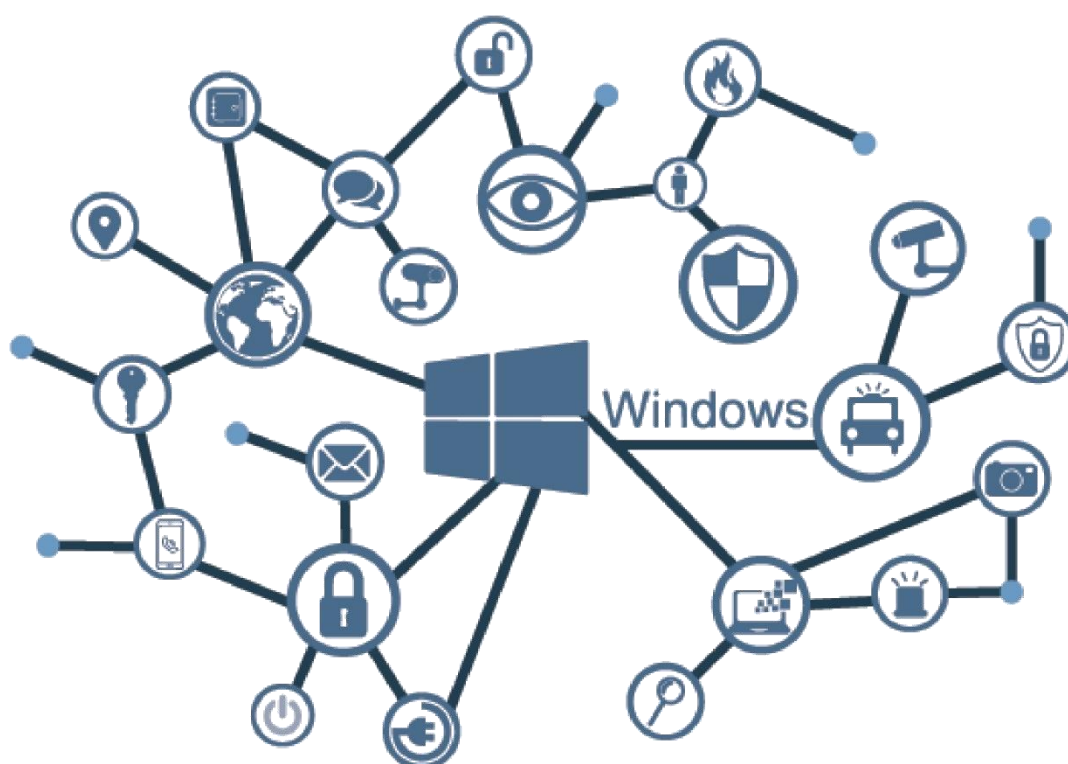


Guía de Seguridad de las TIC CCN-STIC 599A19

IMPLEMENTACIÓN DE SEGURIDAD SOBRE MICROSOFT WINDOWS 10 (1809) (CLIENTE MIEMBRO DE DOMINIO)



SEPTIEMBRE 2019



Edita:



© Centro Criptológico Nacional, 2019

NIPO: 083-19-234-7

Fecha de Edición: septiembre de 2019



2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

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).

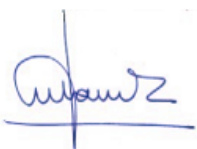
Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad 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 MIEMBRO DE DOMINIO	11
ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE MS WINDOWS 10 EN EL ENS	12
1. APLICACIÓN DE MEDIDAS EN MICROSOFT WINDOWS 10	12
1.1. MARCO OPERACIONAL	13
1.1.1. CONTROL DE ACCESO	13
1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN	13
1.1.1.2. OP. ACC. 2. REQUISITOS DE ACCESO	14
1.1.1.3. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS	15
1.1.1.4. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO	15
1.1.1.5. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN	16
1.1.1.6. OP. ACC. 6. ACCESO LOCAL	17
1.1.1.7. OP. ACC. 7. ACCESO REMOTO	18
1.1.2. EXPLOTACIÓN	18
1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD	18
1.1.2.2. OP. EXP. 4. MANTENIMIENTO	19
1.1.2.3. OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO	21
1.1.2.4. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS	21
1.1.2.5. OP. EXP. 10. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD	22
1.2. MEDIDAS DE PROTECCIÓN	22
1.2.1. PROTECCIÓN DE LOS EQUIPOS	22
1.2.1.1. MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO	23
1.2.1.2. MP. EQ. 3. PROTECCIÓN DE LOS PORTÁTILES	23
1.2.2. PROTECCIÓN DE LAS COMUNICACIONES	23
1.2.2.1. MP. COM. 3. PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD	24
1.2.3. PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS	24
1.2.3.1. MP. INFO. 3. CIFRADO	24
2. RESUMEN Y APLICACIÓN DE MEDIDAS EN MICROSOFT WINDOWS 10	25
ANEXO A.2. CATEGORÍA BÁSICA	28
ANEXO A.2.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS	28
1. PREPARACIÓN DEL DOMINIO	28
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA BÁSICA	48
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO	48
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD	50
4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE CONFIGURACIONES DE SEGURIDAD ..	54
4.1. CONTROL DE CUENTAS DE USUARIO	54

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA BÁSICA.....	57
ANEXO A.3. CATEGORÍA MEDIA	94
ANEXO A.3.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS	94
1. PREPARACIÓN DEL DOMINIO.....	94
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA MEDIA.....	113
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO.....	113
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD.....	115
4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD	119
4.1. CONTROL DE CUENTAS DE USUARIO	119
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA MEDIA	122
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA.....	166
ANEXO A.4.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	166
1. PREPARACIÓN DEL DOMINIO.....	166
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA	186
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO.....	186
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD.....	188
4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD	192
4.1. CONTROL DE CUENTAS USUARIO	192
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA	195
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.....	239
1. PREPARACIÓN DE DOMINIO	241
2. CONFIGURACIÓN DE BITLOCKER EN EL PUESTO CLIENTE.....	256
ANEXO A.5. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	264
ANEXO A.5.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA	264
1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO.....	264
2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CORTAFUEGOS	269
ANEXO A.5.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA MS WINDOWS 10	284

1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO	284
1.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO	284
1.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CONFIGURACIÓN DEL VALOR DE TELEMETRÍA	288
2. INFORMACIÓN ACERCA DEL ÚLTIMO INICIO DE SESIÓN	295
2.1. CREACIÓN DE TAREA PROGRAMADA	295
2.2. DELEGACIÓN DE PERMISOS DE ESCRITURA SOBRE ATRIBUTO DE USUARIO	305
2.3. CONFIGURACIÓN DE SCRIPTS PARA MOSTRAR LA INFORMACIÓN DE INICIO DE SESIÓN ..	311
3. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	313
3.1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	313
3.2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	315
3.3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	316
ANEXO B. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN REDES CLASIFICADAS COMO CLIENTE MIEMBRO DE DOMINIO	323
ANEXO B.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 ENTERPRISE LTSC COMO CLIENTE MIEMBRO DE DOMINIO	325
ANEXO B.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA	325
1. PREPARACIÓN DEL DOMINIO.....	326
2. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10	362
3. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10	378
ANEXO B.1.2. LISTA DE COMPROBACIÓN PASO A PASO	392
1. COMPROBACIONES EN SERVIDOR CONTROLADOR DEL DOMINIO	393
2. COMPROBACIONES EN EQUIPO CLIENTE WINDOWS 10 ENTERPRISE LTSC	496
ANEXO B.2. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	533
ANEXO B.2.1. CIFRADO DE DISCO CON BITLOCKER.....	533
1. ALCANCE	533
2. DESCRIPCIÓN DE USO DE ESTE ANEXO	534
3. REQUISITOS HARDWARE Y SOFTWARE.....	534
4. OBJETO DE DIRECTIVA DE GRUPO (GPO).....	534
4.1. SERVICIOS DEL SISTEMA	535
4.2. PLANTILLAS ADMINISTRATIVAS (EQUIPO)	536
5. GUIA PASO A PASO – BITLOCKER	537
6. LISTA DE COMPROBACIÓN – BITLOCKER	561
ANEXO B.2.2. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19	571
1. PREPARACIÓN DEL DIRECTORIO ACTIVO	571
2. ADMINISTRAR USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES	582
2.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB.....	582
2.2. DESINSTALACIÓN DE CONTROLADORES PARA IMPEDIR EL USO DE DISPOSITIVOS USB.....	591

3. ADMINISTRAR EL USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE EL IDENTIFICADOR DE DISPOSITIVO	594
3.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR.....	594
3.2. IMPEDIR EL USO DE DISPOSITIVOS USB.....	608
ANEXO B.2.3. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19	614
ANEXO B.2.4. CONFIGURACIÓN PARA USO DE NESSUS.....	617
1. HABILITAR AUTENTICACIÓN PARA USO DE NESSUS	617
2. PERMITIR COMUNICACIÓN EN EL FIREWALL.....	624
3. ELIMINACIÓN DE LA CONFIGURACIÓN PARA EL USO DE NESSUS	631
ANEXO B.2.5. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	632
1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	632
2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	634
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	636
ANEXO C. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN EL ENS COMO MIEMBRO DE DOMINIO	644
ANEXO C.1. CATEGORÍA BÁSICA.....	645
ANEXO C.1.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS.....	645
1. PREPARACIÓN DEL DOMINIO.....	645
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA BÁSICA	664
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO.....	665
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD.....	667
4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD	670
4.1. CONTROL DE CUENTAS DE USUARIO	670
ANEXO C.1.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA BÁSICA.....	673
ANEXO C.2. CATEGORÍA MEDIA	710
ANEXO C.2.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS	710
1. PREPARACIÓN DEL DOMINIO.....	710
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA MEDIA.....	729
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO.....	729
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD.....	731
4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD	734
4.1. CONTROL DE CUENTAS DE USUARIO	735

ANEXO C.2.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA MEDIA	737
ANEXO C.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA.....	779
ANEXO C.3.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA.....	779
1. PREPARACIÓN DEL DOMINIO.....	779
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA	799
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO.....	799
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD.....	801
4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD	804
4.1. CONTROL DE CUENTAS USUARIO	804
ANEXO C.3.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA	807
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.....	850
1. PREPARACIÓN DE DOMINIO	851
2. CONFIGURACIÓN DE BITLOCKER EN EL PUESTO CLIENTE.....	865
ANEXO C.4. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	873
ANEXO C.4.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA	873
1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO.....	873
2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CORTAFUEGOS	878
ANEXO C.4.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA MS WINDOWS 10	893
1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO.....	893
1.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO	893
1.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CONFIGURACIÓN DEL VALOR DE TELEMETRÍA	897
2. CONFIGURACIÓN DE OPCIÓN DE MANTENIMIENTO PARA WINDOWS 10.....	903
2.1. CREACIÓN DE GRUPO PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO	904
2.2. CONFIGURACIÓN DE LA GPO DE MICROSOFT WINDOWS 10 PARA ESTABLECER LA OPCIÓN DE MANTENIMIENTO EN MODO RAMA SEMIANUAL PARA LOS EQUIPOS DE LA ORGANIZACIÓN	908
2.3. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA QUE CONFIGURE LA OPCIÓN DE MANTENIMIENTO EN MODO RAMA SEMIANUAL (DIRIGIDA) EN LOS EQUIPOS DE CONTROL.....	912
3. INFORMACIÓN ACERCA DEL ÚLTIMO INICIO DE SESIÓN	920
3.1. CREACIÓN DE TAREA PROGRAMADA	920

3.2. DELEGACIÓN DE PERMISOS DE ESCRITURA SOBRE ATRIBUTO DE USUARIO	930
3.3. CONFIGURACIÓN DE SCRIPTS PARA MOSTRAR LA INFORMACIÓN DE INICIO DE SESIÓN ..	937
4. DESINSTALACIÓN DE APPS (UWP) EN WINDOWS 10.....	939
4.1. IDENTIFICACIÓN DE APPX INSTALADAS	939
4.2. ELIMINACIÓN DE APPX PROVISIONADAS E INSTALADAS.....	940
5. ACTIVACIÓN DE TIENDA DE WINDOWS PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO	942
5.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO	942
5.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA QUE HABILITE EL SERVICIO DE TIENDA DE WINDOWS.....	946
6. ACTIVACIÓN DE MICROSOFT ONEDRIVE PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO	953
6.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO	953
6.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA QUE HABILITE ONEDRIVE DE MICROSOFT.....	957
7. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	963
7.1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	963
7.2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	965
7.3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	966
ANEXO D. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN REDES CLASIFICADAS COMO CLIENTE MIEMBRO DE DOMINIO	973
ANEXO D.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 PRO/ENTERPRISE COMO CLIENTE MIEMBRO DE DOMINIO	975
ANEXO D.1.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA	975
1. PREPARACIÓN DEL DOMINIO.....	976
2. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10	1012
3. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10	1029
ANEXO D.1.2. LISTA DE COMPROBACIÓN PASO A PASO.....	1043
1. COMPROBACIONES EN SERVIDOR CONTROLADOR DEL DOMINIO	1044
2. COMPROBACIONES EN EQUIPO CLIENTE WINDOWS 10 PRO/ENTERPRISE	1145
ANEXO D.2. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD	1182
ANEXO D.2.1. CIFRADO DE DISCO CON BITLOCKER.....	1182
1. ALCANCE	1182
2. DESCRIPCIÓN DE USO DE ESTE ANEXO	1183
3. REQUISITOS HARDWARE Y SOFTWARE.....	1183
4. OBJETO DE DIRECTIVA DE GRUPO (GPO).....	1183
4.1. SERVICIOS DEL SISTEMA	1184
4.2. PLANTILLAS ADMINISTRATIVAS (EQUIPO)	1185
5. GUIA PASO A PASO – BITLOCKER	1186
6. LISTA DE COMPROBACIÓN – BITLOCKER	1210

ANEXO D.2.2. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19	1220
1. PREPARACIÓN DEL DIRECTORIO ACTIVO	1220
2. ADMINISTRAR USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES	1231
2.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB.....	1231
2.2. DESINSTALACIÓN DE CONTROLADORES PARA IMPEDIR EL USO DE DISPOSITIVOS USB...	1240
3. ADMINISTRAR EL USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE EL IDENTIFICADOR DE DISPOSITIVO	1243
3.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR.....	1243
3.2. IMPEDIR EL USO DE DISPOSITIVOS USB	1257
ANEXO D.2.3. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19	1263
ANEXO D.2.4. CONFIGURACIÓN PARA USO DE NESSUS	1266
1. HABILITAR AUTENTICACIÓN PARA USO DE NESSUS	1266
2. PERMITIR COMUNICACIÓN EN EL FIREWALL	1273
3. ELIMINACIÓN DE LA CONFIGURACIÓN PARA EL USO DE NESSUS	1280
ANEXO D.2.5. PREVENCIÓN DE EXFILTRACIÓN DE DATOS Y DE LA EVASIÓN DE SISTEMAS DE AUTENTICACIÓN	1281
1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN	1281
2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD	1283
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS.....	1285

ANEXO A. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 ENTERPRISE LTSC EN EL ENS COMO MIEMBRO DE DOMINIO

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:

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.

El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.

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 MS WINDOWS 10” 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.

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 entornos de 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 recién 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-599A19. 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 miembros de dominio, 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 productos para evitar código dañino 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 deben 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, bien sea del dominio a través de cuentas de Directorio Activo o bien locales en los puestos de trabajo, cuando se diera dicha necesidad. 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.

La gestión de usuarios que aporta el Directorio Activo proporciona los mecanismos de seguridad suficientes para dar debido cumplimiento de esta medida. Si bajo alguna necesidad se debiera disponer de cuentas de servicio para alguna aplicación ejecutada en el puesto de trabajo, el operador deberá tener en consideración la funcionalidad de creación de cuentas específicas para servicios que le permitirán desvincularse de la gestión de dichas cuentas, reduciendo el TOC (tiempo de coste) de administración de las mismas aumentando a la vez las garantías de seguridad. Así la gestión de credenciales será mantenida por el propio Directorio Activo, siguiendo las políticas establecidas para la organización y realizando el cambio de las mismas cuando debiera en los servicios a los que se hubiera asignado. De esta forma podrán mantenerse múltiples servicios con cuentas específicas para ello, sin que el coste de administración repercuta en una gestión insegura. Toda la información de cuentas de servicio lo podrá localizar en el siguiente enlace:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts>

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. Realizar administración del Directorio Activo, 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://docs.microsoft.com/es-es/windows/security/identity-protection/access-control/access-control>

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 Microsoft Windows Server 2008 R2 y Microsoft Windows 7, a través del sistema de Suscripción de eventos con el que Microsoft los dotó.

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 Microsoft Windows Vista y mejorada la experiencia de usuario y funcionalidad en Microsoft Windows 10, 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:

<https://docs.microsoft.com/es-es/windows/security/identity-protection/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, así como el Directorio Activo del que son miembros los puestos de trabajo, 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. Debido a esta necesidad, en el caso de que la organización no disponga de ninguna herramienta para realizar dicho proceso durante la presente guía se proporciona un paso a paso con el fin de solventar esta necesidad a través del punto “2 INFORMACIÓN ACERCA DEL ÚLTIMO INICIO DE SESIÓN”, en el “ANEXO A.5.2 CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA MS WINDOWS 10”.
- 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 exigido.

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 Canal Semi-Anual, 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.

Se mantendrá no obstante determinadas correcciones orientadas en ocasiones a solventar ciertas incidencias que pueden estar dándose en infraestructuras complejas. Por ejemplo, su organización podría verse afectada a la hora de aplicar la configuración derivada de la presente guía por un fallo identificado en clientes MS Windows 10 miembros de un dominio con Controladores de Dominio Windows Server 2012 R2. Dicho problema consiste en el intento de acceso a un espacio de nombres DFS (por ejemplo, \\dominio.local\SYSVOL) en un equipo que está configurado para requerir autenticación mutua (haciendo uso de UNC Hardened Access feature). Esto viene motivado por las siguientes circunstancias:

- a) La configuración de directiva de seguridad de equipo en los clientes Windows 10 “Servidor de red Microsoft: nivel de validación de nombres de destino SPN del servidor” que se establece en el valor “Aceptar si proporcionada por el cliente”. El valor predeterminado para un DC es desactivado.
- b) En los controladores de dominio tienen instalada la actualización 3161561 correspondiente a los expedientes MS16-075 y MS16-076: “Description of the security update for Windows Netlogon and SMB Server” del 14 de Junio de 2016.

Para solucionar dicha circunstancia deberá aplicar en los controladores de dominio Windows Server 2012 R2, en los entornos que hayan sido afectados por los síntomas descritos previamente, el Update Rollup de Agosto de 2016 para Windows RT 8.1, Windows 8.1 y Windows Server 2012 R2.

<https://support.microsoft.com/en-us/kb/3179574>

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.

Las organizaciones deberán por lo tanto proveer de otra solución frente a 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. 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 en el dominio.

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 del nivel 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 o del propio dominio de la seguridad. 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:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-design-guide>

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 LAS APLICACIONES INFORMÁTICAS

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 de dominio o locales.

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de mecanismos articulados en la guía CCN-STIC-570A, adaptándolos a la organización.
OP. ACC. 1	Auditoría y supervisión de actividad	Revisión e implementación de guía CCN-STIC-859, adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de mecanismos articulados en la guía CCN-STIC-570A, 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.

Control	Medida	Mecanismo de aplicación
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.
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.

Control	Medida	Mecanismo de aplicación
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 el “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. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 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 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.

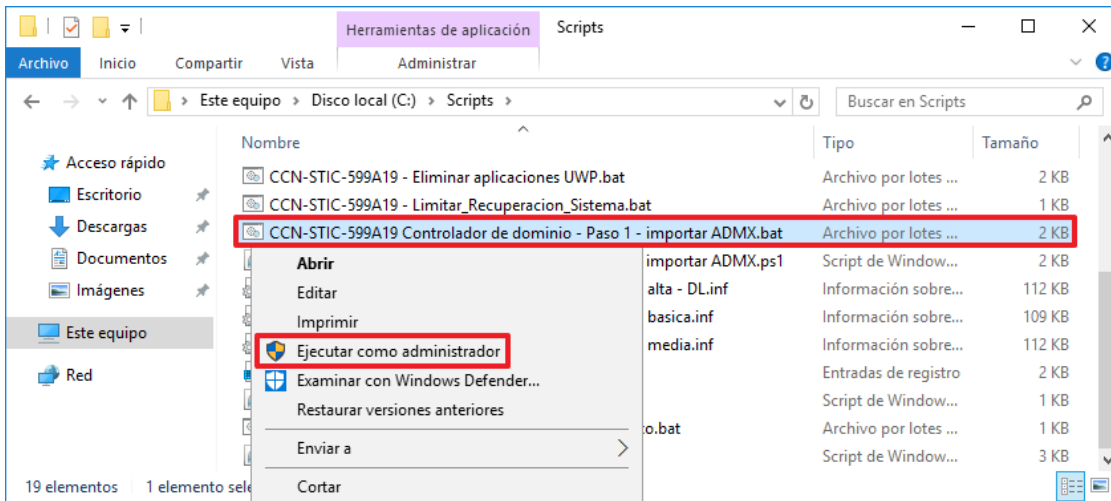
1. PREPARACIÓN DEL DOMINIO

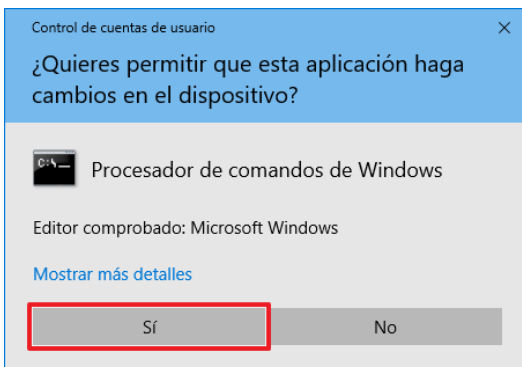
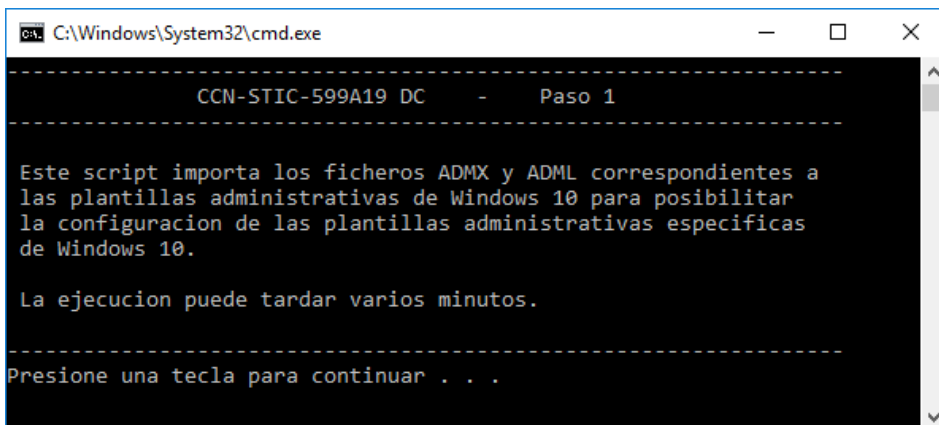
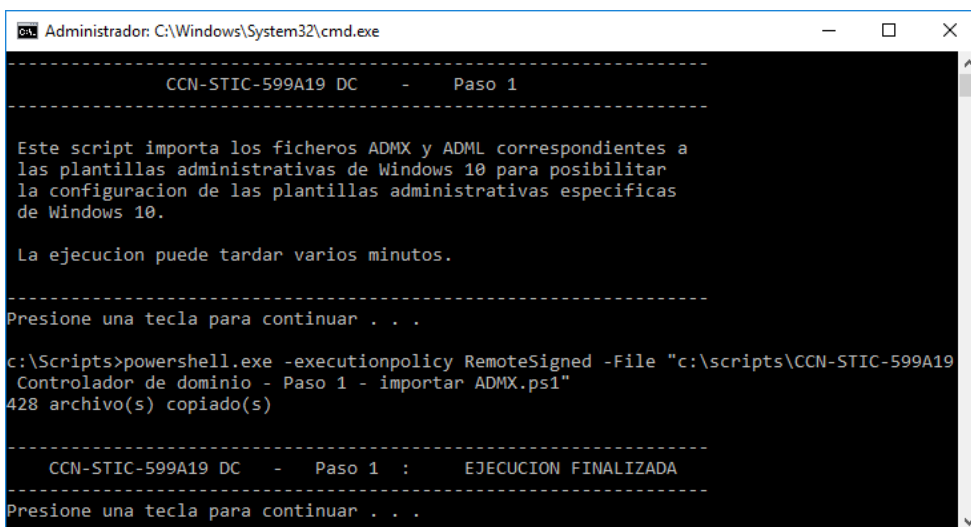
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

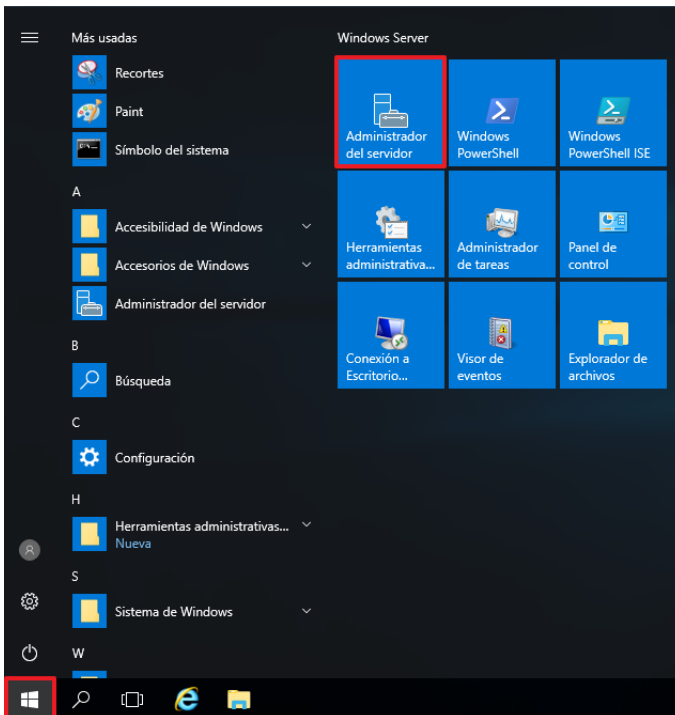
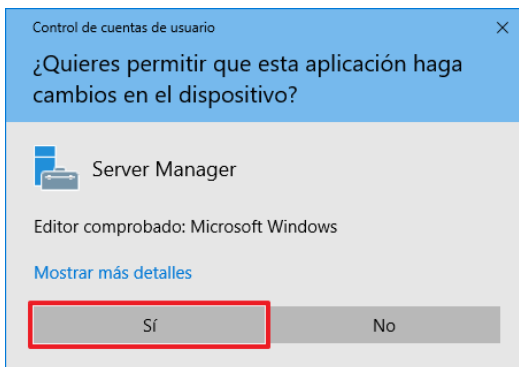
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Si no es así, aplique la guía correspondiente al controlador de dominio, antes de continuar con la aplicación de esta.

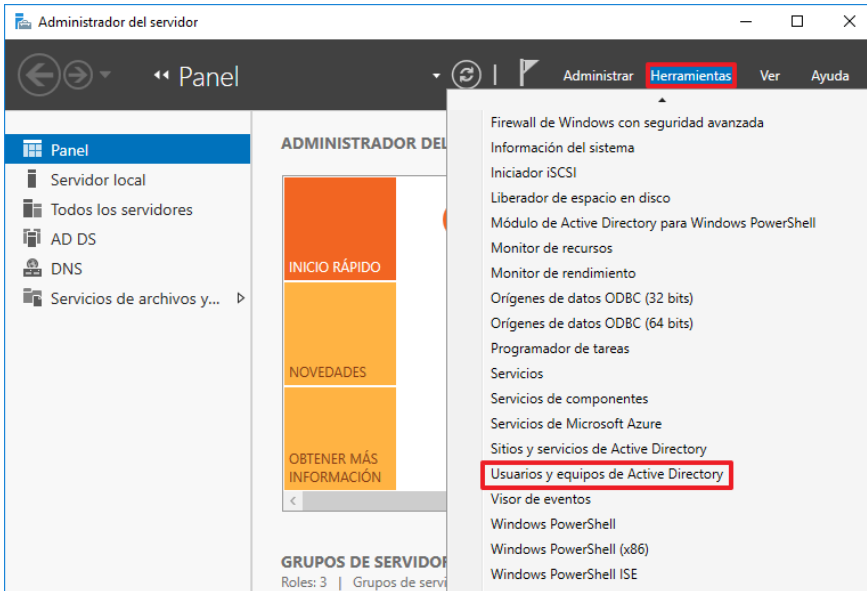
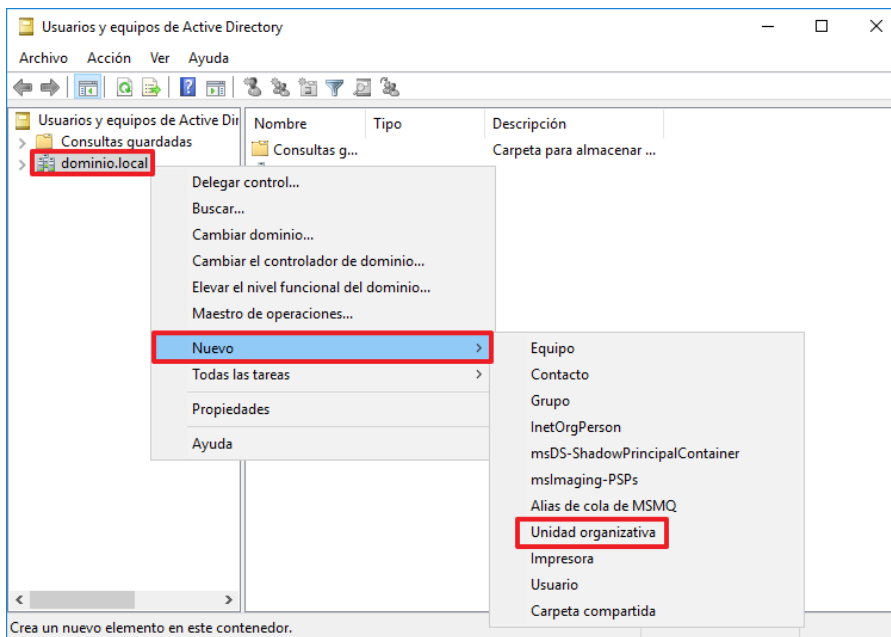
En el ejemplo, las configuraciones y capturas de pantalla han sido realizadas sobre un controlador de dominio al que se le ha instalado Windows Server 2016 y aplicado la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016.

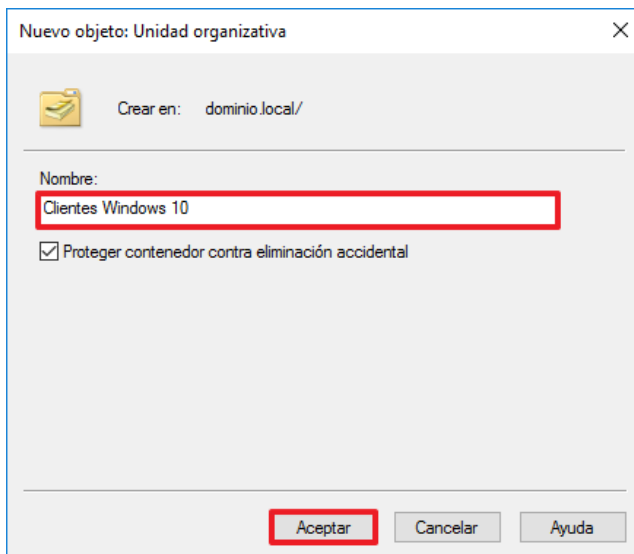
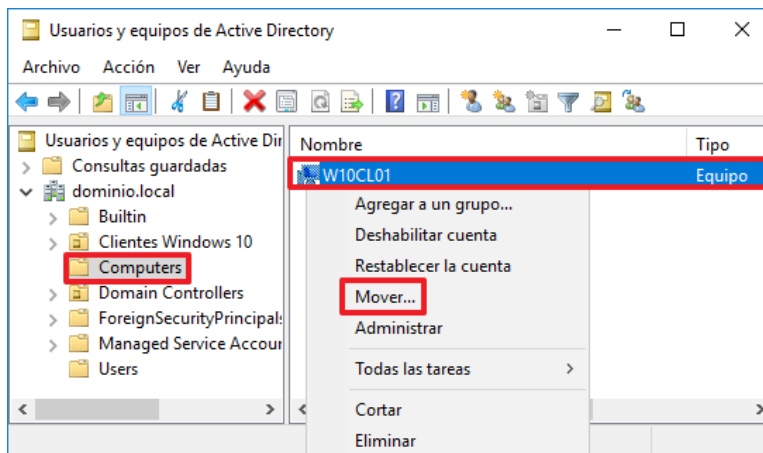
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio.
Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".	

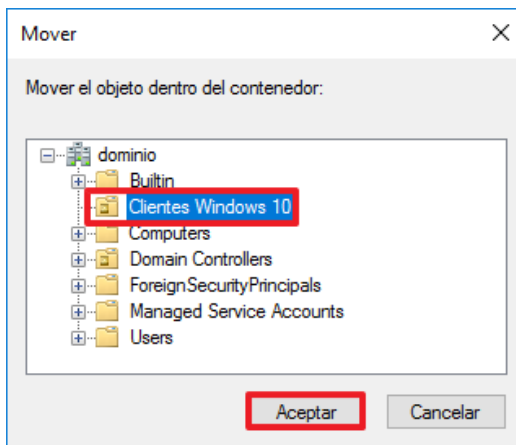
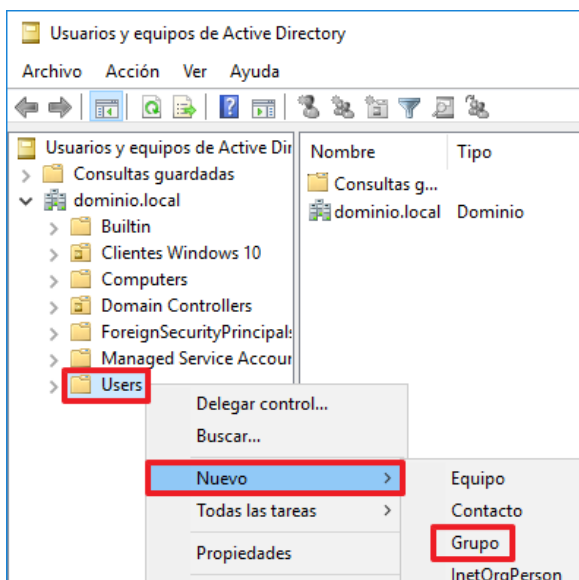
Paso	Descripción
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-599A19 ENS clientes categoria alta - DL (directorio) – CCN-STIC-599A19 ENS clientes categoria media (directorio) – CCN-STIC-599A19 ENS clientes categoria basica (directorio) – CCN-STIC-599A19 ENS Incremental portátiles categoria alta - DL - Bitlocker (directorio) – CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL.inf – CCN-STIC-599A19 ENS Incremental clientes categoria media.inf – CCN-STIC-599A19 ENS Incremental clientes categoria basica.inf – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1 – PolicyDefinitions - (directorio)
6.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

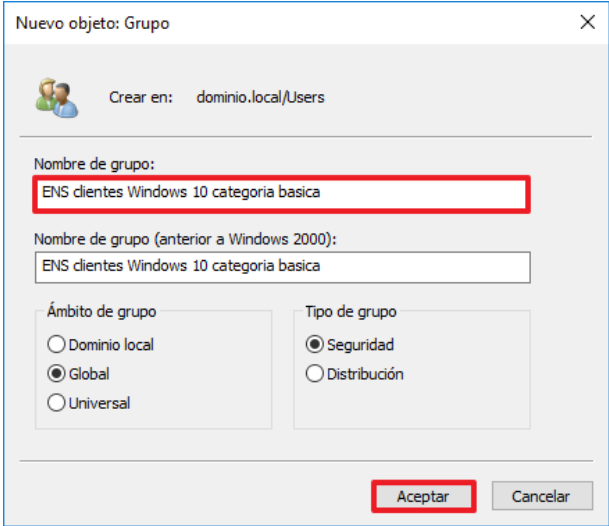
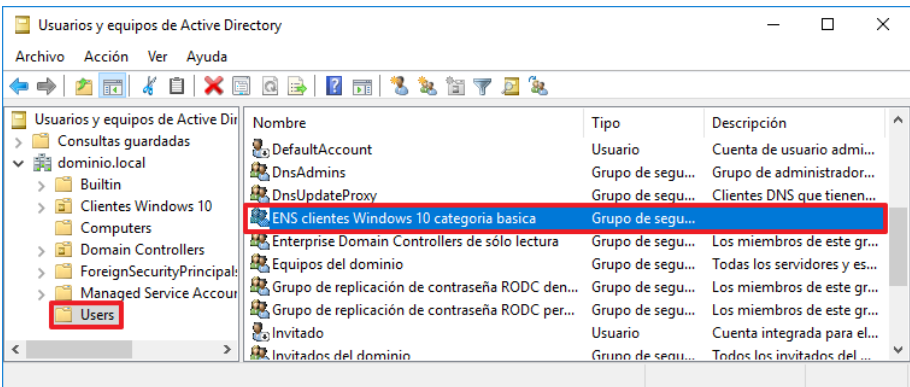
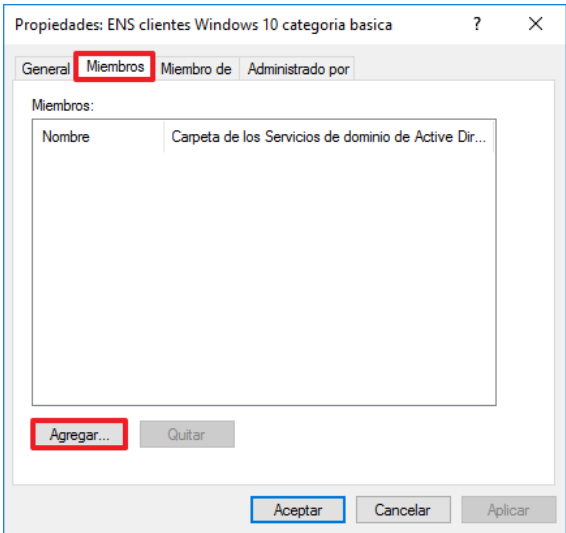
Paso	Descripción
7.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
8.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
9.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 

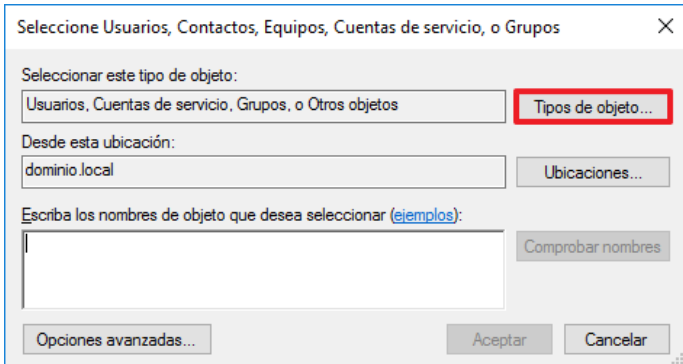
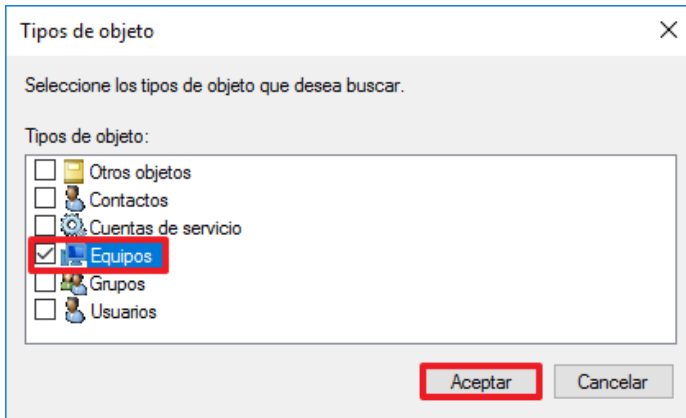
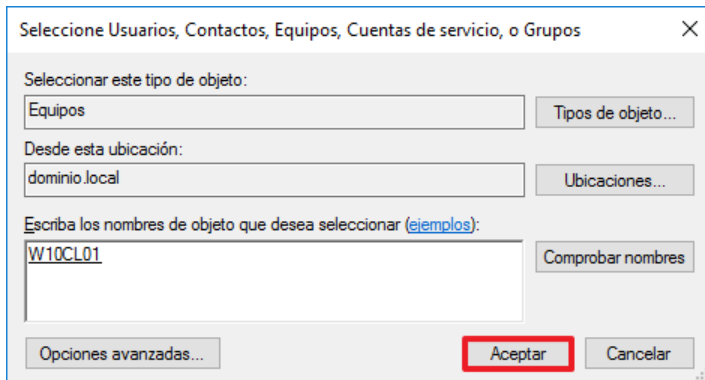
Paso	Descripción
10.	Copie el fichero “CCN-STIC-599A19 ENS incremental clientes categoria basica.inf”, almacenado en la carpeta “C:\Scripts”, al directorio “C:\Windows\Security\Templates” del Controlador de Dominio.
11.	Inicie la herramienta de “Usuarios y equipos de Active Directory”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
12.	Pulse sobre el botón “Sí” para confirmar la operación. 

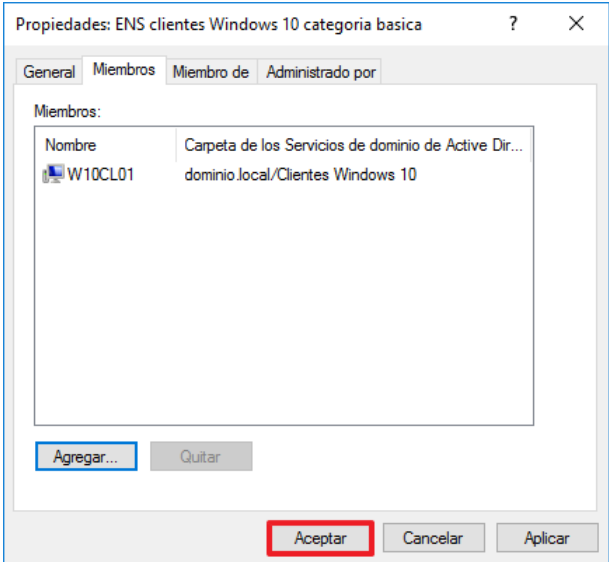
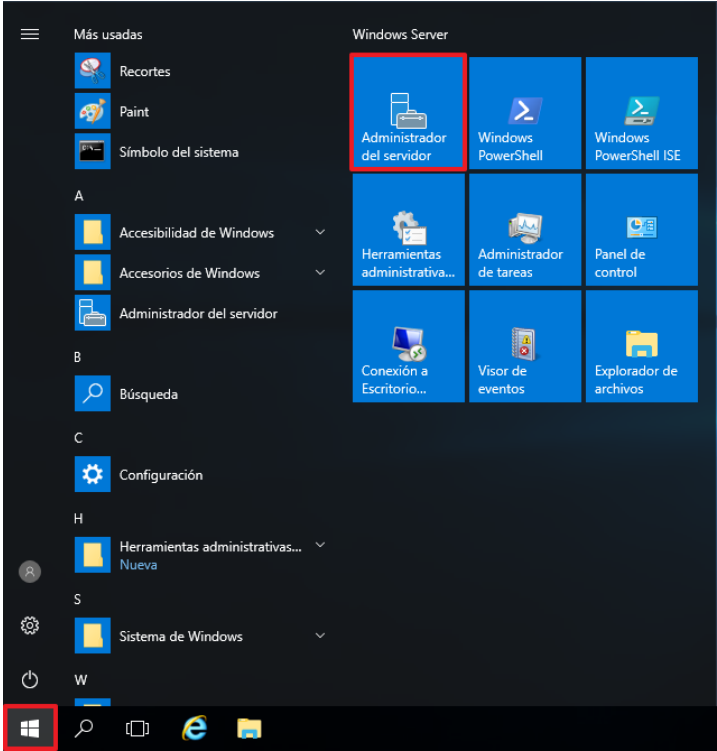
Paso	Descripción
13.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
14.	Pulse con el botón derecho sobre el dominio y seleccione “Nuevo → Unidad organizativa”. 

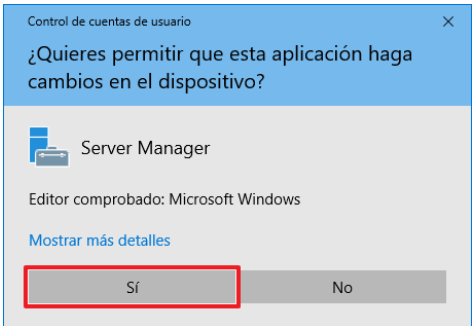
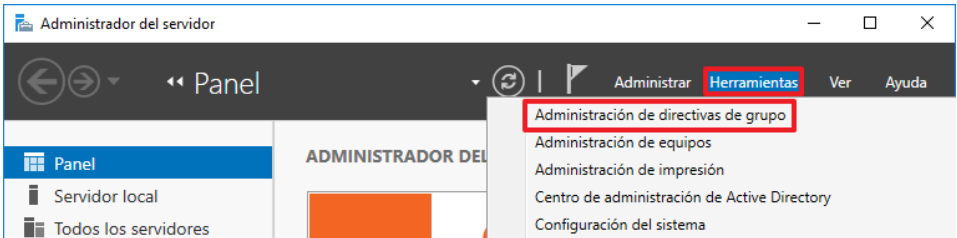
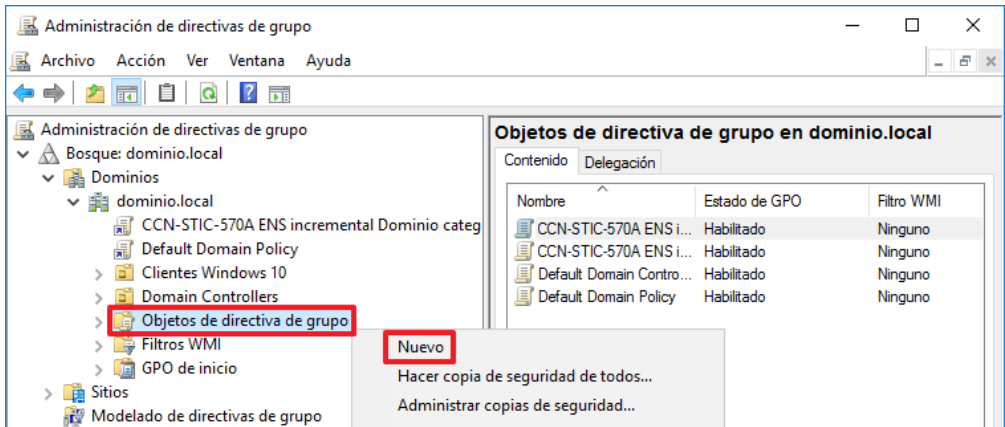
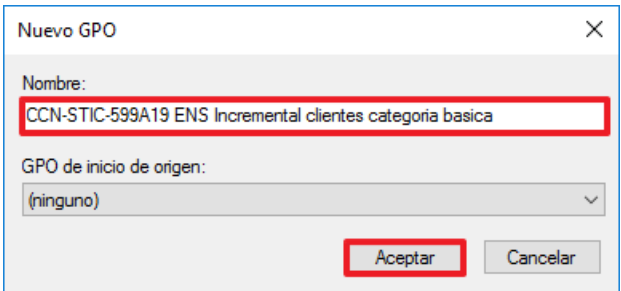
Paso	Descripción
15.	Establezca el nombre para la unidad organizativa con los clientes Windows 10 y pulse “Aceptar”. 
16.	Vaya a las unidades organizativas donde se encuentren los clientes que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover...” en cada uno de ellos.  Nota: En este ejemplo se encuentra bajo la unidad organizativa “Computers”.

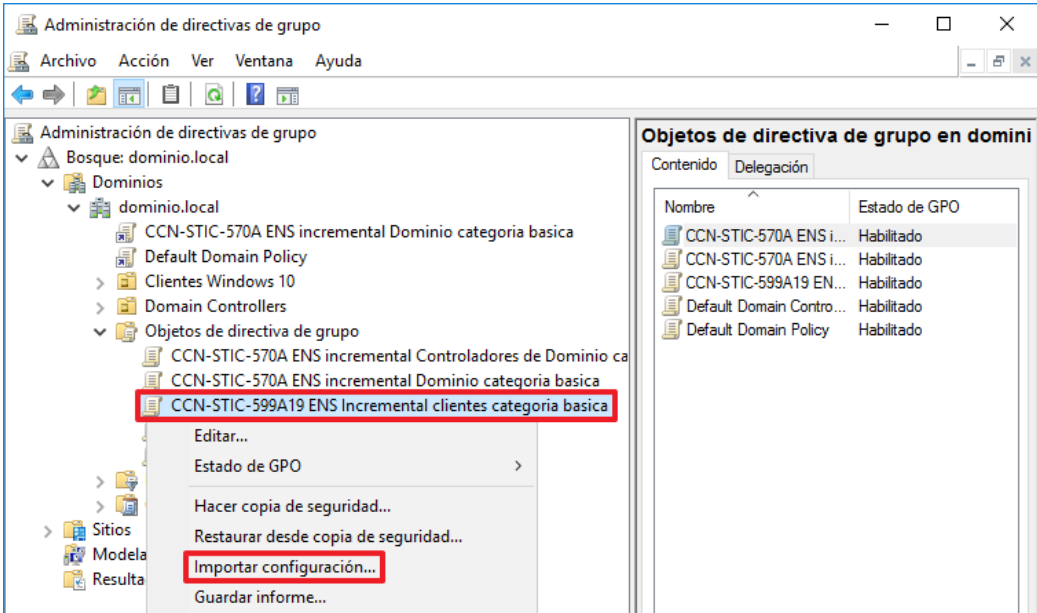
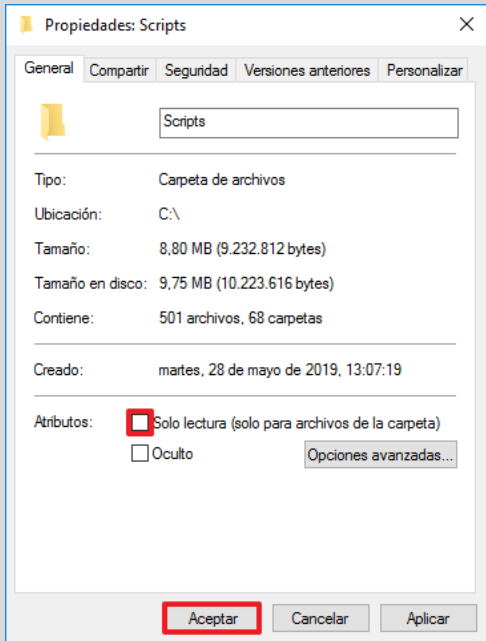
Paso	Descripción
17.	Seleccione la unidad organizativa “Clientes Windows 10” creada anteriormente y pulse “Aceptar”.  Nota: Los siguientes pasos describen el procedimiento para crear un grupo de seguridad donde agregar los puestos de trabajo que le sean de aplicación la categoría básica de seguridad según los criterios definidos del ENS. Si todos los equipos de la organización presentan la misma categoría básica no hace falta la creación de dicho grupo y puede saltar al paso 26. Si por el contrario van a existir puestos de trabajo Windows 10 con categorías media o alta, se deberán crear dichos grupos, siguiendo los pasos de los Anexos A.3 y A.4, de tal forma que la aplicación de políticas de seguridad en función de los niveles se aplique atendiendo a los criterios de pertenencia a grupo.
18.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

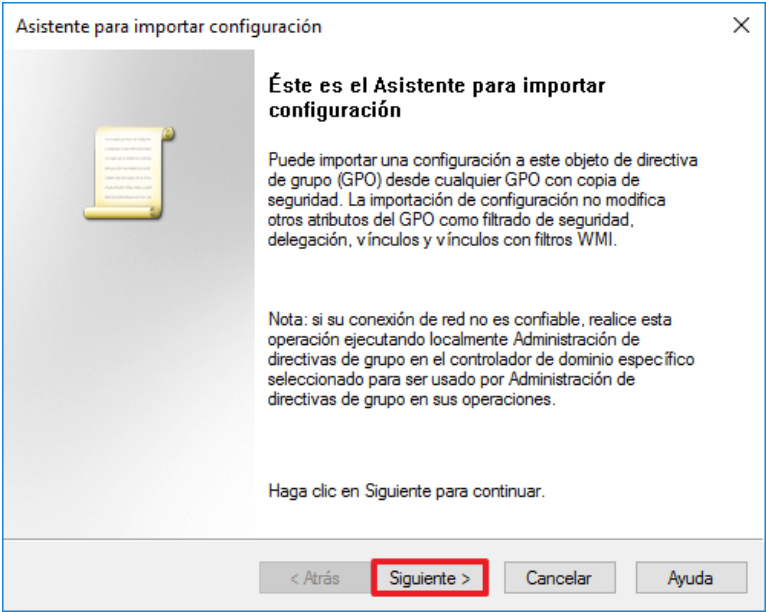
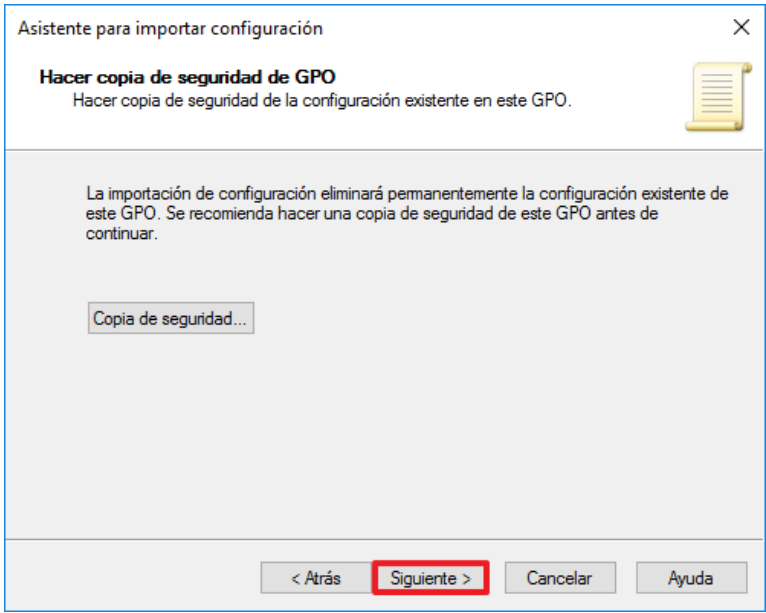
Paso	Descripción
19.	Introduzca como nombre “ENS clientes Windows 10 categoria basica”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio. 
20.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
21.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar...”. 

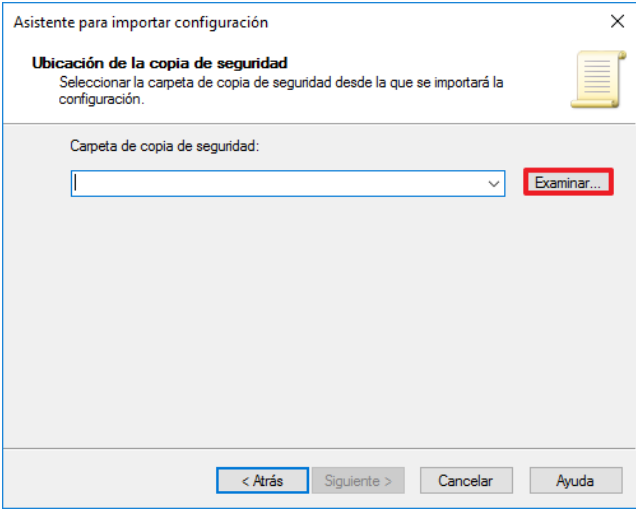
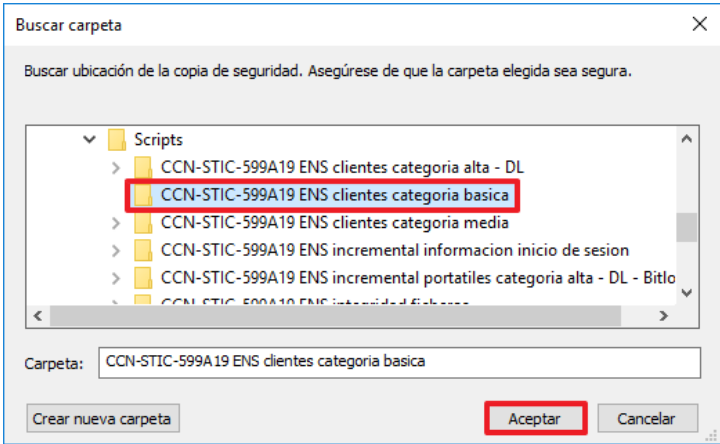
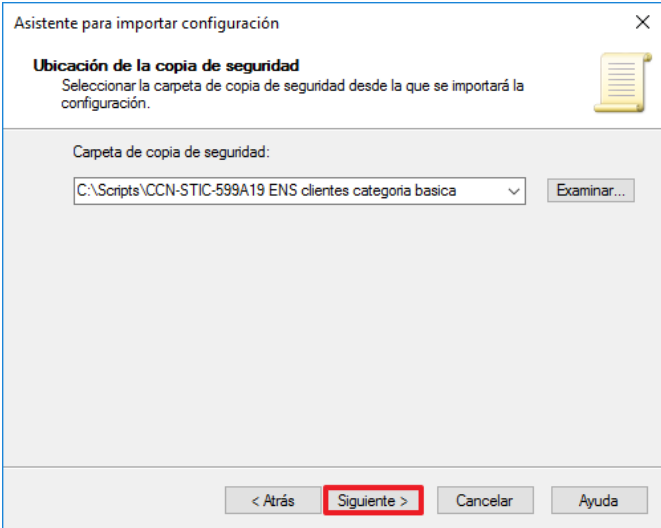
Paso	Descripción
22.	Pulse el botón de “Tipos de objeto...”. 
23.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
24.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad básica y pulse “Aceptar” para agregar la selección.  Nota: No agregue servidores a este grupo.

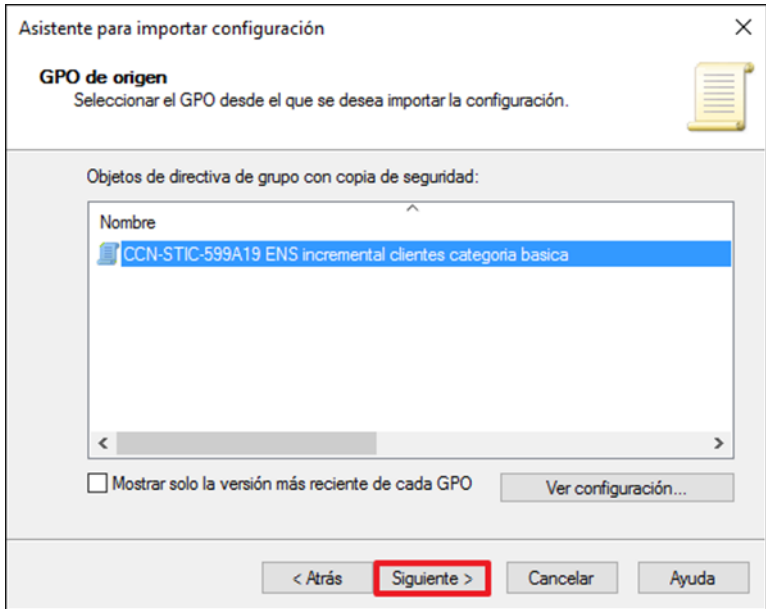
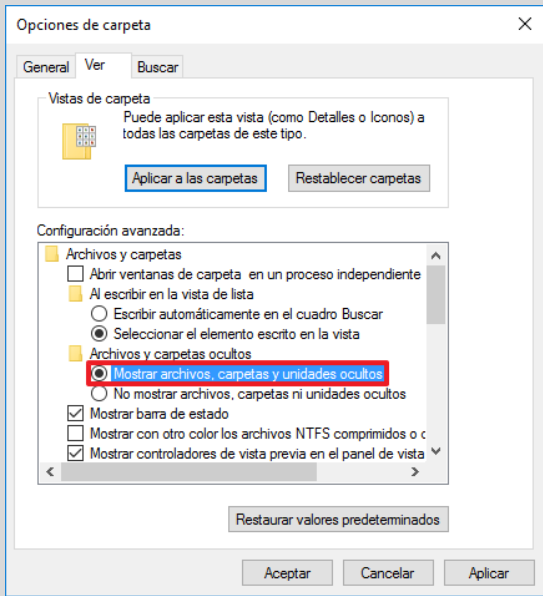
Paso	Descripción
25.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
26.	Cierre la herramienta “Usuarios y equipos e Directorio Activo”.
27.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

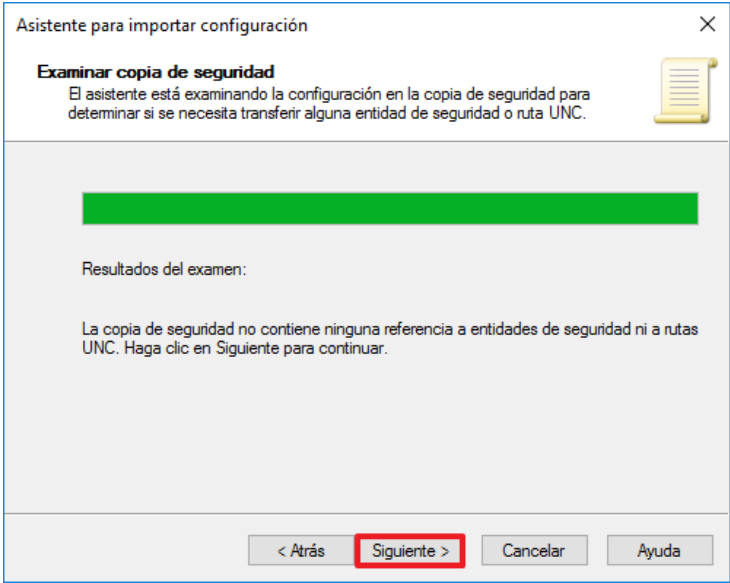
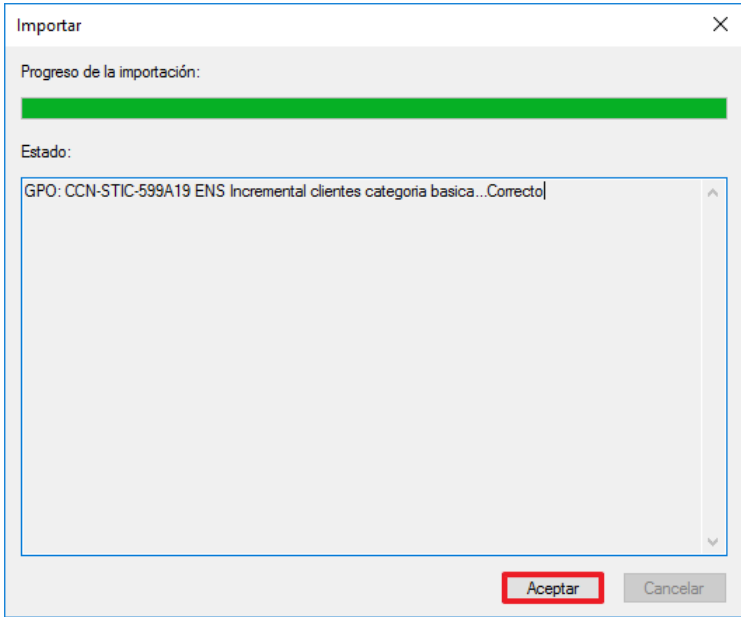
Paso	Descripción
28.	Pulse sobre el botón “Sí” para confirmar la operación. 
29.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
30.	Despliegue los contenedores pertenecientes a su dominio y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
31.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón “Aceptar”. 

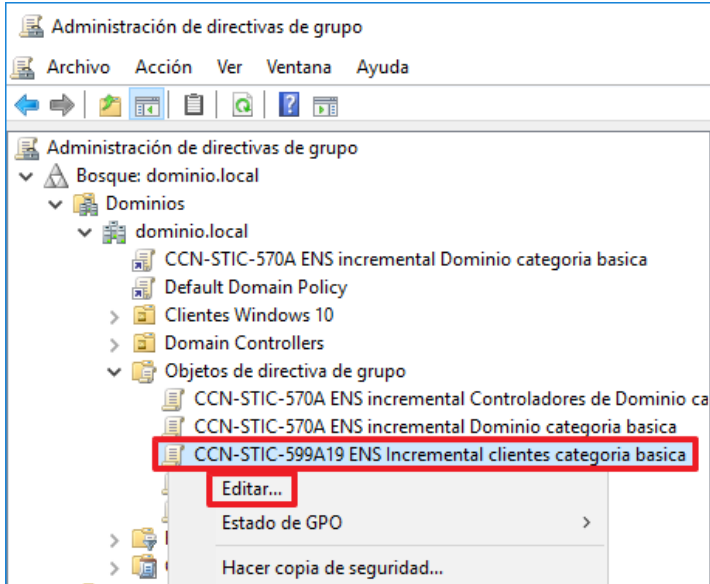
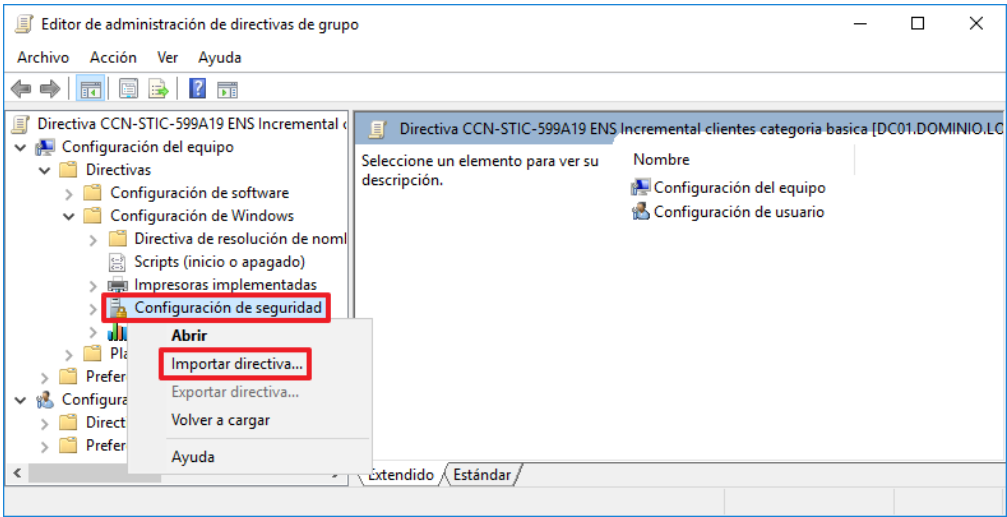
Paso	Descripción												
32.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política con el botón derecho del ratón y seleccione la opción “Importar configuración...”.  Objetos de directiva de grupo en dominio <table border="1"> <thead> <tr> <th>Nombre</th> <th>Estado de GPO</th> </tr> </thead> <tbody> <tr> <td>CCN-STIC-570A ENS incremental Dominio categoria basica</td> <td>Habilitado</td> </tr> <tr> <td>CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica</td> <td>Habilitado</td> </tr> <tr> <td>CCN-STIC-570A ENS incremental Dominio categoria basica</td> <td>Habilitado</td> </tr> <tr> <td>CCN-STIC-599A19 ENS Incremental clientes categoria basica</td> <td>Habilitado</td> </tr> <tr> <td>Default Domain Policy</td> <td>Habilitado</td> </tr> </tbody> </table> Nota: Asegúrese de que los archivos alojados en “C:\Scripts”, así como los archivos dentro de sus subcarpetas, no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 	Nombre	Estado de GPO	CCN-STIC-570A ENS incremental Dominio categoria basica	Habilitado	CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica	Habilitado	CCN-STIC-570A ENS incremental Dominio categoria basica	Habilitado	CCN-STIC-599A19 ENS Incremental clientes categoria basica	Habilitado	Default Domain Policy	Habilitado
Nombre	Estado de GPO												
CCN-STIC-570A ENS incremental Dominio categoria basica	Habilitado												
CCN-STIC-570A ENS incremental Controladores de Dominio categoria basica	Habilitado												
CCN-STIC-570A ENS incremental Dominio categoria basica	Habilitado												
CCN-STIC-599A19 ENS Incremental clientes categoria basica	Habilitado												
Default Domain Policy	Habilitado												

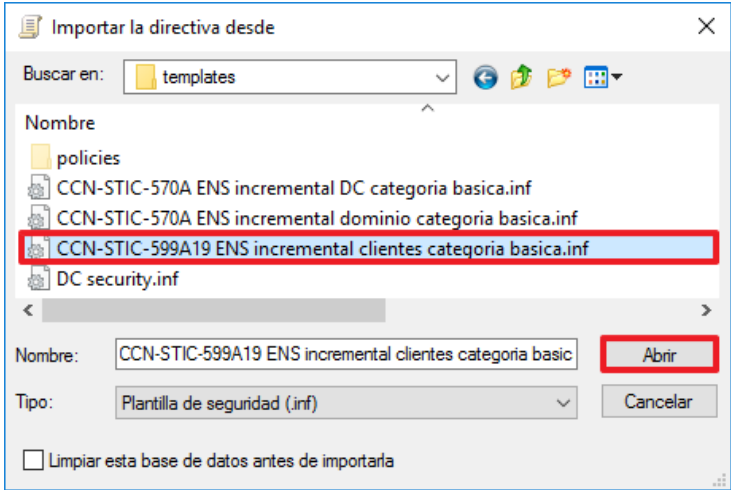
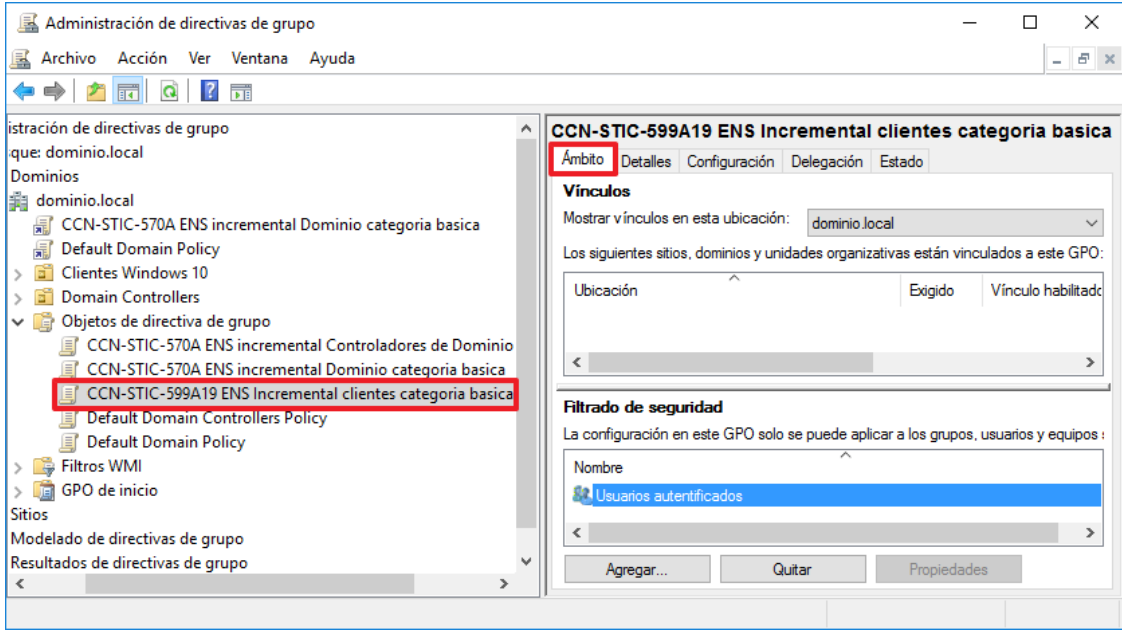
Paso	Descripción
33.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
34.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

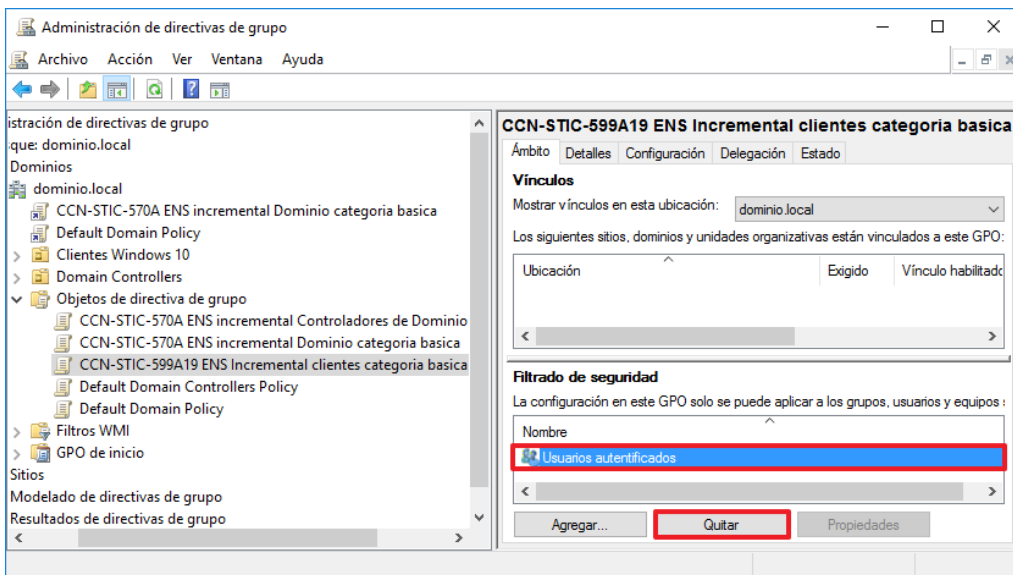
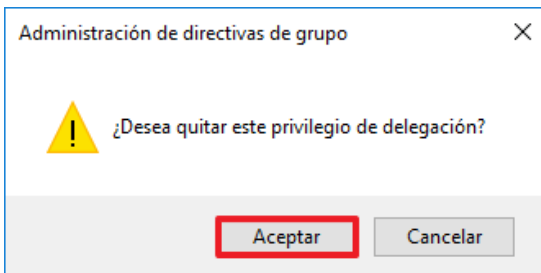
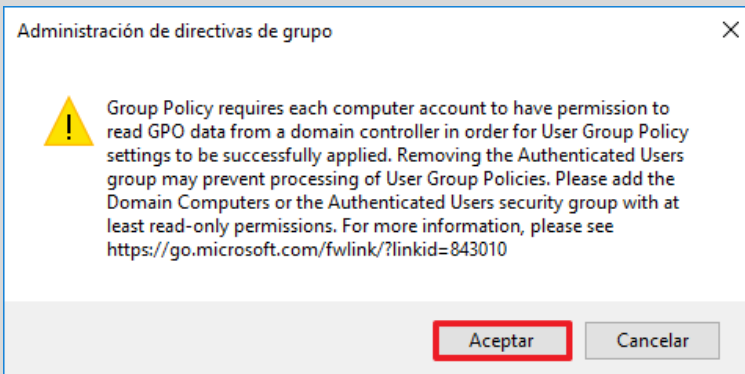
Paso	Descripción
35.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
36.	Seleccione la carpeta “CCN-STIC-599A19 ENS clientes categoria basica” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
37.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

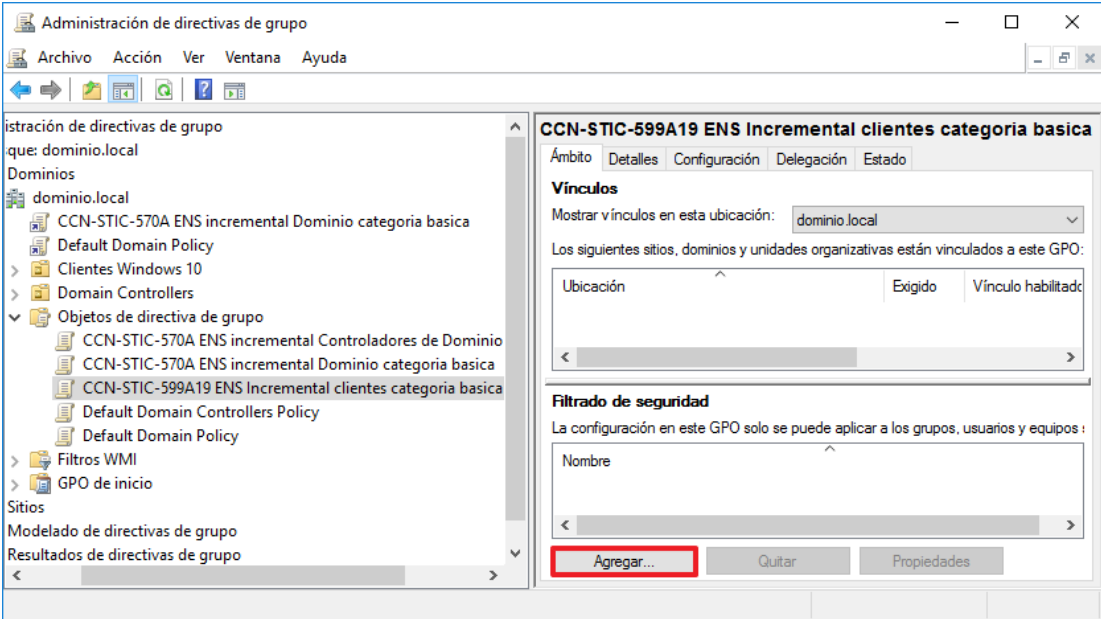
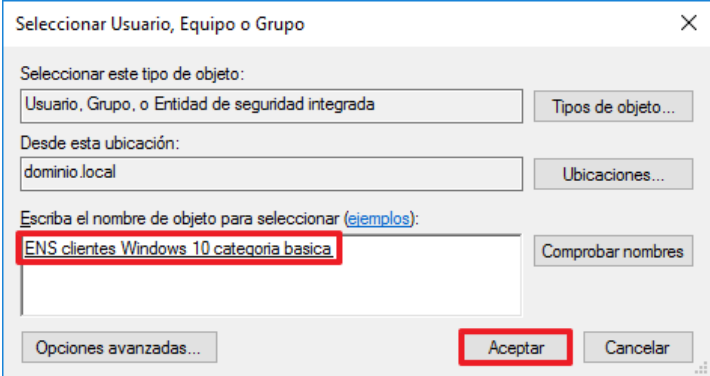
Paso	Descripción
38.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
39.	En la pantalla de examen, pulse el botón “Siguiente >”. 
40.	Para completar el asistente pulse el botón “Finalizar”.
41.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración. 

Paso	Descripción
42.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
43.	Una vez pulsada la opción “Editar...” se abre una ventana de “Editor de administración de directivas de grupo”. Despliegue el objeto de directiva de grupo y sitúe el cursor sobre el nodo Configuración de seguridad. “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”
44.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva...”. 

Paso	Descripción
45.	Seleccione el fichero “CCN-STIC-599A19 ENS incremental clientes categoria basica.inf” ubicado en la ruta “C:\Windows\Security\Templates. Pulse el botón “Abrir”. 
46.	Cierre la política una vez se haya realizado la importación de la configuración de seguridad. Nota: Los siguientes pasos describen el procedimiento para asignar la política al grupo de seguridad creado en los pasos 18 a 25. Si se ha creado el grupo, puesto que va a tener aplicadas diferentes categorías de seguridad en la organización para los puestos de trabajo, siga con el siguiente paso. Si no se creó dicho grupo, diríjase al paso 52.
47.	Vuelva a la herramienta “Administración de directivas de grupo” y seleccione la nueva GPO configurada. Vaya a las opciones de ámbito que se encuentran en el panel derecho. 

Paso	Descripción
48.	En el apartado “Filtrado de seguridad”, seleccione “Usuarios autenticados” y pulse el botón “Quitar”. 
49.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
50.	Pulse ahora sobre el botón “Agregar...”. 
51.	Introduzca como nombre “ENS clientes Windows 10 categoria basica”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
52.	La política se encuentra ya creada correctamente. No obstante, no se aplicará hasta más adelante, una vez haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente Anexo.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA BÁSICA

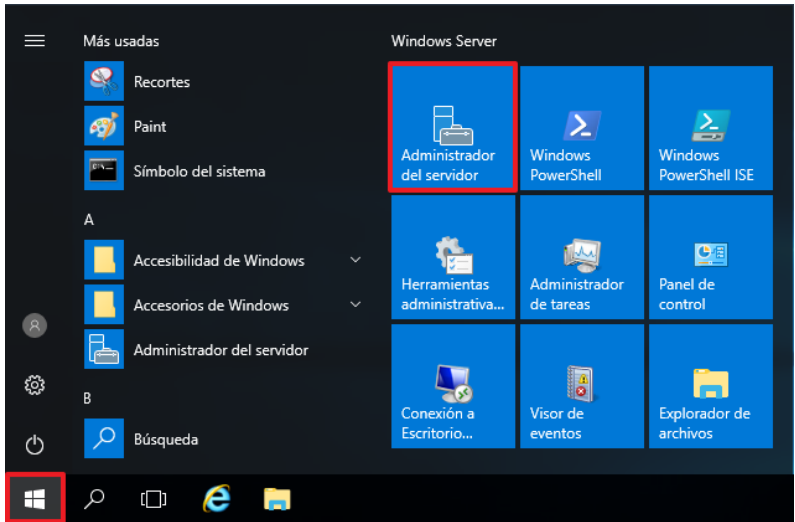
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y por lo tanto deben valorarse con respecto a la aplicación de la presente configuración. La plantilla de seguridad que se ha configurado tiene en consideración los puntos tratados en el Esquema Nacional de seguridad para la categoría básica. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina, como por ejemplo lo relativo al uso de privilegios.

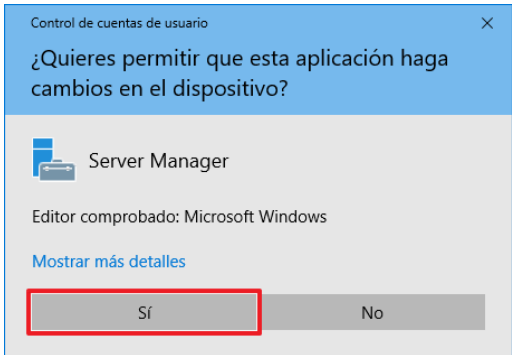
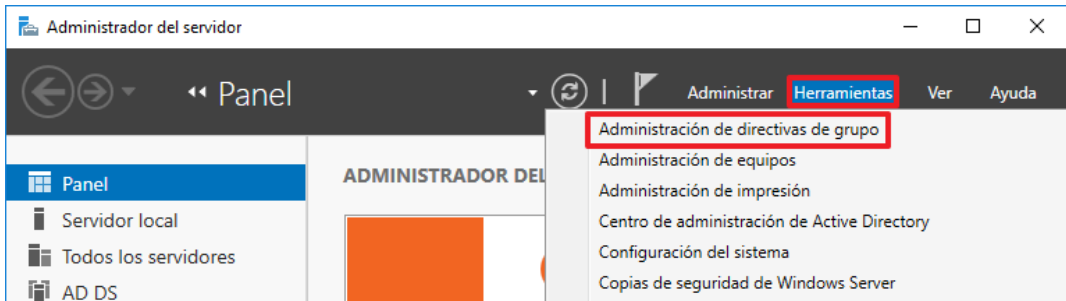
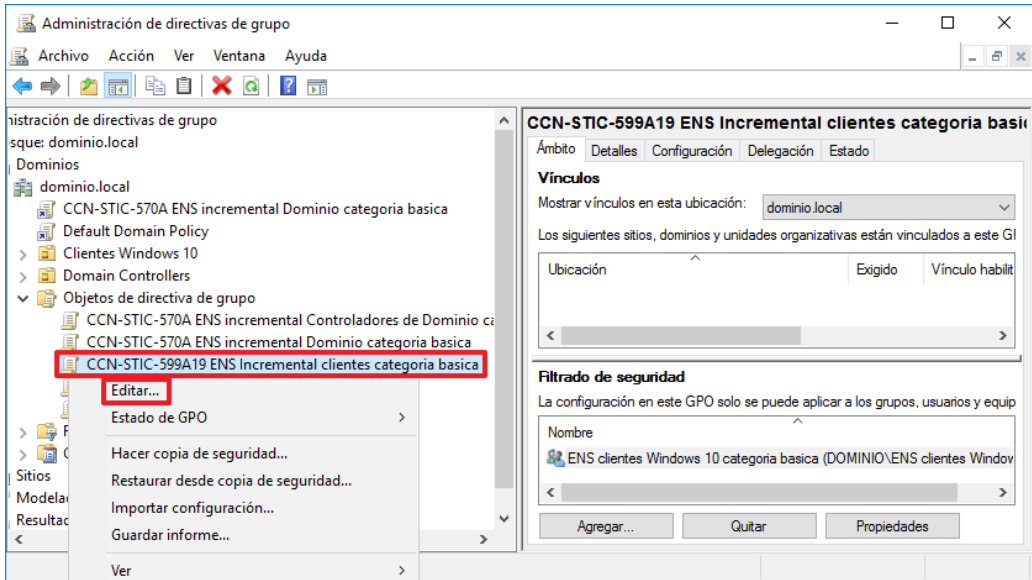
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

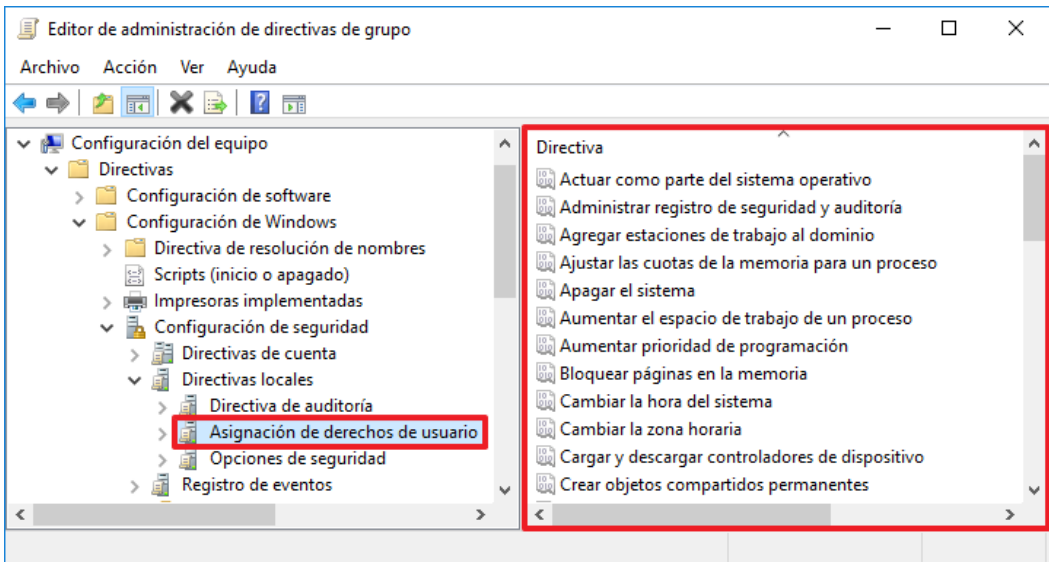
Los objetos de políticas de grupo para puestos de trabajo especifican unos derechos de usuario siguiendo planteamientos de seguridad y siguiendo los principios de mínimos privilegios y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas.

Si esto fuera así deberá realizar las modificaciones sobre el objeto de política creado en el punto previo.

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

Paso	Descripción
53.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
54.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
55.	Edite la política de grupo correspondiente. Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

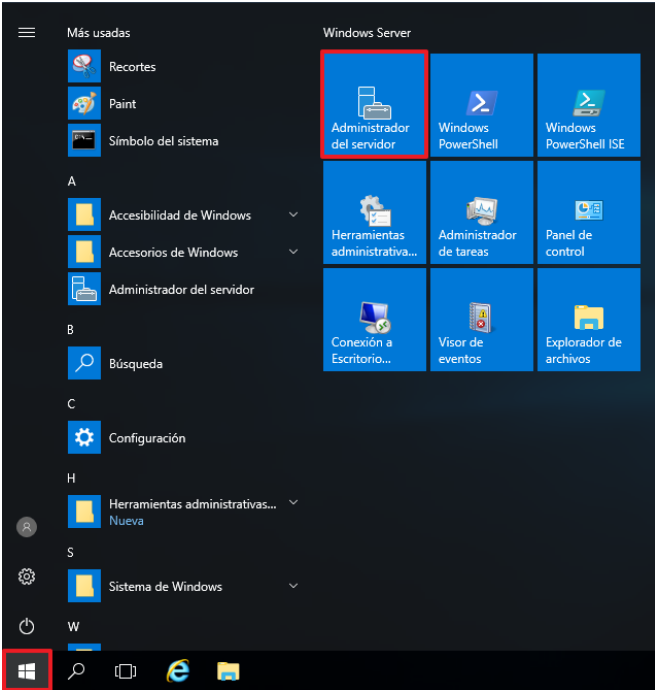
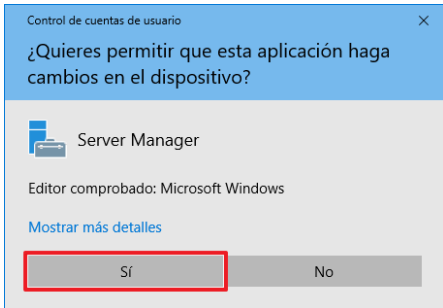
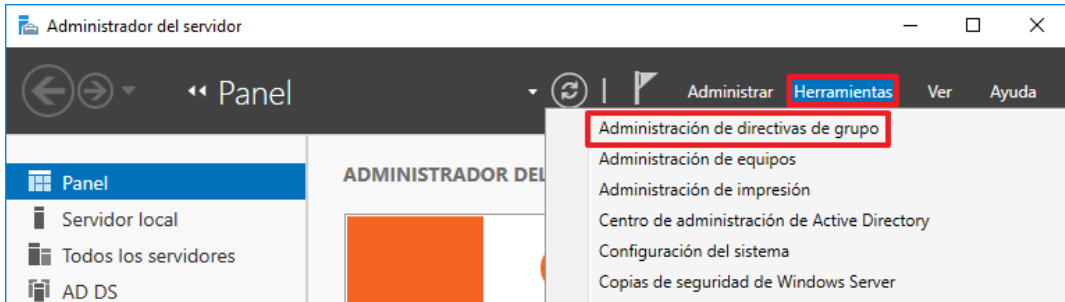
Paso	Descripción
56.	Pulse sobre el botón “Sí” para confirmar la operación. 
57.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
58.	Seleccione la política creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 

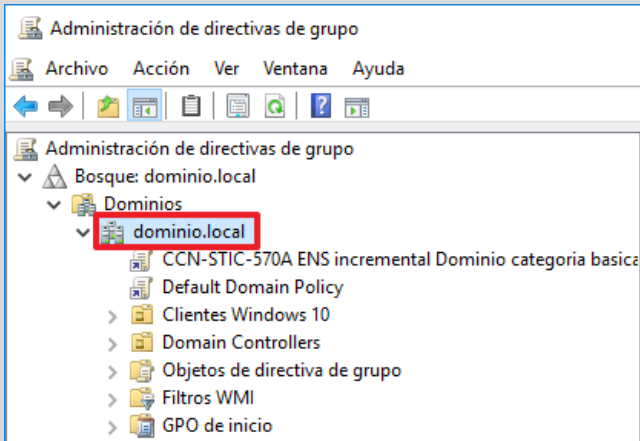
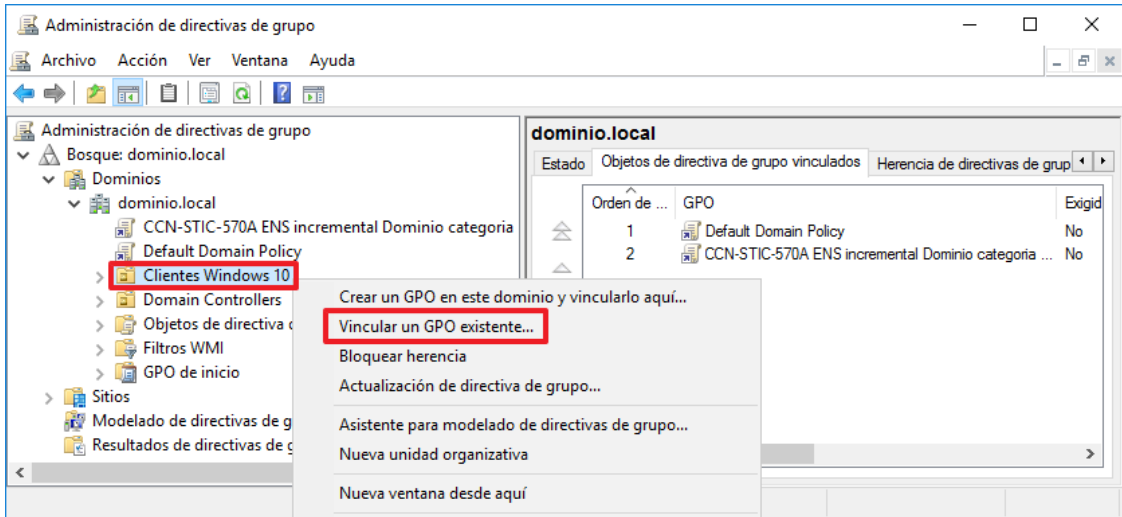
Paso	Descripción
59.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana del editor de administración de directivas de grupo.

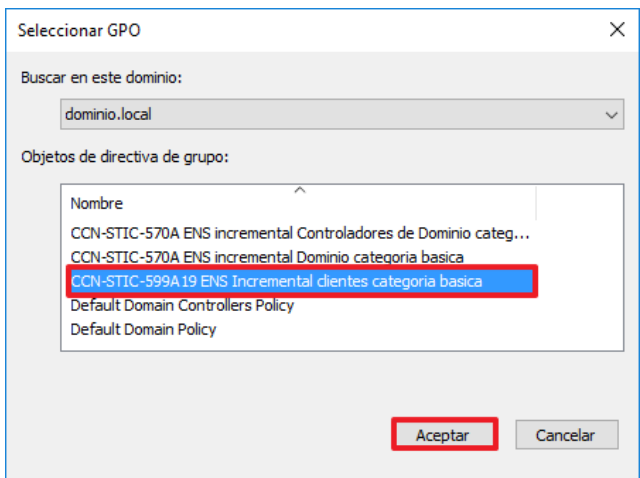
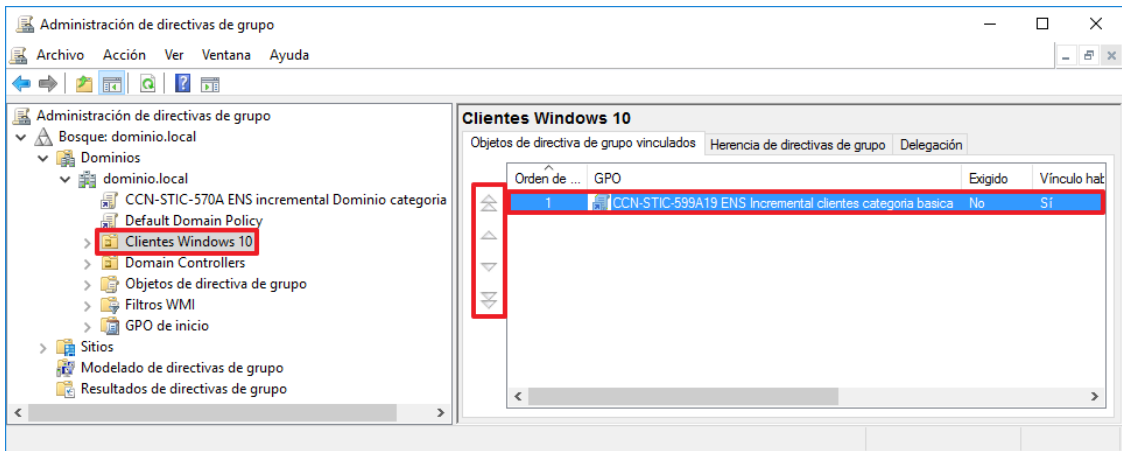
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, una vez que se han tenido en consideración las condiciones definidas en el punto previo.

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

Paso	Descripción
64.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
65.	Pulse sobre el botón "Sí" para confirmar la operación. 
66.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo". 
67.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es "dominio.local".

Paso	Descripción
68.	Identifique las ubicaciones donde se encuentran los Clientes Windows 10 que les son de aplicación las condiciones de seguridad de categoría básica, según estipula el ENS. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” lugar donde se encuentran ubicados los clientes existentes en este escenario. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 
69.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
70.	Seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón “Aceptar”. 
71.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dicha Unidad Organizativa. 
72.	Cierre la herramienta “Administración de directivas de grupo”.
73.	Elimine la carpeta “C:\Scripts”.
74.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE CONFIGURACIONES DE SEGURIDAD

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Es posible que bajo determinadas condiciones pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado Microsoft propone como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

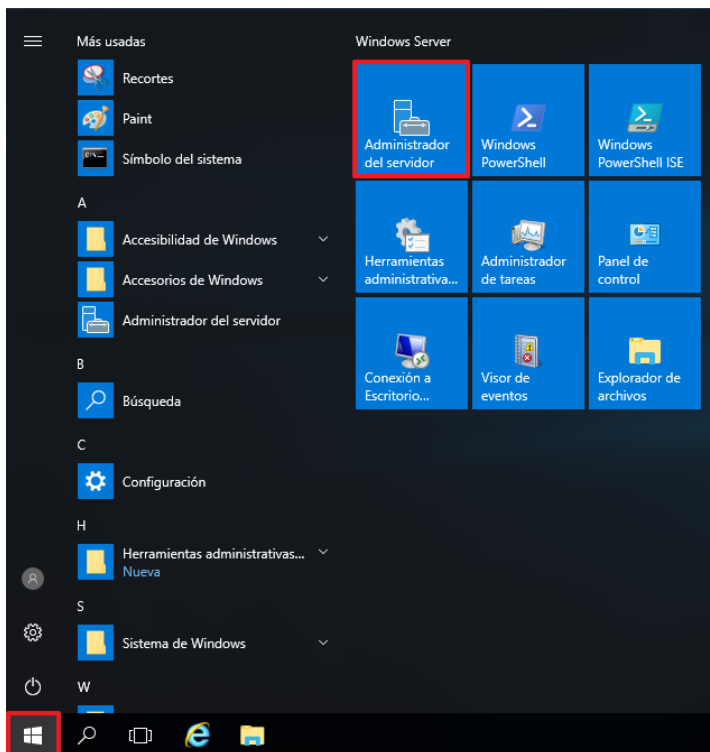
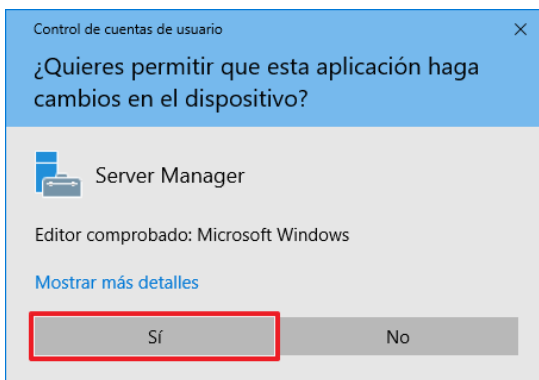
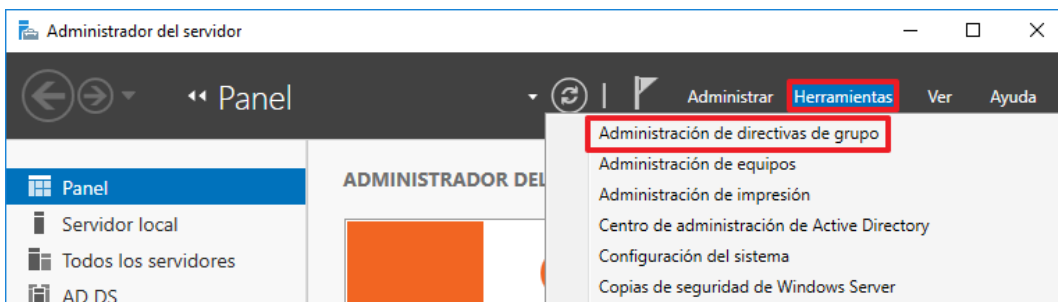
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría básica, aunque con los criterios más laxos de los aplicables.

