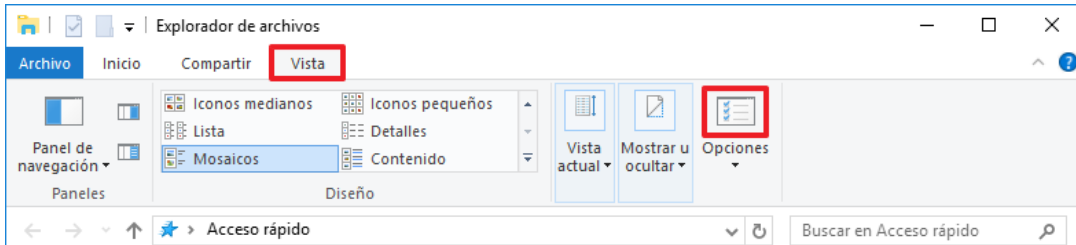
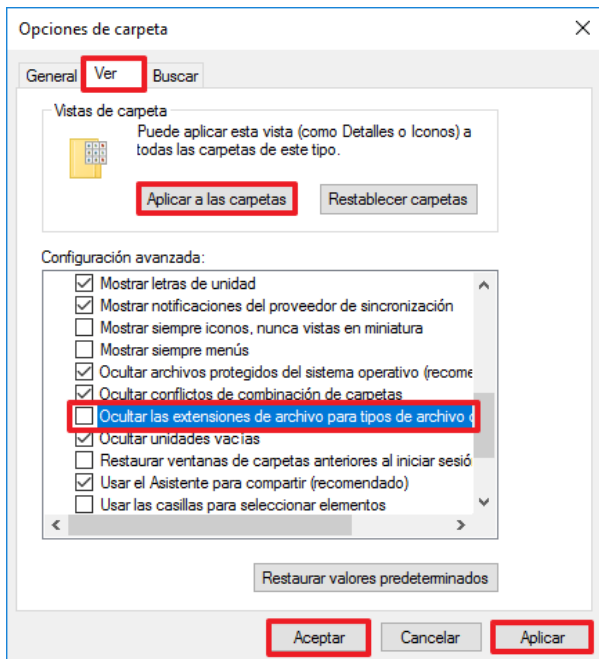
En este apartado se enumeran los pasos necesarios para implementar el cifrado de unidad BitLocker en equipos Windows 10 Enterprise LTSC.

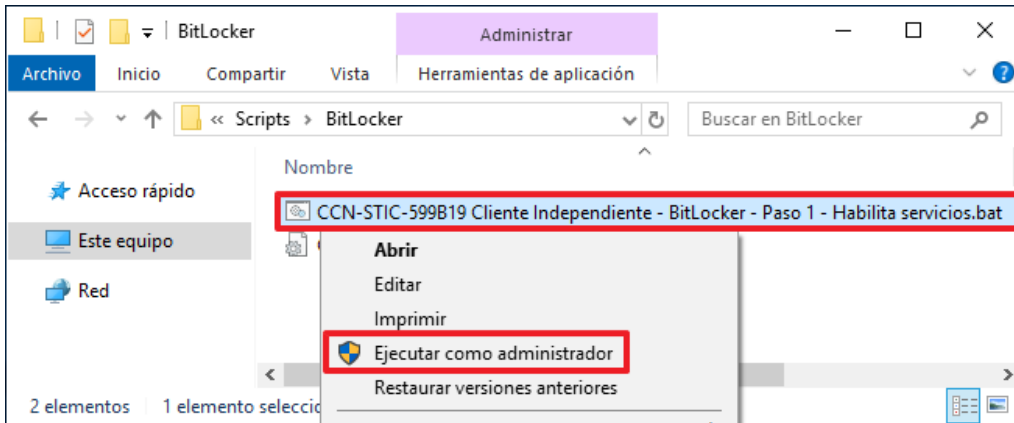
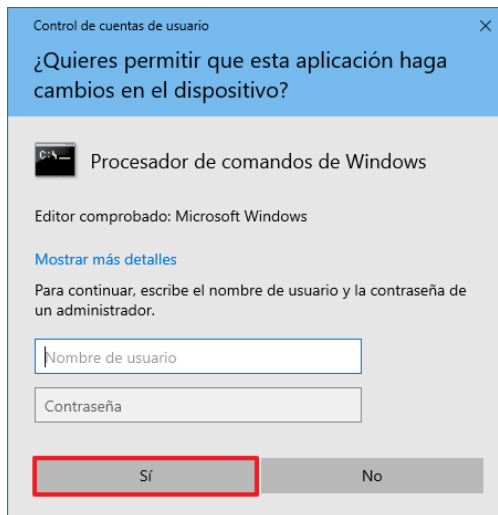
La primera parte hace referencia a las modificaciones que es necesario realizar en la configuración de seguridad aplicada hasta este punto, para implementar el cifrado de unidad BitLocker. Los siguientes pasos deberán realizarse iniciando sesión en el equipo con una cuenta de usuario perteneciente al grupo “Administradores”.

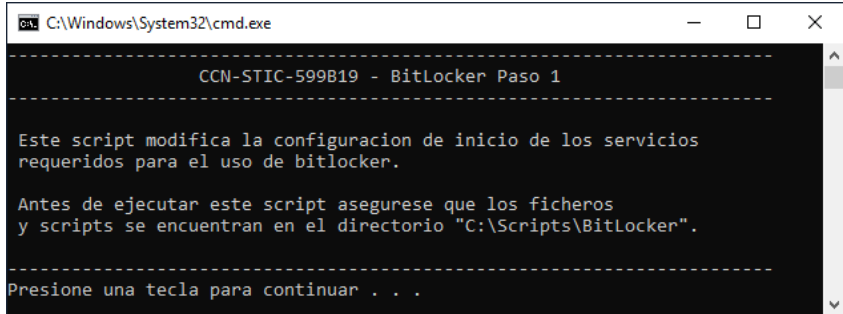
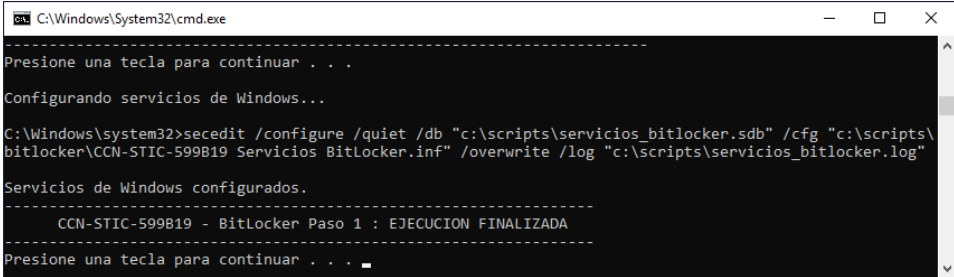
Nota: Recuerde que no podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada, debido a la aplicación de la configuración de seguridad implementada.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores”.
2.	Cree el directorio “Scripts” en la unidad “C:\”
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
4.	Si no lo hizo previamente, configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”.



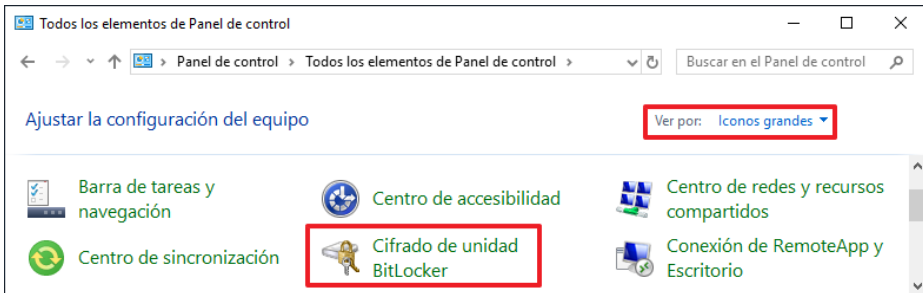
Paso	Descripción
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono “Opciones”. 
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del cliente independiente: – BitLocker (Directorio) – BitLocker\CCN-STIC-599B19 Cliente Independiente - BitLocker - Paso 1 - Habilita servicios.bat – BitLocker\CCN-STIC-599B19 Servicios BitLocker.inf

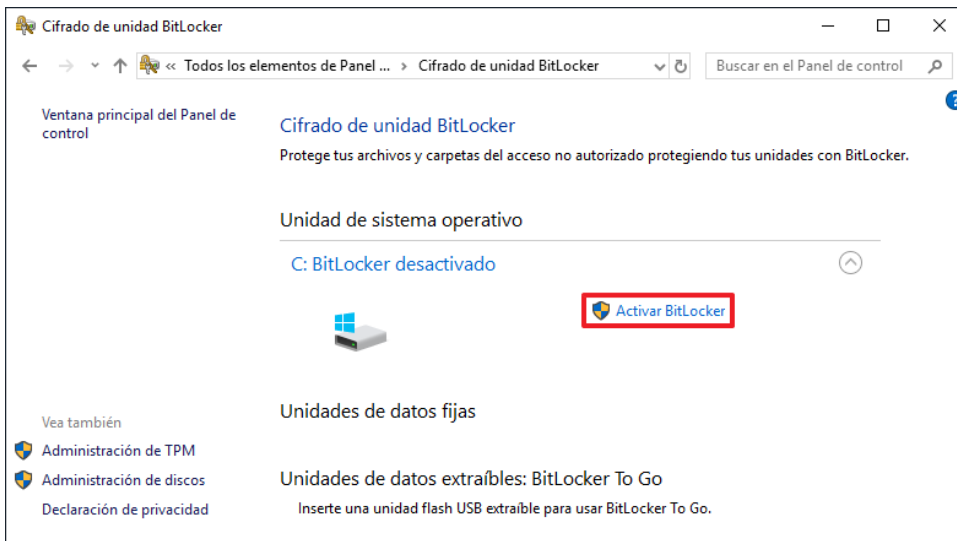
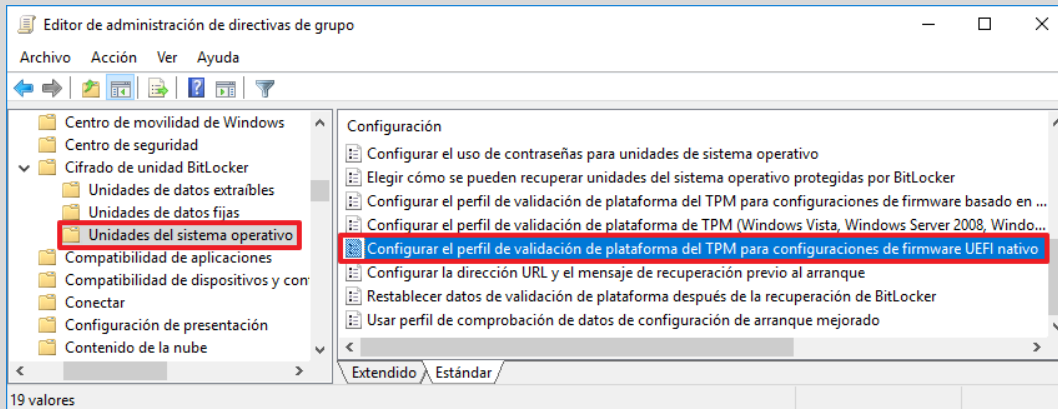
Paso	Descripción
8.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script " CCN-STIC-599B19 Cliente Independiente – BitLocker Paso 1 – Habilita servicios.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario con permisos de administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
9.	El "Control de cuentas de usuario" le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y que pertenezca al grupo "Usuarios de shells". 

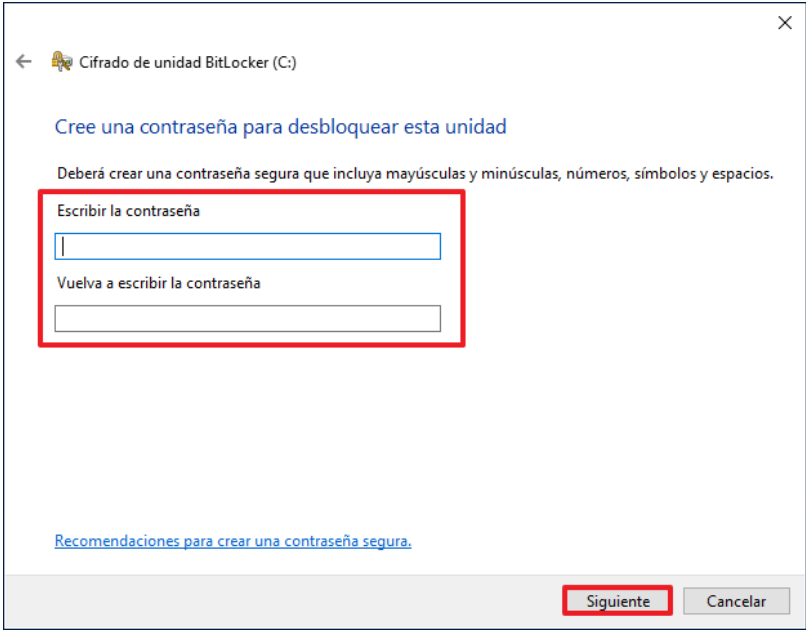
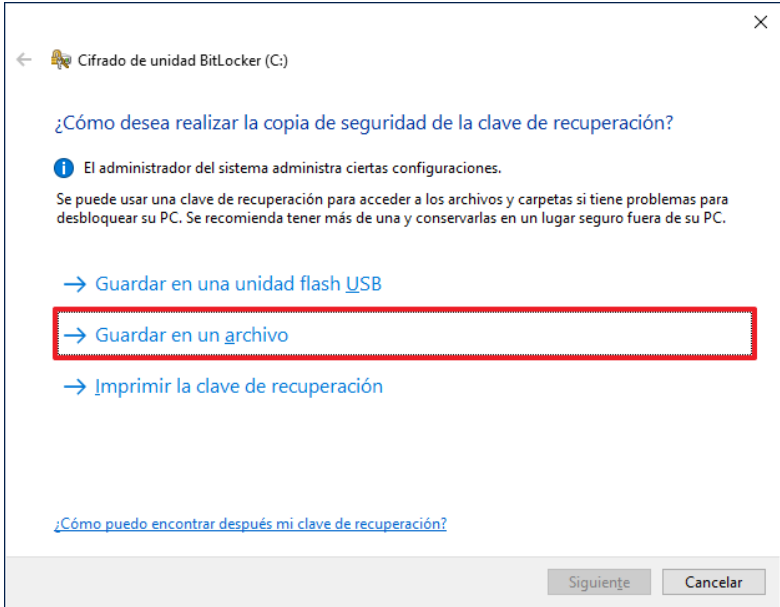
Paso	Descripción
10.	Este script, habilita y configura los servicios necesarios para el uso de BitLocker. Pulse una tecla para continuar. 
11.	Se actualizará el estado de los servicios. Pulse una tecla para cerrar la ventana. 

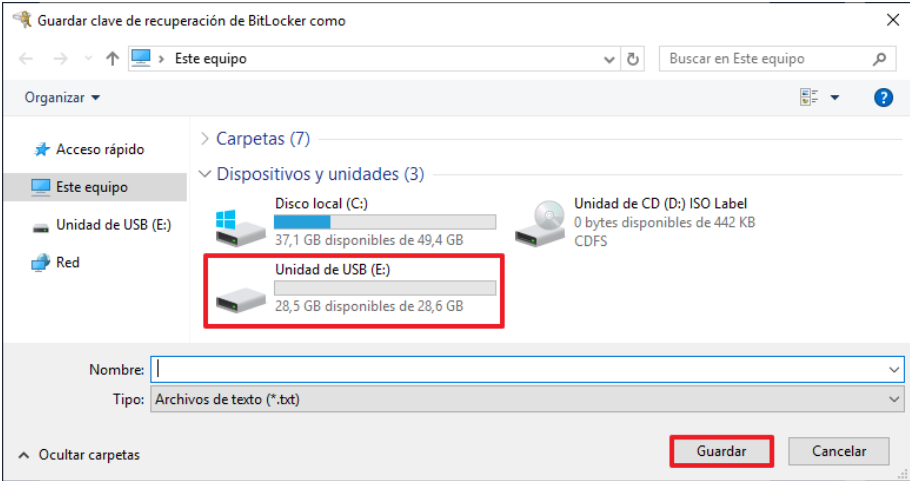
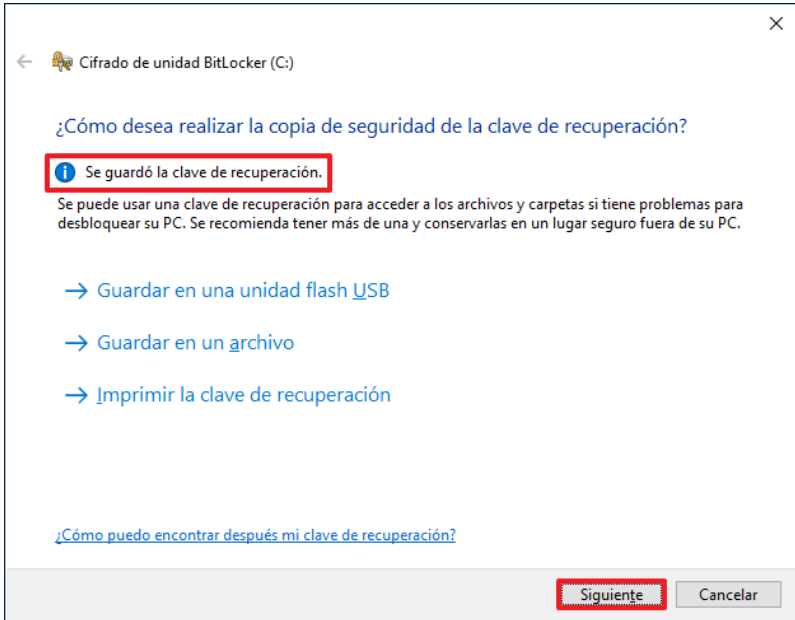
Los siguientes pasos describen el procedimiento para activar el cifrado de unidad BitLocker con PIN (número de identificación personal).

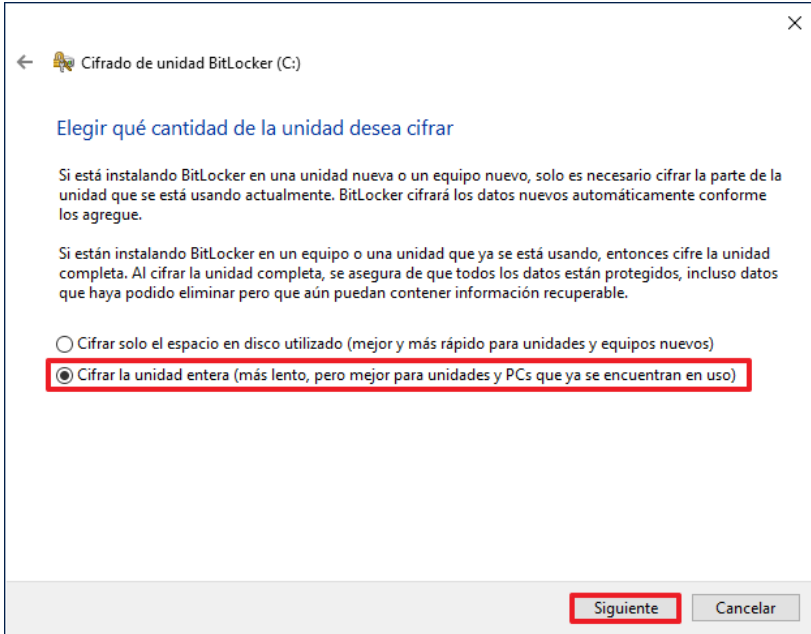
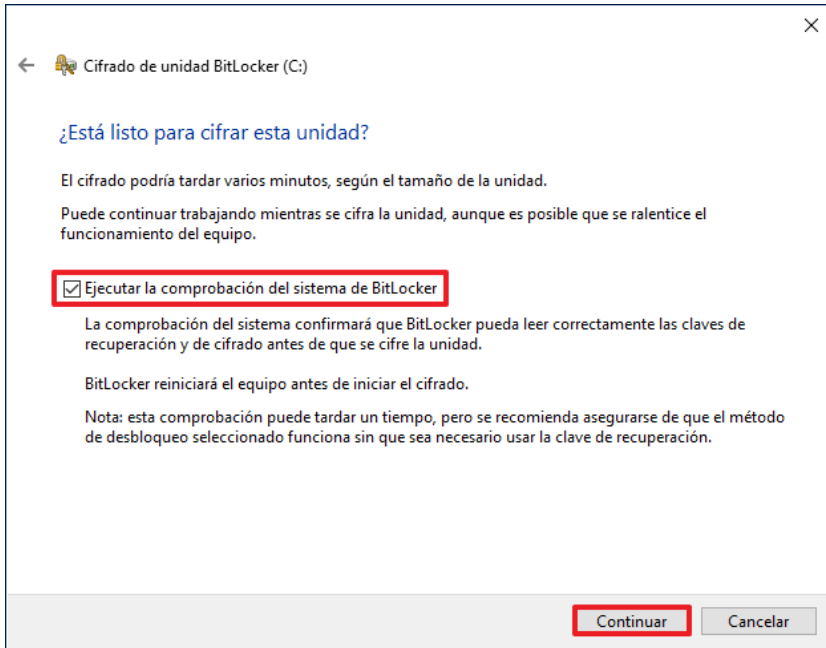
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números. Por tanto, se puede pensar en el PIN más como una "frase de paso" que como un "número".

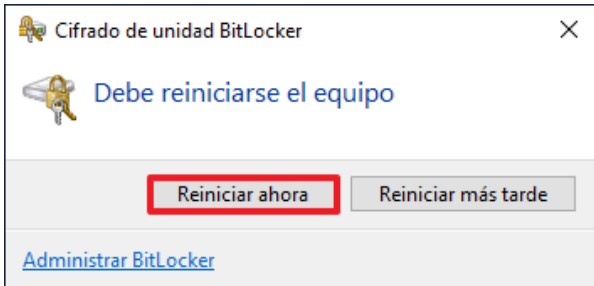
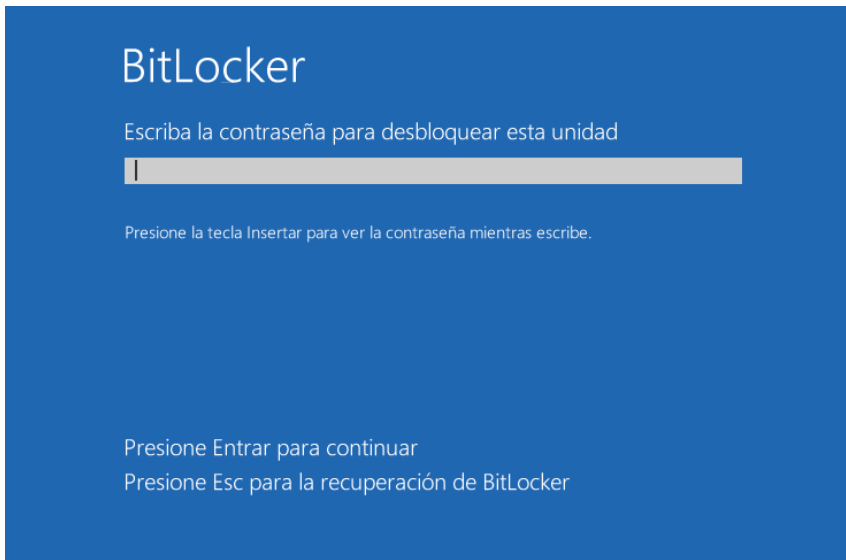
Paso	Descripción
12.	Abra la consola de administración "Cifrado de unidad BitLocker" desde el panel de control a través de la siguiente ruta: "Inicio (clic derecho sobre él) → Panel de control → Cifrado de unidad BitLocker"  Nota: Es posible que la vista de los iconos no se corresponda con la captura anterior. Para solventarlo, seleccione la opción "Iconos grandes" del desplegable "Ver por:". Ver por: Iconos grandes ▼

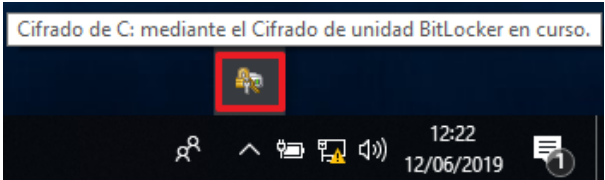
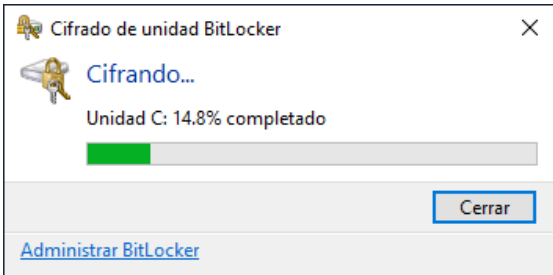
Paso	Descripción
13.	Pulse en “Activar BitLocker” como se indica en la siguiente figura.  Nota: La configuración importada durante la aplicación de la guía establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si su equipo dispone de firmware UEFI nativo, deberá habilitar y configurar la directiva “Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo”. Para ello, con el editor de directivas de grupo (gpedit.msc) diríjase a la ruta “Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo” y habilite la directiva mencionada anteriormente. 
14.	El sistema le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador en la ventana de “Control de cuentas de usuario”.

Paso	Descripción
15.	Introduzca y confirme una contraseña de inicio y pulse “Siguiente”.  Nota: Recuerde que puede utilizar entre 8 y 20 caracteres. A mayor longitud, mayor seguridad.
16.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
17.	Seleccione la ubicación de la unidad USB en la que guardará el archivo que contiene la clave.  Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD. Debe tener en consideración que esta clave, durante el proceso no puede ser almacenado sobre la misma unidad que se está cifrando ni en otra unidad que este cifrada.
18.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

Paso	Descripción
19.	Elija la opción de “Cifrar la unidad entera” y pulse “Siguiente”. 
20.	Marque la opción "Ejecutar la comprobación del sistema de BitLocker" y pulse el botón "Continuar". 

Paso	Descripción
21.	Reinicie el equipo para continuar con el proceso de cifrado de la unidad.  Nota: Si tras reiniciar el sistema aparece un mensaje como el mostrado a continuación pulse el botón “Cerrar” y repita los pasos 12 a 21, pero en este último paso pulse sobre la opción “Reiniciar más tarde” y reinicie el equipo manualmente mediante la ruta “Inicio → “Iniciar/Apagar”. 
22.	Al reiniciar, el sistema le pedirá la contraseña de cifrado de unidad BitLocker. Introduzca la contraseña y pulse “Enter” para continuar. 

Paso	Descripción
23.	Una vez reiniciado, inicie sesión de nuevo con un usuario del grupo “Administradores”. El cifrado inicial de la unidad del sistema se realizará en segundo plano. Mientras dure este proceso es posible que el tiempo de respuesta del sistema se vea afectado por la intensa actividad del disco. Una vez finalizado el proceso de cifrado inicial, el cifrado y descifrado de los datos del disco será imperceptible por el usuario. Durante el proceso puede aparecer el siguiente mensaje informativo. 
24.	Si marca con el ratón en él, o en el icono correspondiente del área de notificación, podrá visualizar la siguiente ventana mostrando el progreso de este proceso de cifrado inicial.  Continúe con los siguientes pasos, aunque no haya finalizado este proceso de cifrado inicial del disco.
25.	Desconecte la memoria USB que contiene la clave de recuperación del cifrado de BitLocker y guárdela en un lugar seguro, como una caja de seguridad. Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD.
26.	Una vez haya reiniciado el sistema, inicie sesión de nuevo con un usuario miembro del grupo “Administradores” y elimine la carpeta “C:\Scripts”. Nota: Todos los volúmenes NTFS del Sistema deberán ser cifrados con la utilidad BitLocker, una vez se haya cifrado totalmente el volumen del Sistema. Si se cambia el TPM asociado al cifrado de unidad BitLocker o si alguien intenta iniciar el equipo desde un disco para evitar el sistema operativo, el equipo cambiará al modo de recuperación hasta que se suministre la clave de recuperación. Si se pierde el PIN, se puede cambiar al modo de recuperación para iniciar el equipo e introducir la clave de recuperación. Para más información sobre el procedimiento de cifrado de unidad BitLocker, puede consultar el siguiente enlace: https://support.microsoft.com/es-es/help/4028713/windows-10-turn-on-device-encryption

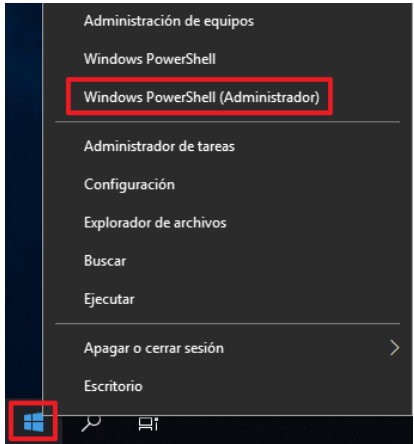
5. LISTA DE COMPROBACIÓN – BITLOCKER

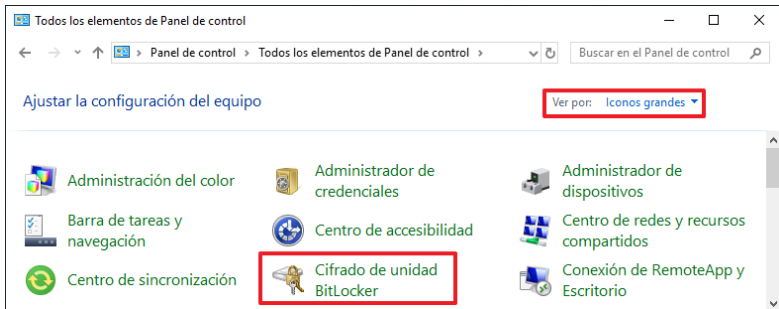
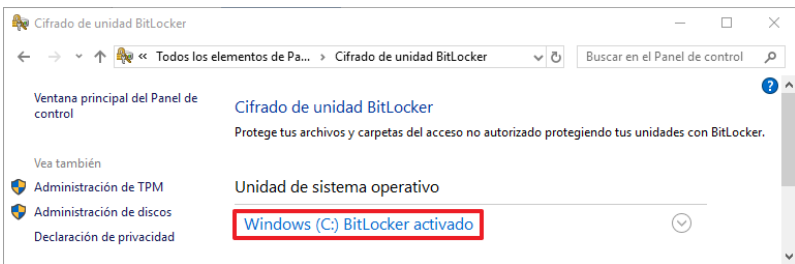
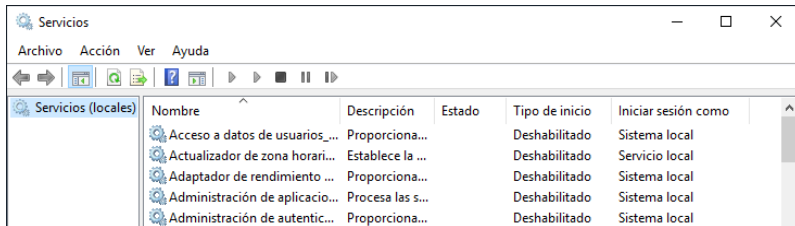
Este anexo se ha diseñado para ayudar a los operadores a verificar que se ha implementado el cifrado de unidad BitLocker en un equipo cliente Windows 10 (versión 1809) Enterprise LTSC independiente de un dominio. La lista de comprobación deberá ejecutarse iniciando sesión en el equipo propio cliente con la cuenta de un usuario miembro del grupo "Administradores" y que sea miembro también del grupo "Usuarios de shells".

Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada, debido a la aplicación de la configuración de seguridad.

Para realizar algunas de las comprobaciones será necesario ejecutar diferentes consolas de administración y herramientas del sistema. Estas herramientas estarán disponibles si no se ha prohibido la utilización de las mismas. Uno de los primeros pasos, por tanto, consistirá en habilitar temporalmente el acceso a ellas. Las consolas y herramientas que se utilizarán son las siguientes:

- Explorador de Windows (explorer.exe)
- Administración de servicios (services.msc)

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo cliente que está comprobando.		Inicie sesión en el equipo cliente que está comprobando con una cuenta de usuario que pertenezca al grupo local "Administradores" y al grupo local "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.
2. Lance una ventana de Powershell con permisos de administrador, para lanzar desde ella en pasos posteriores comandos con permisos de administrador		Haga clic con el botón derecho en el menú de inicio y seleccione "Windows PowerShell (Administrador)".  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario. Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.

Comprobación	OK/NOK	Cómo hacerlo
3. Compruebe que el volumen del sistema operativo está cifrado		Abra la consola de administración "Cifrado de unidad BitLocker". Para ello, ejecute en la ventana de PowerShell el comando "control.exe" y localice "Cifrado de unidad BitLocker".  Compruebe que junto a la letra de unidad del volumen del sistema operativo aparece el estado "Activado", como se muestra en la siguiente figura.  Nota: Si en lugar de "Activado" el estado que aparece es "Cifrar", eso significa que el cifrado inicial del disco todavía está en marcha. Repita la comprobación más tarde, cuando haya finalizado. Puede comprobar el progreso del proceso de cifrado haciendo doble clic en el icono de BitLocker que estará presente en el área de notificación de la barra de tareas durante todo el proceso de cifrado inicial del disco. Cierre la ventana "Cifrado de unidad BitLocker".
4. Compruebe que se han configurado correctamente los servicios relacionados con BitLocker y TPM		Desde la ventana de Powershell abierta anteriormente, ejecute "services.msc". A continuación, se abrirá la consola de "Servicios del sistema".  Compruebe que el tipo de inicio configurado para cada servicio coincide con el mostrado en la siguiente tabla:



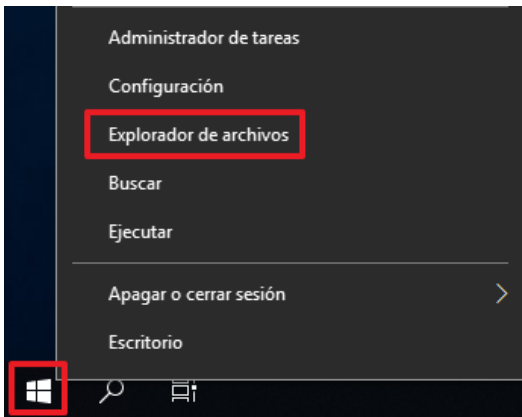
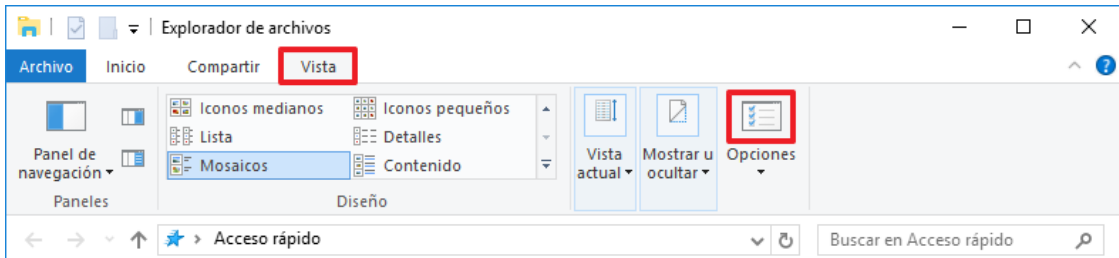
Comprobación	OK/NOK	Cómo hacerlo		
		Servicio	Inicio	OK/NOK
		Servicio Cifrado de unidad BitLocker (bdesvc)	Automático	
		Detección de hardware Shell (shellhwdetection)	Automático	
		Cierre la consola de administración de servicios.		
5. Borre el directorio "C:\Scripts"		Borre el directorio "C:\Scripts" con todo su contenido.		
6. Reinicie el equipo		Reinicie el equipo para comprobar que BitLocker solicita la contraseña para acceder a la unidad de sistema.		
7. Compruebe que el sistema tiene configurado cifrado de unidad BitLocker con la opción de PIN de arranque.		Reinicie el equipo. Compruebe que el sistema requiere que se introduzca la contraseña para desbloquear la unidad, como se muestra en la siguiente figura.		
8. Compruebe que la memoria USB y el listado de contraseñas están almacenados en lugar seguro		Solicite la memoria USB y los listados donde se encuentran almacenadas la contraseña de recuperación de cifrado BitLocker. Debe verificar si éstos se encontraban en una caja de seguridad.		

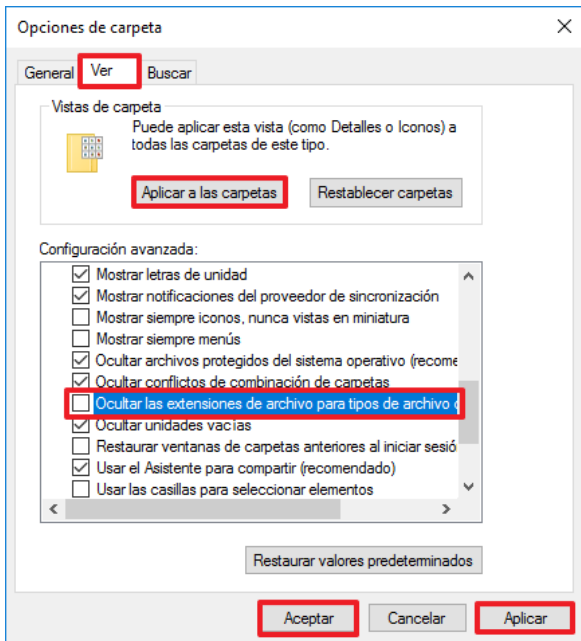
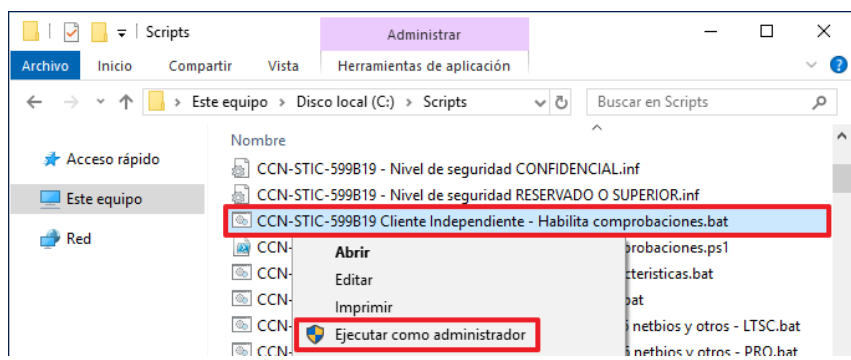
ANEXO B.3.2. USO DE DIFERENTES CONSOLAS DE ADMINISTRACIÓN TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19

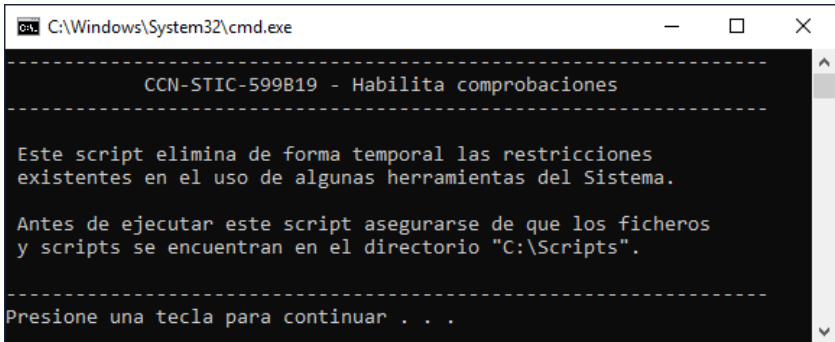
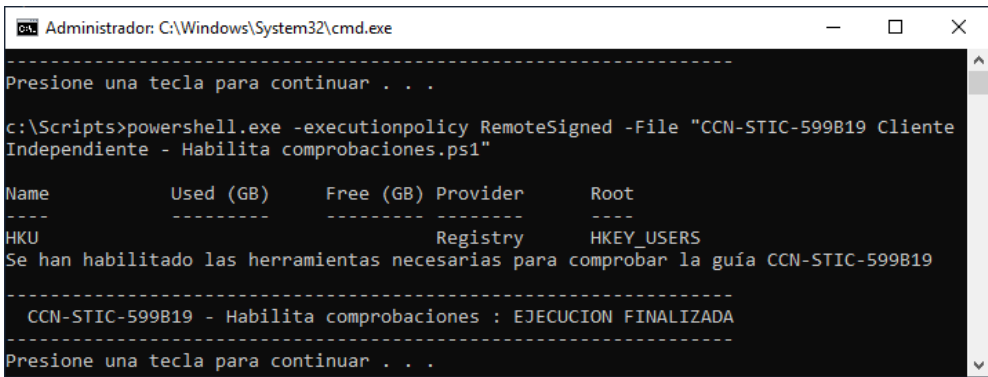
La aplicación de la presente guía conlleva el bloqueo de algunas consolas administrativas, así como el acceso a ciertas características. En el caso de experimentar problemas para acceder a los diferentes componentes de administración de la Consola de Administración de Microsoft (mmc.exe) tales como el "Editor de Directivas de grupo local" (gpedit.msc) o el "Visor de eventos" (eventvwr.msc), puede utilizar el conjunto de scripts facilitados junto con la presente guía, así como seguir los pasos recogidos en el presente anexo.

Del mismo modo, existen otra serie de características deshabilitadas por la guía que, del mismo modo, podrían ser habilitadas temporalmente para realizar tareas administrativas. Un ejemplo de esto sería el hecho de que, tras aplicar la presente guía, en las propiedades de los contenedores y ficheros del “Explorador de archivos”, la pestaña “Seguridad” no aparece.

Este documento recoge el conjunto de pasos necesarios para, de una forma temporal, habilitar consolas y opciones administrativas que, de otro modo, no podrían ser configuradas tras haber aplicado la guía “CCN-STIC-599B19 Windows 10 – Cliente Independiente”.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
4.	Si no lo hizo previamente, configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono “Opciones”. 

Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del cliente independiente: – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.ps1
8.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.bat" desde el directorio “C:\Scripts”.  Nota: El sistema le solicitará elevación de privilegios.

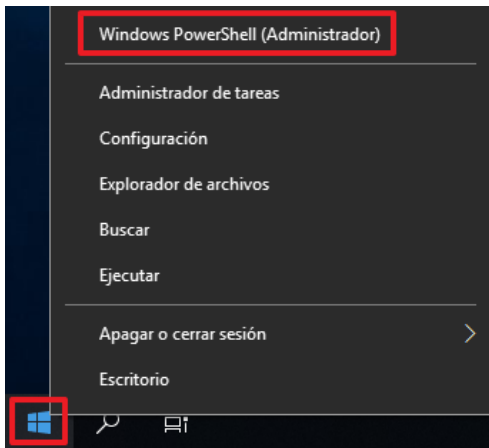
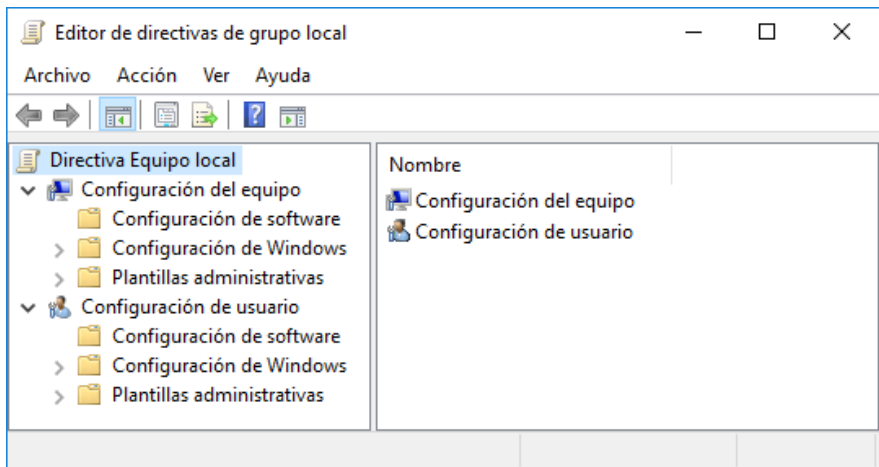
Paso	Descripción
9.	Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá la siguiente ventana. Pulse una tecla para continuar. 
10.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: En caso de que el sistema muestre errores puede ignorarlos. A partir de este momento, las consolas y características de administración bloqueadas por la presente guía vuelven a ser operativas de forma temporal.
11.	Borre el directorio "C:\Scripts".
12.	Una vez haya terminado con las labores de administración, reinicie el equipo o fuerce la aplicación de las directivas de grupo local para que vuelvan a entrar en vigor las políticas de seguridad correctas y definidas por la presente guía.

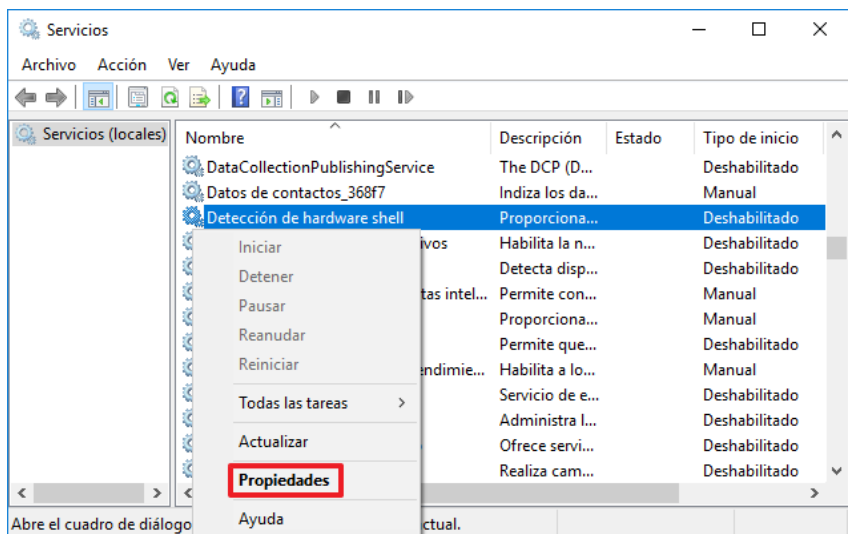
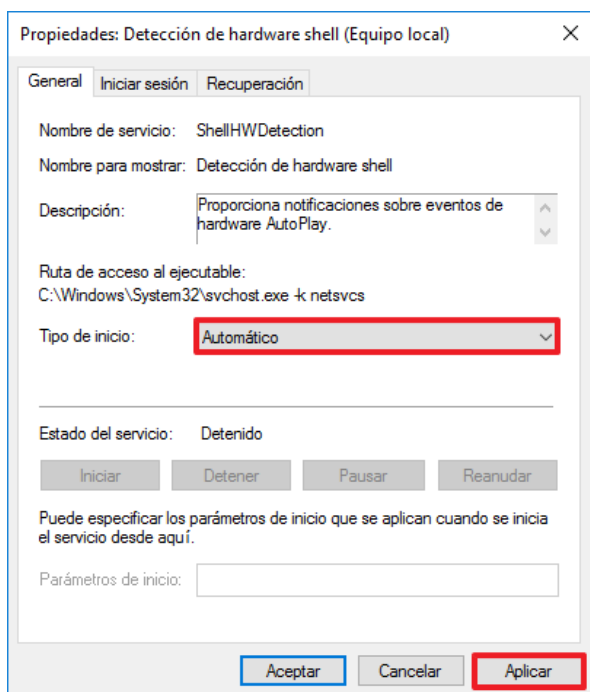
ANEXO B.3.3. USO DE GRABADORA DE CD/DVD TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE

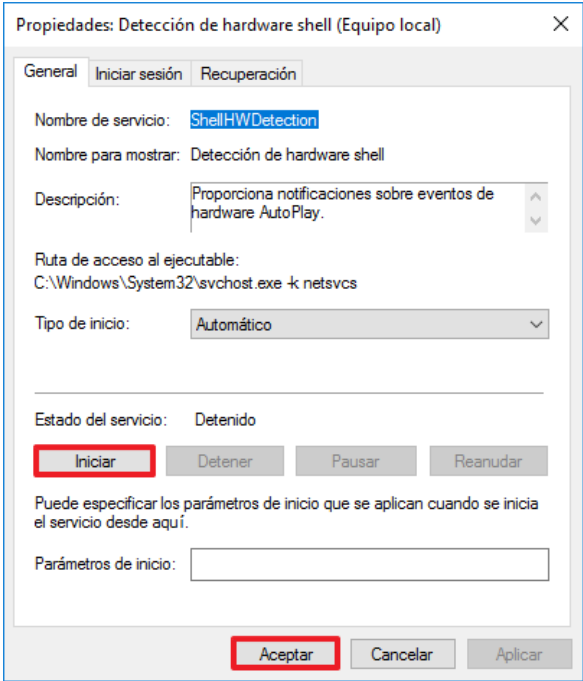
La aplicación de la presente guía conlleva el bloqueo del uso de la grabadora de CD/DVD como herramienta de grabación, transformándose en un lector de CD/DVD y perdiendo el resto de su funcionalidad.

Este documento recoge el conjunto de pasos necesarios para habilitar una serie de directivas y servicios que permitirán hacer uso de la grabadora de CD/DVD con toda su funcionalidad.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo "Administradores" y del grupo "Usuarios de shells".

Paso	Descripción												
2.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 												
3.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local.												
4.	En la ventana de Powershell ejecute "gpedit.msc". Esto abrirá una ventana del Editor de directivas de grupo local, como la mostrada en la siguiente figura. 												
5.	Modifique los valores de equipo para que coincidan con los valores indicados en la tabla mediante la siguiente ruta: “Directiva de Equipo → Configuración del equipo → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble” <table><tr><th>Directiva</th><th>Valor establecido</th><th>Valor a establecer</th></tr><tr><td>CD y DVD: denegar acceso de ejecución</td><td>No configurada</td><td>Deshabilitada</td></tr><tr><td>CD y DVD: denegar acceso de lectura</td><td>No configurada</td><td>Deshabilitada</td></tr><tr><td>CD y DVD: denegar acceso de escritura</td><td>No configurada</td><td>Deshabilitada</td></tr></table>	Directiva	Valor establecido	Valor a establecer	CD y DVD: denegar acceso de ejecución	No configurada	Deshabilitada	CD y DVD: denegar acceso de lectura	No configurada	Deshabilitada	CD y DVD: denegar acceso de escritura	No configurada	Deshabilitada
Directiva	Valor establecido	Valor a establecer											
CD y DVD: denegar acceso de ejecución	No configurada	Deshabilitada											
CD y DVD: denegar acceso de lectura	No configurada	Deshabilitada											
CD y DVD: denegar acceso de escritura	No configurada	Deshabilitada											

Paso	Descripción						
6.	Modifique los valores de usuario indicados en la tabla mediante la siguiente ruta: “Directiva de Equipo → Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Archivos” <table><thead><tr><th>Directiva</th><th>Valor establecido</th><th>Valor a establecer</th></tr></thead><tbody><tr><td>Quitar las características de grabación de CD</td><td>Habilitada</td><td>Deshabilitada</td></tr></tbody></table>	Directiva	Valor establecido	Valor a establecer	Quitar las características de grabación de CD	Habilitada	Deshabilitada
Directiva	Valor establecido	Valor a establecer					
Quitar las características de grabación de CD	Habilitada	Deshabilitada					
7.	Modifique el modo de inicio del servicio “Detección de hardware Shell” (Deshabilitado). Para ello y desde la misma consola de PowerShell, ejecute el comando “services.msc” del mismo modo que ejecutó “gpedit.msc” en pasos anteriores. Haga clic derecho sobre el servicio y seleccione “Propiedades”. 						
8.	En el menú de “Propiedades: Detección de hardware shell (Equipo local)”, en el campo “Tipo de inicio” seleccione la opción “Automático” y pulse sobre el botón “Aplicar”. 						

Paso	Descripción
9.	Pulse sobre el botón “Iniciar” y cuando el estado del servicio sea “Iniciado”, pulse sobre el botón “Aceptar”. 
10.	Borre el directorio “C:\Scripts”. A partir de este momento, será posible hacer uso de la grabadora de CD/DVD con todas sus funciones.

ANEXO B.3.4. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE

Este documento recoge el conjunto de pasos necesarios para activar el uso e instalación de dispositivos USB de almacenamiento en sistemas securizados mediante la aplicación de la guía CCN-STIC-599B19 Windows 10 – Cliente Independiente.

Existen dos métodos para permitir el uso de dispositivos conectados mediante USB:

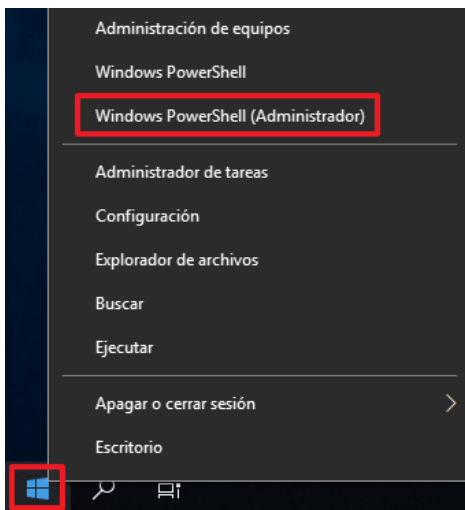
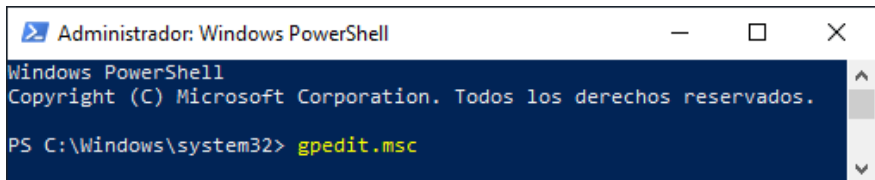
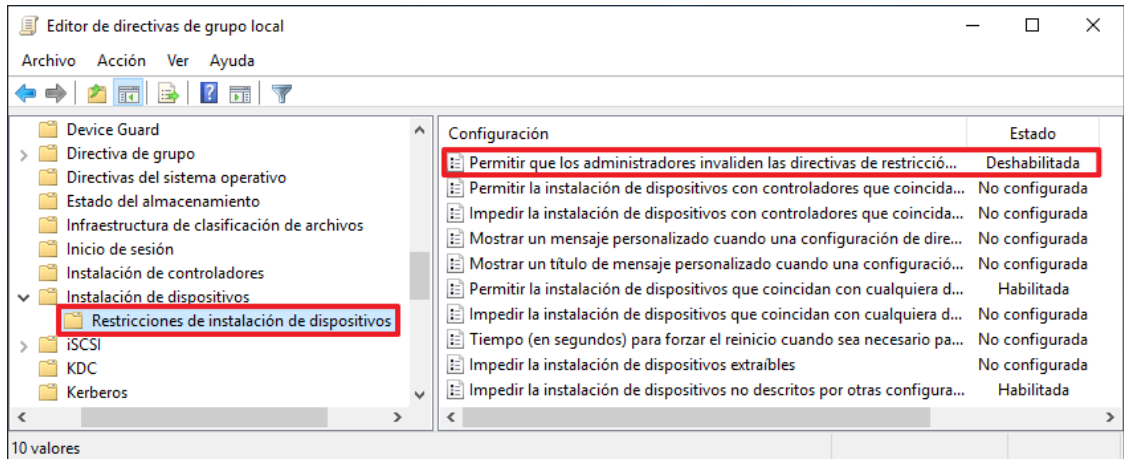
- Instalación de controladores mediante el uso de un usuario administrador de la máquina.
- Filtrado de USB mediante el uso de los identificadores de dispositivo USB.

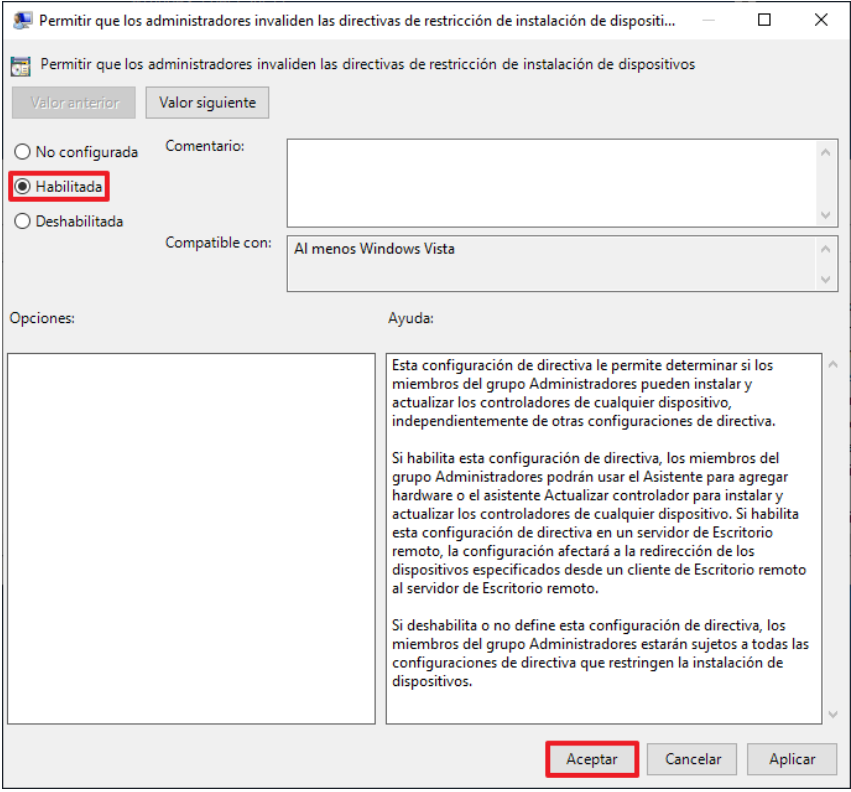
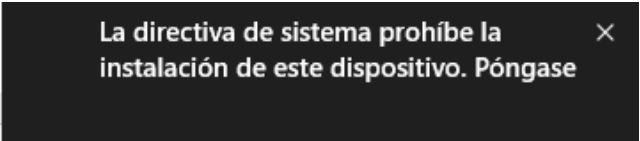
1. ADMINISTRAR DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES

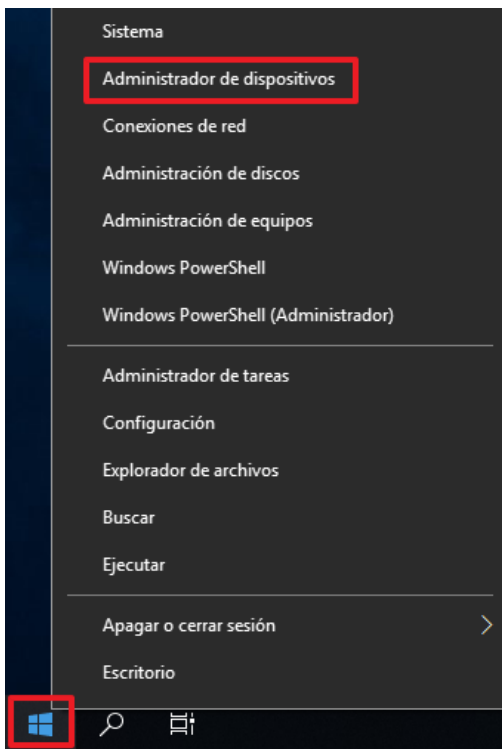
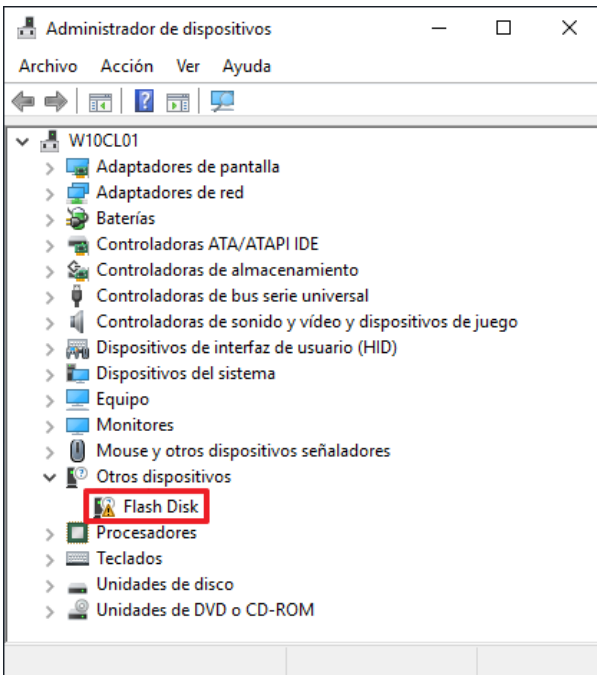
Este punto describe el proceso para instalar y desinstalar el controlador de un dispositivo USB a través de una cuenta que posea privilegios de administrador local de la máquina.

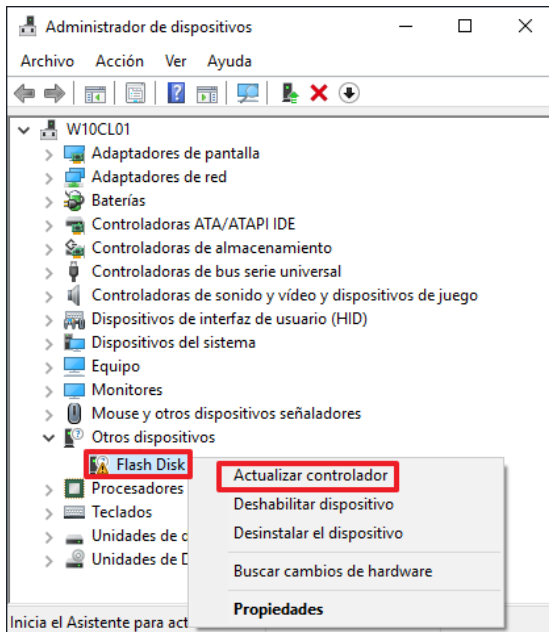
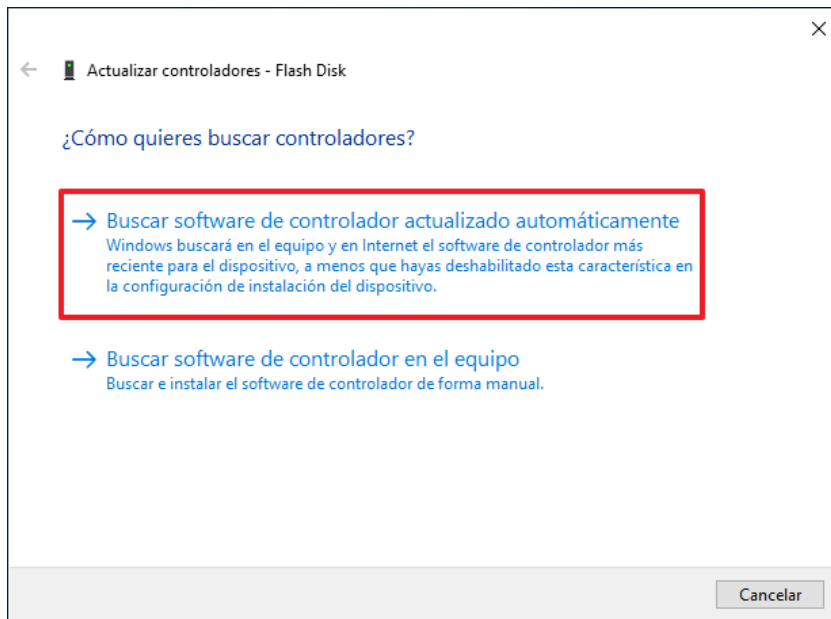
El proceso consta de un paso a paso para instalar un controlador de forma manual y que el dispositivo funcione. Tras su uso e independientemente de que el dispositivo esté conectado o no, se revertirá el uso del dispositivo mediante la desinstalación del controlador.

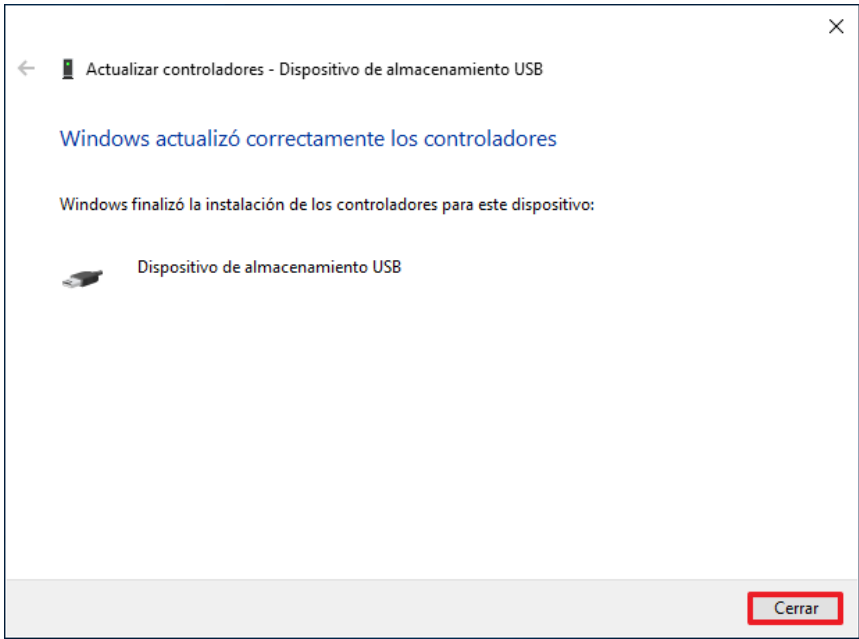
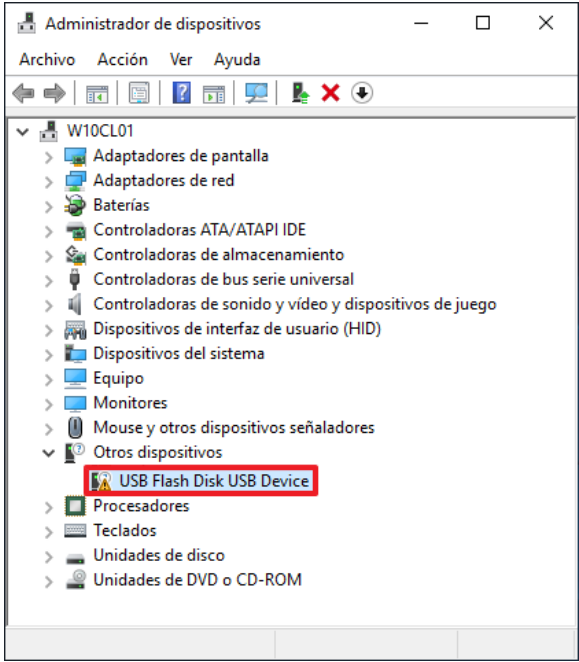
1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB

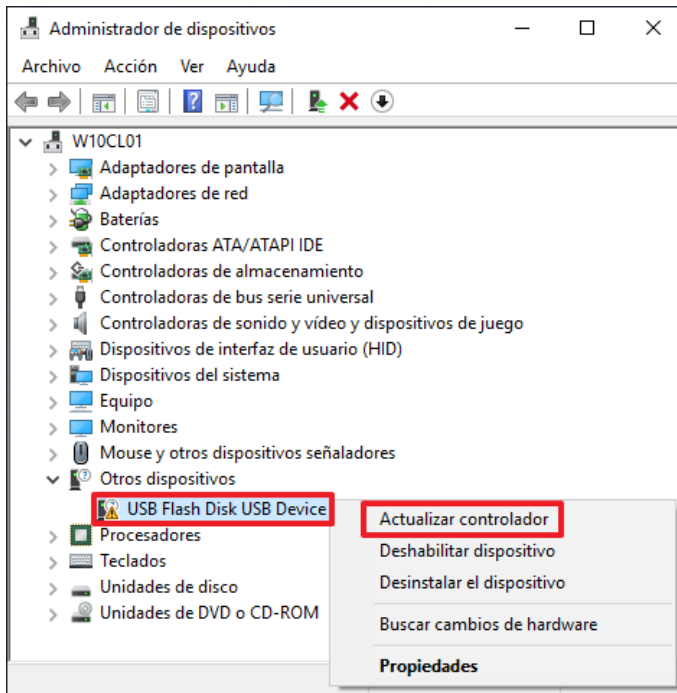
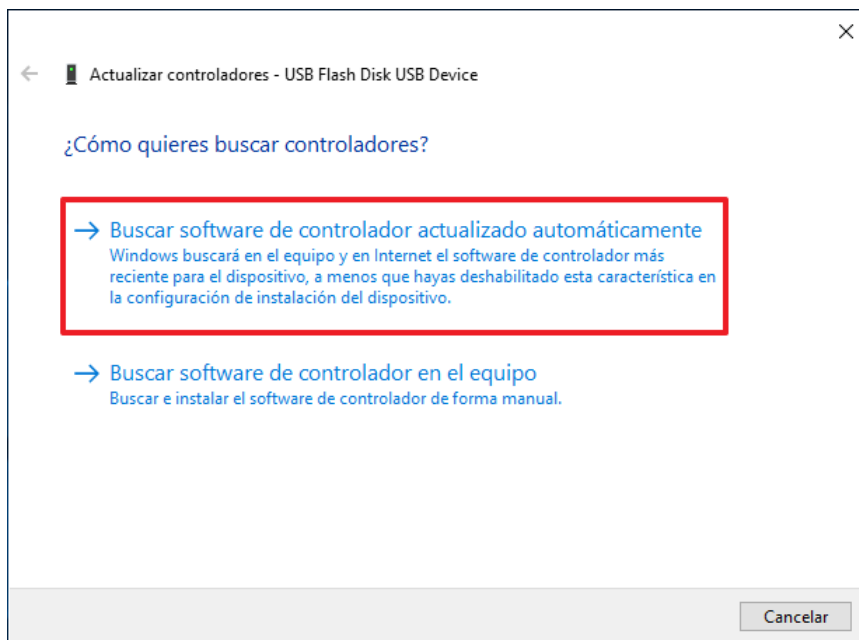
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 
3.	El control de cuentas le solicitará la elevación de privilegios. Introduzca las credenciales de un administrador local de la máquina y pulse “Sí” para continuar.
4.	Introduzca el comando “gpedit.msc” y pulse “Enter”. 
5.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

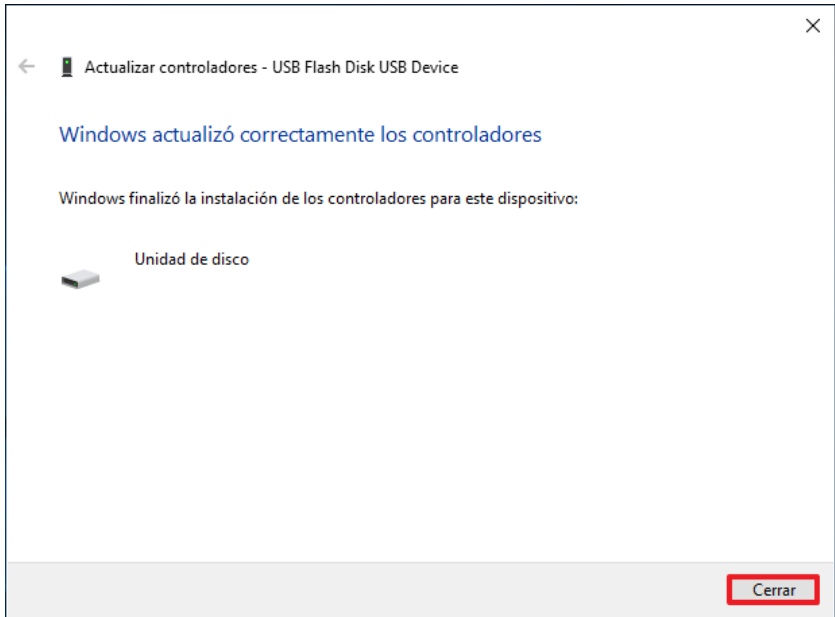
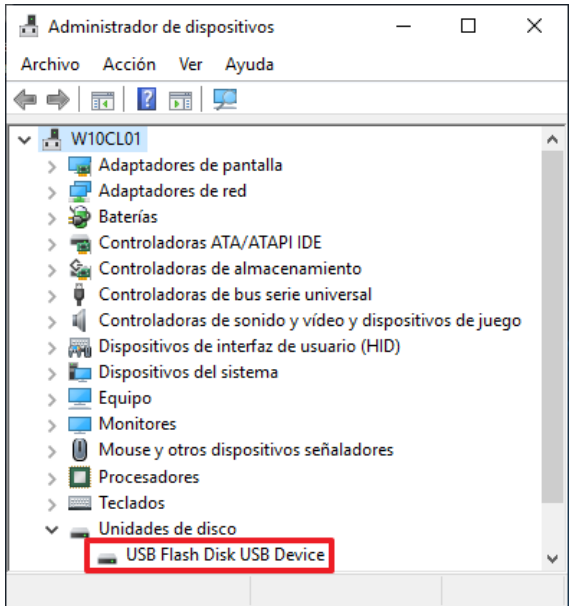
Paso	Descripción
6.	Haga doble clic sobre la directiva “Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos” y configúrela para que su estado sea “Habilitada”. A continuación seleccione “Aceptar”. 
7.	Para iniciar la instalación de un dispositivo USB deberá conectar el dispositivo USB en el equipo. Tras conectarlo aparecerá una notificación indicando que “La directiva de sistema prohíbe la instalación de este dispositivo”.  Nota: Es necesario tener en consideración que la instalación de los dispositivos USB de realizarse de manera manual y por un usuario que pertenezca al grupo local administradores.

Paso	Descripción
8.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
9.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de “Dispositivo desconocido”.

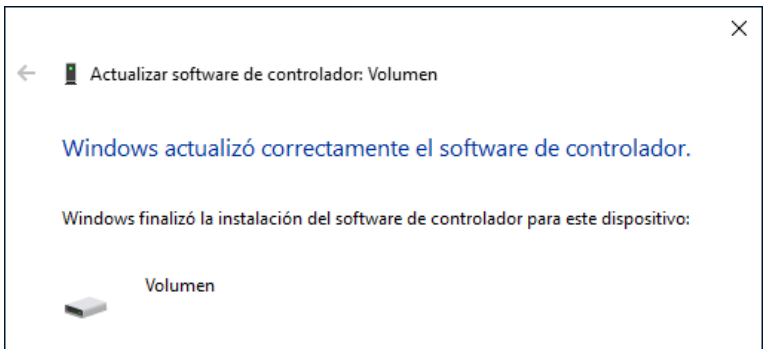
Paso	Descripción
10.	Haga clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 
11.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 

Paso	Descripción
12.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  Nota: No cierre el “Administrador de dispositivos” todavía.
13.	Tras la instalación de los controladores el sistema reconocerá el dispositivo. Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: En este ejemplo se utiliza el dispositivo denominado “USB Flash Disk USB Device”. Si el sistema no reconoce el dispositivo desconéctelo y vuélvalo a conectar para visualizarlo. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.

Paso	Descripción
14.	Haga de nuevo clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 
15.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 

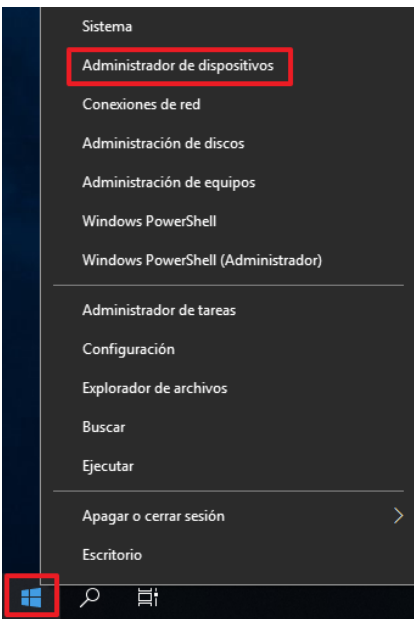
Paso	Descripción
16.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  Nota: Deberá repetir estos pasos hasta que su dispositivo de almacenamiento aparezca en el apartado “Unidades de disco”.
17.	Tras completarse la instalación, despliegue el nodo “Unidades de disco” y compruebe que el USB es reconocido por el equipo.  Nota: Espere a que el dispositivo sea reconocido por el equipo. En caso de no ser así, extraiga y vuelva a conectar el dispositivo para que éste sea reconocido. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.

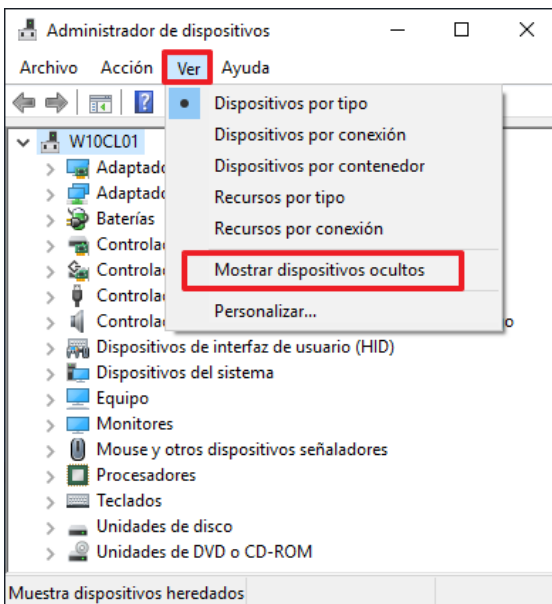
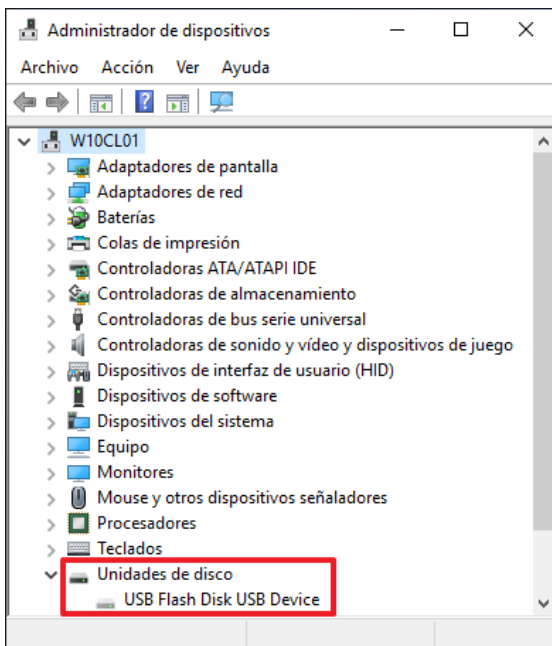


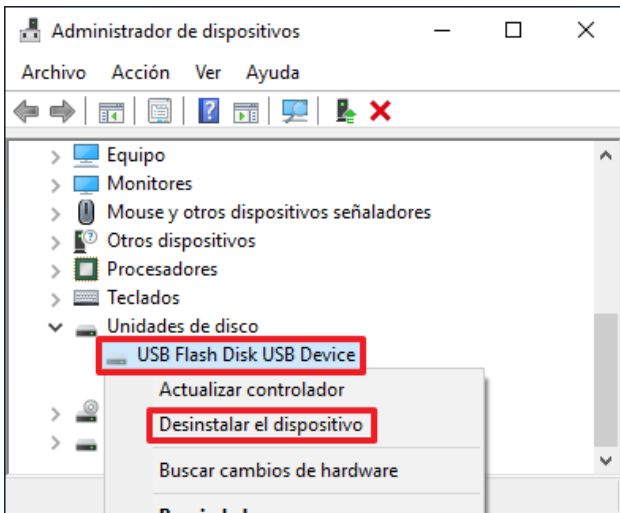
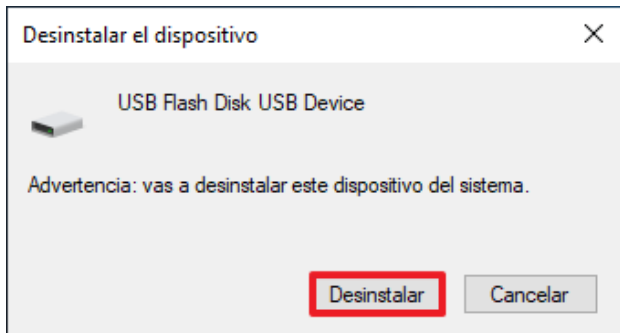
Paso	Descripción
18.	En caso de que el dispositivo aparezca en el apartado “Unidades de disco” pero no puede hacer uso de él a través del explorador de ficheros es posible que dentro del apartado “Otros dispositivos” quede algún “Dispositivo desconocido” que haga referencia a “Volumen”. Deberá instalar este controlador también para poder hacer uso del dispositivo. 
19.	El dispositivo está listo para ser utilizado.

1.2. DESINSTALACIÓN DE CONTROLADORES PARA IMPEDIR EL USO DE DISPOSITIVOS USB

Tras la instalación del dispositivo y su posterior uso, será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

Paso	Descripción
20.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores”.
21.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

Paso	Descripción
22.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 
23.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 

Paso	Descripción
24.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
25.	Pulse “Desinstalar” ante la advertencia emergente.  Nota: Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

2. ADMINISTRAR EL USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE EL IDENTIFICADOR DE DISPOSITIVO

Este apartado establece los procedimientos para la configuración y gestión de los dispositivos USB mediante su identificador de dispositivo.

Nota: Antes de proceder a la configuración de los dispositivos USB mediante el filtrado de su identificador, deberá verificar si el/los dispositivos USB a configurar tienen el mismo identificador/dato primario/chipset. Si es así, al configurar dicho USB, estará autorizando el uso de dispositivos de forma masiva en el sistema. Por lo tanto, antes de instalar los dispositivos USB deberá verificar que su organización no dispone de USB's con el mismo identificador.

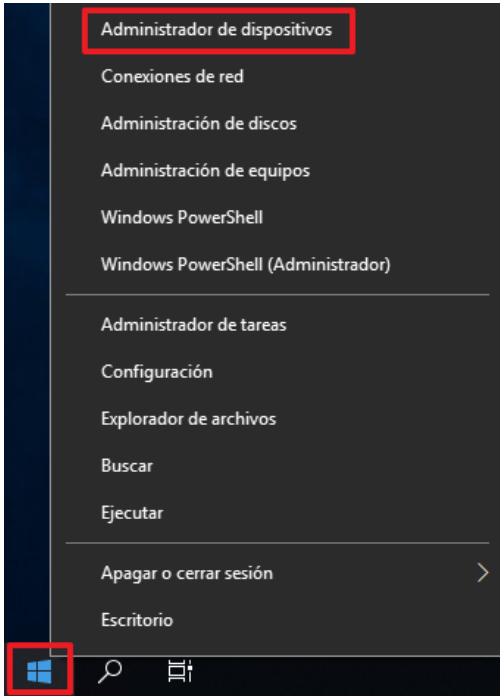
2.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

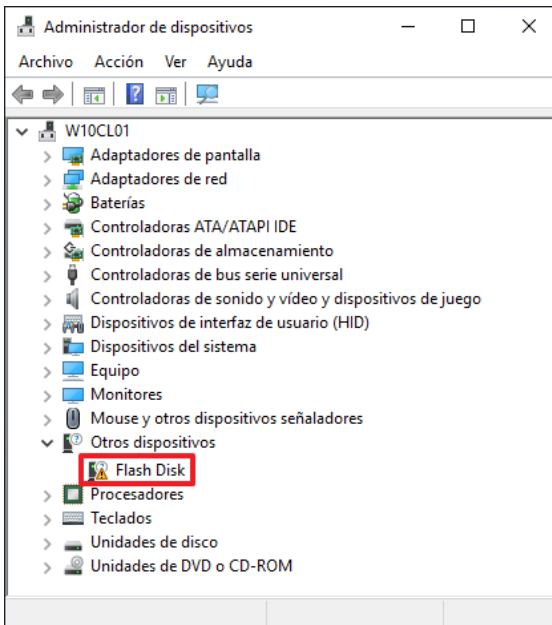
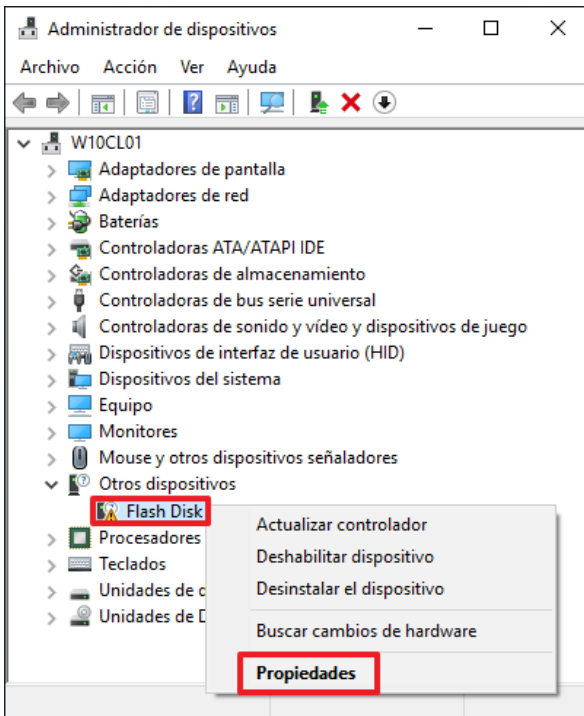
Este punto describe el proceso para permitir el uso un dispositivo mediante el filtrado por su identificador. Cuando el filtro esté realizado, los controladores del dispositivo se instalarán de manera automática y el dispositivo podrá ser utilizado.

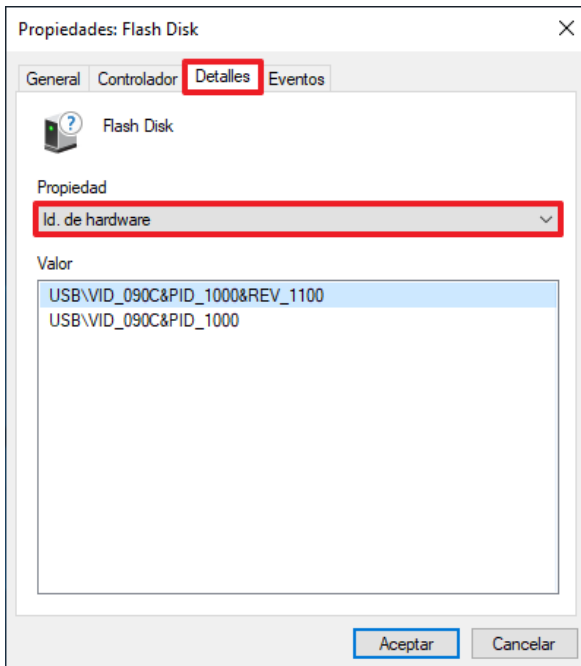
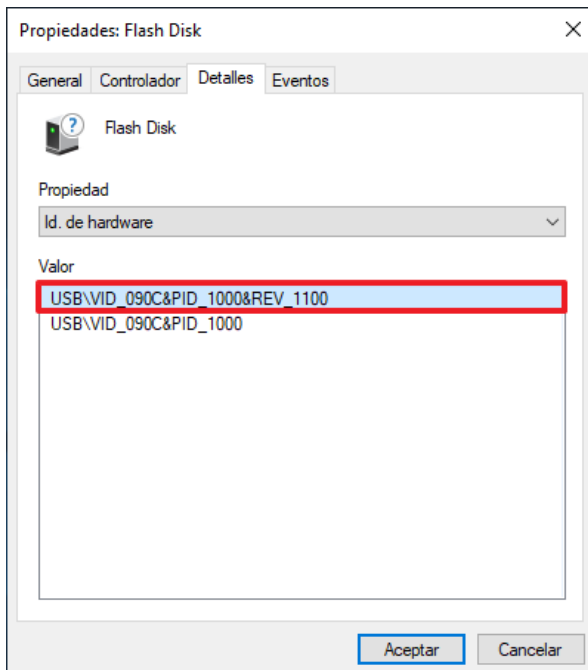
Tras la finalización de su uso, los controladores del dispositivo serán desinstalados tanto si el dispositivo se encuentra conectado al equipo como si no.

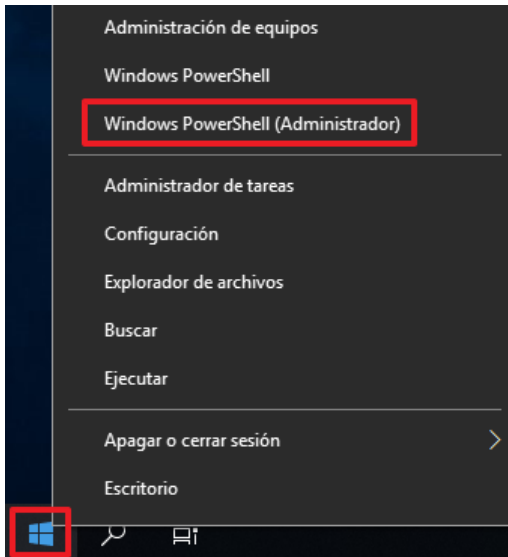
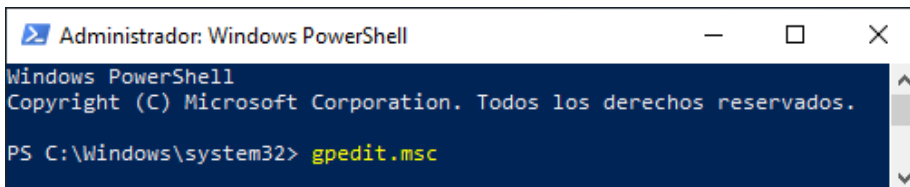
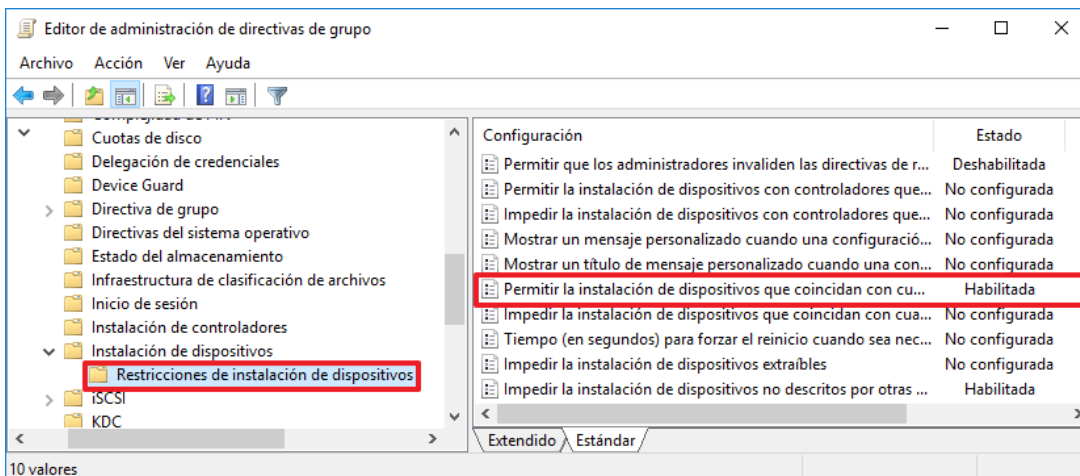
Será necesario añadir varios identificadores para un mismo dispositivo USB. Esto es debido a que el sistema va especificando el tipo de dispositivo de modo que puede concretar los controladores necesarios hasta permitir su funcionamiento.

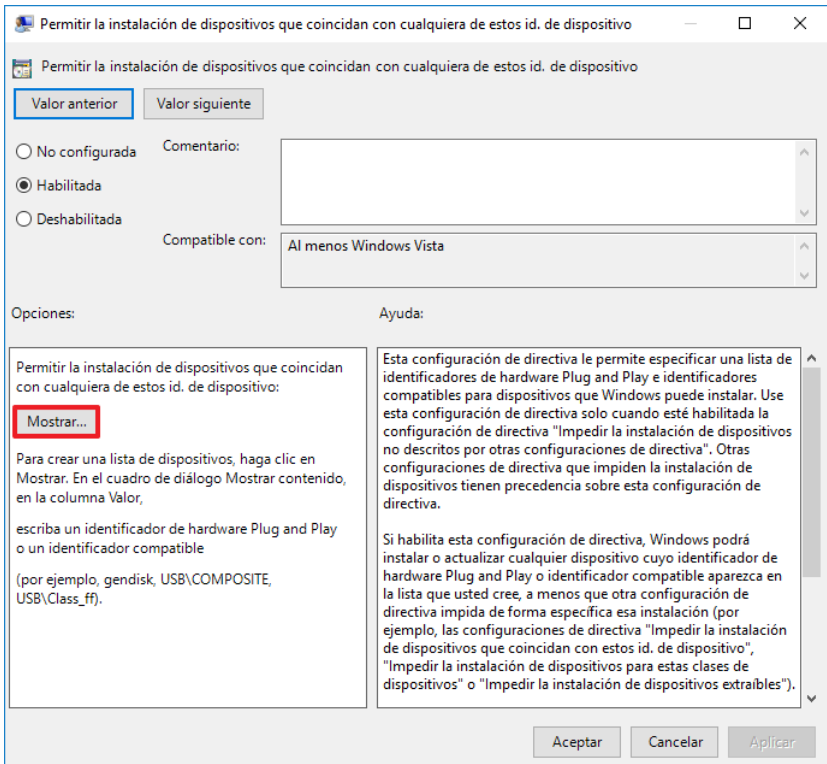
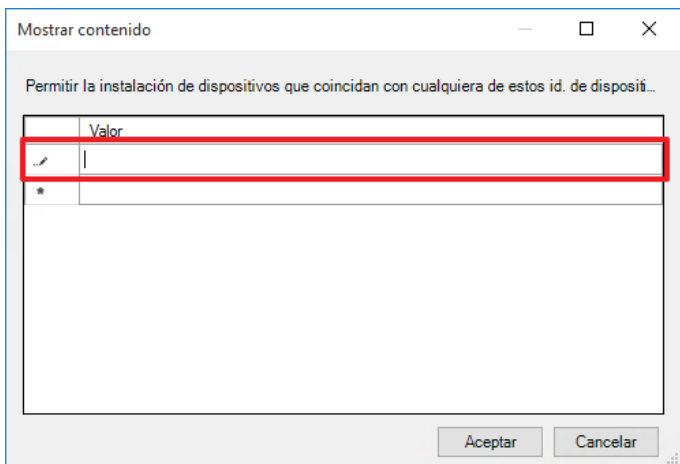
Tras el uso de los dispositivos se procederá a eliminar los identificadores de la lista configurada, y a desinstalar los controladores para evitar el uso de éstos.

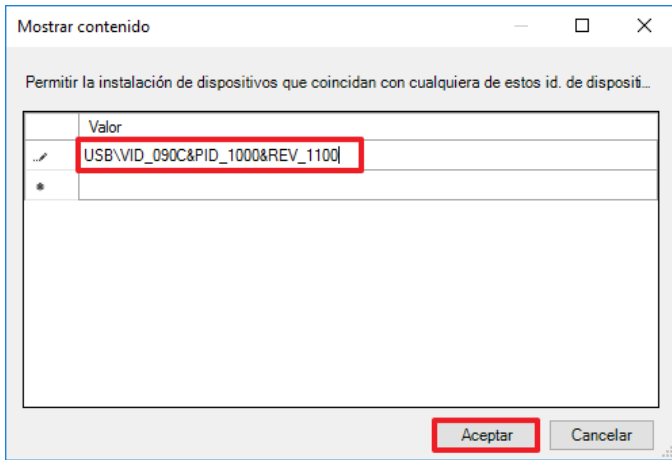
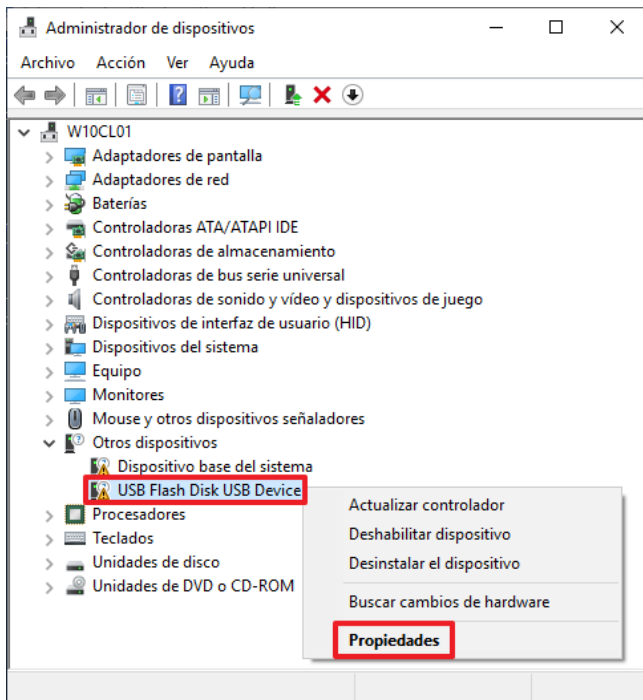
Paso	Descripción
26.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
27.	Para iniciar la instalación de un dispositivo USB deberá conectarlo en el equipo. Nota: Es necesario tener en consideración que la instalación de los dispositivos USB debe realizarse de manera manual y por un usuario con permisos de administrador.
28.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

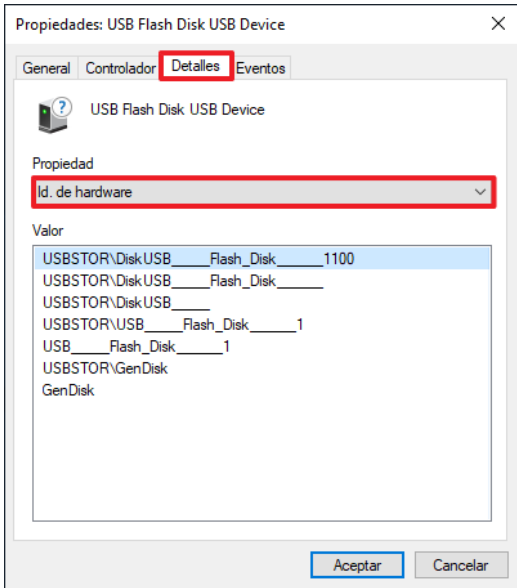
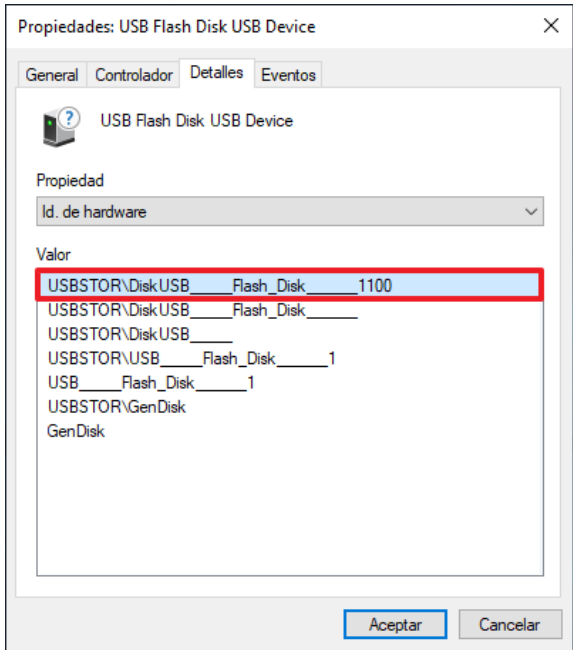
Paso	Descripción
29.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre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

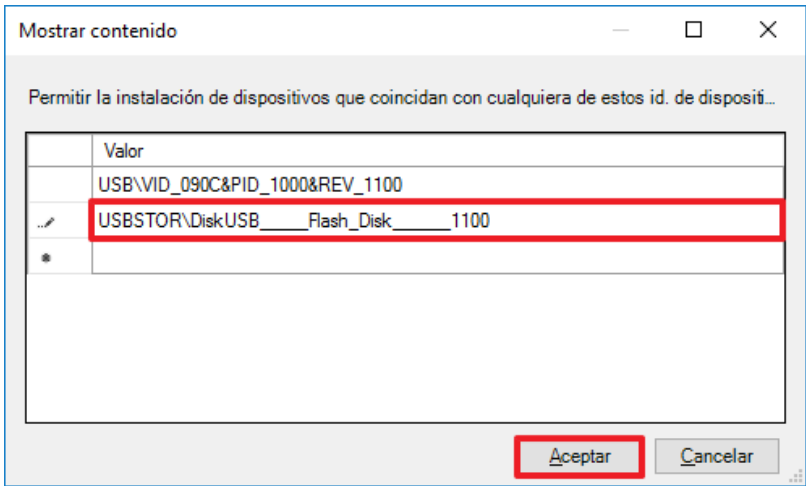
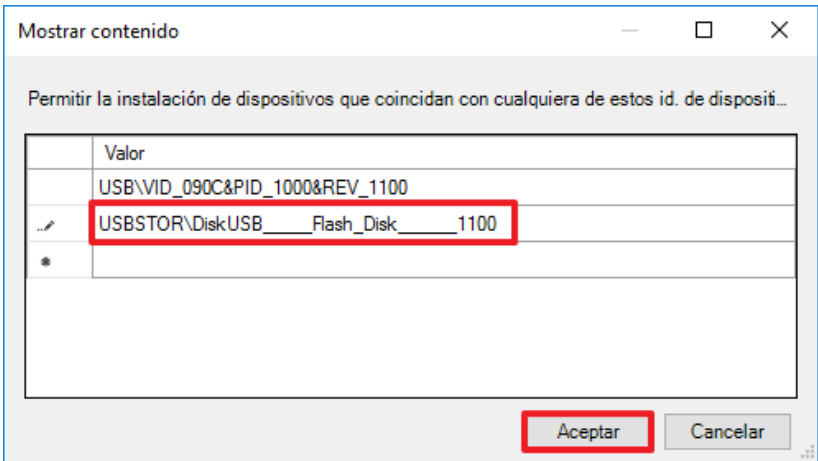
Paso	Descripción
31.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Id. de hardware”. 
32.	Seleccione el identificador que se encuentre en primer lugar y anótelolo para poder introducirlo más adelante.  Nota: Independientemente del numero de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.
33.	Sin cerrar el “Administrador de dispositivos” continúe con el siguiente paso.

Paso	Descripción
34.	Ejecute una consola de PowerShell con permisos de administrador. Para ello, pulse sobre el botón “Inicio” y seleccione “Windows PowerShell → Windows Powershell” .
35.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 
36.	El control de cuentas le solicitará la elevación de privilegios. Introduzca las credenciales de un administrador local de la máquina y pulse “Sí” para continuar.
37.	Introduzca el comando “gpedit.msc” y pulse “Enter”. 
38.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos” . 

Paso	Descripción
39.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar...”. 
40.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la primera línea para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado anteriormente.  Nota: Asegúrese de que no existe ningún espacio en blanco.

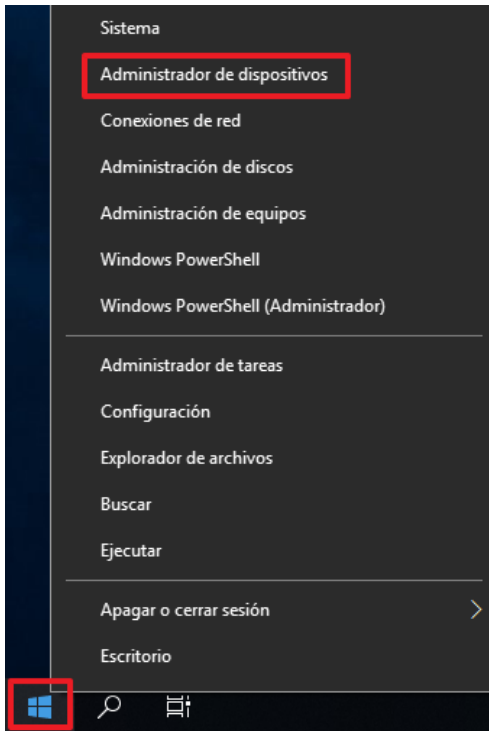
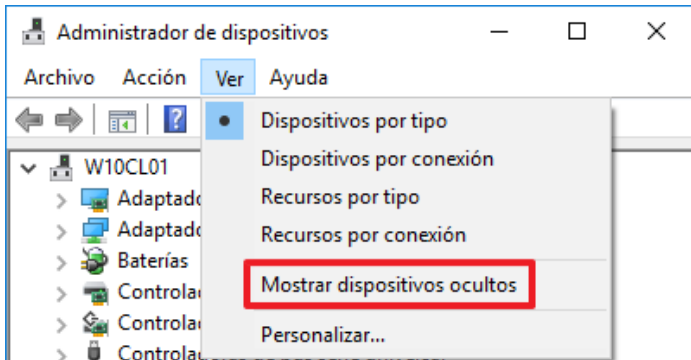
Paso	Descripción
41.	Verifique el identificador introducido y pulse “Aceptar” para continuar. 
42.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.
43.	Sin cerrar el “Editor de directivas de grupo local” continúe con el siguiente paso.
44.	Acceda de nuevo al “Administrador de dispositivos”. En este punto el dispositivo será reconocido por el equipo. Seleccione dicho dispositivo con el botón derecho y pulse sobre la opción “Propiedades”.  Nota: Espere a que el dispositivo sea reconocido por el equipo. En caso de no ser así, extraiga y vuelva a conectar el dispositivo para que éste sea reconocido. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.

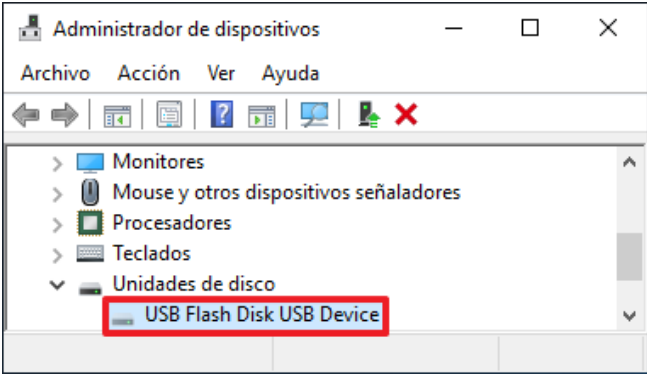
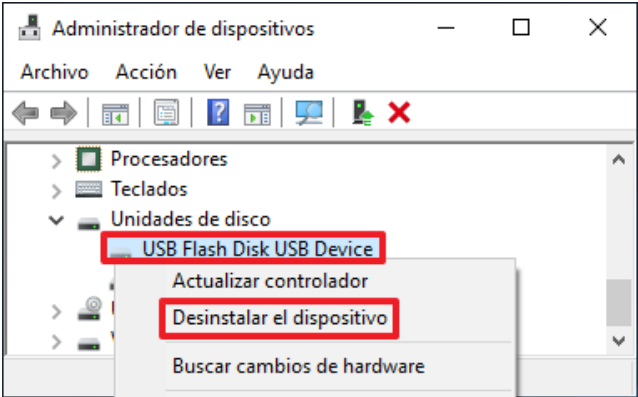
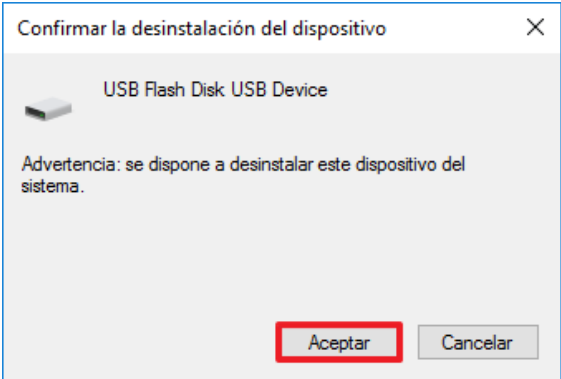
Paso	Descripción
45.	Acceda de nuevo a la pestaña “Detalles” y en el apartado “Propiedad” seleccione “Id. de hardware”.  Nota: Los identificadores del dispositivo han cambiado debido a que el equipo ya no lo toma como dispositivo genérico por lo que proporciona un identificador específico del dispositivo.
46.	Seleccione el identificador que se encuentre en primer lugar y anótelolo para poder introducirlo más adelante.  Nota: Independientemente del número de identificadores existentes deberá seleccionar siempre aquél que se encuentre en primera posición.

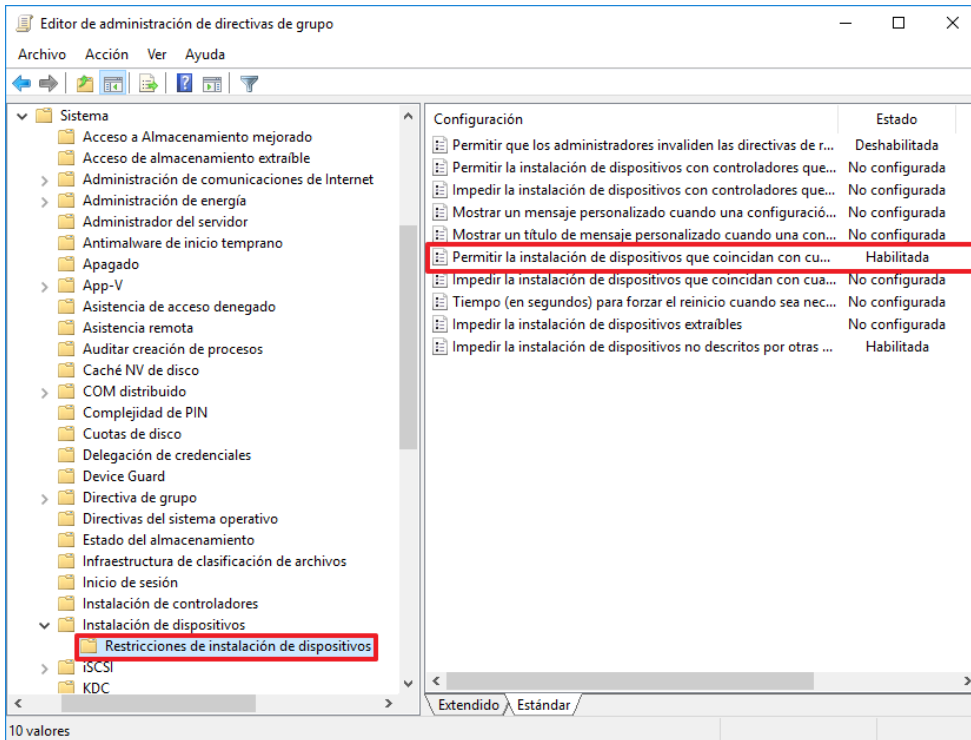
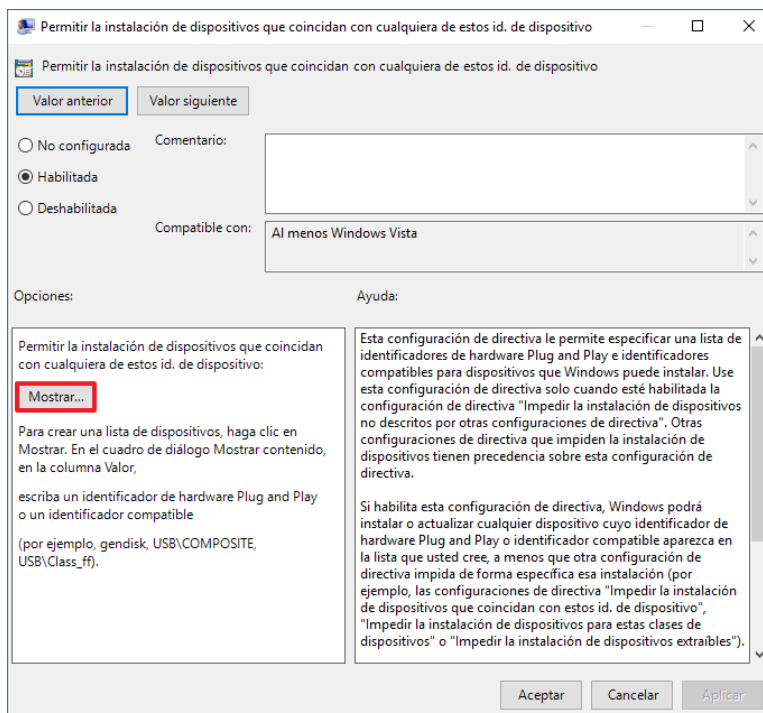
Paso	Descripción
47.	En la ventana “Mostrar contenido” abierta en pasos anteriores desde la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, haga doble clic sobre la segunda línea en blanco. Introduzca entonces el identificador de USB copiado anteriormente. Pulse “Aceptar” para continuar. 
48.	Aparecerá el nuevo identificador del dispositivo. Pulse “Aceptar” para continuar. 
49.	Deberá repetir este proceso hasta que no se muestren nuevos identificadores en la propiedad “ID. de Hardware” del dispositivo que está instalando. Nota: En este ejemplo solo ha sido necesario el uso de dos identificadores. Dependiendo del dispositivo conectado, tendrá un número diferente de identificadores en la lista. Deberá tener en cuenta la posibilidad de necesitar ID’s adicionales referentes al dispositivo “Volumen”.
50.	A partir de este momento el dispositivo estará listo para su uso.

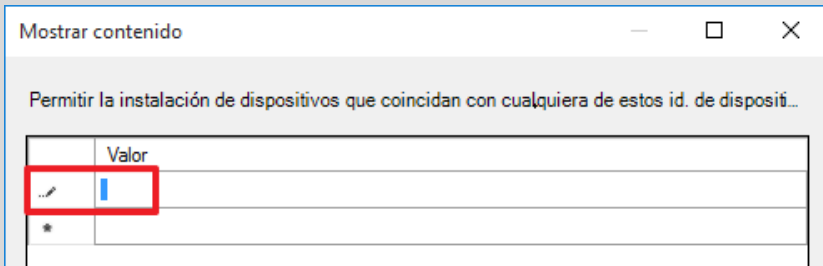
2.2. IMPEDIR EL USO DE DISPOSITIVOS USB

Tras la instalación del dispositivo y su posterior uso, será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

Paso	Descripción
51.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
52.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
53.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

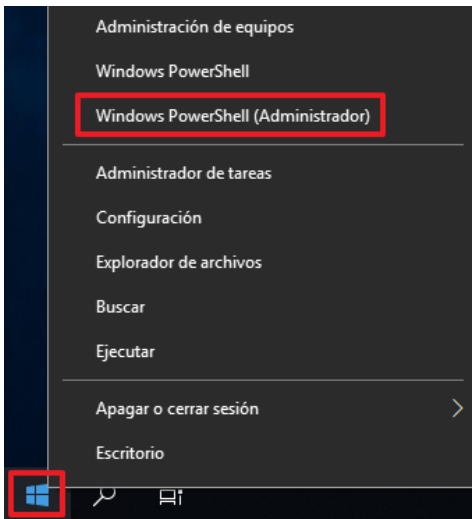
Paso	Descripción
54.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 
55.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
56.	Pulse “Aceptar” ante la advertencia emergente.  Nota: Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo.

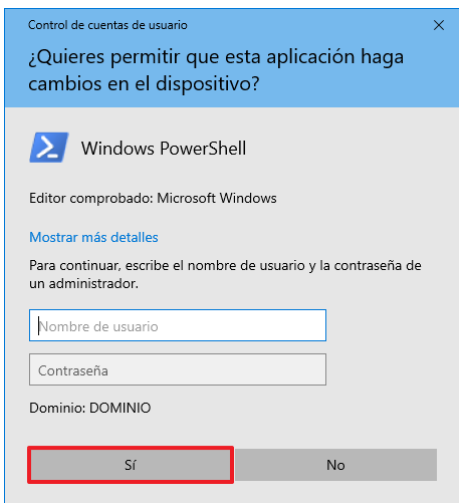
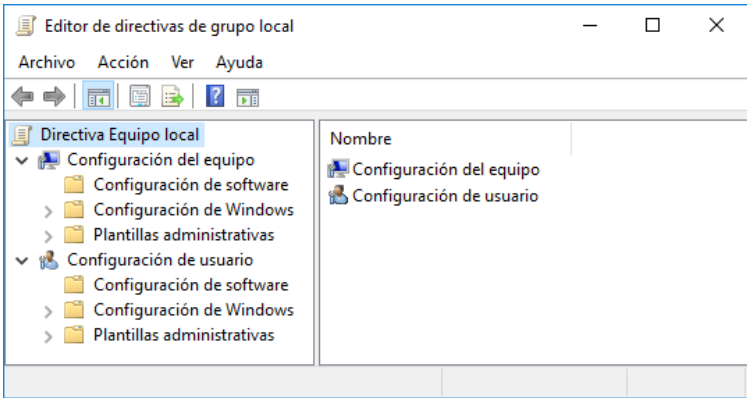
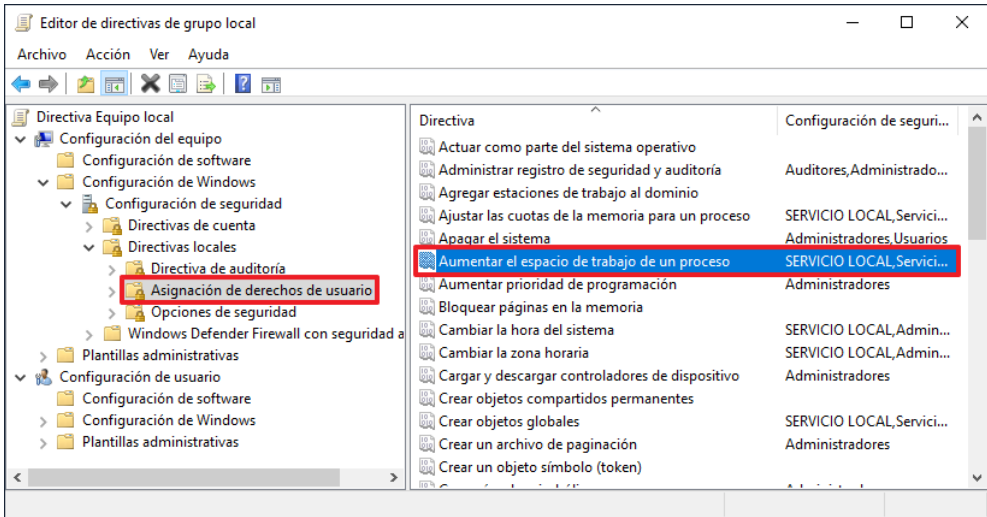
Paso	Descripción
57.	En el “Editor de directivas de grupo local” despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 
58.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón “Mostrar...”. 

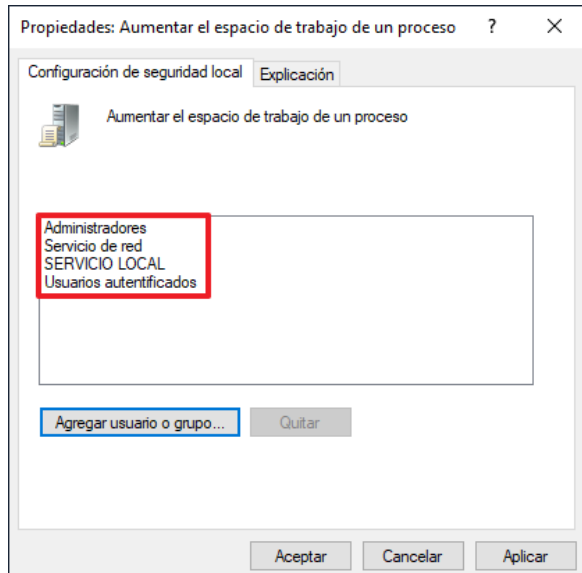
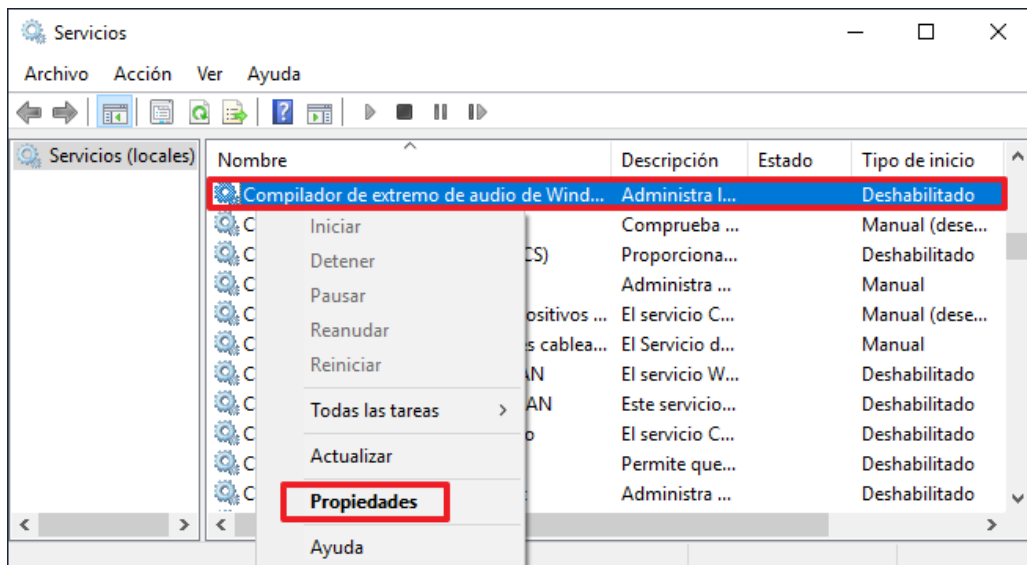
Paso	Descripción
59.	Identifique las líneas que correspondan con el dispositivo. Haga doble clic sobre cada línea y elimine su contenido. Nota: En caso de eliminar todas las líneas debe dejarse al menos una línea con un espacio en blanco para poder cerrar la configuración de la directiva. En caso contrario se mostrará un error. 

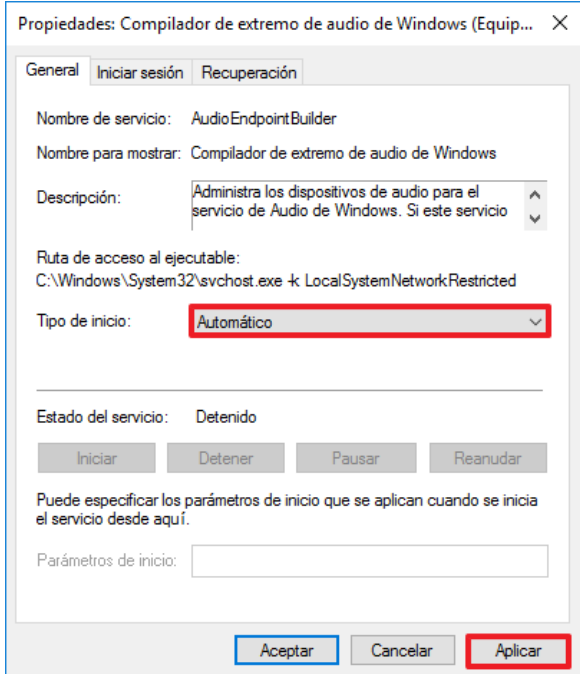
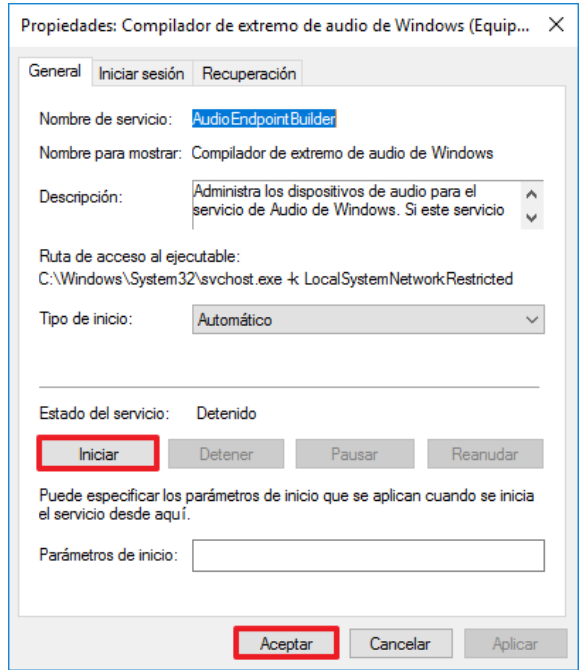
ANEXO B.3.5. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19

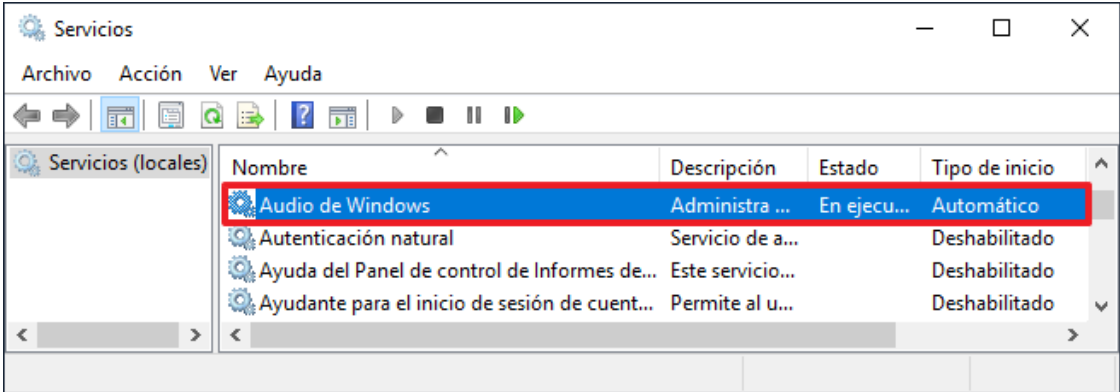
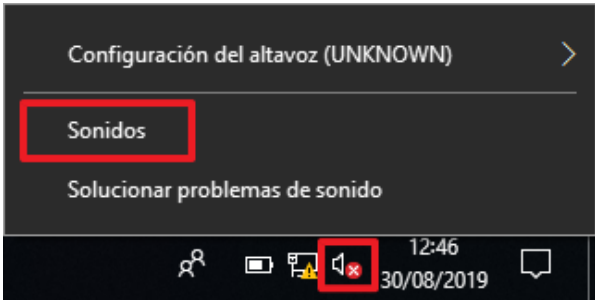
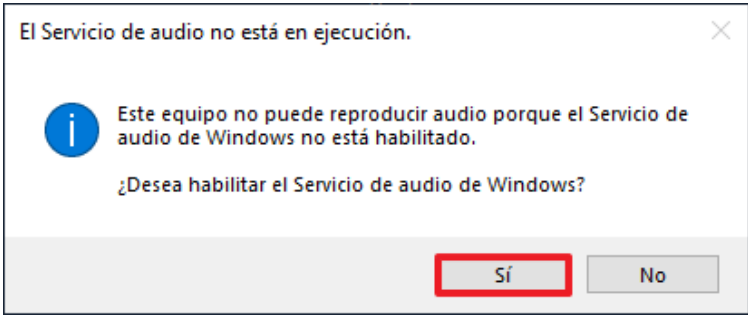
A continuación, se indican los pasos a realizar para modificar la plantilla de seguridad a aplicar sobre equipos Microsoft Windows 10, independientes del dominio, con el objetivo de habilitar el audio del sistema. Para habilitar el audio en los equipos, se deberá actualizar el objeto de directiva de grupo local siguiendo la configuración que se indica a continuación.

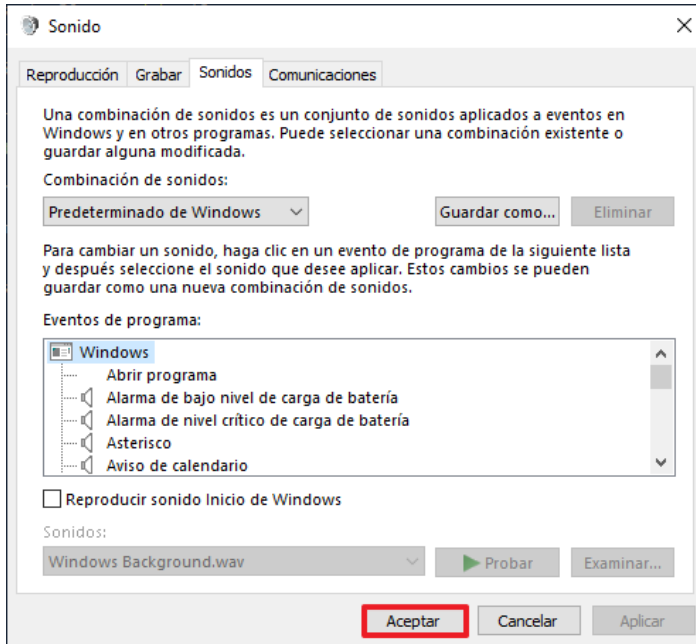
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 

Paso	Descripción
3.	Eleve privilegios ante el control de cuentas de usuario 
4.	En la ventana de PowerShell ejecute "gpedit.msc". Esto abrirá una ventana del Editor de directivas de grupo local, como la mostrada en la siguiente figura. 
5.	Despliegue el nodo “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” y seleccione con doble clic la directiva “Aumentar el espacio de trabajo de un proceso”. 

Paso	Descripción						
6.	Modifique los valores de equipo indicados en la tabla. Para ello, pulse “Agregar usuario o grupo...”. Seleccione los grupos correspondientes hasta que la configuración coincida con la tabla que se muestra a continuación. 						
	<table><tr><th>Directiva</th><th>Valor</th><th>Descripción</th></tr><tr><td>Aumentar el espacio de trabajo de un proceso</td><td> - Administradores - Servicio de red - SERVICIO LOCAL - Usuarios autenticados </td><td>Aumentar el espacio de trabajo de un proceso</td></tr></table>	Directiva	Valor	Descripción	Aumentar el espacio de trabajo de un proceso	- Administradores - Servicio de red - SERVICIO LOCAL - Usuarios autenticados	Aumentar el espacio de trabajo de un proceso
Directiva	Valor	Descripción					
Aumentar el espacio de trabajo de un proceso	- Administradores - Servicio de red - SERVICIO LOCAL - Usuarios autenticados	Aumentar el espacio de trabajo de un proceso					
7.	Modifique el modo de inicio del servicio de “Compilador de extremo de audio de Windows”. Para ello y desde la misma consola de PowerShell, ejecute el comando “Services.msc” del mismo modo que ejecutó “gpedit.msc” en pasos anteriores. Haga clic derecho sobre el servicio y seleccione “Propiedades”. 						

Paso	Descripción
8.	En el menú de “Propiedades: Compilador de extremo de audio de Windows (Equipo local)”, en el campo “Tipo de inicio” seleccione la opción “Automático” y pulse sobre el botón “Aplicar”. 
9.	Pulse sobre el botón “Iniciar” y cuando el estado del servicio sea “Iniciado”, pulse sobre el botón “Aceptar”. 

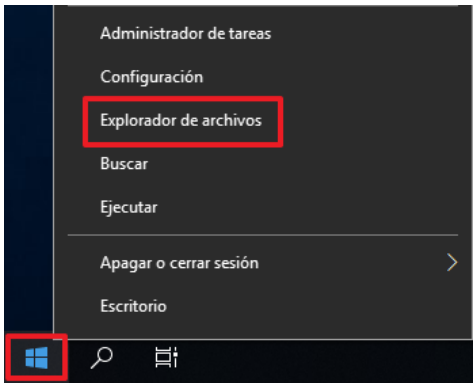
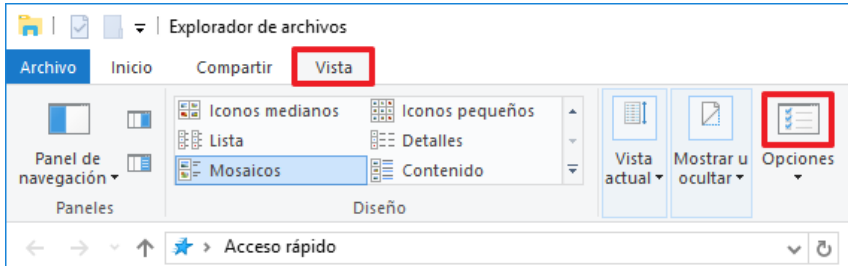
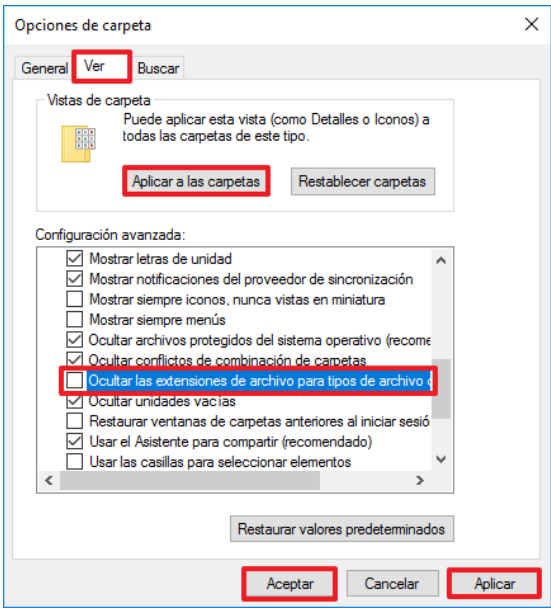
Paso	Descripción
10.	Realice el mismo procedimiento para iniciar el servicio “Audio de Windows”. 
11.	A continuación, en la barra de tareas, localice el icono de audio y pulsando con el botón derecho del ratón sobre él seleccione “Sonidos”. 
12.	En el siguiente mensaje del servicio de audio, pulse “Sí” para habilitar el servicio de audio de Windows. 
13.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores” y pulse “Sí”.