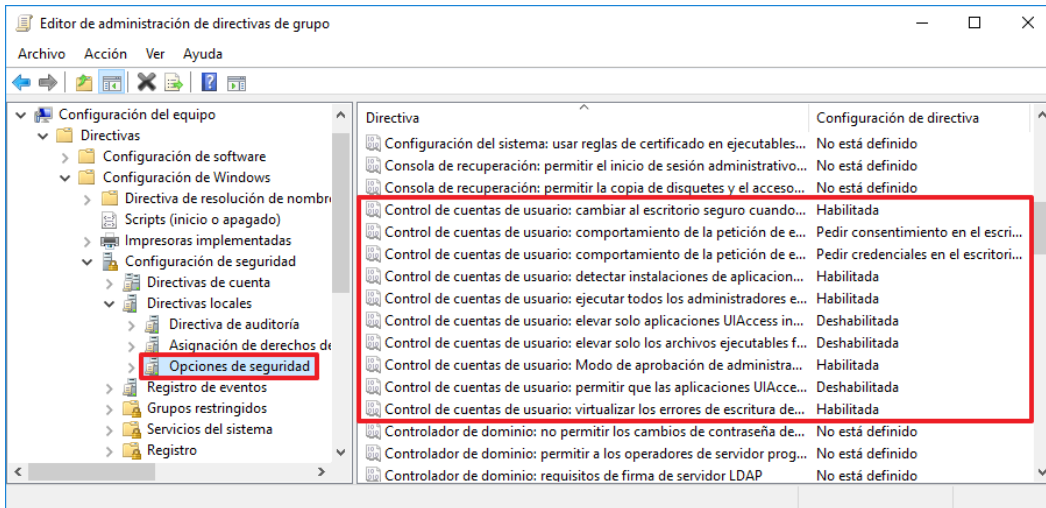
No obstante, y ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría básica por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación a los clientes que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

4.1. CONTROL DE CUENTAS DE USUARIO

Paso	Descripción
75.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
76.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
77.	Identifique los puestos de trabajo que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS clientes Windows 10 categoria basica”. En el caso de que no haya tenido que crear dicho grupo siga al paso siguiente.
78.	Cree un nuevo grupo de forma similar al ya creado, siguiendo los pasos 11 a 26 del presente Anexo.

Paso	Descripción
79.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
80.	Pulse sobre el botón "Sí" para confirmar la operación. 
81.	Seleccione la pestaña "Administración de directivas de grupo" 

Paso	Descripción
82.	Cree una nueva política de grupo con un nombre diferente (p.e. “CCN-STIC-599A19 ENS incremental clientes categoria basica incidencias UAC”) que será asignable a los clientes Windows 10 con una categoría básica e incidencias de funcionalidad del UAC. Siga para ello los pasos 27 a 46. Incluya al nuevo grupo de puestos de trabajo creado anteriormente en lugar del grupo “ENS clientes Windows 10 categoria basica”.
83.	Edite el nuevo objeto de GPO “CCN-STIC-599A19 ENS incremental clientes categoria basica incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar...” del menú contextual.
84.	Despliegue la política y sitúese en la siguiente ruta: Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad
85.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
86.	Realice las modificaciones oportunas.
87.	Cierre la política.
88.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se efectúa cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Debe tener en consideración que, si ha alterado la política de control de cuentas y esta es menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Deberá evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presenten funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

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 GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

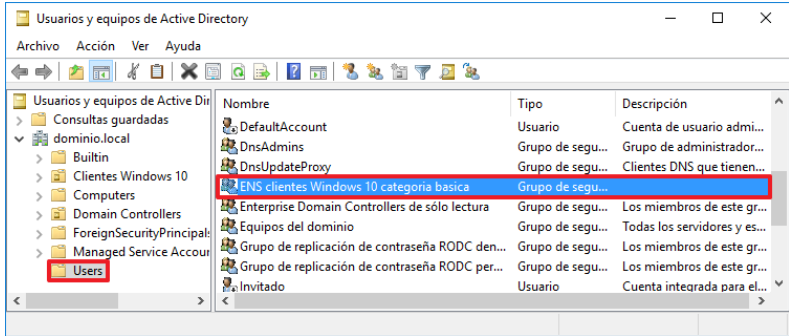
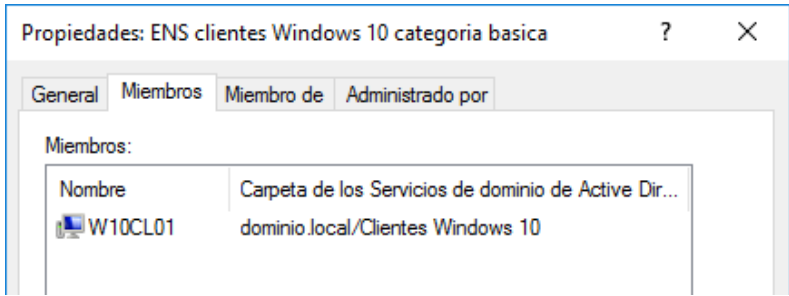
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

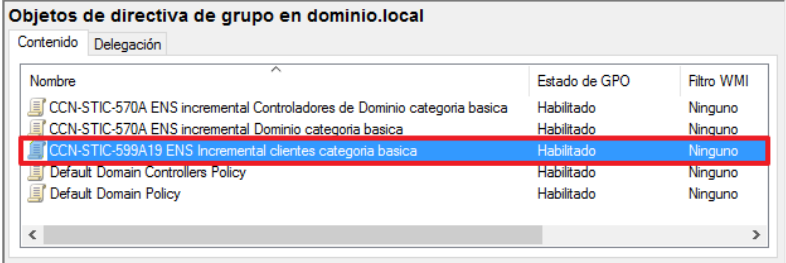
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

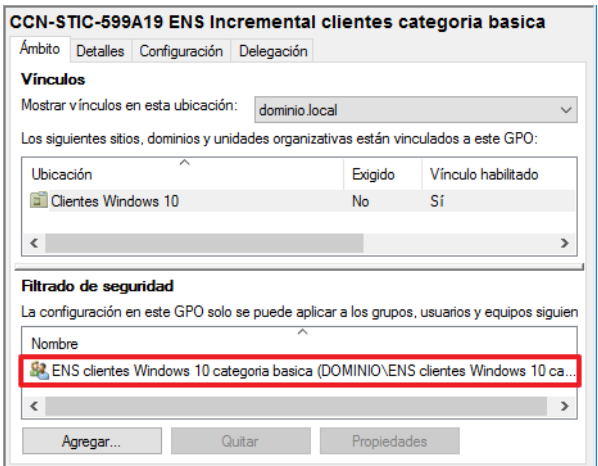
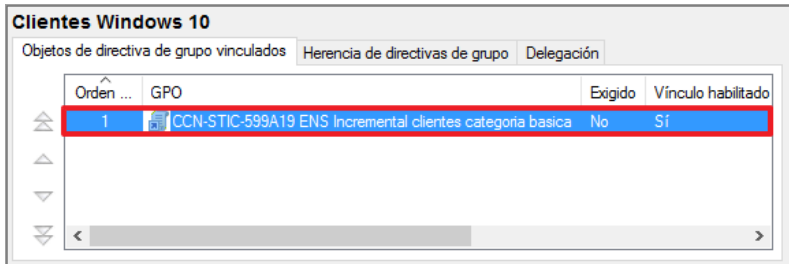
También deberá ejecutar una parte del análisis en los clientes Windows 10 a los que se les haya aplicado la configuración de seguridad de categoría básica. En éstos deberá ejecutar la siguiente aplicación.

- a) Conjunto resultante de directivas (rsop.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creado el grupo “ENS clientes Windows 10 categoria basica” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory” desde: “Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory” Seleccione el contenedor “Users”, situada en “[Su dominio] → Users” y a continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS clientes Windows 10 categoria basica”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.
3. Verifique que los clientes que han sido catalogados como de categoría de seguridad básica, siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS clientes Windows 10 categoria basica”.		Pulse doble clic sobre el grupo “ENS clientes Windows 10 categoria basica” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los clientes que corresponden a esta categoría de seguridad aparecen en el listado.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.

Comprobación	OK/NOK	Cómo hacerlo		
4. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” ha sido creado y está habilitado.		Ejecute la herramienta “Administrador de directivas de grupo” desde: “Menú inicio → Herramientas administrativas → Administrador de directivas de grupo” Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo” Verifique que está creado el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” y que en la columna “Estado de la GPO” figura como habilitado.		
				
		Directiva	Estado	OK/NOK
		CCN-STIC-599A19 ENS incremental clientes categoria basica	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” tiene definido el Ámbito al grupo “ENS clientes Windows 10 categoria basica”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS clientes Windows 10 categoria basica”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.
6. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” es aplicado a todos aquellos equipos Windows 10 que le son de aplicación las condiciones de categoría básica.		Evalúe que la política de seguridad es aplicada en un orden superior a otras políticas aplicables a los puestos de trabajo en todas aquellas ubicaciones donde se encuentren clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría básica. En el árbol de la izquierda, seleccione la ubicación donde se encuentren los clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría básica: 

Comprobación	OK/NOK	Cómo hacerlo		
7. Verifique la directiva de contraseñas en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Pulse el botón derecho del ratón y seleccione la opción “Editar...”. Se abrirá el editor de directivas de grupo. Deberá navegar sobre los elementos del árbol de directorios para verificar las distintas configuraciones. Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directiva de cuentas → Directiva de contraseñas”		
		Directiva	Valor	OK/NOK
		Exigir historial de contraseñas	24	
		Longitud mínima de la contraseña	8	
		Vigencia máxima de la contraseña	90	
		Vigencia mínima de la contraseña	2	
8. Verifique la directiva de bloqueo de cuenta en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directiva de cuentas → Directiva de bloqueo de cuenta”		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	30	
		Restablecer el bloqueo de cuenta después de	30	
		Umbral del bloqueo de cuenta	8	

Comprobación	OK/NOK	Cómo hacerlo		
9. Verifique las directivas de auditoría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
10. Verifique la asignación de derechos de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	BUILTIN\Administradores	

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

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Generar auditorías de seguridad	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Generar perfiles de un solo proceso	BUILTIN\Administradores
		Generar perfiles del rendimiento del sistema	BUILTIN\Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	
		Hacer copias de seguridad de archivos y directorios	BUILTIN\Administradores
		Iniciar sesión como proceso por lotes	
		Iniciar sesión como servicio	
		Modificar la etiqueta de un objeto	
		Modificar valores de entorno firmware	BUILTIN\Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	
		Omitir comprobación de recorrido	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores, NT AUTHORITY\Usuarios autenticados
		Permitir el inicio de sesión local	BUILTIN\Administradores BUILTIN\Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	
		Realizar tareas de mantenimiento del volumen	BUILTIN\Administradores
		Reemplazar un símbolo (token) de nivel de proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Restaurar archivos y directorios	BUILTIN\Administradores

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Tener acceso a este equipo desde la red	BUILTIN\Administradores, BUILTIN\Usuarios	
		Tomar posesión de archivos y otros objetos	BUILTIN\Administradores	
11.Verifique las opciones de seguridad en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesible anónimamente		
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitado	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitado	
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitado	
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitado	
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitado	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		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	Habilitado
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitado
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitado
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitado
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitado
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitado
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitado
		Cuentas: estado de la cuenta de invitado	Deshabilitado
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitado
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		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	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitado
		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	Habilitado
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitado
		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)	Habilitado
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitado
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitado
		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	Habilitado
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
12.Verifique los servicios del sistema definidos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema” Nota: 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 para cada servicio. En la ventana del editor de administración de directivas de grupo 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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
Agente de conexión de red	NcbService	Manual	Configurado	
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	wcnscvc	Manual	Configurado	
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento	pla	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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	WbioSvc	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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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.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	

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		
13.Verifique los valores del sistema de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos” Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".		
Archivo		Usuario	Permiso	OK/NOK
%ProgramFiles%\Netmeeting		Administradores	Control total	
		System	Control total	
%Public%\		Administradores	Control total	
		System	Control total	
		Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
		Administradores	Control total	
		System	Control total	
14.Verifique la directiva de almacén digital en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva		OK/NOK
		No permitir que se ejecute el almacén digital		
		Habilitado		
15.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva		OK/NOK
		Desactivar la ayuda activa		
		Habilitado		

Comprobación	OK/NOK	Cómo hacerlo		
16.Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	
17.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
18.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
19.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
20.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
21.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

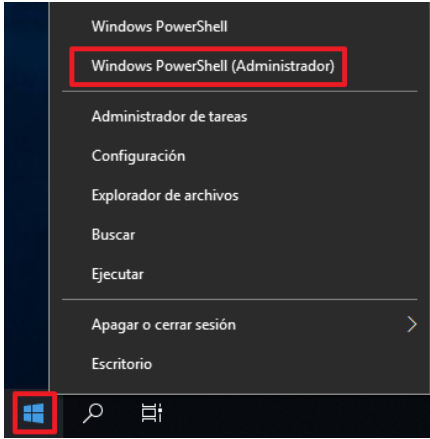
Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Impedir que se eliminen datos del sitio de favoritos	Deshabilitado	
		Impedir que se eliminen los archivos temporales de Internet	Deshabilitado	
		Impedir que se eliminen los datos de filtrado InPrivate	Deshabilitado	
		Impedir que se eliminen 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	
22.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
23.Verifique las directivas de OneDrive en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive”		

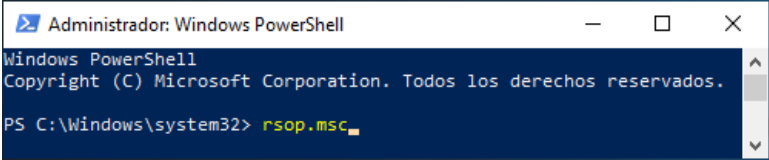
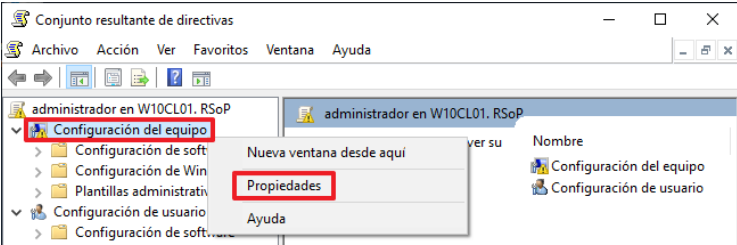
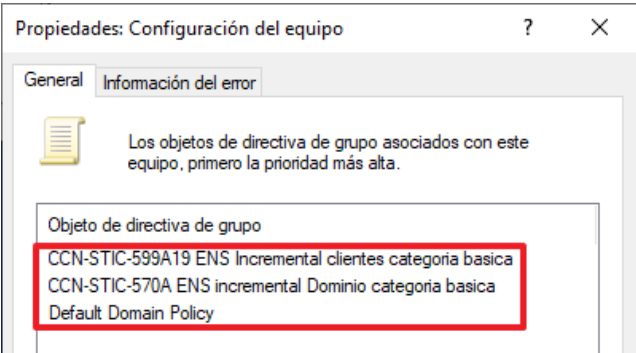
Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Impedir el uso de OneDrive para almacenar archivos.		Habilitado	
24.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows →Privacidad de la aplicación”		
	Directiva		Valor	OK/NOK
	Permitir que las aplicaciones de Windows accedan a dispositivos de confianza		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows accedan a la cámara		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 accedan a la información de la cuenta		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows accedan a la ubicación		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows accedan a las notificaciones		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows accedan a las tareas		Habilitado (Forzar denegación)	
	Permitir que las aplicaciones de Windows accedan a los mensajes		Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	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 controlen las radios	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)
25.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	Habilitado	
		Permitir telemetría	Habilitado	
26.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
27.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
28.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitado	
		Desactivar sensores	Habilitado	
		Desactivar ubicación	Habilitado	
29.Verifique la directiva de Windows Update en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	

Comprobación	OK/NOK	Cómo hacerlo		
30.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
31.Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador.		Inicie sesión en el equipo que está comprobando con una cuenta de usuario de Windows con permisos de administrador.		
32.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. 		

Comprobación	OK/NOK	Cómo hacerlo
33.Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse "Enter" para abrir la consola de administración "Conjunto resultante de directivas". 
34.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 ENS incremental clientes categoria basica".		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las políticas deberán aparecer y "CCN-STIC-599A19 ENS incremental clientes categoria basica" deberá estar situada encima de la GPO que se establece a nivel de dominio, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 ENS incremental clientes categoria basica" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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.

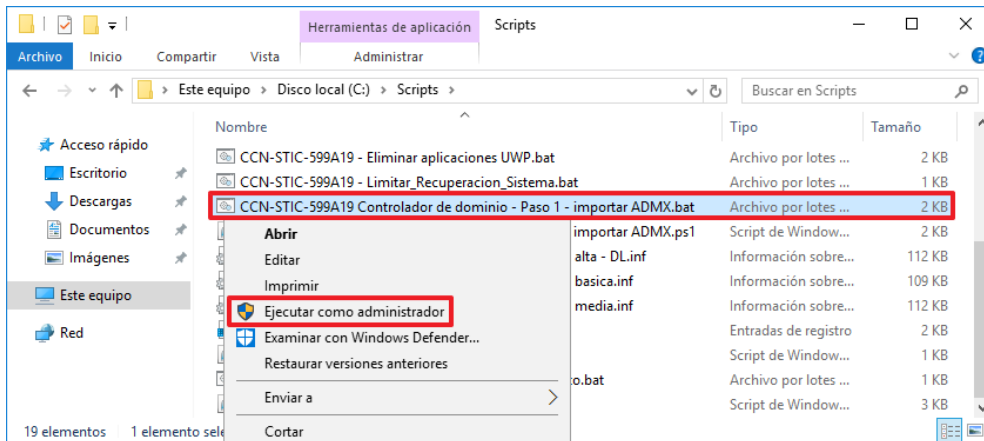
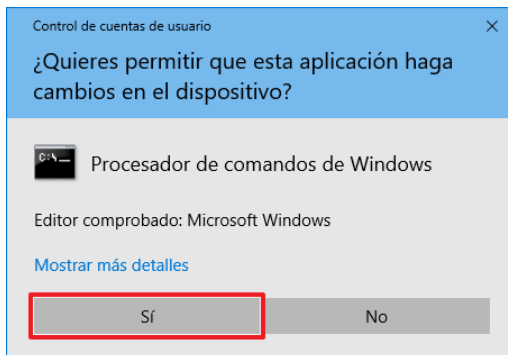
1. PREPARACIÓN DEL DOMINIO

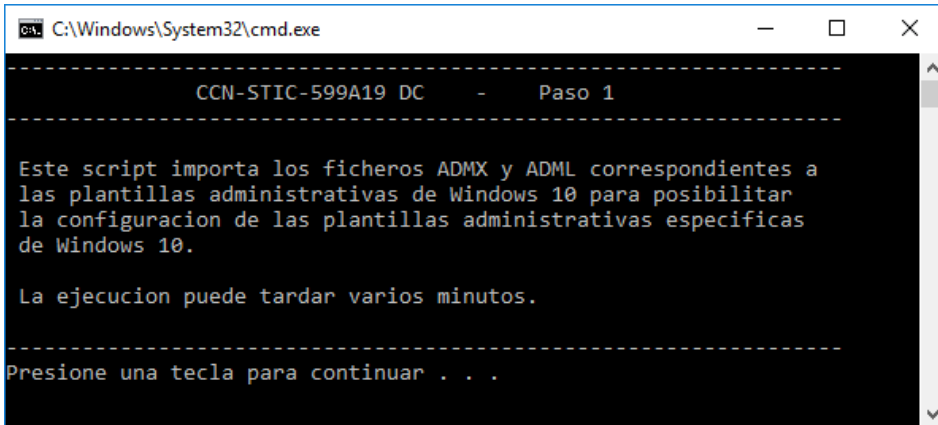
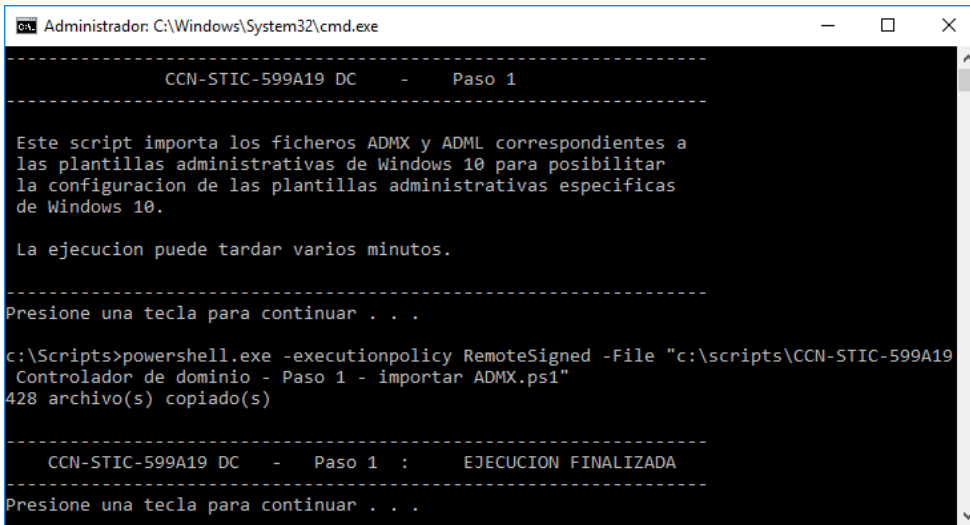
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

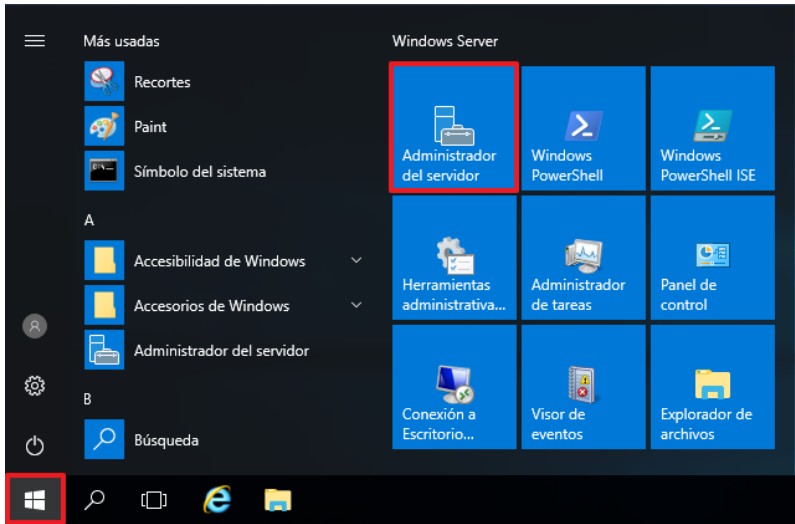
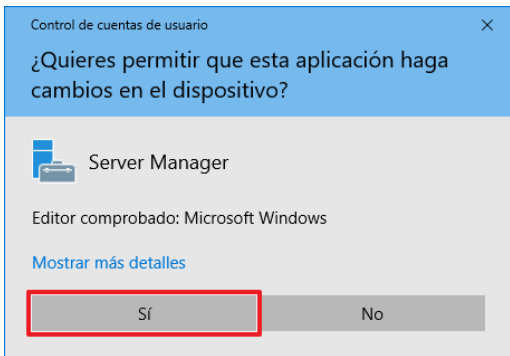
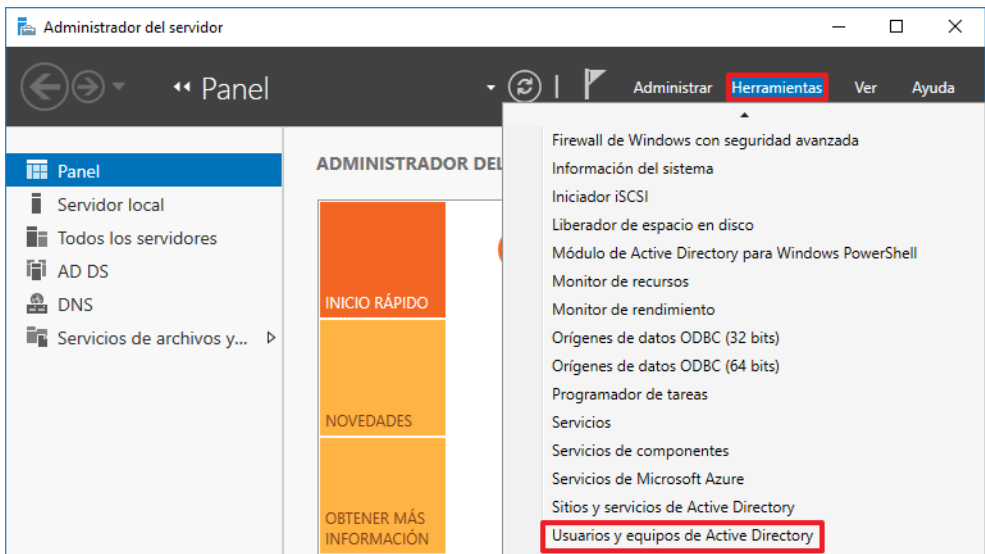
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Si no es así, aplique la guía correspondiente al controlador de dominio, antes de continuar con la aplicación de esta.

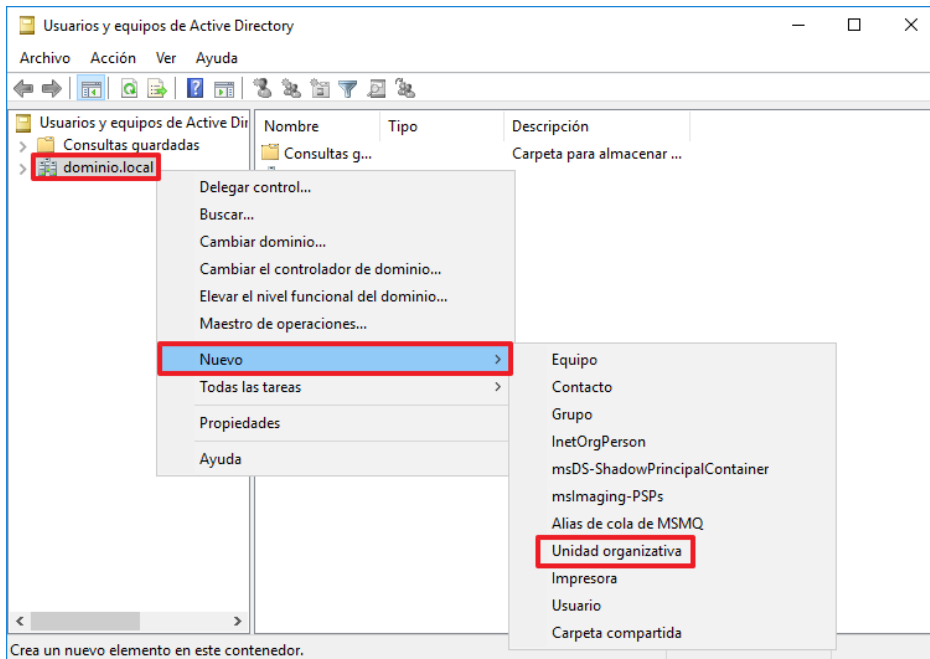
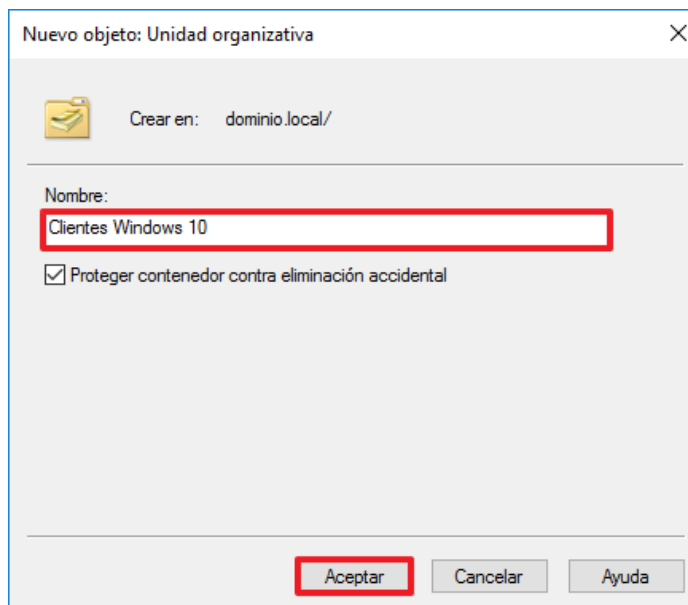
En el ejemplo, las configuraciones y capturas de pantalla han sido realizadas sobre un controlador de dominio al que se le ha instalado Windows Server 2016 y aplicado la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016.

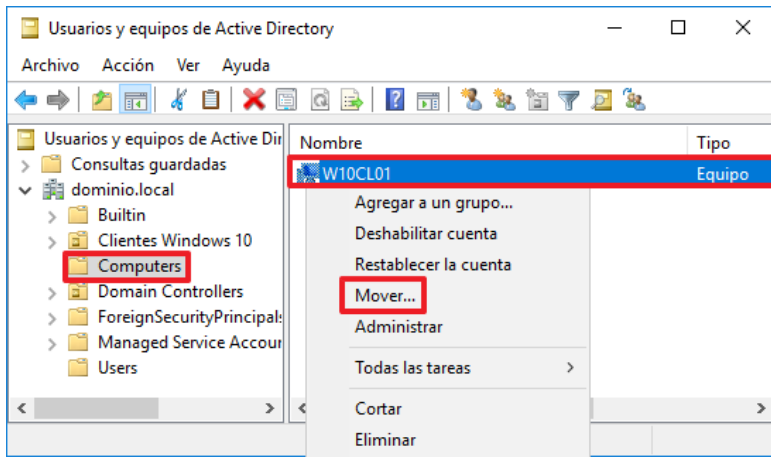
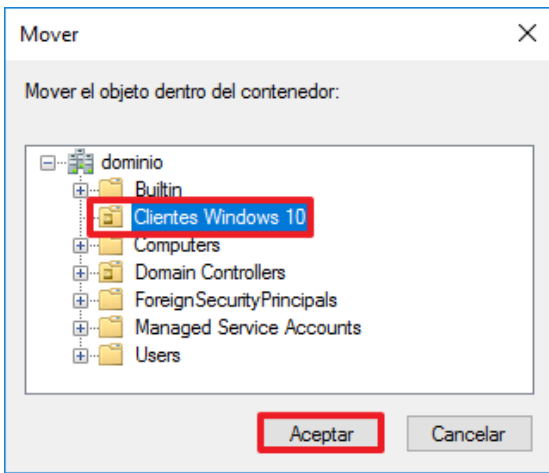
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio.
	Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".

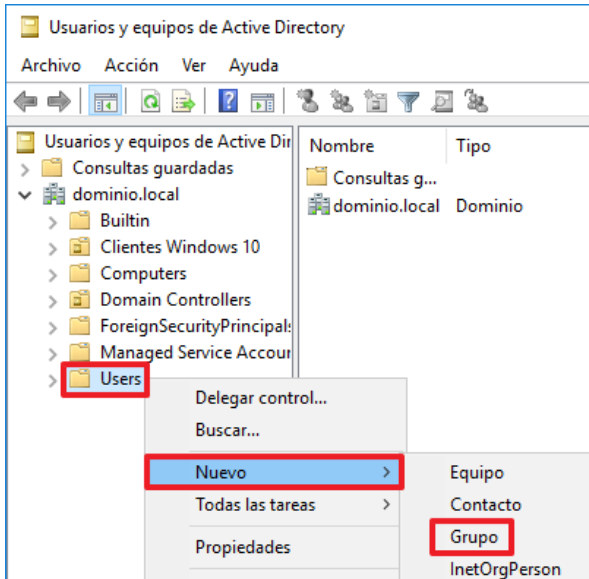
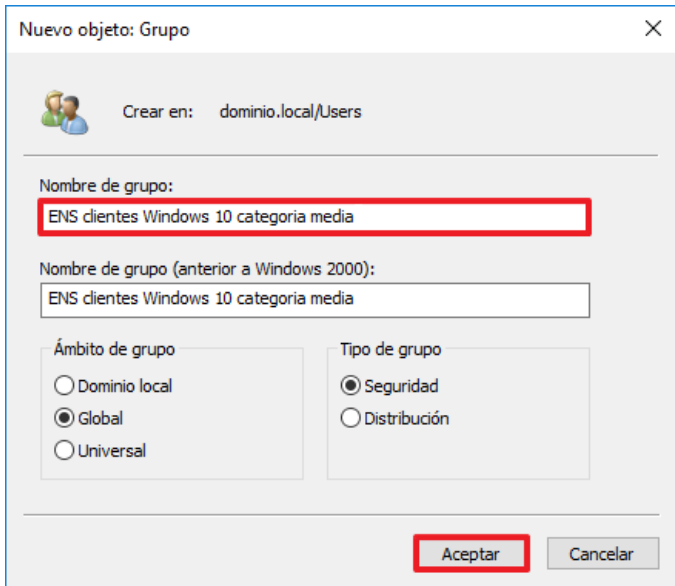
Paso	Descripción
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-599A19 ENS clientes categoria alta - DL (directorio) – CCN-STIC-599A19 ENS clientes categoria media (directorio) – CCN-STIC-599A19 ENS clientes categoria basica (directorio) – CCN-STIC-599A19 ENS Incremental portátiles categoria alta - DL - Bitlocker (directorio) – CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL.inf – CCN-STIC-599A19 ENS Incremental clientes categoria media.inf – CCN-STIC-599A19 ENS Incremental clientes categoria basica.inf – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1 – PolicyDefinitions - (directorio)
6.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
7.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 

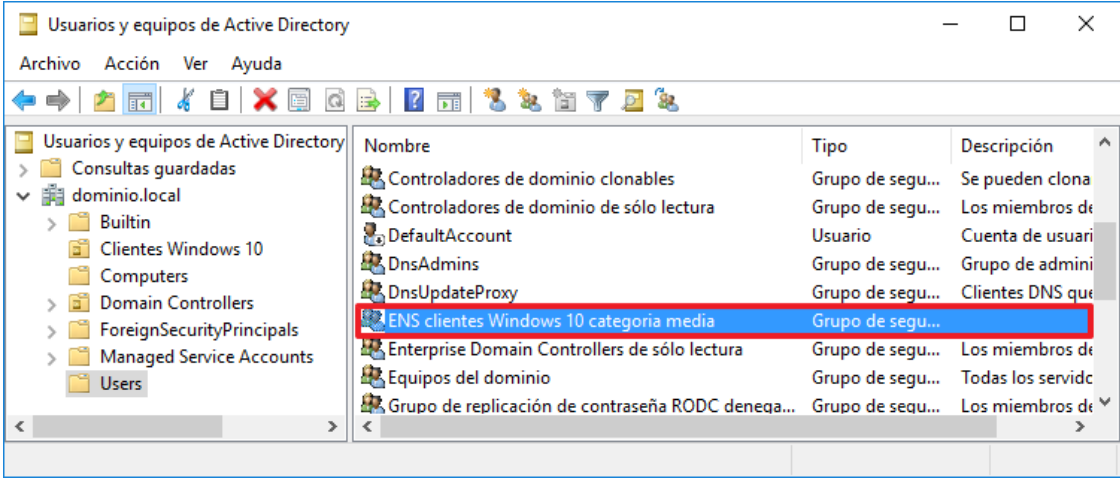
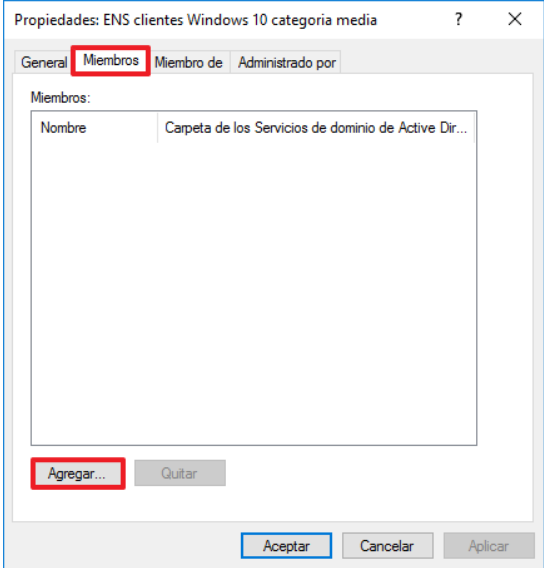
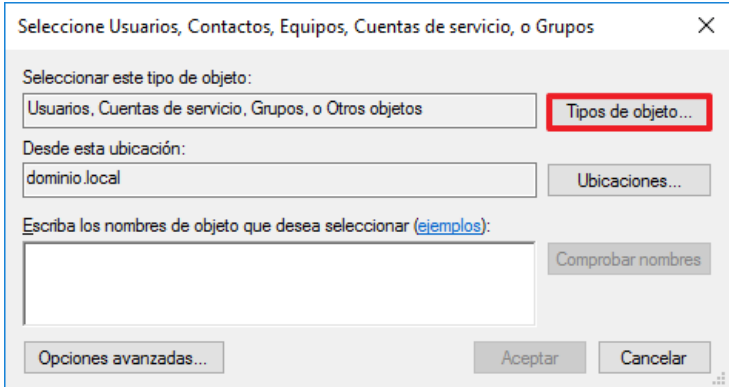
Paso	Descripción
8.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
9.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 
10.	Copie el fichero “CCN-STIC-599A19 ENS incremental clientes categoria media.inf”, almacenado en la carpeta “C:\Scripts”, al directorio “C:\Windows\Security\Templates” del Controlador de Dominio.

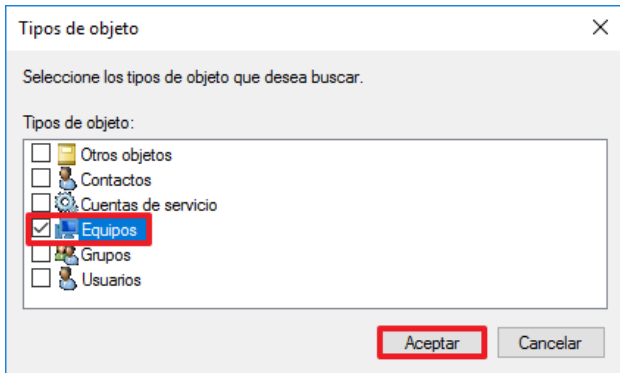
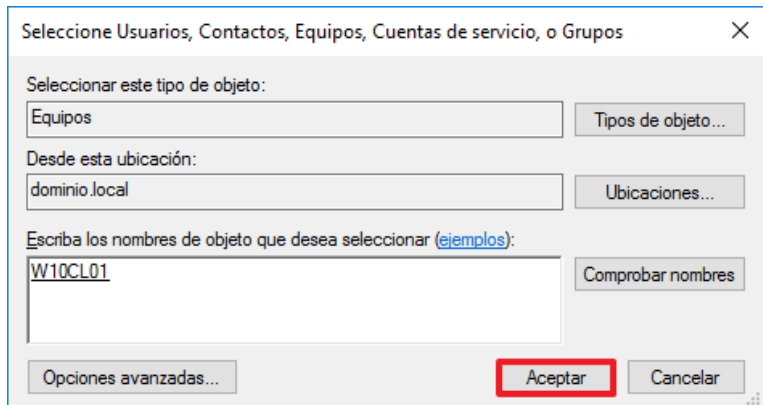
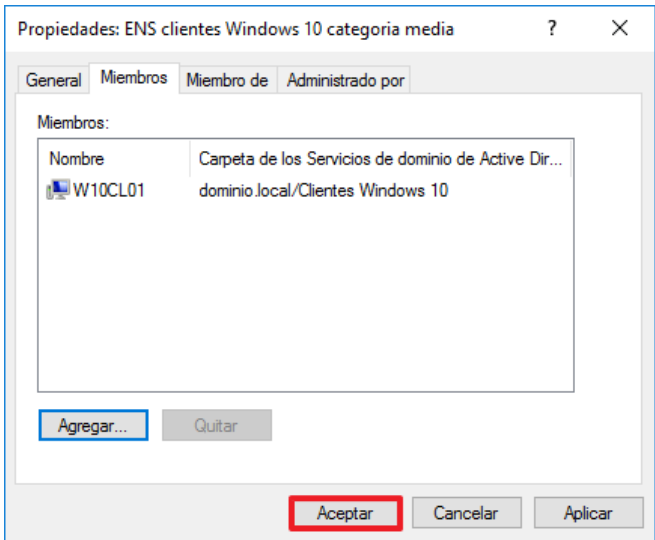
Paso	Descripción
11.	Inicie la herramienta de “Usuarios y equipos de Active Directory”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
12.	Pulse sobre el botón “Sí” para confirmar la operación. 
13.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 

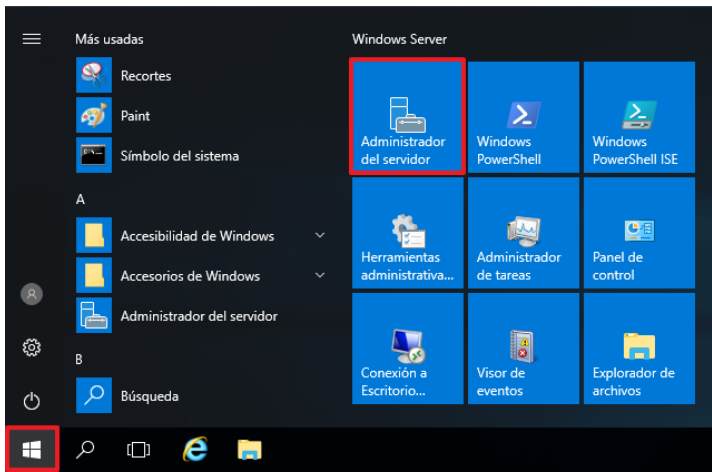
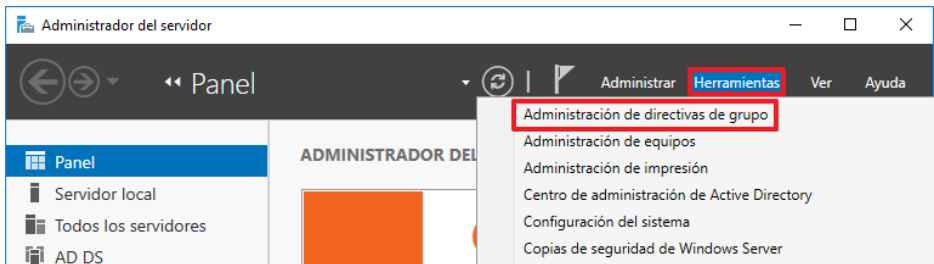
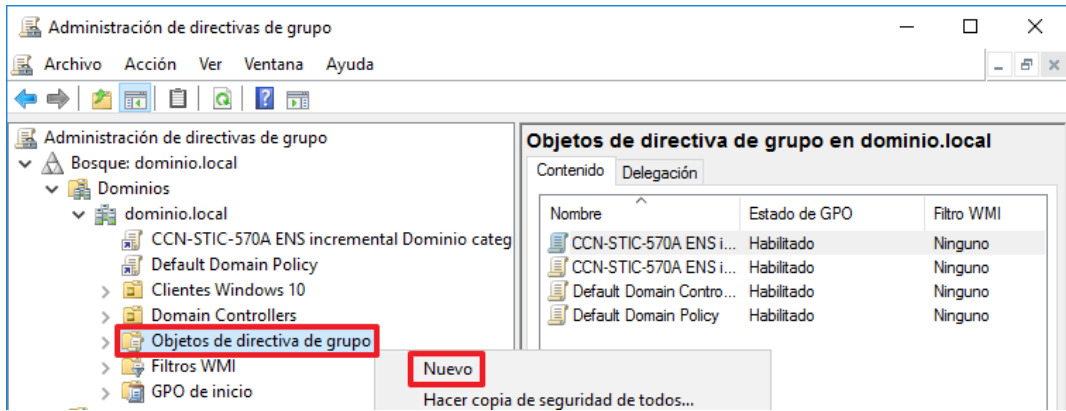
Paso	Descripción
14.	Pulse con el botón derecho sobre el dominio y seleccione “Nuevo → Unidad organizativa”. 
15.	Establezca el nombre para la unidad organizativa con los clientes Windows 10 y pulse “Aceptar”. 

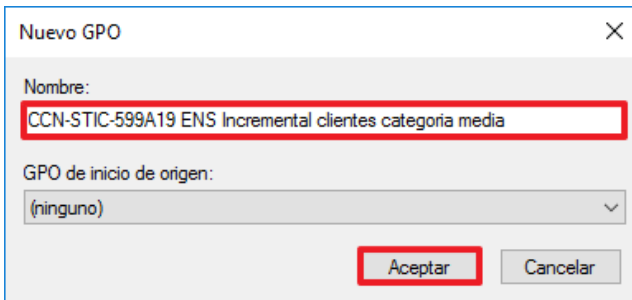
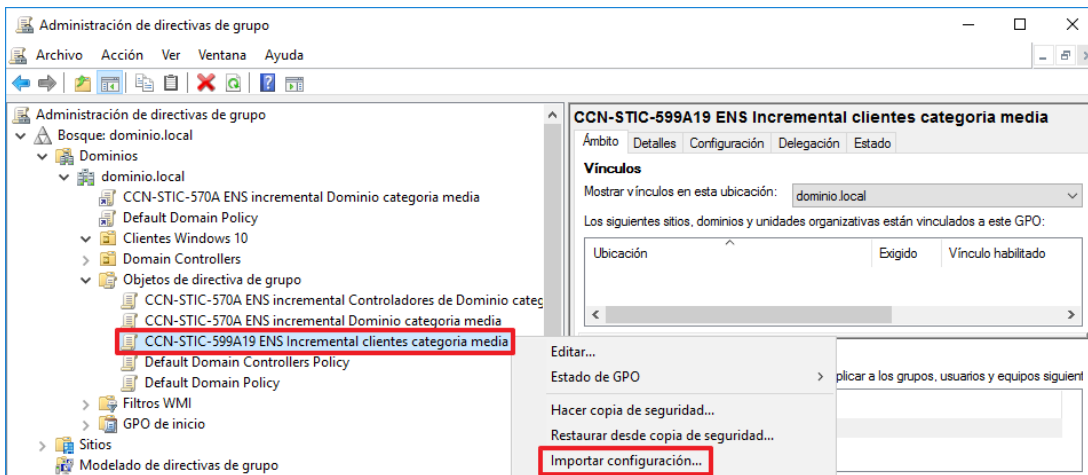
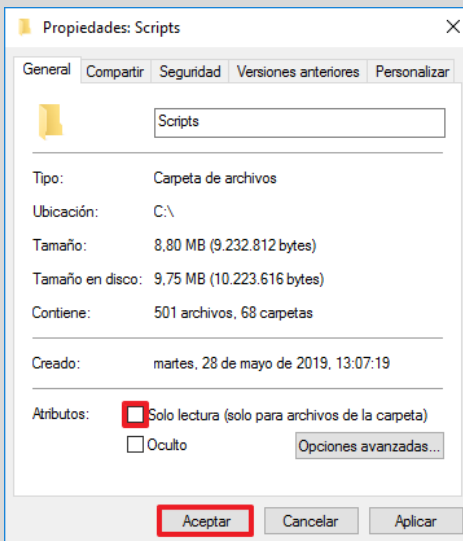
Paso	Descripción
16.	Vaya a las unidades organizativas donde se encuentren los clientes que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover...” en cada uno de ellos.  Nota: En este ejemplo se encuentra bajo la unidad organizativa “Computers”.
17.	Seleccione la unidad organizativa “Clientes Windows 10” creada anteriormente y pulse “Aceptar”.  Nota: Los siguientes pasos describen el procedimiento para crear un grupo de seguridad donde agregar los puestos de trabajo que le sean de aplicación la categoría media de seguridad según los criterios definidos del ENS. Si todos los equipos de la organización presentan la misma categoría media no hace falta la creación de dicho grupo y puede saltar al paso 26. Si por el contrario van a existir puestos de trabajo Windows 10 con categorías básica o alta, se deberán crear dichos grupos, siguiendo los pasos de los Anexos A.3 y A.4, de tal forma que la aplicación de políticas de seguridad en función de los niveles se aplique atendiendo a los criterios de pertenencia a grupo.

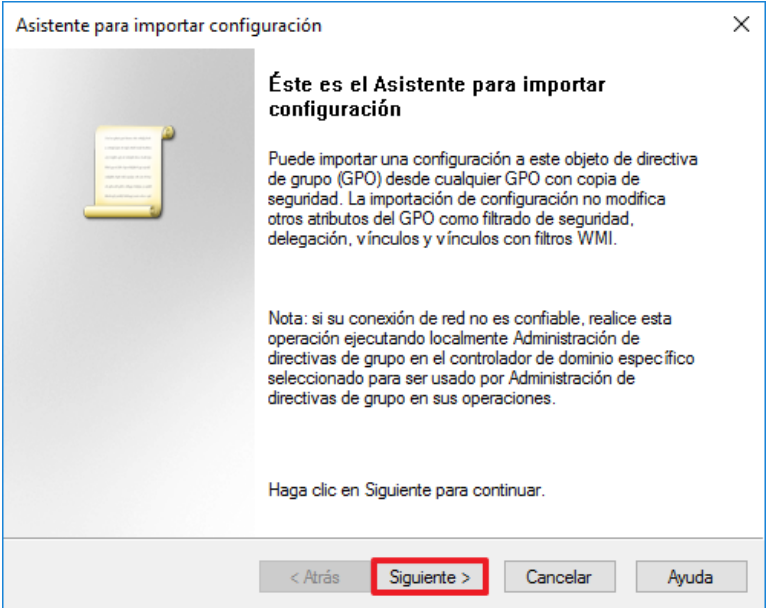
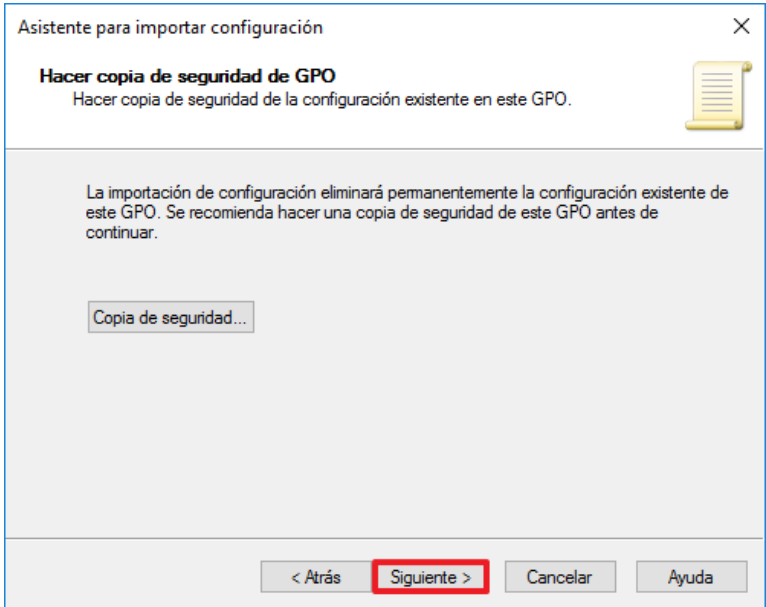
Paso	Descripción
18.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
19.	Introduzca como nombre “ENS clientes Windows 10 categoría media”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio. 

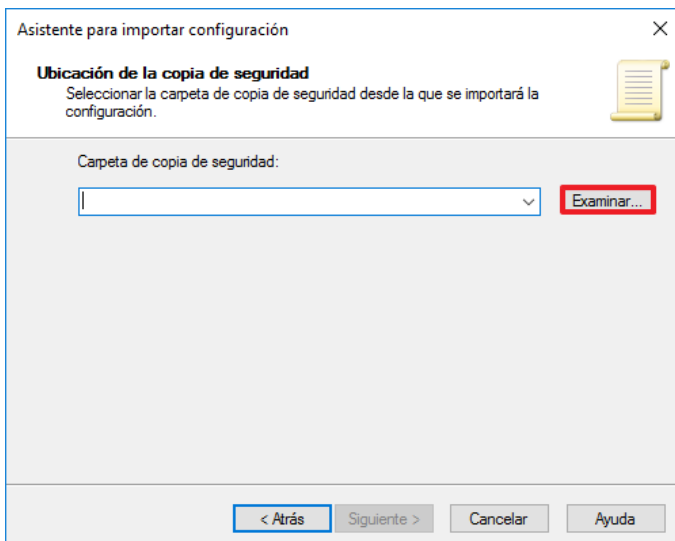
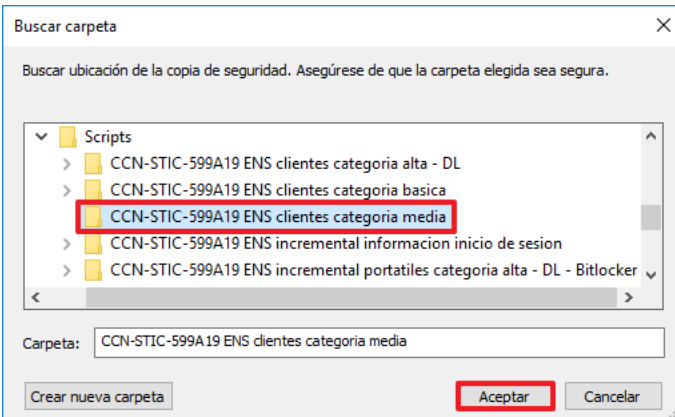
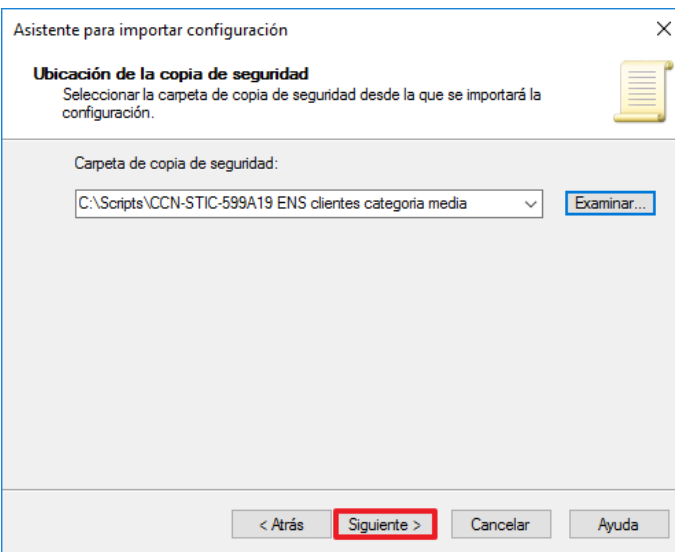
Paso	Descripción
20.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
21.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar...”. 
22.	Pulse el botón de “Tipos de objeto...”. 

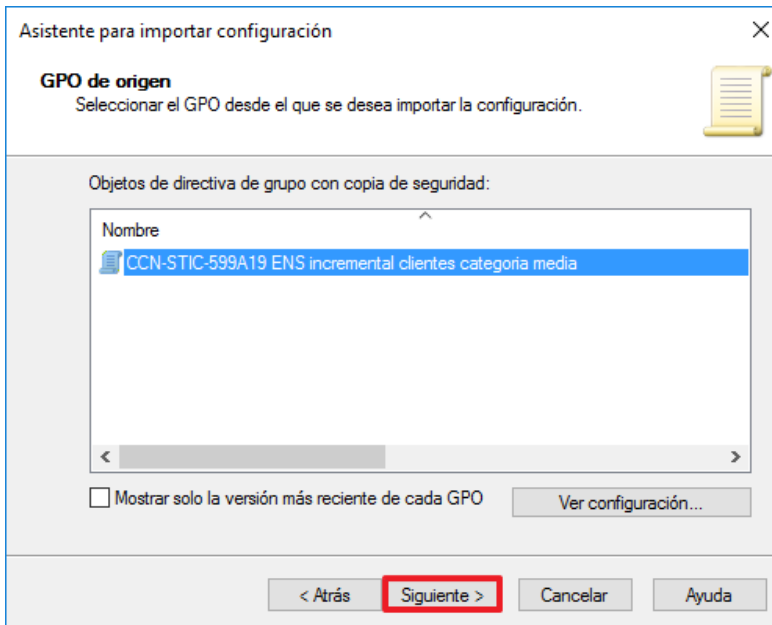
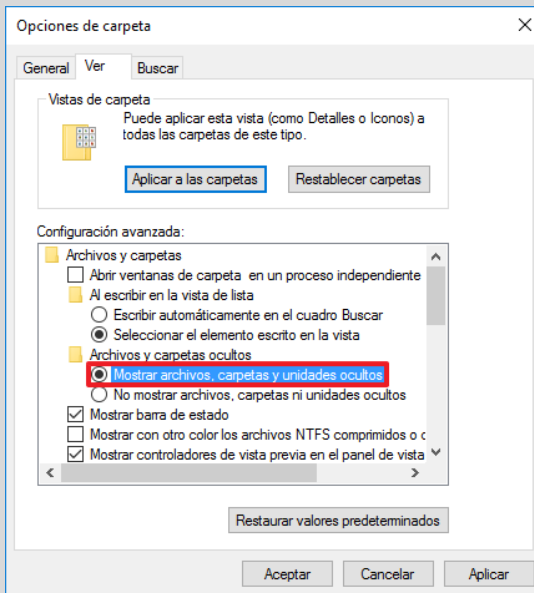
Paso	Descripción
23.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
24.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad media y pulse “Aceptar” para agregar la selección.  Nota: No agregue servidores a este grupo.
25.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 

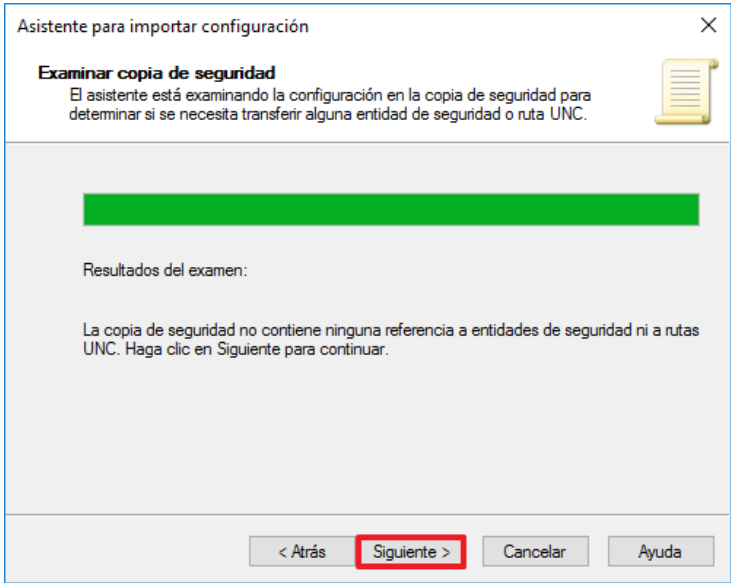
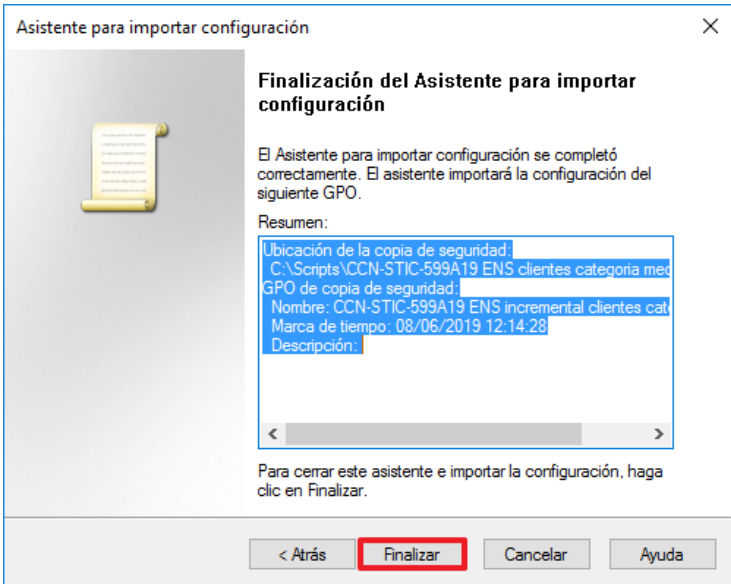
Paso	Descripción
26.	Cierre la herramienta “Usuarios y equipos e Directorio Activo”.
27.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
28.	Pulse sobre el botón “Sí” para confirmar la operación.
29.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
30.	Despliegue los contenedores pertenecientes a su dominio y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 

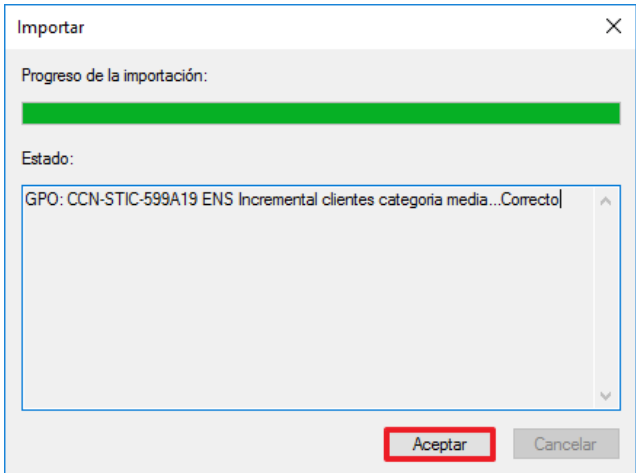
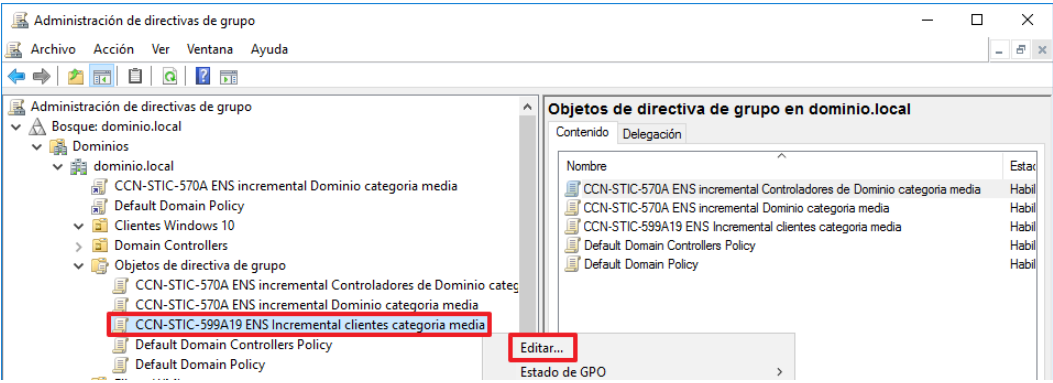
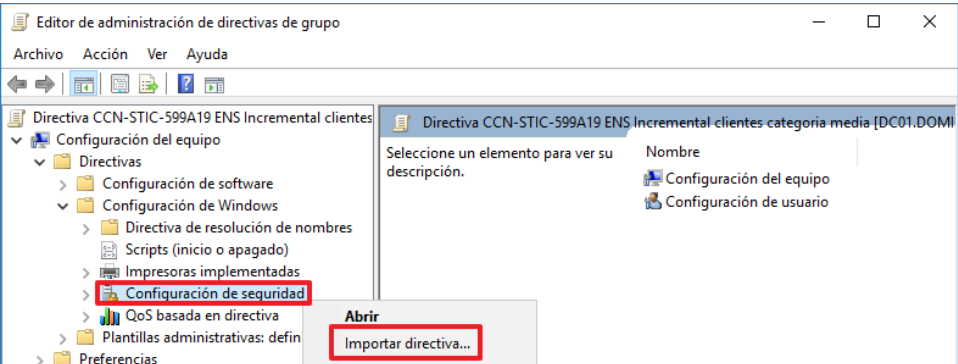
Paso	Descripción
31.	Introduzca como nombre “CCN-STIC-599A19 ENS Incremental clientes categoría media” y pulse el botón “Aceptar”. 
32.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política con el botón derecho del ratón y seleccione la opción “Importar configuración...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts”, así como los archivos dentro de sus subcarpetas, no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

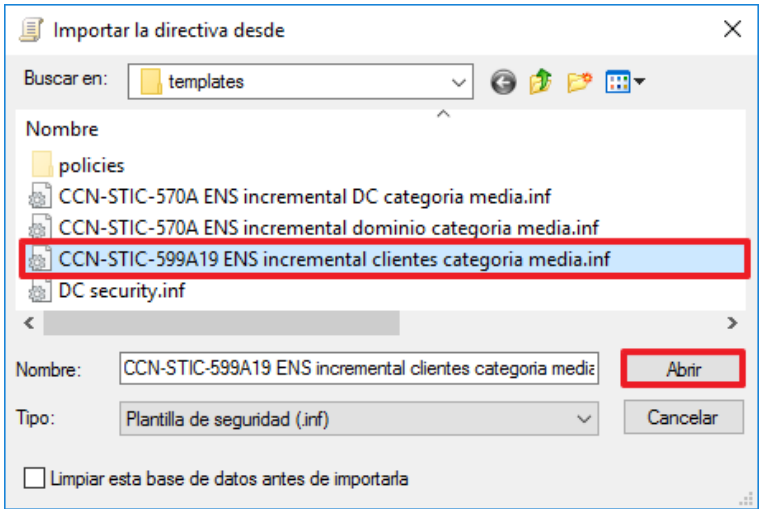
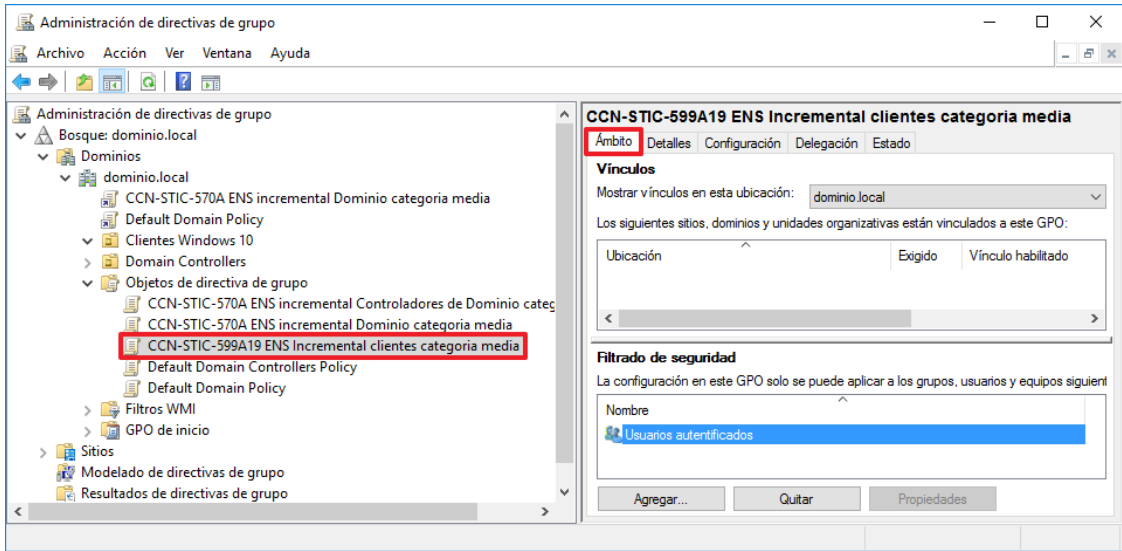
Paso	Descripción
33.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
34.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

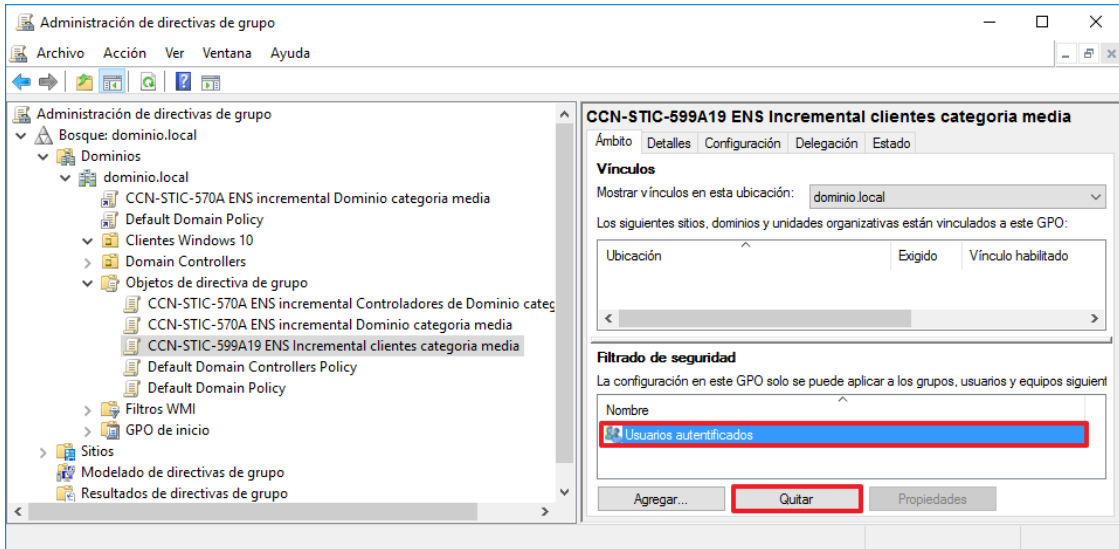
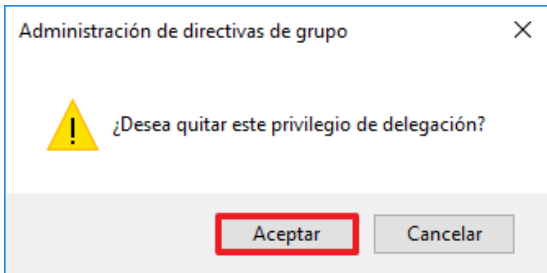
Paso	Descripción
35.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
36.	Seleccione la carpeta “CCN-STIC-599A19 ENS clientes categoria media” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
37.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

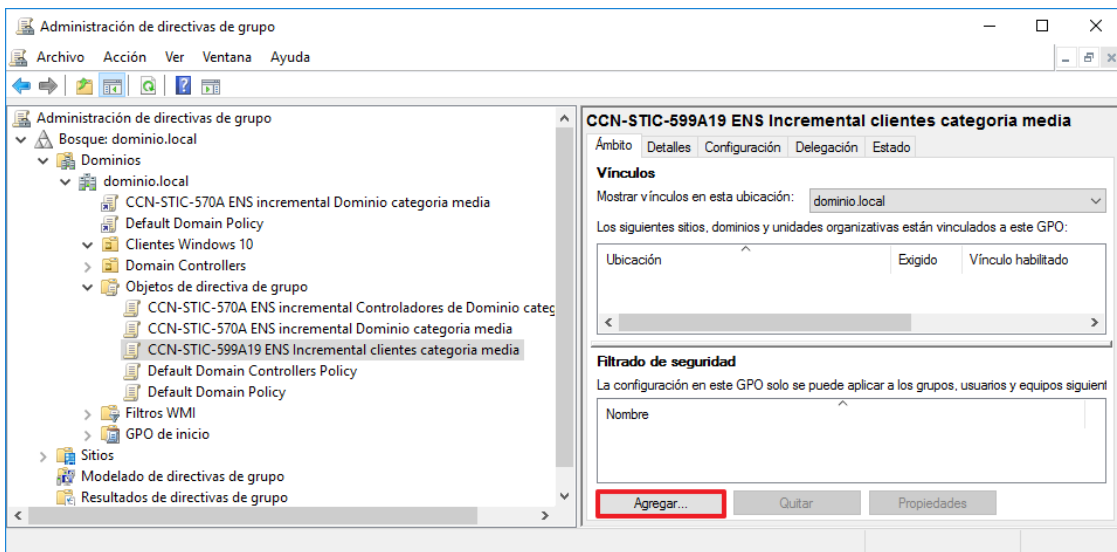
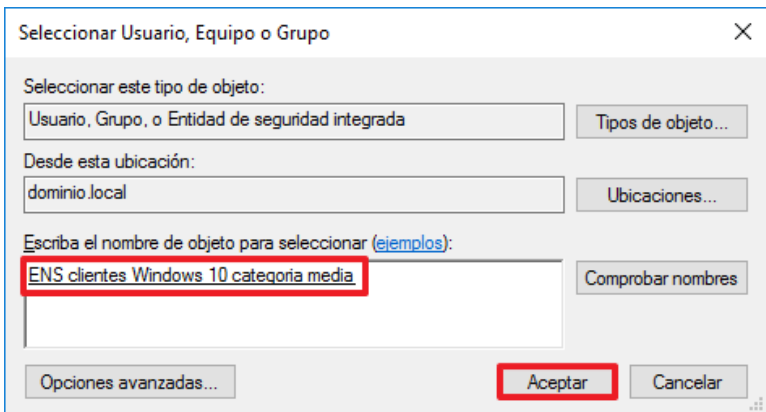
Paso	Descripción
38.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental puestos de trabajo medio” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
39.	En la pantalla de examen, pulse el botón “Siguiente >”. 
40.	Para completar el asistente pulse el botón “Finalizar”. 

Paso	Descripción
41.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración. 
42.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
43.	Una vez pulsada la opción “Editar...” se abre una ventana de “Editor de administración de directivas de grupo”. Despliegue el objeto de directiva de grupo y sitúe el cursor sobre el nodo Configuración de seguridad. “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”
44.	Pulse con el botón derecho en “Configuración de seguridad” y seleccione la opción “Importar directiva...”. 

Paso	Descripción
45.	Seleccione el fichero “CCN-STIC-599A19 ENS incremental clientes categoria media.inf” ubicado en la ruta “C:\Windows\Security\Templates”. Pulse el botón “Abrir”. 
46.	Cierre la política una vez se haya realizado la importación de la configuración de seguridad. Nota: Los siguientes pasos describen el procedimiento para asignar la política al grupo de seguridad creado en los pasos 18 a 25. Si usted creó el grupo, puesto que va a tener aplicadas diferentes categorías de seguridad en la organización para los puestos de trabajo, siga con el siguiente paso. Si no creo dicho grupo, diríjase al paso 52.
47.	Vuelva a la “Administración de directivas de grupo” y seleccione la nueva política de grupo configurada. Vaya a las opciones de ámbito que se encuentran en el panel derecho. 

Paso	Descripción
48.	En el apartado “Filtrado de seguridad”, seleccione “Usuarios autenticados” y pulse el botón “Quitar”. 
49.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
50.	Pulse ahora sobre el botón “Agregar...”. 
51.	Introduzca como nombre “ENS clientes Windows 10 categoria media”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
52.	La política se encuentra ya creada correctamente. No obstante, no se aplicará hasta más adelante, una vez haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente Anexo.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA MEDIA

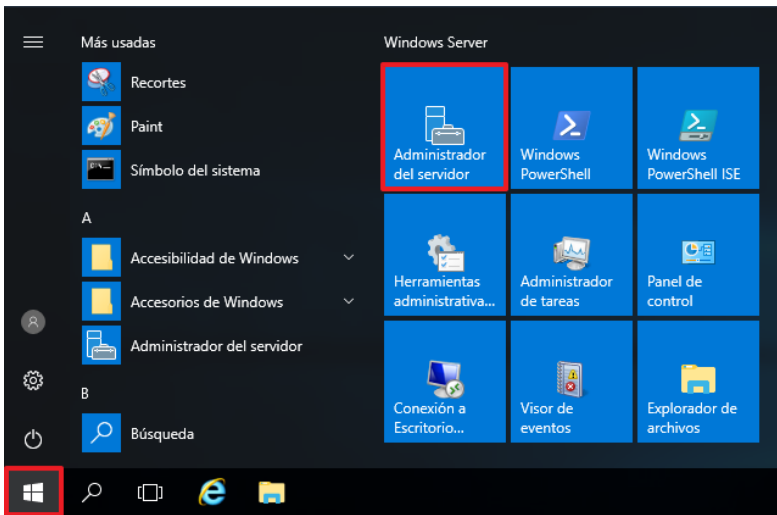
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y por lo tanto deben valorarse con respecto a la aplicación de la presente configuración. La plantilla de seguridad que se ha configurado tiene en consideración los puntos tratados en el Esquema Nacional de seguridad para la categoría media. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina, como por ejemplo lo relativo al uso de privilegios.

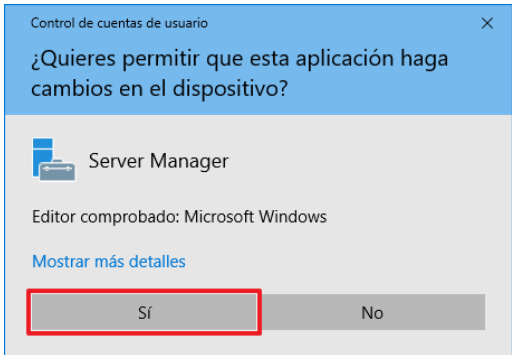
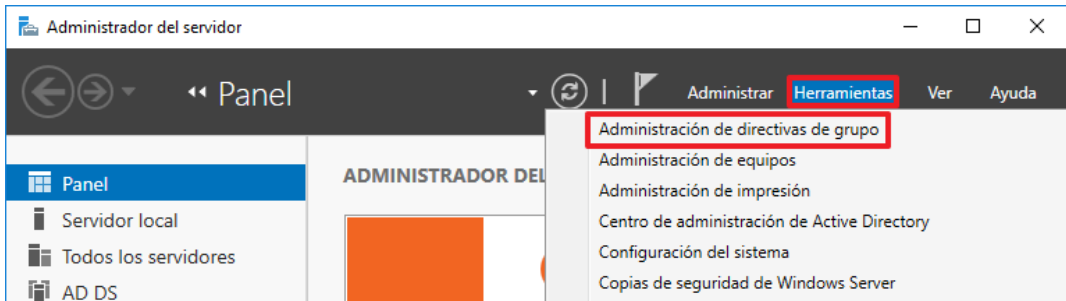
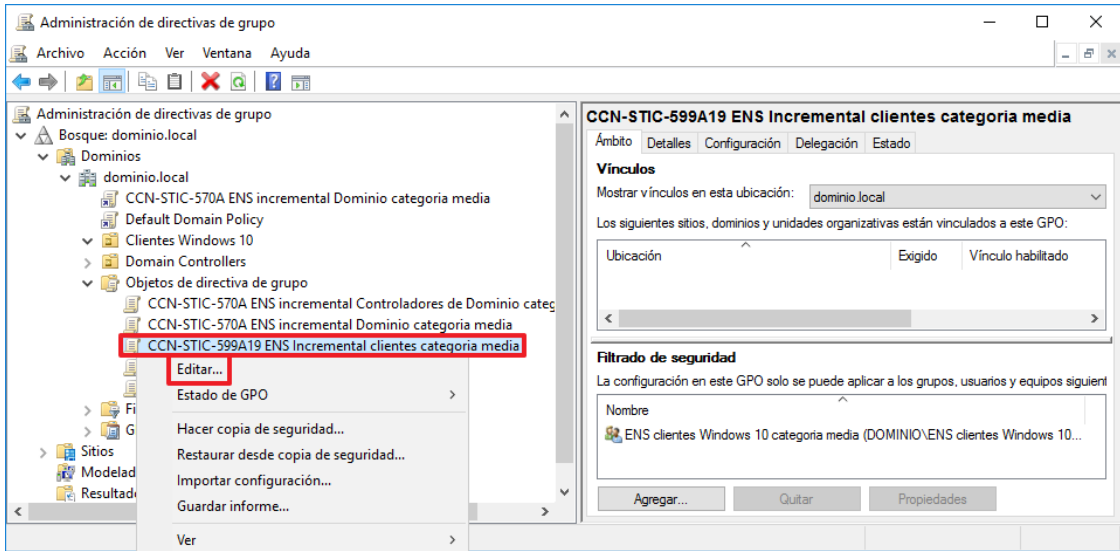
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

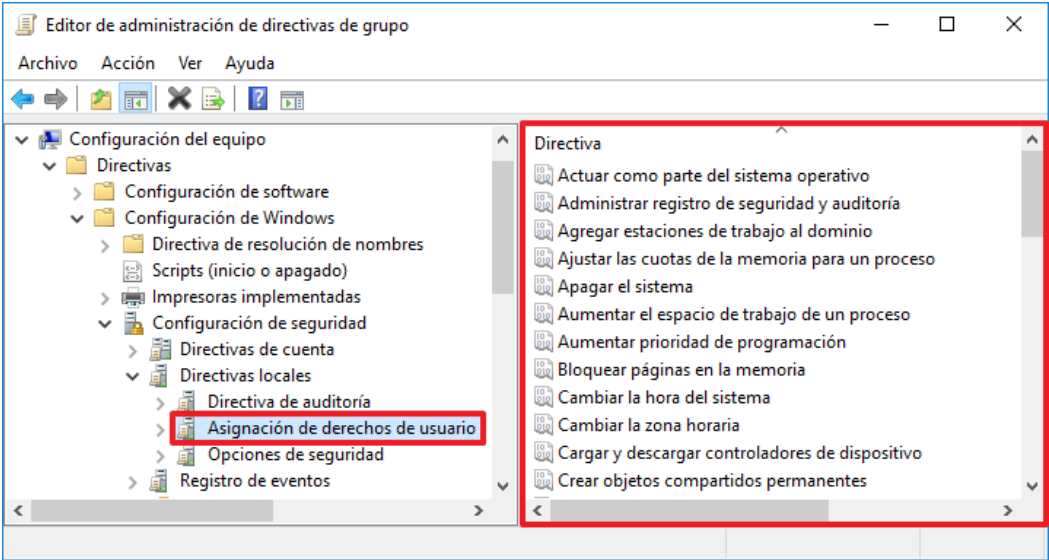
Los objetos de políticas de grupo para puestos de trabajo especifican unos derechos de usuario siguiendo planteamientos de seguridad siguiendo los principios de mínimos privilegios y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas.

Si esto fuera así deberá realizar las modificaciones sobre el objeto de política creado en el punto previo.

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

Paso	Descripción
53.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
54.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
55.	Edite la política de grupo correspondiente. Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

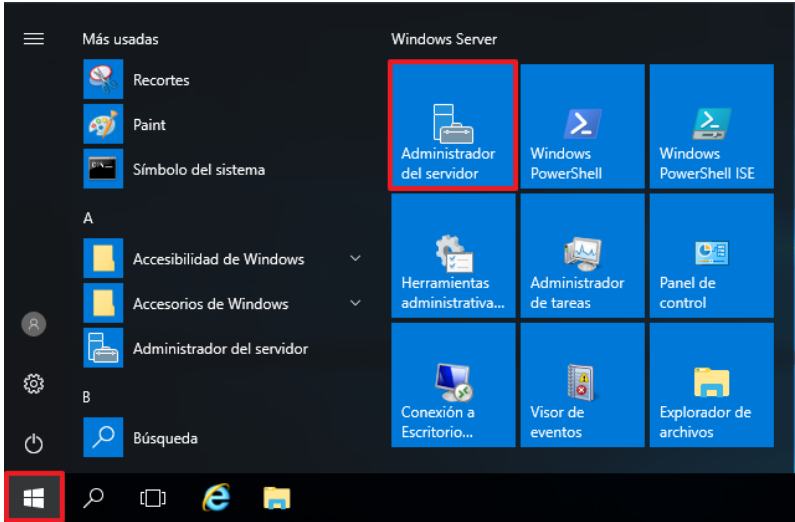
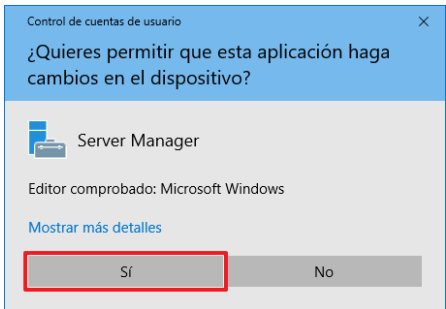
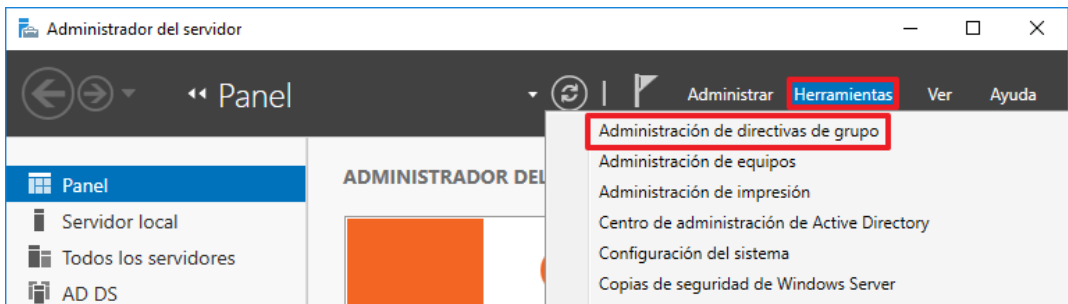
Paso	Descripción
56.	Pulse sobre el botón “Sí” para confirmar la operación. 
57.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
58.	Seleccione la política creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 

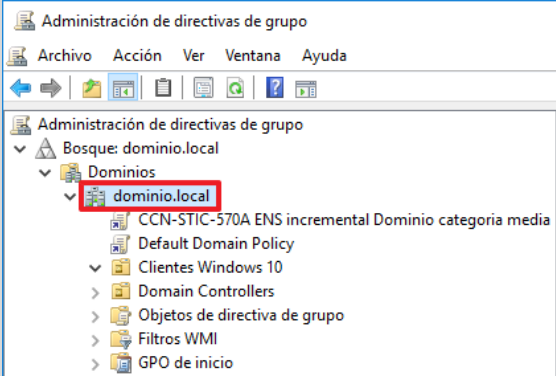
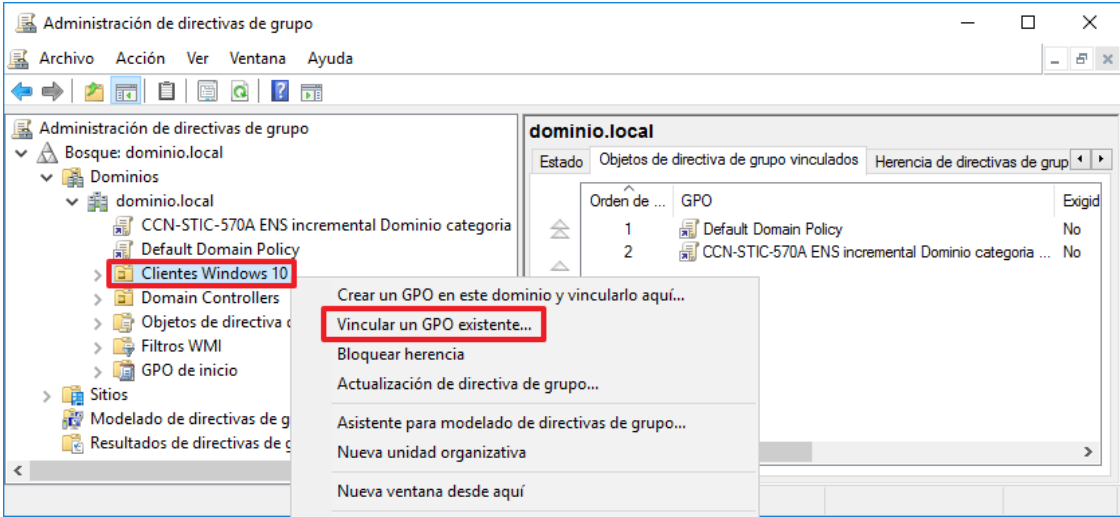
Paso	Descripción
59.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana del editor de administración de directivas de grupo.

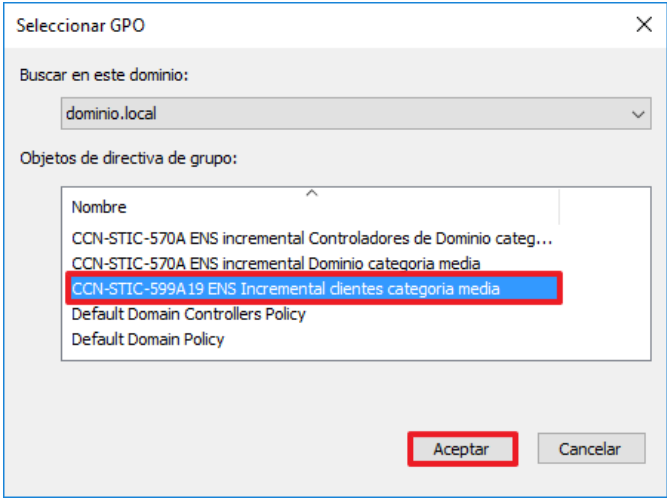
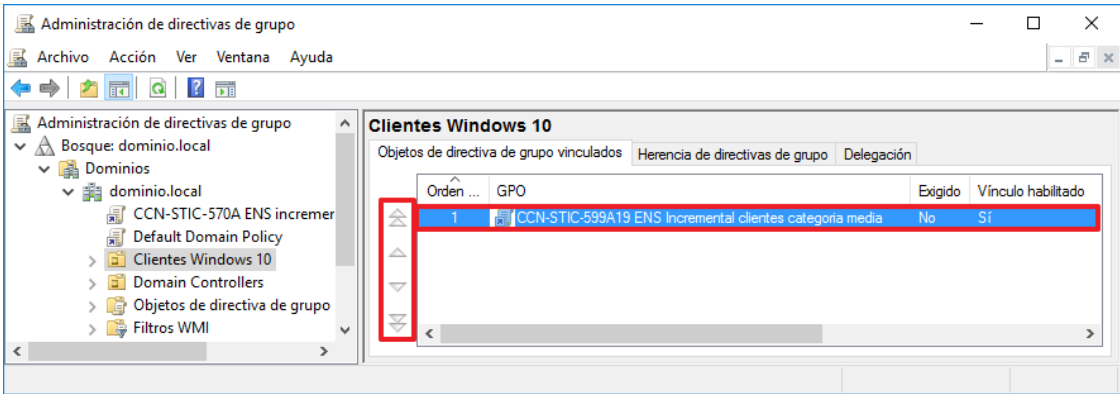
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, una vez que se han tenido en consideración las condiciones definidas en el punto previo.

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

Paso	Descripción
64.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
65.	Pulse sobre el botón "Sí" para confirmar la operación. 
66.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo". 
67.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es "dominio.local".

Paso	Descripción
68.	Identifique las ubicaciones donde se encuentran los Clientes Windows 10 que les son de aplicación las condiciones de seguridad de categoría media, según estipula el ENS. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC ENS incremental clientes categoria media”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” lugar donde se encuentran ubicados los clientes existentes en este escenario. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 
69.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
70.	Seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria media” y pulse el botón “Aceptar”. 
71.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria media” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dichas Unidades Organizativas. 
72.	Cierre la herramienta “Administración de directivas de grupo”.
73.	Elimine la carpeta “C:\Scripts”.
74.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Es posible que bajo determinadas condiciones pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado Microsoft propone como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

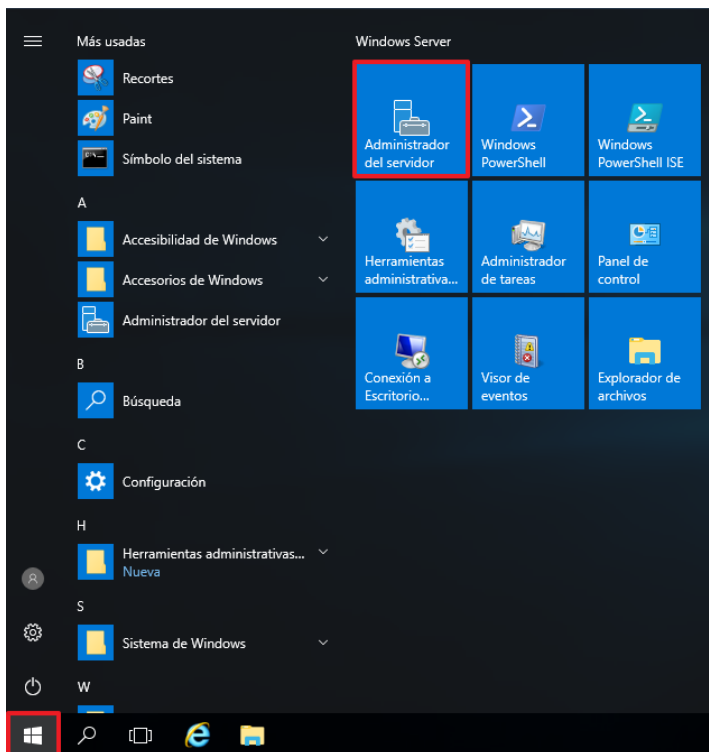
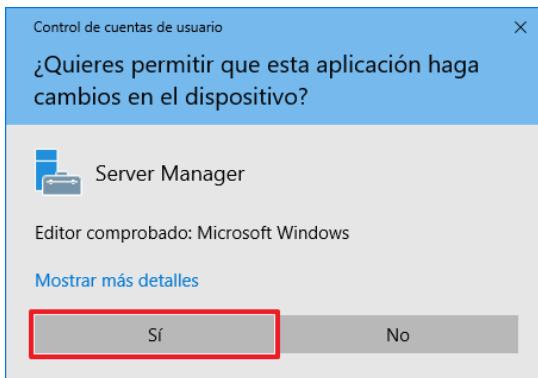
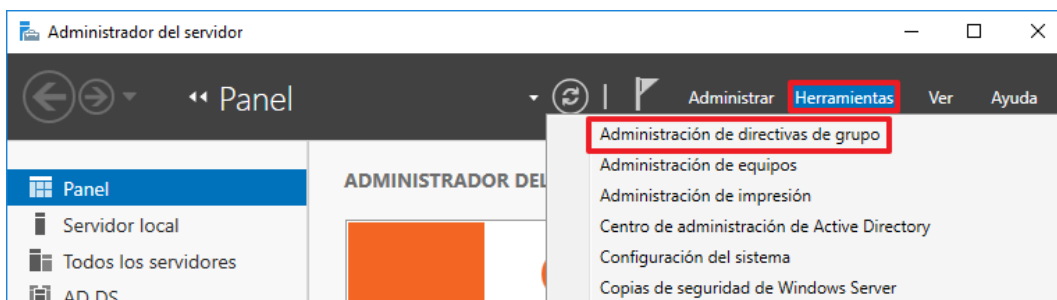
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría media, aunque con los criterios más laxos de los aplicables.

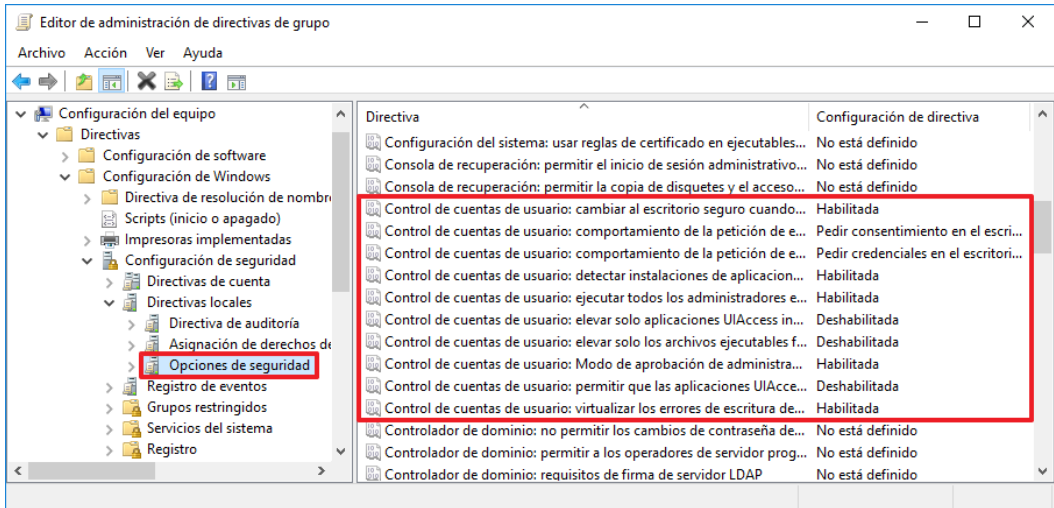
No obstante, y ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría media por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación en los clientes que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

4.1. CONTROL DE CUENTAS DE USUARIO

Paso	Descripción
75.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
76.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
77.	Identifique los puestos de trabajo que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS clientes Windows 10 categoría media”. En el caso de que no haya tenido que crear dicho grupo siga al paso siguiente.
78.	Cree un nuevo grupo de forma similar al ya creado, siguiendo los pasos 18 a 25 del presente Anexo.

Paso	Descripción
79.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
80.	Pulse sobre el botón "Sí" para confirmar la operación. 
81.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo". 

Paso	Descripción
82.	Cree una nueva política de grupo con un nombre diferente (p.e. “CCN-STIC-599A19 ENS incremental clientes categoria media incidencias UAC”) que será asignable a los clientes Windows 10 con una categoría media e incidencias de funcionalidad del UAC. Siga para ello los pasos 27 a 46. Incluya al nuevo grupo de puestos de trabajo creados en lugar del grupo “ENS clientes Windows 10 categoria media” creado en el proceso previo.
83.	Edite el nuevo objeto de GPO “CCN-STIC-599A19 ENS incremental clientes categoria media incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar...” del menú contextual.
84.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”
85.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
86.	Realice las modificaciones oportunas.
87.	Cierre la política.
88.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Debe tener en consideración que, si ha alterado la política de control de cuentas y esta es menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presenten funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

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 GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

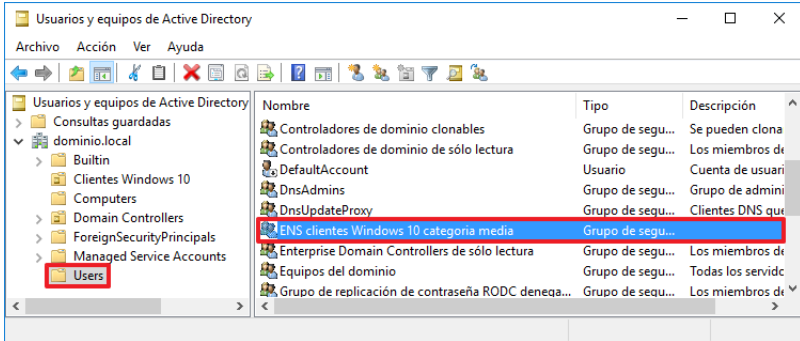
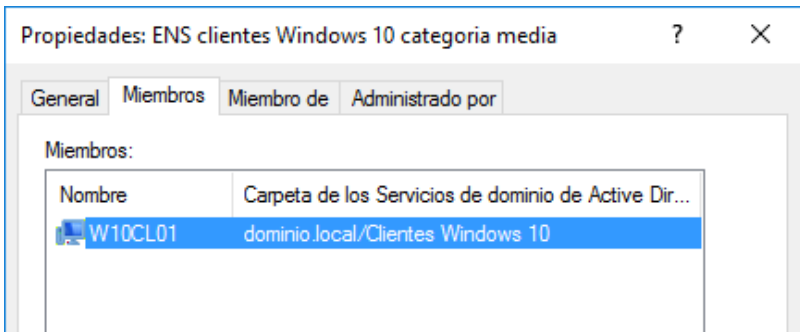
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

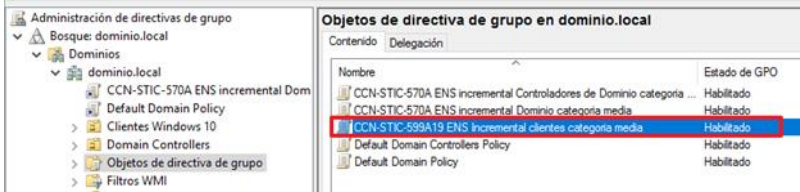
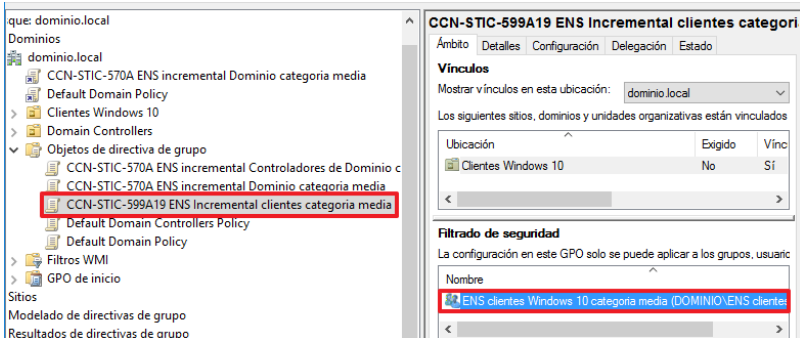
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

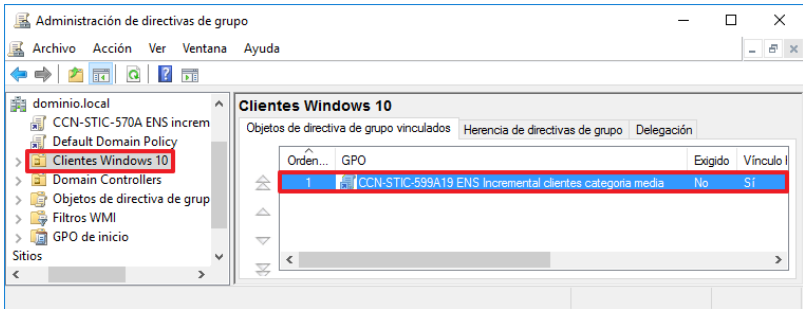
También deberá ejecutar una parte del análisis en los clientes Windows 10 a los que se les haya aplicado la configuración de seguridad de categoría media. En éstos deberá ejecutar la siguiente aplicación.

- a) Conjunto resultante de directivas (rsop.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creado el grupo “ENS clientes Windows 10 categoria media” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory” desde: “Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory” Seleccione el contenedor “Users”, situada en “[Su dominio] → Users” y a continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS clientes Windows 10 categoria media”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.
3. Verifique que los clientes que han sido catalogados como de categoría de seguridad media, siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS clientes Windows 10 categoria media”.		Pulse doble clic sobre el grupo “ENS clientes Windows 10 categoria media” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los clientes que corresponden a esta categoría de seguridad aparecen en el listado.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.

Comprobación	OK/NOK	Cómo hacerlo						
4. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” ha sido creado y está habilitado.		Ejecute la herramienta “Administrador de directivas de grupo” desde: “Menú inicio → Herramientas administrativas → Administrador de directivas de grupo” Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo” Verifique que está creado el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” y que en la columna “Estado de la GPO” figura como habilitado. 						
		<table border="1"> <thead> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>CCN-STIC-599A19 ENS incremental clientes categoria media</td><td>Habilitado</td><td></td></tr> </tbody> </table>	Directiva	Valor	OK/NOK	CCN-STIC-599A19 ENS incremental clientes categoria media	Habilitado	
Directiva	Valor	OK/NOK						
CCN-STIC-599A19 ENS incremental clientes categoria media	Habilitado							
5. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” tiene definido el Ámbito al grupo “ENS clientes Windows 10 categoría media”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS clientes Windows 10 categoría media”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.						

Comprobación	OK/NOK	Cómo hacerlo															
6. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” es aplicado a todos aquellos equipos Windows 10 que le son de aplicación las condiciones de categoría media.		Evalúe que la política de seguridad es aplicada en un orden superior a otras políticas aplicables a los puestos de trabajo en todas aquellas ubicaciones donde se encuentren clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría media. En el árbol de la izquierda, seleccione la ubicación donde se encuentren los clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría media: 															
7. Verifique la directiva de contraseñas en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Pulse el botón derecho del ratón y seleccione la opción “Editar...”. Se abrirá el editor de directivas de grupo. Deberá navegar sobre los elementos del árbol de directorios para verificar las distintas configuraciones. Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas” <table border="1"> <thead> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Exigir historial de contraseñas</td><td>24</td><td></td></tr> <tr> <td>Longitud mínima de la contraseña</td><td>10</td><td></td></tr> <tr> <td>Vigencia máxima de la contraseña</td><td>60</td><td></td></tr> <tr> <td>Vigencia mínima de la contraseña</td><td>2</td><td></td></tr> </tbody> </table>	Directiva	Valor	OK/NOK	Exigir historial de contraseñas	24		Longitud mínima de la contraseña	10		Vigencia máxima de la contraseña	60		Vigencia mínima de la contraseña	2	
Directiva	Valor	OK/NOK															
Exigir historial de contraseñas	24																
Longitud mínima de la contraseña	10																
Vigencia máxima de la contraseña	60																
Vigencia mínima de la contraseña	2																

Comprobación	OK/NOK	Cómo hacerlo		
8. Verifique la directiva de bloqueo de cuenta en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de bloqueo de cuenta”		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	60	
		Restablecer el bloqueo de cuenta después de	30	
		Umbral del bloqueo de cuenta	8	
9. Verifique las directivas de auditoría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
10.Verifique la asignación de derechos de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	BUILTIN\Administradores	
		Ajustar las cuotas de la memoria para un proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores	
		Apagar el sistema	BUILTIN\Usuarios, BUILTIN\Administradores	
		Aumentar el espacio de trabajo de un proceso	BUILTIN\Usuarios, NT AUTHORITY\SERVICIO LOCAL, BUILTIN\Administradores	
		Aumentar prioridad de programación	BUILTIN\Administradores	
		Cambiar la hora del sistema	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cambiar la zona horaria	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cargar y descargar controladores de dispositivo	BUILTIN\Administradores	
		Crear objetos compartidos permanentes		
		Crear un archivo de paginación	BUILTIN\Administradores	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Crear un objeto símbolo (token)	
		Crear vínculos simbólicos	BUILTIN\Administradores
		Denegar el acceso a este equipo desde la red	BUILTIN\Invitados, NT AUTHORITY\ANONYMOUS LOGON
		Denegar el inicio de sesión como servicio	BUILTIN\Invitados
		Denegar el inicio de sesión como trabajo por lotes	BUILTIN\Invitados
		Denegar el inicio de sesión local	BUILTIN\Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	BUILTIN\Administradores
		Forzar cierre desde un sistema remoto	BUILTIN\Administradores
		Generar auditorías de seguridad	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Generar perfiles de un solo proceso	BUILTIN\Administradores
		Generar perfiles del rendimiento del sistema	BUILTIN\Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	
		Hacer copias de seguridad de archivos y directorios	BUILTIN\Administradores
		Iniciar sesión como proceso por lotes	
		Iniciar sesión como servicio	
		Modificar la etiqueta de un objeto	
		Modificar valores de entorno firmware	BUILTIN\Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Omitir comprobación de recorrido	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores, NT AUTHORITY\Usuarios autenticados	
		Permitir el inicio de sesión local	BUILTIN\Usuarios, BUILTIN\Administradores	
		Permitir inicio de sesión a través de Servicios de Escritorio remoto		
		Realizar tareas de mantenimiento del volumen	BUILTIN\Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red	
		Restaurar archivos y directorios	BUILTIN\Administradores	
		Tener acceso a este equipo desde la red	BUILTIN\Usuarios, BUILTIN\Administradores	
		Tomar posesión de archivos y otros objetos	BUILTIN\Administradores	
11.Verifique las opciones de seguridad en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	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 enumeraciones anónimas de cuentas SAM	Habilitado
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitado
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitado
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitado
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitado
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitado
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitado
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitado
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitado
		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

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		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	Habilitado
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitado
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitado
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitado
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitado
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitado
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitado
		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.
		Cuentas: estado de la cuenta de invitado	Deshabilitado
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitado
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitado
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitado
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		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	Habilitado
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitado
		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	Habilitado
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitado
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitado
		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)	Habilitado
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitado
		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	Habilitado
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado
		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
12.Verifique el registro de eventos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro de seguridad	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro del sistema	Habilitado	
13.Verifique los servicios del sistema definidos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema” Nota: 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 para cada servicio. En la ventana del editor de administración de directivas de grupo 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	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Agente de conexión de red	NcbService	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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	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		
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	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	Manual	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		wuauserv	Manual	Configurado	
Windows Update Medic Service		WaaSMedicSvc	Manual	Configurado	
Xbox Accessory Management Service		XboxGipSvc	Deshabilitado	Configurado	
14.Verifique los valores del sistema de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos” Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".			
Archivo			Usuario	Permiso	OK/NOK
%ProgramFiles%\Netmeeting			Administradores	Control total	
			SYSTEM	Control total	
%Public%\			Administradores	Control total	
			SYSTEM	Control total	
			Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo	Usuario	Permiso	OK/NOK	
%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\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		
15.Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
16.Verifique la directiva de almacén digital en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Almacén digital”			

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitado	
17.Verifique la directiva de Antivirus en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitado	
18.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
19.Verifique las directivas de biometría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
20.Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
21.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
22.Verifique las directivas de reproducción automática en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar reproducción automática	Habilitado (Todas las unidades)	
		Establece el comportamiento predeterminado para la ejecución automática	Habilitado (No ejecutar ningún comando de ejecución automática)	

Comprobación	OK/NOK	Cómo hacerlo		
23.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar Windows SmartScreen de Windows defender	Habilitado (Advertir e impedir la omisión)	
24.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
25.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
26.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de Internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
27.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
28.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
29.Verifique las directivas de OneDrive en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	
30.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
	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		Deshabilitado	
31.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”			
	Directiva		Valor	OK/NOK
	Modo de descarga		Habilitado (Solo HTTP (0))	
32.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”			
	Directiva		Valor	OK/NOK
	Permitir que las aplicaciones de Windows accedan a dispositivos de confianza		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 accedan a la información de diagnóstico sobre otras aplicaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	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 controlen las radios	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)

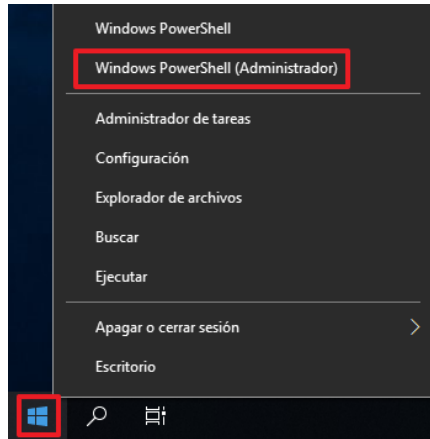
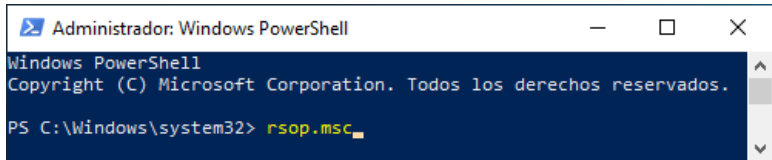
Comprobación	OK/NOK	Cómo hacerlo		
33.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”		
		Directiva	Valor	OK/NOK
		No volver a mostrar notificaciones de comentarios	Habilitado	
		Permitir telemetría	Habilitado	
34.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”		
		Directiva	Valor	OK/NOK
		Permitir acceso a Shell remoto	Deshabilitado	

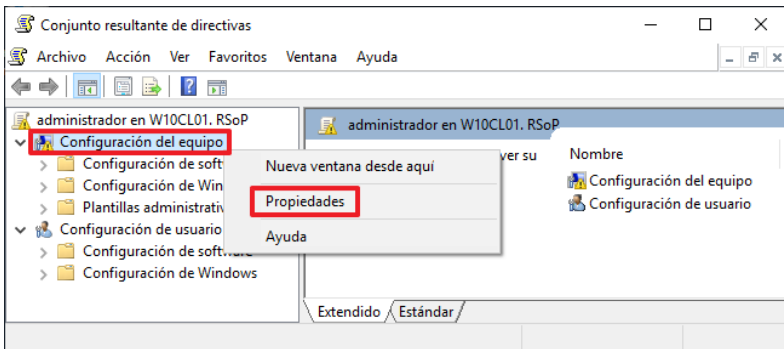
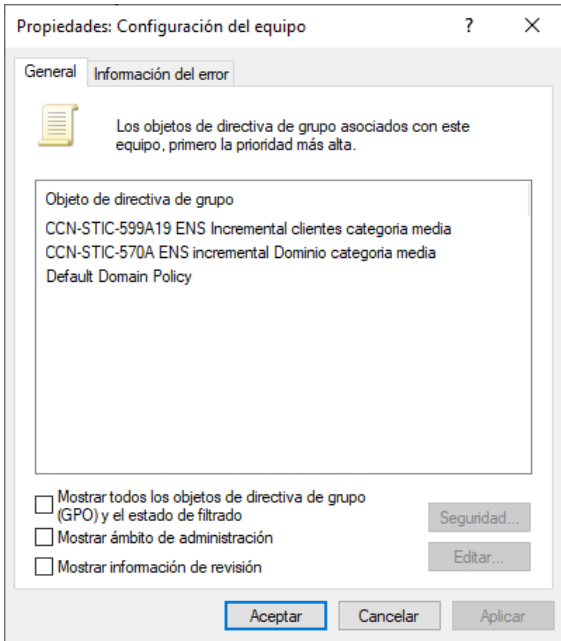
Comprobación	OK/NOK	Cómo hacerlo		
35.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
36.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
37.Verifique la directiva de Tienda en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitado	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitado	
38.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitado	
		Desactivar sensores	Habilitado	
		Desactivar ubicación	Habilitado	
39.Verifique la directiva de Windows Update en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	

Comprobación	OK/NOK	Cómo hacerlo		
40.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitado	
41.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet → Configuración de comunicaciones de Internet”		
		Directiva	Valor	OK/NOK
		Desactivar el acceso a la 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
	Desactivar la 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
42.Verifique la directiva de Net Logon en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Net Logon”		
	Directiva		Valor
	Permitir algoritmos de criptografía compatibles con Windows NT 4.0		Deshabilitado
43.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Perfiles de usuario”		

Comprobación	OK/NOK	Cómo hacerlo		
		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	
44. Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador.		Inicie sesión en el equipo que está comprobando con una cuenta de usuario de Windows con permisos de administrador.		
45. 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. 		
46. Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse "Enter" para abrir la consola de administración "Conjunto resultante de directivas": 		

Comprobación	OK/NOK	Cómo hacerlo
47.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 ENS incremental clientes categoria media".		En la consola de administración "Conjunto resultante de directivas, seleccione el contenedor "Configuración del equipo", márkuelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las políticas deberán aparecer y "CCN-STIC-599A19 ENS incremental clientes categoria media" deberá estar situada encima de la GPO que se establece a nivel de dominio, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 ENS incremental clientes categoria media" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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.

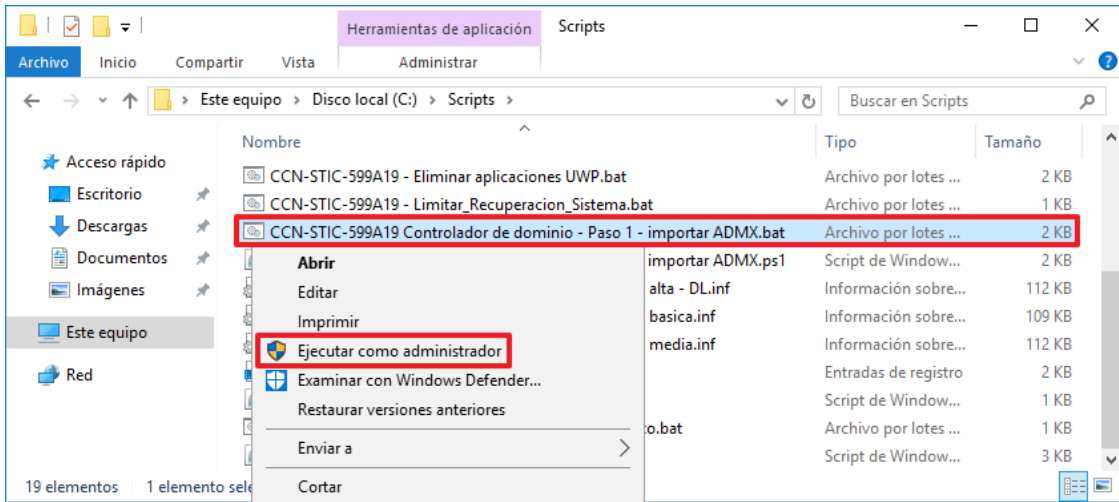
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

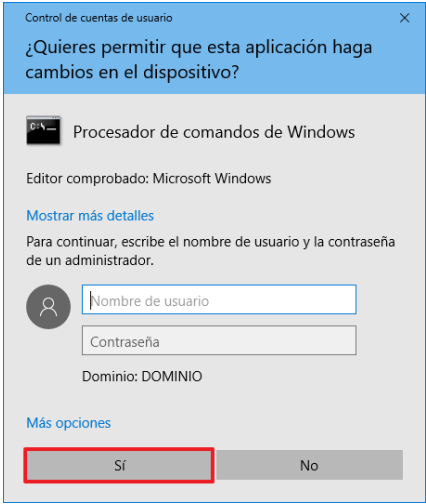
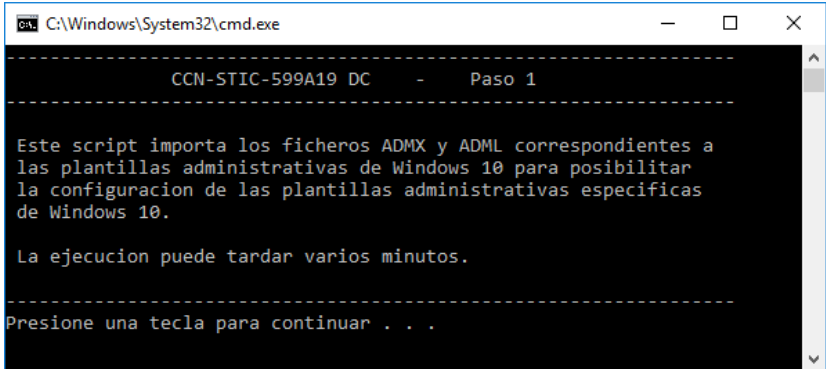
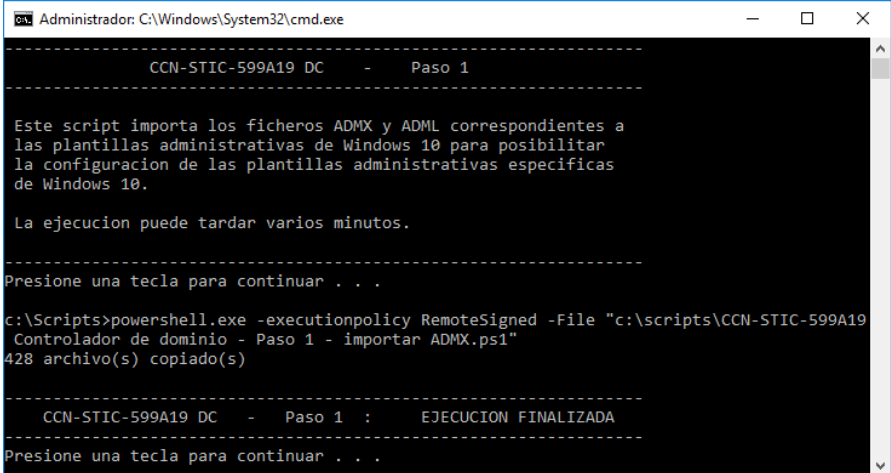
1. PREPARACIÓN DEL DOMINIO

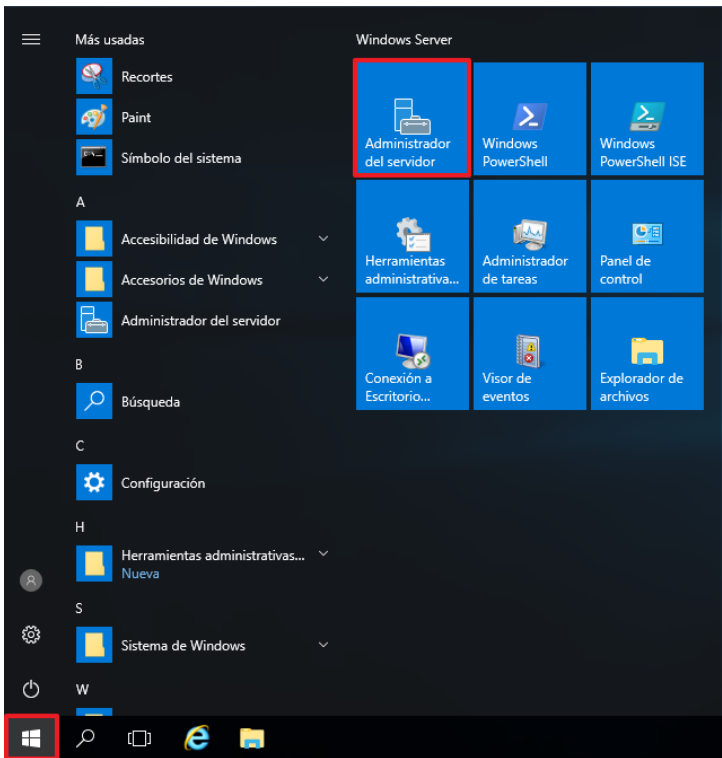
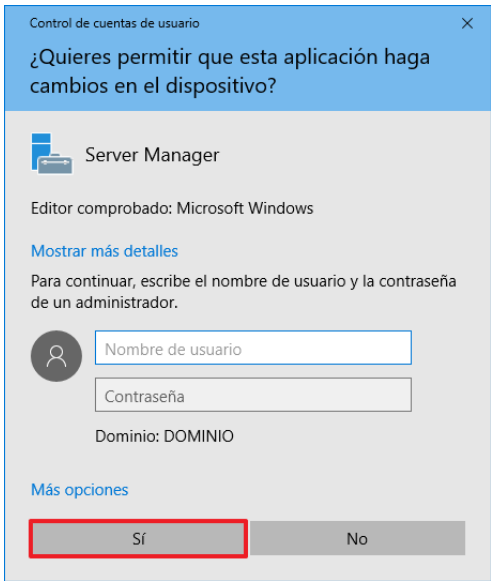
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

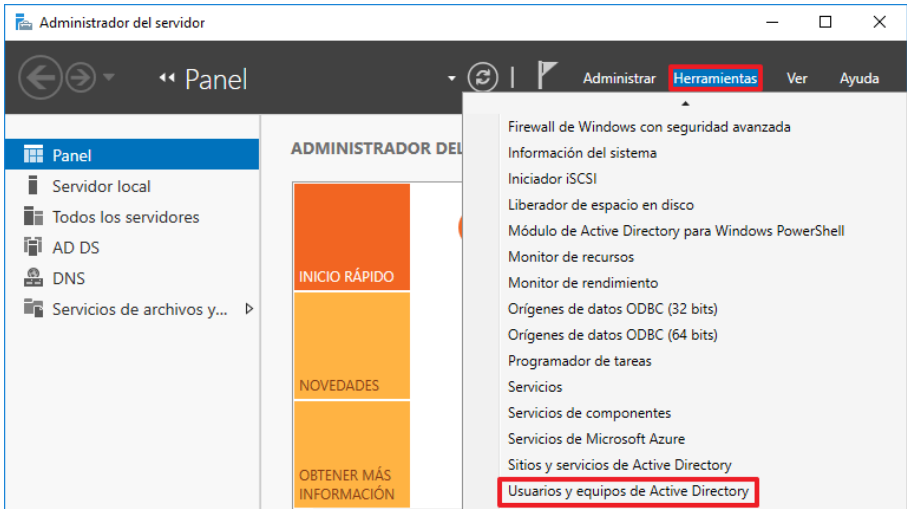
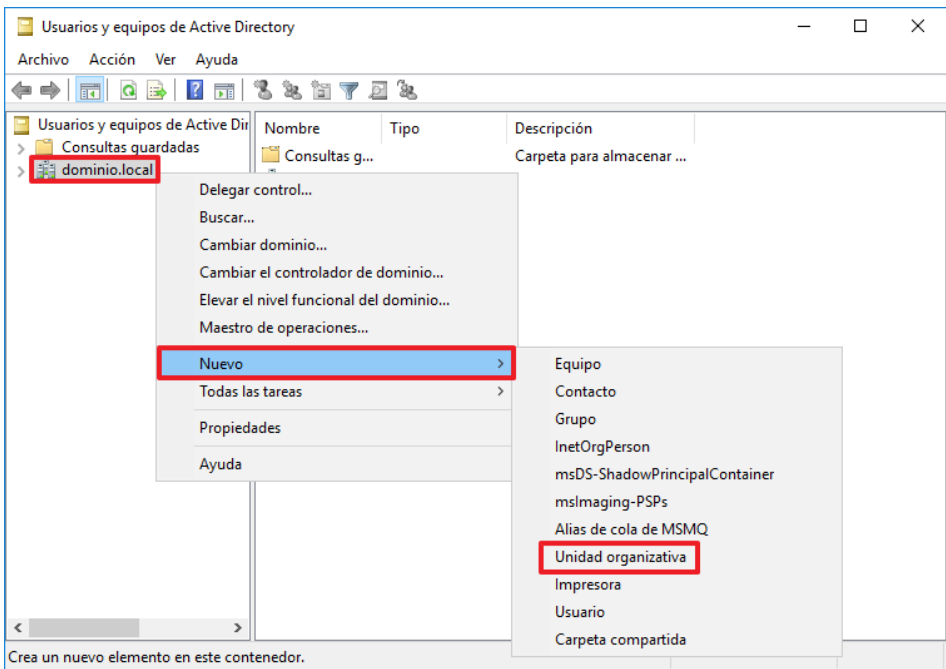
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Si no es así, aplique la guía correspondiente al controlador de dominio, antes de continuar con la aplicación de esta. En el ejemplo, las configuraciones y capturas de pantalla han sido realizadas sobre un controlador de dominio al que se le ha instalado Windows Server 2016 y aplicado la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016.

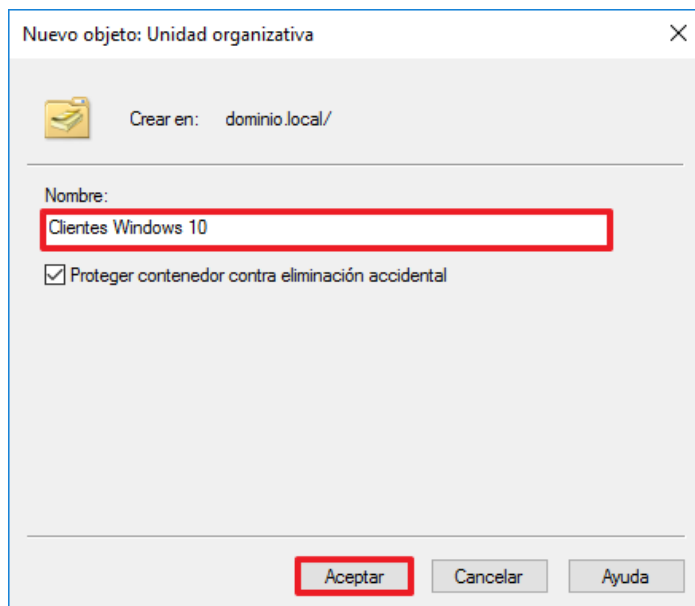
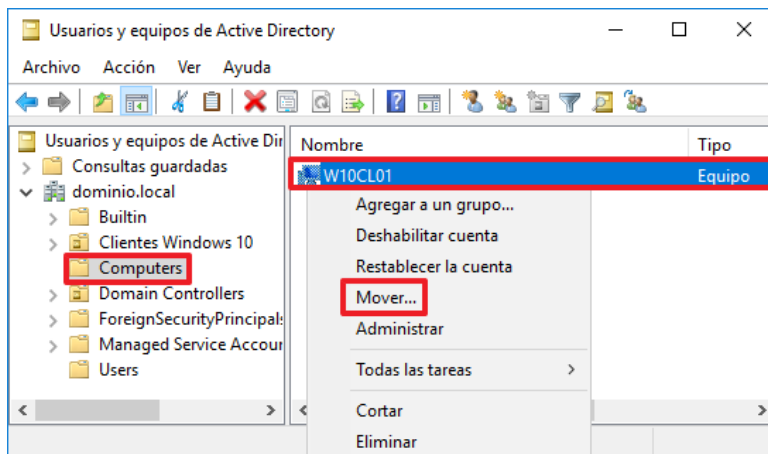
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.

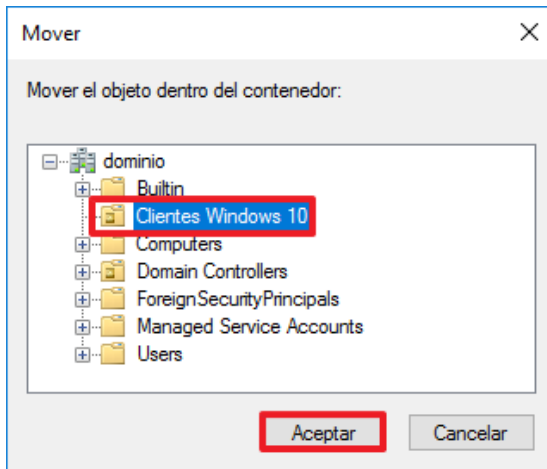
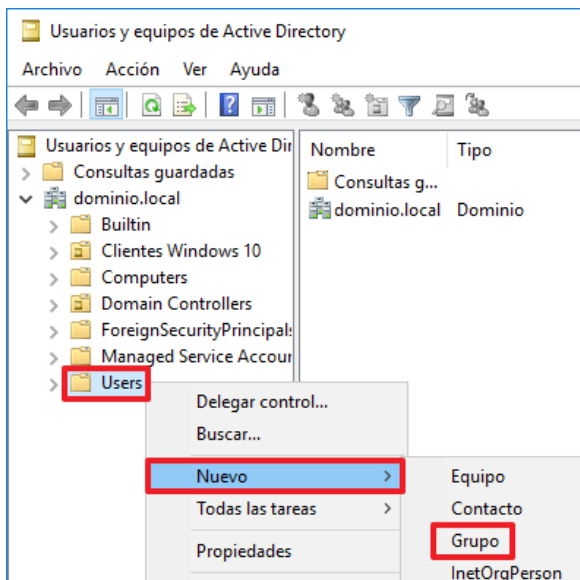
Paso	Descripción
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio. Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-599A19 ENS clientes categoria alta - DL (directorio) – CCN-STIC-599A19 ENS clientes categoria media (directorio) – CCN-STIC-599A19 ENS clientes categoria basica (directorio) – CCN-STIC-599A19 ENS Incremental portátiles categoria alta - DL - Bitlocker (directorio) – CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL.inf – CCN-STIC-599A19 ENS Incremental clientes categoria media.inf – CCN-STIC-599A19 ENS Incremental clientes categoria basica.inf – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1 – PolicyDefinitions - (directorio)
6.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

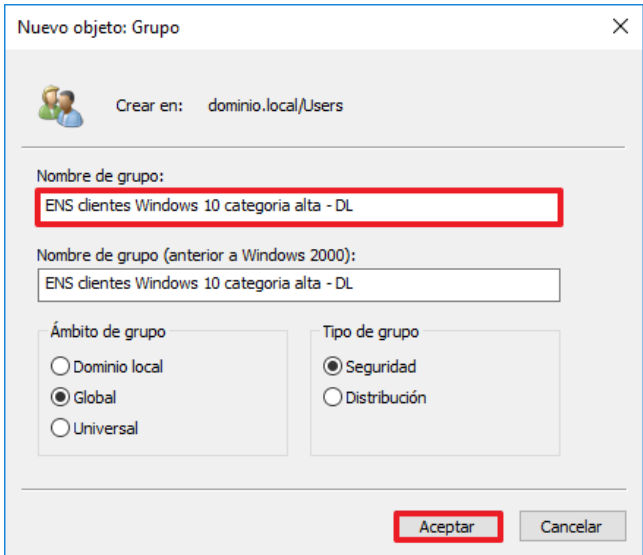
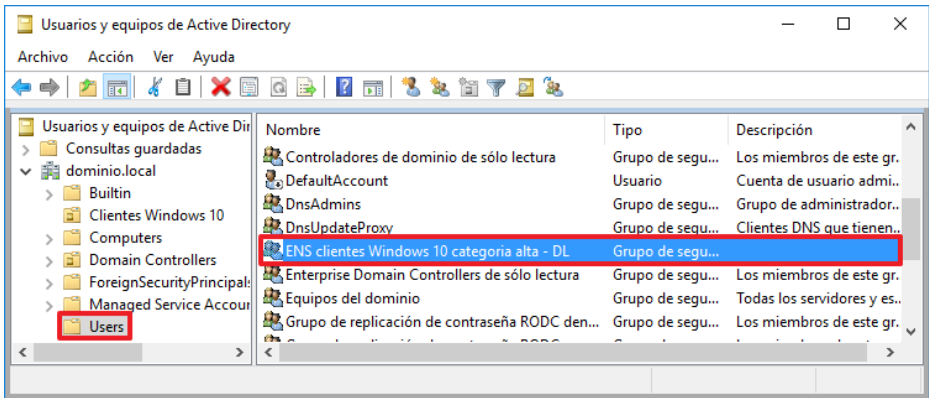
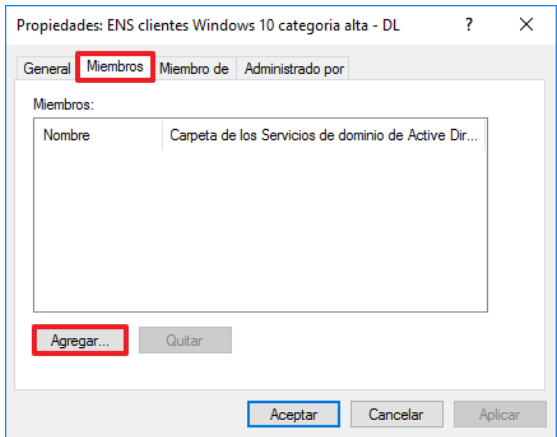
Paso	Descripción
7.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
8.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
9.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 

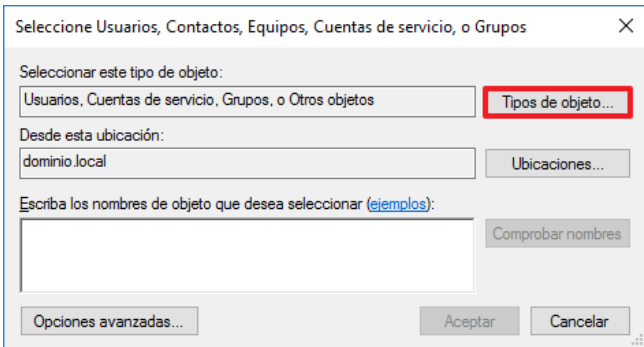
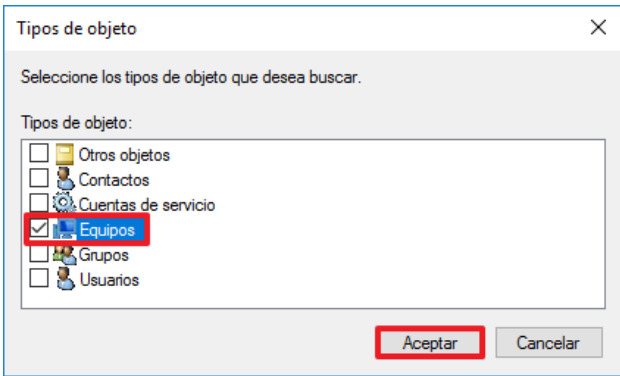
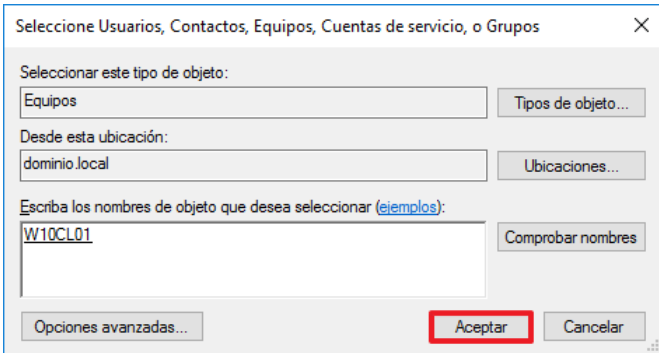
Paso	Descripción
10.	Copie el fichero “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL.inf”, almacenado en la carpeta “C:\Scripts”, al directorio “C:\Windows\Security\Templates” del Controlador de Dominio.
11.	Inicie la herramienta de “Usuarios y equipos de Active Directory”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
12.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 

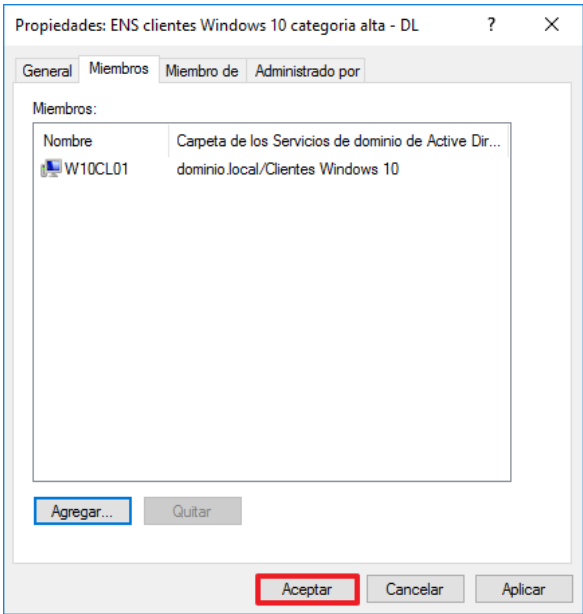
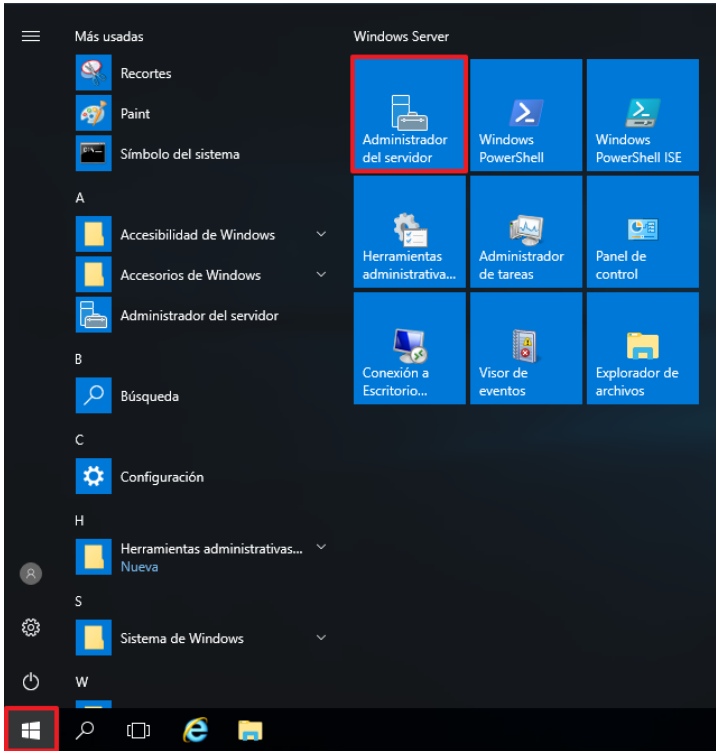
Paso	Descripción
13.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
14.	Pulse con el botón derecho sobre el dominio y seleccione “Nuevo → Unidad organizativa”. 

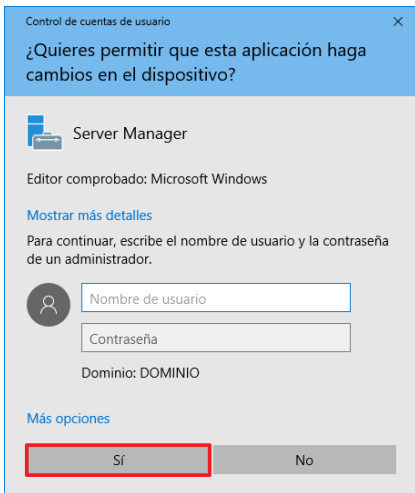
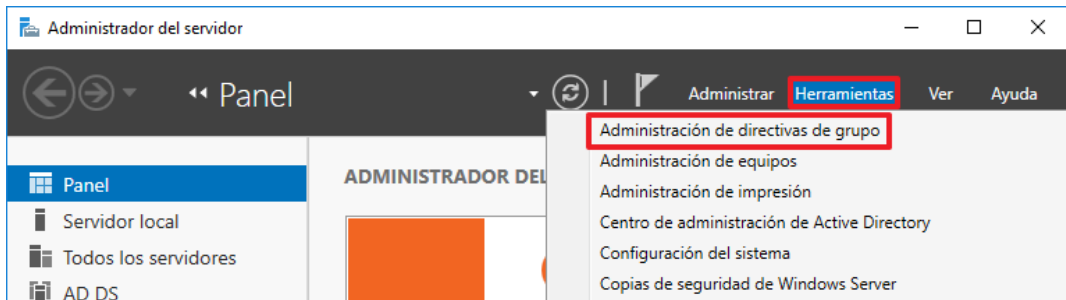
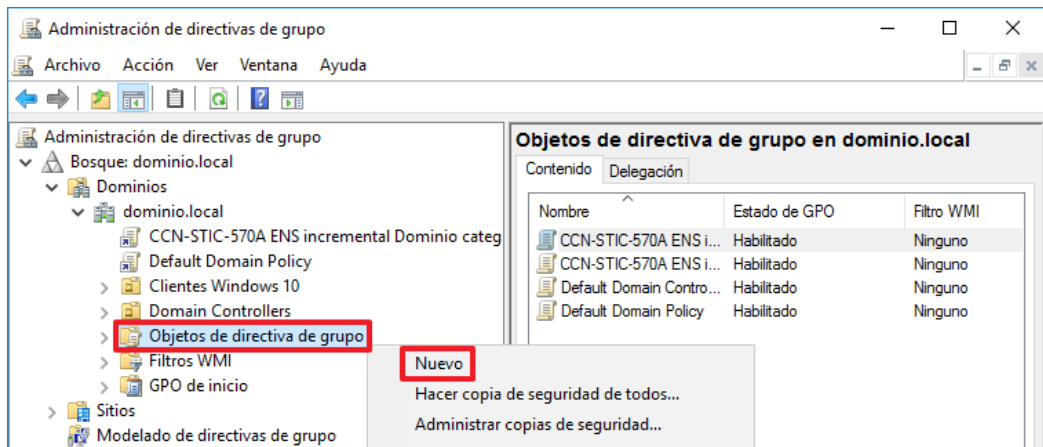
Paso	Descripción
15.	Establezca el nombre para la unidad organizativa con los clientes Windows 10 y pulse “Aceptar”. 
16.	Vaya a las unidades organizativas donde se encuentren los clientes que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover...” en cada uno de ellos.  Nota: En este ejemplo se encuentra bajo la unidad organizativa “Computers”.

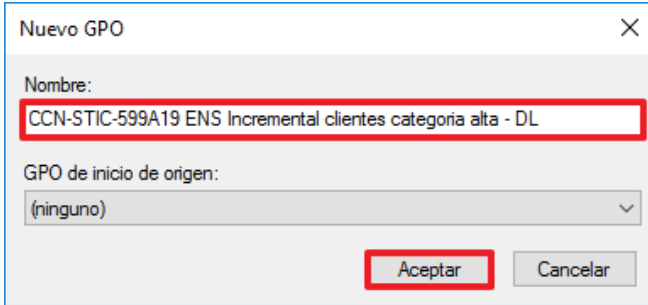
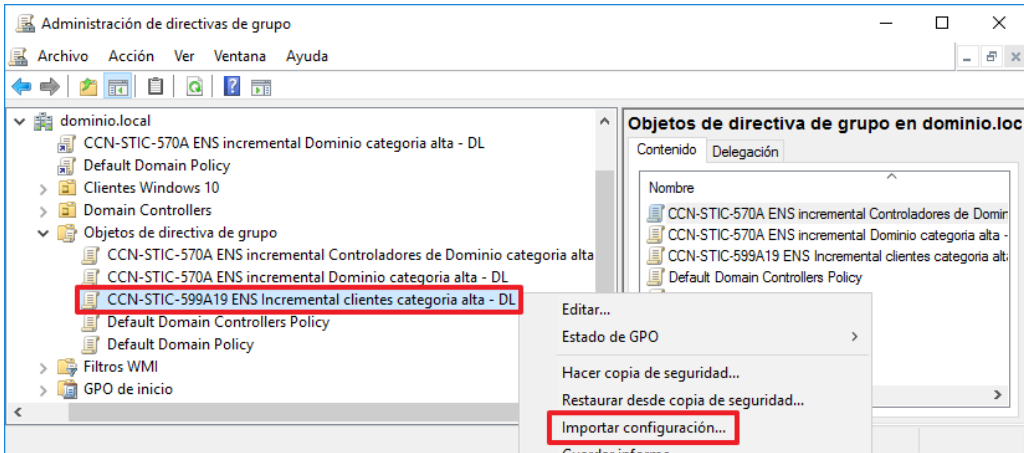
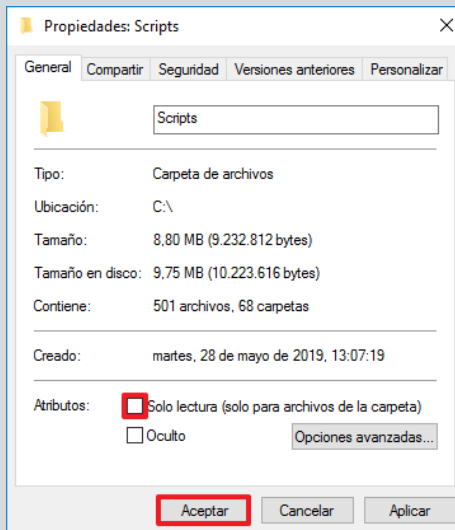
Paso	Descripción
17.	Seleccione la unidad organizativa “Clientes Windows 10” creada anteriormente y pulse “Aceptar”.  Nota: Los siguientes pasos describen el procedimiento para crear un grupo de seguridad donde agregar los puestos de trabajo que le sean de aplicación la categoría alta de seguridad según los criterios definidos del ENS. Si todos los equipos de la organización presentan la misma categoría alta no hace falta la creación de dicho grupo y puede saltar al paso 26. Si por el contrario van a existir puestos de trabajo Windows 10 con categorías básica o media, se deberán crear dichos grupos, siguiendo los pasos de los Anexos A.3 y A.4, de tal forma que la aplicación de políticas de seguridad en función de los niveles se aplique atendiendo a los criterios de pertenencia a grupo.
18.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

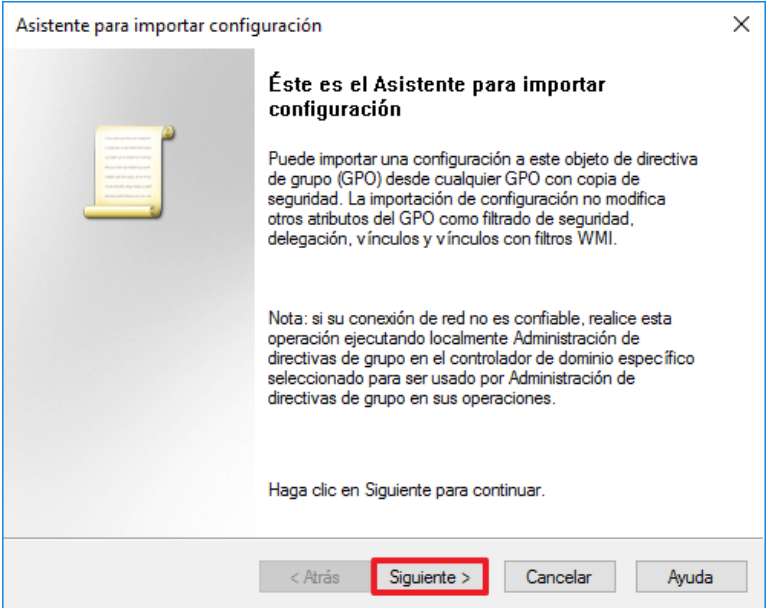
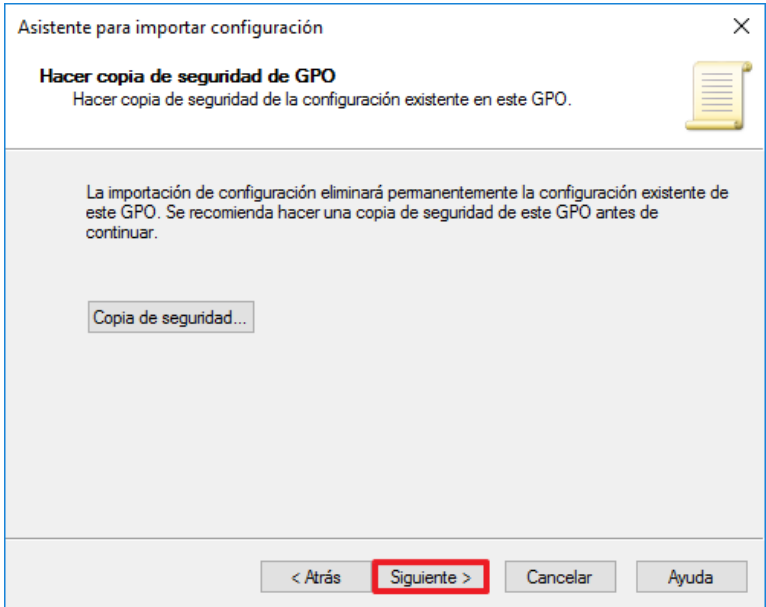
Paso	Descripción
19.	Introduzca como nombre “ENS clientes Windows 10 categoria alta - DL”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio. 
20.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
21.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar...”. 

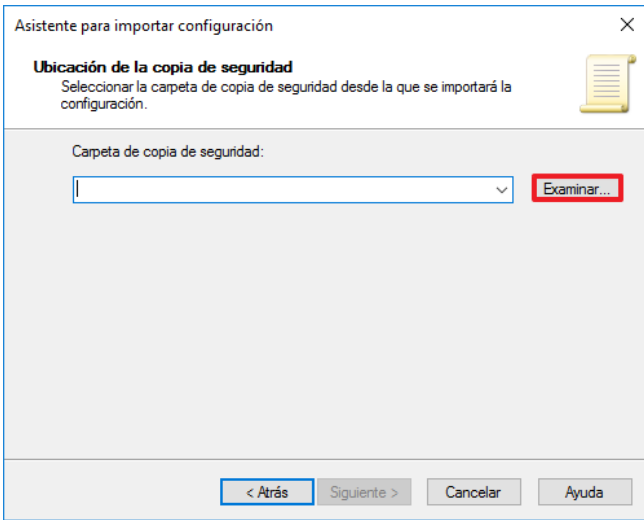
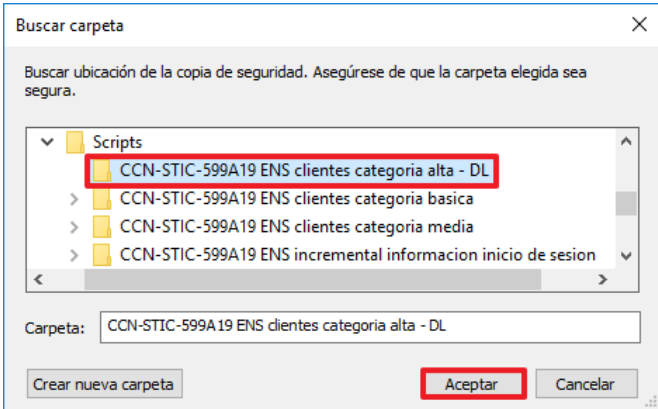
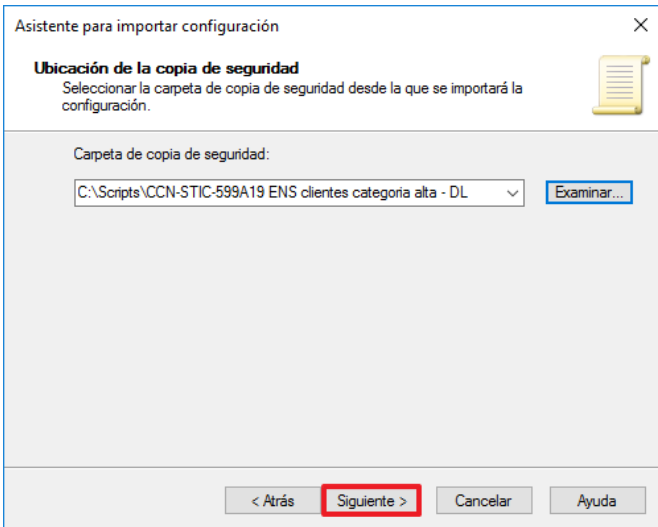
Paso	Descripción
22.	Pulse el botón de “Tipos de objeto...”. 
23.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
24.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad alta y pulse “Aceptar” para agregar la selección.  Nota: No agregue servidores a este grupo.

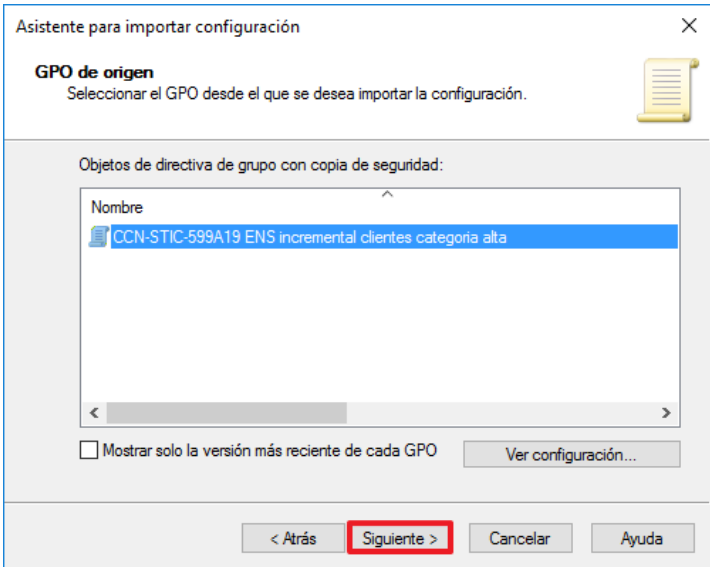
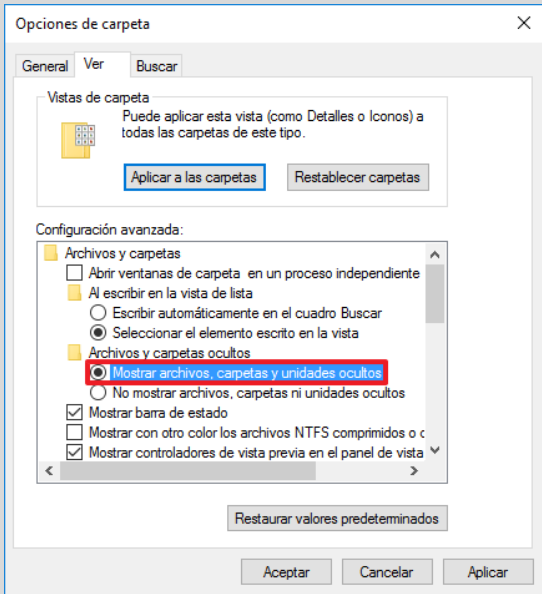
Paso	Descripción
25.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
26.	Cierre la herramienta “Usuarios y equipos e Directorio Activo”.
27.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

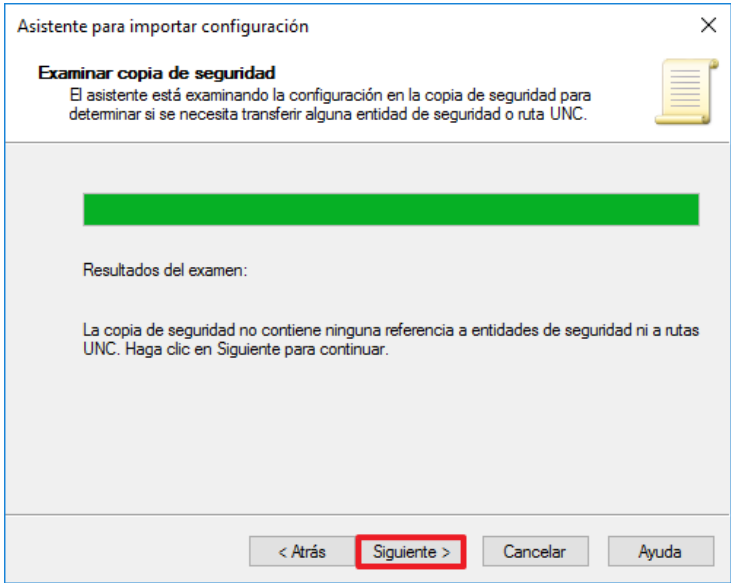
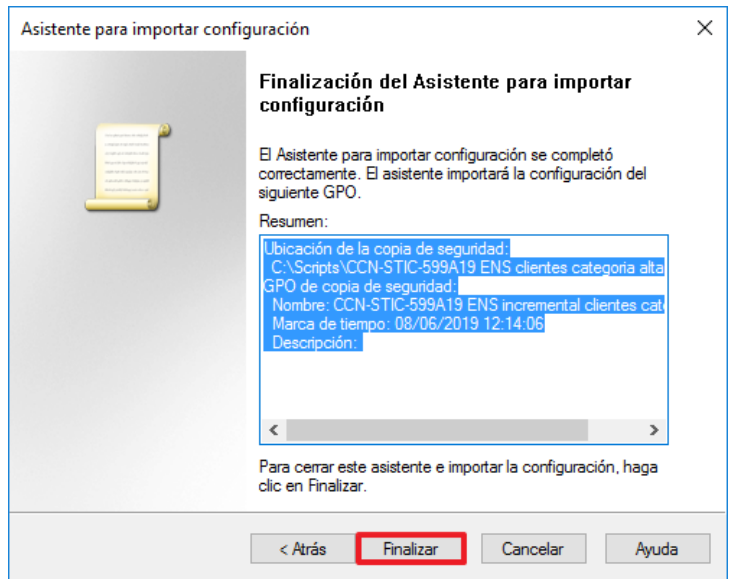
Paso	Descripción															
28.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 															
29.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 															
30.	Despliegue los contenedores pertenecientes a su dominio y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”.  <table><tr><th>Nombre</th><th>Estado de GPO</th><th>Filtro WMI</th></tr><tr><td>CCN-STIC-570A ENS incremental</td><td>Habilitado</td><td>Ninguno</td></tr><tr><td>CCN-STIC-570A ENS i...</td><td>Habilitado</td><td>Ninguno</td></tr><tr><td>Default Domain Contro...</td><td>Habilitado</td><td>Ninguno</td></tr><tr><td>Default Domain Policy</td><td>Habilitado</td><td>Ninguno</td></tr></table>	Nombre	Estado de GPO	Filtro WMI	CCN-STIC-570A ENS incremental	Habilitado	Ninguno	CCN-STIC-570A ENS i...	Habilitado	Ninguno	Default Domain Contro...	Habilitado	Ninguno	Default Domain Policy	Habilitado	Ninguno
Nombre	Estado de GPO	Filtro WMI														
CCN-STIC-570A ENS incremental	Habilitado	Ninguno														
CCN-STIC-570A ENS i...	Habilitado	Ninguno														
Default Domain Contro...	Habilitado	Ninguno														
Default Domain Policy	Habilitado	Ninguno														

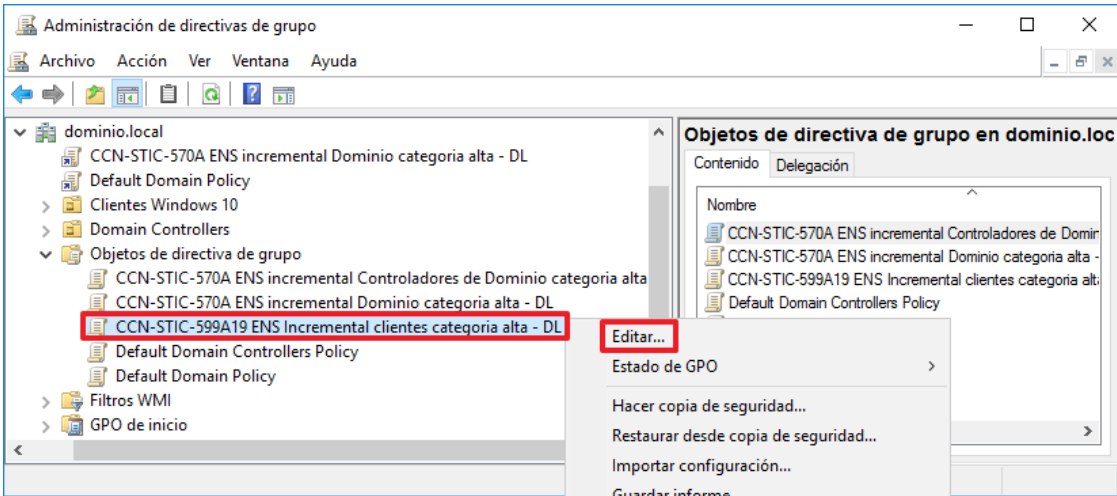
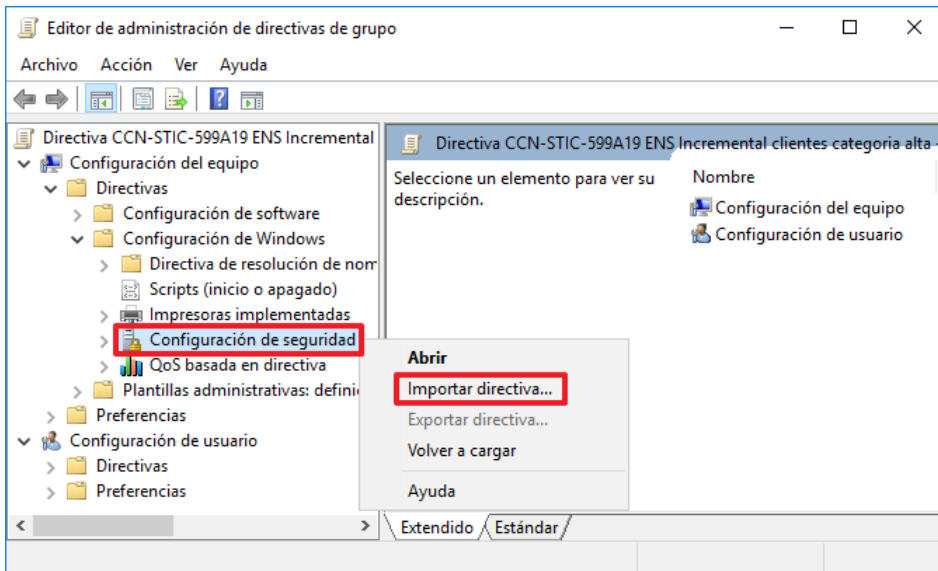
Paso	Descripción
31.	Introduzca como nombre “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” y pulse el botón “Aceptar”. 
32.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política con el botón derecho del ratón y seleccione la opción “Importar configuración...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts”, así como los archivos dentro de sus subcarpetas, no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

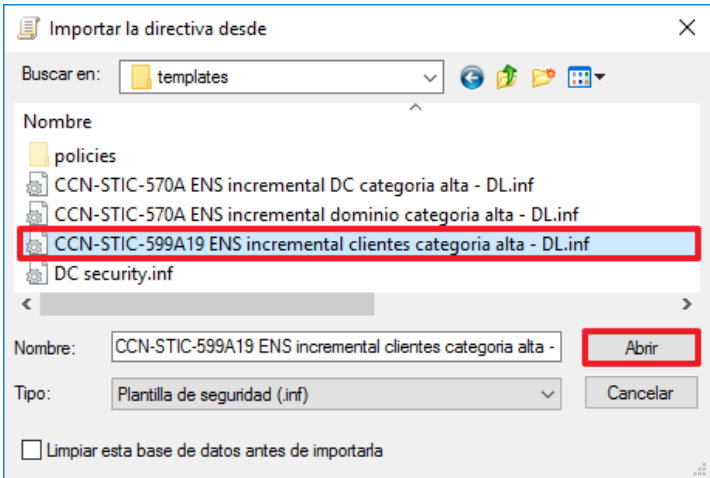
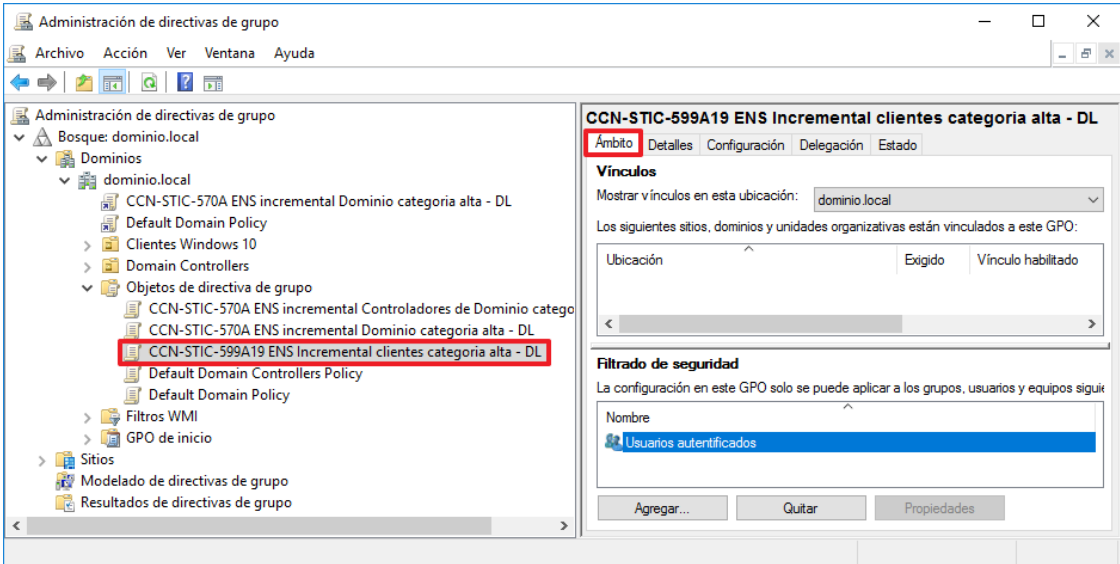
Paso	Descripción
33.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
34.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

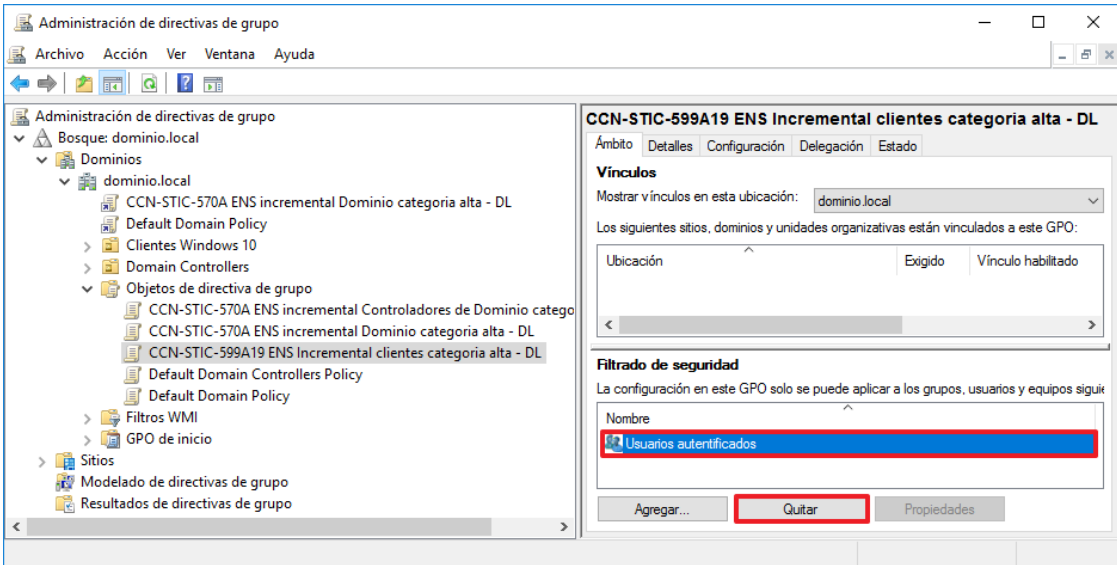
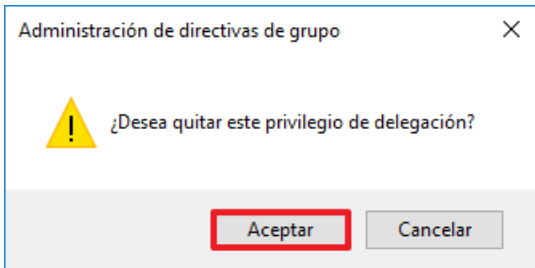
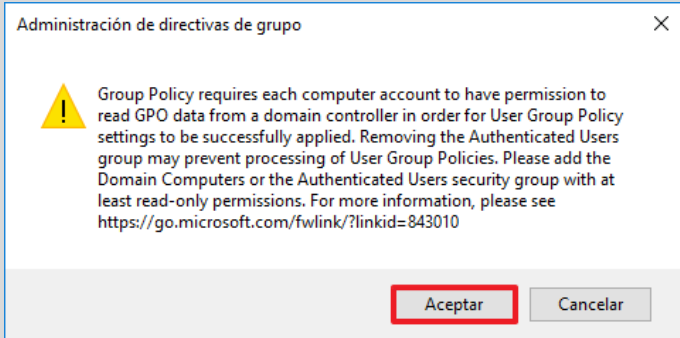
Paso	Descripción
35.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
36.	Seleccione la carpeta “CCN-STIC-599A19 ENS clientes categoria alta - DL” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
37.	Pulse el botón “Siguiendo >” una vez seleccionada la carpeta adecuada. 

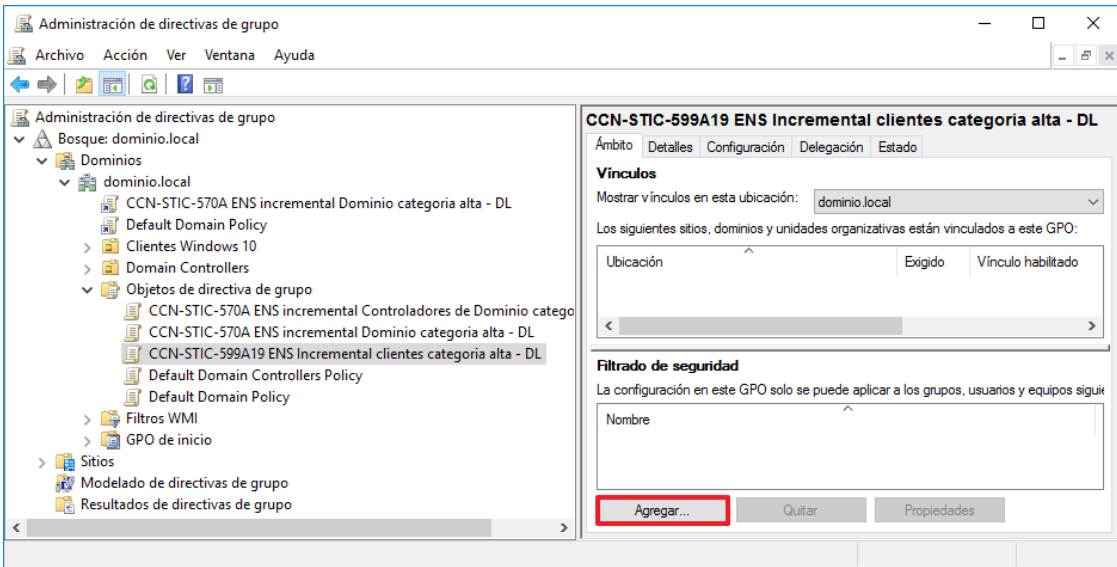
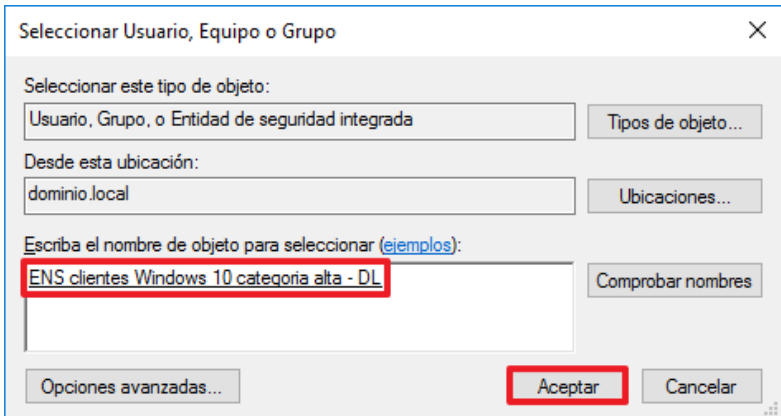
Paso	Descripción
38.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental clientes categoria alta – DL” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
39.	En la pantalla de examen, pulse el botón “Siguiente >”. 
40.	Para completar el asistente pulse el botón “Finalizar”. 
41.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.

Paso	Descripción
42.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
43.	Una vez pulsada la opción “Editar...” se abre una ventana de “Editor de administración de directivas de grupo”. Despliegue el objeto de directiva de grupo y sitúe el cursor sobre el nodo Configuración de seguridad. “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”
44.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva...”. 

Paso	Descripción
45.	Seleccione el fichero “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL.inf” ubicado en la ruta “C:\Windows\Security\Templates” y pulse el botón “Abrir”. 
46.	Cierre la política una vez se haya realizado la importación de la configuración de seguridad. Nota: Los siguientes pasos describen el procedimiento para asignar la política al grupo de seguridad creado en los pasos 18 a 25. Si usted creó el grupo puesto que va a tener aplicadas diferentes categorías de seguridad en la organización para los puestos de trabajo, siga con el siguiente paso. Si no creo dicho grupo, diríjase al paso 52.
47.	Seleccione la nueva política de grupo configurada y vaya a las opciones de ámbito que se encuentran en el panel derecho. 

Paso	Descripción
48.	En el apartado “Filtrado de seguridad”, seleccione “Usuarios autenticados” y pulse el botón “Quitar”. 
49.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
50.	Pulse ahora sobre el botón “Agregar...”. 
51.	Introduzca como nombre “ENS clientes Windows 10 categoria alta - DL”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
52.	La política se encuentra ya creada correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente Anexo.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

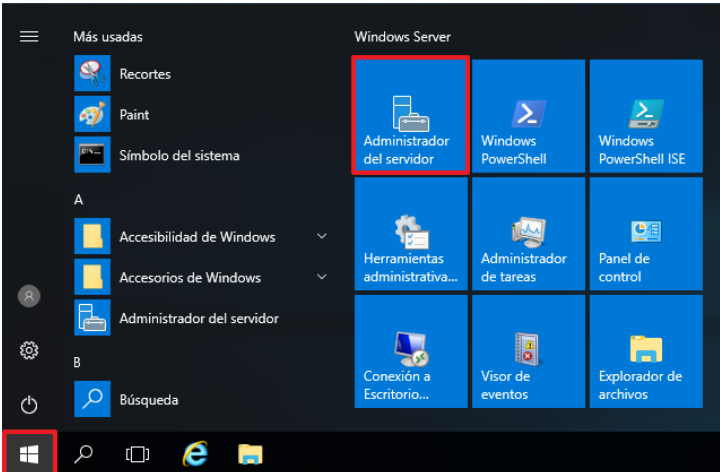
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y por lo tanto deben valorarse con respecto a la aplicación de la presente configuración. La plantilla de seguridad que se ha configurado tiene en consideración los puntos tratados en el Esquema Nacional de seguridad para la categoría alta / Difusión Limitada. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina, como por ejemplo lo relativo al uso de privilegios.

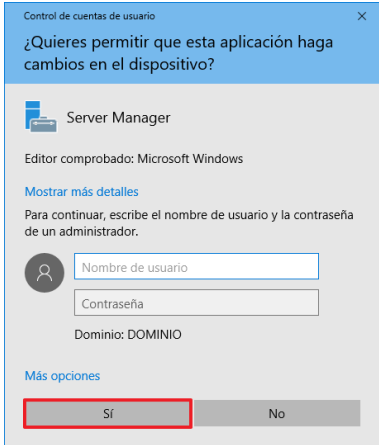
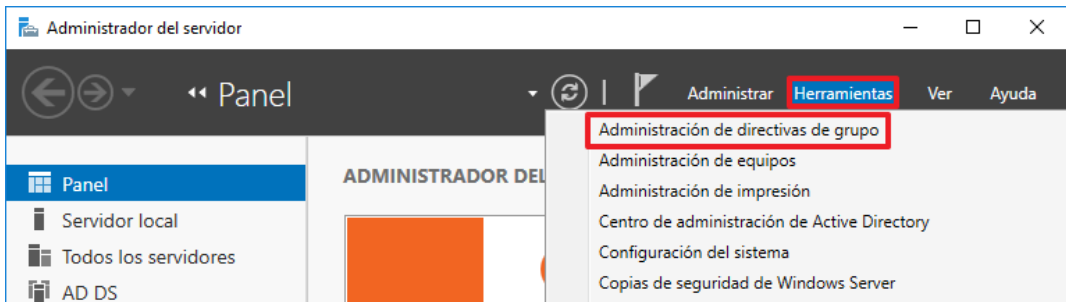
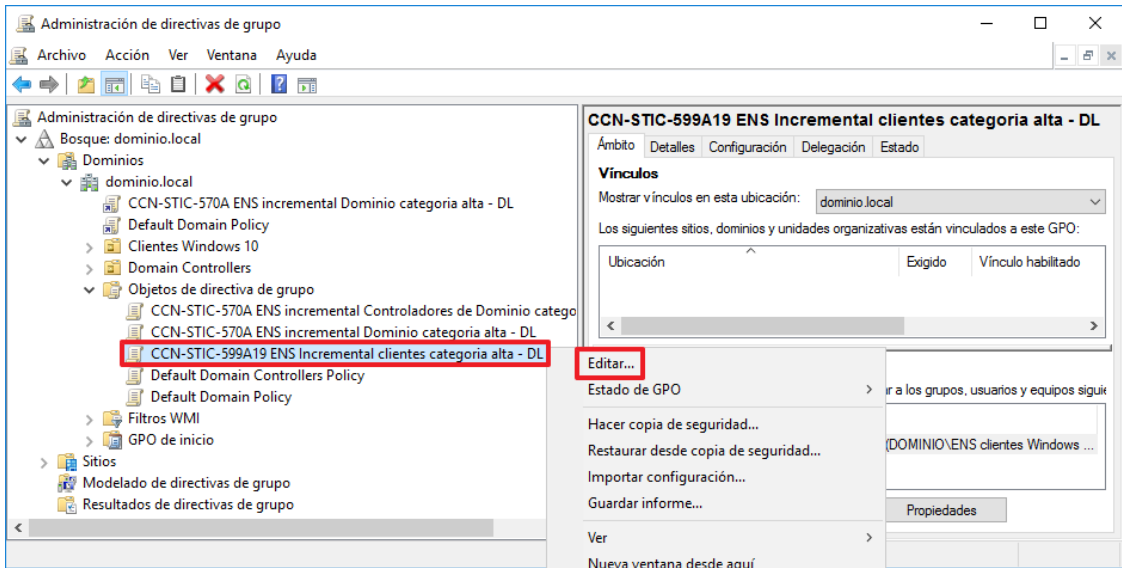
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

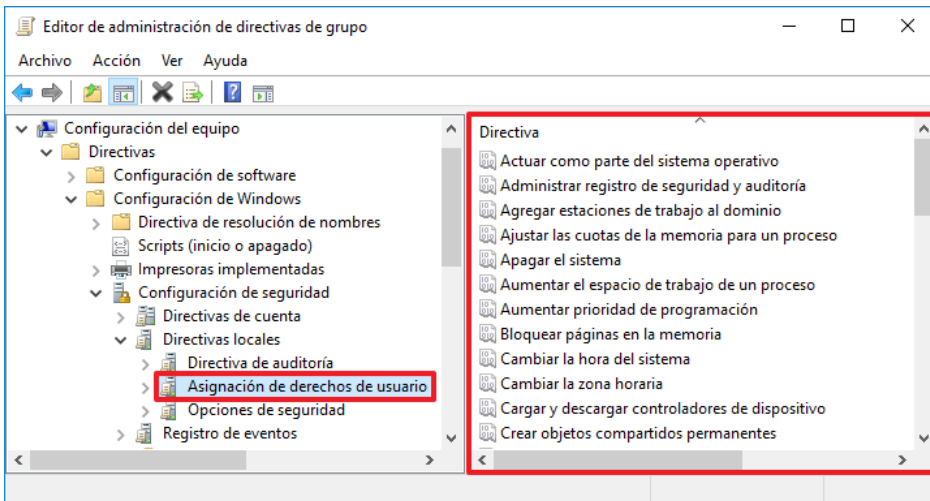
Los objetos de políticas de grupo para puestos de trabajo especifican unos derechos de usuario siguiendo planteamientos de seguridad siguiendo los principios de mínimos privilegios y mínima exposición. No obstante, resulta factible que su organización tenga creados grupos o usuarios a los que les haya asignado derechos determinados para la administración o gestión de los sistemas.

Si esto fuera así deberá realizar las modificaciones sobre el objeto de política creado en el punto previo.

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

Paso	Descripción
53.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
54.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
55.	Edite la política de grupo correspondiente. Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

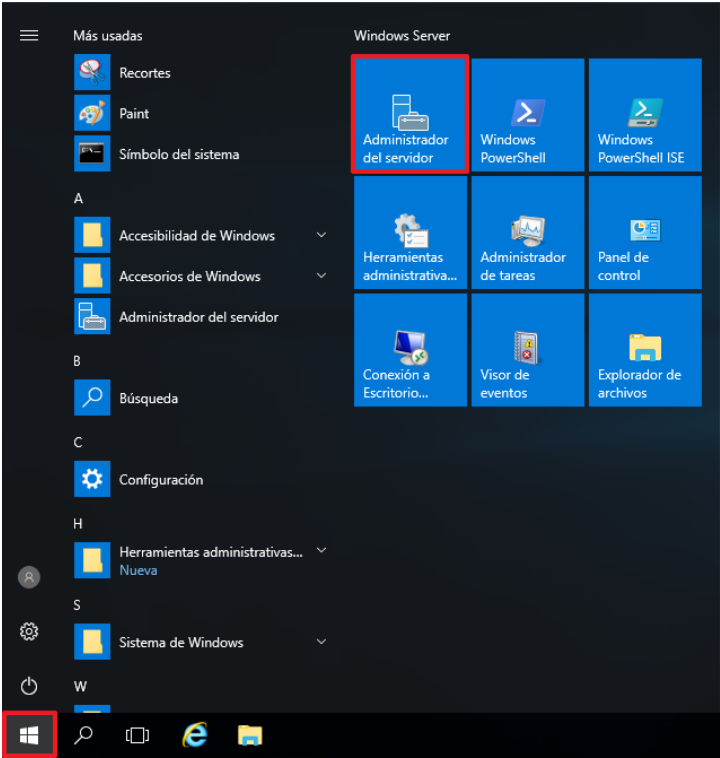
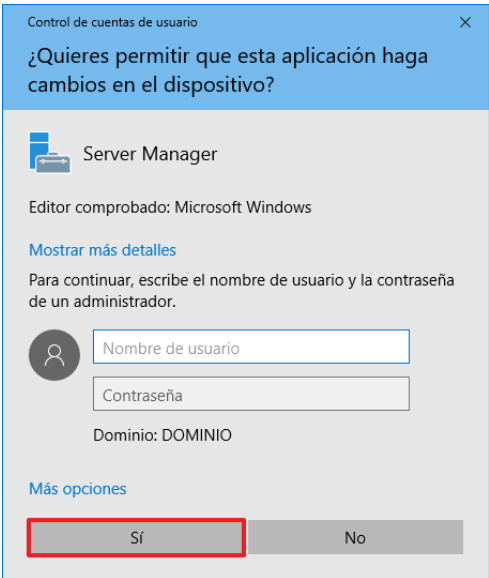
Paso	Descripción
56.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
57.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
58.	Seleccione la política creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 

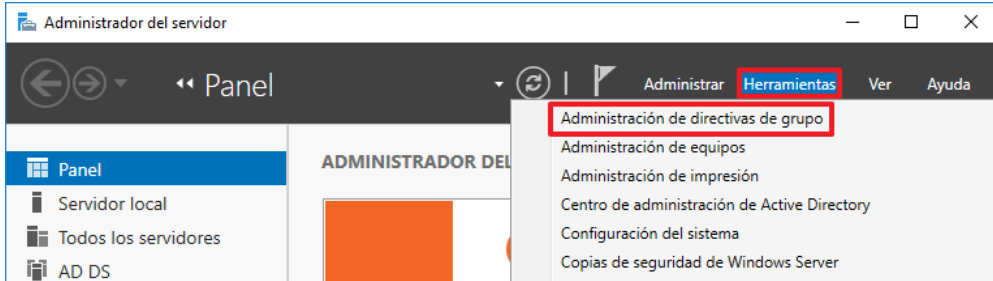
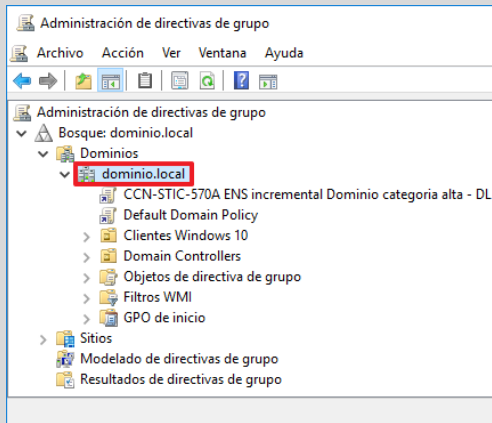
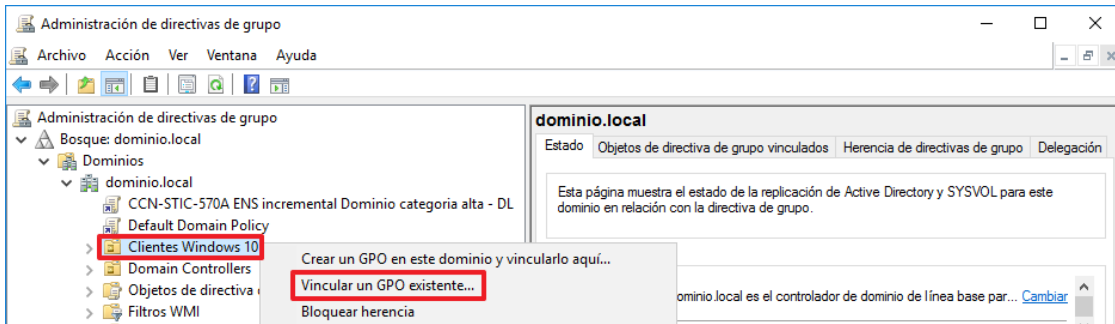
Paso	Descripción
59.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana del editor de administración de directivas de grupo.

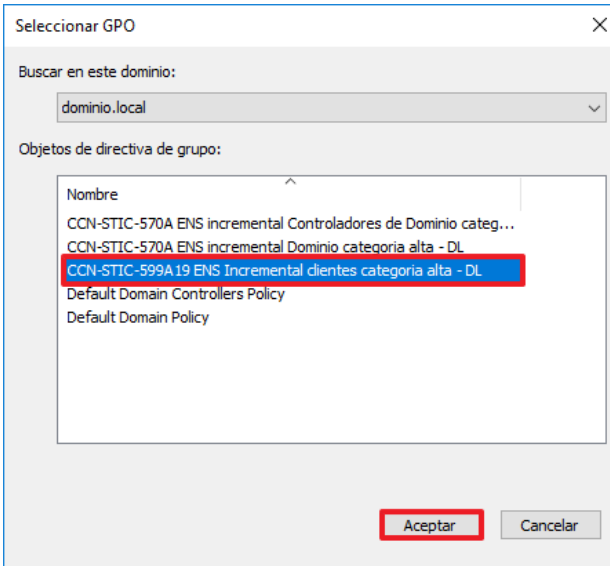
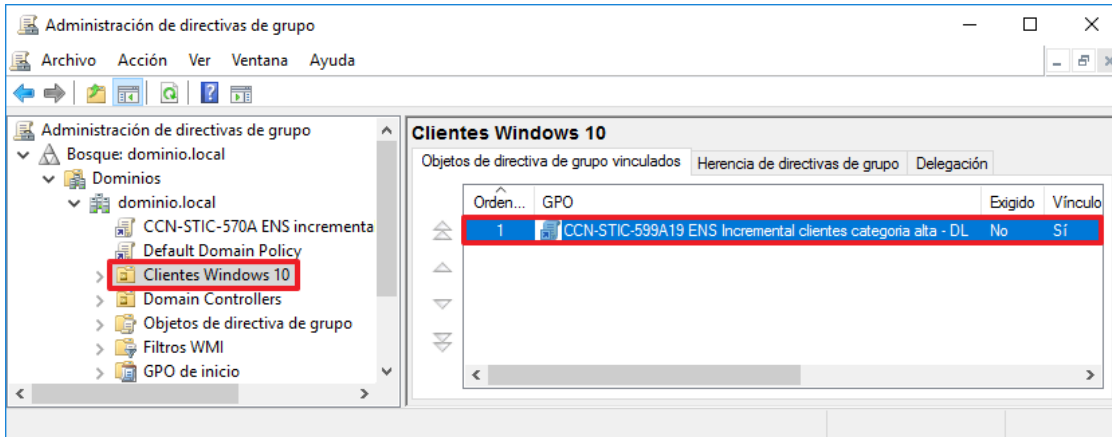
3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, una vez que se han tenido en consideración las condiciones definidas en el punto previo.

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

Paso	Descripción
64.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
65.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 

Paso	Descripción
66.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
67.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es “dominio.local”.
68.	Identifique las ubicaciones donde se encuentran los Clientes Windows 10 que les son de aplicación las condiciones de seguridad de categoría alta, según estipula el ENS. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” que es donde se encuentran ubicados los clientes existentes en este escenario. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 
69.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
70.	Seleccione la política “CCN-STIC-599A19 ENS Incremental categoria alta - DL” y pulse el botón “Aceptar”. 
71.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dichas Unidades Organizativas. 
72.	Cierre la herramienta “Administración de directivas de grupo”.
73.	Elimine la carpeta “C:\scripts”.
74.	Para que la nueva política sea efectiva necesita reiniciar el o los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Es posible que bajo determinadas condiciones pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado Microsoft propone como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

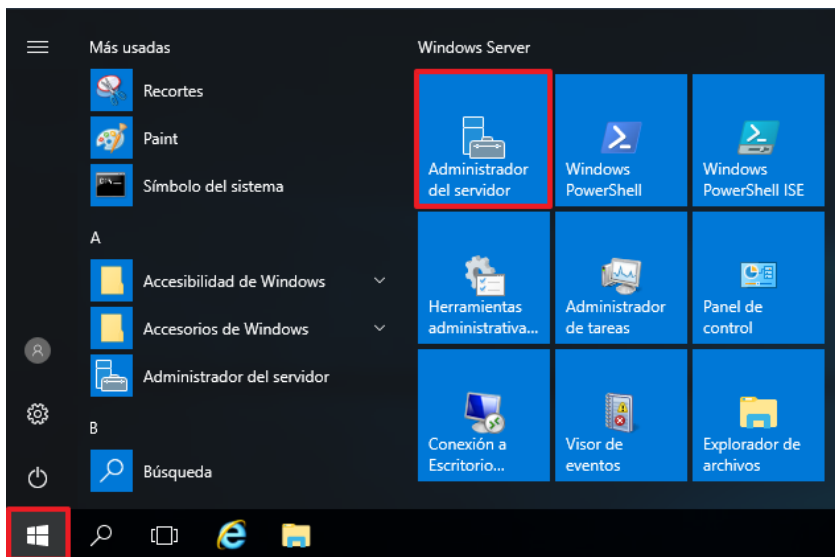
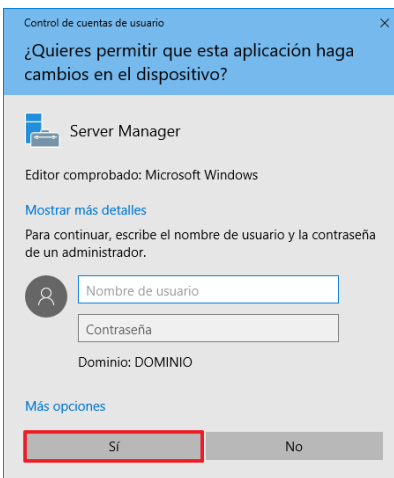
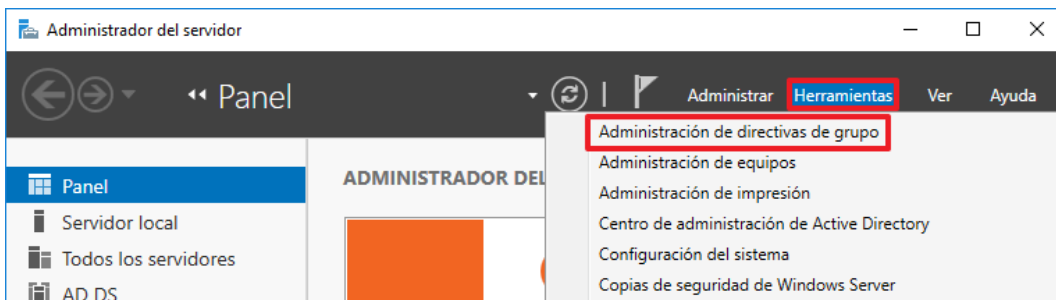
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría alta.

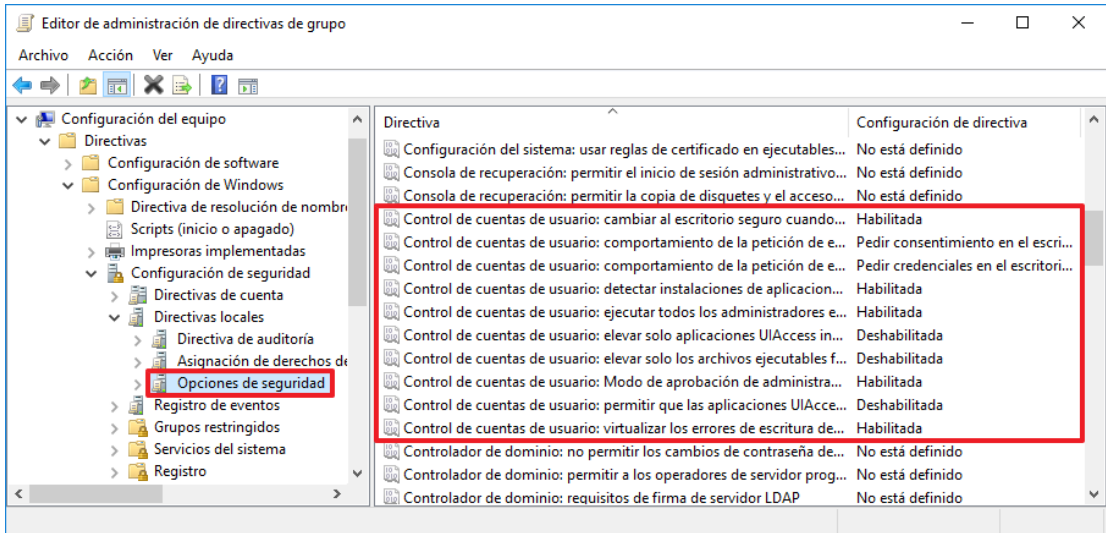
No obstante, y ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría alta por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación en los clientes que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

4.1. CONTROL DE CUENTAS USUARIO

Paso	Descripción
75.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
76.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
77.	Identifique los puestos de trabajo que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS clientes Windows 10 categoría alta - DL”. En el caso de que no haya tenido que crear dicho grupo siga al paso siguiente.
78.	Cree un nuevo grupo de forma similar al ya creado, siguiendo los pasos 18 a 25 del presente Anexo.

Paso	Descripción
79.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
80.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
81.	Seleccione la pestaña "Administración de directivas de grupo". 

Paso	Descripción
82.	Cree una nueva política de grupo con un nombre diferente (p.e. “CCN-STIC-599A19 ENS incremental clientes categoria alta – DL - incidencias UAC”) que será asignable a los clientes Windows 10 con una categoría alta e incidencias de funcionalidad del UAC. Siga para ello los pasos 27 a 46. Incluya al nuevo grupo de puestos de trabajo creados en lugar del grupo “ENS clientes Windows 10 categoria alta - DL” creado en el proceso previo.
83.	Edite el nuevo objeto de GPO “CCN-STIC-599A19 ENS incremental clientes categoria alta – DL - incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar...” del menú contextual.
84.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”
85.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
86.	Realice las modificaciones oportunas.
87.	Cierre la política.
88.	Para que la nueva política sea efectiva necesita reiniciar el o los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Debe tener en consideración que, si ha alterado la política de control de cuentas y esta es menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presenten funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

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 GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 con implementación de seguridad de categoría alta del ENS / Difusión Limitada.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

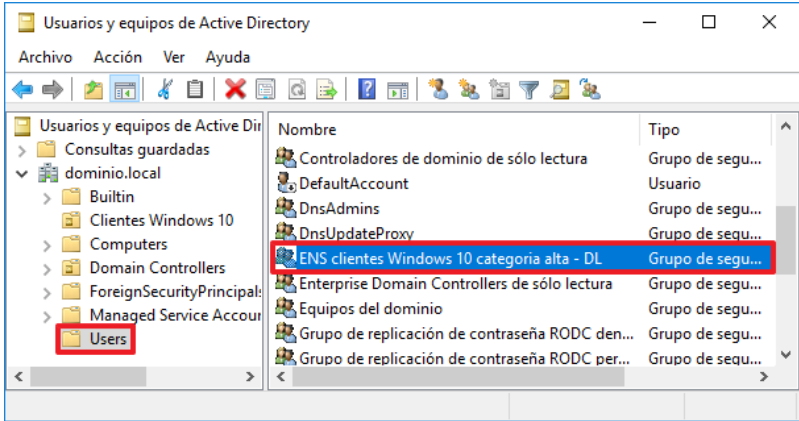
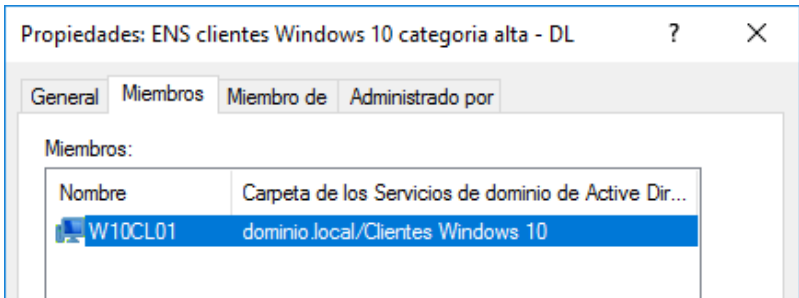
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

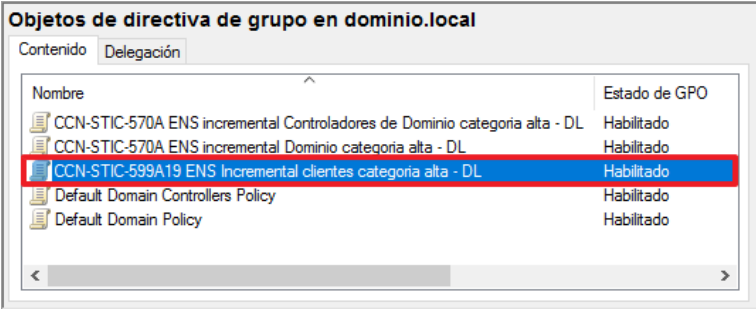
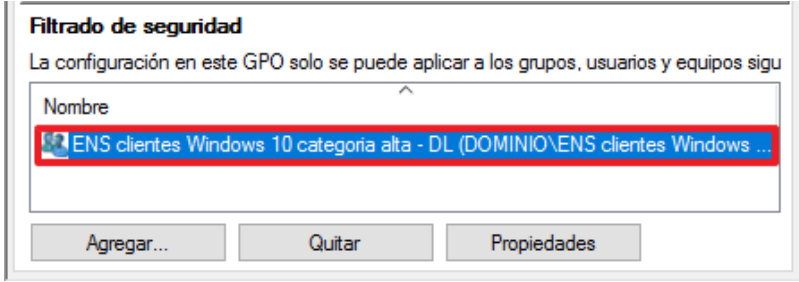
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

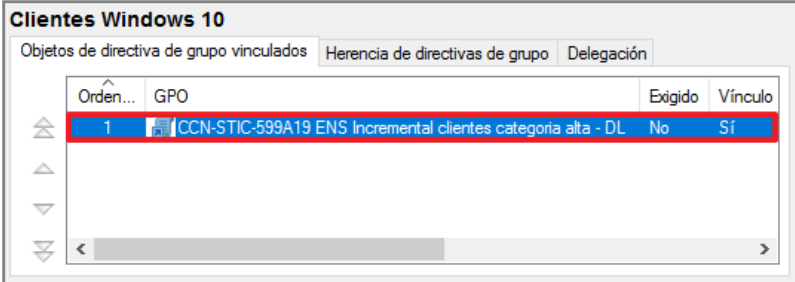
También deberá ejecutar una parte del análisis en los clientes Windows 10 a los que se les haya aplicado la configuración de seguridad de categoría alta – Difusión Limitada. En éstos deberá ejecutar la siguiente aplicación.