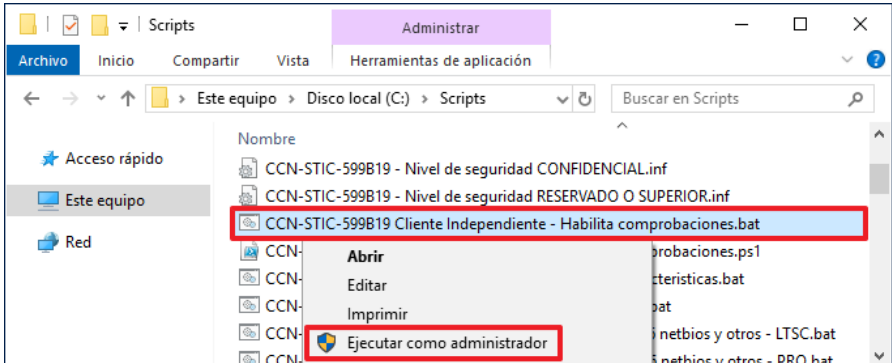
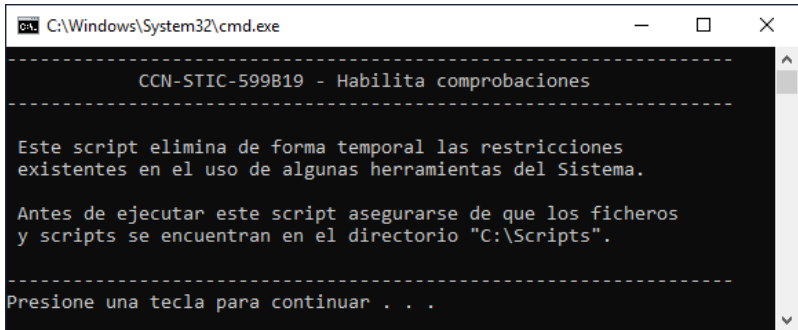
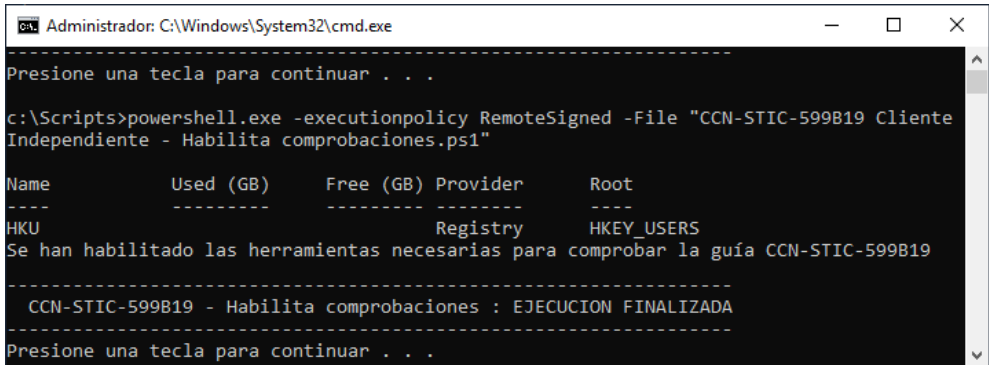
Paso	Descripción
14.	Tras aparecer la siguiente ventana de configuración de sonido, podrá hacer uso del sonido del sistema. Pulse “Aceptar” para cerrar la ventana. 
15.	Borre el directorio “C:\Scripts”. A partir de este momento, será posible hacer uso del sonido.

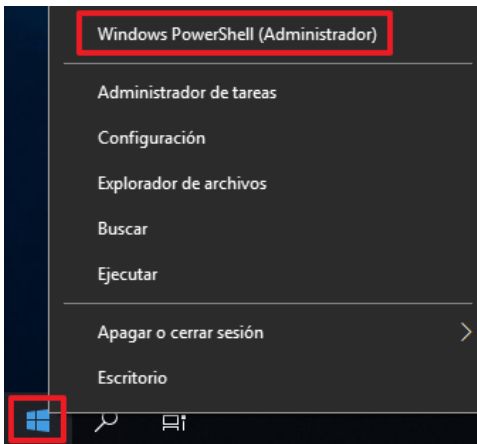
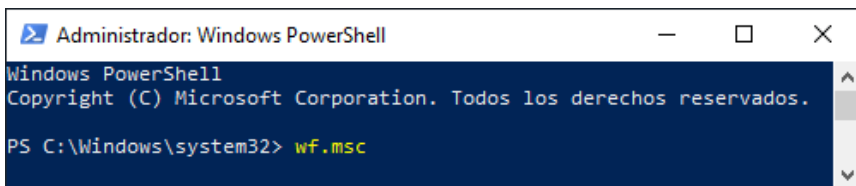
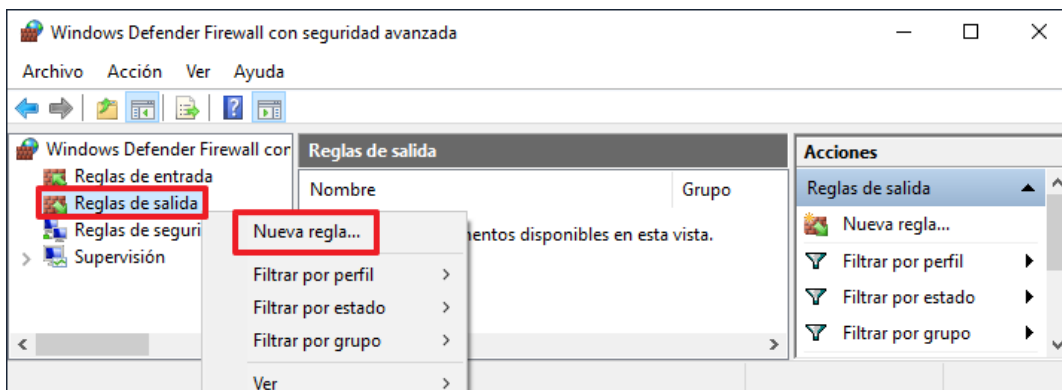
ANEXO B.3.6. CONFIGURACIÓN DE CLIENTE INDEPENDIENTE PARA PODER ACCEDER A UN RECURSO COMPARTIDO EN LA RED

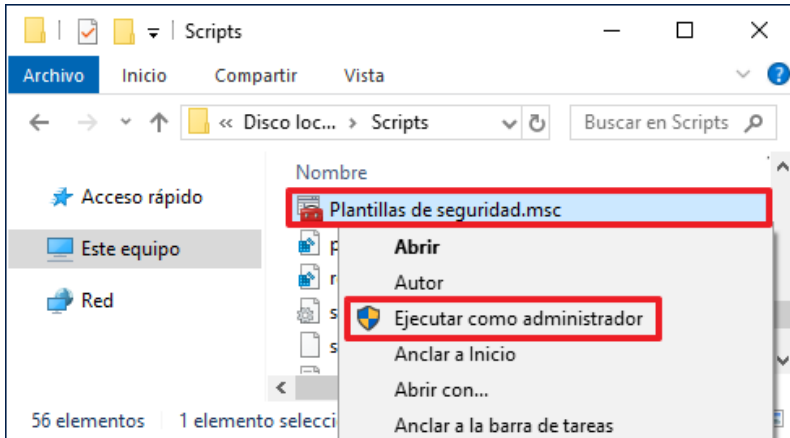
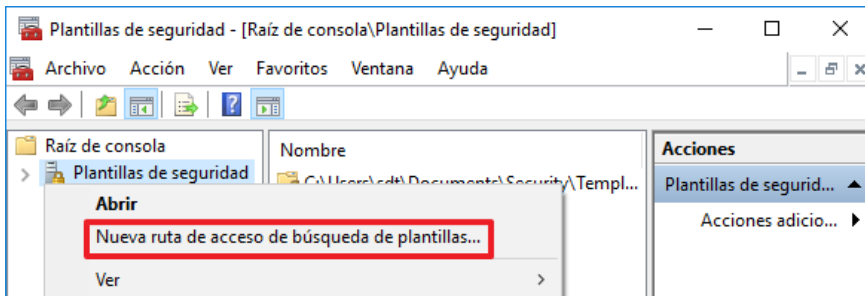
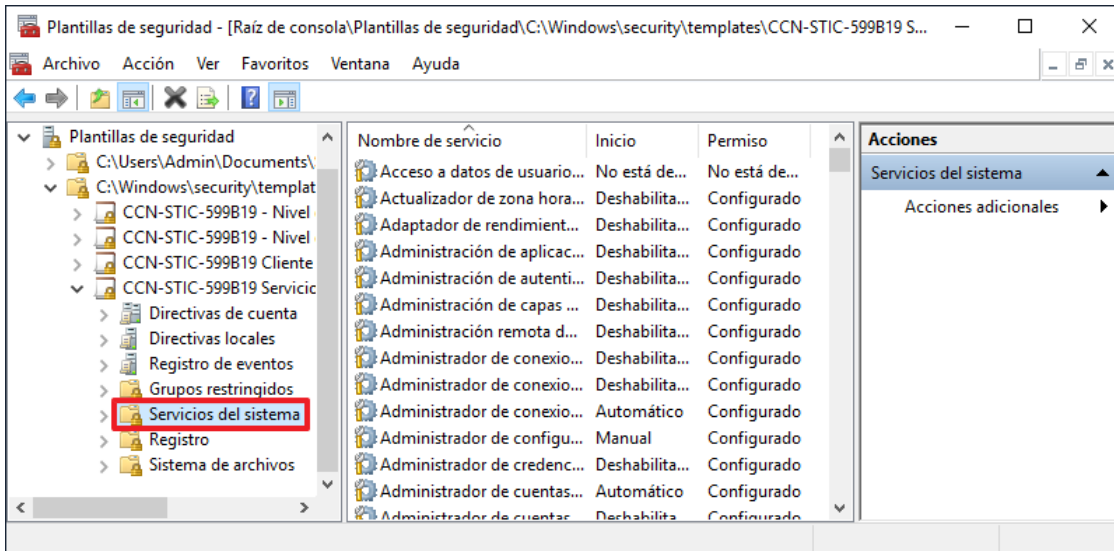
A continuación, se indican los pasos a realizar para modificar la configuración de un sistema Windows 10 que permita una conexión de un cliente independiente securizado con la guía CCN-STIC-599B19 a un recurso que se encuentre compartido dentro de la red.

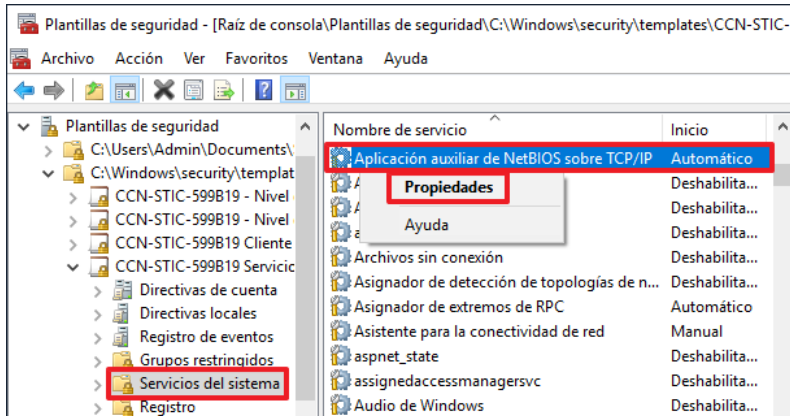
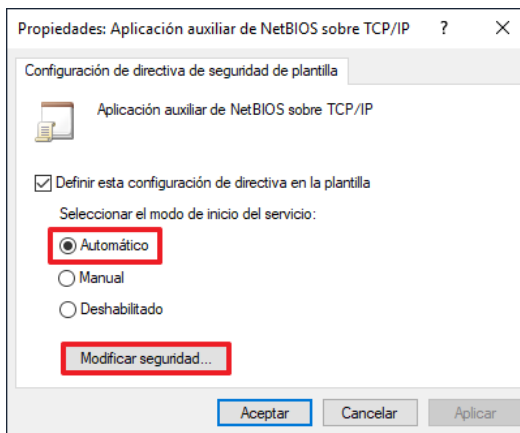
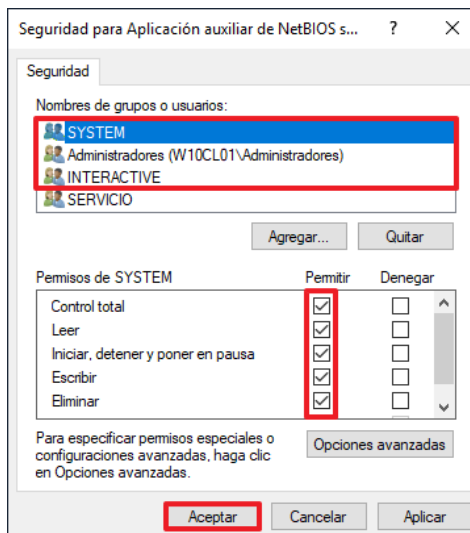
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Cree el directorio “Scripts” en la unidad “C:”
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

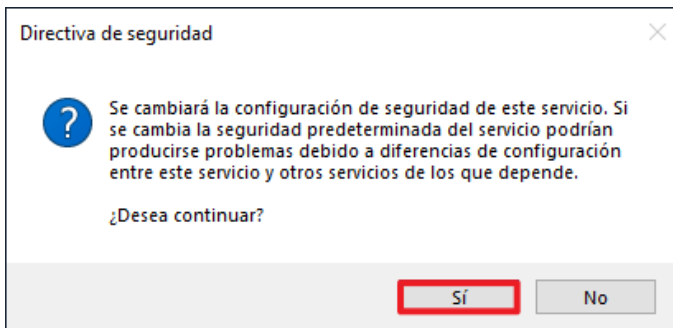
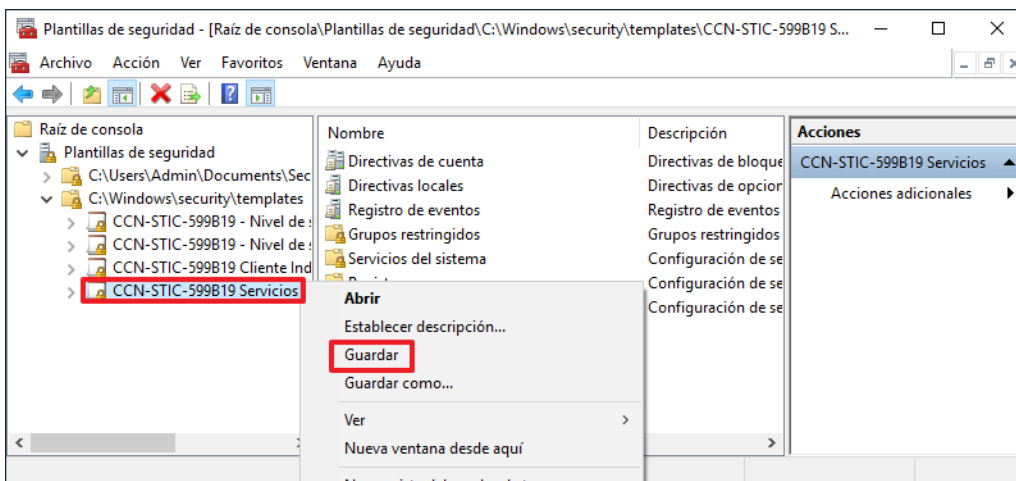
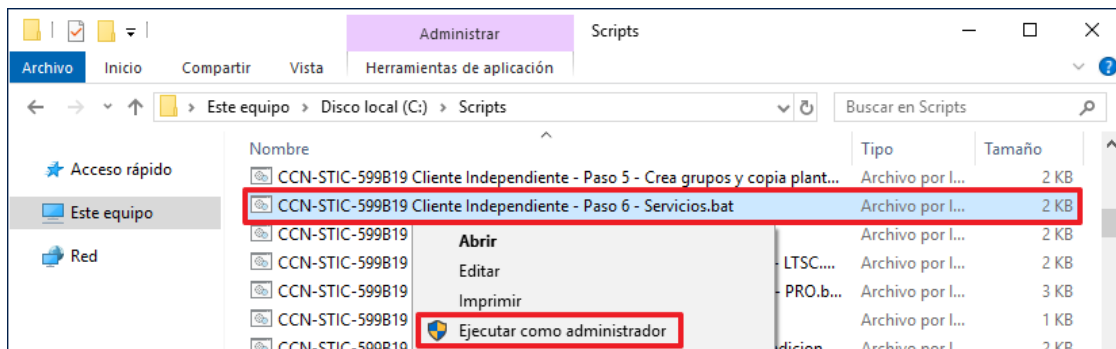
Paso	Descripción
4.	Si no lo hizo previamente, configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono “Opciones”. 
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 

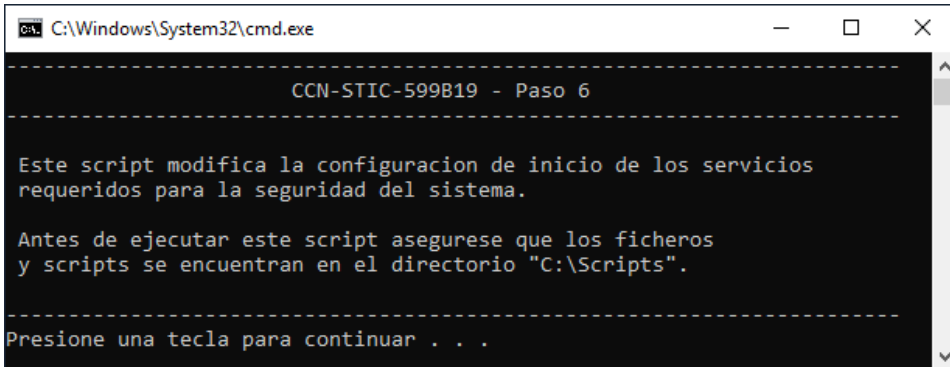
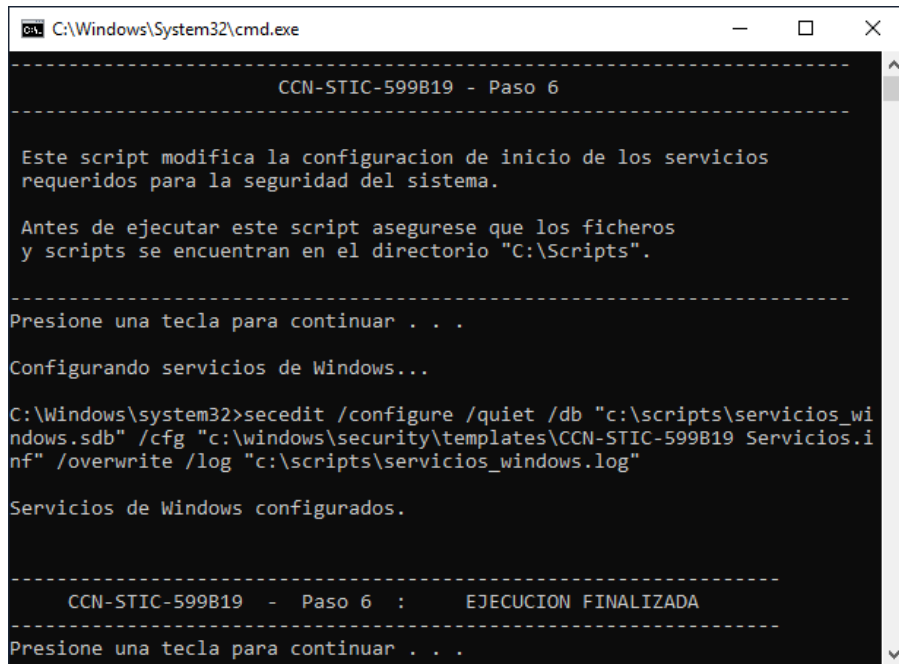
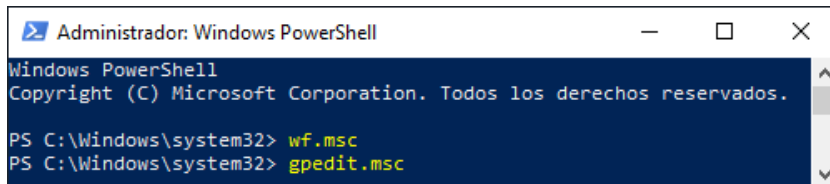
Paso	Descripción
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del cliente independiente: – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.ps1
8.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.bat" desde el directorio "C:\Scripts".  Nota: El sistema le solicitará elevación de privilegios.
9.	Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá la siguiente ventana. Pulse una tecla para continuar. 
10.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: En caso de que el sistema muestre errores puede ignorarlos. A partir de este momento, las consolas y características de administración bloqueadas por la presente guía vuelven a ser operativas de forma temporal.

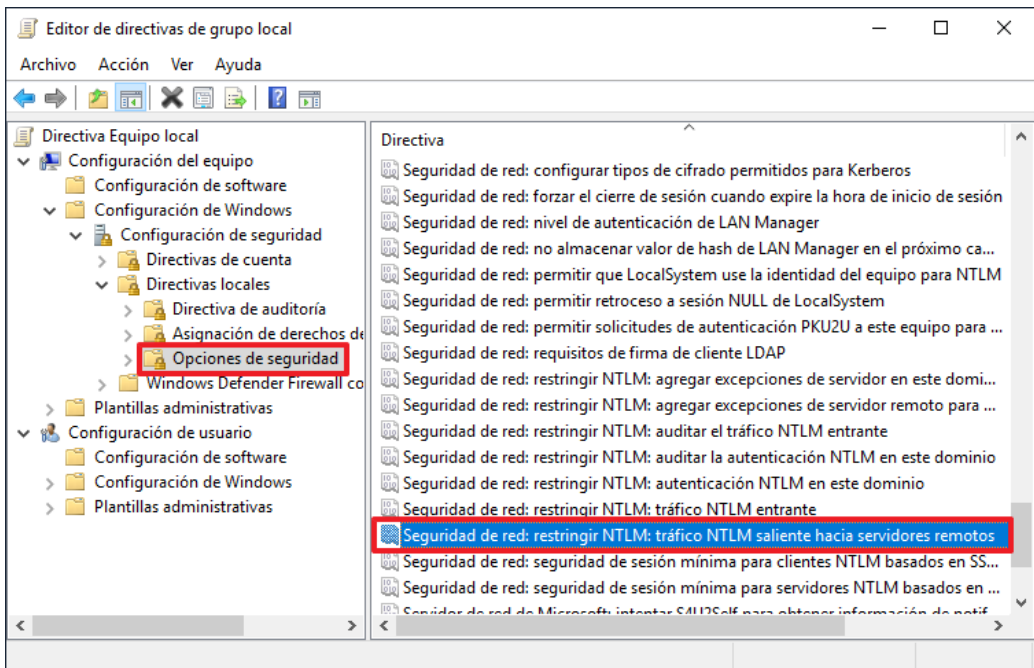
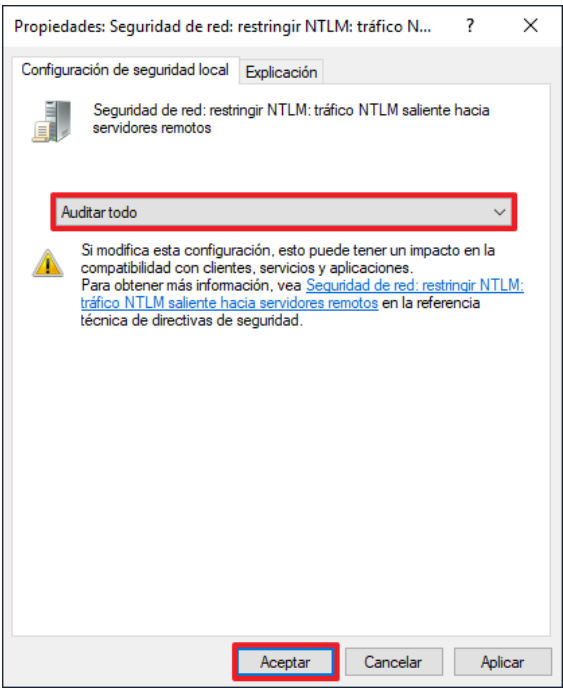
Paso	Descripción
11.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 
12.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local.
13.	Introduzca el comando “wf.msc” para abrir la consola de administración de Firewall. 
14.	En la consola abierta del administrador de Firewall vaya a “Reglas de salida” y pulse botón derecho sobre el mismo y selecciones la opción “Nueva regla...”.  Nota: Utilice el asistente personalizado para crear una regla que permita la conexión a la dirección IP en la cual se encuentra el recurso al que desea conectarse.
15.	Una vez creada las reglas necesarias cierre la consola del Firewall.
16.	Desde el explorador de archivos, sitúese en la ruta “C:\Scripts”.

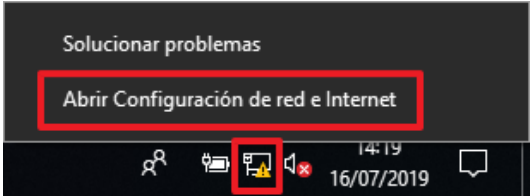
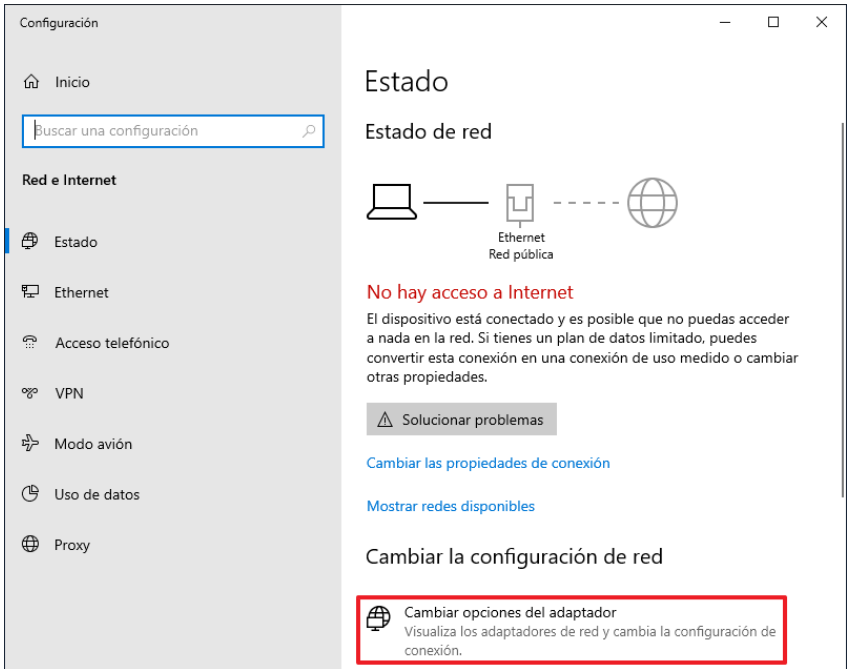
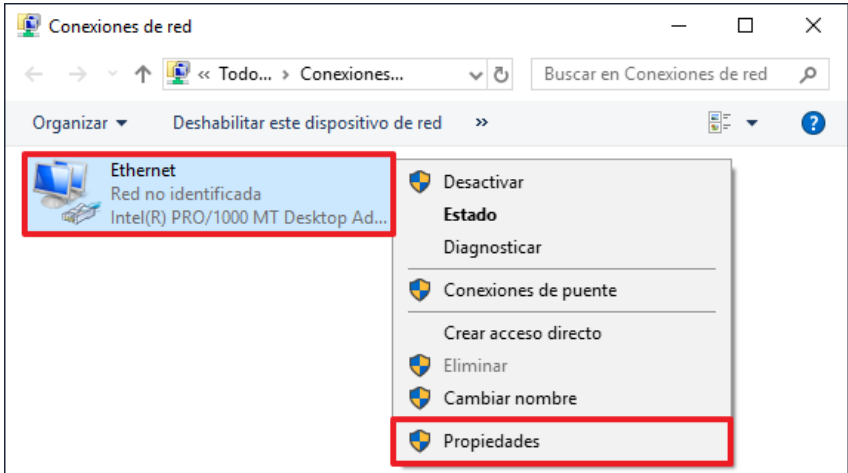
Paso	Descripción
17.	Pulse con el botón derecho del ratón sobre el fichero “Plantillas de seguridad.msc” y seleccione la opción “Ejecutar como administrador”.  Nota: El sistema le solicitará elevación de privilegios, introduzca las credenciales de un usuario con privilegios de administración sobre el puesto de trabajo.
18.	En la consola pulse con el botón derecho del ratón sobre plantillas de seguridad y seleccione la opción “Nueva ruta de acceso de búsqueda de plantillas...”. 
19.	En la ruta abierta seleccione “C:\Windows\Security\Templates”.
20.	Despliegue la plantilla “CCN-STIC-599B19 Servicios” y dentro de ella vaya a “Servicios del sistema”. 

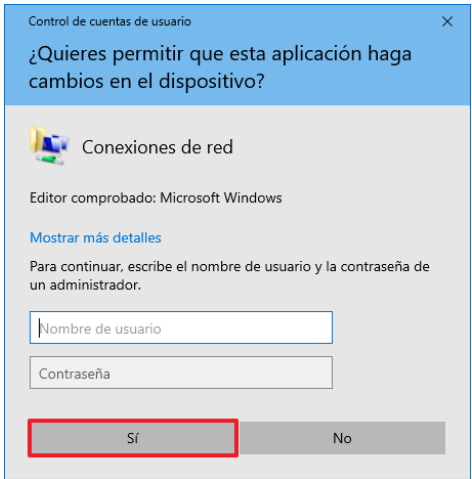
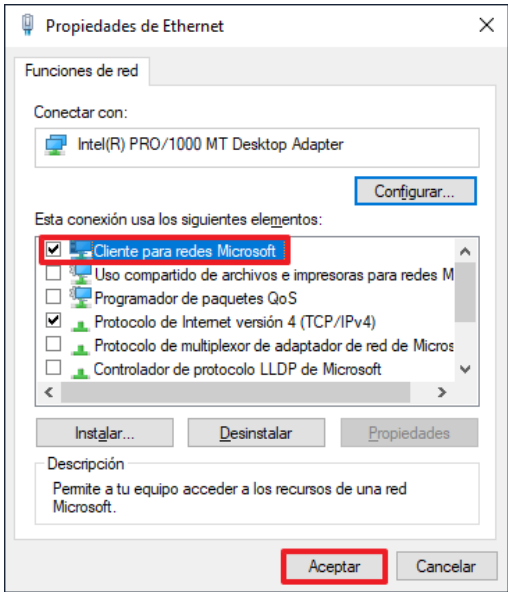
Paso	Descripción
21.	Pulse con el botón derecho del ratón sobre el servicio “Aplicación auxiliar de NetBIOS sobre TCP/IP” y seleccione la opción “Propiedades”. 
22.	En la nueva ventana abierta compruebe que el servicio se encuentra configurado en modo automático y pulse el botón “Modificar seguridad...” 
23.	En la nueva ventana abierta compruebe que el grupo de Administradores tiene el permiso concedido de “Control Total”. Asigne el permiso de “Control total” al usuario SYSTEM e INTERACTIVE. 

Paso	Descripción
24.	Pulse el botón “Aceptar” para guardar los cambios de los permisos.
25.	A la advertencia de seguridad que le aparecerá, pulse el botón “Sí” para continuar. 
26.	Guarde la plantilla ("C:\Windows\Security\Templates\CCN-STIC-599B19 Servicios.inf") con las modificaciones realizadas. Para ello utilice la opción "Guardar" del menú contextual que aparece al marcar con el botón derecho del ratón el nombre de la plantilla, como se muestra en la figura. 
27.	Cierre la consola de edición de plantillas. A la pregunta que aparecerá al cerrarla, "¿Guardar la configuración de la consola en Plantillas de seguridad.msc?", es indiferente que responda “Sí” o “No”.
28.	A continuación, vaya nuevamente a la carpeta “C:\Scripts” y pulse con el botón derecho sobre el fichero “CCN-STIC-599B19 Cliente independiente – Paso 6 –Servicios.bat” y pulse sobre la opción del menú contextual “Ejecutar como Administrador”. 

Paso	Descripción
29.	Cuando se le solicite, introduzca credenciales de administrador.
30.	Pulse una tecla para iniciar el proceso de reconfiguración de los servicios del sistema. 
31.	Una vez completado el proceso de configuración de servicios, pulse una tecla para finalizar el proceso. 
32.	Sobre la consola de PowerShell que todavía se encuentra abierta, ejecute la siguiente sintaxis "gpedit.msc" para abrir la consola de políticas locales. 

Paso	Descripción
33.	En el editor de directivas de grupo local despliegue el nodo “Directivas de equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”. Seleccione con doble clic la directiva “Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos”. 
34.	Cambie la configuración existente por la opción “Auditar todo”. Pulse el botón “Aceptar” para guarda el nuevo valor de configuración. 
35.	Cierre la consola del Editor de Directivas de grupo.

Paso	Descripción
36.	A continuación, en la barra de tareas, localice el icono de conexiones de red y pulsando con el botón derecho del ratón sobre él seleccione “Abrir Configuración de red e Internet”. 
37.	En el menú de configuración, seleccione la opción “Cambiar opciones del adaptador”. 
38.	Pulse con el botón derecho sobre el adaptador de red y seleccione “Propiedades”. 

Paso	Descripción
39.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local "Administradores". 
40.	En la ventana de Propiedades de las diferentes conexiones de red, además del "Protocolo de Internet versión 4 (TCP/IPv4)" (ya marcado durante la aplicación de la guía) marque también el elemento "Cliente para redes Microsoft". Pulse el botón "Aceptar" para guardar los cambios. 
41.	Ya habrá completado de realizar todos los cambios necesarios para realizar la conexión. Para finalizar borre el directorio "C:\Scripts" y reinicie el equipo para hacer efectiva la configuración, especialmente de los servicios.
42.	Una vez iniciada la sesión podrá conectarse a un recurso compartido remoto. Nota: Recuerde que si el cliente se comunica con un servidor existente en un dominio securizado con la guía CCN-STIC-570A el sistema remoto rechazará la conexión NTLM. Deberá crear una política incremental para dicho servidor, con objeto de permitir conexiones y autenticaciones remotas NTLM. Configure el sistema para permitir exclusivamente NTLMv2, rechazando LM y NTLM.

ANEXO B.3.7. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN

Tras la securización del sistema, existirían todavía determinados vectores de ataque, que deberán ser corregidos con el fin de evitar la evasión de los sistemas de autorización del sistema operativo. La exploración de dichos vectores de ataque podría ocasionar una posible exfiltración de la información gestionada y almacenada en el sistema, así como una potencial manipulación del comportamiento del mismo.

Para evitar esta situación, dentro del marco de seguridad establecido, se disponen de cuatro soluciones que se relaciona a continuación, y que pueden aplicarse de forma independiente o en conjunción las unas con las otras. Con posterioridad se detallará los mecanismos de su aplicación dentro del presente anexo, con objeto de mejorar la seguridad global del sistema.

Nota: Antes de aplicar las soluciones que se indican a continuación, verifique la compatibilidad de las mismas con su organización, y tenga en consideración los riesgos asumidos por la aplicación de dichas medidas.

Se recomienda verificar la adecuación e idoneidad de la solución para la organización en un entorno de pruebas o “preproducción” de forma previa a su aplicación en un entorno real o de “producción”.

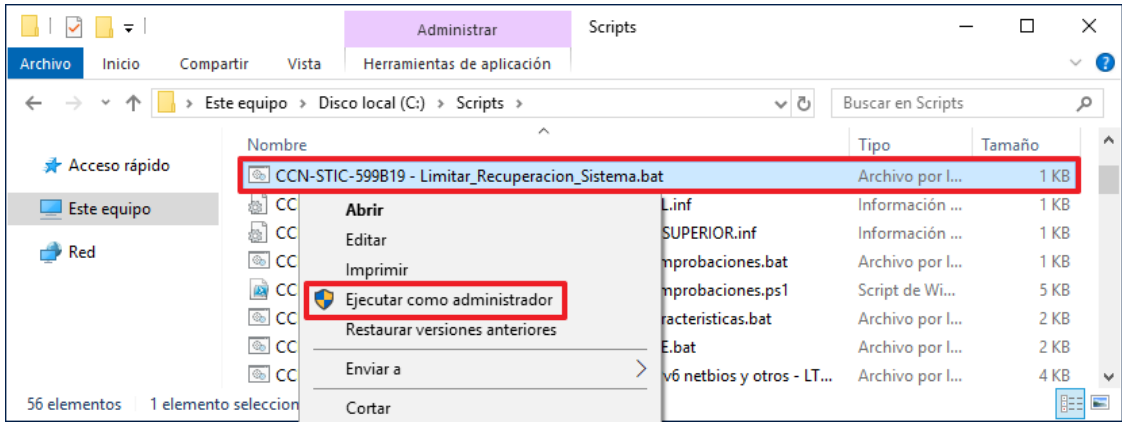
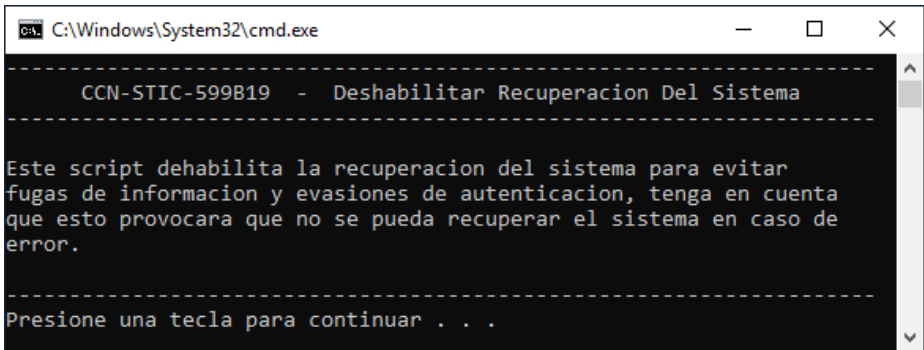
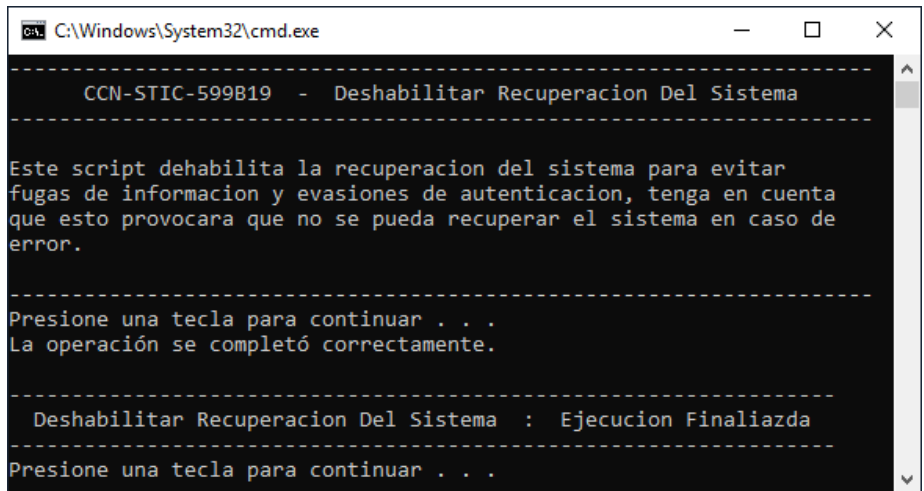
Las medidas a aplicar podrán ser:

- a) Cifrado del sistema de archivos. Utilizar BitLocker u otro sistema de cifrado autorizado para evitar el acceso a la información almacenada y, por tanto, evitar su modificación ya que requiere de la introducción de un PIN o contraseña en el arranque del equipo, o en el momento de acceder a los datos. De las opciones presentadas, ésta es la más recomendada. El presente anexo no incorpora cómo aplicar el mecanismo de protección de Bitlocker ya que ha sido convenientemente tratado en la presente guía.
- b) Deshabilitar la funcionalidad de restauración y/o recuperación del sistema a través de la utilidad “BCEDIT”.
- c) Deshabilitar las opciones de accesibilidad a través de claves de registro, evitando así que estas estén disponibles tanto si el usuario ha iniciado sesión como si no.
- d) Restaurar la integridad de los ficheros “C:\Windows\System32\sethc.exe” y “C:\Windows\System32\utilman.exe” al inicio del sistema.

1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

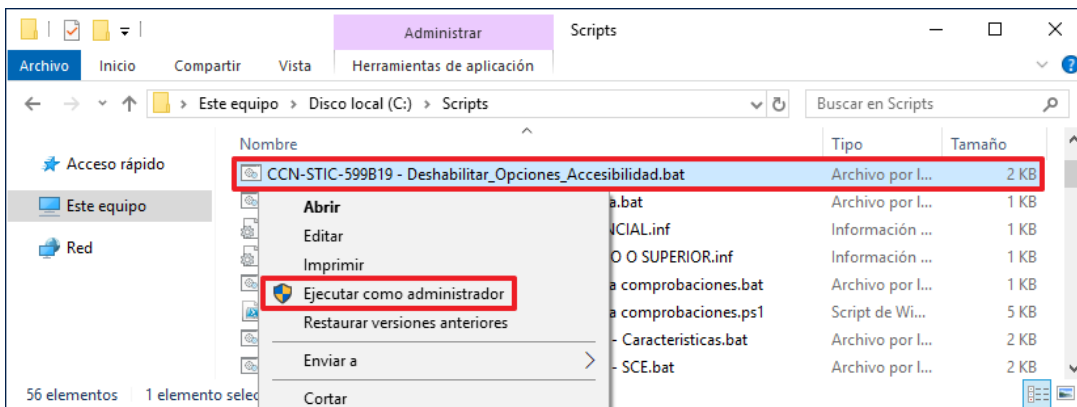
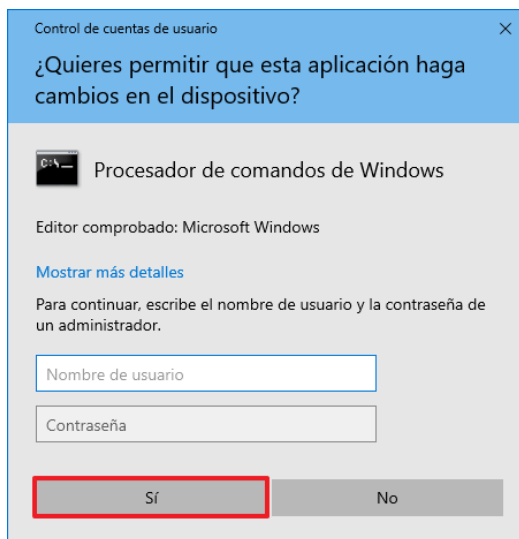
A continuación, se indican los pasos a realizar para deshabilitar la funcionalidad de recuperación del sistema.

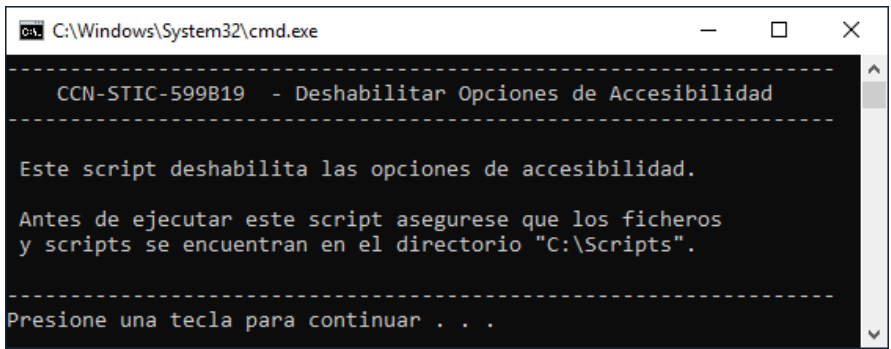
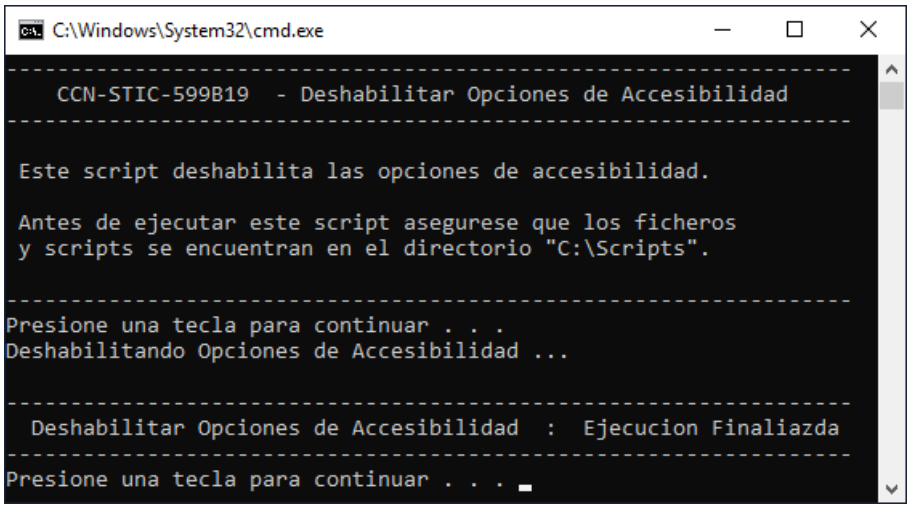
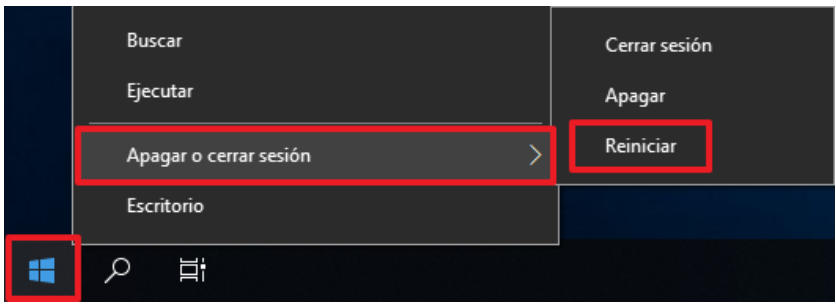
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.

Paso	Descripción
3.	Localice el archivo “CCN-STIC-599B19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”. 
4.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores”.
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script limitará el uso de las opciones de recuperación del sistema. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana. 
7.	Elimine el directorio “C:\Scripts”.

2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD

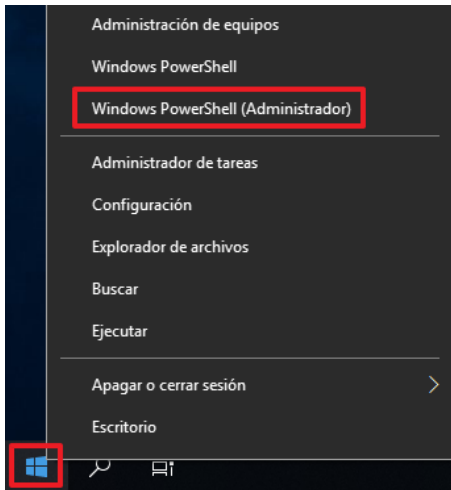
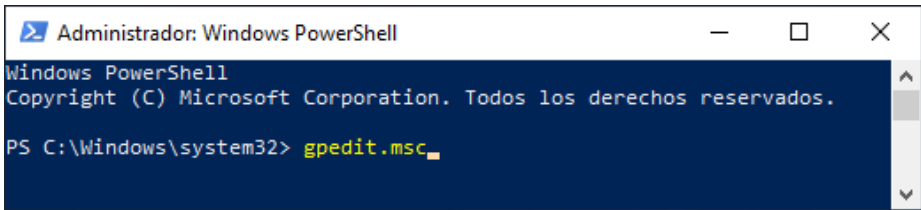
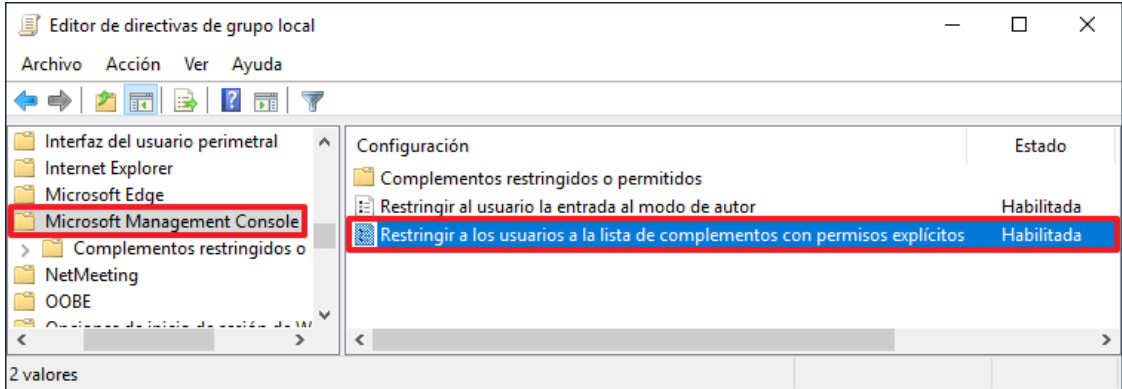
A continuación, se indican los pasos a realizar para deshabilitar las opciones de accesibilidad.

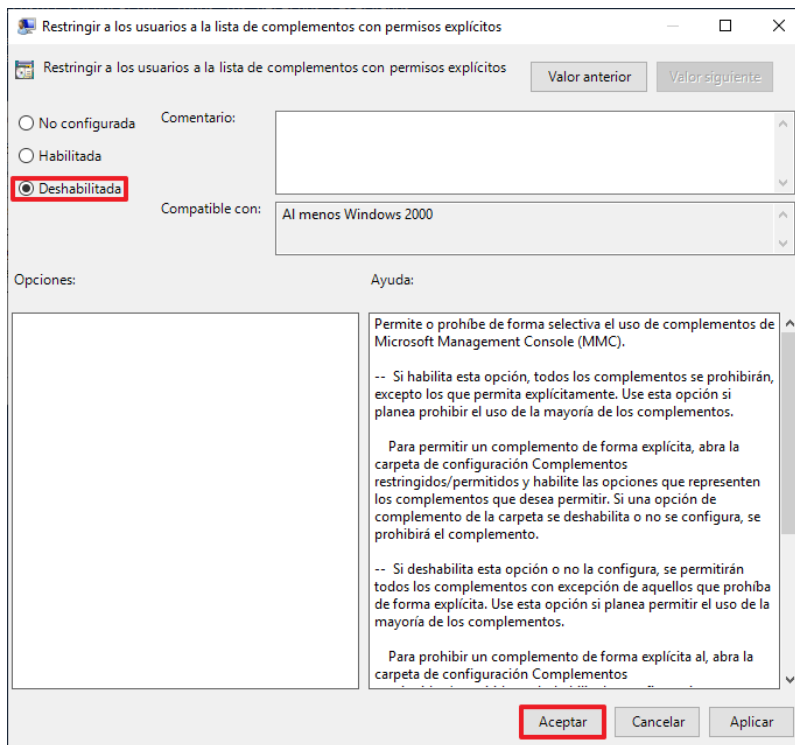
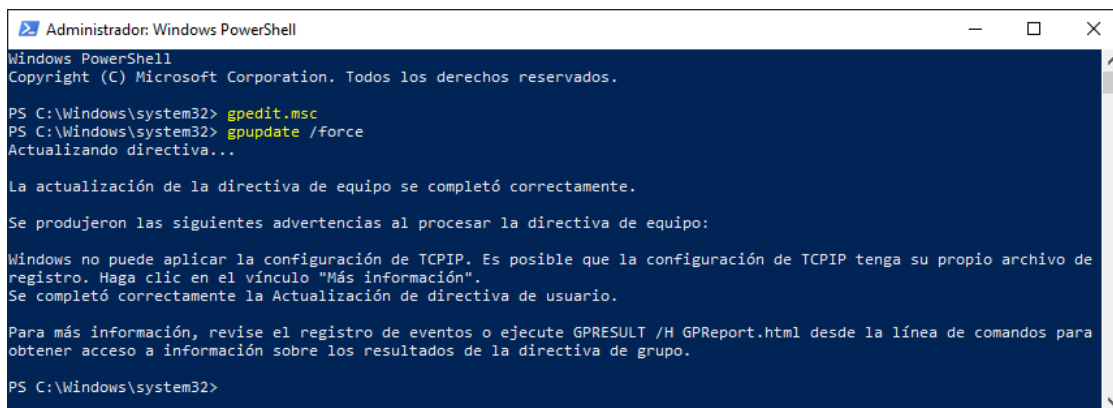
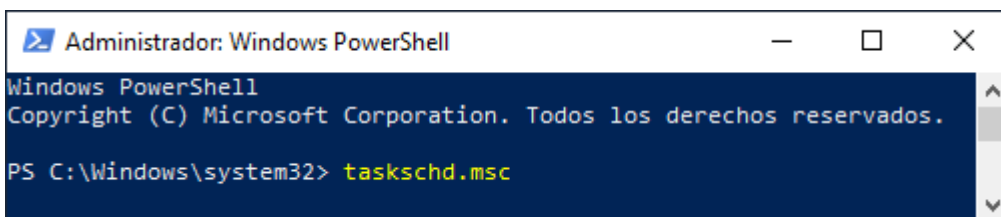
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
3.	Localice el archivo “CCN-STIC-599B19 – Deshabilitar_Opciones_Accesibilidad.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”. 
4.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores”. 

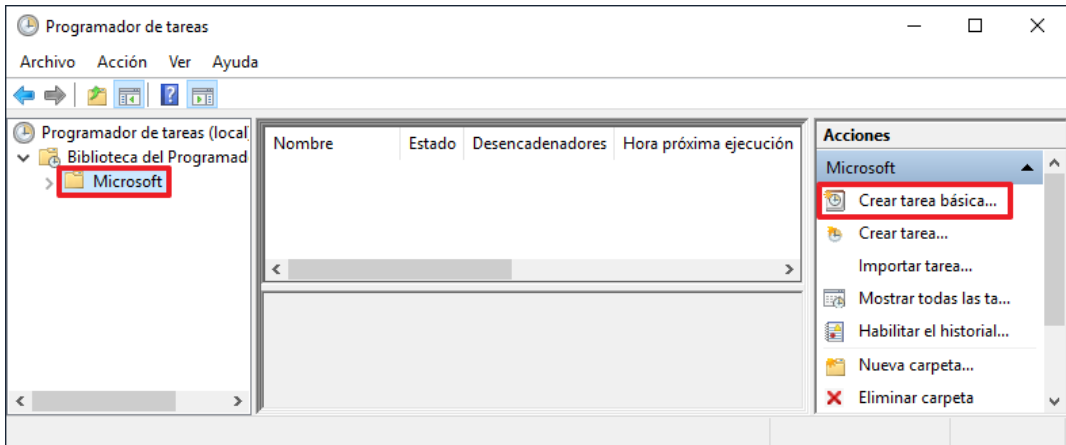
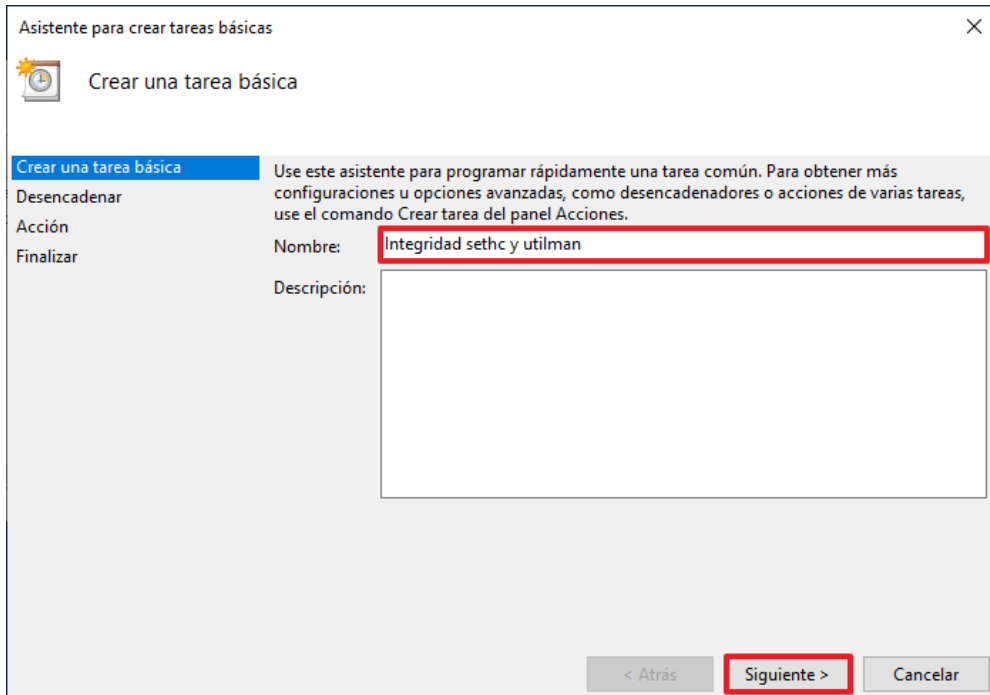
Paso	Descripción
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 
7.	Por último, deberá reiniciar el sistema para que los cambios sean aplicados. Para ello haga clic derecho en el botón “Inicio” y seleccione “Apagar o cerrar sesión → Reiniciar”. 
8.	Elimine el directorio “C:\Scripts”.

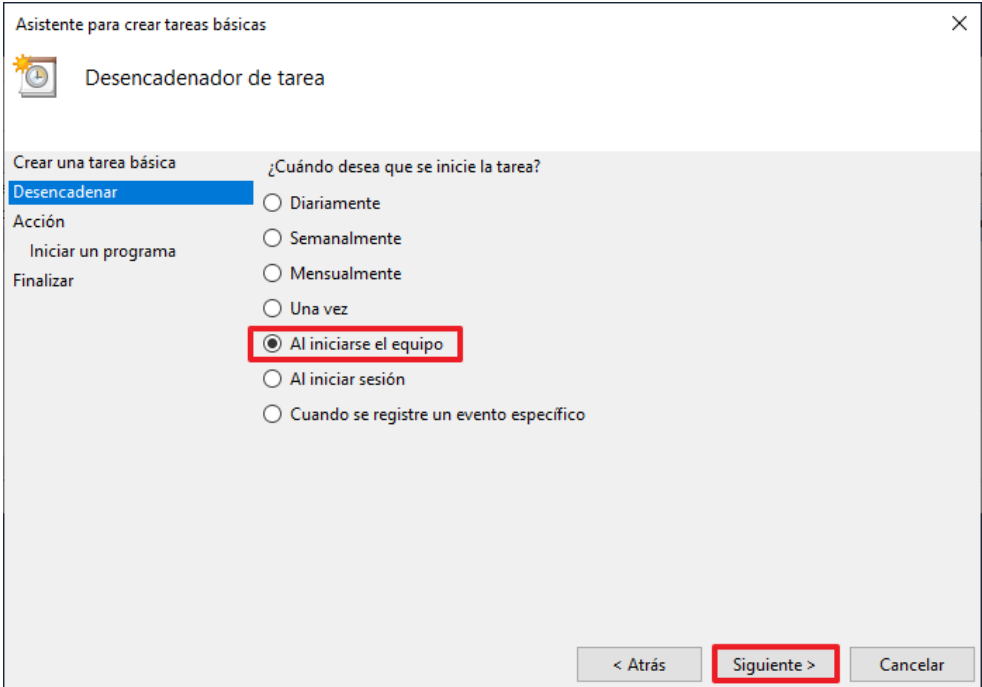
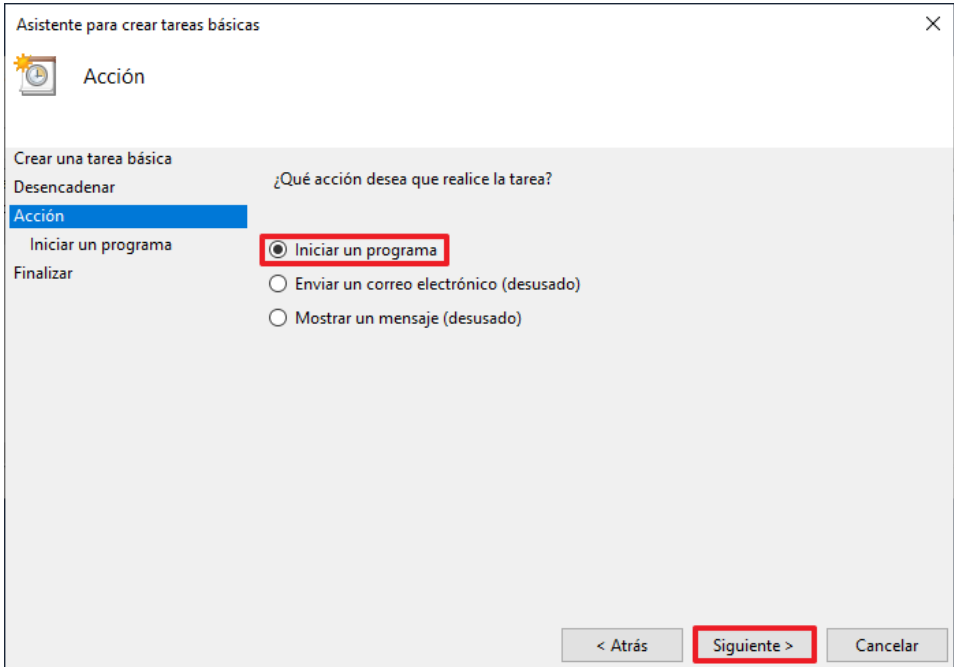
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

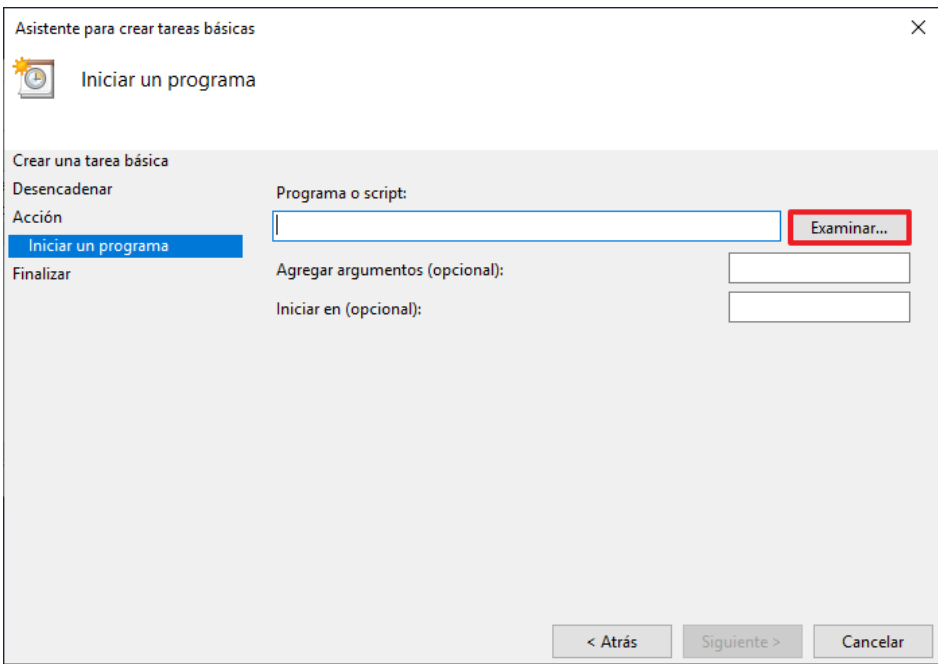
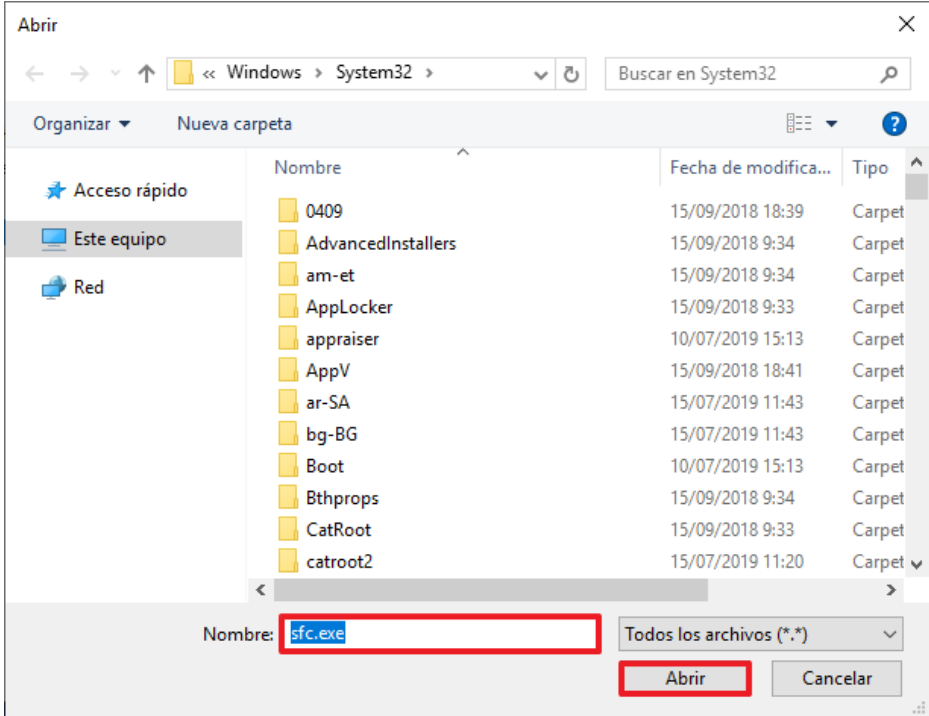
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

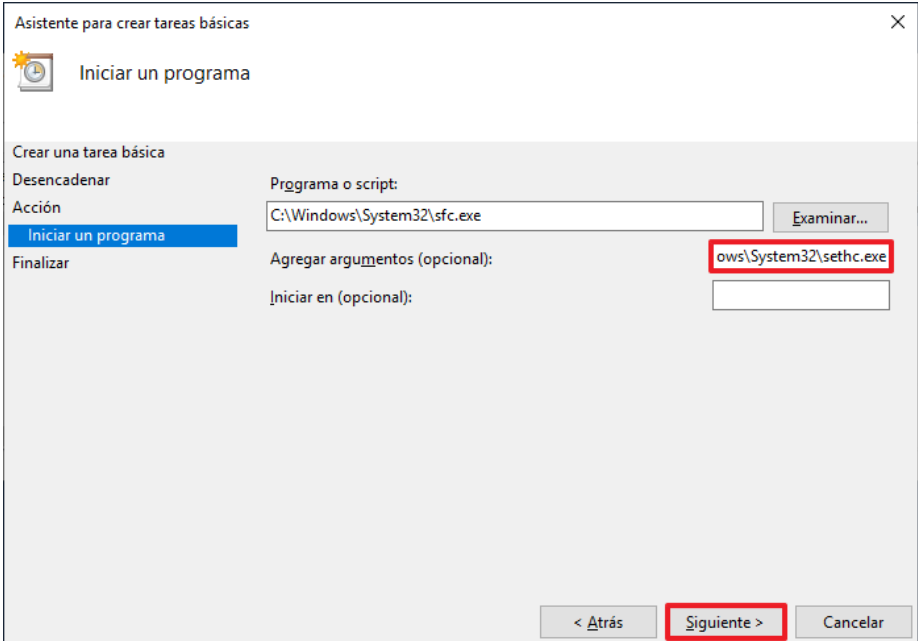
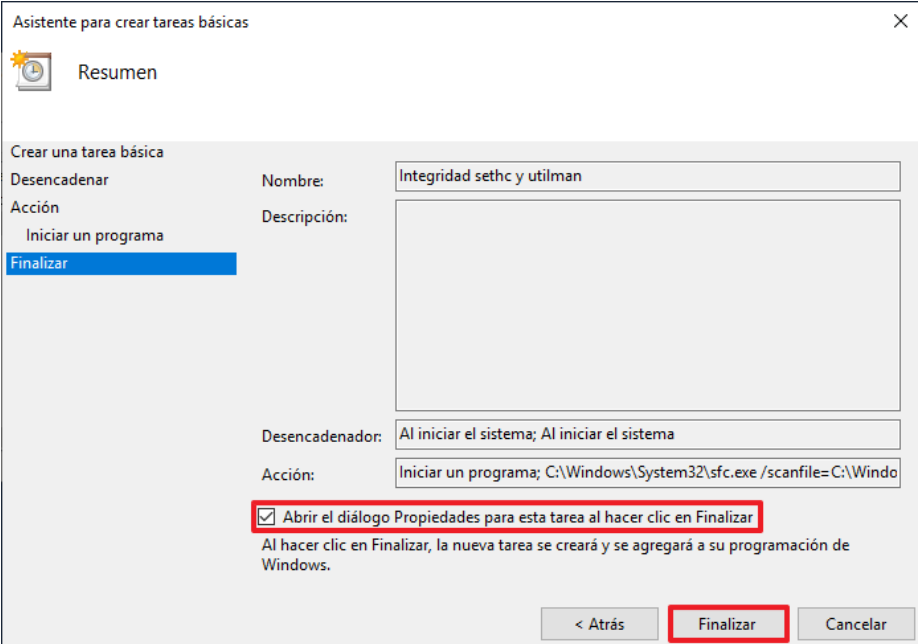
Paso	Descripción
1.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”.  Nota: El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.
2.	Una vez en la consola de PowerShell ejecute el comando “gpedit.msc” para iniciar el editor de directivas de grupo local. 
3.	En el editor de grupo local, sitúese en “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console” y localice la directiva “Restringir a los usuarios a la lista de complementos con permisos explícitos”. 

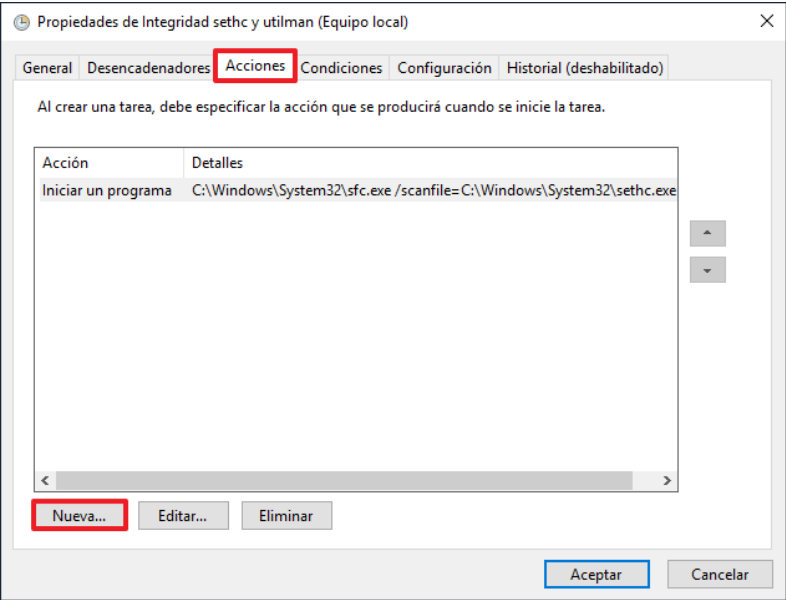
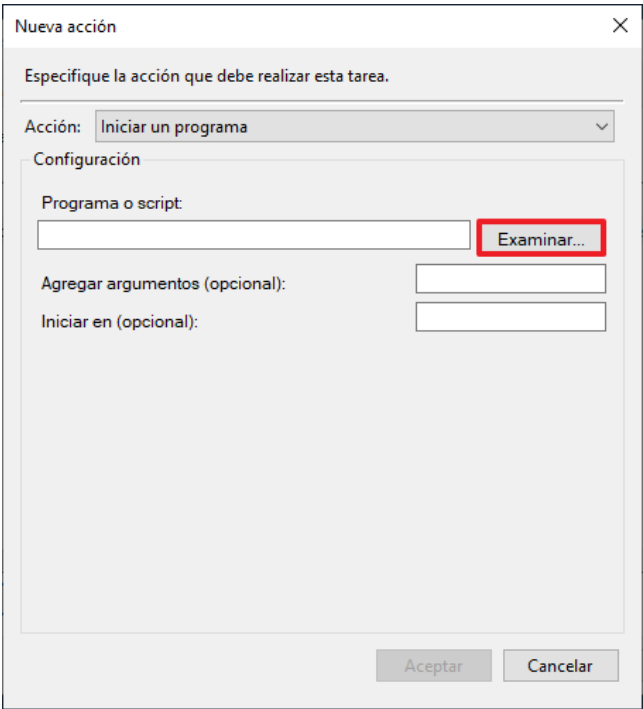
Paso	Descripción
4.	Edite la directiva “Restringir a los usuarios a la lista de complementos con permisos explícitos”, cambie su valor por “Deshabilitada” y haga clic en aceptar.  Nota: No cierre el Editor de directivas de grupo local hasta que se indique lo contrario.
5.	Vuelva a la consola de PowerShell y ejecute el comando “gpupdate /force” para actualizar la configuración de las directivas de grupo. 
6.	Ejecute el comando “taskschd.msc” en la misma consola de PowerShell para abrir el “Programador de tareas”. 

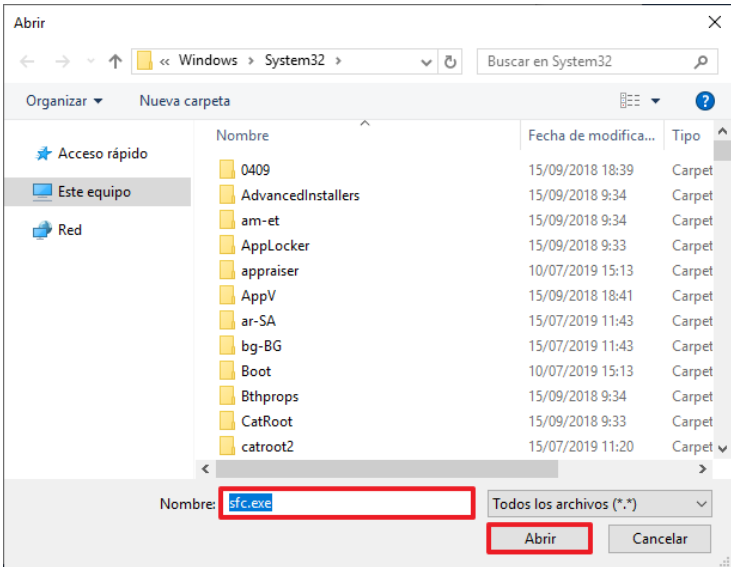
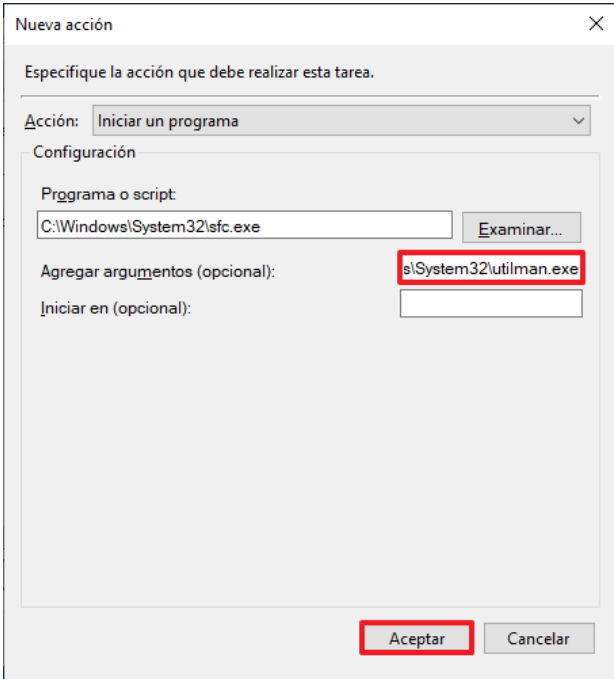
Paso	Descripción
7.	En el programador de tareas sitúese en la ruta “Biblioteca del Programador de tareas → Microsoft”. En el panel de “Acciones” situado en la parte derecha seleccione “Crear tarea básica”. 
8.	Se abrirá un asistente para la creación de la tarea programada. En la primera pestaña, indique el nombre de la tarea y pulse el botón “Siguiente >”.  Nota: En este caso el nombre designado para la tarea es “Integridad sethc y utilman”

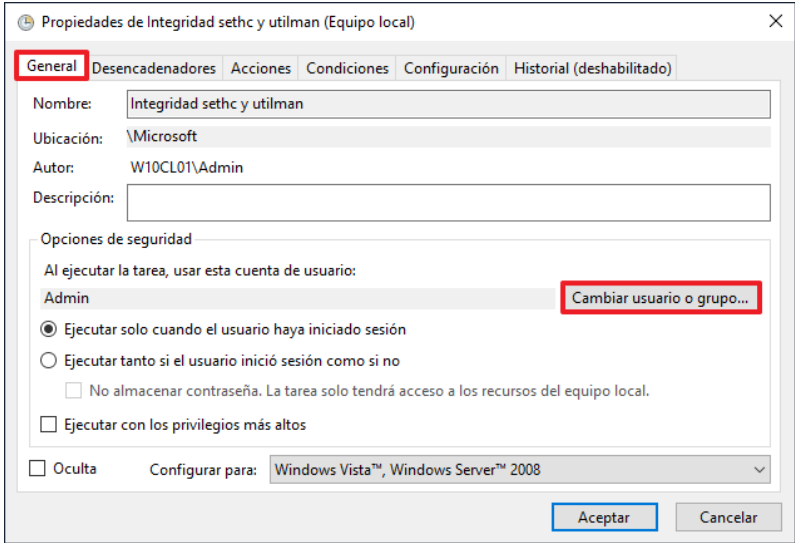
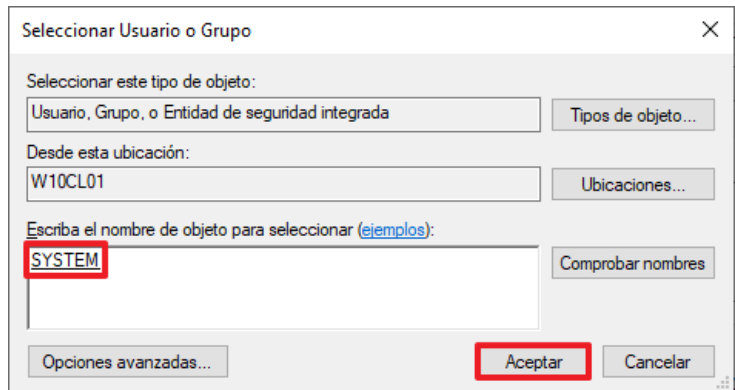
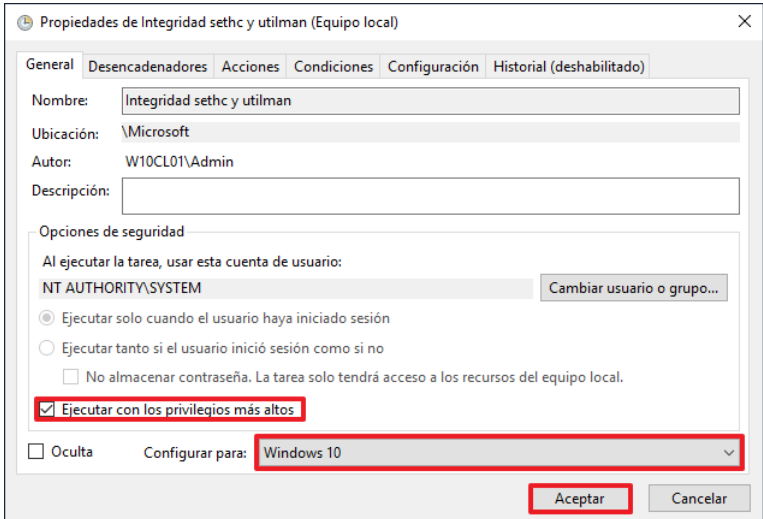
Paso	Descripción
9.	En la ventana “Desencadenar” del asistente seleccione “Al iniciarse el equipo” y pulse sobre el botón “Siguiente >”. 
10.	En la ventana “Acción” del asistente seleccione “Iniciar un programa” y haga clic sobre el botón “Siguiente >”. 

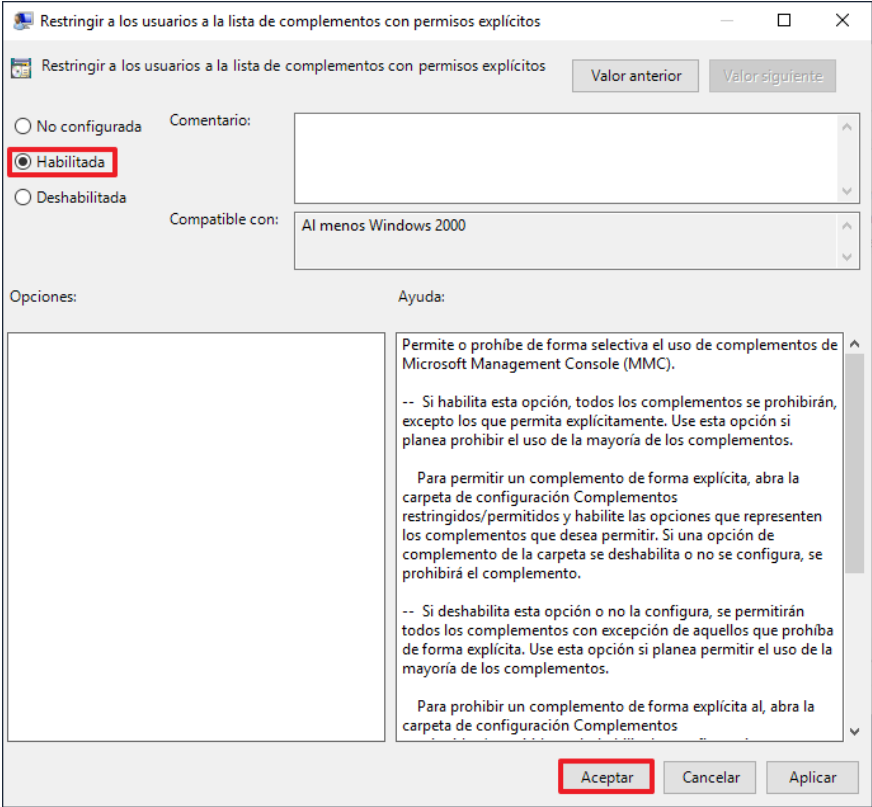
Paso	Descripción
11.	Haga clic sobre el botón “Examinar” para indicar que programa se ejecutará. 
12.	En la ventana emergente acceda a la ruta “C:\Windows\System32”, escriba en el apartado “Nombre” “sfc.exe” y haga clic sobre el botón “Abrir”. 

Paso	Descripción
13.	En el apartado “Agregar argumentos (opcional)” escriba “/scanfile=C:\Windows\System32\sethc.exe” para indicar al programa “sfc” que verifique la integridad del fichero “sethc.exe” situado en “C:\Windows\System32” y haga clic sobre el botón “Siguiente >”. 
14.	En la última ventana (Finalizar), marque la opción “Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar” y haga clic en “Finalizar”. 

Paso	Descripción
15.	Al hacer clic en “Finalizar”, se abrirá el diálogo de propiedades de la tarea, sitúese en la pestaña de “Acciones” y haga clic en “Nueva...”. 
16.	Se abrirá una ventana con la nueva acción a indicar, pulse sobre el botón “Examinar...”. 

Paso	Descripción
17.	En la ventana emergente acceda a la ruta "C:\Windows\System32", escriba en el apartado "Nombre:" "sfc.exe" y haga clic sobre el botón "Abrir". 
18.	En el apartado "Agregar argumentos (opcional)" escriba "/scanfile=C:\Windows\System32\utilman.exe" para indicarle al programa sfc que verifique la integridad del fichero utilman.exe situado en "C:\Windows\System32" y haga clic sobre el botón "Aceptar".  Nota: Si su sistema operativo es de 64 bits, repita el proceso del paso 15 al 18 con los ficheros "C:\Windows\SysWOW64\sethc.exe" y "C:\Windows\SysWOW64\utilman.exe".

Paso	Descripción
19.	A continuación, en la pestaña “General” del dialogo de propiedades de la tarea programada, haga clic en el botón “Cambiar usuario o grupo...”. 
20.	En la ventana emergente, introduzca el nombre “SYSTEM” y pulse aceptar. 
21.	Por último, marque la opción de “Ejecutar con los privilegios más altos”, establezca la opción “Windows 10” del desplegable “Configurar para:” y pulse en “Aceptar”. 

Paso	Descripción
22.	Cierre el programador de tareas.
23.	Vuelva al editor de directivas de grupo y edite la directiva “Restringir a los usuarios a la lista de complementos con permisos explícitos” situada en la ruta “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console”, cambie su valor por “Habilitada” y haga clic en “Aceptar”. 
24.	Cierre el editor de directivas de grupo.

ANEXO C. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN EL ENS COMO CLIENTE INDEPENDIENTE

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un puesto de trabajo con el sistema operativo Microsoft Windows 10 1809 en su versión Pro/Enterprise sin opción de mantenimiento LTSC según criterios del ENS.

Debido a las características de los puestos de trabajo a los que van dirigidas las guías de aplicación del Esquema Nacional de Seguridad, se toma la determinación de establecer la versión Microsoft Windows 10 Enterprise o Pro con las opciones de mantenimiento Canal Semi-Anual o Canal Semi-Anual (Dirigido) como las más adecuadas para su implementación, versión contemplada en este anexo. Esto se basa en los siguientes condicionantes:

- a) Estos equipos pueden estar conectados a Internet por lo cual determinadas funcionalidades como la tienda o Cortana, pueden ser utilizadas o no, en función de las necesidades de cada organización.
- b) El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.
- c) Las opciones de mantenimiento permiten garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con Microsoft Windows. No obstante, deben considerarse siempre las actualizaciones de seguridad como un elemento esencial para garantizar la seguridad de los puestos de trabajo en cualquier infraestructura.

Además de esta determinación existen varias configuraciones que son desactivadas durante la aplicación del “ANEXO C.4.2 CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA WINDOWS 10 INDEPENDIENTE” para garantizar la securización del sistema. Dichas características son:

- a) Sistema Experiencia de Usuario. Este componente se encuentra limitado por la aplicación de la presente guía.
- b) Sistema de telemetría. La configuración de telemetría de la organización deberá establecerse en función de las necesidades y acuerdos establecidos para la misma. En los pasos existentes en los Anexos, se detallará el proceso para que pueda establecer el nivel de telemetría de los sistemas MS Windows 10 existentes en su organización.

Por otro lado, Internet Explorer 11 podrá ser securizado según los mecanismos definidos en la guía CCN-STIC-520 destinada a redes clasificadas, y siguiendo la aplicación de la misma. Las políticas y configuraciones de dicha guía deberán ser adaptadas en función de las necesidades para asegurar el equipo cliente Microsoft Windows 10.

De manera análoga a lo citado anteriormente, el sistema podrá ser securizado con MS Office 2016 según los mecanismos definidos en la guía CCN-STIC-585, y siguiendo la aplicación de la misma. Las políticas y configuraciones de dicha guía deberán ser adaptadas en función de las necesidades para asegurar el equipo cliente Microsoft Windows 10.

No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas, puedan ser modificadas para adaptarlas a sus necesidades operativas.

Se ha de tener en consideración que, en el caso del ENS, el sistema operativo Microsoft Windows 10 se asume instalado y por lo tanto no se dedica ningún apunte respecto a su proceso de instalación.

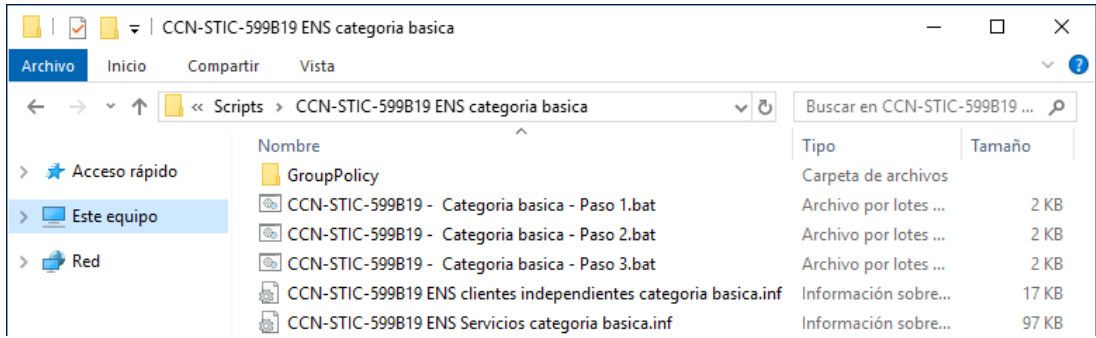
ANEXO C.1. CATEGORÍA BÁSICA

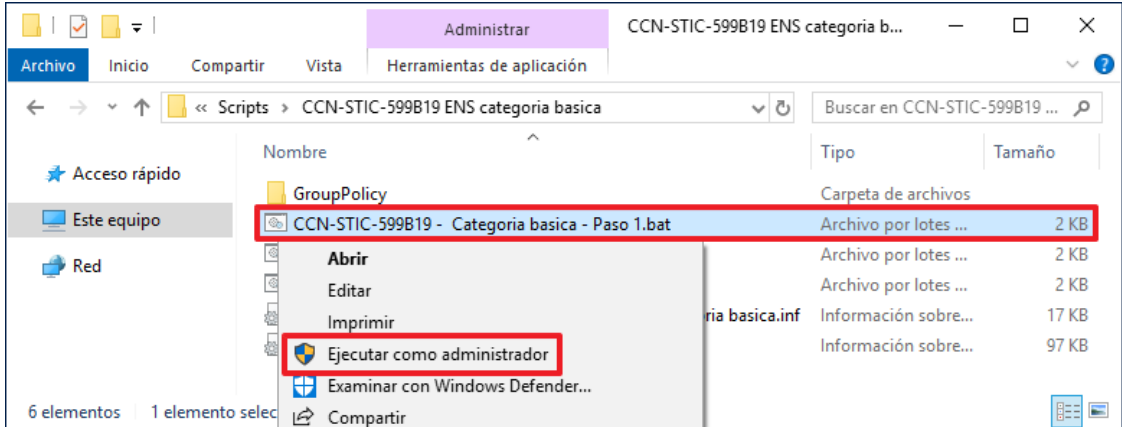
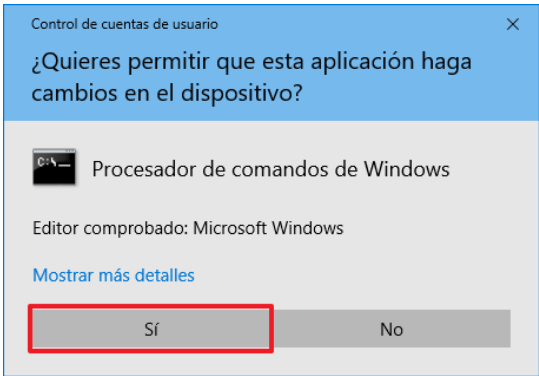
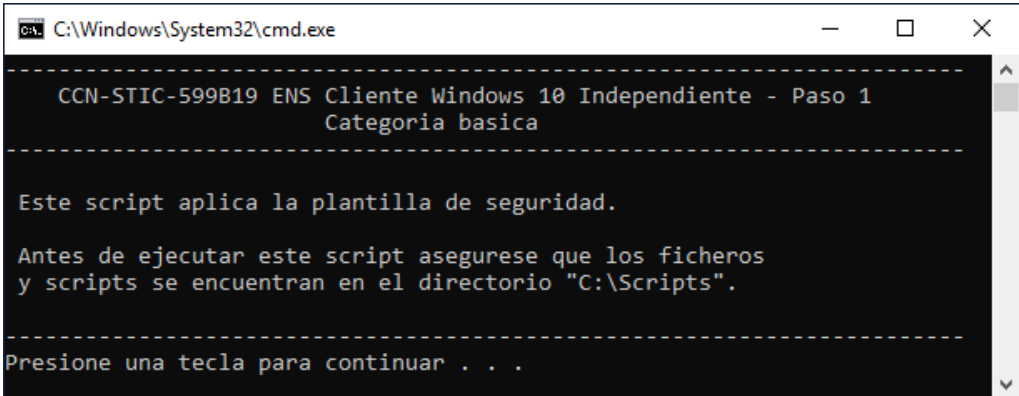
ANEXO C.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes Windows 10 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

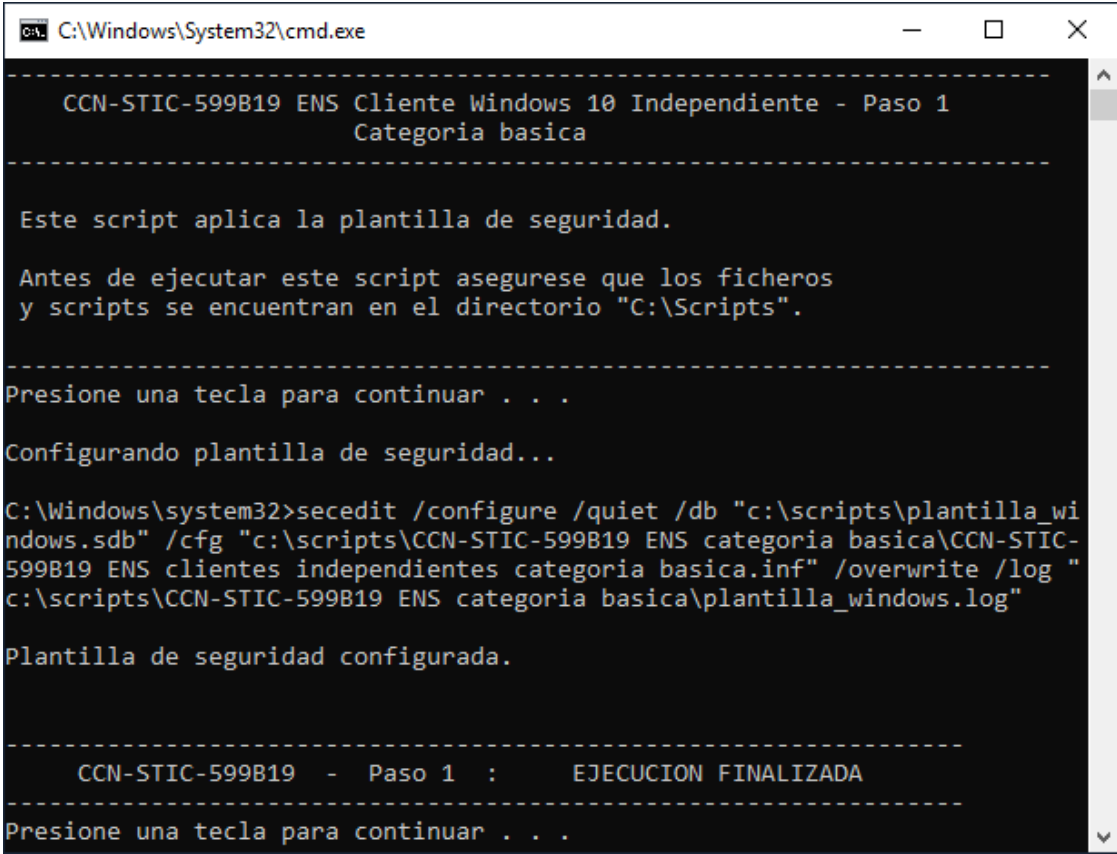
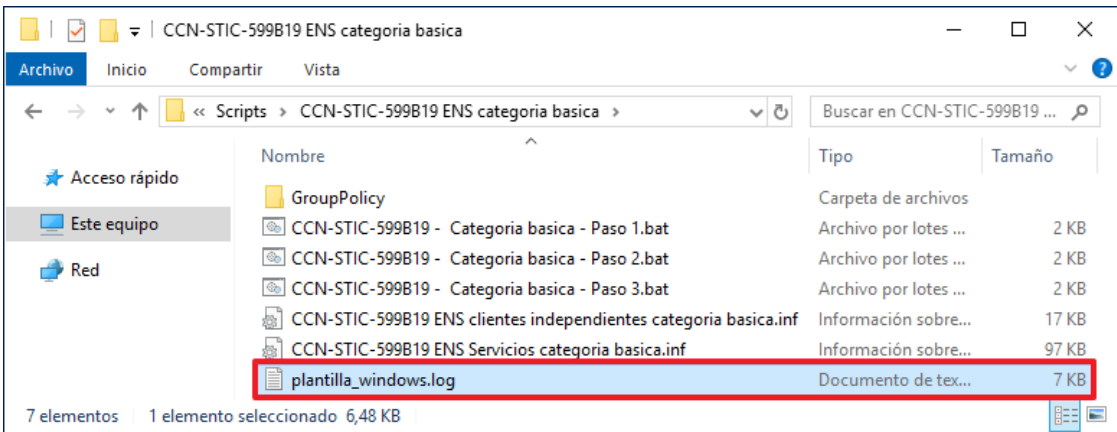
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

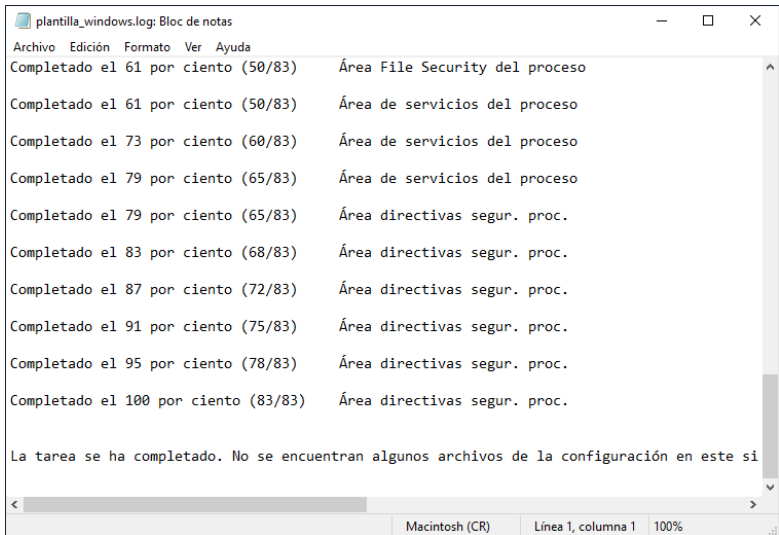
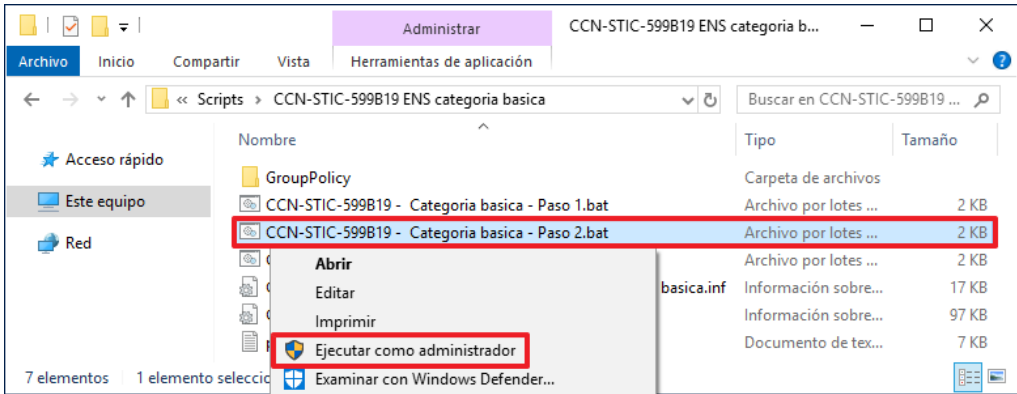
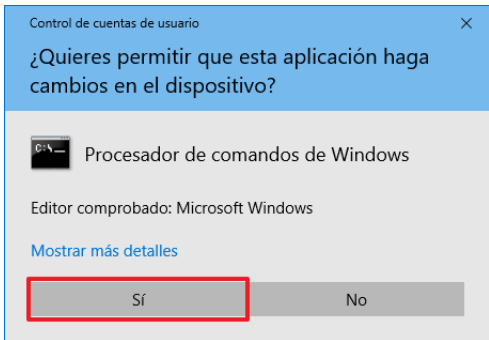
Los pasos que se describen a continuación se realizarán en todos aquellos clientes Windows 10 Pro/Enterprise (versión 1809) sin opción de mantenimiento LTSC, independientes a un dominio, que implementen servicios o información de categoría básica y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

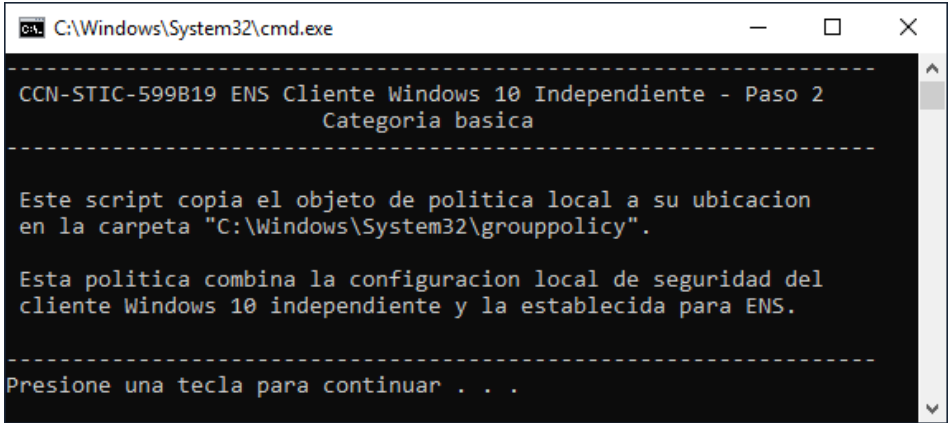
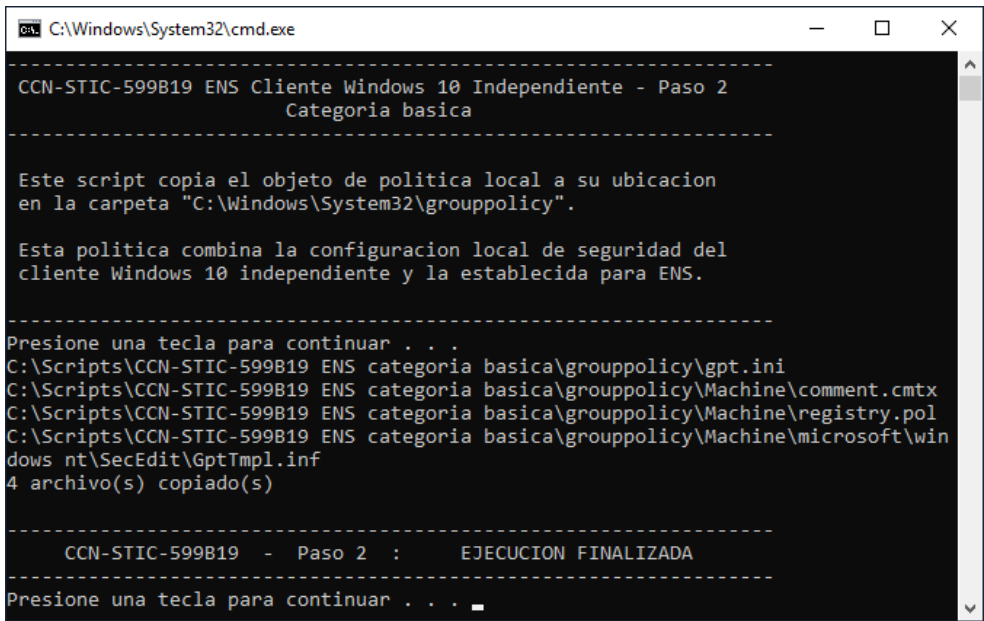
Paso	Descripción
1.	Inicie sesión en el cliente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea administrador local.
3.	Cree el directorio "Scripts" en la unidad "C:\".
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en la ruta "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19".
5.	Abra la carpeta "CCN-STIC-599B19 ENS categoria basica" que encontrará en el directorio "C:\Scripts".  Nota: Los scripts asumen que su ubicación es "C:\Scripts\CCN-STIC-599B19 ENS categoria basica". De no ser así deberá modificar los scripts para que coincida con la ruta deseada.

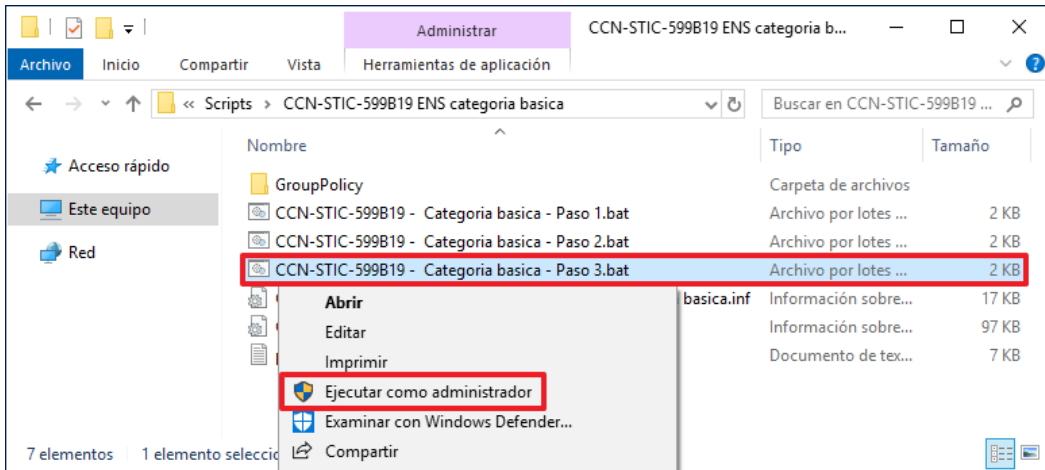
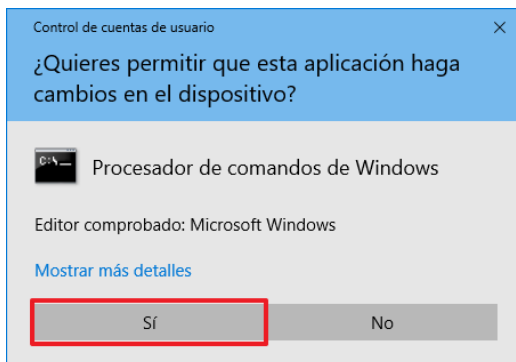
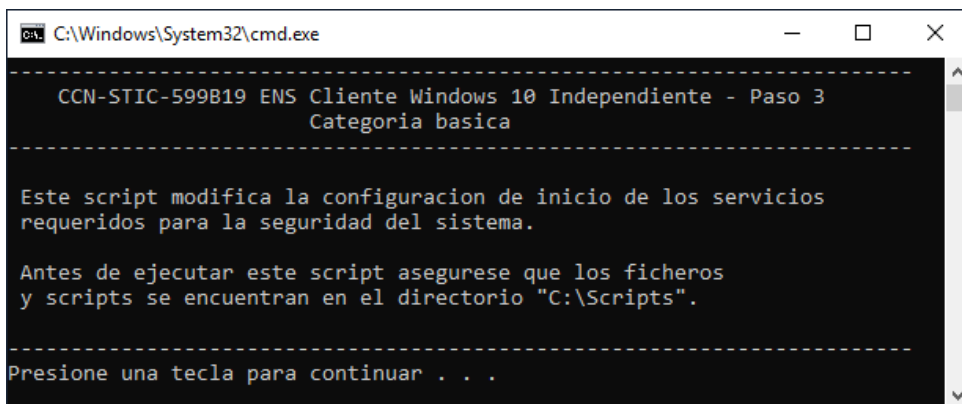
Paso	Descripción
6.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría básica – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”. 
7.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
8.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría básica del ENS. 



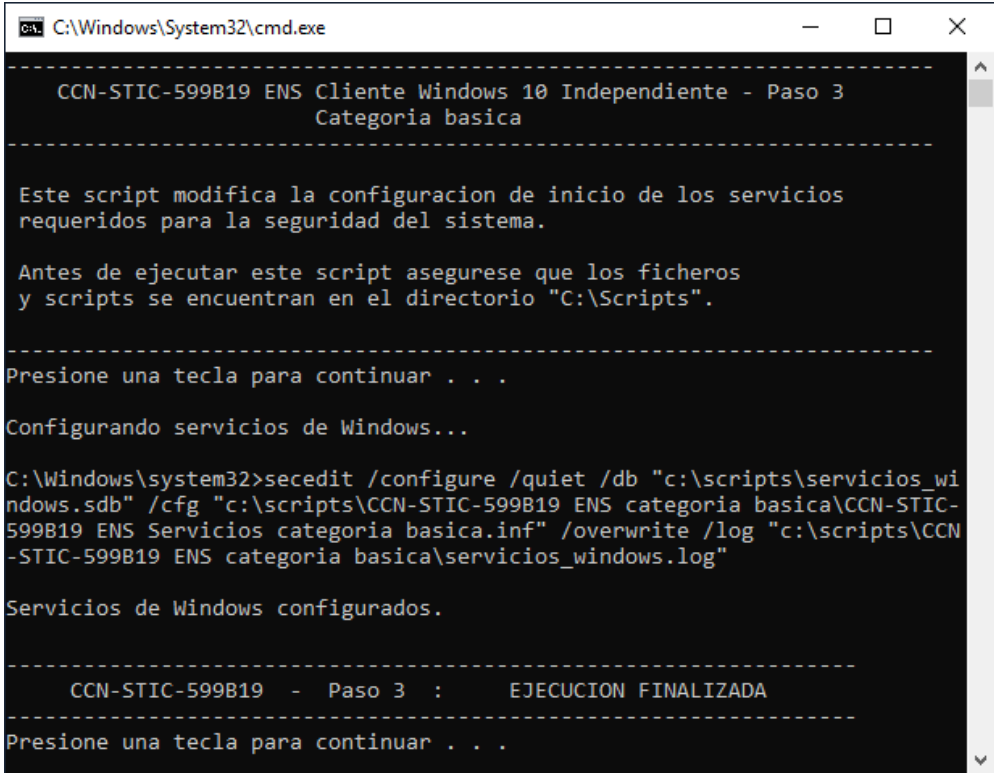
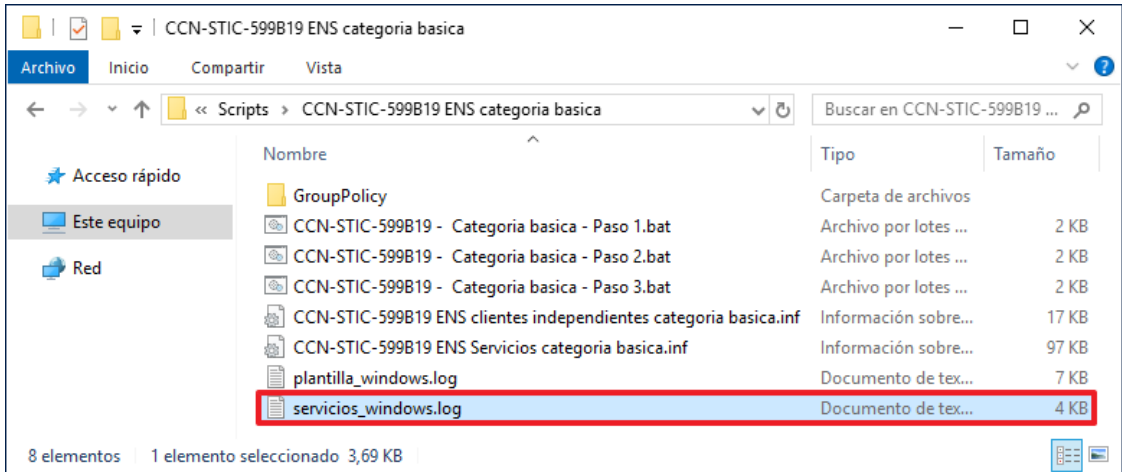
Paso	Descripción
9.	Una vez completado el proceso, deberá pulsar una tecla para continuar. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
10.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 categoria basica” con el nombre “plantilla_windows.log”. 

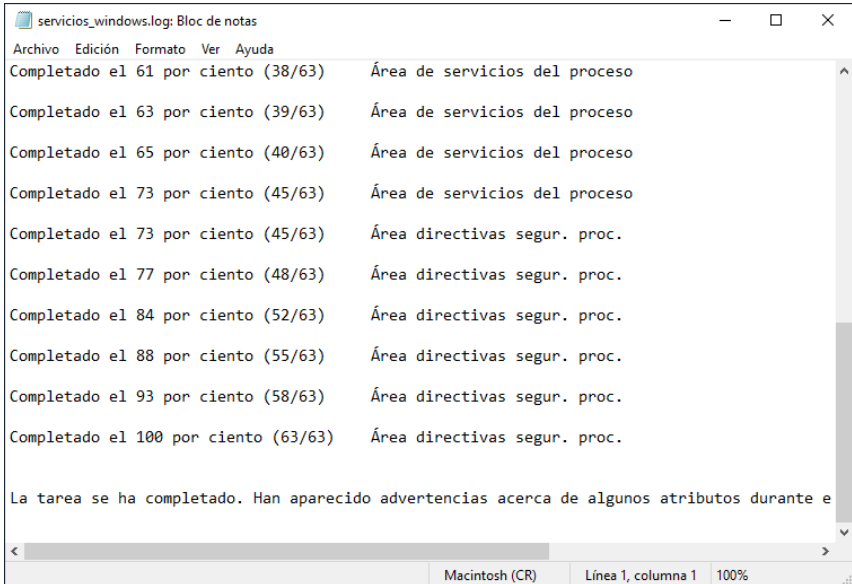
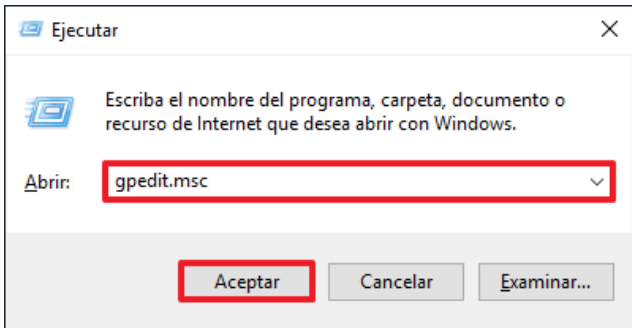
Paso	Descripción
11.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el procedimiento desde el paso 5.
12.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría básica – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”. 
13.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 

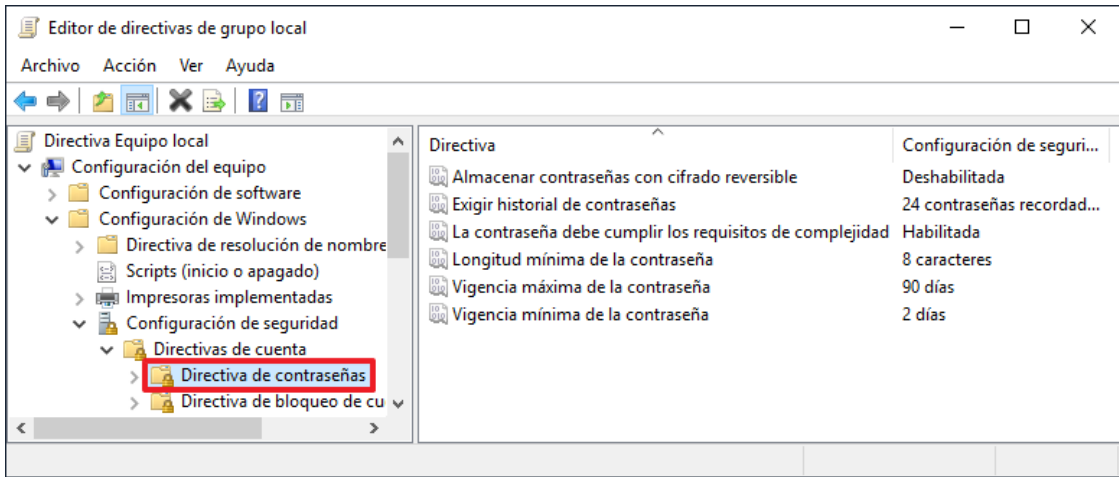
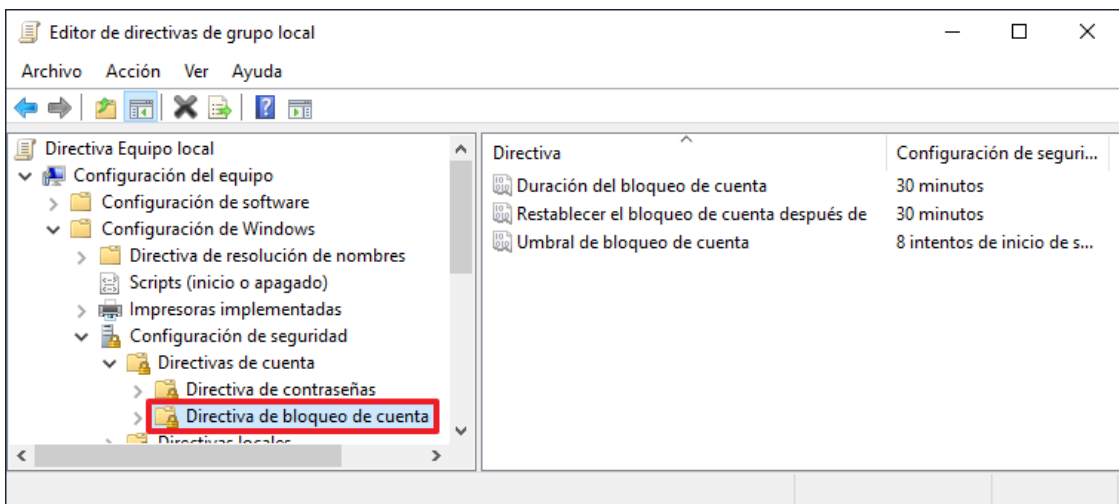
Paso	Descripción
14.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local. 
15.	Completada la copia de los archivos, compruebe que no ha habido errores en la copia de los mismos. Debería obtener el mismo resultado que el mostrado en la siguiente imagen. Pulse una tecla para finalizar la ejecución del script.  Nota: En caso de haberse producido fallos, soluciónelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.

Paso	Descripción
16.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría básica – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”. 
17.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
18.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría básica del ENS. 



Paso	Descripción
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 
20.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 ENS categoria basica” con el nombre de “servicios_windows.log”. 

Paso	Descripción
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados tal y como se muestra en la siguiente imagen.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el procedimiento desde el paso 16.
22.	Elimine la carpeta “C:\Scripts”.
23.	Es factible que su organización cuente con una política de contraseñas consolidada. La implementación de la política de categoría básica implementará una política específica para los clientes de categoría básica. Deberá evaluarla para determinar si esta configuración le es válida, o por el contrario deberá adaptarla a las condiciones de su organización.
24.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”. 
25.	Pulse “S” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.

Paso	Descripción
26.	Despliegue la política y sitúese en la siguiente ruta: “Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas” 
27.	Evalúe la política de contraseñas y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de credenciales es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
28.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que “Directiva de contraseñas”. 
29.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.

ANEXO C.1.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA BÁSICA

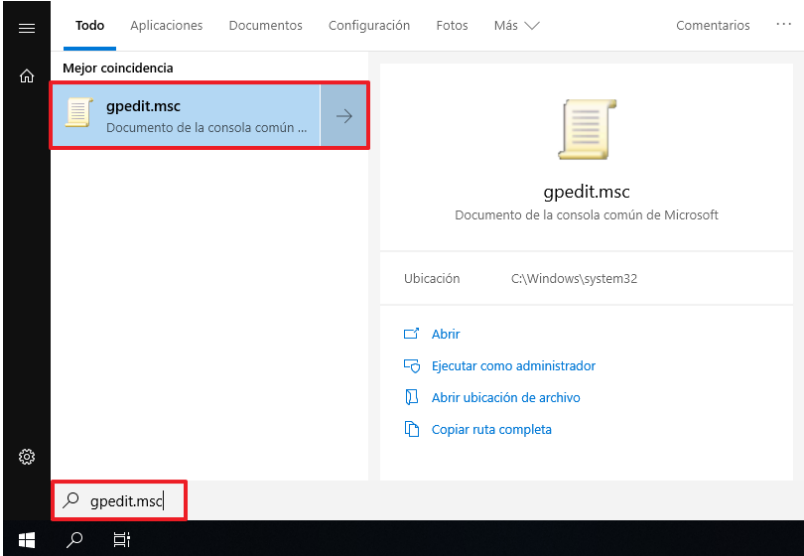
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO C.1.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS”.

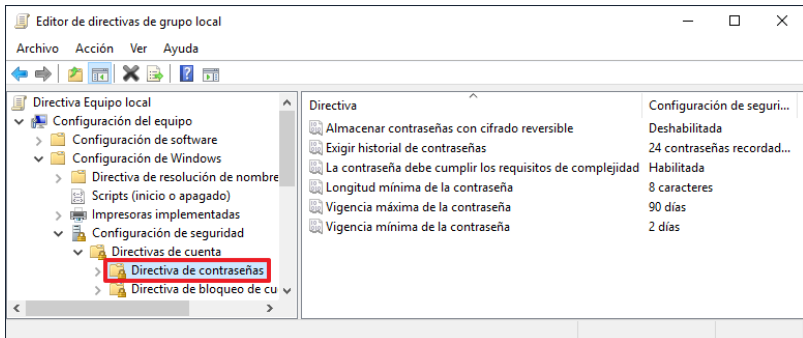
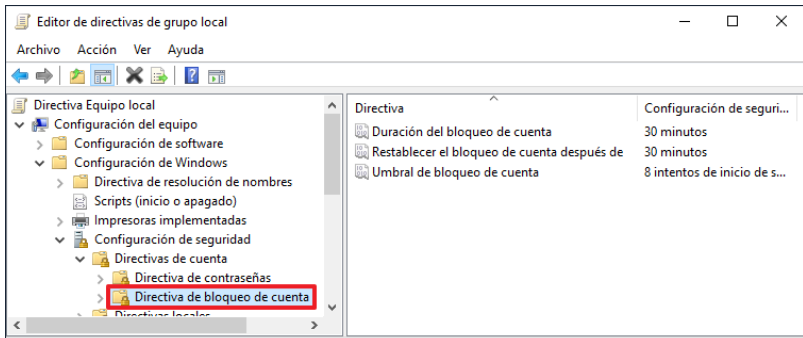
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC, independientes con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de administrador local.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario que es administrador local. Las consolas y herramientas que se utilizarán son las siguientes:

- Editor de objetos de directiva de grupo local (gpedit.msc).
- Editor de registro (regedit.exe).
- Visor de Eventos (eventvwr.exe).
- Servicios (services.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de administración local.
2. Inicie la aplicación de gestión de políticas locales.		Ejecute el “Editor de objetos de directiva de grupo local”. Para ello pulse “Inicio”, teclee “gpedit.msc” y pulse “Enter”. 

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas” Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. 
4. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta” 

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Duración del bloqueo de cuenta		30 minutos	
	Restablecer recuentos de bloqueo de cuenta tras		30 minutos	
	Umbral de bloqueo de cuenta		8 intentos de inicio de sesión no válidos	
5. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.	Seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”			
	Directiva		Valor	OK/NOK
	Auditar el acceso a objetos		Correcto, Erróneo	
	Auditar el acceso del servicio de directorio		Correcto, Erróneo	
	Auditar el cambio de directivas		Correcto, Erróneo	
	Auditar el uso de privilegios		Correcto, Erróneo	
	Auditar eventos de inicio de sesión		Correcto, Erróneo	
	Auditar eventos de inicio de sesión de cuenta		Correcto, Erróneo	
	Auditar eventos del sistema		Correcto, Erróneo	
	Auditar la administración de cuentas		Correcto, Erróneo	
6. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.	Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”			
	Directiva		Valor	OK/NOK
	Actuar como parte del sistema operativo		(Definida, pero sin ningún valor)	
	Administrar registro de seguridad y auditoría		Administradores	
	Agregar estaciones de trabajo al dominio		(Definida, pero sin ningún valor)	
	Actuar como parte del sistema operativo		(Definida, pero sin ningún valor)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red
		Apagar el sistema	Administradores, Usuarios
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL, Usuarios
		Aumentar prioridad de programación	Administradores
		Bloquear páginas en la memoria	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores
		Cargar y descargar controladores de dispositivo	Administradores
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)
		Crear objetos globales	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL
		Crear un archivo de paginación	Administradores
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)
		Crear vínculos simbólicos	Administradores
		Denegar el acceso desde la red a este equipo	ANONYMOUS LOGON, Invitados
		Denegar el inicio de sesión como servicio	Invitados
		Denegar el inicio de sesión como trabajo por lotes	Invitados
		Denegar el inicio de sesión local	Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red
		Generar perfiles de un solo proceso	Administradores

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Actuar como parte del sistema operativo	(Definida, pero sin ningún valor)
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtén un token de suplantación para otro usuario en la misma sesión	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Omitir comprobación de recorrido	SERVICIO LOCAL, Servicio de Red, Administradores, Usuarios Autenticados
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento de volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	(Definida, pero sin ningún valor)
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Tener acceso a este equipo desde la red	Administradores, Usuarios	
		Tomar posesión de archivos y otros objetos	Administradores	
		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
7. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente	(Definida, pero sin ningún valor)	
		Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
		Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Deshabilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, System\Microsoft\Windows NT\CurrentVersion
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	System\CurrentControlSet\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada
		Apagado: borrar el archivo de paginación de la memoria virtual	Deshabilitada
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Deshabilitada
		Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Deshabilitada
		Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitada
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitada
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de registro en diferentes ubicaciones por usuario	Habilitada
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, Firma y operaciones hash	Deshabilitada
		Cuentas: cambiar el nombre de cuenta de invitado	Invitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Cuentas: cambiar el nombre de la cuenta de administrador	Administrador
		Cuentas: estado de la cuenta de administrador	Deshabilitada
		Cuentas: estado de la cuenta de invitado	Deshabilitada
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Deshabilitada
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Habilitada
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		Inicio de sesión interactivo: mostrar información de usuario cuando bloquee la sesión	No mostrar la información del usuario
		Inicio de sesión interactivo: No mostrar último inicio de sesión	Habilitada
		Inicio de sesión interactivo: No requerir Ctrl + Alt + Supr	Deshabilitada
		Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	1 inicios de sesión
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada
		Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	Deshabilitada
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada
		Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada
		Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM	
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
		Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits	
		Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir cifrado de 128 bits	
		Servidor de red de Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	30 minutos	
		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
8. Verifique la directiva de almacén digital en el objeto de directiva de grupo local.		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
9. Verifique la directiva de asistencia en línea en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	
10. Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	
11. Verifique las directivas de contenido en la nube en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Contenido en la Nube”		
		Directiva	Valor	OK/NOK
		Desactivar experiencias del consumidor de Microsoft	Habilitada	
		No mostrar recomendaciones de Windows	Habilitada	
12. Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	

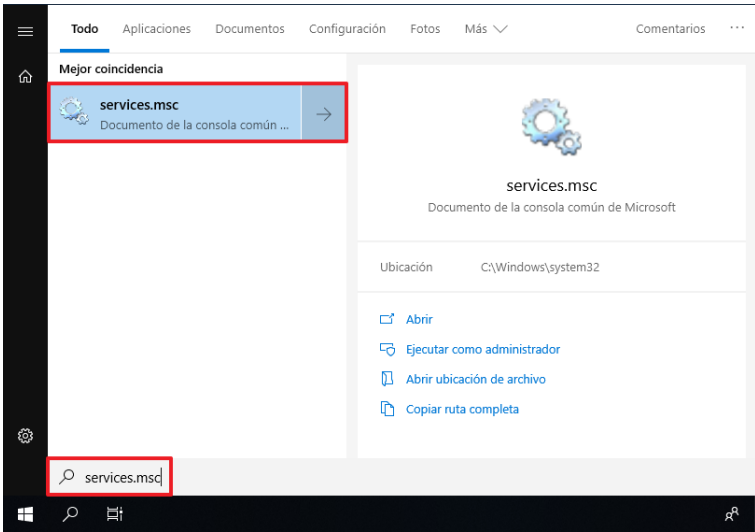
Comprobación	OK/NOK	Cómo hacerlo		
13.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		No enviar datos adicionales	Habilitado	
		Deshabilitar el informe de errores de Windows	Habilitado	
14.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		
		Directiva	Valor	OK/NOK
		Impedir la administración del filtro SmartScreen	Deshabilitado	
		Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	Habilitado	
		Activar sitios sugeridos	Deshabilitado	
15.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Eliminar el historial de exploración”		
		Directiva	Valor	OK/NOK
		Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento.	Deshabilitado	
		Impedir que se elimine el historial de descarga	Deshabilitado	
		Impedir que se eliminen contraseñas	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir que se eliminen cookies	Deshabilitado	
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitado	
		Impedir que se eliminen los archivos temporales de Internet	Deshabilitado	
		Impedir que se eliminen los datos de filtrado InPrivate	Deshabilitado	
		Impedir que se eliminen los datos de formularios	Deshabilitado	
		Impedir que se eliminen los sitios web que el usuario visitó	Deshabilitado	
		Permitir que se elimine el historial de exploración al salir	Habilitado	
16.Verifique las directivas de OneDrive en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	
17.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas.	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows controlen las radios	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitado (Forzar denegación)

Comprobación	OK/NOK	Cómo hacerlo		
18.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”		
		Directiva	Valor	OK/NOK
		No volver a mostrar notificaciones de comentarios	Habilitado	
		Permitir telemetría	Habilitado	
19.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
20.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
21.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitado	
		Desactivar sensores	Habilitado	
		Desactivar ubicación	Habilitado	
22.Verifique la directiva de Windows Update en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	
23.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del equipo → Plantillas Administrativas → Sistema → Perfiles de usuario”		
		Directiva	Valor	OK/NOK
		Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
24.Verifique el modo de configuración de los servicios del sistema.		Ejecute la herramienta de servicios. Para ello pulse “Inicio”, teclee “services.msc” y pulse “Enter”.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto, entre paréntesis) para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de escucha Net.Msmq	NetMsmqActivator	Automático	Configurado	
Adaptador de escucha Net.Pipe	NetPipeActivator	Automático	Configurado	
Adaptador de escucha Net.Tcp	NetTcpActivator	Automático	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado	
Administración de aplicaciones	AppMgmt	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Manual	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Automático	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de cuentas web	TokenBroker	Manual	Configurado		
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMGrSvc	Manual	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Automático	Configurado		
Agrupación de red del mismo nivel	p2psvc	Manual	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Manual	Configurado		
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Audio de Windows	Audiosrv	Automático	Configurado		
Autenticación natural	NaturalAuthentication	Manual	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		
CaptureService	CaptureService	Manual	Configurado		
Carpetas de trabajo	workfoldersvc	Manual	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente para NFS	NfsClnt	Automático	Configurado		
Cliente web	WebClient	Manual	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Automático	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Conexiones de red	Netman	Manual	Configurado		
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración automática de WLAN	WlanSvc	Manual	Configurado		
Configuración automática de WWAN	WwanSvc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado		
ConsentUX	ConsentUxUserSvc	Manual	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Automático	Configurado		
Detección de hardware shell	ShellHWDetection	Automático	Configurado		
Detección SSDP	SSDPSRV	Manual	Configurado		
DevicePicker	DevicePickerUserSvc	Manual	Configurado		
DevicesFlow	DevicesFlowUserSvc	Manual	Configurado		
Diagnostic Execution Service	diagsvc	Manual	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Manual	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
Energía	Power	Automático	Configurado		
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado		
Escucha de RIP	iprip	Automático	Configurado		
Estación de trabajo	LanmanWorkstation	Automático	Configurado		
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado		
Examinador de equipos	Browser	Manual	Configurado		
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado		
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado		
Fax	Fax	Manual	Configurado		
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado		
Firewall de Windows	MpsSvc	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado	
Hora de Windows	W32Time	Manual	Configurado	
Host de proveedor de detección de función	fdPHost	Manual	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Manual	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Manual	Configurado	
Identidad de aplicación	AppIDSvc	Manual	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Manual	Configurado	
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado	
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado	
Instantáneas de volumen	VSS	Manual	Configurado	
Instrumental de administración de Windows	Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado	
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado	
LxssManager	LxssManager	Manual	Configurado	
Message Queue Server	MSMQ	Automático	Configurado	
MessagingService	MessagingService	Manual	Configurado	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado	
Microsoft Passport	NgcSvc	Manual	Configurado	
Modo incrustado	embeddedmode	Manual	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Automático	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	Configurado		
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Manual	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Manual	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Manual	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado		
Registrador de configuración de Windows Connect Now	wcncsvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Manual	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Manual	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático	Configurado		
Servicio AVCTP	BthAvctpSvc	Manual	Configurado		
Servicio biométrico de Windows	WbioSrv	Manual	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Automático	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado		
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado		
Servicio de administración de radio	RmSvc	Manual	Configurado		
Servicio de administración de web	WMSVC	Manual	Configurado		
Servicio de administración de Windows	WManSvc	Manual	Configurado		
Servicio de administración IIS	IISADMIN	Automático	Configurado		
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Manual	Configurado		
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asistente para perfil local	wlpasvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Automático	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de cliente de protección de host	HgClientService	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de datos espacial	SharedRealitySvc	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado	
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado	

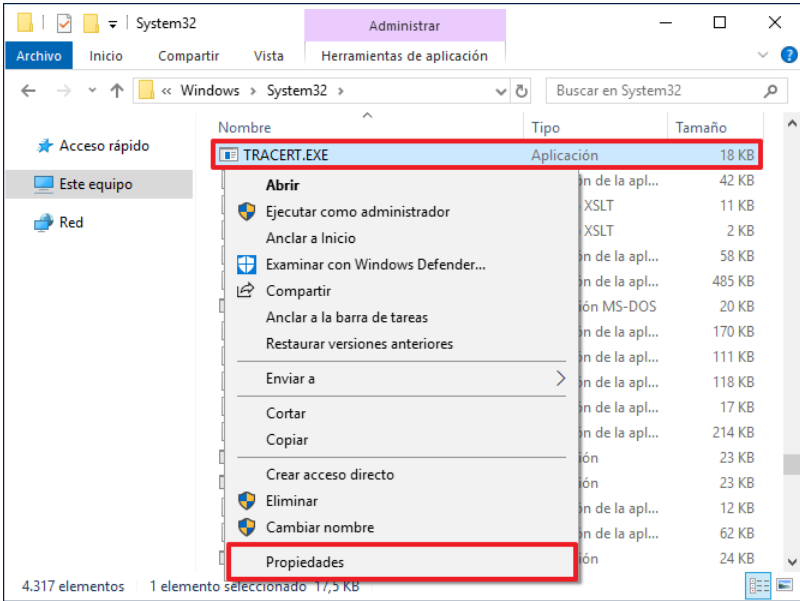
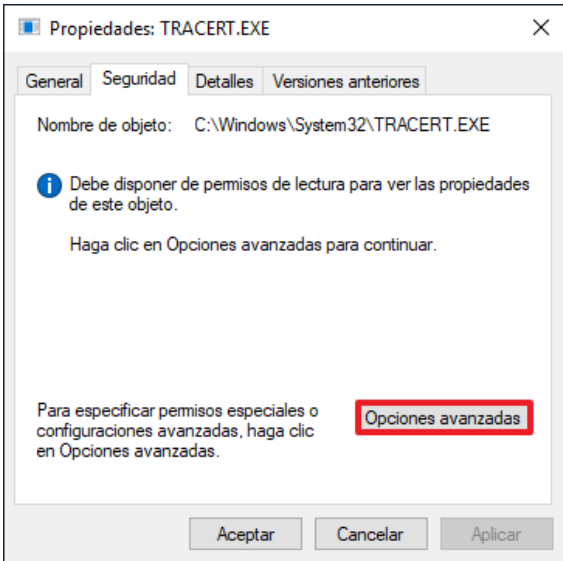
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado		
Servicio de geolocalización	lfsvc	Manual	Configurado		
Servicio de historial de archivos	fhsvc	Manual	Configurado		
Servicio de host HV (Hyper-V)	HvHost	Manual	Configurado		
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado		
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado		
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de instalación de Microsoft Store	InstallService	Manual	Configurado		
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de mejora de visualización	DisplayEnhancementService	Manual	Configurado		
Servicio de monitor de infrarrojos	irmon	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		

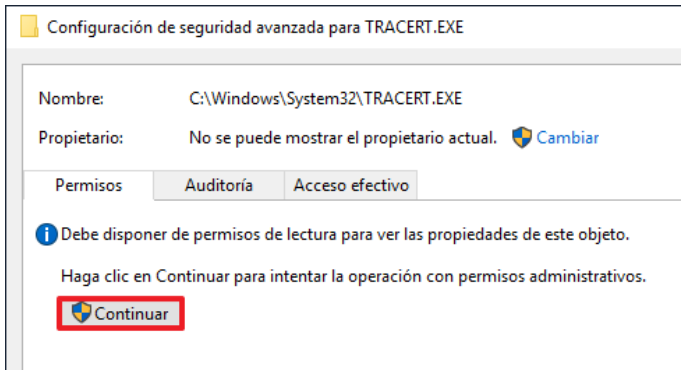
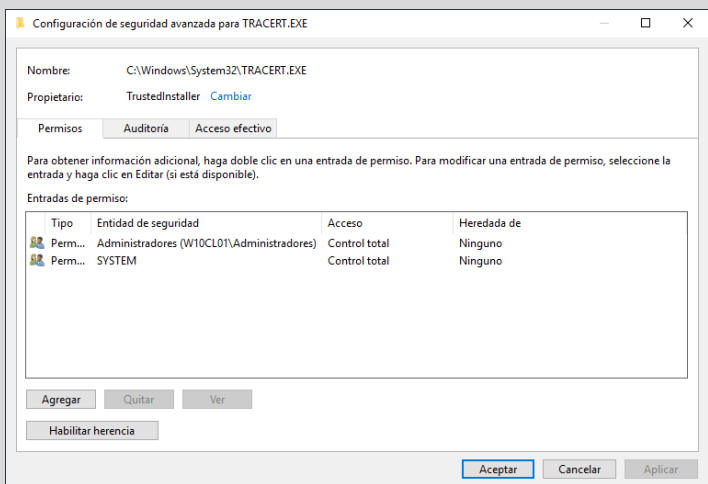
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Manual	Configurado		
Servicio de percepción de Windows	spectrum	Manual	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Manual	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado		
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado		
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Manual	Configurado		
Servicio de publicación World Wide Web	W3SVC	Automático	Configurado		
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Manual	Configurado		
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado		
Servicio de red de host	hns	Manual	Configurado		
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado		
Servicio de registro de W3C	w3logsvc	Manual	Configurado		
Servicio de reparación MultiPoint	WmsRepair	Automático	Configurado		
Servicio de repositorio de estado	StateRepository	Manual	Configurado		
Servicio de sensores	SensorService	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado		
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado		
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Manual	Configurado		
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado		
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Automático	Configurado		
Servicio de uso compartido de datos	DsSvc	Manual	Configurado		
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Manual	Configurado		
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado		
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Automático	Configurado		
Servicio de usuario del portapapeles	cbdhsvc	Manual	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Manual	Configurado		
Servicio de Windows Defender	WinDefend	Automático	Configurado		
Servicio de Windows Insider	wisvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado	
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado	
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado	
Servicio FTP de Microsoft	ftpsvc	Automático	Configurado	
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado	
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado	
Servicio LPD	LPDSVC	Automático	Configurado	
Servicio MultiPoint	Wms	Automático	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado	
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado	
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado	
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado	
Servicio SNMP	SNMP	Deshabilitado	Configurado	
Servicio telefónico	PhoneSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado	
Servicio WAS (Windows Process Activation Service)	WAS	Manual	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Manual	Configurado	
Servicios simples de TCP/IP	simptcp	Automático	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor de roles de DS	DsRoleSvc	Manual	Configurado	
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Automático	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Manual	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Automático	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
Uso de datos	DusmSvc	Automático	Configurado	
WalletService	WalletService	Manual	Configurado	
WarpJITSvc	WarpJITSvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Manual	Configurado	
Windows Search	WSearch	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Windows Update	wuauerv	Manual	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Manual	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	
25.Verifique los permisos asignados a ficheros y carpetas.		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione la opción "Propiedades".		
		 Nota: Deberá tener precaución para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". En la pestaña "Seguridad", seleccione "Opciones Avanzadas". 		