- a) Conjunto resultante de directivas (rsop.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creado el grupo “ENS clientes Windows 10 categoría alta - DL” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory” desde: “Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory” Seleccione el contenedor “Users”, situada en “[Su dominio] → Users” y a continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS clientes Windows 10 categoría alta - DL”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers”.
3. Verifique que los clientes que han sido catalogados como de categoría de seguridad alta, siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS clientes Windows 10 categoría alta”.		Pulse doble clic sobre el grupo “ENS clientes Windows 10 categoría alta - DL” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los clientes que corresponden a esta categoría de seguridad aparecen en el listado.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers”.

Comprobación	OK/NOK	Cómo hacerlo		
4. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” ha sido creado y está habilitado.		Ejecute la herramienta “Administrador de directivas de grupo” desde “Menú inicio → Herramientas administrativas → Administrador de directivas de grupo” Dentro de la consola diríjase a los “Objetos de directiva de grupo” “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo” Verifique que está creado el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” y que en la columna “Estado de la GPO” figura como habilitado. 		
		Directiva	Estado	OK/NOK
		CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL	Habilitado	
5. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” tiene definido el Ámbito al grupo “ENS clientes Windows 10 categoria alta - DL”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” desde “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS clientes Windows 10 categoria alta - DL”. 		
		Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers”.		

Comprobación	OK/NOK	Cómo hacerlo															
6. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” es aplicado a todos aquellos equipos Windows 10 que le son de aplicación las condiciones de categoría alta.		Evalúe que la política de seguridad es aplicada en un orden superior a otras políticas aplicables a los puestos de trabajo en todas aquellas ubicaciones donde se encuentren clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría alta – Difusión Limitada. En el árbol de la izquierda, seleccione la ubicación donde se encuentren los clientes del dominio Windows 10 al que le son de aplicación las condiciones de seguridad de categoría alta – Difusión Limitada: 															
7. Verifique la directiva de contraseñas en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Pulse el botón derecho del ratón y seleccione la opción “Editar...”. Se abrirá el editor de directivas de grupo. Deberá navegar sobre los elementos del árbol de directorios para verificar las distintas configuraciones. Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas” <table border="1"> <thead> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Exigir historial de contraseñas</td><td>24</td><td></td></tr> <tr> <td>Longitud mínima de la contraseña</td><td>12</td><td></td></tr> <tr> <td>Vigencia máxima de la contraseña</td><td>45</td><td></td></tr> <tr> <td>Vigencia mínima de la contraseña</td><td>2</td><td></td></tr> </tbody> </table>	Directiva	Valor	OK/NOK	Exigir historial de contraseñas	24		Longitud mínima de la contraseña	12		Vigencia máxima de la contraseña	45		Vigencia mínima de la contraseña	2	
Directiva	Valor	OK/NOK															
Exigir historial de contraseñas	24																
Longitud mínima de la contraseña	12																
Vigencia máxima de la contraseña	45																
Vigencia mínima de la contraseña	2																

Comprobación	OK/NOK	Cómo hacerlo		
8. Verifique la directiva de bloqueo de cuenta en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de bloqueo de cuenta”		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	0	
		Restablecer el bloqueo de cuenta después de	30	
		Umbral del bloqueo de cuenta	8	
9. Verifique las directivas de auditoría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
10.Verifique la asignación de derechos de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	BUILTIN\Administradores	
		Ajustar las cuotas de la memoria para un proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores	
		Apagar el sistema	BUILTIN\Usuarios, BUILTIN\Administradores	
		Aumentar el espacio de trabajo de un proceso	BUILTIN\Usuarios, NT AUTHORITY\SERVICIO LOCAL, BUILTIN\Administradores	
		Aumentar prioridad de programación	BUILTIN\Administradores	
		Cambiar la hora del sistema	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cambiar la zona horaria	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cargar y descargar controladores de dispositivo	BUILTIN\Administradores	
		Crear objetos compartidos permanentes		
		Crear un archivo de paginación	BUILTIN\Administradores	
		Crear un objeto símbolo (token)		
		Crear vínculos simbólicos	BUILTIN\Administradores	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Denegar el acceso a este equipo desde la red	BUILTIN\Invitados, NT AUTHORITY\ANONYMOUS LOGON
		Denegar el inicio de sesión como servicio	BUILTIN\Invitados
		Denegar el inicio de sesión como trabajo por lotes	BUILTIN\Invitados
		Denegar el inicio de sesión local	BUILTIN\Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	BUILTIN\Administradores
		Forzar cierre desde un sistema remoto	BUILTIN\Administradores
		Generar auditorías de seguridad	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Generar perfiles de un solo proceso	BUILTIN\Administradores
		Generar perfiles del rendimiento del sistema	BUILTIN\Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	
		Hacer copias de seguridad de archivos y directorios	BUILTIN\Administradores
		Iniciar sesión como proceso por lotes	
		Iniciar sesión como servicio	
		Modificar la etiqueta de un objeto	
		Modificar valores de entorno firmware	BUILTIN\Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Omitir comprobación de recorrido	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores, NT AUTHORITY\Usuarios autenticados	
		Permitir el inicio de sesión local	BUILTIN\Usuarios, BUILTIN\Administradores	
		Permitir inicio de sesión a través de Servicios de Escritorio remoto		
		Realizar tareas de mantenimiento del volumen	BUILTIN\Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red	
		Restaurar archivos y directorios	BUILTIN\Administradores	
		Tener acceso a este equipo desde la red	BUILTIN\Usuarios, BUILTIN\Administradores	
		Tomar posesión de archivos y otros objetos	BUILTIN\Administradores	
11.Verifique las opciones de seguridad en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	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	Habilitado
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitado
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitado
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitado
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitado
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitado
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitado
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitado
		Auditoría: auditar el acceso de objetos globales del sistema	Habilitado
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitado
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitado
		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	Habilitado
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitado
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Habilitado
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitado
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitado
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitado
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitado
		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.

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	Habilitado
		Cuentas: estado de la cuenta de invitado	Deshabilitado
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitado
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitado
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitado
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitado
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		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	Habilitado
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitado
		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	Deshabilitado
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitado
		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)	Habilitado
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitado
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitado
		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	Habilitado
		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 Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
12.Verifique el registro de eventos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”		
		Directiva	Valor	OK/NOK
		Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro de seguridad	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro del sistema	Habilitado	
13.Verifique los servicios del sistema definidos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”		
		Nota: 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 para cada servicio. En la ventana del editor de administración de directivas de grupo 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	vmicshutdwn	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	IpplattCfgSvc	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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
14.Verifique los valores del sistema de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos” Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".	
Archivo	Usuario	Permiso	OK/NOK
%ProgramFiles%\Netmeeting	Administradores	Control total	
	SYSTEM	Control total	
%Public%\	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%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	
15.Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
16.Verifique la directiva de almacén digital en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
17.Verifique la directiva de Antivirus en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitado	
18.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	
19.Verifique las directivas de biometría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Biometría”		
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
	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	
20.Verifique las directivas de búsqueda en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		Deshabilitado	
21.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
22.Verifique las directivas de reproducción automática en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar reproducción automática	Habilitado (Todas las unidades)	
		Establece el comportamiento predeterminado para la ejecución automática	Habilitado (No ejecutar ningún comando de ejecución automática)	
23.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar Windows SmartScreen de Windows defender	Habilitado (Advertir e impedir la omisión)	

Comprobación	OK/NOK	Cómo hacerlo		
24.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	
25.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
26.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de Internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitado	
27.Verifique las directivas de Eliminar el historial de navegación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	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	
28.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”		
	Directiva		Valor	OK/NOK
	Configurar SmartScreen de Windows Defender		Deshabilitado	
29.Verifique las directivas de OneDrive en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive”		
	Directiva		Valor	OK/NOK
	Impedir el uso de OneDrive para almacenar archivos.		Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
30.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	Deshabilitado	
31.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitado (Solo HTTP (0))	

Comprobación	OK/NOK	Cómo hacerlo		
32.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	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 accedan a la información de la cuenta	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)	
33.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

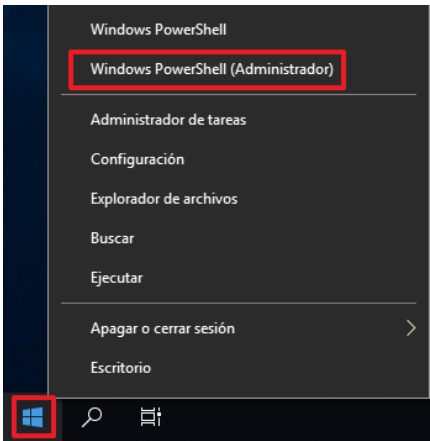
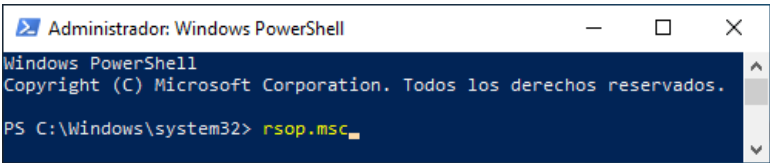
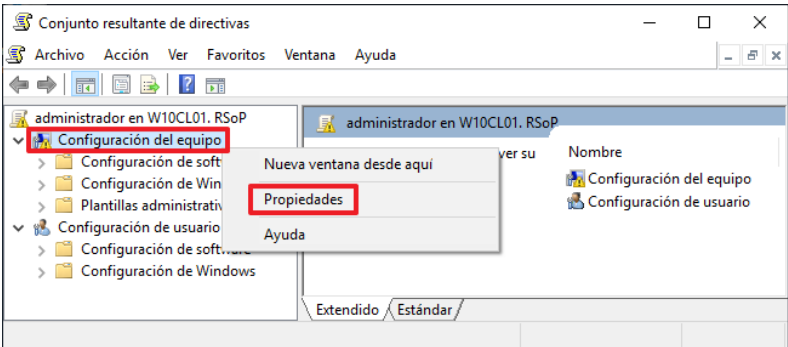
Comprobación	OK/NOK	Cómo hacerlo		
34.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”		
		Directiva	Valor	OK/NOK
		Permitir acceso a Shell remoto	Deshabilitado	
35.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
36.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK

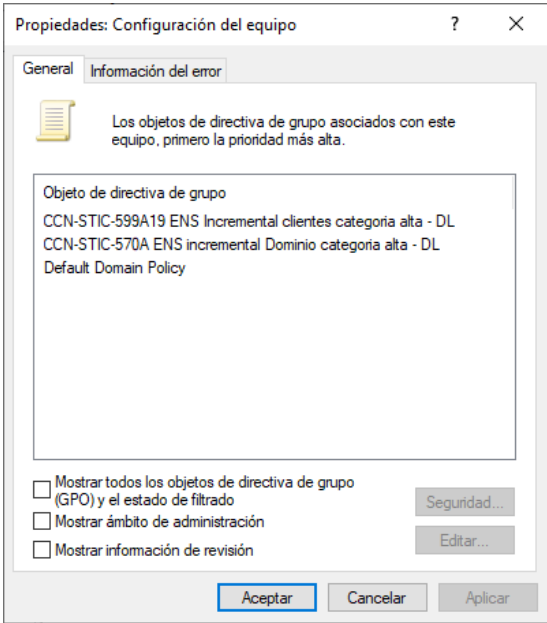
Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
37.Verifique la directiva de Tienda en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitado	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitado	
38.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
39.Verifique la directiva de Windows Update en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	
40.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
41.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
42.Verifique la directiva de Net Logon en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Net Logon”		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitado	
43.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
		Desactivar el identificador de publicidad	Habilitado	
44.Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador.		Inicie sesión en el equipo que está comprobando con una cuenta de usuario de Windows con permisos de administrador.		

Comprobación	OK/NOK	Cómo hacerlo
45.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. 
46.Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse “Enter” para abrir la consola de administración "Conjunto resultante de directivas": 
47.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL".		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura. 

Comprobación	OK/NOK	Cómo hacerlo
		En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las políticas deberán aparecer y "CCN-STIC-599A19 ENS incremental clientes categoria alta - DL" deberá estar situada encima de la GPO que se establece a nivel de dominio, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

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). Dentro de la solución se integra la característica de MBAM (Administración y supervisión de Microsoft BitLocker) que va a permitir centralizar la administración de BitLocker, así como una gestión eficiente de las claves de recuperación. Para más información sobre MBAM, puede consultar la siguiente URL:

<https://technet.microsoft.com/en-us/itpro/mdop/mbam-v25/about-mbam-25-sp1>

La implementación de BitLocker requiere de unos requisitos específicos de tipo hardware y software:

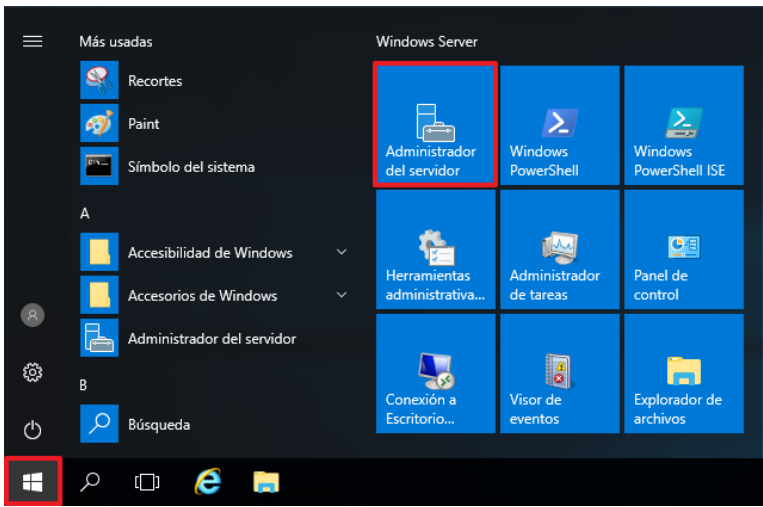
- a) Un equipo que cumpla los requisitos mínimos para Windows 10.
- b) Un chip TPM versión 1.2 o 2.0 activado. La activación de dicho chip se realiza a través de la BIOS, siendo necesaria su implementación para garantizar su funcionalidad.
- c) BIOS compatible con TCG (Trusted Computing Group).
- d) 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 sin darse cuenta. Una vez que la unidad está preparada, debe reiniciarse el equipo.

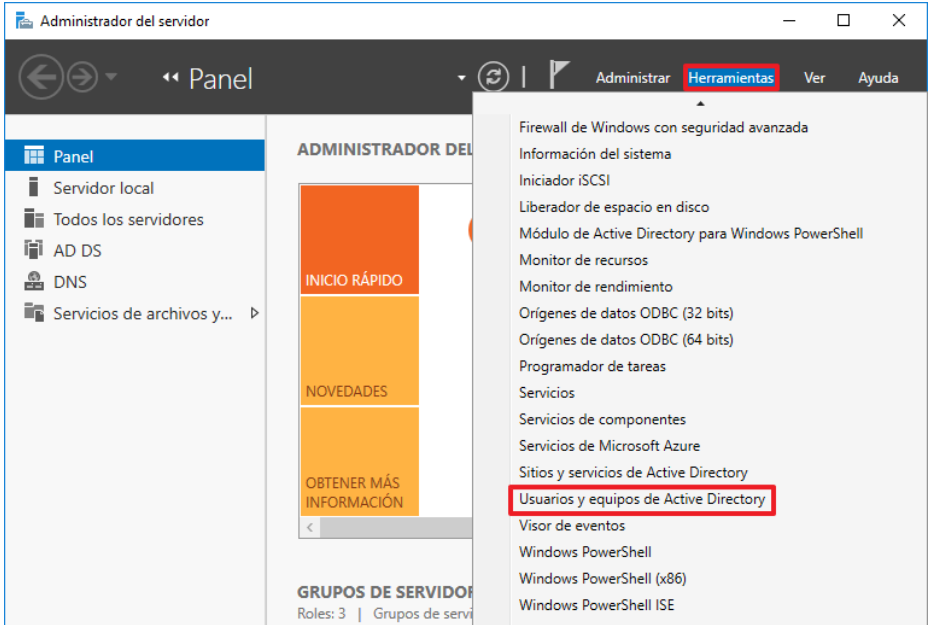
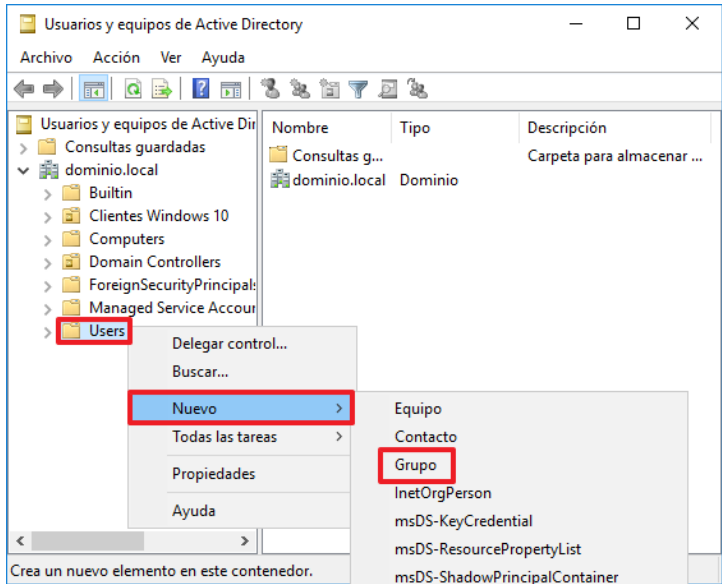
No obstante, si se ha realizado una instalación por defecto de Windows 10, el programa de instalación ya habrá creado durante la instalación las dos particiones de disco necesarias para activar BitLocker.

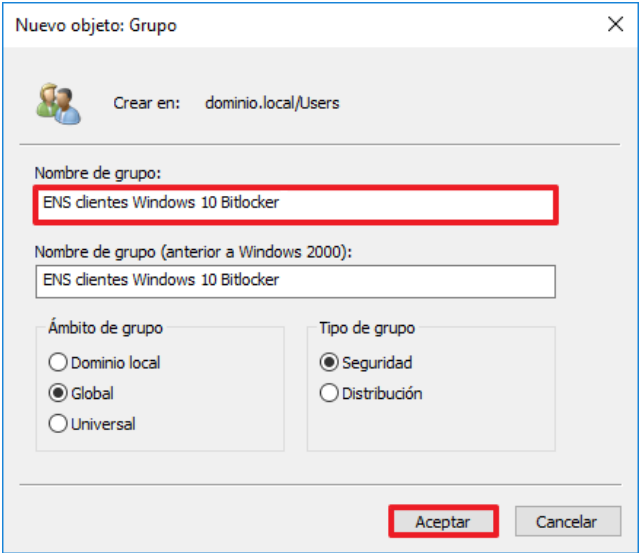
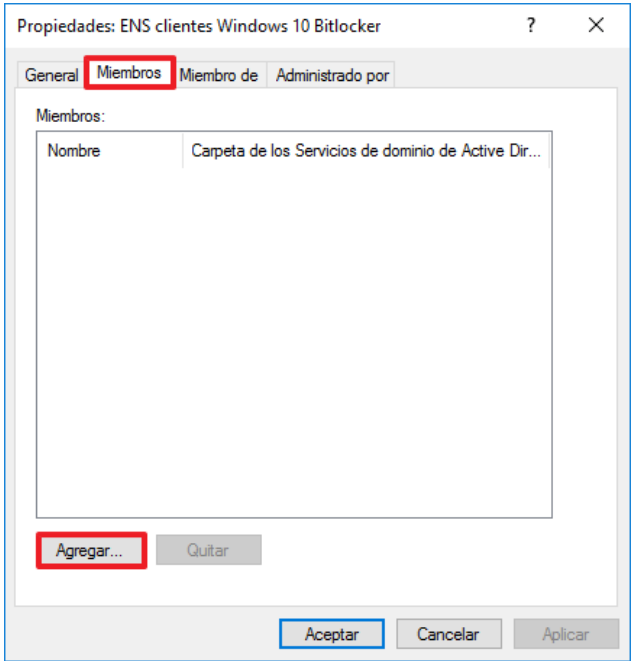
- a) Una unidad flash USB para almacenar claves de inicio y recuperación.
- b) Una configuración BIOS para iniciar primero desde el disco duro, no desde las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como la clave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

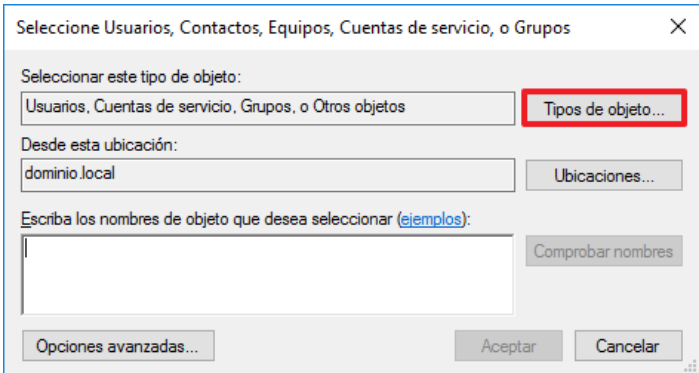
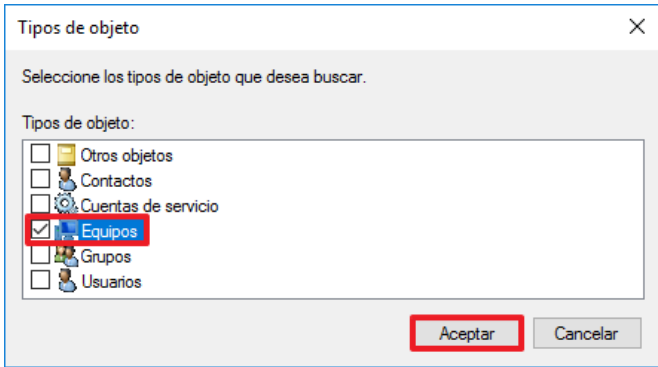
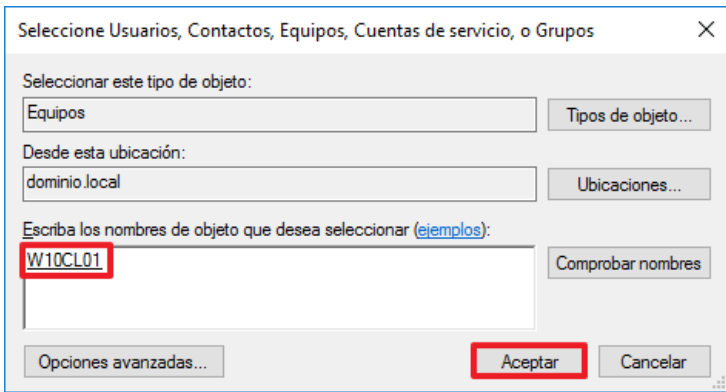
1. PREPARACIÓN DE DOMINIO

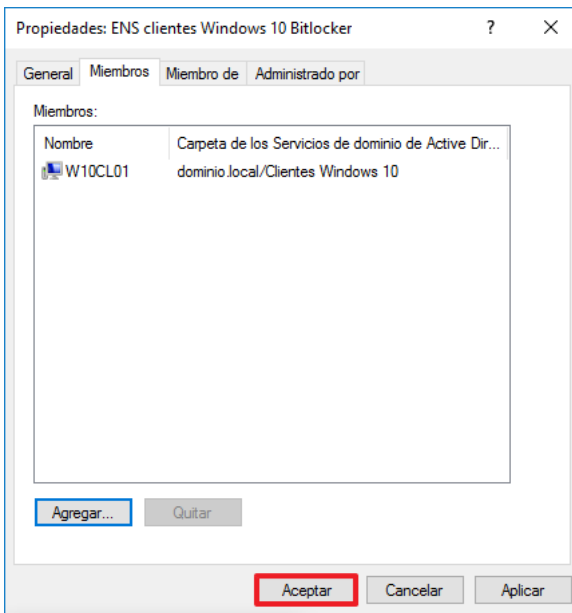
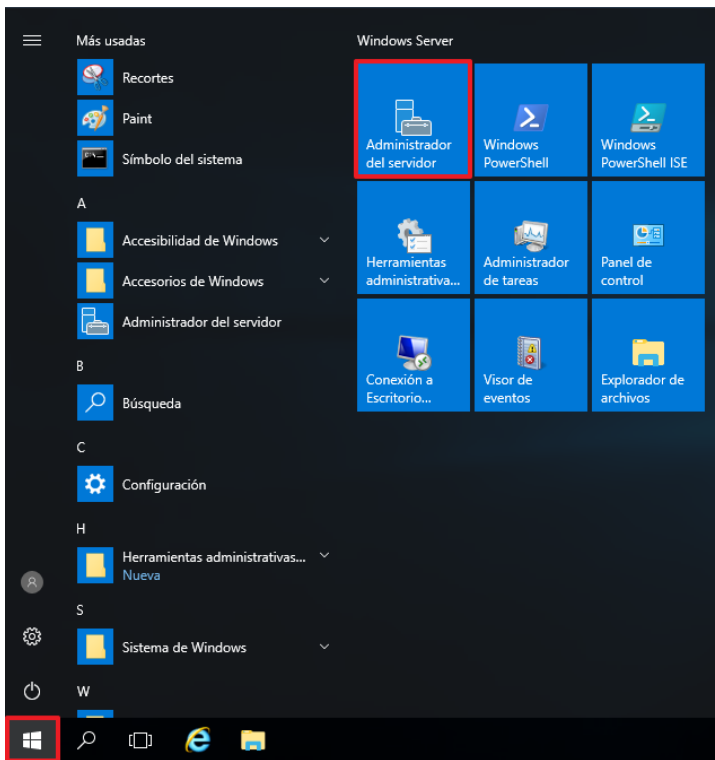
La implementación de BitLocker se basará en la aplicación de una política de seguridad aplicada sobre un grupo de equipos determinados. Para ello deberán seguirse los siguientes pasos.

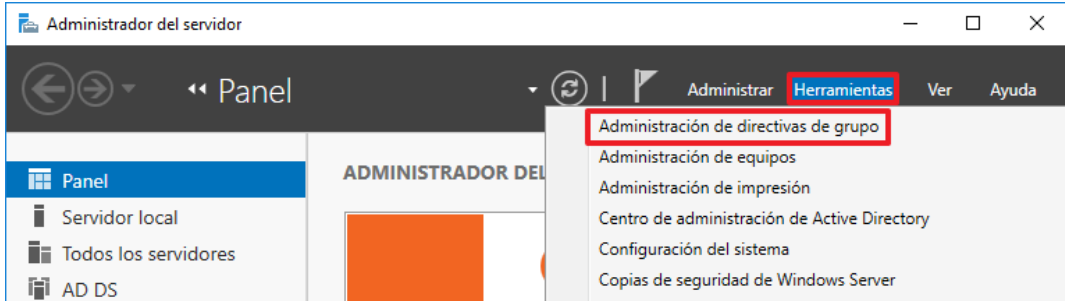
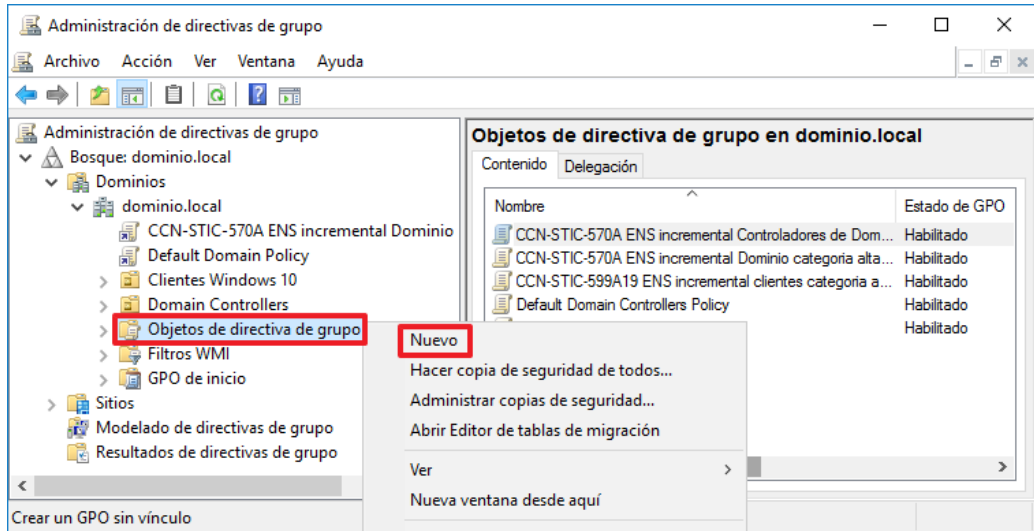
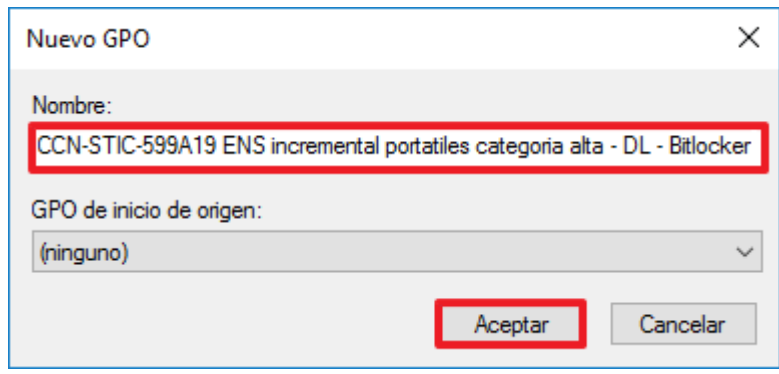
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
5.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

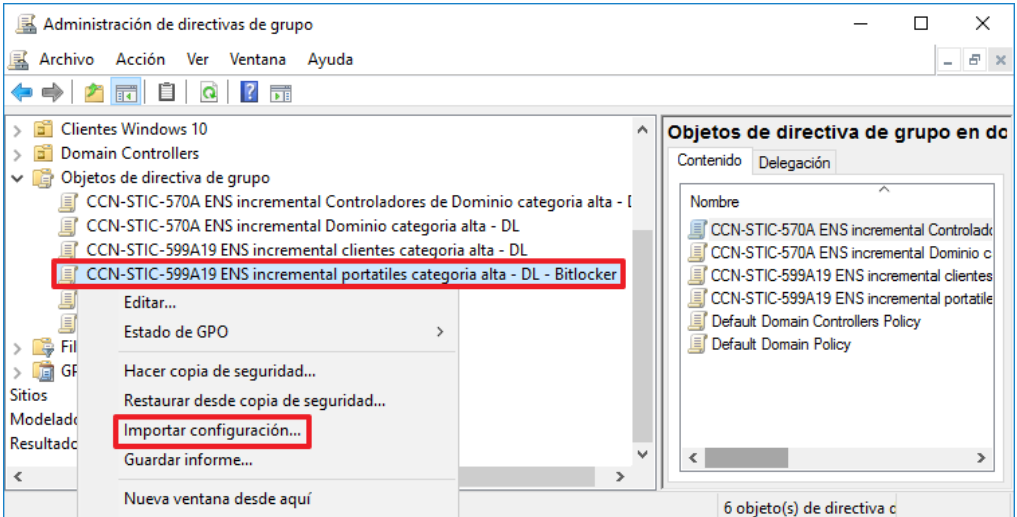
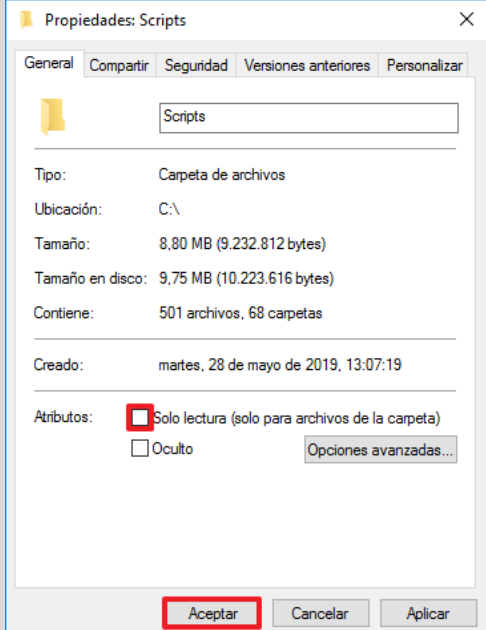
Paso	Descripción
6.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
7.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

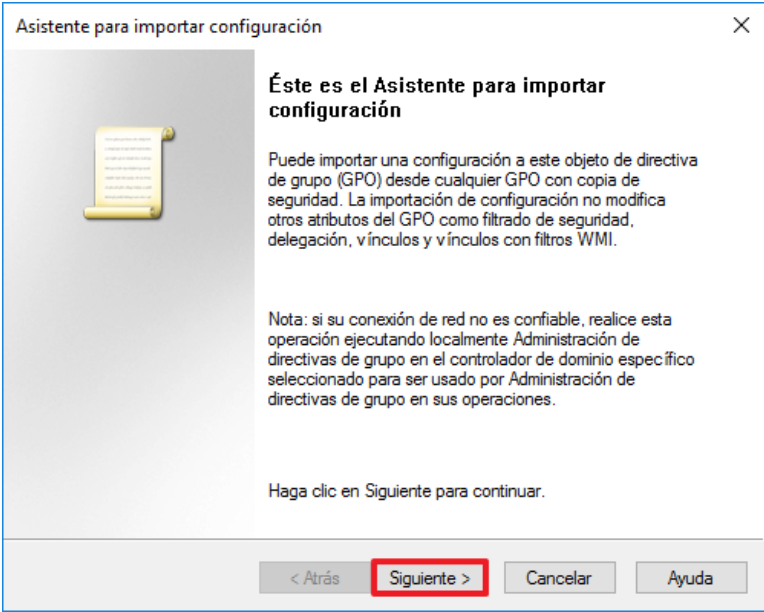
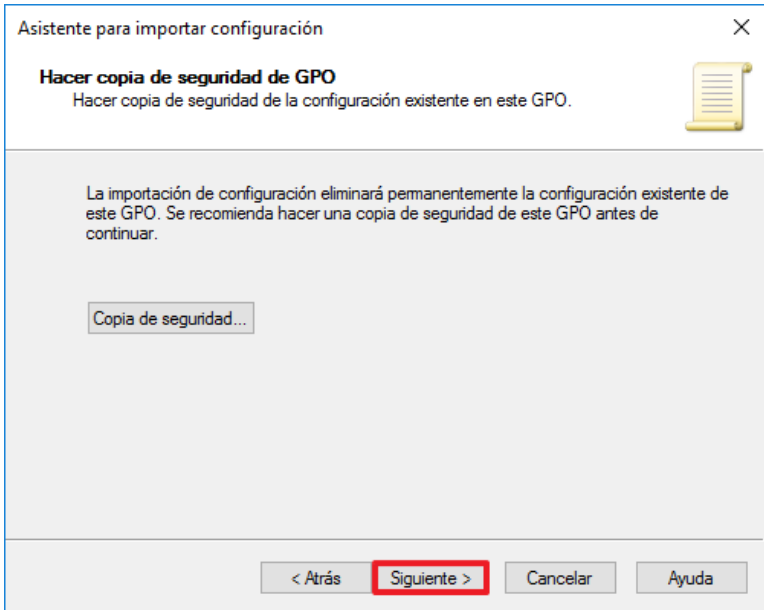
Paso	Descripción
8.	Introduzca como nombre “ENS clientes Windows 10 BitLocker”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio sobre los que se vaya a realizar implementación de BitLocker. 
9.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.
10.	Pulse el botón “Agregar...”. 

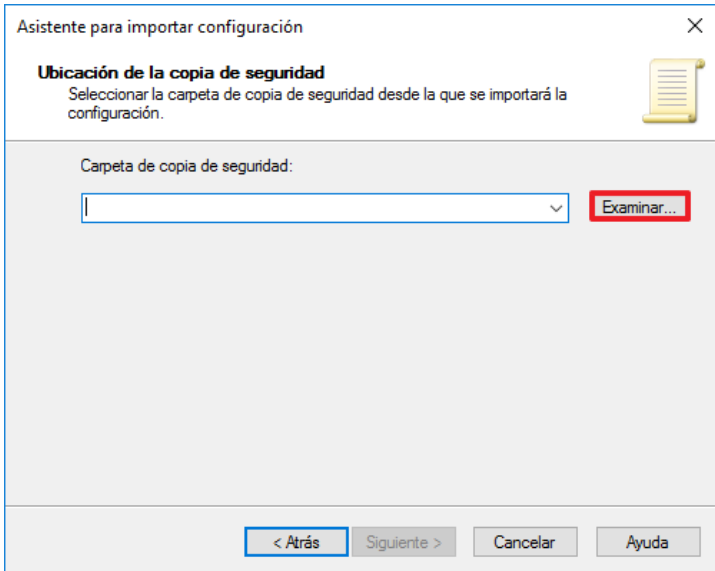
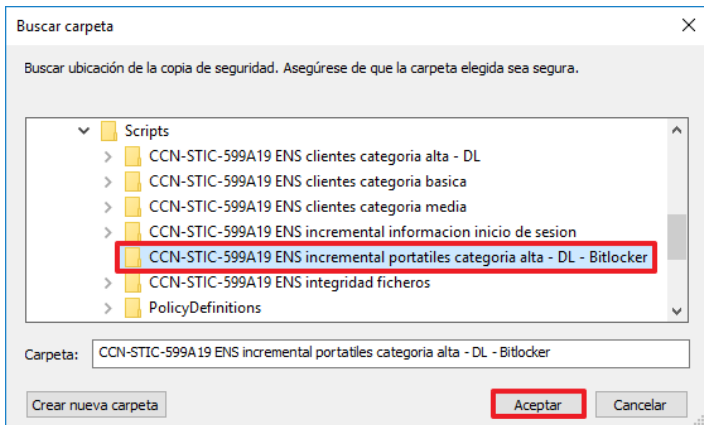
Paso	Descripción
11.	Pulse el botón “Tipos de objeto...”. 
12.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
13.	Introduzca el nombre o utilice las opciones avanzadas para agregar aquellos portátiles que manejen datos de categoría alta para los que debe garantizarse la confidencialidad o bien aquellos equipos que desee proteger mediante el cifrado de unidad BitLocker.  Nota: No agregue servidores a este grupo.
14.	Pulse el botón “Aceptar” para agregar la selección.

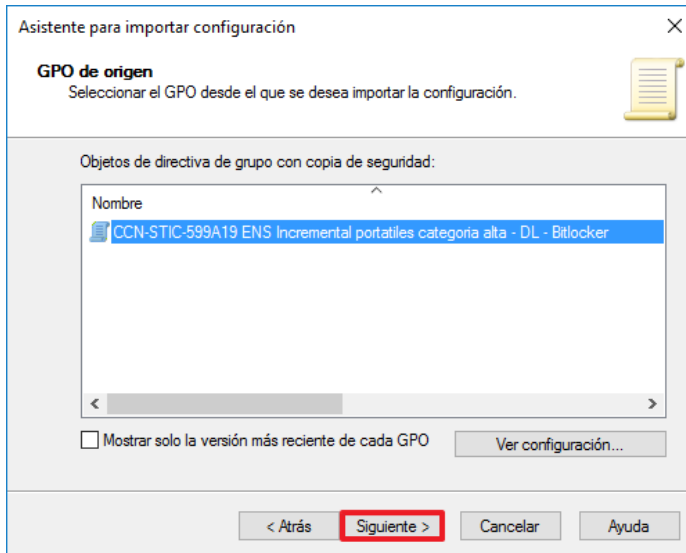
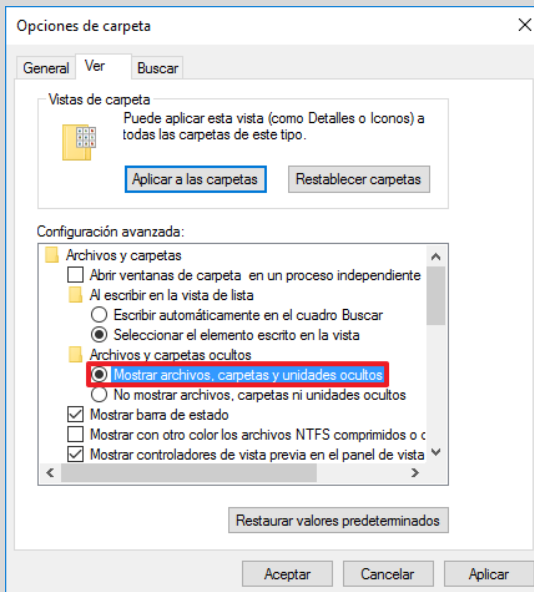
Paso	Descripción
15.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

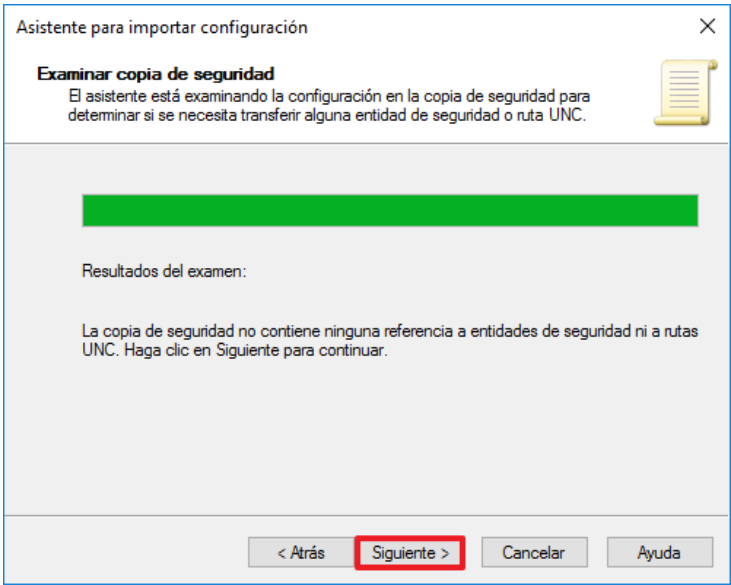
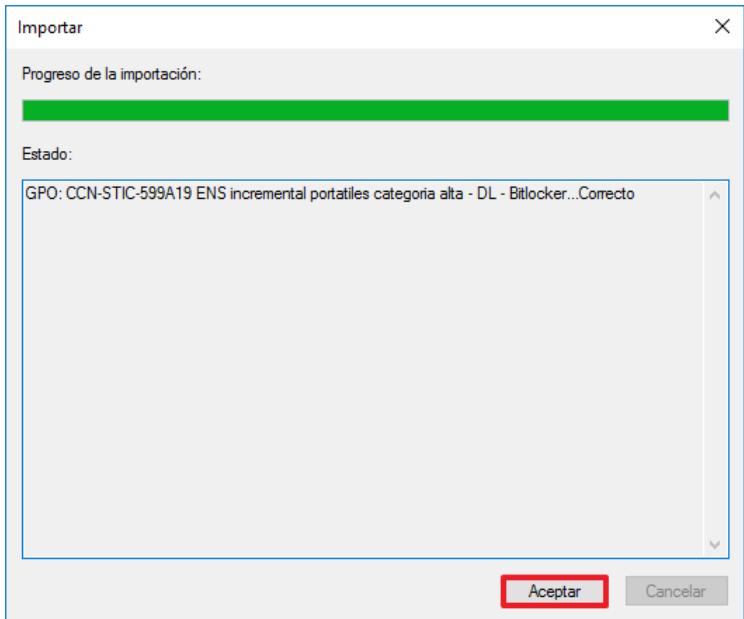
Paso	Descripción
18.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo” 
19.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
20.	Pulse con el botón derecho del ratón sobre dicho contenedor y seleccione la opción “Nuevo”. 
21.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental portátiles categoría alta – DL - BitLocker” y pulse el botón “Aceptar”. 

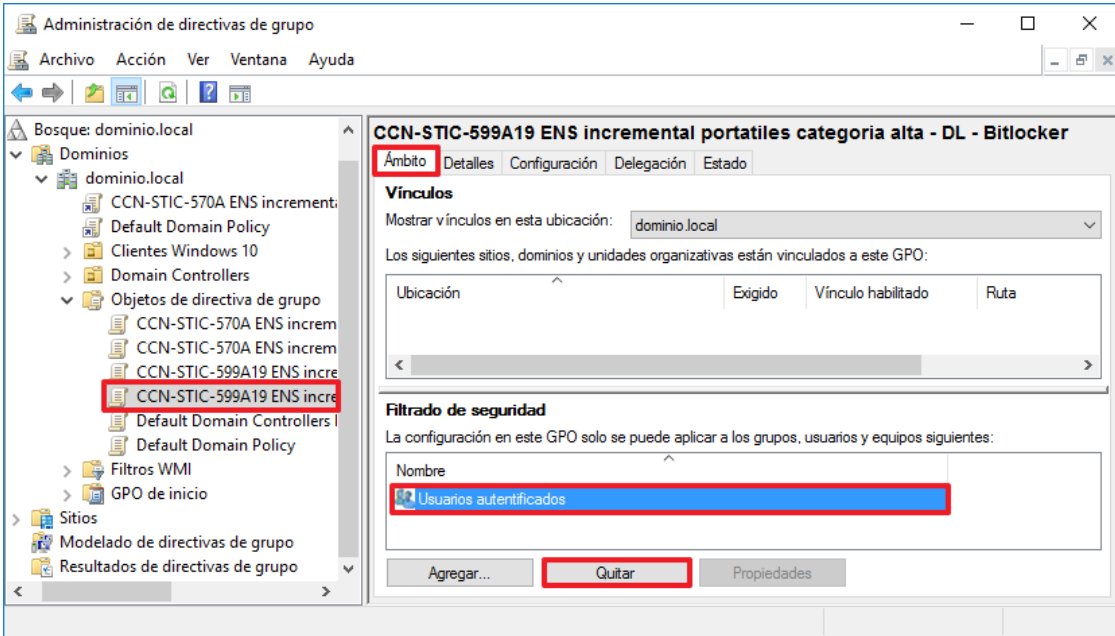
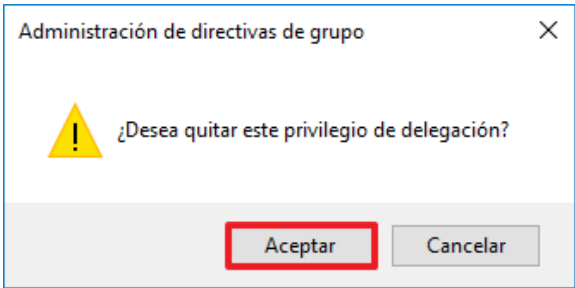
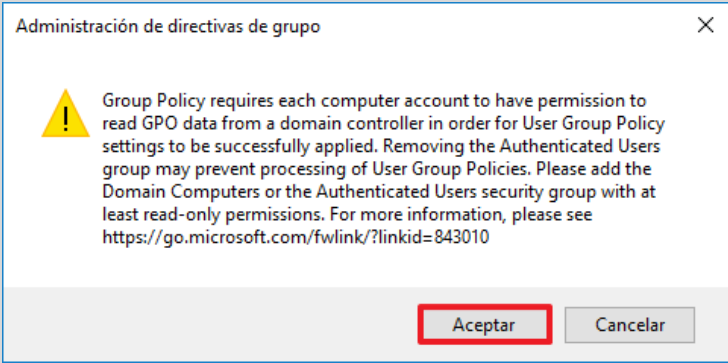
Paso	Descripción
22.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política, pulse con el botón derecho del ratón sobre la misma y seleccione la opción “Importar configuración...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts” no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

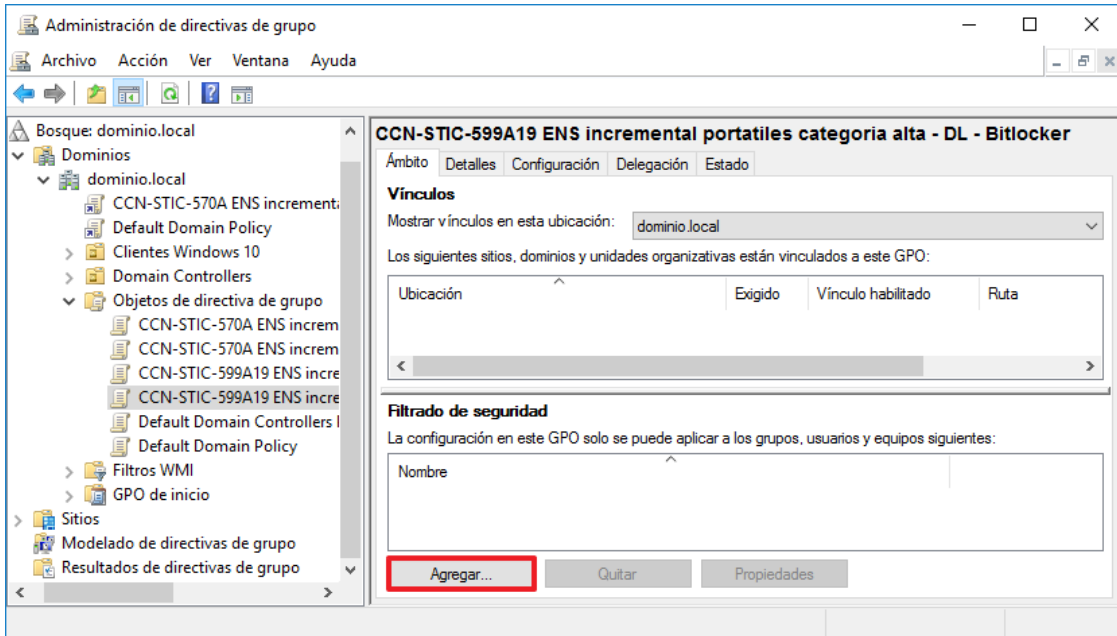
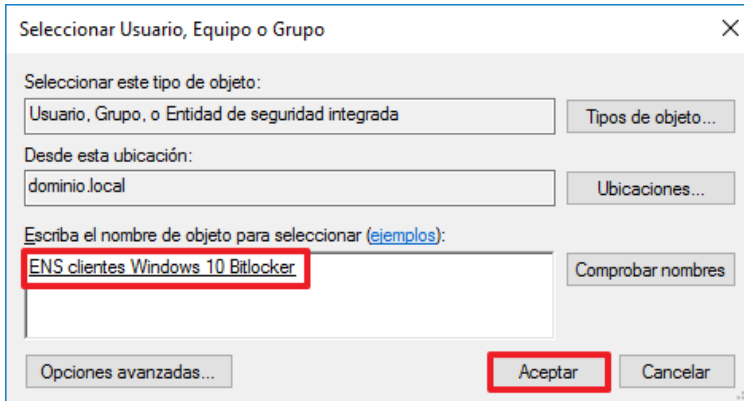
Paso	Descripción
23.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
24.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

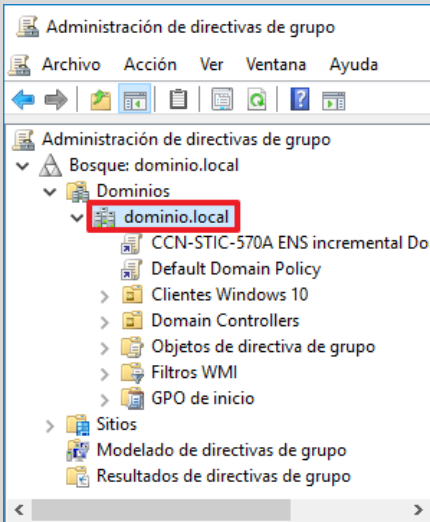
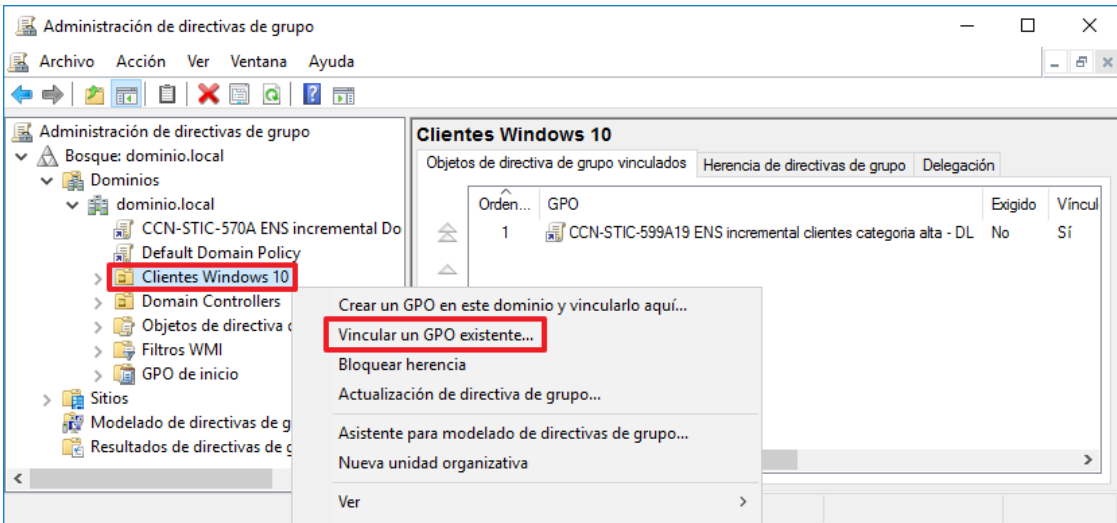
Paso	Descripción
25.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
26.	Seleccione la carpeta “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
27.	Pulse el botón “Siguiete >” cuando haya sido seleccionada la carpeta correspondiente.

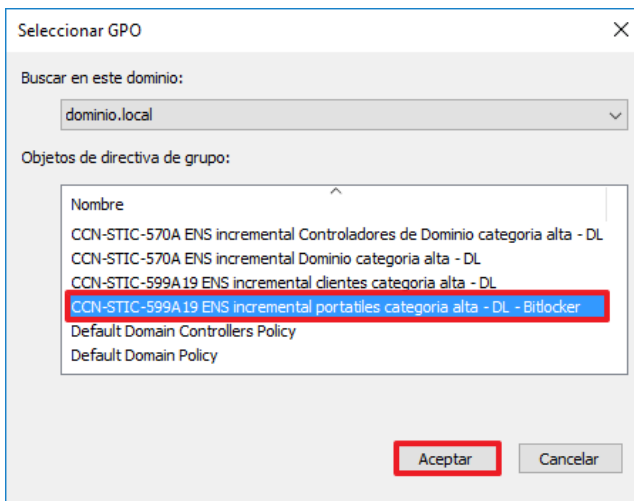
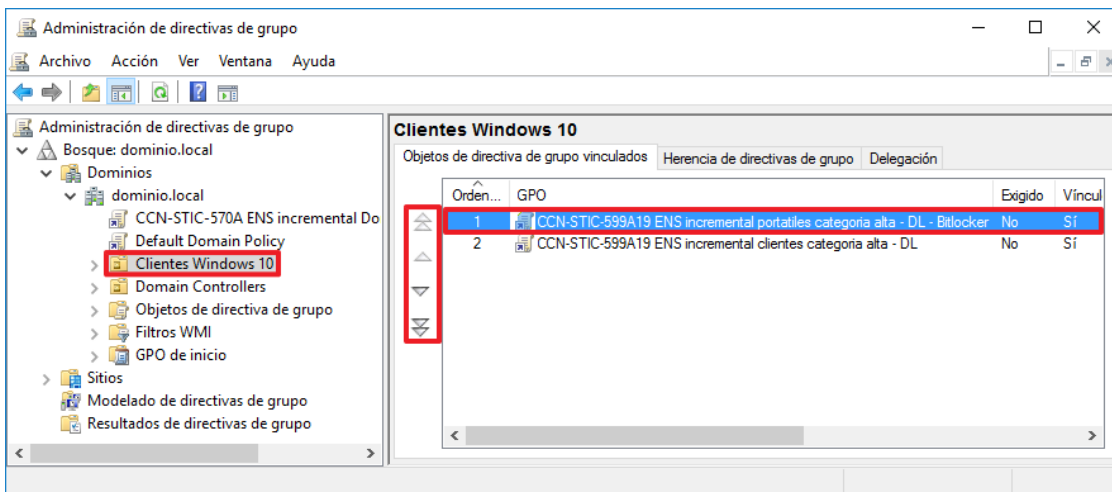
Paso	Descripción
28.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

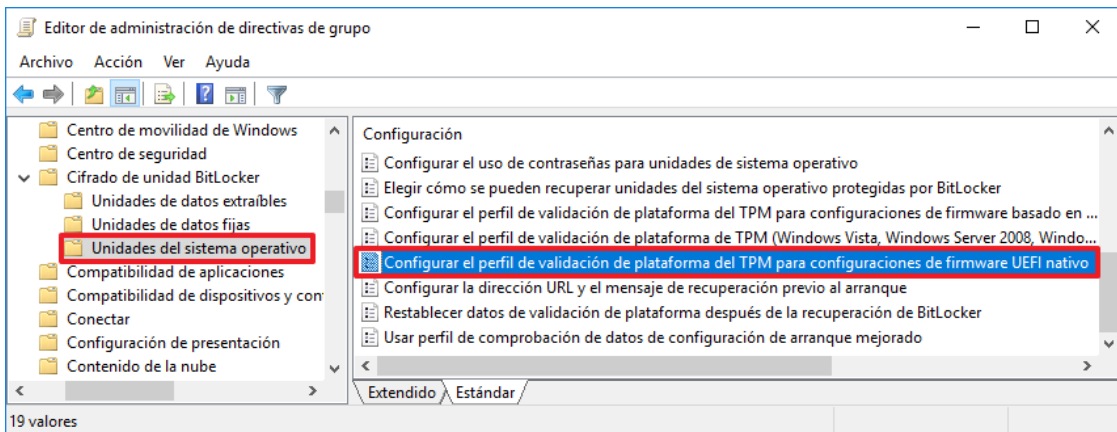
Paso	Descripción
29.	En la pantalla de examen, pulse el botón “Siguiente >”. 
30.	Para completar el asistente pulse el botón “Finalizar”.
31.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración. 

Paso	Descripción
32.	En el apartado “Filtrado de seguridad” del objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker”, seleccione la pestaña “Ámbito”, marque “Usuarios autenticados” y pulse el botón “Quitar”. 
33.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
34.	Una vez quitado, pulse el botón “Agregar...”. 
35.	Introduzca como nombre “ENS clientes Windows 10 BitLocker”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 

Paso	Descripción
36.	Identifique las ubicaciones donde se encuentran los portátiles Windows 10 donde desea realizar la aplicación del cifrado de unidad BitLocker. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC ENS incremental portátiles alto BitLocker”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” lugar donde se encuentran ubicados los clientes existentes en este entorno. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminadas de “computers” y no los haya movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 
37.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente, en el ejemplo “Clientes Windows 10”, y seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
38.	Seleccione la política “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker” y pulse el botón “Aceptar”. 
39.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental portátiles categoria alta - DL - BitLocker” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dichas Unidades Organizativas. 

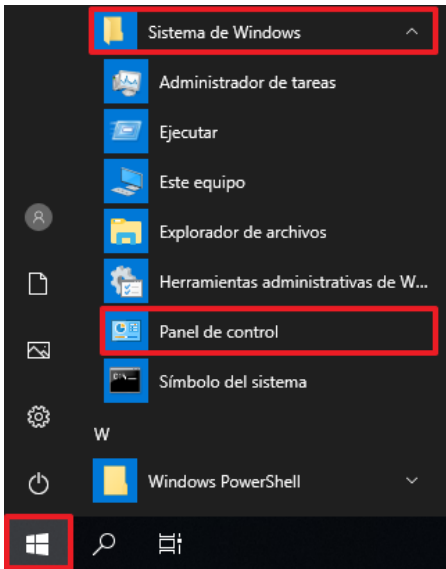
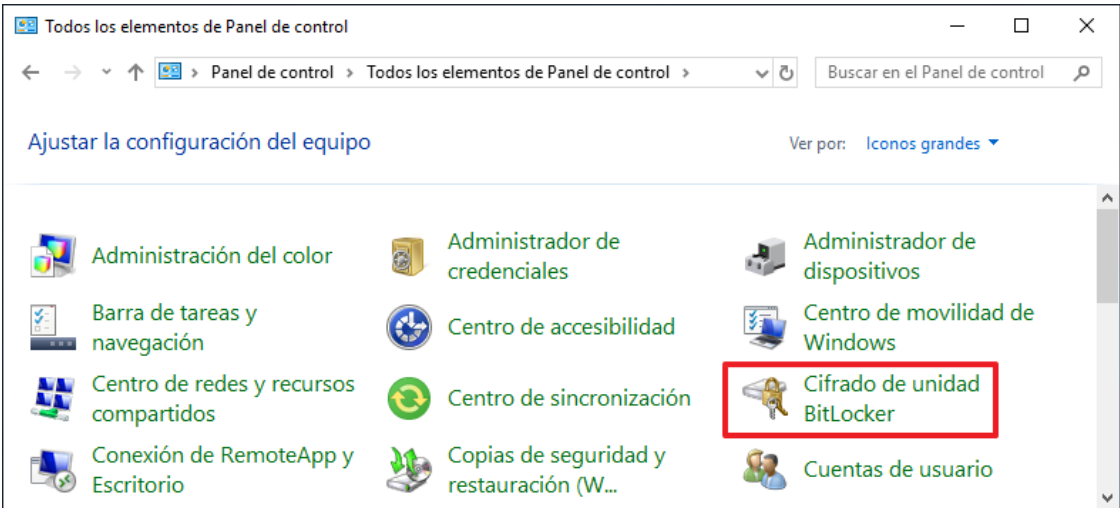
Paso	Descripción
40.	La configuración importada en la GPO desde la copia de seguridad establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si dispone de equipos con firmware UEFI nativo, deberá habilitar y configurar la directiva “Directiva CCN-STIC-599A19 ENS incremental portatiles categoria alta – DL - Bitlocker → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo → Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo” de la GPO configurada en este apartado. 
41.	Cierre la herramienta “Administración de directivas de grupo”.
42.	Elimine la carpeta “C:\Scripts”.

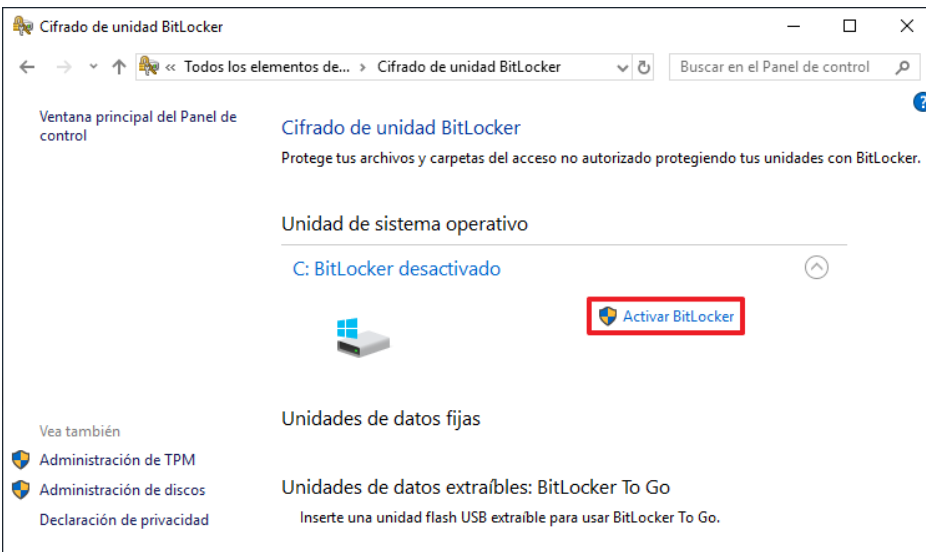
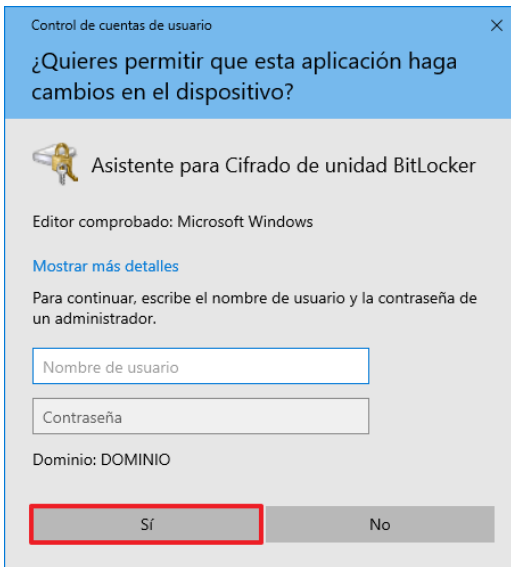
2. CONFIGURACIÓN DE BITLOCKER EN EL PUESTO CLIENTE

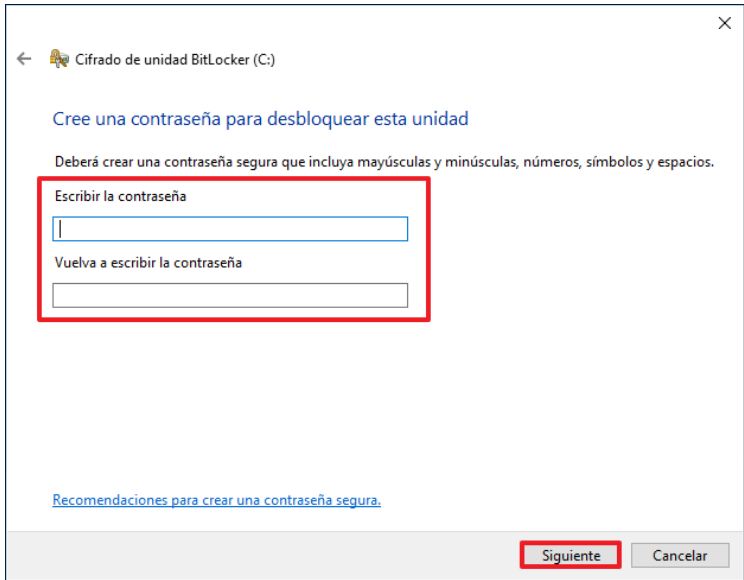
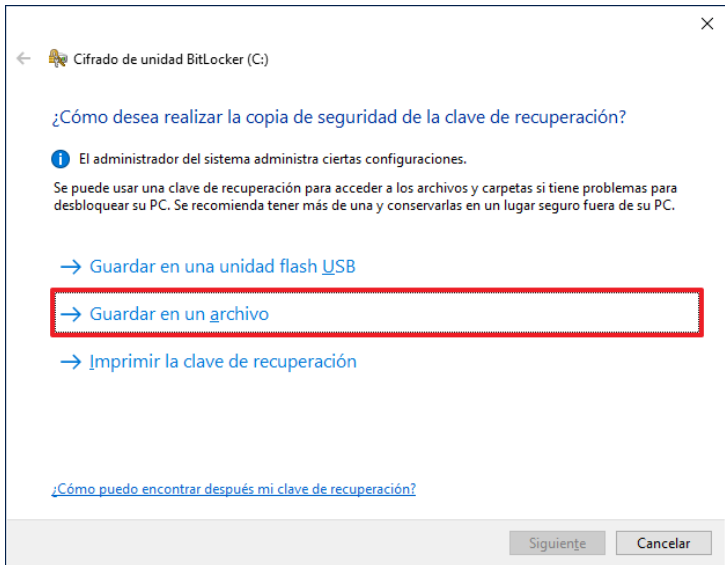
El presente punto establece los pasos que deberá efectuar el operador para realizar la implementación de BitLocker en los clientes, así como la aplicación de una contraseña para el desbloqueo de la unidad.

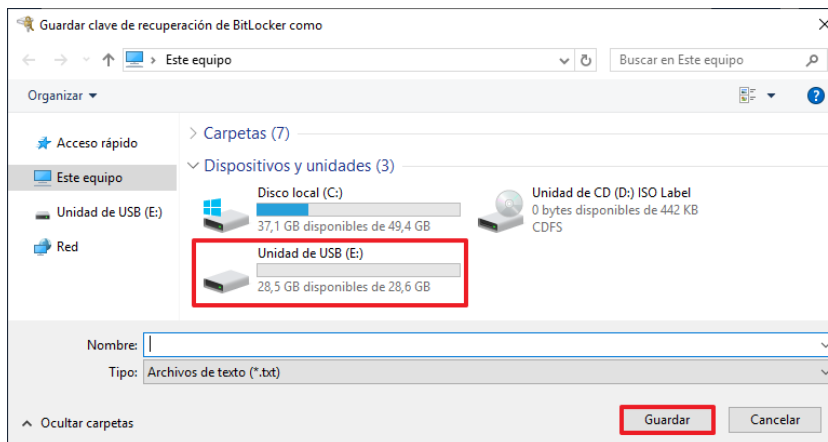
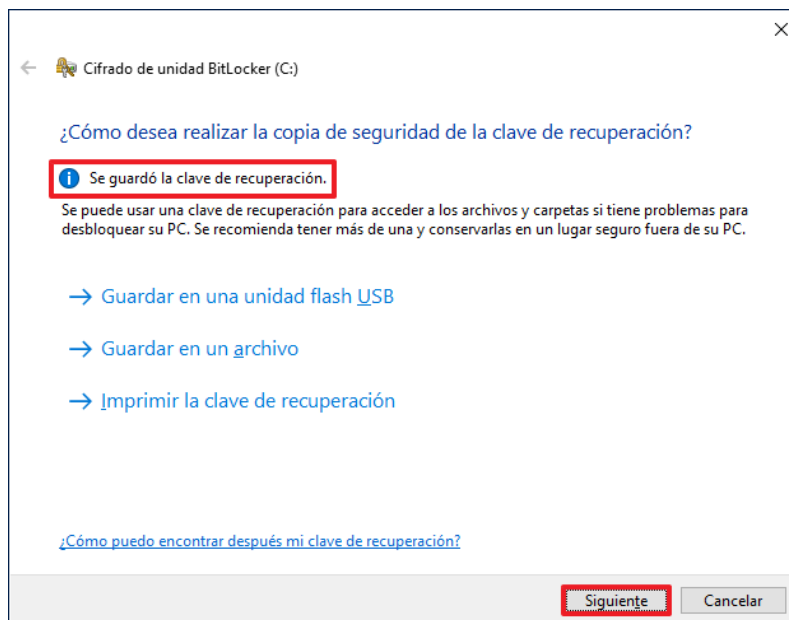
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números.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

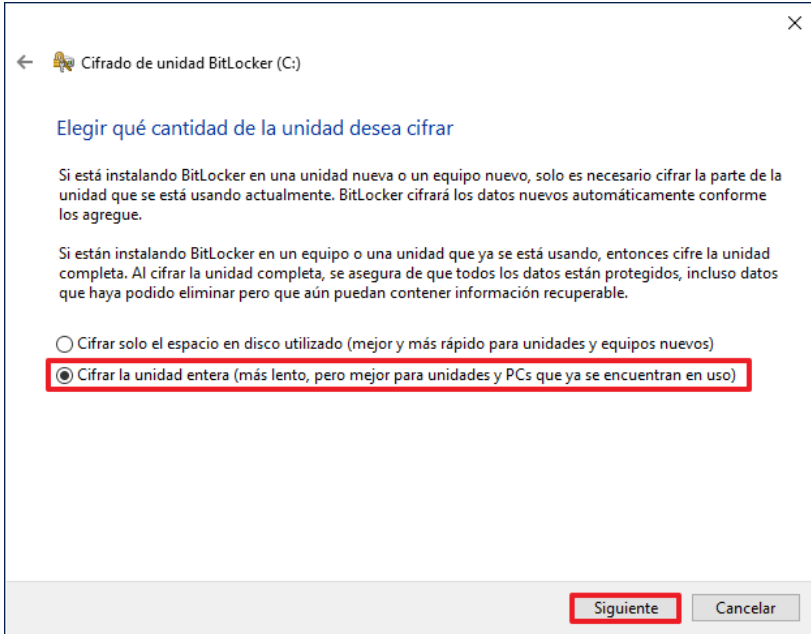
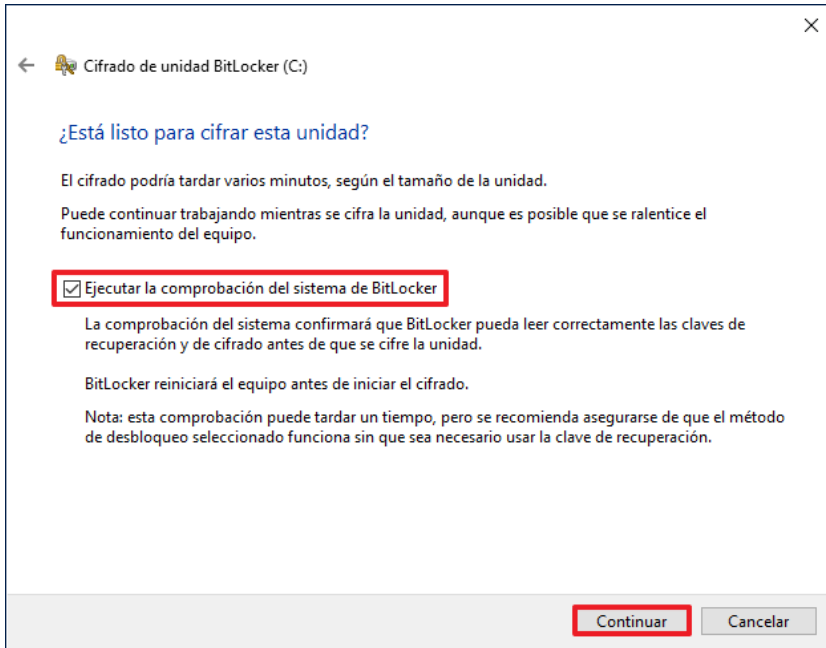
Paso	Descripción
43.	Si el equipo estaba arrancado, inicie sesión en el cliente donde desee realizar implementación del cifrado de BitLocker y reinicie el equipo. Si el equipo estaba apagado y lo ha arrancado siga en el siguiente paso. El reinicio permitirá que el equipo le sea de aplicación la membresía al grupo creado, así como la aplicación de la política de BitLocker.
44.	Inicie sesión en el cliente con un usuario con privilegio de administrador.

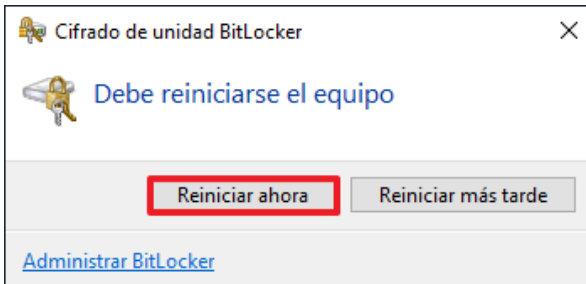
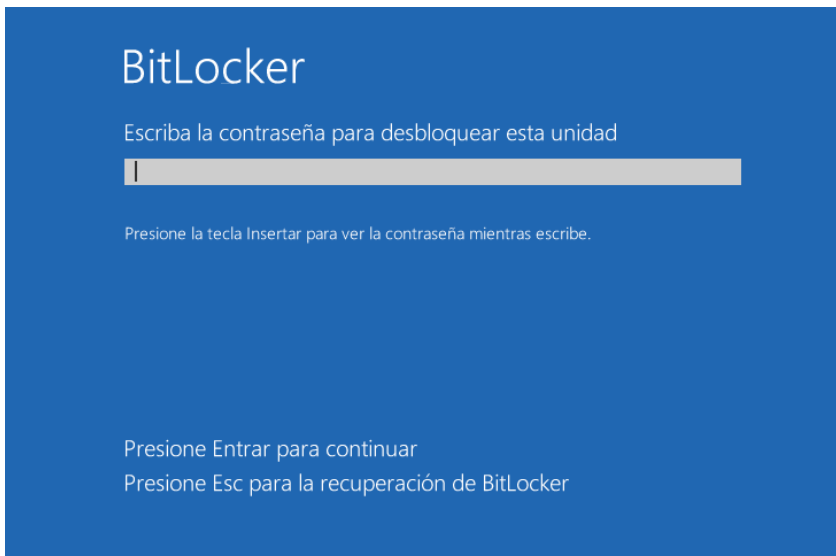
Paso	Descripción
45.	Abra el panel de control desde “Inicio → Sistema de Windows → Panel de control”. 
46.	Seleccione dentro del “Panel de control” el apartado “Cifrado de unidad BitLocker”.  Nota: Tenga en cuenta la visualización del Panel de control. En la parte superior derecha podrá cambiar el modo en que se muestran los iconos.

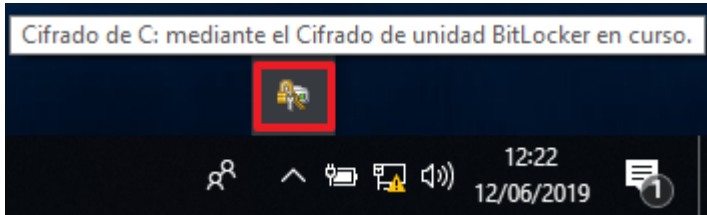
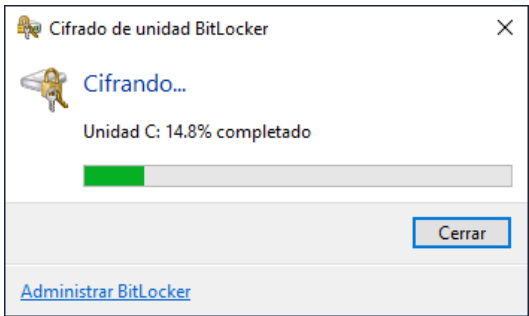
Paso	Descripción
47.	Pulse sobre “Activar BitLocker” como se indica en la siguiente imagen. 
48.	El sistema le solicitará elevación de privilegios. Introduzca credenciales de un usuario con privilegios de administrador en la ventana “Control de cuentas de usuario”. 

Paso	Descripción
49.	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.
50.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
51.	Seleccione la ubicación de la memoria 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.
52.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

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

Paso	Descripción
55.	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 45 a 55, pero en este último paso pulse sobre la opción “Reiniciar más tarde” y reinicie el equipo manualmente mediante la ruta “Inicio → “Iniciar/Apagar””. 
56.	Al reiniciar, el sistema le pedirá la contraseña de cifrado de unidad BitLocker. Introduzca la contraseña y pulse “Enter” para continuar. 

Paso	Descripción
57.	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.  Si marca con el ratón en él, o sobre 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.
58.	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.

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 del cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los clientes Windows 10. 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 una política de firewall dependerá de si los clientes presentan servicios o aplicaciones que necesitan la conexión remota desde otros sistemas, por ejemplo, si la organización emplea algún sistema para realizar tareas de soporte o asistencia remota. A partir de Windows Vista, Microsoft proporciona un servicio de cortafuegos con seguridad avanzada. Este 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: pública, privada o dominio.

De forma predeterminada el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local. No obstante, existe la posibilidad de realizar un control centralizado a través de la aplicación de objetos de políticas de grupo. Esta opción proporciona dos condiciones fundamentales:

- a) Mejorar las condiciones de seguridad, al establecer las mismas por parte de los administradores de dominio, sin que una alteración de tipo local afecte a dicha configuración.
- b) Centralizar la administración de tal forma que exista un único punto de control.

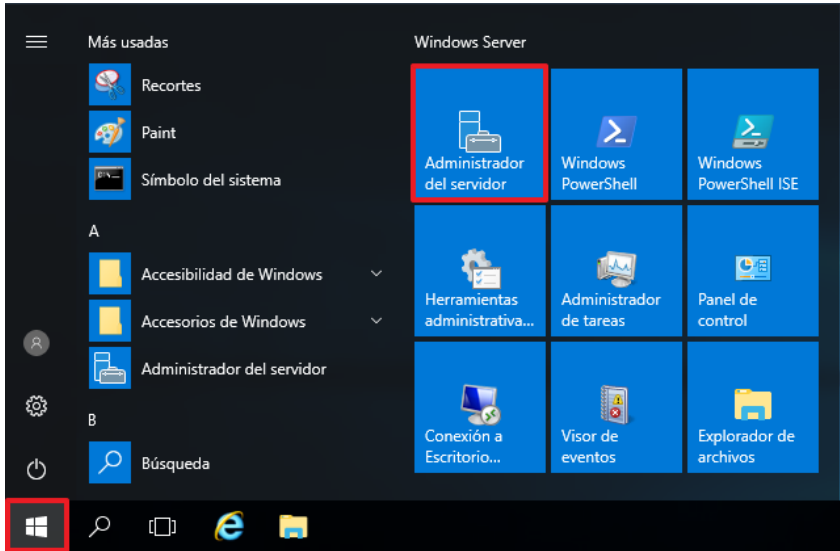
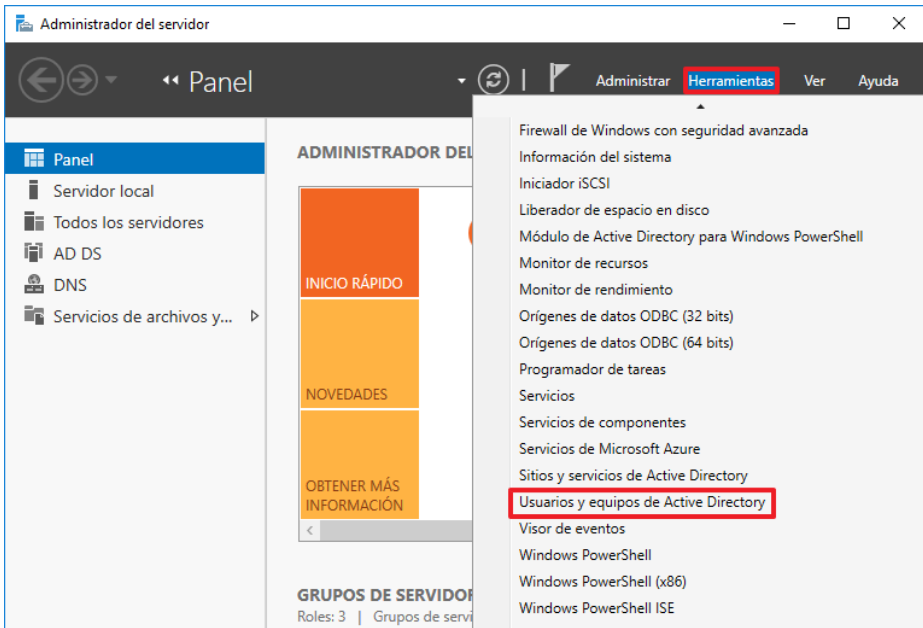
No obstante, este mecanismo de administración centralizado exige por parte de los administradores un control elevado y tener claro la creación y aplicación de diferentes políticas de seguridad en función de las necesidades demandadas por los servicios.

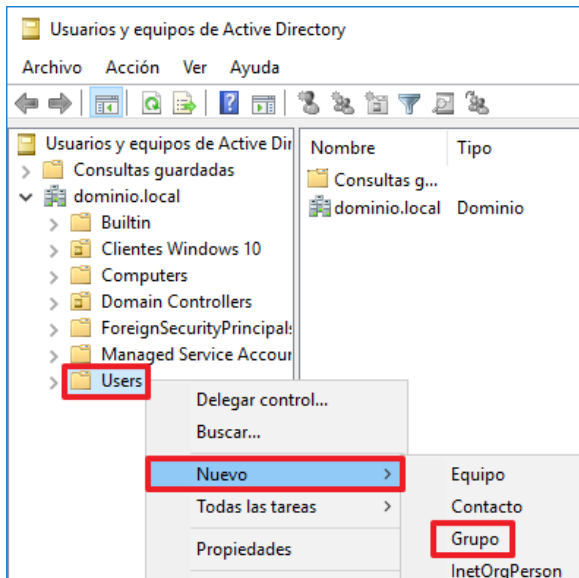
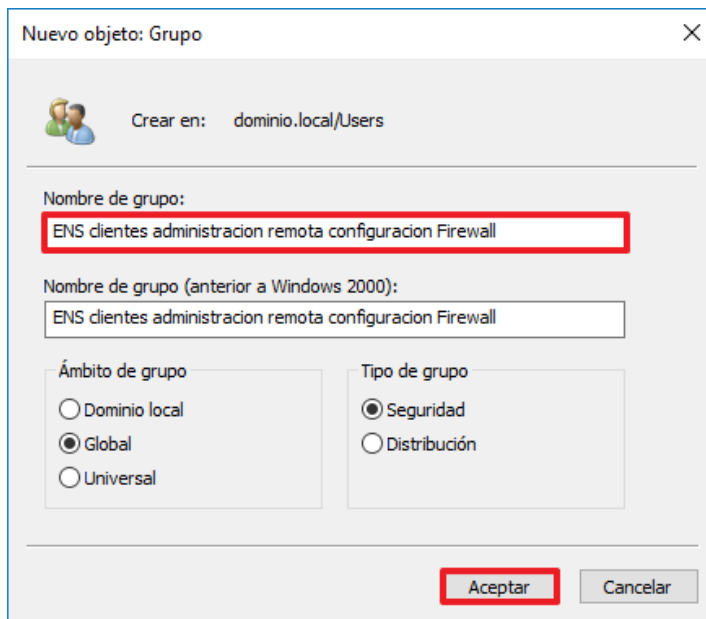
En este Anexo se darán recomendaciones necesarias para la creación y gestión de GPO para la administración centralizada de la seguridad del cortafuegos. Como en los Anexos previos, los operadores deberán realizar pruebas en entornos de preproducción antes de realizar una implementación en el entorno de producción.

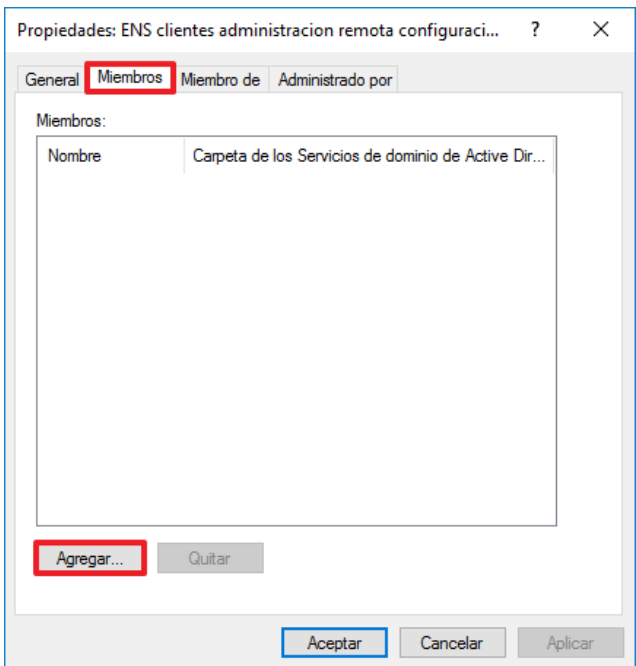
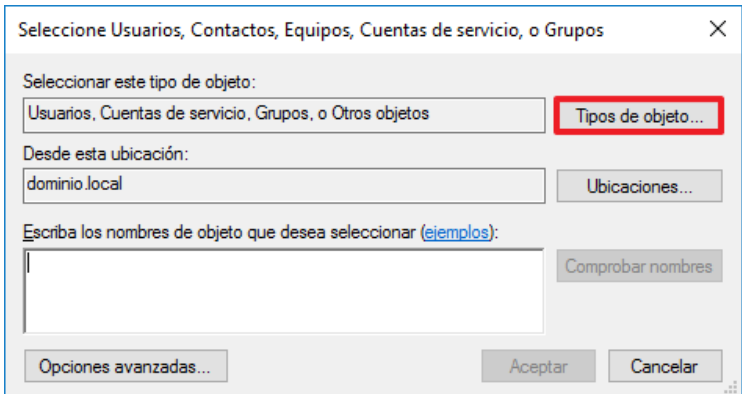
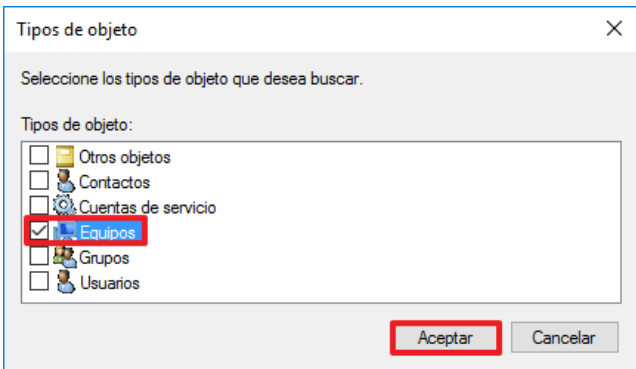
1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

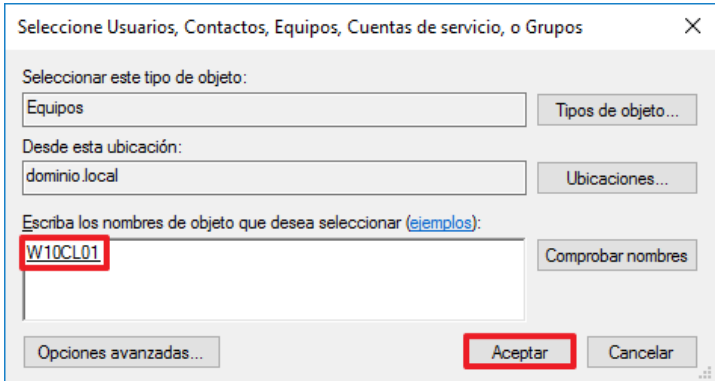
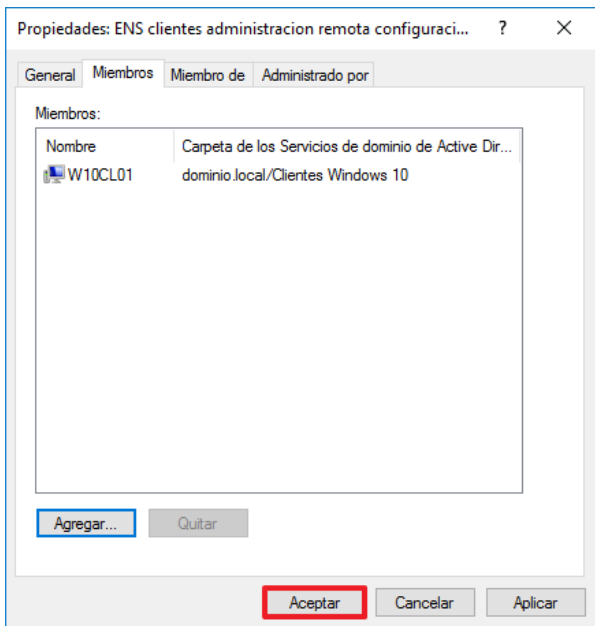
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos que permita la apertura de puertos para la realización de soporte remoto mediante el empleo de RDP (protocolo de escritorio remoto).

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
4.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 

Paso	Descripción
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
6.	Introduzca como nombre “ENS clientes administracion remota configuracion Firewall”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad en el cortafuegos.  Nota: Recuerde que este paso a paso es un ejemplo de cómo configurar un objeto de política de grupo para aplicar sobre un conjunto de clientes determinados con motivo de aplicarles una configuración específica. El presente ejemplo se basa en la agrupación de clientes sobre los que se va a realizar administración remota.
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.

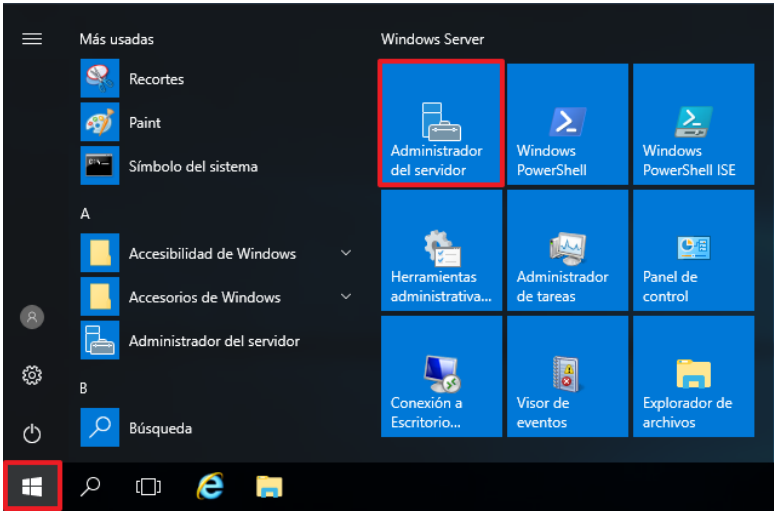
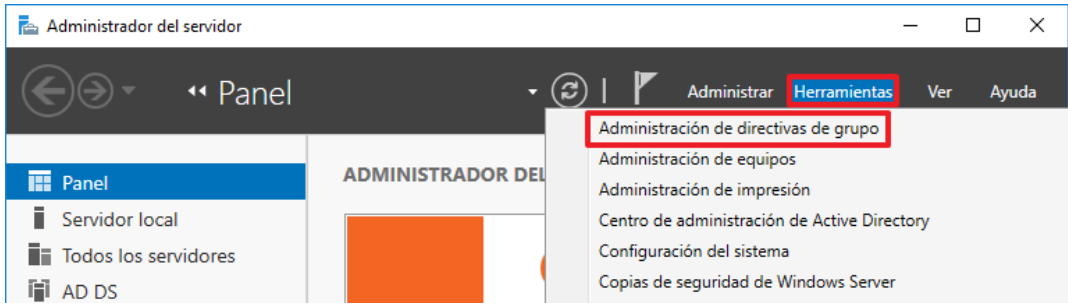
Paso	Descripción
8.	Pulse el botón “Agregar...”. 
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

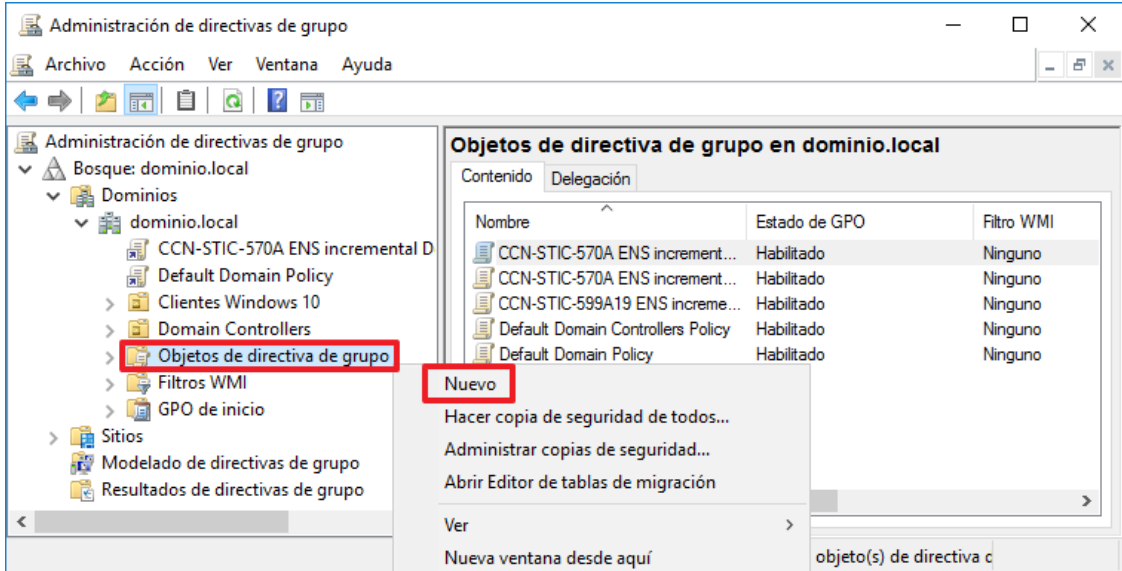
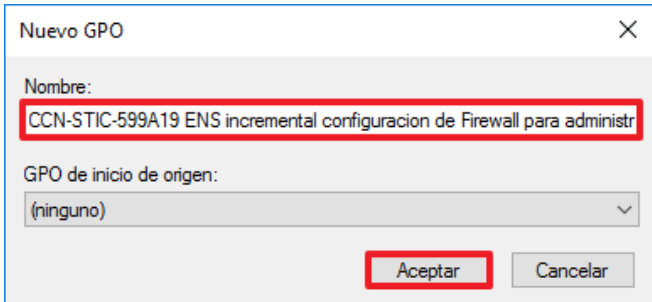
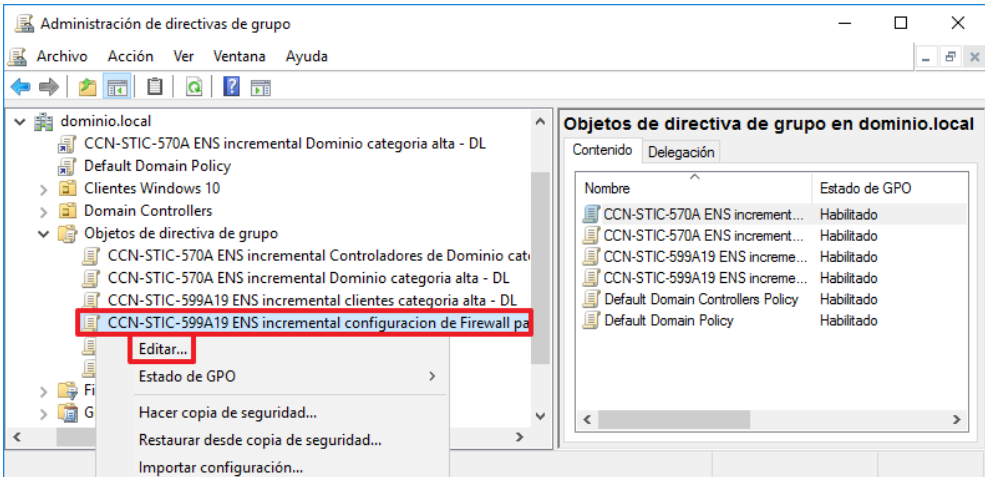
Paso	Descripción
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos equipos que cumplan las condiciones de aplicación de la GPO para la configuración del firewall. En este caso clientes sobre los que se vayan a efectuar tareas de administración remota con el protocolo RDP. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo. 
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”. Nota: El grupo creado, aunque en el ejemplo se va a emplear para la configuración del cortafuegos, se podría emplear para la aplicación de una configuración de seguridad aplicable a través de GPO diferente del resto de servidores de la organización.

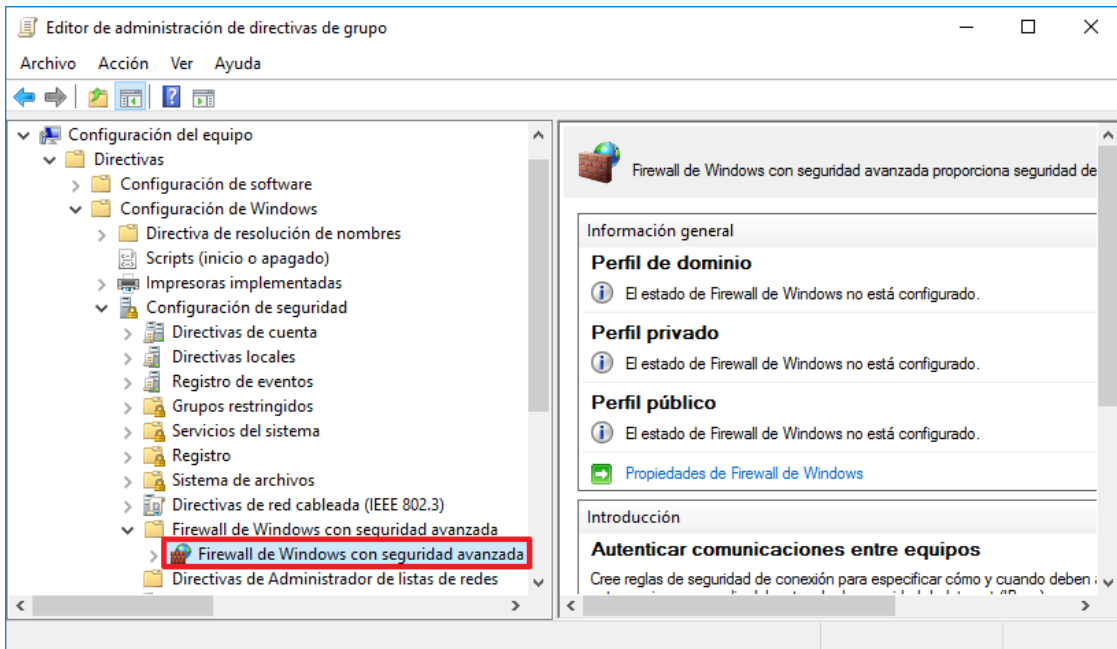
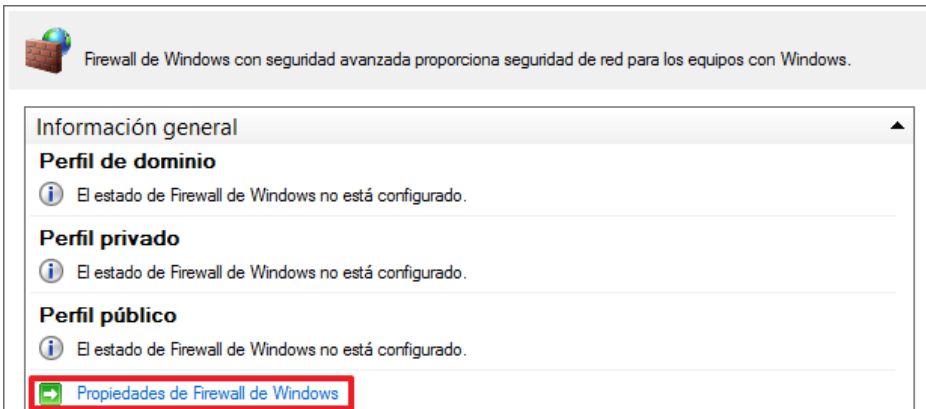
2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CORTAFUEGOS

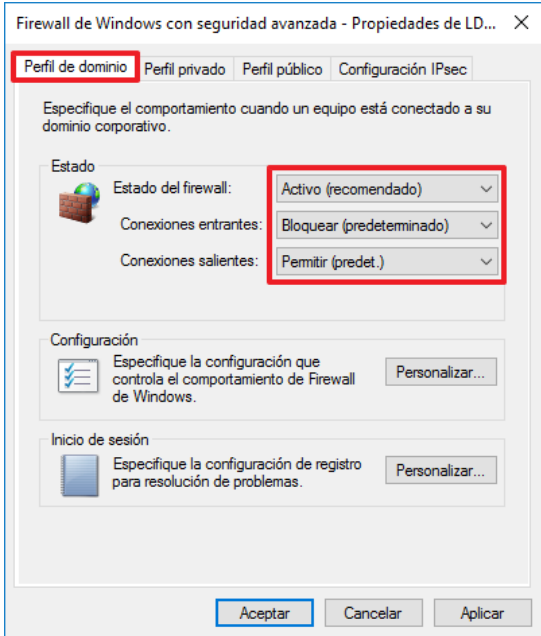
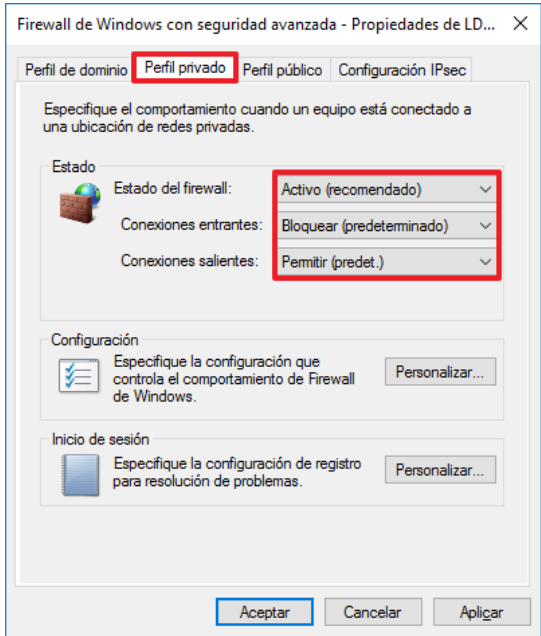
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política de cortafuegos. Deberá tomar en consideración las necesidades de qué puertos y/o aplicaciones o servicios son necesarios permitir para el conjunto de equipos clientes Windows 10.

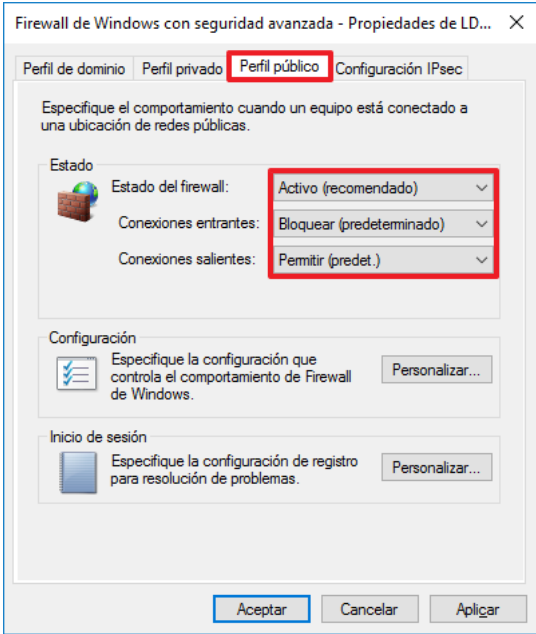
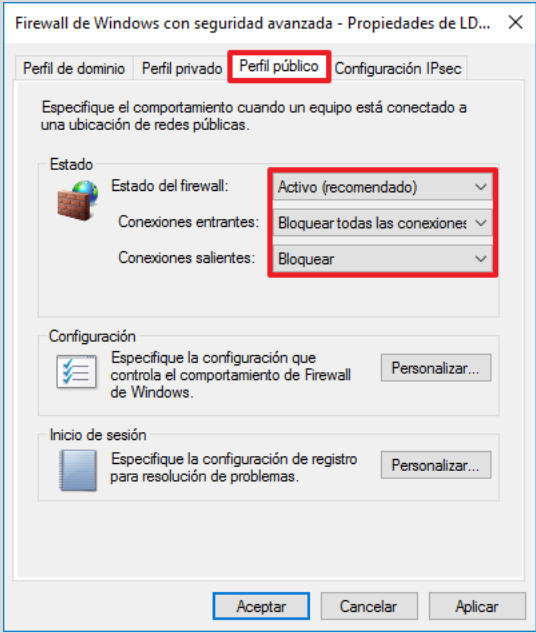
Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos para un conjunto de clientes a los que se va a permitir conexión para administración remota mediante RDP.

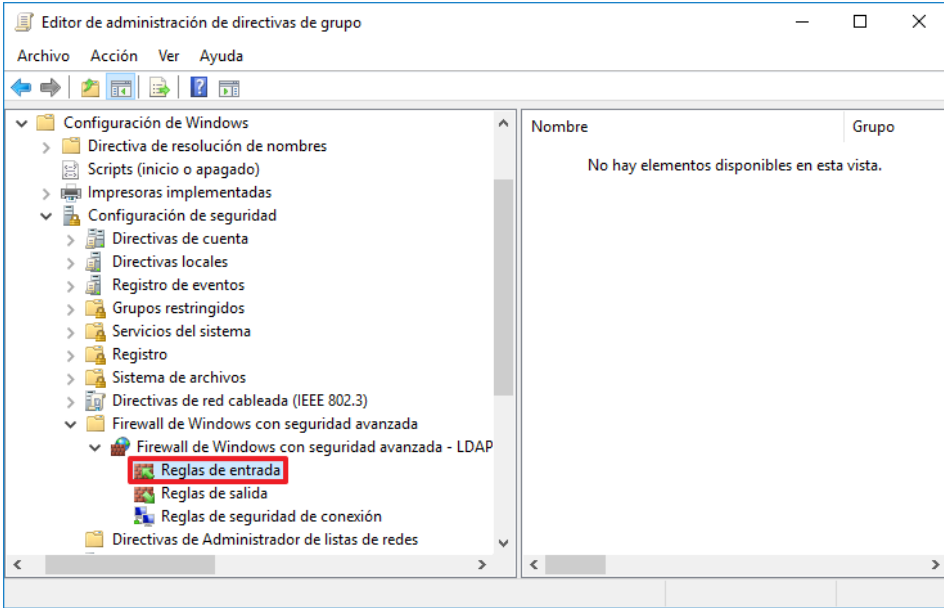
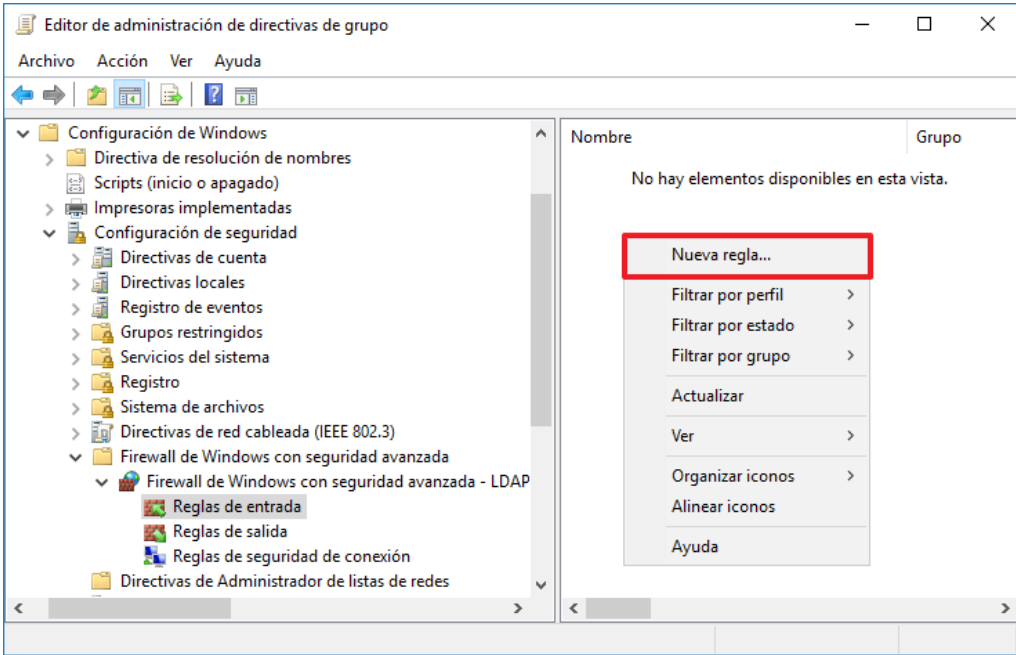
Paso	Descripción
14.	Inicie sesión en un servidor Controlador de Dominio del dominio.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
17.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas grupo". 
18.	Despliegue los contenedores y sitúese sobre la carpeta "Objetos de directiva de grupo".

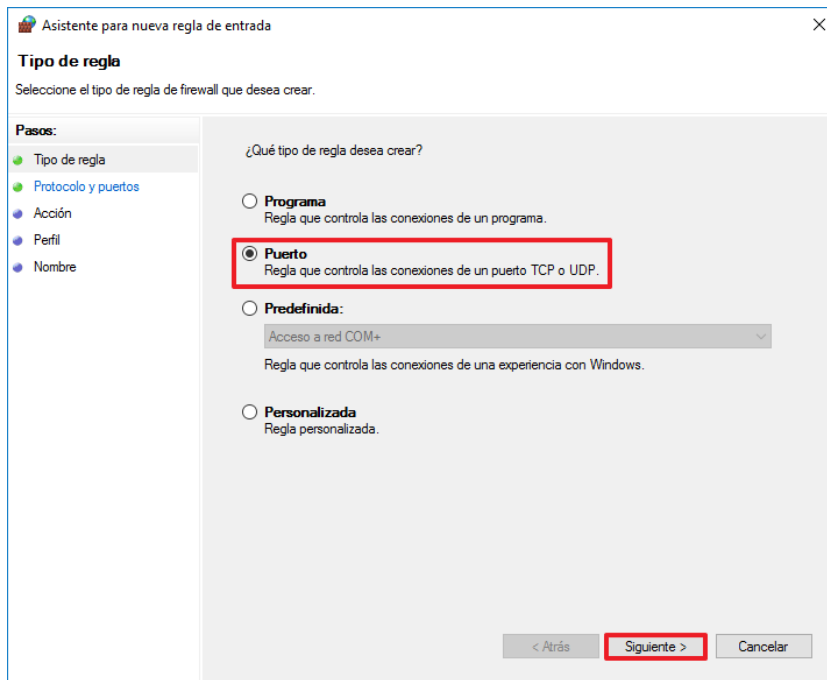
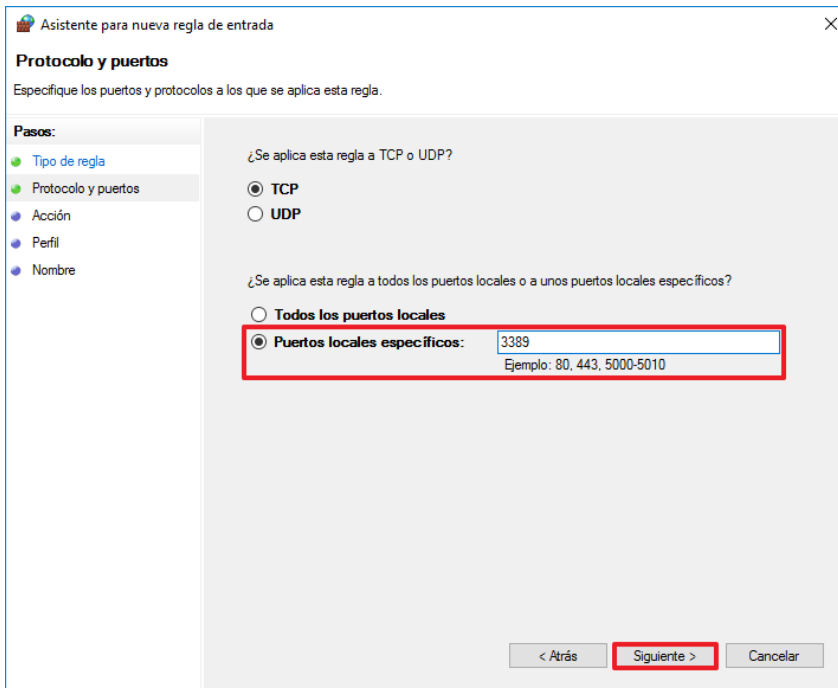
Paso	Descripción
19.	Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
20.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental configuracion de Firewall para administracion remota de cliente” y pulse el botón “Aceptar”. 
21.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 

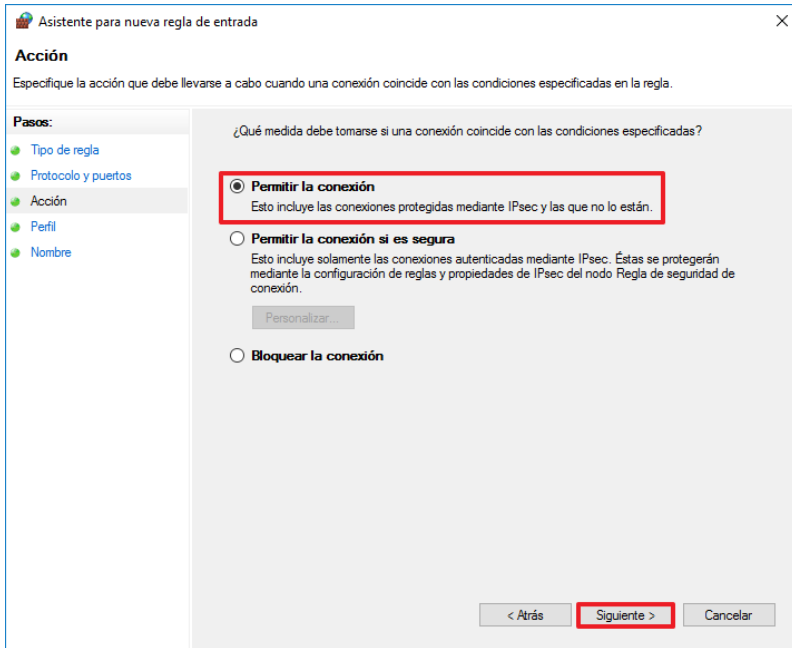
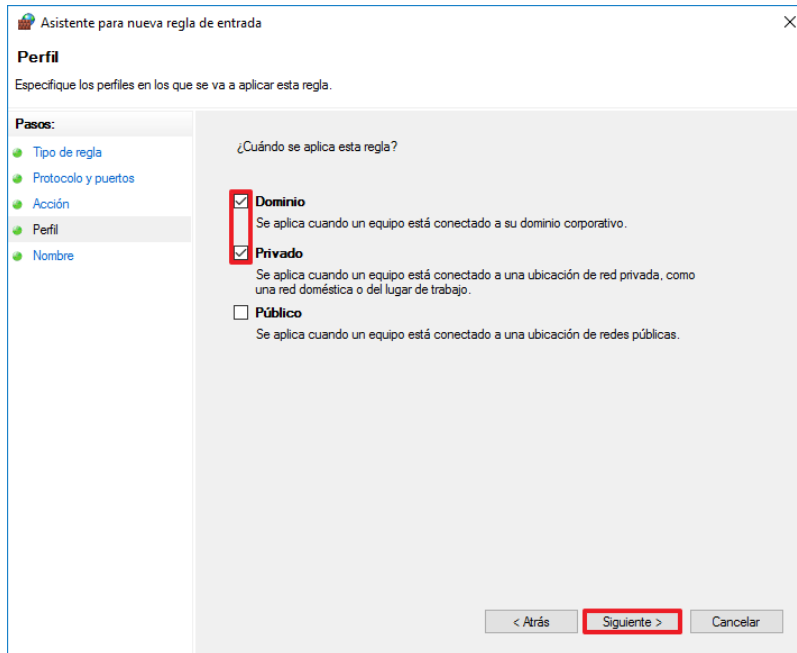
Paso	Descripción
22.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada – LDAP://CN=... 
23.	Pulse sobre las “Propiedades de Firewall de Windows” que aparece en el panel derecho. 

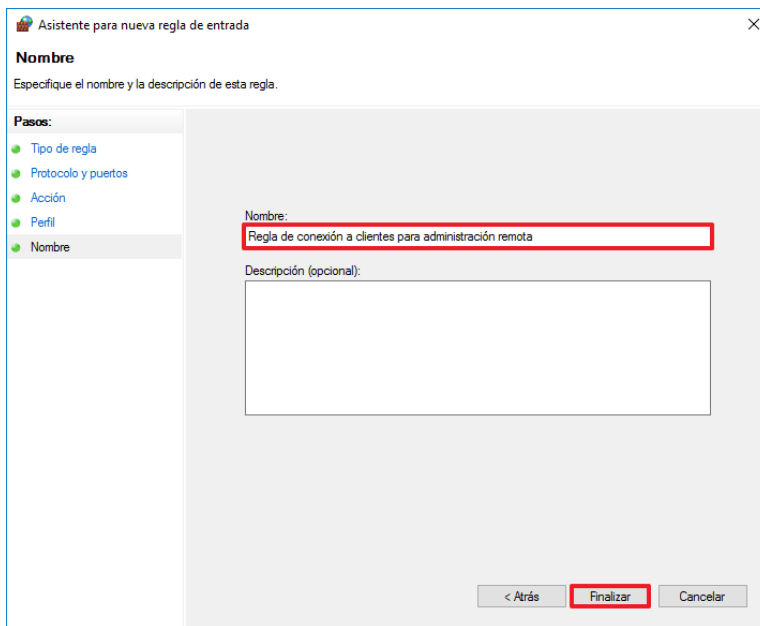
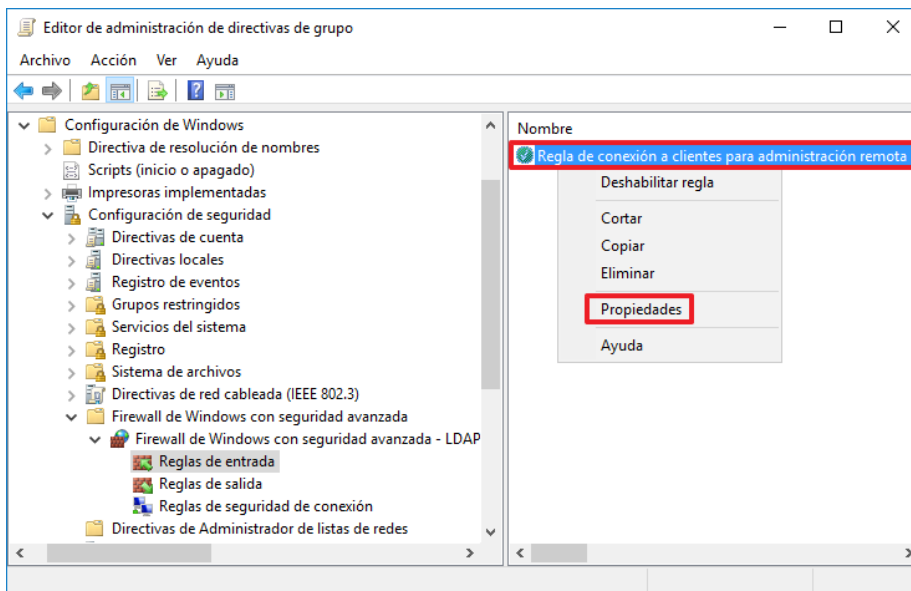
Paso	Descripción
24.	La primera de las pestañas, “Perfil de dominio”, configúrela como aparece en la siguiente imagen. 
25.	A continuación, vaya a la pestaña “Perfil privado” y configúrela tal y como aparece en la siguiente imagen. 

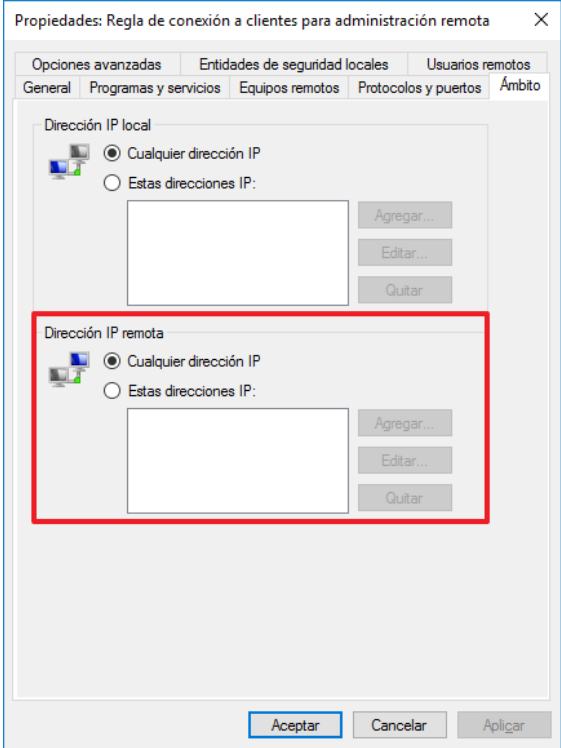
Paso	Descripción
26.	Vaya posteriormente a la pestaña “Perfil público” y establezca la configuración que aparece en la siguiente imagen.  Nota: En el caso de que los clientes estuvieran categorizados como alta, sería recomendable que el perfil público quedara configurado como aparece en la siguiente imagen. 
27.	Pulse el botón “Aceptar” para guardar los cambios introducidos en los diferentes perfiles.

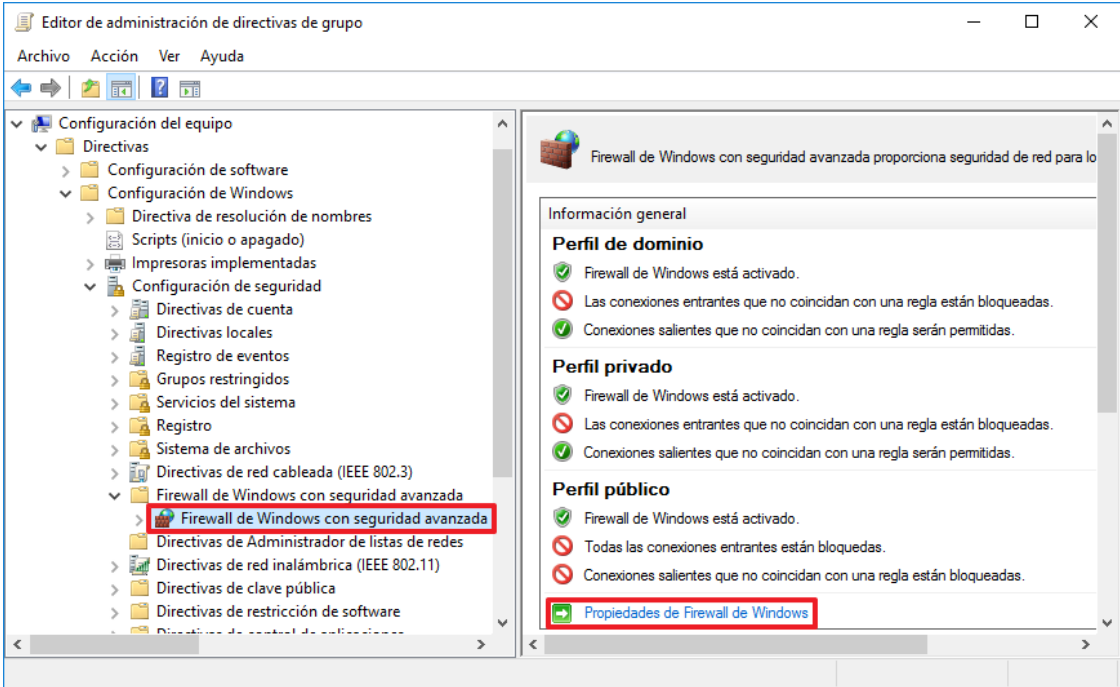
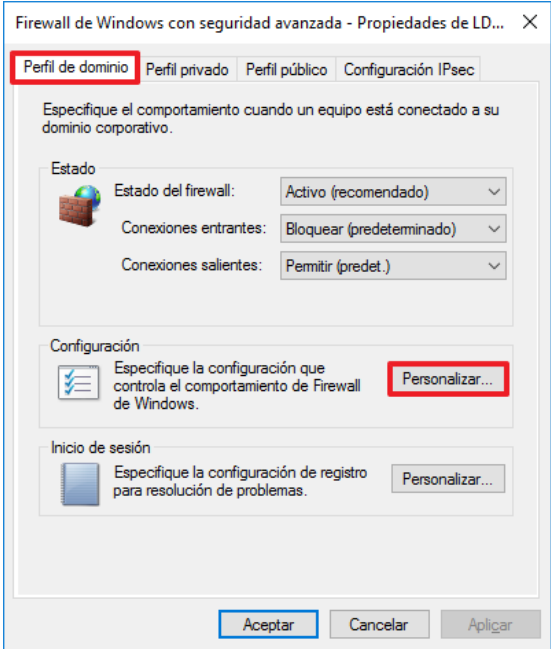
Paso	Descripción
28.	Despliegue el Firewall con seguridad avanzada y vaya al apartado “Reglas de entrada”. 
29.	Pulse con el botón derecho sobre un espacio en blanco en el panel derecho y seleccione la opción “Nueva regla...”. 

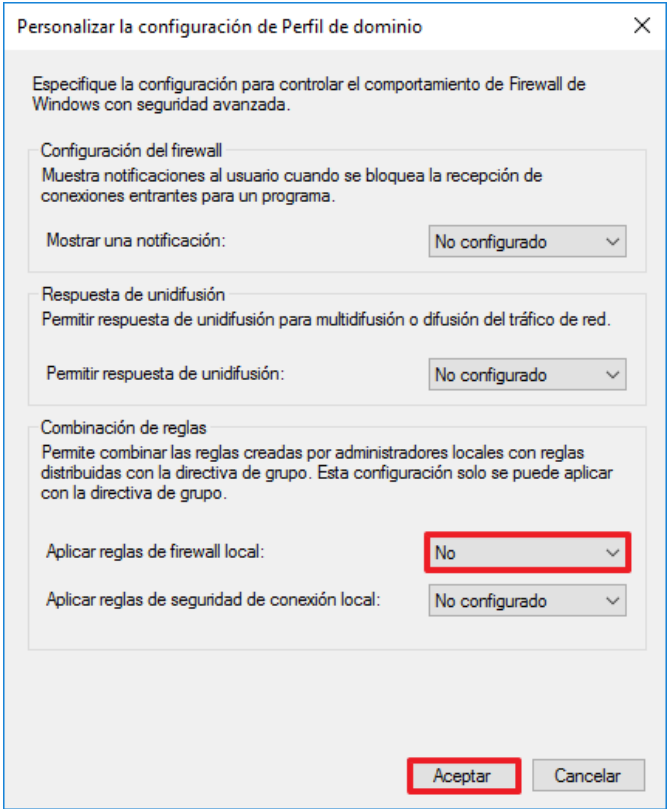
Paso	Descripción
30.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiete >”. 
31.	Seleccione la opción “Puertos locales específicos” e introduzca los puertos necesarios. Pulse el botón “Siguiete >”.  Nota: Para este ejemplo se utiliza el puerto “3389”.

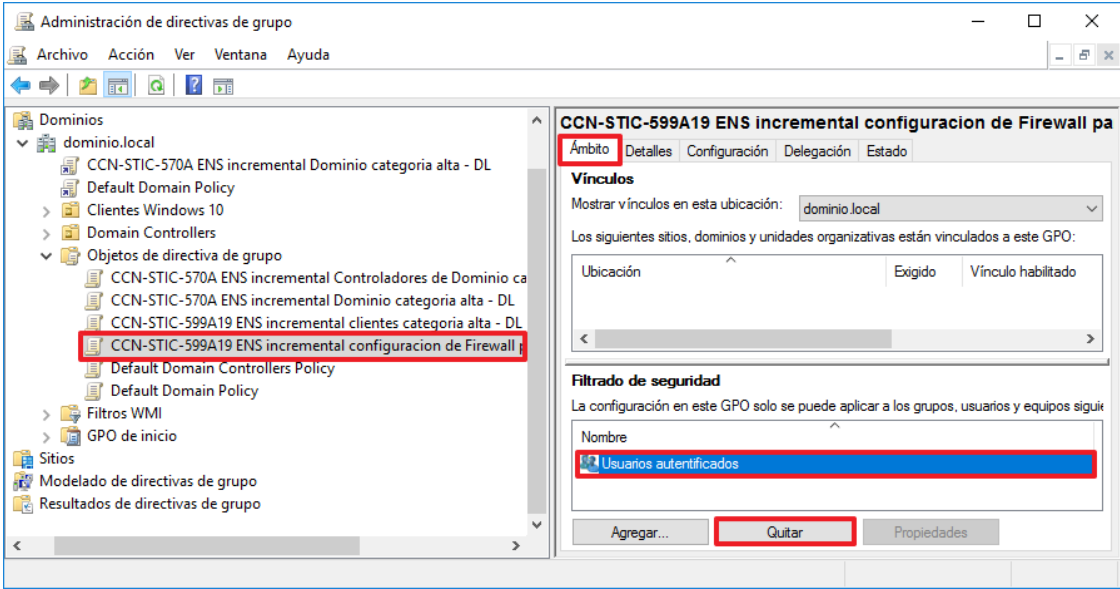
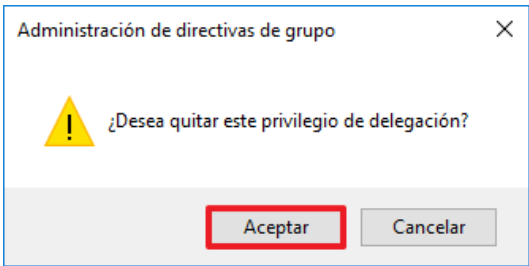
Paso	Descripción
32.	En la pantalla “Acción”, mantenga la configuración y pulse el botón “Siguiente >”. 
33.	En “Perfil”, marque los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 

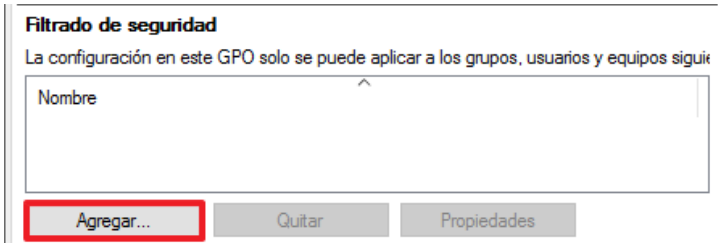
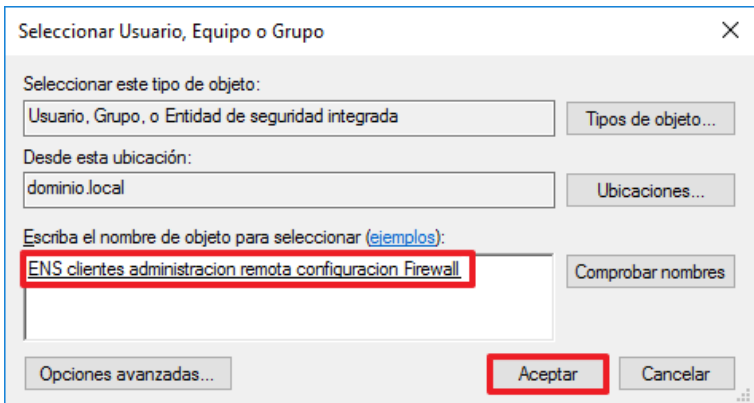
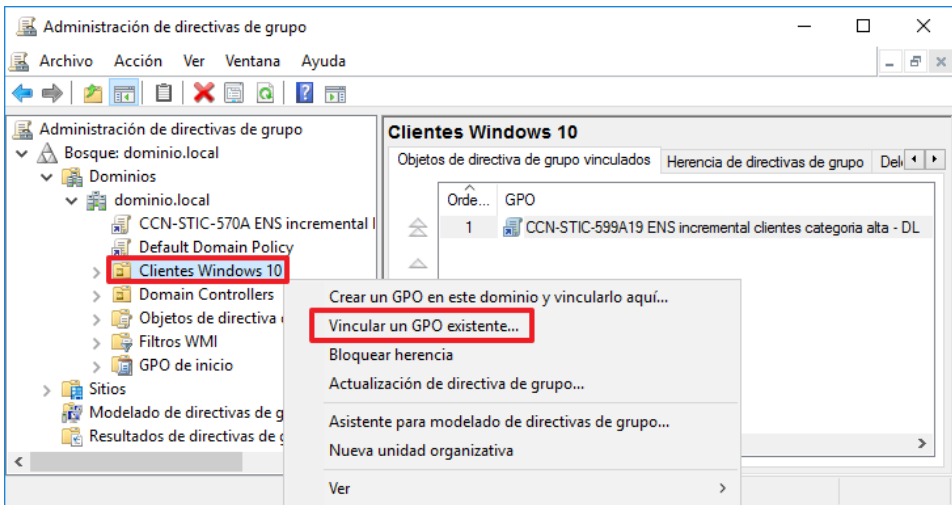
Paso	Descripción
34.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”.  Nota: En este ejemplo se asigna el nombre “Regla de conexión a clientes para administración remota”.
35.	La nueva regla ya se encuentra creada. Puede editarla pulsando con el botón derecho del ratón sobre la misma y seleccionando la opción “Propiedades”. 

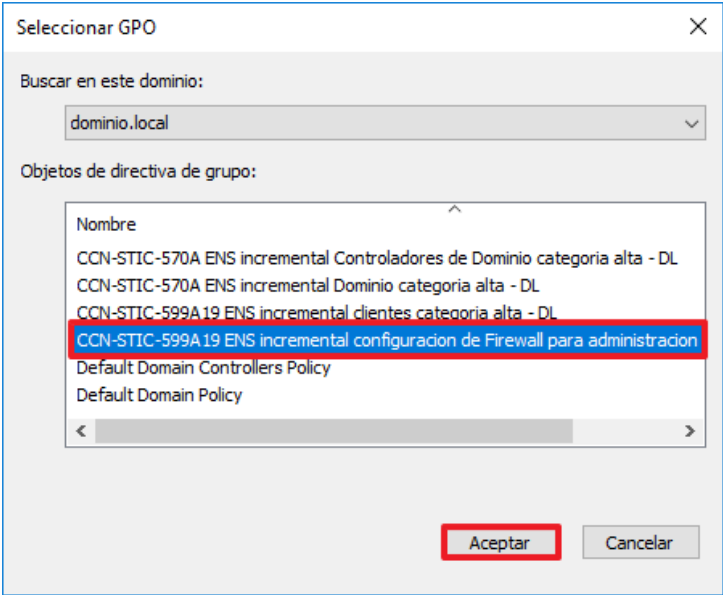
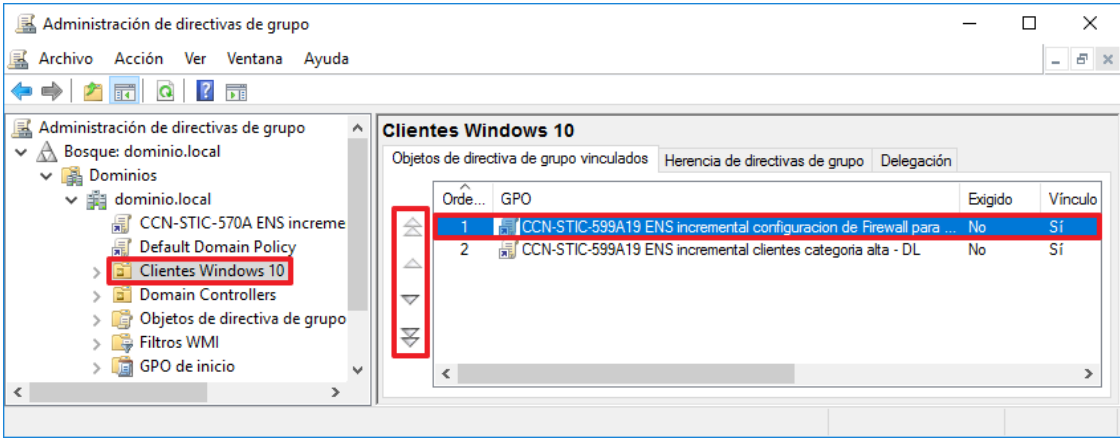
Paso	Descripción
36.	Se podría, por ejemplo, limitar las IP remotas o rangos de redes que podrían conectarse a los clientes para la administración remota, por ejemplo, si el personal de soporte o los administradores emplean una red concreta, direcciones IP fijas o bien asignada por asociación de MAC. De forma predetermina se admite cualquier IP, pero podría establecerse un límite a las mismas. 
37.	Una vez creada las reglas de entrada para los puertos del servicio de administración remota, debería determinarse si existe la necesidad de abrir otros puertos. Por ejemplo, si hay algún servicio en escucha en los clientes por ejemplo para la recolección de eventos. Deberá crear tantas reglas como sean necesarias en función de la necesidad de los clientes.
38.	En el caso de que los servicios fueran de categoría básica o media, deberá cerrarse la política y continuar en el paso 45. En el caso de que la categoría fuera alta/Difusión Limitada, deberá continuar con los siguientes pasos.

Paso	Descripción
39.	Seleccione nuevamente “Firewall con seguridad avanzada – LDAP://CN...” y seleccione la opción del panel derecho “Propiedades de Firewall de Windows”. 
40.	En la pestaña de dominio pulse el botón “Personalizar” del apartado “Configuración”. 

Paso	Descripción
41.	En “Combinación de reglas” configure la opción “Aplicar reglas de firewall local”. Seleccione “No” y pulse el botón “Aceptar”. 
42.	Haga lo mismo para los perfiles “Privado” y “Público”.
43.	Una vez modificado los tres perfiles pulse el botón “Aceptar”. Esto impedirá que la configuración de cortafuegos que se realice localmente tenga alguna validez. Solo será de aplicación la configuración del dominio. Nota: Tenga en cuenta este hecho para agregar reglas que se estuvieran aplicando localmente en los clientes al objeto GPO que se está creando”.
44.	Cierre la política creada.
45.	Una vez creada la política, ésta deberá asignarse al grupo creado en pasos anteriores, del presente Anexo. Para ello seleccione la política recién creada y vaya al panel derecho de su configuración en la herramienta “Administración de directivas de grupo”.

Paso	Descripción
46.	En la pestaña “Ámbito” seleccione el grupo “Usuarios autenticados” y pulse el botón “Quitar”. 
47.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
48.	A continuación, pulse el botón “Agregar...”. 
49.	Introduzca el nombre del grupo creado en el primer paso del presente Anexo y pulse el botón “Aceptar”. 
50.	Solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.
51.	Seleccione la Unida Organizativa y pulsando con el botón derecho haga uso de la opción “Vincular un GPO existente...”. 

Paso	Descripción
52.	En la pantalla de selección, marque la GPO creada previamente y pulse el botón “Aceptar”. 
53.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el panel derecho. 
54.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.
55.	Deberá crear tantos objetos GPO como fueran necesarias, siendo asignados a los clientes Windows 10.

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

1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO

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 GPO. 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 ésta con Microsoft para el mantenimiento de sus equipos.

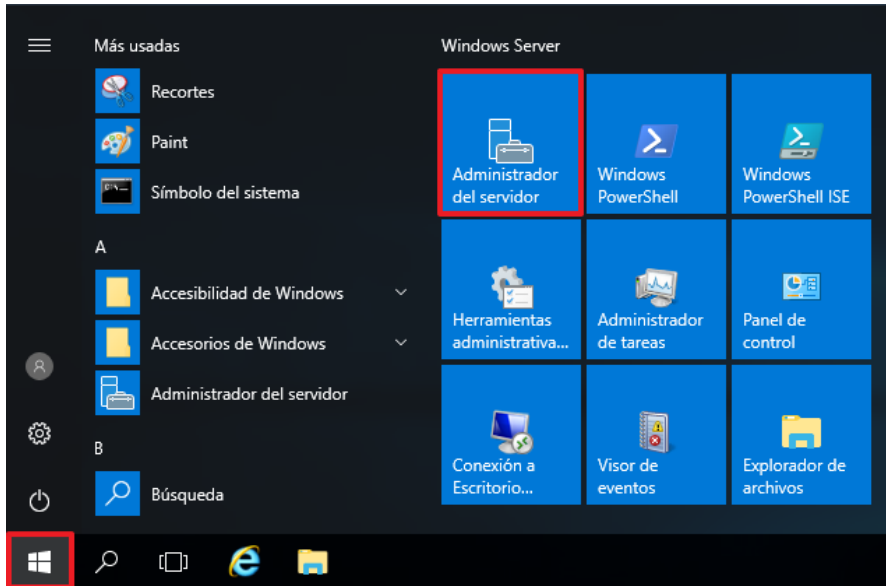
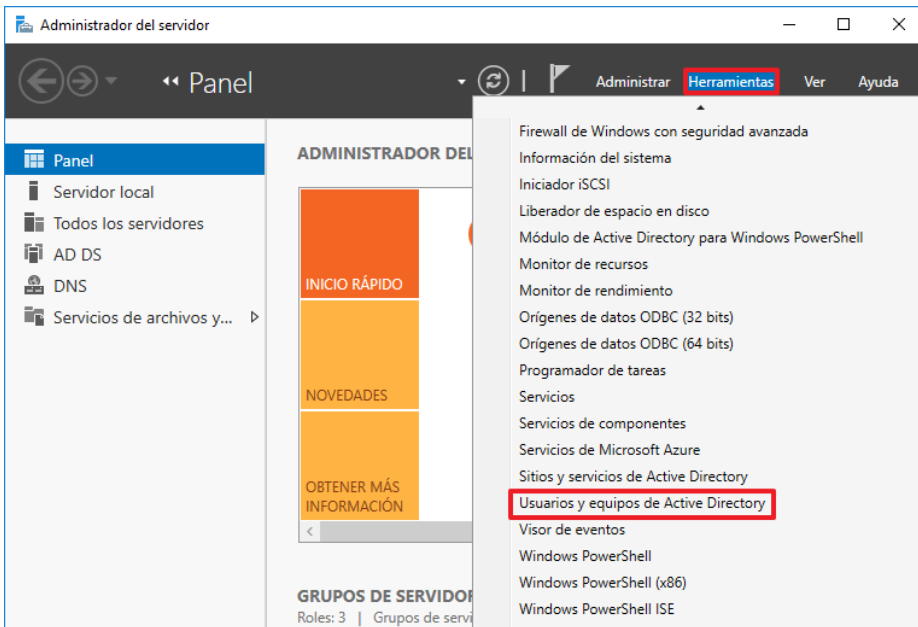
Debe tener en consideración que determinados componentes tales como Windows Defender ATP, podrían llegar a requerir al menos un nivel de telemetría de tipo básico.

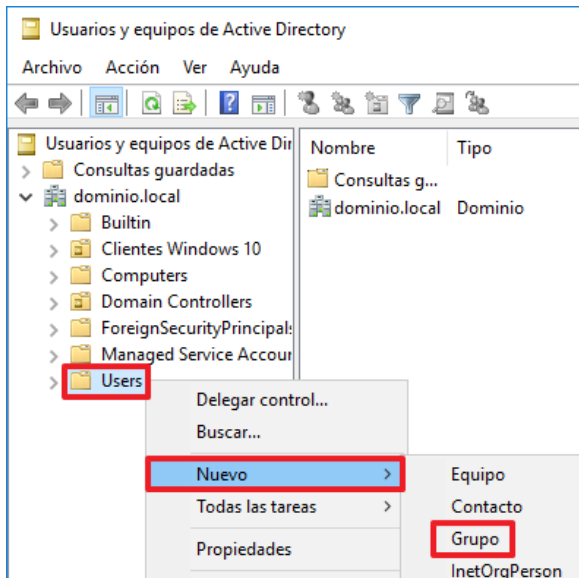
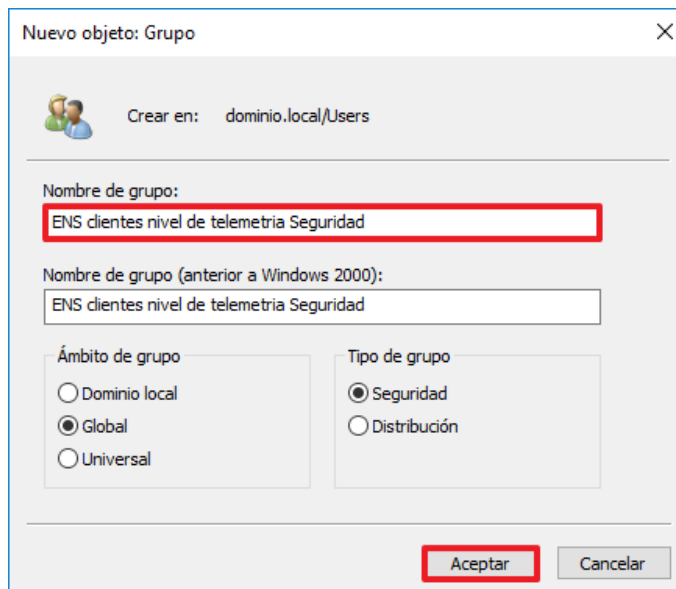
1.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

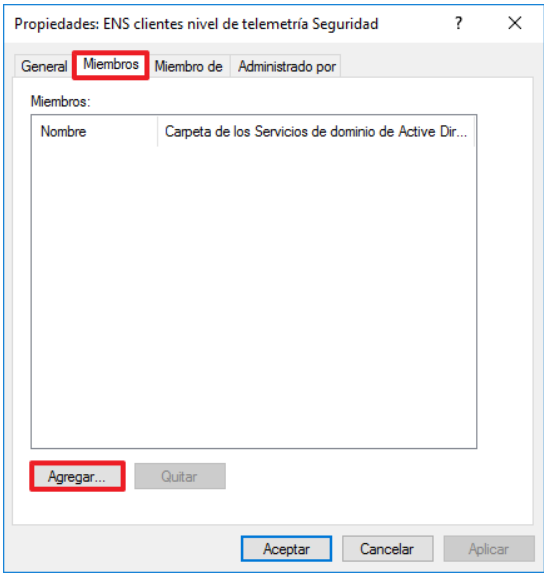
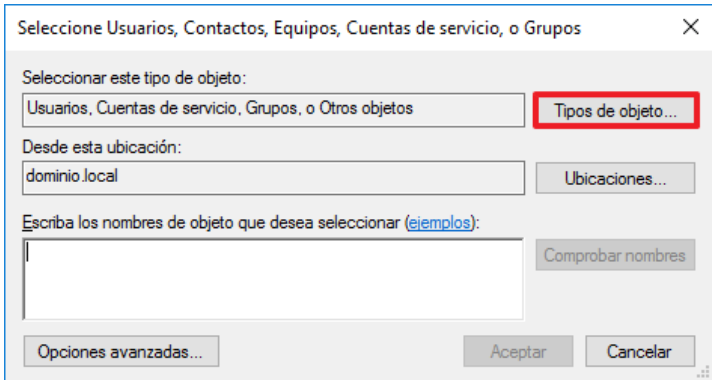
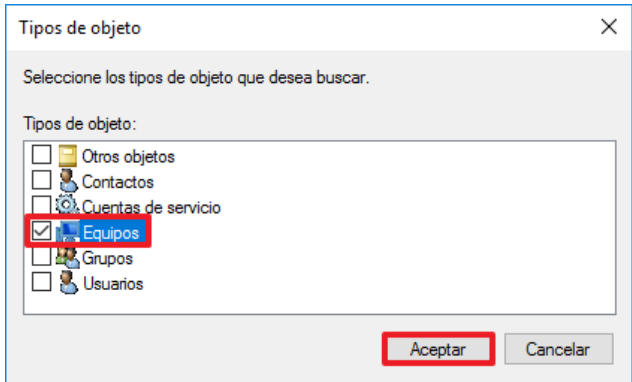
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

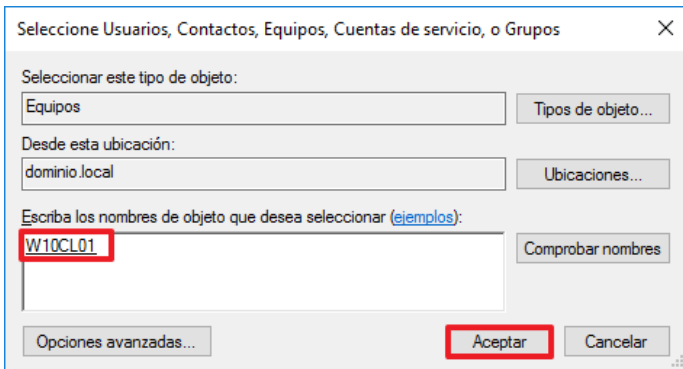
Nota: En el presente ejemplo se va a crear una política de grupo para la configuración del valor de telemetría que permita a la organización adaptar sus equipos a las exigencias establecidas por el ENS. Se van a mostrar las distintas posibilidades de configuración para dicho valor. En caso de precisar de distintos niveles de telemetría, sería conveniente crear un grupo para cada uno de estos niveles.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
4.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 

Paso	Descripción
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
6.	Introduzca como nombre “ENS clientes nivel de telemetría Seguridad”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO que implementen el nivel de telemetría estipulado para dicho grupo.  Nota: Recuerde que este paso a paso es un ejemplo de cómo configurar un objeto de política de grupo para aplicar sobre un conjunto de clientes determinados con motivo de aplicarles una configuración específica. Una sugerencia para los nombres de grupo en caso de precisar distintos niveles de telemetría sería incluir el nivel que se va a estipular para cada grupo. En este caso al establecer un nivel de telemetría de “Seguridad” el nombre a aplicar será “ENS clientes nivel de telemetría Seguridad”.

Paso	Descripción
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.
8.	Pulse el botón “Agregar...”. 
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

Paso	Descripción
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos servidores miembro que cumplan las condiciones de aplicación de la GPO para los distintos niveles de telemetría. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”. Nota: El grupo creado, aunque en el ejemplo se va a emplear para la configuración del nivel para la telemetría, se podría emplear para la aplicación de una configuración de seguridad aplicable a través de GPO diferente del resto de servidores de la organización.

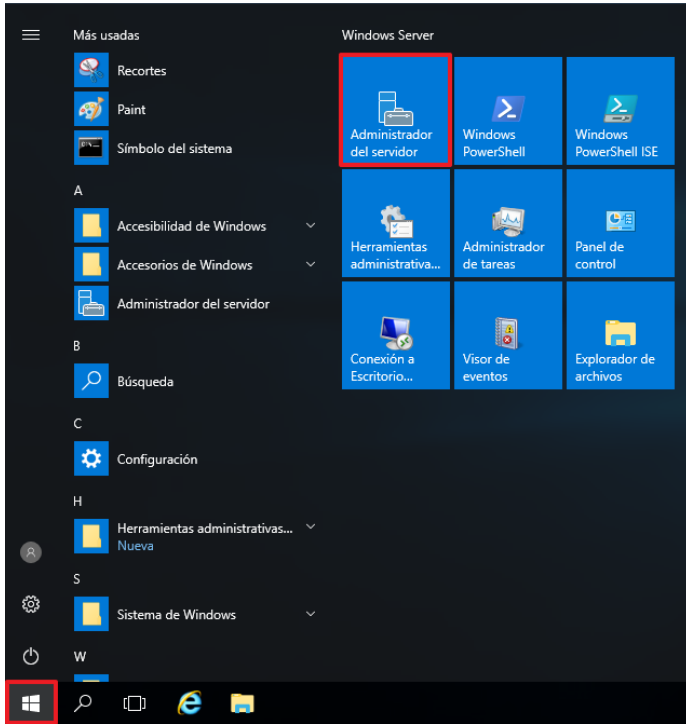
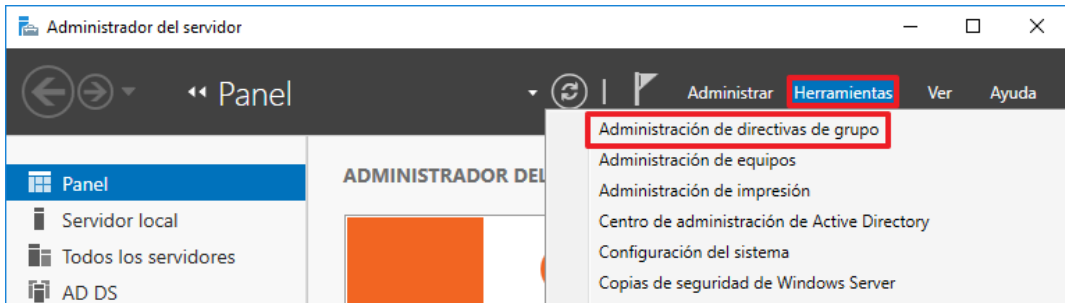
1.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CONFIGURACIÓN DEL VALOR DE TELEMETRÍA

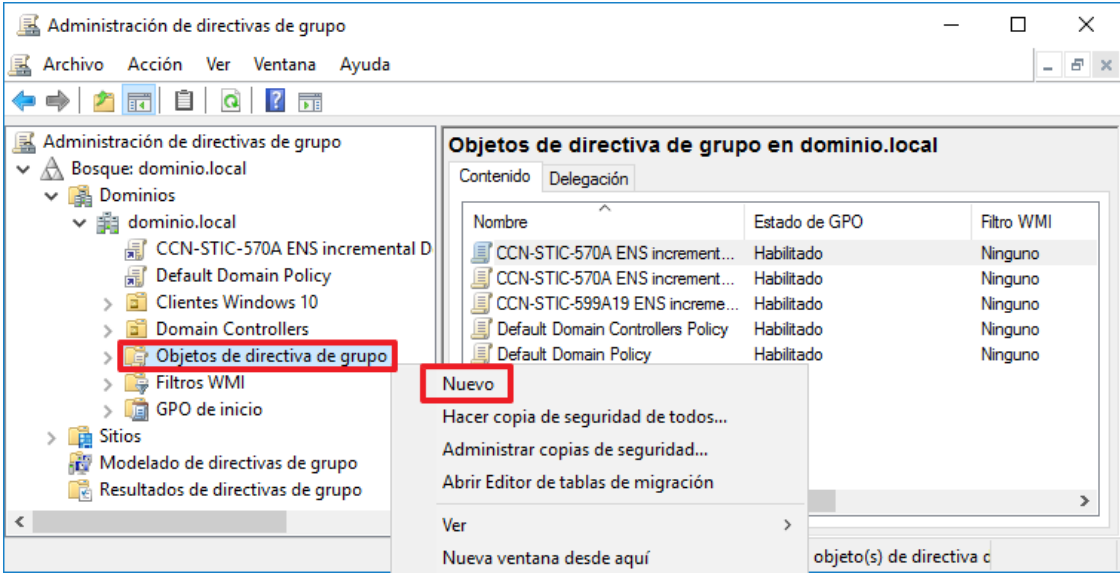
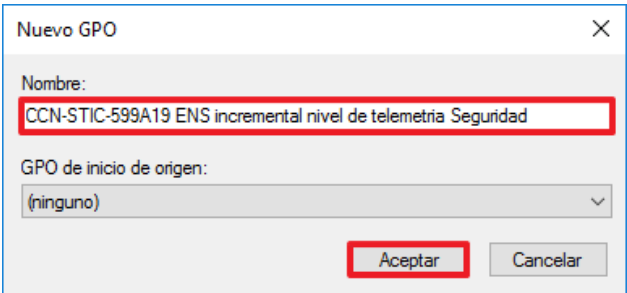
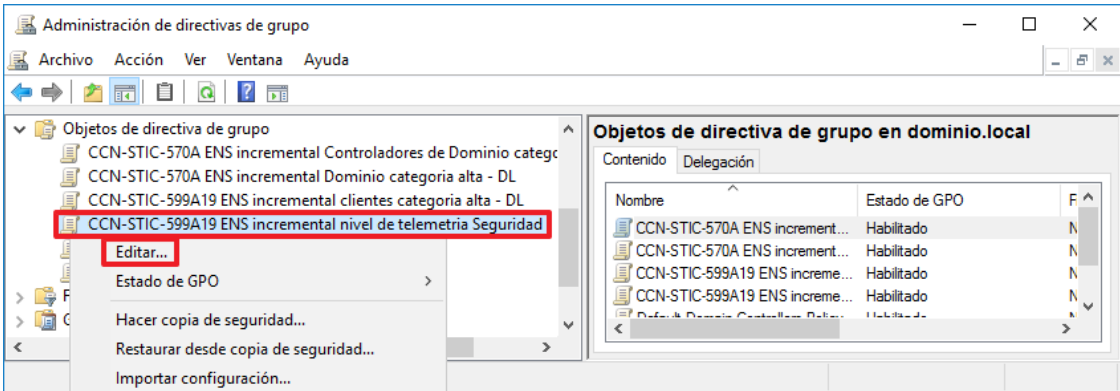
El comportamiento de la telemetría difiere dependiendo de la edición utilizada de Windows 10, Enterprise o Pro. En el caso de la edición Enterprise la telemetría puede establecerse hasta de un valor 0 (Seguridad) mientras que en la edición Pro en el caso de establecer un valor 0, esta será tomada por parte del sistema operativo como un valor 1 (Básico) no siendo posible la configuración en valor 0 (Seguridad) en las ediciones Pro de Windows 10.

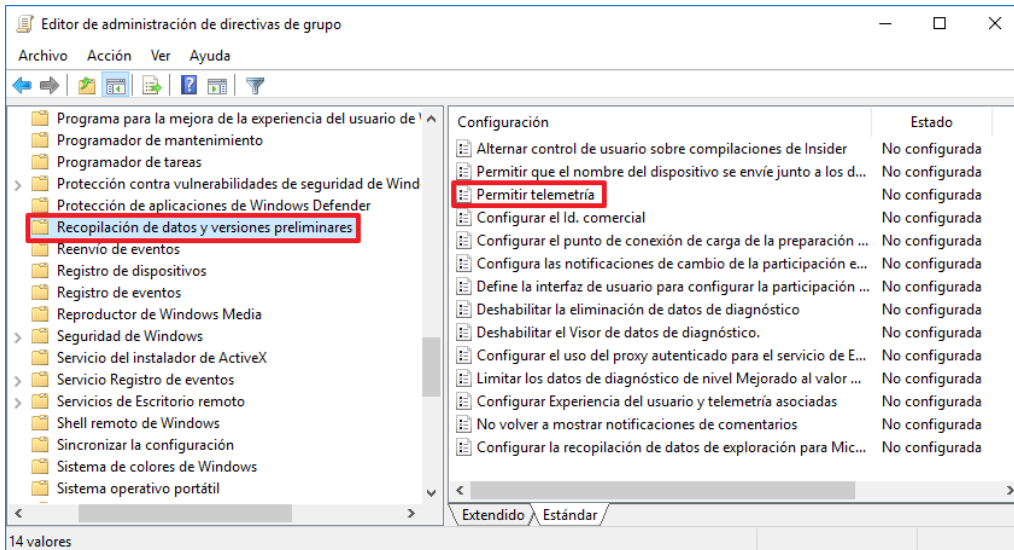
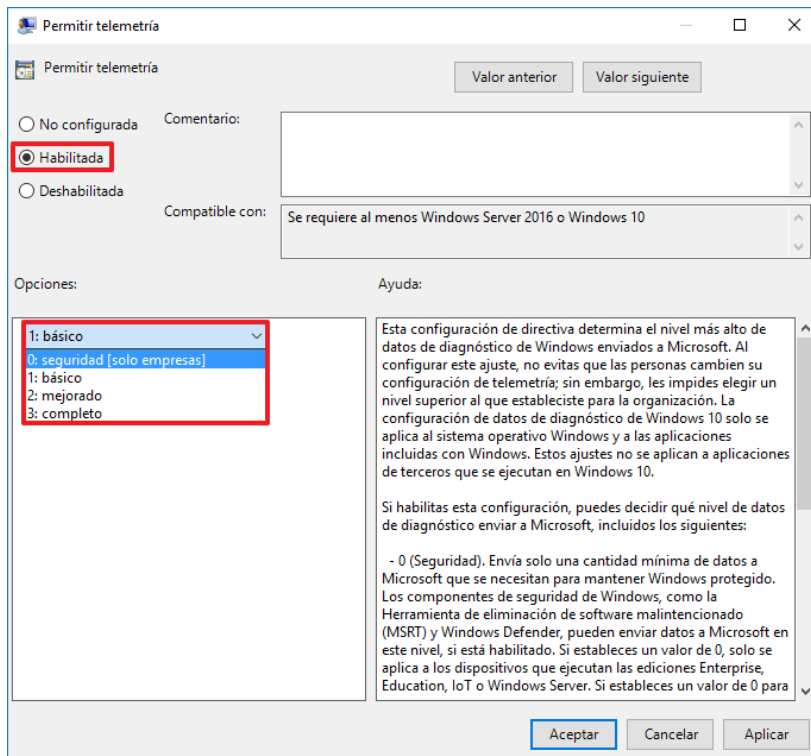
Nota: Establecer un valor de telemetría 0 supone el no funcionamiento de otras directivas como puede ser la aplicación de diferentes opciones de mantenimiento por lo que deberá tener muy en consideración esta casuística.

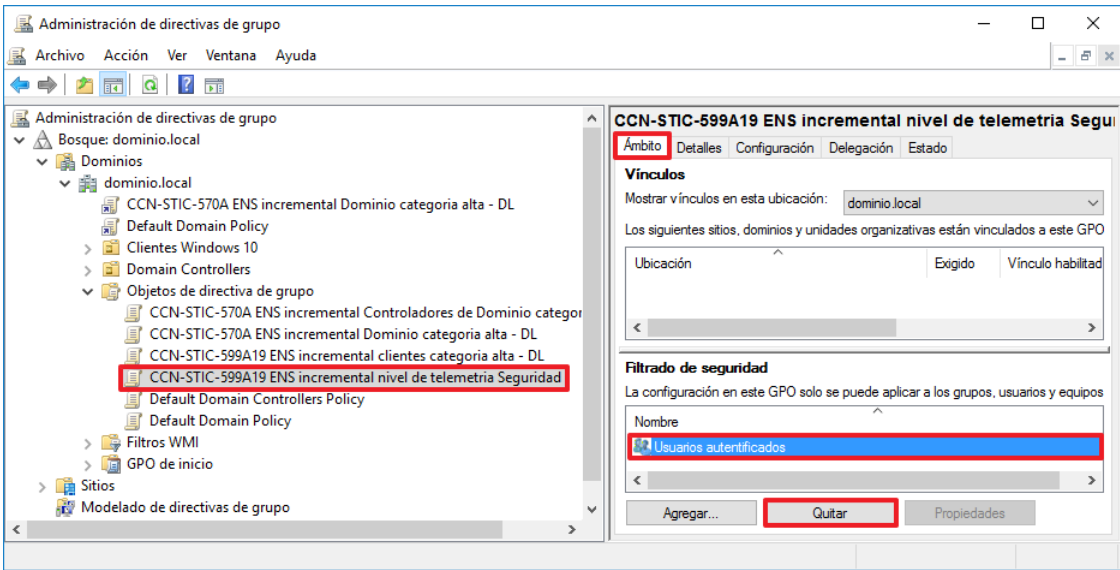
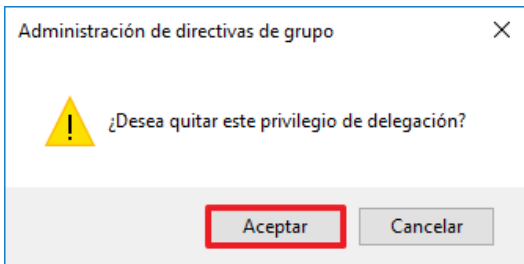
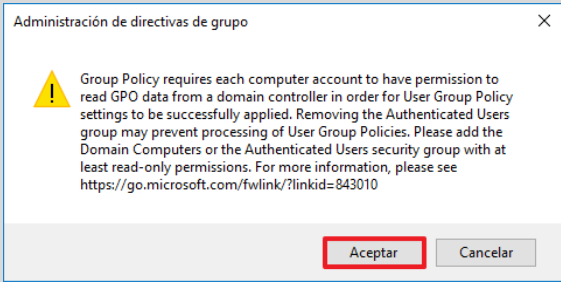
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política de configuración de valor de telemetría.

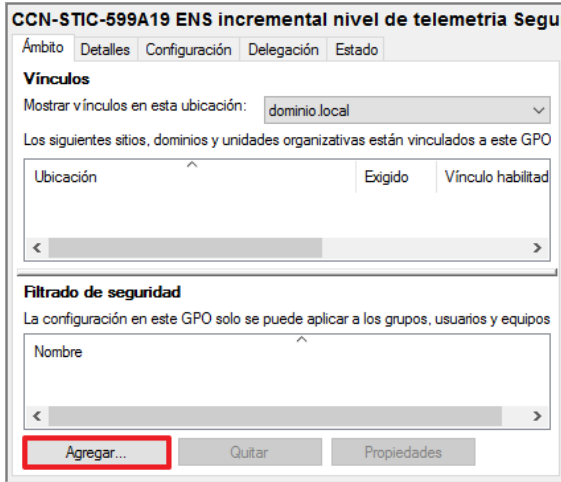
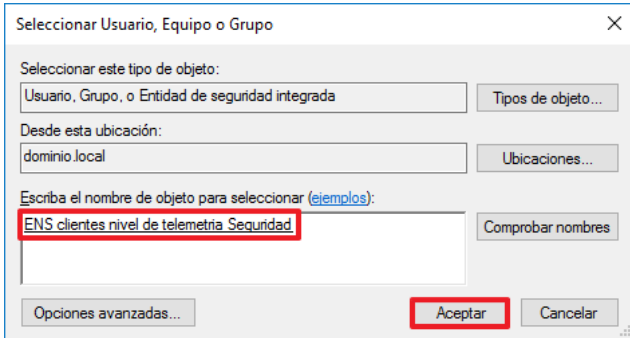
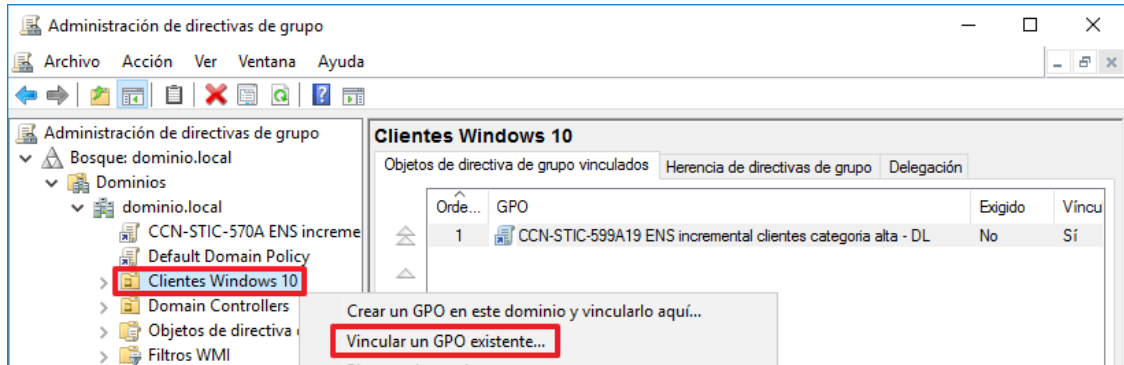
A continuación, se va a mostrar el procedimiento para modificar el valor de telemetría acorde a las necesidades de la organización. Deberá tomar en consideración que determinadas funcionalidades del sistema, como Windows Defender ATP, podrían requerir un mínimo de nivel de telemetría. Consulte la información del fabricante para establecer el nivel de telemetría más adecuado para su organización.

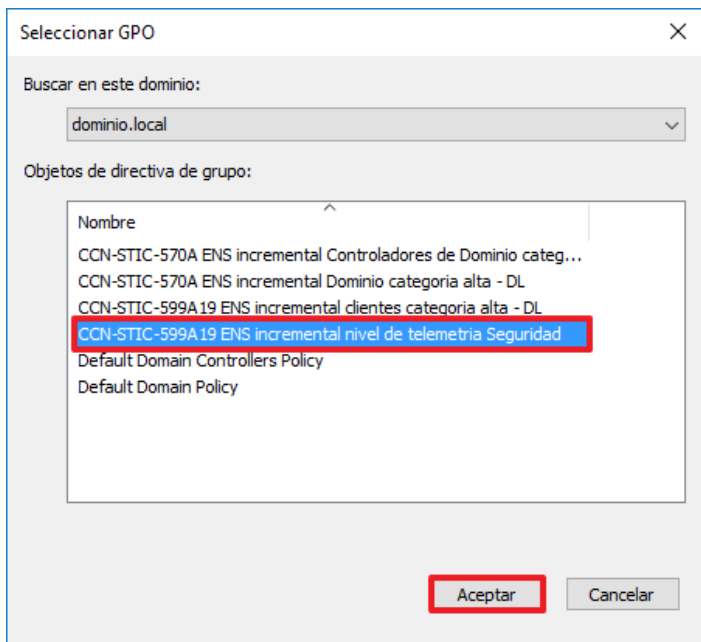
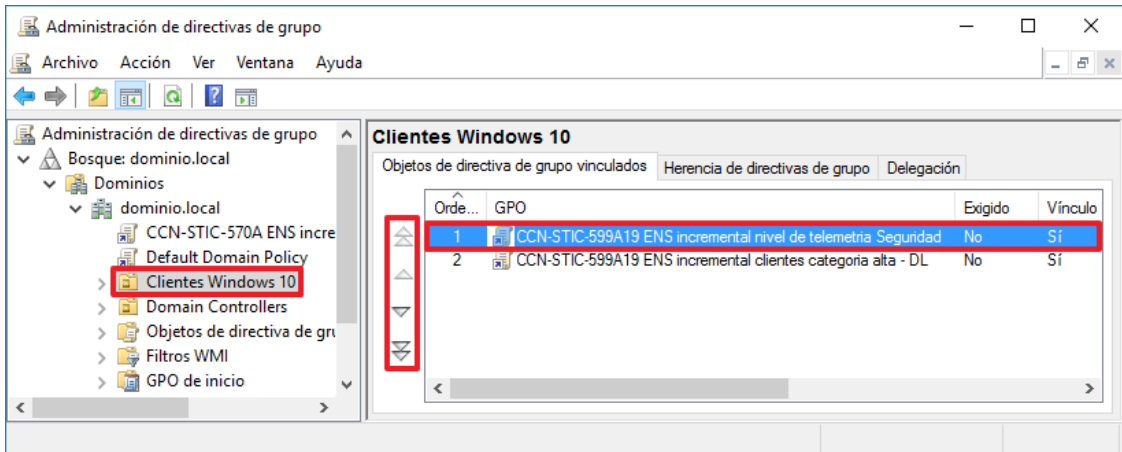
Paso	Descripción
14.	Inicie sesión en un servidor Controlador de Dominio del dominio.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
17.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo". 
18.	Despliegue los contenedores y sitúese sobre la carpeta "Objetos de directiva de grupo".

Paso	Descripción
19.	Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
20.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental nivel de telemetria Seguridad” y pulse el botón “Aceptar”. 
21.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 

Paso	Descripción
22.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. Configuración de equipo → Directivas → Plantillas administrativas → Componentes de Windows → Recopilación de datos y versiones preliminares 
23.	En el panel derecho haga doble clic sobre “Permitir telemetría”. Se abrirá una ventana con la administración de la configuración para el valor de nivel de telemetría.
24.	En la ventana emergente pulse sobre “Habilitada”. En este punto encontrará un desplegable en el que se muestran los diferentes niveles que se le puede otorgar al componente de telemetría acorde a las necesidades de la organización. Establezca el valor de telemetría en función de las necesidades de su organización. 

Paso	Descripción
25.	Una vez definido el valor de telemetría en el desplegable sólo quedaría guardar la configuración pulsando el botón “Aceptar”.
26.	Cierre el editor de políticas.
27.	Una vez editada la política, esta deberá asignarse al grupo creado en pasos anteriores del presente Anexo. Para ello seleccione la política recién creada y vaya al panel derecho de su configuración.
28.	En la pestaña “Ámbito” seleccione el grupo “Usuarios autenticados” y pulse el botón “Quitar”. 
29.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
30.	A continuación, pulse el botón “Agregar...”. 
31.	Introduzca el nombre del grupo creado en el primer paso del presente Anexo y pulse el botón “Aceptar”. 
32.	Solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.
33.	Seleccione la Unida Organizativa y pulsando con el botón derecho sobre ella seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
34.	En la pantalla de selección, marque la GPO creada previamente y pulse el botón “Aceptar”. 
35.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.
36.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el cuadro de la derecha. 

2. INFORMACIÓN ACERCA DEL ÚLTIMO INICIO DE SESIÓN

Dentro del ENS, a partir de la aplicación de su categoría media, es necesario informar al usuario de cuándo fue la última vez que inicio sesión. Hasta ahora, para realizar dicha tarea se hacía uso del inicio interactivo que posee Microsoft Windows de base utilizando las GPO y más concretamente la directiva denominada “Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario”.

La directiva establece la visualización de una fecha y hora concreta en la que el usuario se validó correctamente por última vez. Del mismo modo, indica que en caso de no estar disponible el controlador de dominio no podrá ser posible iniciar sesión en la máquina y no se podrá autenticar.

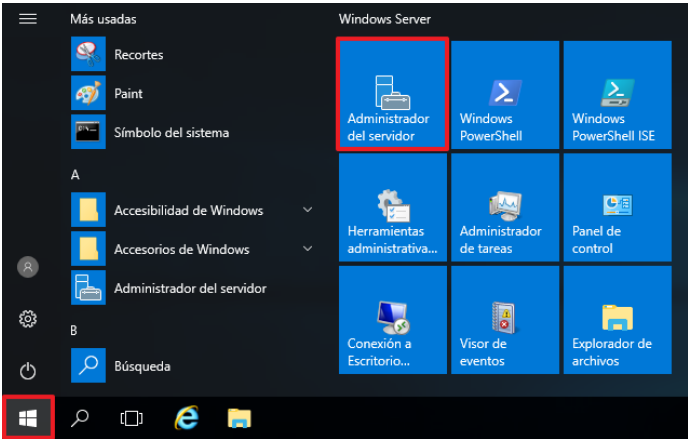
Debido a esta problemática la cual afecta sobre todo a equipos que suelen estar fuera de las organizaciones, se plantea a continuación una solución para llevar a cabo la tarea de informar al usuario de cuándo fue la última vez que inicio sesión correctamente.

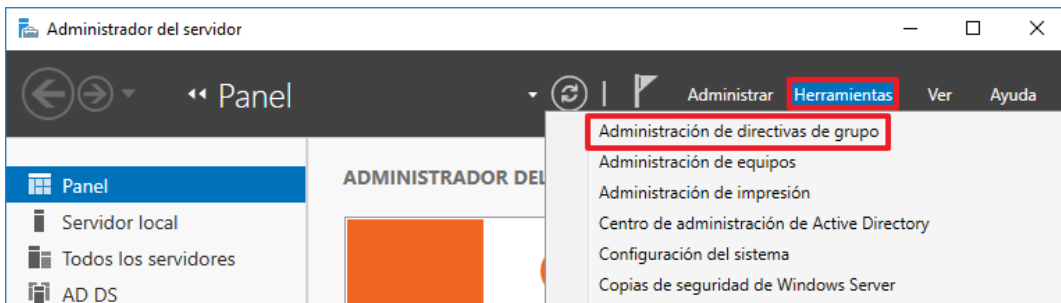
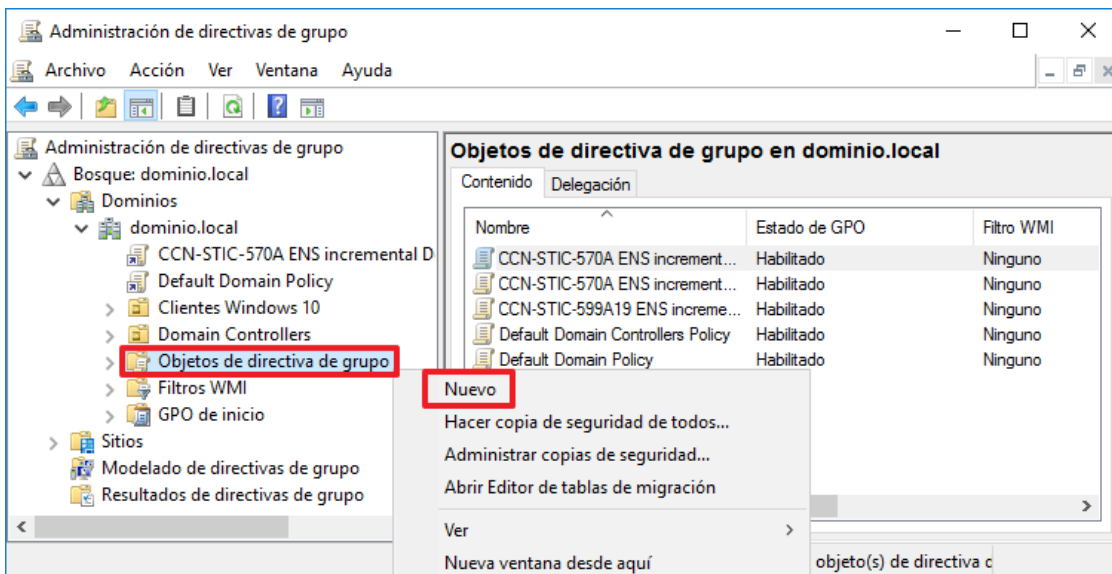
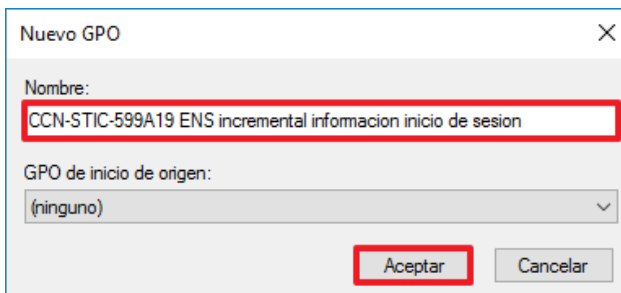
Para realizar dicha tarea se va a hacer uso de una tarea programada que ejecuta un script que muestra el último inicio de sesión correcto del usuario que es almacenado en un atributo del usuario.

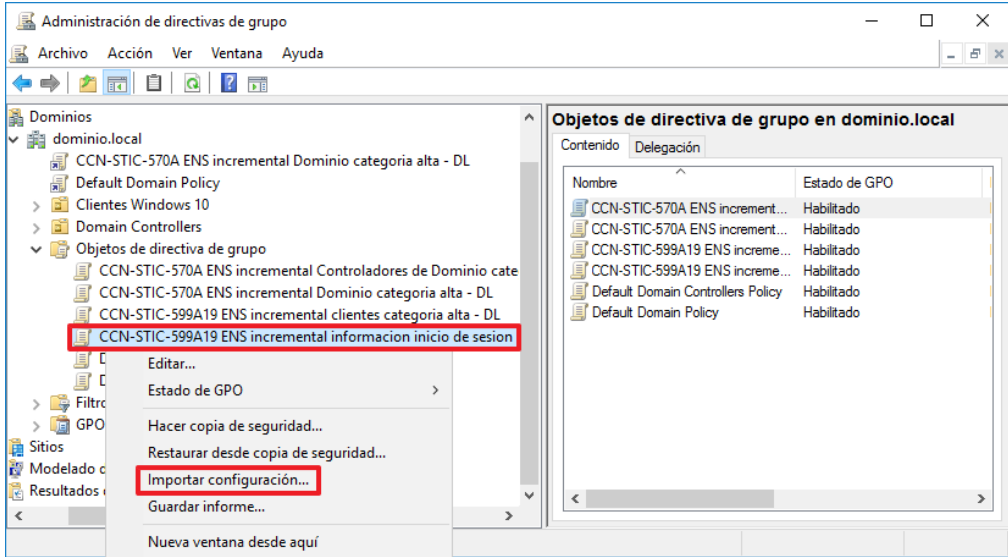
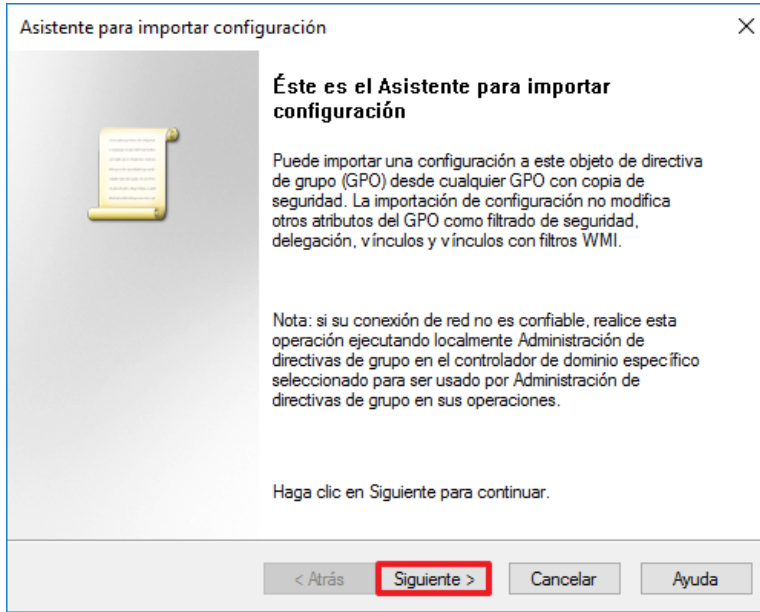
Nota: Puede hacer uso del siguiente enlace para conocer los atributos: [https://msdn.microsoft.com/en-us/library/ms675090\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms675090(v=vs.85).aspx).

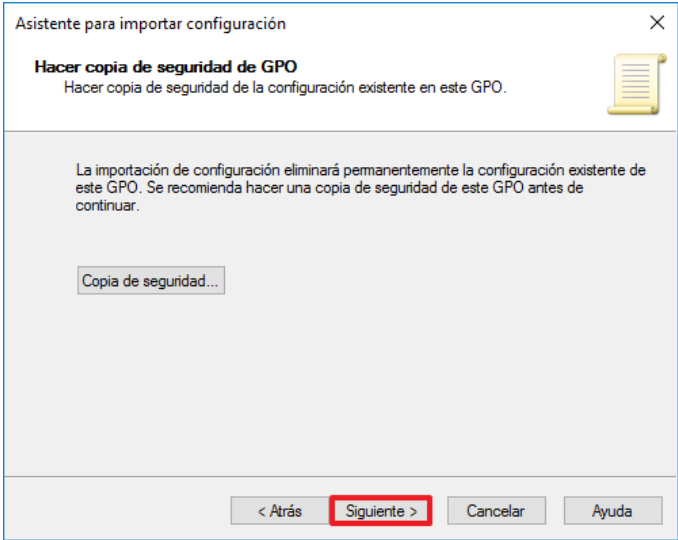
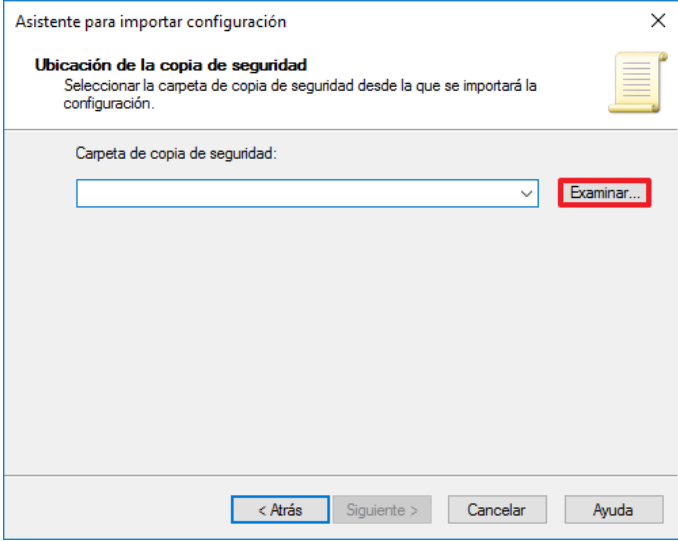
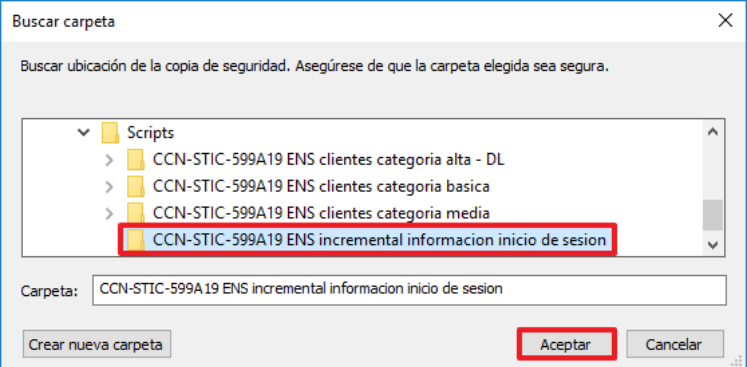
2.1. CREACIÓN DE TAREA PROGRAMADA

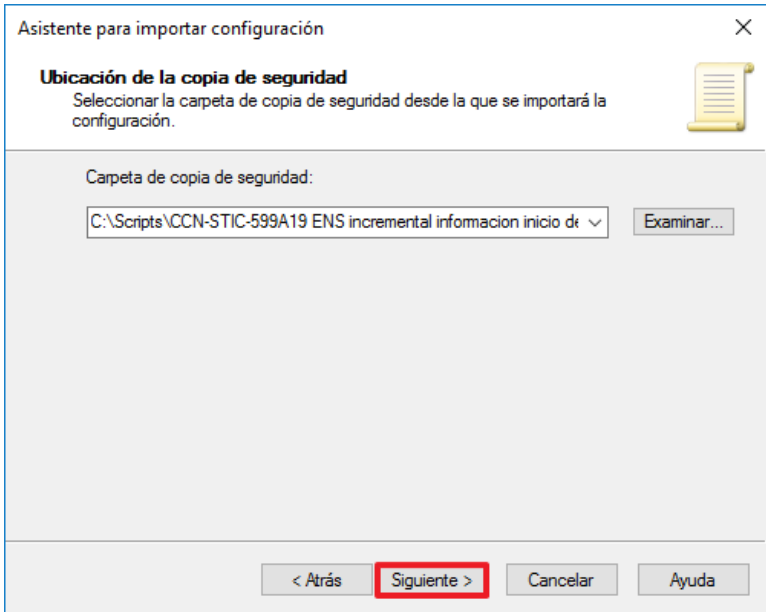
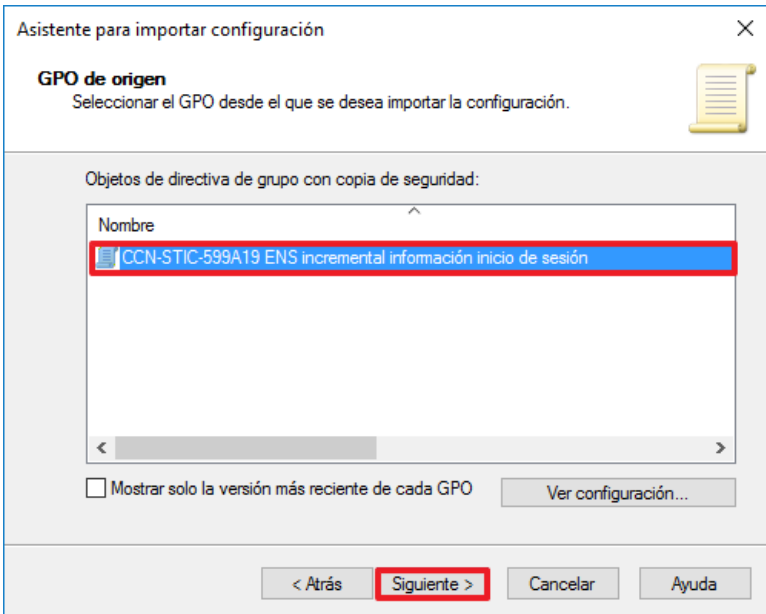
Este apartado permite implementar una tarea programada en los equipos para que los usuarios puedan visualizar el último inicio de sesión correcto mediante la ejecución de un script.

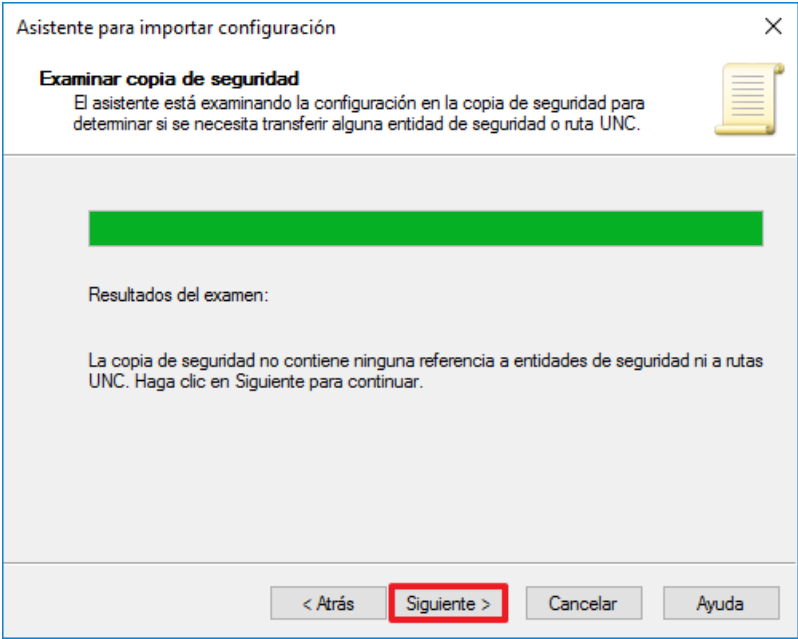
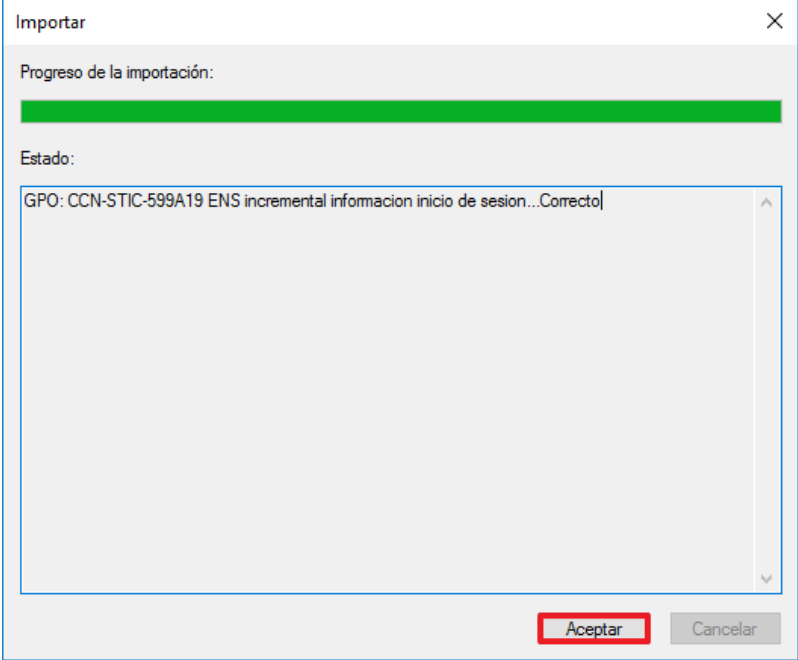
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios del ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Copie los script y plantillas que acompañan a esta guía al directorio “C:\Scripts”.
4.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

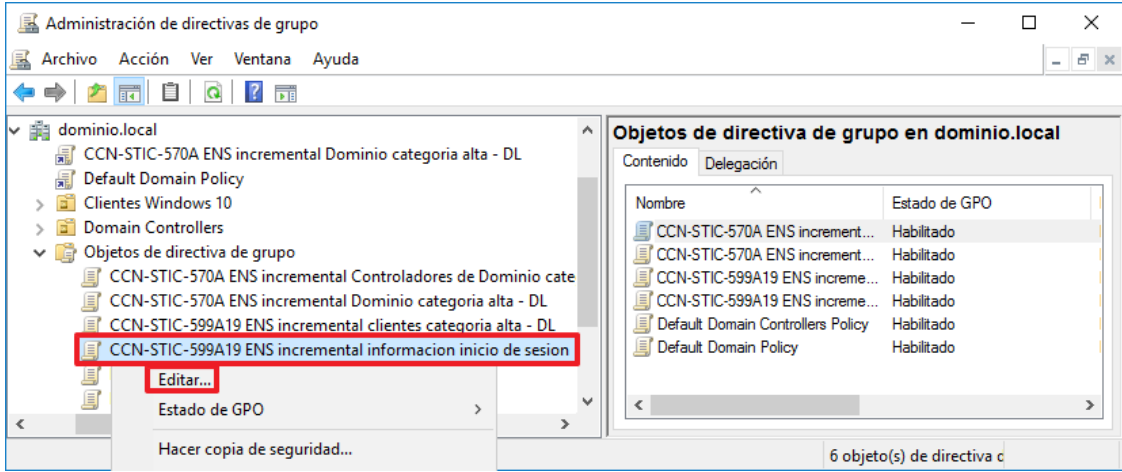
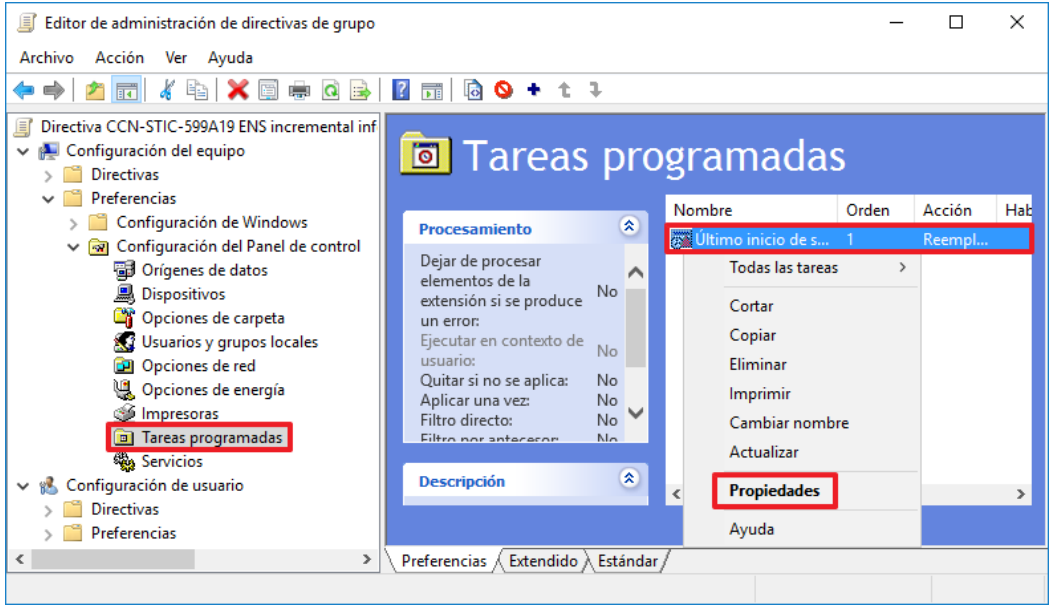
Paso	Descripción
5.	Eleve privilegios para iniciar el “Administrador del servidor”. Nota: Dependiendo de la categoría de seguridad aplicado deberá confirmar la operación o bien introducir las credenciales de un usuario con privilegios de administrador del dominio.
6.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
7.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es “dominio.local”.
8.	Seleccione el nodo “Objetos de directiva de grupo” con el botón derecho y seleccione la opción del menú contextual “Nuevo”. 
9.	Asigne el nombre para la GPO “CCN-STIC-599A19 ENS incremental informacion inicio de sesion” y pulse “Aceptar”. 