Comprobación	OK/NOK	Cómo hacerlo
		Es posible que deba pulsar sobre el botón “Continuar” para ver los permisos asignados.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. En la ventana resultante, compruebe los permisos asignados a cada carpeta o fichero. Nota: Tenga en consideración que es posible que algunos ficheros no se encuentren en el sistema debido a la configuración aplicada y según las necesidades que requiera su organización. 

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%Public%\	Administradores	Control total		
	System	Control total		
	Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura		
%SystemRoot%\security	Administradores	Control total		
	System	Control total		
%SystemRoot%\system32\ras	Administradores	Control total		
	System	Control total		
%SystemRoot%\system32\rasadhlp.dll	Administradores	Control total		
%SystemRoot%\system32\rasauto.dll	Administradores	Control total		
%SystemRoot%\system32\rasautou.exe	Administradores	Control total		
%SystemRoot%\system32\raschap.dll	Administradores	Control total		
%SystemRoot%\system32\rasctrnm.h	Administradores	Control total		
%SystemRoot%\system32\rasctrs.dll	Administradores	Control total		
%SystemRoot%\system32\rasctrs.ini	Administradores	Control total		
%SystemRoot%\system32\rasdial.exe	Administradores	Control total		
%SystemRoot%\system32\rasmans.dll	Administradores	Control total		
%SystemRoot%\system32\rasmontr.dll	Administradores	Control total		
%SystemRoot%\system32\rasphone.exe	Administradores	Control total		
%SystemRoot%\system32\rasppp.dll	Administradores	Control total		
%SystemRoot%\system32\rastapi.dll	Administradores	Control total		
%SystemRoot%\system32\rastls.dll	Administradores	Control total		
%SystemRoot%\system32\tftp.exe	Administradores	Control total		
	System	Control total		
%SystemRoot%\system32\tracert.exe	Administradores	Control total		
	System	Control total		

ANEXO C.2. CATEGORÍA MEDIA

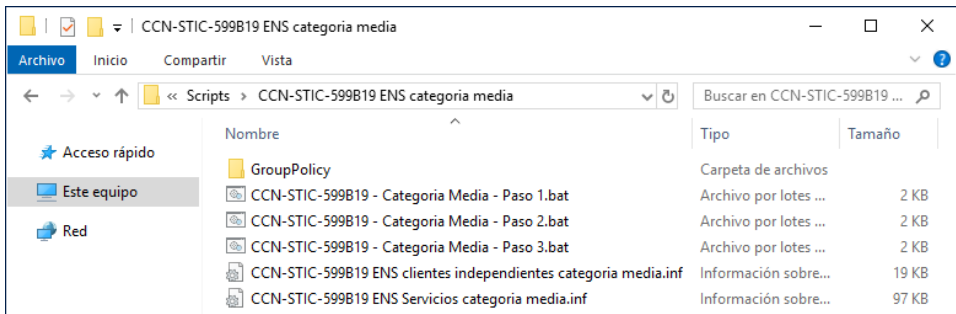
ANEXO C.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes Windows 10 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

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

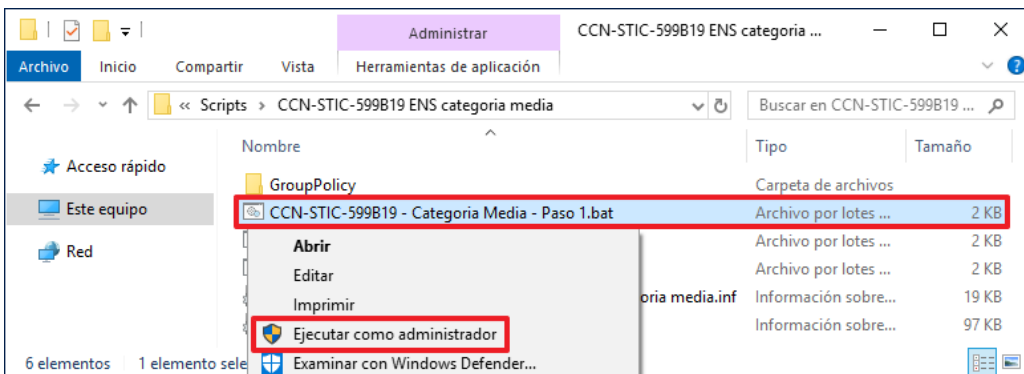
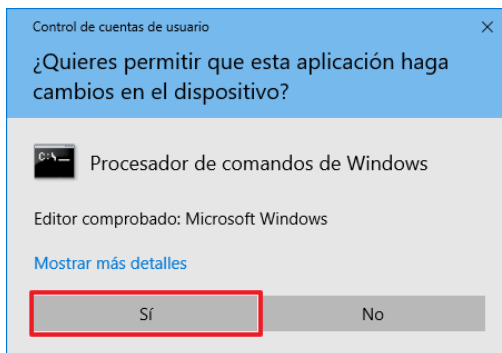
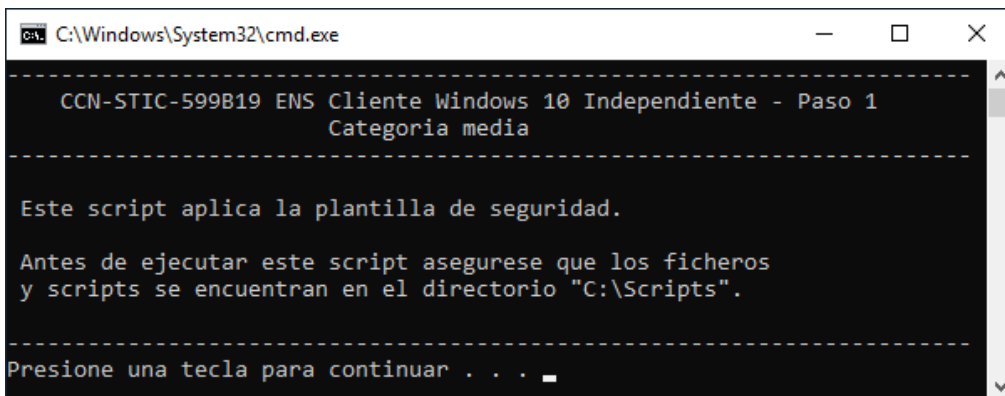
Los pasos que se describen a continuación se realizarán en todos aquellos clientes Windows 10 Pro/Enterprise (versión 1809) sin opción de mantenimiento LTSC, independientes a un dominio, que implementen servicios o información de categoría media y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador local.
3.	Cree el directorio “Scripts” en la unidad “C:\”.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en la ruta “C:\Scripts”.
	Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”.
5.	Abra la carpeta “CCN-STIC-599B19 ENS categoria media” que encontrará en el directorio “C:\Scripts”.

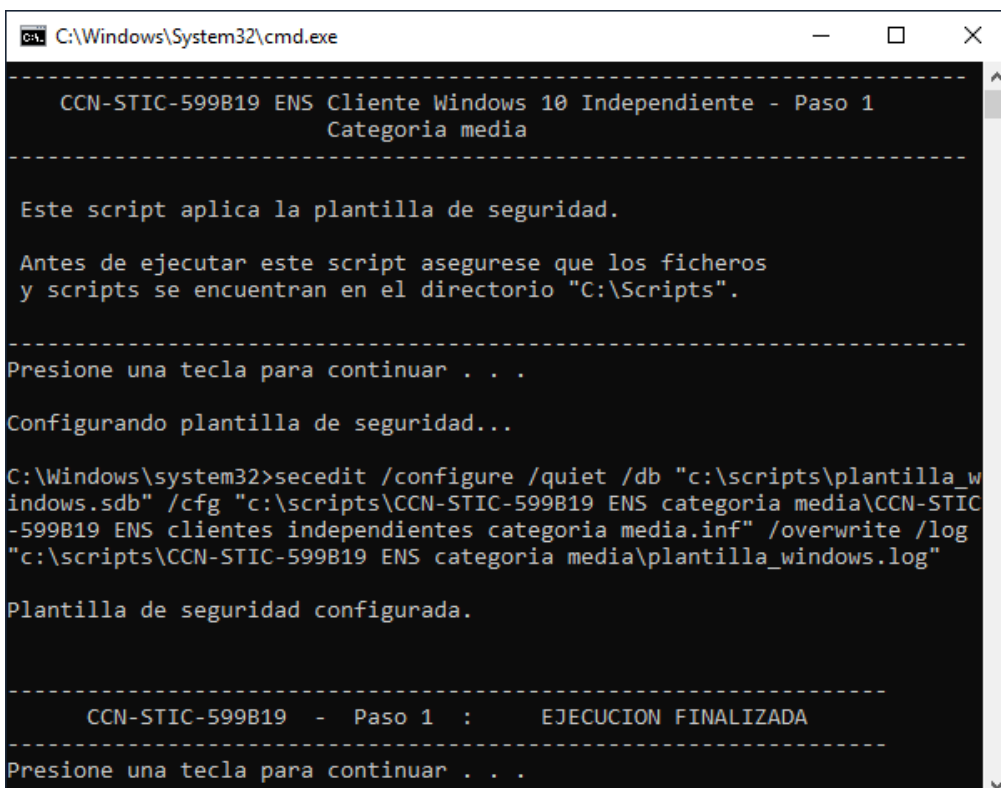
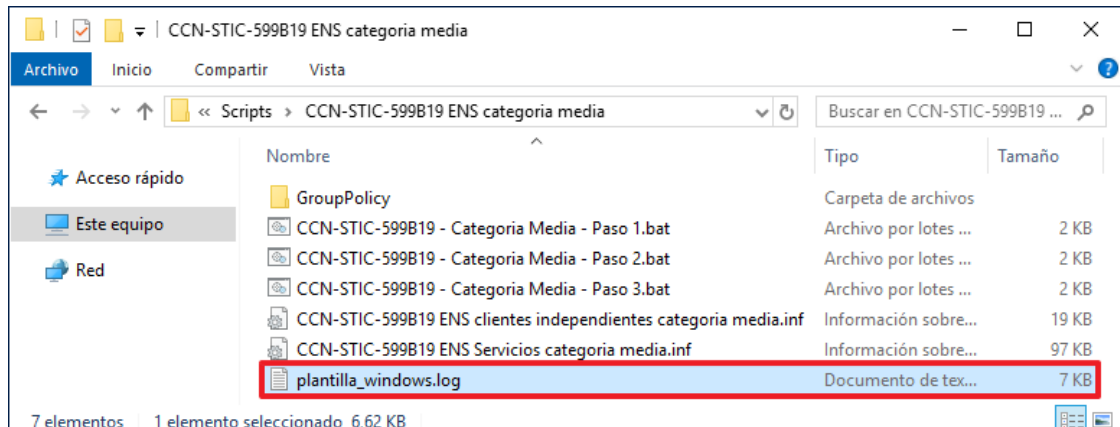


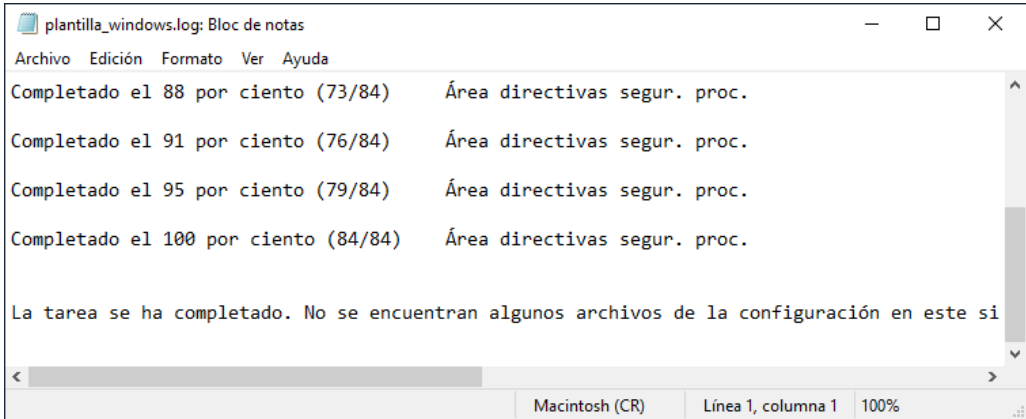
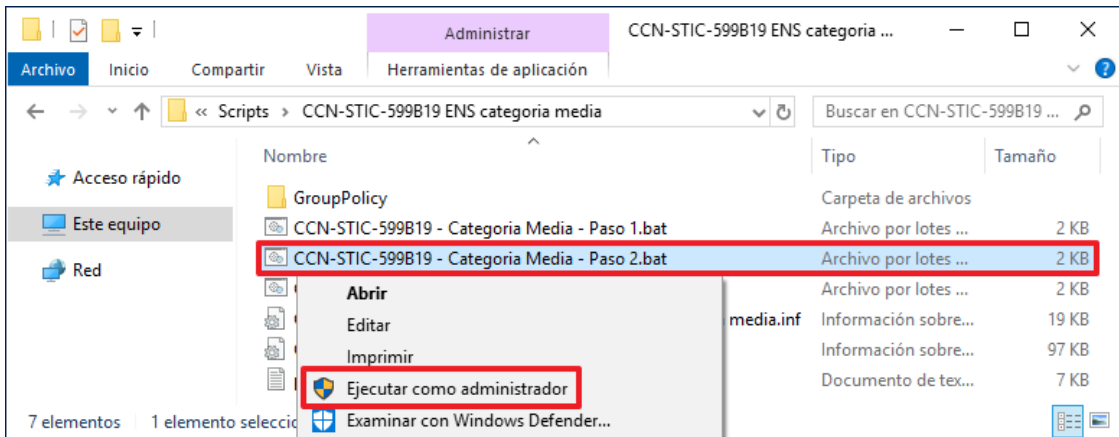
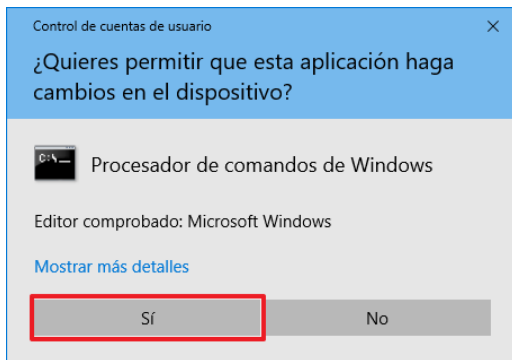
Nombre	Tipo	Tamaño
GroupPolicy	Carpeta de archivos	
CCN-STIC-599B19 - Categoria Media - Paso 1.bat	Archivo por lotes ...	2 KB
CCN-STIC-599B19 - Categoria Media - Paso 2.bat	Archivo por lotes ...	2 KB
CCN-STIC-599B19 - Categoria Media - Paso 3.bat	Archivo por lotes ...	2 KB
CCN-STIC-599B19 ENS clientes independientes categoria media.inf	Información sobre...	19 KB
CCN-STIC-599B19 ENS Servicios categoria media.inf	Información sobre...	97 KB

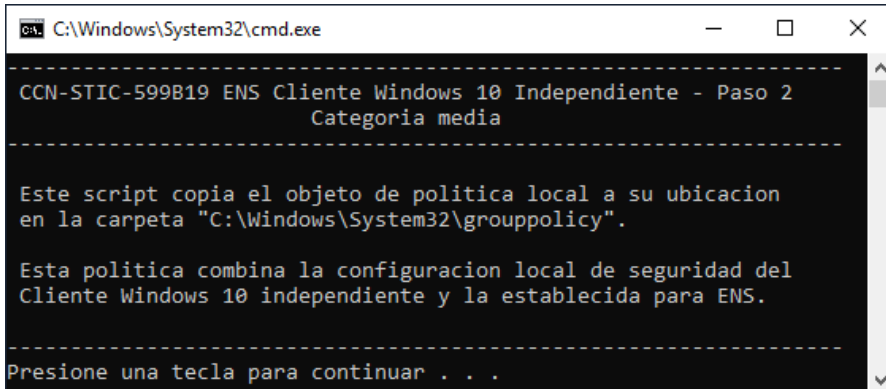
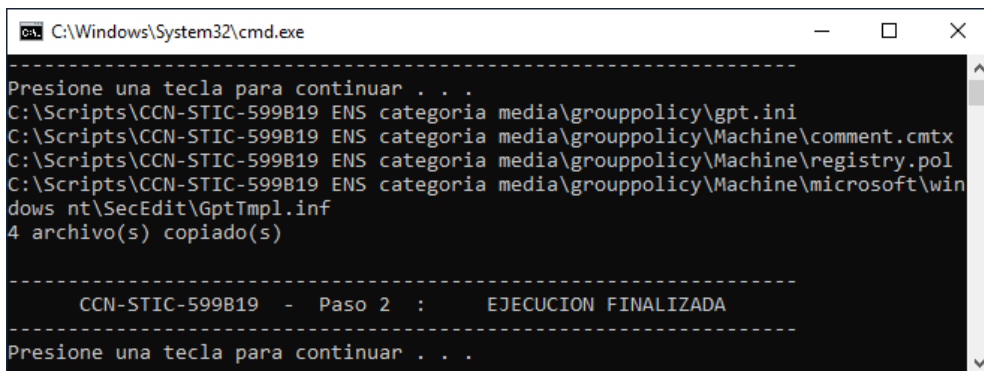
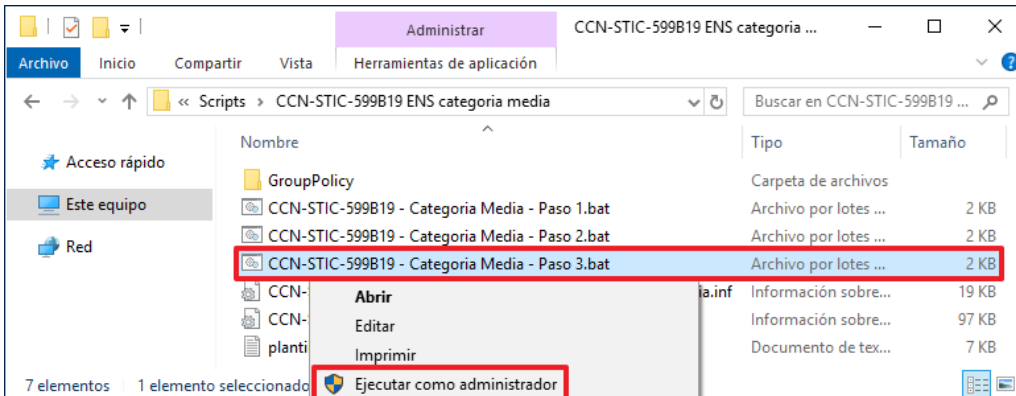
Nota: Los scripts asumen que su ubicación es “C:\Scripts\CCN-STIC-599B19 ENS categoria media”. De no ser así deberá modificar los scripts para que coincidan con la ruta deseada.
--

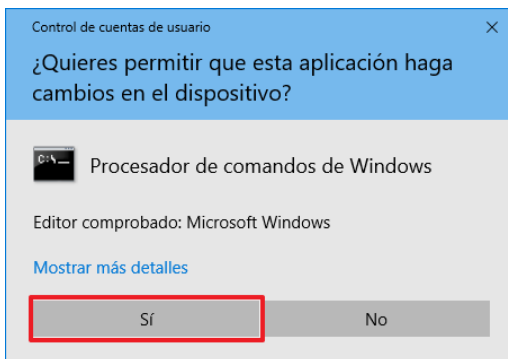
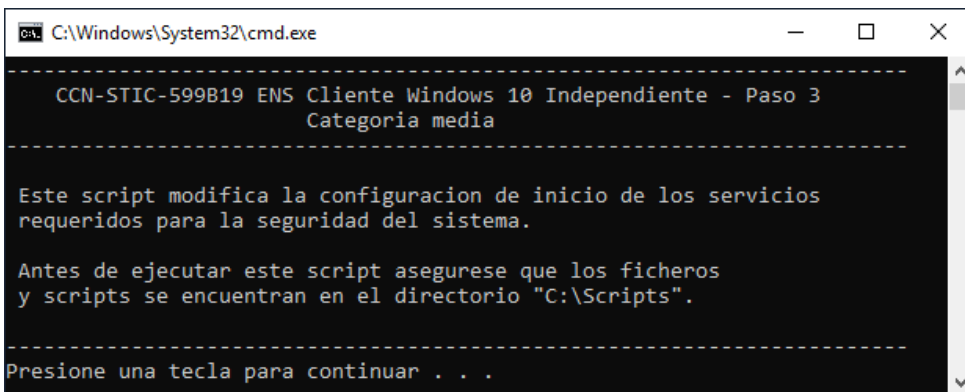
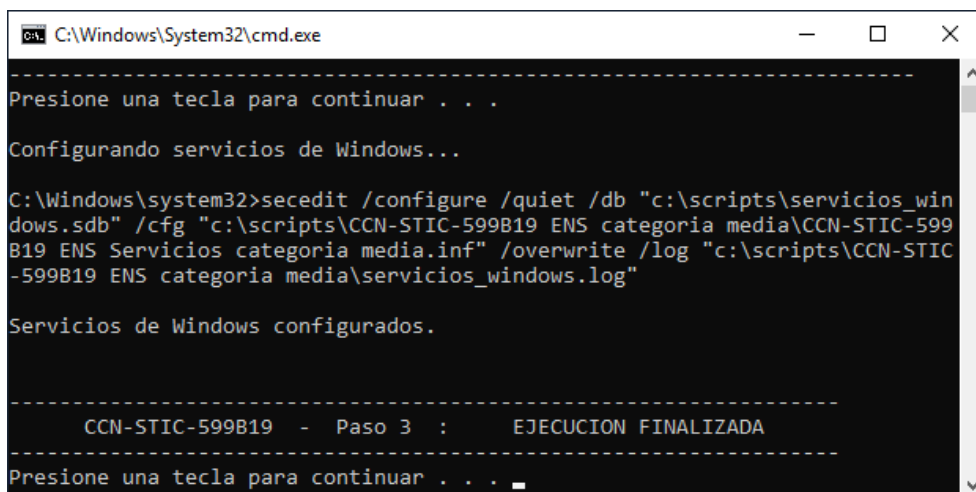
Paso	Descripción
6.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Media – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”. 
7.	Pulse “S” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
8.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría media del ENS. 

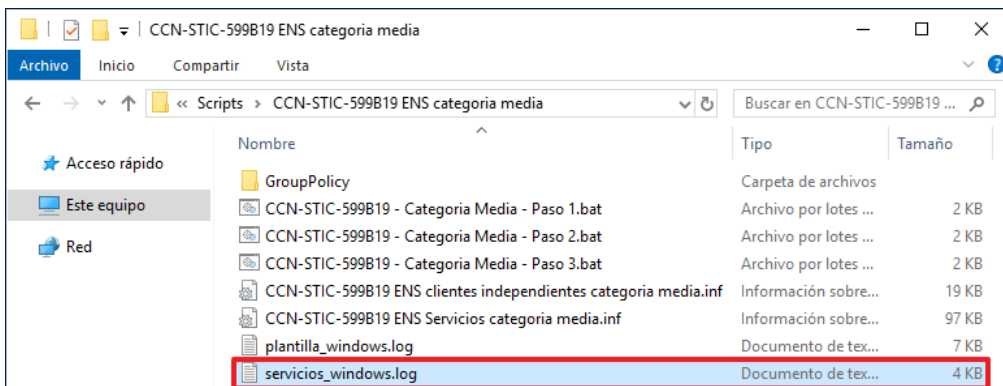
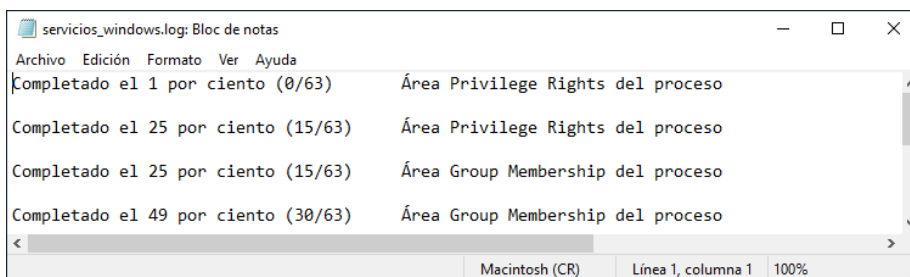
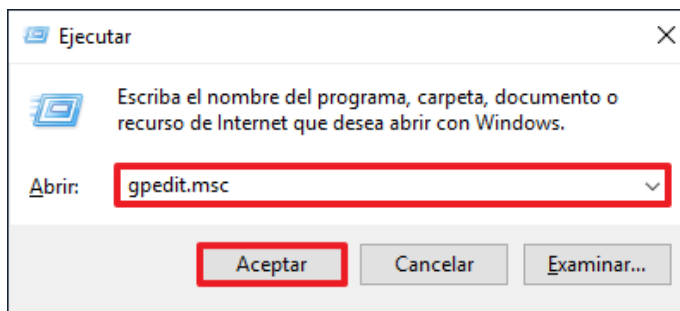


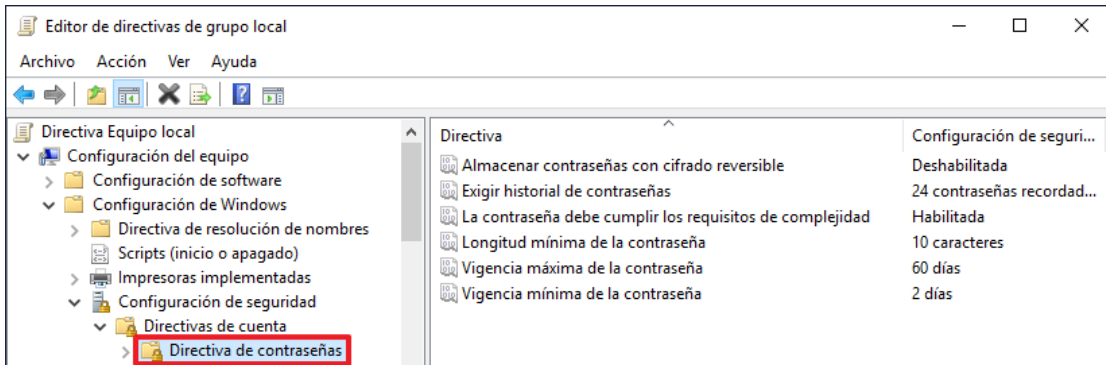
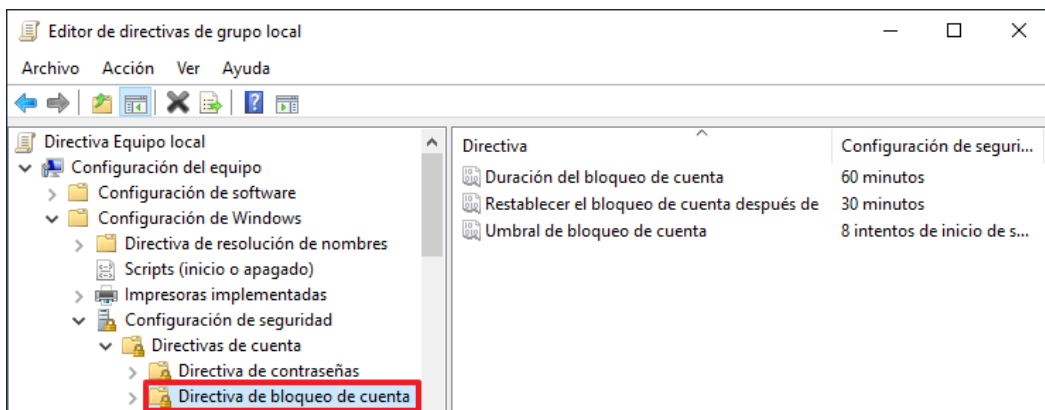
Paso	Descripción
9.	Una vez completado el proceso, deberá pulsar una tecla para continuar. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
10.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 categoria media” con el nombre “plantilla_windows.log”. 

Paso	Descripción
11.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el procedimiento desde el paso 5.
12.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Media – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”. 
13.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 

Paso	Descripción
14.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local. 
15.	Completada la copia de los archivos, compruebe que no ha habido errores en la copia de los mismos. Debería obtener el mismo resultado que el mostrado en la siguiente imagen. Pulse una tecla para finalizar la ejecución del script.  Nota: En caso de haberse producido fallos, solúcelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.
16.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Media – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”. 

Paso	Descripción
17.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 
18.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría media del ENS. 
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 

Paso	Descripción
20.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 ENS categoria media” con el nombre de “servicios_windows.log”. 
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 16.
22.	Elimine la carpeta “C:\Scripts”.
23.	Es factible que su organización cuente con una política de contraseñas consolidada. La implementación de la política de categoría media implementará una política específica para los clientes de categoría media. Deberá evaluarla para determinar si esta configuración le es válida, o por el contrario debe adaptarla a las condiciones de su organización.
24.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse “Aceptar”. 

Paso	Descripción
25.	Pulse “S” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.
26.	Despliegue la política y sitúese en la siguiente ruta: “Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña” 
27.	Evalúe la política de contraseñas y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de credenciales es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.
28.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que “Directiva de contraseñas”. 
29.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración implementada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.

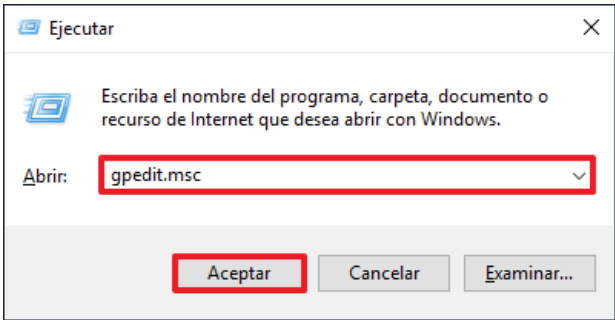
Hasta ahora han sido aplicados cambios, entre otros aspectos, sobre las directivas de contraseña y cuenta, aunque es importante señalar que existen más directivas interesantes a la hora de configurar el sistema.

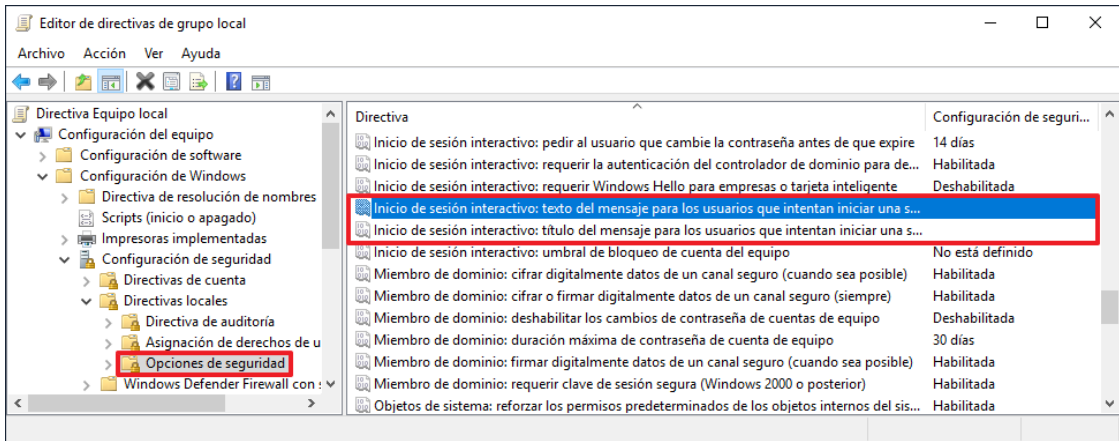
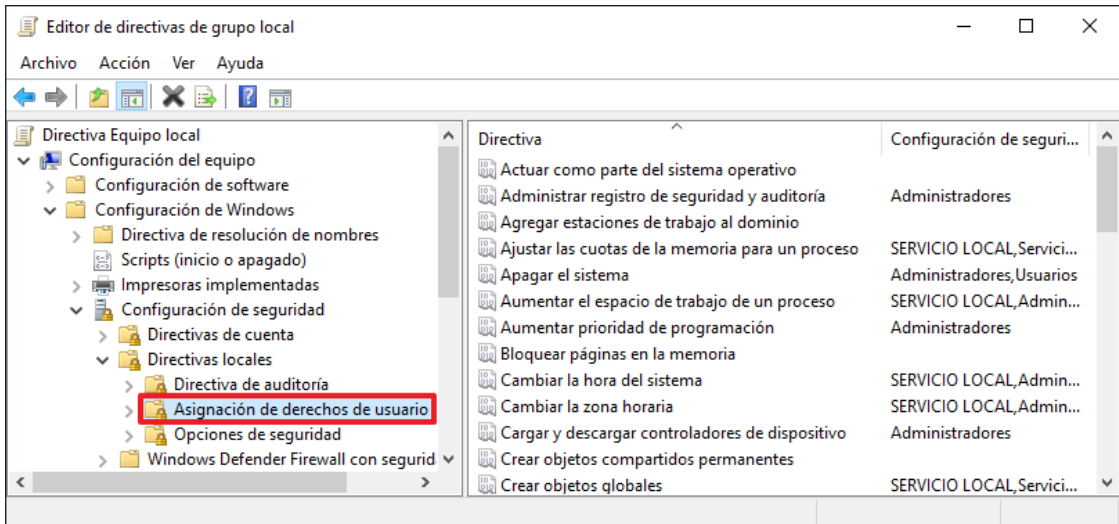
Uno de los aspectos que marca el ENS, desde su requisito de categoría media en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

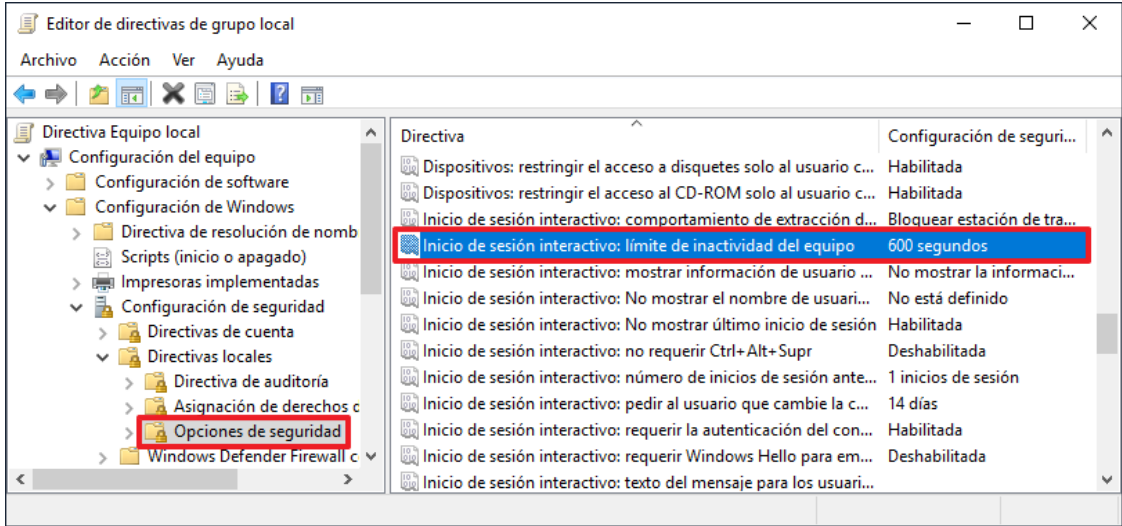
Los sistemas Windows presentan mecanismos para implementar mensajes que realizan advertencias al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

Si su organización no está haciendo uso de este mecanismo realice los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según queda estipulado en la política de seguridad de la organización.

Paso	Descripción
30.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
31.	Debe iniciar sesión con una cuenta que sea Administrador local.
32.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas "Windows + R", escriba "gpedit.msc" en la ventana emergente y pulse "Aceptar". 
33.	Pulse "Sí" cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo.
34.	Para informar de las obligaciones sitúese en la siguiente ruta: "Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"

Paso	Descripción
35.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intenta iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intenta iniciar una sesión”. 
36.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
37.	Por último, la política de seguridad local especifica unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así, deberá realizar las modificaciones sobre la configuración de política local.
38.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 
39.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.

Paso	Descripción
40.	Se establece a partir de la categoría media, según MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de la política local aplicable sobre equipo, puede establecerse la medida de protección que habilita el protector de pantalla y por lo tanto el bloqueo de la sesión. Nota: Si la organización presenta algún mecanismo para realizar el bloqueo del equipo ante inactividad no es necesario que aplique la siguiente configuración. No obstante, revise la configuración para adaptarse a la normativa vigente. Si la organización no tiene medidas dispuestas siga los siguientes pasos.
41.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad” Habilite y configure la siguiente directiva de seguridad: – Inicio de sesión interactivo: límite de inactividad del equipo. Establezca el valor en 600 segundos (10 minutos). 
42.	Cierre el editor de política de grupo local.
43.	Reinicie el puesto de trabajo.

ANEXO C.2.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA MEDIA

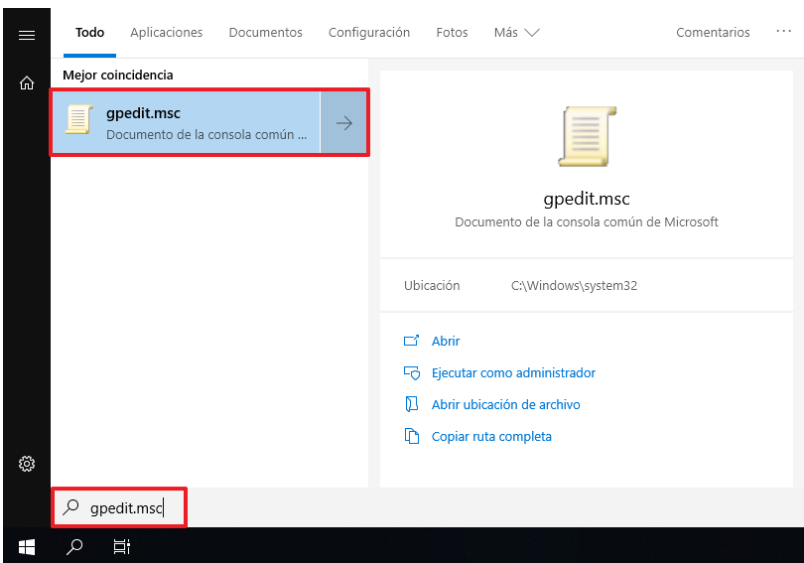
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO C.2.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS”.

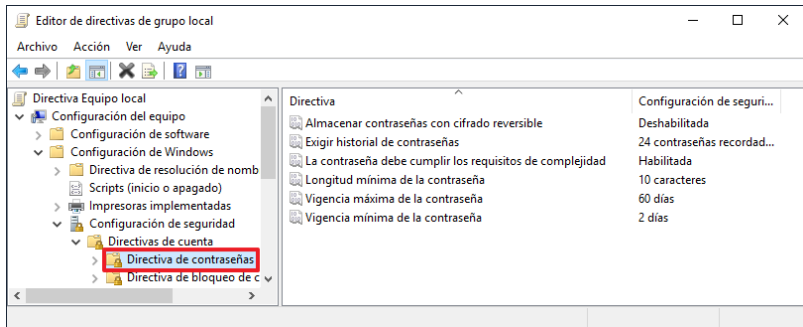
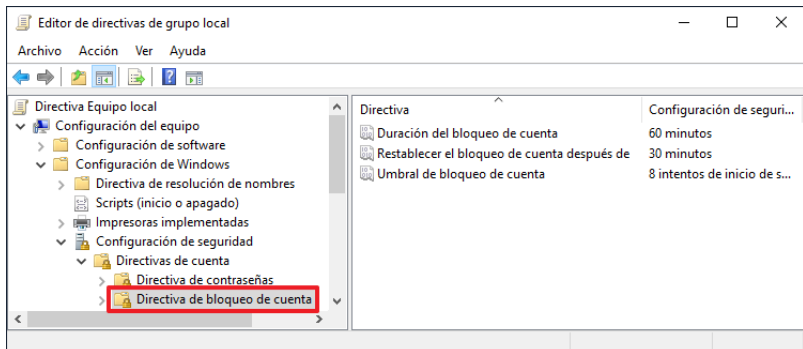
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC, independientes con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de administrador local.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario que es administrador local. Las consolas y herramientas que se utilizarán son las siguientes:

- Editor de objetos de directiva de grupo local (gpedit.msc).
- Editor de registro (regedit.exe).
- Visor de Eventos (eventvwr.exe).
- Servicios (services.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de administración local.
2. Inicie la aplicación de gestión de políticas locales.		Ejecute el “Editor de objetos de directiva de grupo local”. Para ello pulse “Inicio”, teclee “gpedit.msc” y pulse “Enter”. 

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas” Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. 
4. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta” 

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Duración del bloqueo de cuenta		60 minutos	
	Restablecer el bloqueo de cuenta después de		30 minutos	
	Umbral de bloqueo de cuenta		8 intentos de inicio de sesión no válidos	
5. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.	Seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”			
	Directiva		Valor	OK/NOK
	Auditar el acceso a objetos		Correcto, Erróneo	
	Auditar el acceso del servicio de directorio		Correcto, Erróneo	
	Auditar el cambio de directivas		Correcto, Erróneo	
	Auditar el uso de privilegios		Correcto, Erróneo	
	Auditar eventos de inicio de sesión		Correcto, Erróneo	
	Auditar eventos de inicio de sesión de cuenta		Correcto, Erróneo	
	Auditar eventos del sistema		Correcto, Erróneo	
	Auditar la administración de cuentas		Correcto, Erróneo	
6. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.	Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”			
	Directiva		Valor	OK/NOK
	Actuar como parte del sistema operativo		(Definida, pero sin ningún valor)	
	Administrar registro de seguridad y auditoría		Administradores	
	Agregar estaciones de trabajo al dominio		(Definida, pero sin ningún valor)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red	
		Apagar el sistema	Administradores, Usuarios	
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL, Usuarios	
		Aumentar prioridad de programación	Administradores	
		Bloquear páginas en la memoria	(Definida, pero sin ningún valor)	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores	
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)	
		Crear objetos globales	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL	
		Crear un archivo de paginación	Administradores	
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)	
		Crear vínculos simbólicos	Administradores	
		Denegar el acceso a este equipo desde la red	ANONYMOUS LOGON, Invitados	
		Denegar el inicio de sesión como servicio	Invitados	
		Denegar el inicio de sesión como trabajo por lotes	Invitados	
		Denegar el inicio de sesión local	Invitados	
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos	
		Depurar programas	Administradores	
		Forzar cierre desde un sistema remoto	Administradores	
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red	
		Generar perfiles de un solo proceso	Administradores	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtén un token de suplantación para otro usuario en la misma sesión	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Omitir comprobación de recorrido	SERVICIO LOCAL, Servicio de Red, Administradores, Usuarios Autenticados
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	(Definida, pero sin ningún valor)
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento de volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	(Definida, pero sin ningún valor)
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Tener acceso a este equipo desde la red	Administradores, Usuarios	
		Tomar posesión de archivos y otros objetos	Administradores	
		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
7. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente	(Definida, pero sin ningún valor)	
		Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
		Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Deshabilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, System\Microsoft\Windows NT\CurrentVersion
		Acceso a redes: rutas y subrutas del Registro accesibles remotamente	System\CurrentControlSet\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Deshabilitada
		Auditoría: auditar el acceso de objetos globales del sistema	Deshabilitada
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada
		Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitada
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitada
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de registro en diferentes ubicaciones por usuario	Habilitada
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, Firma y operaciones hash	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva	Valor	OK/NOK
	Cuentas: cambiar el nombre de cuenta de invitado	Invitado	
	Cuentas: cambiar el nombre de la cuenta de administrador	Administrador	
	Cuentas: estado de la cuenta de administrador	Deshabilitada	
	Cuentas: estado de la cuenta de invitado	Deshabilitada	
	Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada	
	Dispositivos: impedir que los usuarios instalen controladores de impresora	Deshabilitada	
	Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada	
	Dispositivos: restringir el acceso a disquetes solo al usuario con sesión iniciada localmente	Habilitada	
	Dispositivos: restringir el acceso al CD-ROM solo al usuario con sesión iniciada localmente	Habilitada	
	Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
	Inicio de sesión interactivo: mostrar información de usuario cuando bloquee la sesión	No mostrar la información del usuario	
	Inicio de sesión interactivo: No mostrar último inicio de sesión	Habilitada	
	Inicio de sesión interactivo: No requerir Ctrl + Alt + Supr	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	1 inicios de sesión
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada
		Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	Deshabilitada
		Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión	(Definida, pero sin ningún valor)
		Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión	(Definida, pero sin ningún valor)
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada
		Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada
		Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitada
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits
		Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits
		Servidor de red de Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos	
8. Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media”		
		Directiva	Valor	OK/NOK
		Impedir el acceso a internet de Windows Media DRM	Habilitado	
9. Verifique la directiva de almacén digital en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
10. Verifique la directiva de Antivirus en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitado	
11. Verifique la directiva de asistencia en línea en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	
12. Verifique las directivas de biometría en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Habilitado	
		Permitir que los usuarios de dominio inicien sesión mediante biometría	Habilitado	
		Permitir que los usuarios inicien sesión mediante biometría	Habilitado	
13. Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		Permitir el uso de Cortana	Deshabilitado	
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
14. Verifique las directivas de contenido en la nube en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Contenido en la Nube”		
		Directiva	Valor	OK/NOK
		Desactivar experiencias del consumidor de Microsoft	Habilitada	
		No mostrar recomendaciones de Windows	Habilitada	
15. Verifique las directivas de reproducción automática en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Establece el comportamiento predeterminado para la ejecución automática	Habilitado (No ejecutar ningún comando de ejecución automática)	
		Desactivar reproducción automática	Habilitado (Todas las unidades)	
16. Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
17. Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	
18.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		
		Directiva	Valor	OK/NOK
		Activar sitios sugeridos	Deshabilitado	
		Impedir administración del filtro SmartScreen	Deshabilitado	
		Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	Habilitado	
19.Verifique las directivas de autocompletar en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitado	
20.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Eliminar el historial de exploración”		
		Directiva	Valor	OK/NOK
		Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento.	Deshabilitado	
		Impedir que se elimine el historial de descarga	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir que se eliminen contraseñas	Deshabilitado	
		Impedir que se eliminen cookies	Deshabilitado	
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitado	
		Impedir que se eliminen los archivos temporales de Internet	Deshabilitado	
		Impedir que se eliminen los datos de filtrado InPrivate	Deshabilitado	
		Impedir que se eliminen los datos de formularios	Deshabilitado	
		Impedir que se eliminen los sitios web que el usuario visitó	Deshabilitado	
		Permitir que se elimine el historial de exploración al salir	Habilitado	
21.Verifique las directivas de OneDrive en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	
22.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK
		Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario	Habilitado	
		Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	Habilitado	

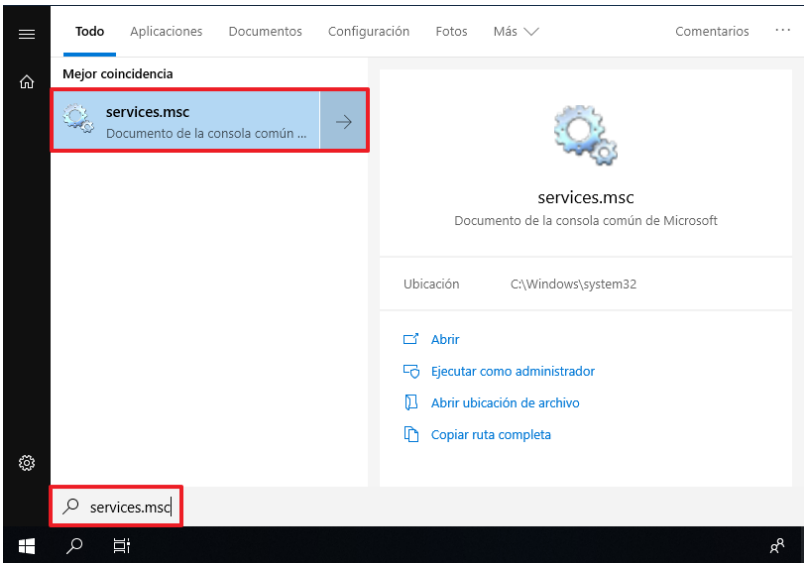
Comprobación	OK/NOK	Cómo hacerlo		
23.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitado (Solo HTTP (0))	
24.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas.	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desparejados	Habilitado (Forzar denegación)	
25.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”		
		Directiva	Valor	OK/NOK
		No volver a mostrar notificaciones de comentarios	Habilitado	
		Permitir telemetría	Habilitado	
26.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”		
		Directiva	Valor	OK/NOK
		Permitir acceso a Shell remoto	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
27.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
28.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
29.Verifique la directiva de Store en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Store”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitado	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitado	
30.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitado	
		Desactivar sensores	Habilitado	
		Desactivar ubicación	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
31.Verifique la directiva de Windows Update en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	
32.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitado	
33.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Desactivar el acceso a Store	Habilitado	
		Desactivar el contenido “¿Sabías que...?” del Centro de ayuda y soporte técnico	Habilitado	
		Desactivar el informe de errores de Windows	Habilitado	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows	Habilitado	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger	Habilitado	
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitado	
		Desactivar la actualización de archivos de contenido del Asistente para búsqueda	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico		Habilitado	
	Desactivar la tarea de imágenes "Pedir copias fotográficas"		Habilitado	
	Desactivar los vínculos "Event.asp" del Visor de eventos		Habilitado	
	Desactivar uso compartido de datos de personalización de escritura a mano		Habilitado	
34.Verifique la directiva de Net Logon en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. "Configuración del Equipo → Plantillas Administrativas → Sistema → Net Logon"			
	Directiva		Valor	OK/NOK
	Permitir algoritmos de criptografía compatibles con Windows NT 4.0		Deshabilitado	
35.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. "Configuración del Equipo → Plantillas Administrativas → Sistema → Perfiles de usuario"			
	Directiva		Valor	OK/NOK
	Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)		Habilitado	
	Desactivar el identificador de publicidad		Habilitado	
36.Verifique la directiva de personalización en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. "Configuración del Usuario → Plantillas Administrativas → Panel de control → Personalización"			

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Habilitar protector de pantalla	Habilitado	
		Proteger el protector de pantalla mediante contraseña	Habilitado	
		Tiempo de espera del protector de pantalla	Habilitado (600 segundos)	
		Aplicar un protector de pantalla específico	Habilitado	
37.Verifique el modo de configuración de los servicios del sistema.		Ejecute la herramienta de servicios. Para ello pulse “Inicio”, teclee “services.msc” y pulse “Enter”.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto, entre paréntesis) para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado		
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado		
Adaptador de escucha Net.Msmq	NetMsmqActivator	Automático	Configurado		
Adaptador de escucha Net.Pipe	NetPipeActivator	Automático	Configurado		
Adaptador de escucha Net.Tcp	NetTcpActivator	Automático	Configurado		
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado		
Administración de aplicaciones	AppMgmt	Manual	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Manual	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Automático	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de cuentas web	TokenBroker	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMgrSvc	Manual	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Automático	Configurado		
Agrupación de red del mismo nivel	p2psvc	Manual	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		
Archivos sin conexión	CscService	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Asignador de detección de topologías de nivel de vínculo	ltdsvc	Manual	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Manual	Configurado		
Audio de Windows	Audiosrv	Automático	Configurado		
Autenticación natural	NaturalAuthentication	Manual	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Manual	Configurado		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		
CaptureService	CaptureService	Manual	Configurado		
Carpetas de trabajo	workfoldersvc	Manual	Configurado		
CDPUserSvc	CDPUserSvc	Automático	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente para NFS	NfsClnt	Automático	Configurado		
Cliente web	WebClient	Manual	Configurado		
Cola de impresión	Spooler	Automático	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Automático	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Conexiones de red	Netman	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración automática de WLAN	WlanSvc	Manual	Configurado		
Configuración automática de WWAN	WwanSvc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado		
ConsentUX	ConsentUxUserSvc	Manual	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Automático	Configurado		
Detección de hardware shell	ShellHWDetection	Automático	Configurado		
Detección SSDP	SSDPSRV	Manual	Configurado		
DevicePicker	DevicePickerUserSvc	Manual	Configurado		
DevicesFlow	DevicesFlowUserSvc	Manual	Configurado		
Diagnostic Execution Service	diagsvc	Manual	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Manual	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Escucha de RIP	iprip	Automático	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	
Examinador de equipos	Browser	Manual	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado	
Fax	Fax	Manual	Configurado	
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado	
Firewall de Windows	MpsSvc	Automático	Configurado	
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado	
Hora de Windows	W32Time	Manual	Configurado	
Host de proveedor de detección de función	fdPHost	Manual	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Manual	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Manual	Configurado	
Identidad de aplicación	AppIDSvc	Manual	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Manual	Configurado	
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado	
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado	
Instantáneas de volumen	VSS	Manual	Configurado	
Instrumental de administración de Windows	Winmgmt	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
LxssManager	LxssManager	Manual	Configurado		
Message Queue Server	MSMQ	Automático	Configurado		
MessagingService	MessagingService	Manual	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Manual	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Manual	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Manual	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Manual	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado		
Registrador de configuración de Windows Connect Now	wcnscvc	Manual	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Manual	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Manual	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático	Configurado		
Servicio AVCTP	BthAvctpSvc	Manual	Configurado		
Servicio biométrico de Windows	WbioSrv	Manual	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administración de web	WMSVC	Manual	Configurado	
Servicio de administración de Windows	WManSvc	Manual	Configurado	
Servicio de administración IIS	IISADMIN	Automático	Configurado	
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asistente para perfil local	wlpcsvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Automático	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de cliente de protección de host	HgClientService	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Manual	Configurado	
Servicio de datos del sensor	SensorDataService	Manual	Configurado	
Servicio de datos espacial	SharedRealitySvc	Manual	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado	
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado	
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado	
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado	
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado	
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado	
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado	
Servicio de geolocalización	lfsvc	Manual	Configurado	
Servicio de historial de archivos	fhsvc	Manual	Configurado	
Servicio de host HV (Hyper-V)	HvHost	Manual	Configurado	
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado		
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de instalación de Microsoft Store	InstallService	Manual	Configurado		
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado		
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de mejora de visualización	DisplayEnhancementService	Manual	Configurado		
Servicio de monitor de infrarrojos	irmon	Manual	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Manual	Configurado		
Servicio de percepción de Windows	spectrum	Manual	Configurado		
Servicio de perfil de usuario	ProfSvc	Automático	Configurado		
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado		
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Manual	Configurado		



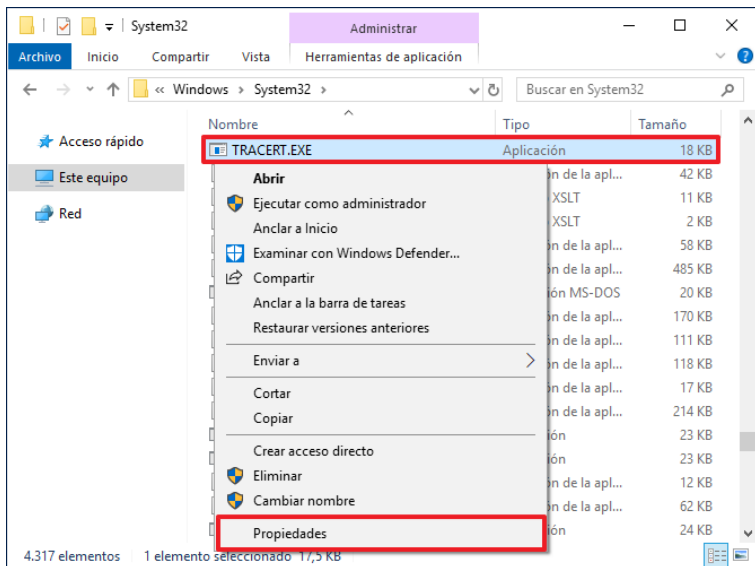
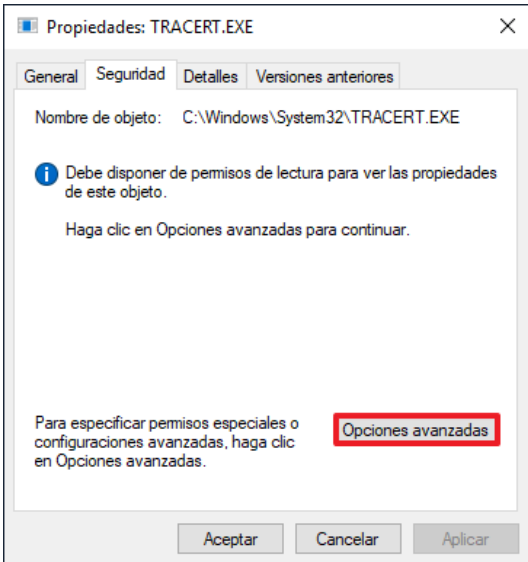
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado	
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado	
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Manual	Configurado	
Servicio de publicación World Wide Web	W3SVC	Automático	Configurado	
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado	
Servicio de registro de W3C	w3logsvc	Manual	Configurado	
Servicio de reparación MultiPoint	WmsRepair	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Manual	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Automático	Configurado	

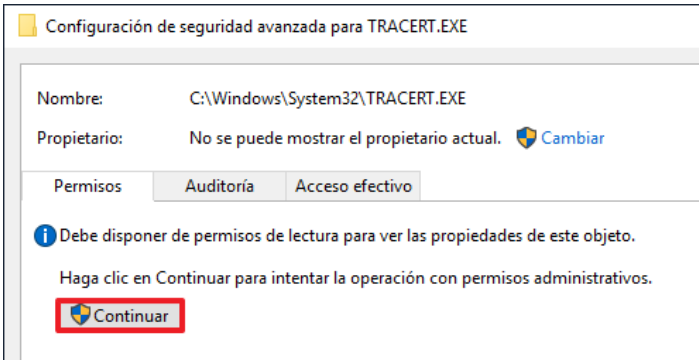
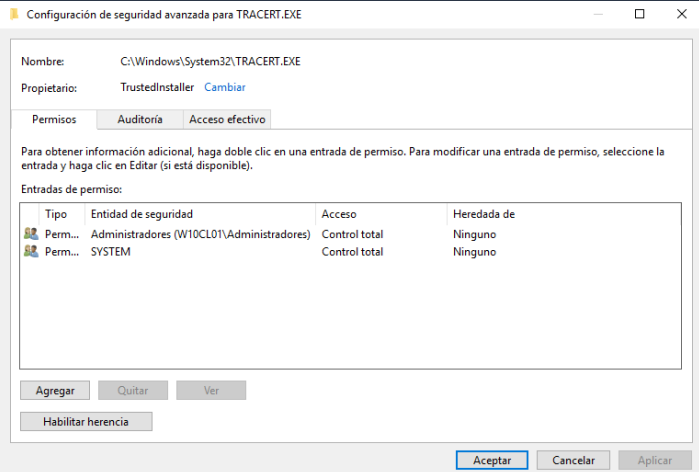
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Manual	Configurado	
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado	
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Automático	Configurado	
Servicio de usuario del portapapeles	cbdhsvc	Manual	Configurado	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Manual	Configurado	
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de virtualización de red	nvagent	Manual	Configurado	
Servicio de Windows Defender	WinDefend	Manual	Configurado	
Servicio de Windows Insider	wisvc	Manual	Configurado	
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado	
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado	
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Manual	Configurado	
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado		
Servicio FTP de Microsoft	ftpsvc	Automático	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio LPD	LPDSVC	Automático	Configurado		
Servicio MultiPoint	Wms	Automático	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado		
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio telefónico	PhoneSvc	Manual	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Manual	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Manual	Configurado		



Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicios simples de TCP/IP	simptcp	Automático	Configurado	
Servidor	LanmanServer	Automático	Configurado	
Servidor de roles de DS	DsRoleSvc	Manual	Configurado	
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado	
Sincronizar host	OneSyncSvc	Automático	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado	
Sistema de eventos COM+	EventSystem	Automático	Configurado	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado	
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado	
Superfetch	SysMain	Automático	Configurado	
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Manual	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Automático	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
Uso de datos	DusmSvc	Automático	Configurado	
WalletService	WalletService	Manual	Configurado	
WarpJITSvc	WarpJITSvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Manual	Configurado	
Windows Search	WSearch	Automático	Configurado	
Windows Update	wuauserv	Manual	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Manual	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo
38.Verifique los permisos asignados a ficheros y carpetas.		Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione la opción “Propiedades”.  Nota: Deberá tener cuidado para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”. 

Comprobación	OK/NOK	Cómo hacerlo												
		Es posible que deba pulsar sobre el botón “Continuar” para ver los permisos asignados.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. En la ventana resultante, compruebe los permisos asignados a cada carpeta o fichero. Nota: Tenga en consideración que es posible que algunos ficheros no se encuentren en el sistema debido a la configuración aplicada y según las necesidades que requiera su organización.  <table><thead><tr><th>Tipo</th><th>Entidad de seguridad</th><th>Acceso</th><th>Heredada de</th></tr></thead><tbody><tr><td>Perm...</td><td>Administradores (W10CL01\Administradores)</td><td>Control total</td><td>Ninguno</td></tr><tr><td>Perm...</td><td>SYSTEM</td><td>Control total</td><td>Ninguno</td></tr></tbody></table>	Tipo	Entidad de seguridad	Acceso	Heredada de	Perm...	Administradores (W10CL01\Administradores)	Control total	Ninguno	Perm...	SYSTEM	Control total	Ninguno
Tipo	Entidad de seguridad	Acceso	Heredada de											
Perm...	Administradores (W10CL01\Administradores)	Control total	Ninguno											
Perm...	SYSTEM	Control total	Ninguno											

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%Public%\		Administradores	Control total	
		System	Control total	
		Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\security		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control total	
%SystemRoot%\system32\raschap.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\rastls.dll		Administradores	Control total	
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

ANEXO C.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO C.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen clientes Windows 10 con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría alta, deberá realizar las implementaciones según se referencian en el presente anexo.

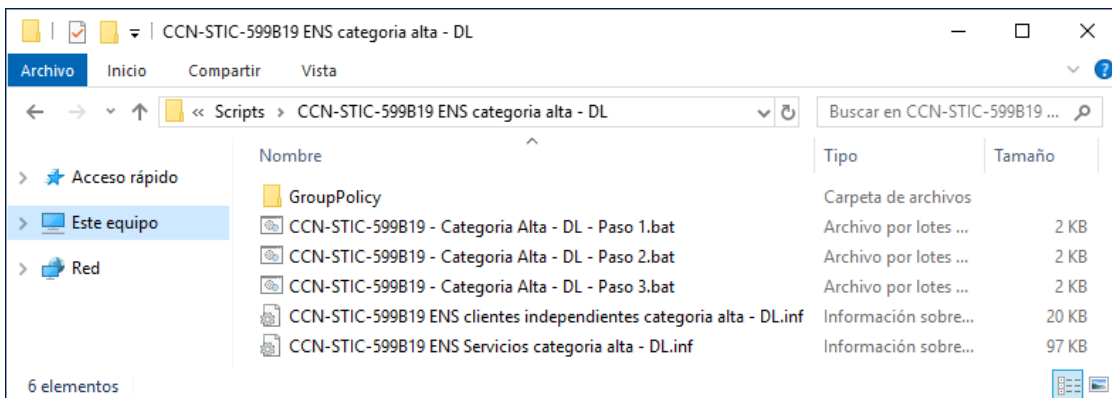
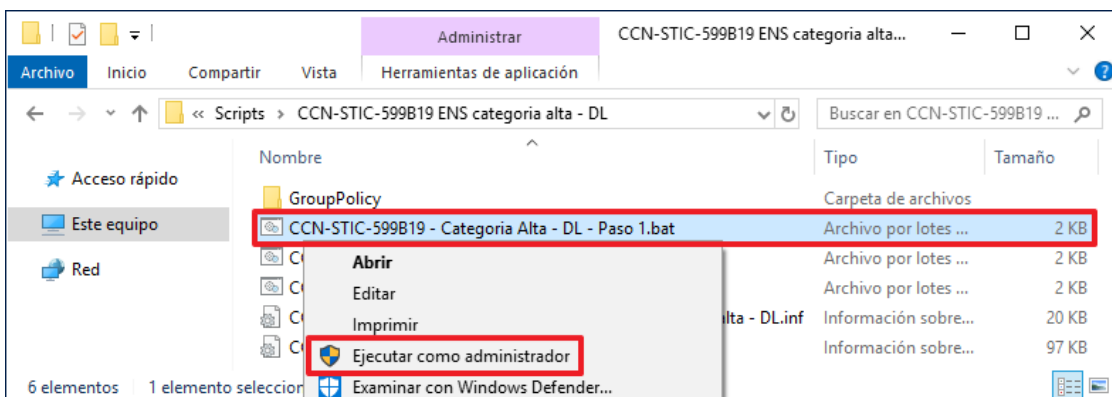
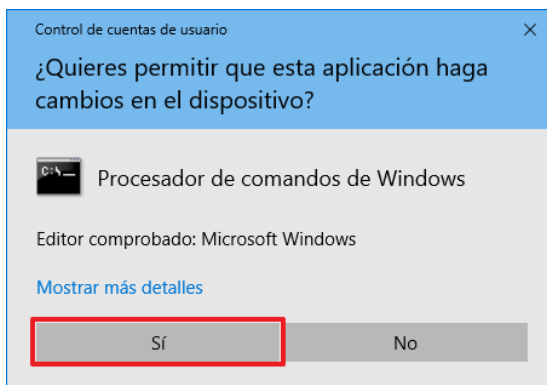
Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

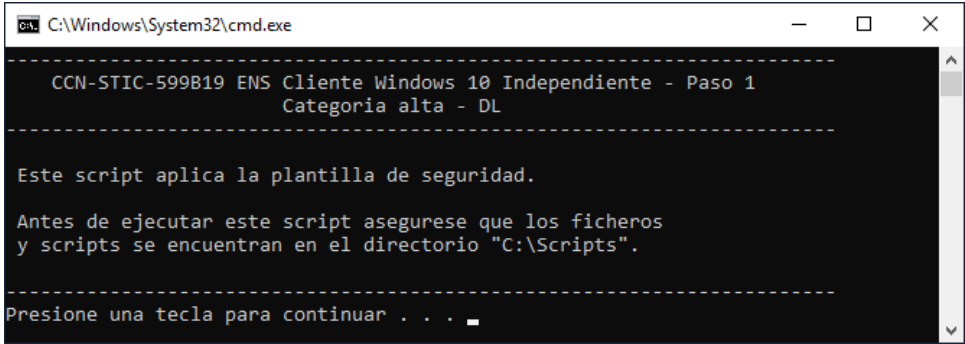
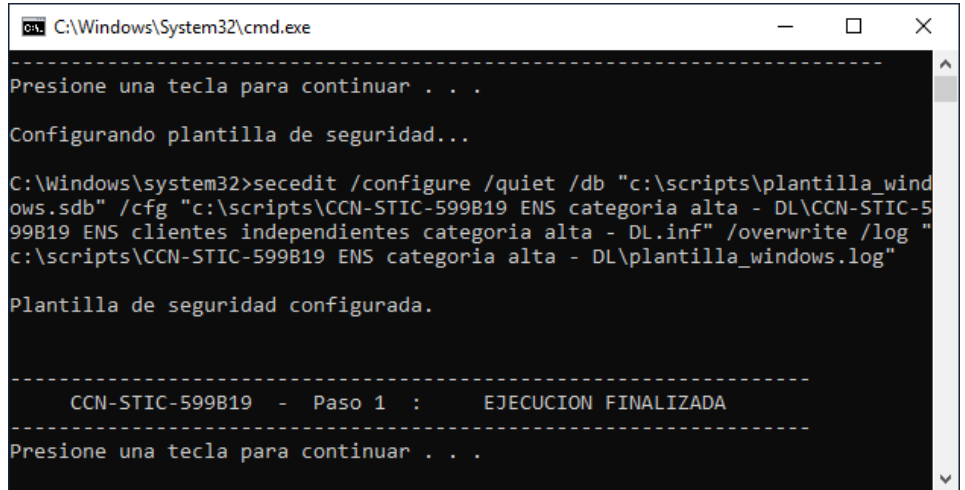
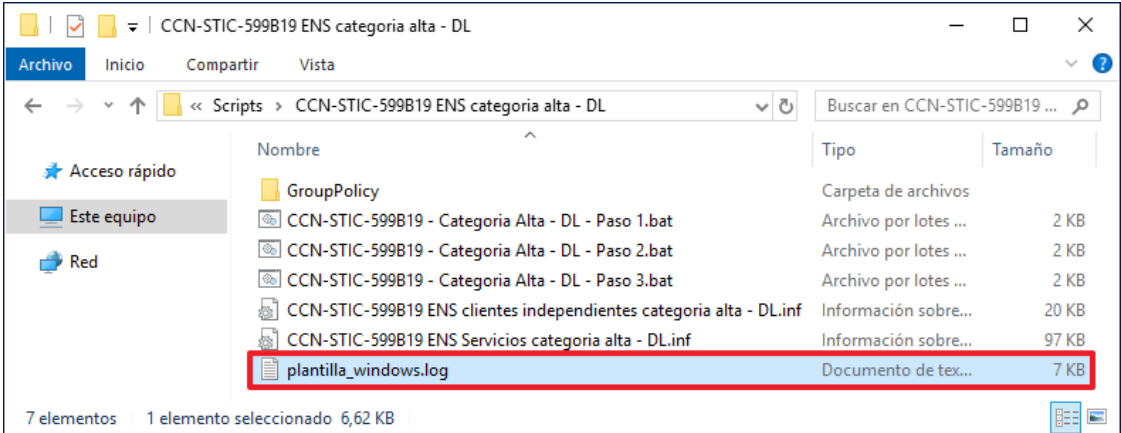
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará uso de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho caso.

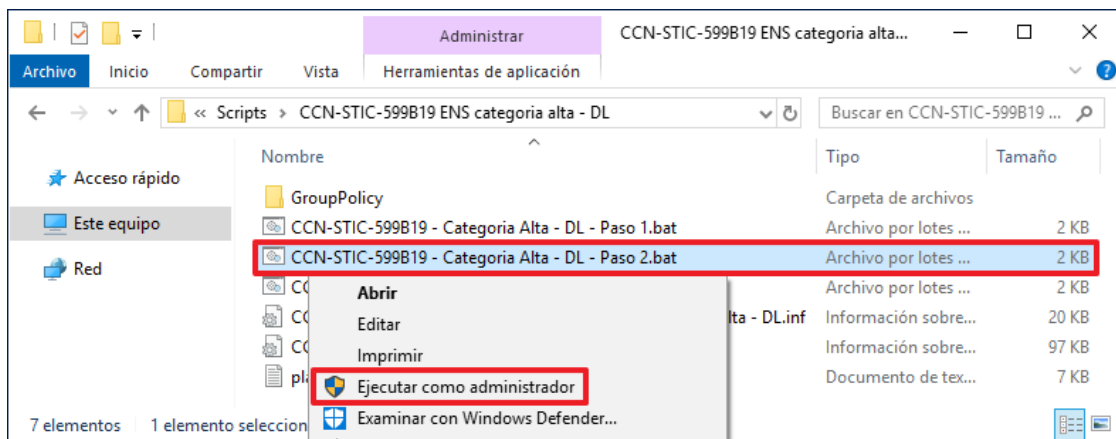
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

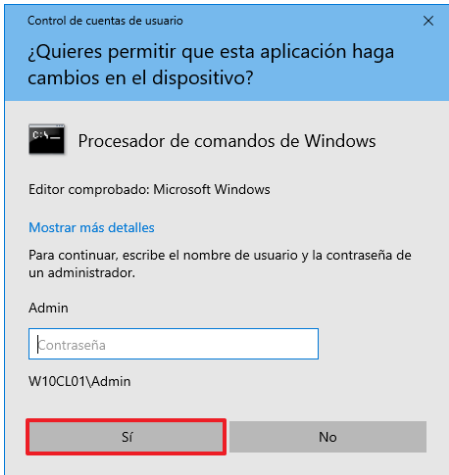
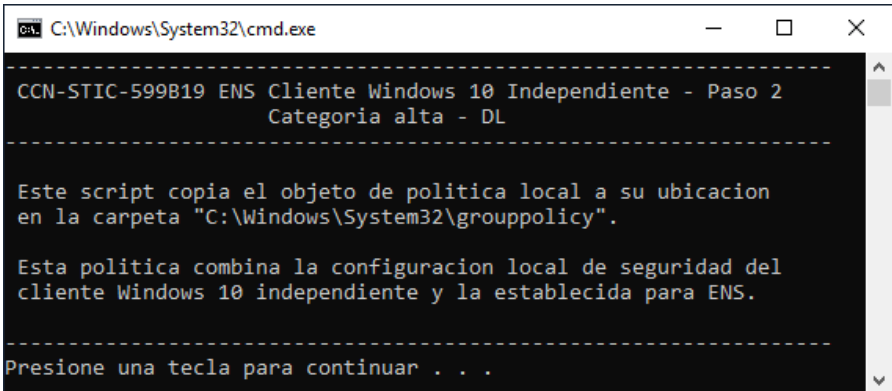
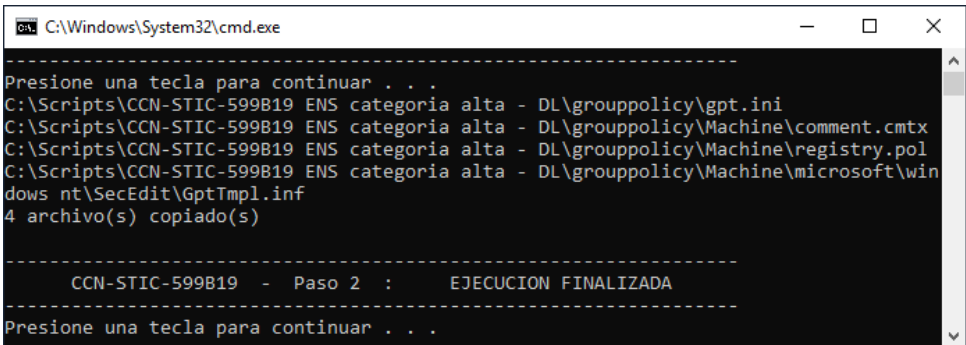
Los pasos que se describen a continuación se realizarán en todos aquellos clientes Windows 10 Pro/Enterprise (versión 1809) sin opción de mantenimiento LTSC, independientes a un dominio, que implementen servicios o información de categoría alta y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad / Difusión Limitada.

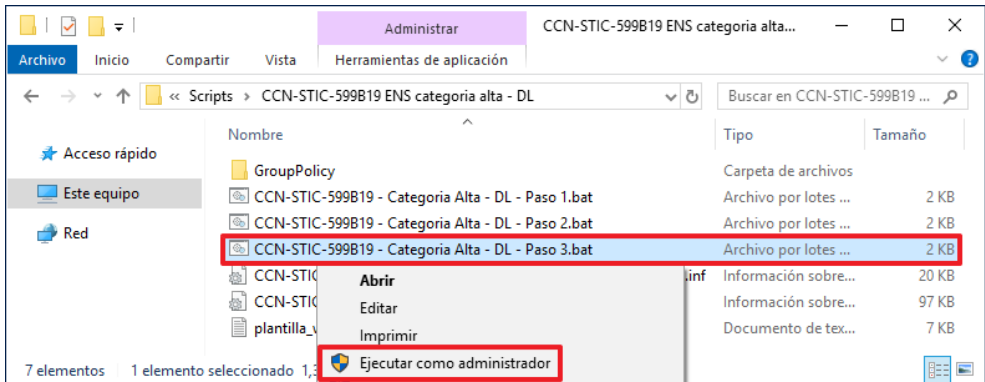
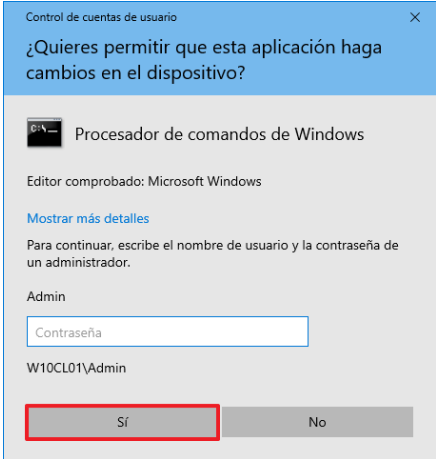
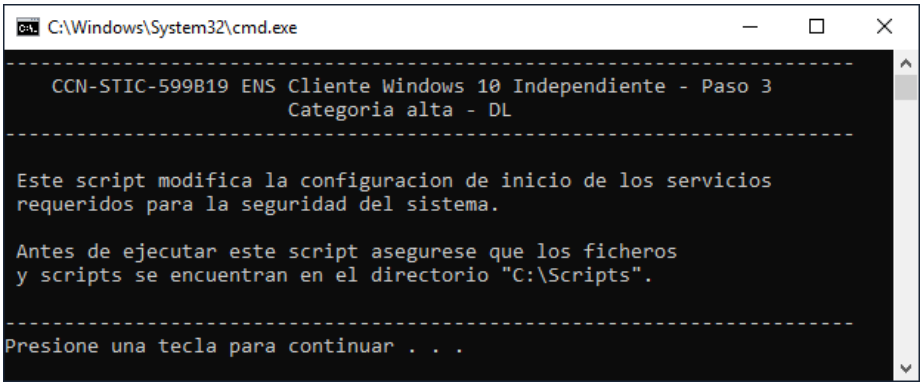
Paso	Descripción
1.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador local.
3.	Cree el directorio "Scripts" en la unidad "C:\".
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19".	

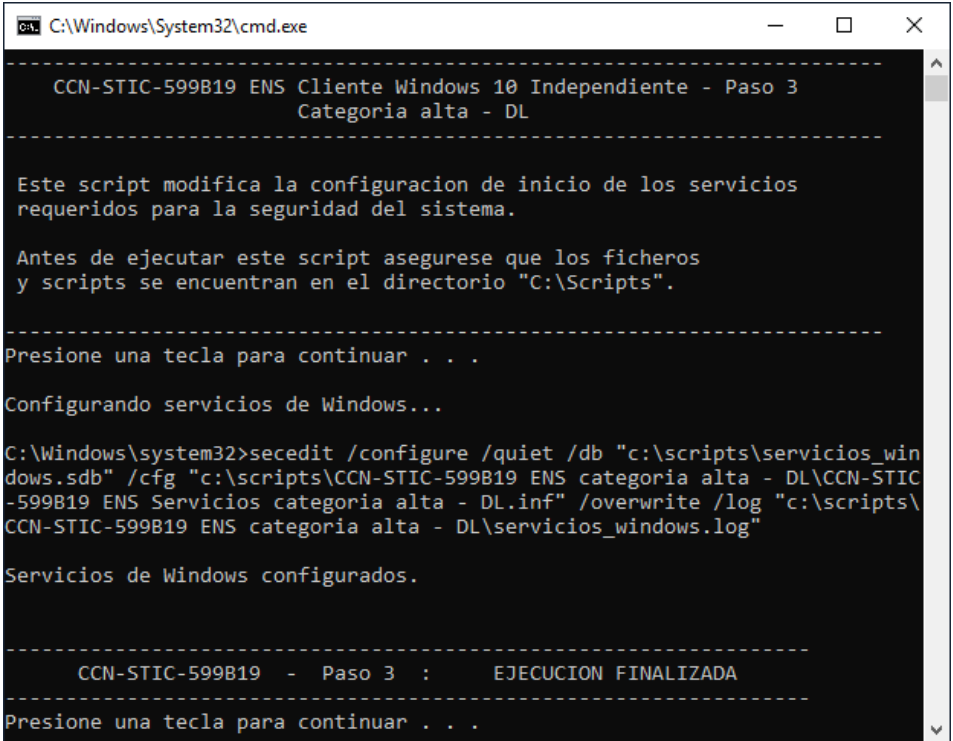
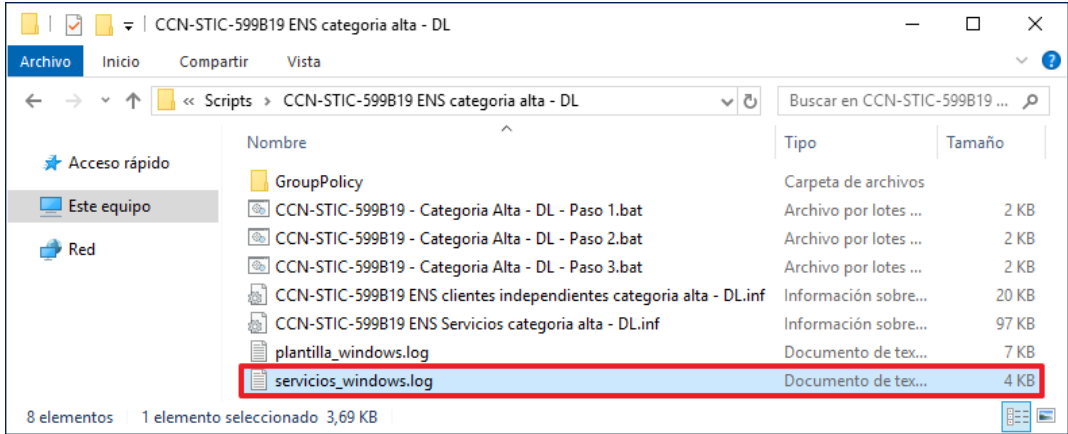
Paso	Descripción
5.	Abra la carpeta “CCN-STIC-599B19 ENS categoria alta” que encontrará en el directorio “C:\Scripts”.  Nota: Los scripts asumen que su ubicación es “C:\Scripts\CCN-STIC-599B19 ENS categoria alta - DL”. De no ser así deberá modificar los scripts para que coincidan con la ruta deseada.
6.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Alta - DL – Paso 1.bat” y seleccione la opción “Ejecutar como administrador”. 
7.	Pulse “Sí” cuando el control de cuentas de usuario, le solicite si desea que el programa realice cambios en el equipo. 

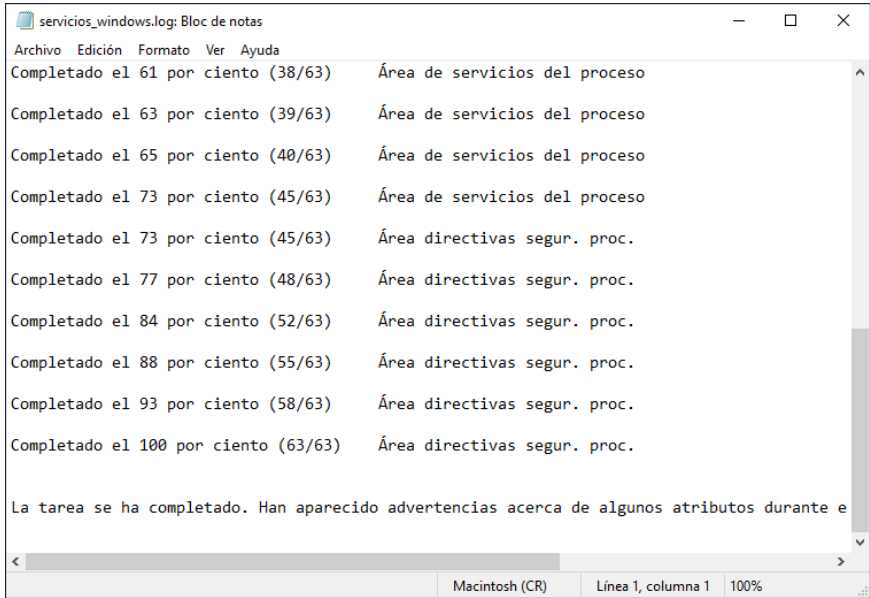
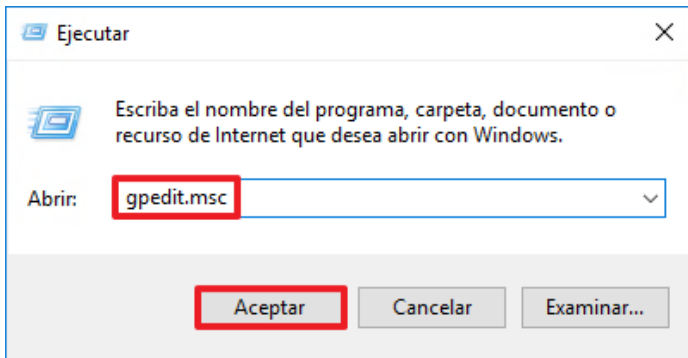
Paso	Descripción
8.	Pulse una tecla para iniciar la ejecución del script que configurará la plantilla de seguridad con la seguridad requerida para la categoría alta del ENS / Difusión Limitada. 
9.	Una vez completado el proceso, deberá pulsar una tecla para continuar. Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 
10.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 categoría alta - DL” con el nombre de “plantilla_windows.log”. 

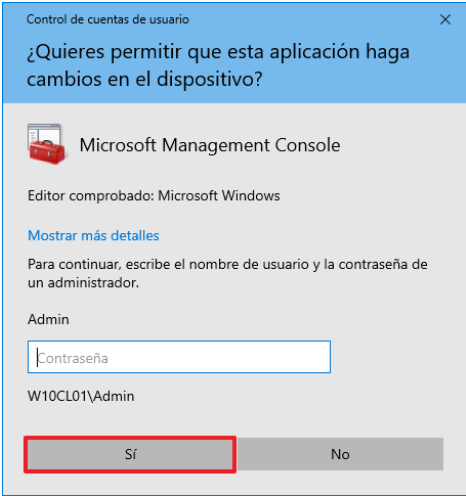
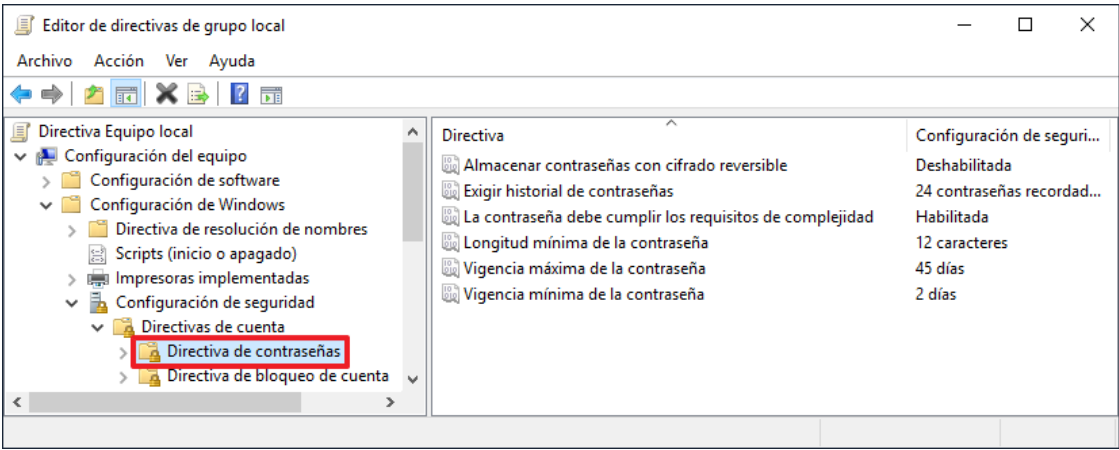
Paso	Descripción
11.	Abra este registro para comprobar si la configuración de la plantilla ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 5.
12.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Alta - DL – Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.

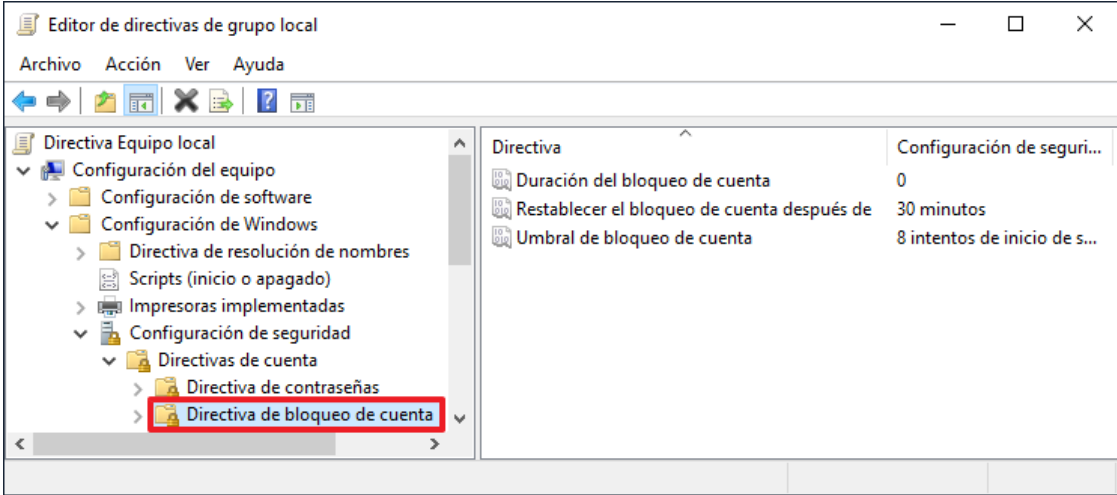
Paso	Descripción
13.	Introduzca las credenciales y pulse el botón “Sí”. 
14.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local. 
15.	Completada la copia de los archivos, compruebe que no ha habido errores en la copia de los mismos. Debería obtener el mismo resultado que el mostrado en la siguiente imagen. Pulse una tecla para finalizar la ejecución del script.  Nota: En caso de haberse producido fallos, solúcelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.

Paso	Descripción
16.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 – Categoría Alta - DL – Paso 3.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.
17.	Introduzca las credenciales y pulse el botón “Sí”. 
18.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la categoría alta del ENS / Difusión Limitada. 

Paso	Descripción
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 
20.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 ENS categoria alta - DL” con el nombre de “servicios_windows.log”. 

Paso	Descripción
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 16.
22.	Elimine la carpeta “C:\Scripts”.
23.	Es factible que su organización cuente con una política de contraseñas consolidada. La implementación de la política de categoría alta implementará una política específica para los clientes de categoría alta. Deberá evaluarla para determinar si esta configuración le es válida o por el contrario debe adaptarla a las condiciones de su organización.
24.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar la herramienta.

Paso	Descripción
25.	Introduzca las credenciales y pulse el botón “Sí”. 
26.	Despliegue la política y sitúese en la siguiente ruta: “Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseña” 
27.	Evalúe la política de contraseñas y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de credenciales es menos rigurosa que la marcada en la configuración deseada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de contraseñas a lo marcado por la configuración recomendada.

Paso	Descripción
28.	De forma similar a lo anterior, deberá evaluar la política de bloqueo de cuenta. Para ello y sin cerrar la política, seleccione “Directiva de bloqueo de cuenta” que encontrará al mismo nivel que “Directiva de contraseñas”. 
29.	Evalúe la política de bloqueo de cuenta y modifíquela convenientemente. Nota: Debe tener en consideración que, si su política de bloqueo de cuenta es menos rigurosa que la marcada en la configuración deseada se encuentra por debajo de los requerimientos de seguridad actuales. Debería plantear la adaptación progresiva de la directiva de bloqueo de cuenta a lo marcado por la configuración recomendada.

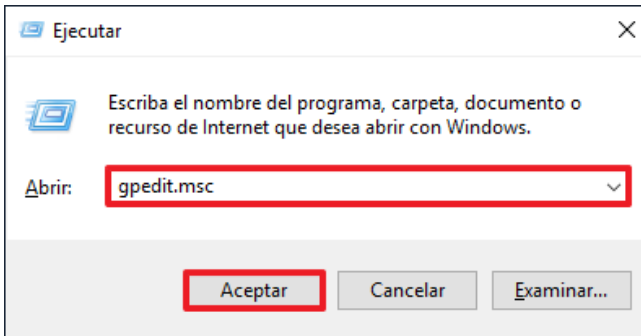
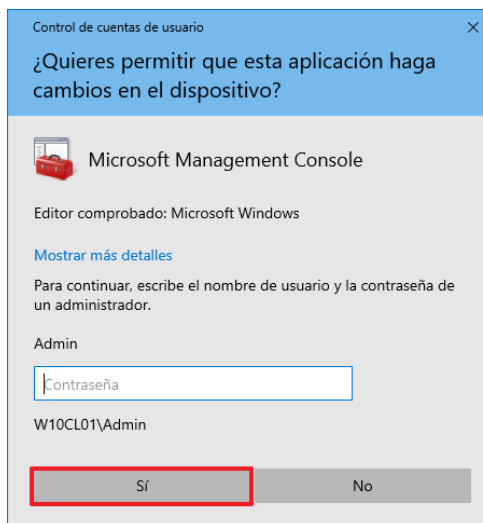
Hasta ahora han sido aplicados cambios, entre otros aspectos, sobre las directivas de contraseña y cuenta, aunque es importante señalar que existen más directivas interesantes a la hora de configurar el sistema.

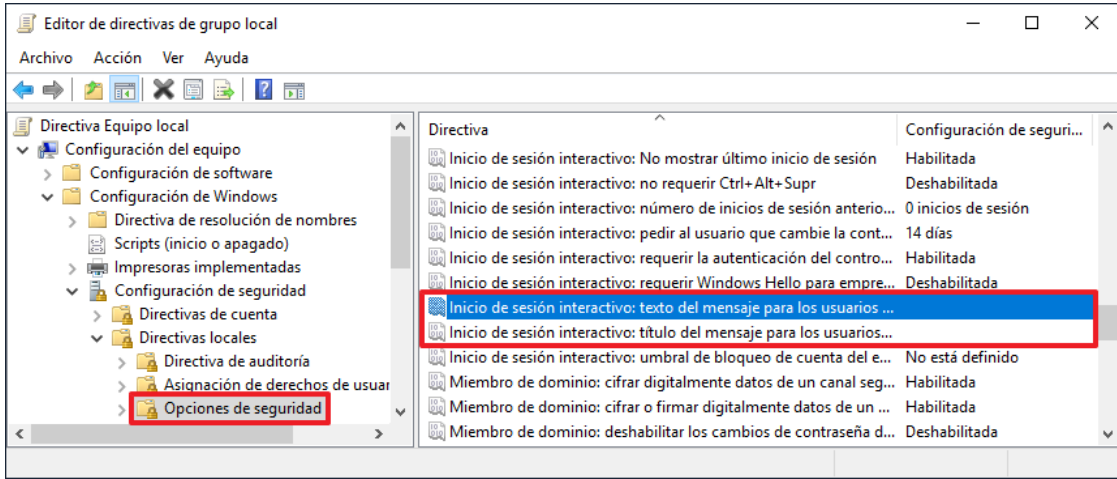
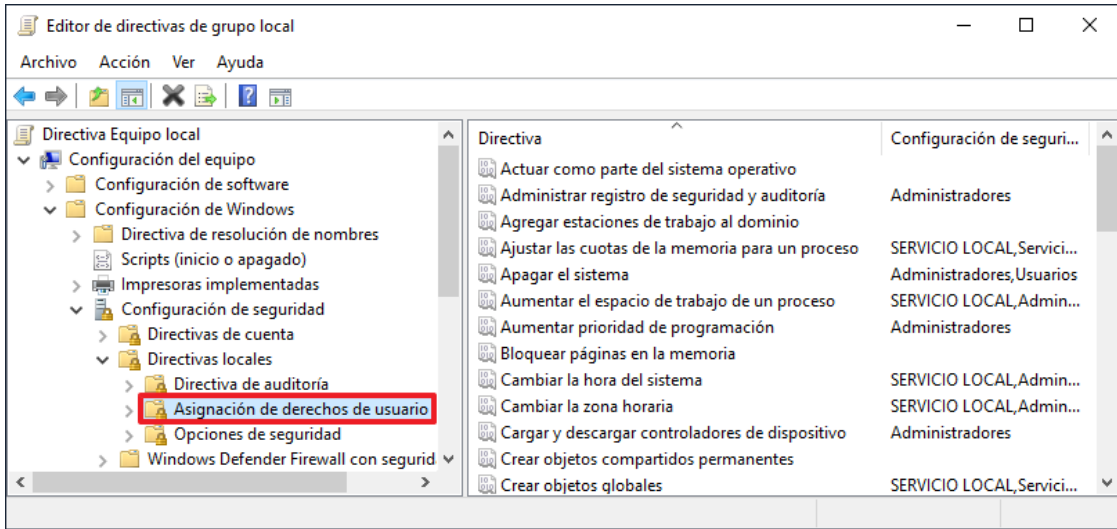
Uno de los aspectos que marca el ENS, desde su requisito de categoría alta en el Marco Operacional para el acceso local, consiste en la necesidad de informar al usuario de sus obligaciones.

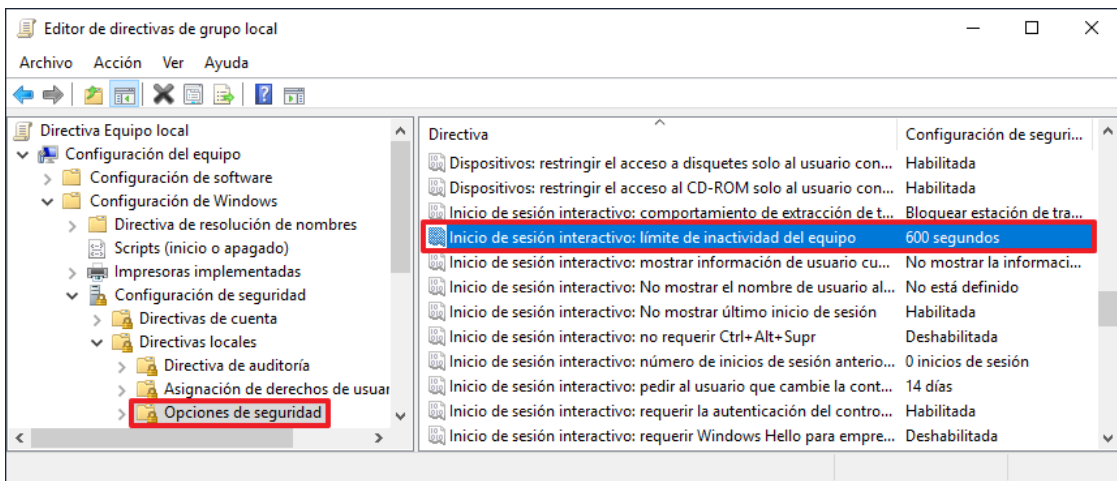
Los sistemas Windows presentan mecanismos para implementar mensajes que realizan advertencias al usuario cuando va a realizar el inicio de la sesión. Aunque pudieran emplearse otros tales como la ejecución de scripts, el empleo de este mecanismo es altamente recomendable. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Si fuera así, modifique el mensaje mostrado para adaptarlo también al cumplimiento del ENS según lo estipulado en la política de seguridad de su organización.

Si su organización no está haciendo uso de este mecanismo realice los siguientes pasos para habilitar el sistema de advertencia, con objeto de informar al usuario de sus obligaciones, según queda estipulado en la política de seguridad de la organización.

Paso	Descripción
30.	Inicie sesión en el cliente independiente donde se va a aplicar seguridad según criterios de ENS.
31.	Debe iniciar sesión con una cuenta que sea Administrador local.
32.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar la herramienta.
33.	Introduzca las credenciales y pulse el botón “Sí”. 
34.	Para informar de las obligaciones sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”

Paso	Descripción
35.	Identifique las directivas “Inicio de sesión interactivo: texto del mensaje para los usuarios que intenta iniciar una sesión” e “Inicio de sesión interactivo: título del mensaje para los usuarios que intenta iniciar una sesión”. 
36.	Edite ambas directivas incluyendo el título de la advertencia y el mensaje a facilitar a los usuarios según se estipule en las políticas de seguridad de la organización.
37.	Por último, la política de seguridad local especifica unos derechos de usuario siguiendo planteamientos de seguridad que aplican los principios de mínimo privilegio y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas. Si esto fuera así deberá realizar las modificaciones sobre la configuración de política local.
38.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 

Paso	Descripción
39.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
40.	Se establece a partir de la categoría media, según MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO la necesidad de realizar el bloqueo del equipo ante un tiempo razonable de inactividad. A través de la política local aplicable sobre equipo, puede establecerse la medida de protección que habilita el protector de pantalla y por lo tanto el bloqueo de la sesión. Nota: Si la organización presenta algún mecanismo para realizar el bloqueo del equipo ante inactividad no es necesario que aplique la siguiente configuración. No obstante, revise la configuración para adaptarse a la normativa vigente. Si la organización no tiene medidas dispuestas siga los siguientes pasos.
41.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad” Habilite y configure la siguiente directiva de seguridad: Inicio de sesión interactivo: límite de inactividad del equipo. Establezca el valor en 600 segundos (10 minutos). 
42.	Cierre el editor de política de grupo local.
43.	Reinicie el puesto de trabajo.

ANEXO C.3.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

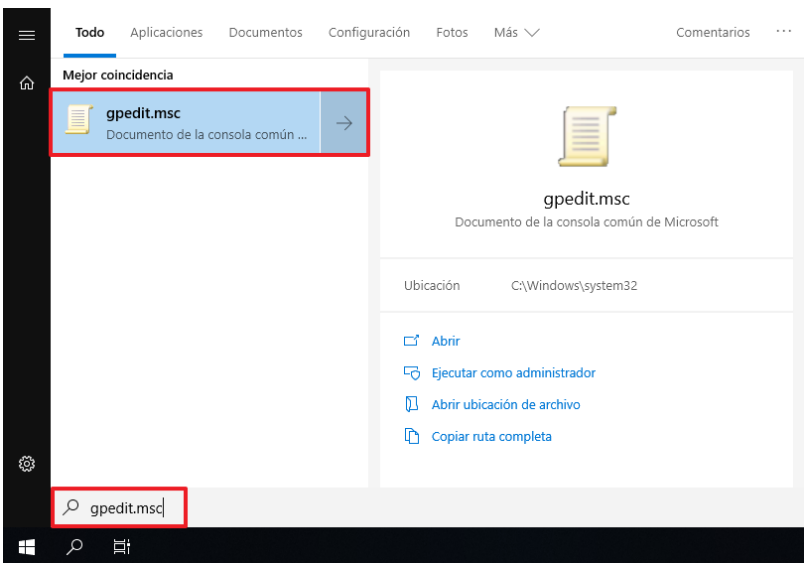
Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía “ANEXO C.3.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA”.

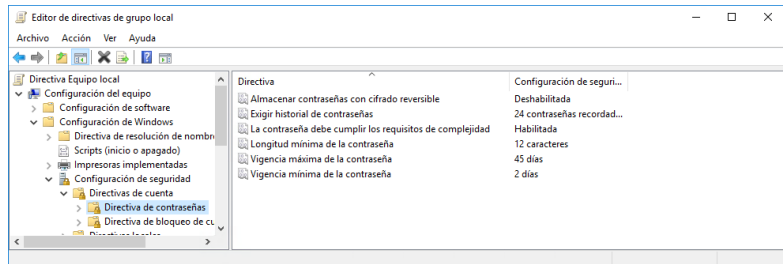
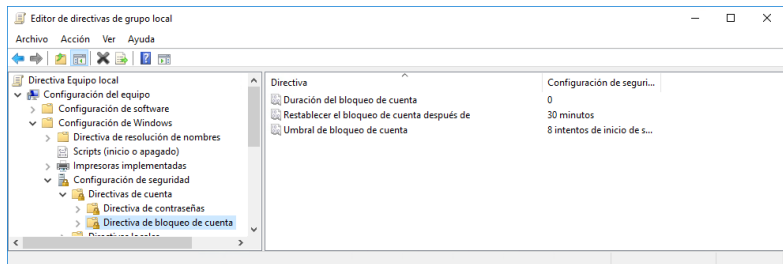
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los clientes Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC, independientes con implementación de seguridad de categoría alta del ENS/Difusión Limitada.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de administrador local.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario que es administrador local. Las consolas y herramientas que se utilizarán son las siguientes:

- Editor de objetos de directiva de grupo local (gpedit.msc)
- Editor de registro (regedit.exe)
- Visor de Eventos (eventvwr.exe)
- Servicios (services.msc)

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el cliente.		En el cliente, inicie sesión con una cuenta con privilegios de administración local.
2. Inicie la aplicación de gestión de políticas locales.		Ejecute el “Editor de objetos de directiva de grupo local”. Para ello pulse “Inicio”, teclee “gpedit.msc” y pulse “Enter”. 

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique la directiva de contraseñas en el editor de objetos de directiva de grupo local.		En el “Editor de objetos de directiva de grupo local” seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de contraseñas” Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. 
4. Verifique las directivas de bloqueo de cuenta en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas de Cuenta → Directiva de bloqueo de cuenta” 

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Duración del bloqueo de cuenta		0 minutos	
	Restablecer recuentos de bloqueo de cuenta tras		30 minutos	
	Umbral de bloqueo de cuenta		8 intentos de inicio de sesión no válidos	
5. Verifique las directivas de auditoría en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo: “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”		
	Directiva		Valor	OK/NOK
	Auditar el acceso a objetos		Correcto, Erróneo	
	Auditar el acceso del servicio de directorio		Correcto, Erróneo	
	Auditar el cambio de directivas		Correcto, Erróneo	
	Auditar el uso de privilegios		Correcto, Erróneo	
	Auditar eventos de inicio de sesión		Correcto, Erróneo	
	Auditar eventos de inicio de sesión de cuenta		Correcto, Erróneo	
	Auditar eventos del sistema		Correcto, Erróneo	
	Auditar la administración de cuentas		Correcto, Erróneo	
6. Verifique la asignación de derechos de usuario en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo Local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”		
	Directiva		Valor	OK/NOK
	Actuar como parte del sistema operativo		(Definida, pero sin ningún valor)	
	Administrar registro de seguridad y auditoría		Administradores	
	Agregar estaciones de trabajo al dominio		(Definida, pero sin ningún valor)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Ajustar las cuotas de la memoria para un proceso	Administradores, SERVICIO LOCAL, Servicio de red
		Apagar el sistema	Administradores, Usuarios
		Aumentar el espacio de trabajo de un proceso	Administradores, SERVICIO LOCAL, Usuarios
		Aumentar prioridad de programación	Administradores
		Bloquear páginas de la memoria	
		Cambiar la hora del sistema	SERVICIO LOCAL, Administradores
		Cambiar la zona horaria	SERVICIO LOCAL, Administradores
		Cargar y descargar controladores de dispositivo	Administradores
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)
		Crear objetos globales	SERVICIO LOCAL, Servicio de red, Administradores, SERVICIO
		Crear un archivo de paginación	Administradores
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)
		Crear vínculos simbólicos	Administradores
		Denegar el acceso desde la red	ANONYMOUS LOGON, Invitados
		Denegar el inicio de sesión como servicio	Invitados
		Denegar el inicio de sesión como trabajo por lotes	Invitados
		Denegar el inicio de sesión local	Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	SERVICIO LOCAL, Servicio de red
		Generar perfiles de un solo proceso	Administradores
		Generar perfiles del rendimiento del sistema	Administradores

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Obtén un token de suplantación para otro usuario de la misma sesión	Administradores
		Omitir comprobación de recorrido	SERVICIO LOCAL, Servicio de Red, Administradores, Usuarios Autenticados
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	(Definida, pero sin ningún valor)
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento de volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	SERVICIO LOCAL, Servicio de red
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	(Definida, pero sin ningún valor)
		Suplantar a un cliente tras la autenticación	Administradores, SERVICIO, Servicio de red, SERVICIO LOCAL
		Tener acceso a este equipo desde la red	Administradores, Usuarios
		Tomar posesión de archivos y otros objetos	Administradores

Comprobación	OK/NOK	Cómo hacerlo		
7. Verifique las opciones de seguridad en el editor de objetos de directiva de grupo local.		Seleccione el siguiente nodo. “Directiva Equipo local → Configuración del Equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente	(Definida, pero sin ningún valor)	
		Acceso a redes: modelo de seguridad y uso compartido para cuentas locales	Clásico: usuarios locales se autentican con credenciales propias	
		Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red	Habilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitada	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitada	
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitada	
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitada	
		Acceso a redes: rutas del Registro accesibles remotamente	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Server Applications Software\Microsoft\WindowsNT\CurrentVersion	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Acceso a redes: rutas y subrutinas del Registro accesibles remotamente	System\CurrentControlSet\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
		Acceso a red: permitir traducción SID/nombre anónima	Deshabilitada
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitada
		Apagado: permitir apagar el sistema sin tener que iniciar sesión	Habilitada
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitada
		Auditoría: auditar el acceso a objetos globales del sistema	Habilitada
		Auditoría: auditar el uso del privilegio de copias de seguridad y restauración	Habilitada
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitada
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Configuración del sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software	Deshabilitada	
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitada	
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitada	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitada	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento en el escritorio seguro	
		Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Pedir credenciales en el escritorio seguro	
		Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación	Habilitada	
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitada	
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitada
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitada
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitada
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de registro en diferentes ubicaciones por usuario	Habilitada
		Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo	El usuario debe escribir una contraseña cada vez que use una clave
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	Habilitada
		Cuentas: cambiar el nombre de cuenta de invitado	invitado
		Cuentas: cambiar el nombre de la cuenta de administrador	Administrador
		Cuentas: estado de la cuenta de administrador	Deshabilitada
		Cuentas: estado de la cuenta de invitado	Deshabilitada
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitada
		Dispositivos: impedir que los usuarios instalen controladores de impresora	Deshabilitada

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitada	
		Dispositivos: restringir el acceso a disquetes solo al usuario con sesión iniciada localmente	Habilitada	
		Dispositivos: restringir el acceso al CD-ROM solo al usuario con sesión iniciada localmente	Habilitada	
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo	
		Inicio de sesión interactivo: mostrar información de usuario cuando bloquee la sesión	No mostrar la información del usuario	
		Inicio de sesión interactivo: No mostrar último inicio de sesión	Habilitada	
		Inicio de sesión interactivo: No requerir Ctrl + Alt + Supr	Deshabilitada	
		Inicio de sesión interactivo: Número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)	0 inicios de sesión	
		Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire	14 días	
		Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo	Habilitada	
		Inicio de sesión interactivo: requerir Windows Hello para empresas o tarjeta inteligente	Deshabilitada	
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitada	
		Miembro de dominio: duración máxima de contraseña de cuenta de equipo	30 días	
		Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)	Habilitada	
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitada	
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitada	
		Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows	Habilitada	
		Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Habilitada	
		Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM	
		Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada	
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma	
		Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	
		Servidor de red de Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitada	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitada	
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitada	
		Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor	Requerido del cliente	
		Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión	15 minutos	
8. Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media”		
		Directiva	Valor	OK/NOK
		Impedir el acceso a internet de Windows Media DRM	Habilitada	
9. Verifique la directiva de almacén digital en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Almacén digital”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitada	
10.Verifique la directiva de Antivirus en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitada	
11.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitada	
12.Verifique las directivas de biometría en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Habilitada	
		Permitir que los usuarios de dominio inicien sesión mediante biometría	Habilitada	
		Permitir que los usuarios inicien sesión mediante biometría	Habilitada	
13.Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Buscar”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	No buscar en Internet o mostrar resultados de Internet en Search		Habilitada	
	Permitir el uso de Cortana		Deshabilitada	
14. Verifique las directivas de contenido en la nube en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Contenido en la Nube”		
	Directiva		Valor	OK/NOK
	Desactivar experiencias del consumidor de Microsoft		Habilitada	
	No mostrar recomendaciones de Windows		Habilitada	
15. Verifique las directivas de reproducción automática en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
	Directiva		Valor	OK/NOK
	Desactivar reproducción automática		Habilitada (Todas las unidades)	
	Establece el comportamiento predeterminado para la ejecución automática		Habilitada (No ejecutar ningún comando de ejecución automática)	
16. Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
	Directiva		Valor	OK/NOK
	Configurar Windows SmartScreen de Windows Defender		Habilitada (Advertir e impedir la omisión)	

Comprobación	OK/NOK	Cómo hacerlo		
17.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitada	
		No enviar datos adicionales	Habilitada	
18.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer”		
		Directiva	Valor	OK/NOK
		Activar sitios sugeridos	Deshabilitada	
		Impedir la administración del filtro SmartScreen	Deshabilitada	
		Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	Habilitada	
19.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de Internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitada	
20.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Eliminar el historial de exploración”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento.	Deshabilitada	
		Impedir que se elimine el historial de descarga	Deshabilitada	
		Impedir que se eliminen contraseñas	Deshabilitada	
		Impedir que se eliminen cookies	Deshabilitada	
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitada	
		Impedir que se eliminen los archivos temporales de Internet	Deshabilitada	
		Impedir que se eliminen los datos de filtrado InPrivate	Deshabilitada	
		Impedir que se eliminen los datos de formularios	Deshabilitada	
		Impedir que se eliminen los sitios web que el usuario visitó	Deshabilitada	
		Permitir que se elimine el historial de exploración al salir	Habilitada	
21.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitada	
22.Verifique las directivas de OneDrive en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitada	

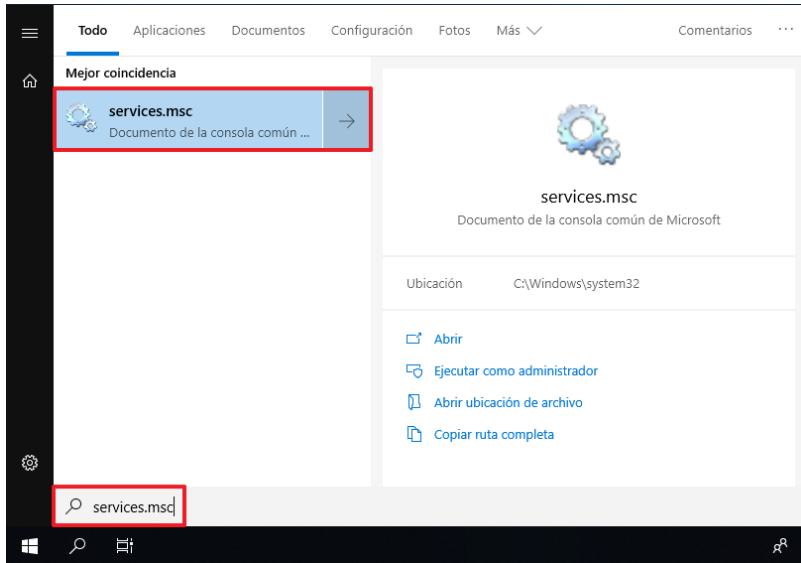
Comprobación	OK/NOK	Cómo hacerlo		
23.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK
		Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario	Habilitada	
		Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	Habilitada	
24.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitada (Solo HTTP (0))	
25.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitada (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows controlen las radios	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitada (Forzar denegación)
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitada (Forzar denegación)
26.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	No volver a mostrar notificaciones de comentarios		Habilitada	
	Permitir telemetría		Habilitada	
27.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”			
	Directiva		Valor	OK/NOK
	Permitir acceso a Shell remoto		Deshabilitada	
28.Verifique la directiva de Smart Screen en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”			
	Directiva		Valor	OK/NOK
	Configurar SmartScreen de Windows Defender		Habilitada (Advertir e impedir la omisión)	
29.Verifique la directiva de Tienda en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Tienda”			
	Directiva		Valor	OK/NOK
	Desactivar la aplicación Store		Habilitada	
	Deshabilita todas las aplicaciones de Microsoft Store		Deshabilitada	
30.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo local.	Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”			

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar scripting de ubicación		Habilitada	
	Desactivar sensores		Habilitada	
	Desactivar ubicación		Habilitada	
31.Verifique la directiva de Windows Update en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
	Directiva		Valor	OK/NOK
	Administrar preliminares		Habilitada (Deshabilitar preliminares)	
32.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		
	Directiva		Valor	OK/NOK
	Desactivar el aprendizaje automático		Habilitada	
33.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
	Directiva		Valor	OK/NOK
	Desactivar el acceso a Store		Habilitada	
	Desactivar el contenido “¿Sabías que...?” del Centro de ayuda y soporte técnico		Habilitada	
	Desactivar el informe de errores de Windows		Habilitada	
	Desactivar el Programa para la mejora de la experiencia del usuario de Windows		Habilitada	
	Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitada
		Desactivar la actualización de archivos de contenido del Asistente para búsqueda	Habilitada
		Desactivar búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico	Habilitada
		Desactivar la tarea de imágenes "Pedir copias fotográficas"	Habilitada
		Desactivar los vínculos "Event.asp" del Visor de eventos	Habilitada
		Desactivar uso compartido de datos de personalización de escritura a mano	Habilitada
34.Verifique la directiva de Net Logon en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. "Configuración del Equipo → Plantillas Administrativas → Sistema → Net Logon"	
		Directiva	Valor
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada
35.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. "Configuración del Equipo → Plantillas Administrativas → Sistema → Perfiles de usuario"	
		Directiva	Valor
		Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)	Habilitada
		Desactivar el identificador de publicidad	Habilitada

Comprobación	OK/NOK	Cómo hacerlo															
36.Verifique la directiva de personalización en el objeto de directiva de grupo local.		Seleccione el siguiente nodo. “Configuración del Usuario → Plantillas Administrativas → Panel de control → Personalización”															
		<table><tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Habilitar protector de pantalla</td><td>Habilitada</td><td></td></tr><tr><td>Proteger el protector de pantalla mediante contraseña</td><td>Habilitada</td><td></td></tr><tr><td>Tiempo de espera del protector de pantalla</td><td>Habilitada (600 segundos)</td><td></td></tr><tr><td>Aplicar un protector de pantalla específico</td><td>Habilitada</td><td></td></tr></table>	Directiva	Valor	OK/NOK	Habilitar protector de pantalla	Habilitada		Proteger el protector de pantalla mediante contraseña	Habilitada		Tiempo de espera del protector de pantalla	Habilitada (600 segundos)		Aplicar un protector de pantalla específico	Habilitada	
	Directiva	Valor	OK/NOK														
	Habilitar protector de pantalla	Habilitada															
	Proteger el protector de pantalla mediante contraseña	Habilitada															
Tiempo de espera del protector de pantalla	Habilitada (600 segundos)																
Aplicar un protector de pantalla específico	Habilitada																
37.Verifique el modo de configuración de los servicios del sistema.		Ejecute la herramienta de servicios. Para ello pulse “Inicio”, teclee “services.msc” y pulse “Enter”.															
		 Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto, entre paréntesis) para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el sistema o el nombre corto si no lo está. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.															



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Acceso a datos de usuarios	UserDataSvc	Manual	Configurado		
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado		
Adaptador de escucha Net.Msmq	NetMsmqActivator	Automático	Configurado		
Adaptador de escucha Net.Pipe	NetPipeActivator	Automático	Configurado		
Adaptador de escucha Net.Tcp	NetTcpActivator	Automático	Configurado		
Adaptador de rendimiento de WMI	wmiApSrv	Manual	Configurado		
Administración de aplicaciones	AppMgmt	Manual	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Manual	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Automático	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Manual	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Manual	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Automático	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Manual	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administrador de cuentas web	TokenBroker	Manual	Configurado		
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMgrSvc	Manual	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Manual	Configurado		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Manual	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Automático	Configurado		
Agrupación de red del mismo nivel	p2psvc	Manual	Configurado		
Aislamiento de claves CNG	KeyIso	Manual	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Manual	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Manual	Configurado		
Aplicación auxiliar IP	iphlpvc	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Manual	Configurado		



Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Archivos sin conexión	CscService	Manual	Configurado	
Asignador de detección de topologías de nivel de vínculo	ltdsvc	Manual	Configurado	
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado	
Asistente para la conectividad de red	NcaSvc	Manual	Configurado	
ASP.NET State Service	aspnet_state	Manual	Configurado	
Audio de Windows	Audiosrv	Automático	Configurado	
Autenticación natural	NaturalAuthentication	Manual	Configurado	
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado	
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Manual	Configurado	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado	
BranchCache	PeerDistSvc	Manual	Configurado	
Captura SNMP	SNMPTRAP	Manual	Configurado	
CaptureService	CaptureService	Manual	Configurado	
Carpetas de trabajo	workfoldersvc	Manual	Configurado	
CDPUserSvc	CDPUserSvc	Automático	Configurado	
Centro de seguridad	wscsvc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Automático	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	
Cliente para NFS	NfsClnt	Automático	Configurado	
Cliente web	WebClient	Manual	Configurado	
Cola de impresión	Spooler	Automático	Configurado	
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Automático	Configurado	
Comprobador puntual	svsvc	Manual	Configurado	
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado	
Conexiones de red	Netman	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración automática de WLAN	WlanSvc	Manual	Configurado		
Configuración automática de WWAN	WwanSvc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Manual	Configurado		
ConsentUX	ConsentUxUserSvc	Manual	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Manual	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Manual	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Automático	Configurado		
Detección de hardware shell	ShellHWDetection	Automático	Configurado		
Detección SSDP	SSDPSRV	Manual	Configurado		
DevicePicker	DevicePickerUserSvc	Manual	Configurado		
DevicesFlow	DevicesFlowUserSvc	Manual	Configurado		
Diagnostic Execution Service	diagsvc	Manual	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Manual	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Manual	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Energía	Power	Automático	Configurado	
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado	
Escucha de RIP	iprip	Automático	Configurado	
Estación de trabajo	LanmanWorkstation	Automático	Configurado	
Eventos de adquisición de imágenes estáticas	WiaRpc	Manual	Configurado	
Examinador de equipos	Browser	Manual	Configurado	
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado	
Extensiones y notificaciones de impresora	PrintNotify	Manual	Configurado	
Fax	Fax	Manual	Configurado	
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado	
Firewall de Windows	MpsSvc	Automático	Configurado	
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado	
Hora de Windows	W32Time	Manual	Configurado	
Host de proveedor de detección de función	fdPHost	Manual	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Manual	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Manual	Configurado	
Identidad de aplicación	AppIDSvc	Manual	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Manual	Configurado	
Instalador de ActiveX (AxInstSV)	AxInstSV	Manual	Configurado	
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado	
Instantáneas de volumen	VSS	Manual	Configurado	
Instrumental de administración de Windows	Winmgmt	Automático	Configurado	



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Manual	Configurado		
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Manual	Configurado		
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado		
LxssManager	LxssManager	Manual	Configurado		
Message Queue Server	MSMQ	Automático	Configurado		
MessagingService	MessagingService	Manual	Configurado		
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado		
Microsoft Passport	NgcSvc	Manual	Configurado		
Modo incrustado	embeddedmode	Manual	Configurado		
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Manual	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Manual	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Manual	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Manual	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Manual	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Manual	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Manual	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado		
Registrador de configuración de Windows Connect Now	wcnscvc	Manual	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Manual	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Manual	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Automático	Configurado		
Servicio AVCTP	BthAvctpSvc	Manual	Configurado		
Servicio biométrico de Windows	WbioSrv	Manual	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado	
Servicio de administración de aplicaciones de empresa	EntAppSvc	Manual	Configurado	
Servicio de administración de radio	RmSvc	Manual	Configurado	
Servicio de administración de web	WMSVC	Manual	Configurado	
Servicio de administración de Windows	WManSvc	Manual	Configurado	
Servicio de administración IIS	IISADMIN	Automático	Configurado	
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Manual	Configurado	
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado	
Servicio de almacenamiento	StorSvc	Manual	Configurado	
Servicio de asistente para perfil local	wlpcsvc	Manual	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Automático	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdown	Manual	Configurado	
Servicio de cliente de protección de host	HgClientService	Manual	Configurado	
Servicio de compatibilidad con Bluetooth	bthserv	Manual	Configurado	
Servicio de configuración de red	NetSetupSvc	Manual	Configurado	
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de datos del sensor	SensorDataService	Manual	Configurado		
Servicio de datos espacial	SharedRealitySvc	Manual	Configurado		
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Manual	Configurado		
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado		
Servicio de dispositivo de interfaz humana	hidserv	Manual	Configurado		
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado		
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado		
Servicio de geolocalización	lfsvc	Manual	Configurado		
Servicio de historial de archivos	fhsvc	Manual	Configurado		
Servicio de host HV (Hyper-V)	HvHost	Manual	Configurado		
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado		
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado		
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado	
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado	
Servicio de instalación de Microsoft Store	InstallService	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Manual	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Manual	Configurado	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado	
Servicio de lista de redes	netprofm	Manual	Configurado	
Servicio de mejora de visualización	DisplayEnhancementService	Manual	Configurado	
Servicio de monitor de infrarrojos	irmon	Manual	Configurado	
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado	
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Manual	Configurado	
Servicio de percepción de Windows	spectrum	Manual	Configurado	
Servicio de perfil de usuario	ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados	CDPSvc	Automático	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Manual	Configurado	
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Manual	Configurado	
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Manual	Configurado	
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado	
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Manual	Configurado	



Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de publicación World Wide Web	W3SVC	Automático	Configurado	
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Manual	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Manual	Configurado	
Servicio de red de host	hns	Manual	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado	
Servicio de registro de W3C	w3logsvc	Manual	Configurado	
Servicio de reparación MultiPoint	WmsRepair	Automático	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Manual	Configurado	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Manual	Configurado	
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Manual	Configurado	
Servicio de supervisión de sensores	SensrSvc	Manual	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Automático	Configurado	
Servicio de uso compartido de datos	DsSvc	Manual	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Manual	Configurado	
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado	
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado	

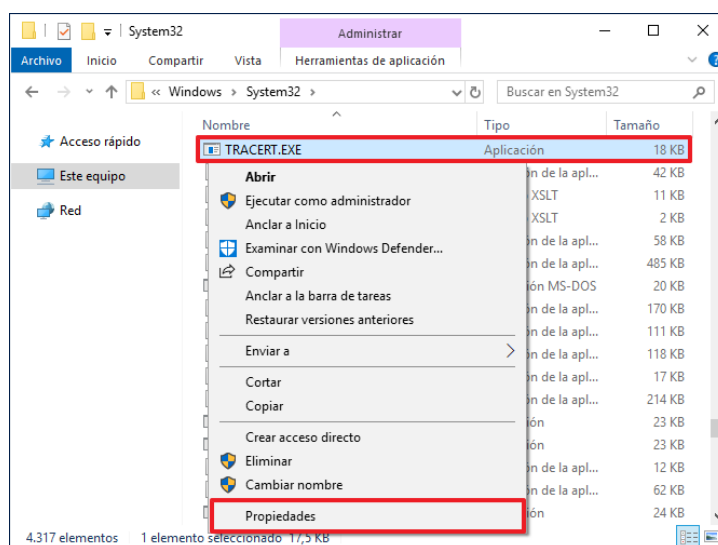
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Automático	Configurado		
Servicio de usuario del portapapeles	cbdhsvc	Manual	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Manual	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Manual	Configurado		
Servicio de Windows Defender	WinDefend	Manual	Configurado		
Servicio de Windows Insider	wisvc	Manual	Configurado		
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado		
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Manual	Configurado		
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Manual	Configurado		
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado		
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Manual	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Manual	Configurado		
Servicio FTP de Microsoft	ftpsvc	Automático	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio LPD	LPDSVC	Automático	Configurado		
Servicio MultiPoint	Wms	Automático	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado		
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Manual	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio telefónico	PhoneSvc	Manual	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Manual	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Manual	Configurado		
Servicios simples de TCP/IP	simptcp	Automático	Configurado		
Servidor	LanmanServer	Automático	Configurado		
Servidor de roles de DS	DsRoleSvc	Manual	Configurado		
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado		
Sincronizar host	OneSyncSvc	Automático	Configurado		
Sistema de cifrado de archivos (EFS)	EFS	Manual	Configurado		
Sistema de eventos COM+	EventSystem	Automático	Configurado		
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado		
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Manual	Configurado		
Superfetch	SysMain	Automático	Configurado		

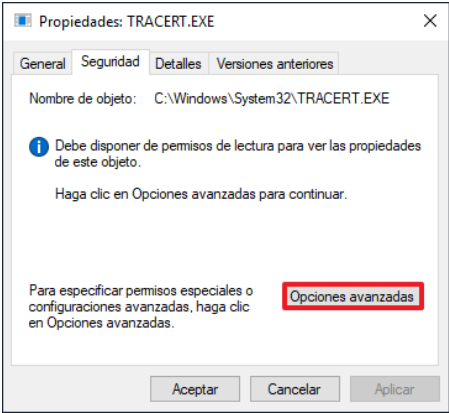
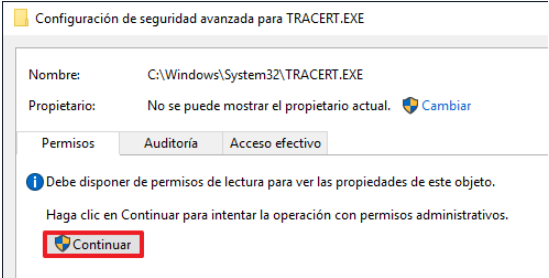
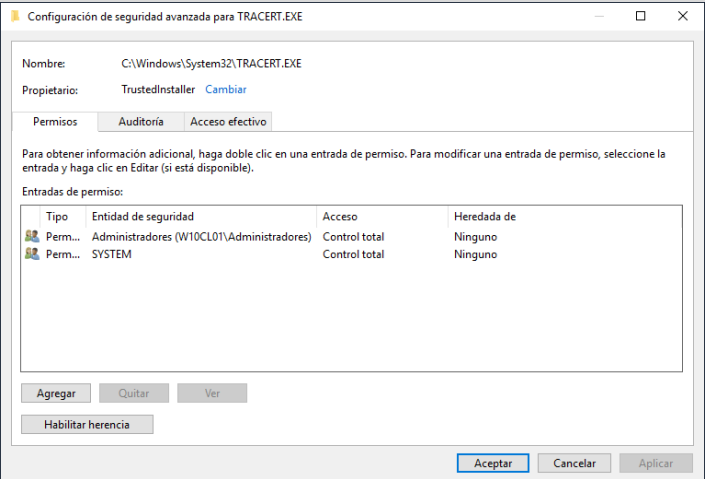
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado	
Telefonía	TapiSrv	Manual	Configurado	
Telemetría y experiencias del usuario conectado	DiagTrack	Automático	Configurado	
Temas	Themes	Automático	Configurado	
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado	
Uso de datos	DusmSvc	Automático	Configurado	
WalletService	WalletService	Manual	Configurado	
WarpJITSvc	WarpJITSvc	Manual	Configurado	
Windows Installer	msiserver	Manual	Configurado	
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Manual	Configurado	
Windows Search	WSearch	Automático	Configurado	
Windows Update	wuauserv	Manual	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Manual	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	

38. Verifique los permisos asignados a ficheros y carpetas.

Abra una ventana de Windows Explorer y diríjase a cada una de las rutas que indica el listado. Haga clic derecho con el ratón y seleccione la opción "Propiedades".