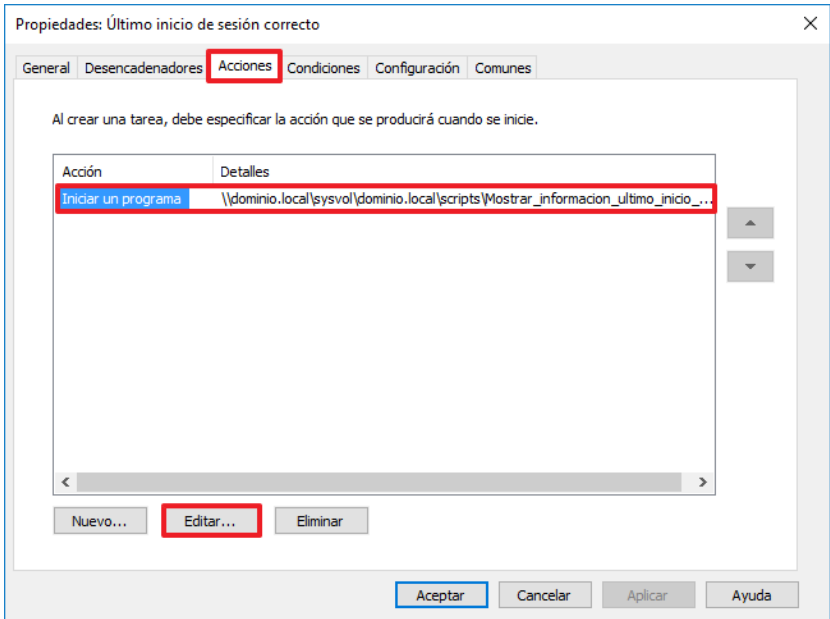
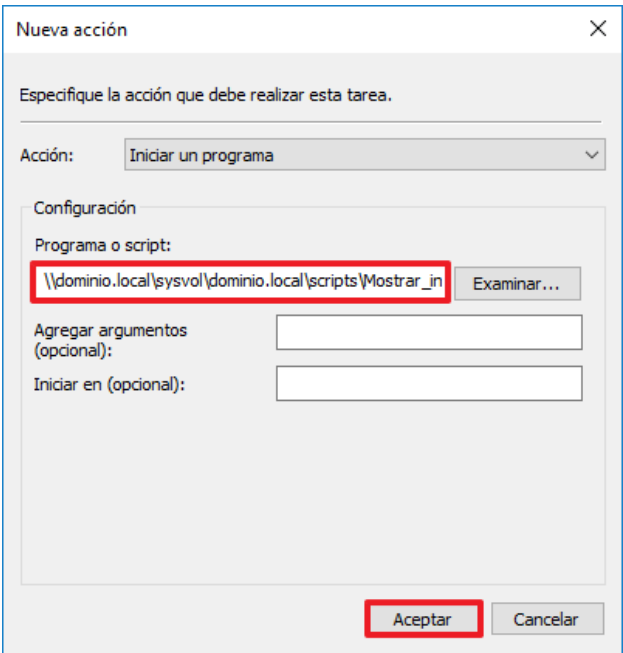
Paso	Descripción
10.	Seleccione con el botón derecho la GPO recién creada y pulse sobre la opción del menú contextual “Importar configuración...”. 
11.	En el “Asistente para importar configuración” pulse “Siguiente >”. 

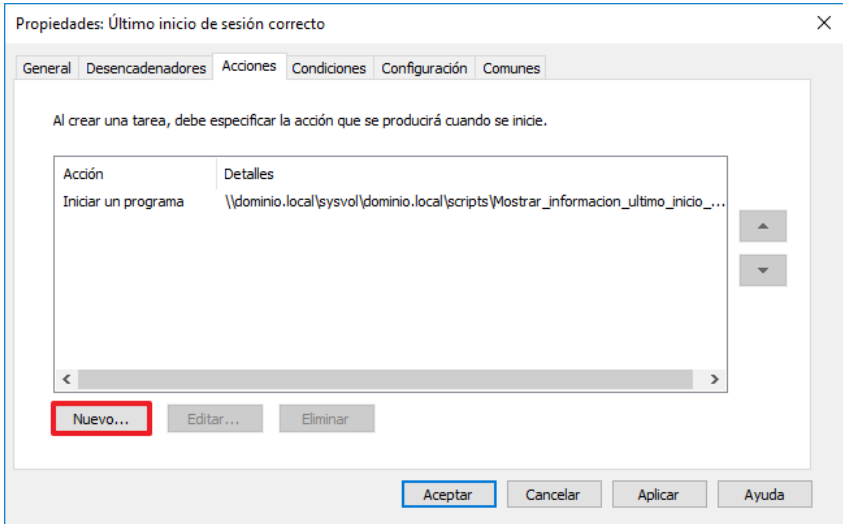
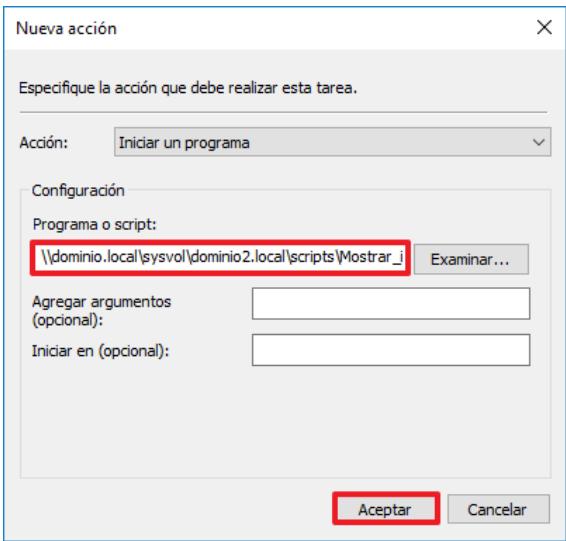
Paso	Descripción
12.	En apartado “Hacer copia de seguridad de GPO” pulse de nuevo “Siguiete >”. 
13.	En “Ubicación de copia de seguridad” pulse sobre “Examinar...”. 
14.	Navegue a la ubicación “C:\Scripts” y seleccione la carpeta “CCN-STIC-599A19 ENS incremental informacion inicio de sesion”. Pulse “Aceptar” para continuar. 

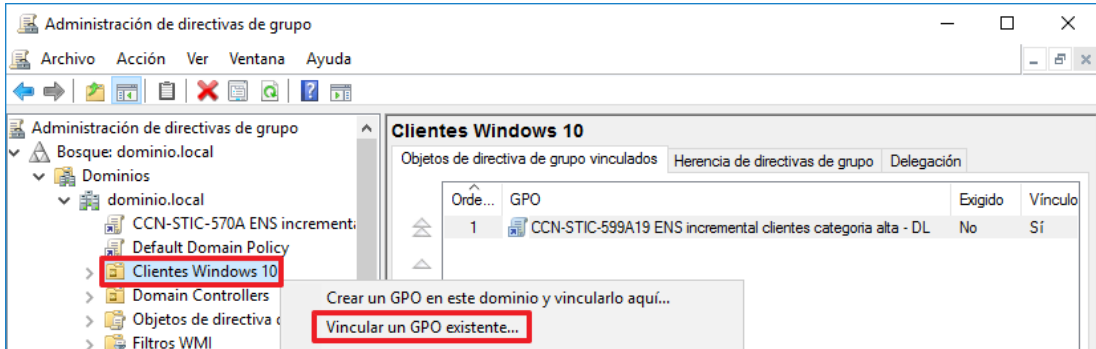
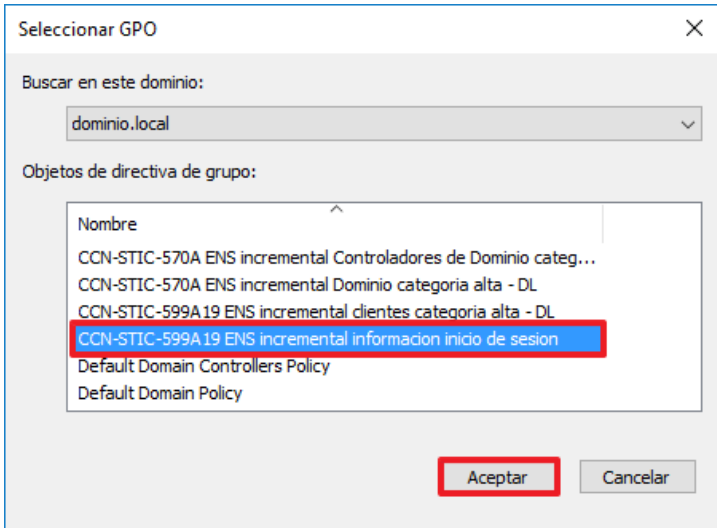
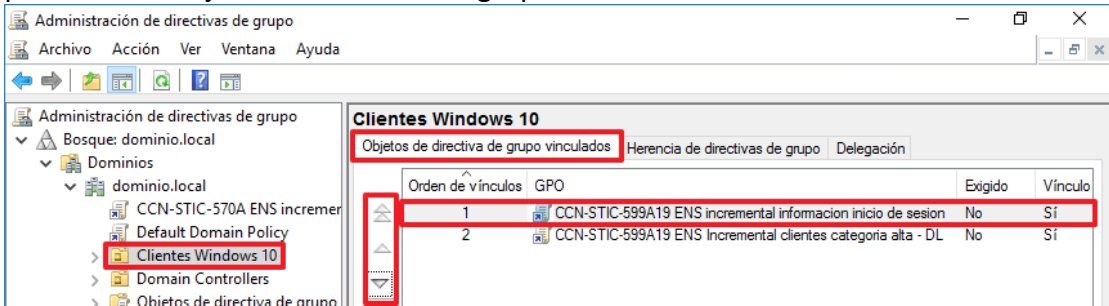
Paso	Descripción
15.	Pulse “Siguiete >” para seguir con la importación de seguridad. 
16.	Pulse de nuevo “Siguiete >” en el apartado “GPO de origen”. 

Paso	Descripción
17.	En el apartado “Examinar copia de seguridad” pulse “Siguiente >”. 
18.	Pulse “Finalizar” para terminar de importar la copia de seguridad.
19.	Pulse “Aceptar” para continuar. 

Paso	Descripción
20.	Seleccione de nuevo la GPO recién creada con el botón derecho y seleccione la opción del menú contextual “Editar...”. 
21.	Despliegue en el editor de administración de directivas de grupo el nodo “Configuración de equipo → Preferencias → Configuración del Panel de control → Tareas programadas”.
22.	Seleccione con el botón derecho la tarea programada existente y seleccione “Propiedades”. 
23.	En la ventana emergente selecciones la pestaña “Acciones”.

Paso	Descripción
24.	A continuación, seleccione la línea existente y pulse sobre “Editar...”. 
25.	En la ventana emergente edite el apartado “Programa o script:” añadiendo la información de su organización.  Nota: En el ejemplo se utiliza el dominio denominado “dominio.local”. Deberá adaptar estos nombres a los utilizados en su organización teniendo en consideración la ruta del dominio y/o subdominio utilizado.

Paso	Descripción
26.	En caso de necesitar esta tarea en otros dominios o subdominios del bosque deberá, en la ventana “Propiedades:”, dentro de la pestaña “Acciones” seleccionar la opción “Nuevo...”. 
27.	En la ventana “Nueva acción” indique la ruta del dominio o subdominio deseado. Pulse “Aceptar” para continuar.  Nota: En este ejemplo se utiliza el subdominio “dominio2.local”. Adapte los nombres a las necesidades de su organización.
28.	Repita la operativa por cada dominio o subdominio en el que necesite la ejecución del script. Solo será necesario editar la ruta al dominio ya que la carpeta “sysvol” y “scripts” se crean por defecto en los sistemas en una implementación de Active Directory.
29.	Pulse “Aceptar” para finalizar la configuración de la tarea programada y cierre el editor de administración de directivas de grupo.
30.	Identifique ahora las unidades organizativas sobre las que se está aplicando seguridad según criterios del ENS.

Paso	Descripción
31.	Seleccione la unidad organizativa sobre la que desee aplicar la GPO recién configurada con el botón derecho y seleccione la opción del menú contextual “Vincular GPO existente...”.  Nota: En este ejemplo se utiliza la unidad organizativa “Clientes Windows 10”. Deberá adaptar estos pasos a las necesidades de su organización.
32.	Seleccione la GPO “CCN-STIC-599A19 incremental informacion inicio de sesion”. 
33.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la primera posición del orden de vínculos en la pestaña de “Objetos de directiva de grupo vinculados”. 

2.2. DELEGACIÓN DE PERMISOS DE ESCRITURA SOBRE ATRIBUTO DE USUARIO

Debido a la necesidad de almacenar la información del último inicio de sesión en un atributo propio de cada usuario es necesario delegar el permiso sobre cada usuario para que pueda modificar el valor de dicho atributo.

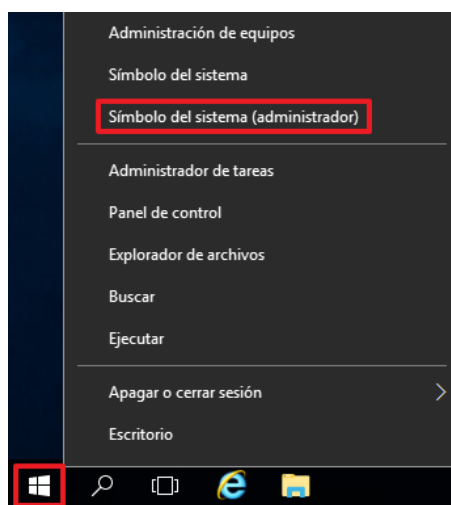
Durante esta implementación se utiliza el atributo “groupsTolgnore”. Este atributo no es utilizado habitualmente por lo que es idóneo para realizar dicha tarea. No obstante, si su organización hace uso de este atributo, deberá determinar qué atributo utilizar dentro de su organización y adaptar los scripts en consecuencia.

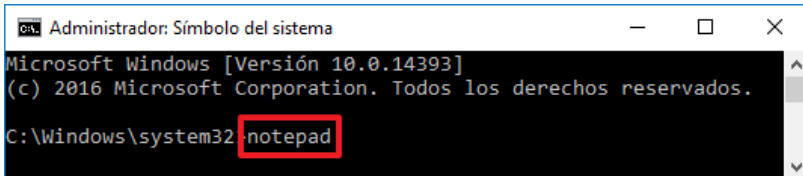
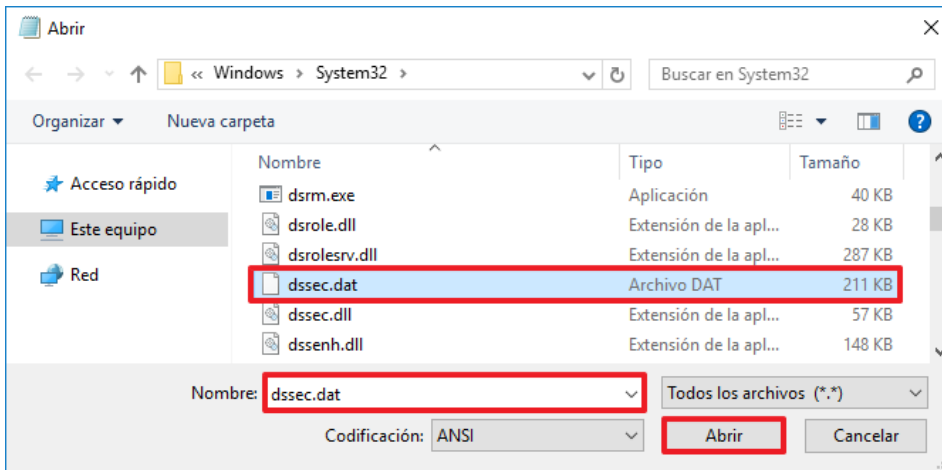
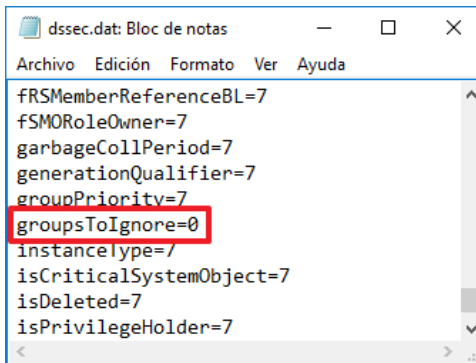
Nota: Deberá modificar el atributo utilizado para almacenar dicha información teniendo en cuenta los siguientes condicionantes:

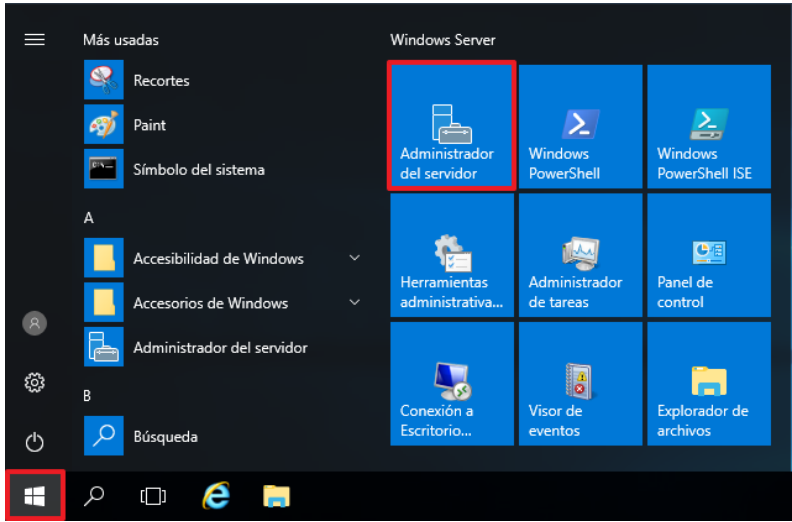
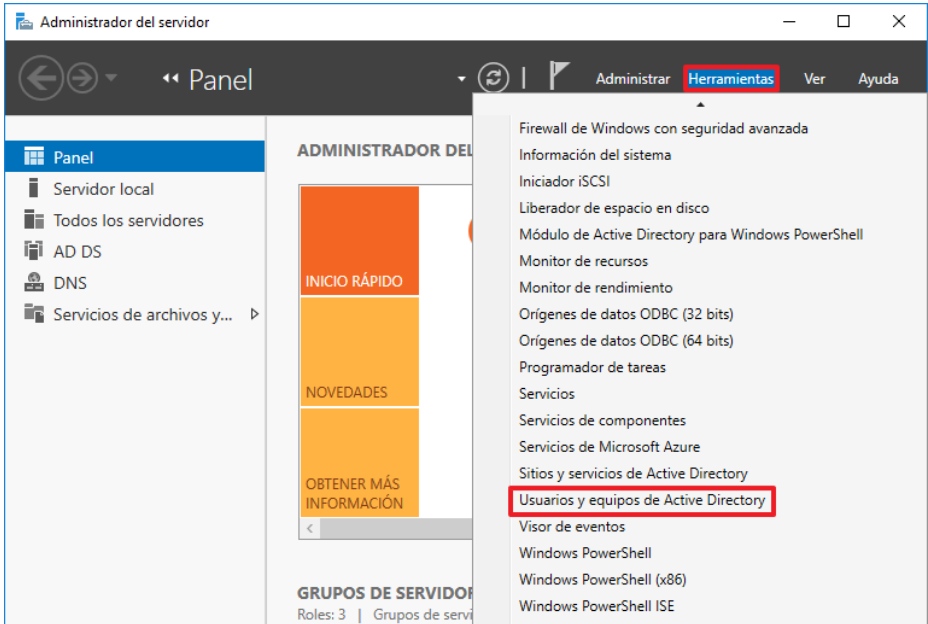
- El atributo no está en uso actualmente.
- El atributo ya no se utiliza/está obsoleto (véase un atributo de Windows NT por ejemplo).
- El atributo debe poder almacenar una cadena de caracteres.
- El atributo puede ser modificado por el propio usuario (de lo contrario deberá delegar el permiso de escritura sobre el atributo).
- Tener previsión de que el atributo utilizado no va a ser modificado por el sistema.

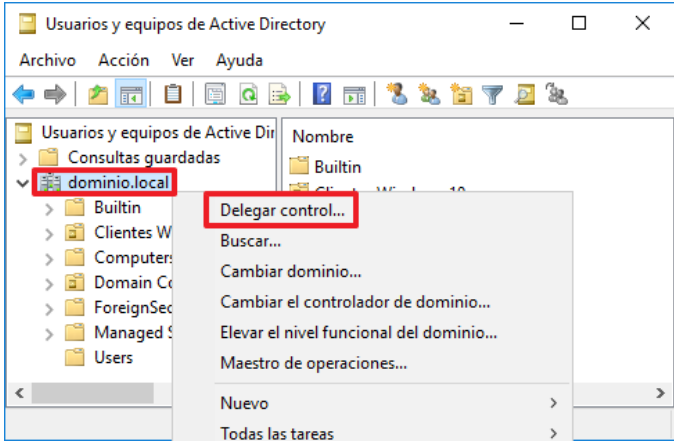
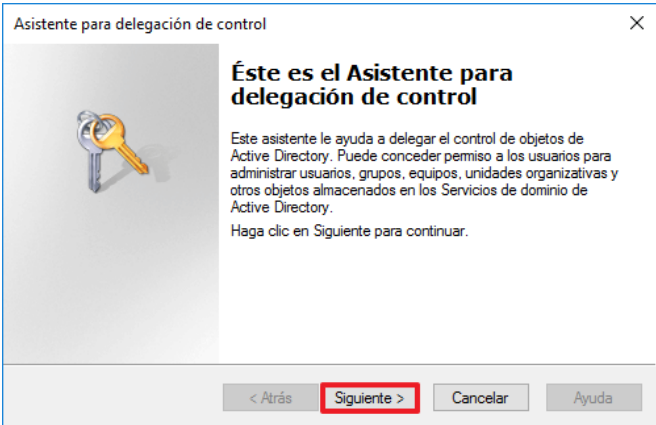
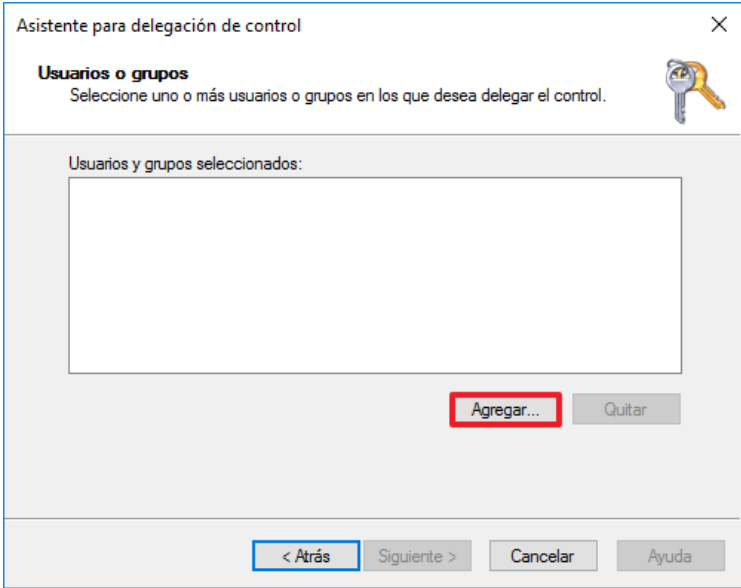
Los pasos que se definen a continuación pueden no ser necesarios en caso de que vaya a utilizarse un atributo diferente al indicado durante este paso a paso. Deberá determinar el atributo deseado y comprobar sus permisos y disponibilidad.

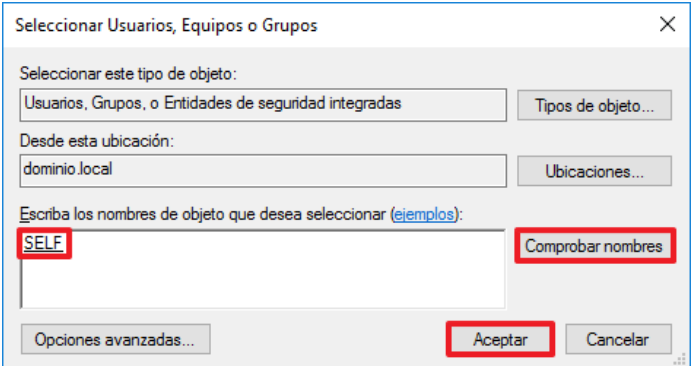
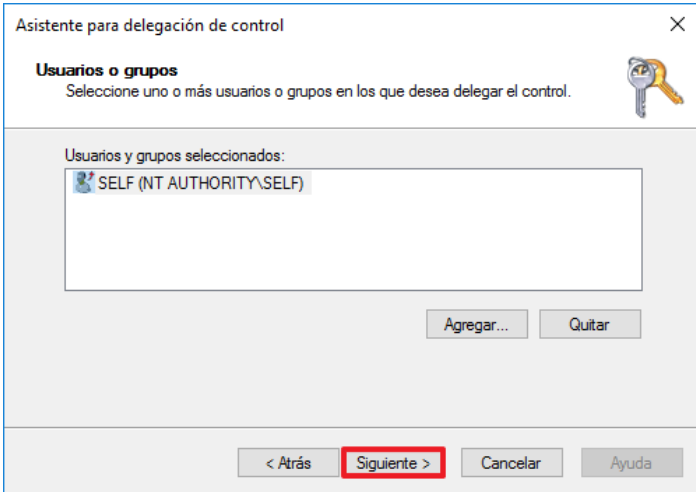
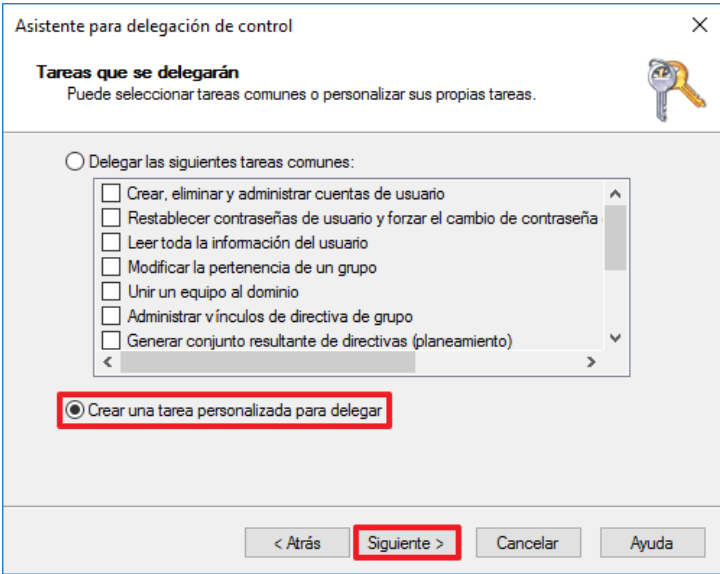
Paso	Descripción
34.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
35.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
36.	Ejecute una consola de comandos como un usuario administrador. Para ello pulse con el botón derecho sobre “Inicio” y seleccione la opción “Símbolo del sistema (administrador)”.

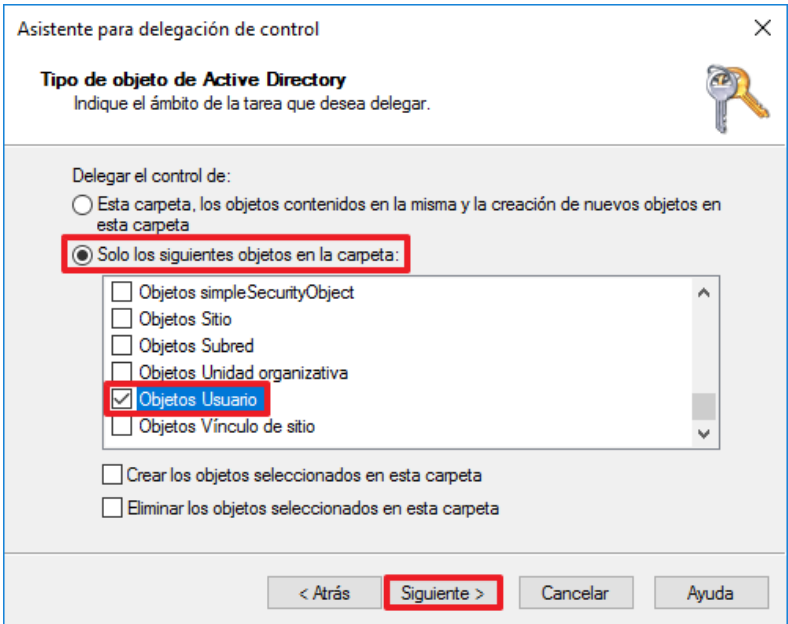
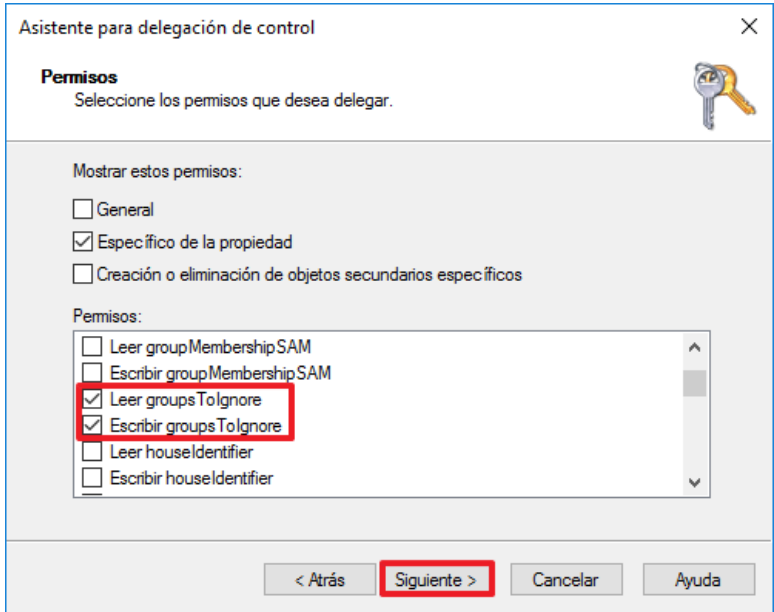


Paso	Descripción
37.	Eleve privilegios para poder acceder a la consola. Nota: Dependiendo de la categoría de seguridad aplicada sobre el sistema deberá elevar privilegios simplemente o bien introducir las credenciales de un usuario con permisos de administrador del dominio.
38.	En la consola escriba “notepad”. 
39.	Abra el fichero denominado “dssec.dat” ubicado en “%SYSTEMROOT%\System32”. Introduzca el nombre “dssec.dat” y pulse el botón “Abrir”.  Nota: Este fichero debe ser editado como administrador para que pueda ser guardado en la ubicación.
40.	En el apartado “[User]” del fichero localice el atributo “groupsToIgnore” y establezca su valor en “0”. Utilice la ruta “Edición → Buscar” para localizar el atributo.  Nota: Tenga en consideración que pueden existir más atributos con el mismo nombre dentro del fichero, pero ubicados en distintos apartados, como pueda ser el apartado “[computer]”. Asegúrese de que modifica el atributo en el apartado “[User]”.

Paso	Descripción
41.	Guarde la configuración realizada desde la ruta “Archivo → Guardar” .
42.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
43.	Eleve privilegios para iniciar el “Administrador del servidor”. Nota: Dependiendo de la categoría de seguridad aplicada deberá confirmar la operación o bien introducir las credenciales de un usuario con privilegios de administrador del dominio.
44.	Inicie la herramienta “Usuarios y equipos de Active Directory” en el apartado “Herramientas”. 

Paso	Descripción
45.	Seleccione con el botón derecho sobre el dominio en uso y pulse sobre la opción del menú contextual “Delegar control...”. 
46.	En el “Asistente para delegación de control” pulse “Siguiente >”. 
47.	Pulse el botón “Agregar...”. 

Paso	Descripción
48.	En la ventana emergente introduzca el usuario “SELF”, pulse sobre “Comprobar nombres” y pulse sobre “Aceptar” para continuar. 
49.	Pulse “Siguiente >” para continuar con la configuración de delegación. 
50.	Seleccione la opción “Crear una tarea personalizada para delegar” y pulse “Siguiente >”. 

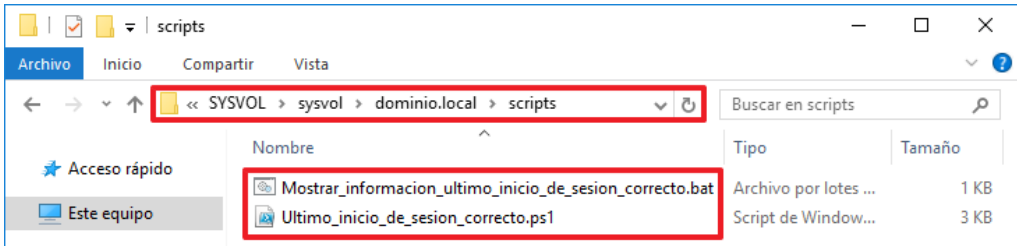
Paso	Descripción
51.	A continuación, marque la opción “Solo los siguientes objetos en la carpeta:” y marque el objeto “Objetos Usuario”. Pulse “Siguiente >” para continuar. 
52.	En el apartado permisos seleccione la opción “Específico de la propiedad” y marque los permisos “Leer groupsTolgnore” y “Escribir groupsTolgnore”. Pulse “Siguiente >” para continuar. 
53.	Pulse “Finalizar” para completar la delegación de control.

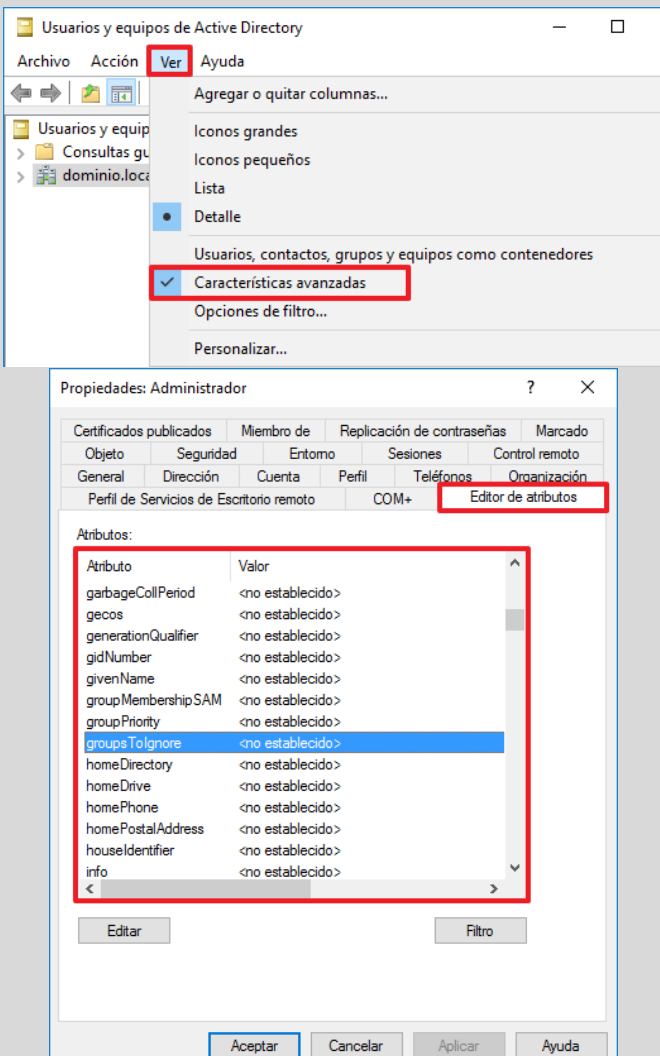
En este punto, cuando un usuario inicie sesión por primera vez no tendrá almacenada información de sesión, pero el siguiente inicio ya mostrará la información (fecha y hora) del último inicio de sesión realizado correctamente.

2.3. CONFIGURACIÓN DE SCRIPTS PARA MOSTRAR LA INFORMACIÓN DE INICIO DE SESIÓN

En este momento existe una GPO configurada y asociada a una unidad organizativa. Esta GPO crea una tarea programada en cada equipo que esté asociado a esta GPO, y ejecuta un script que muestra el ultimo inicio de sesión correcto que ha realizado el usuario.

Los pasos definidos a continuación establecen la configuración a realizar para que el script se ejecute al inicio de cada sesión de usuario. Este script no ha sido diseñado para que se ejecute como script de inicio de sesión ya que estos están deshabilitados por otras directivas.

Paso	Descripción
54.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
55.	Pulse con botón derecho en el menú de inicio y seleccione el “Explorador de archivos”.
56.	Copie los siguientes ficheros al directorio “%SYSTEMROOT%\SYSVOL\sysvol\nombre_de_su_dominio\scripts”: – “Mostrar_informacion_ultimo_inicio_de_sesion_correcto.bat” – “Ultimo_inicio_de_sesion_correcto.ps1  Nota: Adapte esta ruta a la configuración que posea su organización. En el ejemplo está establecida la ruta por defecto del directorio “sysvol\dominio.local\scripts”. Deberá tener en consideración la replicación de estos ficheros en los diferentes dominio y subdominios que posea su organización para que estos ejecutados. El sistema le solicitará elevación de privilegios.
57.	Edite el fichero “Mostrar_informacion_ultimo_inicio_de_sesion_correcto.bat” y modifique el nombre del dominio para que coincida con el de su organización. <pre>@echo off powershell.exe -nopprofile -executionpolicy bypass -File "\\dominio.local\sysvol\dominio.local\scripts\Ultimo_inicio_de_se @echo off</pre> Nota: En este ejemplo se utiliza el nombre de dominio “dominio.local” y la ruta por defecto “\\sysvol\dominio.local\scripts”. Deberá editar esta ruta para que se adapte al nombre de su organización.

Paso	Descripción
58.	A continuación, edite el fichero “Ultimo_inicio_de_sesion_correcto.ps1”. Este script hace uso de los atributos del usuario para almacenar la información del último inicio de sesión tal y como se muestra en la imagen. <pre> \$objs = @() \$errorActionPreference = 'SilentlyContinue' \$ADProperty = 'groupstoignore' </pre> Nota: Para este ejemplo se ha utilizado el atributo de usuario “groupsToIgnore”. Para determinar que atributo es modificado puede hacer uso del siguiente enlace: https://msdn.microsoft.com/en-us/library/ms675090(v=vs.85).aspx. Podrá comprobar los atributos en uso dentro de la herramienta “Usuarios y Equipos de Active Directory” existente en el controlador de dominio, visualizando las “Características avanzadas”. Seleccione la que más se adecúe a las necesidades de su organización. 

3. 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:

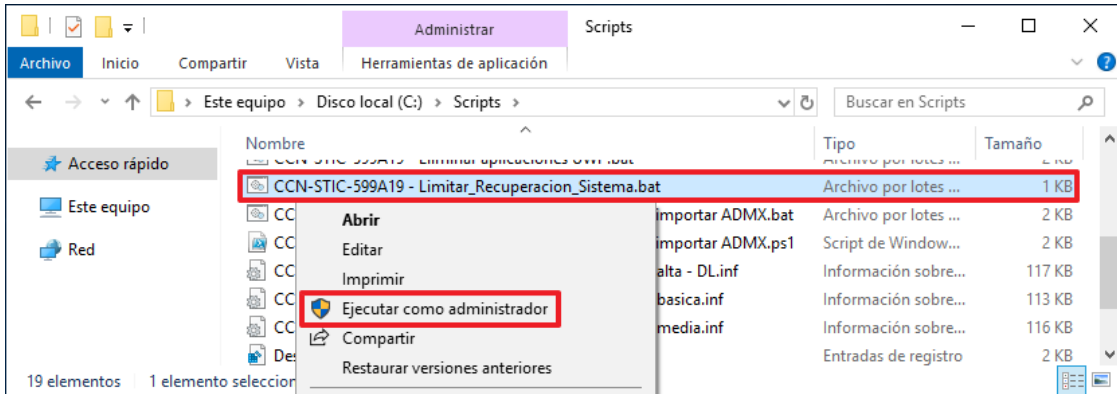
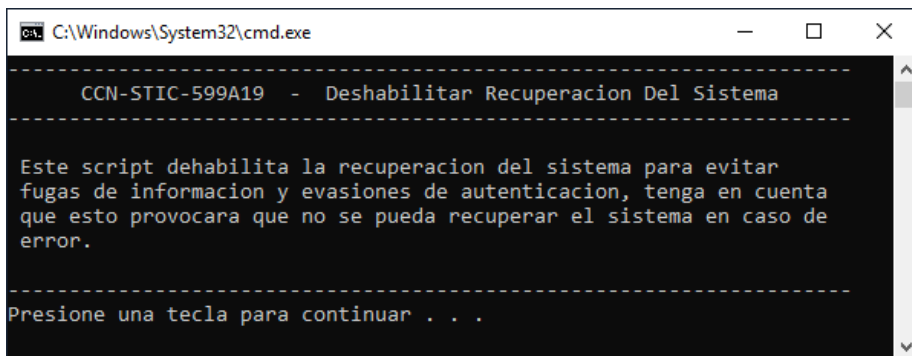
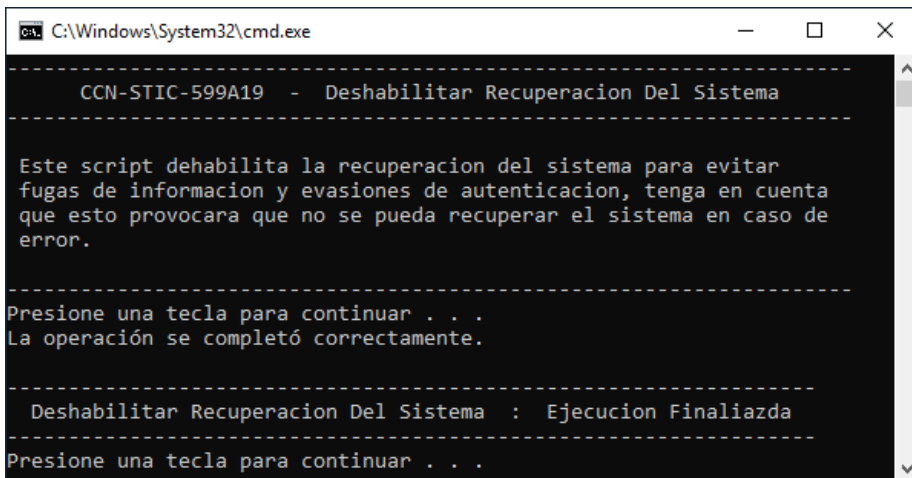
- Cifrado del sistema de archivos. Utilizar BitLocker u otro sistema de cifrado autorizado para evitar el acceso a la información almacenada y, por tanto, evitar su modificación ya que requiere de la introducción de un PIN o contraseña en el arranque del equipo, o en el momento de acceder a los datos. 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.

3.1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

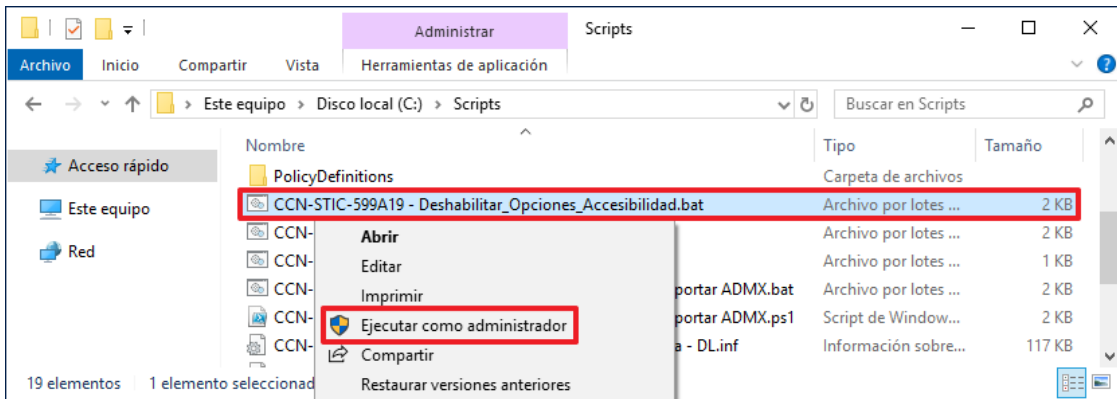
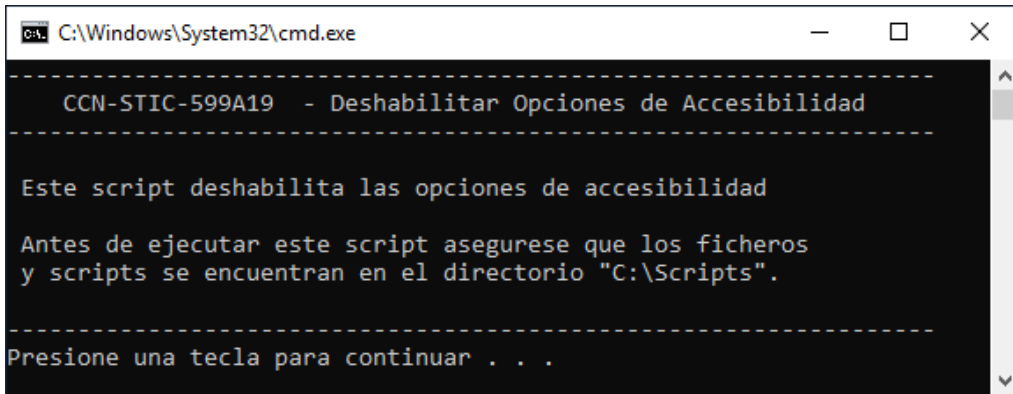
A continuación, se indican los pasos a realizar para deshabilitar la funcionalidad de recuperación del sistema.

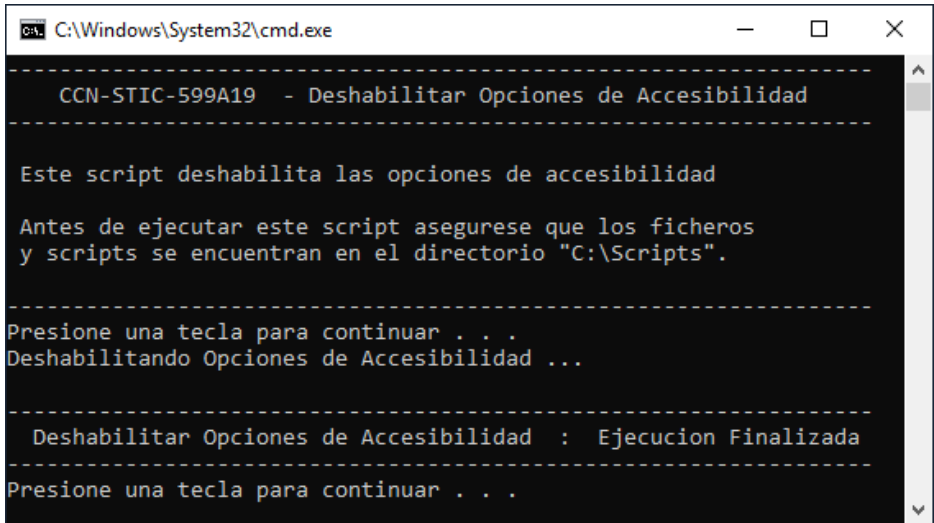
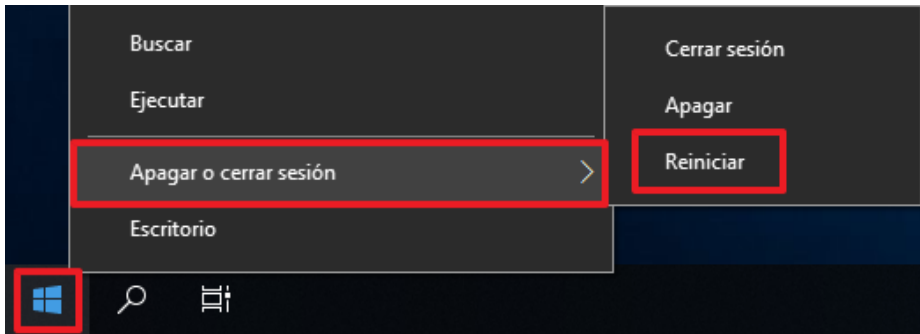
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador del dominio.

Paso	Descripción
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-599A19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.  Nota: El sistema le solicitará elevación de privilegios.
4.	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. 
5.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana. 
6.	Elimine el directorio “C:\Scripts”.

3.2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD

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

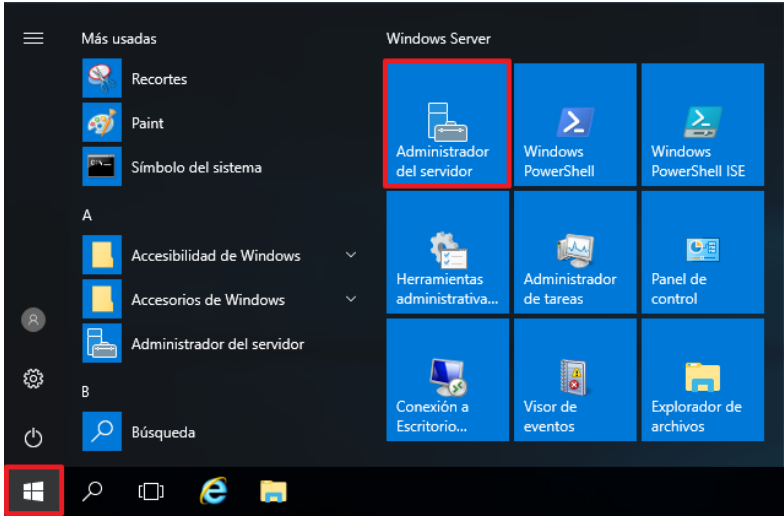
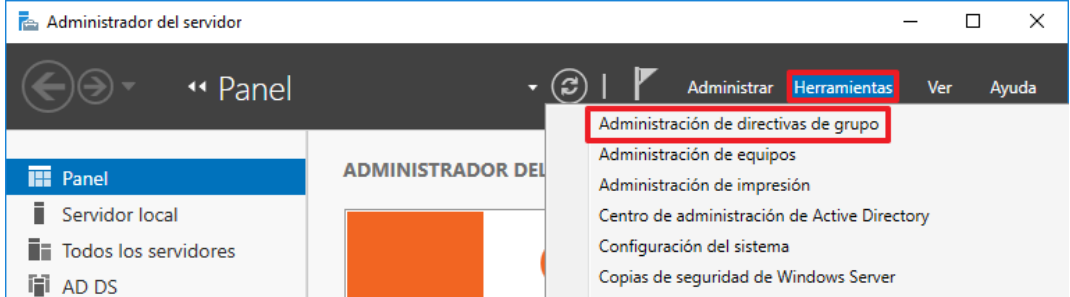
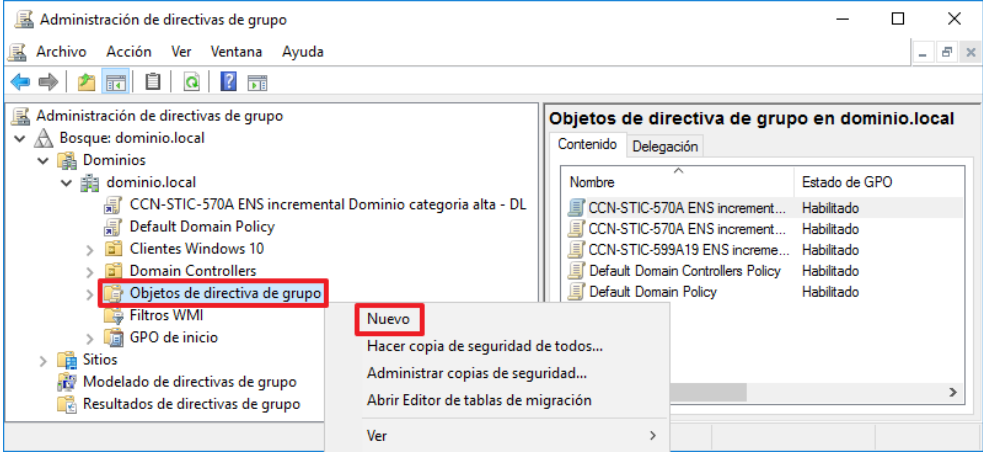
Paso	Descripción
7.	Inicie sesión en el equipo con una cuenta con permisos de administrador del dominio.
8.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
9.	Localice el archivo “CCN-STIC-599A19 – Deshabilitar_Opciones_Accesibilidad.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.  Nota: El sistema le solicitará elevación de privilegios.
10.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 

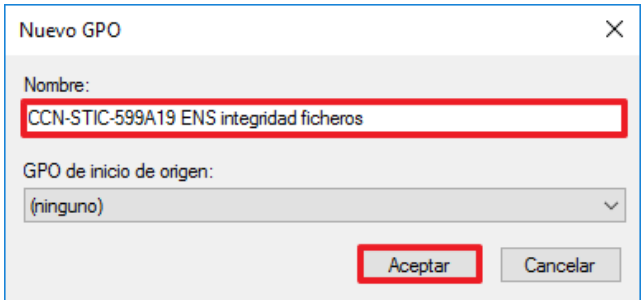
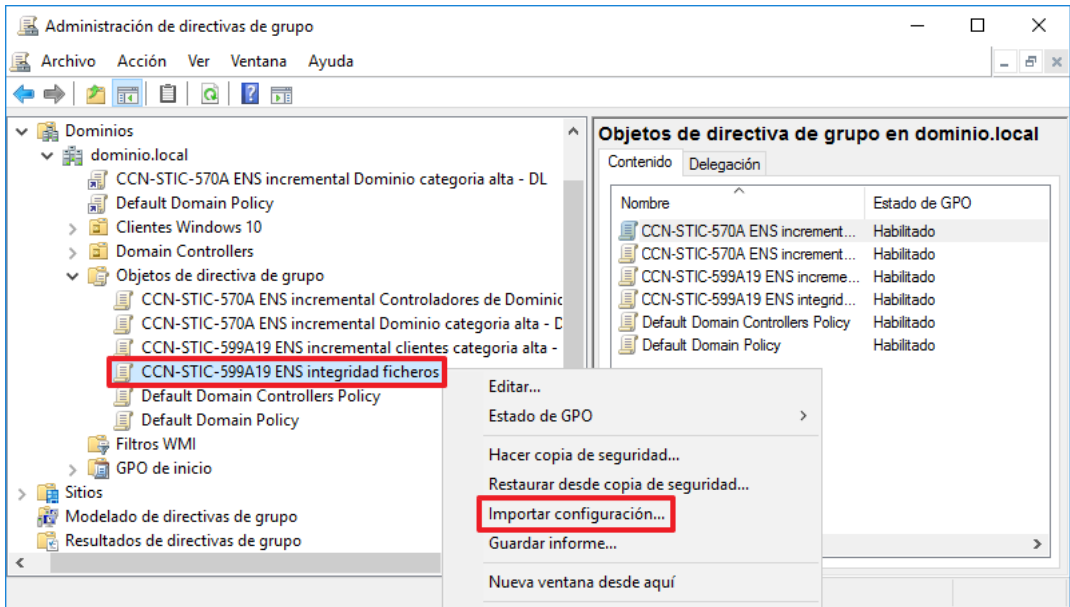
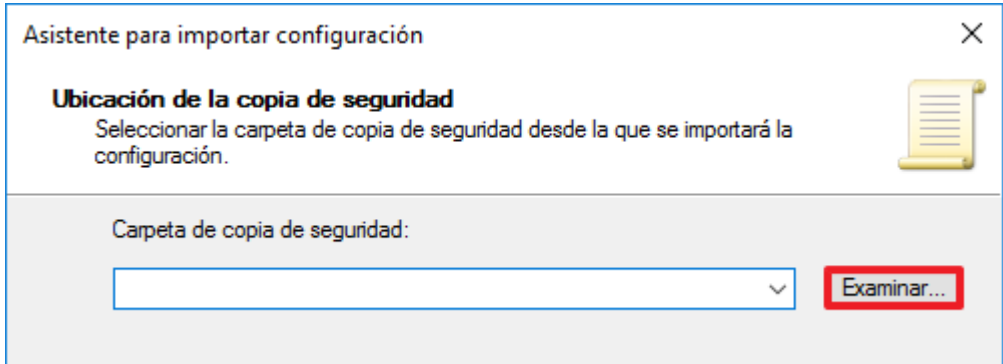
Paso	Descripción
11.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comando 
12.	Por último, deberá reiniciar el sistema para que los cambios sean aplicados. Para ello haga clic derecho en el botón de “Inicio” y seleccione “Apagar o cerrar sesión → Reiniciar”. 
13.	Elimine el directorio “C:\Scripts”.

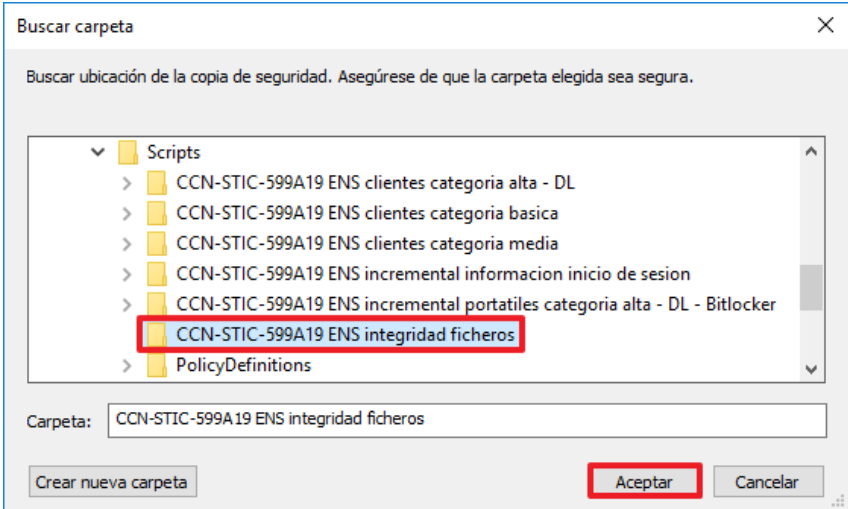
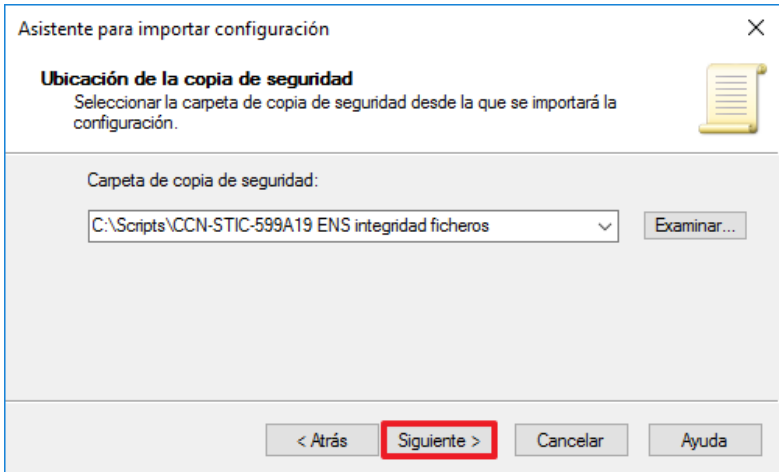
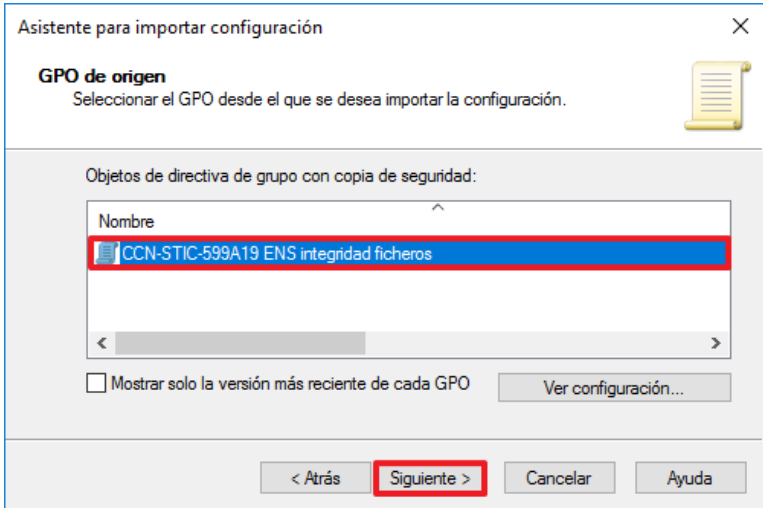
3.3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

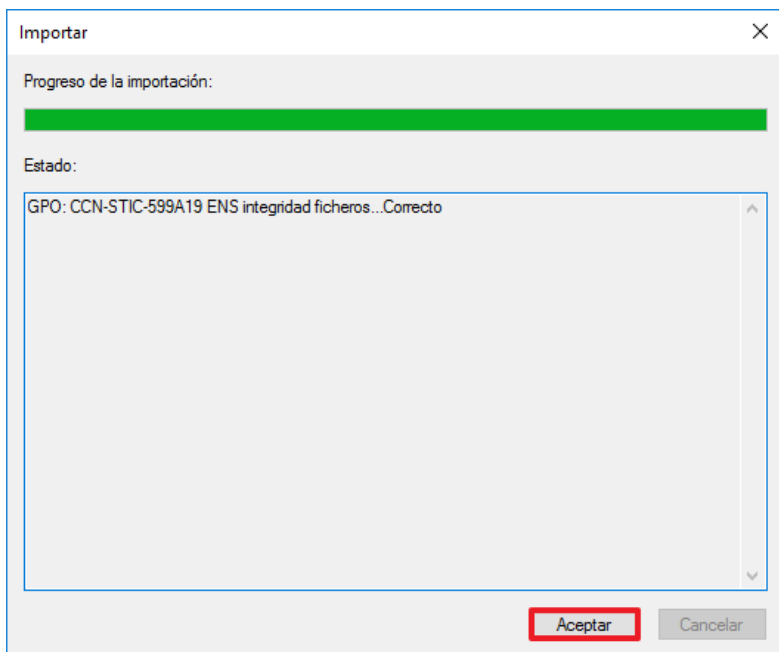
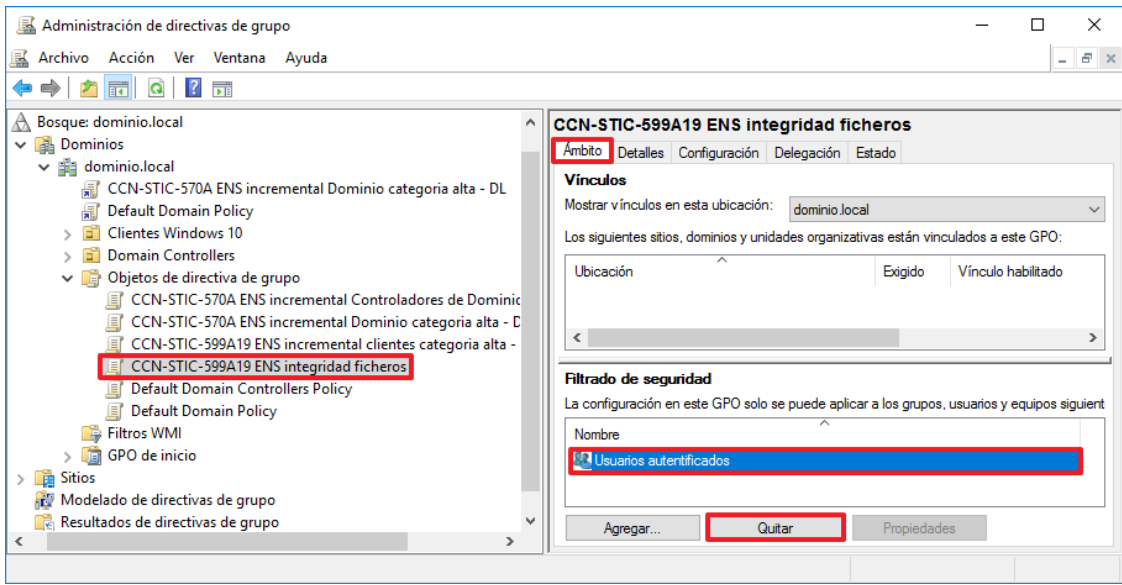
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

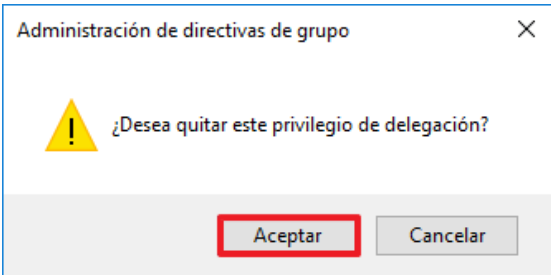
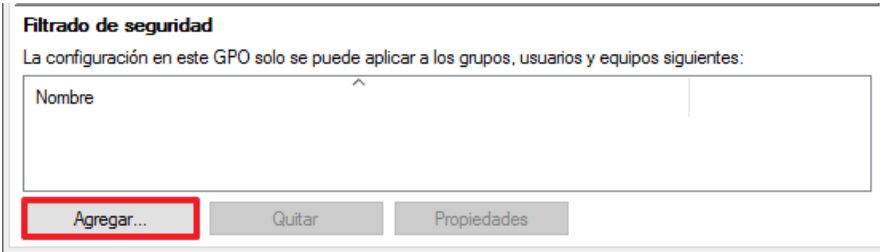
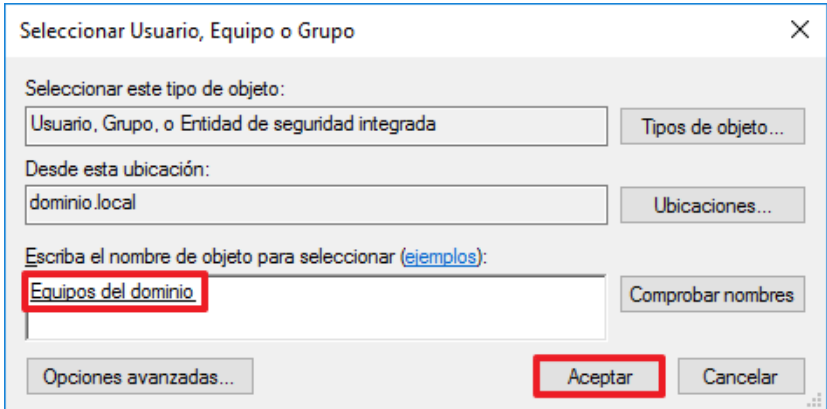
Paso	Descripción
14.	Inicie sesión en el servidor controlador de dominio al que pertenecen los equipos cliente que van a asegurar, con una cuenta con derechos de administración en el dominio.
15.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.

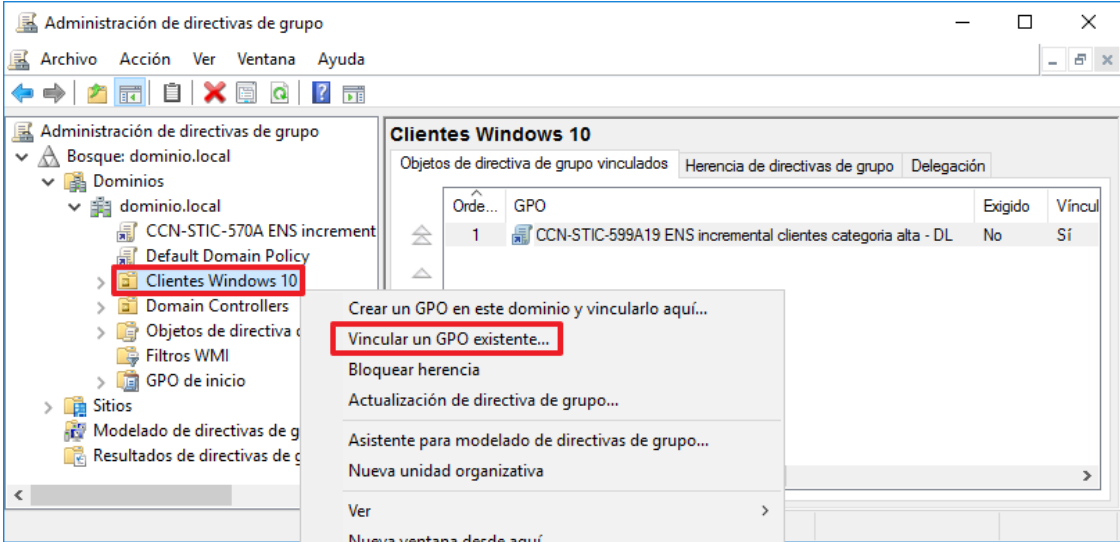
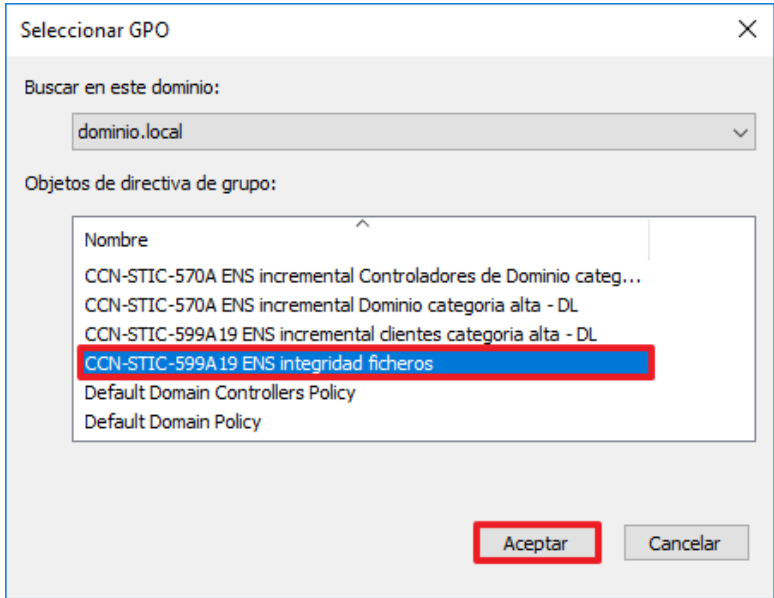
Paso	Descripción
16.	Inicie el “Administrador del servidor” desde el icono correspondiente en el menú de inicio. 
17.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Administración de directivas de grupo”. 
18.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
19.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" y, marcando con el botón derecho sobre él, elija la opción "Nuevo" del menú contextual que aparecerá. 

Paso	Descripción
20.	Asigne el siguiente nombre "CCN-STIC-599A19 integridad ficheros" a la nueva GPO y pulse "Aceptar". 
21.	Seleccione la GPO recién creada, "CCN-STIC-599A19 integridad ficheros" con el botón derecho y pulse sobre la opción "Importar configuración..." en el menú contextual que aparecerá. 
22.	En el "Asistente para importar configuración" pulse "Siguiente >".
23.	En apartado "Hacer copia de seguridad de GPO" pulse de nuevo "Siguiente >".
24.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 

Paso	Descripción
25.	Localice la carpeta “CCN-STIC-599A19 ENS Integridad Ficheros” en el directorio “C:\Scripts” y pulse “Aceptar”. 
26.	Pulse “Siguiente >” para continuar. 
27.	En “GPO de origen” pulse “Siguiente >”. 

Paso	Descripción
28.	En el apartado “Examinar copia de seguridad” pulse “Siguiente >”.
29.	Pulse “Finalizar” para terminar de importar la copia de seguridad.
30.	Pulse “Aceptar” para continuar. 
31.	Seleccione la nueva política de grupo configurada y vaya a las opciones de ámbito que se encuentran en el panel derecho. Seleccione el grupo “Usuarios autenticados” y pulse sobre el botón “Quitar”. 

Paso	Descripción
32.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 
33.	Pulse ahora sobre el botón “Agregar...”. 
34.	Introduzca como nombre “Equipos del dominio”. A continuación, pulse el botón “Aceptar”. 

Paso	Descripción
35.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
36.	Seleccione “CCN-STIC-599A19 integridad ficheros” de la lista y pulse “Aceptar”. 
37.	Elimine el directorio “C:\Scripts”.

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

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 anexo 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-599A19” 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 (versión 1809) sin opción de mantenimiento LTSC. 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 mediante GPO. En el anexo para la versión Pro/Enterprise, además de la configuración descrita anteriormente, se limita por la aplicación de la presente guía.

- 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.

Internet Explorer 11 será securizado según los mecanismos definidos en la guía CCN-STIC-520, tal y como se indicará en el correspondiente paso a paso. Las políticas y configuraciones de dicha guía se aplican junto con las de la presente durante los pasos que aseguran el equipo cliente Microsoft Windows 10.

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.

ANEXO B.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 ENTERPRISE LTSC COMO CLIENTE MIEMBRO DE DOMINIO

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) miembro de un dominio de Windows.

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.2.1 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.
- j) Deberá disponer de la guía CCN-STIC-520 – INTERNET EXPLORER 11 para aplicarla durante los pasos finales de la presente sección.

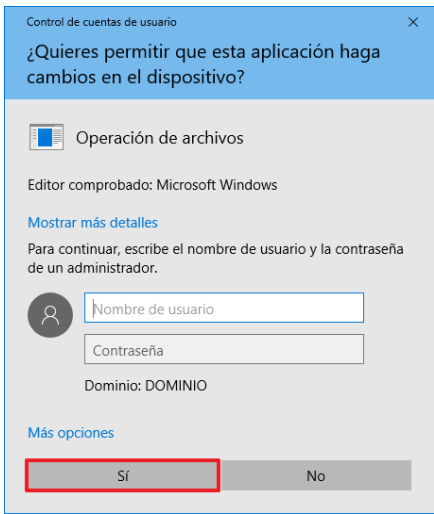
El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación. No se proporciona un fichero de respuestas automáticas, como se hacía en otras guías para versiones anteriores de Windows, porque la instalación por defecto de Microsoft 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.

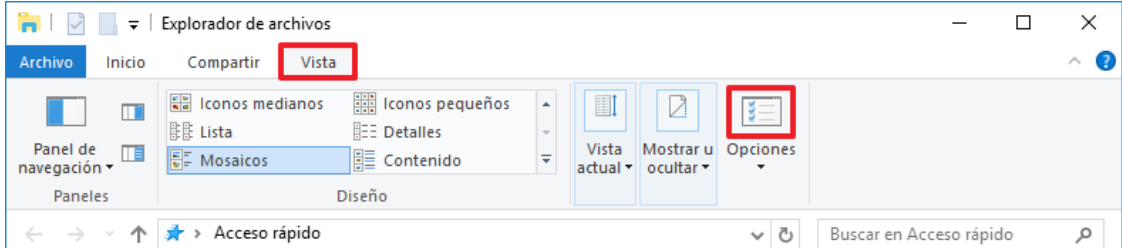
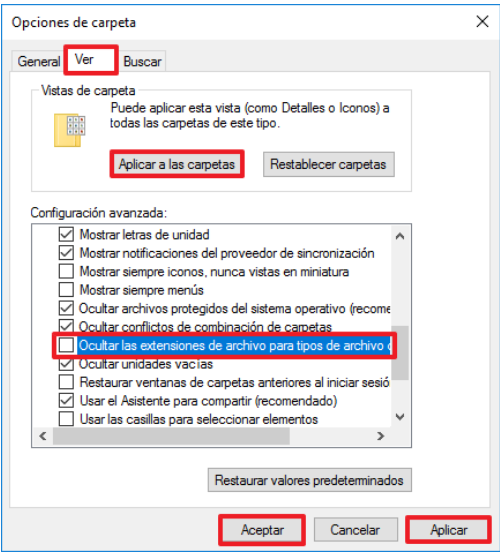
1. PREPARACIÓN DEL DOMINIO

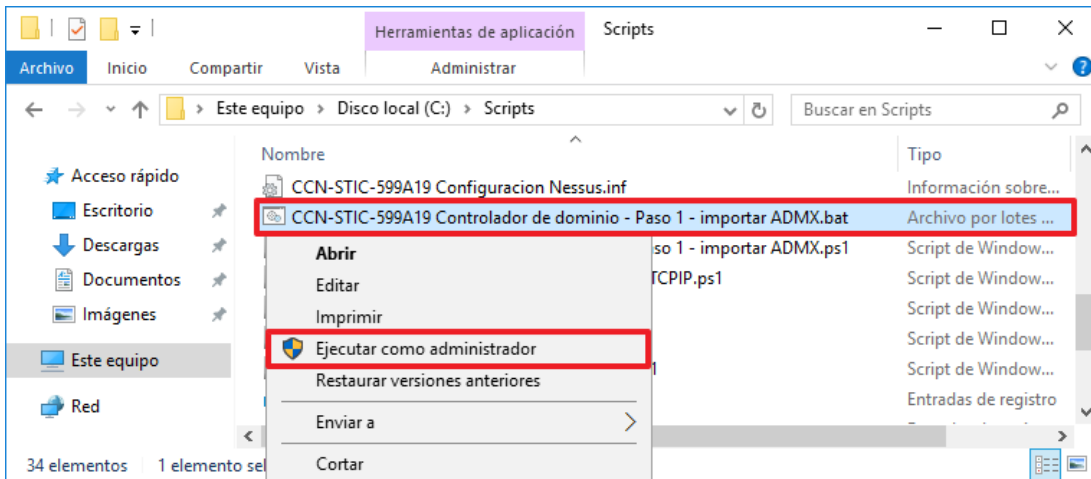
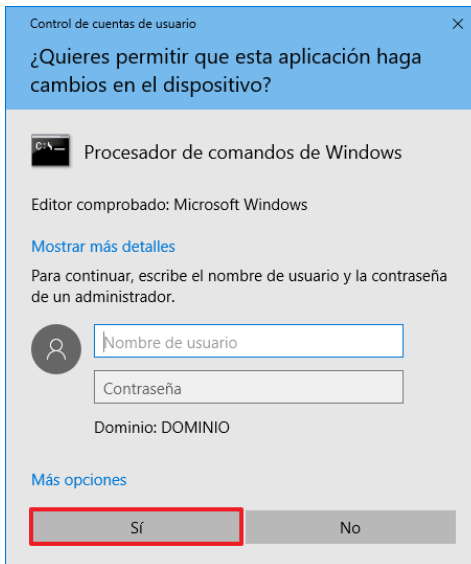
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

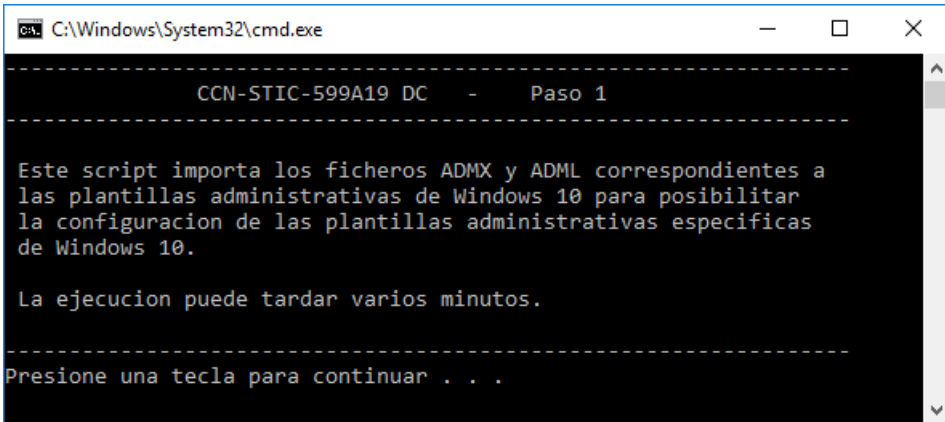
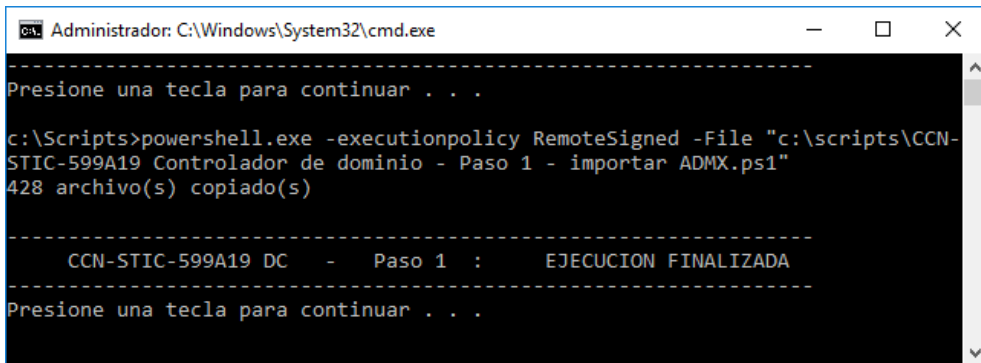
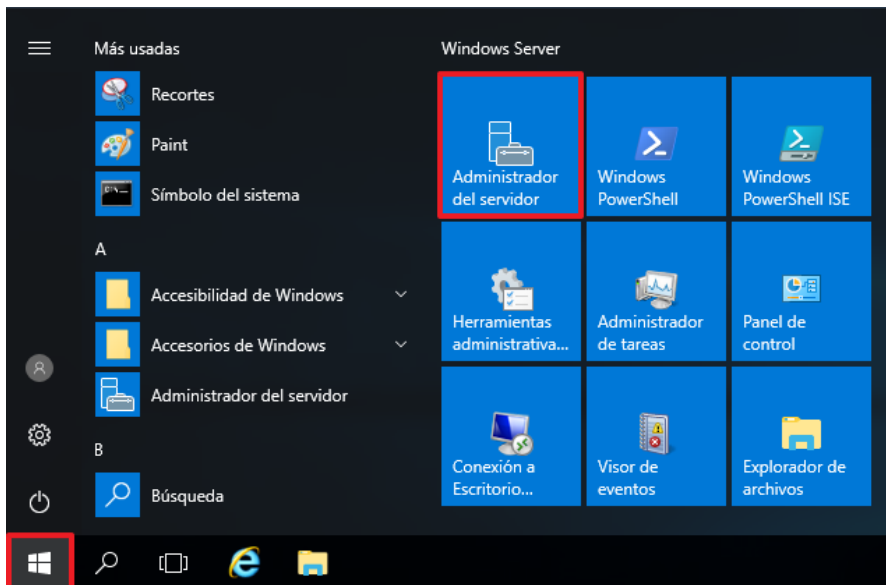
Para el resto de clientes Windows 10 miembros del mismo dominio deberá saltar estos pasos e ir directamente al paso 85, ya que esos clientes compartirán la configuración establecida en este punto y, de forma automática, recibirán las configuraciones de dominio y las relativas a la Unidad Organizativa "Clientes Windows 10 - Equipos".

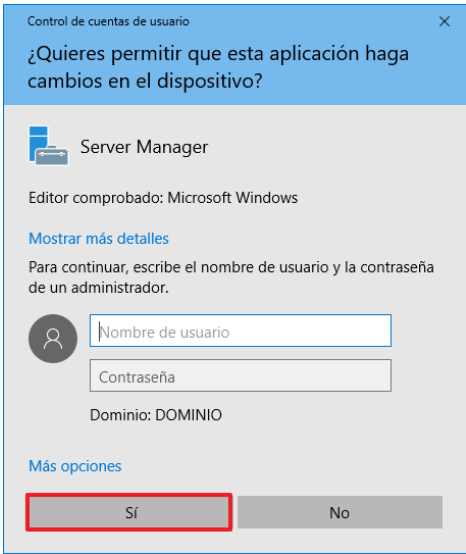
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía “CCN-STIC-570A WINDOWS SERVER 2016 CONTROLADOR DE DOMINIO”. Si no es así, aplique la guía correspondiente a los controladores de dominio, antes de continuar con la aplicación de ésta.

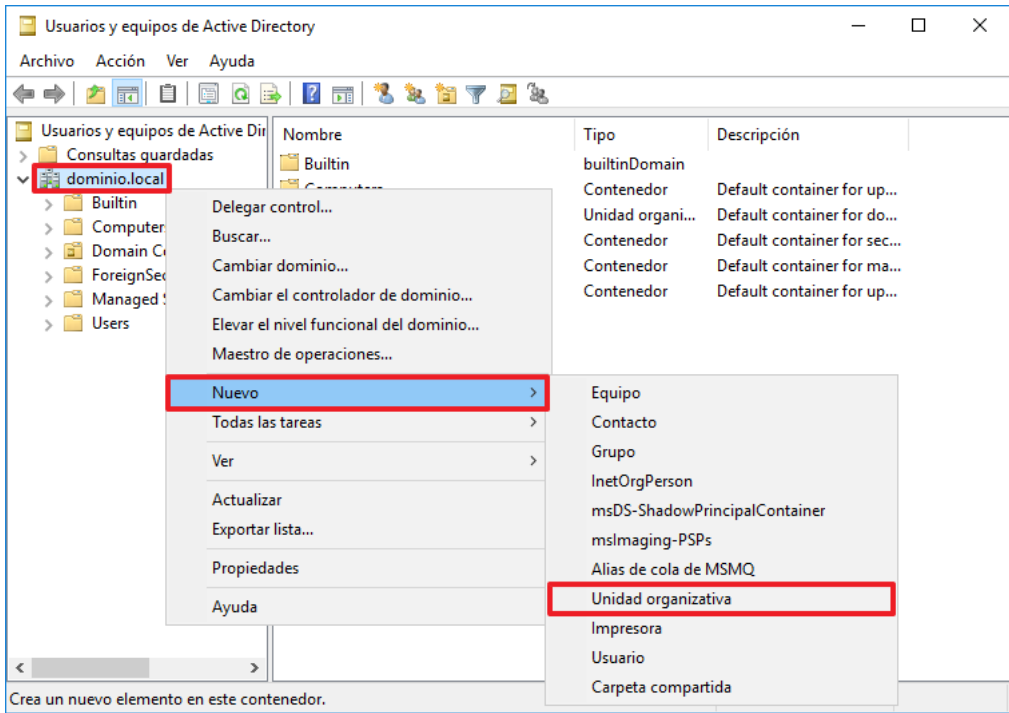
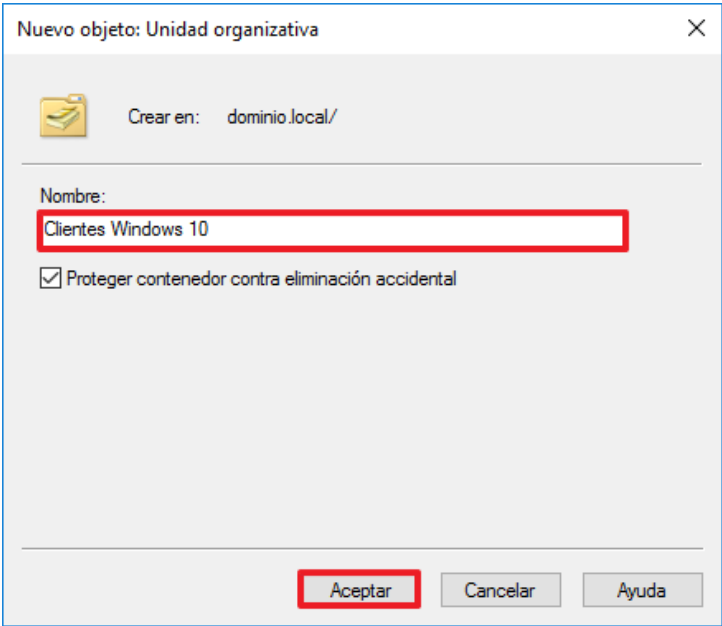
Paso	Descripción
1.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. El sistema le solicitará elevación de privilegios, introduzca las credenciales de un usuario con permisos de administrador. 

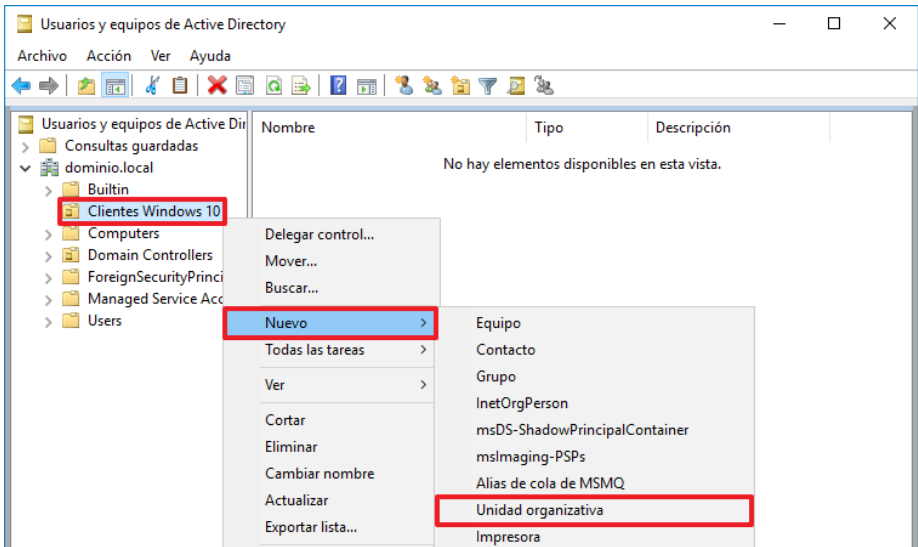
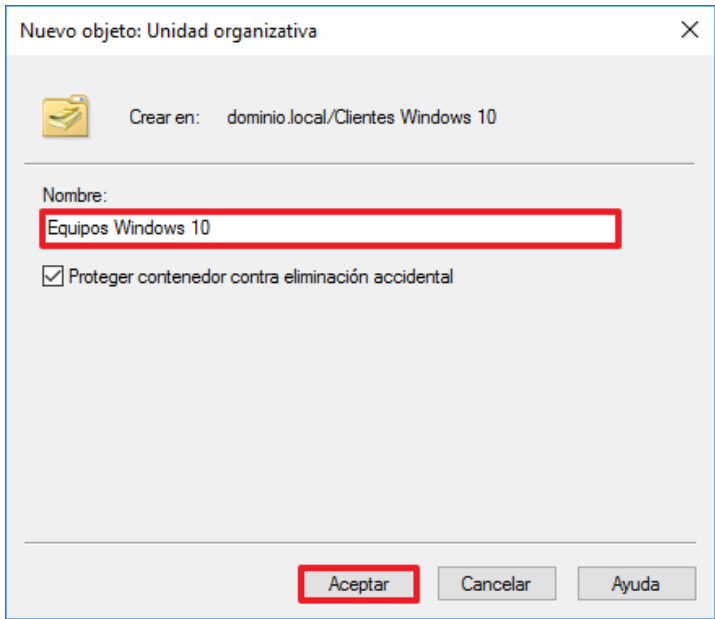
Paso	Descripción
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio. El sistema le solicitará elevación de privilegios. Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". Los scripts asumen que su 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.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-599A19 Windows 10 - Equipos (directorio) – CCN-STIC-599A19 Windows 10 - Usuarios (directorio) – CCN-STIC-599A19 Cliente Miembro.inf – CCN-STIC-599A19 Cliente Miembro.wfw – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1
5.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 
6.	En "Opciones de carpeta" sitúese en la pestaña "Ver" y en el campo "Configuración avanzada" localice y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos". Pulse primero sobre el botón "Aplicar", después sobre "Aplicar a las carpetas" (Pulse "Sí" ante el mensaje de confirmación) y, por último, pulse "Aceptar". 

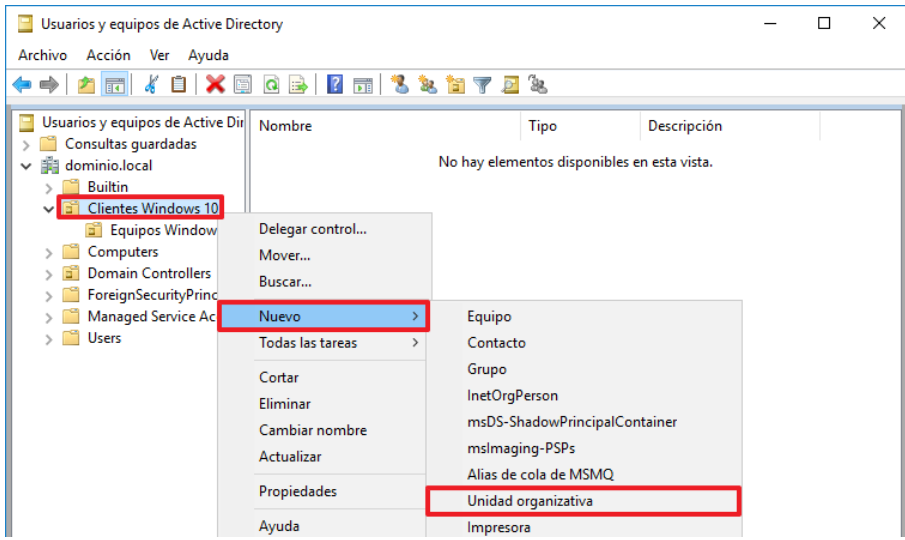
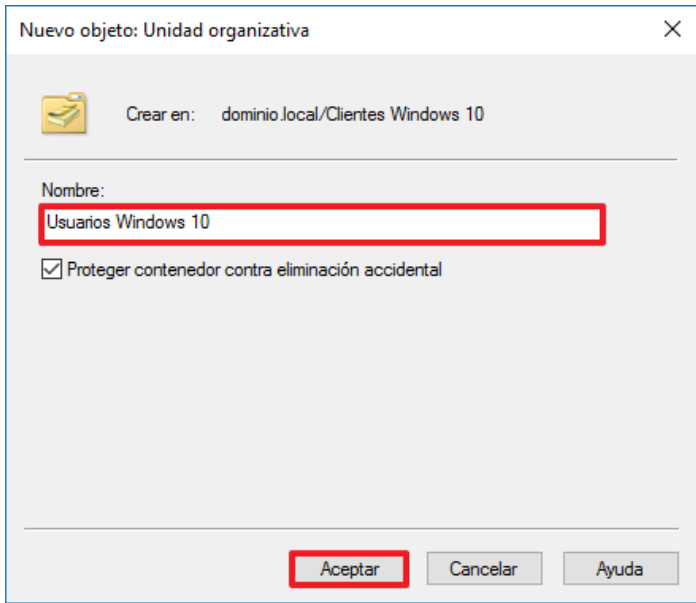
Paso	Descripción
7.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
8.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio y administración de esquema. 

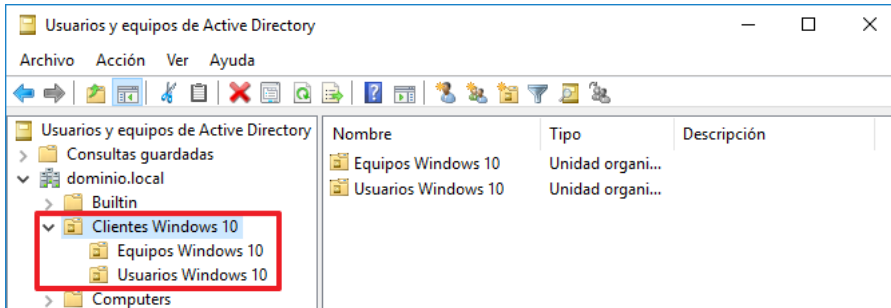
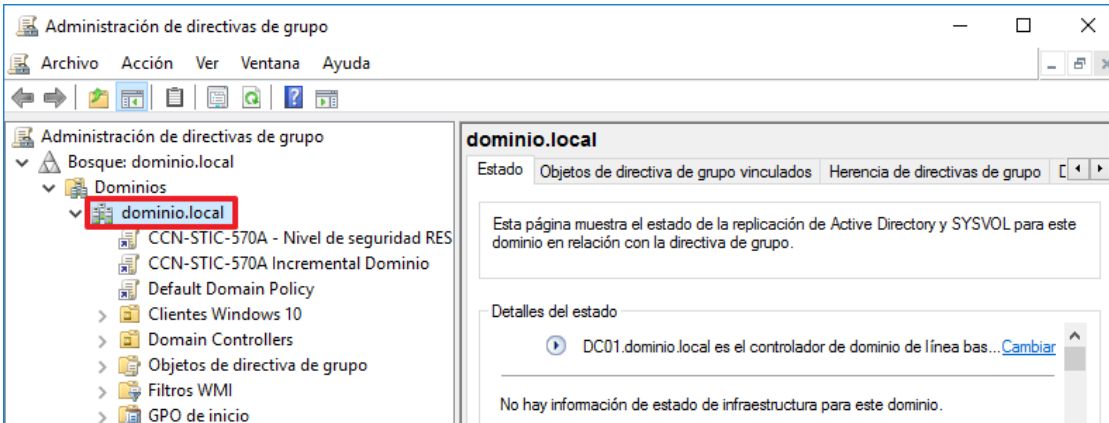
Paso	Descripción
9.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
10.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 
11.	Cree la unidad organizativa "Clientes Windows 10". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

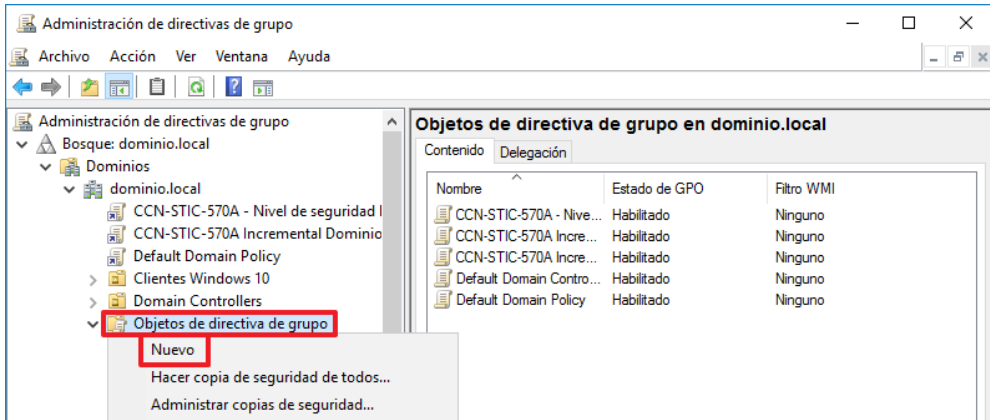
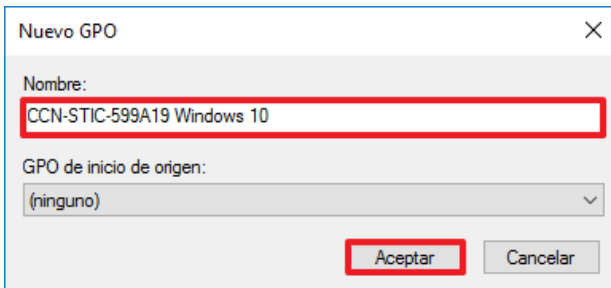
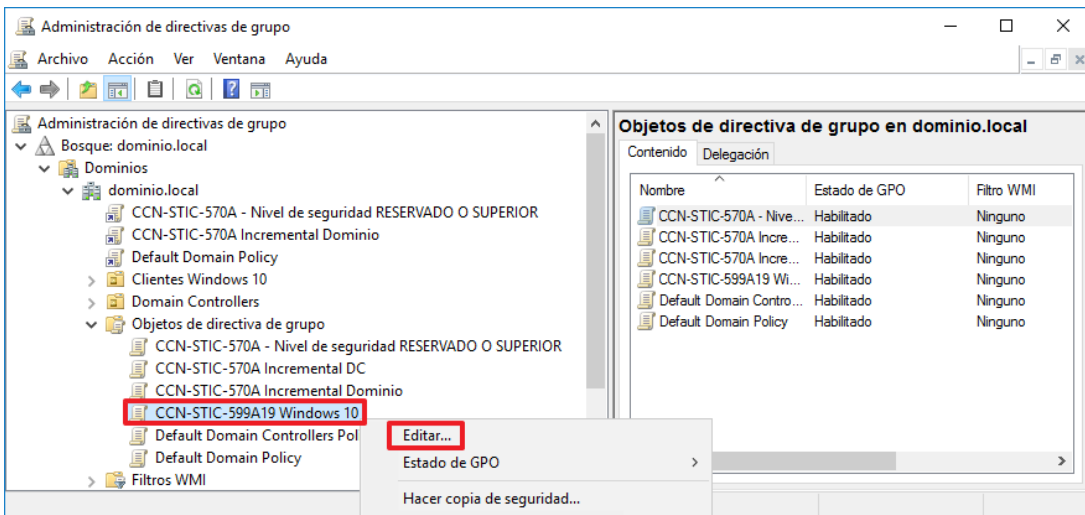
Paso	Descripción
12.	El sistema le solicitará elevación de privilegios. Introduzca las credenciales de un administrador del dominio. 
13.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Usuarios y equipos de Active Directory”. 