Nota: Deberá tener precaución para no realizar cambios sobre los permisos. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Comprobación	OK/NOK	Cómo hacerlo
		En la pestaña “Seguridad”, seleccione “Opciones Avanzadas”.  Es posible que deba pulsar sobre el botón “Continuar” para ver los permisos asignados.  Nota: Es posible que debido a la categoría de seguridad establecida en el sistema aparezca una ventana de Control de cuentas de usuario solicitando elevación o aceptación. Acepte o complete los espacios en blanco. En la ventana resultante, compruebe los permisos asignados a cada carpeta o fichero. Nota: Tenga en consideración que es posible que algunos ficheros no se encuentren en el sistema debido a la configuración aplicada y según las necesidades que requiera su organización. 



Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%Public%\		Administradores	Control total	
		System	Control total	
		Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\security		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\ras		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control total	
%SystemRoot%\system32\raschap.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control total	
%SystemRoot%\system32\rastls.dll		Administradores	Control total	
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
%SystemRoot%\system32\tracert.exe		Administradores	Control total	
		System	Control total	

ANEXO C.3.3. IMPLEMENTACIÓN DE BITLOCKER PARA CIFRADO DE DISCO EN CLIENTES WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

Tal y como se comentó en el punto “1.2.1.2. MP. EQ. 3. PROTECCIÓN DE LOS PORTÁTILES” sobre las medidas de protección de los portátiles en la categoría alta, es una necesidad de cumplimiento la implementación de medidas que garantizaran la confidencialidad de los datos almacenados. La implementación de BitLocker como mecanismo para el cifrado, permite garantizar el cumplimiento de esta medida.

Debe tenerse en consideración que la funcionalidad de BitLocker en Windows 10 se encuentra disponible en las versiones Enterprise y Pro. Si tiene implementado en su organización otra versión de Windows no podrá hacer uso de BitLocker y por lo tanto no deberá implementar este Anexo. Recuerde que no es una exigencia del ENS el que se haga implementación de BitLocker, puede hacer uso de otra solución que garantice la confidencialidad de los datos y que cumpla con los requerimientos de criptografía.

Este anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar la implementación de cifrado. Debe tomarse en consideración que el cifrado con BitLocker se basa en el uso de un sistema de cifrado basado en AES más CBC y un difusor denominado Elephant. No obstante, para poder acceder a la información cifrada es necesaria hacer uso de una clave de descifrado almacenado en una unidad flash USB o un PIN que libera la clave almacenada en el módulo de plataforma segura (TPM).

Se aconseja el uso de TPM como mecanismo para garantizar la funcionalidad de BitLocker. Aunque podría implementarse la unidad flash USB para almacenar la clave de descifrado, se desaconseja dicho mecanismo puesto que sería bastante habitual que el usuario ubicara dicha unidad en la misma ubicación donde transporta el portátil. Ante un eventual robo o pérdida del maletín, se estaría facilitando el mecanismo para acceder a la información cifrada.

Debe tener en cuenta que ante un potencial problema del módulo TPM podría necesitar acceder a la información cifrada sin la posibilidad de uso del mismo. BitLocker permite generar una clave de recuperación que almacenada de forma original en un dispositivo de memoria USB deberá almacenar posteriormente en algún lugar seguro.

Todas aquellas organizaciones que tengan acuerdo con Microsoft para cliente con Software Assurance tendrán a su disposición la solución MDOP (Microsoft Desktop Optimization Pack).

La implementación de BitLocker requiere de ciertos requisitos de tipo hardware y software:

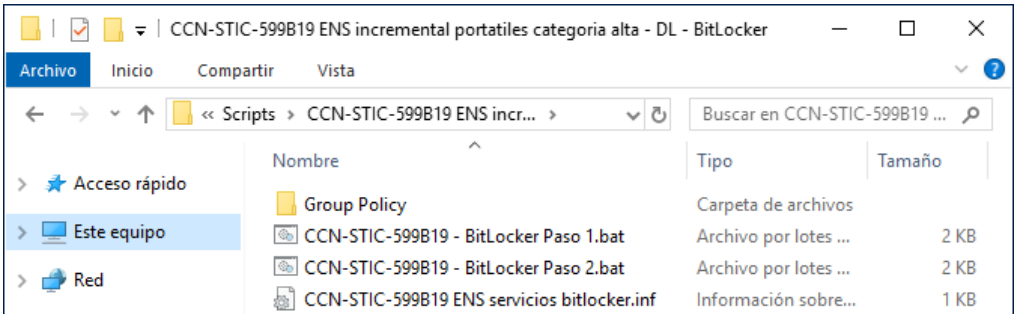
- a) Un equipo que cumpla los requisitos mínimos para Windows 10.
- b) Un chip TPM versión 1.2 o 2.0 activado. La activación de dicho chip se realiza a través del BIOS, siendo necesaria su implementación para garantizar su funcionalidad.
- c) BIOS compatible con TCG (Trusted Computing Group).

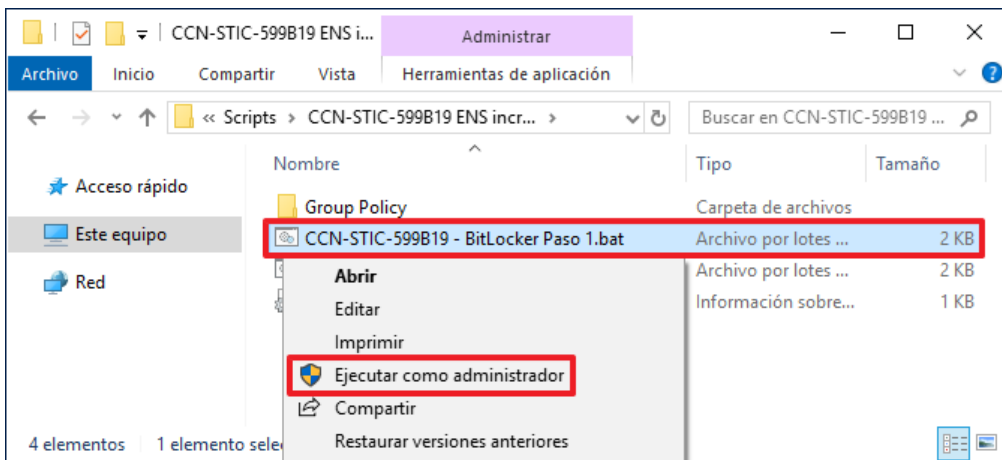
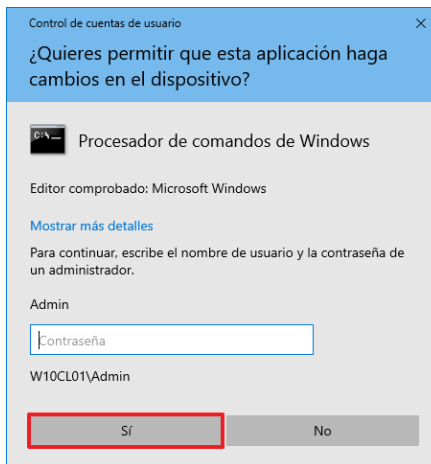
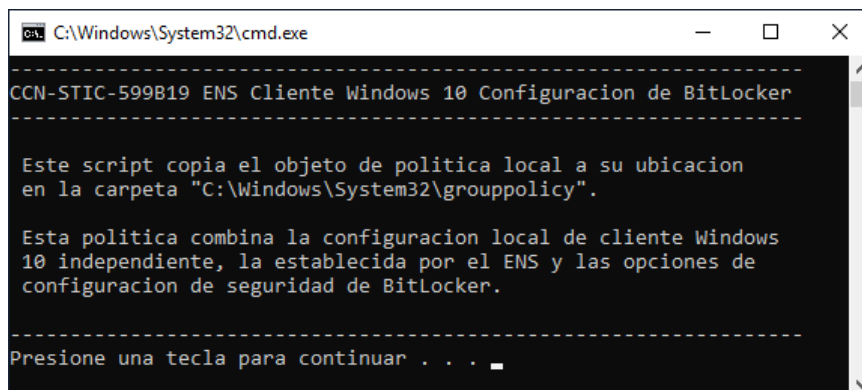
- d) Una partición de disco para la unidad del sistema, además de la partición que alberga el sistema operativo. En Windows 10, si cuenta con una sola partición de disco, BitLocker preparará automáticamente la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema que albergará los archivos del sistema que se necesitan para iniciar o recuperar el sistema operativo y que no se pueden cifrar. Esta unidad no tendrá una letra de unidad para evitar que se almacenen archivos de datos en esta unidad sin darse cuenta. Una vez que la unidad está preparada, debe reiniciarse el equipo.

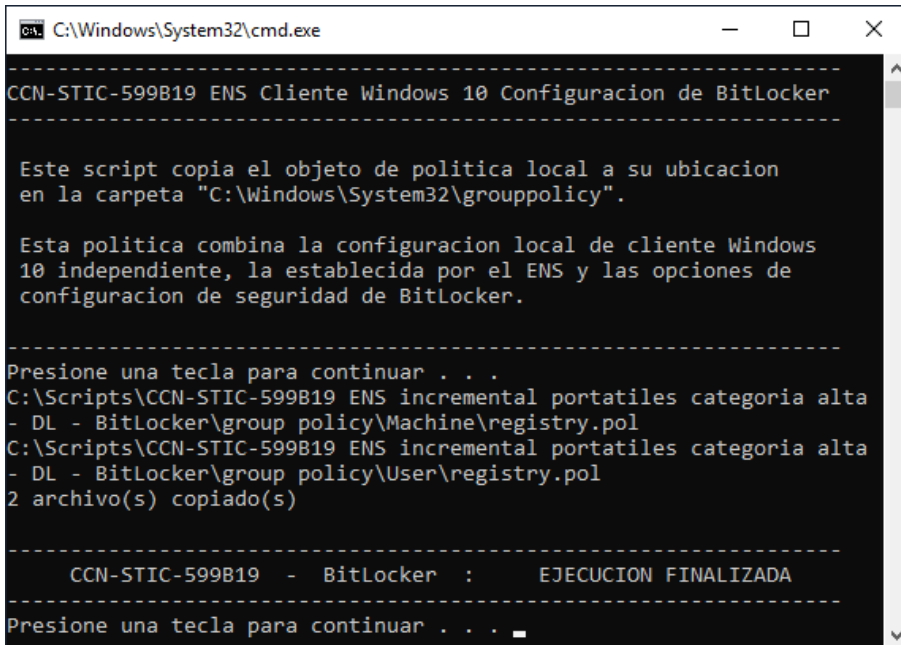
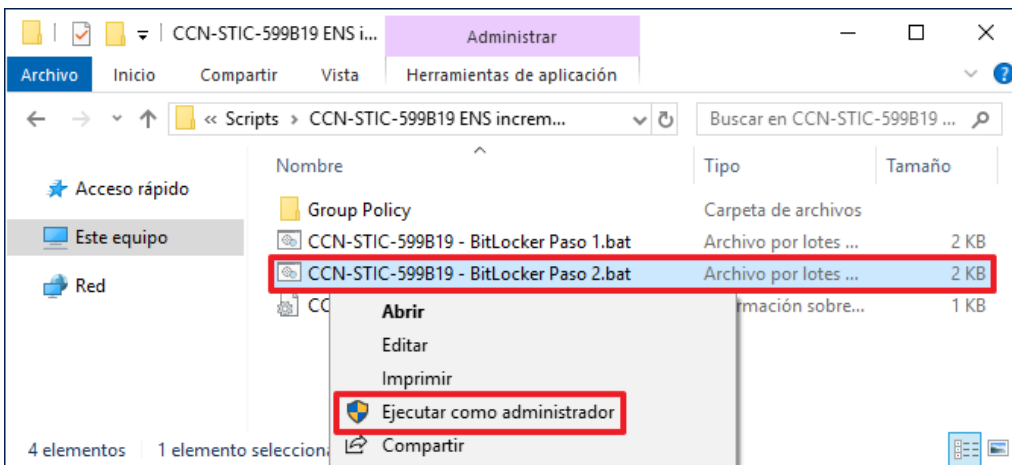
No obstante, si se ha realizado una instalación por defecto de Windows 10, el programa de instalación ya habrá creado, durante la instalación, las dos particiones de disco necesarias para activar BitLocker.

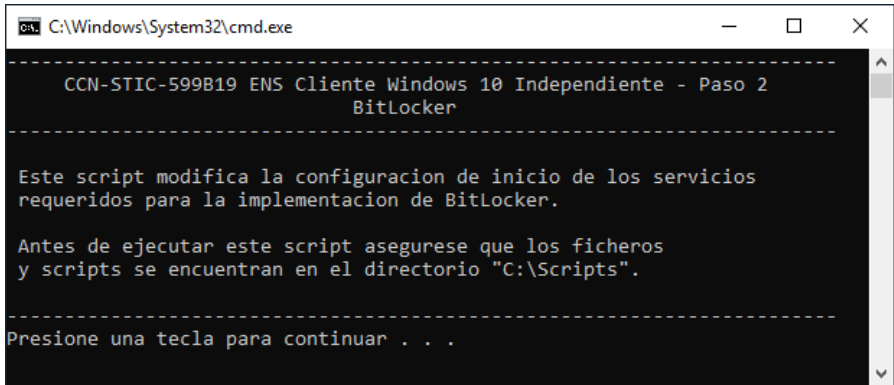
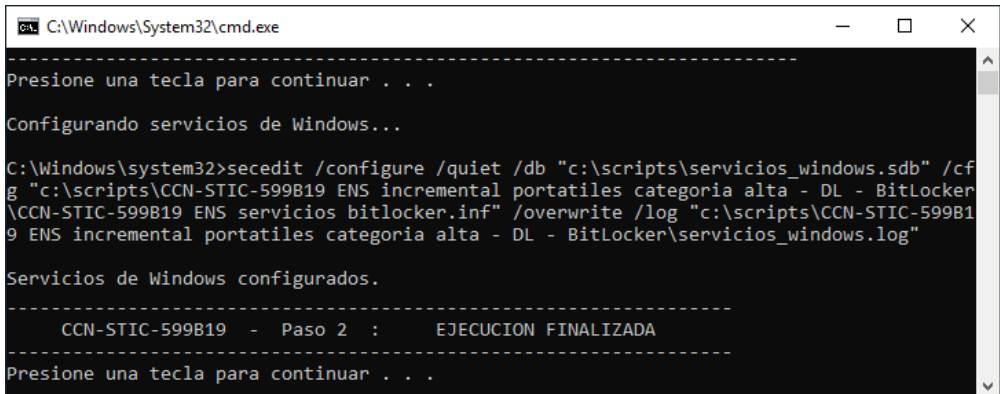
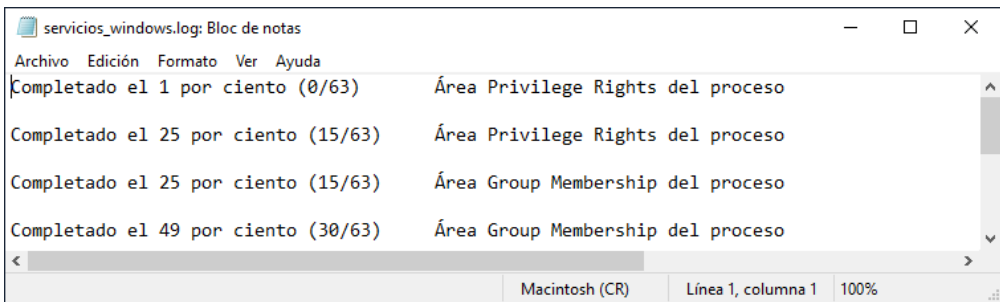
- Una unidad flash USB para almacenar claves de inicio y recuperación.
- Una configuración BIOS para iniciar primero desde el disco duro, no desde las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como la clave de recuperación), el BIOS debe admitir la lectura de unidades flash USB en el inicio.
- Opcionalmente, se puede disponer de una impresora conectada y configurada, para la impresión de las claves de recuperación. Alternativamente, se podrá tomar nota manualmente de las claves de recuperación.

La implementación de BitLocker se basará en la aplicación de la política de seguridad aplicada sobre un grupo de equipos determinados. Para ello deberán seguirse los siguientes pasos.

Paso	Descripción
1.	Inicie sesión en el cliente con un usuario con privilegios de administrador.
2.	Cree el directorio "Scripts" en la unidad C:\.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
4.	Abra la carpeta "CCN-STIC-599B19 ENS incremental portátiles categoría alta – DL - BitLocker" que encontrará en la carpeta "C:\Scripts" que ha copiado.  Nota: Los scripts asumen que su ubicación es "C:\Scripts\CCN-STIC-599B19 ENS incremental portátiles categoría alta – DL - BitLocker". De no ser así deberá modificar los scripts para que coincidan con la ruta deseada.

Paso	Descripción
5.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 BitLocker Paso 1.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.
6.	Introduzca las credenciales y pulse el botón “Sí”. 
7.	Pulse una tecla para iniciar la ejecución del script que configurará las plantillas para la seguridad de la política de seguridad local para el uso de BitLocker. 

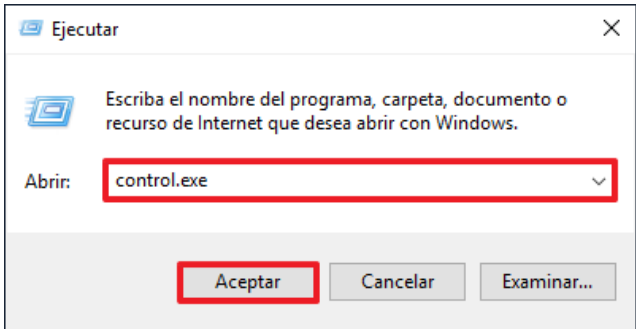
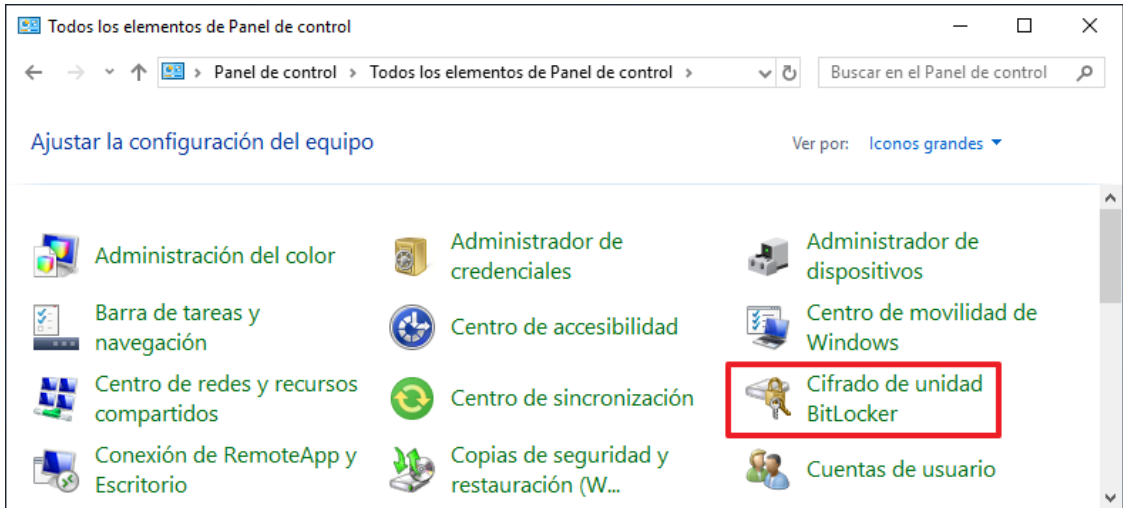
Paso	Descripción
8.	Completada la copia de los archivos, pulse una tecla para finalizar la ejecución del script. Compruebe que no ha habido errores en la copia de los archivos. Debería obtener el mismo resultado que se muestra en la imagen siguiente.  Nota: En caso de haberse producido fallos, solúcelos y vuelva a ejecutar el script. Normalmente los fallos se habrán producido porque no ha ejecutado el script con privilegios de administrador y por lo tanto no se habrán concedido los privilegios adecuados para copiar en la ruta de destino.
9.	A continuación, pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-599B19 BitLocker Paso 2.bat” y seleccione la opción “Ejecutar como administrador”.  Nota: Puesto que la configuración del control de cuentas de usuarios ya se encuentra aplicada deberá introducir las credenciales de un usuario con privilegios de administrador para ejecutar el script.
10.	Introduzca las credenciales y pulse el botón “Sí”.

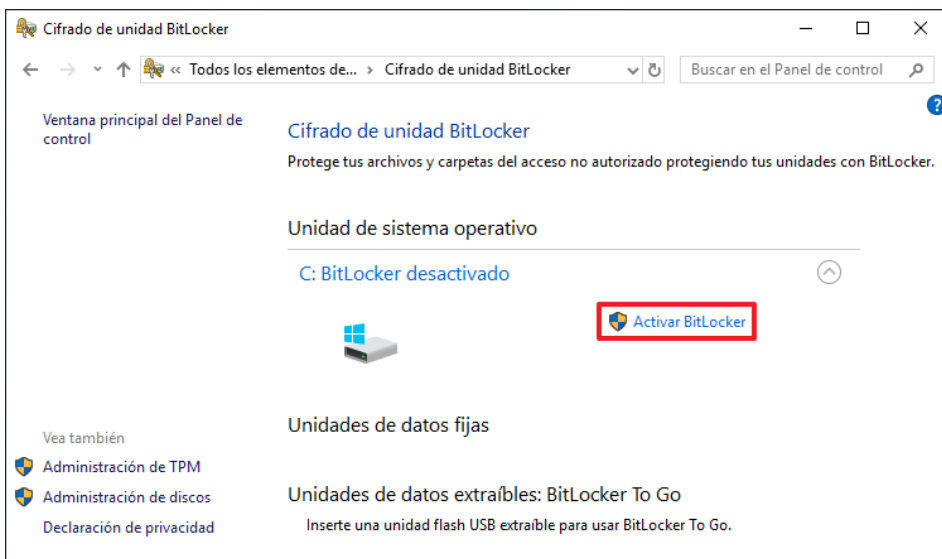
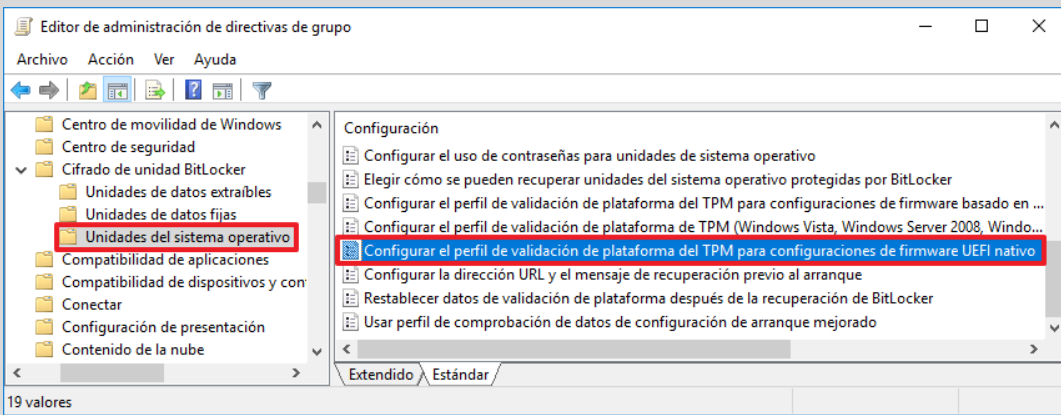
Paso	Descripción
11.	Pulse una tecla para iniciar la ejecución del script que configurará los servicios de Windows con la seguridad requerida para la implementación de BitLocker. 
12.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 
13.	La ejecución del script genera un registro (log) en la carpeta “C:\Scripts\CCN-STIC-599B19 incremental portatiles categoria alta – DL - Bitlocker” con el nombre de “servicios_windows.log”.
14.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados que se muestran a continuación.  Nota: En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script desde el paso 4.
15.	Elimine la carpeta “C:\Scripts” y reinicie el puesto de trabajo.

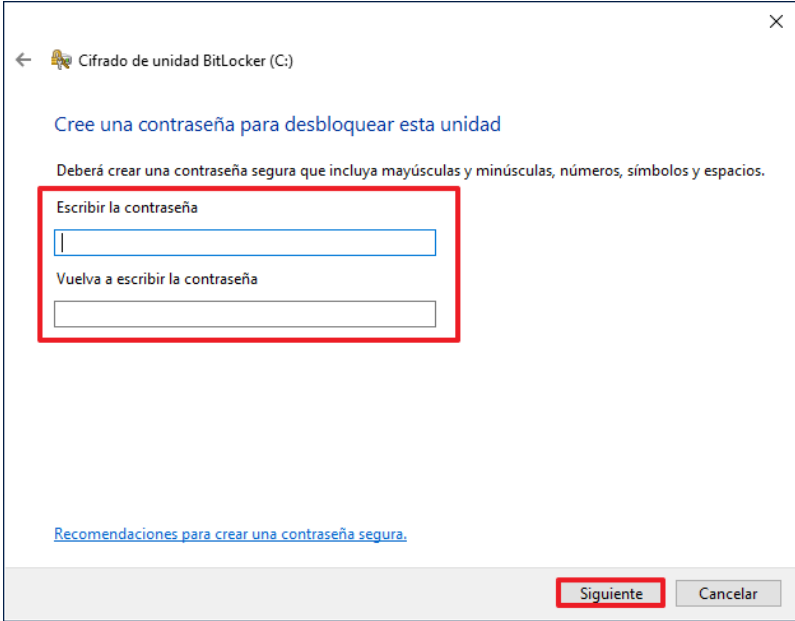
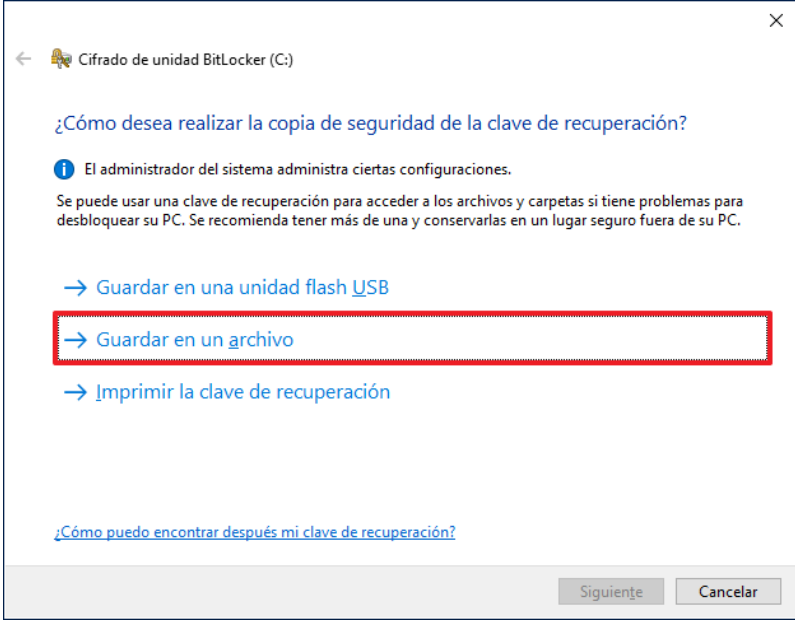
Si se cambia el TPM asociado al cifrado de unidad BitLocker o si alguien intenta iniciar el equipo desde un disco para evitar el sistema operativo, el equipo cambiará el modo de recuperación hasta que se suministre la clave de recuperación. Si se pierde la contraseña o PIN o bien hay un fallo, se puede entrar a través del modo de recuperación introduciendo la contraseña de recuperación.

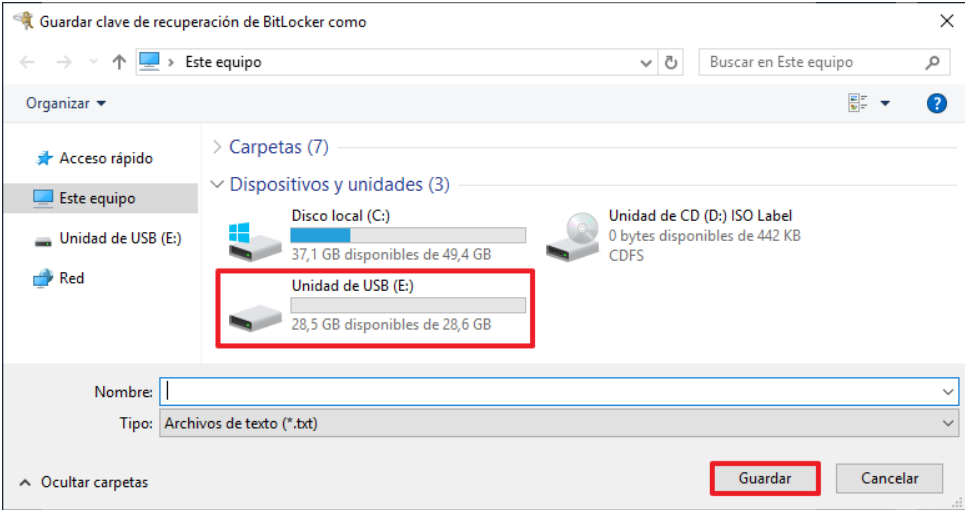
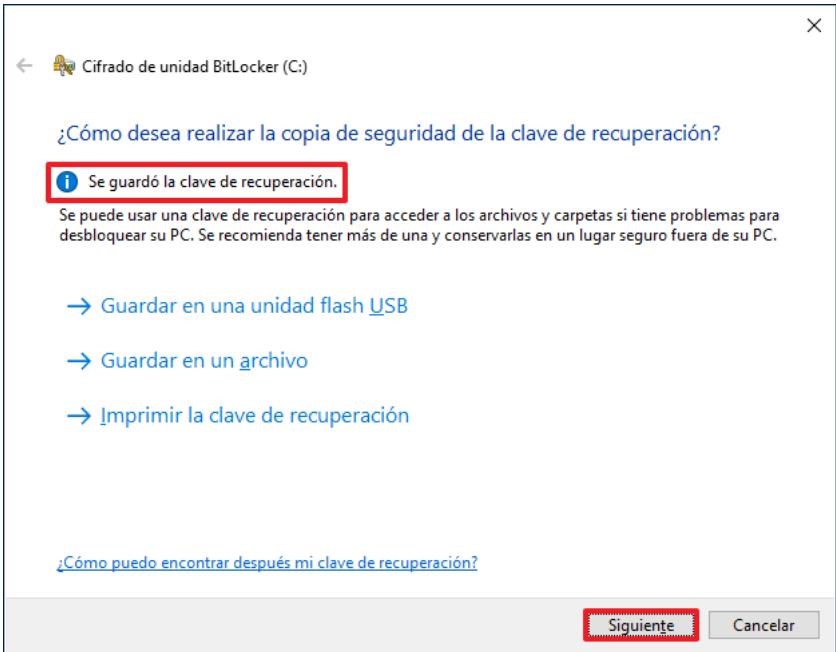
Los siguientes pasos describen el procedimiento para activar el cifrado de unidad BitLocker con contraseña.

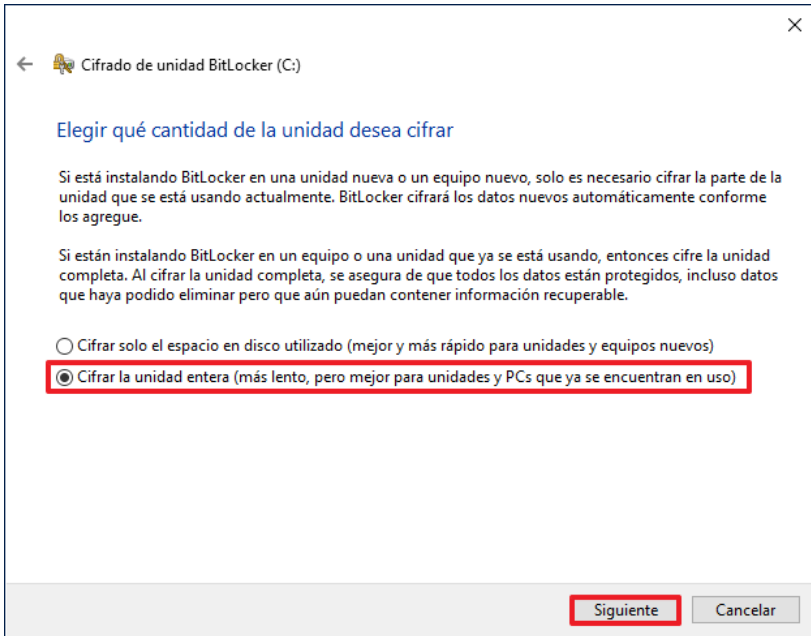
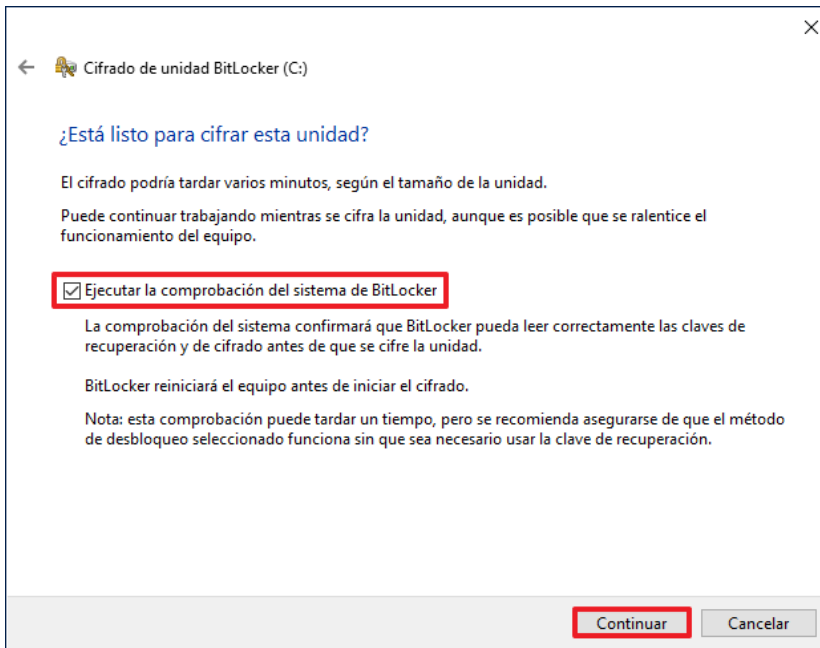
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números. Por tanto, se puede pensar en el PIN más como una "frase de paso" que como un "número".

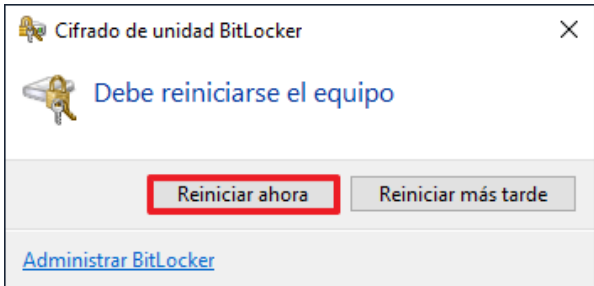
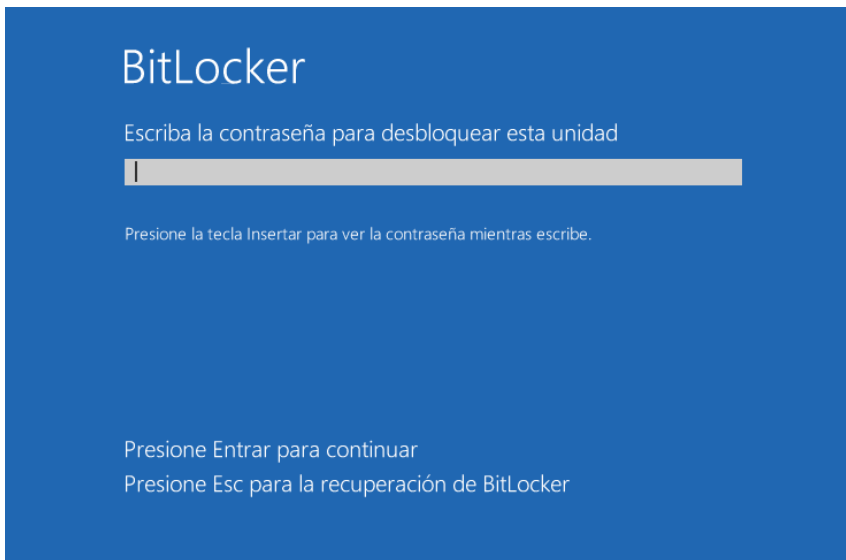
Paso	Descripción
16.	Inicie el "Panel de Control". Para ello pulse la combinación de teclas "Windows + R", escriba "control.exe" en la ventana emergente y pulse el botón "Aceptar". 
17.	Seleccione dentro del "Panel de control" el apartado "Cifrado de unidad BitLocker".  Nota: Tenga en cuenta la visualización del Panel de control. En la parte superior derecha podrá cambiar el modo en que se muestran los iconos.

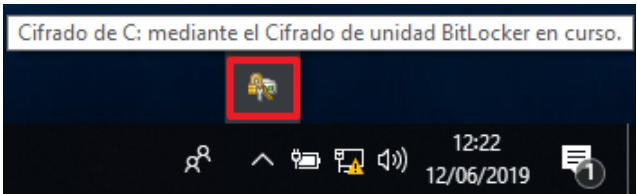
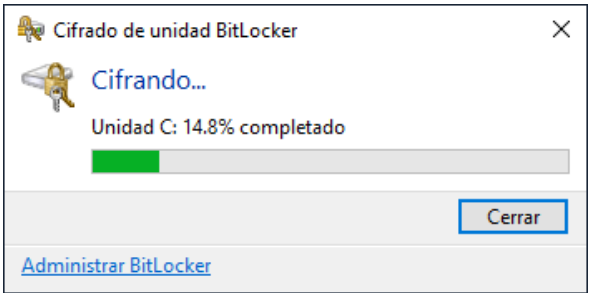
Paso	Descripción
18.	Pulse “Activar BitLocker”.  Nota: La configuración importada durante la aplicación de la guía establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si su equipo dispone de firmware UEFI nativo, deberá habilitar y configurar la directiva “Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo”. Para ello, con el editor de directivas de grupo (gpedit.msc) diríjase a la ruta “Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo” y habilite la directiva mencionada anteriormente. 
19.	El sistema le solicitará elevación de privilegios. Introduzca credenciales de administrador en la ventana de “Control de cuentas de usuario”. Pulse “Si” para continuar.

Paso	Descripción
20.	Introduzca y confirme una contraseña de inicio y pulse “Siguiente”.  Nota: Recuerde que puede utilizar entre 8 y 20 caracteres. A mayor longitud, mayor seguridad.
21.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
22.	Seleccione la ubicación de la unidad USB en la que guardará el archivo que contiene la clave y pulse el botón “Guardar”.  Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD. Debe tener en consideración que esta clave, durante el proceso no puede ser almacenado sobre la misma unidad que se está cifrando ni en otra unidad que este cifrada.
23.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

Paso	Descripción
24.	A continuación, elija la opción “Cifrar la unidad entera” y pulse “Siguiente”. 
25.	Marque la opción "Ejecutar la comprobación del sistema de BitLocker" y pulse el botón "Continuar". 

Paso	Descripción
26.	Reinicie el equipo para continuar con el proceso de cifrado de la unidad.  Nota: Si tras reiniciar el sistema aparece un mensaje como el mostrado a continuación pulse el botón “Cerrar” y repita los pasos del 17 al 26, pero en este último paso pulse sobre la opción “Reiniciar más tarde” y reinicie el equipo manualmente mediante la ruta “Inicio → “Iniciar/Apagar”. 
27.	Al reiniciar, el sistema le pedirá el PIN de cifrado de unidad BitLocker. Introduzca el PIN y pulse “Enter” para continuar. 

Paso	Descripción
28.	Una vez reiniciado el sistema, abra la sesión de nuevo con un usuario del grupo “Administradores”. El cifrado inicial de la unidad del sistema se realizará en segundo plano. Mientras dure este proceso es posible que el tiempo de respuesta del sistema se vea afectado por la intensa actividad del disco. Una vez finalizado el proceso de cifrado inicial, el cifrado y descifrado de los datos del disco será imperceptible por el usuario. Durante el proceso puede aparecer el siguiente mensaje informativo. Continúe con los siguientes pasos, aunque no haya finalizado este proceso de cifrado inicial del disco. 
29.	Si marca con el ratón en él, o en el icono correspondiente del área de notificación, podrá visualizar la siguiente ventana mostrando el progreso de este cifrado inicial. 
30.	Desconecte la memoria USB que contiene la clave de recuperación del cifrado de BitLocker y guárdela en un lugar seguro, como una caja de seguridad. Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD.
31.	Una vez haya reiniciado el sistema, inicie sesión de nuevo con un usuario miembro del grupo “Administradores” y elimine la carpeta “C:\Scripts”. Nota: Todos los volúmenes NTFS del Sistema deberán ser cifrados con la utilidad BitLocker, una vez se haya cifrado totalmente el volumen del Sistema. Si se cambia el TPM asociado al cifrado de unidad BitLocker o si alguien intenta iniciar el equipo desde un disco para evitar el sistema operativo, el equipo cambiará al modo de recuperación hasta que se suministre la clave de recuperación. Si se pierde el PIN, se puede cambiar al modo de recuperación para iniciar el equipo e introducir la clave de recuperación. Para más información sobre el procedimiento de cifrado de unidad BitLocker, puede consultar el siguiente enlace: https://support.microsoft.com/es-es/help/4028713/windows-10-turn-on-device-encryption

ANEXO C.4. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO C.4.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA

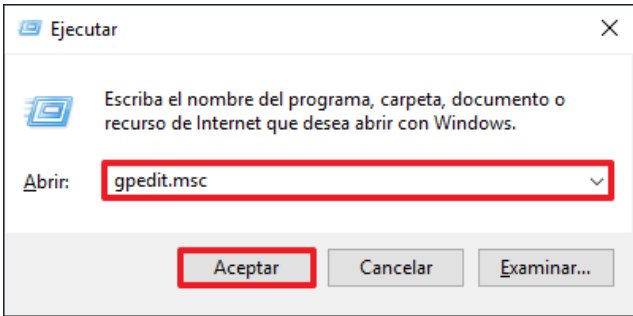
El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los clientes Windows 10 independientes. Este Anexo ha sido diseñado para atender al principio de mínima exposición que faculta a un sistema a reducir los riesgos minimizando los puntos de entrada al mismo.

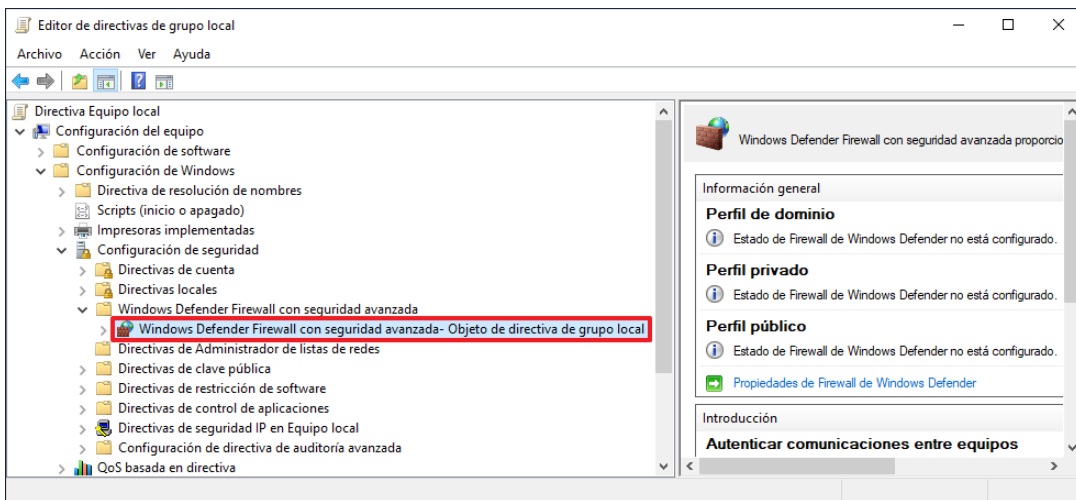
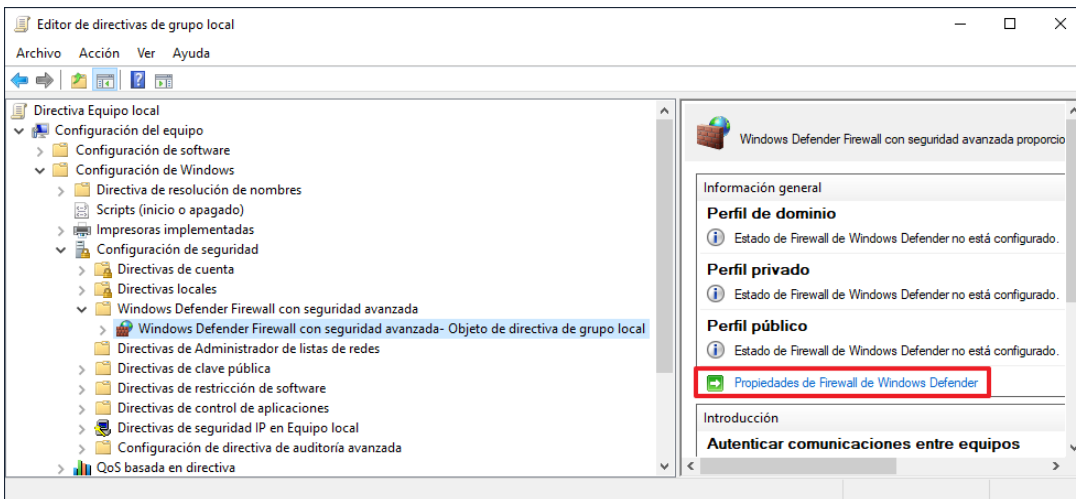
Debe tenerse en consideración que la implementación de un cortafuegos de cliente independiente dependerá, en sí misma, de la funcionalidad del mismo y de los servicios que este ofrece a la infraestructura. No tendrá, evidentemente, la misma funcionalidad y, por lo tanto, la necesidad de puertos abiertos, un servidor que actúe para dar soporte a sitios web que un servidor que mantenga bases de datos. A partir de Windows Vista, Microsoft proporciona un servicio de cortafuegos con seguridad avanzada. Éste permite realizar el control tanto de lo que entra como de lo que sale y para las diferentes categorías de redes en la que puede estar un sistema: públicas, privadas o dominio.

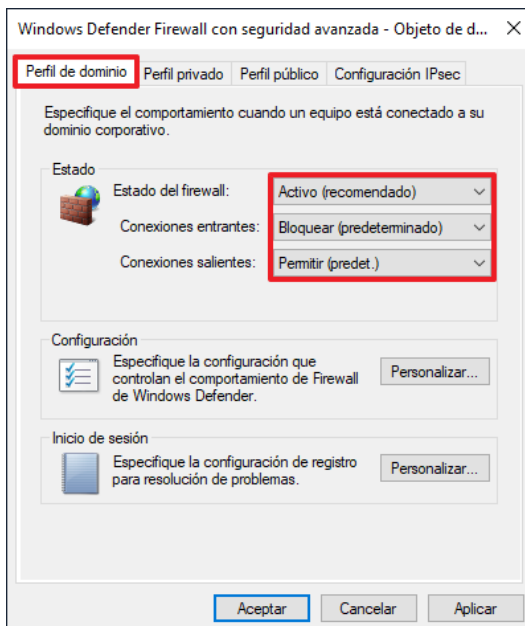
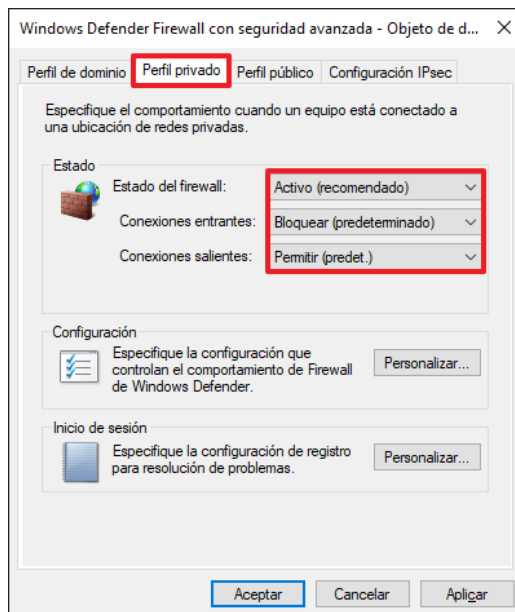
De forma predeterminada, el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local. No obstante, en un cliente independiente puede establecerse la configuración del mismo a través de la política local, de tal forma que, aunque se realizara una modificación del firewall, a través de la consola local o bien mediante una modificación directa por código dañino, a este sería de aplicación la configuración establecida a través de política local.

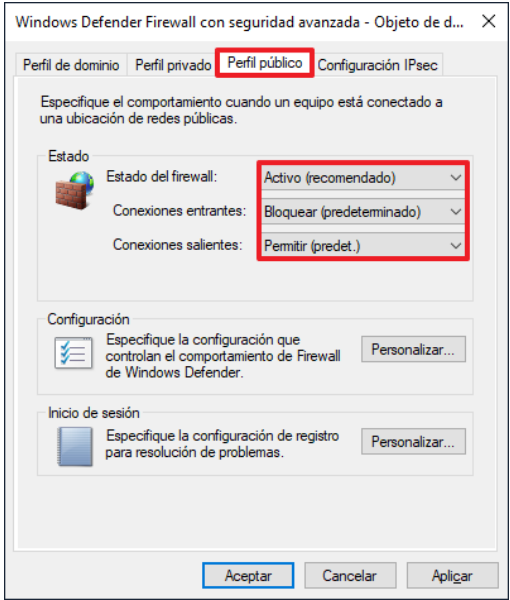
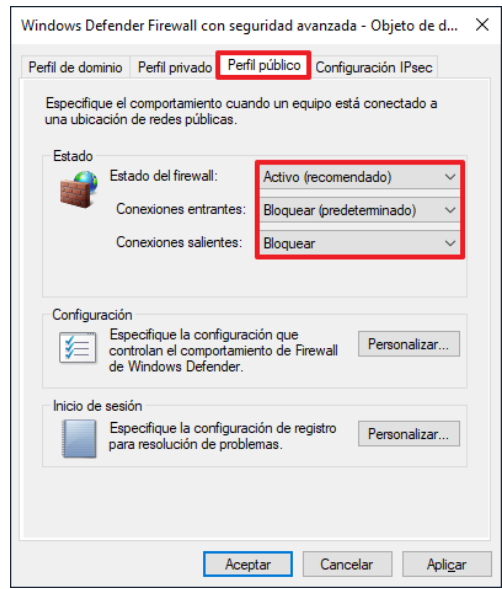
Teniendo en cuenta este hecho, a través de este Anexo se establecerá la configuración del cortafuegos mediante la aplicación de la política local. Como en los Anexos previos, los operadores deberán realizar pruebas en entornos de preproducción antes de realizar una implementación en el entorno de producción.

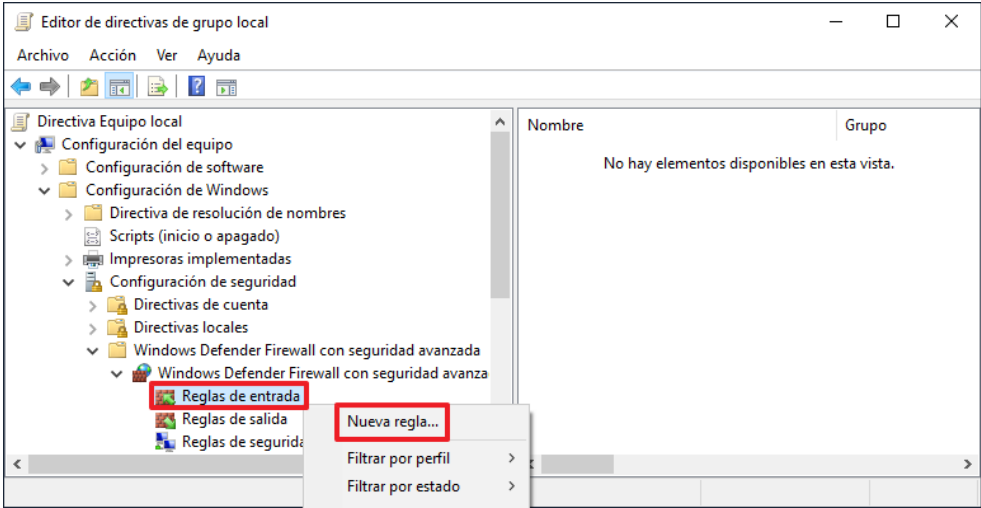
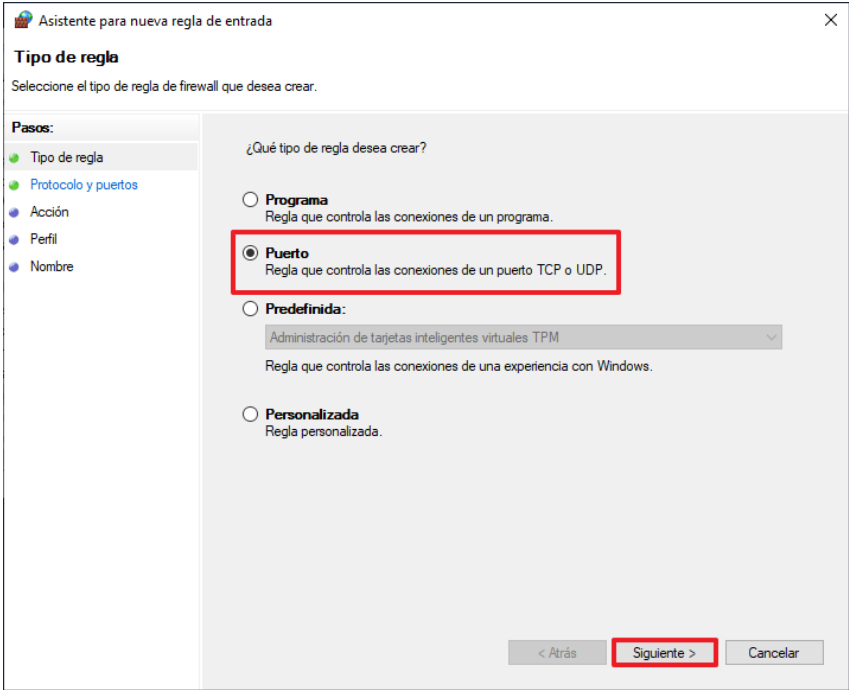
Nota: A modo de ejemplo, en este Anexo se va a mostrar cómo configurar la política local para la aplicación de seguridad de cortafuegos para permitir administración remota a través del puerto 3389.

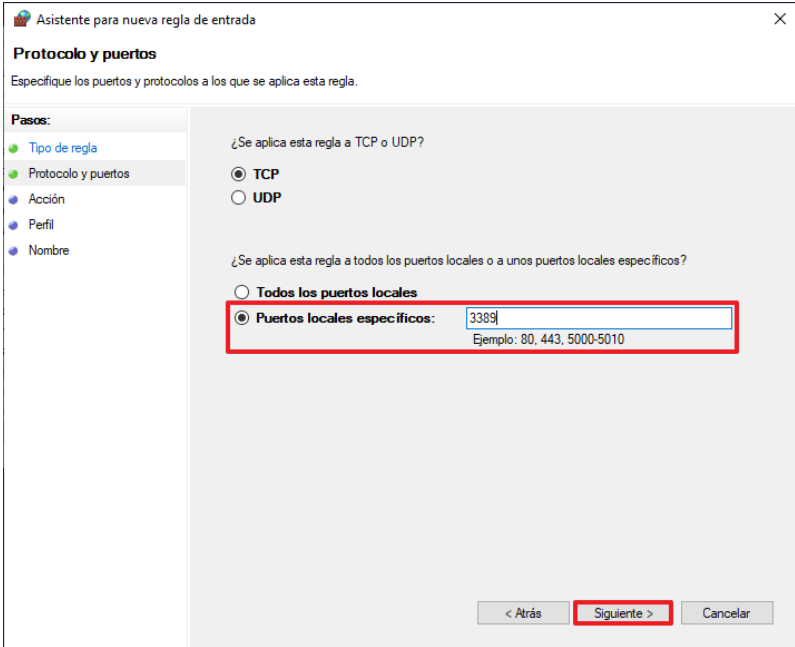
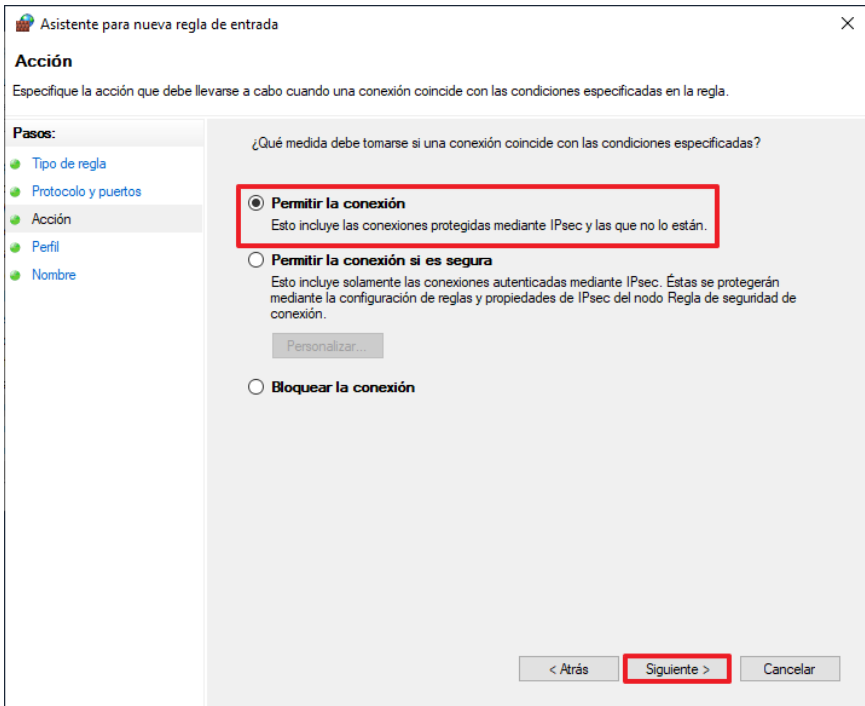
Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse “Aceptar”. 

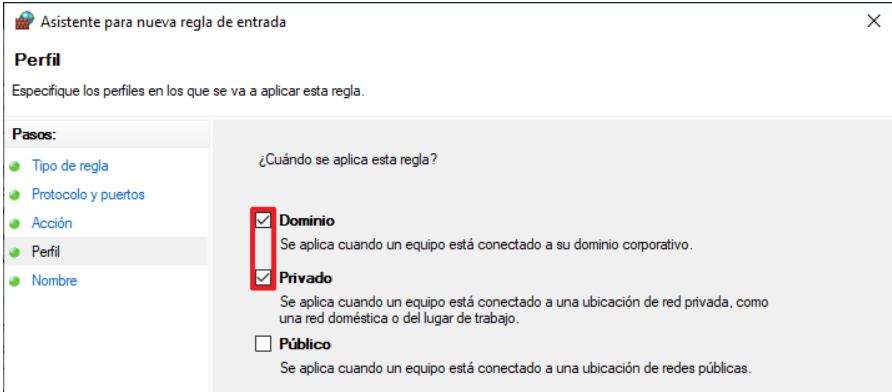
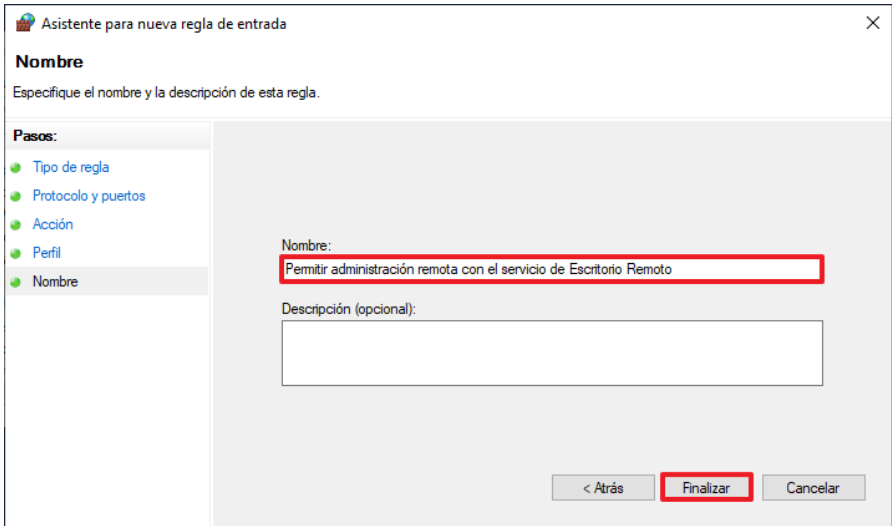
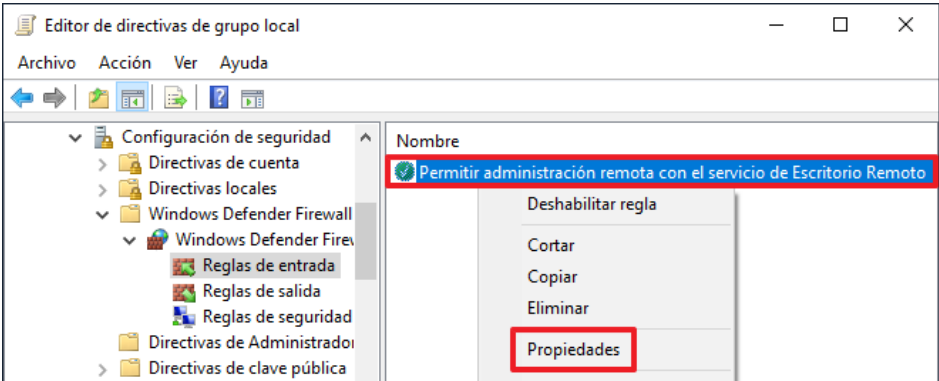
Paso	Descripción
3.	En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
4.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: “Directiva Equipo local → Configuración de equipo → Configuración de Windows → Configuración de seguridad → Windows Defender Firewall con seguridad avanzada → Windows Defender Firewall con seguridad avanzada- Objeto de directiva de grupo local” 
5.	Pulse sobre “Propiedades de Firewall de Windows” que aparecen en la configuración de “Información General”, existentes en el panel derecho. 

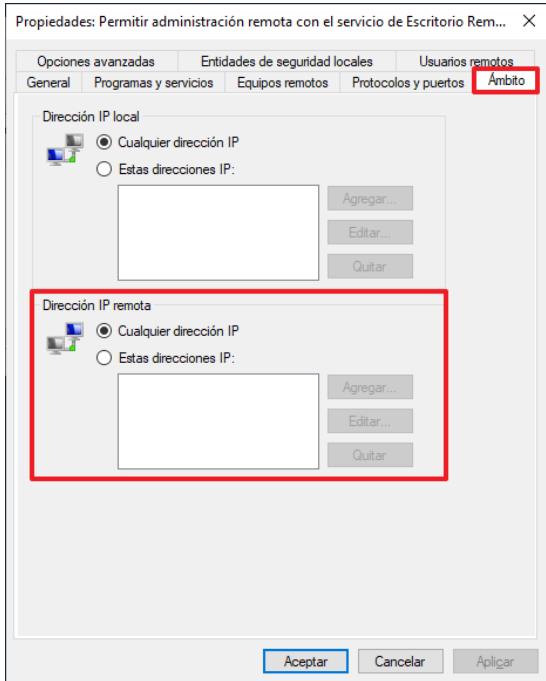
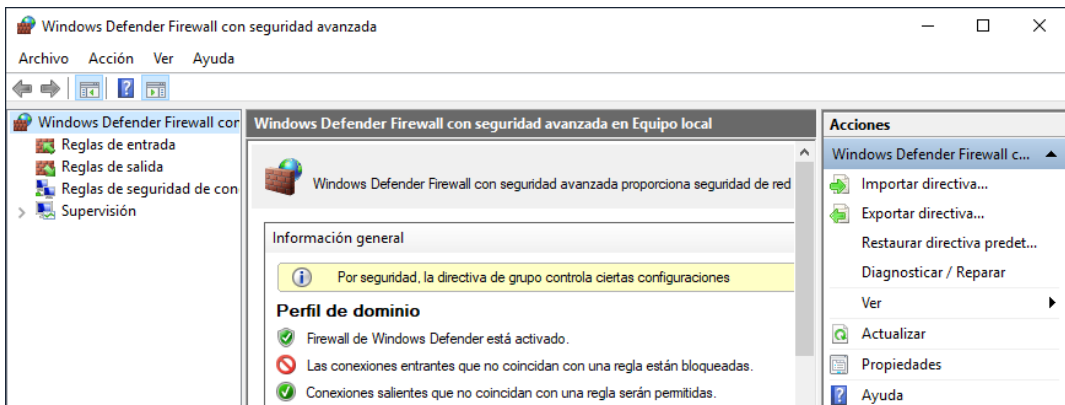
Paso	Descripción
6.	La primera de las pestañas “Perfil de dominio” configúrela como aparece en la siguiente imagen.  Nota: Debe tener en consideración que el presente cliente que está configurando es un cliente de tipo independiente y por lo tanto no formará parte de un dominio. No obstante, es adecuado establecer la configuración del dominio por si el cliente cambiara en algún momento su situación y este pasara a forma parte de un dominio.
7.	A continuación, vaya a la pestaña “Perfil privado” y configúrela tal y como aparece en la siguiente imagen. 

Paso	Descripción
8.	Vaya posteriormente a la pestaña “Perfil público” y establezca la configuración que aparece en la siguiente imagen.  Verifique que la configuración de la conexión de red con el que conecta el sistema a la red interna o a una DMZ, se encuentra en el perfil privado y no en perfil público.
9.	En el caso de que los clientes proporcionaran servicios de categoría alta, sería recomendable que el perfil público quedara configurado como aparece en la siguiente imagen. 
10.	Pulse el botón “Aceptar” para guardar los cambios introducidos en los diferentes perfiles.
11.	Despliegue el Firewall con seguridad avanzada y vaya al apartado “Reglas de entrada”.

Paso	Descripción
12.	Pulse con el botón derecho sobre “Reglas de entrada” y seleccione la opción “Nueva regla...”. 
13.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiente >”. 

Paso	Descripción
14.	En el siguiente apartado seleccione la opción “Puertos locales específicos” e introduzca el puerto “3389”. Pulse el botón “Siguiente >”. 
15.	En el apartado “Acción”, mantenga la configuración y pulse el botón “Siguiente >”. 

Paso	Descripción
16.	En el apartado “Perfil”, deje marcados los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 
17.	Por último, asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”.  Nota: En el ejemplo se utiliza el nombre “Permitir administración remota con el servicio de Escritorio Remoto”.
18.	La nueva regla ya se encuentra creada. Puede editarla pulsando con el botón derecho del ratón sobre ella y seleccionando la opción “Propiedades”. 

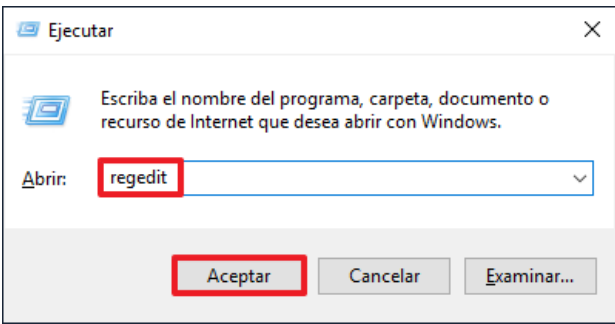
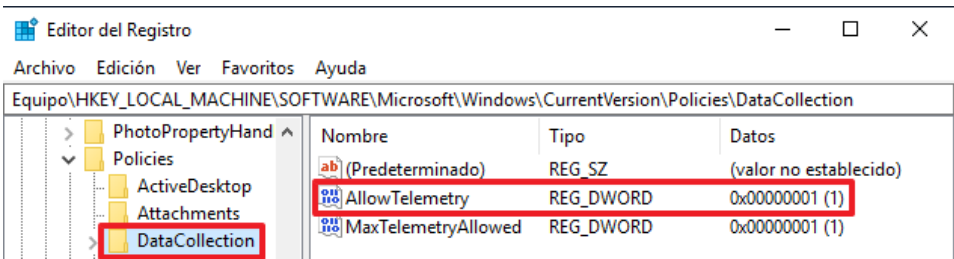
Paso	Descripción
19.	Podrían, por ejemplo, limitarse las IP remotas o rangos de redes que podrían conectarse a los puestos de trabajo a través del puerto 3389. De forma predeterminada se admite cualquier IP. 
20.	Cierre la política de seguridad local. La configuración se habrá aplicado en el puesto de trabajo y lo podrá comprobar ejecutando la configuración del Firewall. Para ello podrá ejecutar desde el menú "Ejecutar" (combinación de teclas "Windows + R") la aplicación "wf.msc".  Nota: La documentación existente en la web de Technet o MSDN de Microsoft le podrá servir de orientación para conocer los puertos que emplean los servicios y aplicaciones de productos Microsoft. La siguiente URL de soporte de Microsoft referencia los puertos habitualmente usados por los servicios de Windows. https://support.microsoft.com/es-es/help/832017/service-overview-and-network-port-requirements-for-windows

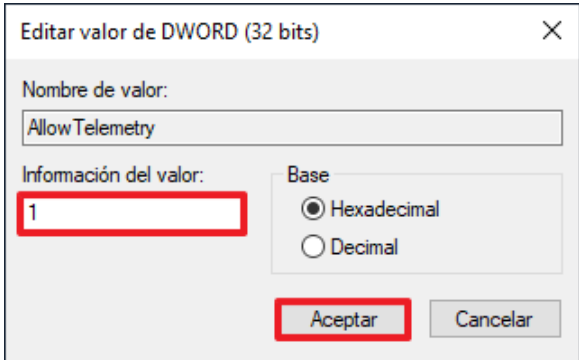
ANEXO C.4.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA WINDOWS 10 INDEPENDIENTE

1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 INDEPENDIENTES

Este anexo ha sido diseñado para ayudar a los operadores a configurar el servicio de telemetría acorde a las necesidades de conectividad de los puestos de trabajo en las administraciones. Dicha funcionalidad de telemetría opera tanto de forma interna generando registros internos de actividad, como remitiendo en determinadas condiciones el envío de información a Microsoft. En este punto se va a explicar cómo realizar cambios en los valores otorgados al componente de telemetría a través de la modificación de una clave de registro. Este valor viene definido tanto por la categoría de seguridad establecida por parte de la organización en sus sistemas, como por los acuerdos que pueda tener esta con Microsoft para el mantenimiento de sus equipos.

Debe tener en consideración que determinados componentes tales como Windows Defender ATP, podrían llegar a requerir al menos un nivel de telemetría de tipo básico (1).

Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie el registro de Windows. Para ello pulse la combinación de teclas “Windows + R”, escriba “regedit” en la ventana emergente y pulse el botón “Aceptar”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
3.	Se abrirá una consola, “Editor de registro” en la cual hay que desplegar el árbol de la izquierda de la pantalla hasta la siguiente clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection 

Paso	Descripción
4.	En panel de la derecha haga doble clic sobre “AllowTelemetry” y modifique el valor más adecuado acorde a las necesidades de su organización. Pulse “Aceptar” para finalizar.  Nota: Recuerde que en el caso de versiones MS Windows 10 Pro, el valor no podrá establecerse la telemetría en valor 0.
5.	Cierre la consola “Editor del Registro”.

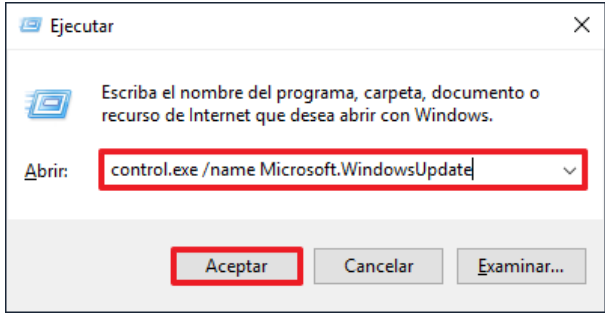
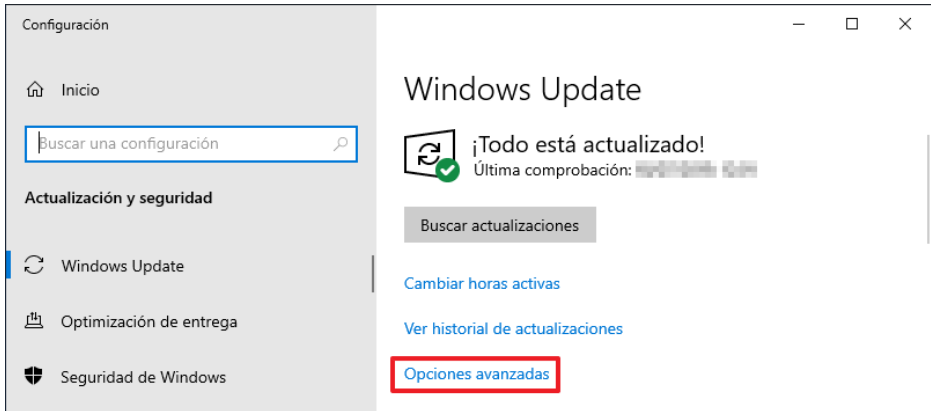
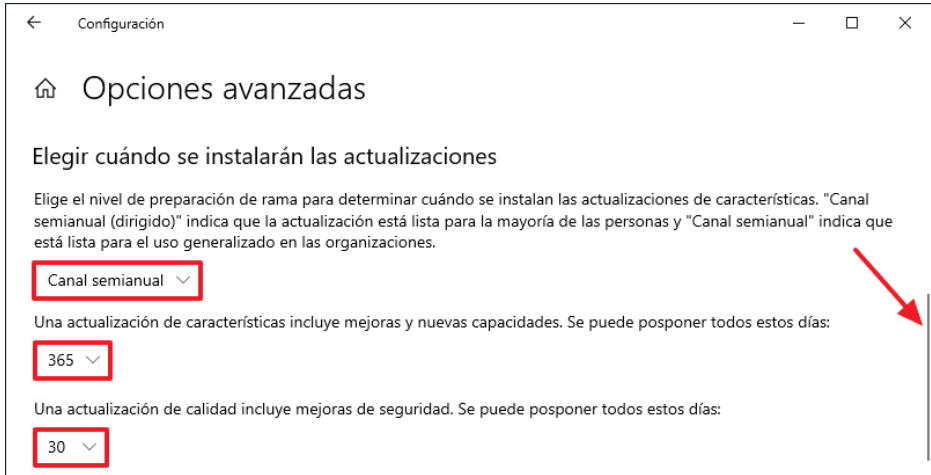
2. CONFIGURACIÓN DE OPCIÓN DE MANTENIMIENTO PARA WINDOWS 10 INDEPENDIENTE

Tal y como ya se había comentado adicionalmente al versionado del Sistema Operativo, MS Windows 10 implementa las opciones de mantenimiento. Se aconseja para las organizaciones que realicen implementación del modo “Canal-Semianual” de tal forma que tengan tiempo para realizar pruebas de la funcionalidad de los cambios en el Sistema Operativo. Para ello deberá configurar los sistemas para implementar la opción “Canal-Semianual”, tal y como se determina el siguiente paso a paso.

Adicionalmente para que pueda realizar pruebas anticipadas que permitan evaluar los cambios que provocan las actualizaciones de Windows 10, sería aconsejable establecer un grupo de equipos en modo “Canal-Semianual (dirigido)” a efectos de que recibían las actualizaciones de funcionalidades dentro del ciclo tempranos. Debe tomar en consideración que la configuración establecida mediante este paso a paso aplica la opción de mantenimiento en modo “Canal-Semianual”. Establecer determinados sistemas en modo “Canal-Semianual (dirigido)” le permite anticipar las consecuencias que tendrán las nuevas actualizaciones con respecto a los equipos de su organización.

Recuerde realizar las pruebas de funcionalidad en dichos equipos antes de aprobar las actualizaciones al resto de equipos de la organización.

Si no implementa el siguiente paso a paso los equipos de su organización estarán configurados de forma predeterminada con la opción de mantenimiento “Canal-Semianual (dirigido)”.

Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie Windows Update. Para ello pulse la combinación de teclas “Windows + R”, escriba “control.exe /name Microsoft.WindowsUpdate” en la ventana emergente y pulse el botón “Aceptar”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
3.	En la consola de “Windows Update” emergente seleccione “Opciones avanzadas”. 
4.	En la nueva ventana marque las opciones como en la siguiente imagen. Haga uso de la barra lateral para acceder a las mismas. 

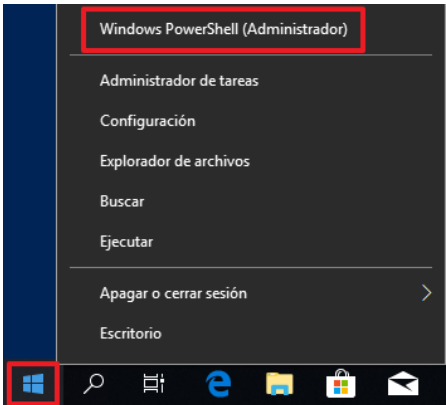
Paso	Descripción
5.	Cierre todas las ventanas de configuración de Windows Update y cierre la consola de configuración.
6.	Con estos pasos ya estaría configurado Windows 10 Independiente para la opción "Canal-Semianual" de actualización.
	Nota: Todas las informaciones vertidas en este documento están sujetas a las posibles modificaciones derivadas de las actualizaciones del fabricante.

3. DESINSTALACIÓN DE APPS (UWP) EN WINDOWS 10

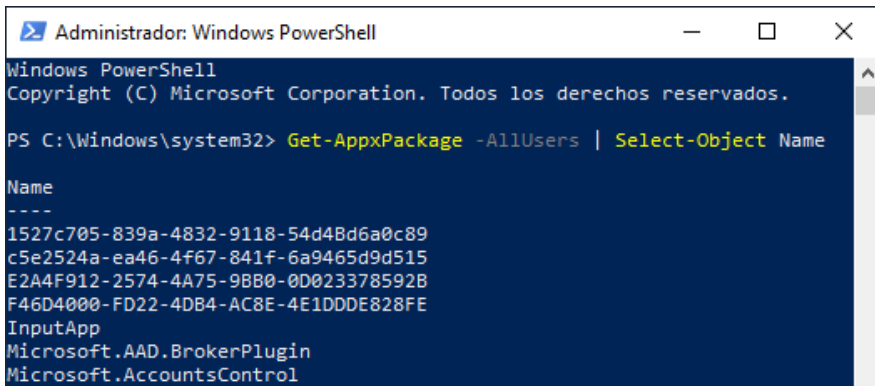
En este punto se van a tratar los procesos que pueden ser llevados a cabo para desinstalar las Apps (Plataforma Universal de Windows - UWP) también conocidas como Appx, que ya vengan precargadas en Windows 10. Debe tomar en consideración que no deberá desinstalar todas las aplicaciones, ya que determinados componentes esenciales tales como el menú inicio funcionan como una App. Existen algunas de ellas que no se pueden desinstalar mediante este método como es el caso de Edge.

Existen dos tipos de aplicaciones. Aquellas nativas al sistema que se instalan junto con Windows 10 y aquellas que están preparadas para su ejecución (AppxProvisioned). El siguiente proceso describe la desinstalación de ambos tipos de Appx.

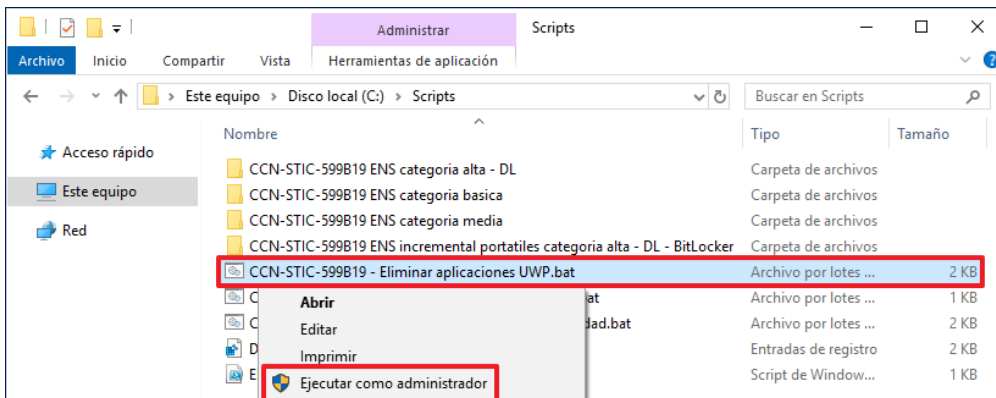
3.1. IDENTIFICACIÓN DE APPX INSTALADAS

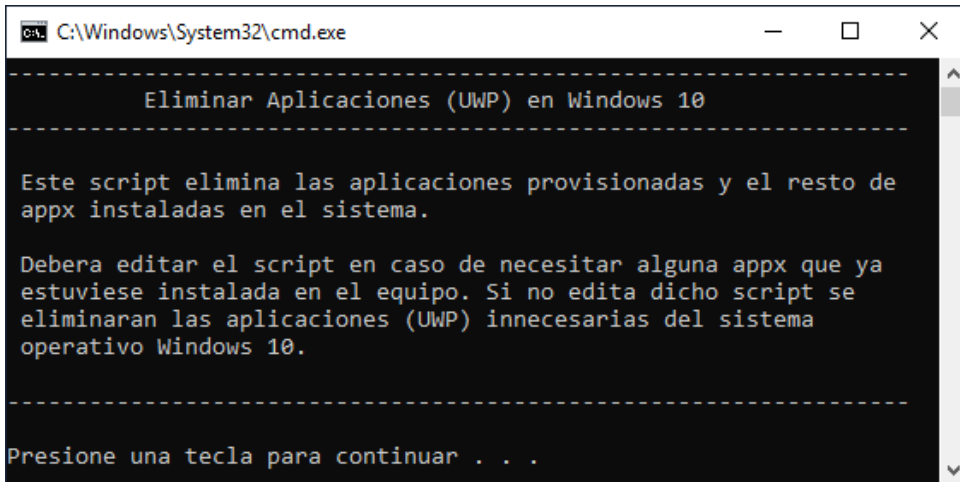
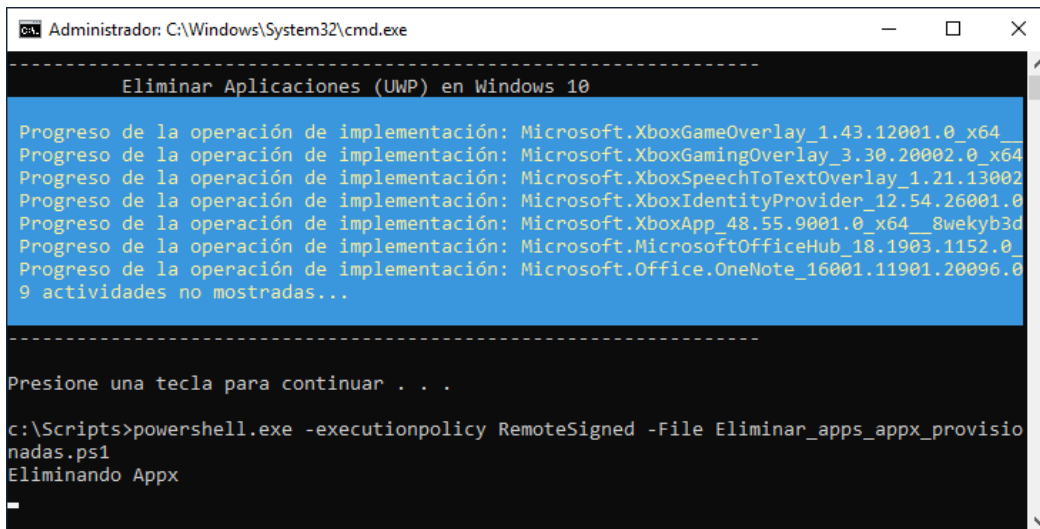
Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Ejecute una consola de "PowerShell" con permisos de administrador. Para ello pulse con el botón derecho sobre "Inicio" y seleccione "Windows PowerShell (Administrador)".
	
3.	Eleve privilegios para poder acceder a la consola.
	Nota: Dependiendo de la categoría de seguridad aplicada sobre el sistema deberá elevar privilegios simplemente o bien introducir las credenciales de un usuario con permisos de administrador del dominio.



Paso	Descripción
4.	Ejecute la siguiente sintaxis para listar las aplicaciones instaladas y pulse “Enter”: Get-AppxPackage –Allusers Select-Object Name 
5.	Con esto tendrá un listado de las Appx instaladas en su sistema.

3.2. ELIMINACIÓN DE APPX PROVISIONADAS E INSTALADAS

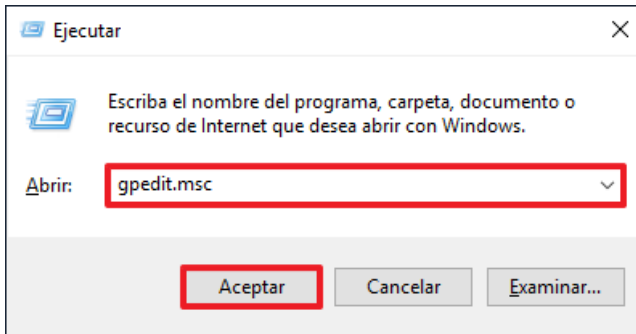
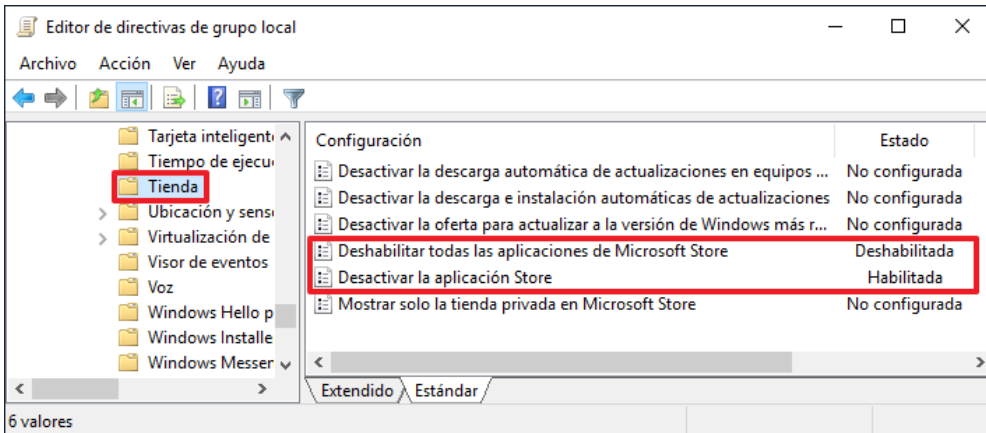
Paso	Descripción
6.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
7.	Cree el directorio “Scripts” en “C:\”
8.	Copie los ficheros y scripts que acompañan a esta guía en el directorio “C:\Scripts” y asegúrese que al menos los siguientes ficheros se encuentran en el directorio: - CCN-STIC-599B19 - Eliminar aplicaciones UWP.bat - Eliminar_apps_appx_provisionadas.ps1
9.	Acceda al directorio “C:\Script”. Pulse con el botón derecho el fichero “CCN-STIC-599B19 - Eliminar aplicaciones UWP.bat” y seleccione la opción “Ejecutar como administrador” del menú contextual que aparecerá. 
10.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Nota: Dependiendo de la categoría de seguridad aplicada sobre el sistema deberá elevar privilegios simplemente o bien introducir las credenciales de un usuario con permisos de administrador del dominio.

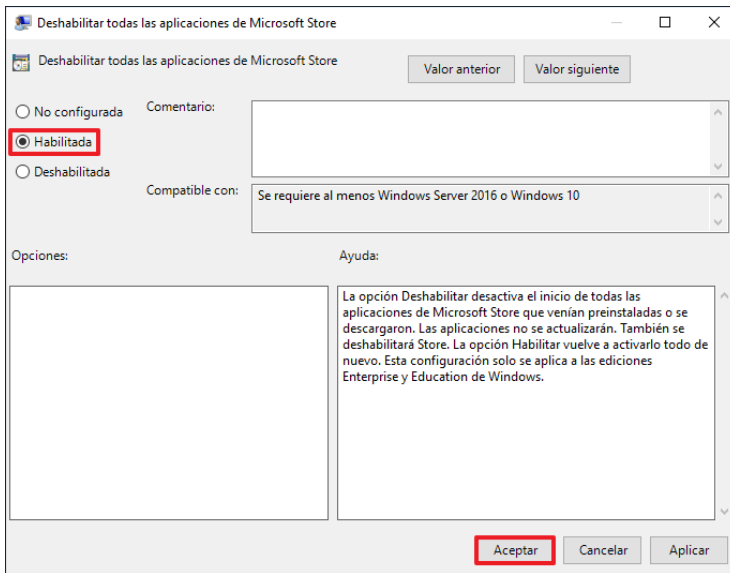
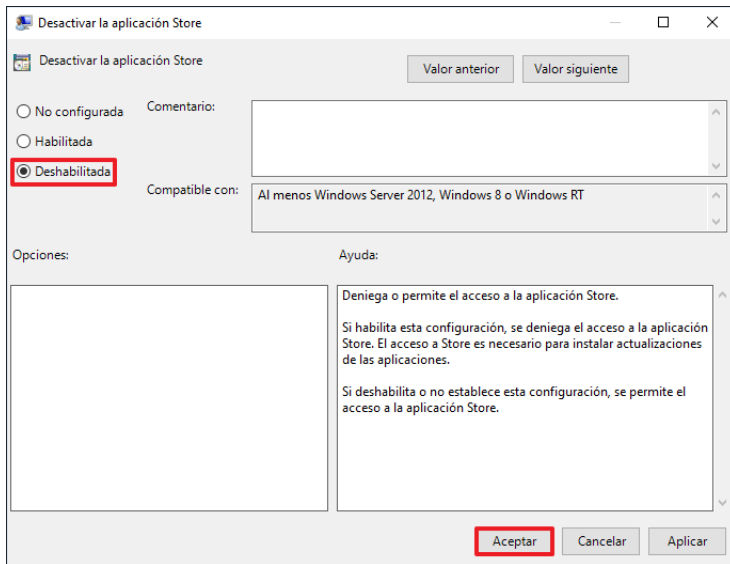
Paso	Descripción
11.	La ejecución del script comenzará. Pulse una tecla para continuar con el script.  Nota: Tenga en consideración que si en su organización se requiere alguna de estas aplicaciones deberá editar el script para eliminar del listado de aplicaciones incluido en el propio script, y así mantener dichas aplicaciones instaladas en el sistema operativo. Con este script se desinstalan todas las aplicaciones UWP de Windows incluidas en el listado del script.
12.	Durante la ejecución del script se mostrarán diferentes mensajes de información y error. Puede ignorar las advertencias de error ya que son de aplicaciones que no pueden ser desinstaladas debido a la necesidad de ellas por parte del sistema. 
13.	Pulse una tecla cuando finalice el script.
14.	A partir de este momento no se dispone de aplicaciones UWP innecesarias. Elimine el directorio "C:\Script" y todo su contenido.

4. ACTIVACIÓN DE TIENDA DE WINDOWS PARA CLIENTES WINDOWS 10 INDEPENDIENTES

En este punto se va a tratar la posibilidad de activación del servicio de Tienda de Microsoft por necesidades propias de la entidad.

La activación del servicio de Tienda y de instalación de aplicaciones propias de la Tienda se habilita a través de la modificación de dos parámetros previamente configurados. De esta manera se cumple con el principio de mínima exposición. Estos parámetros a modificar se encuentran en el “Editor de directivas de grupo local”.

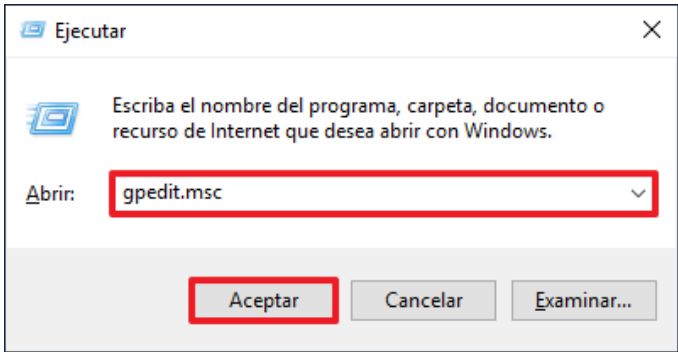
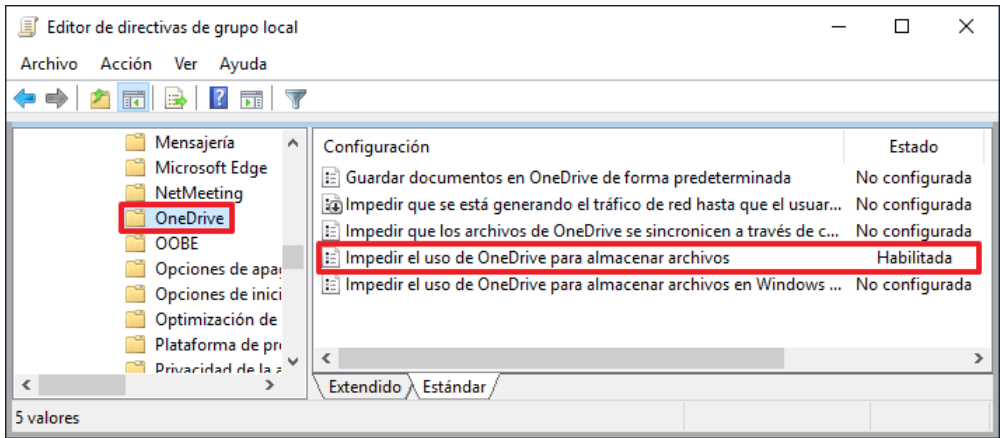
Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse el botón “Aceptar”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
3.	Despliegue la política de grupo local y acceda a la siguiente ruta: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Tienda” 

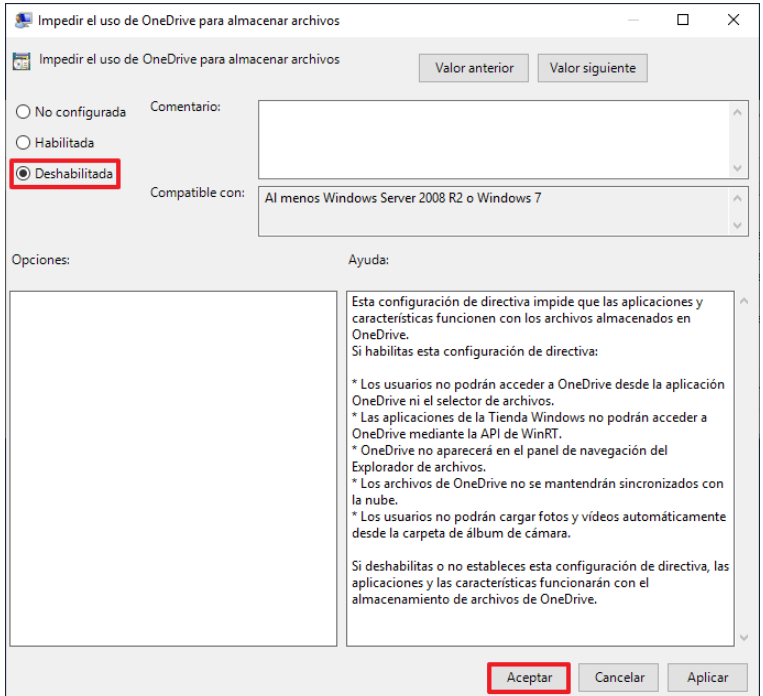
Paso	Descripción
4.	En el cuadro de la derecha debe realizar la modificación de dos directivas, la primera a modificar es “Deshabilita todas las aplicaciones de Microsoft Store”. Haga doble clic sobre ella y establezca su configuración en “Habilitada”. Pulse “Aceptar” para guardar los cambios.  Nota: Debido a la aplicación de la seguridad a partir de la categoría media del ENS ésta se establece como “Deshabilitada”.
5.	El siguiente valor a modificar es “Desactivar la aplicación Store”. Haga doble clic sobre ella y establezca su configuración en “Deshabilitada”. Pulse “Aceptar” para guardar los cambios.  Nota: Debido a la aplicación de la seguridad a partir de la categoría media del ENS ésta se establece como “Habilitada”.
6.	Con estos pasos ya estaría la aplicación “Microsoft Store” habilitada en el sistema.

5. ACTIVACIÓN DE MICROSOFT ONEDRIVE PARA CLIENTES WINDOWS 10 INDEPENDIENTES

En este anexo se va a tratar la posibilidad de activación del servicio de Microsoft OneDrive por necesidades propias de la entidad debido a que en la categoría alta del ENS se deshabilita dicho servicio.

La activación del servicio de OneDrive se habilita a través de la modificación de un parámetro previamente configurado. De esta manera se cumple con el principio de mínima exposición. Este parámetro a modificar se encuentra en el “Editor de directivas de grupo local”.

Paso	Descripción
1.	Inicie sesión con una cuenta de usuario que sea administrador local del equipo.
2.	Inicie el editor de políticas locales. Para ello pulse la combinación de teclas “Windows + R”, escriba “gpedit.msc” en la ventana emergente y pulse “Aceptar”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
3.	Despliegue la política de grupo local y acceda a la siguiente ruta. “Configuración del equipo → Plantillas administrativas → Componentes de Windows → OneDrive” 

Paso	Descripción
4.	En el cuadro de la derecha haga doble clic sobre la directiva “Impedir el uso de OneDrive para almacenar archivos” y establezca su configuración en “Deshabilitada”. Pulse “Aceptar” para guardar los cambios.  Nota: Debido a la aplicación de la seguridad a partir de la categoría media del ENS ésta se establece como “Habilitada”.
5.	Una vez finalizada la modificación de la directiva quedaría el servicio de OneDrive reestablecido en su sistema.

ANEXO C.4.3. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN

Tras la aplicación de seguridad en el sistema, existirían todavía determinados vectores de ataque, que deberán ser corregidos con el fin de evitar la evasión de los sistemas de autorización del sistema operativo. La exploración de dichos vectores de ataque podría ocasionar una posible exfiltración de la información gestionada y almacenada en el sistema, así como una potencial manipulación del comportamiento del mismo.

Para evitar esta situación, dentro del marco de seguridad establecido, se disponen de cuatro soluciones que se relaciona a continuación, y que pueden aplicarse de forma independiente o en conjunción las unas con las otras. Con posterioridad se detallará los mecanismos de su aplicación dentro del presente anexo, con objeto de mejorar la seguridad global del sistema.

Nota: Antes de aplicar las soluciones que se indican a continuación, verifique la compatibilidad de las mismas con su organización, y tenga en consideración los riesgos asumidos por la aplicación de dichas medidas.

Se recomienda verificar la adecuación e idoneidad de la solución para la organización en un entorno de pruebas o “preproducción” de forma previa a su aplicación en un entorno real o de “producción”.

Las medidas a aplicar podrán ser:

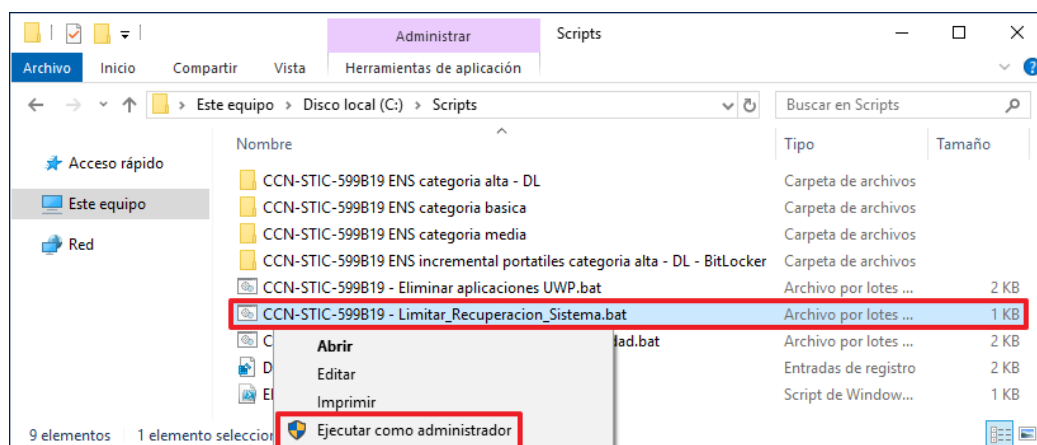
- Cifrado del sistema de archivos. Utilizar BitLocker u otro sistema de cifrado autorizado para evitar el acceso a la información almacenada y, por tanto, evitar su modificación ya que requiere de la introducción de un PIN o contraseña en el arranque del equipo, o en el momento de acceder a los datos. De las opciones presentadas, ésta es la más recomendada. El presente anexo no incorpora cómo aplicar el mecanismo de protección de BitLocker ya que ha sido convenientemente tratado en la presente guía.
- Deshabilitar la funcionalidad de restauración y/o recuperación del sistema a través de la utilidad “BCEDIT”.
- Deshabilitar las opciones de accesibilidad a través de claves de registro, evitando así que estas estén disponibles tanto si el usuario ha iniciado sesión como si no.
- Restaurar la integridad de los ficheros “C:\Windows\System32\sethc.exe” y “C:\Windows\System32\utilman.exe” al inicio del sistema.

Atendiendo al RD 1494/2007, será necesario permitir el uso de esta funcionalidad de accesibilidad a aquellas personas que, por su discapacidad, requieran hacer uso de esta tecnología de accesibilidad. Se deberá tener en consideración los riesgos de seguridad que se asumen si se activan estas opciones, y se deberán implantar las medidas adecuadas para minimizar el grado de exposición del sistema en estos términos.

1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

A continuación, se indican los pasos a realizar para deshabilitar la funcionalidad de recuperación del sistema.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
3.	Localice el archivo “CCN-STIC-599B19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.



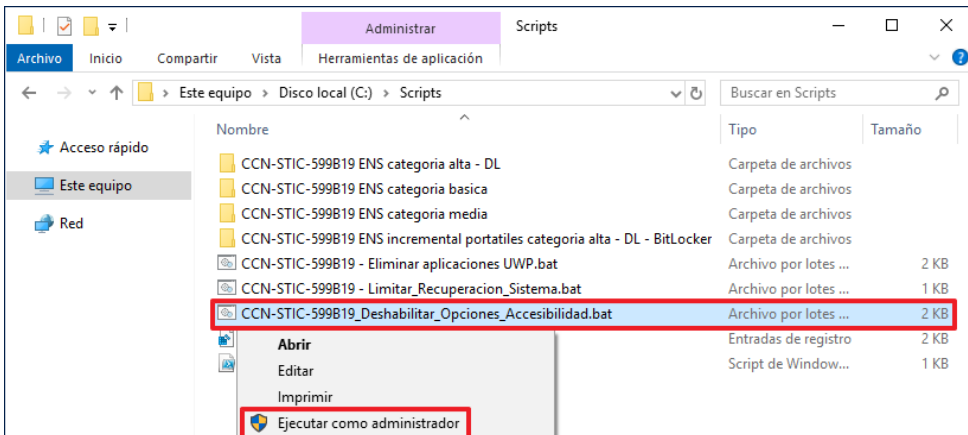
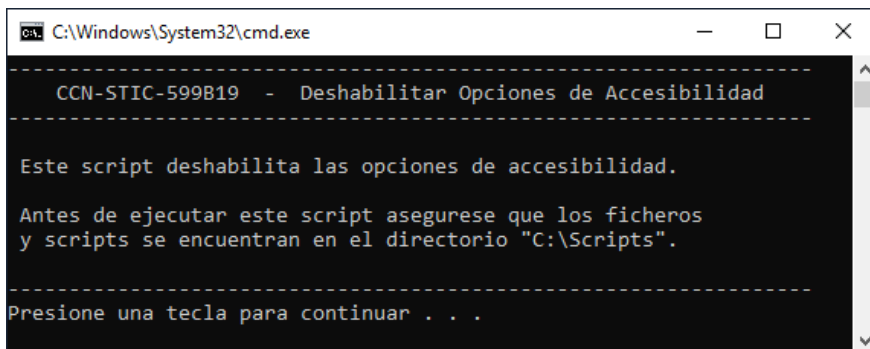
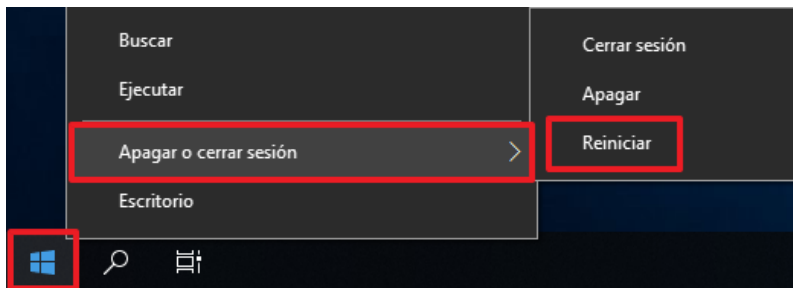


Paso	Descripción
4.	En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script limitará el uso de las opciones de recuperación del sistema. <pre> C:\Windows\System32\cmd.exe ----- CCN-STIC-599B19 - Deshabilitar Recuperacion Del Sistema ----- Este script deshabilita la recuperacion del sistema para evitar fugas de informacion y evasiones de autentificacion, tenga en cuenta que esto provocara que no se pueda recuperar el sistema en caso de error. ----- Presione una tecla para continuar . . . </pre>
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana. <pre> C:\Windows\System32\cmd.exe ----- CCN-STIC-599B19 - Deshabilitar Recuperacion Del Sistema ----- Este script deshabilita la recuperacion del sistema para evitar fugas de informacion y evasiones de autentificacion, tenga en cuenta que esto provocara que no se pueda recuperar el sistema en caso de error. ----- Presione una tecla para continuar . . . La operaci3n se complet3 correctamente. ----- Deshabilitar Recuperacion Del Sistema : Ejecucion Finalizada ----- Presione una tecla para continuar . . . </pre>
7.	Elimine el directorio "C:\Scripts".

2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD

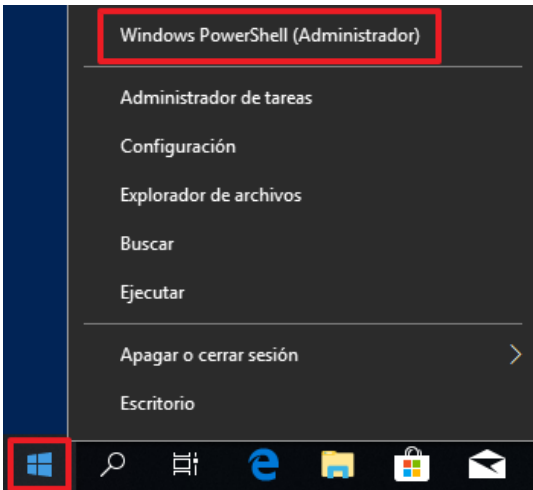
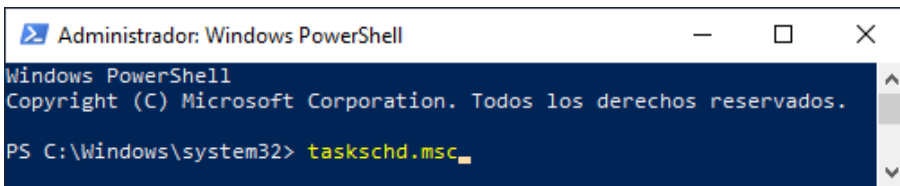
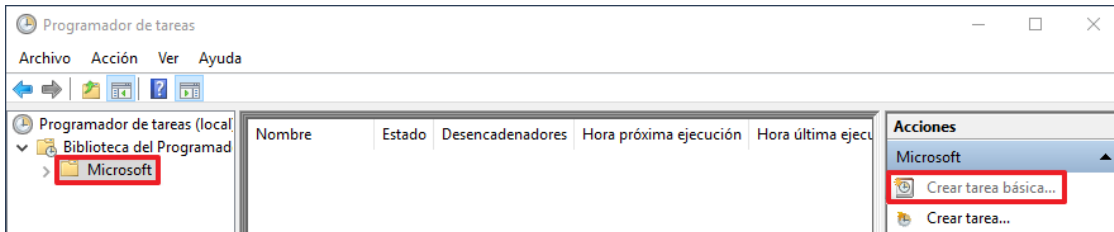
A continuación, se indican los pasos a realizar para deshabilitar las opciones de accesibilidad.

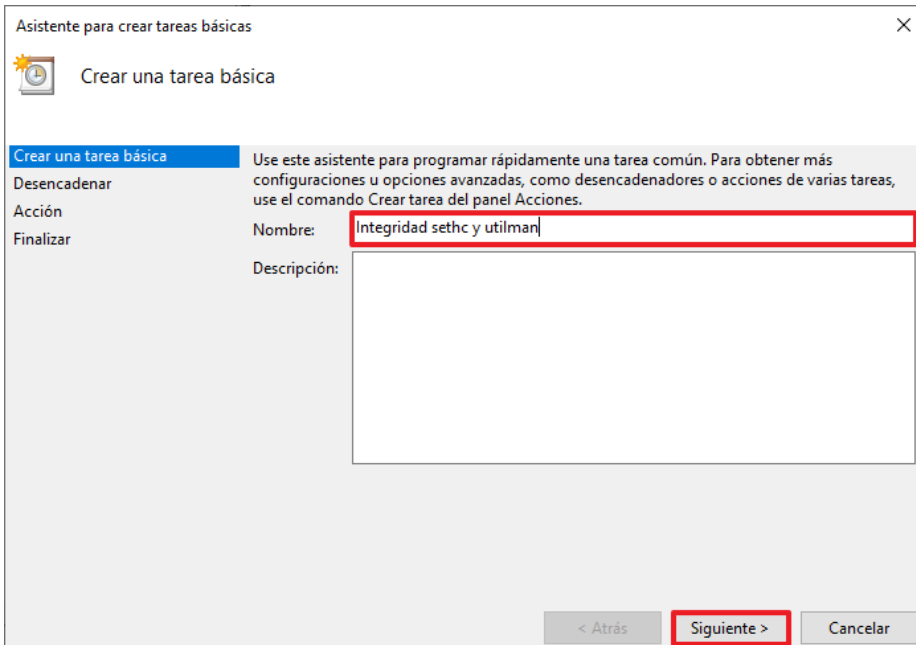
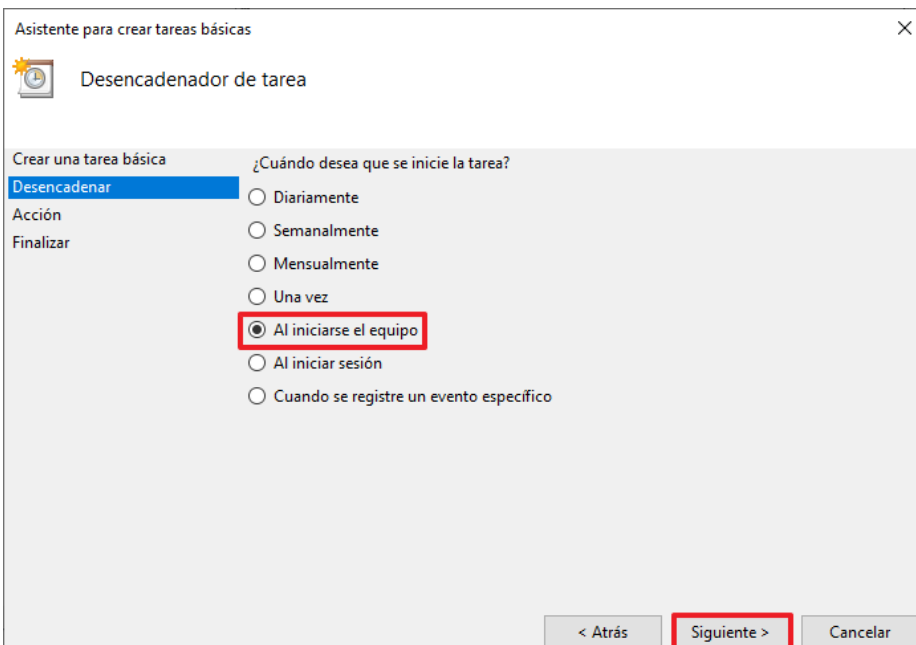
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio "C:\Scripts" y sitúese en dicho directorio.

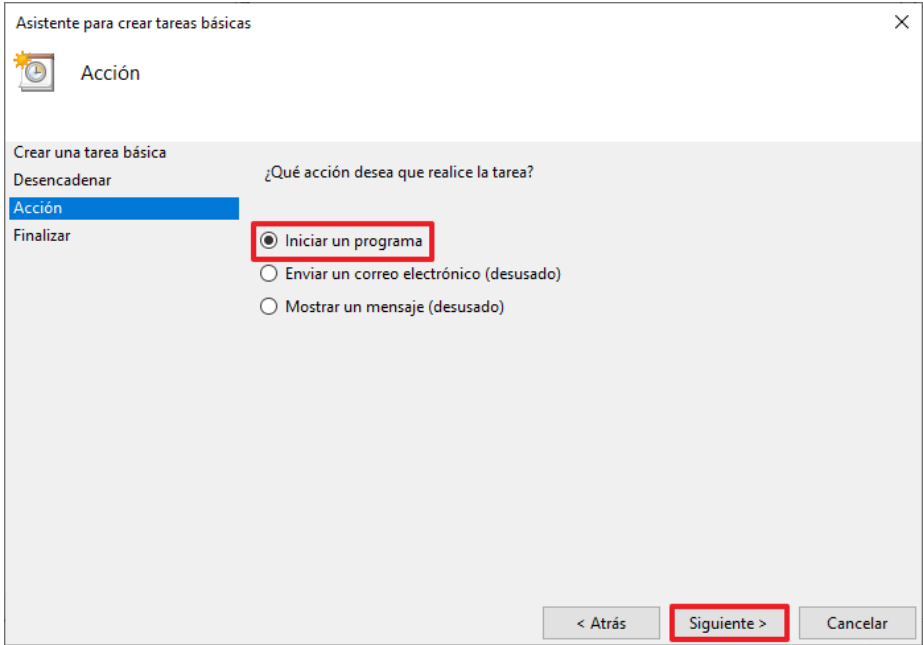
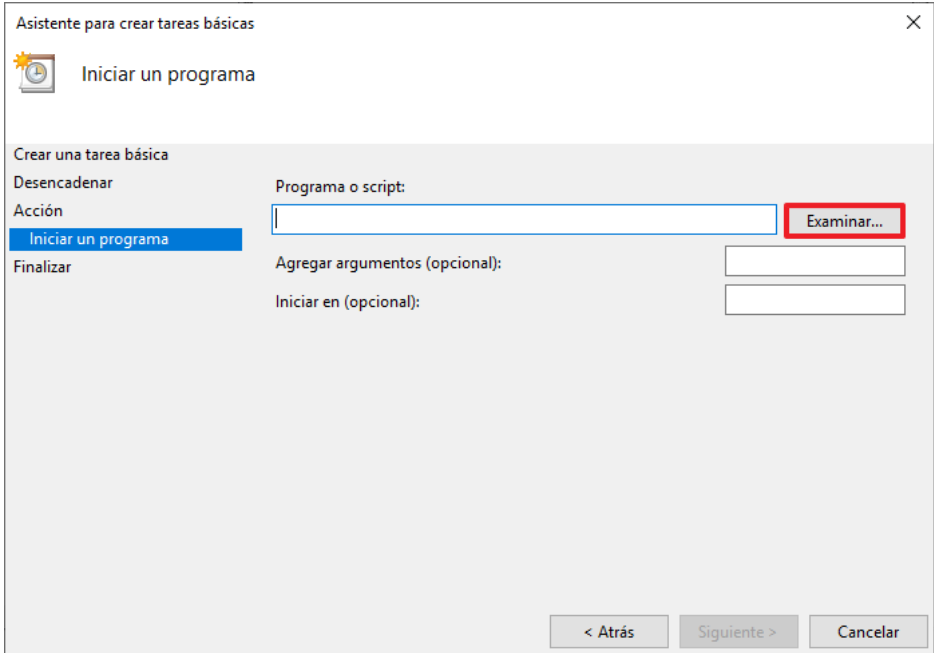
Paso	Descripción
3.	Localice el archivo “CCN-STIC-599B19 – Deshabilitar_Opciones_Accesibilidad.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
4.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 
5.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana.
6.	Por último, deberá reiniciar el sistema para que los cambios sean aplicados. Para ello haga clic derecho en el botón sobre “Inicio → Apagar o cerrar sesión → Reiniciar”. 
7.	Elimine el directorio “C:\Scripts” .

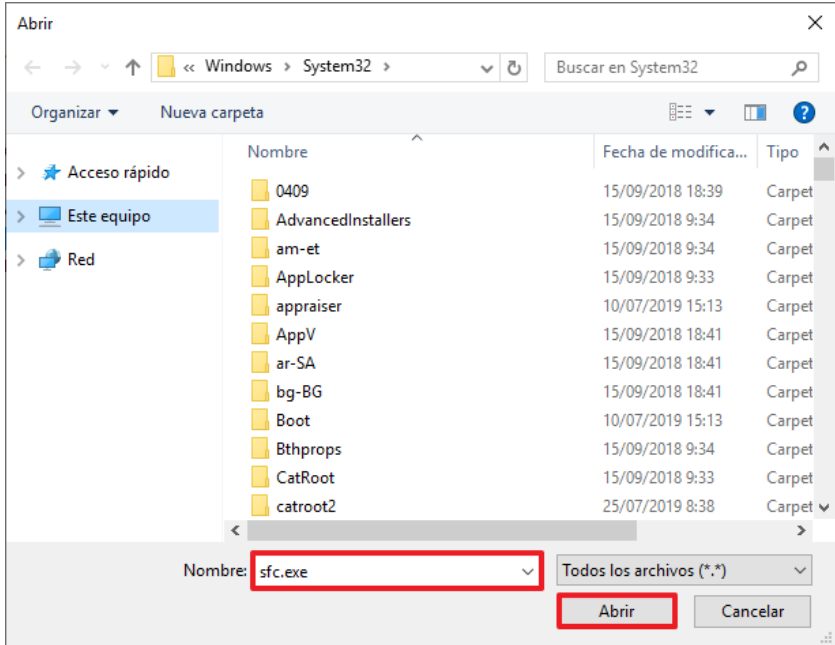
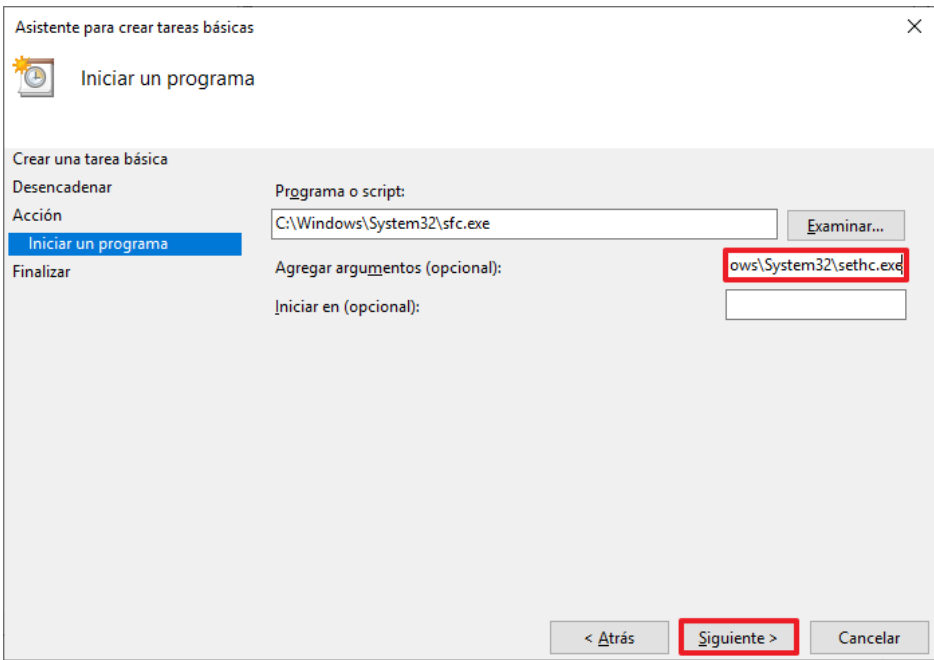
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

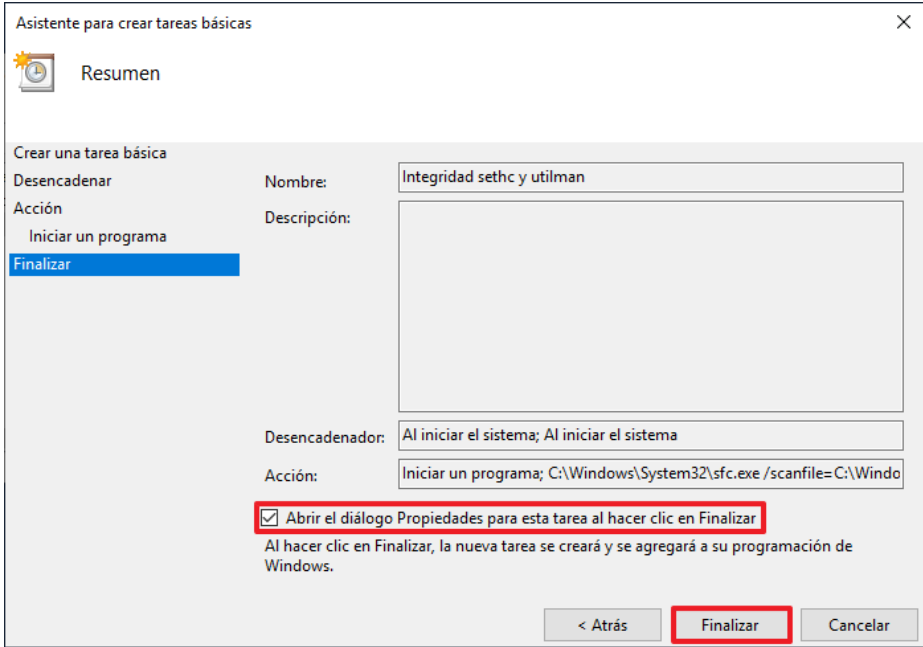
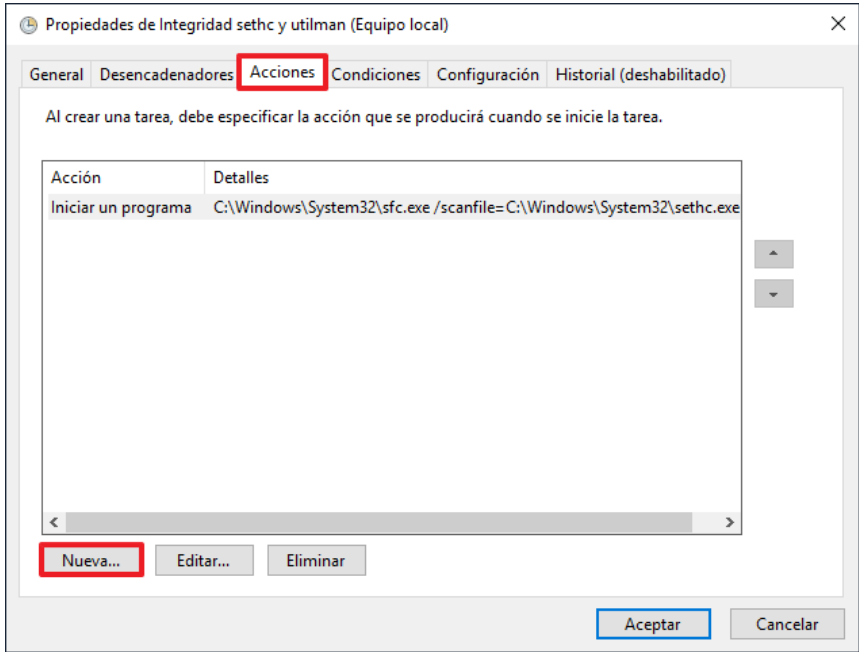
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

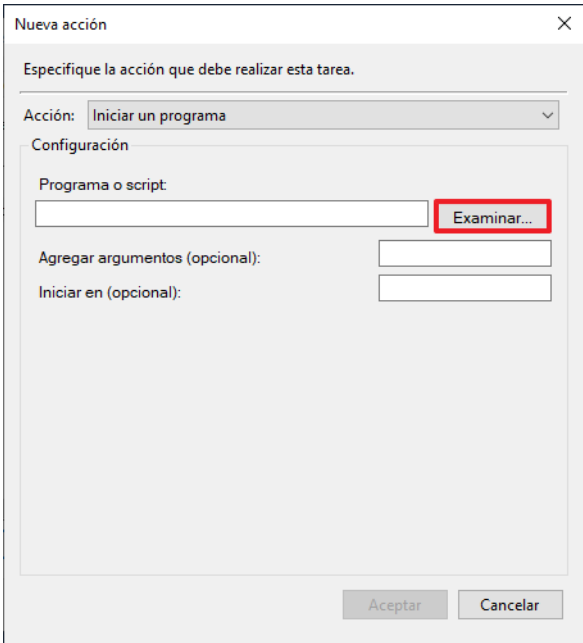
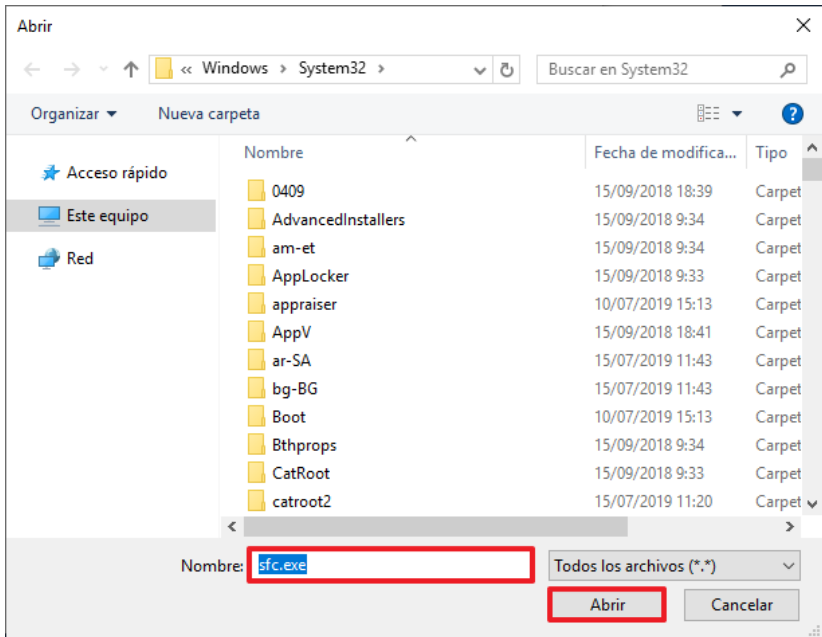
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador. Pulse con botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”.  Nota: En función de la categoría de seguridad que tenga implementada en el cliente se le solicitará bien la elevación de privilegios o bien la necesidad de introducir credenciales del usuario con privilegios de administrador.
2.	Ejecute el comando “taskschd.msc” en la misma consola de PowerShell para abrir el programador de tareas. 
3.	En el programador de tareas sitúese en la ruta “Biblioteca del Programador de tareas\Microsoft” y en el panel de “Acciones” situado en la parte derecha seleccione “Crear tarea básica”. 

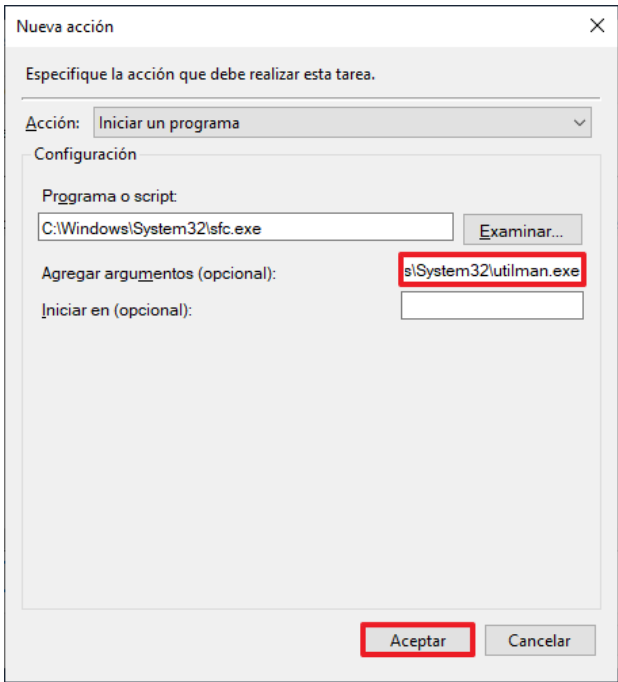
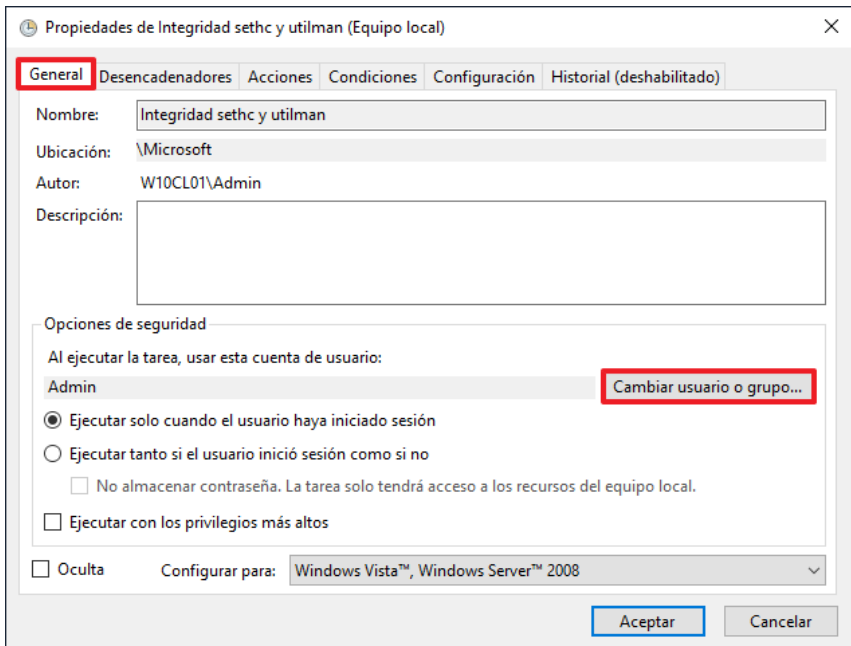
Paso	Descripción
4.	Se abrirá un asistente para la creación de la tarea programada. En la primera pestaña, indique el nombre de la tarea, en este caso “Integridad sethc y utilman” y pulse el botón “Siguiente >”. 
5.	En la ventana “Desencadenar” del asistente seleccione “Al iniciarse el equipo” y pulse sobre el botón “Siguiente >”. 

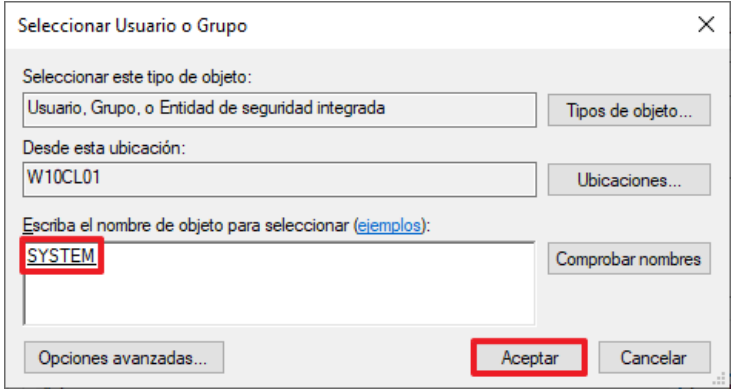
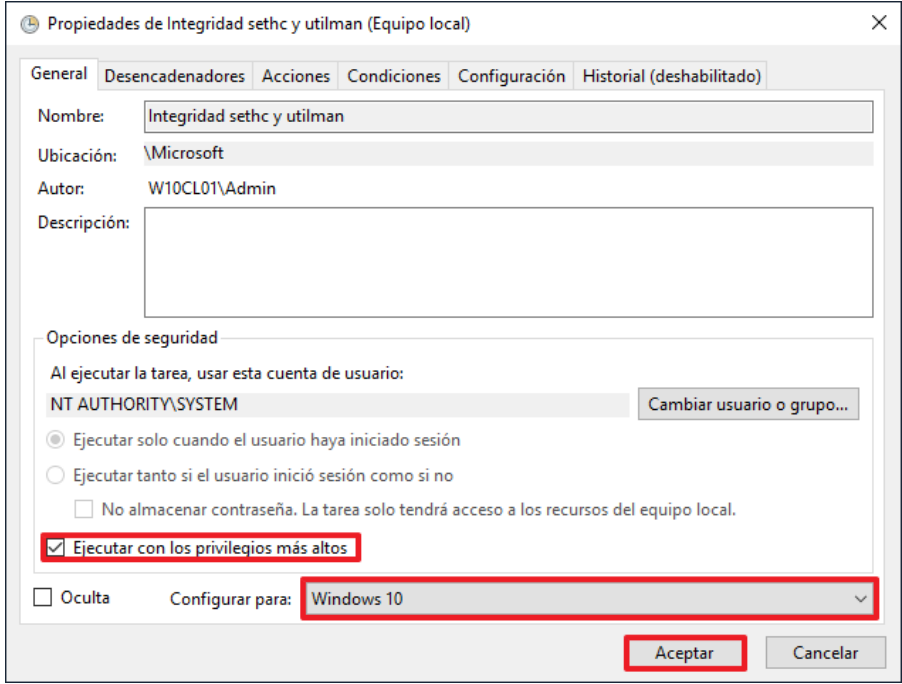
Paso	Descripción
6.	En la ventana “Acción” del asistente seleccione “Iniciar un programa” y haga clic sobre el botón “Siguiente >”. 
7.	Haga clic sobre el botón “Examinar” para indicar que programa se ejecutará. 

Paso	Descripción
8.	En la ventana emergente acceda a la ruta "C:\Windows\system32", escriba en el apartado "Nombre" "sfc.exe" y haga clic sobre el botón "Abrir". 
9.	En el apartado "Agregar argumentos (opcional)" escriba "/scanfile=C:\Windows\System32\sethc.exe" para indicarle al programa "sfc" que verifique la integridad del fichero "sethc.exe" situado en "C:\Windows\System32" y haga clic sobre el botón "Siguiente >". 

Paso	Descripción
10.	En la última ventana (Finalizar), marque la opción “Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar” y haga clic en “Finalizar”. 
11.	Al hacer clic en “Finalizar”, se abrirá el diálogo de propiedades de la tarea, sitúese en la pestaña de “Acciones” y haga clic en “Nueva...”. 

Paso	Descripción
12.	Se abrirá una ventana con la nueva acción a indicar, pulse sobre el botón “Examinar”. 
13.	En la ventana emergente acceda a la ruta “C:\Windows\System32”, escriba en el apartado “Nombre” “sfc.exe” y haga clic sobre el botón “Abrir”. 

Paso	Descripción
14.	En el apartado “Agregar argumentos (opcional)” escriba “/scanfile=C:\Windows\System32\utilman.exe” para indicarle al programa sfc que verifique la integridad del fichero utilman.exe situado en “C:\Windows\System32” y haga clic sobre el botón “Aceptar”.  Nota: Si su sistema operativo es de 64 bits, repita el proceso del paso 15 al 18 con los ficheros “C:\Windows\SysWOW64\sethc.exe” y “C:\Windows\SysWOW64\utilman.exe”.
15.	A continuación, en la pestaña “General” del dialogo de propiedades de la tarea programada, haga clic en el botón “Cambiar usuario o grupo...”. 

Paso	Descripción
16.	En la ventana emergente, introduzca el nombre “SYSTEM” y pulse aceptar. 
17.	Por último, marque la opción de “Ejecutar con los privilegios más altos”, establezca la opción “Windows 10” del desplegable “Configurar para:” y pulse en “Aceptar”. 
18.	Cierre el programador de tareas.

ANEXO D. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN REDES CLASIFICADAS COMO CLIENTE INDEPENDIENTE

Nota: Si no lo ha hecho ya, acuda a los puntos principales de esta guía establecidos en el documento principal de la guía. En estos puntos se indican el objeto, alcance y otra información que se debe tener en consideración como paso previo a la aplicación de este anexo.

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un puesto de trabajo con el sistema operativo Microsoft Windows 10 Pro/Enterprise sin opción de mantenimiento LTSC (versión 1809) en un entorno aislado, es decir, no conectado a una red no segura, como es Internet.

Nota: Todas las referencias indicadas en este anexo hacen referencia a la guía codificada como "CCN-STIC-599B19" correspondiente con el ANEXO D enfocado a redes clasificadas.

Debido a las características de los puestos de trabajo a los que van dirigidas las guías de la serie 500, se recomienda establecer la versión Microsoft Windows 10 Enterprise 1809 con la opción de mantenimiento LTSC como la más adecuada para su implementación. Esto se basa en los siguientes condicionantes:

- a) Estos equipos no estarán conectados a Internet por lo cual determinadas funcionalidades como la tienda o Cortana, que no son proporcionadas por la opción de mantenimiento LTSC, se consideran prescindibles.
- b) El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.
- c) La opción de mantenimiento a largo plazo permite garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con Microsoft Windows 10 y que, siendo críticas, no permitan, por sus características, cambios en funcionalidades habituales. No obstante, deben considerarse siempre las actualizaciones de seguridad como un elemento esencial para garantizar la seguridad de los puestos de trabajo en cualquier infraestructura, siendo aún más crítico en una red clasificada.

Pese a la recomendación anterior también está admitida la versión Windows 10 Pro/Enterprise sin opción de mantenimiento LTSC, en su versión 1809 (versión contemplada en este anexo). Para la correcta implementación y adecuar dicha versión de Windows para un entorno de Redes Clasificadas, existen varias configuraciones y características que son desactivadas durante la presente guía para garantizar la securización del sistema. Dichas características son:

- a) Autenticación: Microsoft Passport y Windows Hello. Esta funcionalidad está inhabilitada con la aplicación del presente anexo.
- b) Sistema de telemetría. La configuración de telemetría se deshabilitará mediante la aplicación del presente anexo. Se inhabilitarán los servicios asociados a dicho componente.
- c) Tienda de Microsoft: La versión Enterprise con la opción de mantenimiento LTSC, utilizada para la realización de dicho anexo no posee esta herramienta, aunque es desactivada con la aplicación del presente anexo.

- d) Aplicaciones para la plataforma universal de Windows (UWP). Al igual que en el caso anterior las Appx o Modern App no existen con la opción de mantenimiento LTSC y en la versión Pro/Enterprise se limita por la aplicación de la presente guía.
- e) Sistema Experiencia de Usuario. Este componente se encuentra limitado por la aplicación de la presente guía.
- f) Microsoft Edge. Al igual que sucede con la Tienda no está disponible en la versión Enterprise con opción de mantenimiento LTSC y en la versión Pro/Enterprise se limita por la aplicación de la presente guía.
- g) Opciones de privacidad. El presente anexo tiene en consideración todos los aspectos e inhabilita el envío de información para cada uno de los elementos anteriormente citados. Tampoco permite la interacción de las aplicaciones con dichos componentes.
- h) Internet Explorer 11. IE 11 es securizado según los mecanismos definidos en la guía CCN-STIC-520.

A continuación, se describe la configuración específica de seguridad que va a ser aplicada sobre los puestos de trabajo en redes clasificadas.

Se ha de tener en consideración que la aplicación de esta guía se debe realizar en un sistema formateado (sin datos) siguiendo las indicaciones que se describen en este anexo.

A través del procedimiento indicado a continuación se establece la máxima seguridad posible teniendo en consideración la guía CCN-STIC-301 – Requisitos STIC. Si su sistema requiere de otra configuración menos restrictiva, y está autorizado para ello, consulte el apartado “ANEXO D.2 APLICACIÓN DE NIVELES DE CLASIFICACIÓN” para realizar los pasos adecuados.

ANEXO D.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 COMO CLIENTE INDEPENDIENTE

ANEXO D.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA

Este anexo ha sido diseñado para ayudar a los operadores a implementar las distintas configuraciones de seguridad. A continuación, se describe, paso a paso, como realizar la instalación y configuración de seguridad de un cliente Windows 10 Pro/Enterprise sin opción de mantenimiento LTSC (versión 1809) independiente de un dominio.

Esta guía incorpora todos los ficheros y scripts necesarios para realizar la configuración segura de los equipos.

Antes de empezar deberán tenerse en cuenta las siguientes recomendaciones:

- a) Todos los discos y particiones deberán formatearse utilizando el sistema de archivos NTFS.

Por defecto el programa de instalación da a todos los sistemas de ficheros el formato NTFS, por lo que normalmente no será necesario indicarlo explícitamente.

A diferencia de lo que ocurría en Windows Vista, el programa de instalación de Windows 10 creará por defecto las particiones de disco necesarias para poder habilitar posteriormente el cifrado de disco BitLocker.

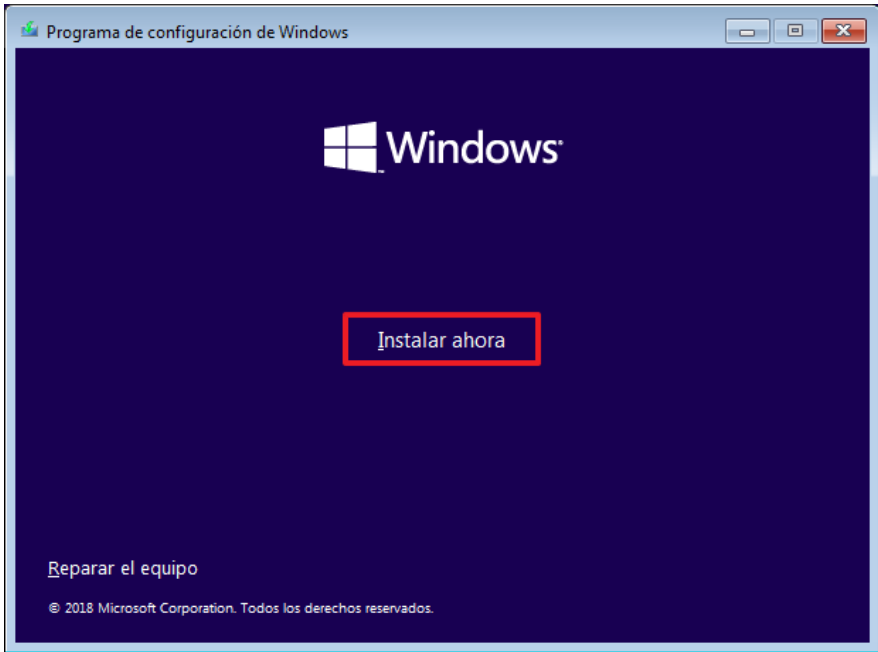
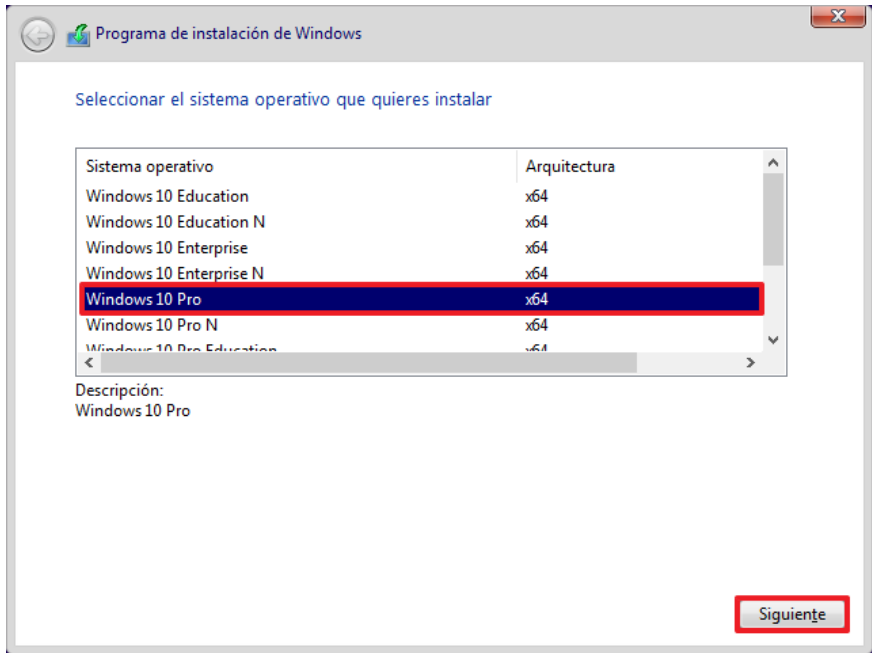
En el “ANEXO D.3.1 CIFRADO DE DISCO CON BITLOCKER” de la presente guía podrá consultar detalles sobre BitLocker y una guía paso a paso para poder aplicarlo en los equipos Windows 10 que requieran de su uso.

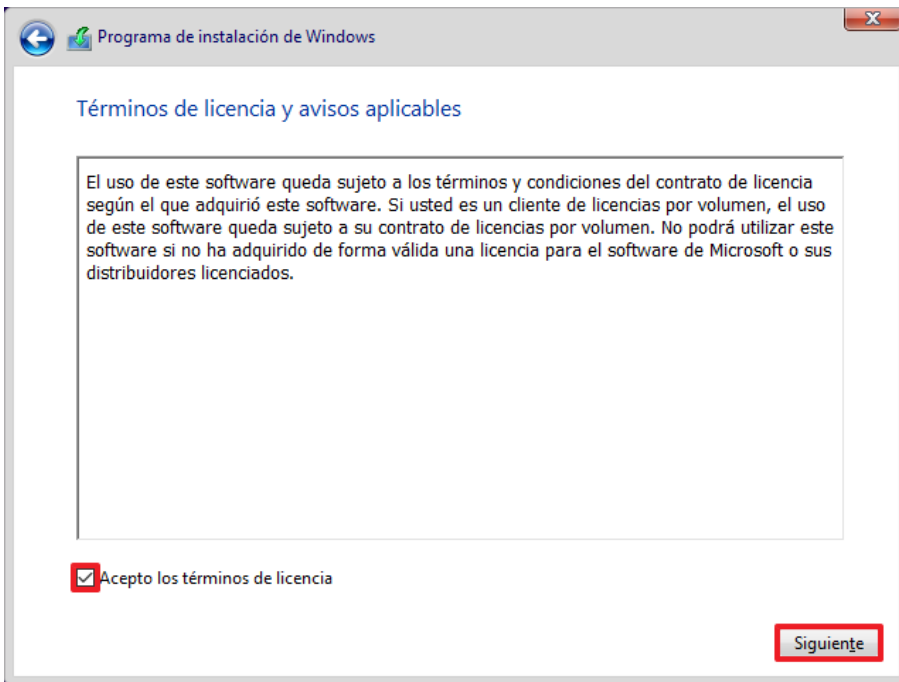
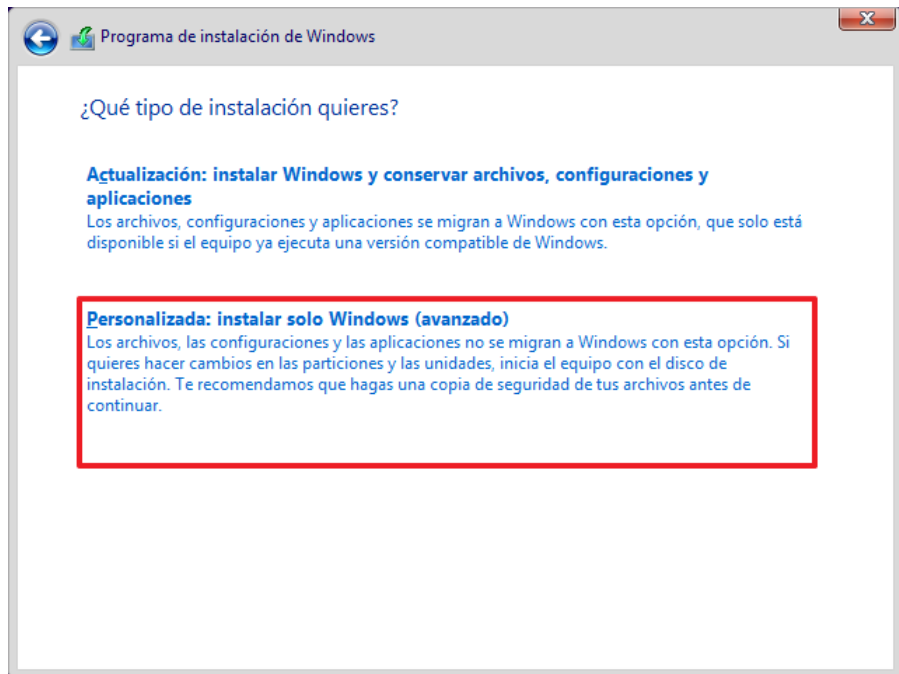
- b) Es importante separar datos, aplicaciones y sistema operativo en distintos dispositivos de almacenamiento, tanto para mejorar el rendimiento como para evitar ataques que se realizan navegando entre directorios. Para la seguridad de un equipo con sólo Windows 10 no se requiere la existencia de distintas particiones, pero se deberá tener en cuenta durante el proceso de instalación, ya que existen roles para los cuales se requiere que existan estas particiones diferenciadas.
- c) Si existen datos en el equipo antes del proceso de instalación, deberán eliminarse antes de comenzar el proceso.
- d) No deberán realizarse actualizaciones desde versiones previas, ya que de lo contrario no podrá garantizarse que los valores por defecto de los parámetros de seguridad se hayan aplicado.
- e) No utilizar discos o particiones que utilicen el sistema de archivos FAT.
- f) No instalar otros sistemas operativos en el equipo.
- g) Asignar una contraseña compleja a la cuenta de usuario que se crea durante el proceso de instalación.
- h) Una vez finalizada la instalación básica del sistema, asegurarse de que se instalan 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.
- i) Deberá realizarse la activación de Windows antes de comenzar el proceso de securización con el equipo conectado a una red segura.

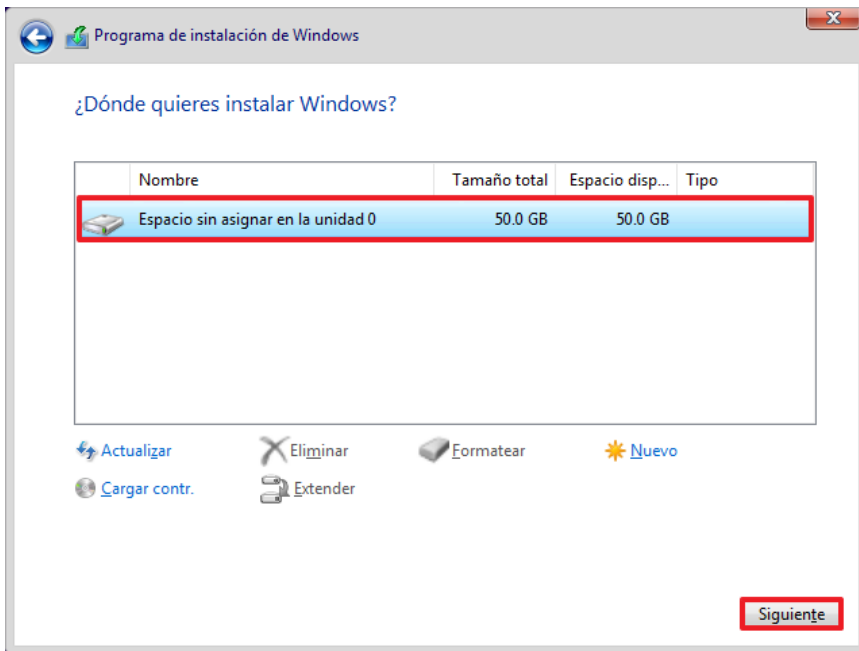
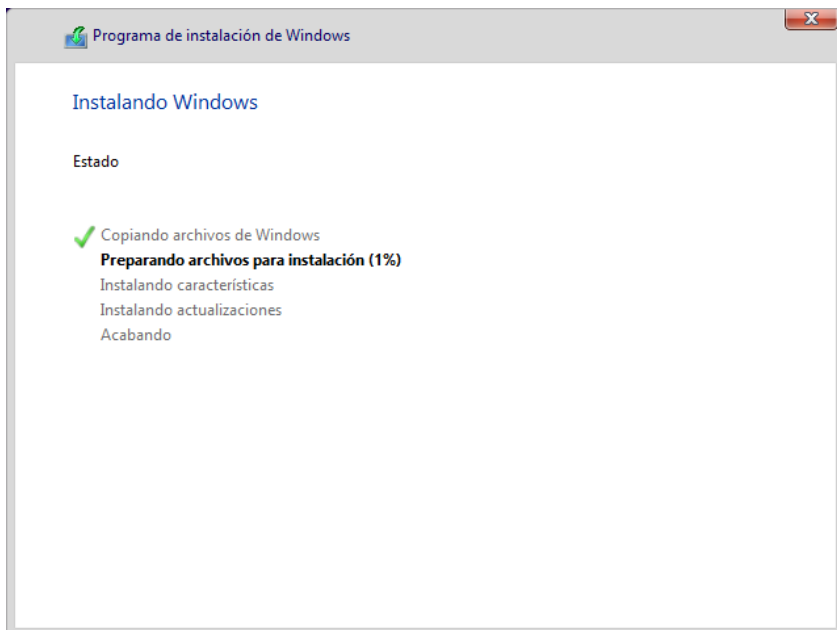
1. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10

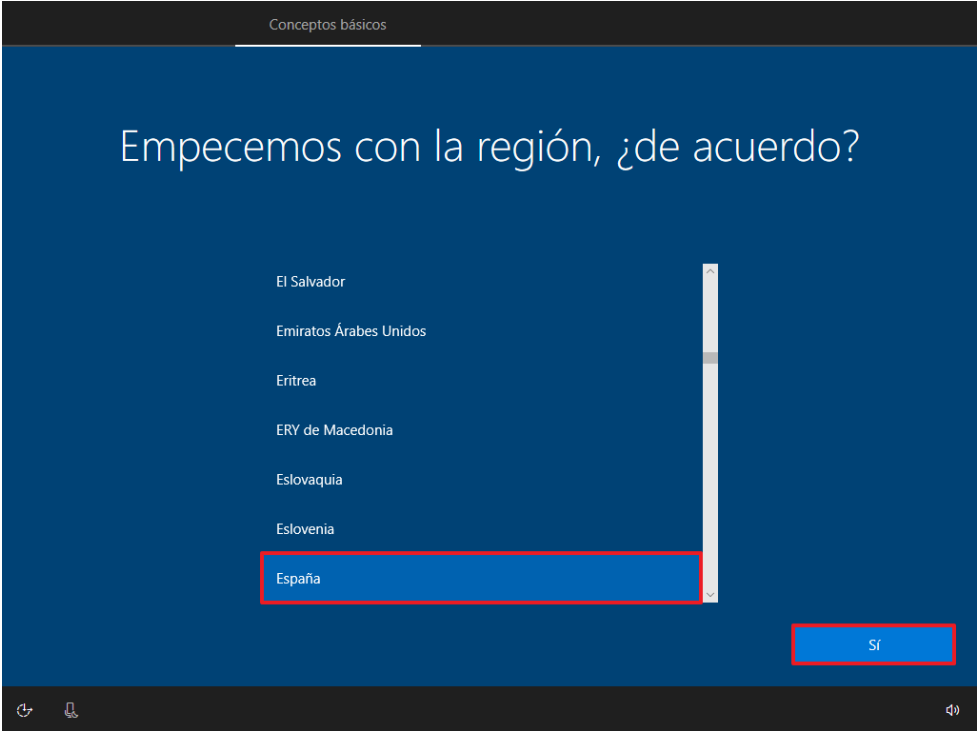
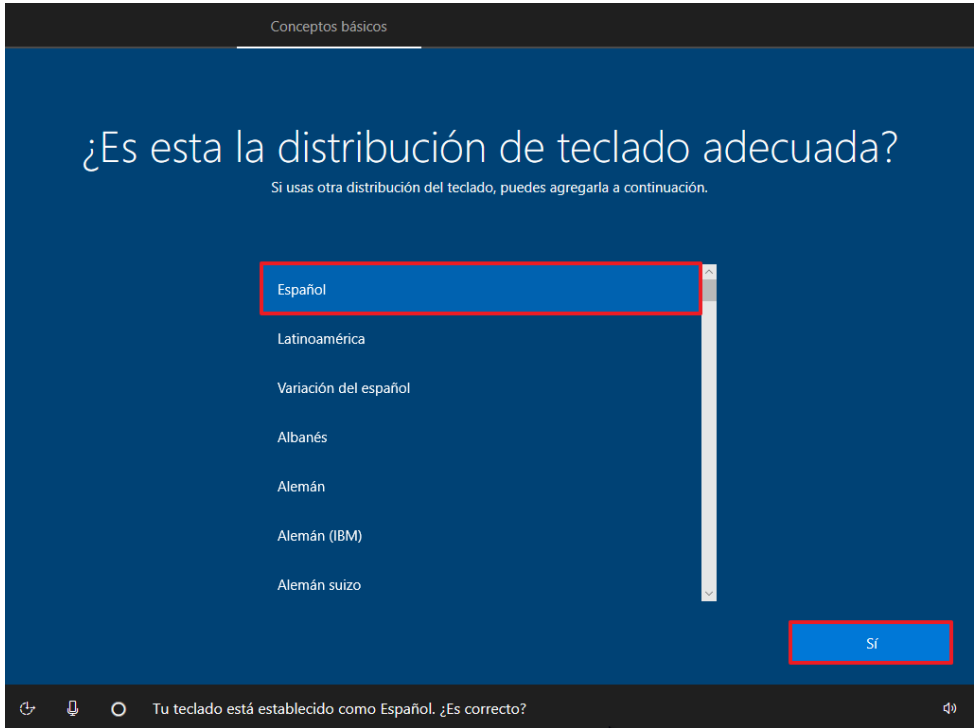
El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación. No se proporciona un fichero de respuestas automáticas, como se hacía en otras guías para versiones anteriores de Windows, esto se debe a que la instalación por defecto de Windows 10 habilita una serie de características opcionales, que serán fácilmente eliminadas a posteriori y antes del primer inicio del sistema. La eliminación de esta serie de características es parte del proceso de aplicación de esta guía.

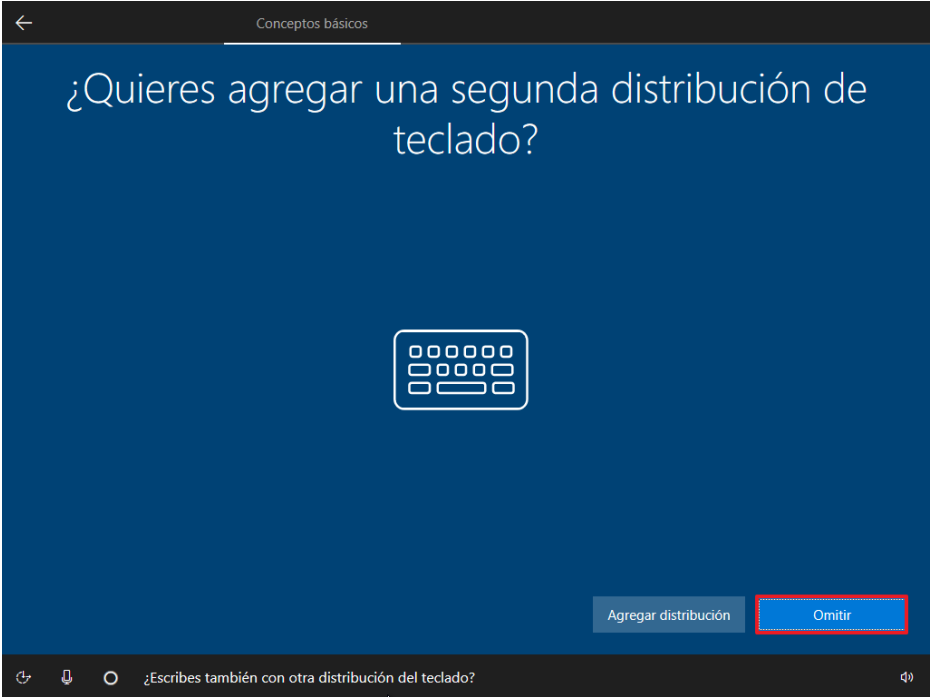
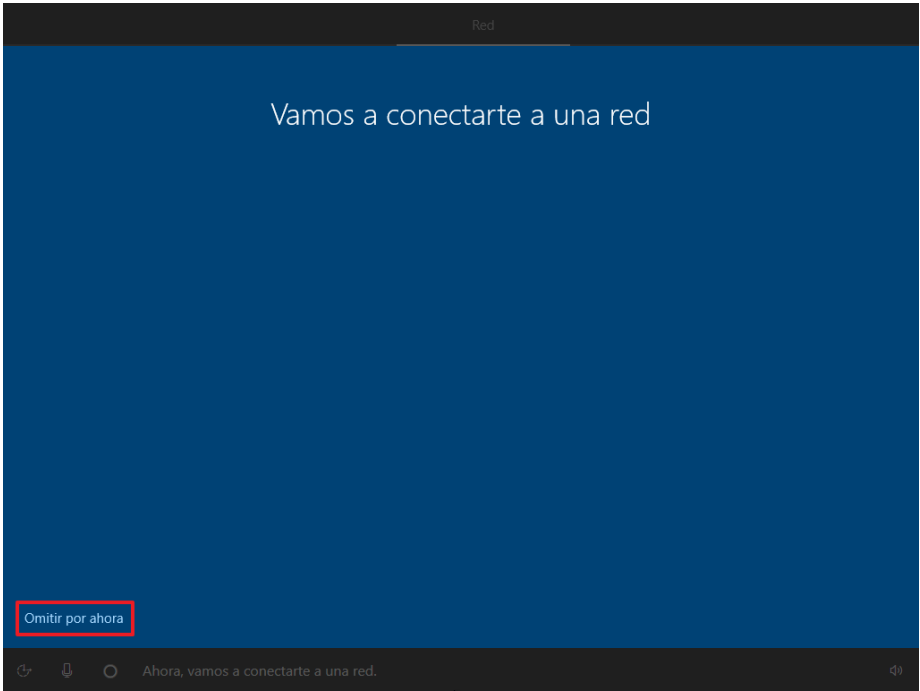
Paso	Descripción
1.	Introduzca el dispositivo USB o DVD de Windows 10 Pro/Enterprise y, si fuera necesario, reinicie la máquina para iniciar la instalación del sistema.
2.	Cuando aparezca el mensaje “Presionar una tecla para arrancar desde el DVD”, pulse una tecla. Si el equipo no se inicia desde DVD revise los parámetros de la BIOS.
3.	Cuando se le indique en pantalla, seleccione el idioma y la configuración de teclado (Español). Pulse “Siguiente” para continuar. 

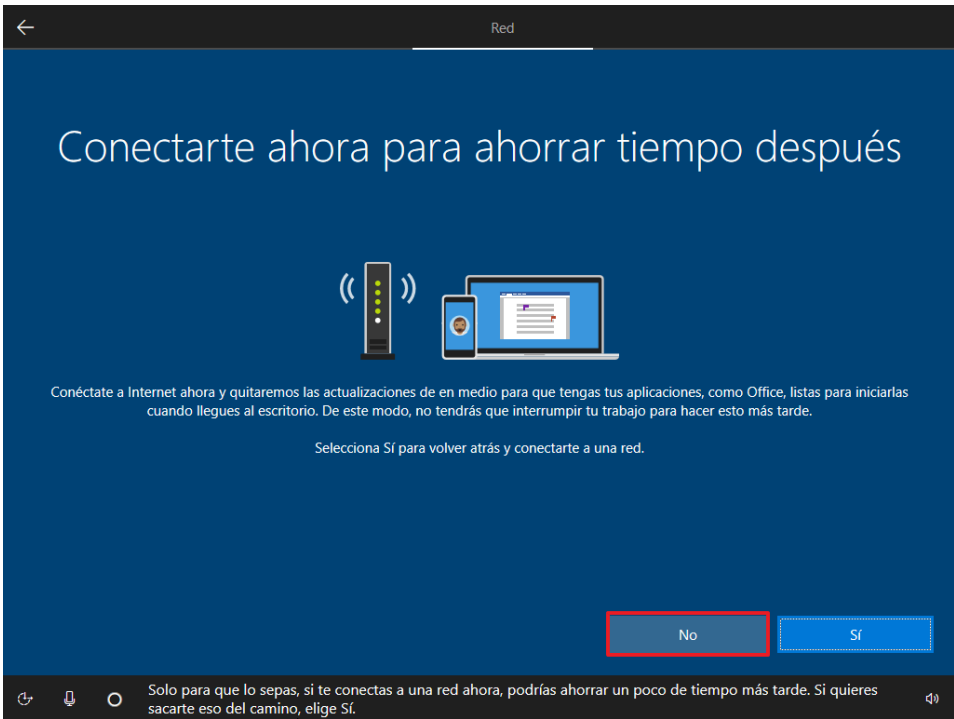
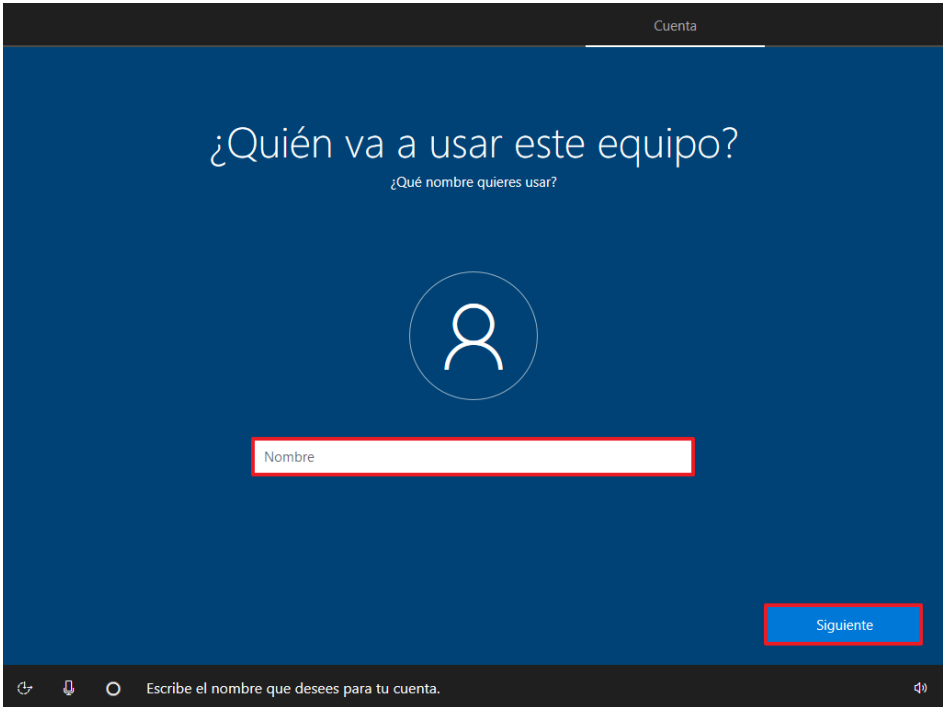
Paso	Descripción
4.	Pulse sobre “Instalar ahora”. 
5.	Seleccione la opción “Windows 10 Pro” y pulse “Siguiente”.  Nota: En este ejemplo se realiza la instalación del sistema operativo en su versión Pro, aunque la versión Enterprise también está contemplada en el presente anexo. Deberá seleccionar la opción más adecuada para su organización.

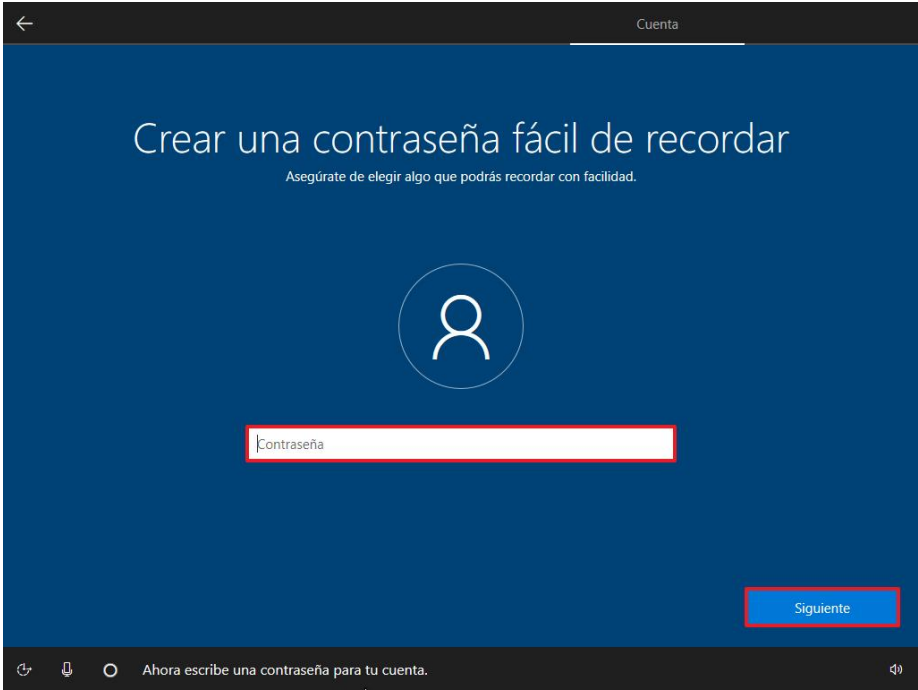
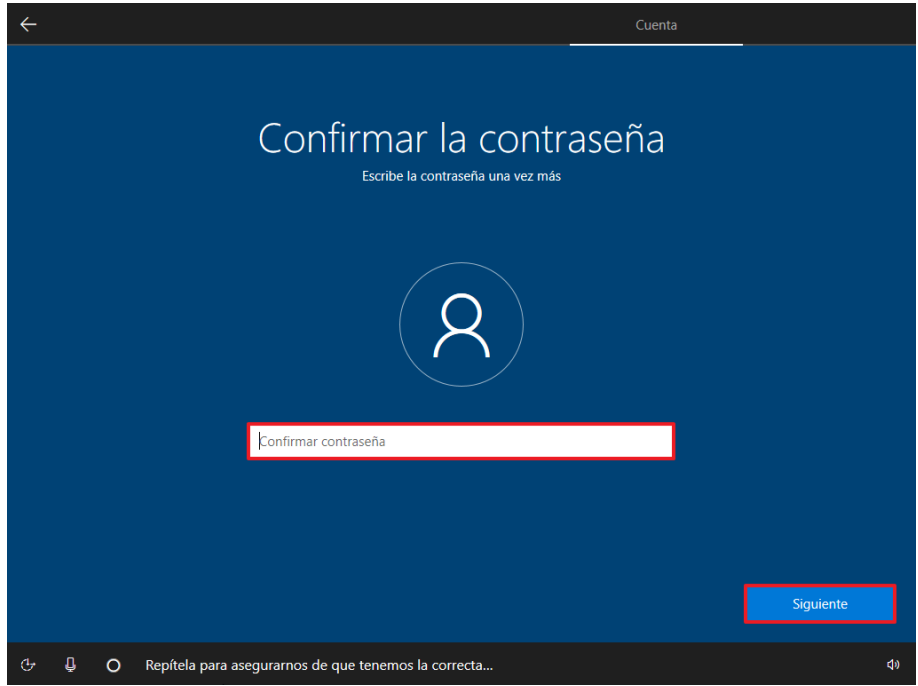
Paso	Descripción
6.	Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”. 
7.	Seleccione la opción tipo de instalación “Personalizada: instalar solo Windows (avanzado)”. 

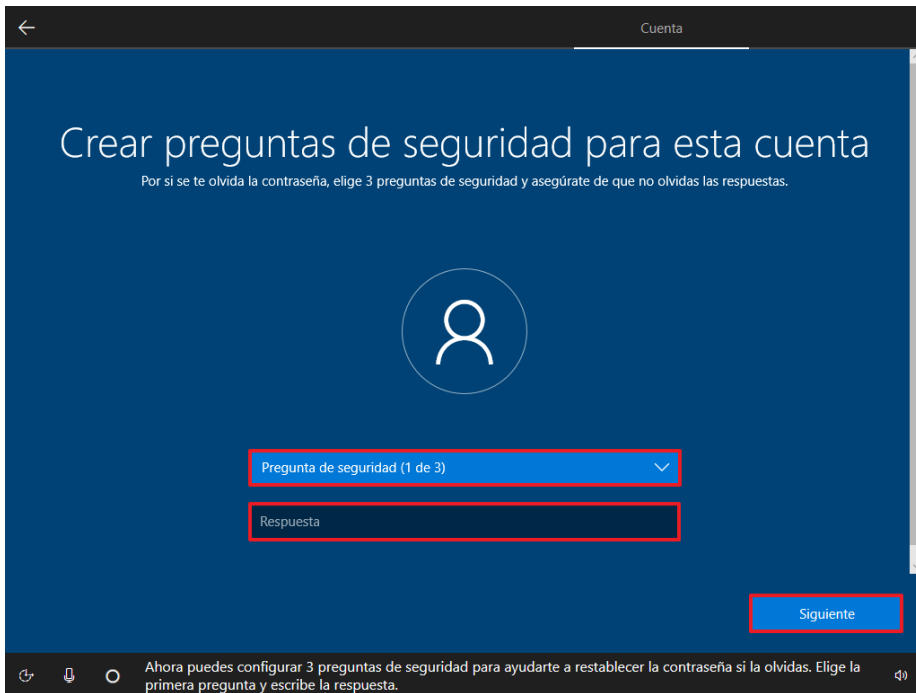
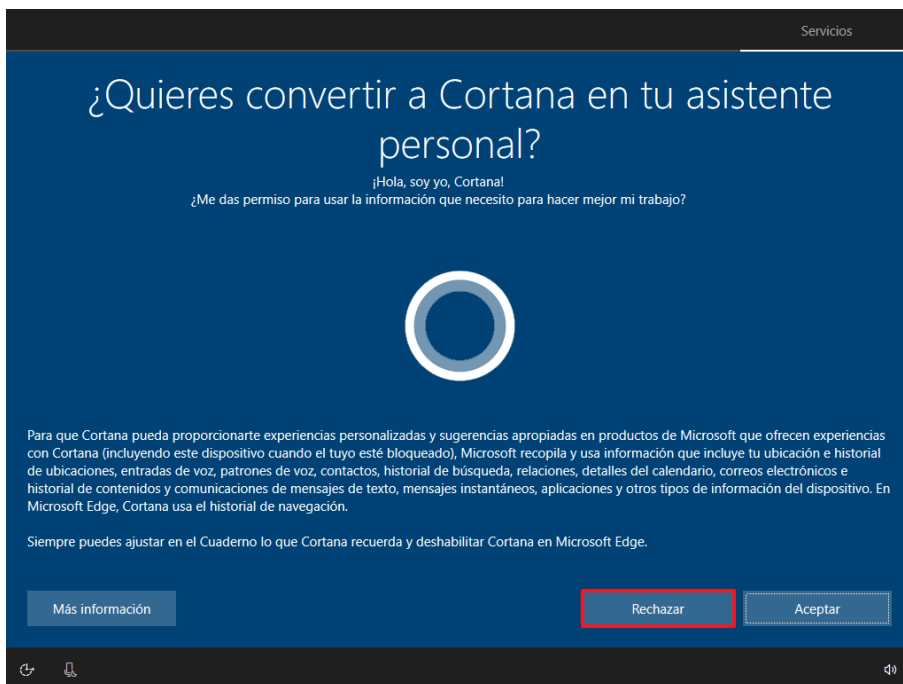
Paso	Descripción
8.	Seleccione el disco en el que se realizará la instalación y pulse “Siguiente”.  Nota: En caso de necesitar establecer particiones o formatear particiones o discos, es en este momento de la instalación en el que será necesario realizar dichos pasos. No es objeto de esta guía la explicación de los pasos a seguir para realizar este tipo de tareas, por tanto y si quiere realizar tareas de esta índole, puede consultar los pasos a seguir a través de este enlace: https://support.microsoft.com/es-es/help/15088/windows-10-create-installation-media#1TC=windows-10
9.	Comenzará la instalación en este momento. Este proceso durará varios minutos dependiendo de las prestaciones del dispositivo sobre el que se instale Windows 10 y, posiblemente, requerirá reiniciar en varias ocasiones. Espere a que aparezca la ventana “Conceptos básicos” y continúe con el siguiente paso. 

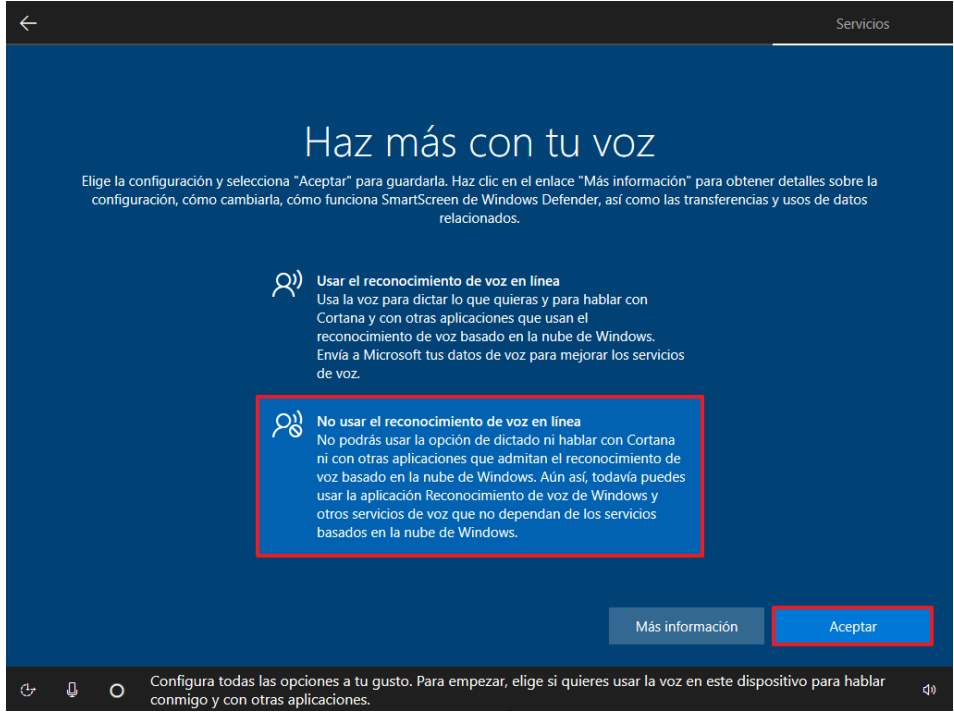
Paso	Descripción
10.	En la ventana “Conceptos básicos” seleccione la región “España” y pulse “Sí”. 
11.	Seleccione la distribución de teclado “Español” y pulse “Sí” para continuar. 

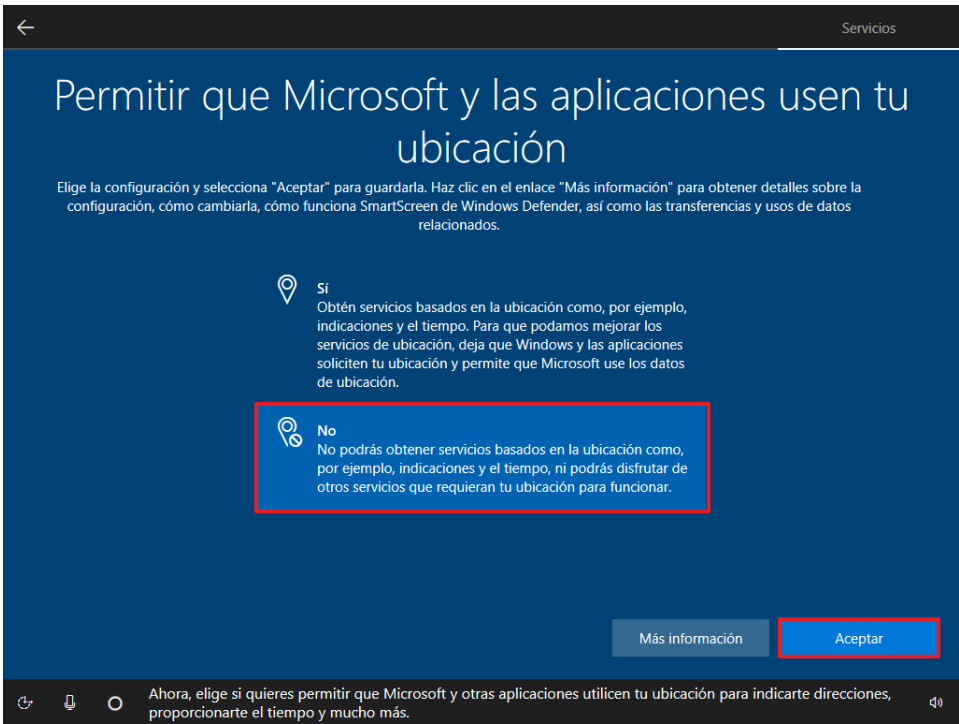
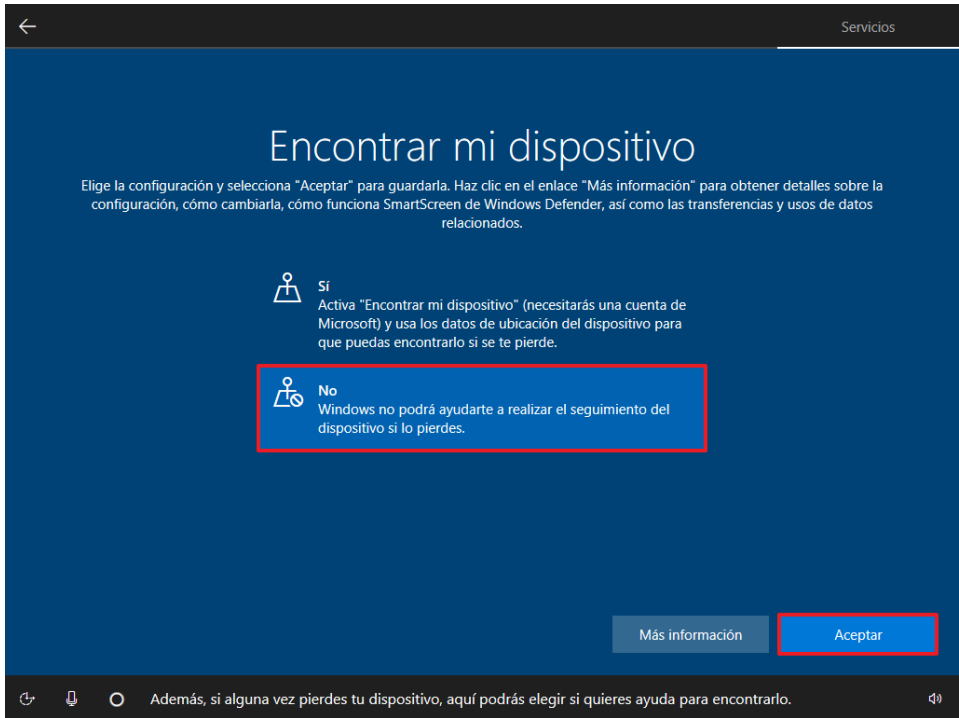
Paso	Descripción
12.	Pulse “Omitir” para no agregar una segunda distribución de teclado. 
13.	En el apartado de red seleccione la opción “Omitir por ahora”. 

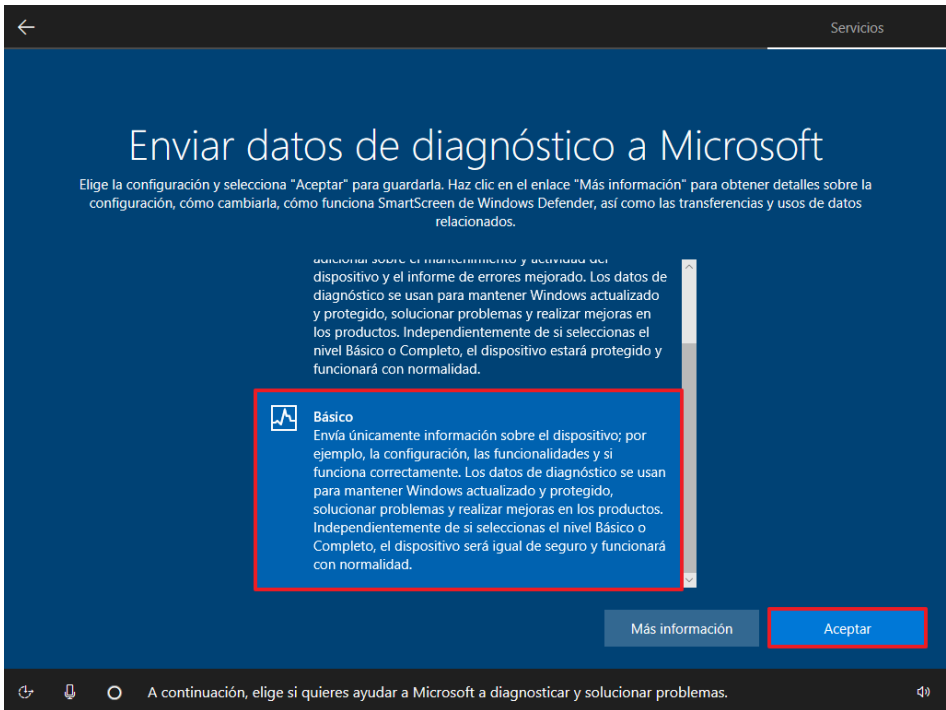
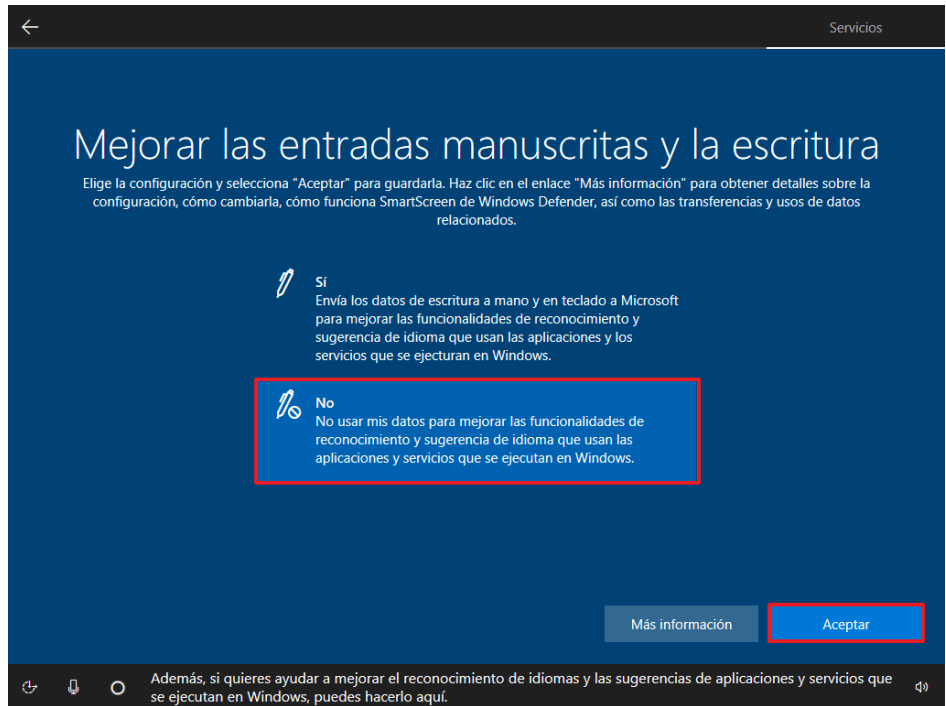
Paso	Descripción
14.	Pulse “No” para continuar. 
15.	En la ventana “Cuenta”, introduzca un nombre de usuario (por ejemplo "Admin") que se creará con permisos de administrador local. Pulse “Siguiente” para continuar.  Nota: Deberá elegir un nombre de usuario adecuado para su entorno. Los nombres aquí indicados sólo se proporcionan a modo de ejemplo.

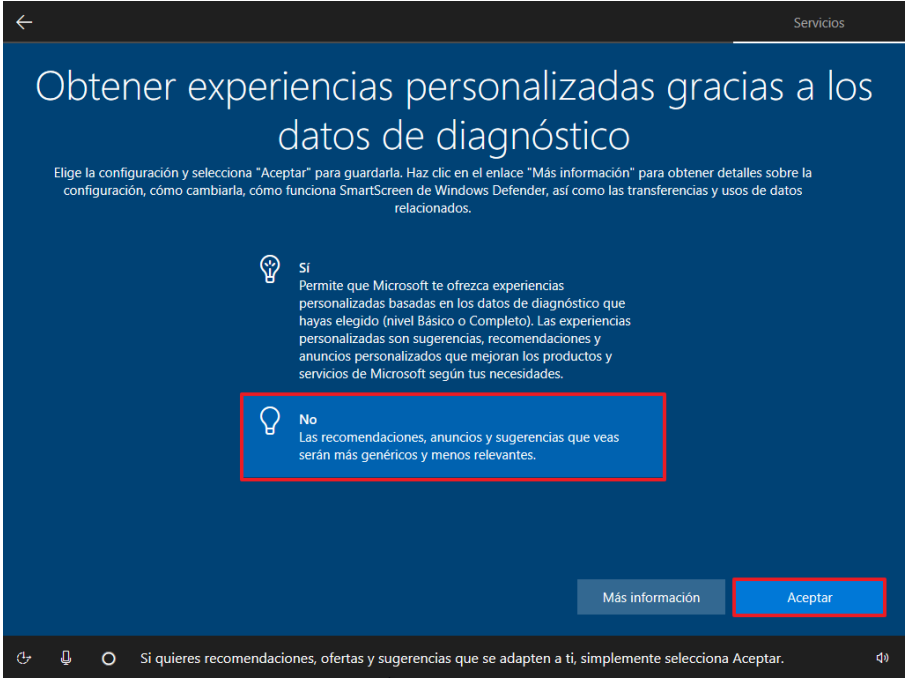
Paso	Descripción
16.	Introduzca una contraseña para el usuario administrador local y pulse “Siguiente”. 
17.	Introduzca nuevamente la contraseña y pulse “Siguiente”. 

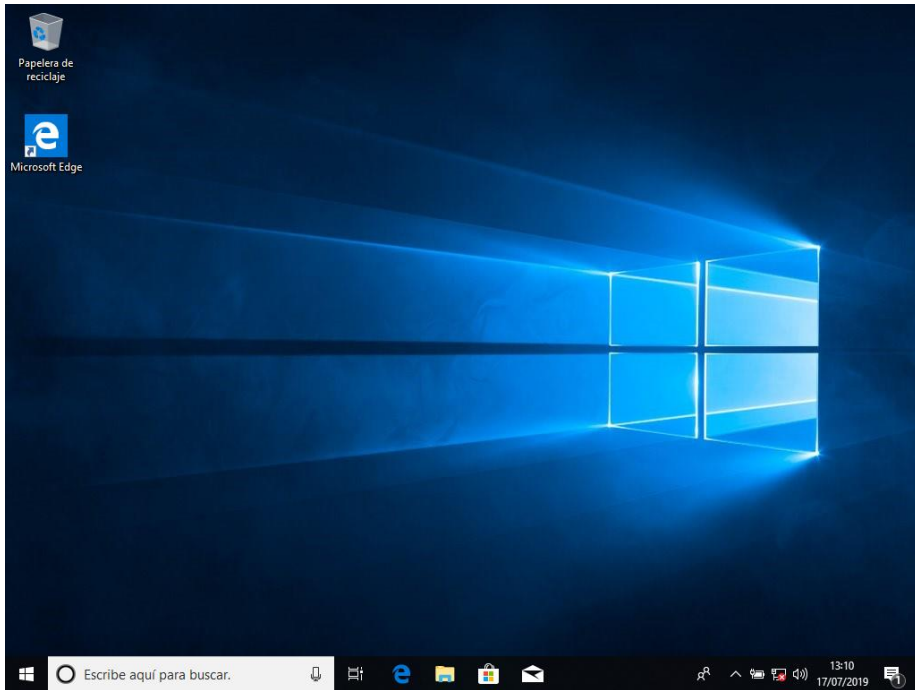
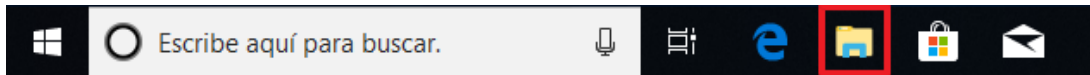
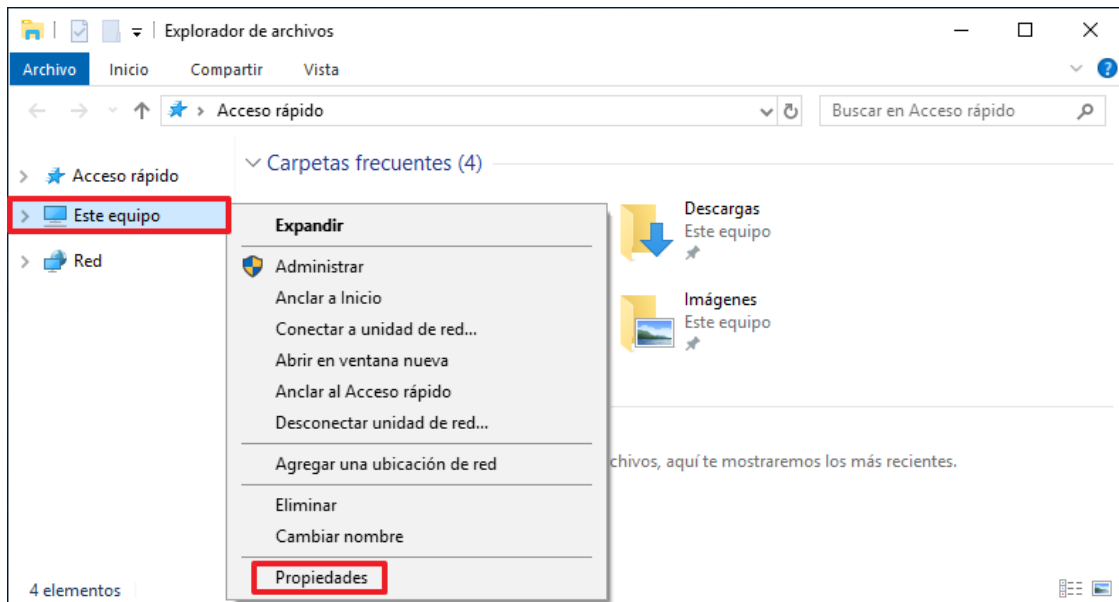
Paso	Descripción
18.	El instalador le solicitará tres preguntas de seguridad en caso de olvidar la contraseña. Seleccione las preguntas, respóndalas y pulse “Siguiente” para continuar.  Nota: Más adelante se establecerá el bloqueo de la cuenta en caso de introducir erróneamente la contraseña repetidas veces.
19.	Pulse “Rechazar” para no dar permisos al asistente personal “Cortana” para que recopile información. 

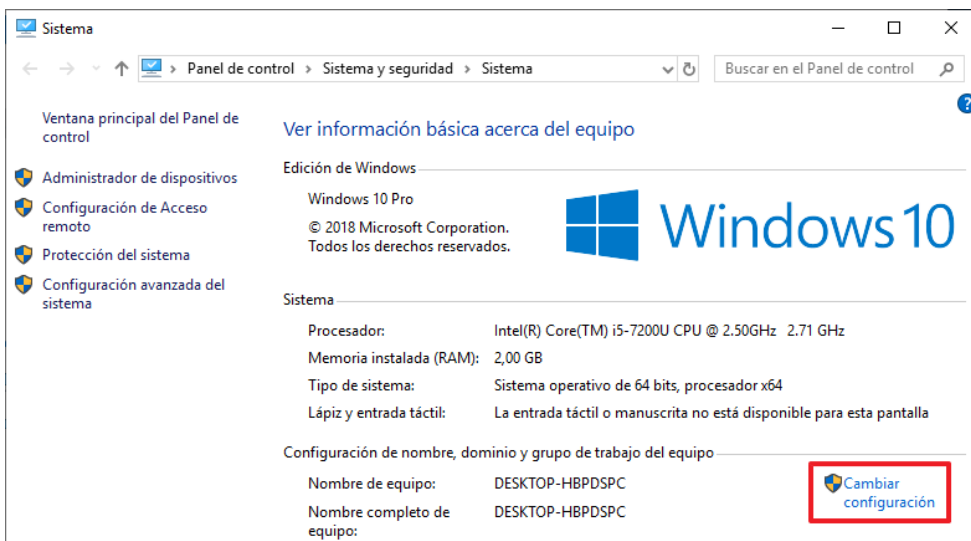
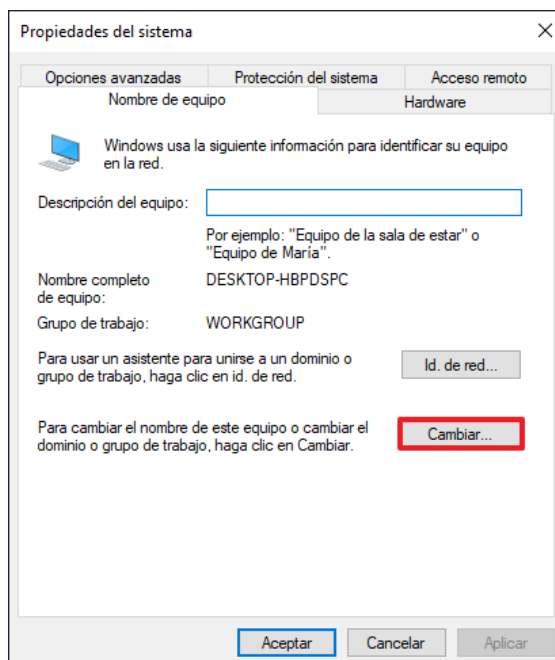
Paso	Descripción
20.	Pulse “No” para desactivar el historial de actividad. 
21.	Seleccione “No” para no usar el reconocimiento de voz en línea y pulse “Aceptar”. 

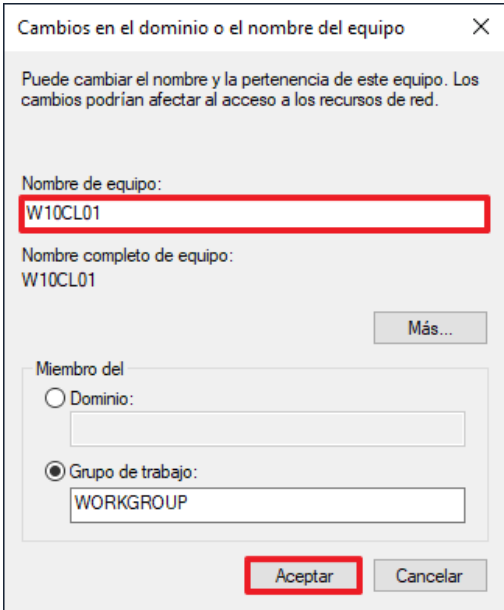
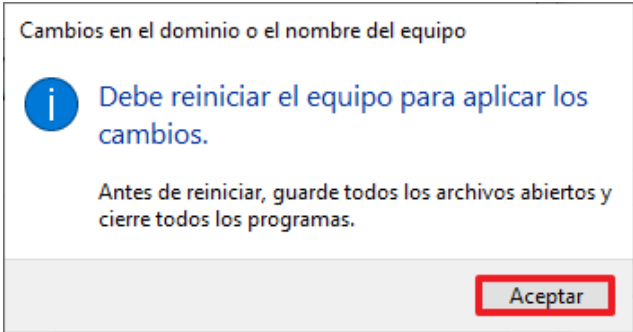
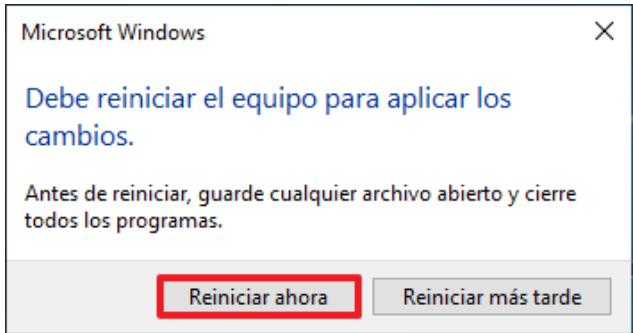
Paso	Descripción
22.	Seleccione “No” para impedir que las aplicaciones usen la ubicación y pulse “Aceptar”. 
23.	Seleccione “No” para desactivar la funcionalidad de “Encontrar mi dispositivo”. Pulse “Aceptar” para continuar. 

Paso	Descripción
24.	Seleccione la opción “Básico” y pulse “Aceptar”.  Nota: Más adelante se impedirá toda comunicación con los servidores de Windows y se desactiva la telemetría.
25.	Seleccione “No” y pulse “Aceptar”. 

Paso	Descripción
26.	Seleccione “No” para no enviar datos de diagnóstico. Pulse “Aceptar” para continuar.  Obtener experiencias personalizadas gracias a los datos de diagnóstico Elige la configuración y selecciona “Aceptar” para guardarla. Haz clic en el enlace “Más información” para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Windows Defender, así como las transferencias y usos de datos relacionados. Sí Permite que Microsoft te ofrezca experiencias personalizadas basadas en los datos de diagnóstico que hayas elegido (nivel Básico o Completo). Las experiencias personalizadas son sugerencias, recomendaciones y anuncios personalizados que mejoran los productos y servicios de Microsoft según tus necesidades. No Las recomendaciones, anuncios y sugerencias que veas serán más genéricos y menos relevantes. Más información Aceptar Si quieres recomendaciones, ofertas y sugerencias que se adapten a ti, simplemente selecciona Aceptar.
27.	Seleccione “No” para impedir que las aplicaciones usen el identificador de publicidad. Pulse “Aceptar” para continuar.  Permitir que las aplicaciones usen el id. de publicidad Elige la configuración y selecciona “Aceptar” para guardarla. Haz clic en el enlace “Más información” para obtener detalles sobre la configuración, cómo cambiarla, cómo funciona SmartScreen de Windows Defender, así como las transferencias y usos de datos relacionados. Sí Las aplicaciones pueden usar el id. de publicidad para proporcionar anuncios más personalizados de acuerdo con la directiva de privacidad del proveedor de la aplicación. No El número de anuncios que veas no cambiará, pero pueden ser menos relevantes. Más información Aceptar Para finalizar la configuración, elige si quieres recibir anuncios que sean más interesantes para ti o no.

Paso	Descripción
28.	El sistema iniciará sesión tras unos momentos de preparación, con el usuario recién creado con las configuraciones especificadas, el cual pertenecerá al grupo “Administradores”, y finalmente se mostrará el escritorio. 
29.	En la barra de tareas, seleccione el icono del “Explorador de archivos”. 
30.	En el “Explorador de archivos” pulse con el botón derecho del ratón sobre “Este equipo” y seleccione “Propiedades”. 

Paso	Descripción
31.	En la ventana “Sistema” localice el apartado “Configuración de nombre, dominio y grupo de trabajo del equipo” y pulse sobre “Cambiar configuración” 
32.	En “Propiedades del sistema”, seleccione la pestaña “Nombre de equipo”, pulse sobre “Cambiar”. 

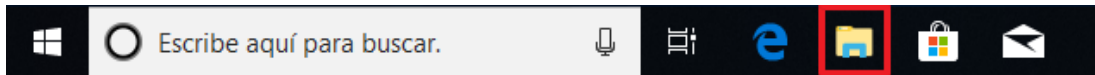
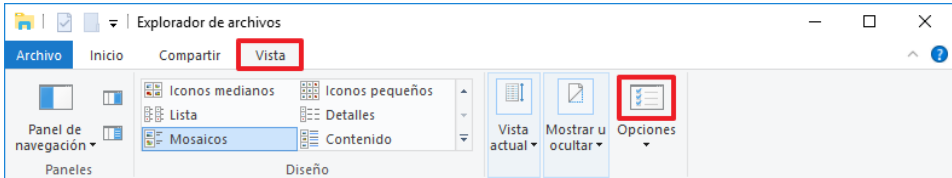
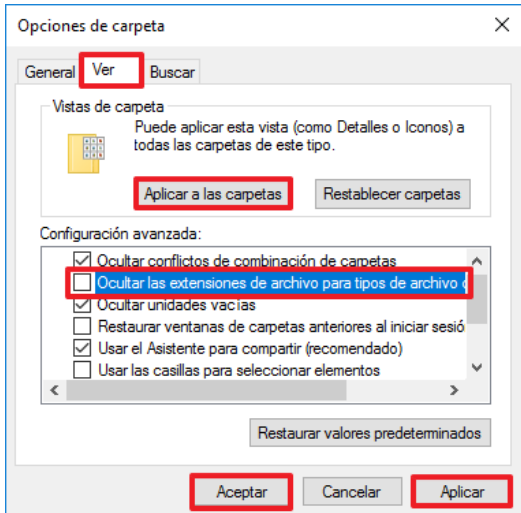
Paso	Descripción
33.	Establezca un nombre de equipo y pulse “Aceptar”.  Nota: En el ejemplo, el equipo se denomina “W10CL01”. Establezca el nombre más adecuado para su organización.
34.	El sistema deberá reiniciar para guardar los cambios. Pulse “Aceptar” en la ventana de “Cambios en el dominio o el nombre de equipo”. 
35.	Pulse sobre “Cerrar” en “Propiedades del sistema” y “Reiniciar ahora” para que se reinicie el equipo y hagan efecto los cambios. 

2. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10

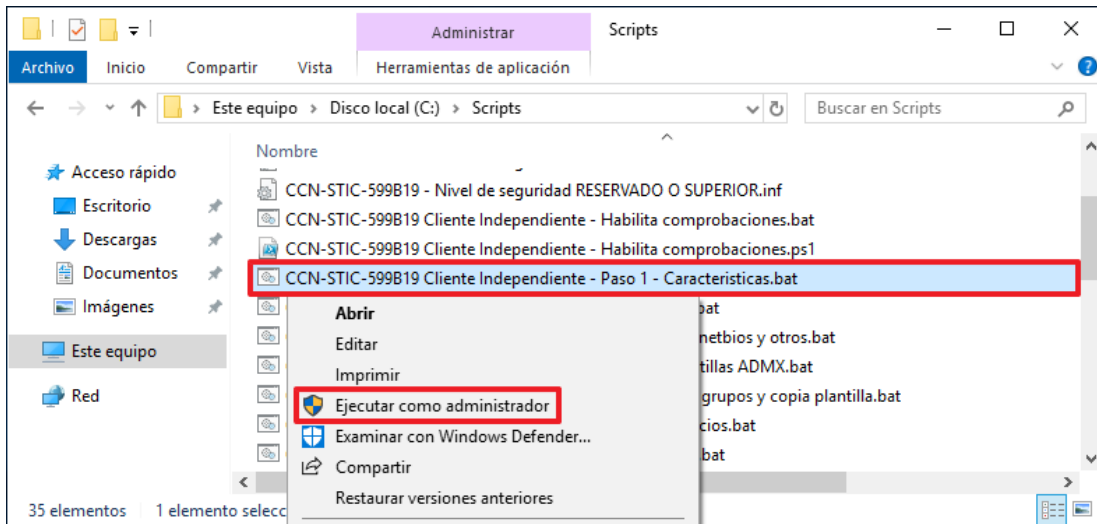
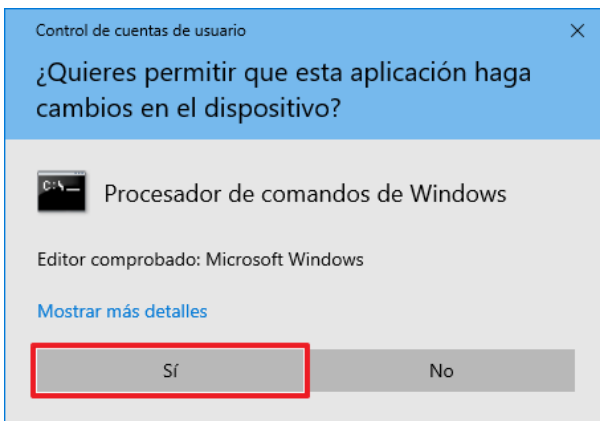
A continuación, y una vez instalado el sistema operativo en el cliente Windows 10 independiente, se procederá a configurar el equipo.

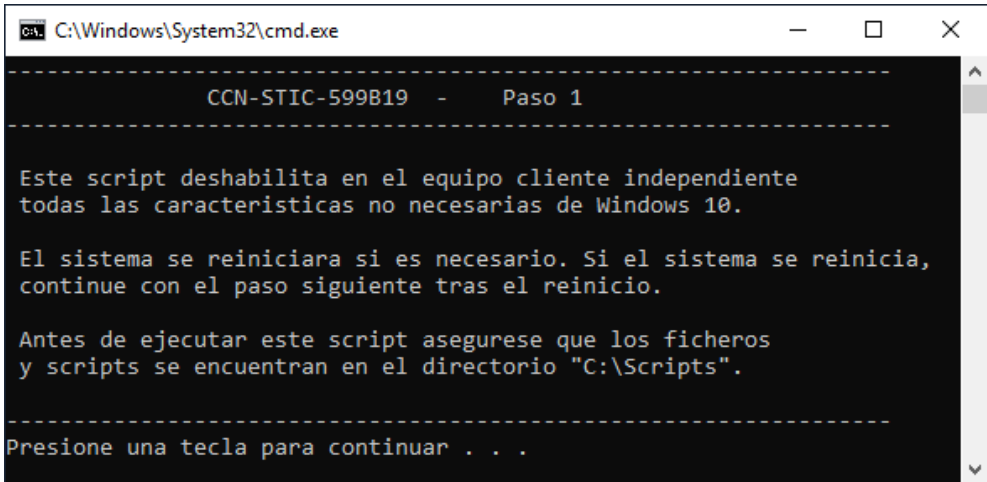
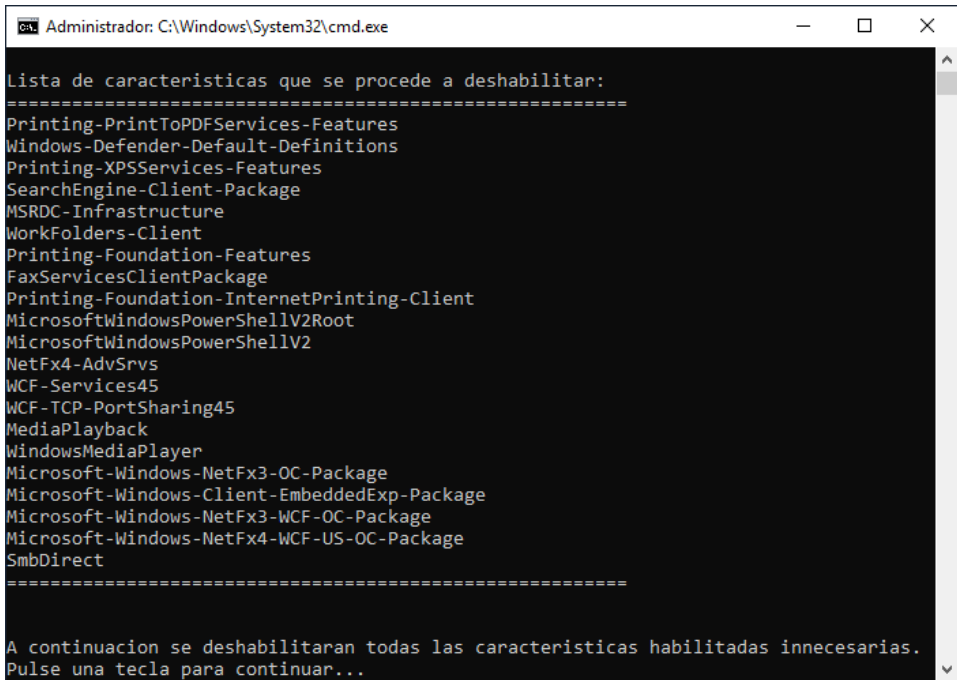
Nota: En este punto es conveniente recordar que, aunque en esta guía paso a paso no se dedica ningún apartado concreto a ello, será necesario instalar las actualizaciones de seguridad disponibles y realizar la activación de Windows en el equipo.

Los pasos que se describen a continuación contemplan el uso de Windows 10 en un equipo independiente. En este caso se incluirán los elementos de seguridad tanto para el sistema operativo como para Internet Explorer 11.

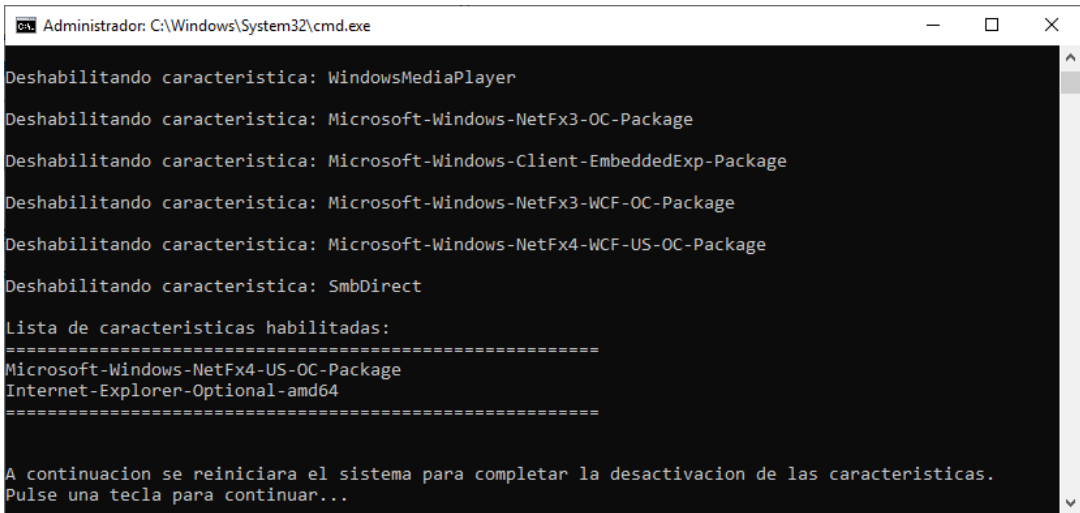
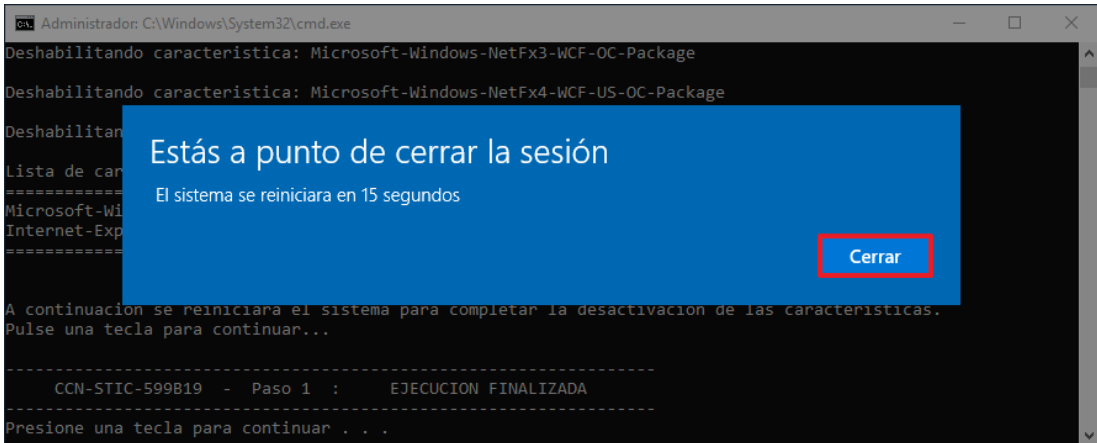
Paso	Descripción
36.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador.
37.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, en la barra de tareas, seleccione el icono del “Explorador de archivos”. 
38.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
39.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y en “Aceptar”. 

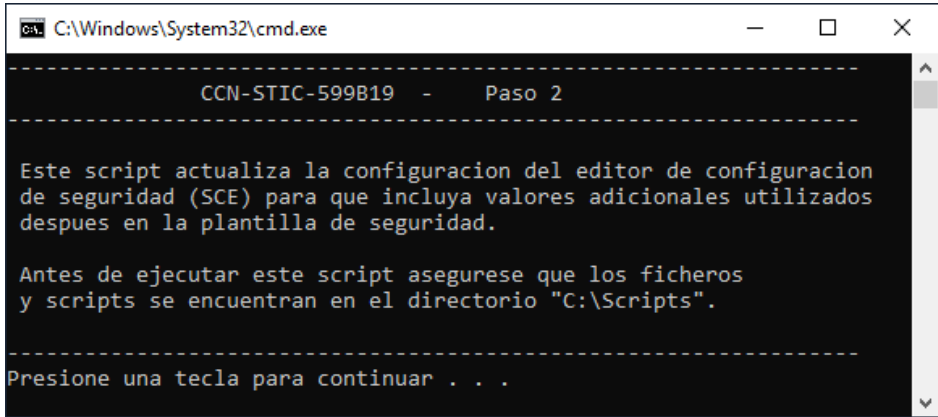
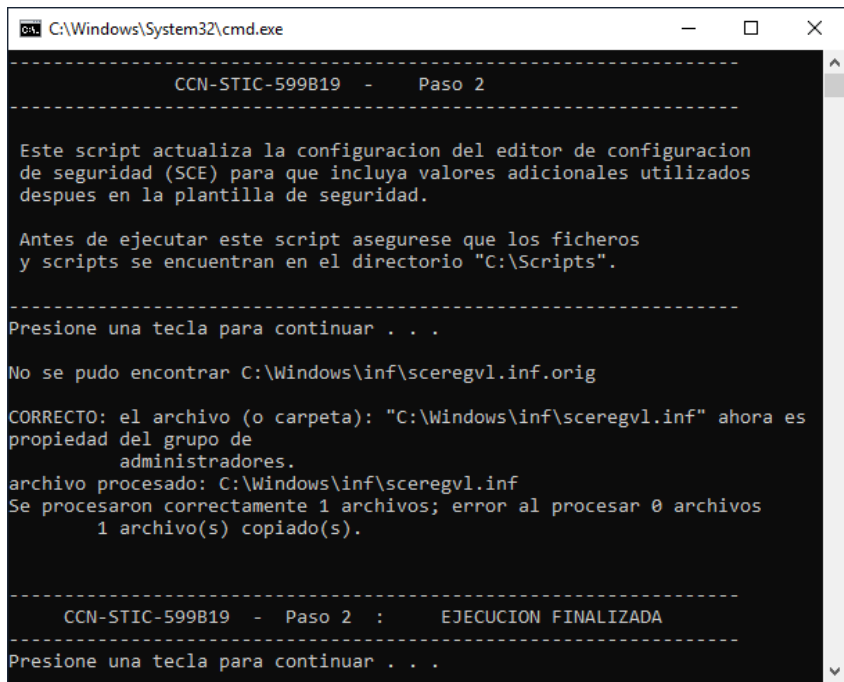
Paso	Descripción
40.	Cree el directorio "Scripts" en la unidad "C:\".
41.	Copie los ficheros asociados a esta guía en el directorio "C:\Scripts". Nota: Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación tendría que editar los scripts para reflejar la nueva ubicación.
42.	Compruebe que en el directorio "C:\Scripts" se encuentran al menos los siguientes directorios y ficheros: – Group Policy (Directorio) – PolicyDefinitions (Directorio) – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.ps1 – CCN-STIC-599B19 Cliente Independiente - Paso 1 - Caracteristicas.bat – CCN-STIC-599B19 Cliente Independiente - Paso 2 - SCE.bat – CCN-STIC-599B19 Cliente Independiente - Paso 3b - IPv6 netbios y otros - PRO.bat – CCN-STIC-599B19 Cliente Independiente - Paso 4 – Plantillas ADMX.bat – CCN-STIC-599B19 Cliente Independiente - Paso 5 – Crea grupos y copia plantilla.bat – CCN-STIC-599B19 Cliente Independiente - Paso 6 – Servicios.bat – CCN-STIC-599B19 Cliente Independiente - Paso 7 – GPO.bat – CCN-STIC-599B19 Cliente Independiente - Paso 8b – Deshabilita Appx - PRO.bat – CCN-STIC-599B19 Cliente Independiente - Paso 9 – Firewall.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10a - Aplica plantilla adicional CONFIDENCIAL.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat – CCN-STIC-599B19 Cliente Independiente - Paso 11 – Aplica plantilla y reinicia.bat – CCN-STIC-599B19 Cliente Independiente.inf – CCN-STIC-599B19 Cliente Independiente.wfw – CCN-STIC-599B19 Importar ADMX.ps1 – CCN-STIC-599B19 Servicios.inf – CCN-STIC-599B19_Deshabilita_NetBIOS_sobre_TCPIP.ps1 – CCN-STIC-599B19_Desinstala_Appx_LTSC.ps1 – CCN-STIC-599B19_Desinstala_Appx_Pro.ps1 – CCN-STIC-599B19_Desinstala_caracteristicas.ps1 – CCN-STIC-599B19_No_IPv6.reg – deshab_appx.reg – drwatson.reg – Plantillas de seguridad.msc – posix.reg – refusereset.reg – scereglv.inf – ssdp.reg – Start_Layout.xml

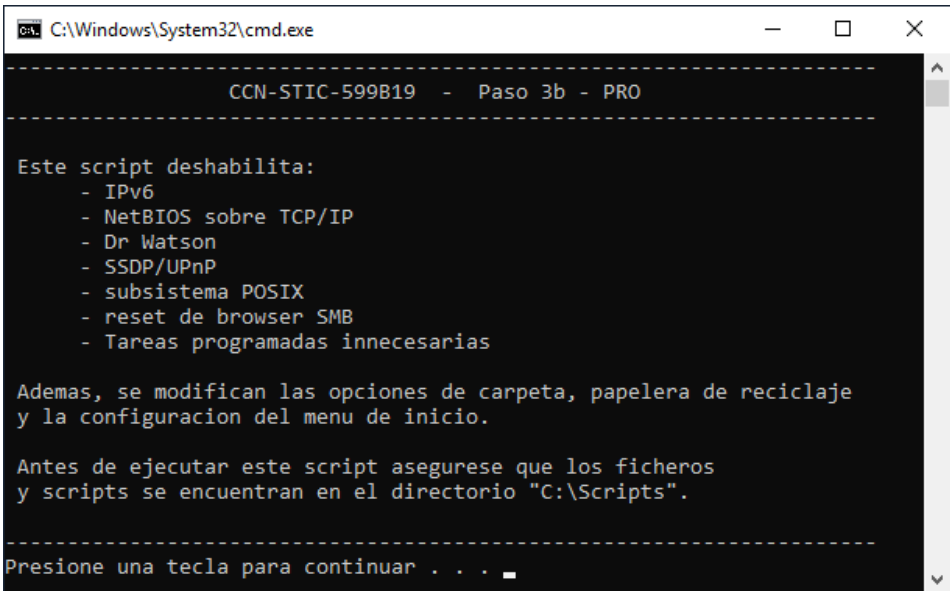
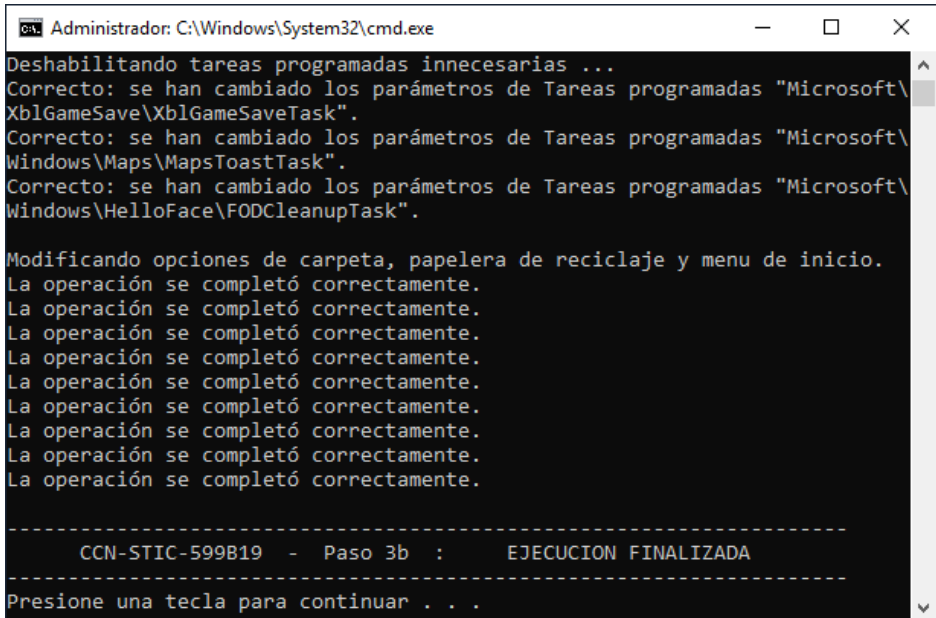
Paso	Descripción
43.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 1 - Características.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario con permisos de administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
44.	Pulse "Sí" en la ventana de "Control de cuentas de usuario". 

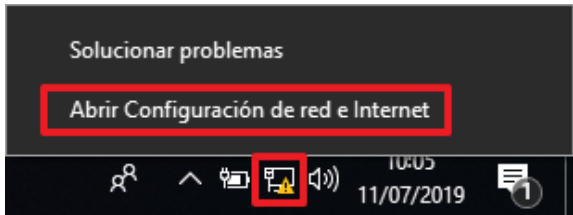
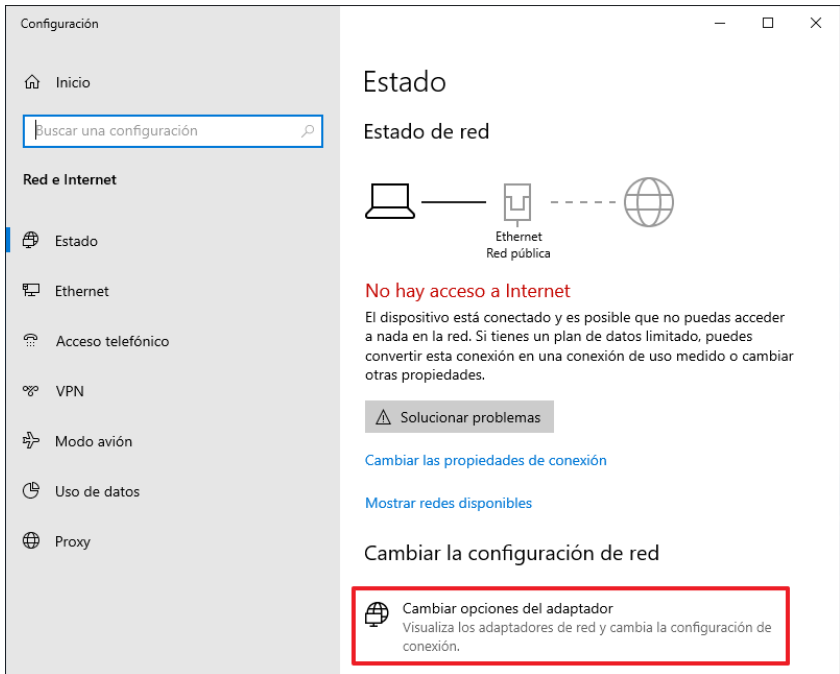
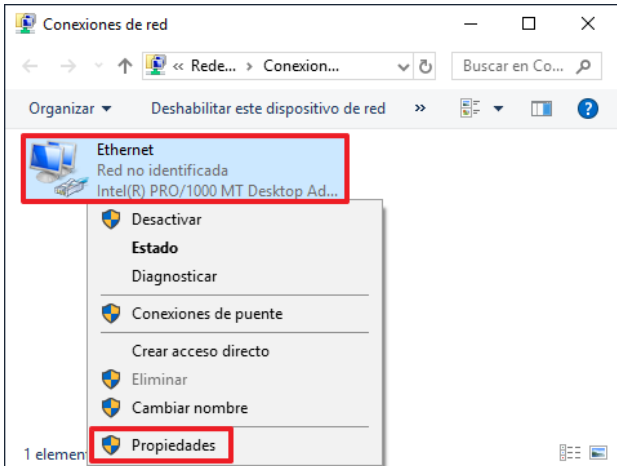
Paso	Descripción
45.	Este script deshabilitará todas las características opcionales que se encuentren habilitadas en el equipo. Pulse una tecla para continuar el proceso. 
46.	El sistema mostrará una lista de las características instaladas que no son necesarias y que deberán ser eliminadas. Pulse una tecla para continuar con el proceso de eliminación de las características.  Nota: Internet Explorer 11 se mantendrá instalada por ser la herramienta autorizada para la navegación. Como se ha indicado anteriormente, la aplicación de la presente guía incluirá también la seguridad de Internet Explorer 11 que aplica la guía CCN-STIC-520.

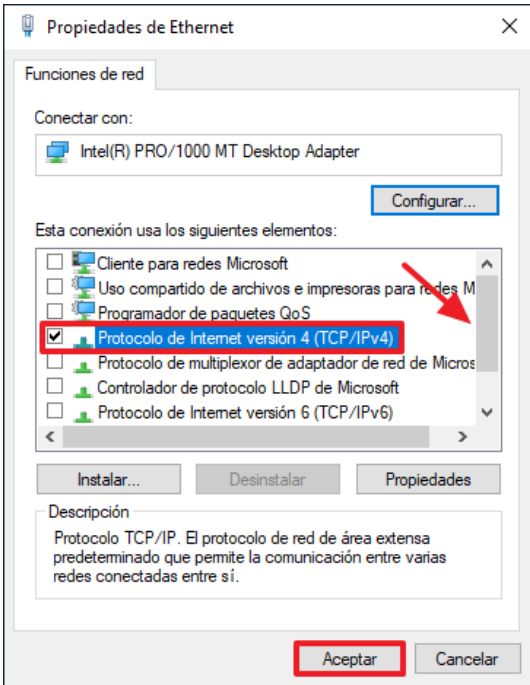
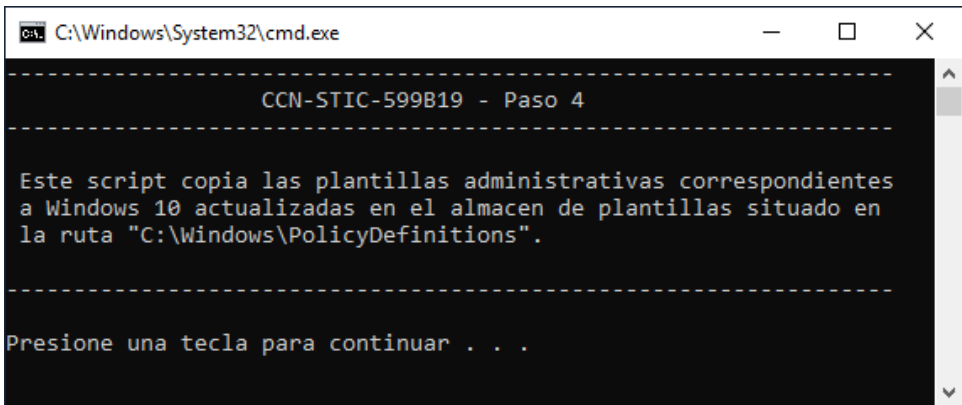


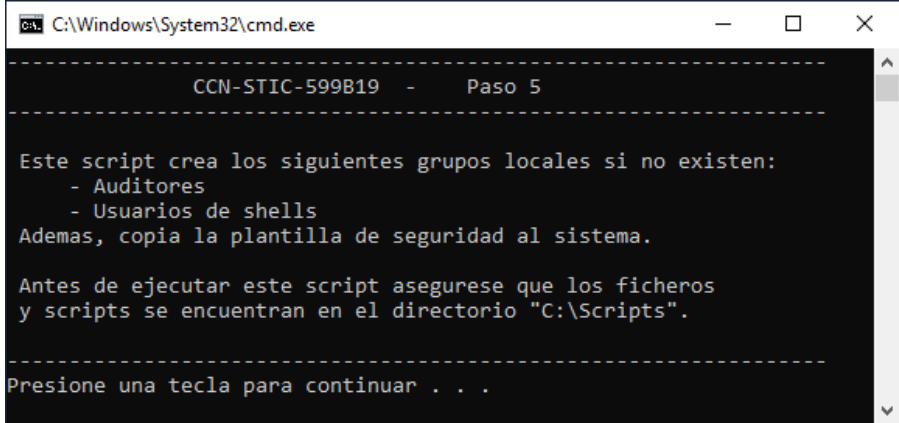
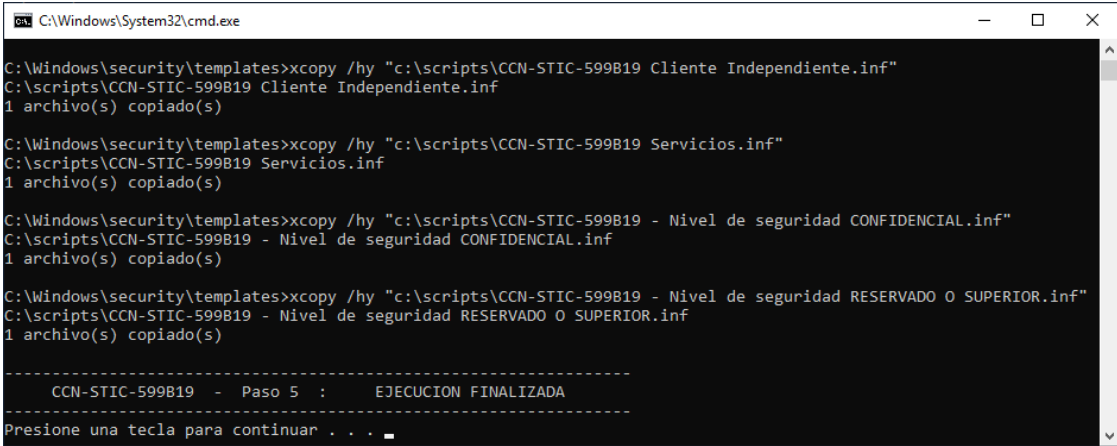
Paso	Descripción
47.	Una vez desinstaladas las características innecesarias compruebe que únicamente se mantienen instaladas las características “Internet-Explorer-Optional-amd64” y “Microsoft-Windows-NetFx4-US-OC-Package”, que son necesarias para la funcionalidad del cliente Windows 10.  Nota: Si apareciese el error “0x800f080c” durante la desinstalación se debe a un error con las dependencias de las características ya desinstaladas. Ignórelo y continúe con el siguiente paso.
48.	Será necesario que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. Al finalizar la ejecución, se reiniciará automáticamente el sistema. Pulse “Cerrar” en el mensaje de confirmación y cuando el sistema se inicie, continúe con el siguiente paso. 

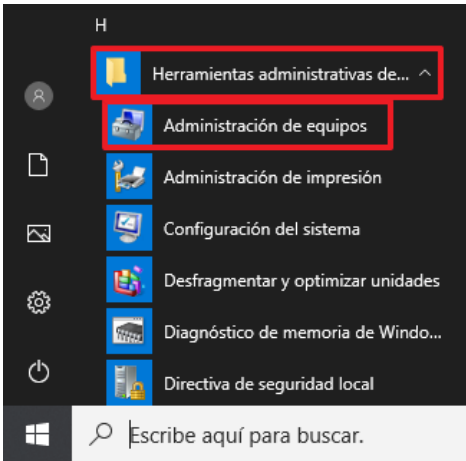
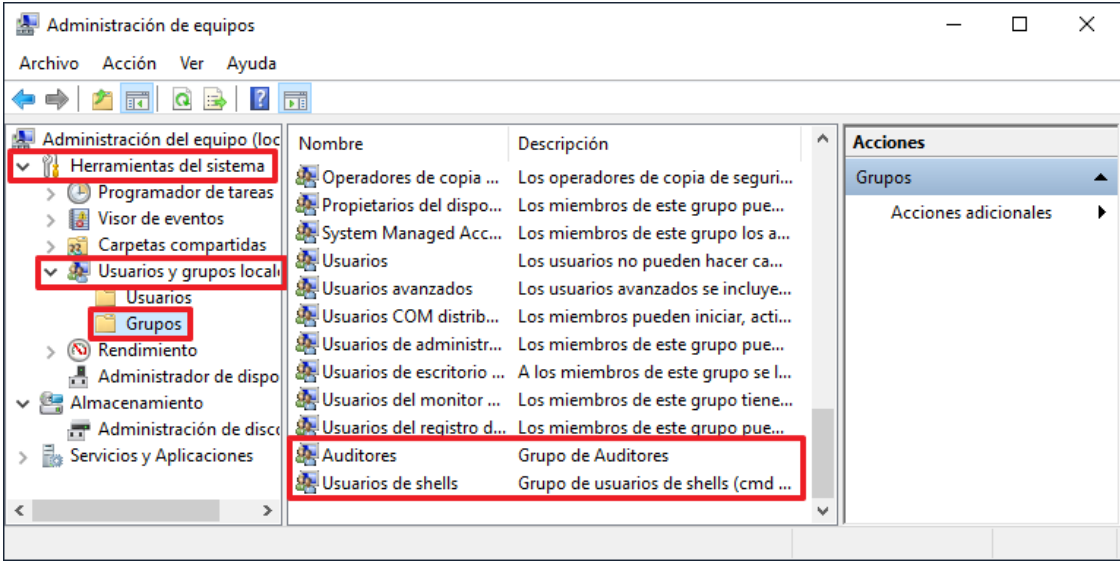
Paso	Descripción
49.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 2 - SCE.bat" situado en la carpeta "C:\Scripts" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: El sistema le solicitará elevación de privilegios.
50.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: Este script actualiza la configuración de SCE (editor de configuración de seguridad) para que incluya valores adicionales. Si aparece el aviso "No se pudo encontrar C:\Windows\inf\sceregl.inf.orig", este aviso se puede ignorar. Sólo se debe a que no se encontró una copia de seguridad anterior del fichero "sceregl.inf". No representa ningún problema y se puede continuar con el siguiente paso.

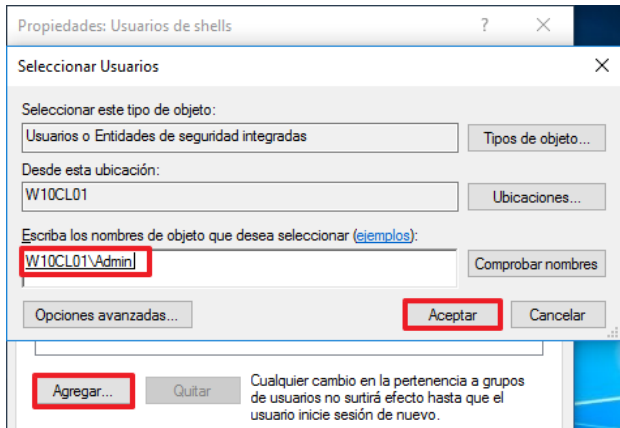
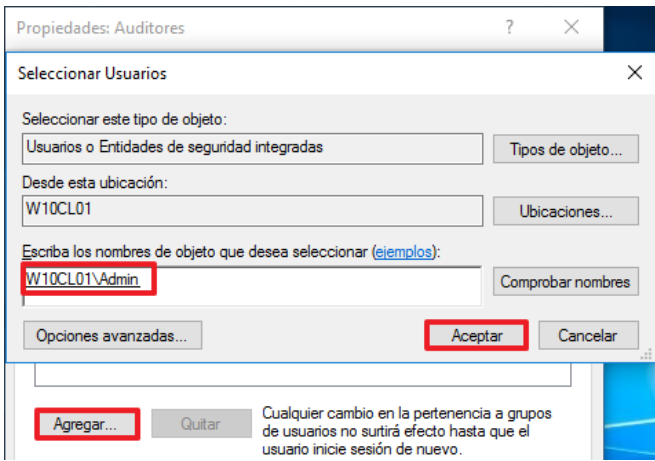
Paso	Descripción
51.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 3b – Ipv6 netbios y otros - PRO.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: El sistema le solicitará elevación de privilegios.
52.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 

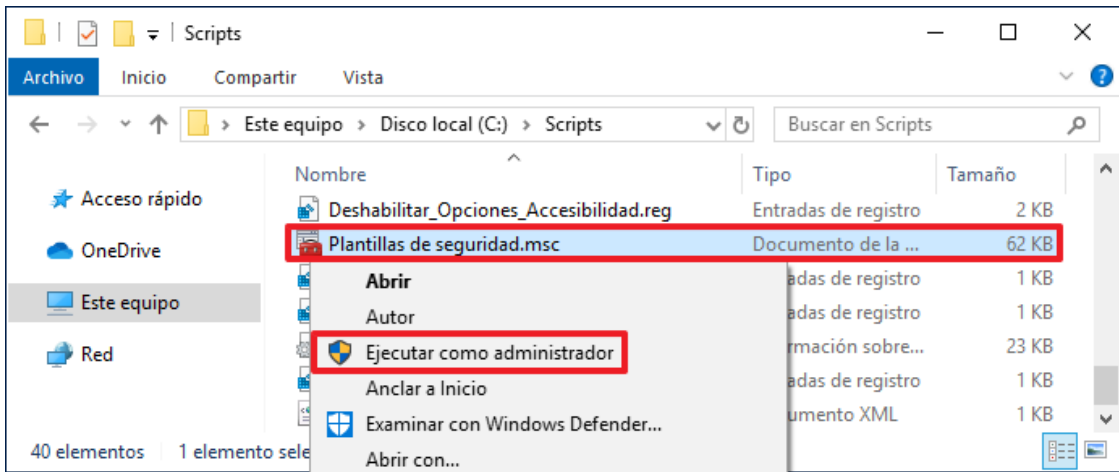
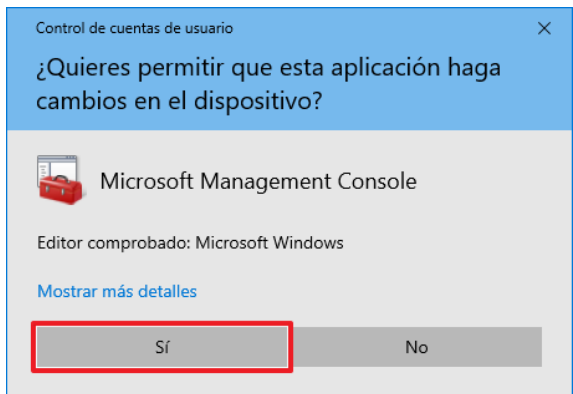
Paso	Descripción
53.	A continuación, en la barra de tareas, localice el icono de conexiones de red y pulsando con el botón derecho sobre él, seleccione “Abrir Configuración de red e Internet”.  Nota: Los pasos que se describen a continuación deberá realizarlos únicamente si dispone de adaptador de red. Si no es el caso, continúe en el punto 58 del presente anexo.
54.	En el menú izquierdo del “Centro de redes y recursos compartidos” pulse sobre “Cambiar configuración del adaptador”. 
55.	Pulse con el botón derecho sobre el adaptador de red y seleccione “Propiedades”. 

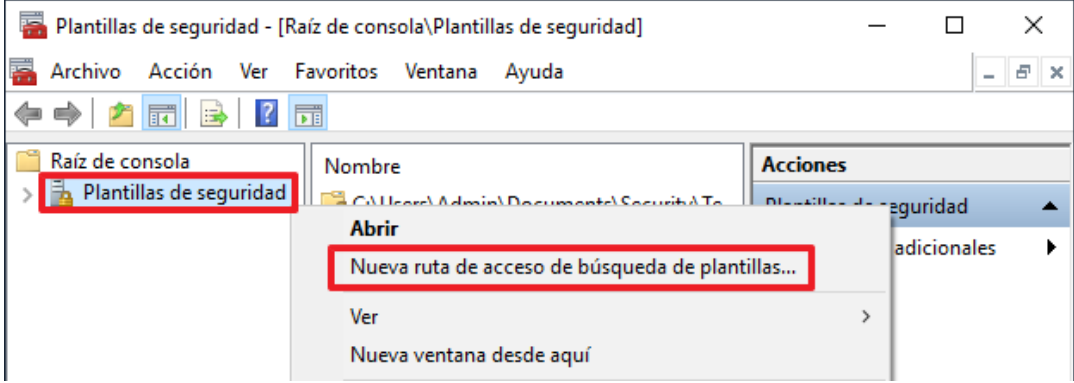
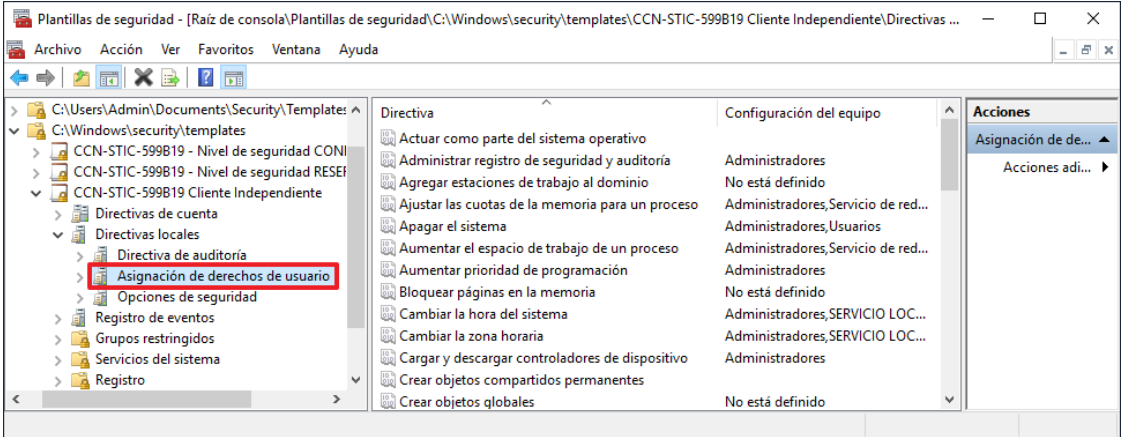
Paso	Descripción
56.	En la ventana "Propiedades de Ethernet" de las diferentes conexiones de red, desmarque si están marcados todos los elementos excepto "Protocolo de Internet versión 4 (TCP/IPv4)" como se muestra en la siguiente figura.  Nota: Recuerde hacer uso de la barra lateral para mostrar y deshabilitar todos los elementos.
57.	Pulse el botón "Aceptar", para cerrar la ventana guardando los cambios.
58.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 4 – Plantillas ADMX.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: El sistema solicitará elevación de privilegios.
59.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar.

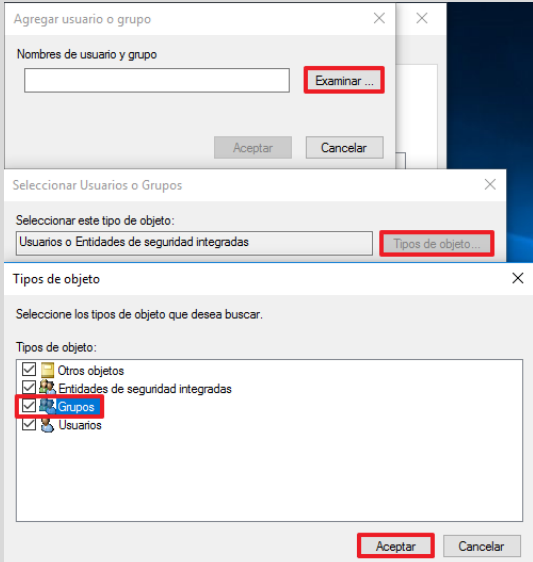
Paso	Descripción
60.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 5 – Crea grupos y copia plantilla.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script crea los grupos locales "Auditores" y "Usuarios de shells" y copia la plantilla de seguridad al sistema, bajo "C:\Windows\Security\Templates", para que pueda ser editada antes de su aplicación, tal y como se describe en los siguientes pasos.  Nota: Si el directorio principal de Windows no se encuentra en "C:\Windows", será necesario modificar el script para reflejar la ubicación correcta.
61.	Pulse una tecla de nuevo para cerrar la ventana de comandos. 

Paso	Descripción
62.	Incluya los usuarios adecuados de su organización en los grupos recién creados, "Auditores" y "Usuarios de shells". En el grupo "Usuarios de shells" deberá incluir al menos el usuario Administrador cuya identidad está utilizando para aplicar esta guía. Se recomienda incluir todos los miembros del grupo "Administradores". Para ello, ejecute la herramienta "Administración de equipos" haciendo clic sobre ella mediante la siguiente ruta: "Inicio → Herramientas administrativas de Windows → Administración de equipos"  Nota: Las plantillas de seguridad no pueden incluir a usuarios y grupos concretos de un dominio particular en los derechos de usuario ni en los permisos asignados a servicios o ficheros, puesto que éstos se incluyen mediante su SID que varía en cada instalación. Por ello, las plantillas de seguridad proporcionadas con estas guías no pueden aplicarse directamente y es necesario que se verifiquen y ajusten antes de su aplicación, para que presenten los valores adecuados.
63.	Una vez abierta la herramienta "Administrador de Equipos", expanda la siguiente rama: "Administración del equipo (local) → Herramientas del sistema → Usuarios y grupos locales → Grupos" 

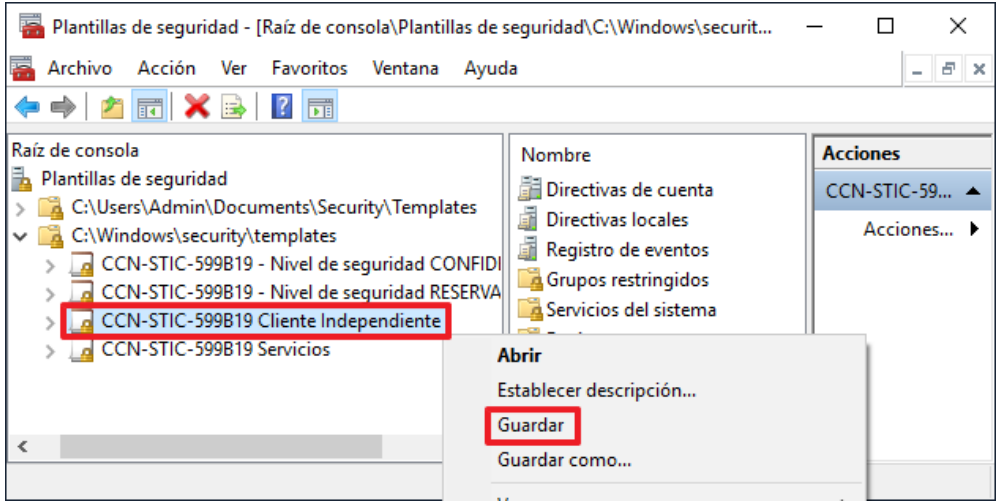
Paso	Descripción
64.	Haga doble clic en el grupo "Usuarios de shells" para mostrar sus propiedades y añada al menos como miembro al usuario administrador que está utilizando para aplicar esta guía. Para ello, pulse sobre el botón "Agregar..." y en la ventana "Seleccionar usuarios" escriba el nombre del usuario a añadir y pulse "Aceptar".  Adicionalmente y del mismo modo descrito, añada al grupo "Usuarios de shells" los demás usuarios que deban pertenecer a él, de acuerdo a las necesidades de su entorno. Los miembros del grupo "Usuarios de shells", y sólo ellos, tendrán permiso para ejecutar las shells del sistema, cmd.exe, powershell.exe y Powershell_ISE.exe. Pulse "Aceptar", de nuevo, para cerrar las propiedades del grupo "Usuarios de shells". Nota: La pertenencia a este grupo da a los usuarios permiso de ejecución sobre los archivos ejecutables (.exe) de ambas shells del sistema. Sin embargo, el acceso a cmd.exe estará restringido además por una directiva de plantillas administrativas, con lo que no podrá ser ejecutado, aunque el usuario pertenezca al grupo "Usuario de shells" mientras la directiva esté activa.
65.	Del mismo modo que en el paso anterior, haga doble clic en el grupo "Auditores" para mostrar sus propiedades y añada los usuarios que deban pertenecer a él de acuerdo a las necesidades de su entorno. Los miembros del grupo Auditores tendrán asignado el derecho "Administrar registro de seguridad y auditoría", lo que les permitirá especificar opciones de auditoría de acceso a objetos como archivos, objetos de Active Directory o claves del registro. 

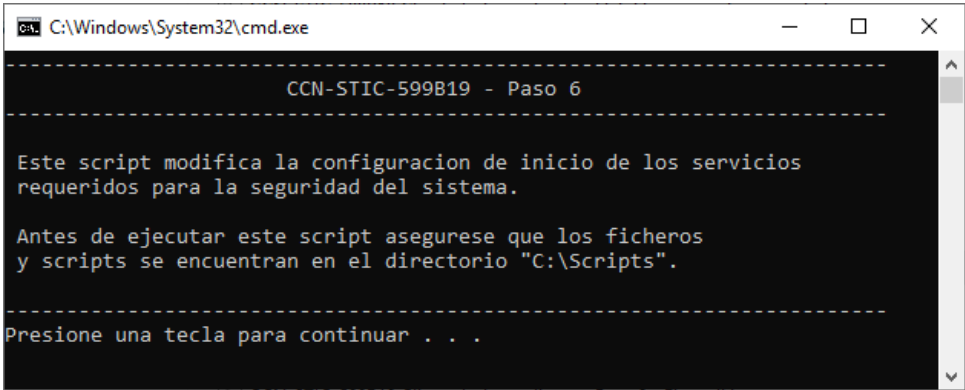
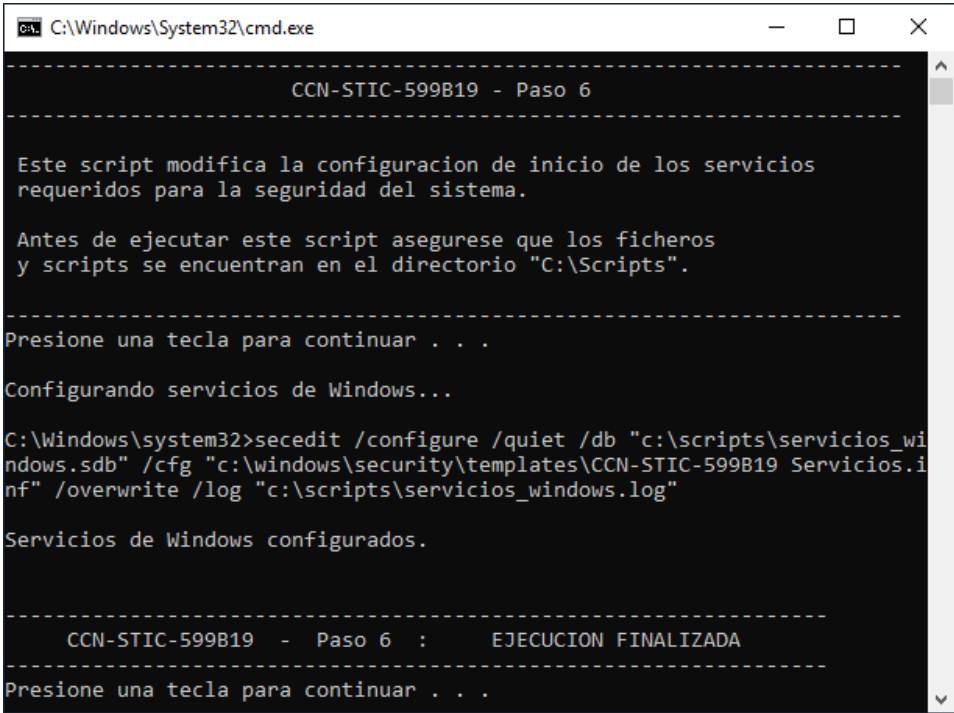
Paso	Descripción
66.	Utilizando el explorador de Windows, compruebe que el fichero "CCN-STIC-599B19 Cliente Independiente.inf" se encuentra en el directorio "C:\Windows\Security\Templates". Si no se encontrase allí, cópielo del directorio "C:\Scripts". Nota: Si el directorio principal de Windows no se encuentra en "C:\Windows", sustituya "C:\Windows" por la ubicación correspondiente.
67.	Edite la plantilla de seguridad "CCN-STIC-599B19 Cliente Independiente.inf" para incluir, en las reglas de asignación de derechos de usuario, los usuarios locales concretos del equipo que está asegurando. Para editar la plantilla ejecute con permisos de administrador (opción "Ejecutar como administrador" del menú contextual al marcarla con el botón derecho del ratón) la consola de administración "Plantillas de seguridad.msc" incluida en el directorio "C:\Scripts". 
68.	Pulse "Sí" cuando el control de cuentas de usuario le solicite elevación de privilegios. 

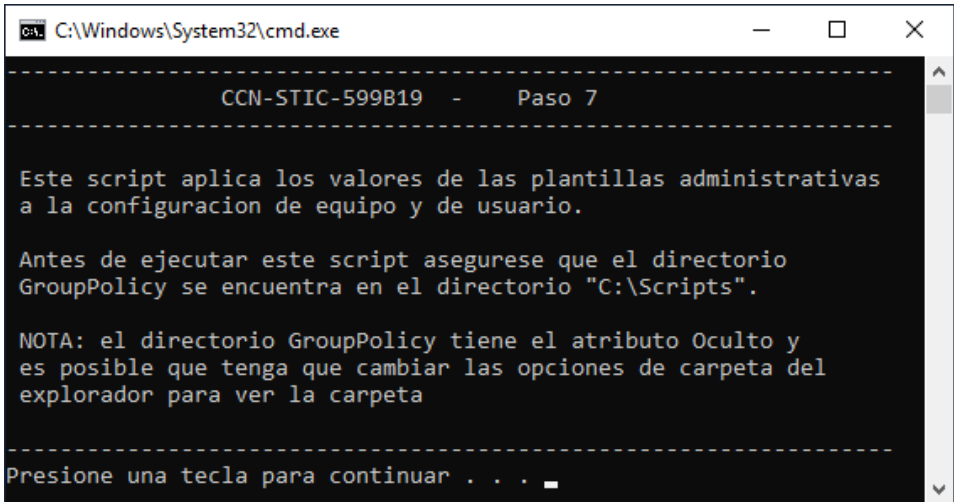
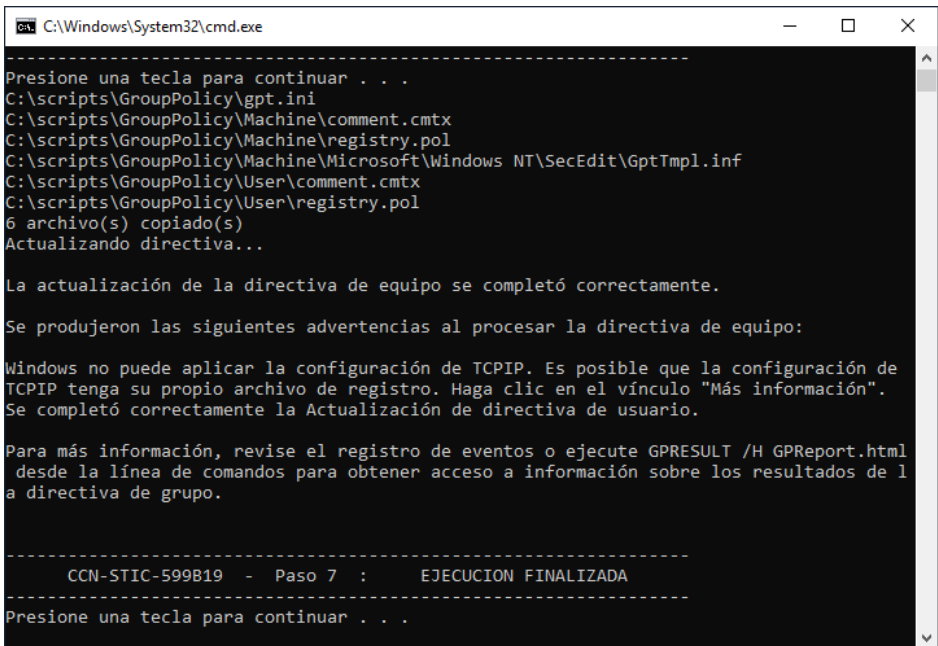
Paso	Descripción
69.	Para que el editor muestre las plantillas situadas en "C:\Windows\Security\Templates" será necesario marcar con el botón derecho el contenedor "Plantillas de seguridad", en la parte izquierda de la ventana, seleccionar la opción "Nueva ruta de acceso de búsqueda de plantillas..." en el menú contextual que aparecerá, y seleccionar entonces la ruta "Equipo\C:\Windows\Security\Templates". 
70.	Expanda entonces la plantilla "CCN-STIC-599B19 Cliente Independiente.inf" y, dentro de ella, seleccione el siguiente contenedor: "Directivas locales → Asignación de derechos de usuarios"  Haciendo doble clic en cada uno de los derechos de usuario correspondientes, deberá editar los derechos de usuario que se muestran a continuación. Estos derechos de usuario tendrán asignados algunos valores, pero deberán editarse para incluir los valores concretos de cuentas de usuarios locales del equipo. Para la edición de los derechos de usuario pulse sobre "Agregar Usuario o grupo..." y añada el usuario o grupo marcado en gris en la tabla que se muestra a continuación mediante el botón "Examinar..." y escribiendo el nombre del objeto correspondiente. Por último, pulse "Aceptar".