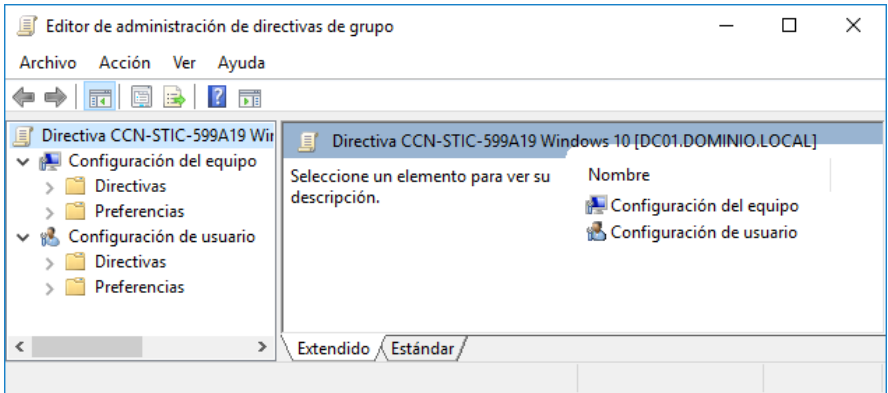
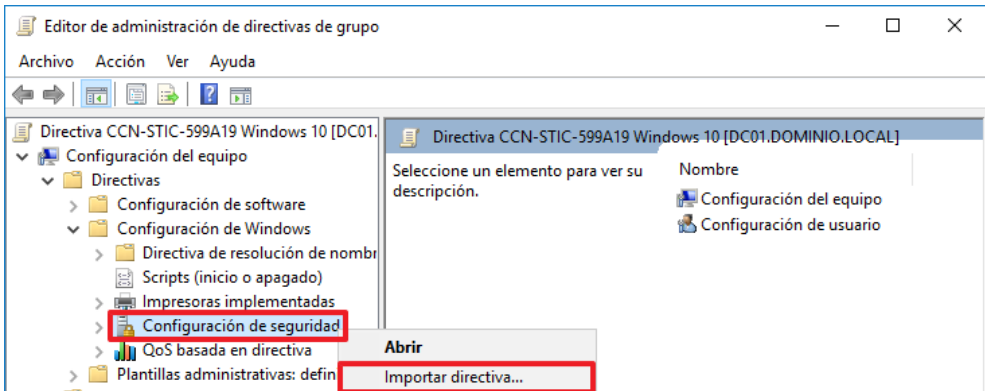
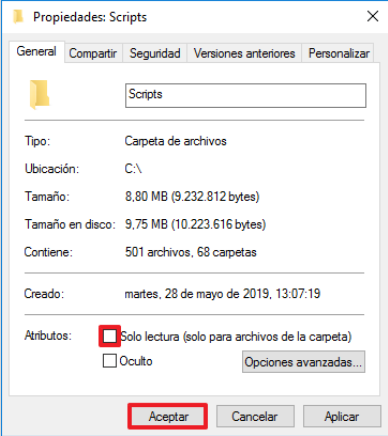
Paso	Descripción
14.	En la consola “Usuarios y equipos de Active Directory” sitúese sobre el objeto con el nombre del dominio y, pulsando con el botón derecho del ratón sobre él, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá, como se muestra en la siguiente figura.  Nota: En el ejemplo, el dominio se denomina “dominio.local”.
15.	Asigne el nombre "Clientes Windows 10" a la nueva unidad organizativa, y deje marcada la opción "Proteger contenedor contra eliminación accidental". A continuación, pulse “Aceptar”. 

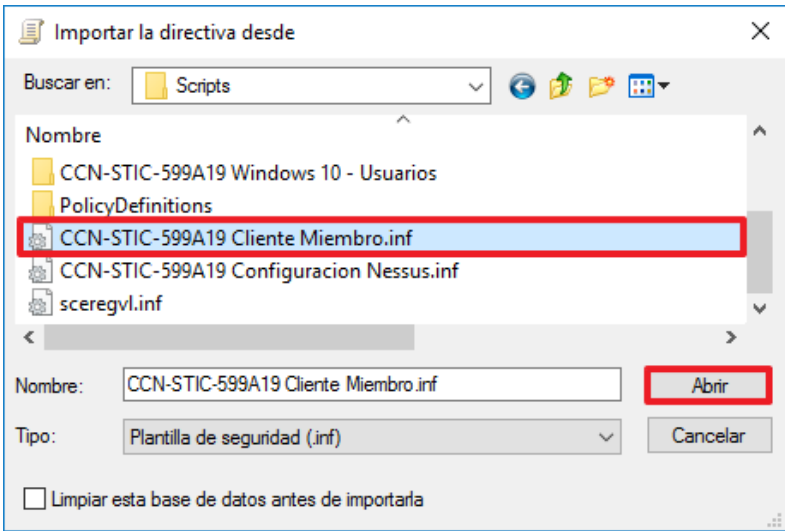
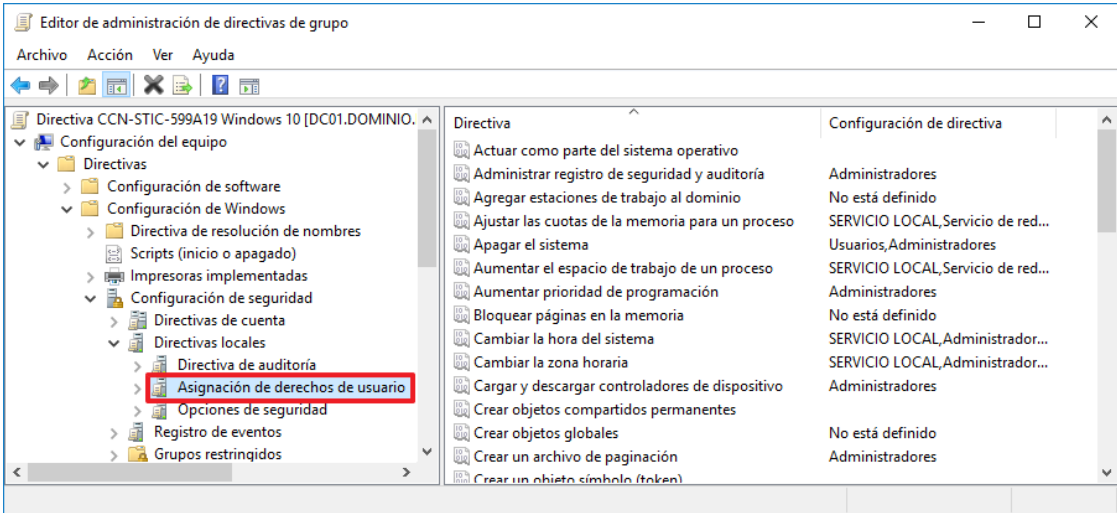
Paso	Descripción
16.	A continuación, cree las unidades organizativas "Equipos Windows 10" y "Usuarios Windows 10" colgando de la unidad organizativa que acaba de crear en el paso anterior, "Clientes Windows 10". Para ello, y utilizando de nuevo la herramienta "Usuarios y equipos de Active Directory", expanda y seleccione el siguiente contenedor: "<Nombre de su dominio> → Clientes Windows 10" Marcándolo con el botón derecho del ratón, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá. 
17.	Asigne el nombre "Equipos Windows 10", mantenga marcado "Proteger contenedor contra eliminación accidental" y pulse "Aceptar". 

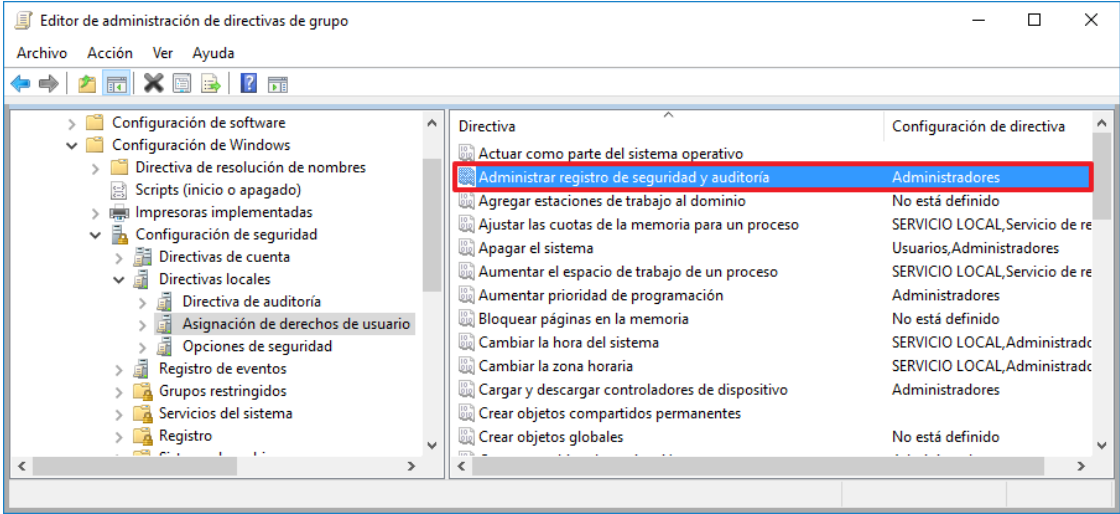
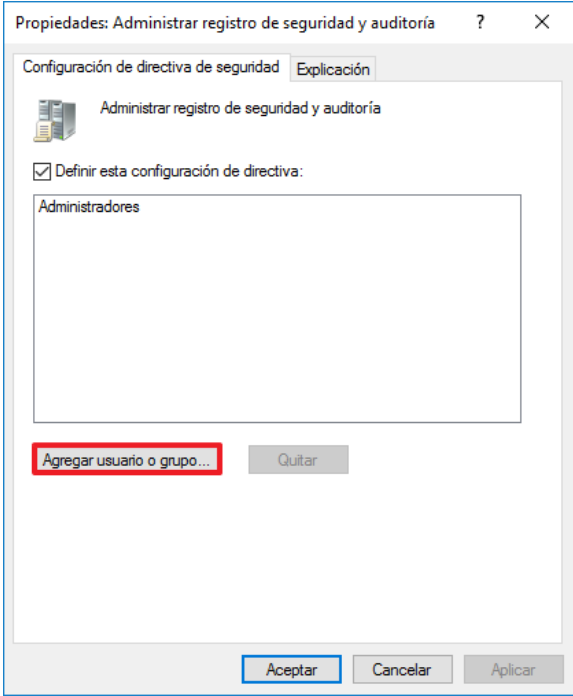
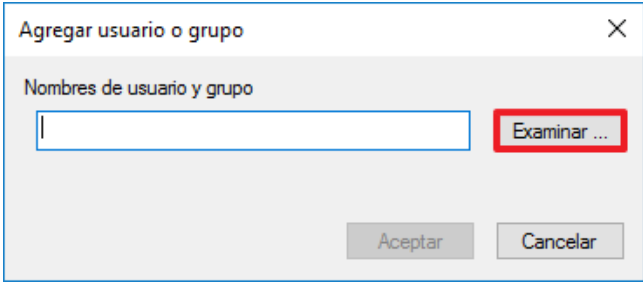
Paso	Descripción
18.	Del mismo modo, vuelva a seleccionar el contenedor “Clientes Windows 10” a través de la ruta “<Nombre de su dominio> → Clientes Windows 10”. Marcándolo con el botón derecho del ratón, seleccione la opción “Nuevo → Unidad organizativa” del menú contextual. 
19.	Asigne el nombre “Usuarios Windows 10” y pulse “Aceptar”. 

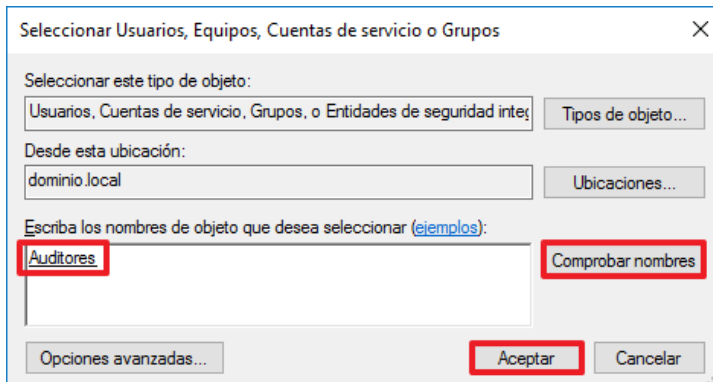
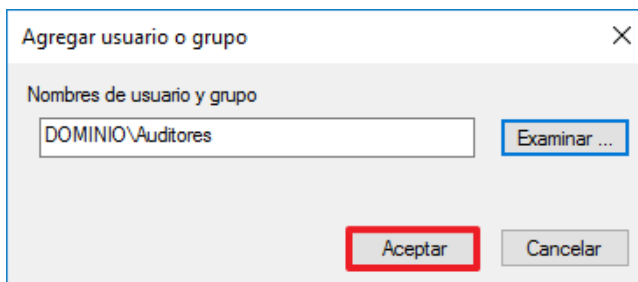
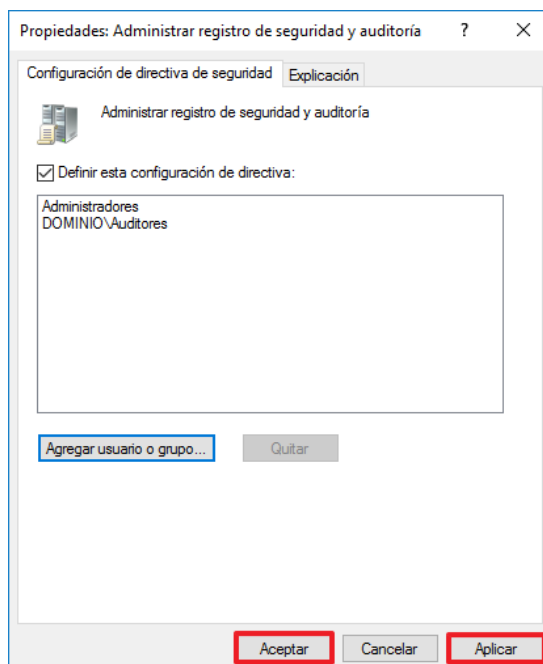
Paso	Descripción
20.	Al finalizar, las nuevas unidades organizativas, "Equipos Windows 10" y "Usuarios Windows 10", aparecerán colgando de "Clientes Windows 10", como se muestra en la siguiente figura.  Nota: Es importante, sobre todo en entornos en que haya clientes Windows 10 con la versión 1607 contemplada en la guía "CCN-STIC-599A18" conviviendo con los clientes Windows 10 con la versión 1809 contemplada en la presente guía, que se diferencien los equipos y usuarios de cada sistema.
21.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.
22.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Administración de directivas de grupo". 
23.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la ruta "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>". A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPO correspondientes. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>). 

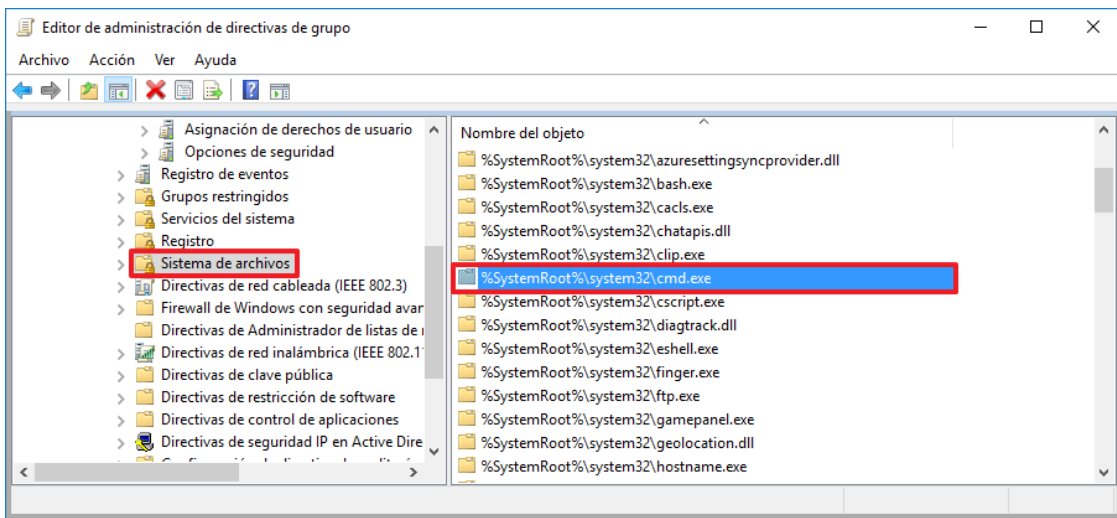
Paso	Descripción
24.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" y, marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá.  Nota: Las GPO que se van a crear y parametrizar en los siguientes pasos deberán vincularse a las unidades organizativas correspondientes a Windows 10 versión 1809 contempladas en la presente guía. Es importante no mezclar equipos, usuarios o GPO de Windows 10 1809 con equipos, usuarios o GPO de Windows 10 1607 (a los cuales les debe aplicar la guía CCN-STIC-599A18, y no la presente guía).
25.	Asigne el siguiente nombre "CCN-STIC-599A19 Windows 10" a la nueva GPO y pulse "Aceptar". 
26.	Seleccione la GPO recién creada, "CCN-STIC-599A19 Windows 10" con el botón derecho y elija la opción "Editar" en el menú contextual que aparecerá. 

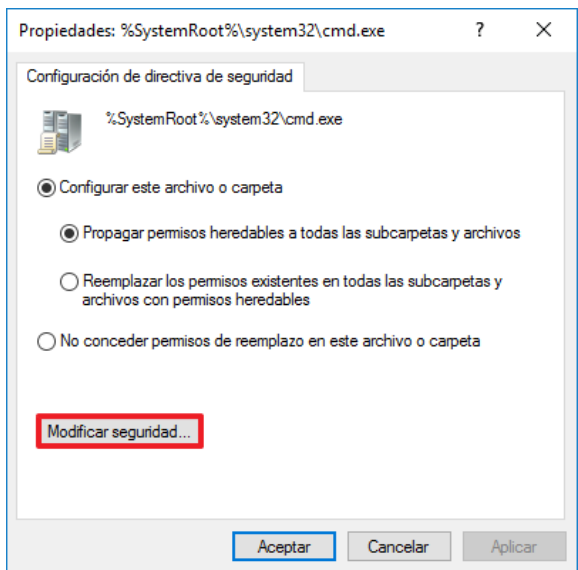
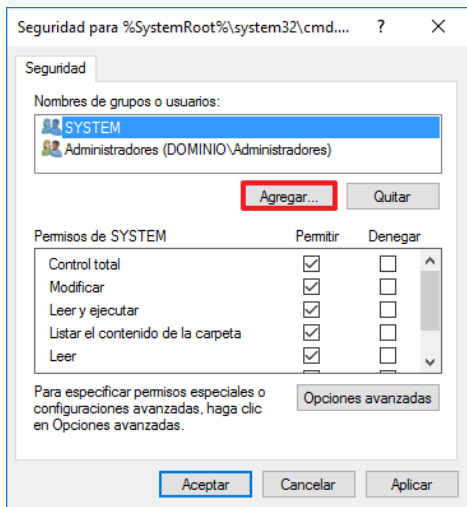
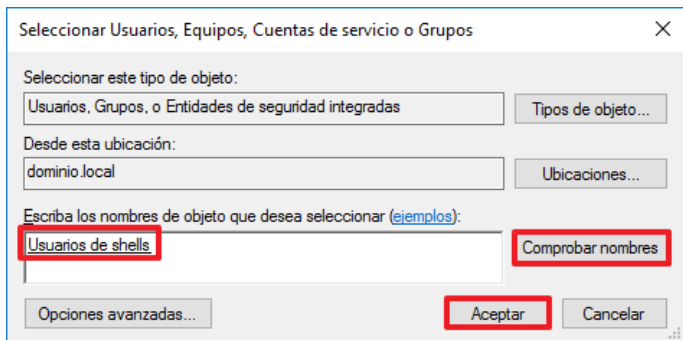
Paso	Descripción
27.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido de la GPO. 
28.	En dicha ventana del editor de administración de directivas de grupo, seleccione el nodo "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad". Marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá.  Nota: Asegúrese de que los archivos alojados en "C:\Scripts" no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

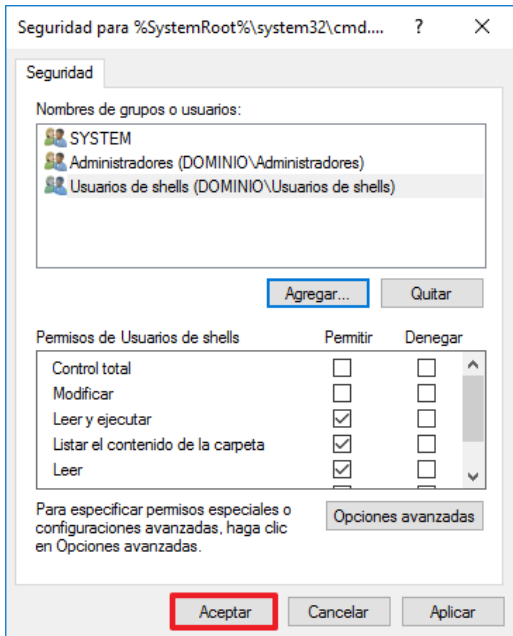
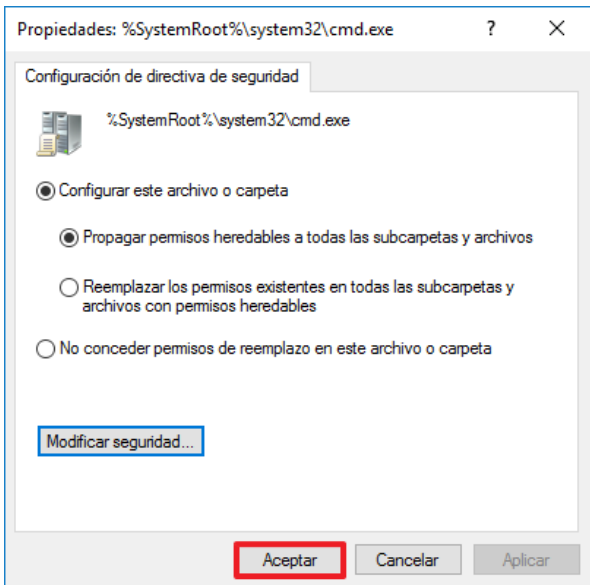
Paso	Descripción
29.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Scripts\CCN-STIC-599A19 Cliente Miembro.inf" y pulse el botón "Abrir". Con eso habrá quedado importada la plantilla en la GPO. No cierre aún el "Editor de directivas de grupo" y continúe con el siguiente paso. 
30.	Utilizando de nuevo el "Editor de administración de directivas de grupo", abierto anteriormente, seleccione "Asignación de derechos de usuarios" a través de la siguiente ruta: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario" 

Paso	Descripción
31.	Haga doble clic sobre la directiva “Administrar registro de seguridad y auditoría”. 
32.	Pulse sobre “Agregar usuario o grupo...” en la ventana emergente. 
33.	Pulse sobre “Examinar”. 

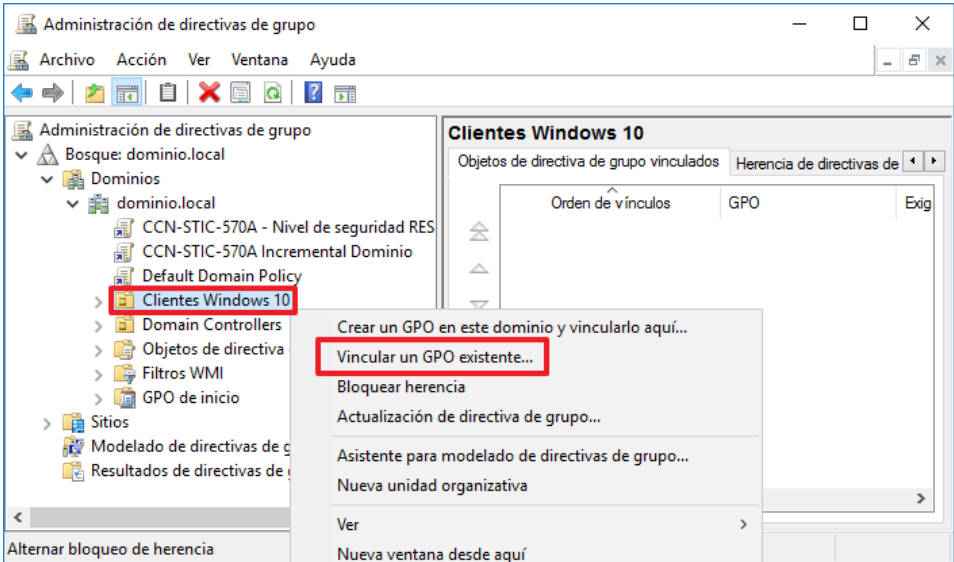
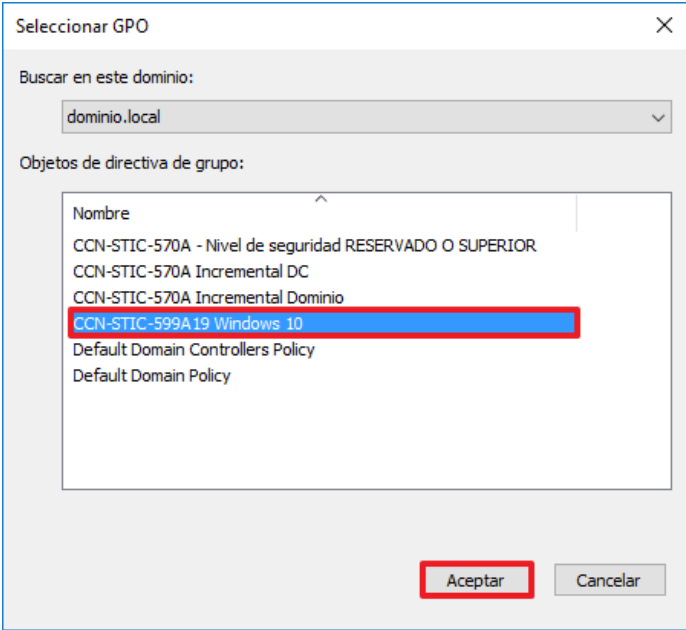
Paso	Descripción
34.	Introduzca el grupo de seguridad “Auditores”, pulse en “Comprobar nombre” y “Aceptar”.  Nota: El grupo "Auditores" ya debe existir en el dominio si se aplicó correctamente la guía CCN-STIC-570A a los controladores de dominio. Si no existe, revise la aplicación de dicha guía. Recuerde también que la cuenta Administrador (administrador integrado del dominio) puede haber sido renombrada por la aplicación de dicha guía.
35.	Pulse “Aceptar”. 
36.	Por último, pulse “Aplicar” y “Aceptar” para confirmar los cambios. 

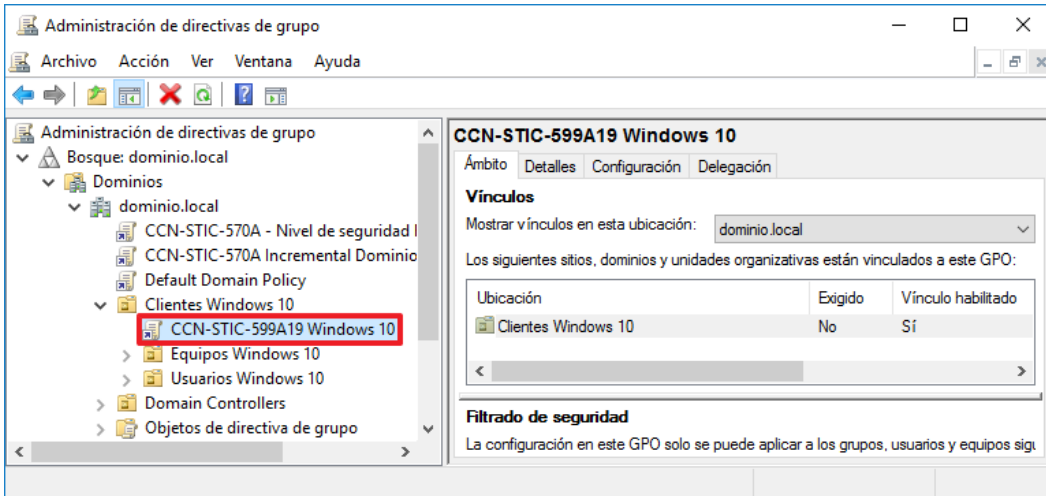
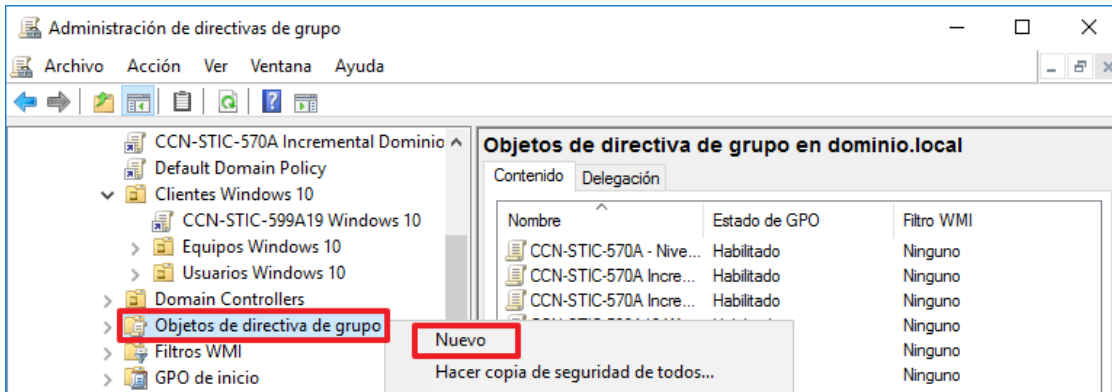
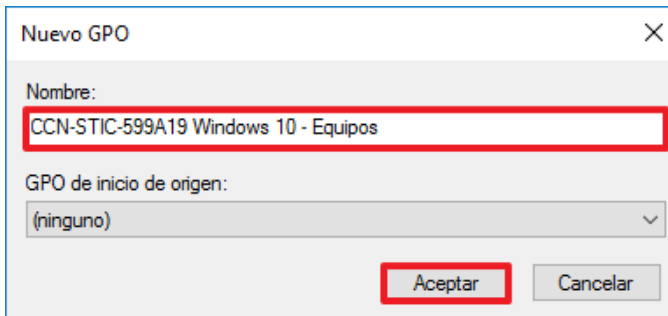
Paso	Descripción		
37.	Repita el proceso con los valores indicados en la siguiente tabla. Concretamente, deberá añadir los usuarios y grupos de seguridad marcados en gris.		
	Directiva	Valor	Descripción
	Administrar registro de seguridad y auditoría	Auditores, Administradores	Este privilegio permite 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
38.	De manera análoga a lo realizado en el paso anterior, despliegue el nodo “Sistema de archivos” mediante la ruta “Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos”.		
39.	Haga doble clic sobre el objeto “%SystemRoot%\system32\cmd.exe”.		
			

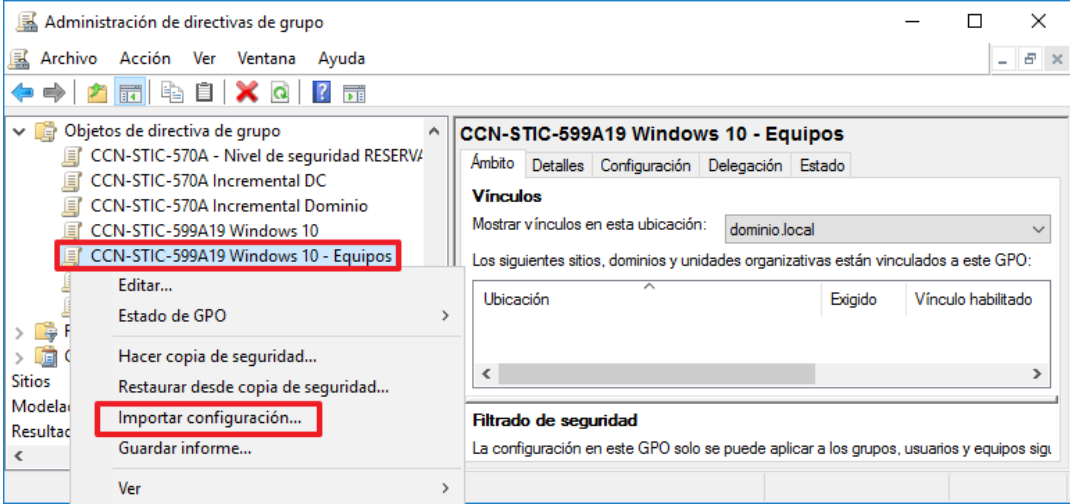
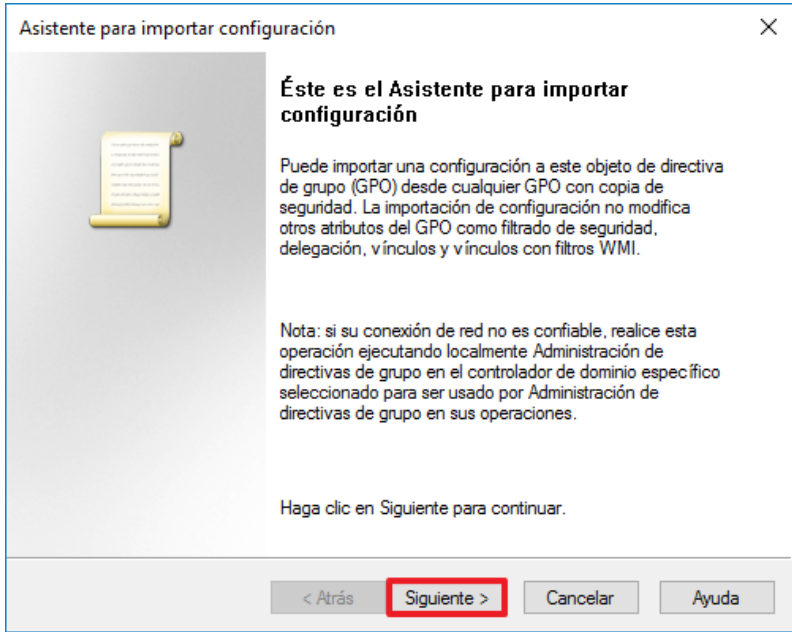
Paso	Descripción
40.	Pulse en “Modificar seguridad...”. 
41.	Pulse “Agregar...” para añadir el grupo de seguridad que tendrá permisos para ejecutar la consola de comandos. 
42.	Introduzca el grupo “Usuarios de shells”, pulse “Comprobar nombre” y “Aceptar”.  Nota: El grupo "Usuarios de shells" ya debe existir en el dominio si se aplicó correctamente la guía CCN-STIC-570A al controlador de dominio. Si no existe, revise la aplicación de dicha guía.

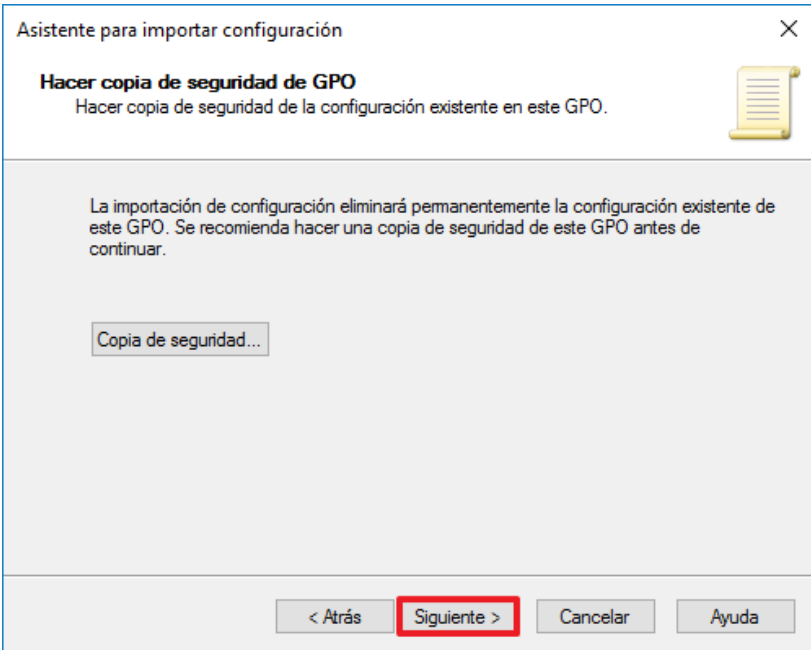
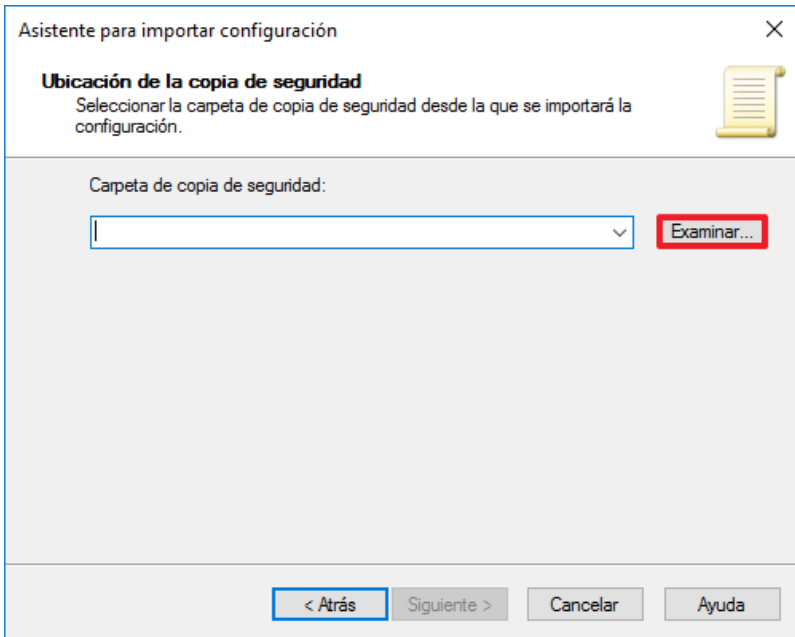
Paso	Descripción
43.	Pulse “Aceptar” sin modificar los permisos asignados por defecto. 
44.	Pulse nuevamente en “Aceptar” para confirmar cambios. 

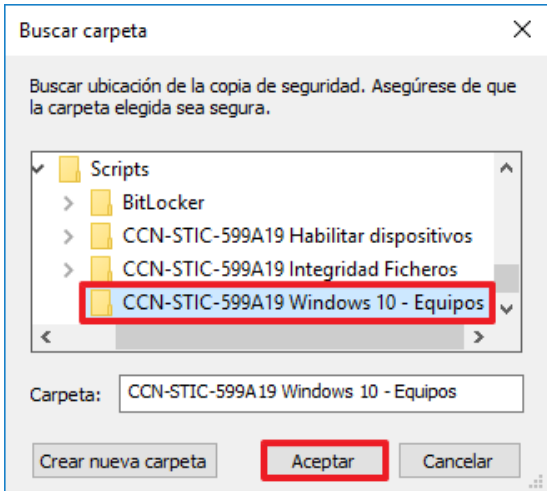
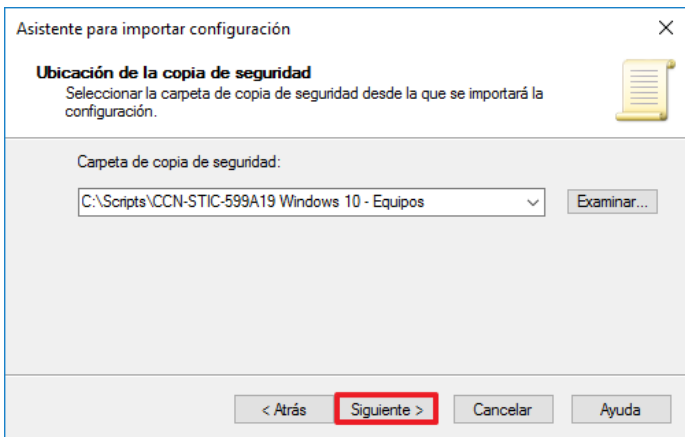
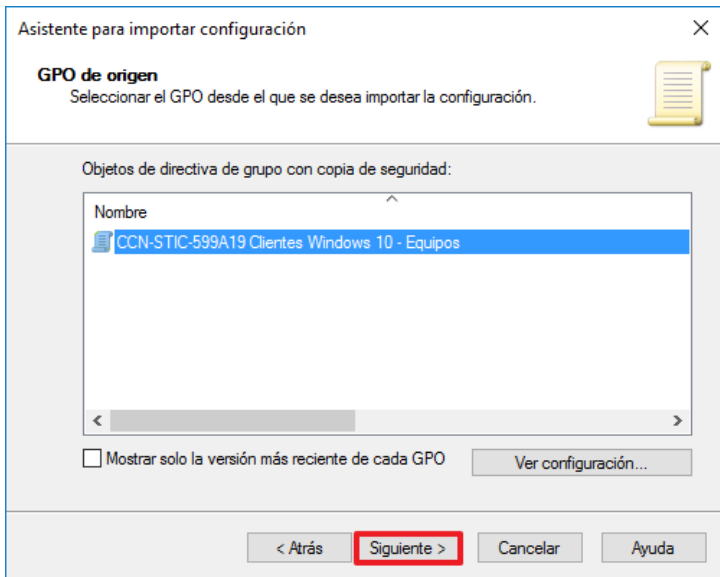
Paso	Descripción		
45.	Repita el proceso con los valores indicados en la siguiente tabla. Concretamente, deberá añadir los usuarios y grupos de seguridad marcados en gris.		
	Archivo o carpeta	Usuarios/Grupos	Permisos
	%SystemRoot%\system32\ cmd.exe	Administradores	Control Total
		SYSTEM	Control Total
		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
	%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
46.	A continuación, cierre el “Editor de administración de directivas de grupo”.		

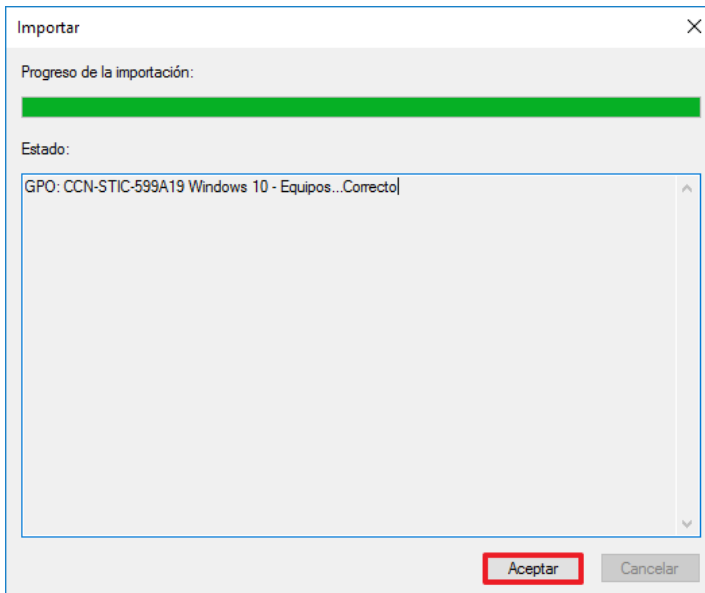
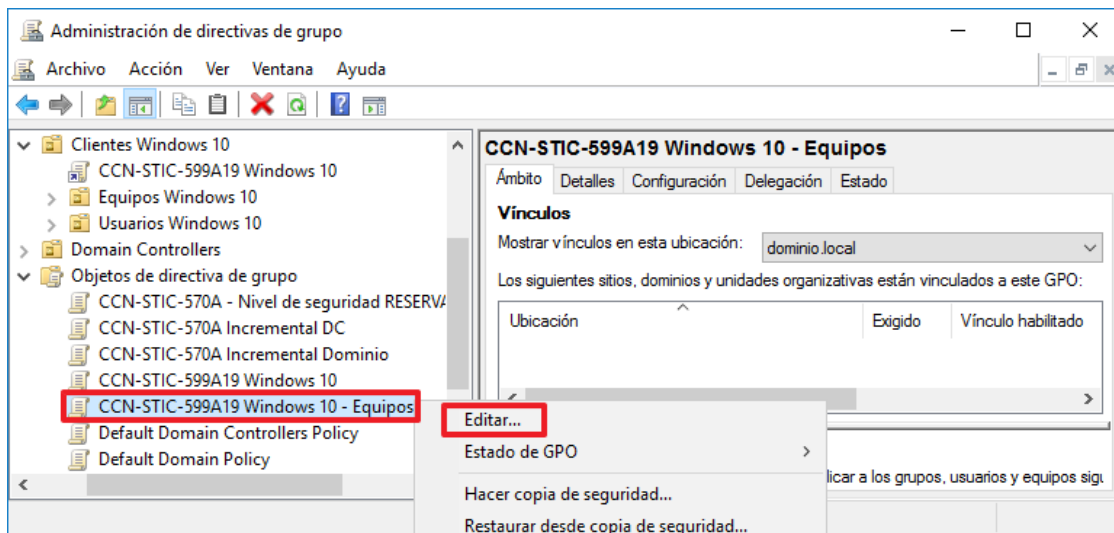
Paso	Descripción
47.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Clientes Windows 10” a través de la ruta “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10”. Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
48.	Seleccione “CCN-STIC-599A19 Windows 10” de la lista y pulse “Aceptar”. 

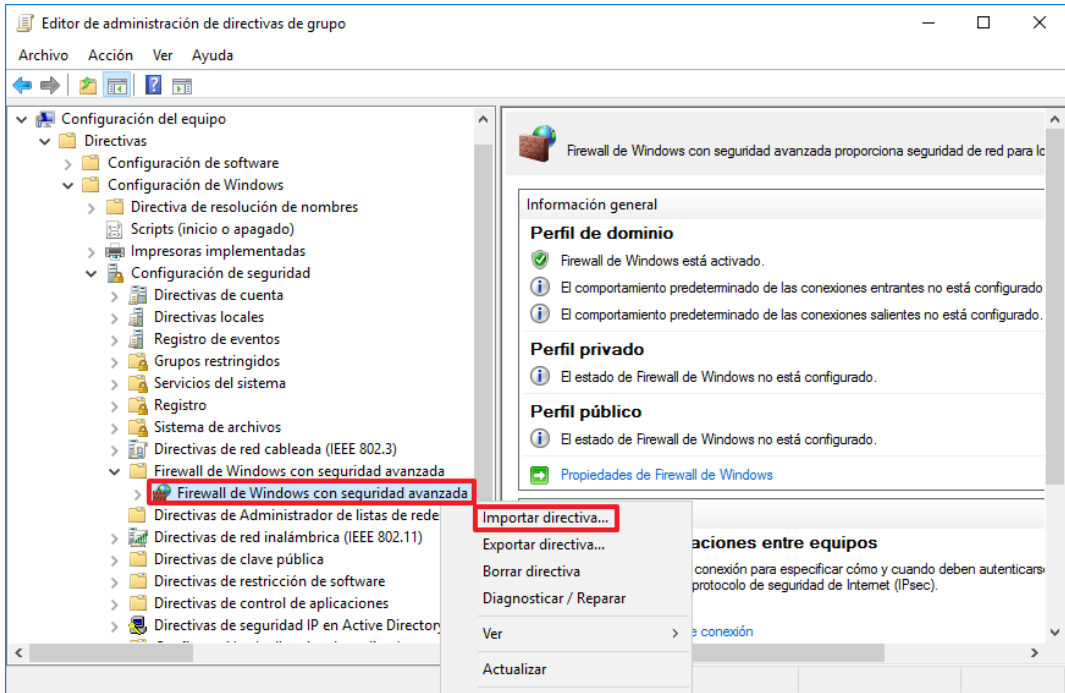
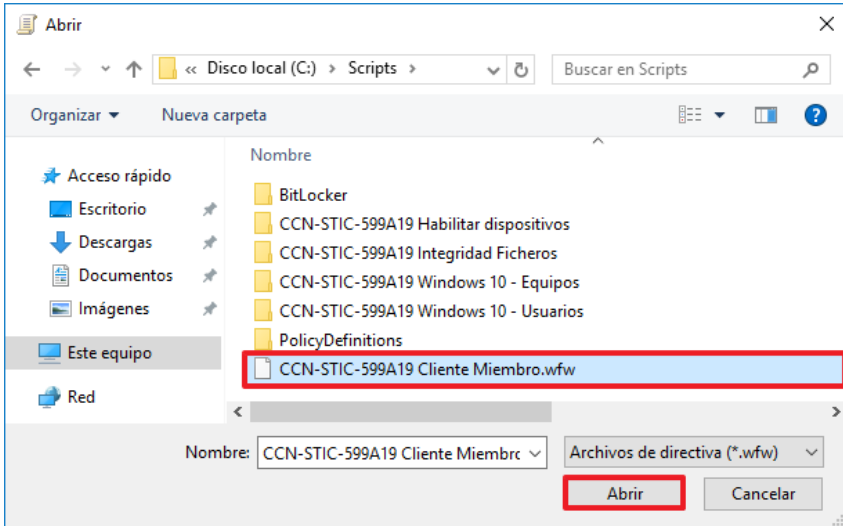
Paso	Descripción
49.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa "Clientes Windows 10". 
50.	De nuevo, en la consola "Administración de directivas de grupo", expanda y seleccione el contenedor "Objetos de directiva de grupo" mediante la ruta "Características → Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo". Pulsando el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
51.	Asigne el nombre "CCN-STIC-599A19 Windows 10 - Equipos" a la nueva GPO y pulse "Aceptar". 

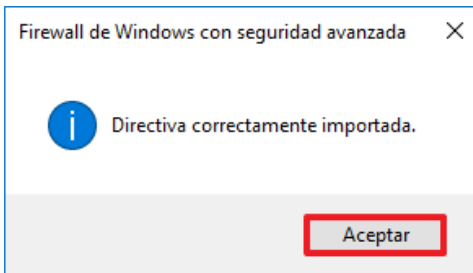
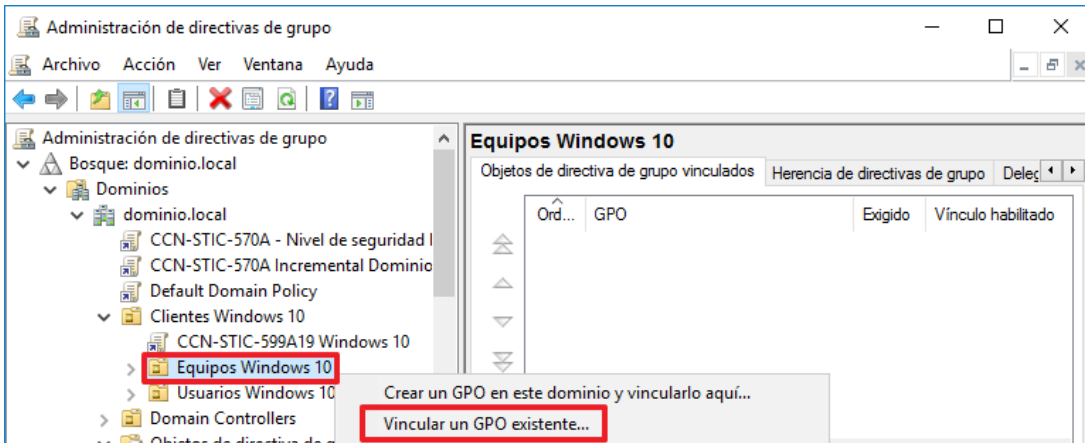
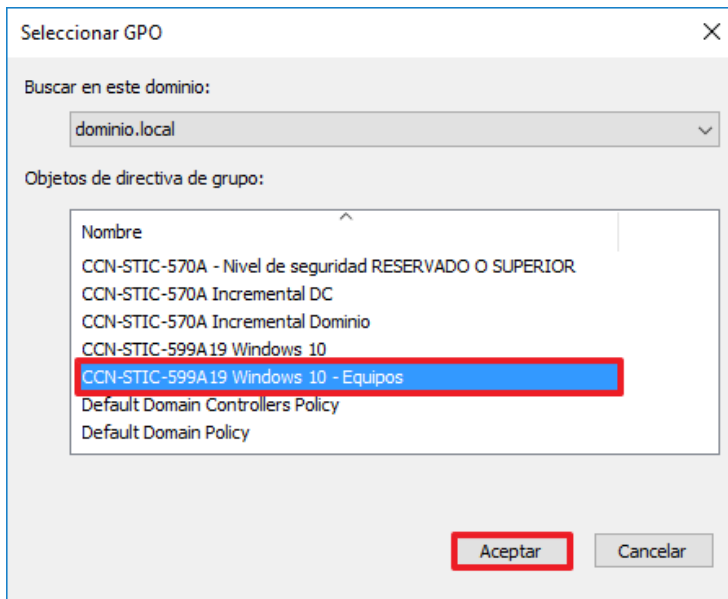
Paso	Descripción
52.	Seleccione la GPO recién creada, “CCN-STIC-599A19 Windows 10 - Equipos” con el botón derecho y elija la opción "Importar configuración..." en el menú contextual que aparecerá. 
53.	En el “Asistente para importar configuración” pulse “Siguiente >”. 

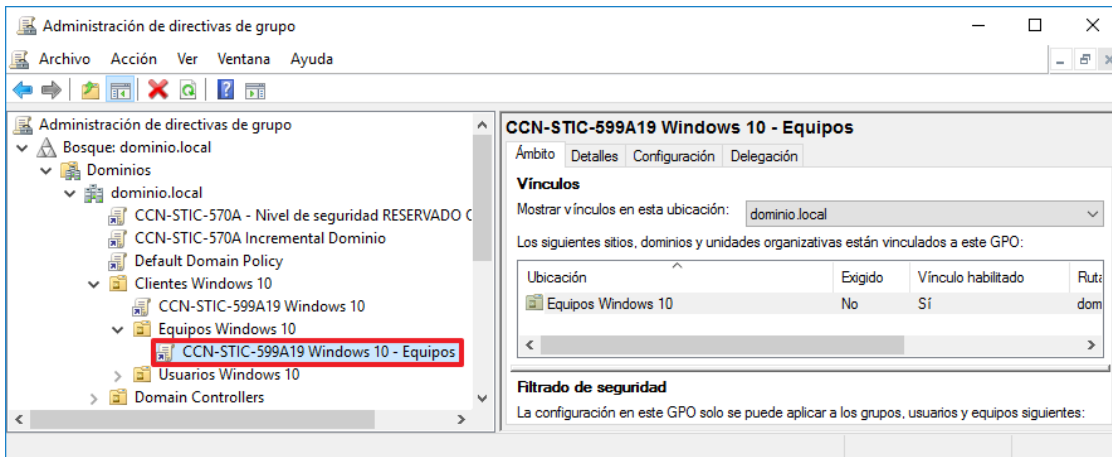
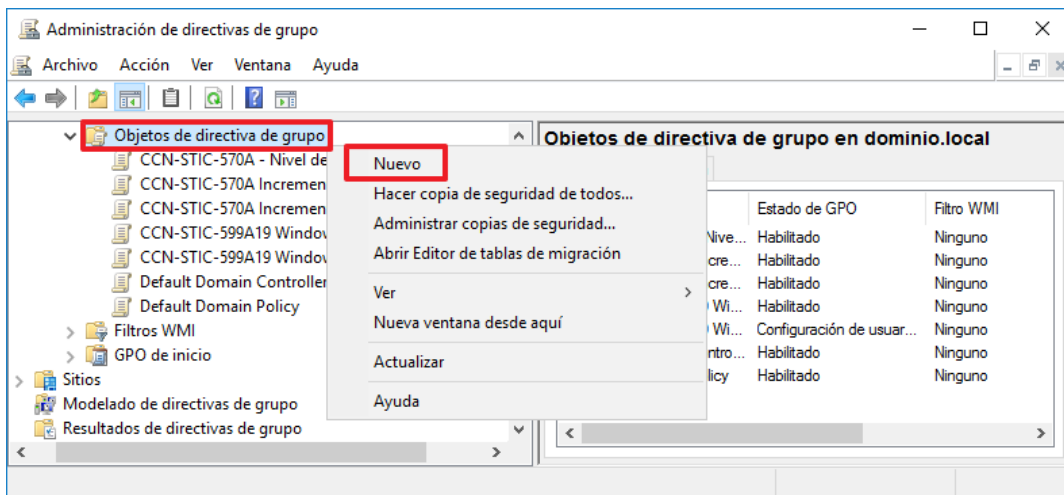
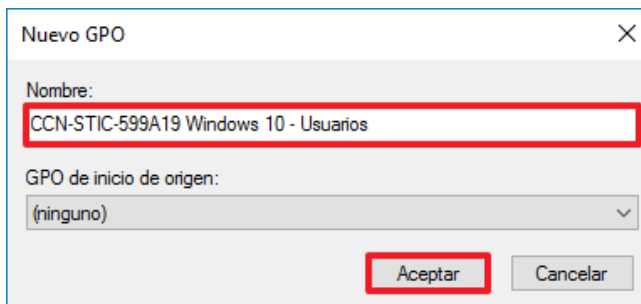
Paso	Descripción
54.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana "Hacer copia de seguridad de GPO". 
55.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 

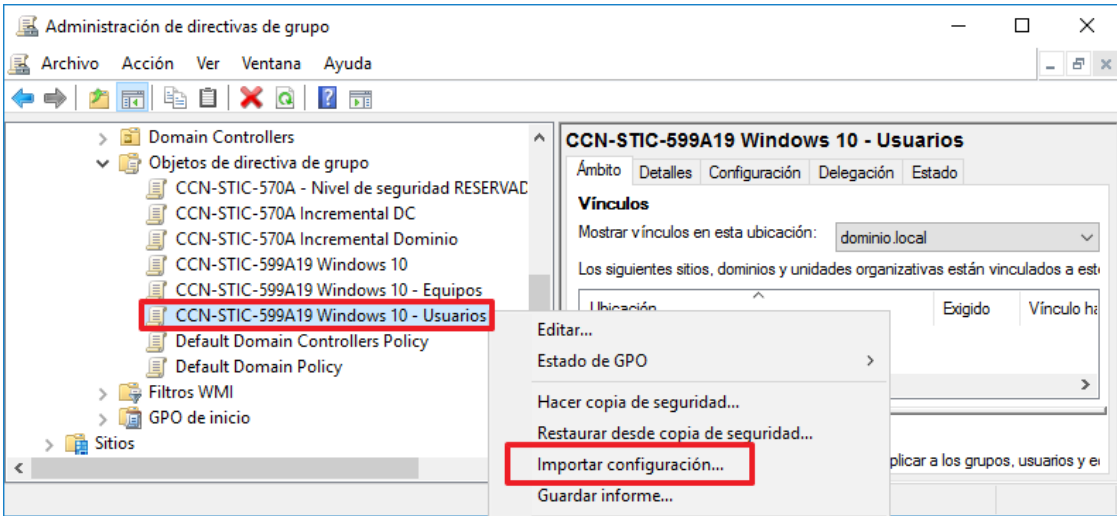
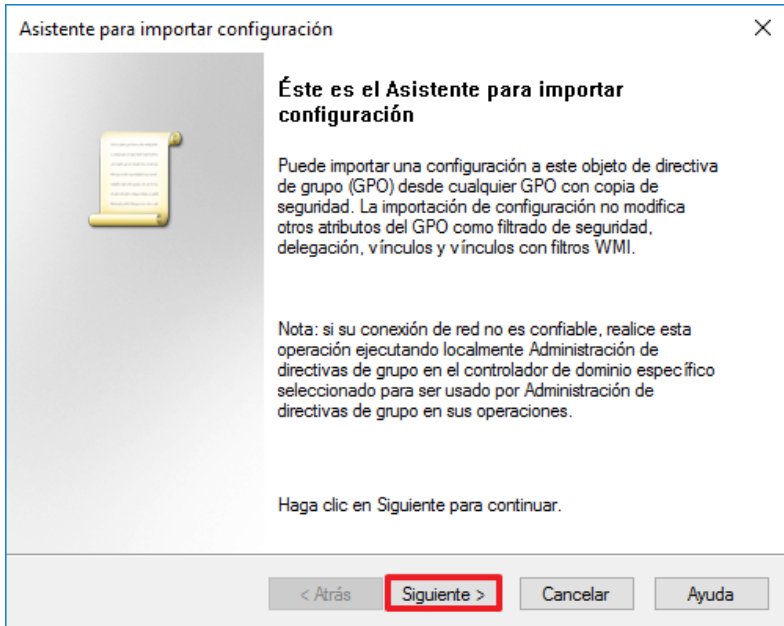
Paso	Descripción
56.	Localice la carpeta “CCN-STIC-599A19 Windows 10- Equipos” dentro de “C:\Scripts” y pulse “Aceptar”. 
57.	Pulse “Siguiente >” para continuar. 
58.	En “GPO de origen” pulse “Siguiente >”. 

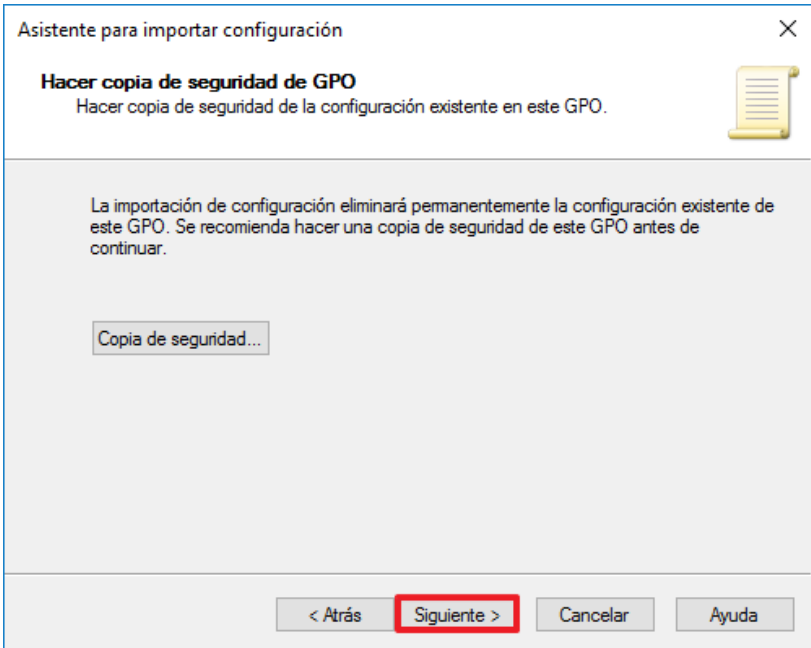
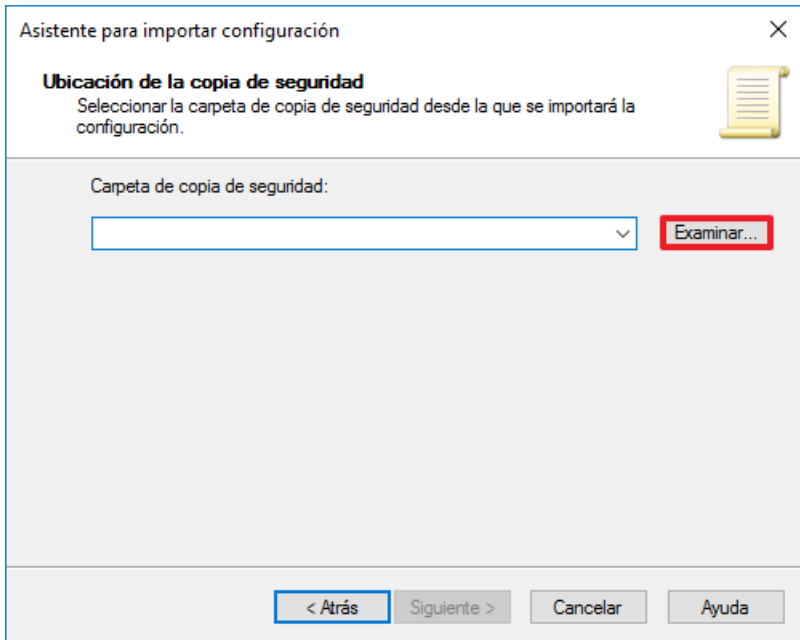
Paso	Descripción
59.	En “Examinar copia de seguridad” pulse “Siguiente >”.
60.	Pulse “Finalizar” para realizar la importación.
61.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 
62.	Seleccione de nuevo la GPO con el botón derecho y pulse sobre la opción del menú contextual “Editar”. 
63.	Despliegue el nodo “Firewall de Windows son seguridad avanzada” a través de la ruta “Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada”.

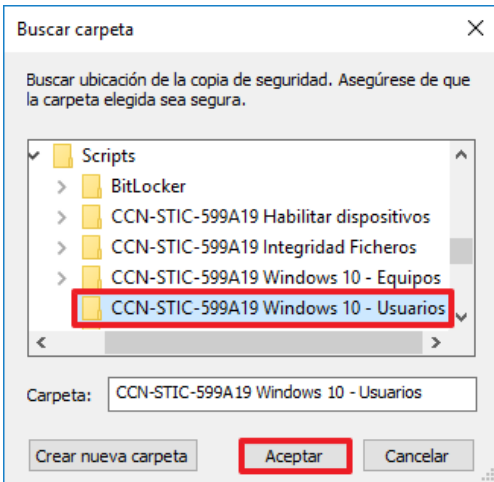
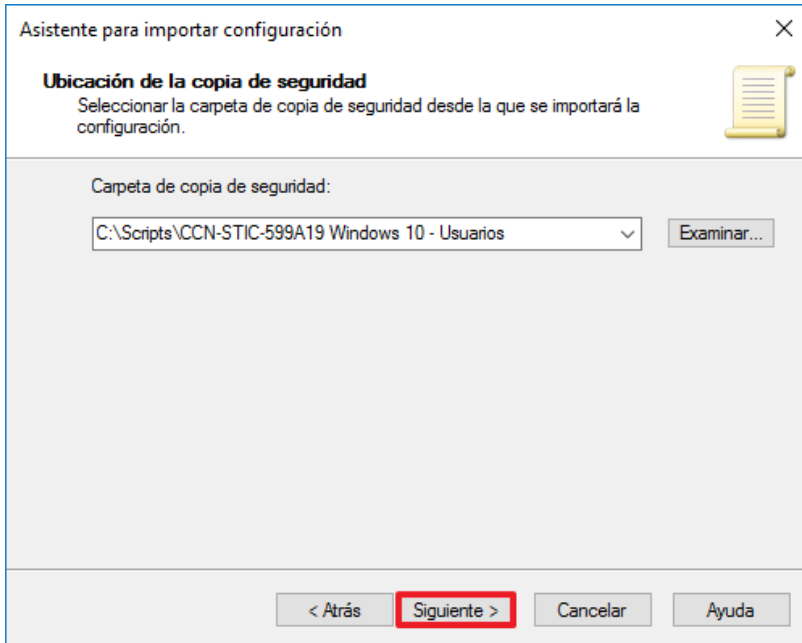
Paso	Descripción
64.	Pulse con el botón derecho sobre “Firewall de Windows con seguridad avanzada” y seleccione la opción del menú contextual “Importar directiva...”. 
65.	Pulse “S” ante el mensaje de advertencia emergente y seleccione el fichero “CCN-STIC-599A19 Cliente Miembro.wfw” ubicado en el directorio “C:\Scripts”. Pulse sobre “Abrir” para cargar el fichero. 

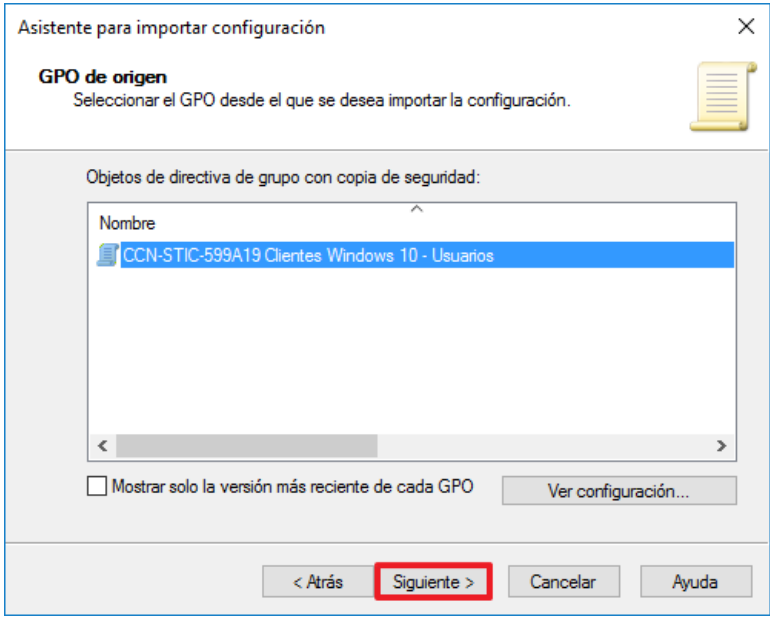
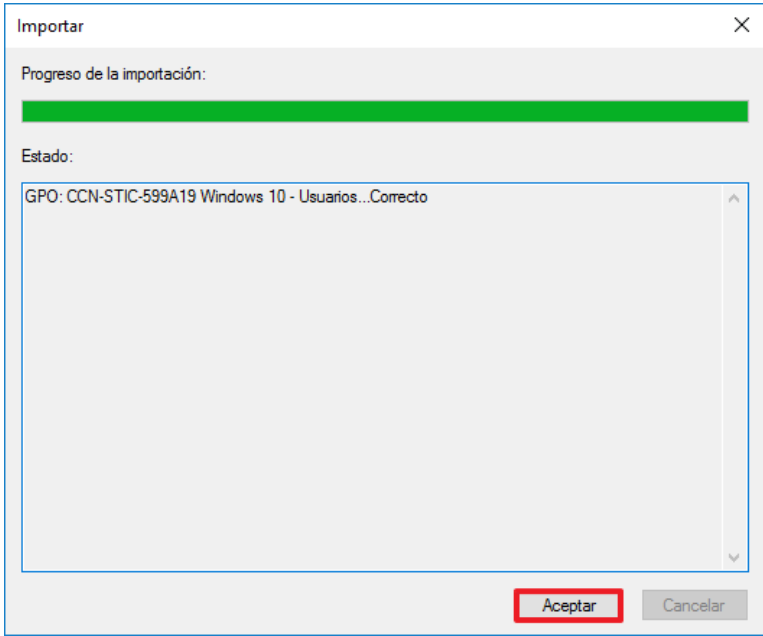
Paso	Descripción
66.	Pulse sobre “Aceptar” en el mensaje emergente y cierre el “Editor de administración de directivas de grupo”. 
67.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la ruta “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10”. Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
68.	Seleccione “CCN-STIC-599A19 Windows 10 - Equipos” de la lista y pulse “Aceptar”. 

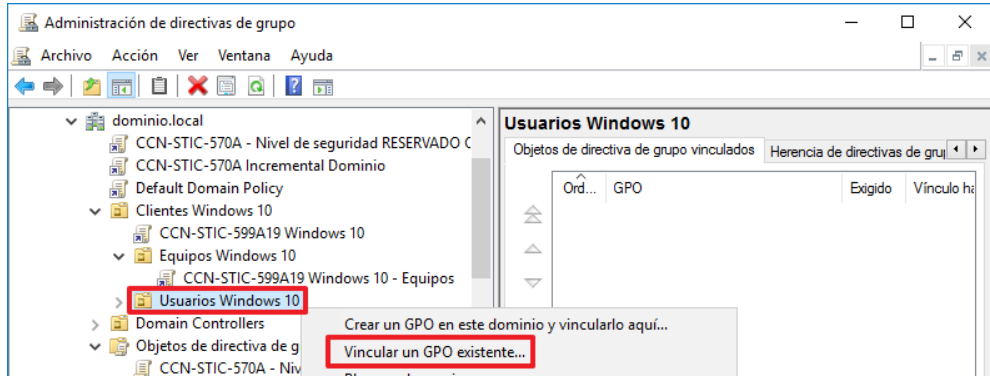
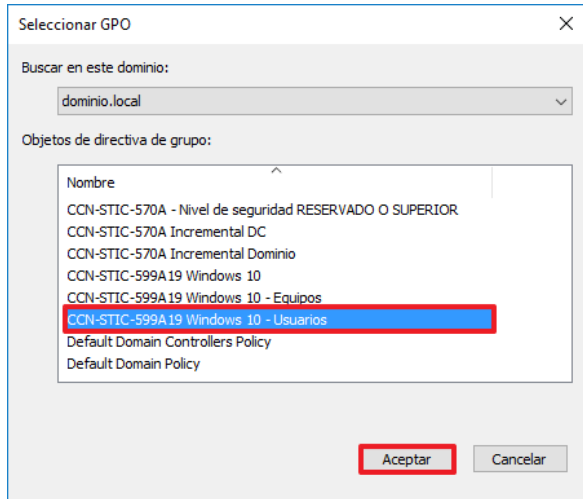
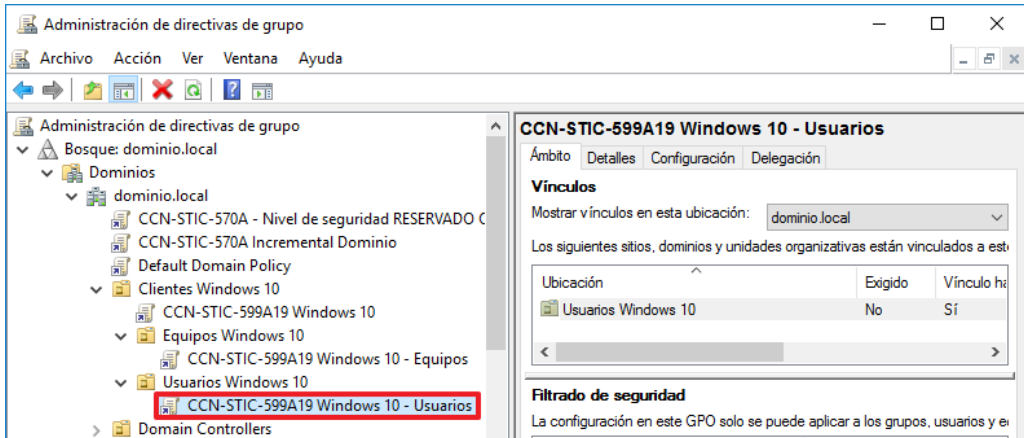
Paso	Descripción
69.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Equipos Windows 10”. 
70.	De nuevo, en la consola “Administración de directivas de grupo”, expanda y seleccione el contenedor "Objetos de directiva de grupo" mediante la siguiente ruta. "Administración de directivas de grupo → Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo" Pulsando el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
71.	Asigne el nombre “CCN-STIC-599A19 Windows 10 – Usuarios” a la nueva GPO y pulse “Aceptar”. 

Paso	Descripción
72.	Seleccione la GPO recién creada, “CCN-STIC-599A19 Windows 10 - Usuarios” con el botón derecho y elija la opción “Importar configuración...” en el menú contextual. 
73.	En el “Asistente para importar configuración” pulse “Siguiente >”. 

Paso	Descripción
74.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana "Hacer copia de seguridad de GPO". 
75.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 

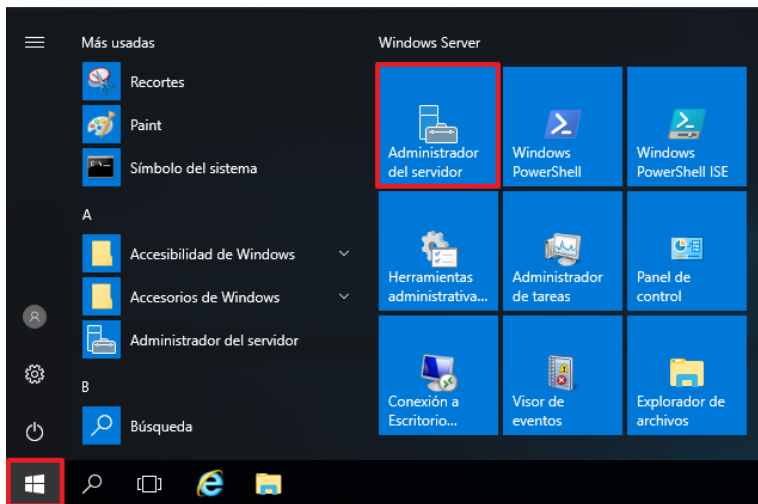
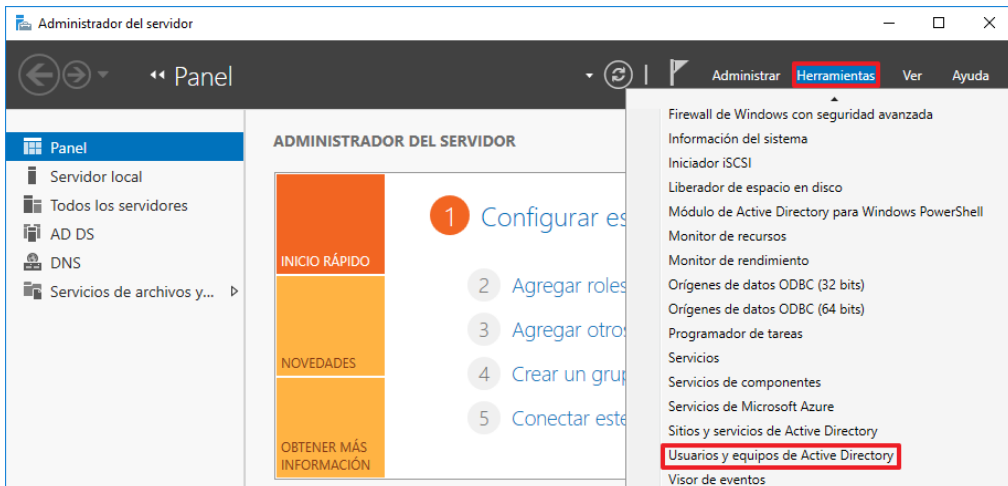
Paso	Descripción
76.	Localice la carpeta “CCN-STIC-599A19 Windows 10- Usuarios” y pulse “Aceptar”. 
77.	Pulse “Siguiente >” para continuar. 

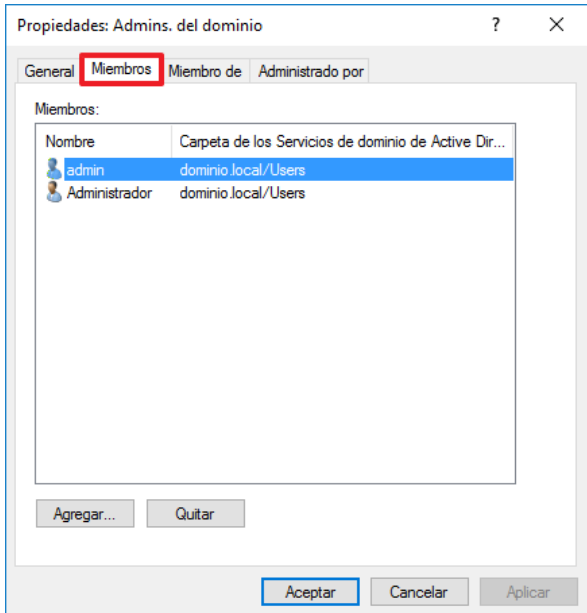
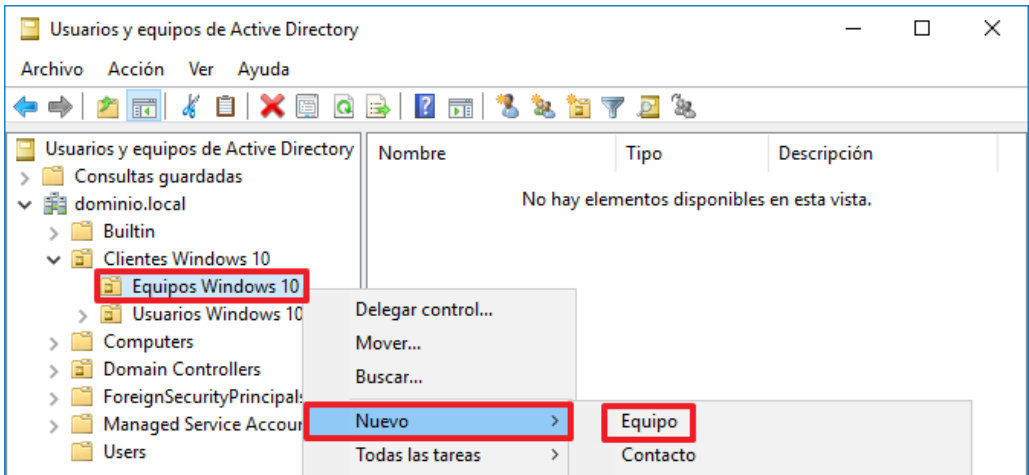
Paso	Descripción
78.	En “GPO de origen” pulse “Siguiente >”. 
79.	En “Examinar copia de seguridad” pulse “Siguiente >”.
80.	Pulse “Finalizar” para realizar la importación.
81.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 

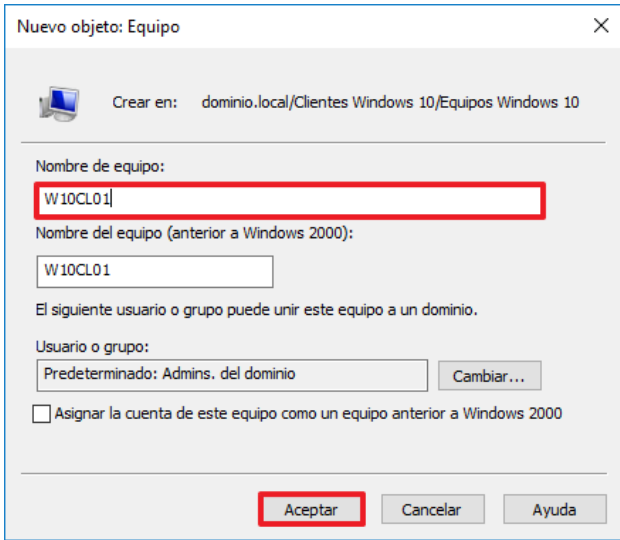
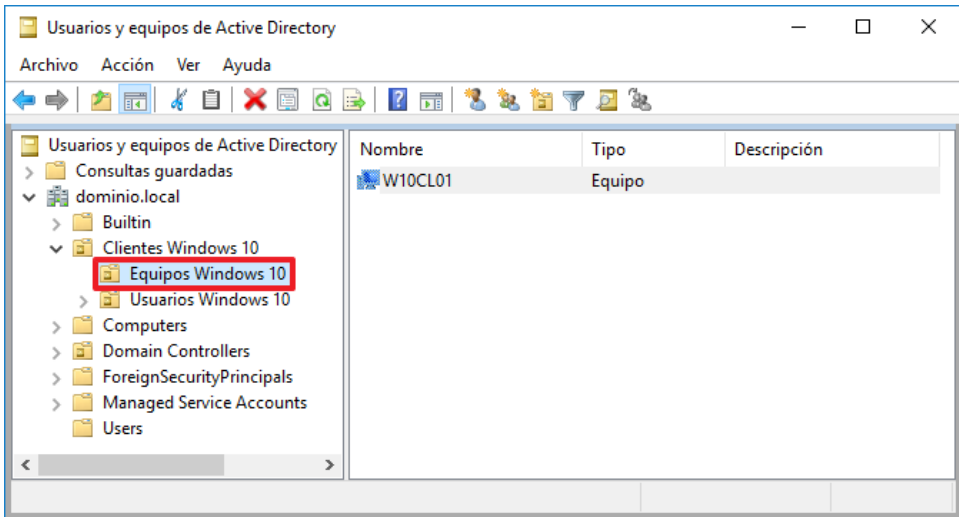
Paso	Descripción						
82.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Usuarios Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”.						
							
83.	Seleccione “CCN-STIC-599A19 Windows 10 - Usuarios” de la lista y pulse “Aceptar”.						
							
84.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Usuarios Windows 10”.						
	 <table><thead><tr><th>Ubicación</th><th>Exigido</th><th>Vínculo ha</th></tr></thead><tbody><tr><td>Usuarios Windows 10</td><td>No</td><td>Sí</td></tr></tbody></table>	Ubicación	Exigido	Vínculo ha	Usuarios Windows 10	No	Sí
Ubicación	Exigido	Vínculo ha					
Usuarios Windows 10	No	Sí					

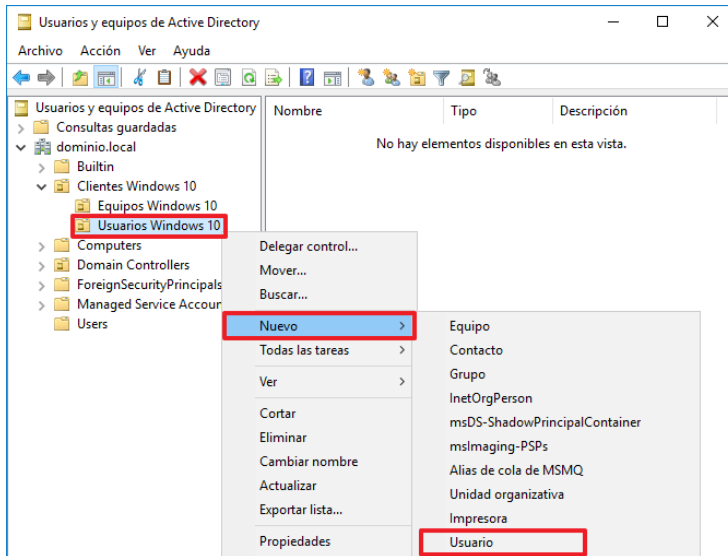
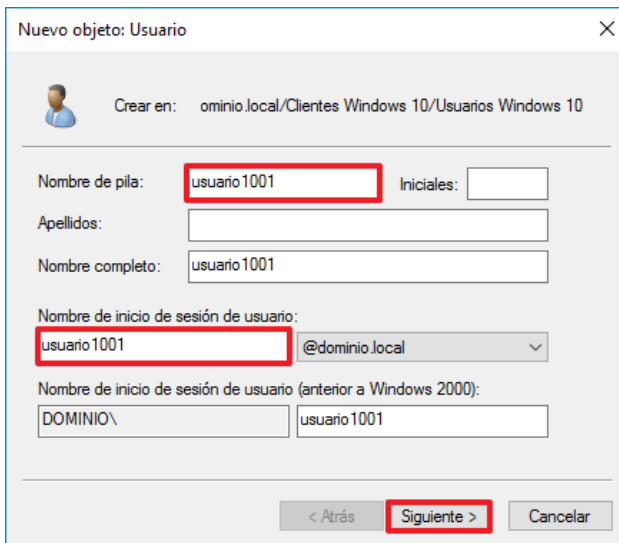
En este punto, las unidades organizativas y las GPO necesarias están ya configuradas correctamente en Active Directory y su configuración se aplicará automáticamente tanto al equipo cliente Microsoft Windows 10 miembro del dominio que está asegurando como a los futuros equipos cliente Microsoft Windows 10 que se añadan.

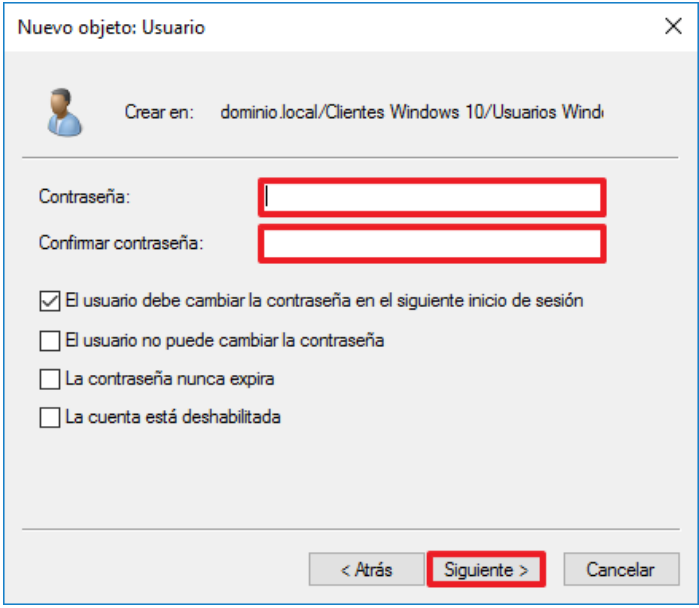
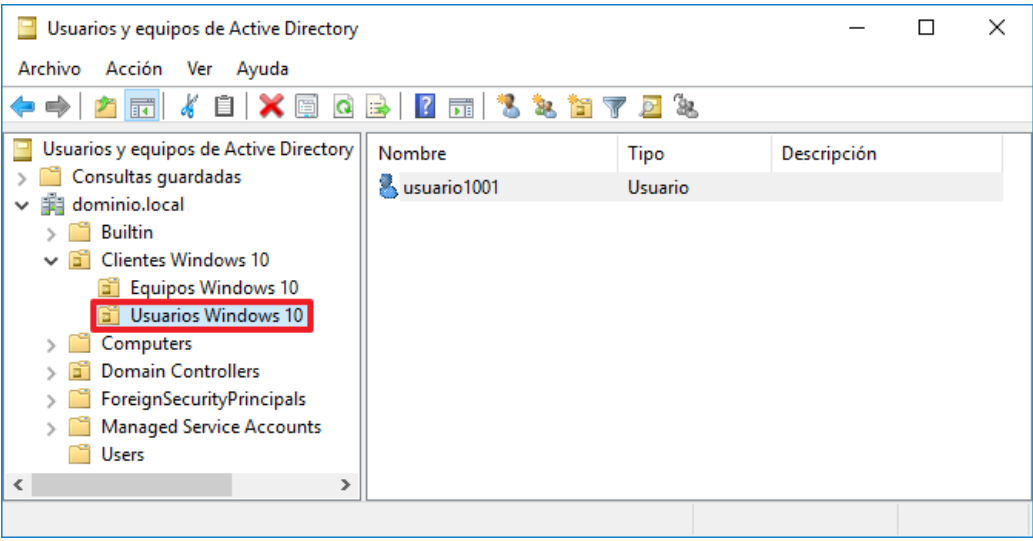
Los siguientes pasos deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo que está asegurando, además, deberá realizarlos cada vez que necesite asegurar un nuevo equipo cliente Windows 10, ya que se trata de preparar en Active Directory una cuenta de equipo para el equipo que está asegurando y que va a unir al dominio.

Paso	Descripción
85.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo que va a asegurar. Deberá iniciar sesión con una cuenta que pertenezca al grupo “Admins. del dominio”.
86.	Asegúrese, antes de continuar, de que los grupos "Administradores" y "Usuarios de shells" contienen los usuarios adecuados para su entorno. Para ello, acceda a la herramienta “Administrador del servidor” mediante el icono correspondiente en el menú de inicio. 
87.	En el menú superior haga clic sobre “Herramientas” y seleccione “Usuarios y equipos de Active Directory”. 

Paso	Descripción
88.	Diríjase al contenedor “Users” mediante la ruta “<Nombre de su dominio> → Users”. Haciendo doble clic sobre estos grupos podrá comprobar sus propiedades. En la pestaña “Miembros” podrá ver qué grupos o usuarios pertenecen a dicho grupo. 
89.	De nuevo en la consola “Usuarios y equipos de Active Directory”, cree una cuenta de equipo con el nombre del equipo que va a incluir en el dominio bajo la unidad organizativa "Equipos Windows 10". Para ello, expanda y seleccione el contenedor “Equipos Windows 10” mediante la siguiente ruta. “<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10” Haga clic con el botón derecho del ratón sobre la unidad organizativa y seleccione la opción “Nuevo → Equipo” del menú contextual que aparecerá. 

Paso	Descripción
90.	En el cuadro de diálogo que aparecerá, titulado "Nuevo objeto: Equipo", introduzca en el campo "Nombre de equipo:" el nombre del equipo que va a unir al dominio y pulse "Aceptar".  Nota: El campo "Nombre del equipo (anterior a Windows 2000):" se rellenará de forma automática, aun así, no marque la opción "Asignar la cuenta de este equipo como un equipo anterior a Windows 2000". En el ejemplo, se utiliza el equipo con nombre "W10CL01".
91.	La nueva cuenta de equipo aparecerá dentro del contenedor "Equipos Windows 10".  Nota: Al estar alojada la cuenta de equipo en este contenedor de Active Directory, el equipo Windows 10 miembro del dominio recibirá la configuración de equipo recomendada en esta guía para equipos clientes Windows 10.

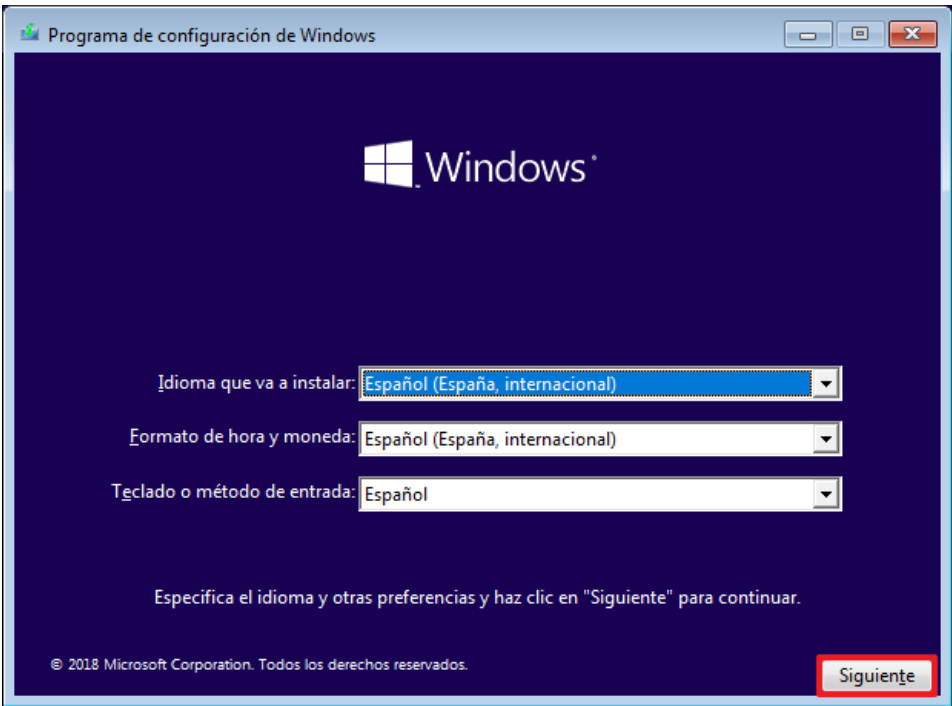
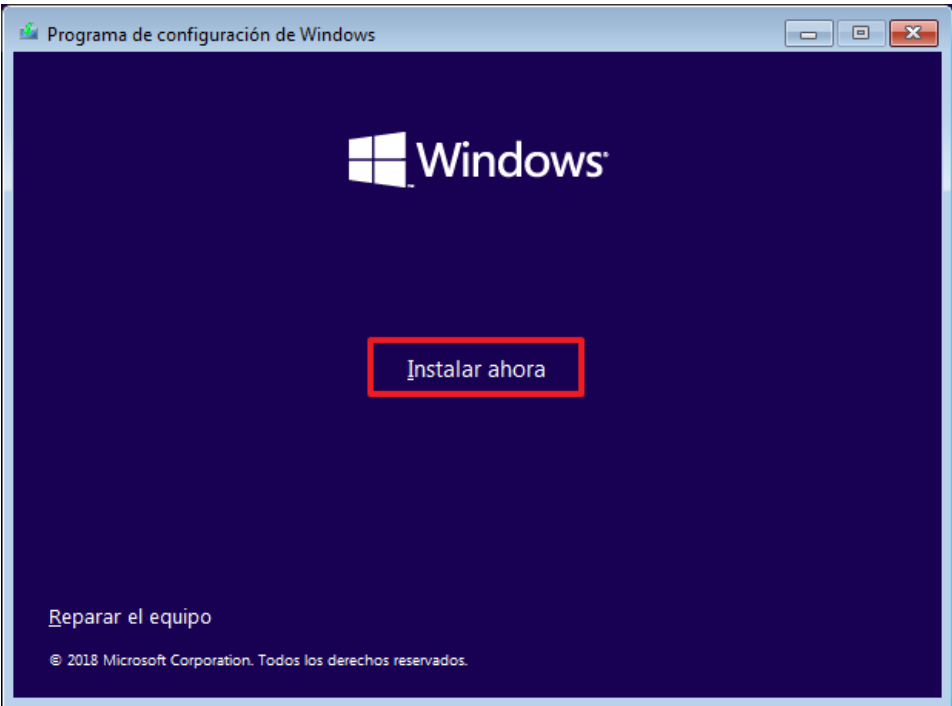
Paso	Descripción
92.	El siguiente paso consiste en crear a cuenta del usuario que vaya a utilizar el equipo cliente que está asegurando, bajo la unidad organizativa “Usuarios Windows 10”. Para ello y utilizando, de nuevo, la consola “Usuarios y equipos de Active Directory”. Para ello, expanda y seleccione el contenedor “Usuarios Windows 10” mediante la siguiente ruta: "<Nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10" Haga clic con el botón derecho del ratón sobre la unidad organizativa y seleccione la opción "Nuevo → Usuario" del menú contextual que aparecerá. 
93.	En el cuadro de diálogo "Nuevo objeto: Usuario", introduzca en el campo “Nombre de pila” y “Nombre de inicio de sesión de usuario:” el nombre que tendrá en el nuevo usuario, El sistema rellenará automáticamente el campo “Nombre completo”. A continuación, pulse “Siguiente >” para continuar.  Nota: En el ejemplo, se utiliza "usuario1001" como nombre del nuevo usuario. Elija un nombre de usuario siguiendo los criterios que sean apropiados para su entorno, y rellene o deje en blanco el resto de datos según sea oportuno para su entorno.

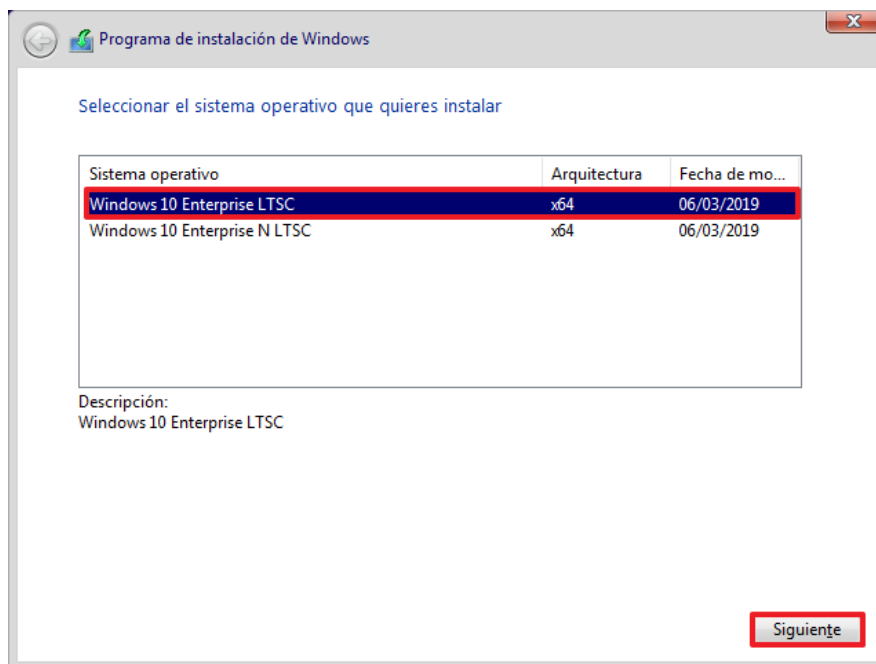
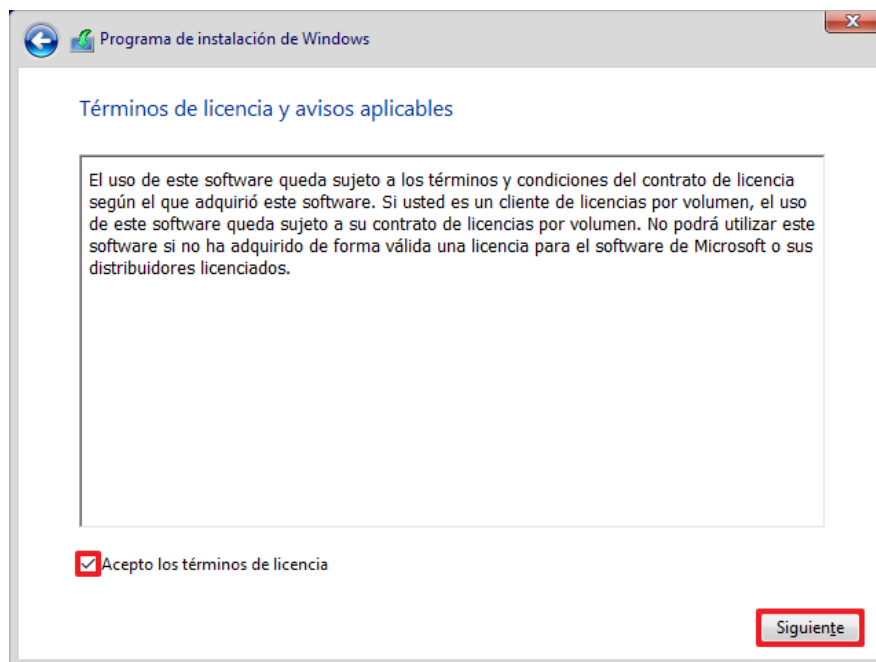
Paso	Descripción
94.	Asigne una contraseña segura al usuario y marque las opciones que sean oportunas para su entorno y pulse “Siguiente >”. 
95.	Pulse “Finalizar” para cerrar la ventana “Nuevo objeto: Usuario”. La cuenta de usuario aparecerá dentro del contenedor "Usuarios Windows 10". 