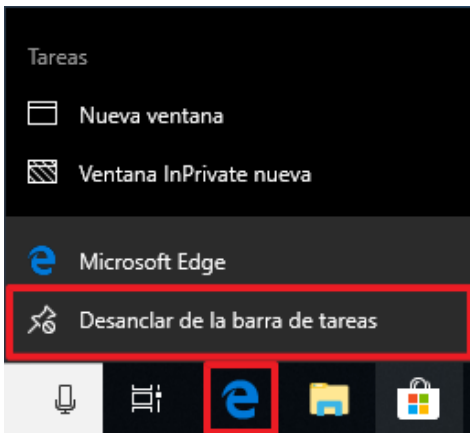
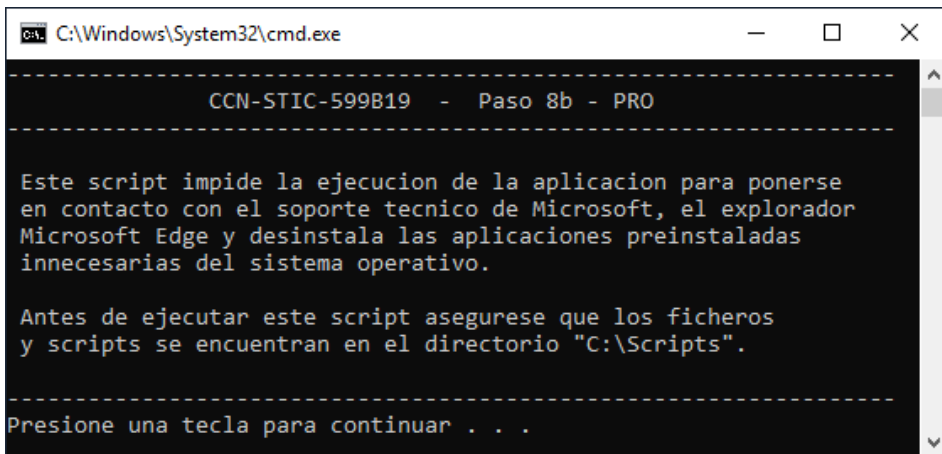
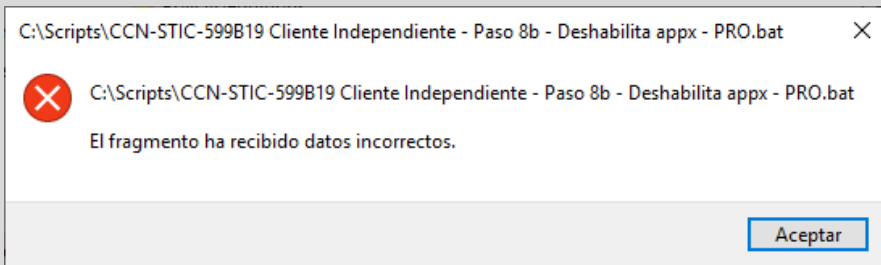
Paso	Descripción		
	Directiva	Valor	Descripción
	Administrar registro de seguridad y auditoría	Auditores, Administradores	Este privilegio permite que un usuario especifique opciones de auditoría de acceso a objetos para recursos individuales como archivos, objetos de Active Directory y claves de registro.
	Denegar el acceso a este equipo desde la red	Invitados, ANONYMOUS LOGON, Administrador	Este permiso determina a qué usuarios se les impide acceder a un ordenador desde la red
	Nota: Si no aparece el grupo Auditores en la lista disponible en el cuadro de diálogo "Seleccionar Usuarios o grupos", marque el botón "Tipos de objeto" y asegúrese de que la entidad "Grupos" está seleccionada, como se muestra en la siguiente figura. 		
71.	Continúe editando la plantilla de seguridad "CCN-STIC-599B19 Cliente Independiente.inf" para incluir, en esta ocasión en la sección "Sistema de archivos", los usuarios locales del equipo. Concretamente se deberán editar los permisos mediante la opción "Modificar seguridad..." y, al pulsar sobre "Agregar...", la operativa será similar a "Agregar grupo o usuario" del paso anterior, tal y como se muestra a continuación. Los permisos de los ficheros tendrán asignados algunos valores, pero deberán editarse para incluir los valores concretos de cuentas de usuarios locales. La tabla muestra el estado definitivo en el que deberán quedar configurados estos permisos, para lo cual deberá añadir las entradas correspondientes de los usuarios o grupos se muestran con fondo gris.		

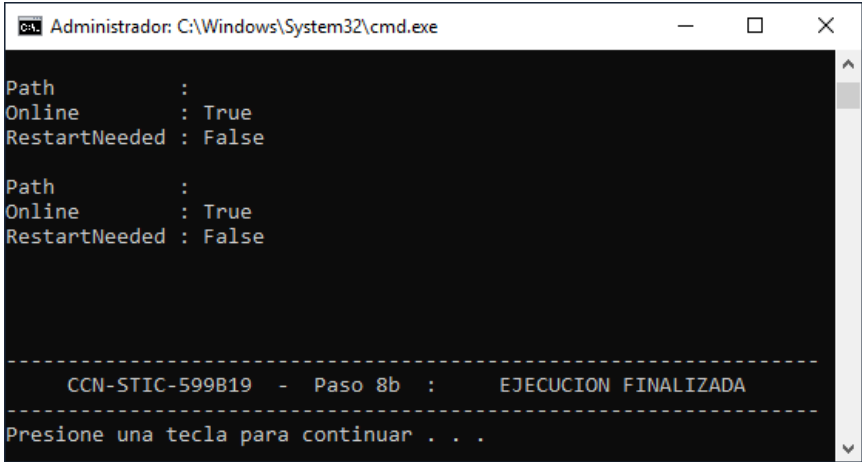
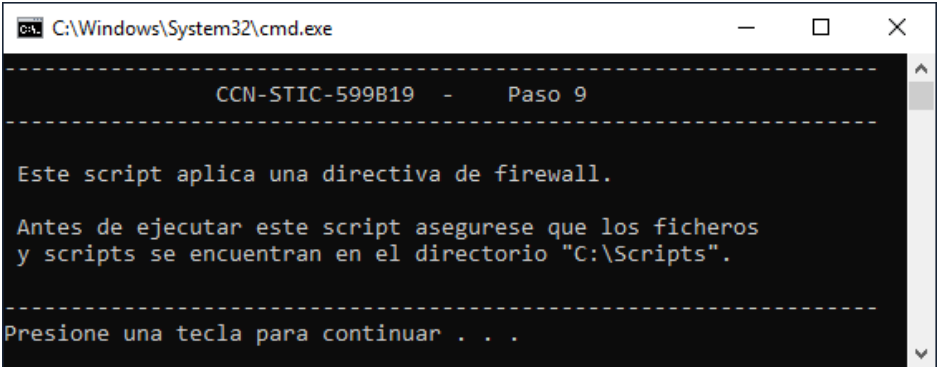
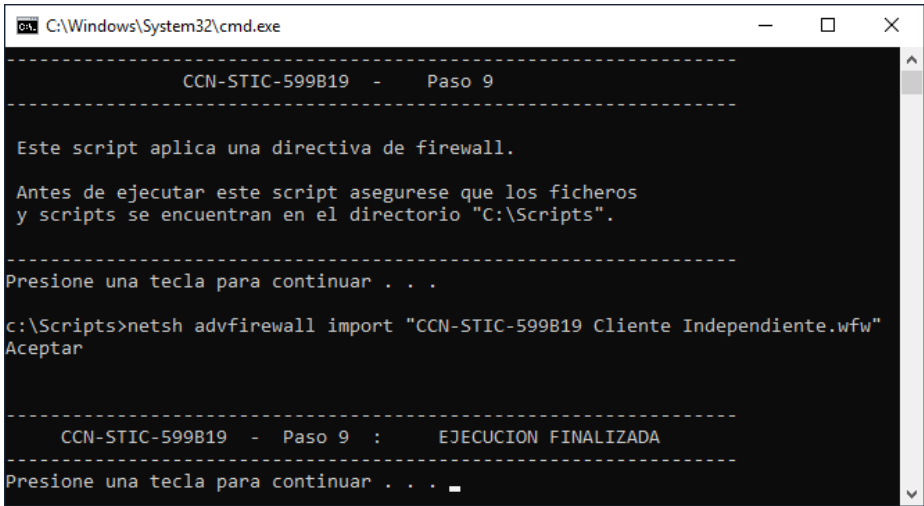
Paso	Descripción																																																	
	Propiedades: %SystemRoot%\system32\cmd.exe Configuración de directiva de seguridad de plantillas %SystemRoot%\system32\cmd.exe ☒ Configurar este archivo o carpeta ☐ Propagar permisos heredables a todas las subcarpetas y archivos ☐ Reemplazar los permisos existentes en archivos con permisos heredables ☐ No conceder permisos de reemplazo en este archivo o carpeta Modificar seguridad... Aceptar Seguridad para %SystemRoot%\system32\cmd.exe Seguridad Nombres de grupos o usuarios: SYSTEM Administradores (W10CL01\Administradores) Agregar... Quitar <table><thead><tr><th>Permisos</th><th>Permitir</th><th>Denegar</th></tr></thead><tbody><tr><td>Control total</td><td>☐</td><td>☐</td></tr><tr><td>Modificar</td><td>☐</td><td>☐</td></tr><tr><td>Leer y ejecutar</td><td>☐</td><td>☐</td></tr><tr><td>Listar el contenido de la carpeta</td><td>☐</td><td>☐</td></tr><tr><td>Leer</td><td>☐</td><td>☐</td></tr></tbody></table> Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas. Opciones avanzadas Aceptar Cancelar Aplicar Una vez seleccionado el usuario o grupo recientemente añadido se podrán marcar los permisos correspondientes. Pulse “Aceptar” una vez añadidos todos los usuarios y/o grupos. <table><thead><tr><th>Archivo o carpeta</th><th>Usuarios/Grupos</th><th>Permisos</th></tr></thead><tbody><tr><td rowspan="3">%SystemRoot%\system32\cmd.exe</td><td>Administradores</td><td>Control Total</td></tr><tr><td>SYSTEM</td><td>Control Total</td></tr><tr><td>Usuarios de shells</td><td>Leer y Ejecutar, Listar el contenido de la carpeta, Leer</td></tr><tr><td rowspan="3">%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe</td><td>Administradores</td><td>Control Total</td></tr><tr><td>SYSTEM</td><td>Control Total</td></tr><tr><td>Usuarios de Shells</td><td>Leer y Ejecutar, Listar el contenido de la carpeta, Leer</td></tr><tr><td rowspan="3">%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ISE.exe</td><td>Administradores</td><td>Control Total</td></tr><tr><td>SYSTEM</td><td>Control Total</td></tr><tr><td>Usuarios de Shells</td><td>Leer y Ejecutar, Listar el contenido de la carpeta, Leer</td></tr><tr><td rowspan="3">%SystemRoot%\SysWOW64\cmd.exe</td><td>Administradores</td><td>Control Total</td></tr><tr><td>SYSTEM</td><td>Control Total</td></tr><tr><td>Usuarios de Shells</td><td>Leer y Ejecutar, Listar el contenido de la carpeta, Leer</td></tr></tbody></table>	Permisos	Permitir	Denegar	Control total	☐	☐	Modificar	☐	☐	Leer y ejecutar	☐	☐	Listar el contenido de la carpeta	☐	☐	Leer	☐	☐	Archivo o carpeta	Usuarios/Grupos	Permisos	%SystemRoot%\system32\cmd.exe	Administradores	Control Total	SYSTEM	Control Total	Usuarios de shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe	Administradores	Control Total	SYSTEM	Control Total	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ISE.exe	Administradores	Control Total	SYSTEM	Control Total	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	%SystemRoot%\SysWOW64\cmd.exe	Administradores	Control Total	SYSTEM	Control Total	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer
Permisos	Permitir	Denegar																																																
Control total	☐	☐																																																
Modificar	☐	☐																																																
Leer y ejecutar	☐	☐																																																
Listar el contenido de la carpeta	☐	☐																																																
Leer	☐	☐																																																
Archivo o carpeta	Usuarios/Grupos	Permisos																																																
%SystemRoot%\system32\cmd.exe	Administradores	Control Total																																																
	SYSTEM	Control Total																																																
	Usuarios de shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																																																
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe	Administradores	Control Total																																																
	SYSTEM	Control Total																																																
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																																																
%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ISE.exe	Administradores	Control Total																																																
	SYSTEM	Control Total																																																
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																																																
%SystemRoot%\SysWOW64\cmd.exe	Administradores	Control Total																																																
	SYSTEM	Control Total																																																
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer																																																

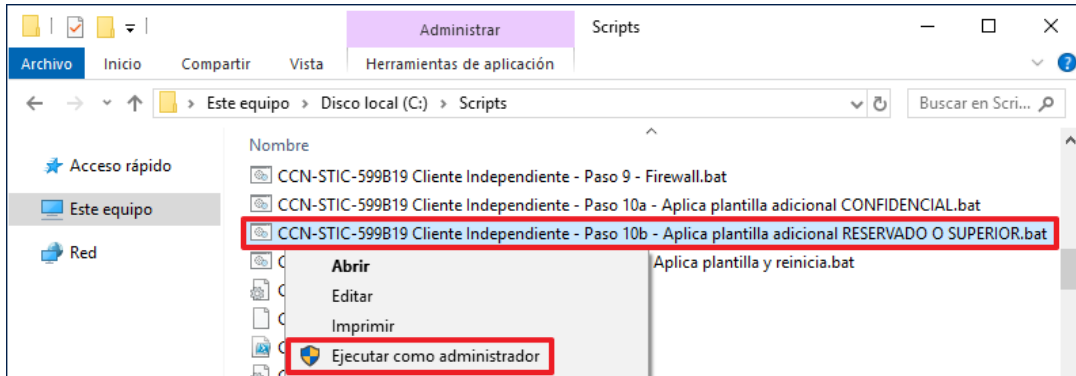
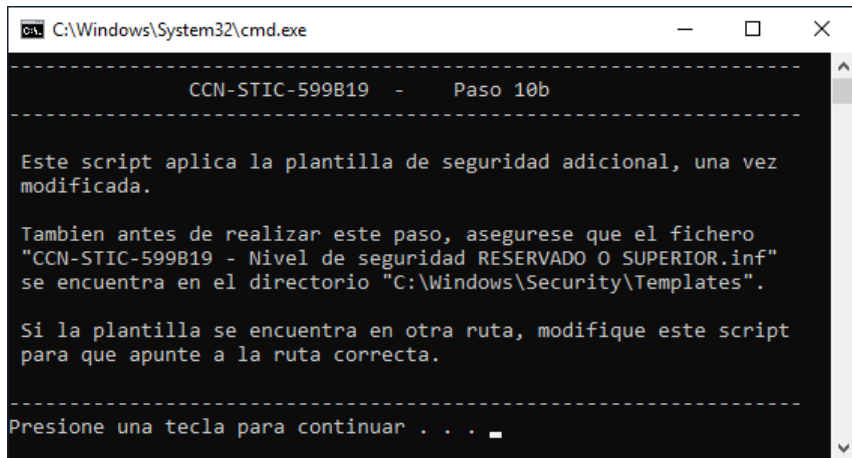
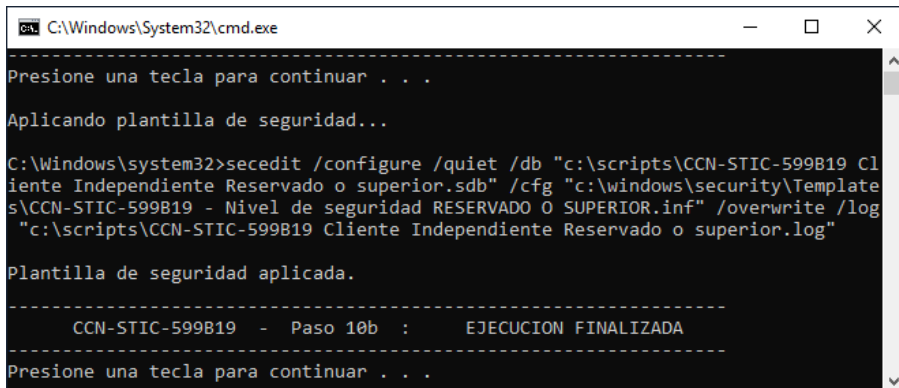
Paso	Descripción		
	Archivo o carpeta	Usuarios/Grupos	Permisos
	%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Administradores	Control Total
		SYSTEM	Control Total
		Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer
	%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell_ISE.exe	Administradores	Control Total
		SYSTEM	Control Total
		Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer
	Sin cerrar el editor de plantillas de seguridad, continúe con el siguiente paso.		
72.	Guarde la plantilla ("C:\Windows\Security\Templates\CCN-STIC-599B19 Cliente Independiente.inf") con las modificaciones realizadas. Para ello utilice la opción "Guardar" del menú contextual que aparece al marcar con el botón derecho del ratón el nombre de la plantilla, como se muestra en la figura.  Una vez salvados los cambios, cierre la consola de edición de plantillas. A la pregunta que aparecerá al cerrarla, "¿Guardar la configuración de la consola en Plantillas de seguridad.msc?", es indiferente que responda Sí o No. La plantilla en este punto habrá quedado lista para ser aplicada, cosa que hará en pasos posteriores.		

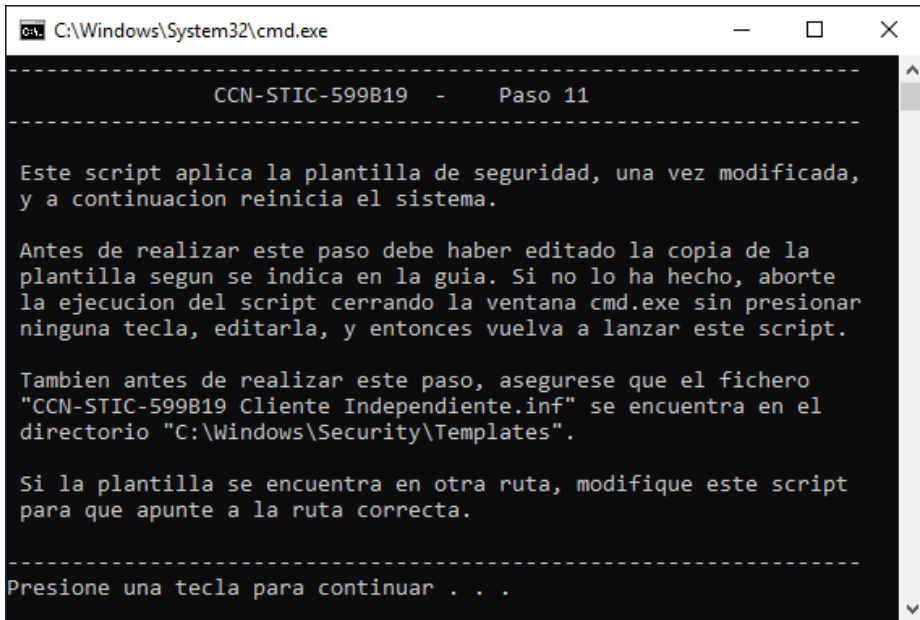
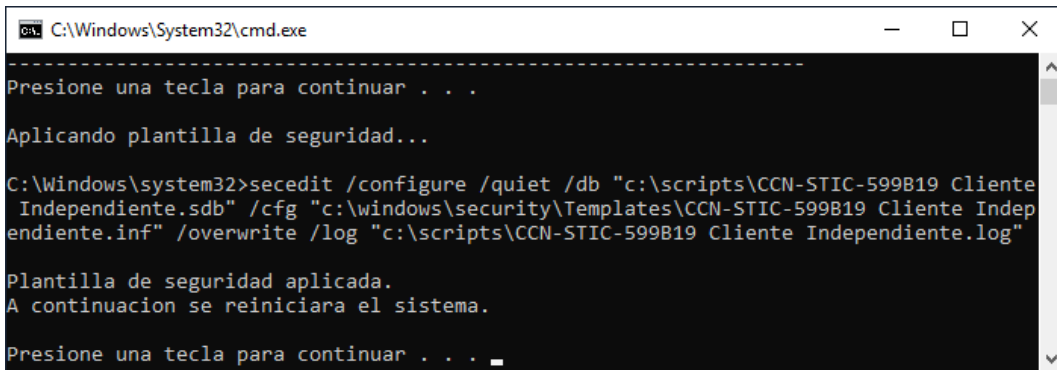
Paso	Descripción
73.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 6 – Servicios.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 
74.	Pulse una tecla de nuevo para cerrar la ventana de comandos.  Nota: Puede comprobar en la carpeta "C:\Scripts" que el proceso se ha realizado correctamente en el fichero de log denominado "servicios_windows.log".

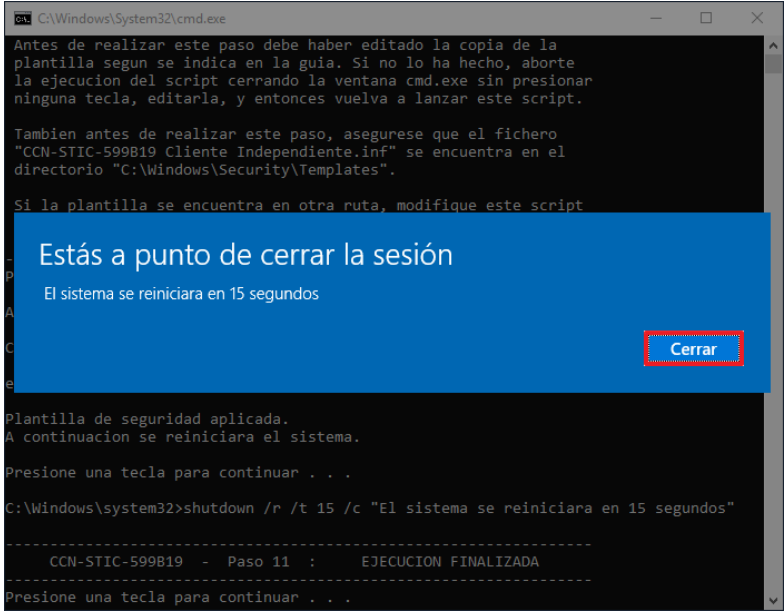
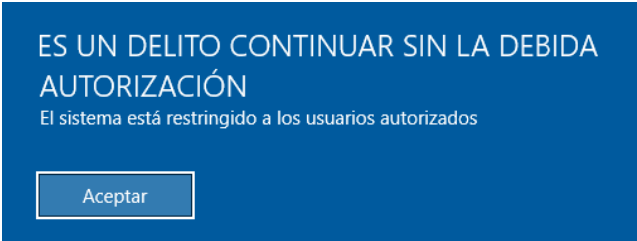
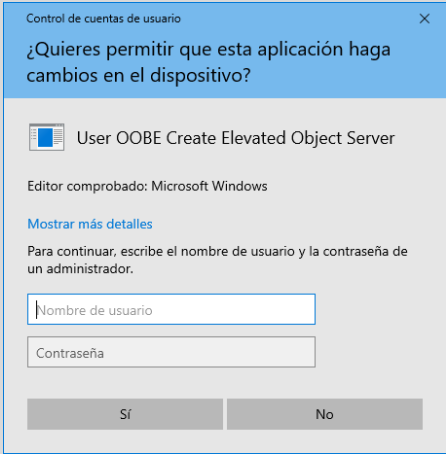
Paso	Descripción
75.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script " CCN-STIC-599B19 Cliente Independiente - Paso 7 – GPO.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script aplica los valores de las plantillas administrativas a la configuración de equipo y usuario, reemplazando la GPO local. 
76.	Pulse una tecla de nuevo para cerrar la ventana de comandos. 

Paso	Descripción
77.	Pulse en el icono de Microsoft Edge con botón derecho en la barra de tareas y seleccione "Desanclar de la barra de tareas". 
78.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 8b – Deshabilita appx - PRO.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilitará las AppX innecesarias y configurará la telemetría.  Nota: Si le aparece el siguiente error, ignórelo y vuelva a ejecutar el paso como administrador. 

Paso	Descripción
79.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 
80.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 9 – Firewall.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script aplicará la configuración del Firewall de Windows con Seguridad Avanzada. 
81.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 

Paso	Descripción
82.	Al igual que anteriormente, ejecute con permisos de administrador, opción “Ejecutar como administrador” el script denominado “CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat”.  Nota: Esta guía ha sido generada en función de la máxima seguridad. Debido a ello se realiza la ejecución de dicho script ya que aplica la máxima seguridad en el equipo. Si desea modificar esta configuración de máxima seguridad consulte el “ANEXO D.2 APLICACIÓN DE NIVELES DE CLASIFICACIÓN”. Consulte además la guía “CCN-STIC-301 Requisitos STIC” para más información.
83.	El control de cuentas le solicitará la elevación de privilegios. Pulse “Sí” para continuar.
84.	Pulse cualquier tecla para comenzar la ejecución del script. 
85.	Pulse de nuevo cualquier tecla para finalizar la ejecución del script. 

Paso	Descripción
86.	Del mismo modo que en pasos anteriores, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Paso 11 – Aplica plantilla y reinicia.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Este script aplicará la configuración de seguridad, asegúrese de que el fichero "CCN-STIC-599B19 Cliente Independiente.inf" se encuentra en el contenedor correspondiente (C:\Windows\Security\Templates).
87.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos.  Nota: Si lo desea, puede comprobar la correcta aplicación de este paso a través del fichero de log denominado "CCN-STIC-599B19 Cliente Independiente.log" que se encuentra en el directorio "C:\Scripts". Es posible que aparezca una nota de advertencia que indica que ésta puede ser ignorada. Aunque aparezca dicha nota, la política ha sido aplicada correctamente.

Paso	Descripción
88.	El equipo reiniciará con la configuración aplicada. 
89.	Una vez reiniciado el sistema y habiendo aplicado la seguridad, pulse “Ctrl+Alt+Supr” para iniciar. Al iniciar sesión aparecerá la leyenda “ES UN DELITO CONTINUAR SIN LA DEBIDA AUTORIZACIÓN. El sistema está restringido a los usuarios autorizados”. Pulse “Aceptar” para continuar y, en este momento podrá introducir las credenciales de inicio de sesión.  Nota: A la hora de crear nuevos usuarios, en el primer inicio de sesión, es posible que el sistema le solicite las credenciales de un usuario administrador para finalizar la configuración inicial. 
90.	Elimine la carpeta “C: \Scripts”.

ANEXO D.1.2. LISTA DE COMPROBACIÓN PASO A PASO

Este apartado se ha diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad de la presente guía.

Se parte de la suposición de que en el equipo que se va a comprobar se ha instalado el sistema operativo Windows 10 Pro/Enterprise sin opción de mantenimiento LTSC (versión 1809), que el equipo es un cliente independiente de un dominio y que en el equipo se ha aplicado la configuración expuesta en la presente guía.

La lista de comprobación deberá ejecutarse iniciando sesión en el equipo con un usuario con permisos de administrador local (miembro del grupo "Administradores"). La cuenta integrada de administrador no podrá usarse porque estará deshabilitada (ver directiva "Cuentas: estado de la cuenta de administrador" en las opciones de seguridad de la plantilla de seguridad).

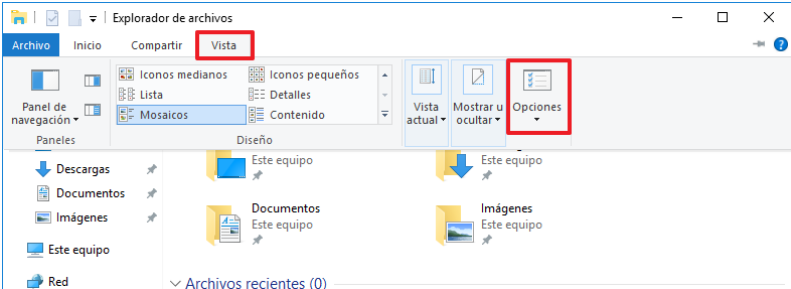
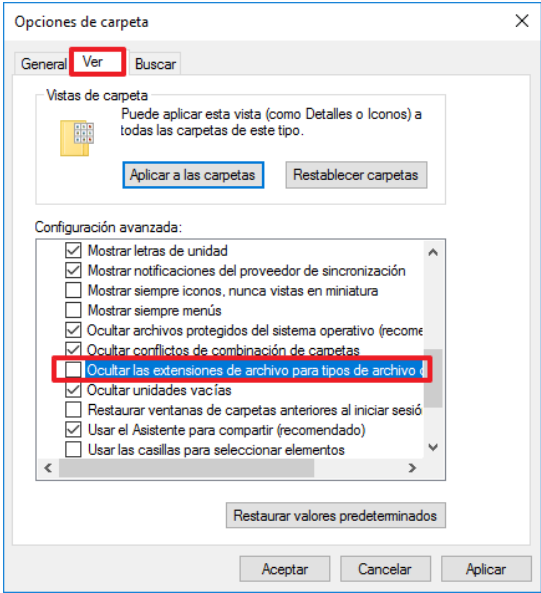
Para realizar algunas de las comprobaciones necesitará ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán son las siguientes:

- a) Explorador de Windows (explorer.exe).
- b) Powershell (powershell.exe)
- c) Editor de objetos directiva de grupo (gpedit.msc).
- d) Varias consolas de administración accesibles desde el panel de control (control.exe)
- e) Consola de administración de Microsoft (mmc.exe)
- f) Editor del registro (regedit.exe)

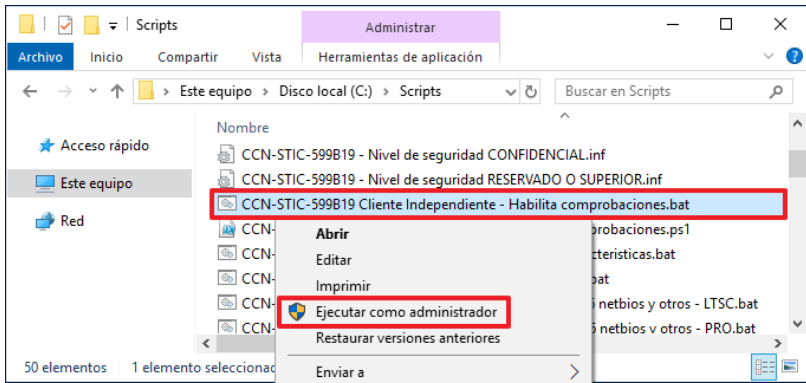
Siguiendo las recomendaciones de seguridad de esta guía, algunas de estas herramientas y consolas de administración estarán inicialmente deshabilitadas en el equipo cliente independiente. Para poder implementar la lista de comprobación será necesario habilitarlas temporalmente. Para ello se suministra junto con esta guía el script "CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat", que deberá ejecutar en uno de los primeros pasos a seguir en la implementación de esta lista de comprobación, tal y como se indica a continuación.

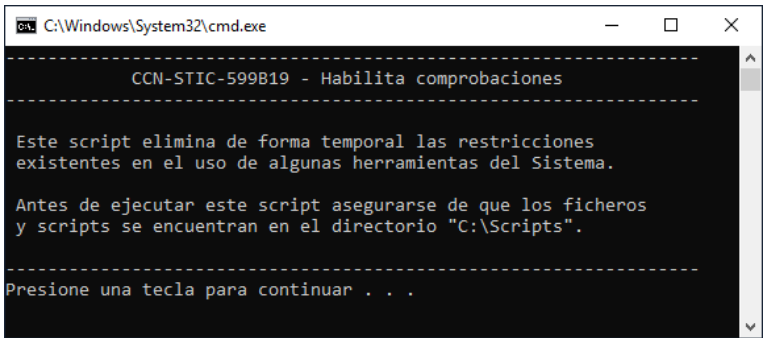
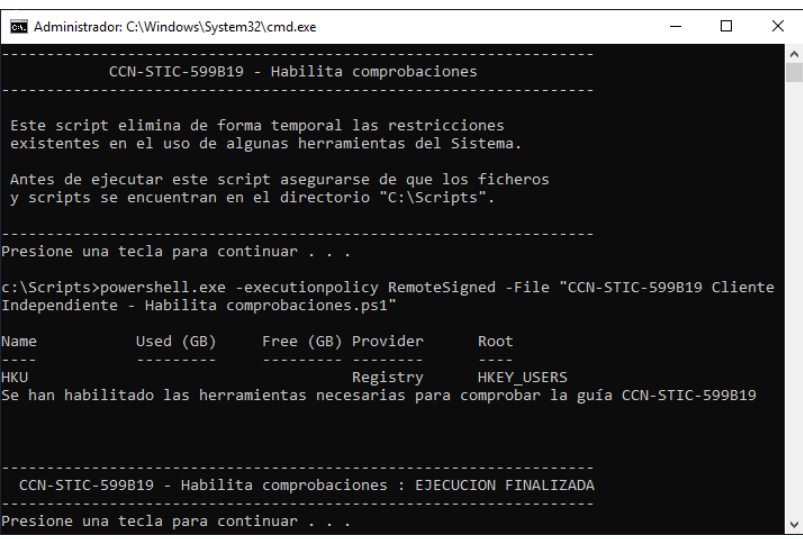
Nota: Tenga en consideración que durante la aplicación de la presente guía se está incluyendo la implementación de seguridad sobre Internet Explorer 11 por lo que será necesario además de verificar las comprobaciones que se indican en este anexo, verificar las comprobaciones de la guía "CCN-STIC-520 Internet Explorer 11".

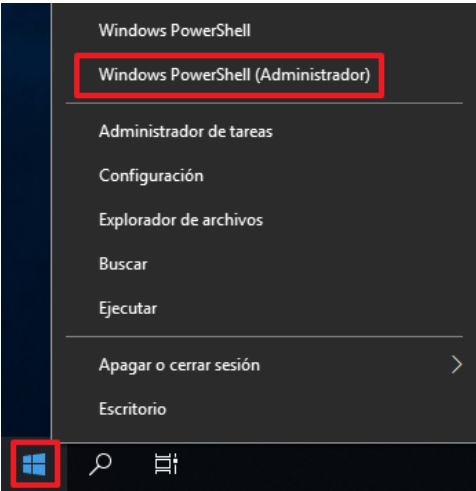
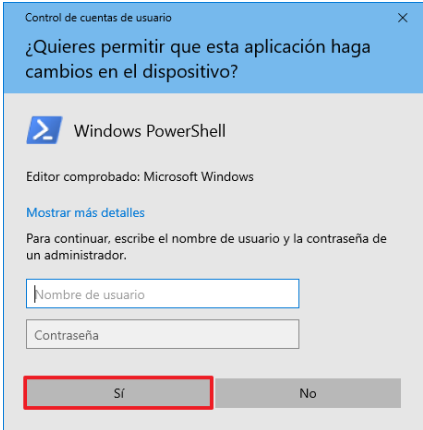
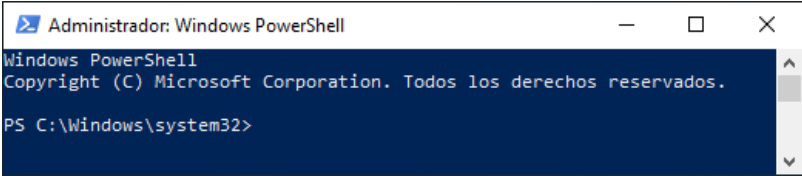
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión con privilegios de administración.		Inicie sesión en el equipo que está comprobando con una cuenta de usuario que pertenezca al grupo local "Administradores" y al grupo local "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.

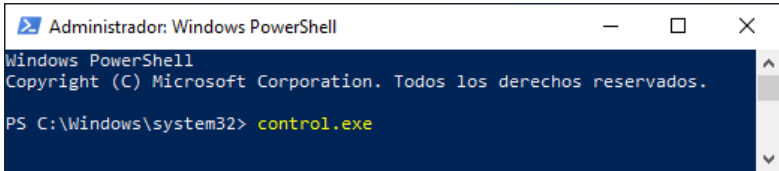
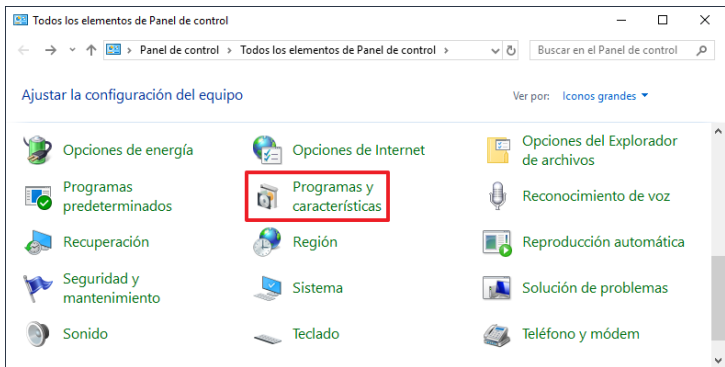
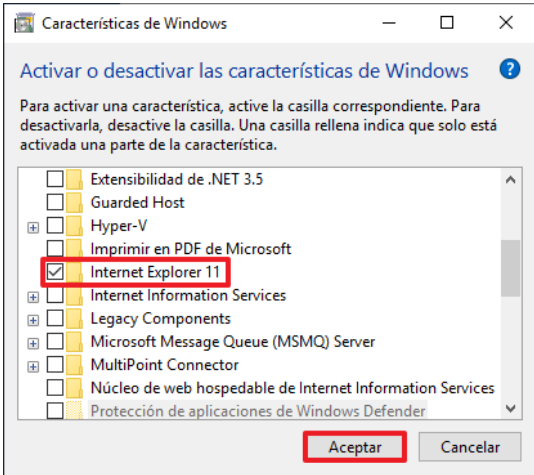
Comprobación	OK/NOK	Cómo hacerlo
2. Configure el Explorador de Windows para que muestre las extensiones de los archivos.		Por defecto Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” sí muestra las extensiones de los archivos. Para configurar “Explorador de Windows” de modo que muestre las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, por ejemplo, desde la siguiente ruta: "Inicio → Explorador de Windows" En el menú superior pulse sobre “Vista” y seleccione “Opciones”.  De la ventana que aparecerá denominada “Opciones de carpeta”, seleccione la pestaña “Ver” y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos” y pulse sobre “Aplicar a las carpetas”, como se muestra en la siguiente figura.  Responda pulsando “Sí” a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse “Aceptar” para cerrar la ventana “Opciones de carpeta”.

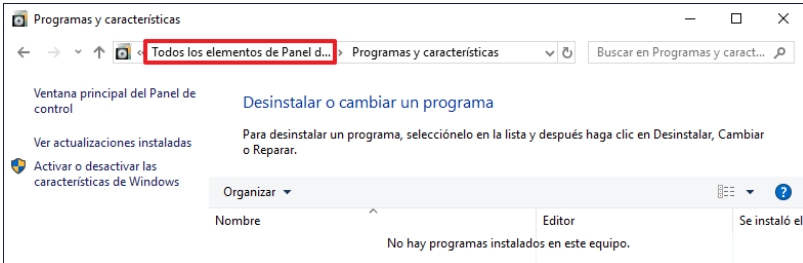
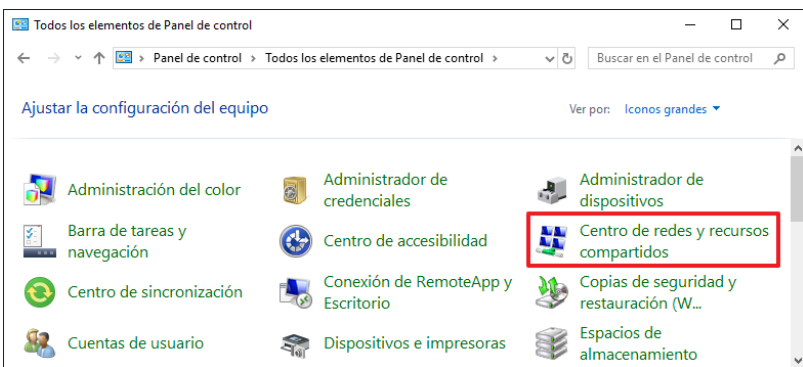
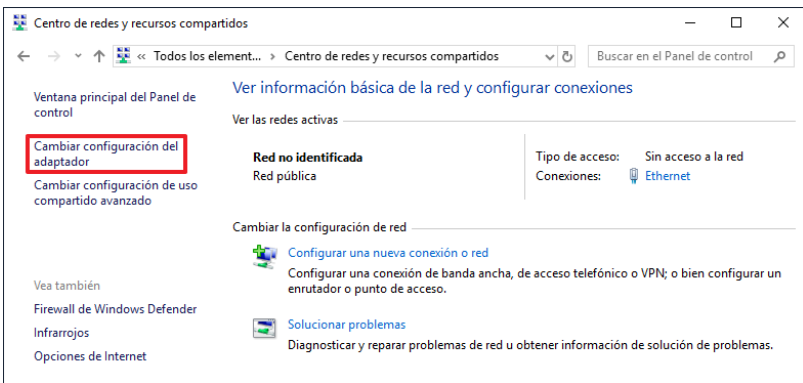
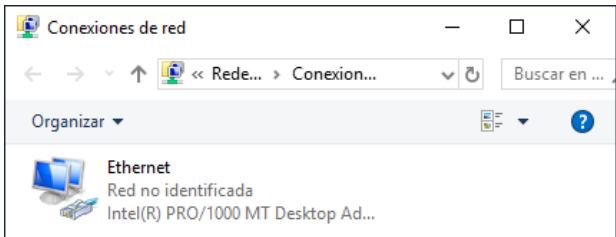


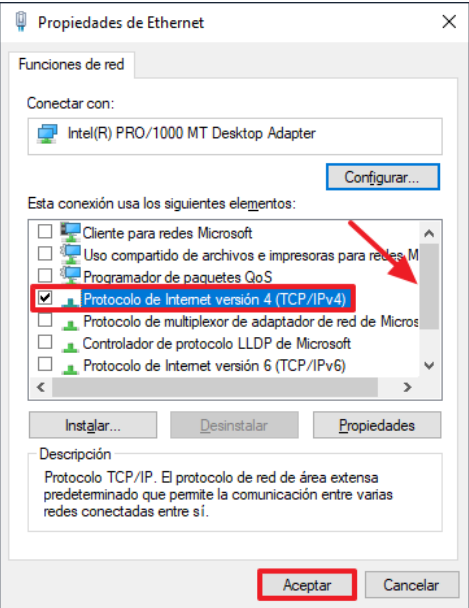
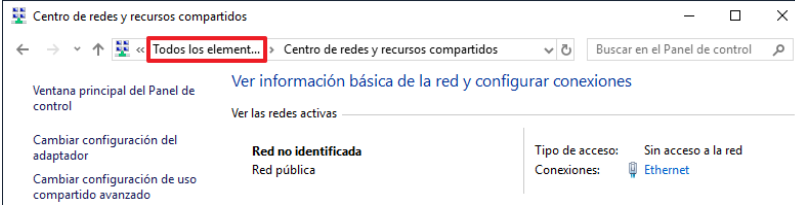
Comprobación	OK/NOK	Cómo hacerlo
3. Cree el directorio "C:\Scripts" y copie en él al menos los ficheros que se indican.		Cree el directorio "scripts" en la unidad "C:" ("C:\Scripts") en el sistema y copie en él al menos los siguientes dos scripts, los cuales están incluidos entre los ficheros que acompañan a esta guía: - CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.bat - CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.ps1 Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19".
4. Ejecute el script que habilita temporalmente las consolas de administración restringidas.		Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual, como se muestra en la siguiente figura. Nota: Aunque la sesión se haya iniciado con un usuario con permisos de administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.  Aparecerá la solicitud de credenciales el escritorio seguro, en el cual deberá introducir las credenciales de un usuario con permisos de administrador y pulse "Sí".

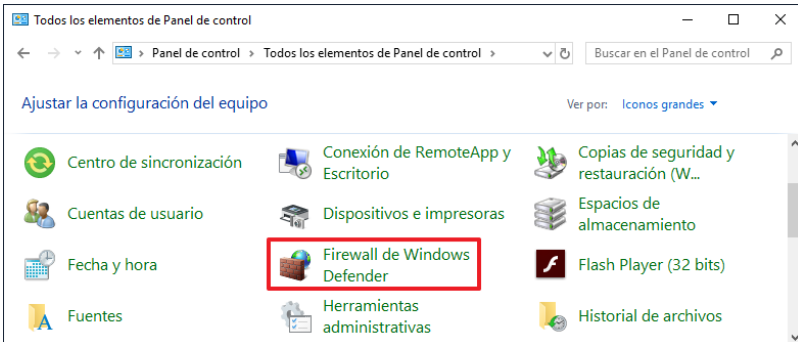
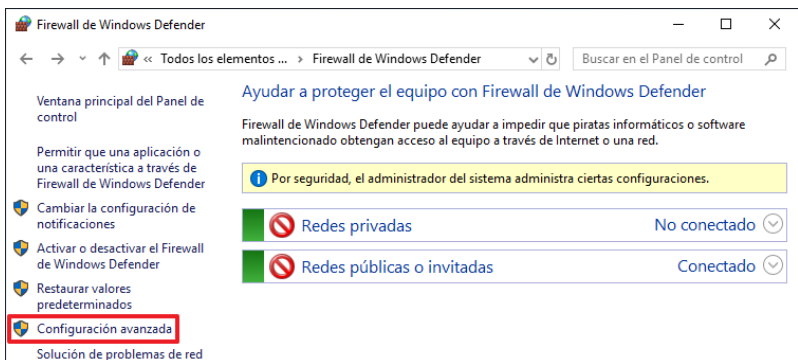
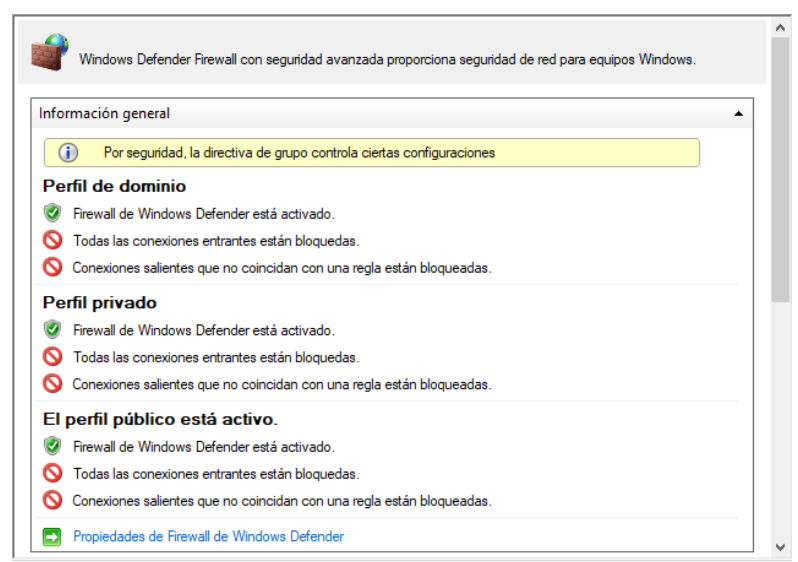
Comprobación	OK/NOK	Cómo hacerlo
5. Habilite temporalmente las consolas de administración restringidas.		Aparecerá una consola de comandos con la ejecución del script. Pulse una tecla para continuar:  Cuando termine la ejecución, pulse una tecla para cerrar la ventana de comandos:  Nota: La próxima vez que se reinicie el sistema o se vuelva a aplicar el objeto de directiva de grupo local las consolas y herramientas volverán a estar deshabilitadas. En caso de que aparezca algún mensaje de error puede ignorarlo y continuar con la comprobación. En caso de que, durante las comprobaciones que se realizarán en el presente anexo, no se pueda realizar alguno de los pasos, esto es debido a que el equipo cliente Windows 10 ha refrescado las políticas locales y, por tanto, se han deshabilitado las comprobaciones. Ante tal eventualidad deberá volver a ejecutar el script “CCN-STIC-599B19 Cliente Independiente- Habilita comprobaciones.bat” del mismo modo en que se describe en los pasos 4 y 5 del presente anexo.

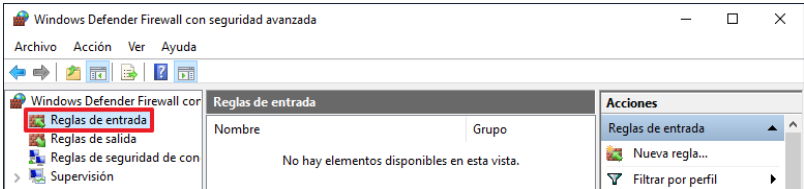
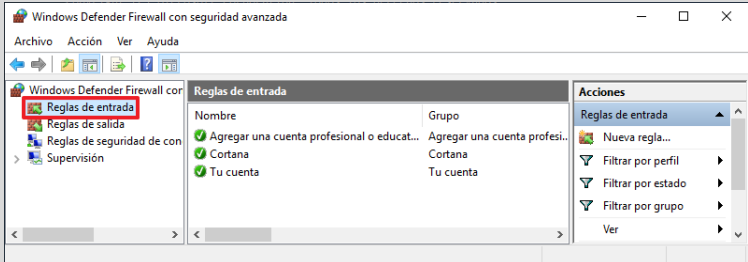
Comprobación	OK/NOK	Cómo hacerlo
6. Lance una ventana de Powershell con permisos de administrador, para lanzar desde ella en pasos posteriores comandos con permisos de administrador.		Haga clic con el botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”.  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.  Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones. 

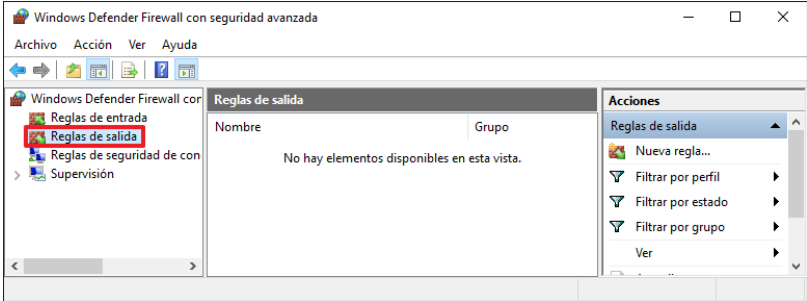
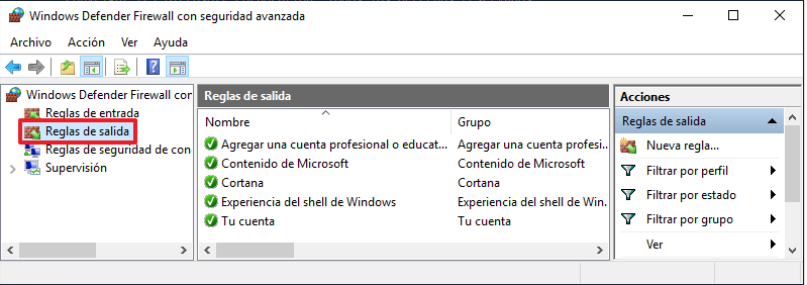
Comprobación	OK/NOK	Cómo hacerlo
7. Compruebe que no hay características opcionales de Windows habilitadas (a excepción de Internet Explorer 11 que deberá estar instalada).		Desde la ventana de Powershell con privilegios de administrador, teclee "control.exe" y pulse "Enter" para abrir el "Panel de Control":  Seleccione la opción "Programas y características":  Dentro de la ventana que aparecerá, seleccione la opción "Activar o desactivar las características de Windows". En la ventana de control de cuentas de usuario, introduzca de nuevo las credenciales de un usuario con permisos de administrador, para acceder a la ventana de Características de Windows:  Compruebe que ninguna característica, excepto Internet Explorer 11, tiene marcada la casilla de selección, lo cual indicaría que dicha característica estaría activa. Todas las características deben estar desactivadas. Una vez comprobado, pulse "Aceptar" para cerrar la ventana.

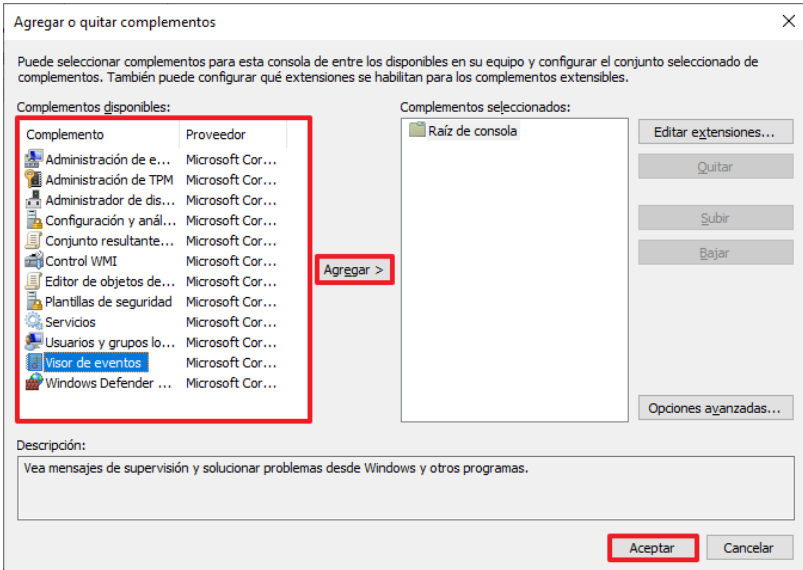
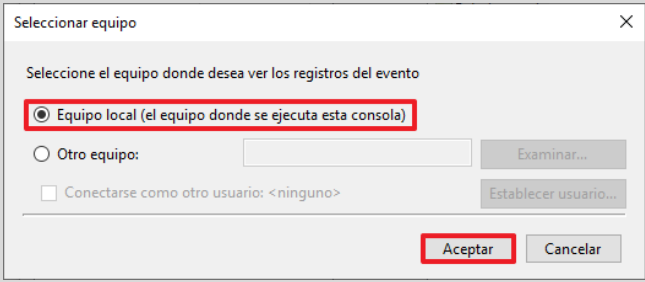
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique los protocolos enlazados a las tarjetas de red.		Vuelva a la pantalla principal del panel de control. Para ello, marque "Todos los elementos de Panel de control" en la barra de navegación superior de la ventana.  Seleccione ahora "Centro de redes y recursos compartidos":  Seleccione "Cambiar configuración del adaptador":  Aparecerá en la ventana del panel de control la lista de tarjetas de red del sistema:  Nota: Deberá realizar esta comprobación únicamente si dispone de tarjetas de red.

Comprobación	OK/NOK	Cómo hacerlo
		Para cada tarjeta de red, marque con el botón derecho del ratón el icono de la tarjeta y seleccione la opción "Propiedades" del menú contextual que aparecerá. Tras introducir las credenciales de un usuario con permisos de administrador de nuevo, aparecerá la ventana de propiedades del adaptador:  Compruebe que el único elemento seleccionado sea "Protocolo de Internet versión 4 (TCP/IPv4)", como se muestra en la figura anterior. Pulse el botón "Cancelar" para cerrar la ventana de propiedades de la interfaz de red. Nota: Recuerde repetir la comprobación para todas las tarjetas de red del equipo.
9. Verifique que ha aplicado la configuración del Firewall de Windows con Seguridad Avanzada.		Vuelva a la pantalla principal del panel de control. Para ello, marque "Todos los elementos de Panel de control" en la barra de navegación superior de la ventana. 

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione “Firewall de Windows” en el “Panel de Control”.  Seleccione “Configuración avanzada”:  Introduzca las credenciales de un usuario con permisos de administrador en el “Control de Cuentas de Usuario” y, a continuación, aparecerá una ventana con la configuración del firewall de Windows con seguridad avanzada:  Compruebe que los valores coinciden con la tabla siguiente.

Comprobación	OK/NOK	Cómo hacerlo																											
		<table> <tr> <th colspan="2">Parámetro</th><th>OK/NOK</th></tr> <tr> <td colspan="2">Por seguridad, la directiva de grupo controla ciertas configuraciones</td><td></td></tr> <tr> <td rowspan="3">Perfil de dominio</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Todas las conexiones entrantes están bloqueadas</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla están bloqueadas</td><td></td></tr> <tr> <td rowspan="3">Perfil privado</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Todas las conexiones entrantes están bloqueadas</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla están bloqueadas</td><td></td></tr> <tr> <td rowspan="3">Perfil público</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Todas las conexiones entrantes están bloqueadas</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla están bloqueadas</td><td></td></tr> </table>	Parámetro		OK/NOK	Por seguridad, la directiva de grupo controla ciertas configuraciones			Perfil de dominio	Firewall de Windows está activado.		Todas las conexiones entrantes están bloqueadas		Conexiones salientes que no coincidan con una regla están bloqueadas		Perfil privado	Firewall de Windows está activado.		Todas las conexiones entrantes están bloqueadas		Conexiones salientes que no coincidan con una regla están bloqueadas		Perfil público	Firewall de Windows está activado.		Todas las conexiones entrantes están bloqueadas		Conexiones salientes que no coincidan con una regla están bloqueadas	
Parámetro		OK/NOK																											
Por seguridad, la directiva de grupo controla ciertas configuraciones																													
Perfil de dominio	Firewall de Windows está activado.																												
	Todas las conexiones entrantes están bloqueadas																												
	Conexiones salientes que no coincidan con una regla están bloqueadas																												
Perfil privado	Firewall de Windows está activado.																												
	Todas las conexiones entrantes están bloqueadas																												
	Conexiones salientes que no coincidan con una regla están bloqueadas																												
Perfil público	Firewall de Windows está activado.																												
	Todas las conexiones entrantes están bloqueadas																												
	Conexiones salientes que no coincidan con una regla están bloqueadas																												
10. Compruebe las reglas de entrada del firewall de Windows con seguridad avanzada.		En la ventana del Firewall de Windows con seguridad avanzada, seleccione el contenedor siguiente: “Firewall de Windows con seguridad avanzada → Reglas de entrada”  Compruebe que en la parte central de la ventana aparece el mensaje "No hay elementos disponibles en esta vista", como en el siguiente ejemplo. Esto significa que no hay ninguna regla de entrada configurada. Nota: Es posible que aparezcan reglas predeterminadas en el sistema. Esto es debido a que la ejecución del script “CCN-STIC-599B19 Cliente Independiente - Paso 9 - Firewall.bat” se realizó con un usuario distinto al que se está revisando este paso. Si es así, vuelva a lanzar dicho script con privilegios de administrador para eliminar las reglas predeterminadas que aparecen. 																											

Comprobación	OK/NOK	Cómo hacerlo
11.Compruebe las reglas de salida del firewall de Windows con seguridad avanzada.		En la ventana del Firewall de Windows con seguridad avanzada, seleccione el contenedor siguiente: “Firewall de Windows con seguridad avanzada → Reglas de salida”  Compruebe que en la parte central de la ventana aparece el mensaje "No hay elementos disponibles en esta vista", como en el siguiente ejemplo. Esto significa que no hay ninguna regla de entrada configurada. Nota: Es posible que aparezcan reglas predeterminadas en el sistema. Esto es debido a que la ejecución del script “CCN-STIC-599B19 Cliente Independiente - Paso 9 - Firewall.bat” se realizó con un usuario distinto al que se está revisando este paso. Si es así, vuelva a lanzar dicho script con privilegios de administrador para eliminar las reglas predeterminadas que aparecen. 

Comprobación	OK/NOK	Cómo hacerlo
12. Ejecute la herramienta "Consola de administración de Microsoft (mmc.exe)" para poder realizar las comprobaciones de los siguientes pasos.		Desde la ventana de PowerShell abierta anteriormente, ejecute "mmc.exe". A continuación, seleccione "Archivo → Agregar o quitar complemento..." y utilice esta combinación para agregar los "Complementos disponibles:", y que son requeridos en los siguientes pasos utilizando el botón, "Agregar >" y pulsando "Aceptar" para agregar el complemento.  Nota: Tenga en consideración que algunos de los elementos agregados tendrán que ser referidos al equipo local. 
13. Agregue el complemento a la consola.		Agregue el "Visor de eventos" (Equipo local) desde la ventana "Complementos disponibles" tal y como se explica en el paso anterior.
14. Verifique la configuración del registro de eventos de Aplicación.		Pulse el botón derecho del ratón sobre el contenedor "Aplicación", que se encuentra en la ruta siguiente: "Visor de eventos → Registros de Windows → Aplicación" Seleccione la opción "Propiedades" del menú contextual que aparecerá a su derecha y compruebe que los valores configurados coinciden con los siguientes:

Comprobación	OK/NOK	Cómo hacerlo		
		Parámetro	Valor	OK/NOK
		Tamaño máximo del registro (KB)	32768	
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)	
15.Verifique la configuración del registro de eventos de Seguridad.		Pulse el botón derecho del ratón sobre el contenedor "Seguridad", que se encuentra en la ruta siguiente: "Visor de eventos → Registros de Windows → Seguridad" Seleccione la opción "Propiedades" del menú contextual que aparecerá y compruebe que los valores configurados coinciden con los siguientes:		
		Parámetro	Valor	OK/NOK
		Tamaño máximo del registro (KB)	163840	
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)	
16.Verifique la configuración del registro de eventos de Sistema.		Pulse el botón derecho del ratón sobre el contenedor "Sistema", que se encuentra en la ruta siguiente: "Visor de eventos → Registros de Windows → Sistema" Seleccione la opción "Propiedades" del menú contextual que aparecerá y compruebe que los valores configurados coinciden con los siguientes:		
		Parámetro	Valor	OK/NOK
		Tamaño máximo del registro (KB)	32768	
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)	
17.Agregue el complemento a la consola.		Agregue la herramienta "Usuarios y grupos locales" (Equipo local) desde la ventana "Complementos disponibles" tal y como se explica en el paso 12.		
18.Verifique que los grupos "Usuarios avanzados" y "Usuarios de escritorio remoto" están vacíos.		Sitúese sobre el contenedor "Grupos", que se encuentra en la ruta siguiente: "Usuarios y grupos locales → Grupos" Compruebe que los siguientes grupos no tienen miembros, haciendo doble clic sobre ellos y observando la lista de miembros que aparecerá:		

Comprobación	OK/NOK	Cómo hacerlo																			
	Grupos		OK/NOK																		
	Usuarios avanzados																				
	Usuarios de escritorio remoto																				
19.Verifique que los grupos "Auditores" y "Usuarios de shells" están creados.		Sitúese sobre el contenedor “Grupos”, que se encuentra en la ruta siguiente: "Usuarios y grupos locales → Grupos" Compruebe que los siguientes grupos aparecen en la lista.																			
	Grupos		OK/NOK																		
	Auditores																				
	Usuarios de shells																				
20.Verifique el resto de grupos.		Adicionalmente, haga doble clic en el resto de los grupos y compruebe que sus miembros corresponden con los usuarios adecuados para su entorno.																			
21.Verifique que se han renombrado los usuarios locales Administrador e Invitado.		Sitúese sobre el contenedor “Usuarios”, que se encuentra en la ruta siguiente: "Usuarios y grupos locales → Usuarios" Compruebe que aparecen los siguientes usuarios y que el icono lleva una flecha indicando que están deshabilitadas como en la siguiente figura.																			
	<table><tr><th>Nombre</th><th>Nombre com...</th><th>Descripción</th></tr><tr><td> aCdCmN599</td><td></td><td>Cuenta integrada para la administración del eq...</td></tr><tr><td> Admin</td><td></td><td></td></tr><tr><td> DefaultAccount</td><td></td><td>Cuenta de usuario administrada por el sistema.</td></tr><tr><td> IcNcVn599</td><td></td><td>Cuenta integrada para el acceso como invitado ...</td></tr><tr><td> WDAGUtilityAccount</td><td></td><td>Una cuenta de usuario que el sistema administr...</td></tr></table>			Nombre	Nombre com...	Descripción	 aCdCmN599		Cuenta integrada para la administración del eq...	 Admin			 DefaultAccount		Cuenta de usuario administrada por el sistema.	 IcNcVn599		Cuenta integrada para el acceso como invitado ...	 WDAGUtilityAccount		Una cuenta de usuario que el sistema administr...
	Nombre	Nombre com...	Descripción																		
	 aCdCmN599		Cuenta integrada para la administración del eq...																		
 Admin																					
 DefaultAccount		Cuenta de usuario administrada por el sistema.																			
 IcNcVn599		Cuenta integrada para el acceso como invitado ...																			
 WDAGUtilityAccount		Una cuenta de usuario que el sistema administr...																			
Usuarios		OK/NOK																			
aCdCmN599																					
IcNcVn599																					

Comprobación	OK/NOK	Cómo hacerlo		
22.Verifique el tipo de inicio configurado para cada uno de los servicios del sistema.		Desde la ventana de PowerShell abierta anteriormente, ejecute "services.msc". A continuación, se abrirá la consola de “Servicios del sistema”. Compruebe que el tipo de inicio configurado para cada servicio coincide con el mostrado en la siguiente tabla: Nota: Dependiendo de los servicios que estén instalados en el equipo, es posible que aparezcan los nombres cortos de los servicios, que no aparezca el servicio e incluso que aparezcan servicios adicionales (antivirus, etc.). En la siguiente tabla se muestran el nombre largo y el nombre corto para cada servicio. En la ventana de la consola de servicios sólo aparecerá uno de los dos: el nombre largo si el servicio está instalado en el equipo en el que esté realizando la comprobación, o el nombre corto, si no lo está. Lo importante es que el modo de inicio de los servicios que aparezcan tanto en la ventana de la consola de servicios como en esta tabla, coincida en ambos casos. Además, deberá tener en cuenta que los números existentes en algunos servicios son aleatorios y cambian en cada equipo.		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
ASP.NET State Service	aspnet_state	Deshabilitado	Configurado	
Acceso a datos de usuarios	UserDataSvc	Deshabilitado	Configurado	
Actualizador de zona horaria automática	tzautoupdate	Deshabilitado	Configurado	
Adaptador de escucha Net.Msmq	NetMsmqActivator	Deshabilitado	Configurado	
Adaptador de escucha Net.Pipe	NetPipeActivator	Deshabilitado	Configurado	
Adaptador de escucha Net.Tcp	NetTcpActivator	Deshabilitado	Configurado	
Adaptador de rendimiento de WMI	wmiApSrv	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Administración de aplicaciones	AppMgmt	Deshabilitado	Configurado		
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado		
Administración de capas de almacenamiento	TieringEngineService	Deshabilitado	Configurado		
Administración de máquinas virtuales de Hyper-V	vmms	Deshabilitado	Configurado		
Administración remota de Windows (WS-Management)	WinRM	Deshabilitado	Configurado		
Administrador de conexiones automáticas de acceso remoto	RasAuto	Deshabilitado	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	Configurado		
Administrador de conexiones de acceso remoto	RasMan	Deshabilitado	Configurado		
Administrador de configuración de dispositivos	DsmSvc	Manual	Configurado		
Administrador de credenciales	VaultSvc	Deshabilitado	Configurado		
Administrador de cuentas de seguridad	SamSs	Automático	Configurado		
Administrador de cuentas web	TokenBroker	Manual	Configurado		
Administrador de identidad de redes de mismo nivel	p2pimsvc	Deshabilitado	Configurado		
Administrador de mapas descargados	MapsBroker	Deshabilitado	Configurado		
Administrador de pagos y NFC/SE	SEMgrSvc	Deshabilitado	Configurado		
Administrador de sesión local	LSM	Automático	Configurado		
Administrador de usuarios	UserManager	Automático	Configurado		
Adquisición de imágenes de Windows (WIA)	stisvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		
Agente de directiva IPsec	PolicyAgent	Deshabilitado	Configurado		
Agente de eventos de tiempo	TimeBrokerSvc	Manual	Configurado		
Agente de eventos del sistema	SystemEventsBroker	Automático	Configurado		
Agente de supervisión en tiempo de ejecución de Protección del sistema	SgrmBroker	Deshabilitado	Configurado		
Agrupación de red del mismo nivel	p2psvc	Deshabilitado	Configurado		
Aislamiento de claves CNG	KeyIso	Deshabilitado	Configurado		
Almacenamiento de datos de usuarios	UnistoreSvc	Deshabilitado	Configurado		
Aplicación auxiliar IP	iphlpvc	Deshabilitado	Configurado		
Aplicación auxiliar de NetBIOS sobre TCP/IP	lmhosts	Automático	Configurado		
Aplicación del sistema COM+	COMSysApp	Deshabilitado	Configurado		
Archivos sin conexión	CscService	Deshabilitado	Configurado		
Asignador de detección de topologías de nivel de vínculo	ltdsvc	Deshabilitado	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
Audio de Windows	Audiosrv	Deshabilitado	Configurado		
Autenticación natural	NaturalAuthentication	Deshabilitado	Configurado		
Auxiliar del servicio de Filtro de escritura unificado	UwfServicingSvc	Deshabilitado	Configurado		
Ayuda del Panel de control de Informes de problemas y soluciones	wercplsupport	Deshabilitado	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Deshabilitado	Configurado		
BranchCache	PeerDistSvc	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Deshabilitado	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CaptureService	CaptureService	Deshabilitado	Configurado		
Carpetas de trabajo	workfolderssvc	Deshabilitado	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Deshabilitado	Configurado		
Cliente para NFS	NfsClnt	Deshabilitado	Configurado		
Cliente web	WebClient	Deshabilitado	Configurado		
Cola de impresión	Spooler	Deshabilitado	Configurado		
Compilador de extremo de audio de Windows	AudioEndpointBuilder	Deshabilitado	Configurado		
Comprobador puntual	svsvc	Manual	Configurado		
Conexiones de red	Netman	Manual	Configurado		
Conexión compartida a Internet (ICS)	SharedAccess	Deshabilitado	Configurado		
Configuración automática de WLAN	WlanSvc	Deshabilitado	Configurado		
Configuración automática de WWAN	WwanSvc	Deshabilitado	Configurado		
Configuración automática de dispositivos conectados a la red	NcdAutoSetup	Manual	Configurado		
Configuración automática de redes cableadas	dot3svc	Manual	Configurado		
Configuración de Escritorio remoto	SessionEnv	Deshabilitado	Configurado		
ConsentUX	ConsentUxUserSvc	Deshabilitado	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Deshabilitado	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Coordinador de transacciones distribuidas	MSDTC	Deshabilitado	Configurado		
Copias de seguridad de Windows	SDRSVC	Deshabilitado	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Deshabilitado	Configurado		
Desencadenadores de Message Queue Server	MSMQTriggers	Deshabilitado	Configurado		
Detección SSDP	SSDPSRV	Deshabilitado	Configurado		
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado		
DevicePicker	DevicePickerUserSvc	Deshabilitado	Configurado		
DevicesFlow	DevicesFlowUserSvc	Deshabilitado	Configurado		
Diagnostic Execution Service	diagsvc	Deshabilitado	Configurado		
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Deshabilitado	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Deshabilitado	Configurado		
Energía	Power	Deshabilitado	Configurado		
Enrutamiento y acceso remoto	RemoteAccess	Deshabilitado	Configurado		
Escucha de RIP	iprip	Deshabilitado	Configurado		
Estación de trabajo	LanmanWorkstation	Automático	Configurado		
Eventos de adquisición de imágenes estáticas	WiaRpc	Deshabilitado	Configurado		
Examinador de equipos	Browser	Deshabilitado	Configurado		
Experiencia de calidad de audio y vídeo de Windows (qWave)	QWAVE	Deshabilitado	Configurado		
Extensiones y notificaciones de impresora	PrintNotify	Deshabilitado	Configurado		
Fax	Fax	Deshabilitado	Configurado		
Filtro de teclado de Microsoft	MsKeyboardFilter	Deshabilitado	Configurado		
Firewall de Windows	mpssvc	Automático	Configurado		
GraphicsPerfSvc	GraphicsPerfSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Hora de Windows	W32Time	Automático	Configurado	
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado	
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado	
Host del servicio de diagnóstico	WdiServiceHost	Deshabilitado	Configurado	
Identidad de aplicación	AppIDSvc	Deshabilitado	Configurado	
Información de la aplicación	Appinfo	Manual	Configurado	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	Configurado	
Inicio de sesión secundario	seclogon	Deshabilitado	Configurado	
Instalador de ActiveX (AxInstSV)	AxInstSV	Deshabilitado	Configurado	
Instalador de módulos de Windows	TrustedInstaller	Manual	Configurado	
Instantáneas de volumen	VSS	Deshabilitado	Configurado	
Instrumental de administración de Windows	Winmgmt	Automático	Configurado	
Interfaz de servicio invitado de Hyper-V	vmicguestinterface	Deshabilitado	Configurado	
KTMRM para DTC (Coordinador de transacciones distribuidas)	KtmRm	Deshabilitado	Configurado	
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	Configurado	
LxssManager	LxssManager	Deshabilitado	Configurado	
Message Queue Server	MSMQ	Deshabilitado	Configurado	
MessagingService	MessagingService	Deshabilitado	Configurado	
Microsoft App-V Client	AppVClient	Deshabilitado	Configurado	
Microsoft Passport	NgcSvc	Deshabilitado	Configurado	
Modo incrustado	embeddedmode	Deshabilitado	Configurado	
Motor de filtrado de base	BFE	Automático	Configurado	
Módulos de creación de claves de IPsec para IKE y AuthIP	IKEEXT	Manual	Configurado	
Net Logon	Netlogon	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Notificaciones del servicio de token de Windows	c2wts	Deshabilitado	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Automático	Configurado		
Optimizar unidades	defragsvc	Manual	Configurado		
Partida guardada en Xbox Live	XblGameSave	Deshabilitado	Configurado		
Plug and Play	PlugPlay	Automático	Configurado		
Preparación de aplicaciones	AppReadiness	Manual	Configurado		
PrintWorkflow	PrintWorkflowUserSvc	Deshabilitado	Configurado		
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Deshabilitado	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	Eaphost	Deshabilitado	Configurado		
Protocolo de resolución de nombres de mismo nivel	PNRPsvc	Deshabilitado	Configurado		
Proveedor de instantáneas de software de Microsoft	swprv	Manual	Configurado		
Publicación de recurso de detección de función	FDResPub	Deshabilitado	Configurado		
Reconoc. ubicación de red	NlaSvc	Automático	Configurado		
Recopilador de eventos de Windows	Weccsvc	Deshabilitado	Configurado		
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Deshabilitado	Configurado		
Registrador de configuración de Windows Connect Now	wcnscvc	Deshabilitado	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	Configurado		
Servicio AVCTP	BthAvctpSvc	Deshabilitado	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Deshabilitado	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Deshabilitado	Configurado		
Servicio FTP de Microsoft	ftpsvc	Deshabilitado	Configurado		
Servicio FrameServer de la Cámara de Windows	FrameServer	Deshabilitado	Configurado		
Servicio Informe de errores de Windows	WerSvc	Deshabilitado	Configurado		
Servicio Interfaz de almacenamiento en red	nsi	Automático	Configurado		
Servicio LPD	LPDSVC	Deshabilitado	Configurado		
Servicio MultiPoint	Wms	Deshabilitado	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Deshabilitado	Configurado		
Servicio PushToInstall de Windows	PushToInstall	Deshabilitado	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standardcollector.service	Deshabilitado	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Deshabilitado	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio biométrico de Windows	WbioSrv	Deshabilitado	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	Configurado		
Servicio de Protección contra amenazas avanzada de Windows Defender	Sense	Deshabilitado	Configurado		
Servicio de Windows Defender	WinDefend	Deshabilitado	Configurado		
Servicio de Windows Insider	wisvc	Deshabilitado	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	Configurado		
Servicio de administración IIS	IISADMIN	Deshabilitado	Configurado		
Servicio de administración de Windows	WManSvc	Deshabilitado	Configurado		
Servicio de administración de aplicaciones de empresa	EntAppSvc	Deshabilitado	Configurado		
Servicio de administración de radio	RmSvc	Deshabilitado	Configurado		
Servicio de administración de web	WMSVC	Deshabilitado	Configurado		
Servicio de administrador de conexiones con servicios Wi-Fi Direct	WFDSConMgrSvc	Deshabilitado	Configurado		
Servicio de administrador de licencias de Windows	LicenseManager	Manual	Configurado		
Servicio de almacenamiento	StorSvc	Manual	Configurado		
Servicio de asistente para perfil local	wlpasvc	Deshabilitado	Configurado		
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado		
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de cierre de invitado de Hyper-V	vmicshuttdown	Deshabilitado	Configurado		
Servicio de cliente de protección de host	HgClientService	Deshabilitado	Configurado		
Servicio de compatibilidad con Bluetooth	bthserv	Deshabilitado	Configurado		
Servicio de configuración de red	NetSetupSvc	Manual	Configurado		
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Deshabilitado	Configurado		
Servicio de datos del sensor	SensorDataService	Deshabilitado	Configurado		
Servicio de datos espacial	SharedRealitySvc	Deshabilitado	Configurado		
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	Deshabilitado	Configurado		
Servicio de directivas de diagnóstico	DPS	Deshabilitado	Configurado		
Servicio de dispositivo de interfaz humana	hidserv	Deshabilitado	Configurado		
Servicio de enrutador de AllJoyn	AJRouter	Deshabilitado	Configurado		
Servicio de enrutamiento de mensajes de inserción del Protocolo de aplicación inalámbrica (WAP) de administración de dispositivos	dmwappushservice	Deshabilitado	Configurado		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Deshabilitado	Configurado		
Servicio de experiencia de idioma	LxpSvc	Deshabilitado	Configurado		
Servicio de geolocalización	lfsvc	Deshabilitado	Configurado		
Servicio de historial de archivos	fhsvc	Deshabilitado	Configurado		
Servicio de host HV (Hyper-V)	HvHost	Deshabilitado	Configurado		

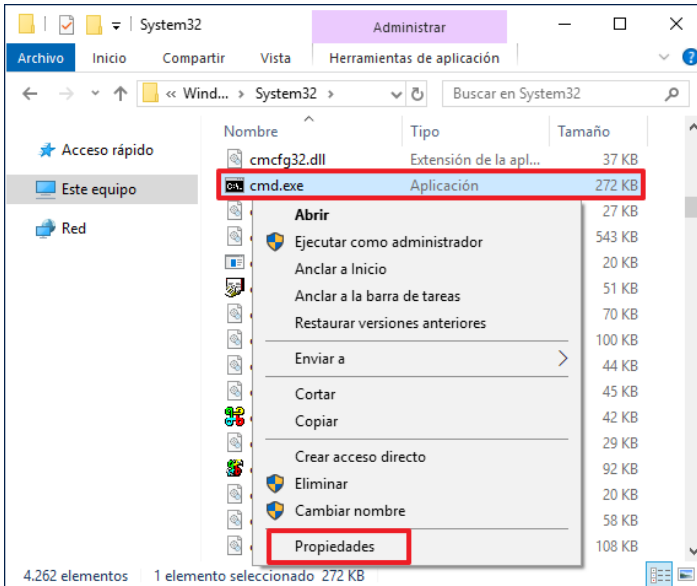
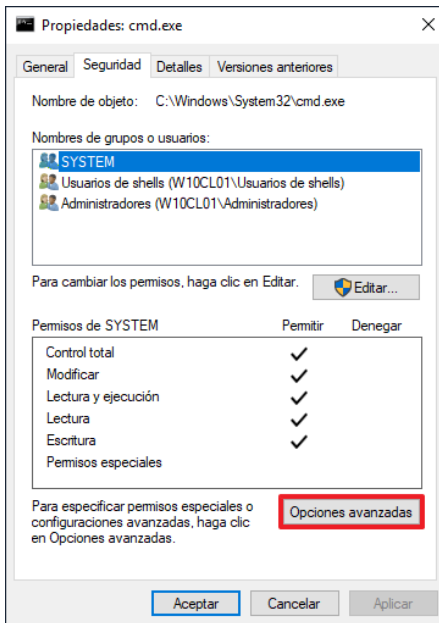
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de implementación de AppX (AppXSVC)	AppXSvc	Manual	Configurado	
Servicio de infraestructura de tareas en segundo plano	BrokerInfrastructure	Automático	Configurado	
Servicio de inscripción de administración de dispositivos	DmEnrollmentSvc	Manual	Configurado	
Servicio de inspección de red de Windows Defender	WdNisSvc	Manual	Configurado	
Servicio de instalación de Microsoft Store	InstallService	Deshabilitado	Configurado	
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Deshabilitado	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Deshabilitado	Configurado	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado	
Servicio de lista de redes	netprofm	Manual	Configurado	
Servicio de mejora de visualización	DisplayEnhancementService	Deshabilitado	Configurado	
Servicio de monitor de infrarrojos	irmon	Deshabilitado	Configurado	
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado	
Servicio de percepción de Windows	spectrum	Deshabilitado	Configurado	
Servicio de perfil de usuario	ProfSvc	Automático	Configurado	
Servicio de plataforma de dispositivos conectados	CDPSvc	Deshabilitado	Configurado	
Servicio de proceso de host de Hyper-V	vmcompute	Deshabilitado	Configurado	
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Deshabilitado	Configurado	
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado	

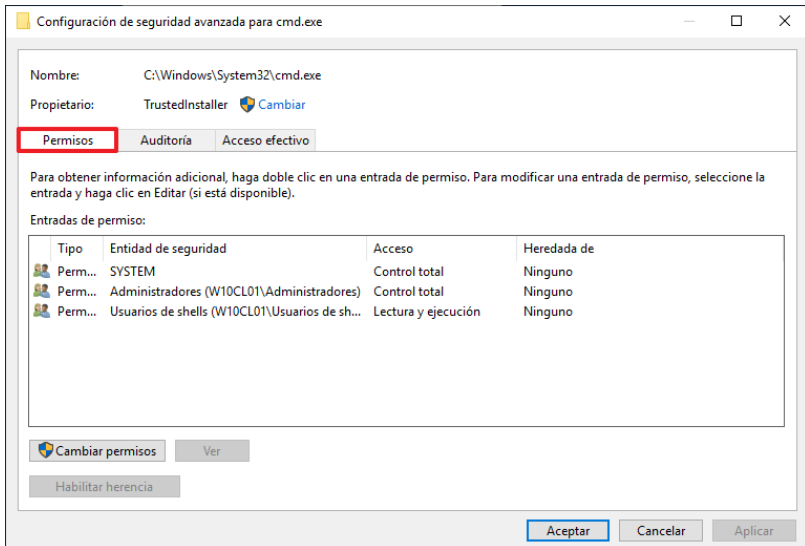
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de publicación World Wide Web	W3SVC	Deshabilitado	Configurado	
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Deshabilitado	Configurado	
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Deshabilitado	Configurado	
Servicio de puerta de enlace de nivel de aplicación	ALG	Deshabilitado	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado	
Servicio de red de host	hns	Deshabilitado	Configurado	
Servicio de registro de W3C	w3logsvc	Deshabilitado	Configurado	
Servicio de reparación MultiPoint	WmsRepair	Deshabilitado	Configurado	
Servicio de repositorio de estado	StateRepository	Manual	Configurado	
Servicio de sensores	SensorService	Deshabilitado	Configurado	
Servicio de simulación de percepción de Windows	perceptionsimulation	Deshabilitado	Configurado	
Servicio de sincronización de hora de Hyper-V	vmictimesync	Deshabilitado	Configurado	
Servicio de soporte técnico de usuario de Bluetooth	BluetoothUserService	Deshabilitado	Configurado	
Servicio de supervisión de sensores	SensrSvc	Deshabilitado	Configurado	
Servicio de transferencia inteligente en segundo plano (BITS)	BITS	Deshabilitado	Configurado	
Servicio de uso compartido de datos	DsSvc	Deshabilitado	Configurado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Deshabilitado	Configurado	
Servicio de uso compartido de red del Reproductor de Windows Media	WMPNetworkSvc	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Deshabilitado	Configurado		
Servicio de usuario del portapapeles	cbdhsvc	Deshabilitado	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdrv	Deshabilitado	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Deshabilitado	Configurado		
Servicio de zona con cobertura inalámbrica móvil de Windows	icssvc	Deshabilitado	Configurado		
Servicio del iniciador iSCSI de Microsoft	MSiSCSI	Deshabilitado	Configurado		
Servicio del módulo de copia de seguridad a nivel de bloque	wbengine	Deshabilitado	Configurado		
Servicio del sistema de notificaciones de inserción de Windows	WpnService	Automático	Configurado		
Servicio enrutador de SMS de Microsoft Windows.	SmsRouter	Deshabilitado	Configurado		
Servicio enumerador de dispositivos portátiles	WPDBusEnum	Deshabilitado	Configurado		
Servicio host de proveedor de cifrado de Windows	WEPHOSTSVC	Manual	Configurado		
Servicio telefónico	PhoneSvc	Deshabilitado	Configurado		
Servicios de Escritorio remoto	TermService	Deshabilitado	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios simples de TCP/IP	simptcp	Deshabilitado	Configurado		
Servidor	LanmanServer	Deshabilitado	Configurado		
Servidor de roles de DS	DsRoleSvc	Deshabilitado	Configurado		



Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado		
Sincronizar host	OneSyncSvc	Deshabilitado	Configurado		
Sistema de cifrado de archivos (EFS)	EFS	Deshabilitado	Configurado		
Sistema de eventos COM+	EventSystem	Automático	Configurado		
Solicitante de instantáneas de volumen de Hyper-V	vmicvss	Deshabilitado	Configurado		
Superfetch	SysMain	Deshabilitado	Configurado		
Tarjeta inteligente	SCardSvr	Deshabilitado	Configurado		
Telefonía	TapiSrv	Deshabilitado	Configurado		
Telemetría y experiencias del usuario conectado	DiagTrack	Deshabilitado	Configurado		
Temas	Themes	Deshabilitado	Configurado		
Ubicador de llamada a procedimiento remoto (RPC)	RpcLocator	Manual	Configurado		
Uso de datos	DusmSvc	Deshabilitado	Configurado		
WalletService	WalletService	Deshabilitado	Configurado		
WarpJITSvc	WarpJITSvc	Deshabilitado	Configurado		
Windows Installer	msiserver	Manual	Configurado		
Windows Presentation Foundation Font Cache 3.0.0.0	FontCache3.0.0.0	Deshabilitado	Configurado		
Windows Search	WSearch	Deshabilitado	Configurado		
Windows Update	wuauserv	Deshabilitado	Configurado		
Windows Update Medic Service	WaaSMedicSvc	Deshabilitado	Configurado		
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo
23.Verifique que se han asignado los permisos correctos en el sistema de archivos.		Desde la ventana de Powershell abierta anteriormente, ejecute "explorer.exe". A continuación, se abrirá el "Explorador de Windows". Localice cada fichero de los mostrados a continuación, siguiendo la ruta definida en la tabla, y seleccione propiedades con el botón derecho del ratón:  En la ventana de "Propiedades", seleccione la pestaña "Seguridad" y pulse sobre "Opciones Avanzadas".  Nota: En caso de que no aparezca la pestaña de seguridad, esto será debido a que las políticas administradas a través de la herramienta "Administración de directivas de grupo local" se han aplicado y, por tanto, se deberá volver a ejecutar el script "CCN-STIC-599B19 Cliente independiente – Habilita comprobaciones.bat".

Comprobación	OK/NOK	Cómo hacerlo	
		En la pestaña “Permisos” de la ventana “Configuración de <archivo a comprobar>”, aparecerán los permisos asignados al contenedor o fichero a comprobar.  Observe los permisos y compárelos con la siguiente tabla: Nota: Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados. Tenga en cuenta que tanto la cuenta Administrador como la cuenta Invitado estarán renombradas y, por tanto, aparecerán con su nuevo nombre. Es importante que no se modifiquen estos permisos, asegúrese de que al cerrar las ventanas de “Propiedades” y “Configuración de seguridad avanzada” pulsa sobre “Cancelar”.	
Archivo	Usuario	Permiso	OK/NOK
%Public%	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemDrive%\	Administradores	Control Total	
	CREATOR OWNER	Permisos especiales ⁴	
	SYSTEM	Control Total	
	Usuarios	Lectura	

⁴ Los permisos especiales que se establecerán para el creador de los objetos %SystemDrive% serán de Control Total pero aplicados a “Sólo subcarpetas y archivos” en lugar de aplicarlos a “Esta carpeta, subcarpeta y archivos”.



Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%SystemDrive%\Users\Default	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\regedit.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\Registration	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarioscmd	Leer y ejecutar	
%SystemRoot%\security	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\arp.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\at.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\azuresettingsyncprovider.dll	Administradores	Control Total	
%SystemRoot%\system32\bash.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\cacls.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\chatapis.dll	Administradores	Control Total	
%SystemRoot%\system32\chatapis.dll	Administradores	Control Total	
%SystemRoot%\system32\clip.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\cmd.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\cscript.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\diagtrack.dll	Administradores	Control Total	
%SystemRoot%\system32\eshell.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\finger.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\ftp.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\gamepanel.exe	Administradores	Control Total	
	SYSTEM	Control Total	

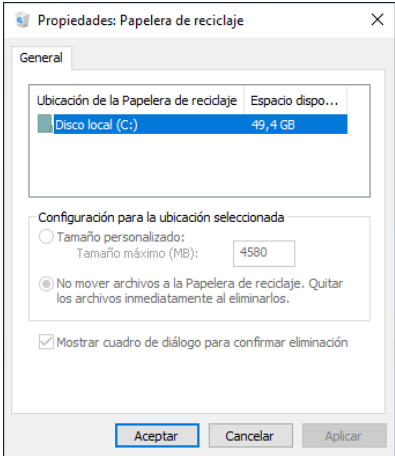
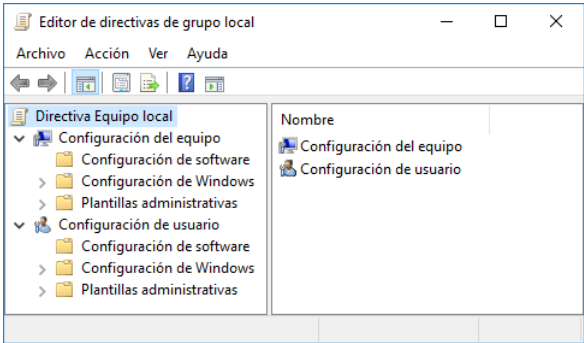
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\geolocation.dll		Administradores	Control Total	
%SystemRoot%\system32\hostname.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\ipconfig.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\iprip.dll		Administradores	Control Total	
%SystemRoot%\system32\nbtstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net1.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\netstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nfsadmin.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nslookup.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\phonecallhistoryapis.dll		Administradores	Control Total	
%SystemRoot%\system32\ping.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\privatecloudhnsplugin.dll		Administradores	Control Total	
%SystemRoot%\system32\ras		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\rasadhlp.dll		Administradores	Control Total	
%SystemRoot%\system32\rasauto.dll		Administradores	Control Total	
%SystemRoot%\system32\rasautou.exe		Administradores	Control Total	
%SystemRoot%\system32\raschap.dll		Administradores	Control Total	
%SystemRoot%\system32\rasctrnm.h		Administradores	Control Total	
%SystemRoot%\system32\rasctrs.dll		Administradores	Control Total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control Total	
%SystemRoot%\system32\rasdial.exe		Administradores	Control Total	
%SystemRoot%\system32\rasmans.dll		Administradores	Control Total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control Total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control Total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control Total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control Total	
%SystemRoot%\system32\rastls.dll		Administradores	Control Total	
%SystemRoot%\system32\regedt32.exe		Administradores	Control Total	
		SYSTEM	Control Total	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\regsvr32.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\route.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\runonce.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\secedit.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\telnet.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\tftp.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\tracert.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\uwfmgr.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\webcamui.dll	Administradores	Control Total		
%SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell.exe	Administradores	Control Total		
	SYSTEM	Control Total		
	Usuarios de shells	Lectura y ejecución, Lectura		
%SystemRoot%\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe	Administradores	Control Total		
	SYSTEM	Control Total		
	Usuarios de shells	Lectura y ejecución, Lectura		
%SystemRoot%\system32\wscript.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\xblgamesave.dll	Administradores	Control Total		
%SystemRoot%\system32\xcopy.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\arp.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\at.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\cacls.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\clip.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\cmd.exe	Administradores	Control Total		
	SYSTEM	Control Total		
	Usuarios de shells	Lectura y ejecución, Lectura		

Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\cscript.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\finger.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\ftp.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\hostname.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\ipconfig.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\net.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\netstat.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\nslookup.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\ping.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\rasadhlp.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasautou.exe	Administradores	Control Total	
%SystemRoot%\syswow64\raschap.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasctnm.h	Administradores	Control Total	
%SystemRoot%\syswow64\rasctrs.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasdial.exe	Administradores	Control Total	
%SystemRoot%\syswow64\rasmontr.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasmxs.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasphone.exe	Administradores	Control Total	
%SystemRoot%\syswow64\rasppp.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rasser.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rastapi.dll	Administradores	Control Total	
%SystemRoot%\syswow64\rastls.dll	Administradores	Control Total	
%SystemRoot%\syswow64\regedt32.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\regsvr32.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\route.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\runonce.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\secedit.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\syswow64\tracert.exe	Administradores	Control Total	
	SYSTEM	Control Total	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\PowerShell.exe		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\PowerShell_ISE.exe		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\syswow64\wscript.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\syswow64\xcopy.exe		Administradores	Control Total	
		SYSTEM	Control Total	
24. Compruebe los valores del registro configurados a través de los scripts de seguridad.		Desde la ventana de Powershell arrancada con anterioridad, ejecute "regedit.exe" para lanzar una ventana del editor del registro. Compruebe que las claves de registro indicadas en la siguiente tabla tienen los correspondientes valores mostrados en ella:		
		Clave	Valor	OK/NOK
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents\	ffffff	
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Data Collection\AllowTelemetry	00000001 (1)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MessagingService\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NgcCtnrSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NgcSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OneSyncSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PimIndexMaintenanceSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PrintWorkflowUserSvc\Start	00000004 (4)	
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sense\Start	00000004 (4)	

Comprobación	OK/NOK	Cómo hacerlo	
		Clave	Valor
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UnistoreSvc\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UserDataSvc\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WpnUserService\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EntAppSvc\Start	00000004 (4)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\LaunchTo	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsHistory	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsMenu	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClearRecentDocsOnExit	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecycleFiles	00000001 (1)
		HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ConfirmFileDelete	00000001 (1)
25.Compruebe las tareas programadas.		Desde la ventana de PowerShell arrancada con anterioridad, ejecute "taskschd.msc" para lanzar una ventana del programador de tareas. Compruebe que las tareas programadas indicadas en la siguiente tabla están deshabilitadas:	
		Tarea programada	
		Microsoft\XblGameSave\XblGameSaveTask	OK/NOK
		Microsoft\Windows\Maps\MapsToastTask	
		Microsoft\Windows\HelloFace\FODCleanupTask	
		Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser	

Comprobación	OK/NOK	Cómo hacerlo
26.Verifique la configuración de la papelera de reciclaje.		Localice la papelera de reciclaje en el escritorio, márkela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá. Esto mostrará la siguiente ventana de propiedades de la papelera de reciclaje:  Compruebe que están seleccionadas las siguientes dos opciones:
	Parámetro	OK/NOK
	No mover archivos a la Papelera de reciclaje. Quitar los archivos inmediatamente al eliminarlos.	
	Mostrar cuadro de diálogo para confirmar eliminación.	
27.Ejecute el editor de directiva de grupo local (gpedit.msc) para poder comprobar el contenido del GPO local en los próximos pasos.		Desde la ventana de Powershell arrancada anteriormente, ejecute "gpedit.msc". Esto abrirá una ventana del Editor de directivas de grupo local, como la mostrada en la siguiente figura.  En los siguientes pasos (identificados con el texto "GPO: ") verificará el contenido del objeto de directiva de grupo local (GPO). Hasta que se le indique, no deberá cerrar la ventana del Editor de directivas de grupo local, y deberá realizar las comprobaciones correspondientes dentro de ella, en las ubicaciones indicadas en cada caso.

Comprobación	OK/NOK	Cómo hacerlo
28.GPO: Compruebe la directiva de contraseñas.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas” Nota: Recuerde que estos datos pueden variar dependiendo del nivel de clasificación del que disponga el equipo. La guía asume la configuración de máxima seguridad.
	Directiva	Valor
	Almacenar contraseñas con cifrado reversible	Deshabilitada
	Exigir historial de contraseñas	24 contraseñas recordadas
	La contraseña debe cumplir los requisitos de complejidad	Habilitada
	Longitud mínima de la contraseña	12 caracteres
	Vigencia máxima de la contraseña	90 días
	Vigencia mínima de la contraseña	2 días
29.GPO: Compruebe la directiva de bloqueo de cuenta.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de bloqueo de cuenta” Nota: Recuerde que estos datos pueden variar dependiendo del nivel de clasificación del que disponga el equipo. La guía asume la configuración de máxima seguridad.
	Directiva	Valor
	Duración del bloqueo de cuenta	0
	Restablecer el bloqueo de cuenta después de	30 minutos
	Umbral de bloqueo de cuenta	3 intentos de inicio de sesión no válidos
30.GPO: Compruebe la directiva de auditoría.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Auditar el acceso a objetos	Correcto/Erróneo	
		Auditar el acceso al servicio de directorio	Correcto/Erróneo	
		Auditar el cambio de directivas	Correcto/Erróneo	
		Auditar el seguimiento de procesos	Sin auditoría	
		Auditar el uso de privilegios	Correcto/Erróneo	
		Auditar eventos de inicio de sesión	Correcto/Erróneo	
		Auditar eventos de inicio de sesión de cuenta	Correcto/Erróneo	
		Auditar eventos del sistema	Correcto/Erróneo	
		Auditar la administración de cuentas	Correcto/Erróneo	
31.GPO: Compruebe la asignación de derechos de usuario.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario”		
		Directiva	Valor	OK/NOK
		Actuar como parte del sistema operativo	(Definida, pero sin ningún valor)	
		Administrar registro de seguridad y auditoría	Audidores, Administradores	
		Ajustar las cuotas de la memoria para un proceso	Administradores, Servicio de red, SERVICIO LOCAL	
		Apagar el sistema	Administradores, Usuarios	
		Aumentar el espacio de trabajo de un proceso	Administradores, Servicio de red, SERVICIO LOCAL	
		Aumentar prioridad de programación	Administradores	
		Cambiar la hora del sistema	Administradores, SERVICIO LOCAL	
		Cambiar la zona horaria	Administradores, SERVICIO LOCAL	
		Cargar y descargar controladores de dispositivo	Administradores	
		Crear objetos compartidos permanentes	(Definida, pero sin ningún valor)	
		Crear un archivo de paginación	Administradores	
		Crear un objeto símbolo (token)	(Definida, pero sin ningún valor)	
		Crear vínculos simbólicos	Administradores	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Denegar el acceso a este equipo desde la red	Invitados, ANONYMOUS LOGON, aCdCmN599
		Denegar el inicio de sesión como servicio	Invitados ANONYMOUS LOGON
		Denegar el inicio de sesión como trabajo por lotes	Invitados ANONYMOUS LOGON
		Denegar el inicio de sesión local	Invitados ANONYMOUS LOGON
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	Administradores
		Forzar cierre desde un sistema remoto	Administradores
		Generar auditorías de seguridad	Servicio de red, SERVICIO LOCAL
		Generar perfiles de un solo proceso	Administradores
		Generar perfiles del rendimiento del sistema	Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	(Definida, pero sin ningún valor)
		Hacer copias de seguridad de archivos y directorios	Administradores
		Iniciar sesión como proceso por lotes	(Definida, pero sin ningún valor)
		Iniciar sesión como servicio	(Definida, pero sin ningún valor)
		Modificar la etiqueta de un objeto	(Definida, pero sin ningún valor)
		Modificar valores de entorno firmware	Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	(Definida, pero sin ningún valor)
		Obtén un token de suplantación para otro usuario en la misma sesión	Administradores
		Omitir comprobación de recorrido	Administradores, Usuarios autenticados Servicio de red SERVICIO LOCAL

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Permitir el inicio de sesión local	Administradores, Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	(Definida, pero sin ningún valor)
		Quitar equipo de la estación de acoplamiento	Administradores, Usuarios
		Realizar tareas de mantenimiento del volumen	Administradores
		Reemplazar un símbolo (token) de nivel de proceso	Servicio de red, SERVICIO LOCAL
		Restaurar archivos y directorios	Administradores
		Sincronizar los datos del servicio de directorio	(Definida, pero sin ningún valor)
		Suplantar a un cliente tras la autenticación	Servicio Local, Servicio de red, Administradores
		Tener acceso a este equipo desde la red	Administradores, Usuarios
		Tomar posesión de archivos y otros objetos	Administradores
32.GPO: Compruebe las opciones de seguridad.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”	
Directiva		Valor	OK/NOK
Acceso a redes: canalizaciones con nombre accesibles anónimamente		(Definida, pero sin ningún valor)	
Acceso a redes: modelo de seguridad y uso compartido para cuentas locales		Clásico: usuarios locales se autentican con credenciales propias	
Acceso a redes: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de la red		Habilitada	
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM		Habilitada	
Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos		Deshabilitada	
Acceso a redes: recursos compartidos accesibles anónimamente		(Definida, pero sin ningún valor)	
Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos		Habilitada	
Acceso a redes: rutas del Registro accesibles remotamente		System ⁵ \CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows NT\CurrentVersion	
Acceso a redes: rutas y subrutas del Registro accesibles remotamente		Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System ⁶ \CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, System\CurrentControlSet\Control\Content Index, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog	

⁵ En este caso "System" hace referencia a HKEY_LOCAL_MACHINE\System, y "Software" a HKEY_LOCAL_MACHINE\Software.

⁶ En este caso "System" hace referencia a HKEY_LOCAL_MACHINE\System, y "Software" a HKEY_LOCAL_MACHINE\Software.

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Acceso de red: permitir traducción SID/nombre anónima		Deshabilitada	
Apagado: borrar el archivo de paginación de la memoria virtual		Habilitada	
Apagado: permitir apagar el sistema sin tener que iniciar sesión		Deshabilitada	
Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad		Habilitada	
Auditoría: auditar el acceso de objetos globales del sistema		Deshabilitada	
Auditoría: forzar la configuración de subcategorías de la directiva de auditoría (Windows Vista o posterior) para invalidar la configuración de la categoría de directiva de auditoría		Deshabilitada	
CCN: (DisableIPSourceRouting) Nivel de protección de enrutamiento de origen IP		2 = Protección alta, el enrutamiento en origen está completamente deshabilitado	
CCN: (DynamicBacklogGrowthDelta) Número de conexiones a crear cuando se necesiten conexiones adicionales para aplicaciones Winsock		10	
CCN: (EnableDeadGWDetect) Permitir detección automática de puertas de enlace de red inactivas		Deshabilitada	
CCN: (EnableDynamicBacklog) Habilitar el registro de envíos dinámico para aplicaciones Winsock		Habilitada	
CCN: (EnableICMPRedirect) Permitir redireccionamientos ICMP que prevalezcan sobre rutas generadas con OSPF		Deshabilitada	
CCN: (EnablePMTUDiscovery) Permitir detección automática de tamaño de MTU		Deshabilitada	



Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
CCN: (KeepAliveTime) Frecuencia en milisegundos de envío de paquetes de mantenimiento de conexión.		300000 o 5 minutos (recomendado)	
CCN: (MaximumDynamicBacklog) Máximo número de conexiones <<cuasi-libres>> para aplicaciones Winsock		20000 (recomendado)	
CCN: (MinimumDynamicBacklog) Mínimo número de conexiones libres para aplicaciones Winsock		20	
CCN: (NoDriveTypeAutoRun) Desactivar Autoejecutar para todas las unidades		255, Deshabilitar Autoejecutar para todas las unidades	
CCN: (NoNameReleaseOnDemand) Permitir al equipo ignorar las solicitudes de publicación de nombres NetBIOS excepto de los servidores WINS		Habilitada	
CCN: (NtfsDisable8dot3NameCreation) Permitir al ordenador detener la generación de nombres de archivo de estilo 8.3		Habilitada	
CCN: (PerformRouterDiscovery) Permitir que IRDP detecte y configure direcciones de puerta de enlace predeterminadas		Deshabilitada	
CCN: (SafeDllSearchMode) Activar el modo de búsqueda seguro de DLLS (recomendado)		Habilitada	
CCN: (ScreenSaverGracePeriod) El tiempo en segundos antes de que expire el periodo de gracia del protector de pantalla (0 recomendado)		0	
CCN: (SynAttackProtect) Nivel de protección frente a ataques SYN		1 = El tiempo de espera de la conexión se consume antes si se detecta un ataque SYN	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
CCN: (TcpMaxConnectResponseRetra nsmissions) Retransmisiones SYN-ACK cuando no se reconoce una solicitud de conexión		2 = Las conexiones medio abiertas o con 3 y 6 segundos de tiempo de espera se cierran después de 21 segundos	
CCN: (TcpMaxDataRetransmissions) Número de retransmisiones de datos no reconocidos		3	
CCN: (TCPMaxPortsExhausted) Número de solicitudes de conexión necesarias para iniciar la protección contra ataques SYN		5	
CCN: (WarningLevel) Umbral de porcentaje para el registro de eventos de seguridad en el cual el sistema generará una advertencia		90%	
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros		Deshabilitada	
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)		Habilitada	
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)		Habilitada	
Configuración del sistema: subsistemas opcionales		(Definida, pero sin ningún valor)	
Configuración de sistema: usar reglas de certificado en ejecutables de Windows para directivas de restricción de software		Deshabilitada	
Consola de recuperación: permitir el inicio de sesión administrativo automático		Deshabilitada	
Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación		Habilitada	
Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador		Pedir credenciales en el escritorio seguro	
Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar		Pedir credenciales en el escritorio seguro	
Control de cuentas de usuario: detectar instalaciones de aplicaciones y pedir confirmación de elevación		Habilitada	
Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador		Habilitada	
Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras		Habilitada	
Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados		Deshabilitada	
Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador		Habilitada	
Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro		Deshabilitada	
Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Controlador de dominio: no permitir los cambios de contraseña de cuenta de equipo		Deshabilitada	
Controlador de dominio: permitir a los operadores de servidor programar tareas		Deshabilitada	
Controlador de dominio: requisitos de firma de servidor LDAP		Requerir firma	
Criptografía de sistema: forzar la protección con claves seguras para las claves de usuario almacenadas en el equipo		El usuario debe escribir una contraseña cada vez que use una clave.	
Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash		Deshabilitada	
Cuentas: bloquear cuentas Microsoft		Los usuarios no pueden agregar cuentas Microsoft ni iniciar sesión	
Cuentas: cambiar el nombre de cuenta de invitado		lcNcVn599	
Cuentas: cambiar el nombre de la cuenta de administrador		aCdCmN599	
Cuentas: estado de la cuenta de administrador		Deshabilitada	
Cuentas: estado de la cuenta de invitado		Deshabilitada	
Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola		Habilitada	
DCOM: restricciones de acceso al equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)		O:BAG:BAD:(A;;CCDCLC;;;AU) Equivale a: Usuarios autenticados: Permitir Acceso local y Acceso remoto	
DCOM: restricciones de inicio de equipo en sintaxis de Lenguaje de definición de descriptores de seguridad (SDDL)		O:BAG:BAD:(A;;CCDCLCSWRP;;;BA)(A;;CCDCSW;;;AU) Equivale a: Administradores: Permitir Ejecución local, Ejecucion remota, Activacion local y Activacion remota Usuarios autenticados: Permitir Ejecución local, Ejecucion remota, Activacion local y Activacion remota	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Dispositivos: impedir que los usuarios instalen controladores de impresora		Habilitada	
Dispositivos: permitir desacoplamiento sin tener que iniciar sesión		Deshabilitada	
Dispositivos: permitir formatear y expulsar medios extraíbles		Administradores	
Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente		Habilitada	
Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente		Habilitada	
Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente		Bloquear estación de trabajo	
Inicio de sesión interactivo: límite de inactividad del equipo		300 segundos (En el caso de estar aplicado el nivel de seguridad RESERVADO O SUPERIOR) 900 segundos (En el caso de estar aplicado el nivel de seguridad CONFIDENCIAL)	
Inicio de sesión interactivo: mostrar información de usuario cuando se bloquee la sesión		No mostrar la información del usuario	
Inicio de sesión interactivo: no mostrar el último nombre de usuario		Habilitada	
Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr		Deshabilitada	
Inicio de sesión interactivo: número de inicios de sesión anteriores que se almacenarán en caché (si el controlador de dominio no está disponible)		0 inicios de sesión	
Inicio de sesión interactivo: pedir al usuario que cambie la contraseña antes de que expire		14 días	
Inicio de sesión interactivo: requerir la autenticación del controlador de dominio para desbloquear la estación de trabajo		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Inicio de sesión interactivo: requerir tarjeta inteligente		Deshabilitada	
Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión		Este sistema está restringido a los usuarios autorizados.	
Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión		ES UN DELITO CONTINUAR SIN LA DEBIDA AUTORIZACIÓN	
Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)		Habilitada	
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)		Habilitada	
Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo		Deshabilitada	
Miembro de dominio: duración máxima de contraseña de cuenta de equipo		30 días	
Miembro de dominio: firmar digitalmente datos de un canal seguro (cuando sea posible)		Habilitada	
Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)		Habilitada	
Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)		Habilitada	
Objetos de sistema: requerir no distinguir mayúsculas de minúsculas para subsistemas que no sean de Windows		Habilitada	
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión		Habilitada	
Seguridad de red: nivel de autenticación de LAN Manager		Enviar sólo respuesta NTLMv2 y rechazar LM y NTLM	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña		Habilitada	
Seguridad de red: permitir que LocalSystem use la identidad del equipo para NTLM		Habilitada	
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem		Deshabilitada	
Seguridad de red: permitir solicitudes de autenticación PKU2U a este equipo para usar identidades en Internet		Deshabilitada	
Seguridad de red: requisitos de firma de cliente LDAP		Negociar firma	
Seguridad de red: restringir NTLM: agregar excepciones de servidor en este dominio		(Definida, pero sin ningún valor)	
Seguridad de red: restringir NTLM: agregar excepciones de servidor remoto para autenticación NTLM		(Definida, pero sin ningún valor)	
Seguridad de red: restringir NTLM: auditar el tráfico NTLM entrante		Habilitar la auditoría para todas las cuentas.	
Seguridad de red: restringir NTLM: auditar la autenticación NTLM en este dominio		Habilitar todo	
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio		Denegar todo	
Seguridad de red: restringir NTLM: tráfico NTLM entrante		Permitir todo	
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos		Permitir todo	
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)		Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits	

Comprobación	OK/NOK	Cómo hacerlo		
Directiva		Valor		OK/NOK
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)		Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits		
Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión		Habilitada		
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)		Habilitada		
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)		Habilitada		
Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor		Requerido del cliente		
Servidor de red Microsoft: tiempo de inactividad requerido antes de suspender la sesión		15 minutos		
33.GPO: Compruebe los valores de Administración de derechos digitales de Windows Media.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Administración de derechos digitales de Windows Media”		
		Directiva	Valor	OK/NOK
		Impedir el acceso a Internet de Windows Media DRM	Habilitada	
34.GPO: Compruebe los valores de Cliente WinRM.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Administración remota de Windows (WinRM) → Cliente WinRM”		
		Directiva	Valor	OK/NOK
		Hosts de confianza	Habilitada (Vacío)	
		Permitir tráfico sin cifrar	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
35.GPO: Compruebe los valores de Servicio WinRM.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Administración remota de Windows (WinRM) → Servicio WinRM”		
		Directiva	Valor	OK/NOK
		Activar escucha HTTP de compatibilidad	Deshabilitada	
		Activar escucha HTTPS de compatibilidad	Deshabilitada	
		No permitir que WinRM almacene credenciales de RunAs	Habilitada	
		Permitir la administración de servidores remotos a través de WinRM	Deshabilitada	
		Permitir tráfico sin cifrar	Deshabilitada	
36.GPO: Compruebe los valores de para Agregar características a Windows 10.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10”		
		Directiva	Valor	OK/NOK
		Impedir que el asistente se ejecute	Habilitada	
37.GPO: Compruebe los valores del almacén digital.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el Almacén digital	Habilitada	
38.GPO: Compruebe los valores de Windows Defender.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus Windows Defender	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
39.GPO: Compruebe los valores de análisis de confiabilidad.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Análisis de confiabilidad de Windows”		
		Directiva	Valor	OK/NOK
		Configurar proveedores de WMI de confiabilidad	Habilitada	
40.GPO: Compruebe los valores de Windows Ink.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Área de trabajo de Windows Ink”		
		Directiva	Valor	OK/NOK
		Permitir el Área de trabajo de Windows Ink	Deshabilitada	
		Permitir las aplicaciones sugeridas en el Área de trabajo de Windows Ink	Deshabilitada	
41.GPO: Compruebe los valores de asistencia en línea.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitada	
42.GPO: Compruebe los valores de biometría.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Deshabilitada	
43.Verifique los valores de búsqueda de la directiva.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Buscar”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Deshabilitar la interrupción del indizador		Deshabilitada	
	Impedir la adición automática de carpetas compartidas al índice de Windows Search		Habilitada	
	No buscar en Internet o mostrar resultados de internet en Search		Habilitada	
	Permitir búsqueda en la nube		Deshabilitada	
	Permitir el uso de Cortana		Deshabilitada	
	Permitir el uso de la ubicación para las búsquedas y Cortana		Deshabilitada	
	Permitir usar Cortana sobre la pantalla de bloqueo		Deshabilitada	
	Impedir que los clientes soliciten el índice de forma remota		Habilitada	
44.GPO: Compruebe los valores de la cámara.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Cámara”			
	Directiva		Valor	OK/NOK
	Permitir el uso de la cámara		Deshabilitada	
45.GPO: Compruebe los valores del centro de movilidad de Windows.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows”			
	Directiva		Valor	OK/NOK
	Desactivar Centro de movilidad de Windows		Habilitada	
46.GPO: Compruebe los valores del centro de seguridad.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Centro de seguridad”			
	Directiva		Valor	OK/NOK
	Activar el Centro de seguridad (solo equipos de dominio)		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
47.GPO: Compruebe los valores de cifrado de unidad BitLocker.		En la misma ventana de Conjunto resultante de directivas, compruebe los valores de directiva de grupo indicados en las siguientes tablas y en la ubicación siguiente: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de unidad BitLocker”		
		Directiva	Valor	OK/NOK
		Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [versión 1511] y posteriores)	Habilitada SO: XTS-AES de 256 bits Fijas: XTS-AES de 256 bits Extraíbles: AES-CBC de 256 bits	
		Impedir la sobrescritura de memoria al reiniciar	Deshabilitada	
48.GPO: Compruebe los valores de cifrado de unidad BitLocker en unidades de datos extraíbles.		En la misma ventana de Conjunto resultante de directivas, compruebe los valores de directiva de grupo indicados en las siguientes tablas y en la ubicación siguiente: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades de datos extraíbles”		
		Directiva	Valor	OK/NOK
		Controlar el uso de BitLocker en unidades extraíbles	Deshabilitada	
49.GPO: Compruebe los valores de cifrado de unidad BitLocker en unidades de sistema operativo.		En la misma ventana de Conjunto resultante de directivas, compruebe los valores de directiva de grupo indicados en las siguientes tablas y en la ubicación siguiente: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades del sistema operativo”		
		Directiva	Valor	OK/NOK
		Configurar longitud mínima de PIN para el inicio	Habilitada, 8	
		Configurar perfil de validación de plataforma del TPM para configuraciones de firmware basado en BIOS	Habilitada, 0,2,4,5,7,8,9,10 y 11	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir los PIN mejorados para el inicio	Habilitada	
		Requerir autenticación adicional al iniciar	Habilitada – Requerir PIN de inicio con TPM (No permitir TPM) – Configurar PIN de inicio del TPM (Requerir PIN de inicio con TPM) – Configurar clave de inicio del TPM (No permitir clave de inicio con TPM) – Configurar la clave de inicio y el PIN del TPM (No permitir clave y PIN de inicio con TPM)	
50.GPO: Compruebe los valores de compatibilidad de aplicaciones.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Compatibilidad de aplicaciones”		
		Directiva	Valor	OK/NOK
		Desactivar el Asistente para la compatibilidad de programas	Habilitada	
		Desactivar el motor de compatibilidad de aplicaciones	Habilitada	
		Desactivar el motor de compatibilidad de SwitchBack	Habilitada	
		Desactivar el recopilador de inventario	Habilitada	
		Desactivar la grabación de acciones	Habilitada	
		Desactivar la telemetría de aplicaciones	Habilitada	
		Impedir el acceso a aplicaciones de 16 bits	Habilitada	
		Quitar página de propiedades de compatibilidad de programas	Habilitada	
51.GPO: Compruebe los valores de configuración de Conectar.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Conectar”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	No permitir que se proyecte nada en este PC		Habilitada	
	Solicitar PIN para emparejar dispositivos		Habilitada	
52.GPO: Compruebe los valores de configuración de presentación.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas administrativas → Componentes de Windows → Configuración de presentación"			
	Directiva		Valor	OK/NOK
	Desactivar la configuración de presentación de Windows		Habilitada	
53.GPO: Compruebe los valores de contenido de la nube.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas administrativas → Componentes de Windows → Contenido de la nube"			
	Directiva		Valor	OK/NOK
	Desactivar experiencias del consumidor de Microsoft		Habilitada	
	No mostrar sugerencias de Windows		Habilitada	
54.GPO: Compruebe los valores de reproducción automática.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas administrativas → Componentes de Windows → Directivas de reproducción automática"			
	Nota: Para comprobar las opciones deberá pulsar doble clic sobre cada directiva.			
	Directiva		Valor	OK/NOK
	Desactivar Reproducción automática		Habilitada, (Todas las unidades)	
	Deshabilitar Reproducción automática para dispositivos que no son de volumen		Habilitada	
	Establece el comportamiento predeterminado para la ejecución automática		Habilitada, (No ejecutar ningún comando de ejecución automática)	
	Evitar que reproducción automática recuerde las elecciones del usuario		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
55.GPO: Compruebe los valores del Explorador de archivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Explorador de Archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitada	
		Desactivar la prevención de ejecución de datos para el Explorador	Deshabilitada	
		Desactivar modo protegido de protocolo de shell	Deshabilitada	
		Desactivar terminación del montón al resultar dañado	Deshabilitada	
56.GPO: Compruebe los valores de las versiones anteriores del Explorador de archivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Explorador de Archivos → Versiones anteriores”		
		Directiva	Valor	OK/NOK
		Impedir la restauración de versiones anteriores remotas	Habilitada	
		Ocultar lista de versiones anteriores para archivos remotos	Habilitada	
57.GPO: Compruebe los valores del Explorador de juegos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Explorador de juegos”		
		Directiva	Valor	OK/NOK
		Desactivar el seguimiento del último juego en la carpeta Juegos	Habilitada	
		Desactivar la actualización de juegos	Habilitada	
		Desactivar la descarga de información sobre juegos	Habilitada	
58.GPO: Compruebe los valores de las Fuentes RSS.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Fuentes RSS”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Activar autenticación básica de la fuente a través de HTTP		Deshabilitada	
	Desactivar sincronización en segundo plano para fuentes y Web Slices		Habilitada	
	Impedir acceso a lista de fuentes		Habilitada	
	Impedir descarga de caracteres enmarcados		Habilitada	
	Impedir detección automática de fuentes y Web Slices		Habilitada	
	Impedir suscripción o eliminación de una fuente o Web Slice		Habilitada	
59.Verifique los valores de la grabación y difusión de juegos de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Grabación y difusión de juegos de Windows”		
	Directiva		Valor	OK/NOK
	Habilita o deshabilita la grabación y difusión de juegos de Windows		Deshabilitada	
60.GPO: Verifique los valores de la grabadora de sonidos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos”		
	Directiva		Valor	OK/NOK
	No permitir que se ejecute la grabadora de sonidos		Habilitada	
61.GPO: Verifique los valores del grupo en el hogar.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Grupo en el hogar”		
	Directiva		Valor	OK/NOK
	Impedir que el equipo se una a un grupo en el hogar		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
62.GPO: Verifique los valores de Implementación de paquetes.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Implementación de paquetes de la aplicación”		
		Directiva	Valor	OK/NOK
		Deshabilitar la instalación de aplicaciones para Windows en volúmenes que no sean del sistema	Habilitada	
		Impedir que los datos de aplicaciones de los usuarios se almacenen en volúmenes que no sean del sistema	Habilitada	
		Permitir que una aplicaciones para Windows comparta datos de aplicaciones entre los usuarios	Deshabilitada	
63.GPO: Verifique los valores del informe de errores de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el Informe de errores de Windows	Habilitada	
		No enviar datos adicionales	Habilitada	
64.GPO: Verifique los valores de la interfaz de usuario de credenciales.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Interfaz de usuario de credenciales”		
		Directiva	Valor	OK/NOK
		Enumerar las cuentas de administración al realizar una elevación	Deshabilitada	
		No mostrar el botón revelar contraseña	Habilitado	
65.GPO: Verifique los valores de Mapas.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Mapas”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar el tráfico de red no solicitado en la página de configuración de Mapas sin conexión		Habilitada	
	Desactivar la descarga automática y la actualización de datos de mapa		Habilitada	
66.GPO: Verifique los valores de MDM.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → MDM”		
	Directiva		Valor	OK/NOK
	Deshabilitar la inscripción de MDM		Habilitada	
67.Verifique los valores de Mensajería.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Mensajería”		
	Directiva		Valor	OK/NOK
	Permitir la sincronización en la nube del servicio de mensajería		Deshabilitada	
68.GPO: Verifique los valores de NetMeeting.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → NetMeeting”		
	Directiva		Valor	OK/NOK
	Deshabilitar el uso compartido de escritorio remoto		Habilitada	
69.GPO: Verifique los valores de las opciones de One Drive.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → One Drive”		
	Directiva		Valor	OK/NOK
	Impedir el uso de OneDrive para almacenar archivos		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
70.GPO: Verifique los valores de las opciones de inicio de sesión de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar o habilitar la secuencia de aviso de seguridad de software	Habilitada (Ninguno)	
		Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario	Deshabilitada	
		Iniciar sesión automáticamente con el último usuario interactivo después de un reinicio iniciado por el sistema	Deshabilitada	
		Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	Habilitada	
71.GPO: Verifique los valores de la plataforma de protección de software.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Plataforma de protección de software”		
		Directiva	Valor	OK/NOK
		Controlar la reactivación de dispositivos comerciales	Habilitada	
72.GPO: Verifique los valores de Privacidad de aplicación.		Desactivar validación AVS en línea del cliente KMS	Habilitada	
		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas administrativas → Componentes de Windows → Privacidad de la aplicación” Nota: Para comprobar las opciones deberá pulsar doble clic sobre cada directiva.		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a la cámara	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows se sincronicen con dispositivos	Habilitada (Force Deny)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitada (Force Deny)	
73.GPO: Verifique los valores del programa para la mejora de la experiencia del usuario.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Programa para la mejora de la experiencia del usuario de Windows”		
		Directiva	Valor	OK/NOK
		Permitir la redirección corporativa de las cargas para la mejora de la experiencia del usuario	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
74.GPO: Verifique los valores de Recopilación de datos y versiones preliminares.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Recopilación de datos y versiones preliminares”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Alternar control de usuario sobre compilaciones de Insider	Deshabilitada	
		No volver a mostrar notificaciones de comentarios	Habilitada	
	Permitir Telemetría	Habilitada (0: Seguridad [solo empresas])		
75.GPO: Verifique los valores del cliente de conexión a escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Cliente de conexión a escritorio remoto”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Configurar la autenticación del servidor para el cliente	Habilitada (No conectarse si hay errores de autenticación)	
		No permitir que se guarden las contraseñas	Habilitada	
	Permitir archivos .rdp de publicadores desconocidos	Deshabilitada		
76.GPO: Verifique los valores de las conexiones de Host de sesión de Escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Conexiones”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que los usuarios se conecten de forma remota mediante Servicios de Escritorio remoto	Deshabilitada	
77.GPO: Verifique los valores de la redirección de dispositivos o recursos de Host de sesión de Escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Redirección de dispositivo o recurso”		
		Directiva	Valor	OK/NOK
		No permitir redirección de unidad	Habilitada	
78.GPO: Verifique los valores de la seguridad de Host de sesión de Escritorio.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Seguridad” Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Establecer el nivel de cifrado de conexión de cliente	Habilitada (Nivel alto)	
		Requerir comunicación RPC segura	Habilitada	
		Requerir la autenticación del usuario para las conexiones remotas mediante Autenticación a nivel de red	Habilitada	
		Solicitar la contraseña siempre al conectar	Habilitada	
79.GPO: Verifique los valores del Shell remoto de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Shell Remoto de Windows”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Especificar número máximo de shells remoto por usuario	Habilitada, (MaxShellsPerUser: 1)	
		MaxConcurrentUsers	Habilitada (MaxConcurrentUsers: 1)	
		Permitir acceso a shell remoto	Deshabilitada	
80.GPO: Verifique los valores de Sincronizar la configuración.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Sincronizar la configuración”		
		Directiva	Valor	OK/NOK
		No sincronizar	Habilitada, (Permitir a los usuarios activar la sincronización: Deshabilitado))	
81.GPO: Verifique los valores de Accesorios.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Tablet PC → Accesorios”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute Windows Journal	Deshabilitada	
82.GPO: Verifique los valores de tarjeta inteligente.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Tarjeta inteligente”		
		Directiva	Valor	OK/NOK
		Activar servicio Plug and Play de tarjeta inteligente	Deshabilitada	
83.GPO: Verifique los valores de la tienda.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitada	
		Deshabilitar todas las aplicaciones de Microsoft Store	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
84.GPO: Verifique los valores de ubicación y sensores.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
85.GPO: Verifique los valores del servicio de localización de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores → Servicio de localización de Windows”		
		Directiva	Valor	OK/NOK
		Desactivar el Servicio de localización de Windows	Habilitada	
86.GPO: Verifique los valores de virtualización de la experiencia del usuario de Microsoft.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Virtualización de la experiencia del usuario de Microsoft”		
		Directiva	Valor	OK/NOK
		Configuración de sincronización de Windows	Deshabilitada	
		No sincronizar aplicaciones de Windows	Habilitada	
		Sincronizar aplicaciones de Windows que no aparecen en la lista	Deshabilitada	
		Sincronizar configuración en conexiones de uso medido	Deshabilitada	
		Sincronizar configuración en conexiones de uso medido incluso si son móviles	Deshabilitada	
		Usar User Experience Virtualization (UE-V)	Deshabilitada	
87.GPO: Verifique los valores de Windows Hello.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Hello para empresas”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Usa Windows Hello para empresas	Deshabilitada	
		Usar biometría	Deshabilitada	
88.GPO: Verifique los valores de Windows Installer.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Installer”		
		Directiva	Valor	OK/NOK
		Impedir advertencias de seguridad de Internet Explorer para Scripts de Windows Installer	Deshabilitada	
		Impedir que los usuarios usen Windows Installer para instalar actualizaciones	Habilitada	
		Instalar siempre con privilegios elevados	Deshabilitada	
		Permitir a los usuarios aplicar revisiones a productos con privilegios elevados	Deshabilitada	
		Permitir a los usuarios buscar el origen cuando tienen privilegios elevados	Deshabilitada	
		Permitir a los usuarios usar el origen de medios cuando tienen privilegios elevados	Deshabilitada	
		Permitir el control del usuario sobre las instalaciones	Deshabilitada	
		Prohibir a los usuarios que no son administradores la aplicación de actualizaciones firmadas por los proveedores	Habilitada	
89.GPO: Verifique los valores de Windows Messenger.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Messenger”		
		Directiva	Valor	OK/NOK
		No ejecutar automáticamente Windows Messenger al inicio	Habilitada	
		No permitir que se ejecute Windows Messenger	Habilitada	
90.GPO: Verifique los valores de Windows Update.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Componentes de Windows → Windows Update”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar Actualizaciones automáticas	Deshabilitada	
91.GPO: Verifique los valores de Impresoras.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Impresoras”		
		Directiva	Valor	OK/NOK
		Ejecutar controladores de impresión en procesos aislados	Habilitado	
		Permitir que se publiquen impresoras	Deshabilitado	
92.Verifique los valores de Notificaciones.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Menú inicio y barra de tareas → Notificaciones”		
		Directiva	Valor	OK/NOK
		Desactivar el uso de la red para notificaciones	Habilitada	
93.Verifique los valores del Panel de control.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Panel de control”		
		Directiva	Valor	OK/NOK
		Permitir recomendaciones en línea	Deshabilitada	
94.GPO: Verifique los valores de Configuración regional e idioma.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma”		
		Directiva	Valor	OK/NOK
		Permitir que los usuarios habiliten servicios de reconocimiento de voz en línea	Deshabilitada	
95.GPO: Verifique los valores de Personalización de escritura a mano.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitada	
96.Verifique los valores de Personalización.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Panel de control → Personalización”		
		Directiva	Valor	OK/NOK
		Evitar la activación de la cámara de la pantalla de bloqueo	Habilitada	
97.Verifique los valores del administrador de conexiones de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Administrador de conexiones de Windows”		
		Directiva	Valor	OK/NOK
		Prohibir la conexión a redes de banda ancha móvil de proveedores móviles	Habilitada	
98.GPO: Verifique los valores de archivos sin conexión.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Archivos sin conexión”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Especificar archivos sin conexión asignados de forma administrativa	Deshabilitada	
		Permitir o denegar el uso de la característica Archivos sin conexión	Deshabilitada	
		Quitar el comando “Disponible sin conexión”	Habilitada	
		Subcarpetas siempre disponibles sin conexión	Deshabilitada	
99.GPO: Verifique los valores de BranchCache.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → BranchCache”		
		Directiva	Valor	OK/NOK
		Activar BranchCache	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
100.GPO: Verifique los valores del perfil de firewall de dominio.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Conexiones de Red → Firewall de Windows Defender → Perfil de dominio” Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Firewall de Windows Defender: No permitir excepciones	Habilitada	
		Firewall de Windows Defender: No permitir notificaciones	Habilitada	
		Firewall de Windows Defender: No permitir respuesta de unidifusión a peticiones de difusión o multidifusión	Deshabilitada	
		Firewall de Windows Defender: Permitir registro	Habilitada (Registro de paquetes perdidos – Deshabilitado) (Registro de conexiones correctas – Deshabilitado) (Ruta y nombre de archivos de registro: %systemroot%\system32\Log Files\Firewall\pfirewall.log) (Límite de tamaño: 4096 KB)	
		Firewall de Windows Defender: Proteger todas las conexiones de red	Habilitada	
101.GPO: Verifique los valores del perfil de firewall estándar.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Conexiones de Red → Firewall de Windows Defender → Perfil estándar”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Firewall de Windows Defender: No permitir excepciones	Habilitada	
		Firewall de Windows Defender: No permitir notificaciones	Habilitada	
		Firewall de Windows Defender: No permitir respuesta de unidifusión a peticiones de difusión o multidifusión	Deshabilitada	
		Firewall de Windows Defender: Permitir registro	Habilitada (Registro de paquetes perdidos – Deshabilitado) (Registro de conexiones correctas – Deshabilitado) (Ruta y nombre de archivos de registro: %systemroot%\system32\Log Files\Firewall\pfirewall.log) (Límite de tamaño: 4096 KB)	
		Firewall de Windows Defender: Proteger todas las conexiones de red	Habilitada	
102.GPO: Verifique los valores de las tecnologías de transición a IPv6.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Configuración de TCPIP → Tecnologías de transición IPv6” Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Estado de 6to4	Habilitada (Estado Deshabilitado)	
		Estado de IP-HTTPS	Habilitada URL: ""(espacio en blanco), (Estado Deshabilitado)	
		Estado de ISATAP	Habilitada (Estado Deshabilitado)	
		Estado de Teredo	Habilitada (Estado Deshabilitado)	

Comprobación	OK/NOK	Cómo hacerlo		
103.GPO: Verifique los valores de la detección de topologías a nivel de vínculo.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Detección de topologías de nivel de vínculo”		
		Directiva	Valor	OK/NOK
		Activar controlador de E/S de asignador (LLTDIO)	Deshabilitada	
		Activar controlador de respuesta (RSPNDR)	Deshabilitada	
104.GPO: Verifique los valores de la estación de trabajo Lanman.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Estación de trabajo Lanman”		
		Directiva	Valor	OK/NOK
		Habilitar inicios de sesión de invitado no seguros	Deshabilitada	
105.GPO: Verifique los valores de Fuentes.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Fuentes”		
		Directiva	Valor	OK/NOK
		Habilitar Proveedores de fuentes	Deshabilitada	
106.GPO: Verifique los valores de Proyección inalámbrica.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Proyección inalámbrica”		
		Directiva	Valor	OK/NOK
		Requerir emparejamiento de PIN	Habilitada	
107.GPO: Verifique los valores de Configuración WLAN.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Servicio WLAN → Configuración WLAN”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permite que Windows se conecte automáticamente a puntos de acceso abiertos sugeridos, redes compartidas por los contactos y puntos de acceso que ofrezcan servicios de pago	Habilitada	
108.Verifique los valores de Acceso a datos móviles de la directiva "CCN-STIC-599B19 Windows 10 - Equipos".		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servicio WWAN → Acceso a datos móviles"		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows tiene acceso a los datos móviles	Habilitada (Forzar denegación)	
109.Verifique los valores de Configuración de la interfaz de usuario de WWAN.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servicio WWAN → Configuración de la interfaz de usuario de WWAN"		
		Directiva	Valor	OK/NOK
		Establecer la visibilidad de interfaz de usuario de acceso de red de telefonía móvil por aplicación	Habilitada (Ocultar)	
110.GPO: Verifique los valores de los servicios de redes de igual a igual de Microsoft.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Red → Servicios de redes de igual a igual de Microsoft"		
		Directiva	Valor	OK/NOK
		Desactivar los Servicios de redes de igual a igual de Microsoft	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
111.GPO: Verifique los valores del servidor Lanman.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Servidor Lanman”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Publicación de hash para BranchCache	Habilitada (No permitir la publicación de hash en ninguna carpeta compartida)	
112.GPO: Verifique los valores de Windows Connect Now.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Red → Windows Connect Now”		
		Directiva	Valor	OK/NOK
		Prohibir el acceso de los asistentes de Windows Connect Now	Habilitada	
113.GPO: Verifique los valores de Acceso de almacenamiento extraíble.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Acceso de almacenamiento extraíble”		
		Directiva	Valor	OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitada	
114.GPO: Verifique los valores de la administración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Restringir comunicaciones de Internet	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
115.GPO: Verifique los valores de la configuración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Desactivar al Asistente para la conexión a Internet si la conexión de direcciones URL hace referencia a Microsoft.com	Habilitada	
		Desactivar descargas de Internet de los asistentes para la publicación en Web y pedidos en línea	Habilitada	
		Desactivar el acceso a Store	Habilitada	
		Desactivar el acceso a todas las características de Windows Update	Habilitada	
		Desactivar el contenido "¿Sabía que...?" del Centro de ayuda y soporte técnico	Habilitada	
		Desactivar el informe de errores de Windows	Habilitada	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows	Habilitada	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger	Habilitada	
		Desactivar el registro si la conexión de direcciones URL hace referencia a Microsoft.com	Habilitada	
		Desactivar el servicio de asociaciones de archivo de Internet	Habilitada	
		Desactivar impresión a través de HTTP	Habilitada	
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitada	
		Desactivar la actualización automática de certificados raíz	Habilitada	
		Desactivar la actualización de archivos de contenido del Asistente para búsqueda	Habilitada	
		Desactivar la búsqueda de controladores de dispositivos en Windows Update	Habilitada	
		Desactivar la búsqueda en Microsoft Knowledge Base del Centro de Ayuda y soporte técnico	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar la descarga de controladores de impresión a través de HTTP	Habilitada	
		Desactivar la tarea "Publicar en Web" para archivos y carpetas	Habilitada	
		Desactivar la tarea de imágenes "Pedir copias fotográficas"	Habilitada	
		Desactivar los vínculos "Events.asp" del Visor de eventos	Habilitada	
		Desactivar pruebas activas del Indicador de estado de conectividad de la red de Windows	Habilitada	
		Desactivar uso compartido de datos de personalización de escritura a mano	Habilitada	
116.GPO: Verifique los valores de App-V.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Sistema → App-V"		
		Directiva	Valor	OK/NOK
		Habilitar el cliente de App-V	Deshabilitada	
117.GPO: Verifique los valores de asistencia remota.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Sistema → Asistencia Remota"		
		Directiva	Valor	OK/NOK
		Asistencia remota solicitada	Deshabilitada	
		Configurar ofrecer Asistencia remota	Deshabilitada	
118.GPO: Verifique los valores de directiva de grupo.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del equipo → Plantillas Administrativas → Sistema → Directiva de grupo"		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar el procesamiento de directivas de mantenimiento de Internet Explorer	Habilitada (Procesar incluso si los objetos de directiva de grupo no han cambiado)	
		Configurar el procesamiento de directivas de seguridad	Habilitada (Procesar incluso si los objetos de directiva de grupo no han cambiado)	
		Configurar el procesamiento de directivas del Registro	Habilitada (Procesar incluso si los objetos de directiva de grupo no han cambiado)	
		Continuar experiencias en este dispositivo	Deshabilitado	
119.Verifique los valores de directiva del sistema operativo.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Directiva del sistema operativo”		
		Directiva	Valor	OK/NOK
		Permitir historial del Portapapeles	Deshabilitada	
		Permitir la sincronización del portapapeles entre dispositivos	Deshabilitada	
		Habilita la fuente de actividades	Deshabilitada	
		Permitir la publicación de las actividades del usuario	Deshabilitada	
		Permitir la carga de actividades del usuario	Deshabilitada	
120.GPO: Verifique los valores de inicio de sesión.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Inicio de sesión”		
		Directiva	Valor	OK/NOK
		Desactivar inicio de sesión con contraseña de imagen	Habilitada	
		Desactivar las notificaciones de aplicaciones en la pantalla de bloqueo	Habilitada	
		Evitar que el usuario muestre detalles de la cuenta al iniciar sesión	Habilitada	
		Mostrar animación de primer inicio de sesión	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	No mostrar la interfaz de usuario de selección de red		Habilitada	
	No procesar la lista de ejecución heredada		Habilitada	
	No procesar la lista de una sola ejecución		Habilitada	
	Ocultar puntos de entrada para el Cambio rápido de usuario		Habilitada	
121.GPO: Verifique los valores de instalación de dispositivos.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Instalación de dispositivos”			
	Directiva		Valor	OK/NOK
	Permitir acceso remoto a la interfaz Plug and Play		Deshabilitada	
122.GPO: Verifique los valores de restricciones de instalación de dispositivos.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”			
	Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.			
	Directiva		Valor	OK/NOK
	Impedir la instalación de dispositivos no descritos por otras configuraciones de directiva		Habilitada	
	Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. De dispositivo		Habilitada (Crear lista de id - espacio en blanco para crear lista)	
	Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos		Deshabilitada	
123.GPO: Verifique los valores de la llamada a procedimiento remoto.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Llamada a procedimiento remoto”			



Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Autenticación de clientes del Asignador de extremos de RPC	Habilitada	
		Restricciones para clientes de RPC no autenticados	Habilitada (Autenticado)	
124.Verifique los valores de Net Logon.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Net Logon”		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada	
125.GPO: Verifique los valores de Perfiles de usuario.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Perfiles de Usuario”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Administración del usuario del uso compartido del nombre de usuario, imagen de cuenta e información del dominio con aplicaciones (que no sean aplicaciones de escritorio)	Habilitada (Siempre desactivado)	
		Desactivar el identificador de publicidad	Habilitada	
126.Verifique los valores de Servicios de configuración regional.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Servicios de configuración regional”		
		Directiva	Valor	OK/NOK
		Denegar el cambio de ubicación geográfica	Habilitada	
127.Verifique los valores de Herramienta de diagnóstico.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del equipo → Plantillas Administrativas → Sistema → Solución de problemas y diagnósticos → Herramienta de diagnóstico para soporte técnico de Microsoft”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Herramienta de diagnóstico para soporte técnico de Microsoft: activar la comunicación interactiva de la herramienta MSDT con el proveedor de soporte técnico		Deshabilitada	
	Herramienta de diagnóstico para soporte técnico de Microsoft: configurar nivel de ejecución		Deshabilitada	
	Herramienta de diagnóstico para soporte técnico de Microsoft: restringir descarga de herramientas		Deshabilitada	
128.GPO: Verifique los valores de Carpetas compartidas.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Carpetas compartidas”			
	Directiva		Valor	OK/NOK
	Permitir publicación de carpetas compartidas		Deshabilitada	
	Permitir publicación de raíces DFS		Deshabilitada	
129.GPO: Verifique los valores del administrador de datos adjuntos.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Administrador de datos adjuntos”			
	Directiva		Valor	OK/NOK
	Confiar en la lógica de datos adjuntos de archivos		Habilitada, Examinar controlador y tipo de archivo	
	Nivel de riesgo predeterminado de los datos adjuntos de archivo		Habilitada, Alto riesgo	
	No conservar la información de zona en los datos adjuntos de archivo		Deshabilitada	
	Notificar a los programas antivirus cuando se abren datos adjuntos		Habilitada	
	Ocultar mecanismos para eliminar la información de zona		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
130.Verifique los valores para Agregar características		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10”		
		Directiva	Valor	OK/NOK
		Impedir que el asistente se ejecute	Habilitada	
131.GPO: Verifique los valores del almacén digital.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el Almacén digital	Habilitada	
132.GPO: Verifique los valores del centro de movilidad de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows”		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	
133.GPO: Verifique los valores de la compatibilidad de aplicaciones.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Compatibilidad de aplicaciones”		
		Directiva	Valor	OK/NOK
		Desactivar el Asistente para la compatibilidad de programas	Habilitada	
134.GPO: Verifique los valores de la configuración de presentación.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Configuración de presentación”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
135.Verifique los valores de la configuración de nube.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Contenido de la nube”		
		Directiva	Valor	OK/NOK
		Configurar Contenido destacado de Windows en la pantalla de bloqueo	Deshabilitada	
		Desactivar todas las ventanas de Contenido destacado de Windows	Habilitada	
		No sugerir contenido de terceros en el contenido destacado de Windows	Habilitada	
136.GPO: Verifique los valores de las directivas de reproducción.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar Reproducción automática	Habilitada, Todas las unidades	
		Deshabilitar Reproducción automática para dispositivos que no son de volumen	Habilitada	
		Establece el comportamiento predeterminado para ejecución automática	Habilitada, No ejecutar ningún comando de ejecución automática	
		Evitar que Reproducción automática recuerde las elecciones del usuario	Habilitada	
137.GPO: Verifique los valores del explorador de archivos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Archivos”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar el almacenamiento en caché de imágenes en miniatura		Habilitada	
	Desactivar la presentación de miniaturas y mostrar sólo iconos		Habilitada	
	Desactivar la presentación de miniaturas y mostrar sólo iconos en las carpetas de red		Habilitada	
	Desactivar modo protegido de protocolo de shell		Deshabilitada	
	Desactivar todas las características de bibliotecas de Windows que dependan de datos de archivos indizados		Habilitada	
	Mostrar el dialogo de confirmación al eliminar archivos		Habilitada	
	No mover los archivos eliminados a la papelera de reciclaje		Habilitada	
	Quitar la pestaña seguridad		Habilitada	
	Quitar las características de grabación de CD		Habilitada	
138.Verifique los valores de diálogo común para abrir archivos.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de archivos → Diálogo común para abrir archivos”			
	Directiva		Valor	OK/NOK
	Ocultar la lista desplegable de archivos recientes		Habilitada	
139.GPO: Verifique los valores del panel de marcos del explorador.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Archivos → Panel de marcos del explorador”			
	Directiva		Valor	OK/NOK
	Desactivar el panel de vista previa		Habilitada	
140.GPO: Verifique los valores de las versiones anteriores del explorador de Windows.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Windows → Versiones anteriores”			

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir la restauración de versiones anteriores remotas	Habilitada	
		Ocultar lista de versiones anteriores para archivos remotos	Habilitada	
141.GPO: Verifique los valores de las fuentes RSS.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Fuentes RSS”		
		Directiva	Valor	OK/NOK
		Activar autenticación básica de la fuente a través de HTTP	Deshabilitada	
		Desactivar sincronización en segundo plano para fuentes y Web Slices	Habilitada	
		Impedir acceso a lista de fuentes	Habilitada	
		Impedir descarga de caracteres enmarcados	Habilitada	
		Impedir detección automática de fuentes y Web Slices	Habilitada	
		Impedir suscripción o eliminación de una fuente o Web Slice	Habilitada	
142.GPO: Verifique los valores de la grabadora de sonidos.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute la grabadora de sonidos	Habilitada	
143.GPO: Verifique los valores del informe de errores de Windows.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el Informe de errores de Windows	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
144.Verifique los valores de la interfaz de credenciales.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Interfaz de usuario de credenciales”		
		Directiva	Valor	OK/NOK
		No mostrar el botón revelar contraseña	Habilitada	
145.GPO: Verifique los valores de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console”		
		Directiva	Valor	OK/NOK
		Restringir a los usuarios a la lista de complementos con permisos explícitos	Habilitada	
		Restringir al usuario la entrada al modo de autor	Habilitada	
146.GPO: Verifique los valores de los complementos restringidos o permitidos de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Complementos restringidos o permitidos”		
		Directiva	Valor	OK/NOK
		Administración de almacenamiento extraíble	Deshabilitado	
		Administración de directivas de seguridad IP	Habilitado	
		Administración de discos	Habilitado	
		Administración de equipos	Habilitado	
		Administración de TPM	Deshabilitado	
		Administrador de clúster de conmutación por error	Deshabilitado	
		Administrador de dispositivos	Habilitado	
		Administrador del servidor	Deshabilitado	
		Autoridad de registro de mantenimiento (HRA)	Deshabilitado	
		Carpetas compartidas	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Directiva	Valor
		OK/NOK	
		Certificados	Deshabilitado
		Configuración de .Net Framework	Habilitado
		Configuración de Servicios de Escritorio remoto	Habilitado
		Configuración del cliente de NAP	Deshabilitado
		Configuración y análisis de seguridad	Habilitado
		Control ActiveX	Deshabilitado
		Control de admisión QoS	Deshabilitado
		Control WMI	Deshabilitado
		Desfragmentador de discos	Deshabilitado
		Dominios y confianza de Active Directory	Deshabilitado
		Edición de ADSI	Deshabilitado
		Enrutamiento y acceso remoto	Habilitado
		Entidad de certificación	Deshabilitado
		Escritorios remotos	Deshabilitado
		Extensiones de servidor de FrontPage	Deshabilitado
		Firewall de Windows con seguridad avanzada	Habilitado
		Información del sistema	Deshabilitado
		Internet Information Services	Deshabilitado
		Monitor de seguridad IP	Deshabilitado
		Monitor inalámbrico	Deshabilitado
		PKI de empresa	Deshabilitado
		Plantillas de certificado	Deshabilitado
		Plantillas de seguridad	Habilitado
		Registros y alertas de rendimiento	Deshabilitado
		Servicio de Fax	Habilitado
		Servicio de respuesta en línea	Deshabilitado
		Servicios	Habilitado
		Servicios de componente	Deshabilitado
		Servicios de Index Server	Deshabilitado
		Servidor de directivas de redes (NPS)	Deshabilitado
		Sistema de archivos distribuido	Deshabilitado
		Sitios y servicios de Active Directory	Deshabilitado
		Telefonía	Habilitado
		Usuarios y equipos de Active Directory	Deshabilitado
		Usuarios y grupos locales	Habilitado
		Vínculo a la dirección web	Deshabilitado
		Visor de eventos (Windows Vista)	Habilitado
		Visor de eventos	Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
147.GPO: Verifique los valores de directiva de grupo de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Complementos restringidos o permitidos → Directiva de grupo”		
		Directiva	Valor	OK/NOK
		Administración de directivas de grupo	Habilitada	
		Editor de objetos de directiva de grupo	Habilitada	
		Conjunto resultante de directivas	Habilitada	
148.GPO: Verifique los valores de las extensiones de complemento de directivas de grupo de Microsoft Management Console.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console → Complementos restringidos o permitidos → Directiva de grupo → Extensiones de complemento de directivas de grupo”		
		Directiva	Valor	OK/NOK
		Configuración de Seguridad	Habilitada	
		Firewall de Windows con seguridad avanzada	Habilitada	
		Plantillas Administrativas (equipos)	Habilitada	
		Plantillas Administrativas (usuarios)	Habilitada	
149.GPO: Verifique los valores de NetMeeting.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting”		
		Directiva	Valor	OK/NOK
		Deshabilitar chat	Habilitada	
		Deshabilitar Pizarra	Habilitada	
		Deshabilitar Pizarra de NetMeeting 2.x	Habilitada	
		Deshabilitar servicios de directorio	Habilitada	
		Impedir el envío de archivos	Habilitada	
		Impedir la aceptación automática de llamadas	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Impedir la adición de servidores de directorio		Habilitada	
	Impedir la modificación del método de realización de llamada		Habilitada	
	Impedir la recepción de archivos		Habilitada	
	Impedir ver el directorio web		Habilitada	
	Audio y video\Deshabilitar audio		Habilitada	
	Audio y video\Deshabilitar audio de dúplex completo		Habilitada	
	Audio y video\Impedir el envío de vídeo		Habilitada	
	Audio y video\Impedir la recepción de vídeo		Habilitada	
150.GPO: Verifique los valores de audio y video de NetMeeting.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting → Audio y vídeo”			
	Directiva		Valor	OK/NOK
	Deshabilitar audio		Habilitada	
	Deshabilitar audio de dúplex completo		Habilitada	
	Impedir el envío de vídeo		Habilitada	
	Impedir la recepción de vídeo		Habilitada	
151.GPO: Verifique los valores de compartir aplicaciones a través de NetMeeting.	Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting → Compartir aplicaciones”			
	Directiva		Valor	OK/NOK
	Deshabilitar el uso compartido de aplicaciones		Habilitada	
	Impedir el control		Habilitada	
	Impedir el uso compartido		Habilitada	
	Impedir el uso compartido de las ventanas del Explorador		Habilitada	
	Impedir el uso compartido de símbolos del sistema		Habilitada	
	Impedir el uso compartido del escritorio		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
152.GPO: Verifique los valores de la página de opciones de NetMeeting.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → NetMeeting → Página de opciones”		
		Directiva	Valor	OK/NOK
		Deshabilitar el botón Llamada avanzada	Habilitada	
		Ocultar la página General	Habilitada	
		Ocultar la página Seguridad	Habilitada	
153.GPO: Verifique los valores del cliente de conexión a escritorio remoto.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Servicios de escritorio remoto → Cliente de conexión a Escritorio remoto”		
		Directiva	Valor	OK/NOK
		No permitir que se guarden las contraseñas	Habilitada	
154.Verifique los valores de Accesorios.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Tablet PC → Accesorios”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute Windows Journal	Habilitada	
155.Verifique los valores de Tienda.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitada	
		Desactivar la oferta para actualizar a la versión de Windows más reciente	Habilitada	
156.GPO: Verifique los valores de ubicación y sensores.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Ubicación y sensores”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
157.GPO: Verifique los valores de uso compartido de red.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Uso compartido de red”		
		Directiva	Valor	OK/NOK
		Impedir que los usuarios compartan archivos dentro de su perfil	Habilitada	
158.GPO: Verifique los valores de virtualización de la experiencia del usuario de Microsoft.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas Administrativas → Componentes de Windows → Virtualización de la experiencia del usuario de Microsoft”		
		Directiva	Valor	OK/NOK
		Configuración de sincronización de Windows	Deshabilitada	
		No sincronizar aplicaciones de Windows	Habilitada	
		Sincronizar configuración en conexiones de uso medido	Deshabilitada	
		Sincronizar configuración en conexiones de uso medido incluso si son móviles	Deshabilitada	
		Usar User Experience Virtualization (UE-V)	Deshabilitada	
159.GPO: Verifique los valores de Windows Messenger.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Windows Messenger”		
		Directiva	Valor	OK/NOK
		No ejecutar automáticamente Windows Messenger al inicio	Habilitada	
		No permitir que se ejecute Windows Messenger	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
160.GPO: Verifique los valores de Windows Update.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Windows Update”		
		Nota: En algunas de las directivas se deberá pulsar doble clic sobre ellas para comprobar la opción de configuración seleccionada.		
		Directiva	Valor	OK/NOK
		Quitar el acceso a todas las características de Windows Update	Habilitada, (0 – No mostrar ninguna notificación)	
161.GPO: Verifique los valores del menú Inicio y barra de tareas.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Menú Inicio y barra de tareas”		
		Directiva	Valor	OK/NOK
		Borrar historial de los documentos abiertos recientemente al salir	Habilitada	
		Borrar lista de programas recientes para nuevos usuarios	Habilitada	
		No guardar historial de documentos abiertos recientemente.	Habilitada	
		Quitar vínculos y accesos a Windows Update	Habilitada	
162.GPO: Verifique los valores del Panel de Control.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Panel de Control”		
		Directiva	Valor	OK/NOK
		Abrir siempre Todos los elementos del Panel de control al abrir el Panel de control	Habilitada	
163.GPO: Verifique los valores de las impresoras.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Panel de Control → Impresoras”		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Impedir la adición de impresoras		Habilitada	
	Impedir la eliminación de impresoras		Habilitada	
164.Verifique los valores de personalización.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Panel de Control → Programas”		
	Directiva		Valor	OK/NOK
	Ocultar "Características de Windows"		Deshabilitada	
165.GPO: Verifique los valores de archivos sin conexión a la red.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Red → Archivos sin conexión”		
	Directiva		Valor	OK/NOK
	Especificar Archivos sin conexión asignados de forma administrativa		Deshabilitada	
	Quitar el comando “Disponible sin conexión”		Habilitada	
	Quitar el comando “Trabajar sin conexión”		Habilitada	
166.Verifique los valores de Windows Connect Now.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración del usuario → Plantillas administrativas → Red → Windows Connect Now”		
	Directiva		Valor	OK/NOK
	Prohibir el acceso a los asistentes de Windows Connect Now		Habilitada	
167.GPO: Verifique los valores de sistema.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema”		
	Directiva		Valor	OK/NOK
	Descargar componentes COM que faltan		Deshabilitada	
	Impedir el acceso a herramientas de edición del Registro		Habilitada, No (¿Desea deshabilitar la ejecución sin notificación de regedit?)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir el acceso al símbolo del sistema	Habilitada, No (¿Desea desactivar también el procesamiento de scripts del símbolo del sistema?)	
168.GPO: Verifique los valores de acceso de almacenamiento extraíble.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble”		
		Directiva	Valor	OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Deshabilitada	
169.GPO: Verifique los valores de administración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Administración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Restringir comunicación de Internet	Habilitada	
170.GPO: Verifique los valores de configuración de comunicaciones de Internet.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: “Configuración de usuario → Plantillas administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Desactivar clasificaciones de la ayuda	Habilitada	
		Desactivar descargas de Internet de los asistentes para la publicación en Web y pedidos en línea	Habilitada	
		Desactivar el programa de mejora de la Ayuda	Habilitada	
		Desactivar el Programa para la mejora de la experiencia del usuario de Windows Messenger	Habilitada	
		Desactivar impresión a través de HTTP	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar informe de errores de reconocimiento de escritura a mano	Habilitada	
		Desactivar la descarga de controladores de impresión a través de HTTP	Habilitada	
		Desactivar la tarea "Publicar en Web" para archivos y carpetas	Habilitada	
		Desactivar la tarea de imágenes "Pedir copias fotográficas"	Habilitada	
		Desactivar uso compartido de datos de personalización de escritura a mano	Habilitada	
		Desactivar Windows Online	Habilitada	
171.GPO: Verifique los valores de Ctrl+Alt+Supr.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración de usuario → Plantillas administrativas → Sistema → Opciones de Ctrl+Alt+Supr"		
		Directiva	Valor	OK/NOK
		Quitar Administrador de tareas	Habilitada	
172.Verifique los valores de Servicios de configuración regional.		Compruebe los valores indicados en la siguiente tabla, en la siguiente ubicación del GPO en la ventana del Editor de directivas de grupo local: "Configuración del usuario → Plantillas administrativas → Sistema → Servicios de configuración regional"		
		Directiva	Valor	OK/NOK
		Denegar el cambio de ubicación geográfica	Habilitada	
173.Realice la comprobación de los valores de Internet Explorer 11.		Compruebe los valores de la lista de comprobación de la guía "CCN-STIC-520 Internet Explorer 11" para verificar la correcta configuración de dicho componente.		
174.Borre "C:\Scripts".		Borre el directorio "C:\Scripts" con todo su contenido.		
175.Reinicie el equipo.		Reinicie el equipo que está comprobando. De esta manera volverán a aplicarse las restricciones sobre las consolas de administración y el equipo quedará en el mismo estado en el que estaba antes de realizar la lista de comprobación.		

ANEXO D.2. APLICACIÓN DE NIVELES DE CLASIFICACIÓN

Este Anexo define el procedimiento a seguir para realizar una configuración específica para el sistema operativo Microsoft Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC en función del nivel de clasificación asignado al equipo según la normativa legal vigente que regula el uso de la información clasificada en equipos informáticos. Los niveles de clasificación disponibles para su aplicación a través de esta guía son los siguientes:

- a) CONFIDENCIAL.
- b) RESERVADO O SUPERIOR.

Antes de proceder a realizar la configuración, deberá conocer el nivel de clasificación del equipo que está securizando con el objeto de aplicar la configuración de seguridad adecuada.

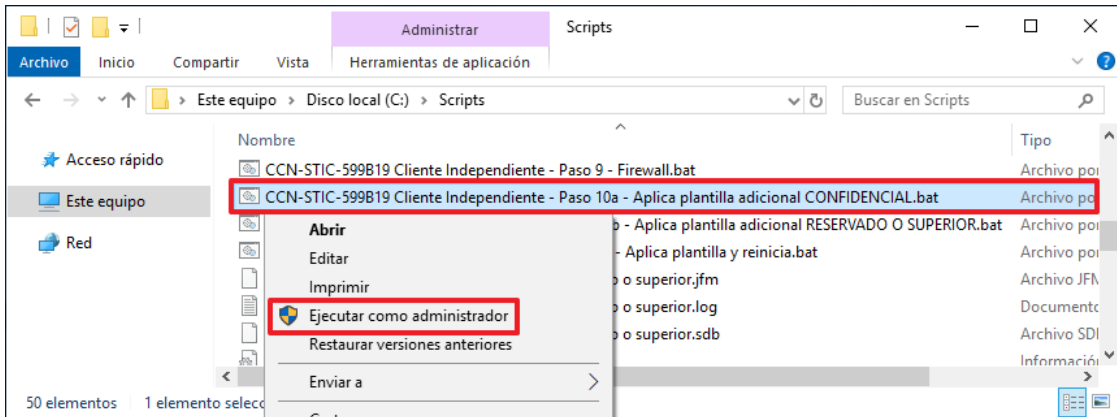
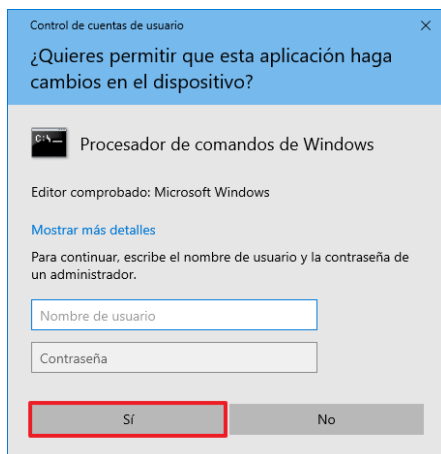
Nota: Si el nivel de clasificación del equipo no se encuentra en el listado de opciones indicadas, deberá establecer la configuración equivalente o superior.

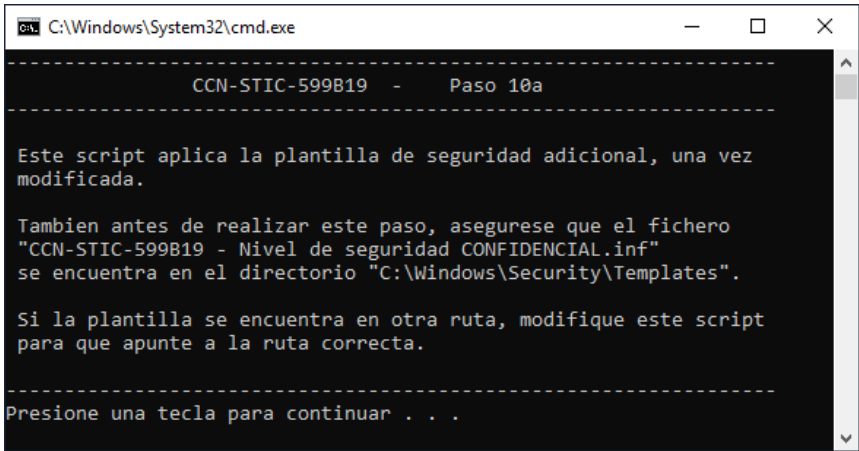
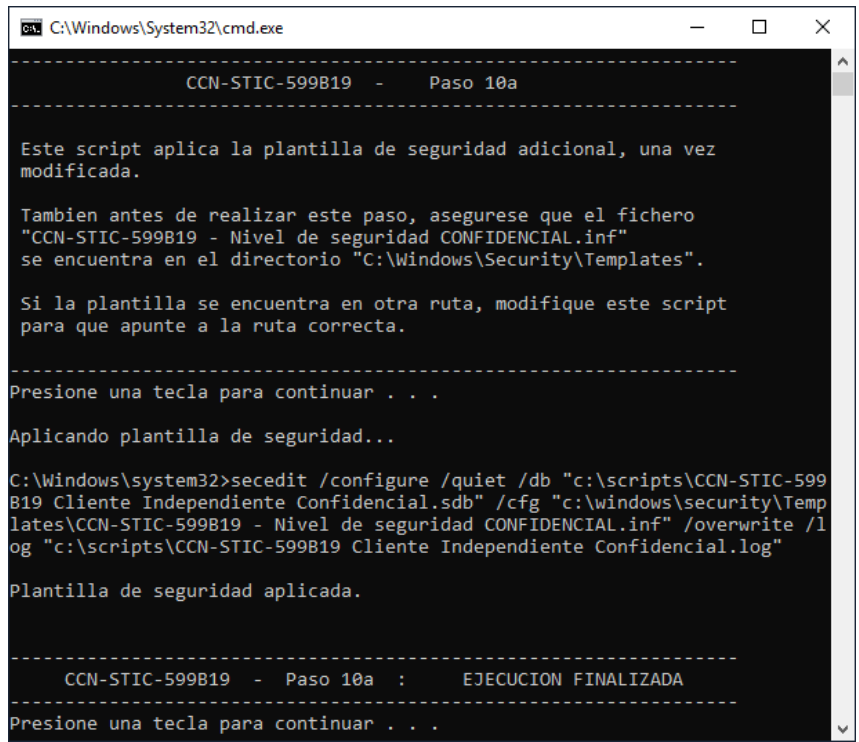
Los siguientes pasos permiten aplicar la configuración del nivel de clasificación correspondiente.

ANEXO D.2.1. NIVEL DE CLASIFICACIÓN CONFIDENCIAL

Los siguientes pasos establecen el procedimiento para establecer la configuración para un entorno de nivel de clasificación "CONFIDENCIAL".

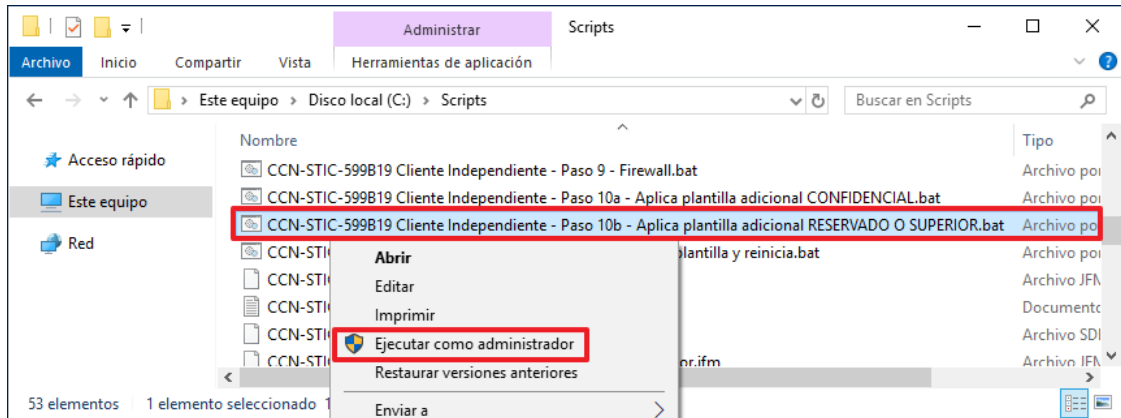
Paso	Descripción
1.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador.
2.	Copie los ficheros que acompañan a esta guía en el directorio "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599B19". Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Se le solicitará elevación de privilegios para realizar la operación.
3.	Localice en el directorio "C:\Scripts" los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf – CCN-STIC-599B19 Cliente Independiente - Paso 10a - Aplica plantilla adicional CONFIDENCIAL.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat

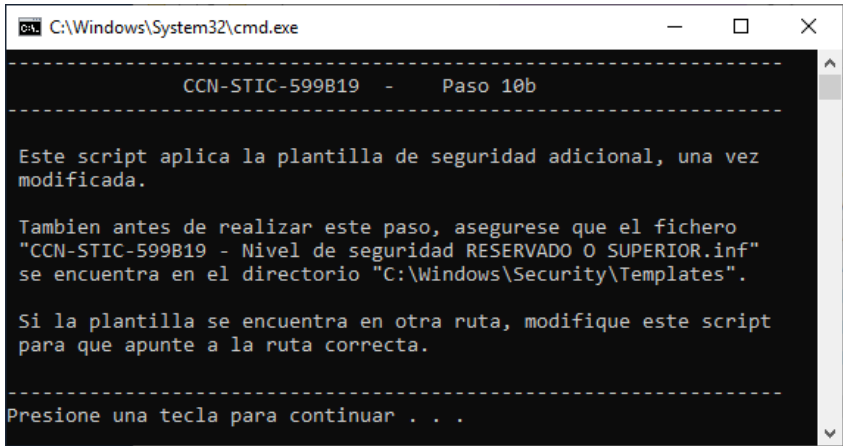
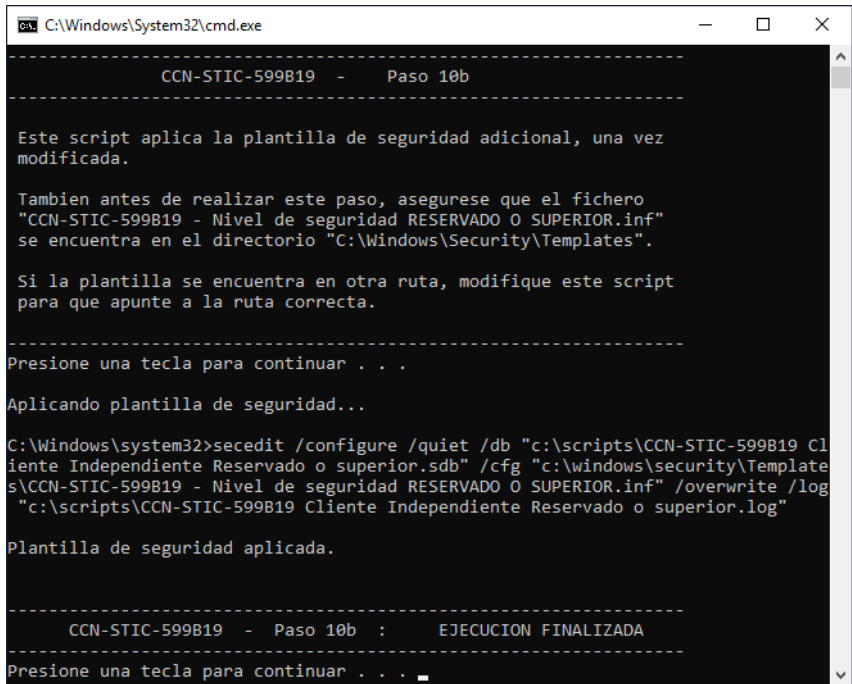
Paso	Descripción
4.	Asegúrese que en el directorio “C:\Windows\Security\Templates” están copiados al menos los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf En caso de no estar cópielos desde el directorio “C:\Scripts”. Nota: Estos ficheros deben estar en la ubicación correcta ya que durante la aplicación de la guía se copian de manera automática. En caso contrario cópielos manualmente.
5.	Acceda al directorio “C:\Scripts” y ejecute con permisos de administrador, opción “Ejecutar como administrador” el fichero “CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional CONFIDENCIAL.bat”. 
6.	El control de cuentas de usuarios le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local del equipo y pulse “Sí”. 

Paso	Descripción
7.	Se lanzará el script. Pulse cualquier tecla para comenzar la ejecución del script. 
8.	Espera a que finalice y pulse de nuevo una tecla para finalizar la ejecución. 
9.	A partir de este momento habrá quedado configurado el equipo con un nivel de clasificación "CONFIDENCIAL".
10.	Borre la carpeta "C:\Scripts" de su sistema.

ANEXO D.2.2. NIVEL DE CLASIFICACIÓN RESERVADO O SUPERIOR

Los siguientes pasos establecen el procedimiento para establecer la configuración para un entorno de nivel de clasificación “RESERVADO O SUPERIOR”.

Paso	Descripción
1.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Tenga en cuenta que para copiar ficheros a esta ubicación tras la aplicación de la guía deberá usar un usuario administrador del sistema. Se le solicitará elevación de privilegios para realizar la operación.
3.	Localice en el directorio “C:\Scripts” los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf – CCN-STIC-599B19 Cliente Independiente - Paso 10a - Aplica plantilla adicional CONFIDENCIAL.bat – CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat
4.	Asegúrese que en el directorio “C:\Windows\Security\Templates” están copiados al menos los siguientes ficheros: – CCN-STIC-599B19 - Nivel de seguridad CONFIDENCIAL.inf – CCN-STIC-599B19 - Nivel de seguridad RESERVADO O SUPERIOR.inf En caso de no estar cópielos desde el directorio “C:\Scripts”. Nota: Estos ficheros deben estar en la ubicación correcta ya que durante la aplicación de la guía se copian de manera automática. En caso contrario cópielos manualmente.
5.	Acceda al directorio “C:\Scripts” y ejecute con permisos de administrador, opción “Ejecutar como administrador” el fichero “CCN-STIC-599B19 Cliente Independiente - Paso 10b - Aplica plantilla adicional RESERVADO O SUPERIOR.bat”. 
6.	El control de cuentas de usuarios le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local del equipo y pulse “Sí”.

Paso	Descripción
7.	Se lanzará el script. Pulse cualquier tecla para comenzar la ejecución del script. 
8.	Espere a que finalice y pulse de nuevo una tecla para finalizar la ejecución. 
9.	A partir de este momento habrá quedado configurado el equipo con un nivel de clasificación "RESERVADO O SUPERIOR".
10.	Borre la carpeta "C:\Scripts" de su sistema.

ANEXO D.3. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO D.3.1. CIFRADO DE DISCO CON BITLOCKER

Este anexo se ha diseñado para ayudar a los operadores a implementar la configuración del cifrado de disco con BitLocker en un equipo cliente Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC, independiente de un dominio.

BitLocker contribuye a la protección de datos en equipos cliente proporcionando el cifrado completo de un volumen de disco y la comprobación de la integridad de los componentes básicos durante el arranque del sistema. También ofrece la opción de bloquear el proceso normal de arranque hasta que el usuario proporcione un número de identificación personal (PIN, Personal Identification Number) o inserte una unidad flash USB con las claves de descifrado correctas.

Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números. Por tanto, se puede pensar en el PIN más como una "frase de paso" que como un "número".

El nivel de protección óptimo se obtiene cuando el equipo dispone de un Módulo de plataforma segura (TPM, del inglés Trusted Platform Module, Windows 10 soporta este módulo desde su versión 1.2 en adelante) para proteger los datos del usuario y reducir las posibilidades de manipulación del equipo cliente con Windows 10 cuando el sistema está desconectado.

Para más información sobre el procedimiento de cifrado de unidad BitLocker, puede consultar los siguientes enlaces:

[http://technet.microsoft.com/es-es/library/dd835565\(Ws.10\).aspx](http://technet.microsoft.com/es-es/library/dd835565(Ws.10).aspx)

<https://blogs.msdn.microsoft.com/mvpawardprogram/2016/01/12/securing-windows-10-with-bitlocker-drive-encryption/>

1. ALCANCE

Este anexo se ha elaborado para proporcionar información sobre cómo implementar la configuración del cifrado de disco con BitLocker sobre la unidad del sistema operativo, en el escenario con modo de autenticación en la secuencia de arranque mediante Módulo de plataforma segura (TPM 1.2) y número de identificación personal (PIN). Aunque existen otros escenarios de configuración del cifrado de disco con BitLocker, como por ejemplo sin uso de TPM, o cifrado de otras unidades lógicas, fijas o extraíbles, estos escenarios no se contemplan para el uso de esta guía.

Las copias de seguridad de la clave de BitLocker se realizarán sobre un dispositivo de memoria USB que posteriormente se almacenará en algún lugar seguro, como una caja de seguridad. Del mismo modo, aunque existen otros escenarios de almacenamiento de claves, como por ejemplo en Active Directory, éstos no se contemplan para el uso de esta guía.

El uso del dispositivo TPM a partir de la versión 1607 es controlado por el sistema operativo de modo que no es necesaria la administración del mismo. Para más información acerca de este echo consulte el siguiente enlace:

<https://docs.microsoft.com/es-es/windows/security/hardware-protection/tpm/change-the-tpm-owner-password>

2. DESCRIPCIÓN DE USO DE ESTE ANEXO

El contenido de este anexo se aplica a equipos independientes de un dominio, con sistema operativo Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC, a los cuales, tras realizar una instalación por defecto, les ha sido aplicada la presente guía.

Para la implementación del cifrado de unidad BitLocker debe tenerse en cuenta que existen requisitos a cumplir adicionales a la instalación del sistema operativo y es necesario comprobarlos antes de comenzar a aplicar este anexo.

El hardware sobre el que se ha verificado el cifrado de unidad BitLocker tiene las siguientes características:

- a) Lenovo ThinkPad 13:
 - i. Intel Core i5 7200U 2.50GHz.
 - ii. SSD 250 GB.
 - iii. 8 GB de RAM.

3. REQUISITOS HARDWARE Y SOFTWARE

La implementación del cifrado de unidad BitLocker tiene los siguientes requisitos de hardware y software:

- a) Un equipo que cumpla los requisitos mínimos para Windows 10.
- b) Un chip TPM, versión 1.2 o superior, activado.
- c) BIOS compatible con TCG (Trusted Computing Group).
- d) Una partición de disco para la unidad del sistema, además de la partición que contiene el sistema operativo. En Windows 10, si cuenta con una sola partición de disco, BitLocker preparará automáticamente la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema que albergará los archivos del sistema que se necesitan para iniciar o recuperar el sistema operativo y que no se pueden cifrar. Esta unidad no tendrá una letra de unidad para evitar que se almacenen archivos de datos en esta unidad por error. Una vez que la unidad está preparada, debe reiniciarse el equipo.

No obstante, si se ha realizado una instalación por defecto de Windows 10, el programa de instalación ya habrá creado, durante la instalación, las dos particiones de disco necesarias para activar BitLocker.

- e) Una unidad flash USB para almacenar claves de inicio y recuperación.
- f) Una configuración BIOS para iniciar primero desde el disco duro, y no desde las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como una clave de inicio o de recuperación), la BIOS debe admitir la lectura de unidades flash USB en el inicio.

- g) Opcionalmente, se puede disponer de una impresora conectada y configurada, para la impresión de las claves de recuperación. Alternativamente, se podrá tomar nota manualmente de las claves de recuperación.

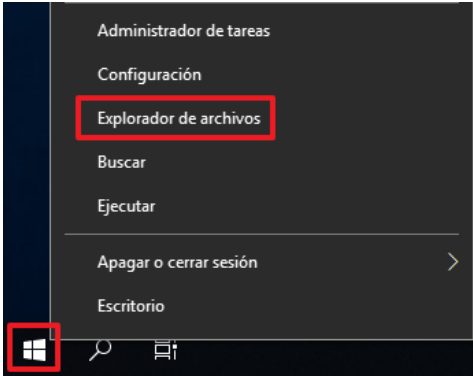
Nota: Tenga en cuenta que el acceso a las impresoras puede estar deshabilitado, debido a la aplicación de la configuración de seguridad implementada. Recuerde que antes de realizar este paso a paso necesitará de una unidad para almacenar las claves necesarias por lo que deberá aplicar la configuración para utilizar el dispositivo de almacenamiento descrito en el “ANEXO D.3.4 DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE”.

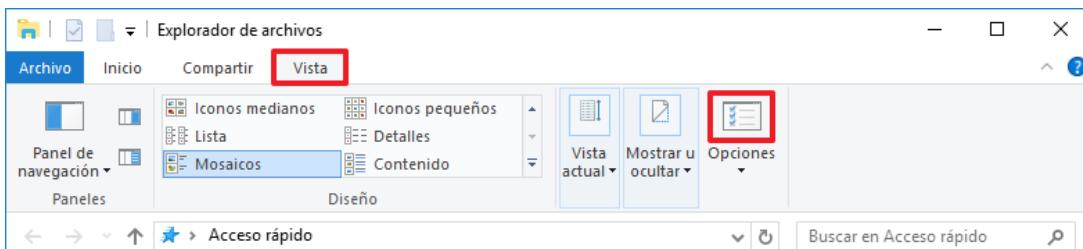
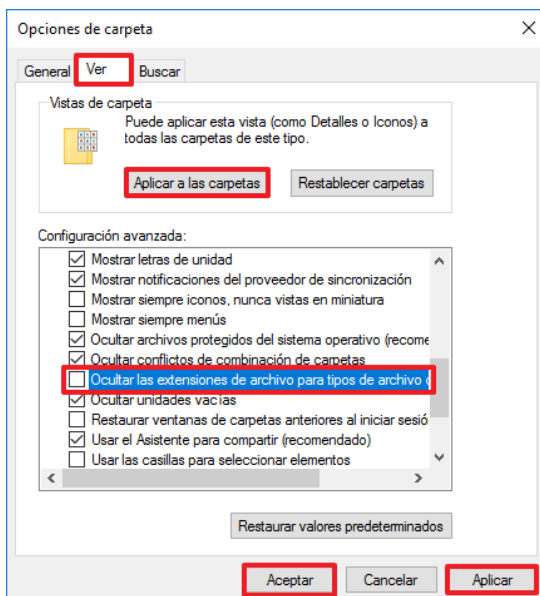
4. GUÍA PASO A PASO – BITLOCKER

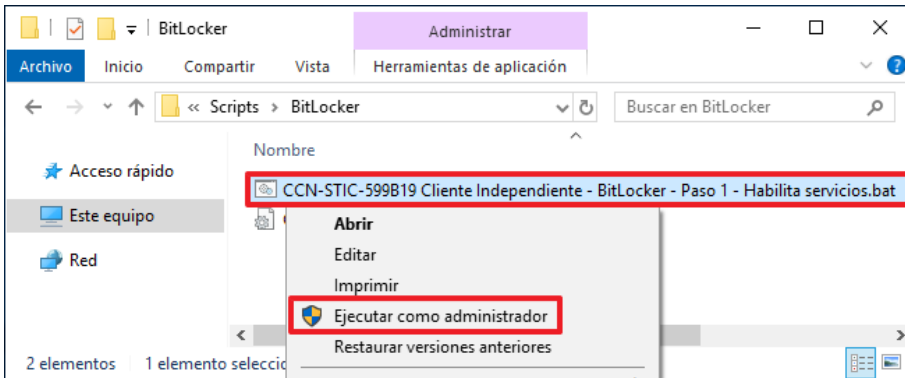
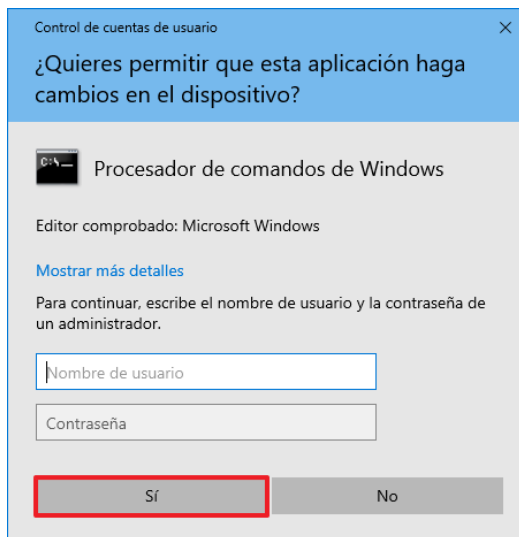
En este apartado se enumeran los pasos necesarios para implementar el cifrado de unidad BitLocker en equipos Windows 10.

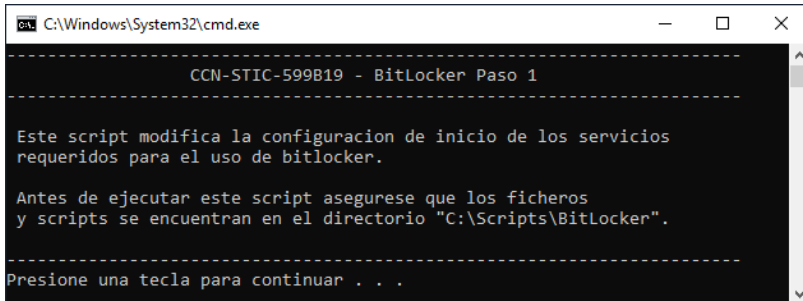
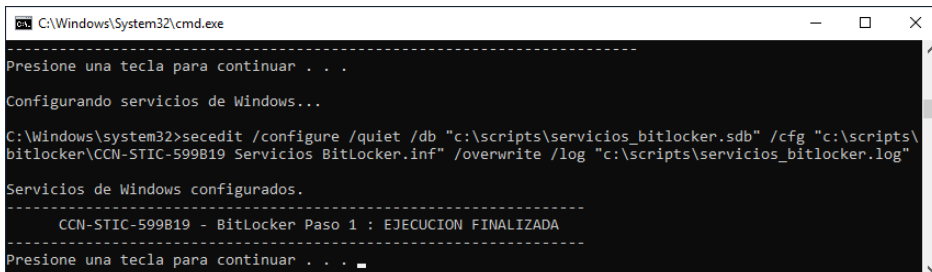
La primera parte hace referencia a las modificaciones que es necesario realizar en la configuración de seguridad aplicada hasta este punto, para implementar el cifrado de unidad BitLocker. Los siguientes pasos deberán realizarse iniciando sesión en el equipo con una cuenta de usuario perteneciente al grupo “Administradores”.

Nota: Recuerde que no podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada, debido a la aplicación de la configuración de seguridad implementada.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores”.
2.	Cree el directorio “Scripts” en la unidad “C:”
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
4.	Si no lo hizo previamente, configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 

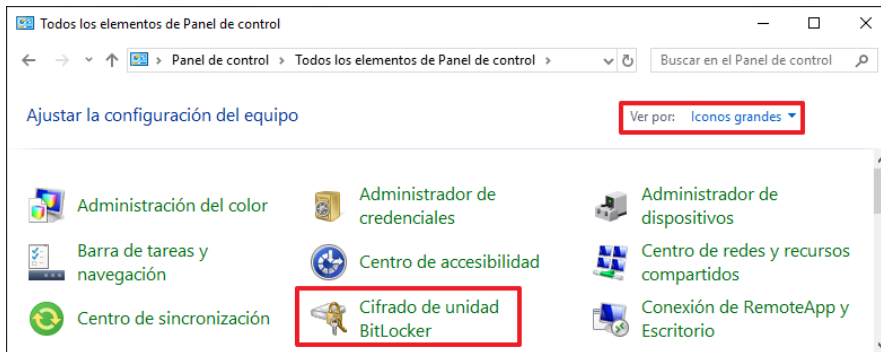
Paso	Descripción
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono “Opciones”. 
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del cliente independiente: – BitLocker (Directorio) – BitLocker\CCN-STIC-599B19 Cliente Independiente - BitLocker - Paso 1 - Habilita servicios.bat – BitLocker\CCN-STIC-599B19 Servicios BitLocker.inf

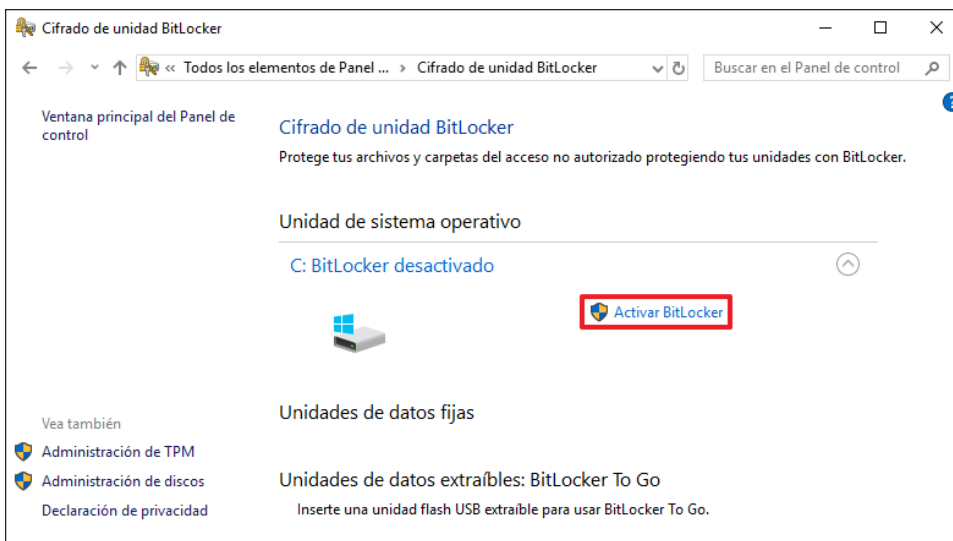
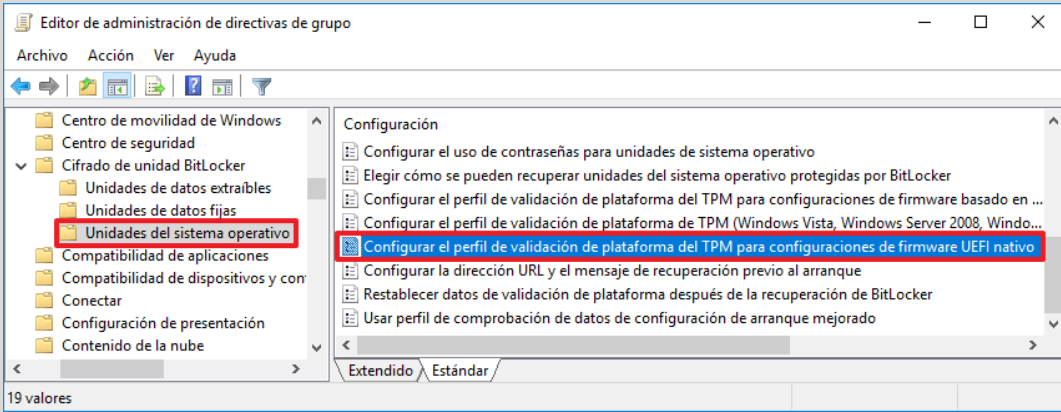
Paso	Descripción
8.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script " CCN-STIC-599B19 Cliente Independiente – BitLocker Paso 1 – Habilita servicios.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario con permisos de administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
9.	El "Control de cuentas de usuario" le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración y que pertenezca al grupo "Usuarios de shells". 

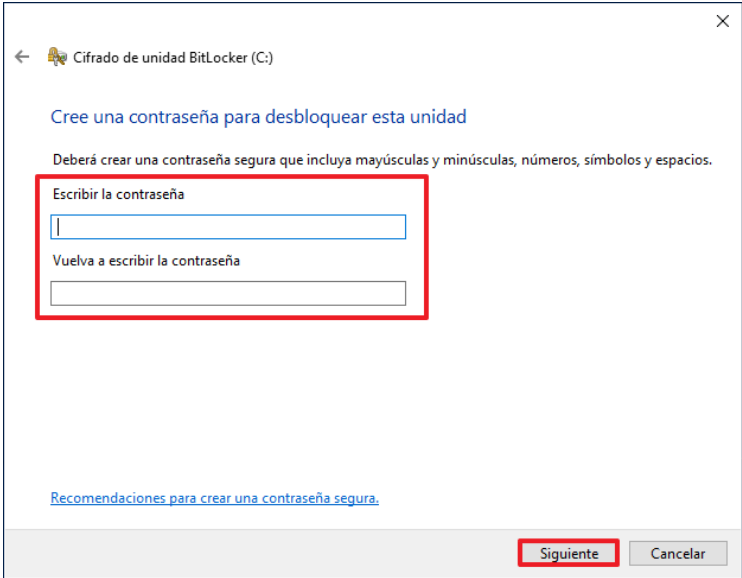
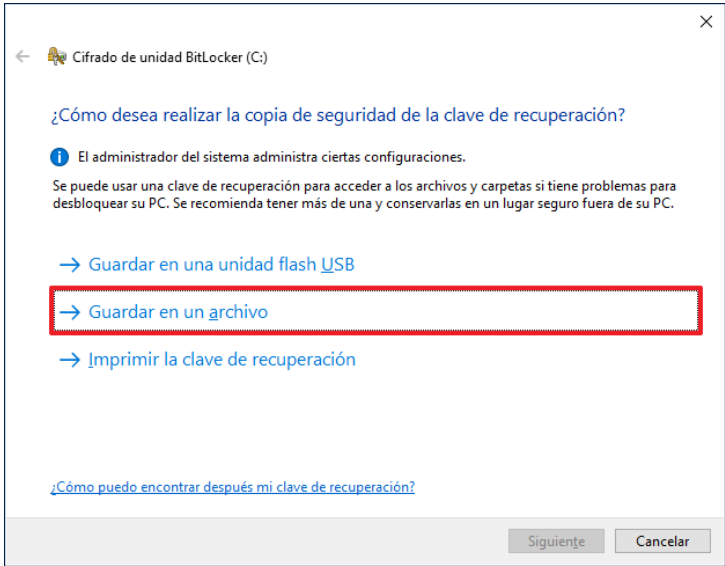
Paso	Descripción
10.	Este script, habilita y configura los servicios necesarios para el uso de BitLocker. Pulse una tecla para continuar. 
11.	Se actualizará el estado de los servicios. Pulse una tecla para cerrar la ventana. 

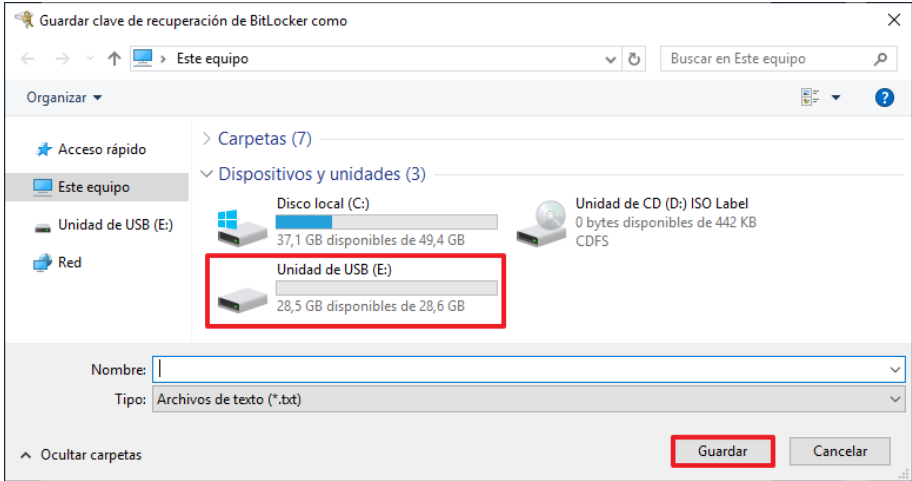
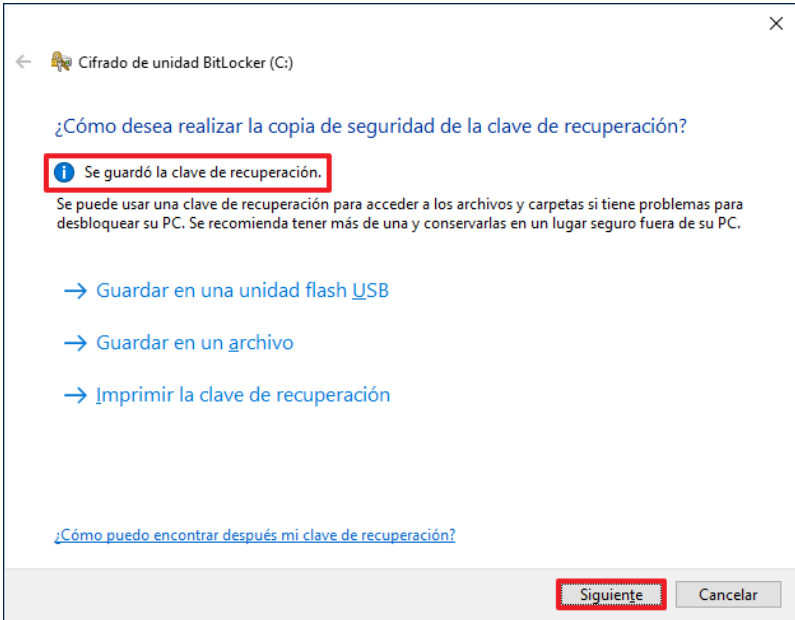
Los siguientes pasos describen el procedimiento para activar el cifrado de unidad BitLocker con PIN (número de identificación personal).

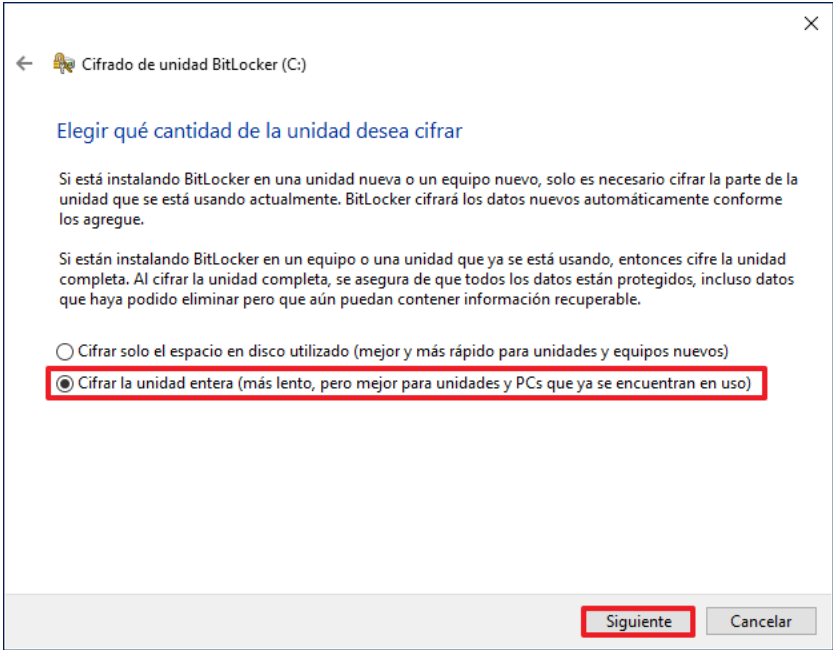
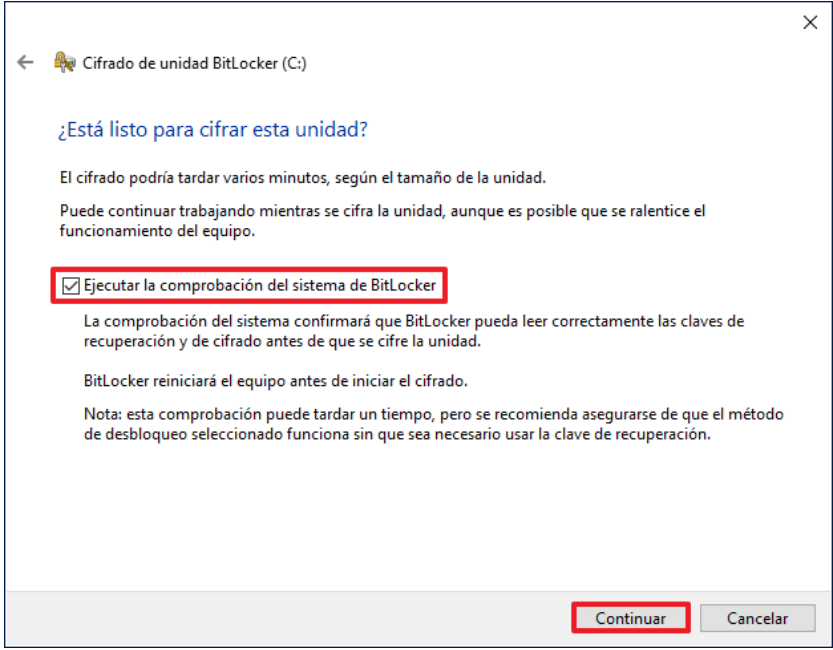
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números. Por tanto, se puede pensar en el PIN más como una "frase de paso" que como un "número".

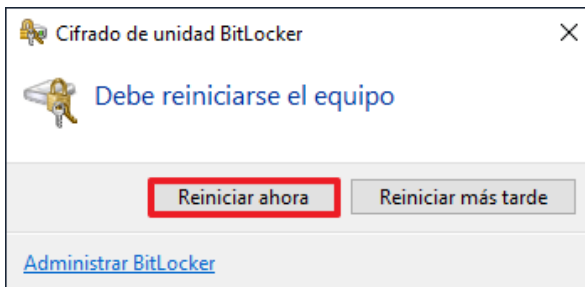
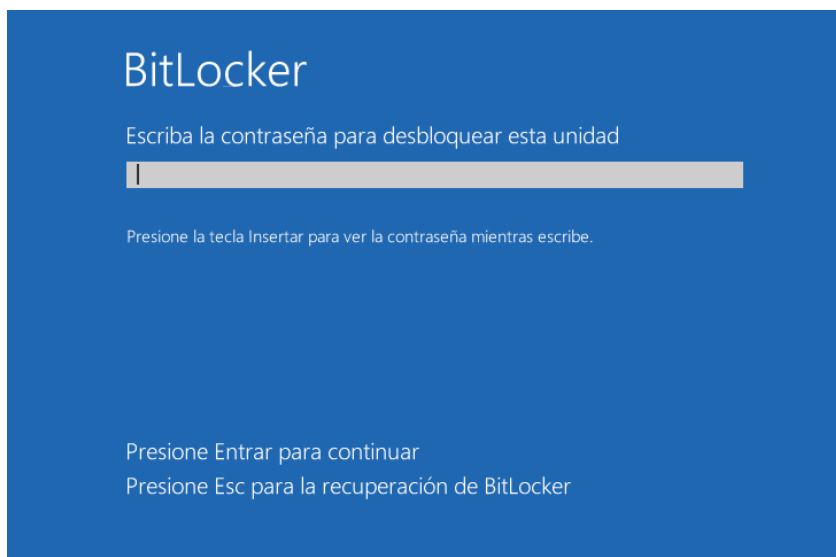
Paso	Descripción
12.	Abra la consola de administración "Cifrado de unidad BitLocker" desde el panel de control a través de la siguiente ruta: "Inicio (clic derecho sobre él) → Panel de control → Cifrado de unidad BitLocker"  Nota: Es posible que la vista de los iconos no se corresponda con la captura anterior. Para solventarlo, seleccione la opción "Iconos grandes" del desplegable "Ver por:". Ver por: Iconos grandes

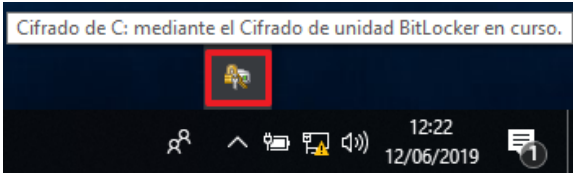
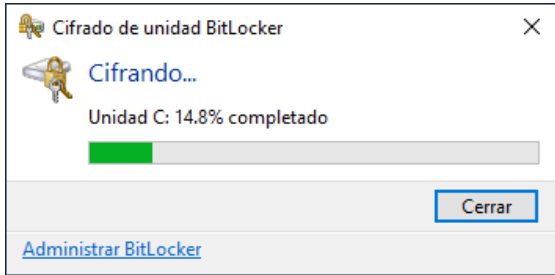
Paso	Descripción
13.	Pulse en “Activar BitLocker” como se indica en la siguiente figura.  Nota: La configuración importada durante la aplicación de la guía establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si su equipo dispone de firmware UEFI nativo, deberá habilitar y configurar la directiva “Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo”. Para ello, con el editor de directivas de grupo (gpedit.msc) diríjase a la ruta “Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo” y habilite la directiva mencionada anteriormente. 
14.	El sistema le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador en la ventana de “Control de cuentas de usuario”.

Paso	Descripción
15.	Introduzca y confirme una contraseña de inicio y pulse “Siguiente”.  Nota: Recuerde que puede utilizar entre 8 y 20 caracteres. A mayor longitud, mayor seguridad.
16.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
17.	Seleccione la ubicación de la unidad USB en la que guardará el archivo que contiene la clave.  Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD. Debe tener en consideración que esta clave, durante el proceso no puede ser almacenado sobre la misma unidad que se está cifrando ni en otra unidad que este cifrada.
18.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

Paso	Descripción
19.	Elija la opción de “Cifrar la unidad entera” y pulse “Siguiente”. 
20.	Marque la opción "Ejecutar la comprobación del sistema de BitLocker" y pulse el botón "Continuar". 

Paso	Descripción
21.	Reinicie el equipo para continuar con el proceso de cifrado de la unidad.  Nota: Si tras reiniciar el sistema aparece un mensaje como el mostrado a continuación pulse el botón “Cerrar” y repita los pasos 12 a 21, pero en este último paso pulse sobre la opción “Reiniciar más tarde” y reinicie el equipo manualmente mediante la ruta “Inicio → “Iniciar/Apagar”. 
22.	Al reiniciar, el sistema le pedirá la contraseña de cifrado de unidad BitLocker. Introduzca la contraseña y pulse “Enter” para continuar. 

Paso	Descripción
23.	Una vez reiniciado, inicie sesión de nuevo con un usuario del grupo “Administradores”. El cifrado inicial de la unidad del sistema se realizará en segundo plano. Mientras dure este proceso es posible que el tiempo de respuesta del sistema se vea afectado por la intensa actividad del disco. Una vez finalizado el proceso de cifrado inicial, el cifrado y descifrado de los datos del disco será imperceptible por el usuario. Durante el proceso puede aparecer el siguiente mensaje informativo. 
24.	Si marca con el ratón en él, o en el icono correspondiente del área de notificación, podrá visualizar la siguiente ventana mostrando el progreso de este proceso de cifrado inicial.  Continúe con los siguientes pasos, aunque no haya finalizado este proceso de cifrado inicial del disco.
25.	Desconecte la memoria USB que contiene la clave de recuperación del cifrado de BitLocker y guárdela en un lugar seguro, como una caja de seguridad. Nota: La contraseña de clave de recuperación es necesaria y suficiente para desbloquear los datos cifrados del volumen si el cifrado de unidad BitLocker está bloqueado. Esta clave de recuperación es única para este cifrado de BitLocker en concreto y no podrá ser utilizada para recuperar datos cifrados de cualquier otra sesión de cifrado de BitLocker. Tanto la memoria USB como la copia impresa (si la imprimió) conteniendo la clave de recuperación DEBEN ESTAR ALMACENADAS EN UNA CAJA DE SEGURIDAD.
26.	Una vez haya reiniciado el sistema, inicie sesión de nuevo con un usuario miembro del grupo “Administradores” y elimine la carpeta “C:\Scripts”. Nota: Todos los volúmenes NTFS del Sistema deberán ser cifrados con la utilidad BitLocker, una vez se haya cifrado totalmente el volumen del Sistema. Si se cambia el TPM asociado al cifrado de unidad BitLocker o si alguien intenta iniciar el equipo desde un disco para evitar el sistema operativo, el equipo cambiará al modo de recuperación hasta que se suministre la clave de recuperación. Si se pierde el PIN, se puede cambiar al modo de recuperación para iniciar el equipo e introducir la contraseña de recuperación. Para más información sobre el procedimiento de cifrado de unidad BitLocker, puede consultar el siguiente enlace: https://support.microsoft.com/es-es/help/4028713/windows-10-turn-on-device-encryption

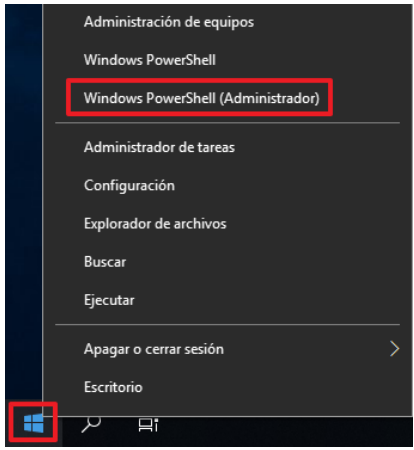
5. LISTA DE COMPROBACIÓN – BITLOCKER

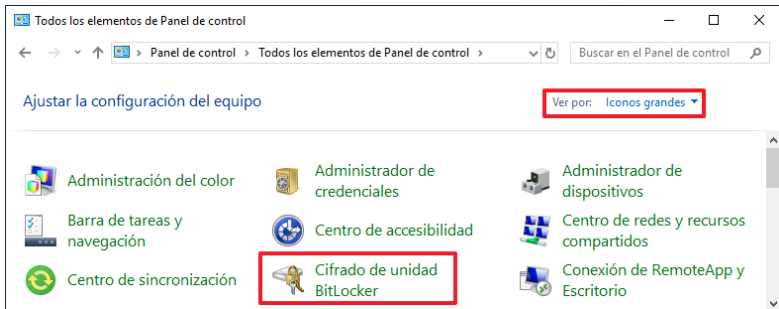
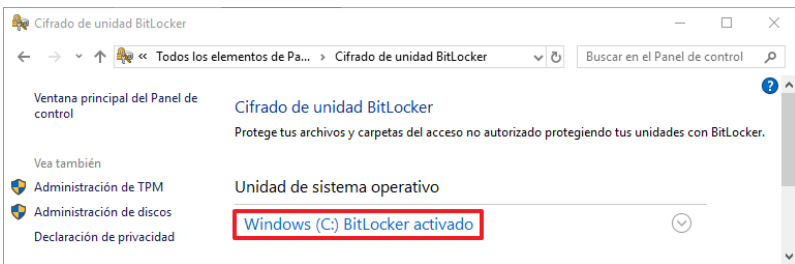
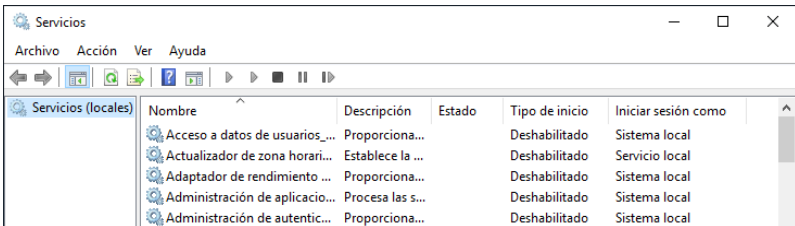
Este anexo se ha diseñado para ayudar a los operadores a verificar que se ha implementado el cifrado de unidad BitLocker en un equipo cliente Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC, independiente de un dominio. La lista de comprobación deberá ejecutarse iniciando sesión en el equipo propio cliente con la cuenta de un usuario miembro del grupo "Administradores" y que sea miembro también del grupo "Usuarios de shells".

Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada, debido a la aplicación de la configuración de seguridad.

Para realizar algunas de las comprobaciones será necesario ejecutar diferentes consolas de administración y herramientas del sistema. Estas herramientas estarán disponibles si no se ha prohibido la utilización de las mismas. Uno de los primeros pasos, por tanto, consistirá en habilitar temporalmente el acceso a ellas. Las consolas y herramientas que se utilizarán son las siguientes:

- a) Explorador de Windows (explorer.exe)
- b) Administración de servicios (services.msc)

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo cliente que está comprobando.		Inicie sesión en el equipo cliente que está comprobando con una cuenta de usuario que pertenezca al grupo local "Administradores" y al grupo local "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.
2. Lance una ventana de Powershell con permisos de administrador, para lanzar desde ella en pasos posteriores comandos con permisos de administrador		Haga clic con el botón derecho en el menú de inicio y seleccione "Windows PowerShell (Administrador)".  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario. Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.

Comprobación	OK/NOK	Cómo hacerlo
3. Compruebe que el volumen del sistema operativo está cifrado		Abra la consola de administración "Cifrado de unidad BitLocker". Para ello, ejecute en la ventana de PowerShell el comando "control.exe" y localice "Cifrado de unidad BitLocker".  Compruebe que junto a la letra de unidad del volumen del sistema operativo aparece el estado "Activado", como se muestra en la siguiente figura.  Nota: Si en lugar de "Activado" el estado que aparece es "Cifrar", eso significa que el cifrado inicial del disco todavía está en marcha. Repita la comprobación más tarde, cuando haya finalizado. Puede comprobar el progreso del proceso de cifrado haciendo doble clic en el icono de BitLocker que estará presente en el área de notificación de la barra de tareas durante todo el proceso de cifrado inicial del disco. Cierre la ventana "Cifrado de unidad BitLocker".
4. Compruebe que se han configurado correctamente los servicios relacionados con BitLocker y TPM		Desde la ventana de Powershell abierta anteriormente, ejecute "services.msc". A continuación, se abrirá la consola de "Servicios del sistema".  Compruebe que el tipo de inicio configurado para cada servicio coincide con el mostrado en la siguiente tabla:



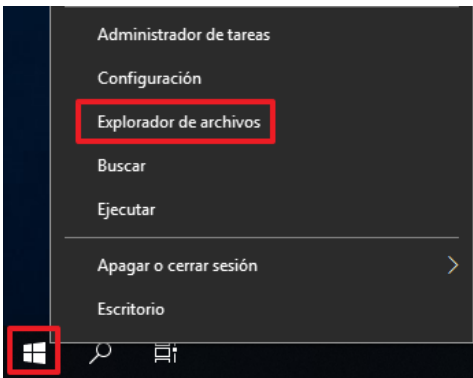
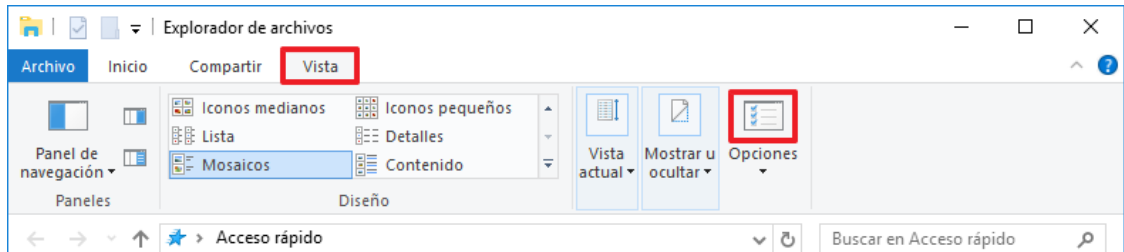
Comprobación	OK/NOK	Cómo hacerlo		
		Servicio	Inicio	OK/NOK
		Servicio Cifrado de unidad BitLocker (bdesvc)	Automático	
		Detección de hardware Shell (shellhwdetection)	Automático	
		Cierre la consola de administración de servicios.		
5. Borre el directorio "C:\Scripts"		Borre el directorio "C:\Scripts" con todo su contenido.		
6. Reinicie el equipo		Reinicie el equipo para comprobar que BitLocker solicita la contraseña para acceder a la unidad de sistema.		
7. Compruebe que el sistema tiene configurado cifrado de unidad BitLocker con la opción de PIN de arranque.		Reinicie el equipo. Compruebe que el sistema requiere que se introduzca la contraseña para desbloquear la unidad, como se muestra en la siguiente figura.		
8. Compruebe que la memoria USB y el listado de contraseñas están almacenados en lugar seguro		Solicite la memoria USB y los listados donde se encuentran almacenadas la contraseña de recuperación de cifrado BitLocker. Debe verificar si éstos se encontraban en una caja de seguridad.		

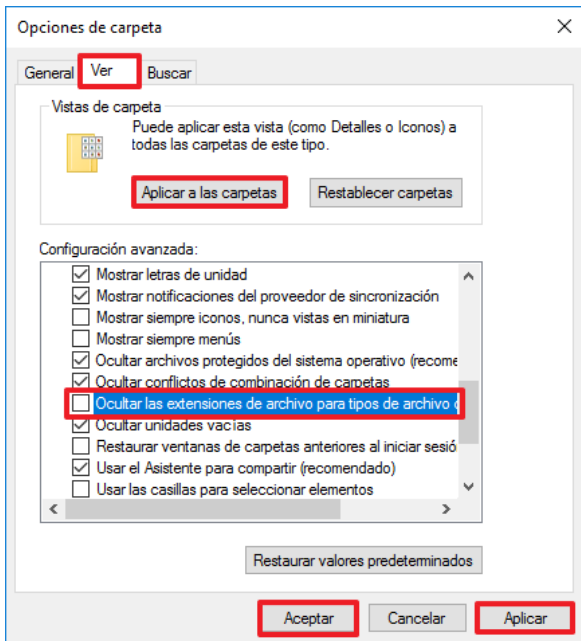
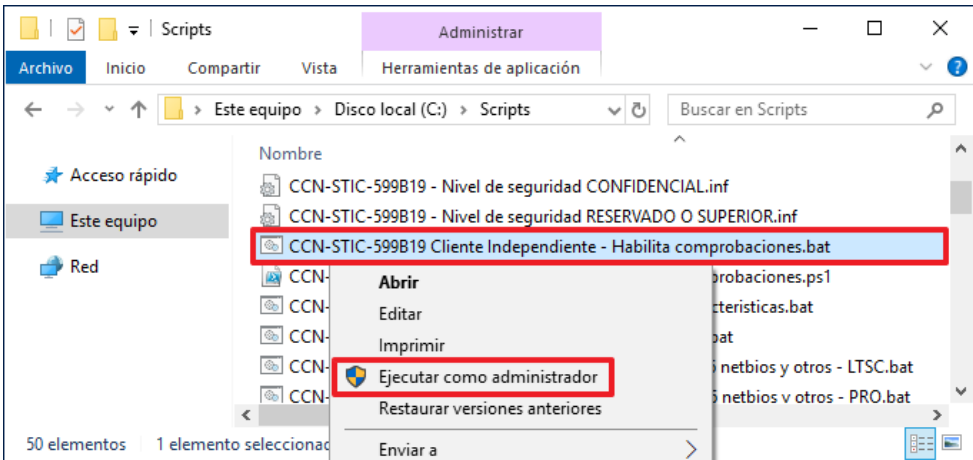
ANEXO D.3.2. USO DE DIFERENTES CONSOLAS DE ADMINISTRACIÓN TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19

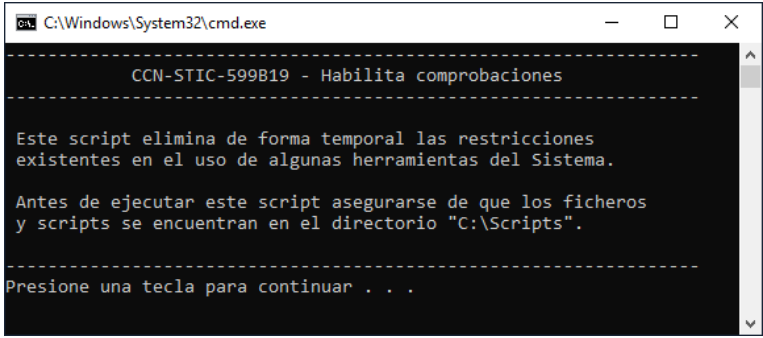
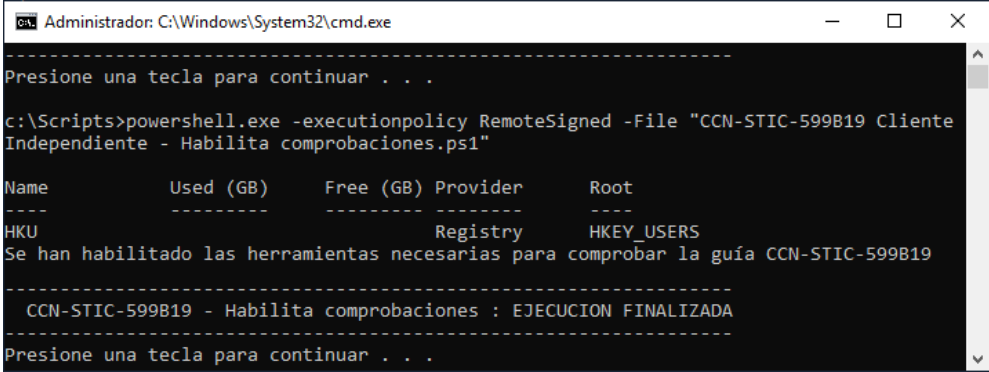
La aplicación de la presente guía conlleva el bloqueo de algunas consolas administrativas, así como el acceso a ciertas características. En el caso de experimentar problemas para acceder a los diferentes componentes de administración de la Consola de Administración de Microsoft (mmc.exe) tales como el "Editor de Directivas de grupo local" (gpedit.msc) o el "Visor de eventos" (eventvwr.msc), puede utilizar el conjunto de scripts facilitados junto con la presente guía, así como seguir los pasos recogidos en el presente anexo.

Del mismo modo, existen otra serie de características deshabilitadas por la guía que, del mismo modo, podrían ser habilitadas temporalmente para realizar tareas administrativas. Un ejemplo de esto sería el hecho de que, tras aplicar la presente guía, en las propiedades de los contenedores y ficheros del “Explorador de archivos”, la pestaña “Seguridad” no aparece.

Este documento recoge el conjunto de pasos necesarios para, de una forma temporal, habilitar consolas y opciones administrativas que, de otro modo, no podrían ser configuradas tras haber aplicado la guía “CCN-STIC-599B19 Windows 10 – Cliente Independiente”.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
4.	Si no lo hizo previamente, configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono “Opciones”. 

Paso	Descripción
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del cliente independiente: – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat – CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.ps1
8.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.bat" desde el directorio “C:\Scripts”.  Nota: El sistema le solicitará elevación de privilegios.

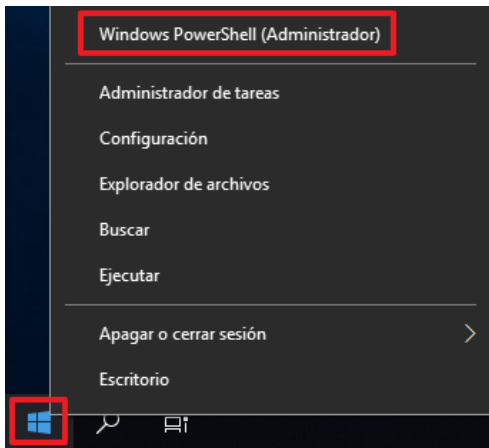
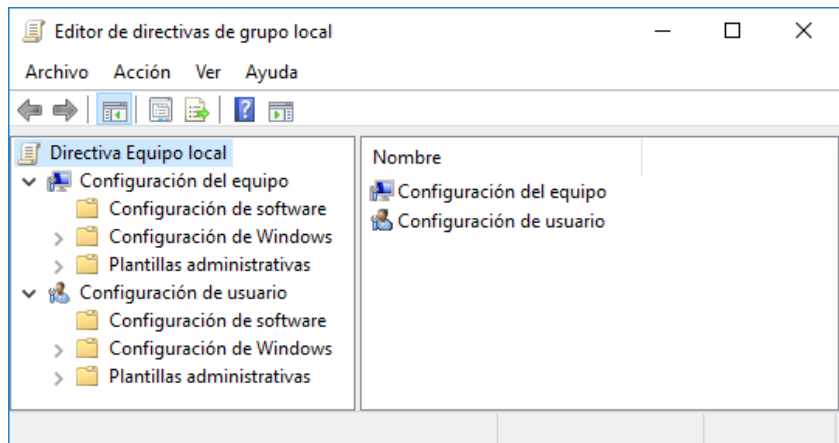
Paso	Descripción
9.	Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá la siguiente ventana. Pulse una tecla para continuar. 
10.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: En caso de que el sistema muestre errores puede ignorarlos. A partir de este momento, las consolas y características de administración bloqueadas por la presente guía vuelven a ser operativas de forma temporal.
11.	Borre el directorio "C:\Scripts".
12.	Una vez haya terminado con las labores de administración, reinicie el equipo o fuerce la aplicación de las directivas de grupo local para que vuelvan a entrar en vigor las políticas de seguridad correctas y definidas por la presente guía.

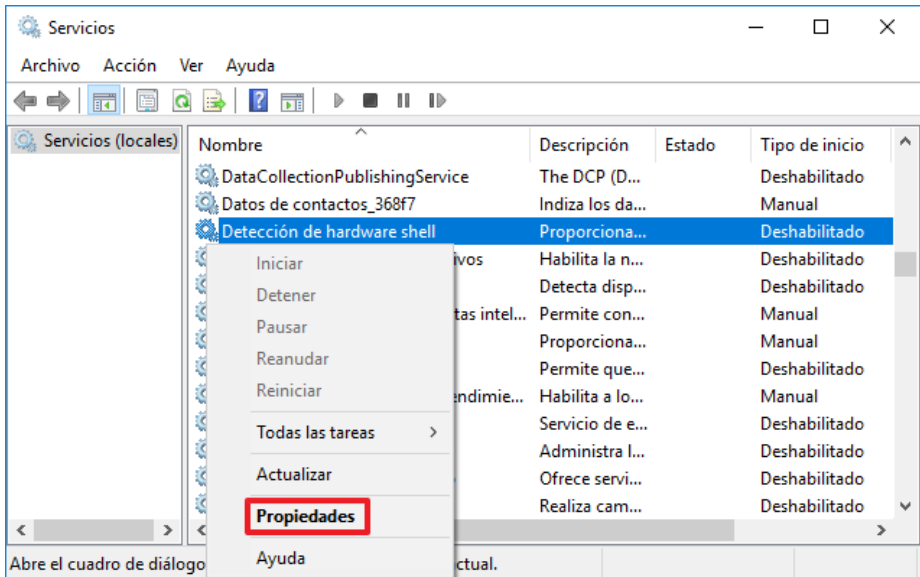
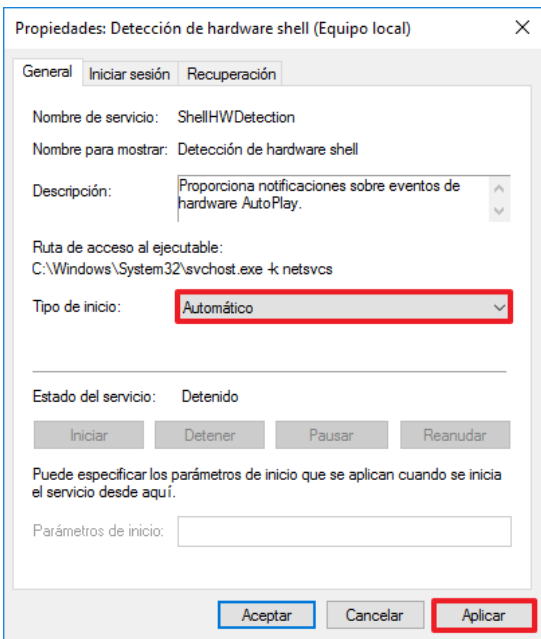
ANEXO D.3.3. USO DE GRABADORA DE CD/DVD TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE

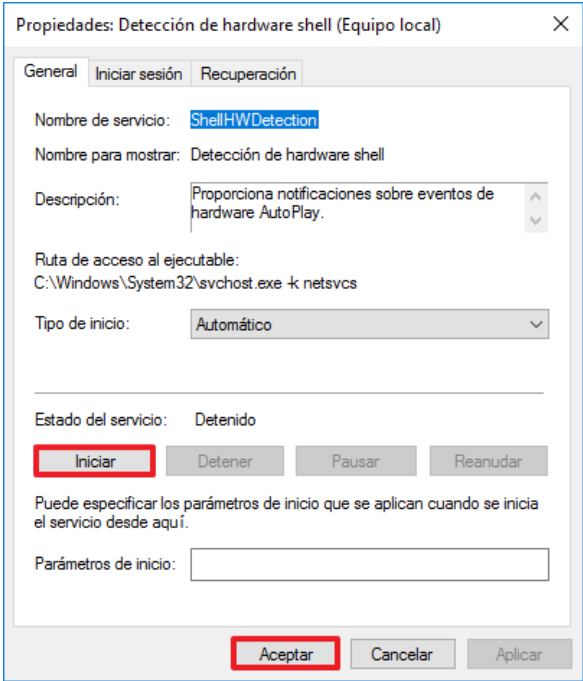
La aplicación de la presente guía conlleva el bloqueo del uso de la grabadora de CD/DVD como herramienta de grabación, transformándose en un lector de CD/DVD y perdiendo el resto de su funcionalidad.

Este documento recoge el conjunto de pasos necesarios para habilitar una serie de directivas y servicios que permitirán hacer uso de la grabadora de CD/DVD con toda su funcionalidad.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo "Administradores" y del grupo "Usuarios de shells".

Paso	Descripción												
2.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 												
3.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local.												
4.	En la ventana de Powershell ejecute "gpedit.msc". Esto abrirá una ventana del Editor de directivas de grupo local, como la mostrada en la siguiente figura. 												
5.	Modifique los valores de equipo para que coincidan con los valores indicados en la tabla mediante la siguiente ruta: “Directiva de Equipo → Configuración del equipo → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble” <table><tr><th>Directiva</th><th>Valor establecido</th><th>Valor a establecer</th></tr><tr><td>CD y DVD: denegar acceso de ejecución</td><td>No configurada</td><td>Deshabilitada</td></tr><tr><td>CD y DVD: denegar acceso de lectura</td><td>No configurada</td><td>Deshabilitada</td></tr><tr><td>CD y DVD: denegar acceso de escritura</td><td>No configurada</td><td>Deshabilitada</td></tr></table>	Directiva	Valor establecido	Valor a establecer	CD y DVD: denegar acceso de ejecución	No configurada	Deshabilitada	CD y DVD: denegar acceso de lectura	No configurada	Deshabilitada	CD y DVD: denegar acceso de escritura	No configurada	Deshabilitada
Directiva	Valor establecido	Valor a establecer											
CD y DVD: denegar acceso de ejecución	No configurada	Deshabilitada											
CD y DVD: denegar acceso de lectura	No configurada	Deshabilitada											
CD y DVD: denegar acceso de escritura	No configurada	Deshabilitada											

Paso	Descripción						
6.	Modifique los valores de usuario indicados en la tabla mediante la siguiente ruta: “Directiva de Equipo → Configuración de usuario → Plantillas administrativas → Componentes de Windows → Explorador de Archivos” <table><thead><tr><th>Directiva</th><th>Valor establecido</th><th>Valor a establecer</th></tr></thead><tbody><tr><td>Quitar las características de grabación de CD</td><td>Habilitada</td><td>Deshabilitada</td></tr></tbody></table>	Directiva	Valor establecido	Valor a establecer	Quitar las características de grabación de CD	Habilitada	Deshabilitada
Directiva	Valor establecido	Valor a establecer					
Quitar las características de grabación de CD	Habilitada	Deshabilitada					
7.	Modifique el modo de inicio del servicio “Detección de hardware Shell” (Deshabilitado). Para ello y desde la misma consola de PowerShell, ejecute el comando “services.msc” del mismo modo que ejecutó “gpedit.msc” en pasos anteriores. Haga clic derecho sobre el servicio y seleccione “Propiedades”. 						
8.	En el menú de “Propiedades: Detección de hardware shell (Equipo local)”, en el campo “Tipo de inicio” seleccione la opción “Automático” y pulse sobre el botón “Aplicar”. 						

Paso	Descripción
9.	Pulse sobre el botón “Iniciar” y cuando el estado del servicio sea “Iniciado”, pulse sobre el botón “Aceptar”. 
10.	Borre el directorio “C:\Scripts”. A partir de este momento, será posible hacer uso de la grabadora de CD/DVD con todas sus funciones.

ANEXO D.3.4. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19 – WINDOWS 10 CLIENTE INDEPENDIENTE

Este documento recoge el conjunto de pasos necesarios para activar el uso e instalación de dispositivos USB de almacenamiento en sistemas securizados mediante la aplicación de la guía CCN-STIC-599B19 Windows 10 – Cliente Independiente.

Existen dos métodos para permitir el uso de dispositivos conectados mediante USB:

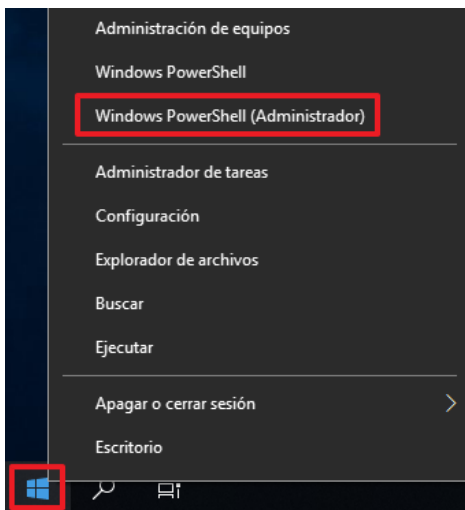
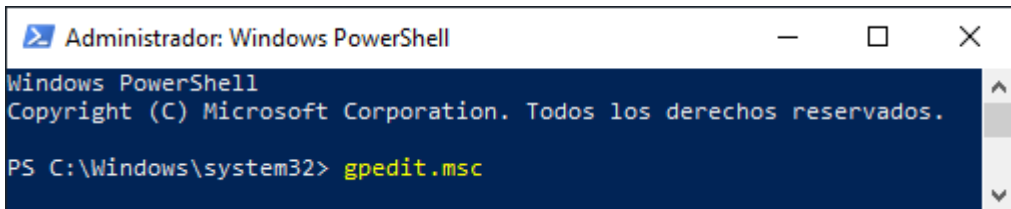
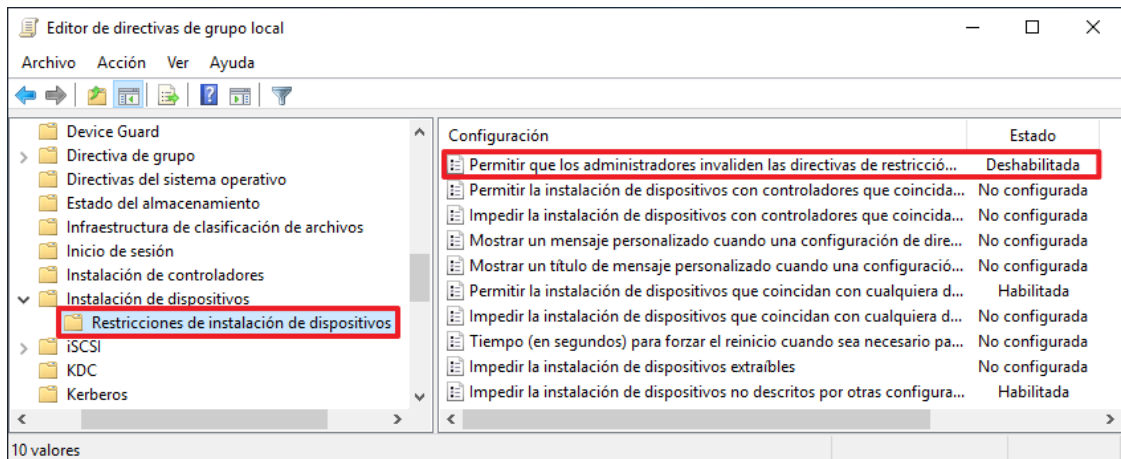
- Instalación de controladores mediante el uso de un usuario administrador de la máquina.
- Filtrado de USB mediante el uso de los identificadores de dispositivo USB.

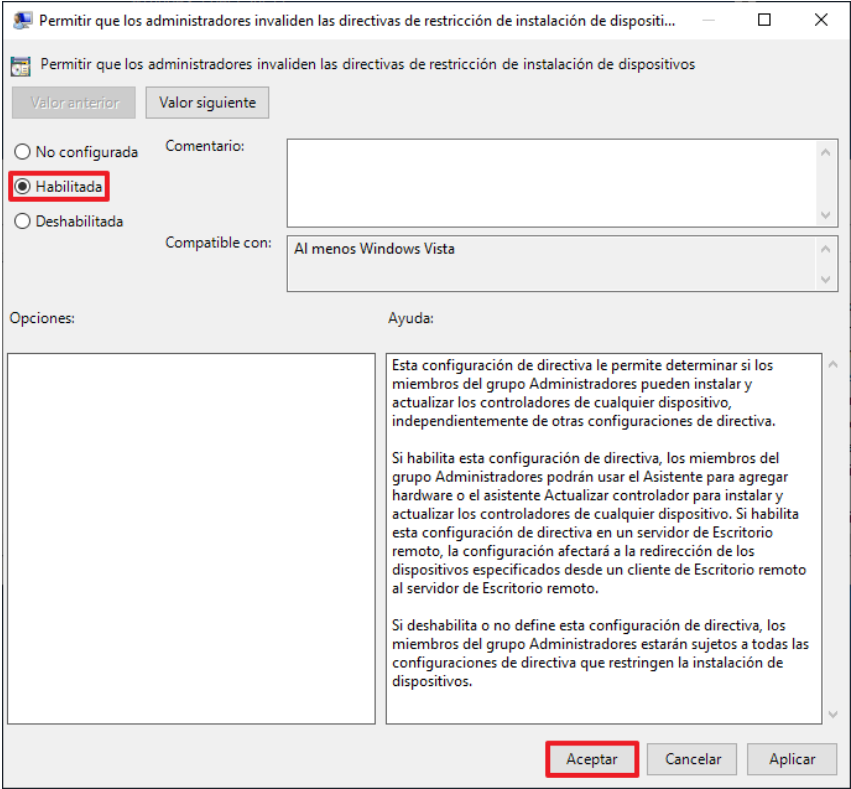
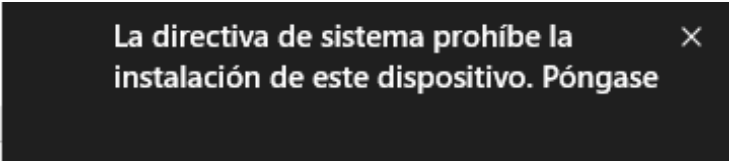
1. ADMINISTRAR DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES

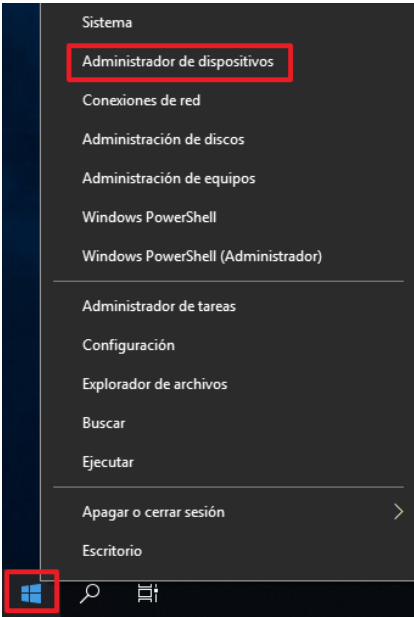
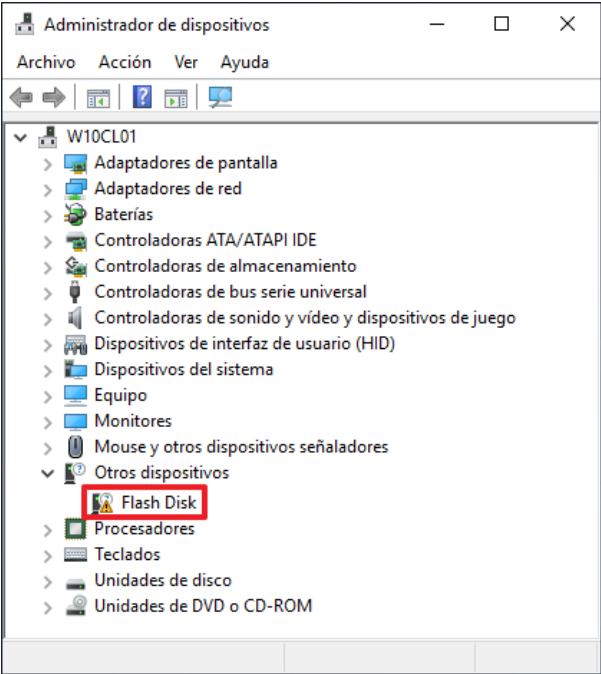
Este punto describe el proceso para instalar y desinstalar el controlador de un dispositivo USB a través de una cuenta que posea privilegios de administrador local de la máquina.

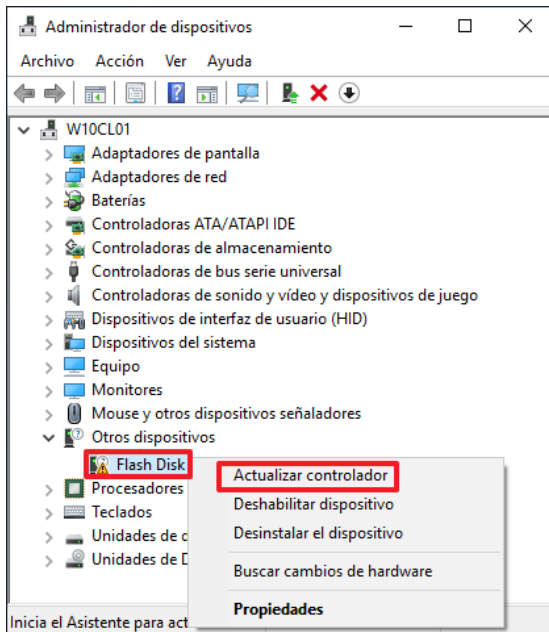
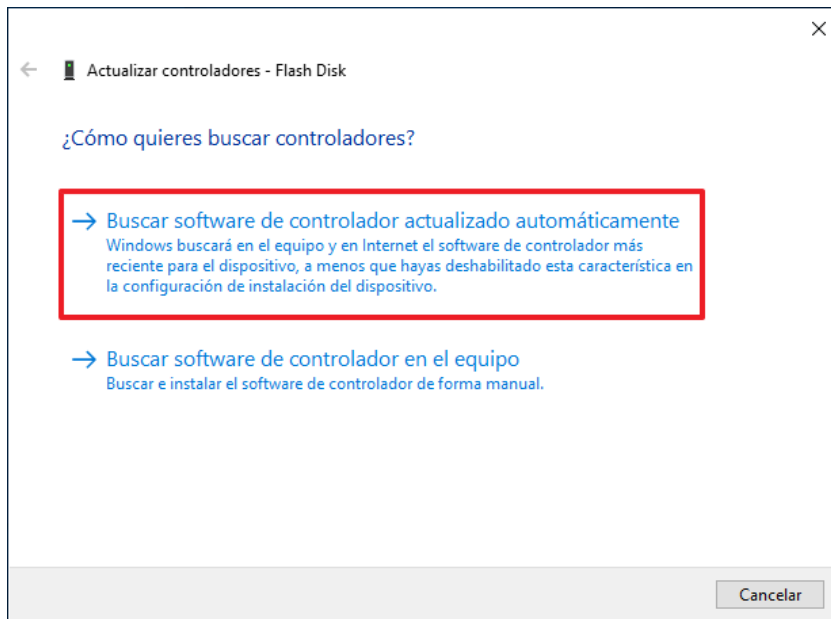
El proceso consta de un paso a paso para instalar un controlador de forma manual y que el dispositivo funcione. Tras su uso e independientemente de que el dispositivo esté conectado o no, se revertirá el uso del dispositivo mediante la desinstalación del controlador.

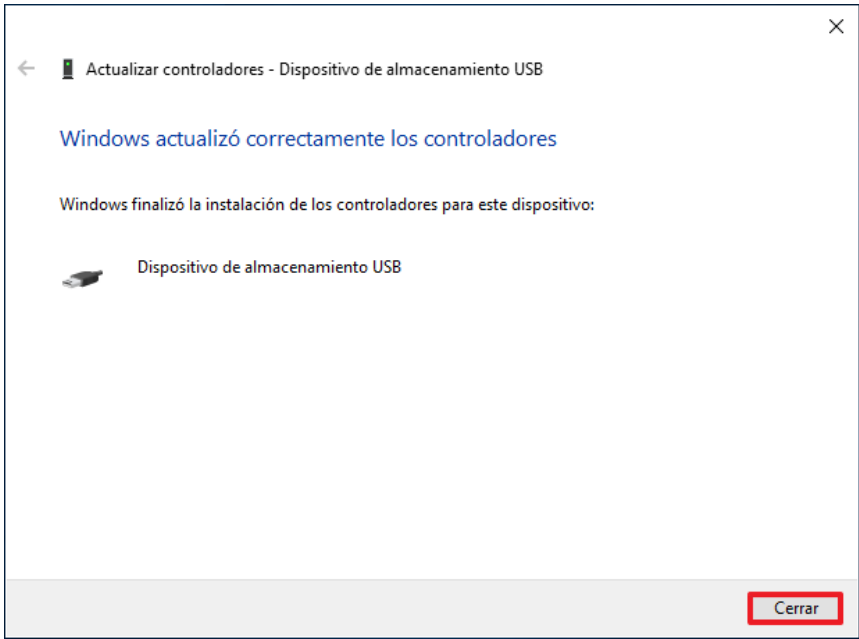
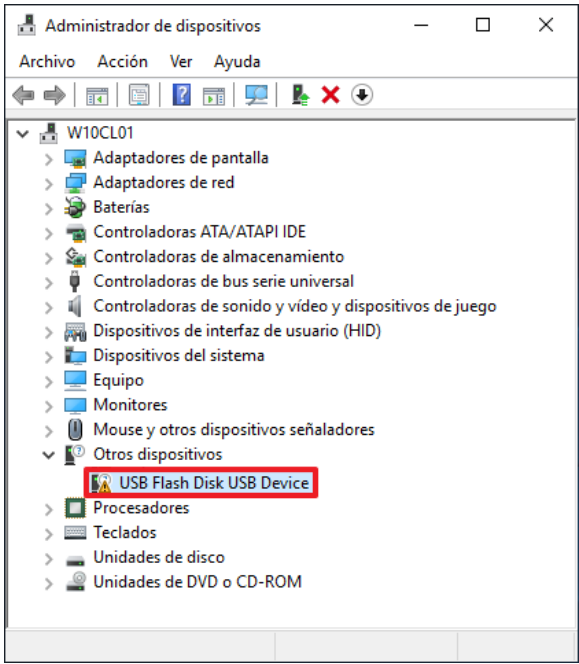
1.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB

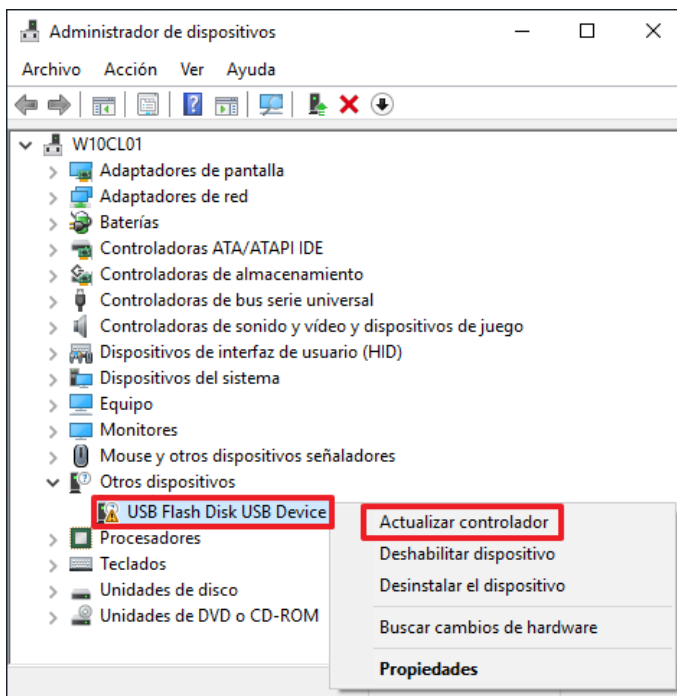
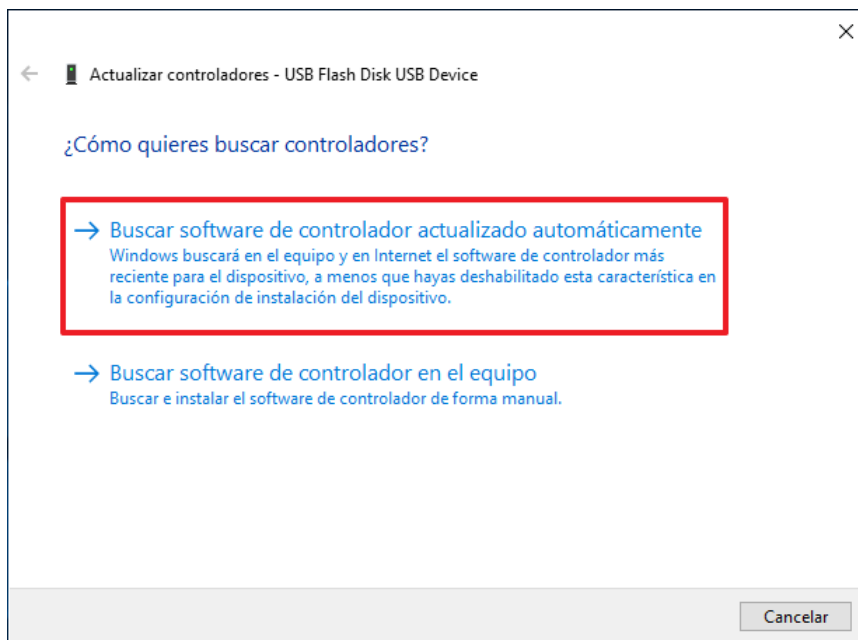
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 
3.	El control de cuentas le solicitará la elevación de privilegios. Introduzca las credenciales de un administrador local de la máquina y pulse “Sí” para continuar.
4.	Introduzca el comando “gpedit.msc” y pulse “Enter”. 
5.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

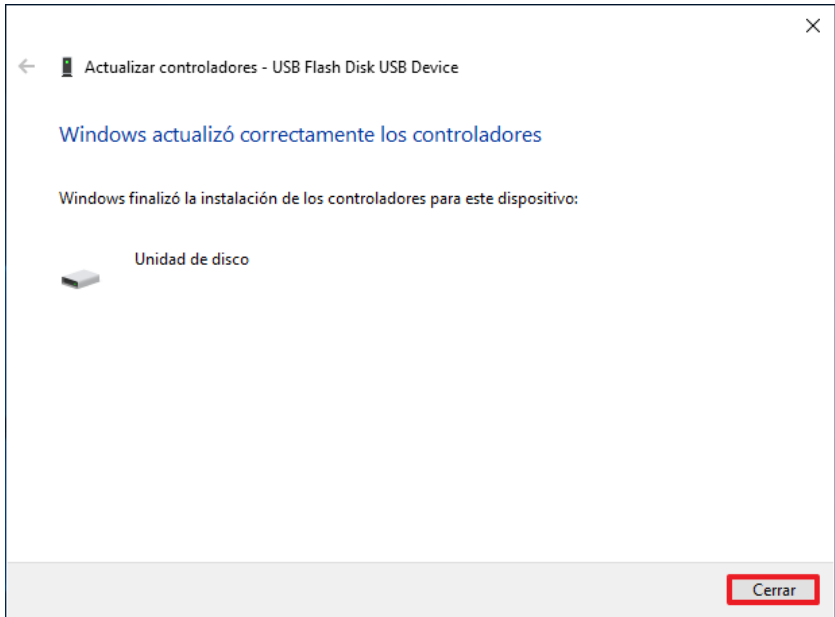
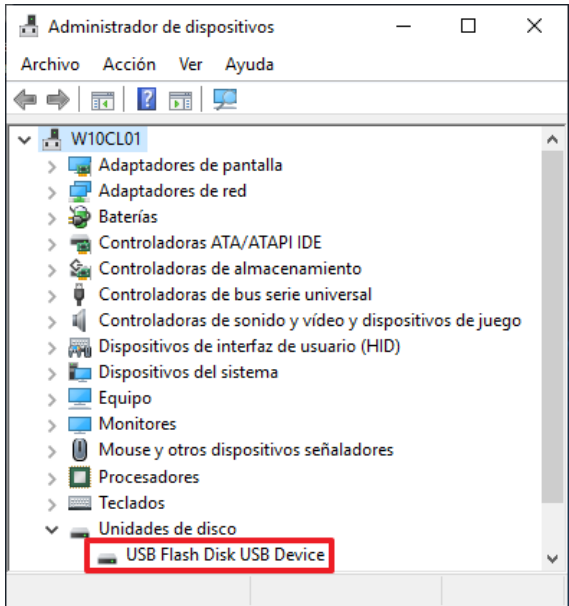
Paso	Descripción
6.	Haga doble clic sobre la directiva “Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos” y configúrela para que su estado sea “Habilitada”. A continuación seleccione “Aceptar”. 
7.	Para iniciar la instalación de un dispositivo USB deberá conectar el dispositivo USB en el equipo. Tras conectarlo aparecerá una notificación indicando que “La directiva de sistema prohíbe la instalación de este dispositivo”.  Nota: Es necesario tener en consideración que la instalación de los dispositivos USB de realizarse de manera manual y por un usuario que pertenezca al grupo local administradores.

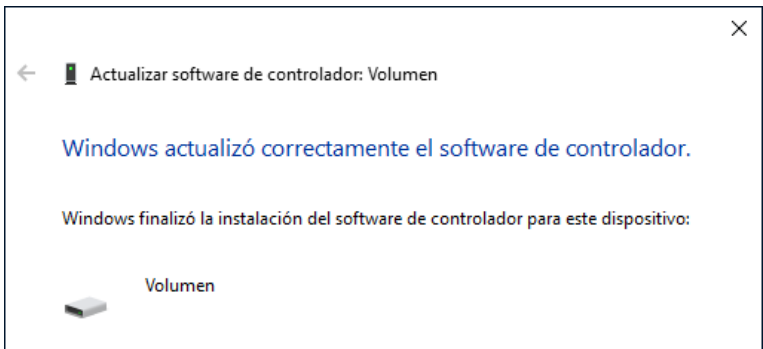
Paso	Descripción
8.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
9.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre de “Dispositivo desconocido”.

Paso	Descripción
10.	Haga clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 
11.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 

Paso	Descripción
12.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  Nota: No cierre el “Administrador de dispositivos” todavía.
13.	Tras la instalación de los controladores el sistema reconocerá el dispositivo. Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: En este ejemplo se utiliza el dispositivo denominado “USB Flash Disk USB Device”. Si el sistema no reconoce el dispositivo desconéctelo y vuélvalo a conectar para visualizarlo. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.

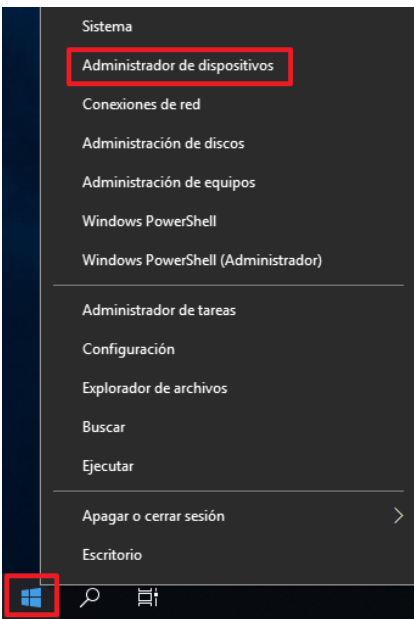
Paso	Descripción
14.	Haga de nuevo clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 
15.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 

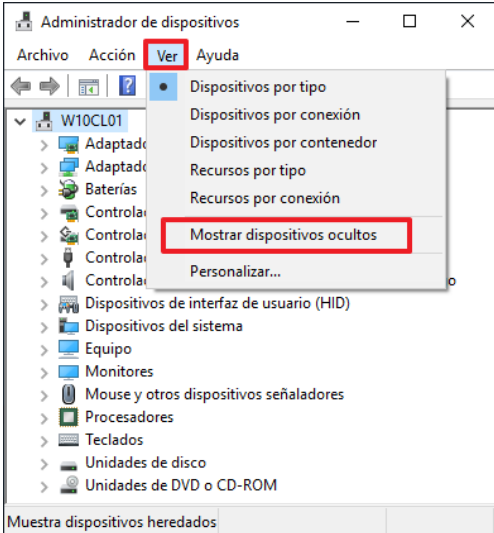
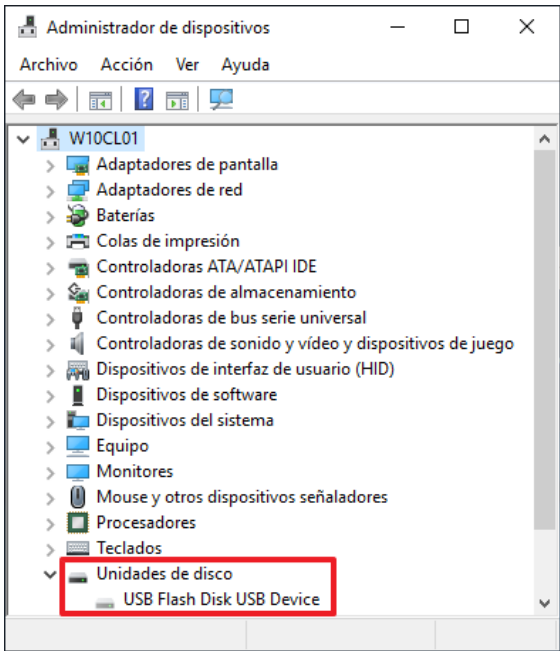
Paso	Descripción
16.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  Nota: Deberá repetir estos pasos hasta que su dispositivo de almacenamiento aparezca en el apartado “Unidades de disco”.
17.	Tras completarse la instalación, despliegue el nodo “Unidades de disco” y compruebe que el USB es reconocido por el equipo.  Nota: Espere a que el dispositivo sea reconocido por el equipo. En caso de no ser así, extraiga y vuelva a conectar el dispositivo para que éste sea reconocido. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.

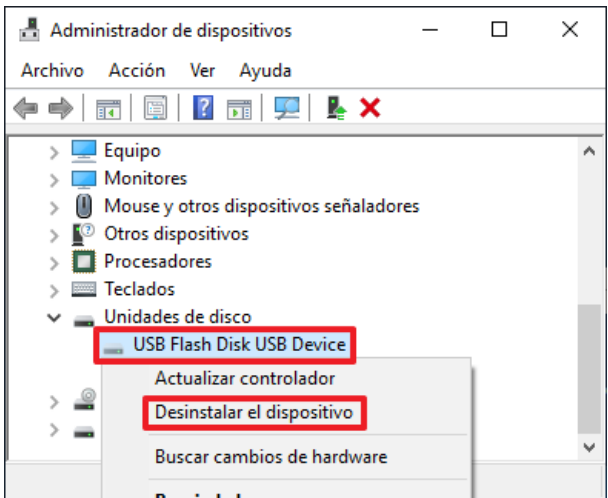
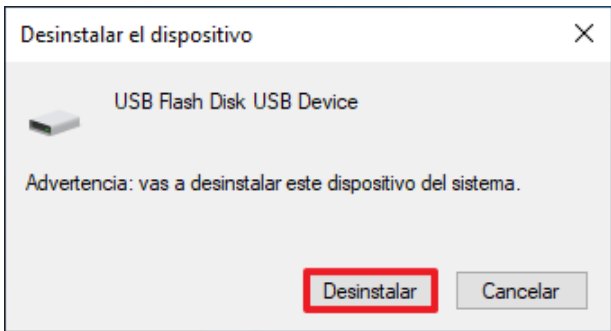
Paso	Descripción
18.	En caso de que el dispositivo aparezca en el apartado “Unidades de disco” pero no puede hacer uso de él a través del explorador de ficheros es posible que dentro del apartado “Otros dispositivos” quede algún “Dispositivo desconocido” que haga referencia a “Volumen”. Deberá instalar este controlador también para poder hacer uso del dispositivo. 
19.	El dispositivo está listo para ser utilizado.

1.2. DESINSTALACIÓN DE CONTROLADORES PARA IMPEDIR EL USO DE DISPOSITIVOS USB

Tras la instalación del dispositivo y su posterior uso, será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

Paso	Descripción
20.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores”.
21.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

Paso	Descripción
22.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 
23.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 

Paso	Descripción
24.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
25.	Pulse “Desinstalar” ante la advertencia emergente.  Nota: Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo a no ser que se vuelva a instalar dicho controlador.

2. ADMINISTRAR EL USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE EL IDENTIFICADOR DE DISPOSITIVO

Este apartado establece los procedimientos para la configuración y gestión de los dispositivos USB mediante su identificador de dispositivo.

Nota: Antes de proceder a la configuración de los dispositivos USB mediante el filtrado de su identificador, deberá verificar si el/los dispositivos USB a configurar tienen el mismo identificador/dato primario/chipset. Si es así, al configurar dicho USB, estará autorizando el uso de dispositivos de forma masiva en el sistema. Por lo tanto, antes de instalar los dispositivos USB deberá verificar que su organización no dispone de USB's con el mismo identificador.

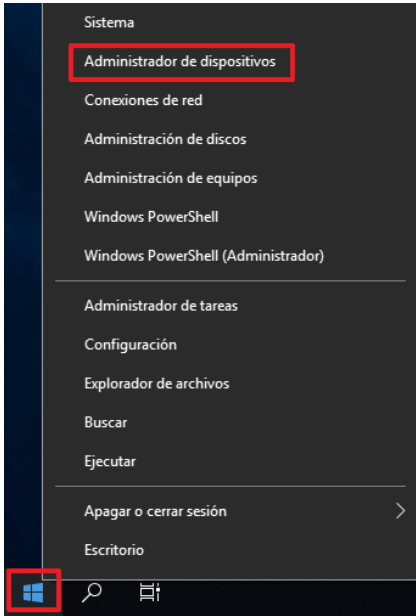
2.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

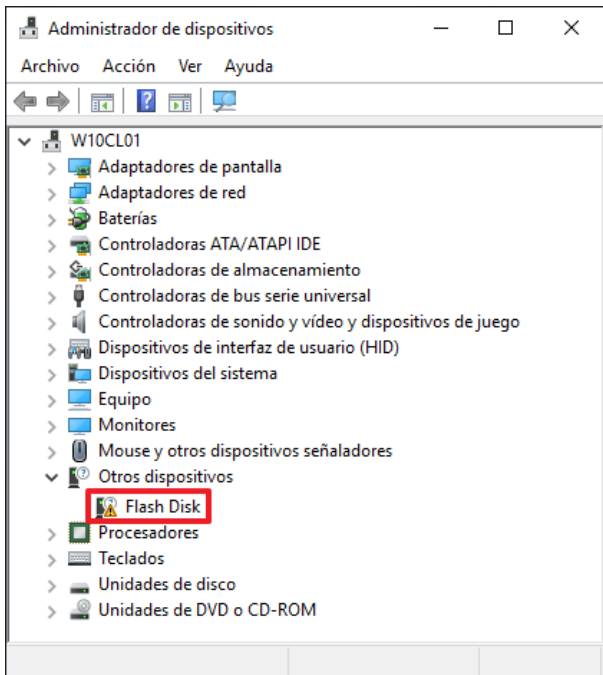
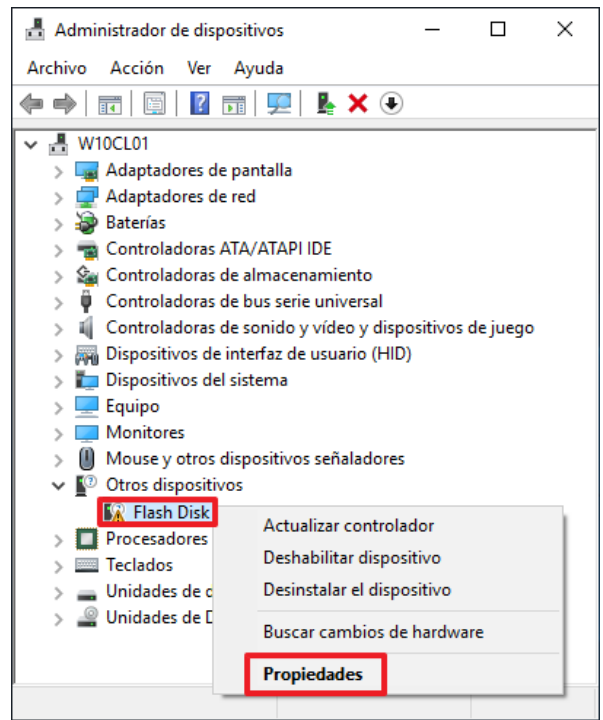
Este punto describe el proceso para permitir el uso un dispositivo mediante el filtrado por su identificador. Cuando el filtro esté realizado, los controladores del dispositivo se instalarán de manera automática y el dispositivo podrá ser utilizado.

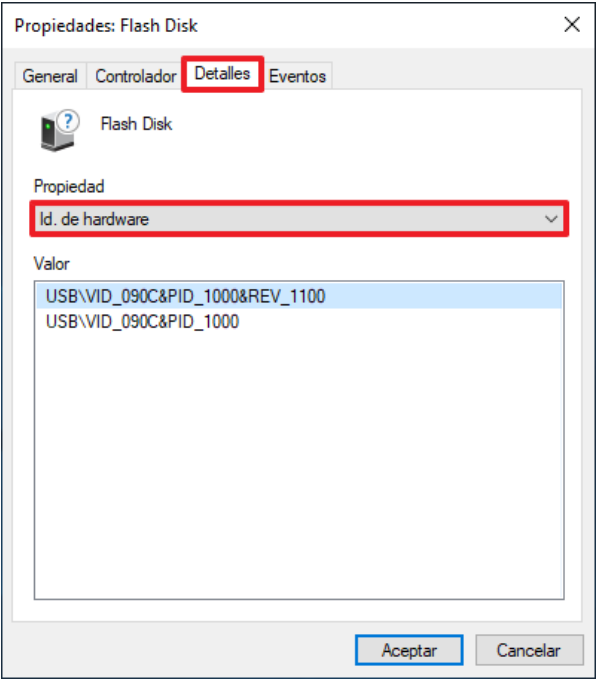
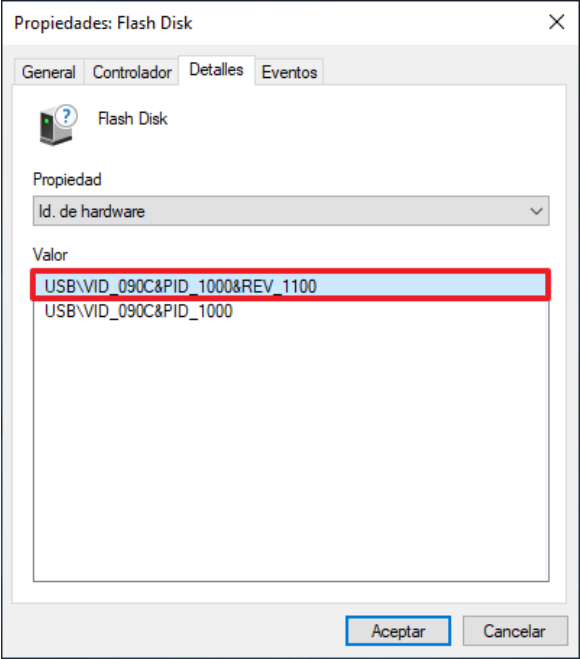
Tras la finalización de su uso, los controladores del dispositivo serán desinstalados tanto si el dispositivo se encuentra conectado al equipo como si no.

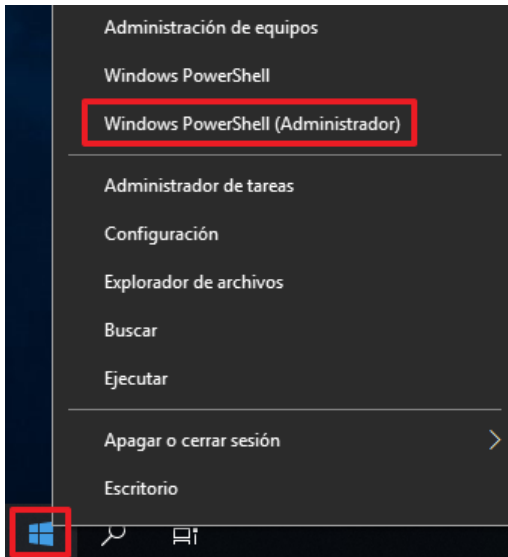
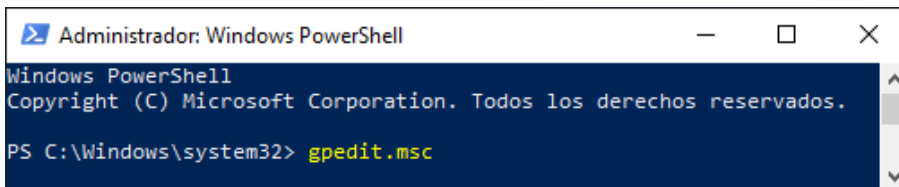
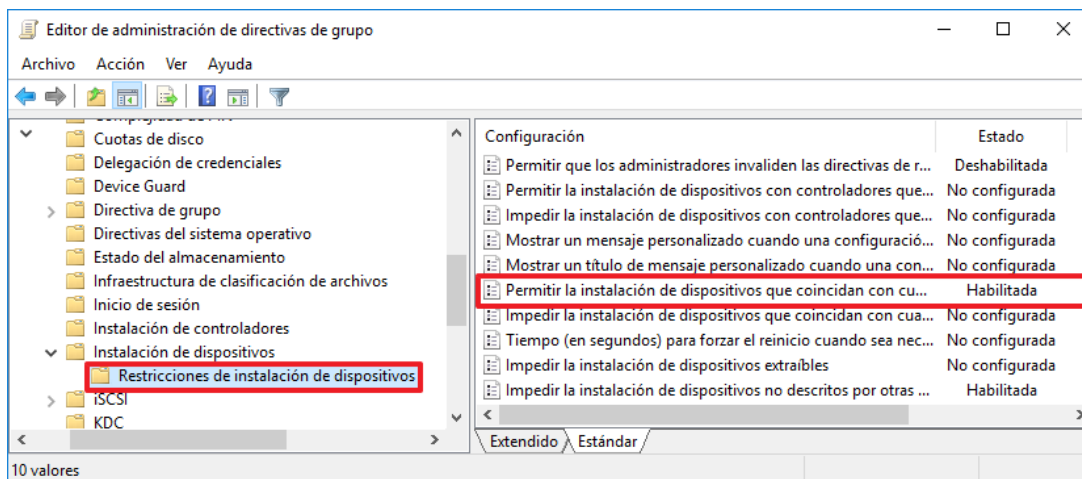
Será necesario añadir varios identificadores para un mismo dispositivo USB. Esto es debido a que el sistema va especificando el tipo de dispositivo de modo que puede concretar los controladores necesarios hasta permitir su funcionamiento.

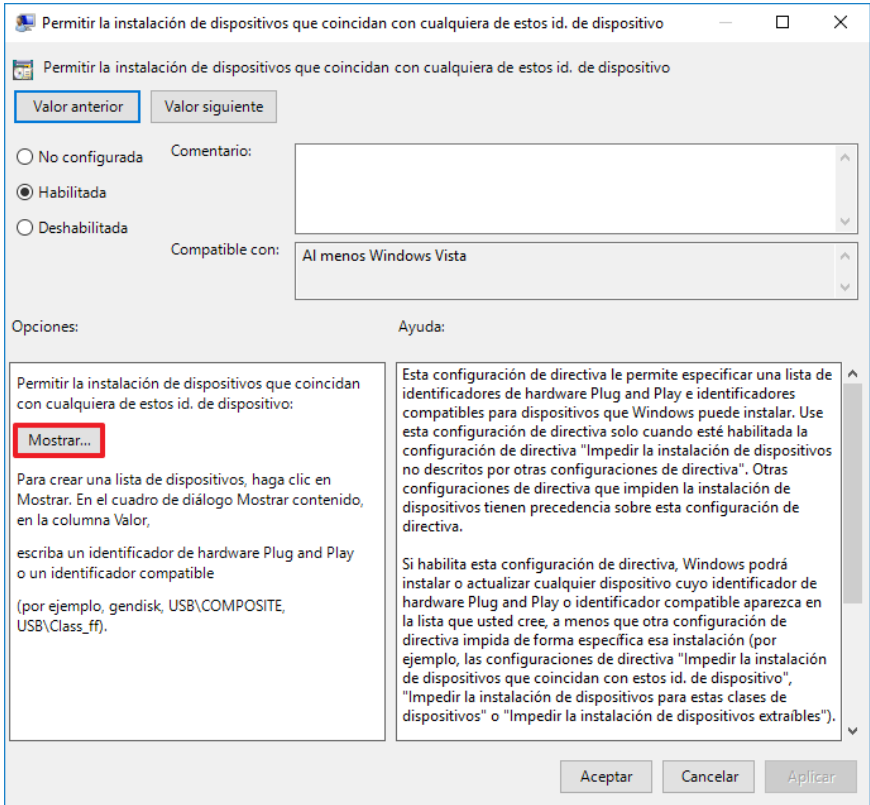
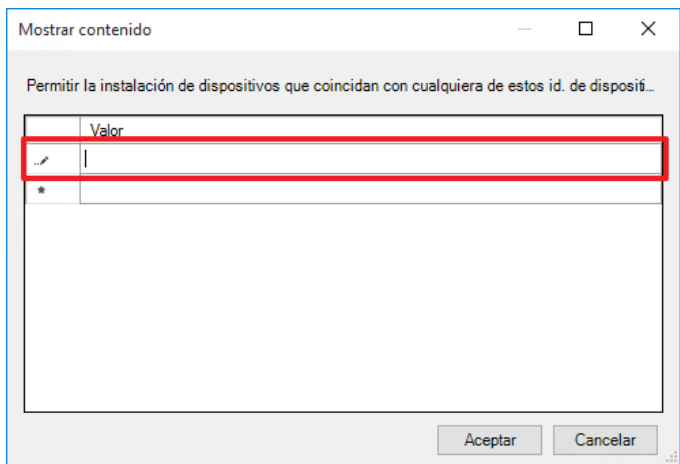
Tras el uso de los dispositivos se procederá a eliminar los identificadores de la lista configurada, y a desinstalar los controladores para evitar el uso de éstos.

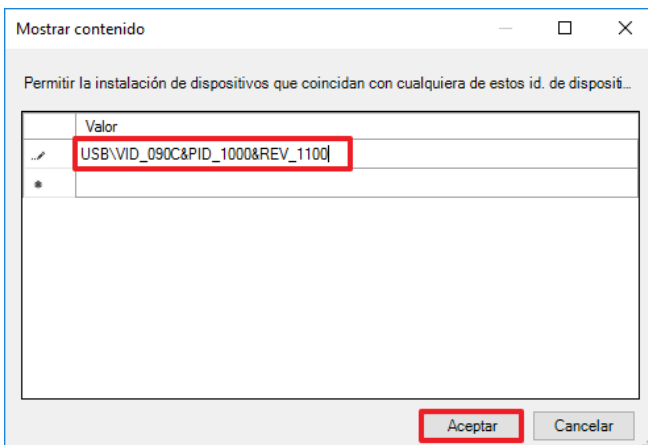
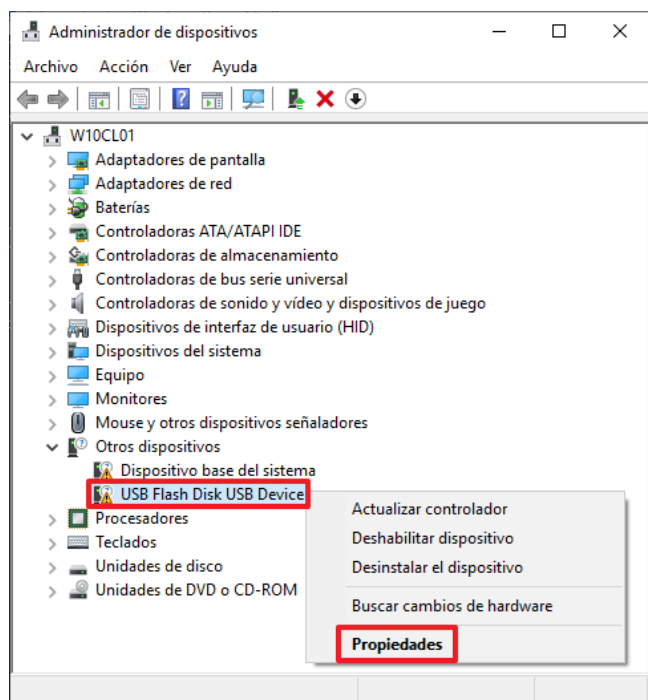
Paso	Descripción
26.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
27.	Para iniciar la instalación de un dispositivo USB deberá conectarlo en el equipo. Nota: Es necesario tener en consideración que la instalación de los dispositivos USB debe realizarse de manera manual y por un usuario con permisos de administrador.
28.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  The screenshot shows the Windows Start menu search results for 'Administrador de dispositivos'. The search bar at the top contains the text 'Administrador de dispositivos'. Below the search bar, a list of results is displayed, including 'Sistema', 'Administrador de dispositivos', 'Conexiones de red', 'Administración de discos', 'Administración de equipos', 'Windows PowerShell', 'Windows PowerShell (Administrador)', 'Administrador de tareas', 'Configuración', 'Explorador de archivos', 'Buscar', 'Ejecutar', 'Apagar o cerrar sesión', and 'Escritorio'. The 'Administrador de dispositivos' result is highlighted with a red box. At the bottom of the screen, the Windows taskbar is visible, with the Start button also highlighted with a red box. Nota: El sistema le solicitará elevación de privilegios.

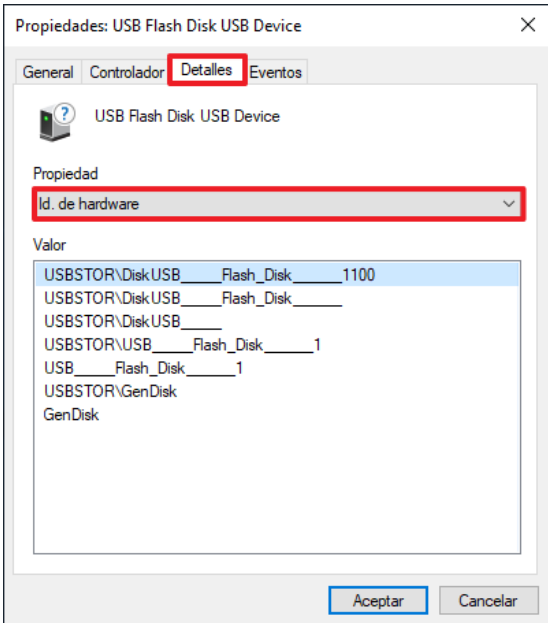
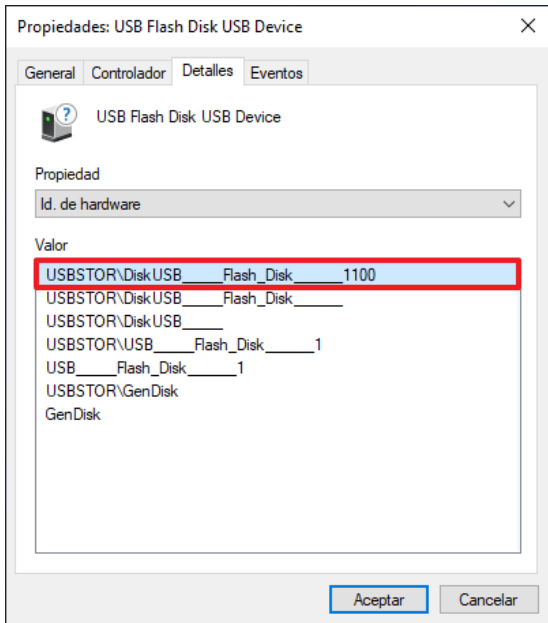
Paso	Descripción
29.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre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

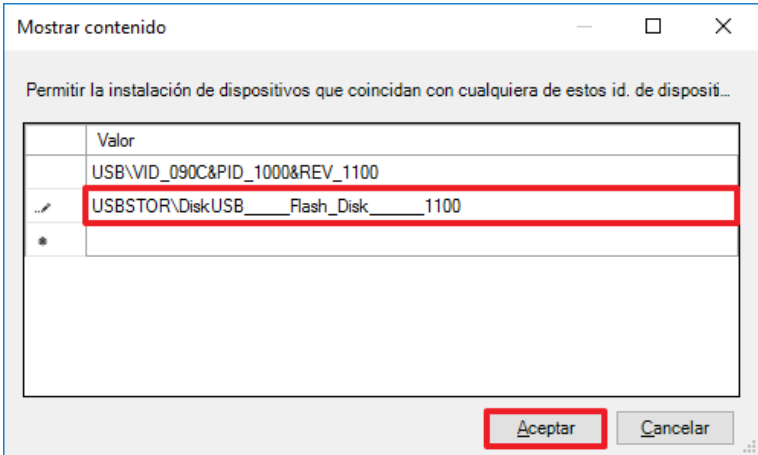
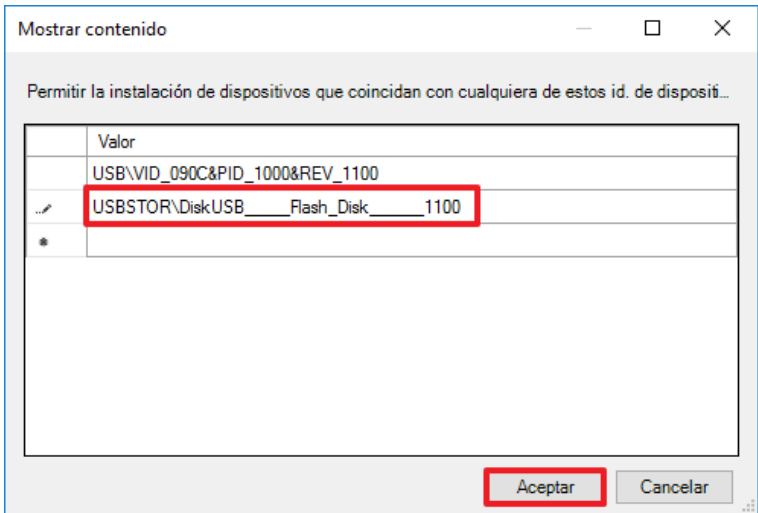
Paso	Descripción
31.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Id. de hardware”. 
32.	Seleccione el identificador que se encuentre en primer lugar y anótelo para poder introducirlo más adelante.  Nota: Independientemente del numero de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.
33.	Sin cerrar el “Administrador de dispositivos” continúe con el siguiente paso.

Paso	Descripción																						
34.	Ejecute una consola de PowerShell con permisos de administrador. Para ello, pulse sobre el botón “Inicio” y seleccione “Windows PowerShell → Windows Powershell” .																						
35.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 																						
36.	El control de cuentas le solicitará la elevación de privilegios. Introduzca las credenciales de un administrador local de la máquina y pulse “Sí” para continuar.																						
37.	Introduzca el comando “gpedit.msc” y pulse “Enter”. 																						
38.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos” .  <table border="1"> <thead> <tr> <th>Configuración</th> <th>Estado</th> </tr> </thead> <tbody> <tr> <td>Permitir que los administradores invaliden las directivas de r...</td> <td>Deshabilitada</td> </tr> <tr> <td>Permitir la instalación de dispositivos con controladores que...</td> <td>No configurada</td> </tr> <tr> <td>Impedir la instalación de dispositivos con controladores que...</td> <td>No configurada</td> </tr> <tr> <td>Mostrar un mensaje personalizado cuando una configuraci...</td> <td>No configurada</td> </tr> <tr> <td>Mostrar un título de mensaje personalizado cuando una con...</td> <td>No configurada</td> </tr> <tr> <td>Permitir la instalación de dispositivos que coincidan con cu...</td> <td>Habilitada</td> </tr> <tr> <td>Impedir la instalación de dispositivos que coincidan con cua...</td> <td>No configurada</td> </tr> <tr> <td>Tiempo (en segundos) para forzar el reinicio cuando sea nec...</td> <td>No configurada</td> </tr> <tr> <td>Impedir la instalación de dispositivos extraíbles</td> <td>No configurada</td> </tr> <tr> <td>Impedir la instalación de dispositivos no descritos por otras ...</td> <td>Habilitada</td> </tr> </tbody> </table>	Configuración	Estado	Permitir que los administradores invaliden las directivas de r...	Deshabilitada	Permitir la instalación de dispositivos con controladores que...	No configurada	Impedir la instalación de dispositivos con controladores que...	No configurada	Mostrar un mensaje personalizado cuando una configuraci...	No configurada	Mostrar un título de mensaje personalizado cuando una con...	No configurada	Permitir la instalación de dispositivos que coincidan con cu...	Habilitada	Impedir la instalación de dispositivos que coincidan con cua...	No configurada	Tiempo (en segundos) para forzar el reinicio cuando sea nec...	No configurada	Impedir la instalación de dispositivos extraíbles	No configurada	Impedir la instalación de dispositivos no descritos por otras ...	Habilitada
Configuración	Estado																						
Permitir que los administradores invaliden las directivas de r...	Deshabilitada																						
Permitir la instalación de dispositivos con controladores que...	No configurada																						
Impedir la instalación de dispositivos con controladores que...	No configurada																						
Mostrar un mensaje personalizado cuando una configuraci...	No configurada																						
Mostrar un título de mensaje personalizado cuando una con...	No configurada																						
Permitir la instalación de dispositivos que coincidan con cu...	Habilitada																						
Impedir la instalación de dispositivos que coincidan con cua...	No configurada																						
Tiempo (en segundos) para forzar el reinicio cuando sea nec...	No configurada																						
Impedir la instalación de dispositivos extraíbles	No configurada																						
Impedir la instalación de dispositivos no descritos por otras ...	Habilitada																						

Paso	Descripción
39.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar...”. 
40.	En la ventana emergente “Mostrar contenido” haga doble clic sobre la primera línea para poder escribir. Introduzca entonces el identificador del dispositivo USB copiado anteriormente.  Nota: Asegúrese de que no existe ningún espacio en blanco.

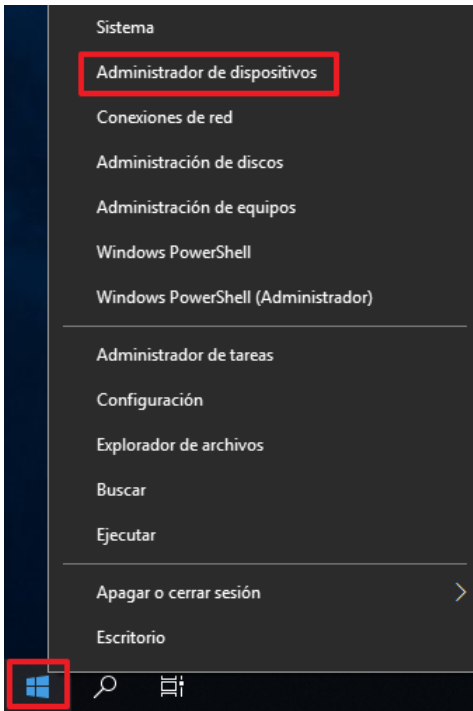
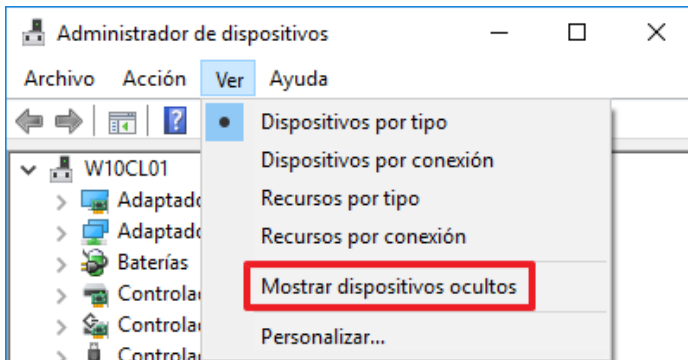
Paso	Descripción
41.	Verifique el identificador introducido y pulse “Aceptar” para continuar. 
42.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.
43.	Sin cerrar el “Editor de directivas de grupo local” continúe con el siguiente paso.
44.	Acceda de nuevo al “Administrador de dispositivos”. En este punto el dispositivo será reconocido por el equipo. Seleccione dicho dispositivo con el botón derecho y pulse sobre la opción “Propiedades”.  Nota: Espere a que el dispositivo sea reconocido por el equipo. En caso de no ser así, extraiga y vuelva a conectar el dispositivo para que éste sea reconocido. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.

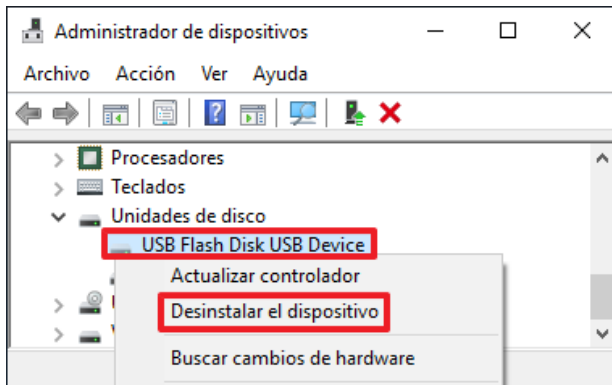
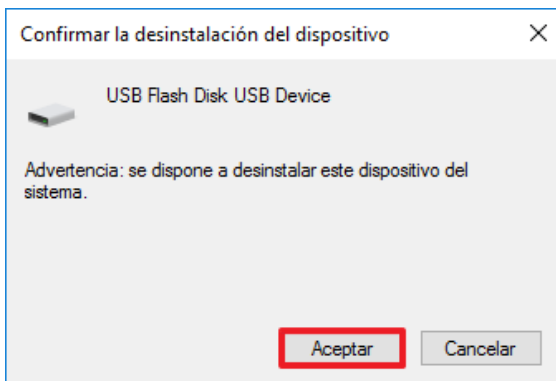
Paso	Descripción
45.	Acceda de nuevo a la pestaña “Detalles” y en el apartado “Propiedad” seleccione “Id. de hardware”.  Nota: Los identificadores del dispositivo han cambiado debido a que el equipo ya no lo toma como dispositivo genérico por lo que proporciona un identificador específico del dispositivo.
46.	Seleccione el identificador que se encuentre en primer lugar y anótelolo para poder introducirlo más adelante.  Nota: Independientemente del numero de identificadores existentes deberá seleccionar siempre aquél que se encuentre en primera posición.

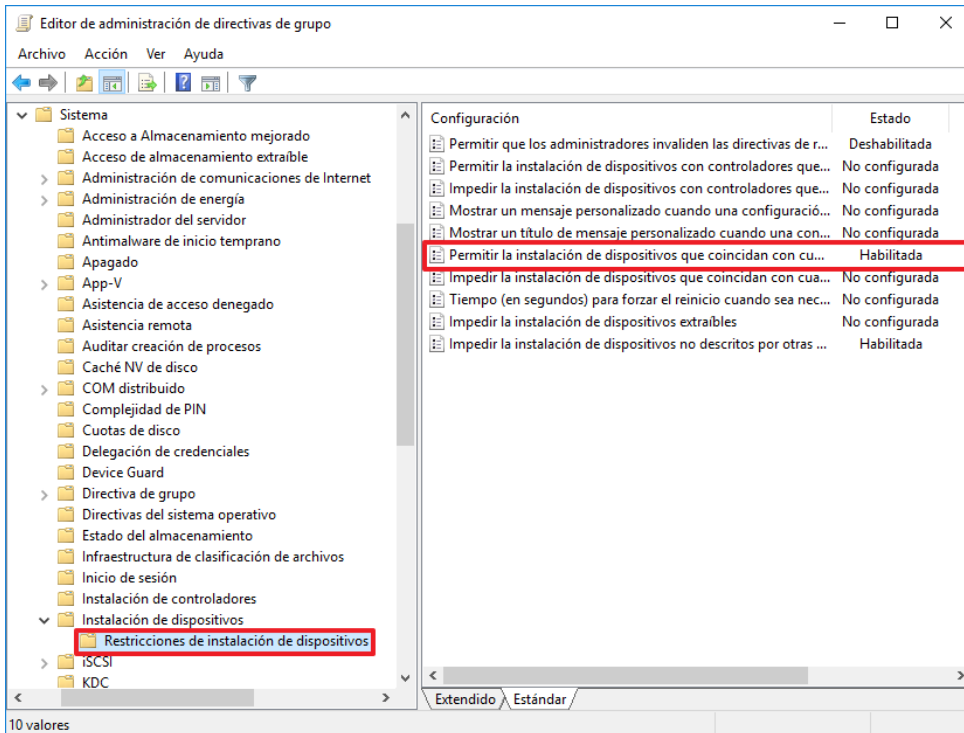
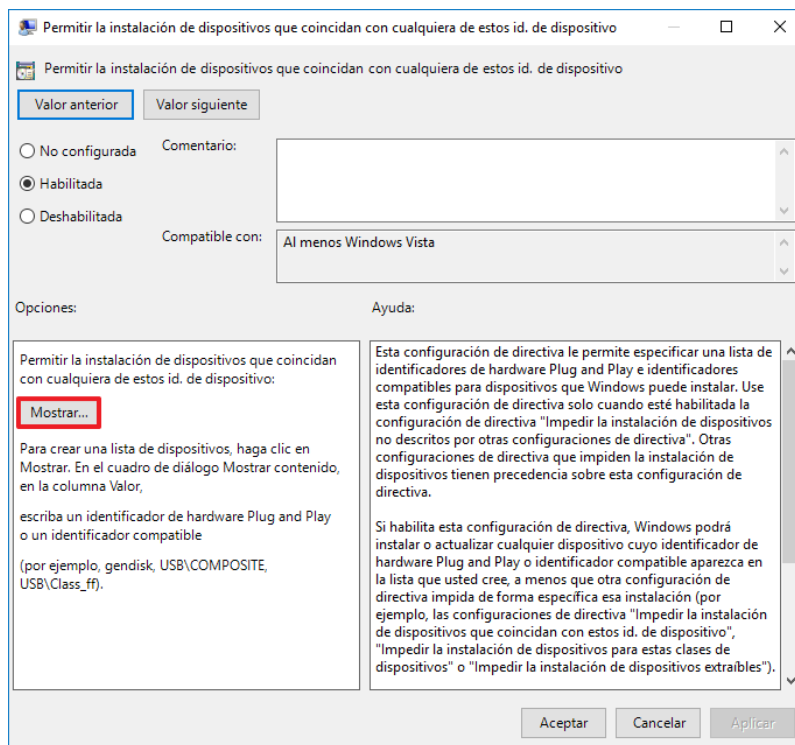
Paso	Descripción
47.	En la ventana “Mostrar contenido” abierta en pasos anteriores desde la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, haga doble clic sobre la segunda línea en blanco. Introduzca entonces el identificador de USB copiado anteriormente. Pulse “Aceptar” para continuar. 
48.	Aparecerá el nuevo identificador del dispositivo. Pulse “Aceptar” para continuar. 
49.	Deberá repetir este proceso hasta que no se muestren nuevos identificadores en la propiedad “ID. de Hardware” del dispositivo que está instalando. Nota: En este ejemplo solo ha sido necesario el uso de dos identificadores. Dependiendo del dispositivo conectado, tendrá un número diferente de identificadores en la lista. Deberá tener en cuenta la posibilidad de necesitar ID’s adicionales referentes al dispositivo “Volumen”.
50.	A partir de este momento el dispositivo estará listo para su uso.

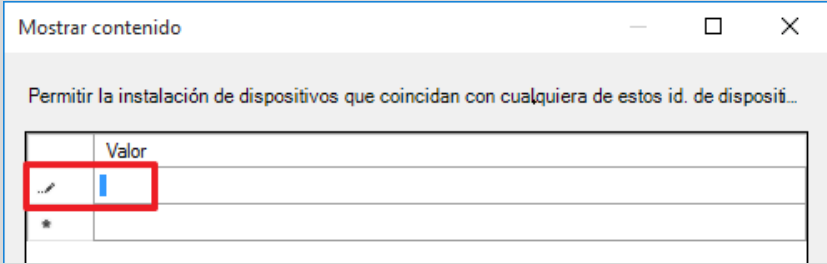
2.2. IMPEDIR EL USO DE DISPOSITIVOS USB

Tras la instalación del dispositivo y su posterior uso, será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

Paso	Descripción
51.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
52.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
53.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

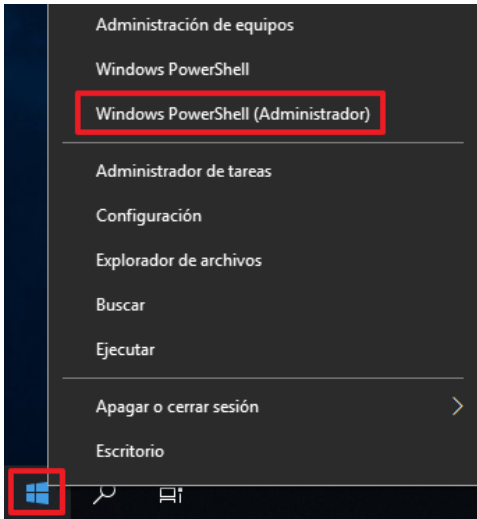
Paso	Descripción
54.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 
55.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
56.	Pulse “Aceptar” ante la advertencia emergente.  Nota: Una vez confirmada la desinstalación, el dispositivo USB no podrá usarse en el equipo.

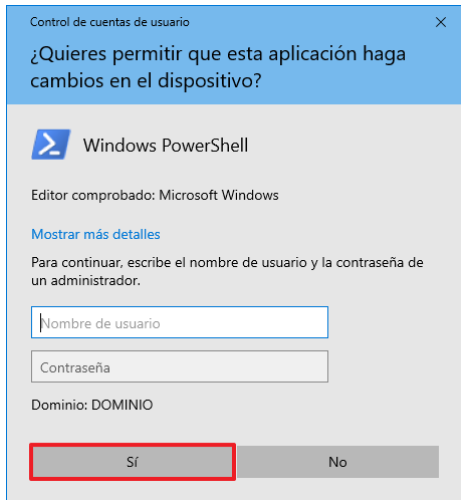
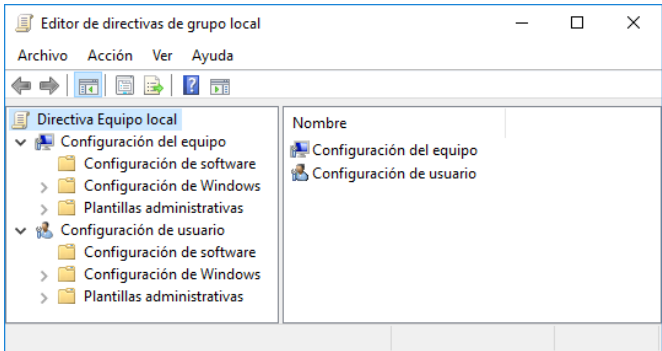
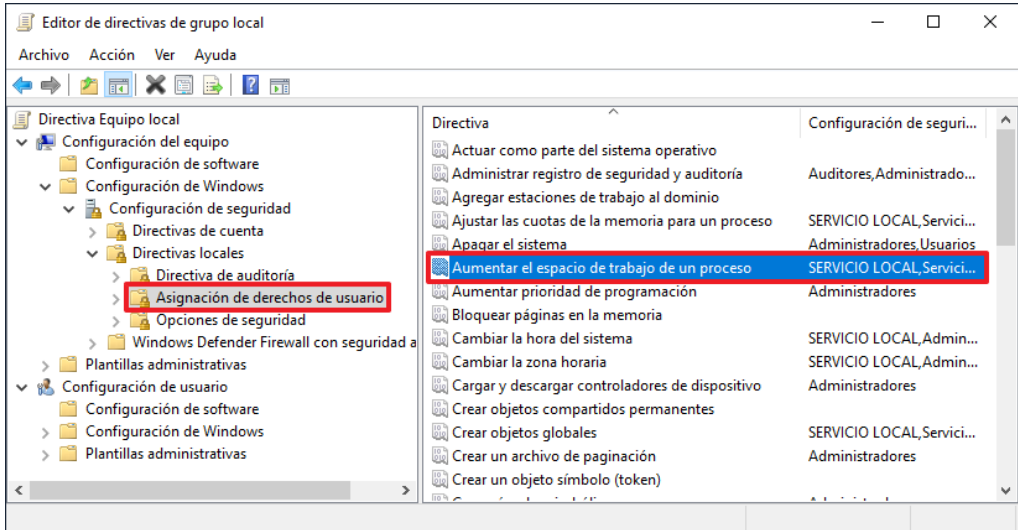
Paso	Descripción
57.	En el “Editor de directivas de grupo local” despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 
58.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón “Mostrar...”. 

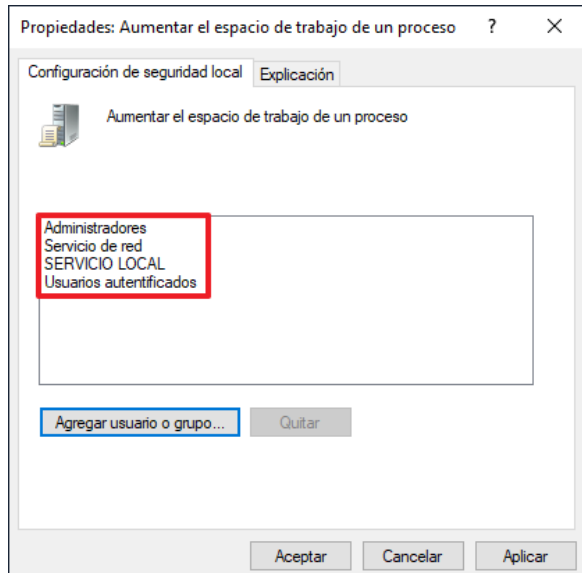
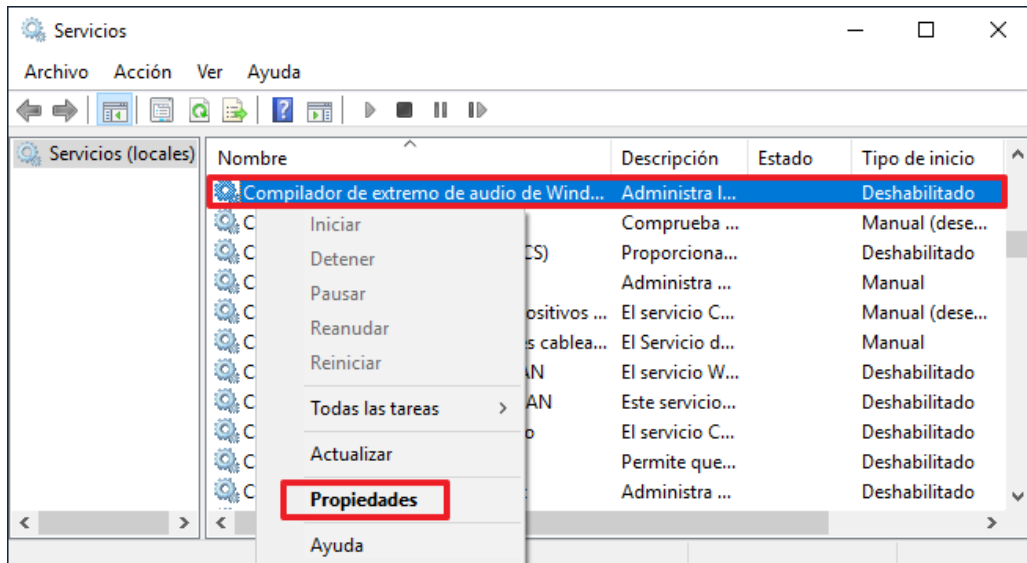
Paso	Descripción
59.	Identifique las líneas que correspondan con el dispositivo. Haga doble clic sobre cada línea y elimine su contenido. Nota: En caso de eliminar todas las líneas debe dejarse al menos una línea con un espacio en blanco para poder cerrar la configuración de la directiva. En caso contrario se mostrará un error. 

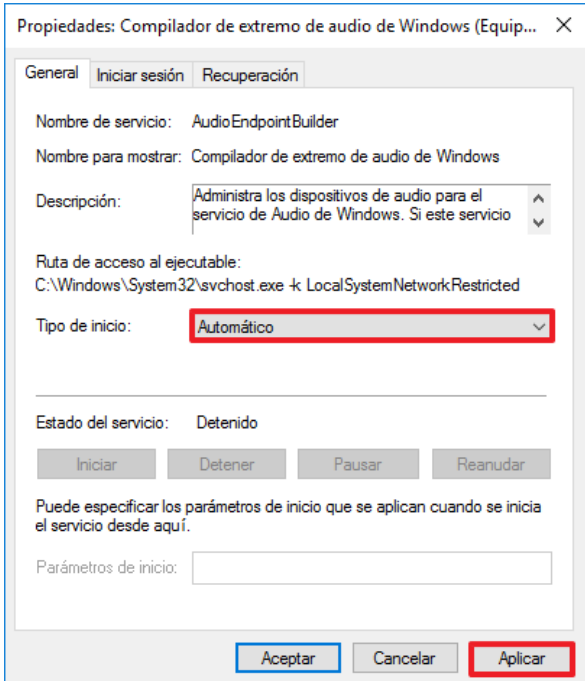
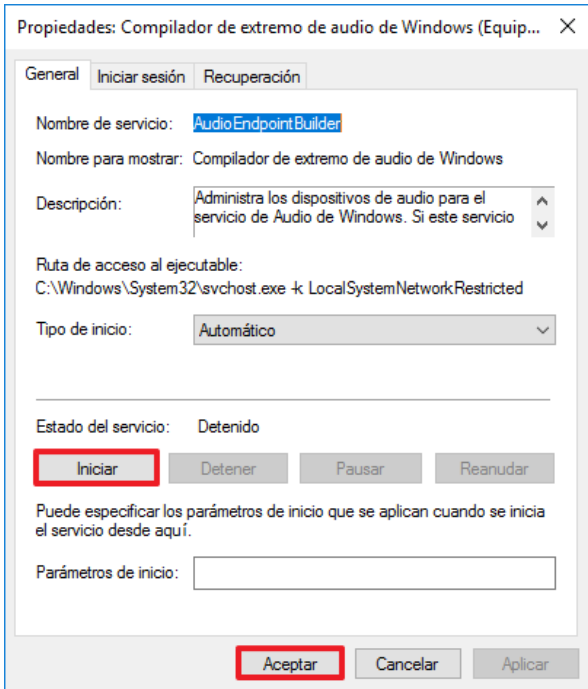
ANEXO D.3.5. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599B19

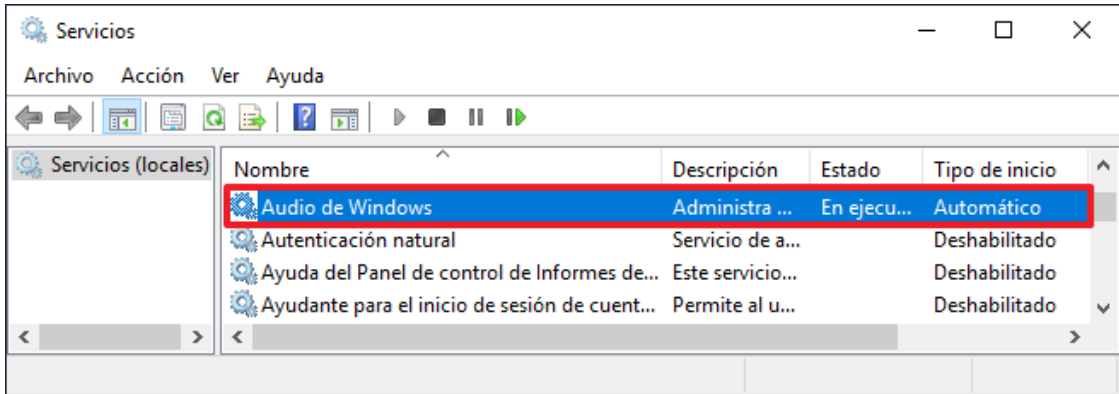
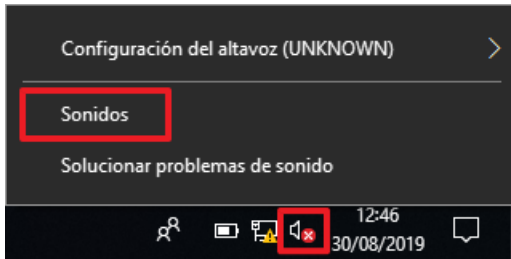
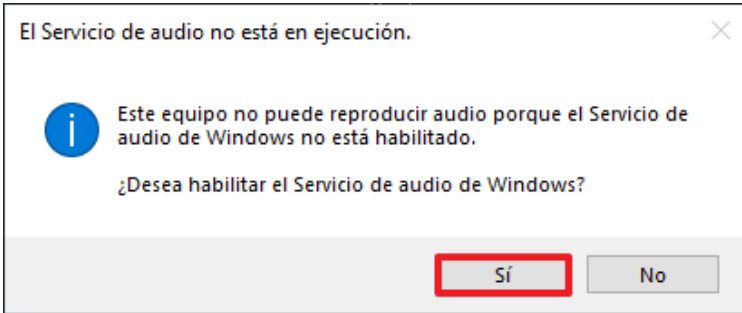
A continuación, se indican los pasos a realizar para modificar la plantilla de seguridad a aplicar sobre equipos Microsoft Windows 10, independientes del dominio, con el objetivo de habilitar el audio del sistema. Para habilitar el audio en los equipos, se deberá actualizar el objeto de directiva de grupo local siguiendo la configuración que se indica a continuación.

Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 

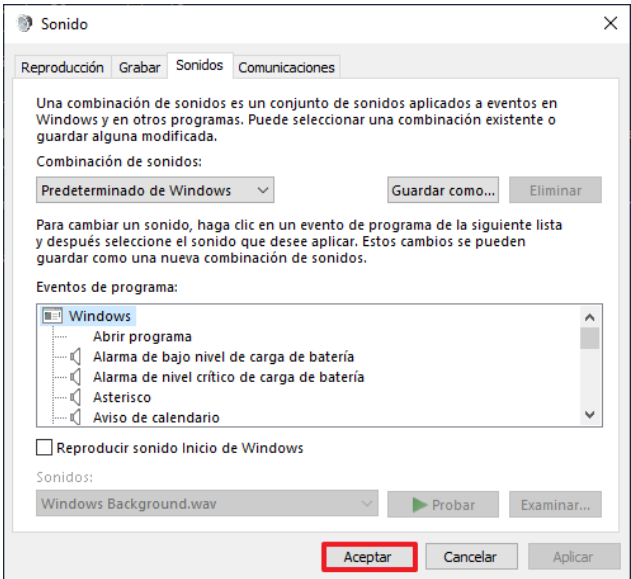
Paso	Descripción
3.	Eleve privilegios ante el control de cuentas de usuario 
4.	En la ventana de PowerShell ejecute "gpedit.msc". Esto abrirá una ventana del Editor de directivas de grupo local, como la mostrada en la siguiente figura. 
5.	Despliegue el nodo “Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” y seleccione con doble clic la directiva “Aumentar el espacio de trabajo de un proceso”. 

Paso	Descripción						
6.	Modifique los valores de equipo indicados en la tabla. Para ello, pulse “Agregar usuario o grupo...”. Seleccione los grupos correspondientes hasta que la configuración coincida con la tabla que se muestra a continuación. 						
	<table><tr><th>Directiva</th><th>Valor</th><th>Descripción</th></tr><tr><td>Aumentar el espacio de trabajo de un proceso</td><td> - Administradores - Servicio de red - SERVICIO LOCAL - Usuarios autenticados </td><td>Aumentar el espacio de trabajo de un proceso</td></tr></table>	Directiva	Valor	Descripción	Aumentar el espacio de trabajo de un proceso	- Administradores - Servicio de red - SERVICIO LOCAL - Usuarios autenticados	Aumentar el espacio de trabajo de un proceso
Directiva	Valor	Descripción					
Aumentar el espacio de trabajo de un proceso	- Administradores - Servicio de red - SERVICIO LOCAL - Usuarios autenticados	Aumentar el espacio de trabajo de un proceso					
7.	Modifique el modo de inicio del servicio de “Compilador de extremo de audio de Windows”. Para ello y desde la misma consola de PowerShell, ejecute el comando “Services.msc” del mismo modo que ejecutó “gpedit.msc” en pasos anteriores. Haga clic derecho sobre el servicio y seleccione “Propiedades”. 						

Paso	Descripción
8.	En el menú de “Propiedades: Compilador de extremo de audio de Windows (Equipo local)”, en el campo “Tipo de inicio” seleccione la opción “Automático” y pulse sobre el botón “Aplicar”. 
9.	Pulse sobre el botón “Iniciar” y cuando el estado del servicio sea “Iniciado”, pulse sobre el botón “Aceptar”. 

Paso	Descripción
10.	Realice el mismo procedimiento para iniciar el servicio “Audio de Windows”. 
11.	A continuación, en la barra de tareas, localice el icono de audio y pulsando con el botón derecho del ratón sobre él seleccione “Sonidos”. 
12.	En el siguiente mensaje del servicio de audio, pulse “Sí” para habilitar el servicio de audio de Windows. 
13.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores” y pulse “Sí”.

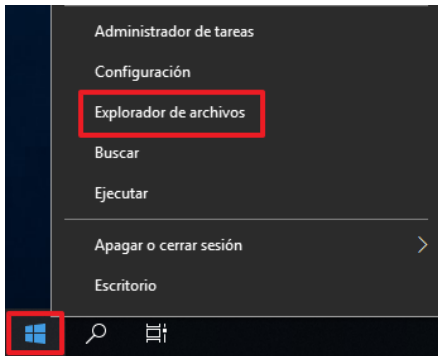
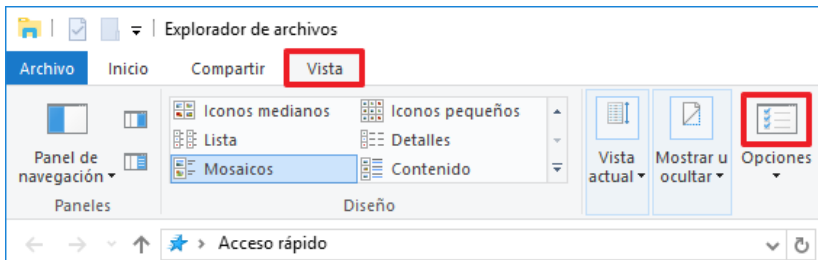
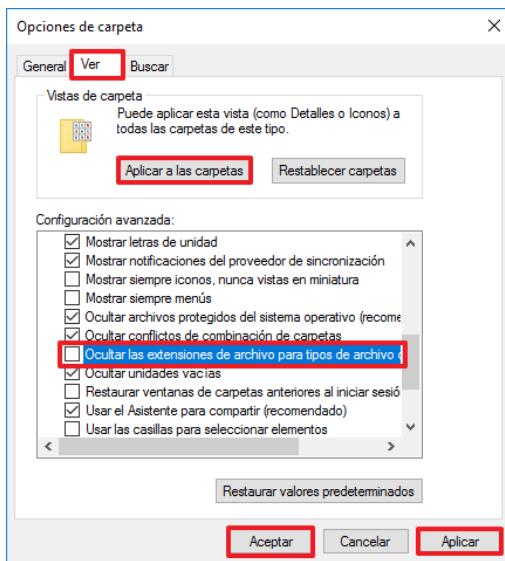


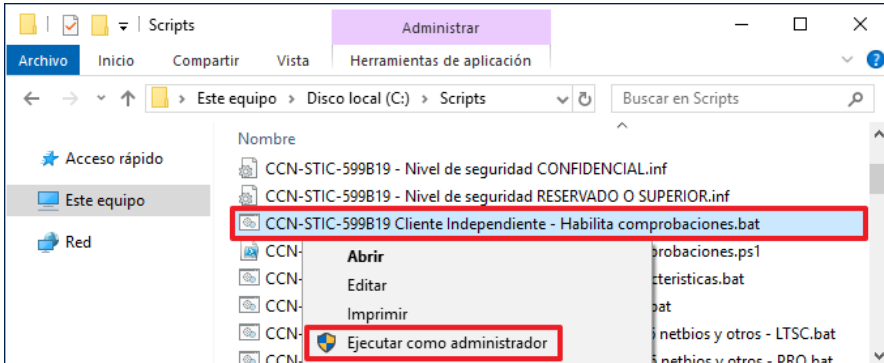
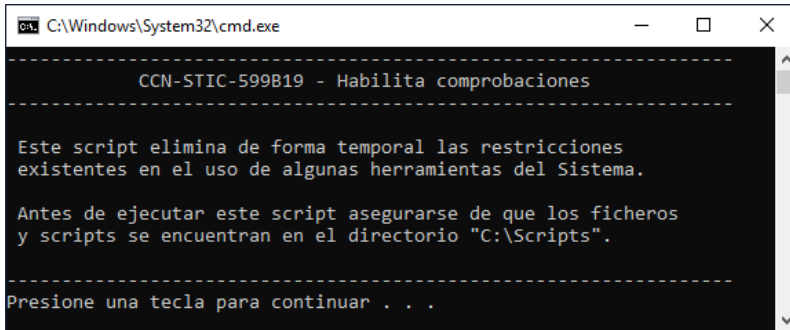
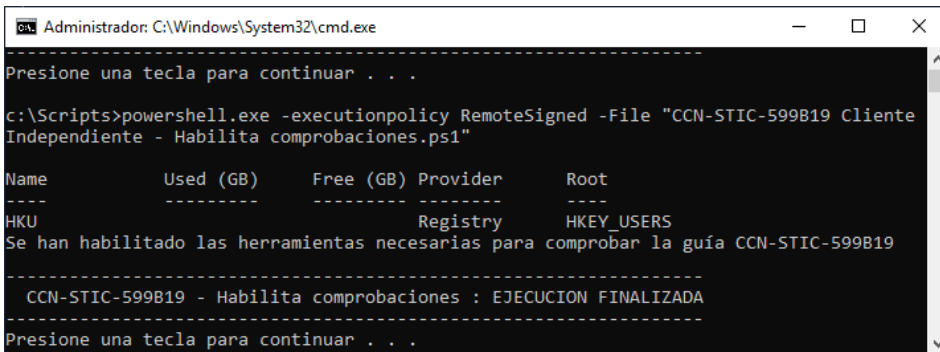
Paso	Descripción
14.	Tras aparecer la siguiente ventana de configuración de sonido, podrá hacer uso del sonido del sistema. Pulse “Aceptar” para cerrar la ventana. 
15.	Borre el directorio “C:\Scripts”. A partir de este momento, será posible hacer uso del sonido.

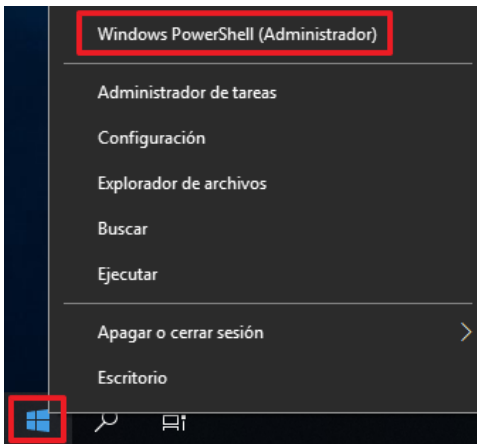
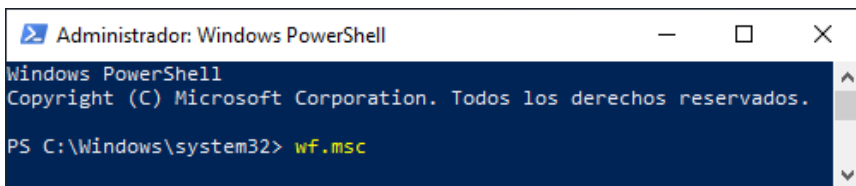
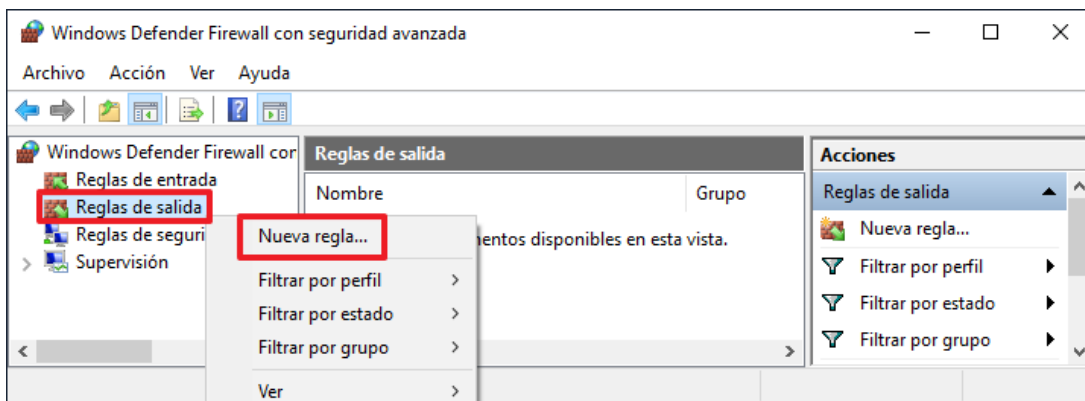
ANEXO D.3.6. CONFIGURACIÓN DE CLIENTE INDEPENDIENTE PARA PODER ACCEDER A UN RECURSO COMPARTIDO EN LA RED

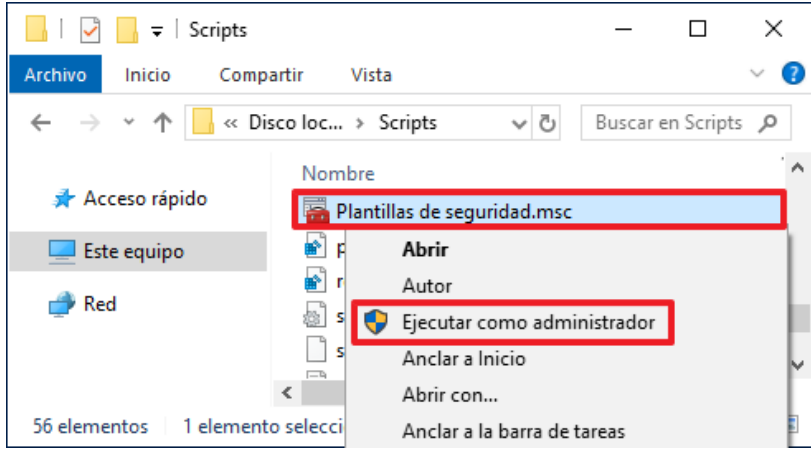
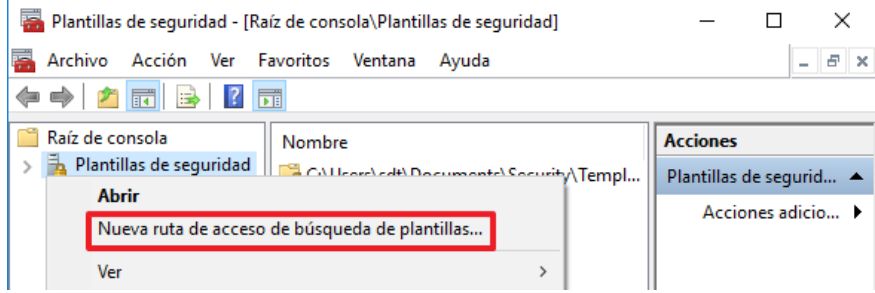
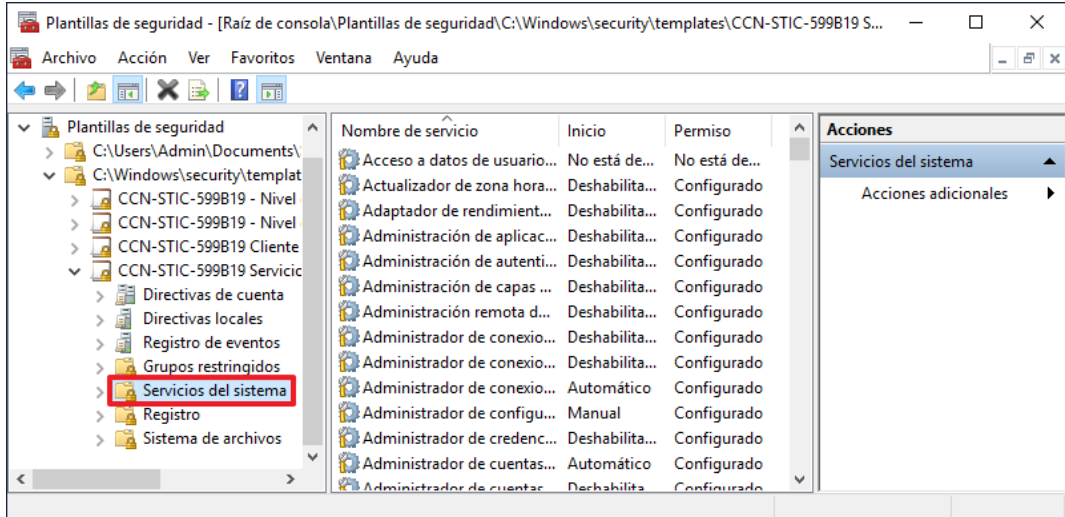
A continuación, se indican los pasos a realizar para modificar la configuración de un sistema Windows 10 que permita una conexión de un cliente independiente securizado con la guía CCN-STIC-599B19 a un recurso que se encuentre compartido dentro de la red.

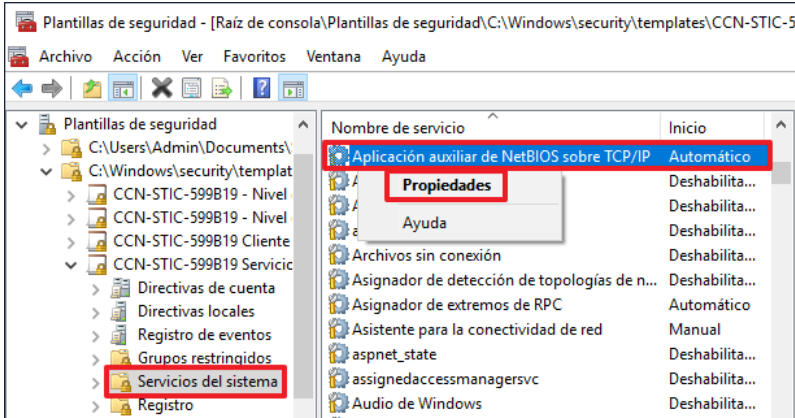
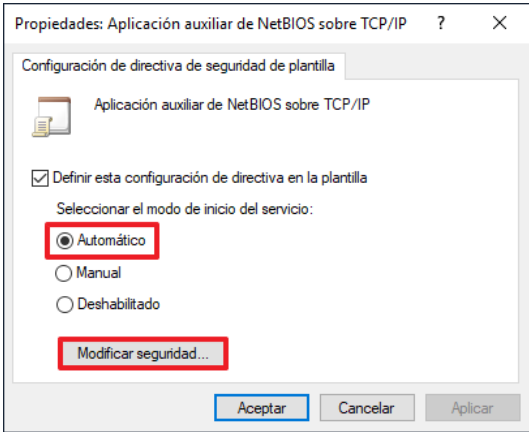
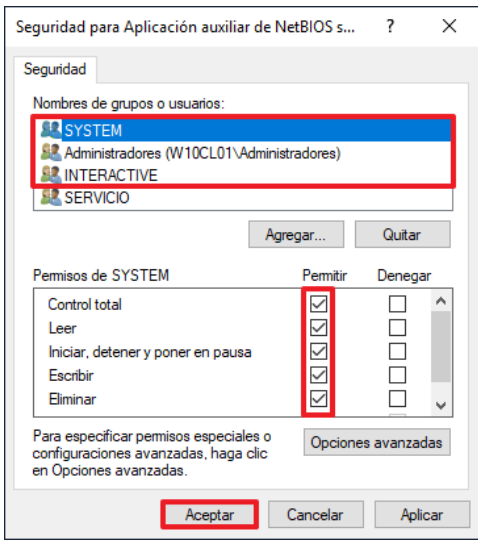
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta de usuario miembro del grupo “Administradores” y del grupo “Usuarios de shells”.
2.	Cree el directorio “Scripts” en la unidad “C:\”
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599B19”. Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

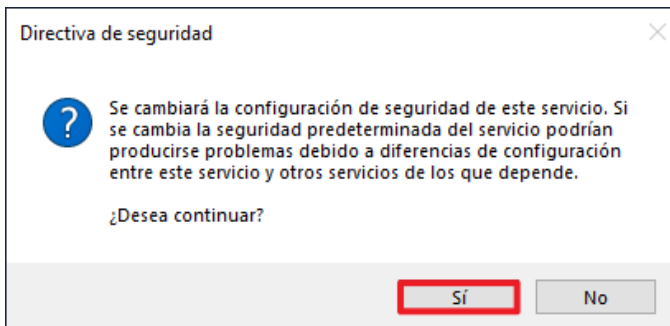
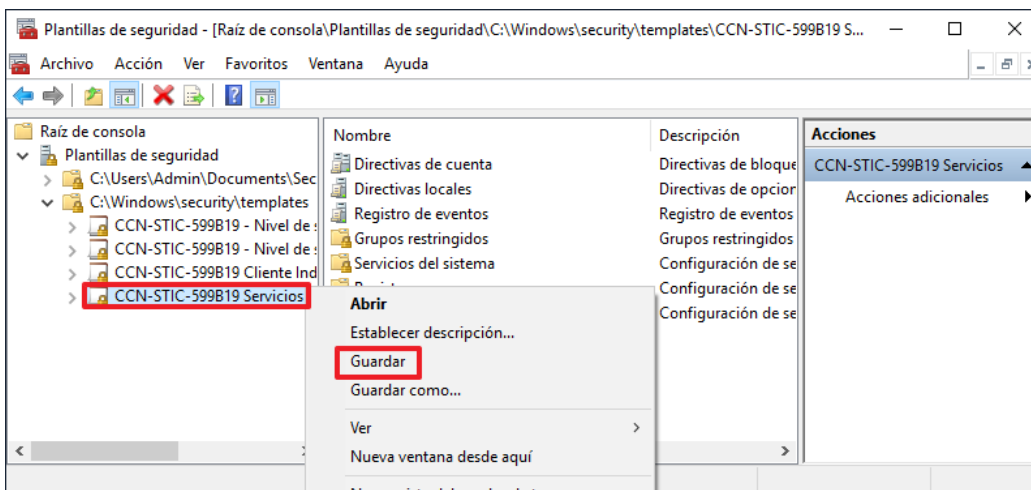
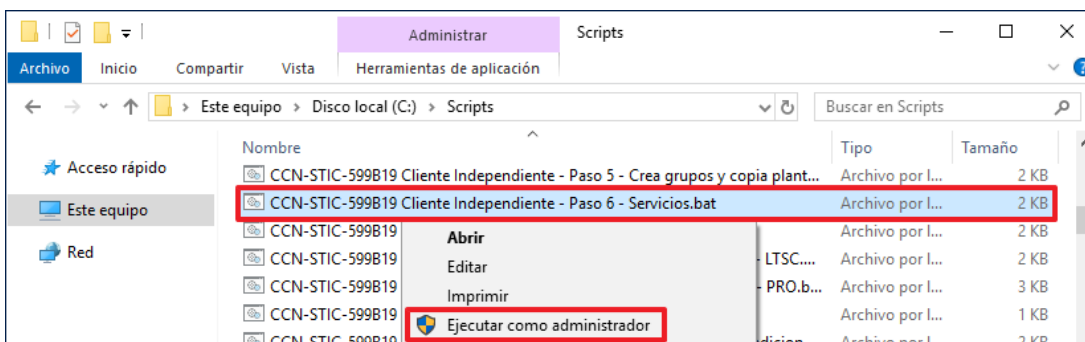
Paso	Descripción
4.	Si no lo hizo previamente, configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el “Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 
5.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono “Opciones”. 
6.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 

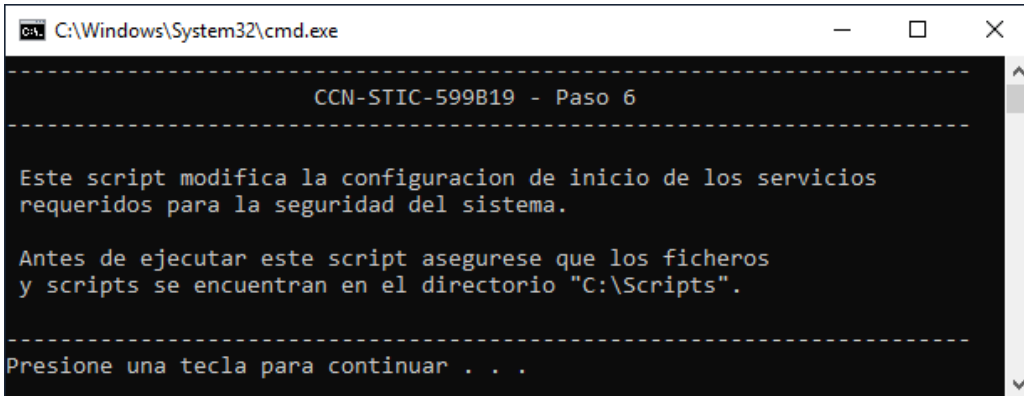
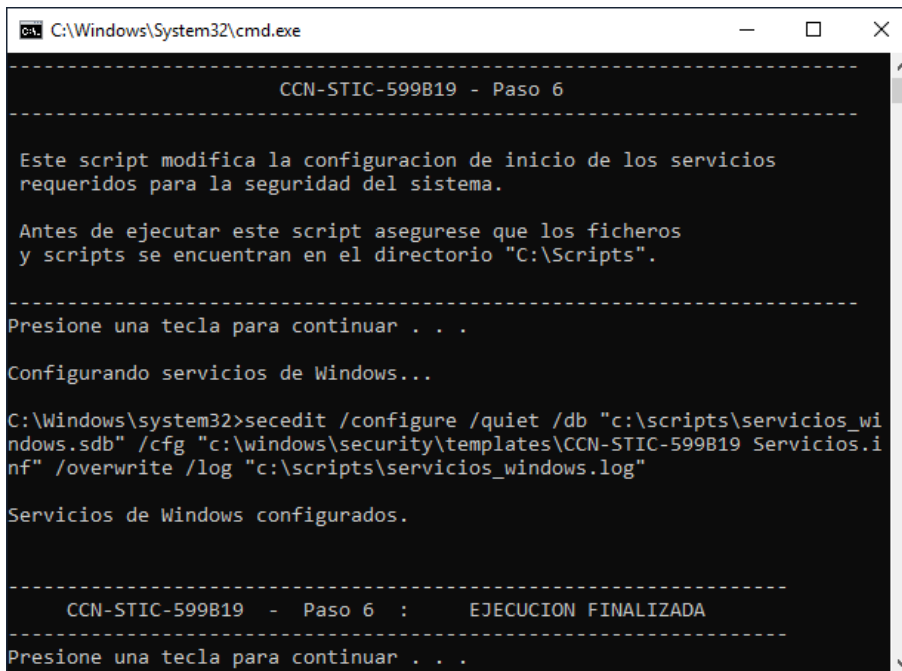
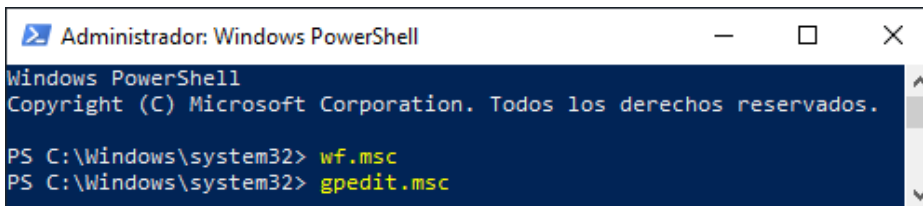
Paso	Descripción
7.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del cliente independiente: - CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.bat - CCN-STIC-599B19 Cliente Independiente - Habilita comprobaciones.ps1
8.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599B19 Cliente Independiente – Habilita comprobaciones.bat" desde el directorio "C:\Scripts".  Nota: El sistema le solicitará elevación de privilegios.
9.	Tras introducir las credenciales de un usuario con permisos de administrador, aparecerá la siguiente ventana. Pulse una tecla para continuar. 
10.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: En caso de que el sistema muestre errores puede ignorarlos. A partir de este momento, las consolas y características de administración bloqueadas por la presente guía vuelven a ser operativas de forma temporal.

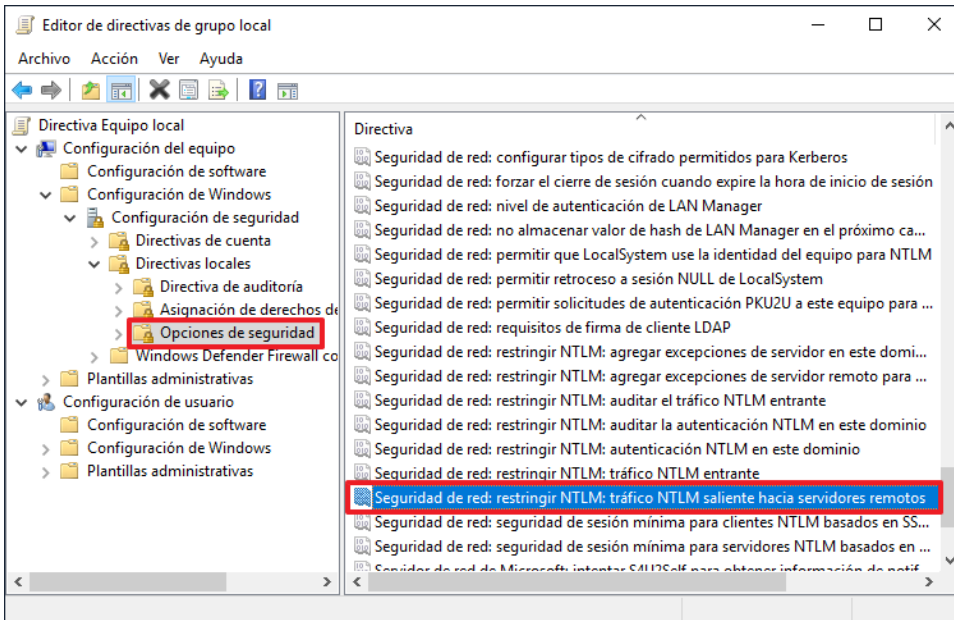
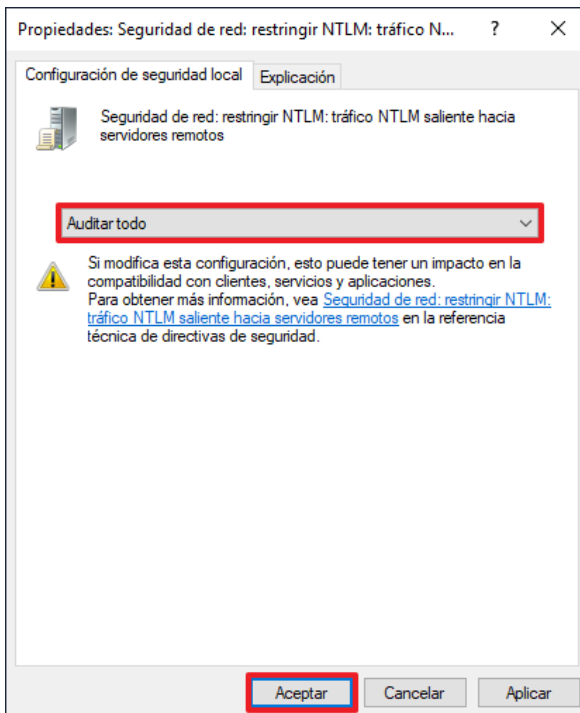
Paso	Descripción
11.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”. 
12.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador local.
13.	Introduzca el comando “wf.msc” para abrir la consola de administración de Firewall. 
14.	En la consola abierta del administrador de Firewall vaya a “Reglas de salida” y pulse botón derecho sobre el mismo y seleccione la opción “Nueva regla...”.  Nota: Utilice el asistente personalizado para crear una regla que permita la conexión a la dirección IP en la cual se encuentra el recurso al que desea conectarse.
15.	Una vez creada las reglas necesarias cierre la consola del Firewall.
16.	Desde el explorador de archivos, sitúese en la ruta “C:\Scripts”.

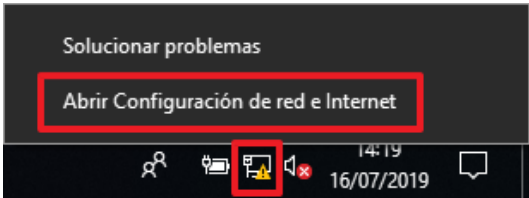
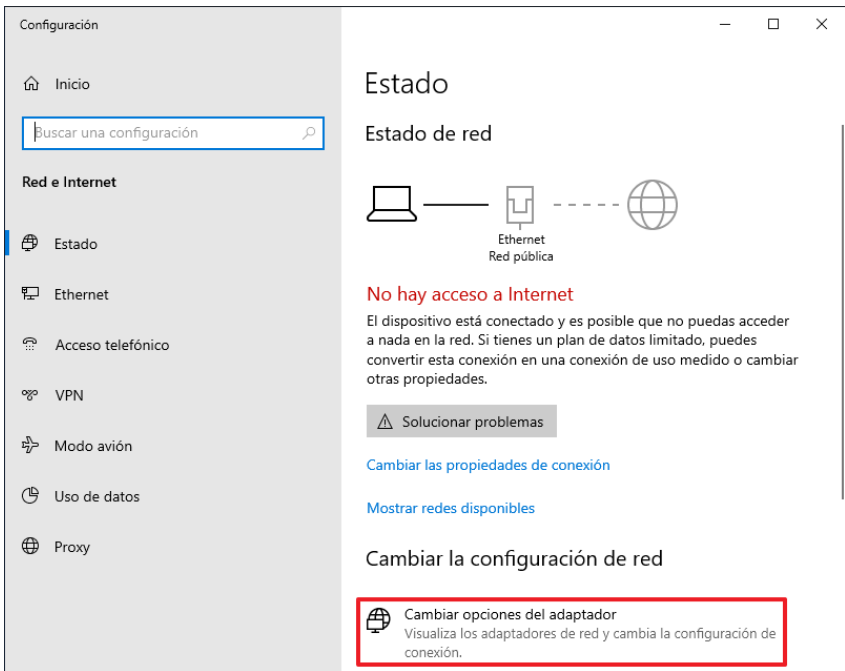
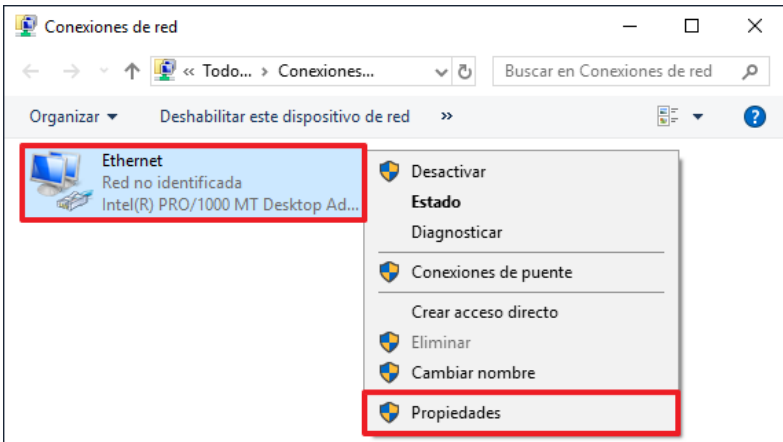
Paso	Descripción
17.	Pulse con el botón derecho del ratón sobre el fichero “Plantillas de seguridad.msc” y seleccione la opción “Ejecutar como administrador”.  Nota: El sistema le solicitará elevación de privilegios, introduzca las credenciales de un usuario con privilegios de administración sobre el puesto de trabajo.
18.	En la consola pulse con el botón derecho del ratón sobre plantillas de seguridad y seleccione la opción “Nueva ruta de acceso de búsqueda de plantillas...”. 
19.	En la ruta abierta seleccione “C:\Windows\Security\Templates”.
20.	Despliegue la plantilla “CCN-STIC-599B19 Servicios” y dentro de ella vaya a “Servicios del sistema”. 

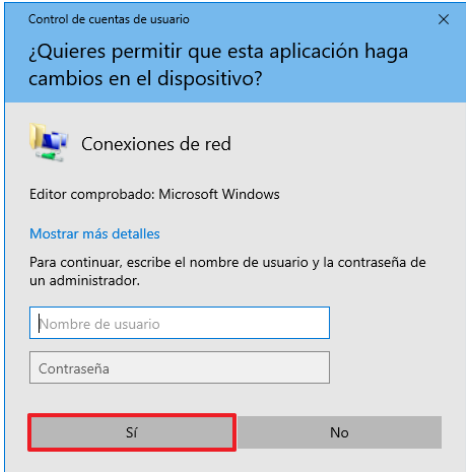
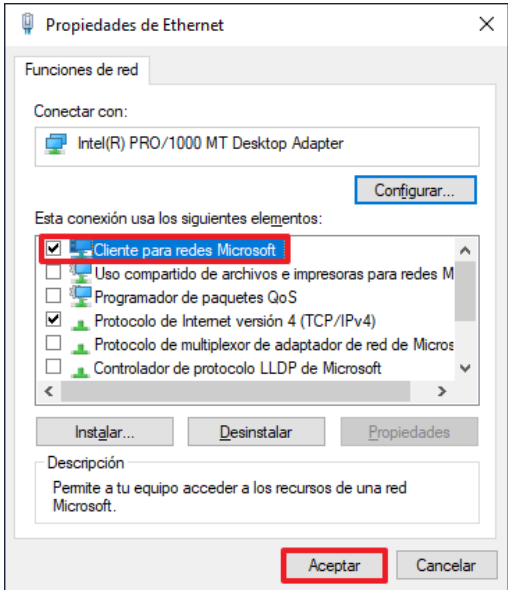
Paso	Descripción
21.	Pulse con el botón derecho del ratón sobre el servicio “Aplicación auxiliar de NetBIOS sobre TCP/IP” y seleccione la opción “Propiedades”. 
22.	En la nueva ventana abierta compruebe que el servicio se encuentra configurado en modo automático y pulse el botón “Modificar seguridad...” 
23.	En la nueva ventana abierta compruebe que el grupo de Administradores tiene el permiso concedido de “Control Total”. Asigne el permiso de “Control total” al usuario SYSTEM e INTERACTIVE. 

Paso	Descripción
24.	Pulse el botón “Aceptar” para guardar los cambios de los permisos.
25.	A la advertencia de seguridad que le aparecerá, pulse el botón “Sí” para continuar. 
26.	Guarde la plantilla ("C:\Windows\Security\Templates\CCN-STIC-599B19 Servicios.inf") con las modificaciones realizadas. Para ello utilice la opción "Guardar" del menú contextual que aparece al marcar con el botón derecho del ratón el nombre de la plantilla, como se muestra en la figura. 
27.	Cierre la consola de edición de plantillas. A la pregunta que aparecerá al cerrarla, "¿Guardar la configuración de la consola en Plantillas de seguridad.msc?", es indiferente que responda “Sí” o “No”.
28.	A continuación, vaya nuevamente a la carpeta “C:\Scripts” y pulse con el botón derecho sobre el fichero “CCN-STIC-599B19 Cliente independiente – Paso 6 –Servicios.bat” y pulse sobre la opción del menú contextual “Ejecutar como Administrador”. 

Paso	Descripción
29.	Cuando se le solicite, introduzca credenciales de administrador.
30.	Pulse una tecla para iniciar el proceso de reconfiguración de los servicios del sistema. 
31.	Una vez completado el proceso de configuración de servicios, pulse una tecla para finalizar el proceso. 
32.	Sobre la consola de PowerShell que todavía se encuentra abierta, ejecute la siguiente sintaxis "gpedit.msc" para abrir la consola de políticas locales. 

Paso	Descripción
33.	En el editor de directivas de grupo local despliegue el nodo “Directivas de equipo local → Configuración del equipo → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”. Seleccione con doble clic la directiva “Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos”. 
34.	Cambie la configuración existente por la opción “Auditar todo”. Pulse el botón “Aceptar” para guarda el nuevo valor de configuración. 
35.	Cierre la consola del Editor de Directivas de grupo.

Paso	Descripción
36.	A continuación, en la barra de tareas, localice el icono de conexiones de red y pulsando con el botón derecho del ratón sobre él seleccione “Abrir Configuración de red e Internet”. 
37.	En el menú de configuración, seleccione la opción “Cambiar opciones del adaptador”. 
38.	Pulse con el botón derecho sobre el adaptador de red y seleccione “Propiedades”. 

Paso	Descripción
39.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores”. 
40.	En la ventana de Propiedades de las diferentes conexiones de red, además del "Protocolo de Internet versión 4 (TCP/IPv4)" (ya marcado durante la aplicación de la guía) marque también el elemento “Cliente para redes Microsoft”. Pulse el botón “Aceptar” para guardar los cambios. 
41.	Ya habrá completado de realizar todos los cambios necesarios para realizar la conexión. Para finalizar borre el directorio “C:\Scripts” y reinicie el equipo para hacer efectiva la configuración, especialmente de los servicios.
42.	Una vez iniciada la sesión podrá conectarse a un recurso compartido remoto. Nota: Recuerde que si el cliente se comunica con un servidor existente en un dominio securizado con la guía CCN-STIC-570A el sistema remoto rechazará la conexión NTLM. Deberá crear una política incremental para dicho servidor, con objeto de permitir conexiones y autenticaciones remotas NTLM. Configure el sistema para permitir exclusivamente NTLMv2, rechazando LM y NTLM.

ANEXO D.3.7. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN

Tras la securización del sistema, existirían todavía determinados vectores de ataque, que deberán ser corregidos con el fin de evitar la evasión de los sistemas de autorización del sistema operativo. La exploración de dichos vectores de ataque podría ocasionar una posible exfiltración de la información gestionada y almacenada en el sistema, así como una potencial manipulación del comportamiento del mismo.

Para evitar esta situación, dentro del marco de seguridad establecido, se disponen de cuatro soluciones que se relaciona a continuación, y que pueden aplicarse de forma independiente o en conjunción las unas con las otras. Con posterioridad se detallará los mecanismos de su aplicación dentro del presente anexo, con objeto de mejorar la seguridad global del sistema.

Nota: Antes de aplicar las soluciones que se indican a continuación, verifique la compatibilidad de las mismas con su organización, y tenga en consideración los riesgos asumidos por la aplicación de dichas medidas.

Se recomienda verificar la adecuación e idoneidad de la solución para la organización en un entorno de pruebas o “preproducción” de forma previa a su aplicación en un entorno real o de “producción”.

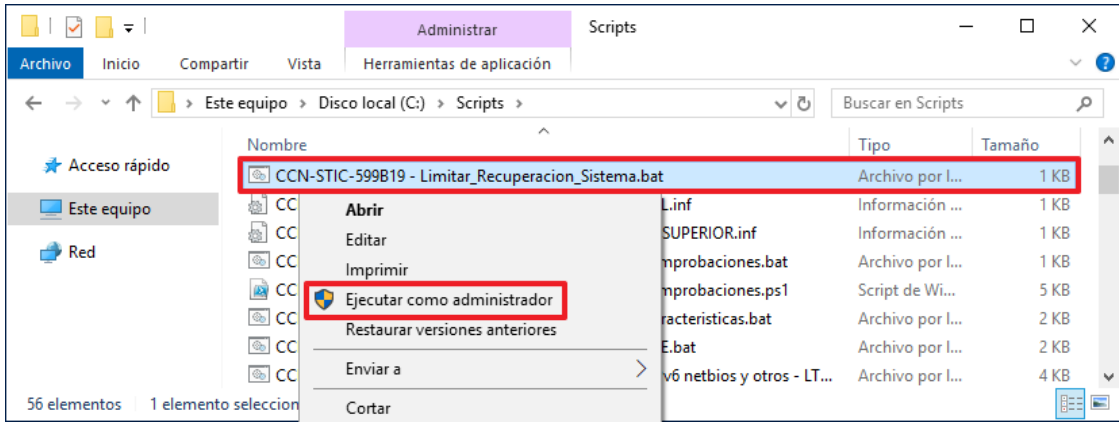
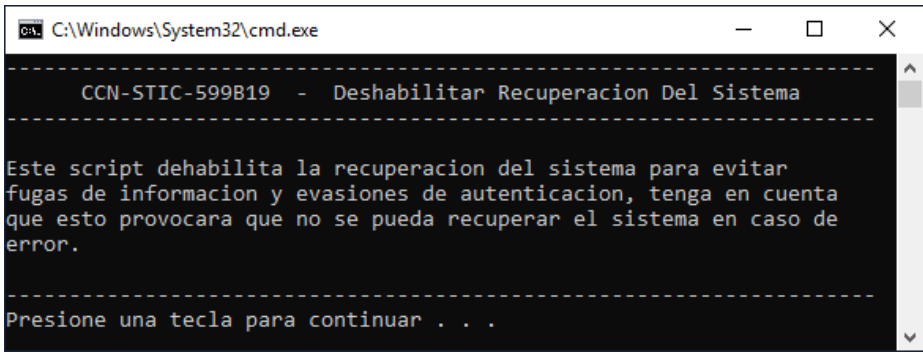
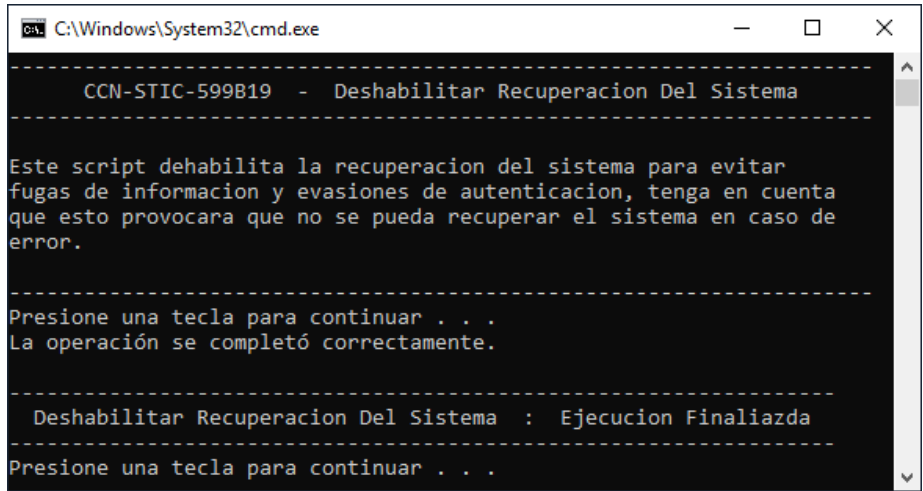
Las medidas a aplicar podrán ser:

- a) Cifrado del sistema de archivos. Utilizar BitLocker u otro sistema de cifrado autorizado para evitar el acceso a la información almacenada y, por tanto, evitar su modificación ya que requiere de la introducción de un PIN o contraseña en el arranque del equipo, o en el momento de acceder a los datos. De las opciones presentadas, ésta es la más recomendada. El presente anexo no incorpora cómo aplicar el mecanismo de protección de Bitlocker ya que ha sido convenientemente tratado en la presente guía.
- b) Deshabilitar la funcionalidad de restauración y/o recuperación del sistema a través de la utilidad “BCEDIT”.
- c) Deshabilitar las opciones de accesibilidad a través de claves de registro, evitando así que estas estén disponibles tanto si el usuario ha iniciado sesión como si no.
- d) Restaurar la integridad de los ficheros “C:\Windows\System32\sethc.exe” y “C:\Windows\System32\utilman.exe” al inicio del sistema.

1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

A continuación, se indican los pasos a realizar para deshabilitar la funcionalidad de recuperación del sistema.

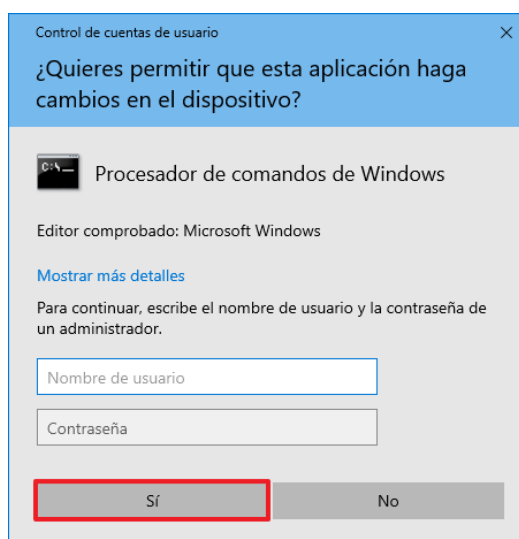
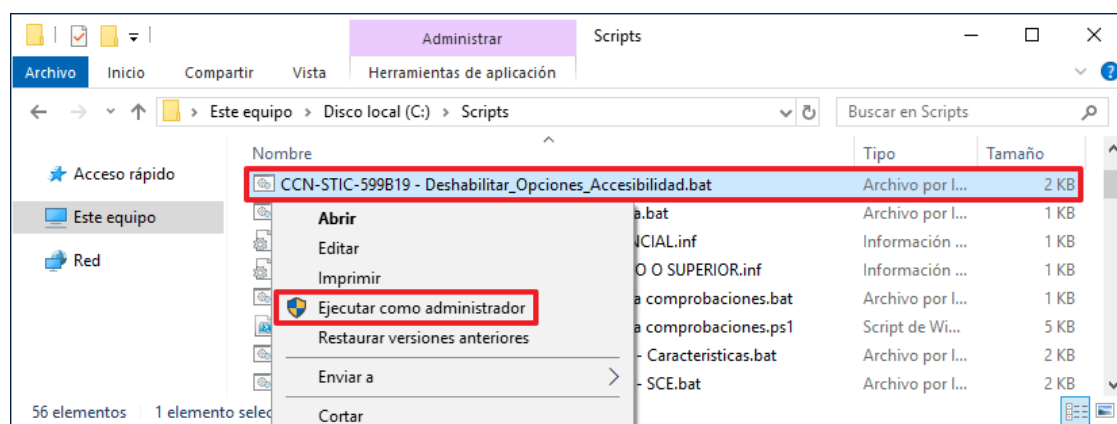
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.

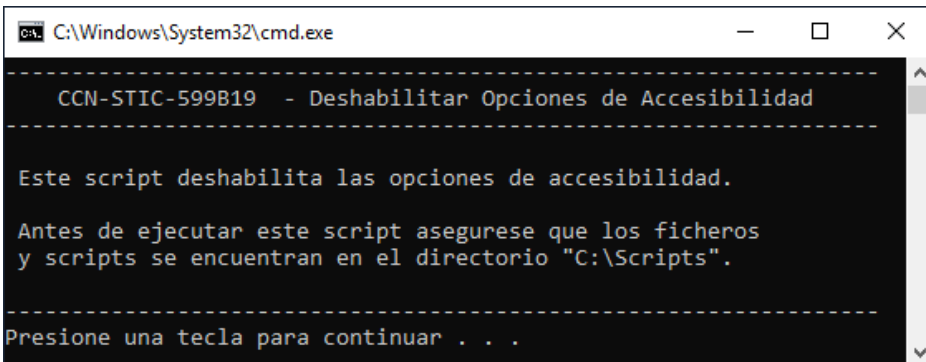
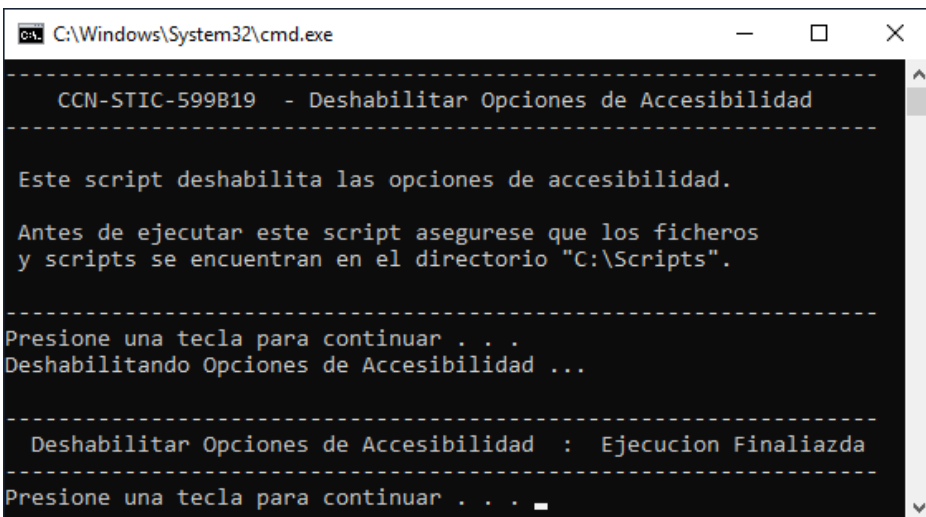
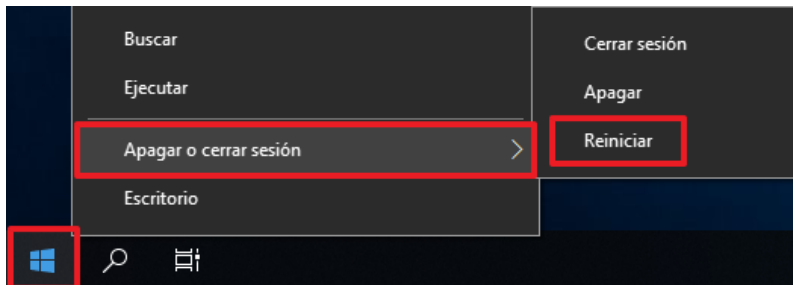
Paso	Descripción
3.	Localice el archivo “CCN-STIC-599B19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”. 
4.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores”.
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script limitará el uso de las opciones de recuperación del sistema. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana. 
7.	Elimine el directorio “C:\Scripts”.

2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD

A continuación, se indican los pasos a realizar para deshabilitar las opciones de accesibilidad.

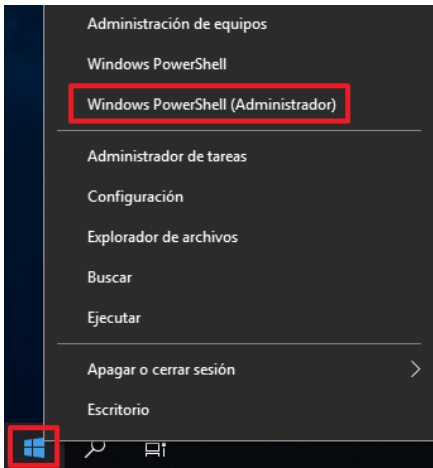
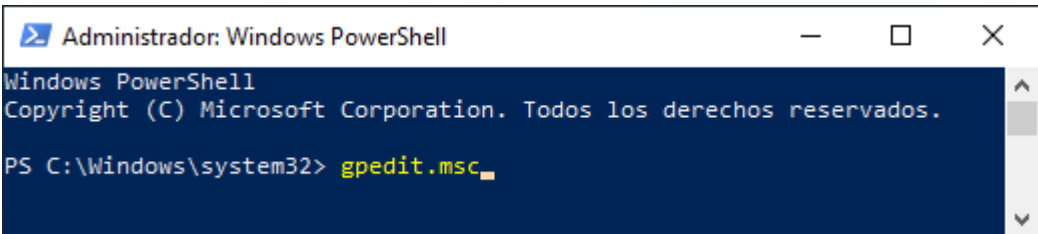
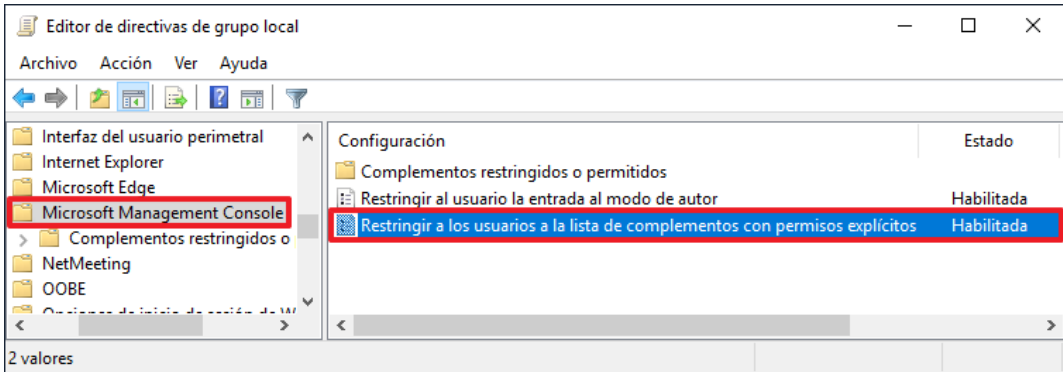
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador local.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
3.	Localice el archivo “CCN-STIC-599B19 – Deshabilitar_Opciones_Accesibilidad.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.
4.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente al grupo local “Administradores”.

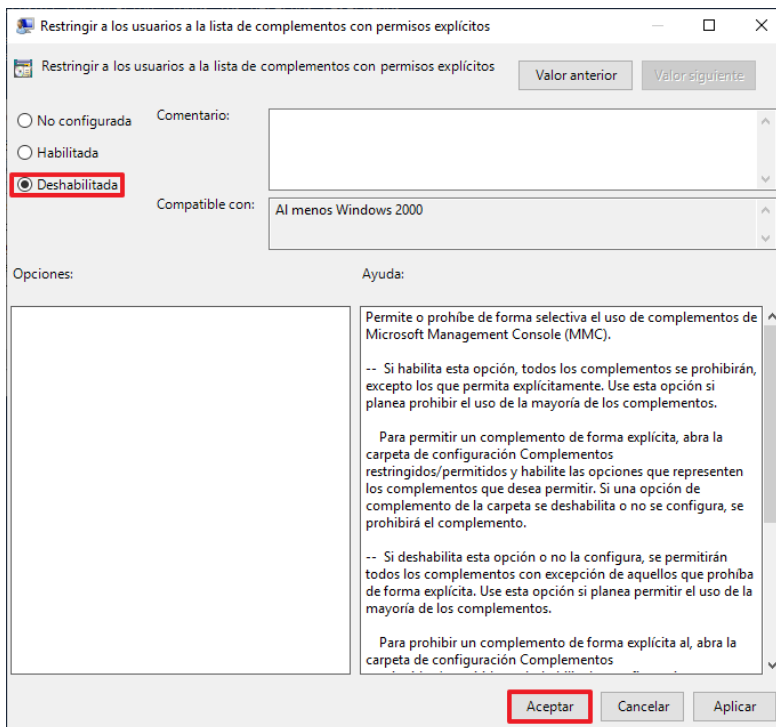
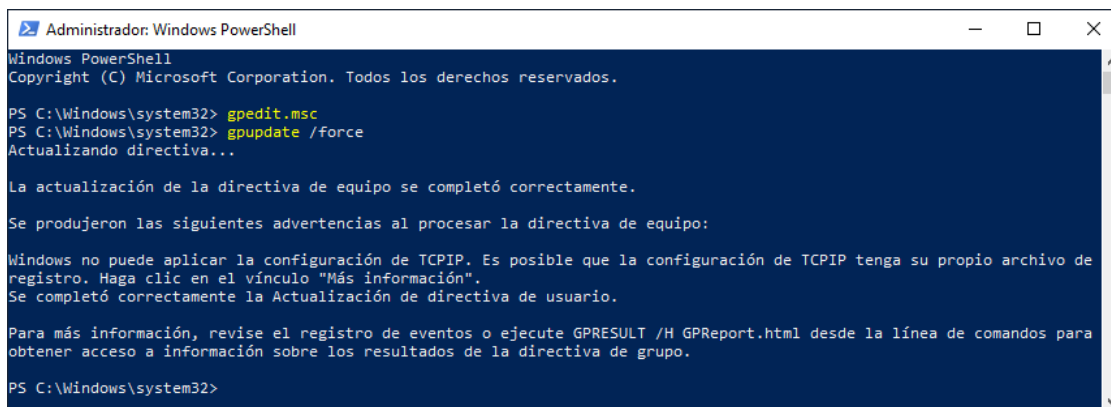
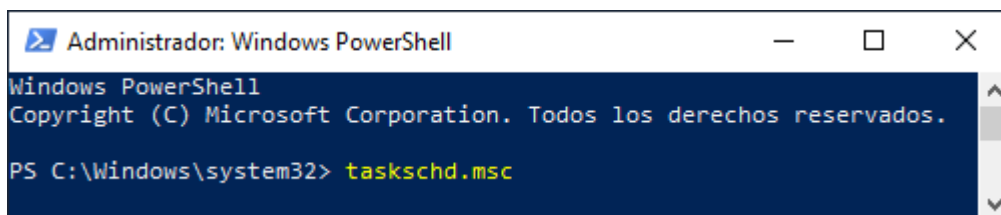


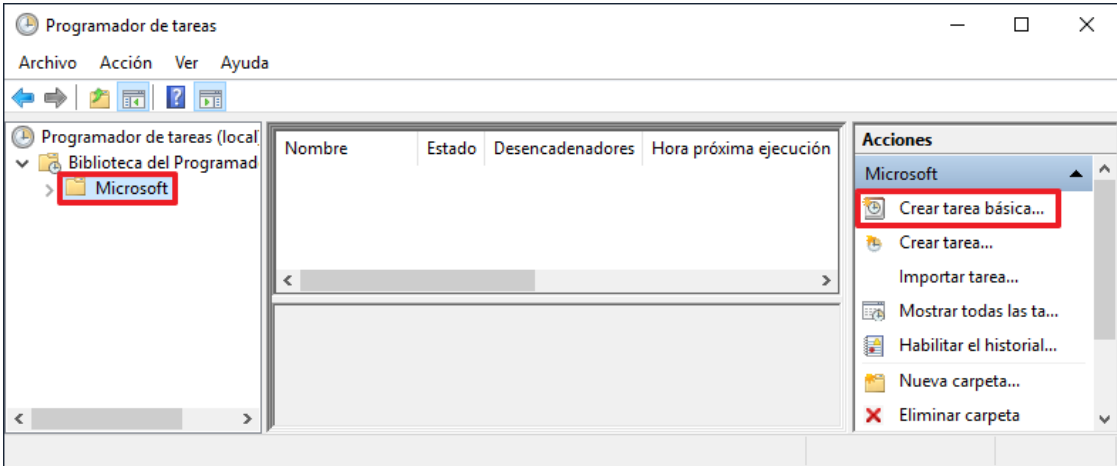
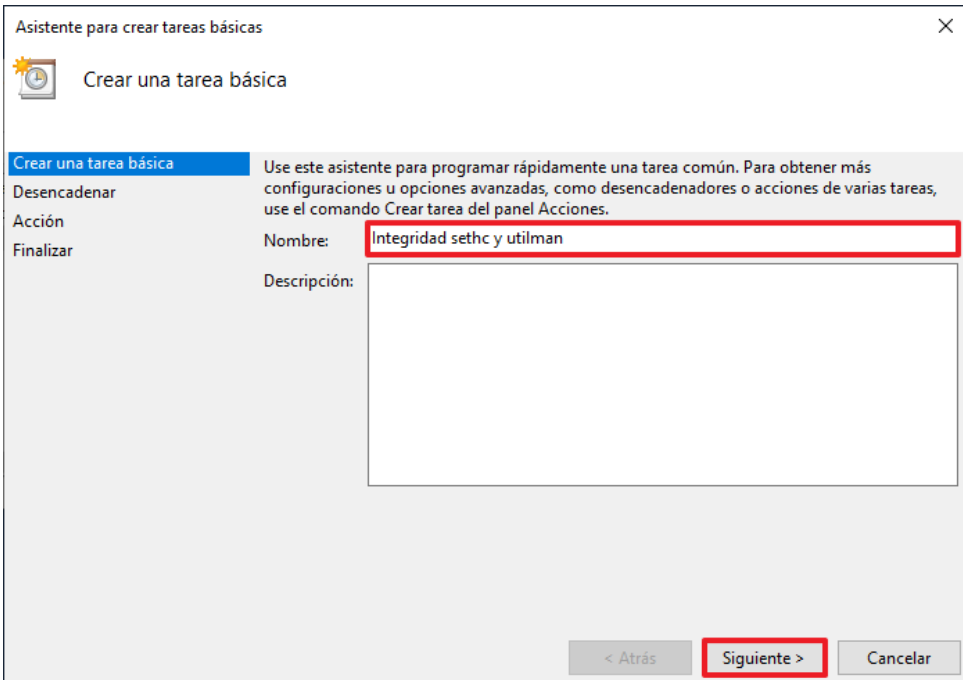
Paso	Descripción
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 
7.	Por último, deberá reiniciar el sistema para que los cambios sean aplicados. Para ello haga clic derecho en el botón “Inicio” y seleccione “Apagar o cerrar sesión → Reiniciar”. 
8.	Elimine el directorio “C:\Scripts”.

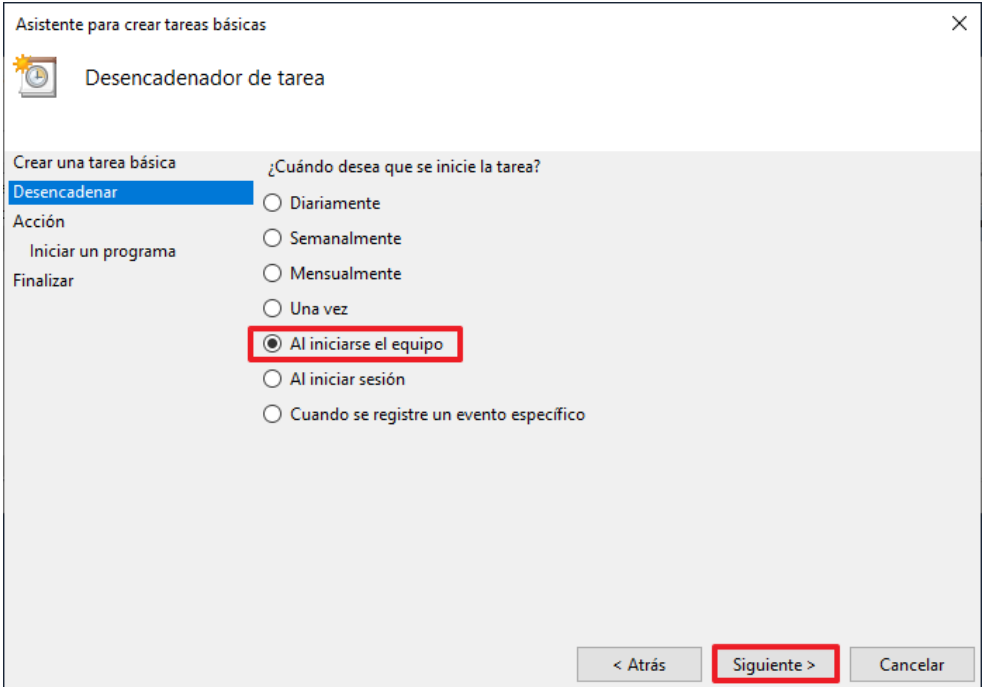
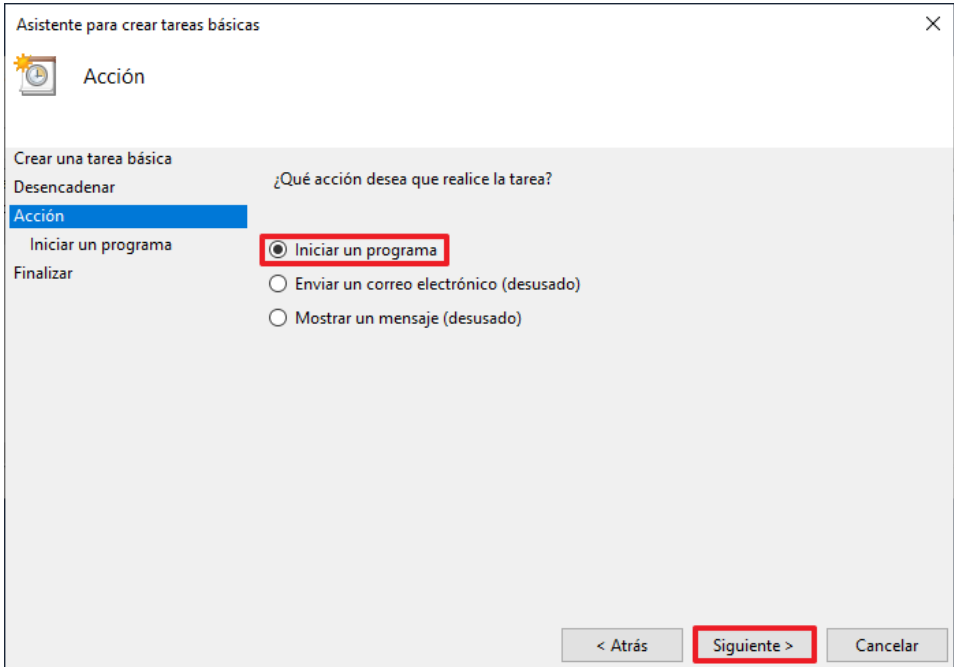
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

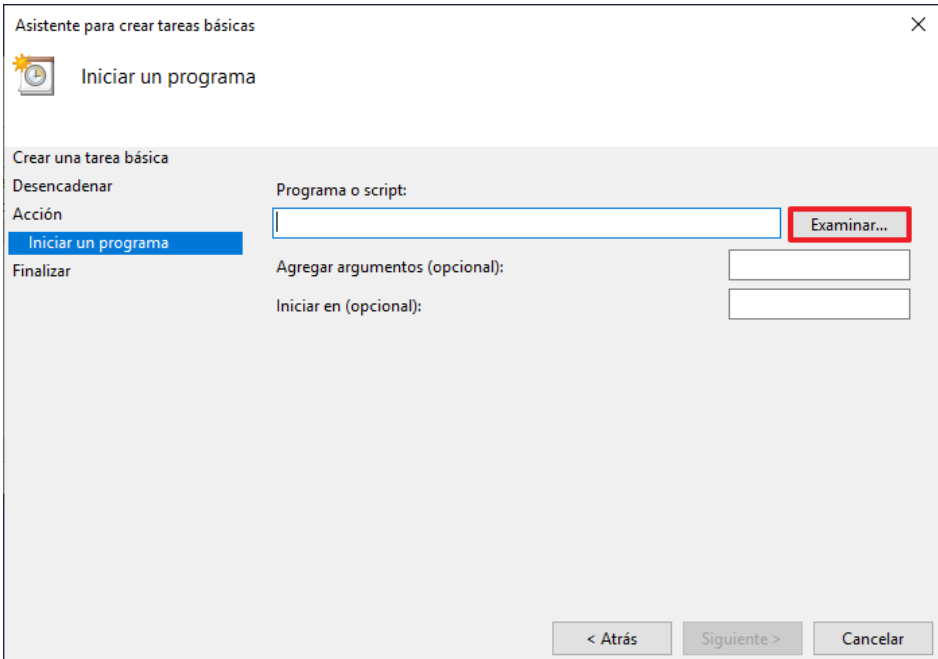
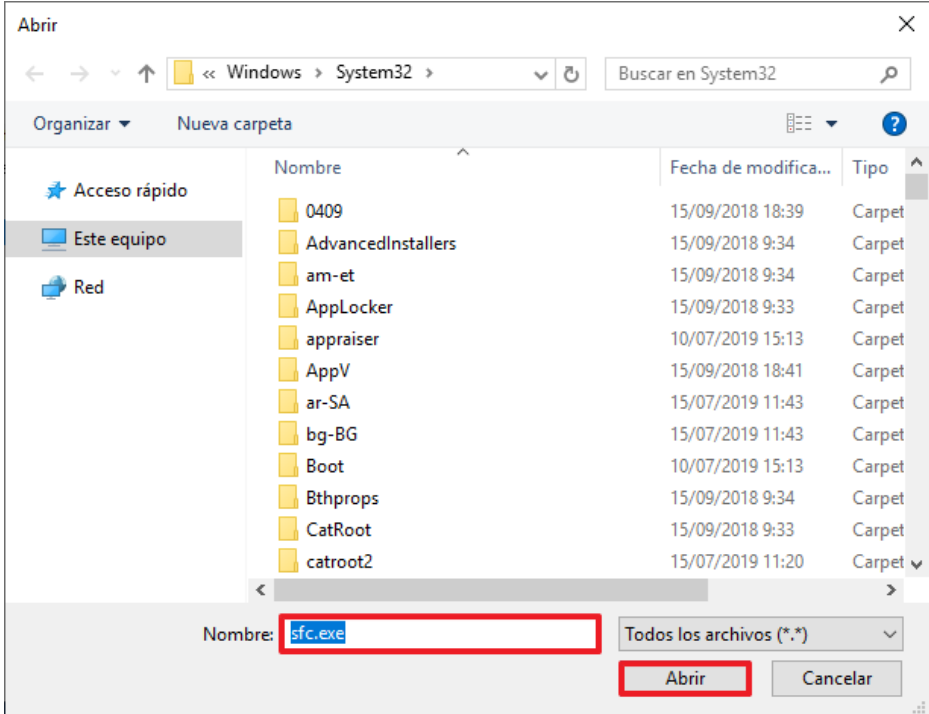
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

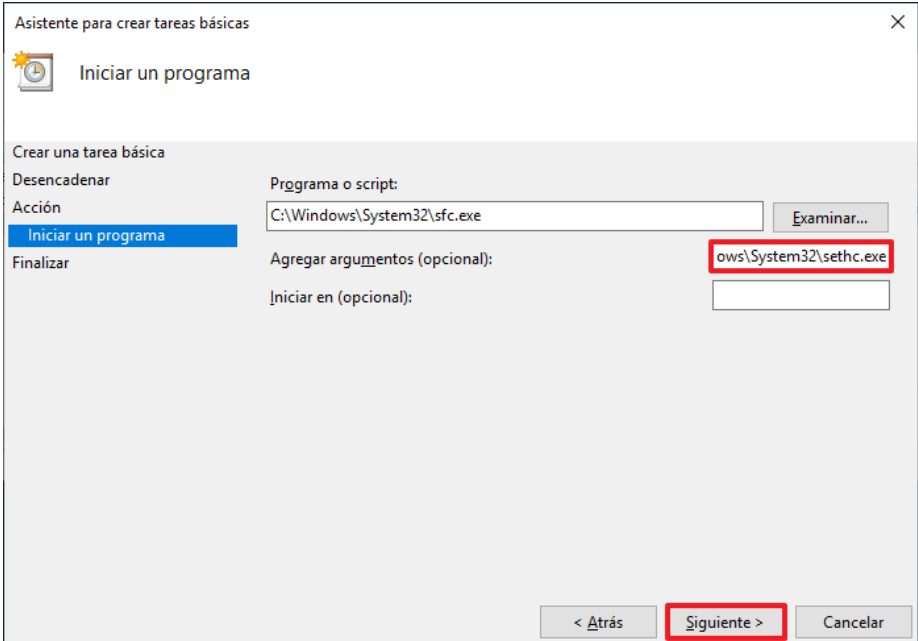
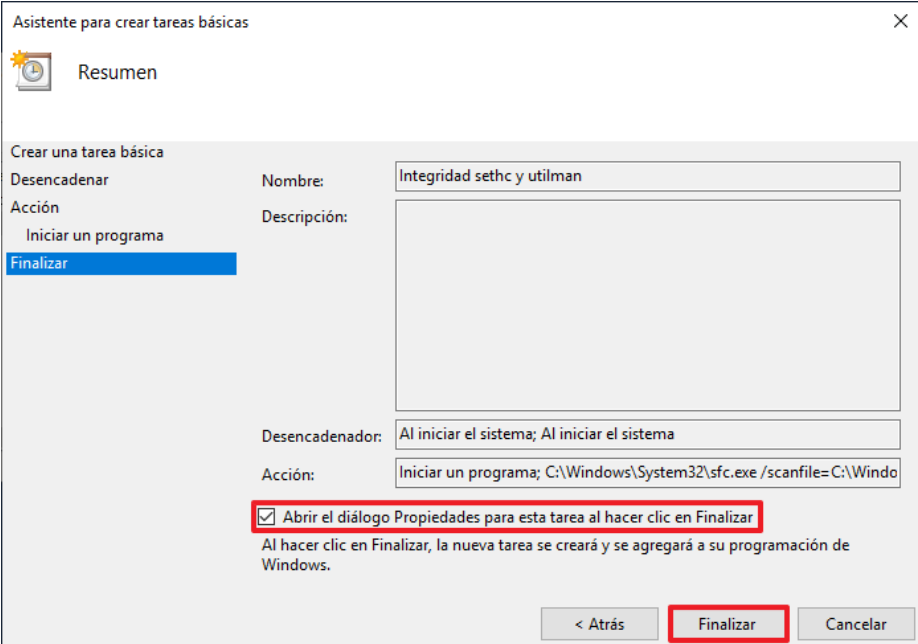
Paso	Descripción
1.	Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”.  Nota: El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.
2.	Una vez en la consola de PowerShell ejecute el comando “gpedit.msc” para iniciar el editor de directivas de grupo local. 
3.	En el editor de grupo local, sitúese en “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console” y localice la directiva “Restringir a los usuarios a la lista de complementos con permisos explícitos”. 

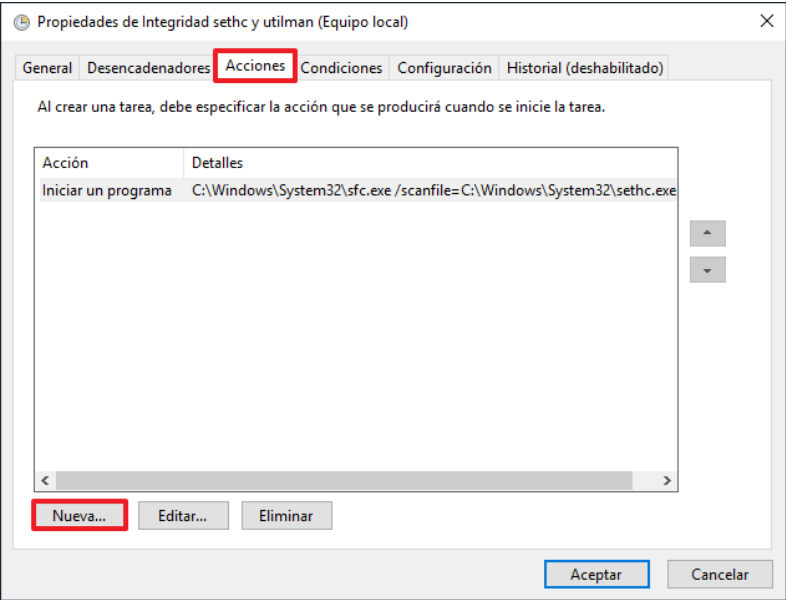
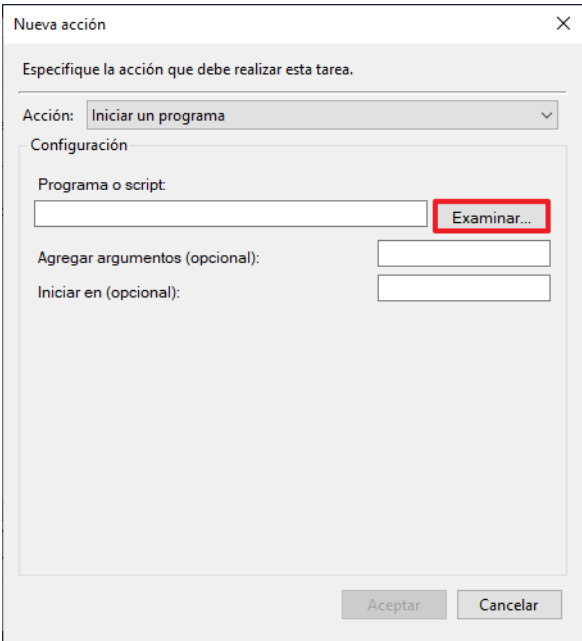
Paso	Descripción
4.	Edite la directiva “Restringir a los usuarios a la lista de complementos con permisos explícitos”, cambie su valor por “Deshabilitada” y haga clic en aceptar.  Nota: No cierre el Editor de directivas de grupo local hasta que se indique lo contrario.
5.	Vuelva a la consola de PowerShell y ejecute el comando “gpupdate /force” para actualizar la configuración de las directivas de grupo. 
6.	Ejecute el comando “taskschd.msc” en la misma consola de PowerShell para abrir el “Programador de tareas”. 

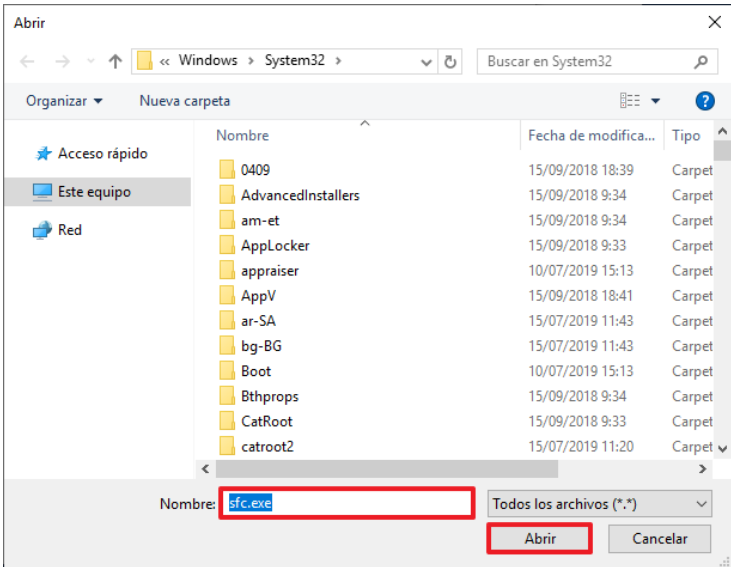
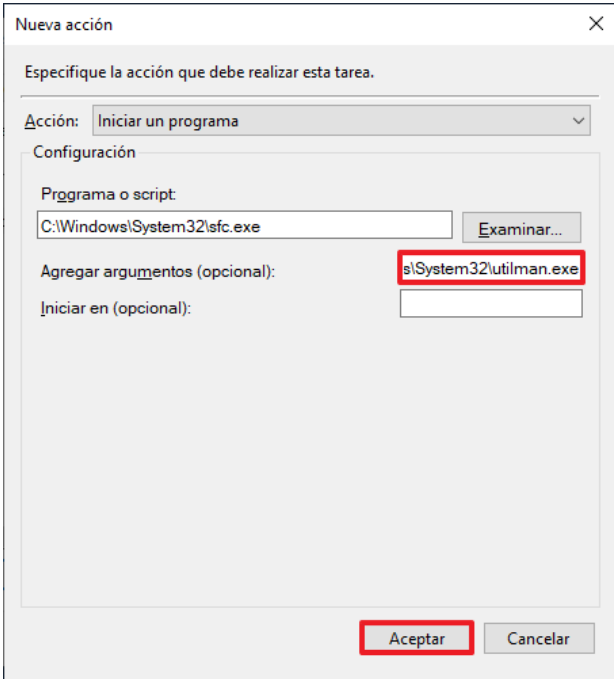
Paso	Descripción
7.	En el programador de tareas sitúese en la ruta “Biblioteca del Programador de tareas → Microsoft”. En el panel de “Acciones” situado en la parte derecha seleccione “Crear tarea básica”. 
8.	Se abrirá un asistente para la creación de la tarea programada. En la primera pestaña, indique el nombre de la tarea y pulse el botón “Siguiente >”.  Nota: En este caso el nombre designado para la tarea es “Integridad sethc y utilman”

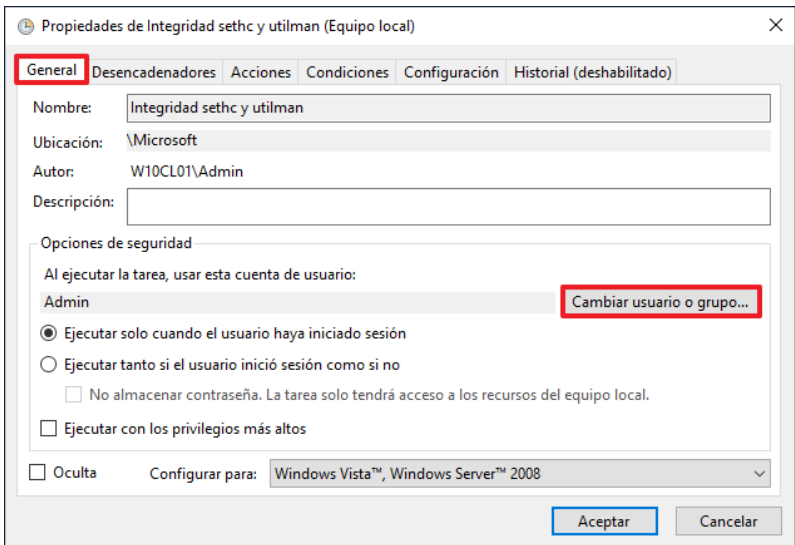
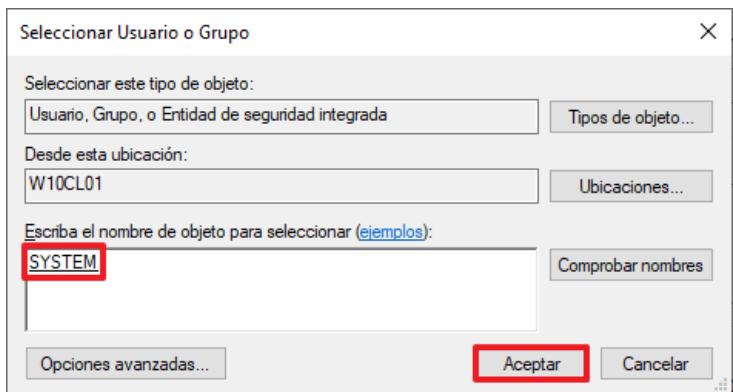
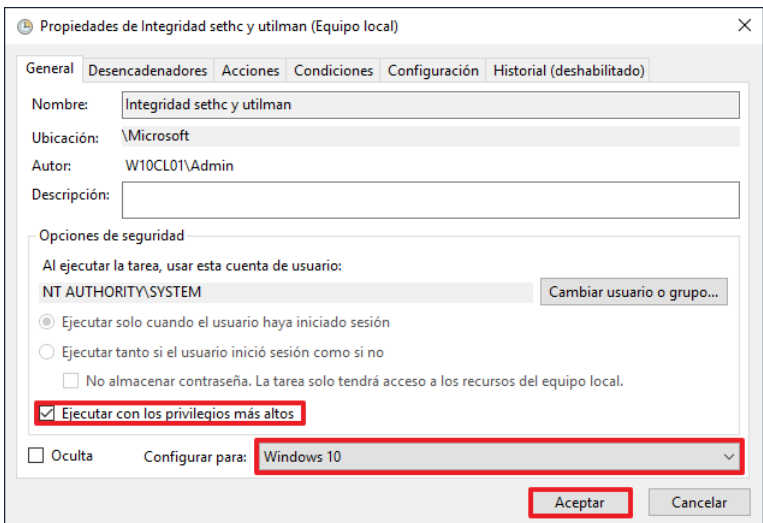
Paso	Descripción
9.	En la ventana “Desencadenar” del asistente seleccione “Al iniciarse el equipo” y pulse sobre el botón “Siguiente >”. 
10.	En la ventana “Acción” del asistente seleccione “Iniciar un programa” y haga clic sobre el botón “Siguiente >”. 

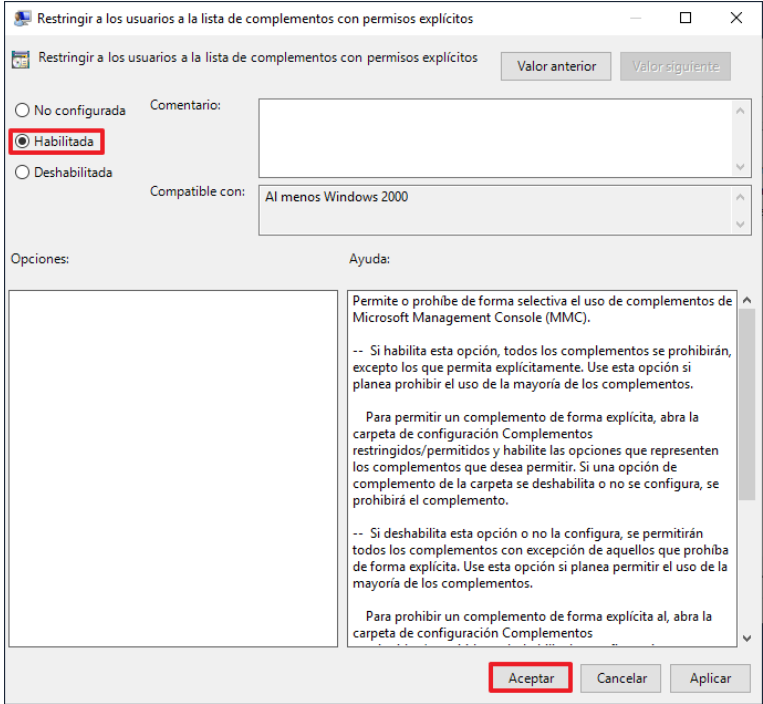
Paso	Descripción
11.	Haga clic sobre el botón “Examinar” para indicar que programa se ejecutará. 
12.	En la ventana emergente acceda a la ruta “C:\Windows\System32”, escriba en el apartado “Nombre” “sfc.exe” y haga clic sobre el botón “Abrir”. 

Paso	Descripción
13.	En el apartado “Agregar argumentos (opcional)” escriba “/scanfile=C:\Windows\System32\sethc.exe” para indicar al programa “sfc” que verifique la integridad del fichero “sethc.exe” situado en “C:\Windows\System32” y haga clic sobre el botón “Siguiente >”. 
14.	En la última ventana (Finalizar), marque la opción “Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar” y haga clic en “Finalizar”. 

Paso	Descripción
15.	Al hacer clic en “Finalizar”, se abrirá el diálogo de propiedades de la tarea, sitúese en la pestaña de “Acciones” y haga clic en “Nueva...”. 
16.	Se abrirá una ventana con la nueva acción a indicar, pulse sobre el botón “Examinar...”. 

Paso	Descripción
17.	En la ventana emergente acceda a la ruta "C:\Windows\System32", escriba en el apartado "Nombre:" "sfc.exe" y haga clic sobre el botón "Abrir". 
18.	En el apartado "Agregar argumentos (opcional)" escriba "/scanfile=C:\Windows\System32\utilman.exe" para indicarle al programa sfc que verifique la integridad del fichero utilman.exe situado en "C:\Windows\System32" y haga clic sobre el botón "Aceptar".  Nota: Si su sistema operativo es de 64 bits, repita el proceso del paso 15 al 18 con los ficheros "C:\Windows\SysWOW64\sethc.exe" y "C:\Windows\SysWOW64\utilman.exe".

Paso	Descripción
19.	A continuación, en la pestaña “General” del dialogo de propiedades de la tarea programada, haga clic en el botón “Cambiar usuario o grupo...”. 
20.	En la ventana emergente, introduzca el nombre “SYSTEM” y pulse aceptar. 
21.	Por último, marque la opción de “Ejecutar con los privilegios más altos”, establezca la opción “Windows 10” del desplegable “Configurar para:” y pulse en “Aceptar”. 

Paso	Descripción
22.	Cierre el programador de tareas.
23.	Vuelva al editor de directivas de grupo y edite la directiva “Restringir a los usuarios a la lista de complementos con permisos explícitos” situada en la ruta “Configuración de usuario → Plantillas administrativas → Componentes de Windows → Microsoft Management Console”, cambie su valor por “Habilitada” y haga clic en “Aceptar”. 
24.	Cierre el editor de directivas de grupo.