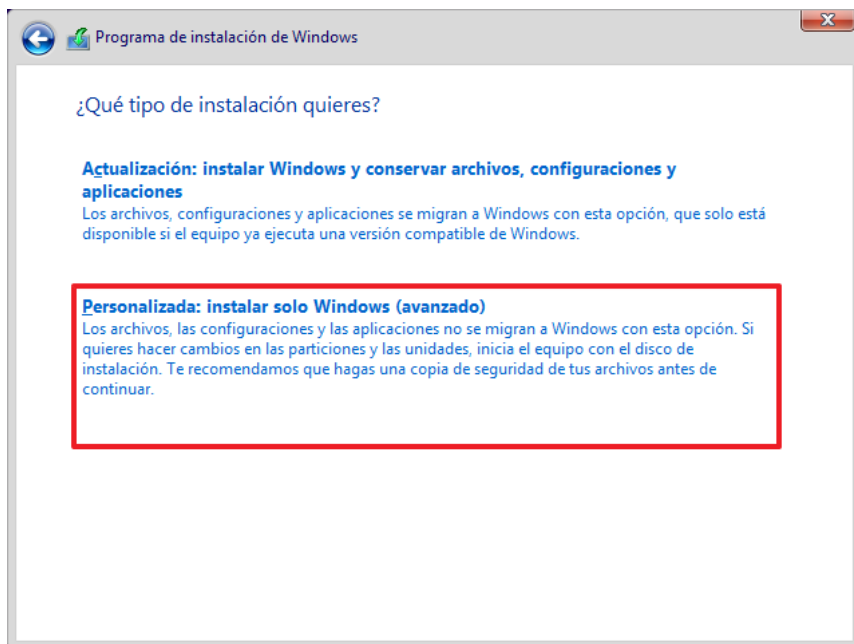
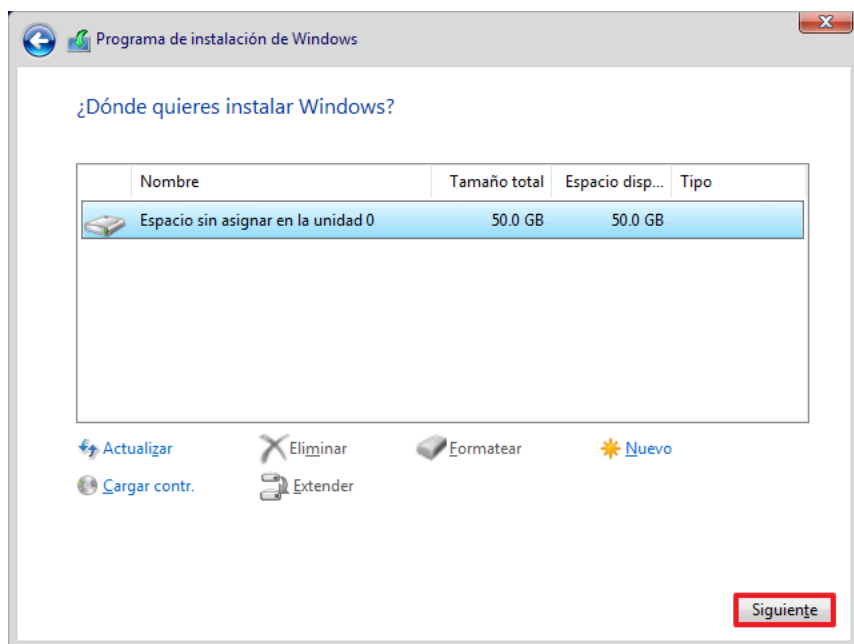
2. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10

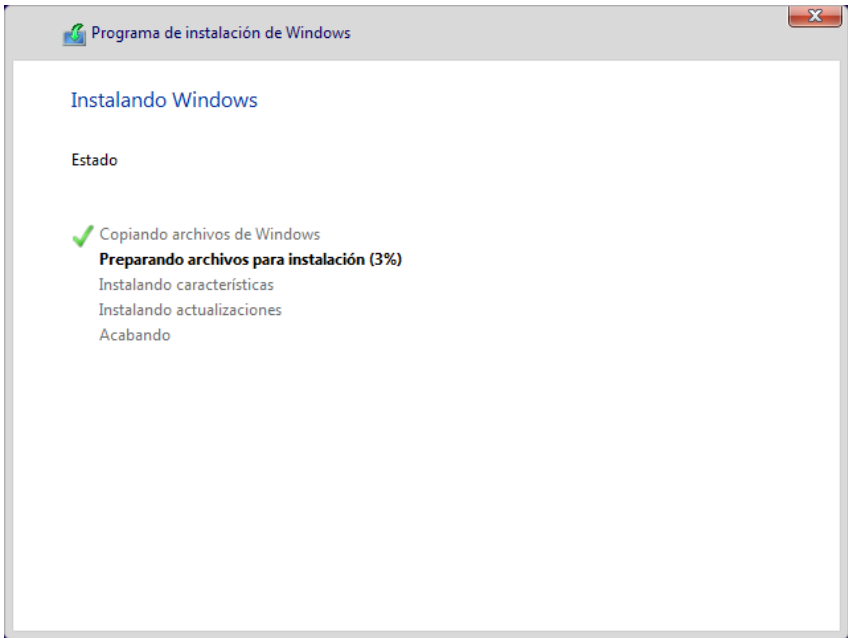
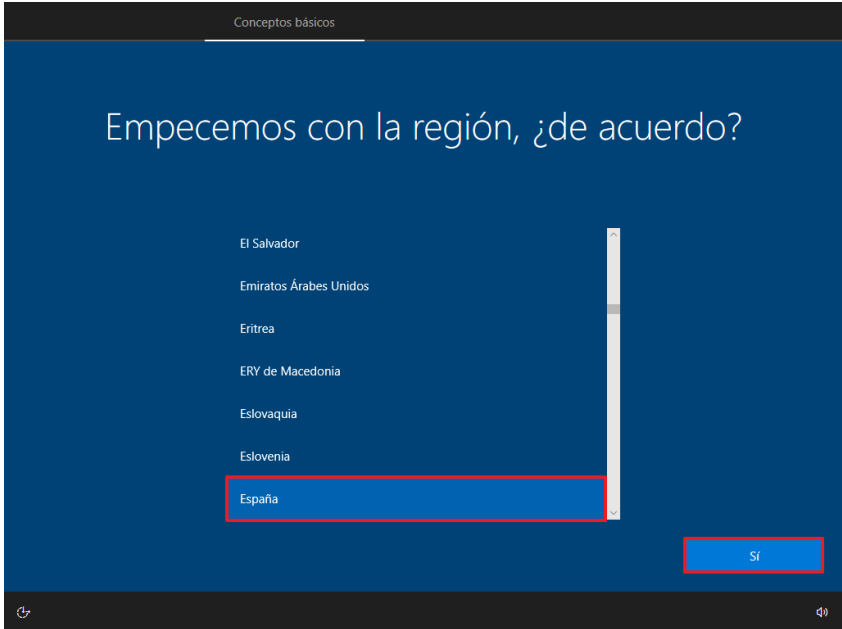
Los pasos que se describen a continuación deberá realizarlos en la máquina donde se instalará y configurará el equipo puesto cliente con sistema operativo Microsoft Windows 10 (versión 1809) Enterprise con opción de mantenimiento LTSC.

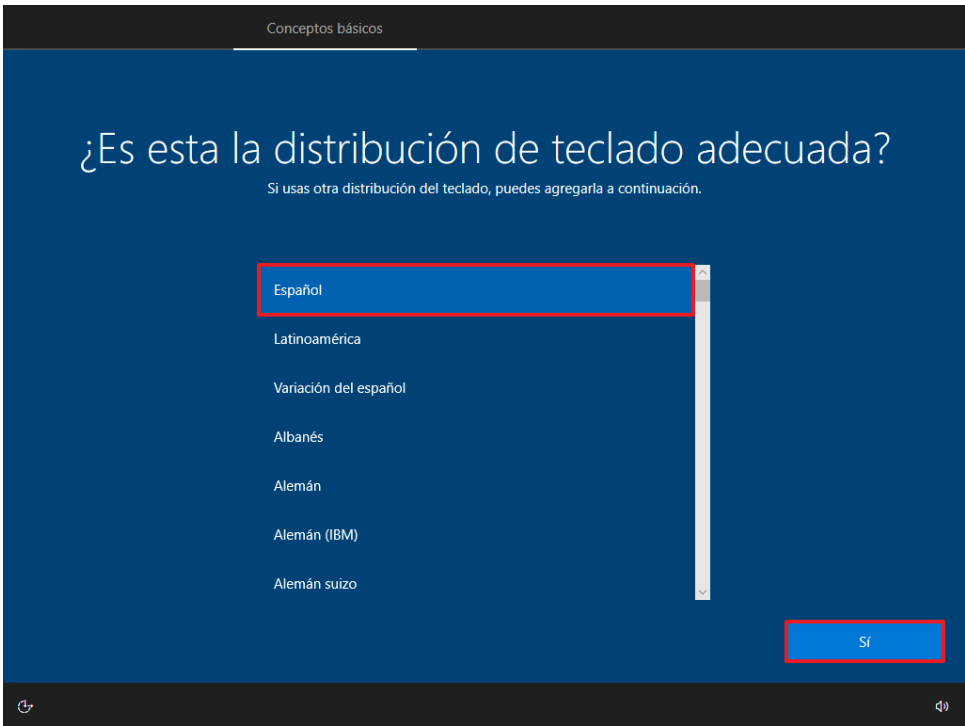
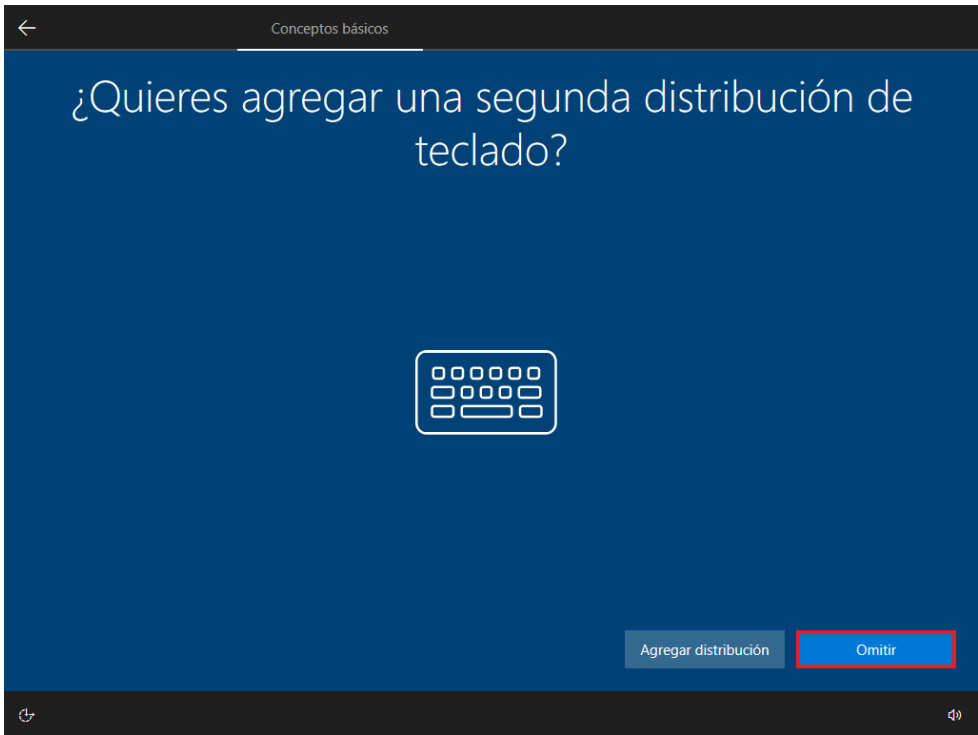
Paso	Descripción
96.	Introduzca el dispositivo USB o DVD de Microsoft Windows 10 Enterprise LTSC y, si fuera necesario, reinicie la máquina para iniciar la instalación del sistema.

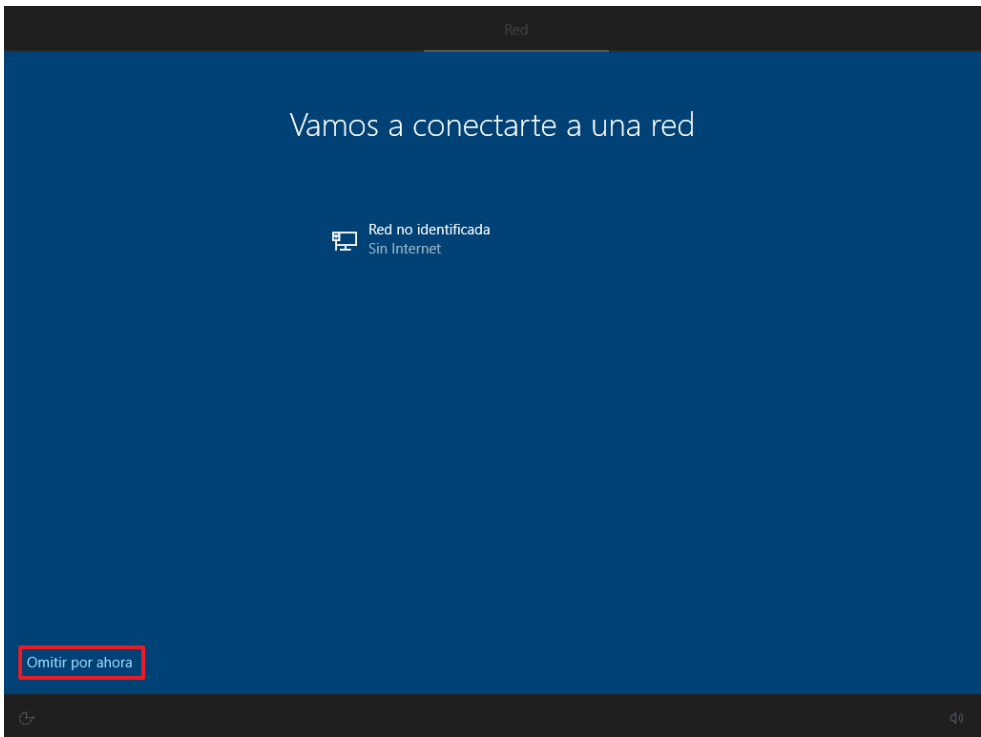
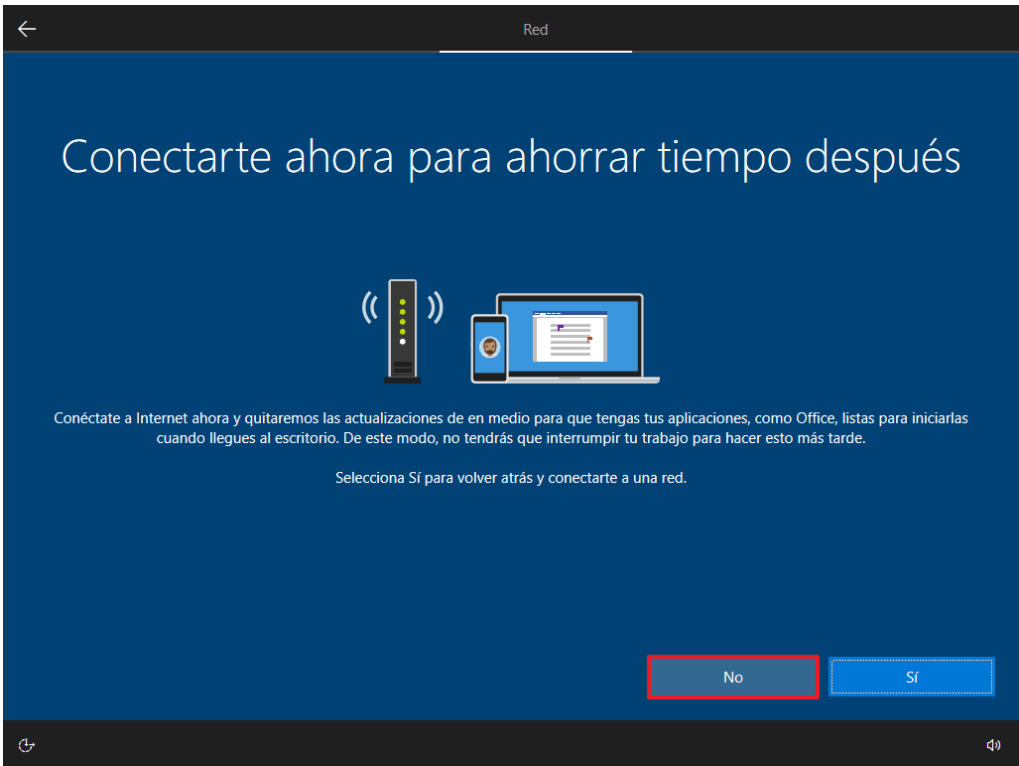
Paso	Descripción
97.	Cuando aparezca el mensaje Presionar una tecla para arrancar desde el DVD, pulse una tecla. Si el equipo no se inicia desde DVD revise los parámetros de la BIOS.
98.	Cuando se le indique en pantalla, seleccione el idioma y la configuración de teclado (español). Pulse “Siguiente” para continuar. 
99.	Pulse sobre “Instalar ahora”. 

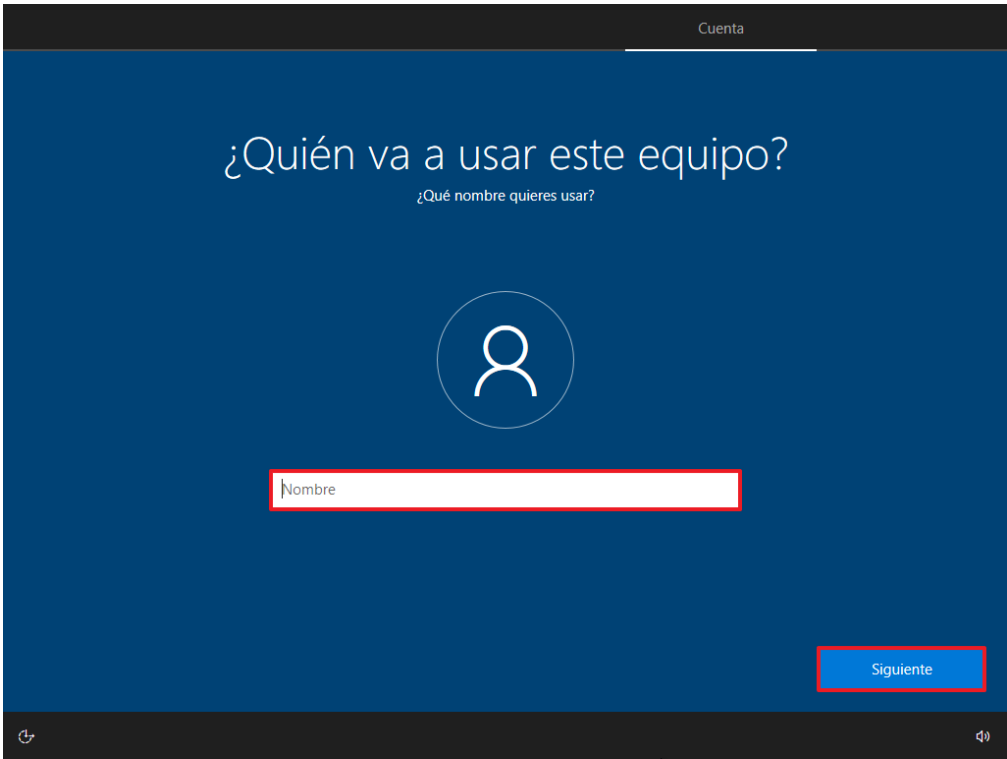
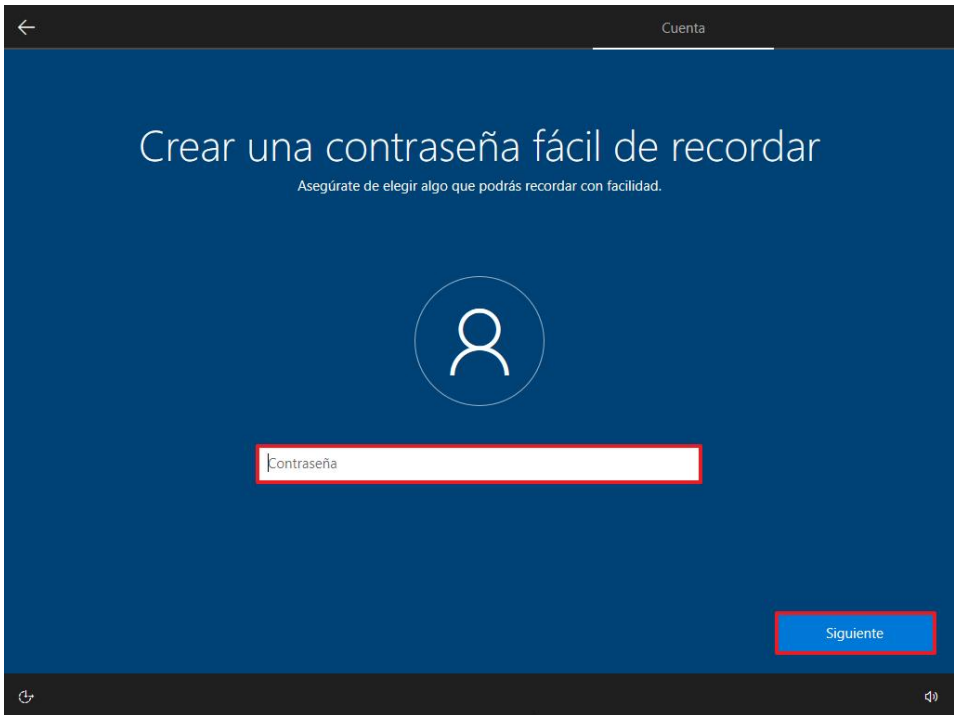
Paso	Descripción									
100.	Seleccione la opción “Windows 10 Enterprise LTSC”.  The screenshot shows the 'Programa de instalación de Windows' window. It prompts the user to 'Seleccionar el sistema operativo que quieres instalar'. A table lists two options: 'Windows 10 Enterprise LTSC' and 'Windows 10 Enterprise N LTSC'. The first option is selected and highlighted with a red box. Below the table, the description 'Windows 10 Enterprise LTSC' is shown. A 'Siguiente' button is highlighted with a red box at the bottom right. <table><tr><th>Sistema operativo</th><th>Arquitectura</th><th>Fecha de mo...</th></tr><tr><td>Windows 10 Enterprise LTSC</td><td>x64</td><td>06/03/2019</td></tr><tr><td>Windows 10 Enterprise N LTSC</td><td>x64</td><td>06/03/2019</td></tr></table> Descripción: Windows 10 Enterprise LTSC Siguiente	Sistema operativo	Arquitectura	Fecha de mo...	Windows 10 Enterprise LTSC	x64	06/03/2019	Windows 10 Enterprise N LTSC	x64	06/03/2019
Sistema operativo	Arquitectura	Fecha de mo...								
Windows 10 Enterprise LTSC	x64	06/03/2019								
Windows 10 Enterprise N LTSC	x64	06/03/2019								
101.	Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  The screenshot shows the 'Programa de instalación de Windows' window. It displays the 'Términos de licencia y avisos aplicables'. The text states that the use of the software is subject to the license terms. At the bottom, the checkbox 'Acepto los términos de licencia' is checked. A 'Siguiente' button is highlighted with a red box at the bottom right. Términos de licencia y avisos aplicables El uso de este software queda sujeto a los términos y condiciones del contrato de licencia según el que adquirió este software. Si usted es un cliente de licencias por volumen, el uso de este software queda sujeto a su contrato de licencias por volumen. No podrá utilizar este software si no ha adquirido de forma válida una licencia para el software de Microsoft o sus distribuidores licenciados. ☒ Acepto los términos de licencia Siguiente									

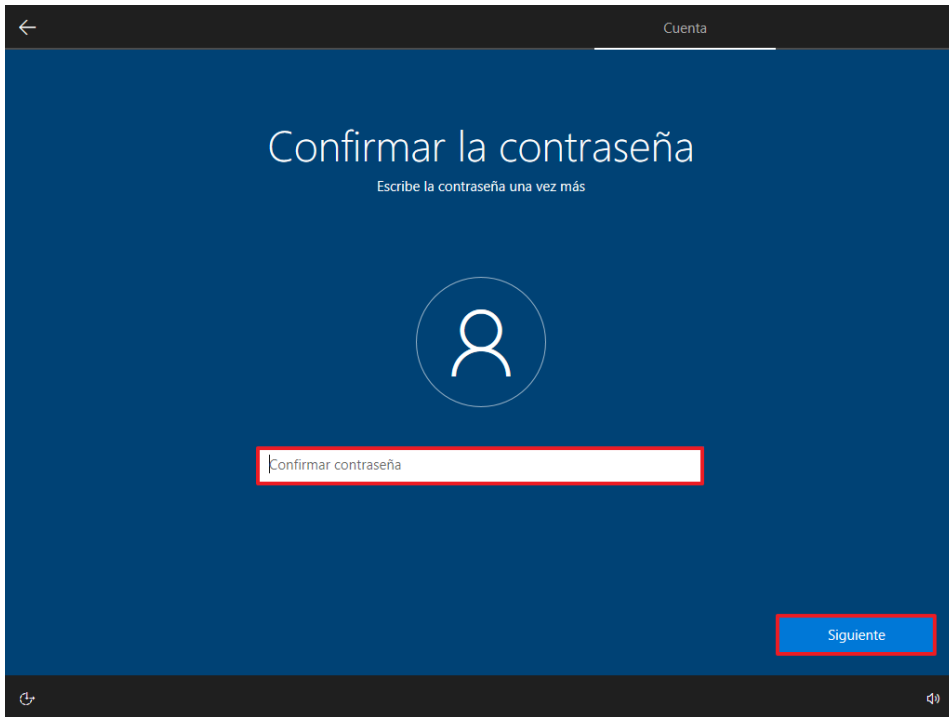
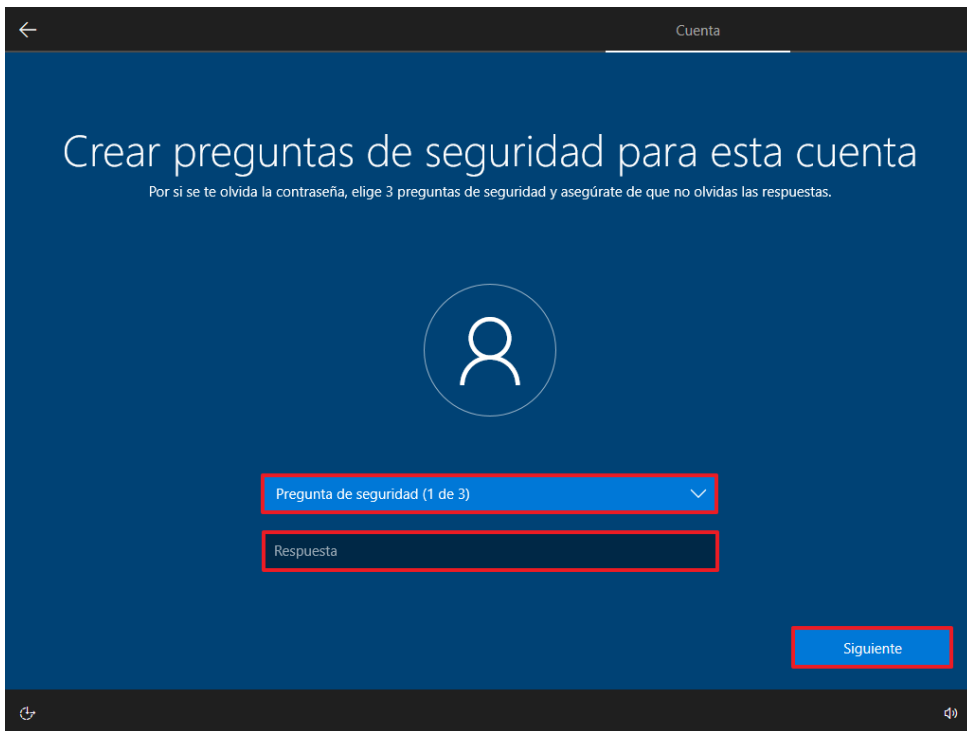
Paso	Descripción
102.	Seleccione la opción tipo de instalación “Personalizada: instalar solo Windows (avanzada)”. 
103.	Seleccione el disco en el que se realizará la instalación y pulse “Siguiente”. 
Nota: En caso de necesitar establecer particiones o formatear particiones o discos, es en este momento 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	

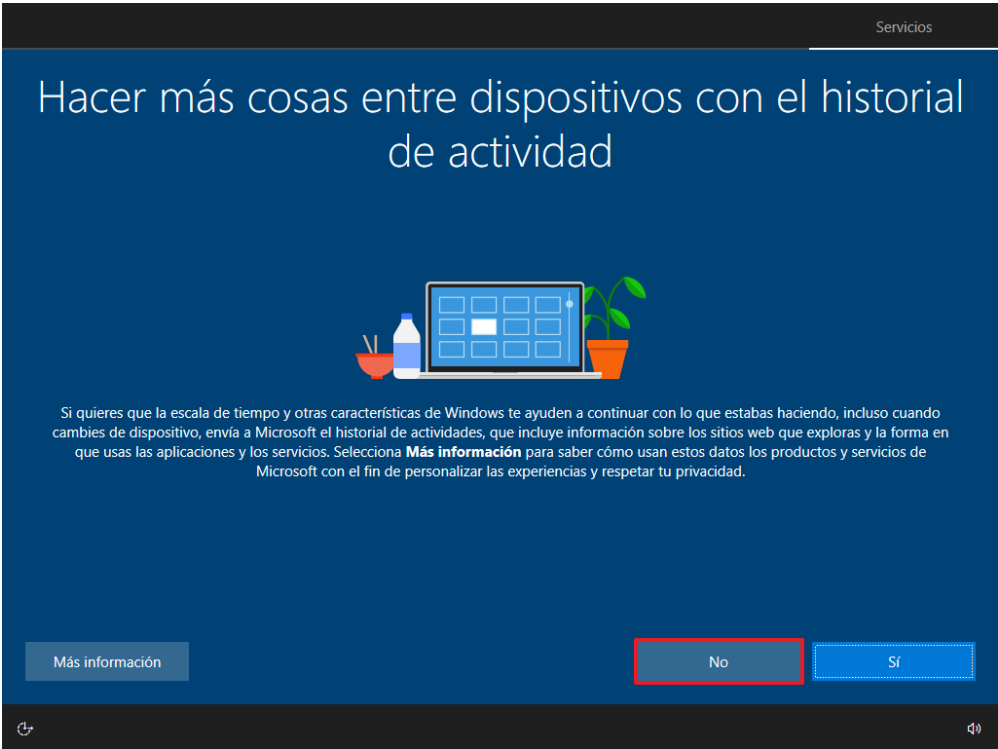
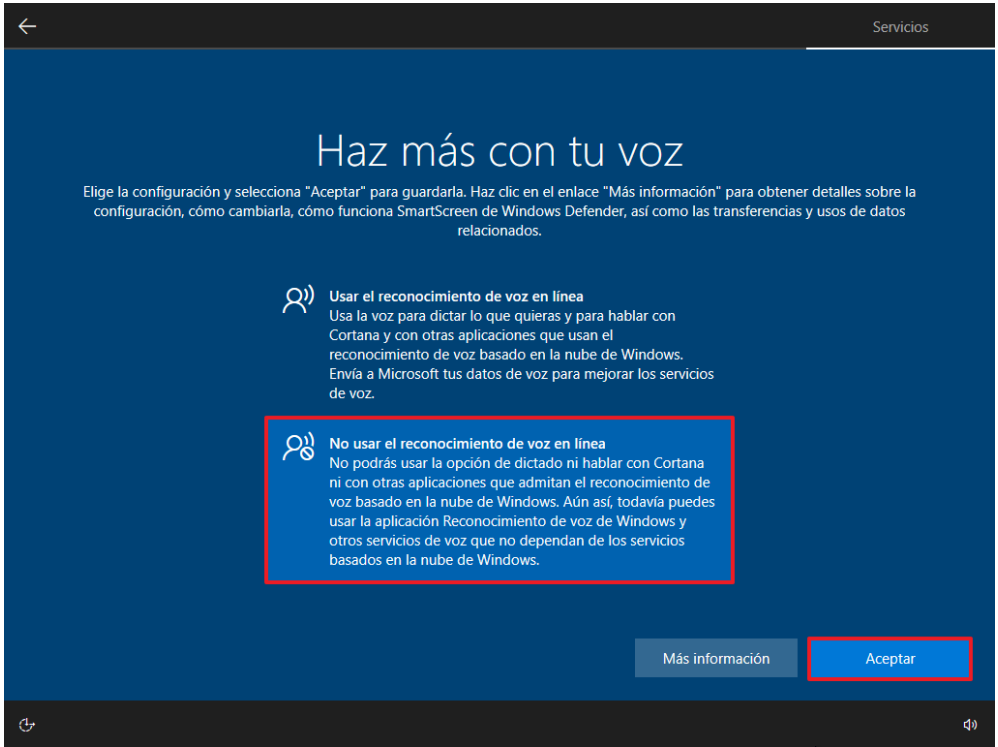
Paso	Descripción
104.	Comenzará la instalación en este momento. Este proceso durará varios minutos dependiendo de las prestaciones del dispositivo sobre el que se instale Microsoft Windows 10 y, posiblemente, requerirá reiniciar en varias ocasiones. Espere a que aparezca la ventana “Conceptos básicos” y continúe con el siguiente paso. 
105.	En la ventana “Conceptos básicos” seleccione la región “España” y pulse “Sí”. 

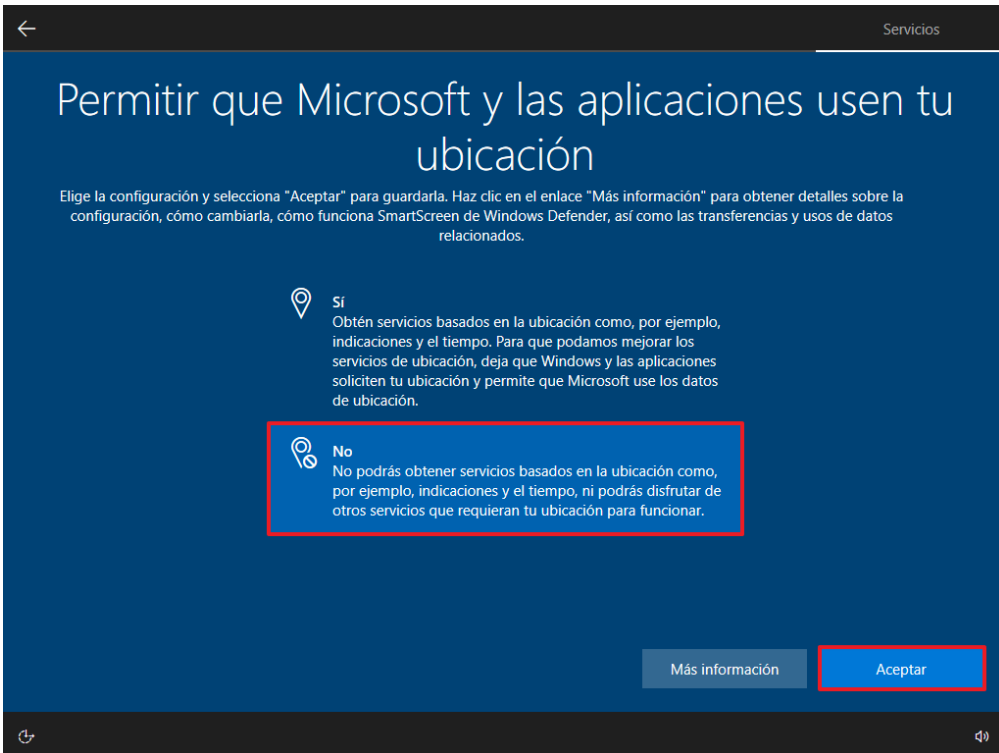
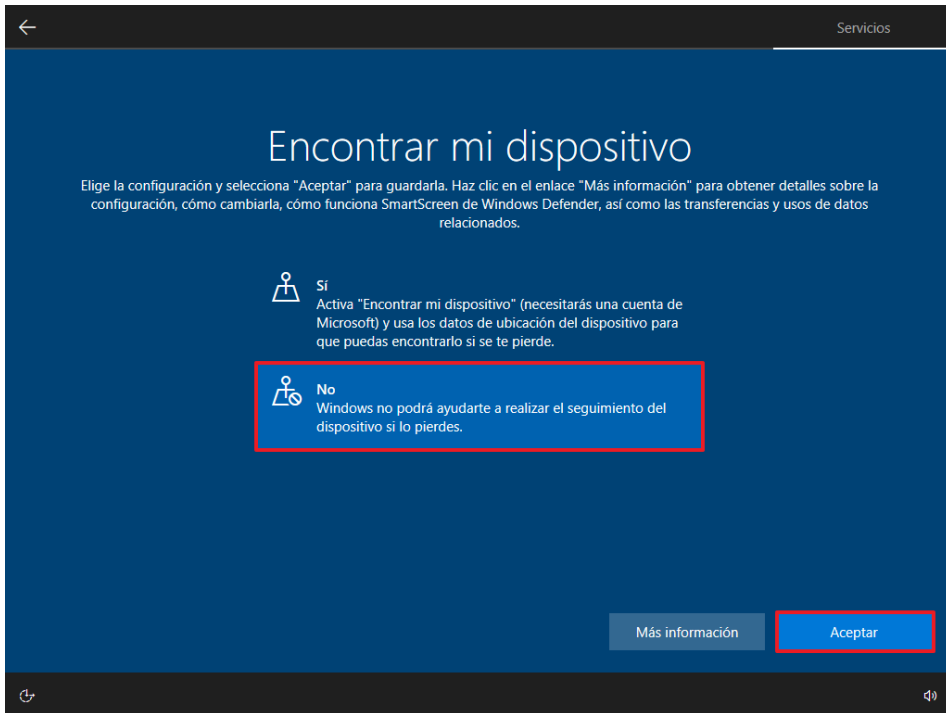
Paso	Descripción
106.	Seleccione la distribución de teclado “Español” y pulse “Sí” para continuar. 
107.	Pulse “Omitir” para no agregar una segunda distribución de teclado. 

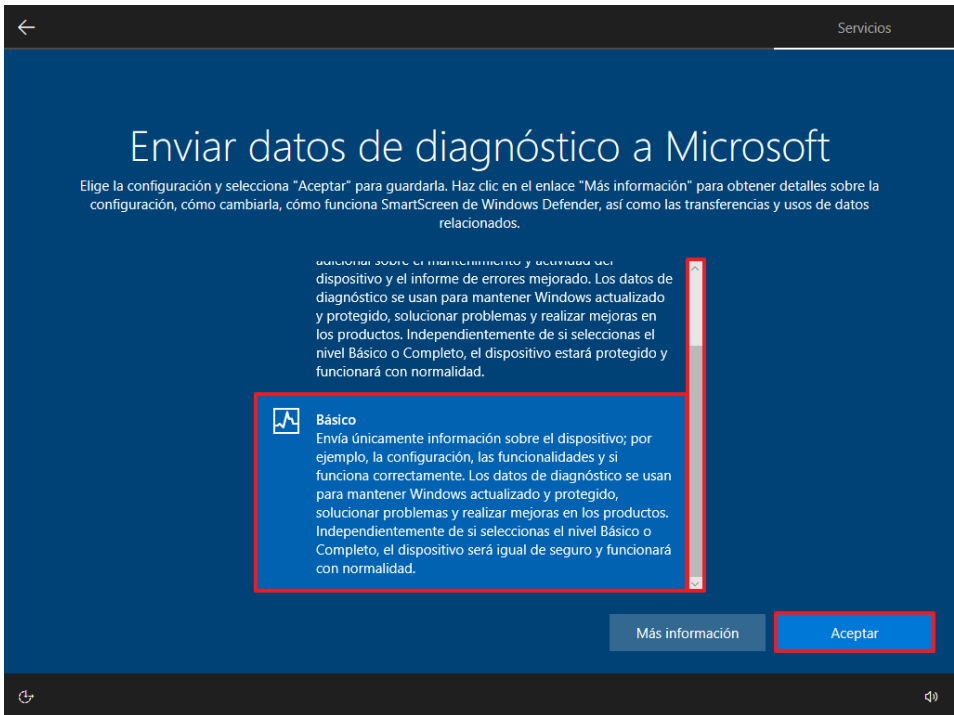
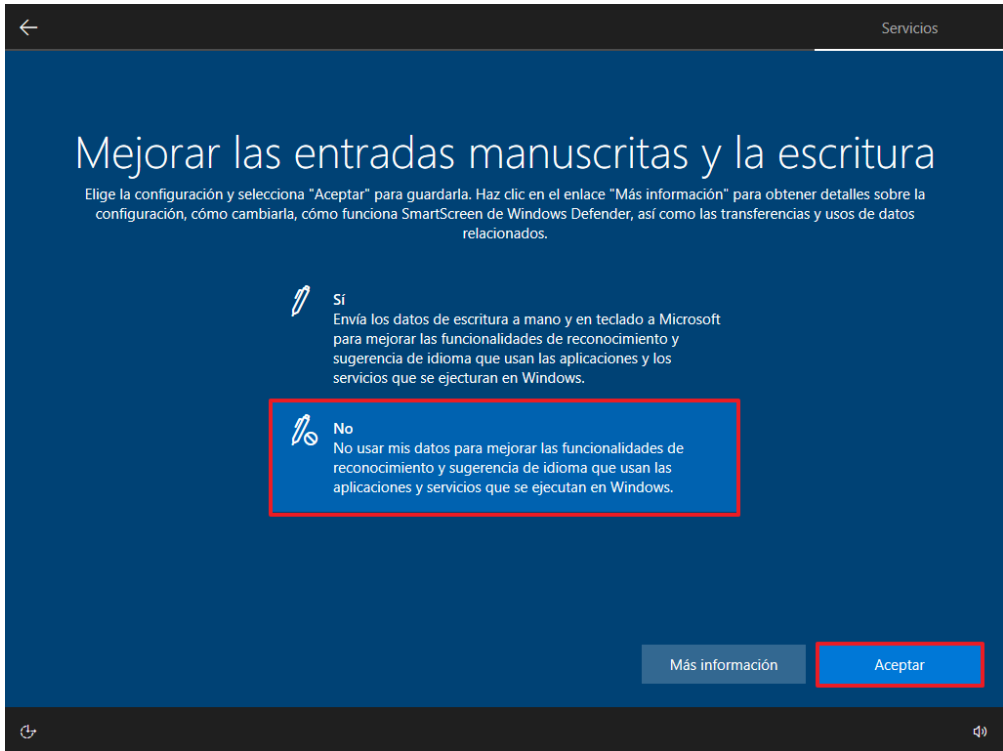
Paso	Descripción
108.	En el apartado de red seleccione la opción “Omitir por ahora”. La configuración de red se establecerá más adelante. 
109.	Pulse “No” para continuar. 

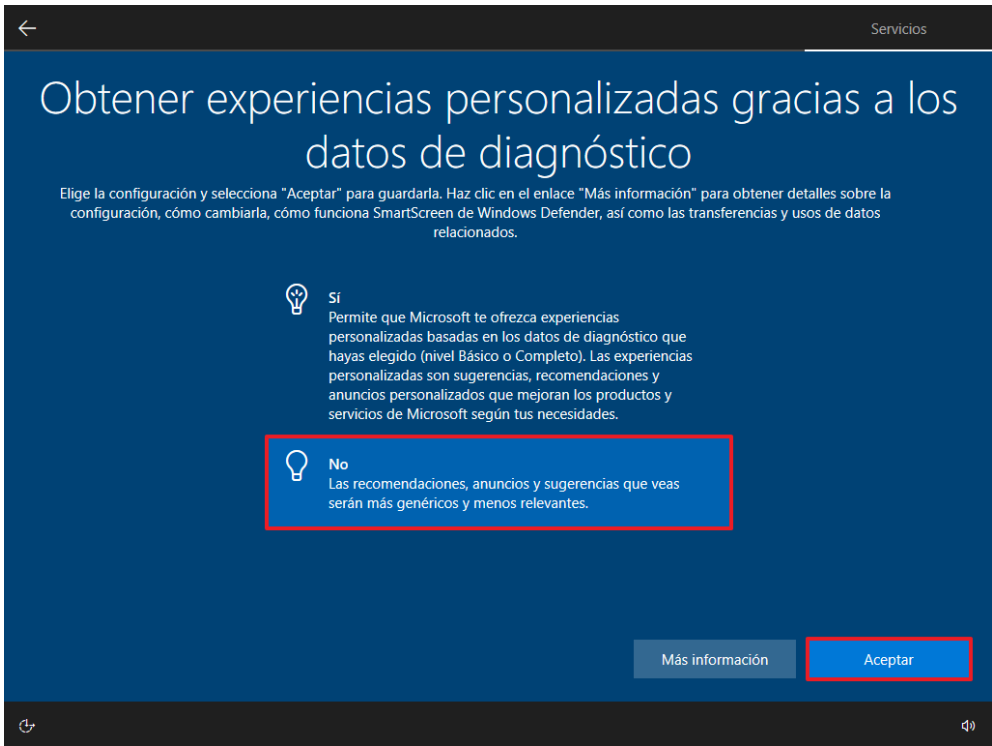
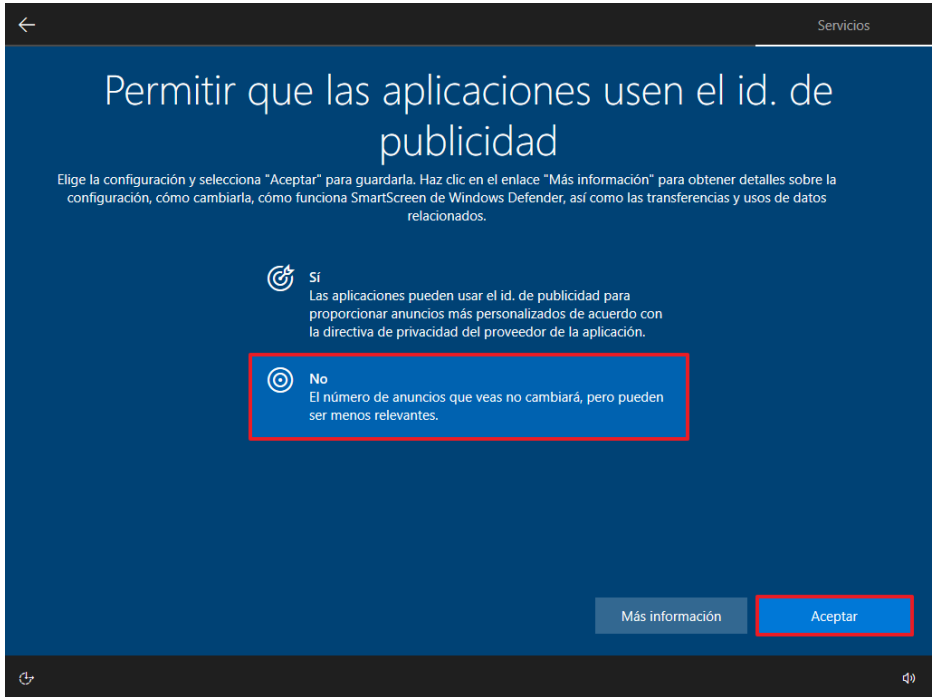
Paso	Descripción
110.	En la ventana “Cuenta”, introduzca un nombre de usuario (por ejemplo "Admin") que se creará con permisos de administrador local. Pulse “Siguiente” para continuar.  Nota: Deberá elegir un nombre de usuario adecuado para su entorno. Los nombres aquí indicados sólo se proporcionan a modo de ejemplo.
111.	Introduzca una contraseña para el usuario administrador local y pulse “Siguiente”. 

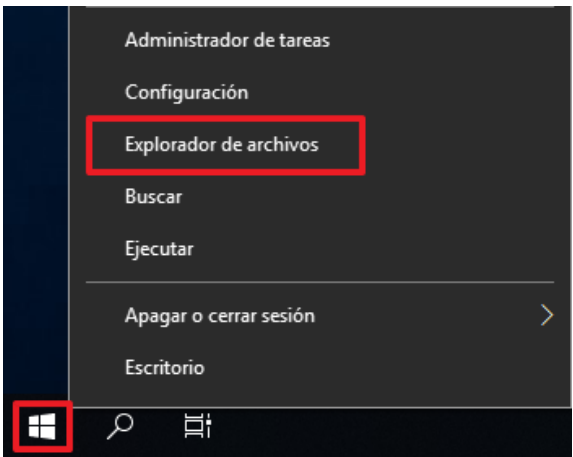
Paso	Descripción
112.	Introduzca nuevamente la contraseña y pulse “Siguiente”. 
113.	El instalador le solicitará tres preguntas de seguridad en caso de olvidar la contraseña. Seleccione las preguntas, respóndalas y pulse “Siguiente” para continuar.  Nota: Más adelante se establecerá el bloqueo de la cuenta en caso de introducir erróneamente la contraseña repetidas veces.

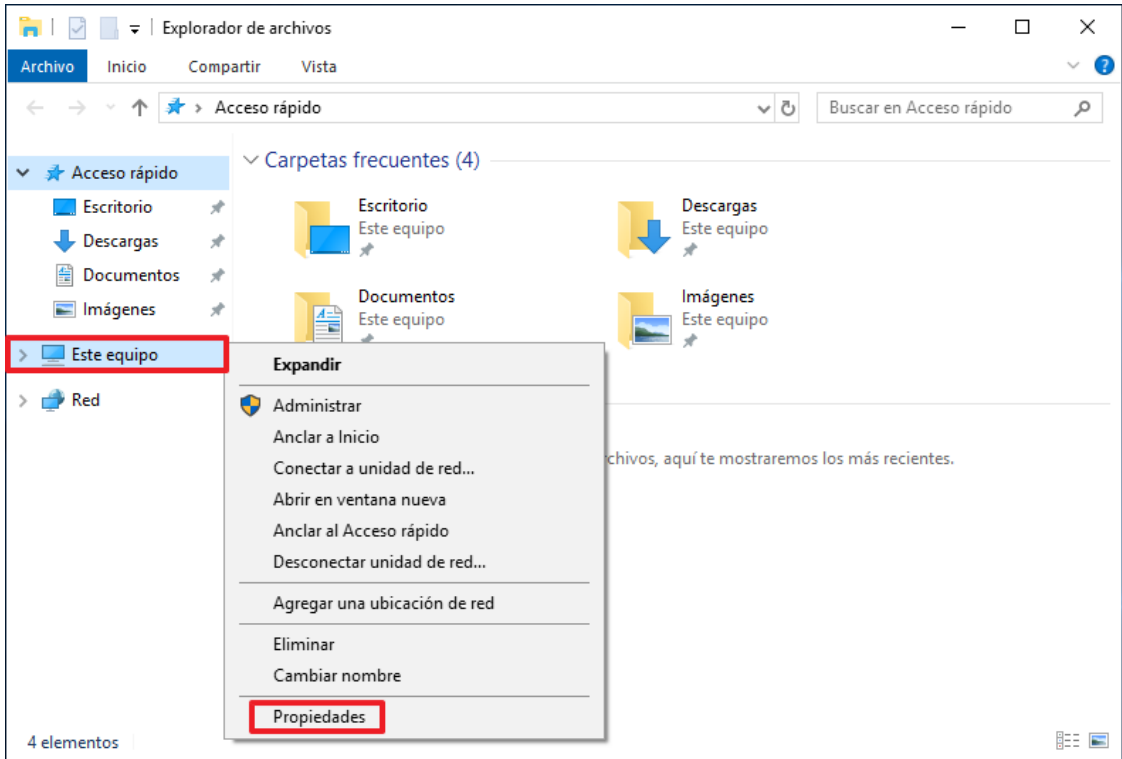
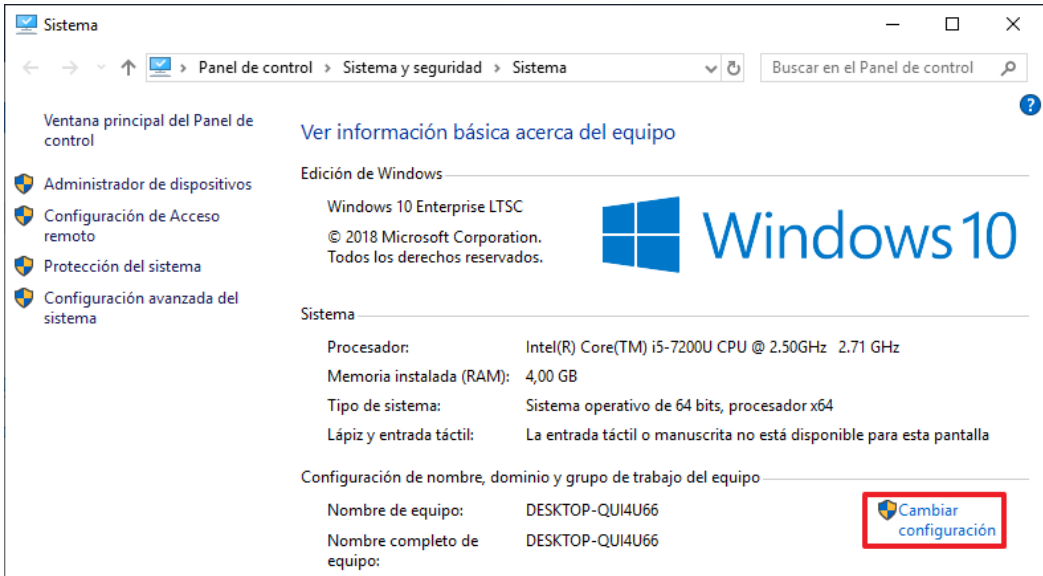
Paso	Descripción
114.	Pulse “No” para desactivar el historial de actividad. 
115.	Seleccione “No” para no usar el reconocimiento de voz en línea y pulse “Aceptar”. 

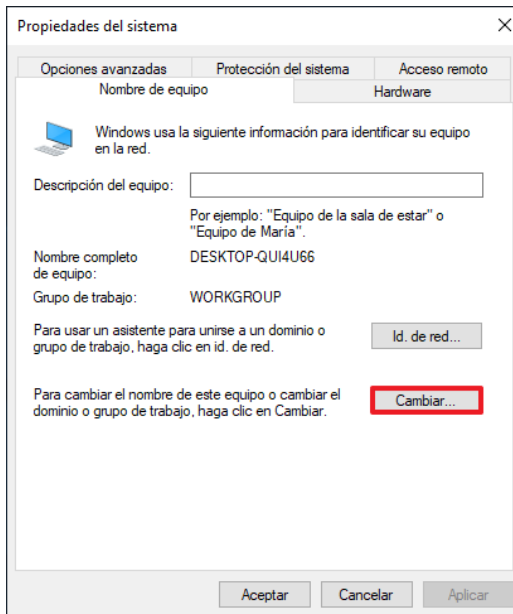
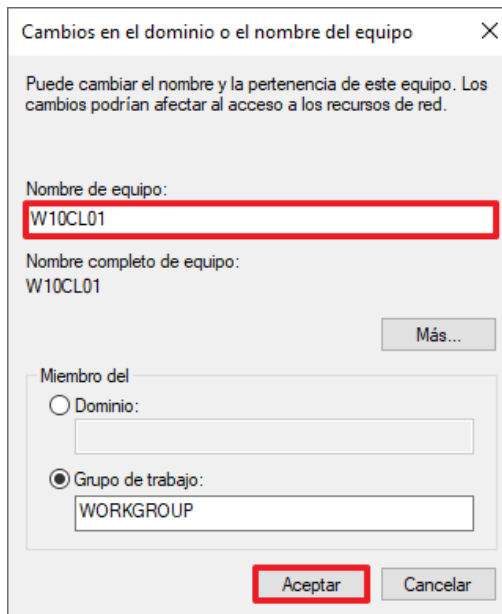
Paso	Descripción
116.	Seleccione “No” para impedir que las aplicaciones usen la ubicación y pulse “Aceptar”. 
117.	Seleccione “No” para desactivar la funcionalidad de “Encontrar mi dispositivo”. Pulse “Aceptar” para continuar. 

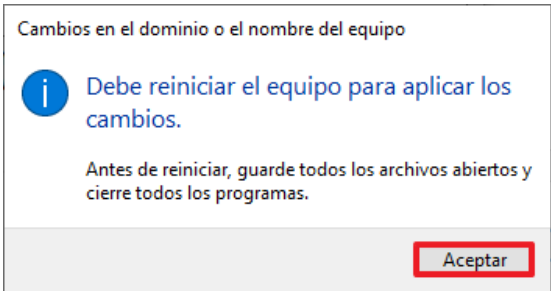
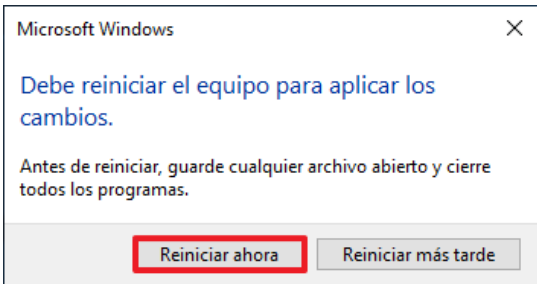
Paso	Descripción
118.	Seleccione la opción “Básico” y pulse “Aceptar”.  Nota: Más adelante se impedirá toda comunicación con los servidores de Windows y se desactiva la telemetría.
119.	Seleccione “No” y pulse “Aceptar”. 

Paso	Descripción
120.	Seleccione “No” para no enviar datos de diagnóstico. Pulse “Aceptar” para continuar. 
121.	Seleccione “No” para impedir que las aplicaciones usen el identificador de publicidad. Pulse “Aceptar” para continuar. 

Paso	Descripción
122.	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. 
123.	En la barra de tareas, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 

Paso	Descripción
124.	En el “Explorador de archivos” pulse con el botón derecho del ratón sobre “Este equipo” y seleccione “Propiedades”. 
125.	En la ventana “Sistema” localice el apartado “Configuración de nombre, dominio y grupo de trabajo del equipo” y pulse sobre “Cambiar configuración” 

Paso	Descripción
126.	En “Propiedades del sistema”, seleccione la pestaña “Nombre de equipo”, pulse sobre “Cambiar”. 
127.	Establezca un nombre de equipo y pulse “Aceptar”.  Nota: En el ejemplo, el equipo se denomina “W10CL01”. Deberá ser el mismo nombre que le asignó en la unidad organizativa “Equipos Windows 10” del controlador de dominio, que le asignó durante la realización del apartado “1 PREPARACIÓN DEL DOMINIO”.

Paso	Descripción
128.	El sistema deberá reiniciar para guardar los cambios. Pulse “Aceptar” en la ventana de “Cambios en el dominio o el nombre de equipo”. 
129.	Pulse sobre “Cerrar” en “Propiedades del sistema” y “Reiniciar ahora” para que se reinicie el equipo y hagan efecto los cambios. 

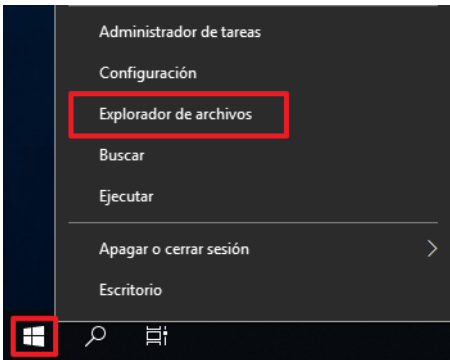
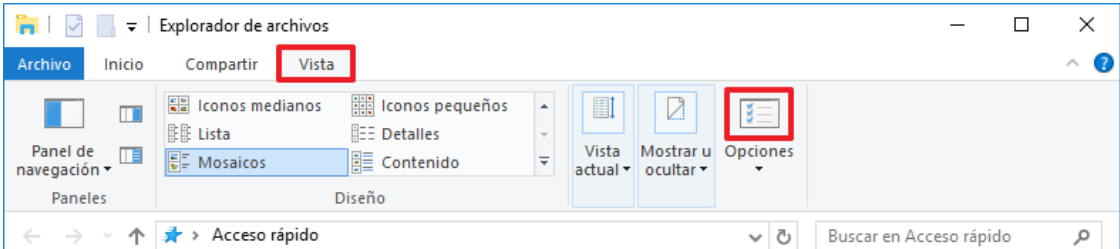
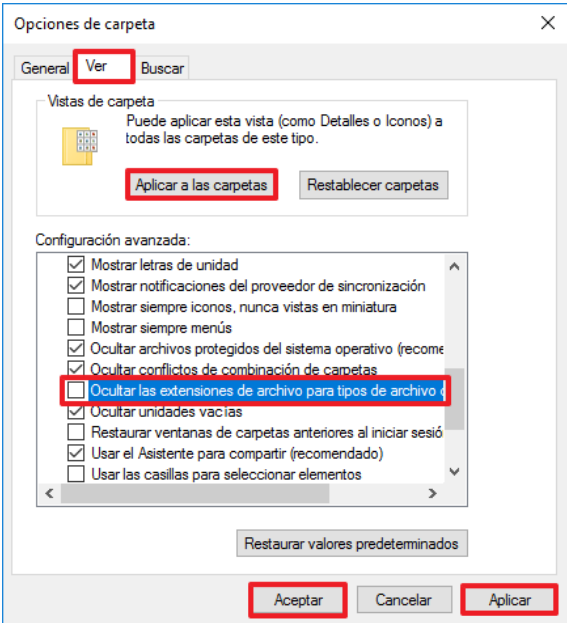
3. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10

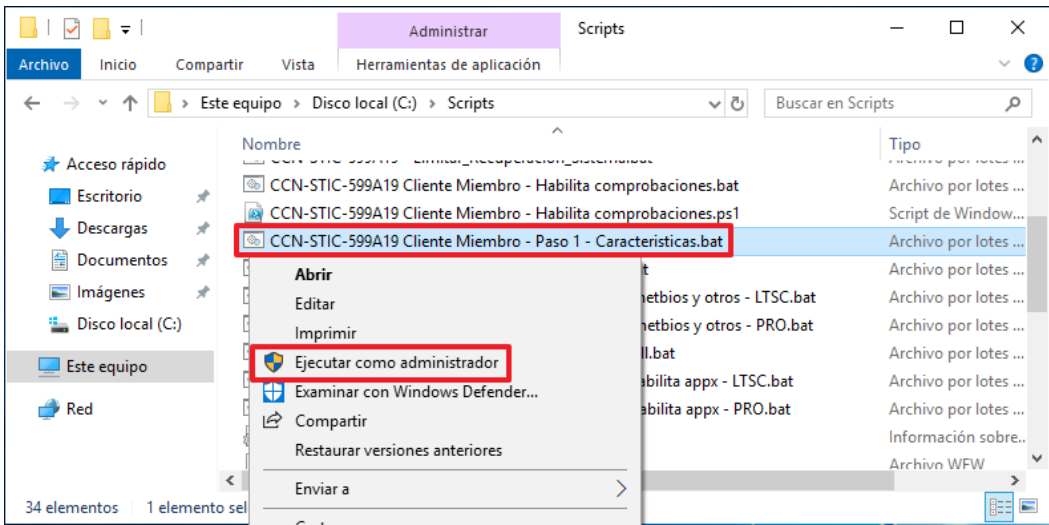
Con el sistema operativo instalado, se procederá a configurar el equipo.

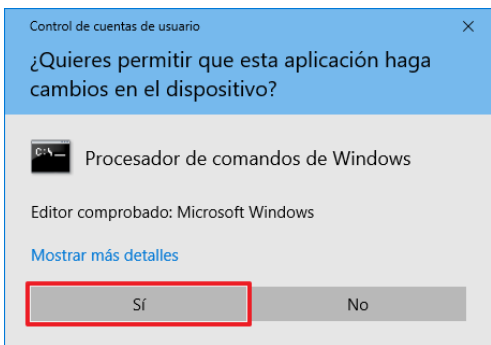
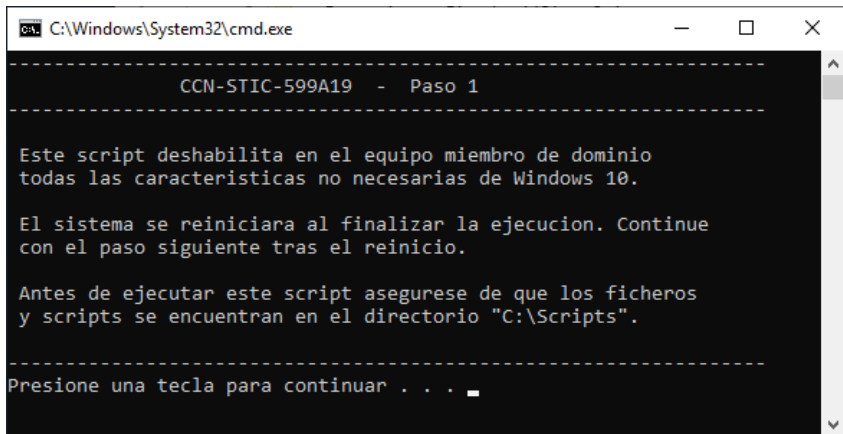
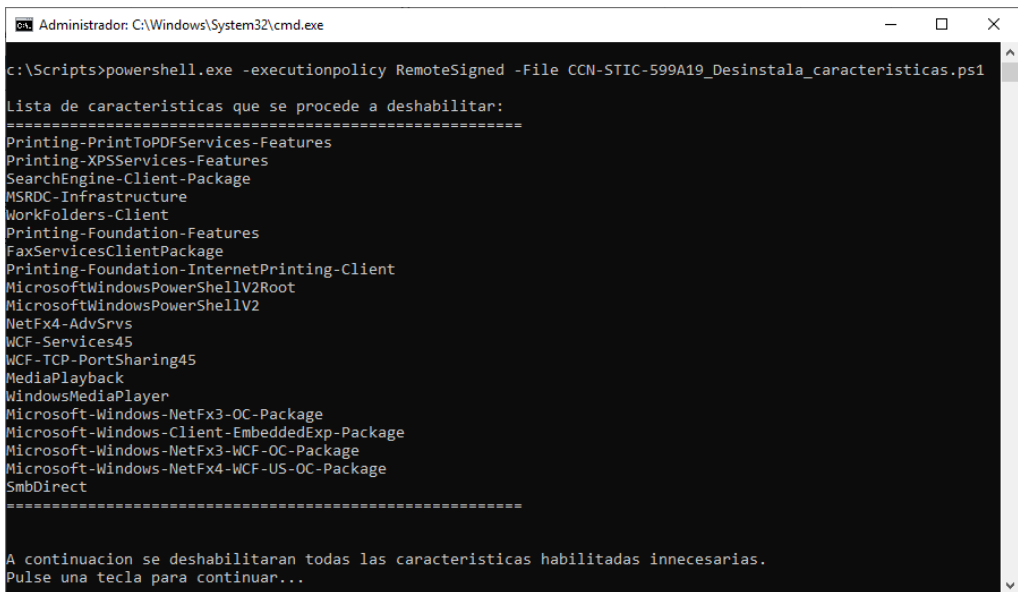
Nota: En este punto es conveniente recordar que, aunque en esta guía paso a paso no se dedica ningún apartado concreto a ello, será necesario instalar las actualizaciones de seguridad disponibles y realizar la activación de Windows en el equipo.

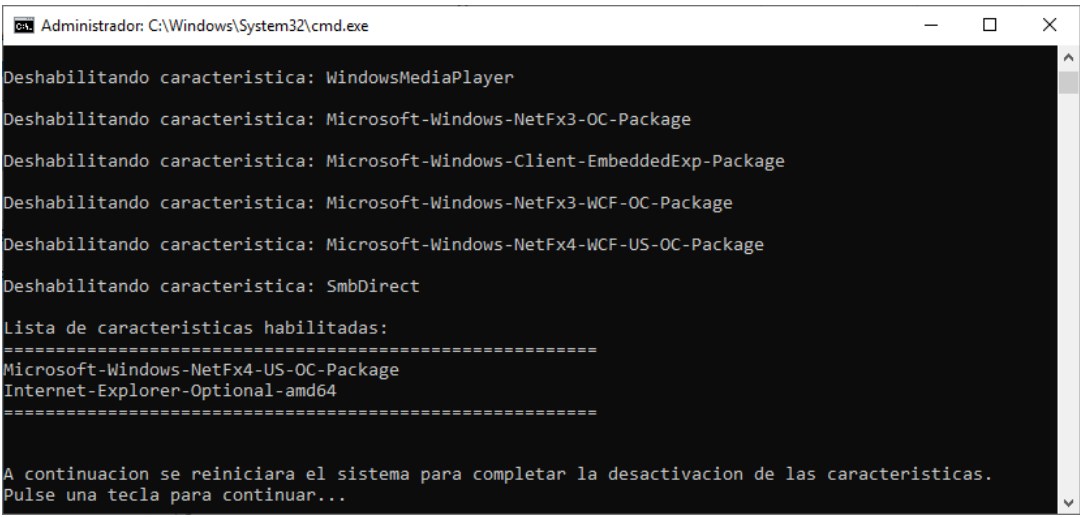
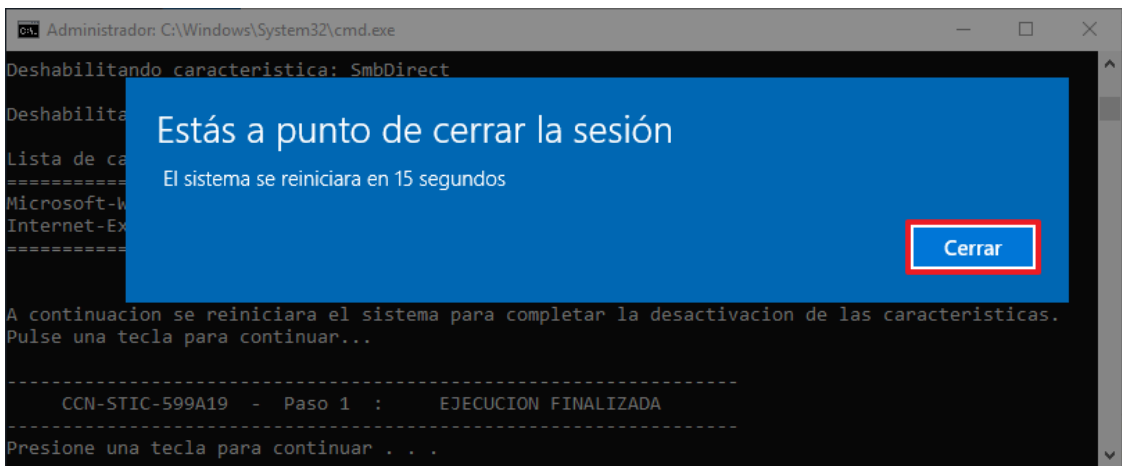
Una vez preparadas las unidades organizativas "Equipos Windows 10" y "Usuarios Windows 10", y creada en Active Directory la cuenta de equipo para el equipo que está asegurando, y para el usuario que lo utilizará, según se ha descrito en pasos anteriores, realice los siguientes pasos en el equipo cliente que está asegurando, para unirlo al dominio y aplicarle la configuración recomendada en esta guía.

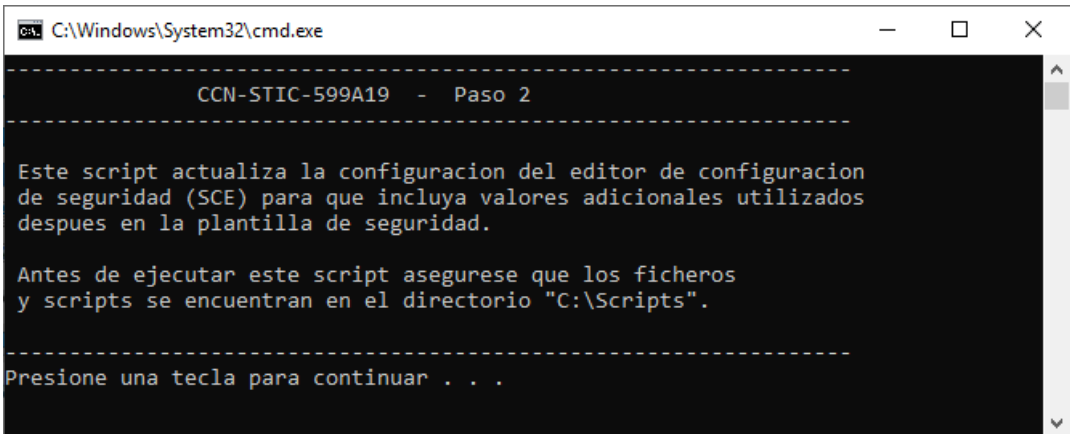
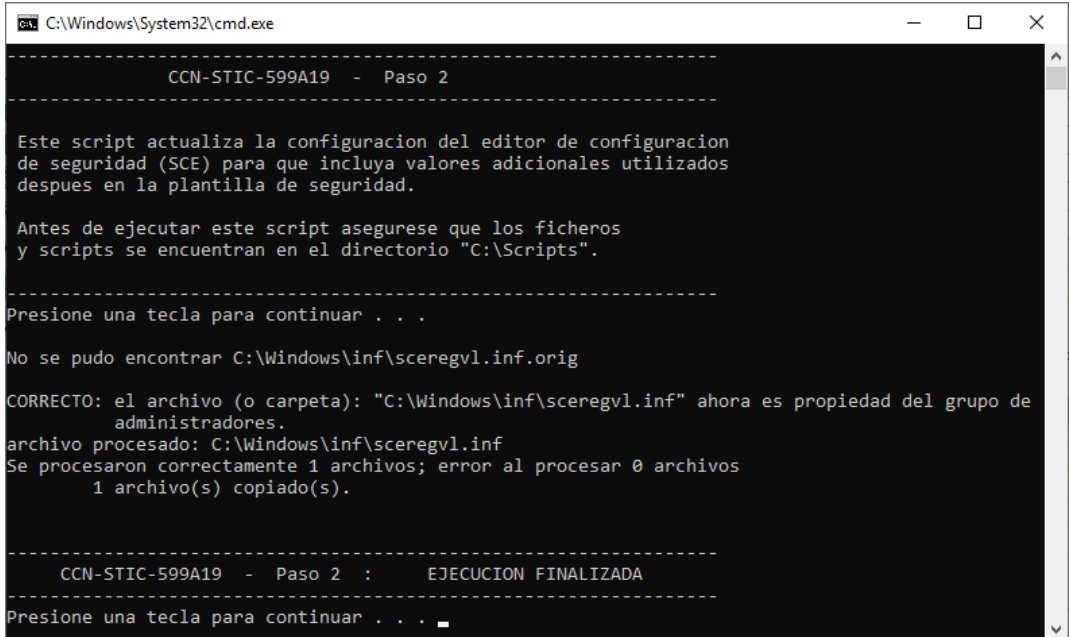
Paso	Descripción
130.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador local (por ejemplo "admin", si ese fue el nombre de usuario administrador que proporcionó durante la instalación).
131.	Cree el directorio “Scripts” en la unidad “C:\”.
132.	Copie los ficheros asociados a esta guía en el directorio “C:\Scripts”. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”. 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.

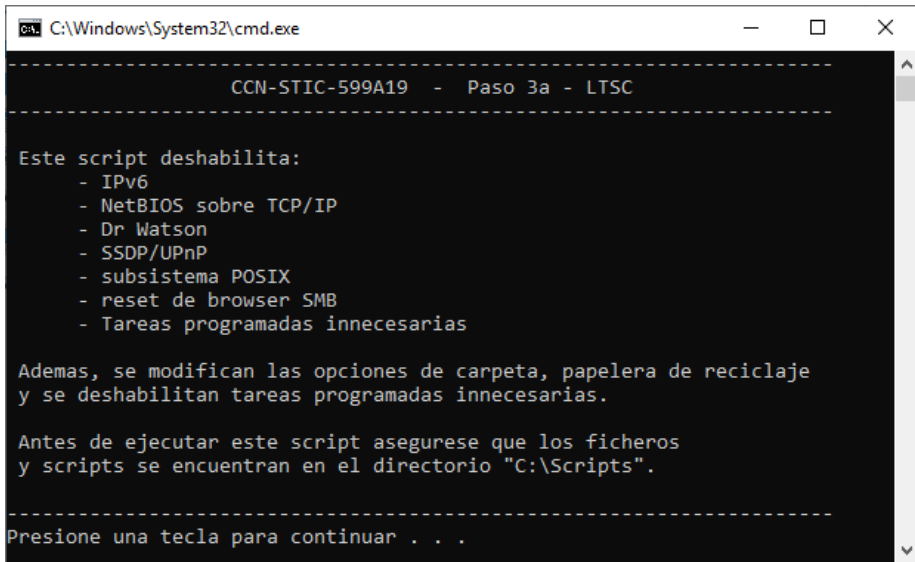
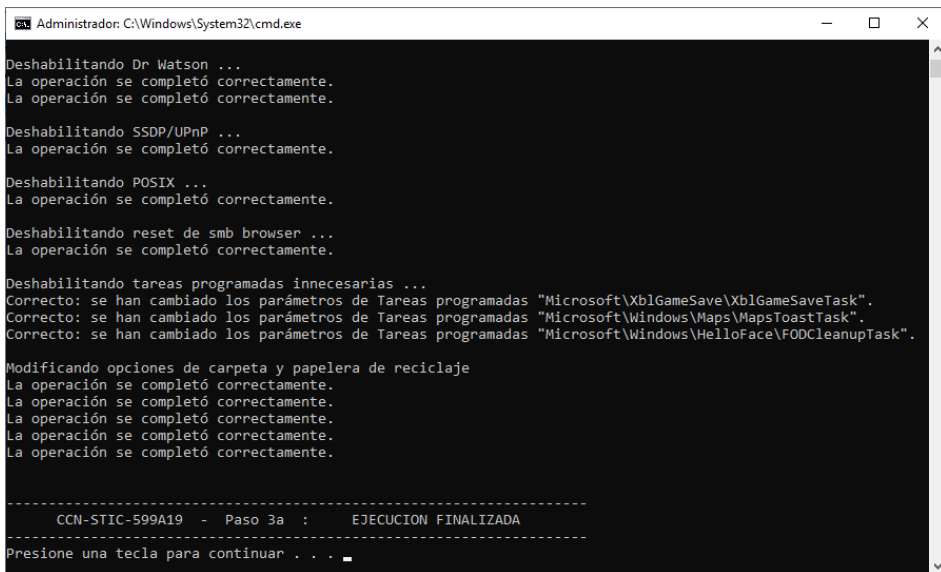
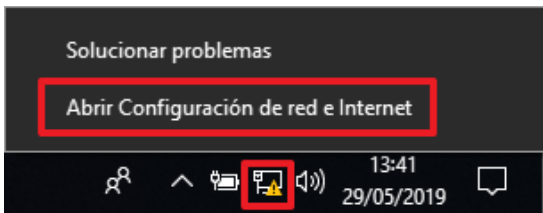
Paso	Descripción
133.	Configure el “Explorador de archivos” para que muestre las extensiones de los archivos ya que, por defecto, el Explorador de archivos” oculta las extensiones conocidas y este hecho dificulta la identificación de los mismos. Para ello, pulse sobre el botón de “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 
134.	En el “Explorador de archivos” pulse sobre la pestaña “Vista” del menú superior y seleccione el icono de “Opciones”. 
135.	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”. 

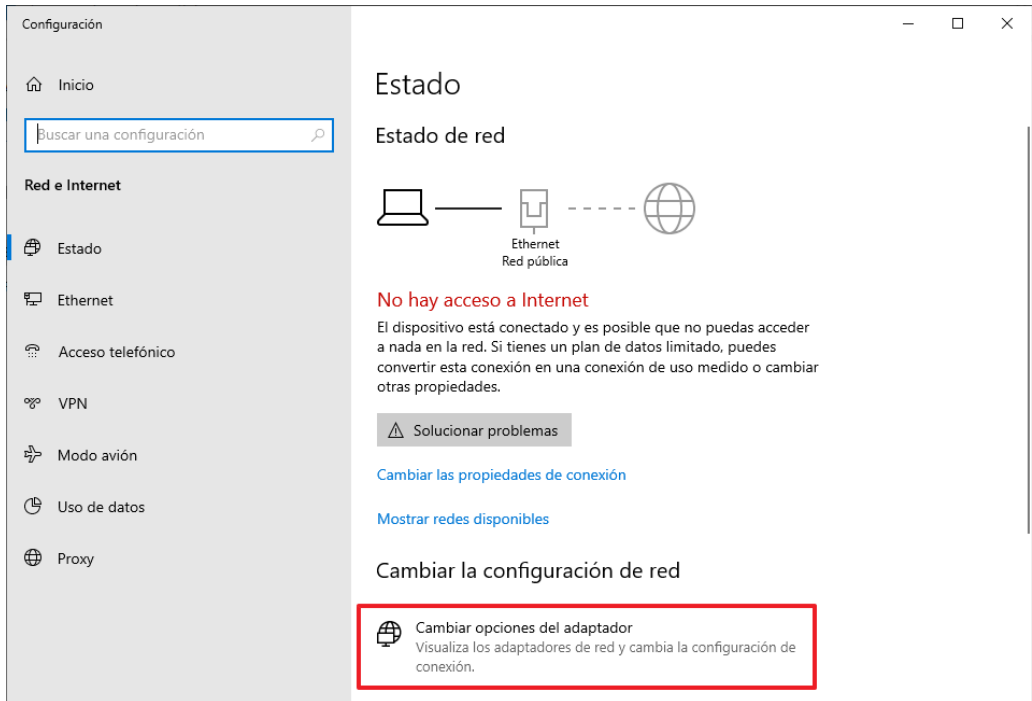
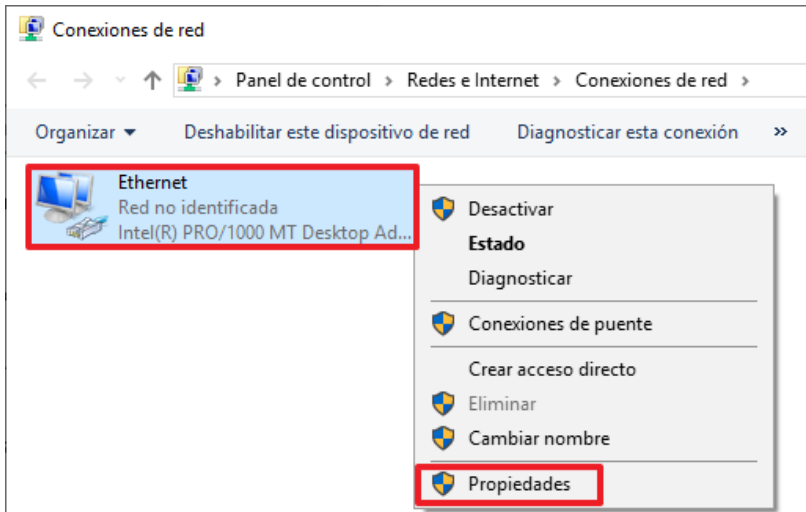
Paso	Descripción
136.	Compruebe que en el directorio “C:\Scripts” se encuentran al menos los siguientes directorios y ficheros: – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.ps1 – CCN-STIC-599A19 Cliente Miembro - Paso 1 - Caracteristicas.bat – CCN-STIC-599A19 Cliente Miembro - Paso 2 - SCE.bat – CCN-STIC-599A19 Cliente Miembro - Paso 3a - IPv6 netbios y otros - LTSC.bat – CCN-STIC-599A19 Cliente Miembro - Paso 4 - Firewall.bat – CCN-STIC-599A19 Cliente Miembro - Paso 5a - Deshabilita Appx - LTSC.bat – CCN-STIC-599A19 Cliente Miembro.wfw – CCN-STIC-599A19_Deshabilita_NetBIOS_sobre_TCPIP.ps1 – CCN-STIC-599A19_Desinstala_Appx_LTSC.ps1 – CCN-STIC-599A19_Desinstala_caracteristicas.ps1 – CCN-STIC-599A19_No_IPv6.reg – drwatson.reg – posix.reg – refusereset.reg – sceregl.inf – ssdp.reg
137.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - 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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

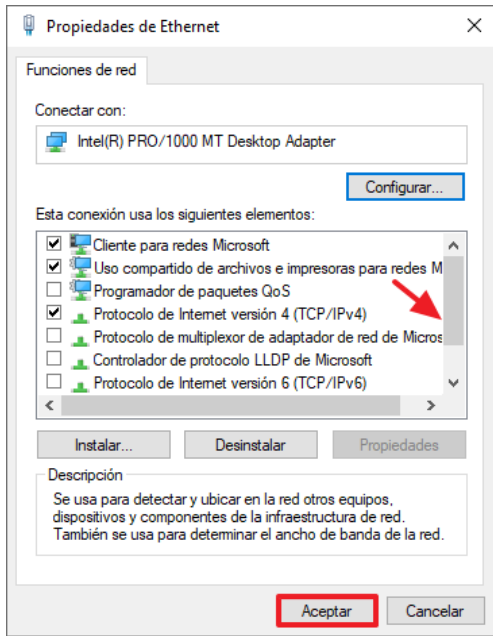
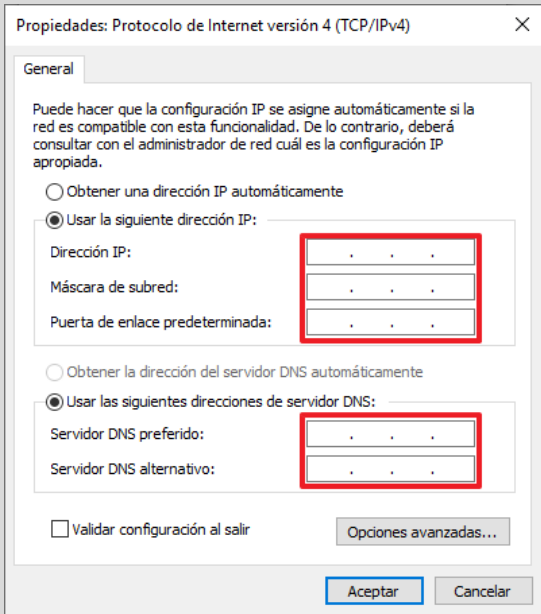
Paso	Descripción
138.	Pulse “S” en la ventana de “Control de cuentas de usuario”. 
139.	Este script deshabilitará todas las características opcionales que se encuentren habilitadas en el equipo. Pulse una tecla para continuar el proceso. 
140.	El sistema mostrará una lista de las características instaladas que no son necesarias y que deberán ser eliminadas. Pulse una tecla para continuar con el proceso de eliminación de las características. 

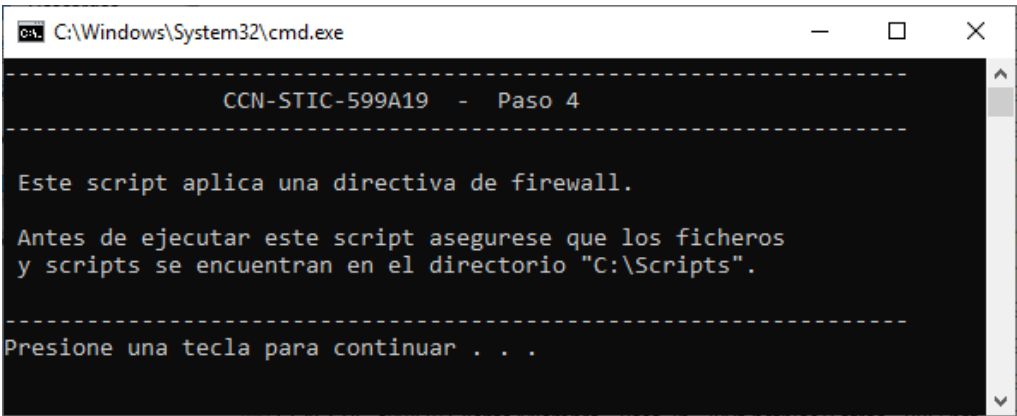
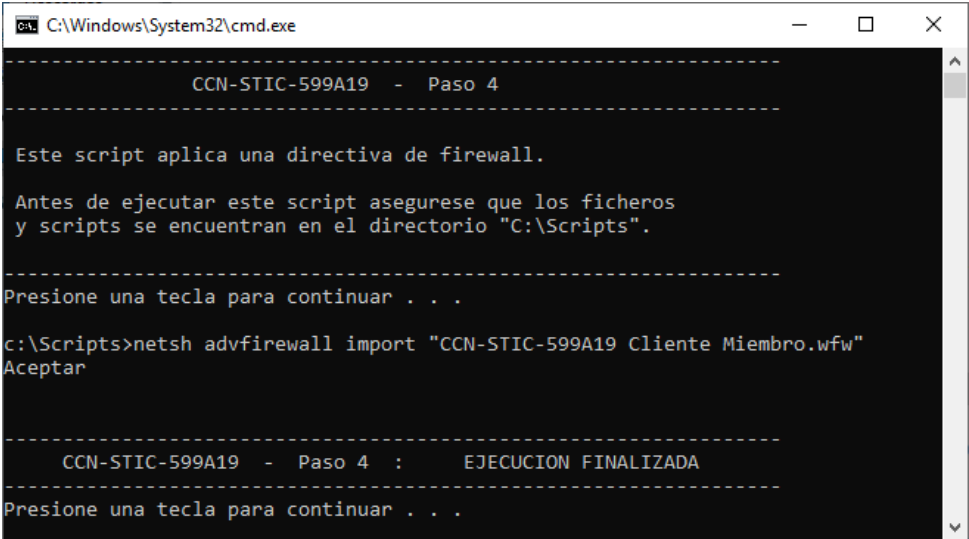
Paso	Descripción
141.	Una vez desinstaladas las características innecesarias compruebe que únicamente se mantienen instaladas las características “Internet-Explorer-Optional-amd64” y “Microsoft-Windows-NetFx4-US-OC-Package”, que son necesarias para la funcionalidad del cliente Windows 10.  Nota: Si apareciese 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.
142.	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. 

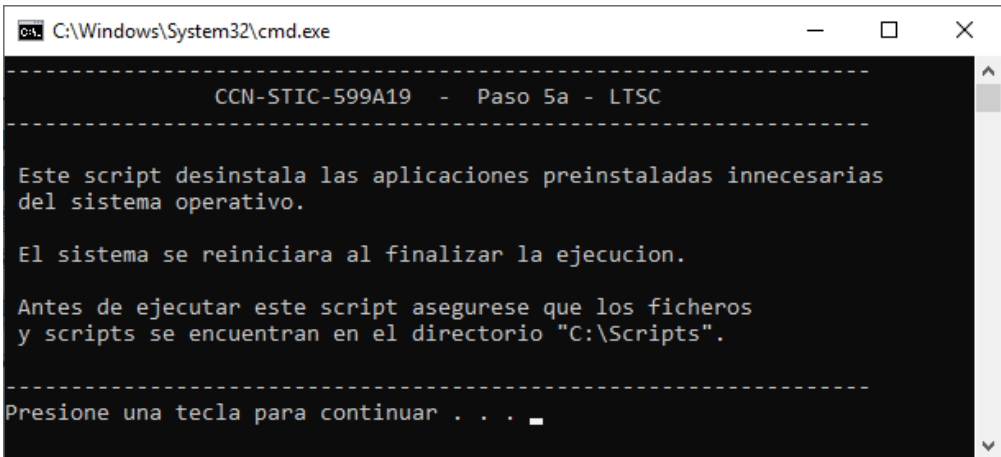
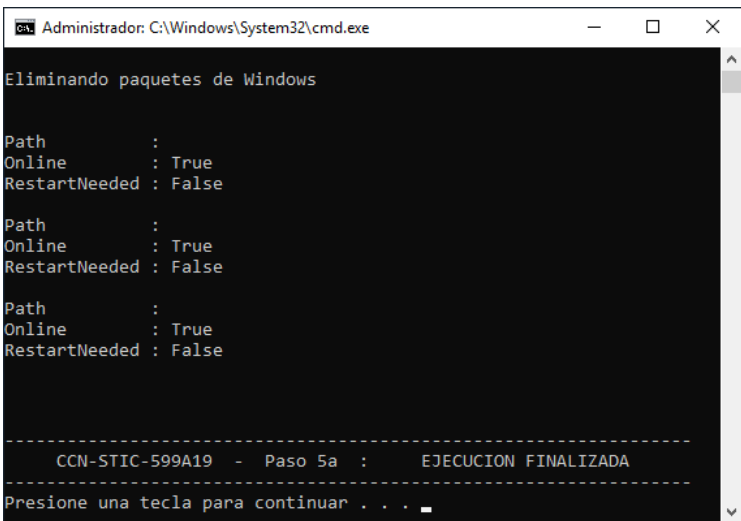
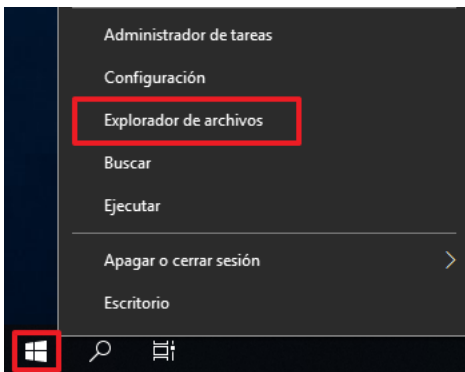
Paso	Descripción
143.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 2 - SCE.bat" situado en la carpeta "C:\Scripts" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 
144.	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 sale el aviso "No se pudo encontrar "C:\Windows\inf\sceregvl.inf.orig", este aviso se puede ignorar. Sólo se debe a que no se encontró una copia de seguridad anterior del fichero "sceregvl.inf". No representa ningún problema y se puede continuar con el siguiente paso.

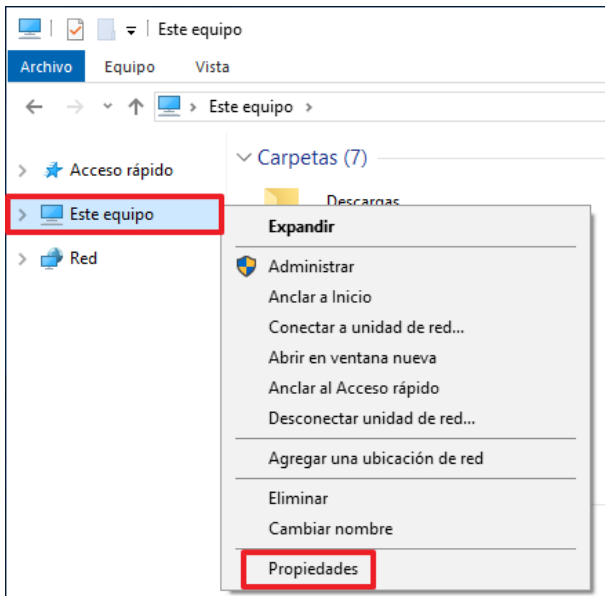
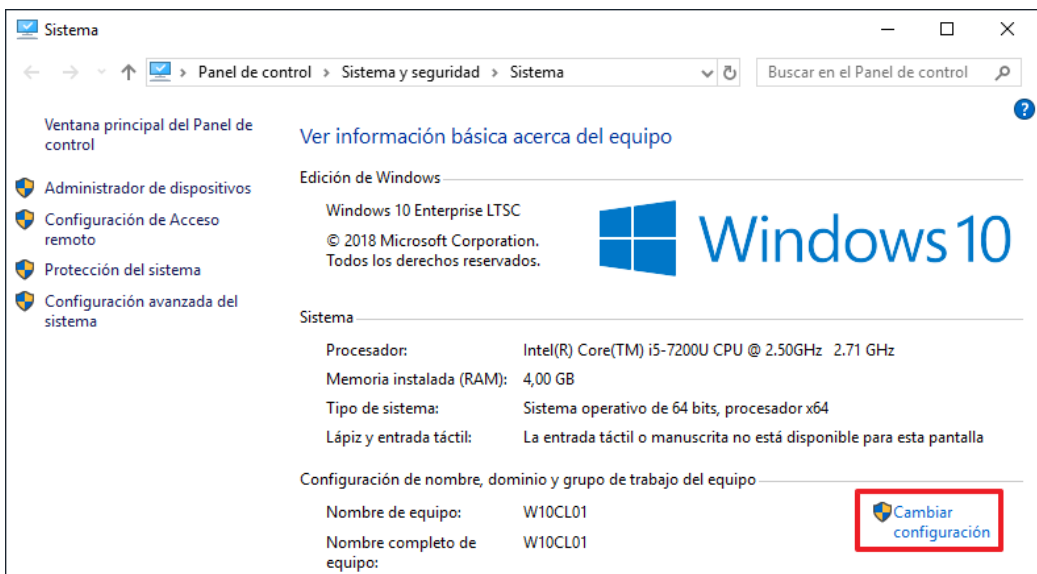
Paso	Descripción
145.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 3a – Ipv6 netbios y otros - LTSC.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 
146.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 
147.	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". 

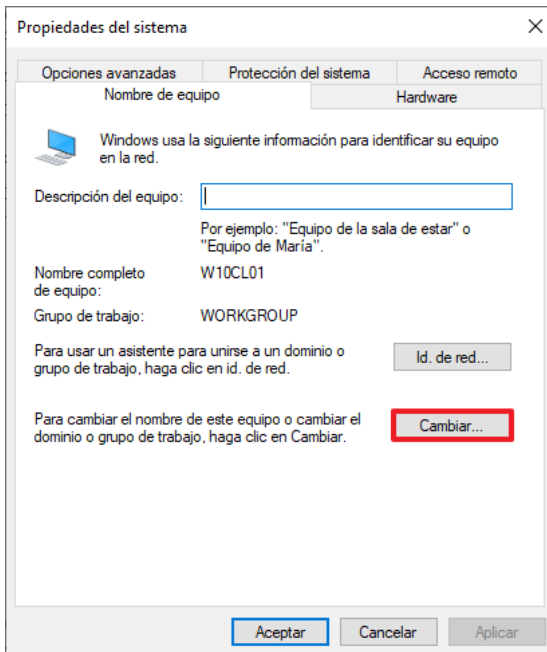
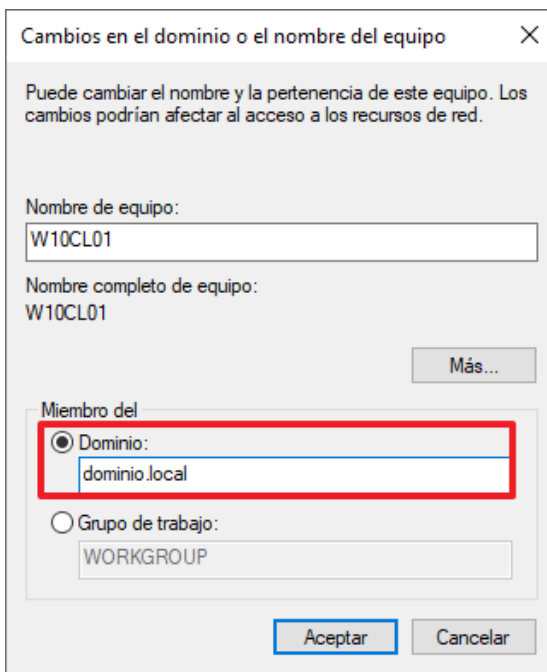
Paso	Descripción
148.	En la ventana de configuración seleccione la opción “Cambiar opciones del adaptador”. 
149.	Pulse con el botón derecho sobre el adaptador de red y seleccione “Propiedades”. 

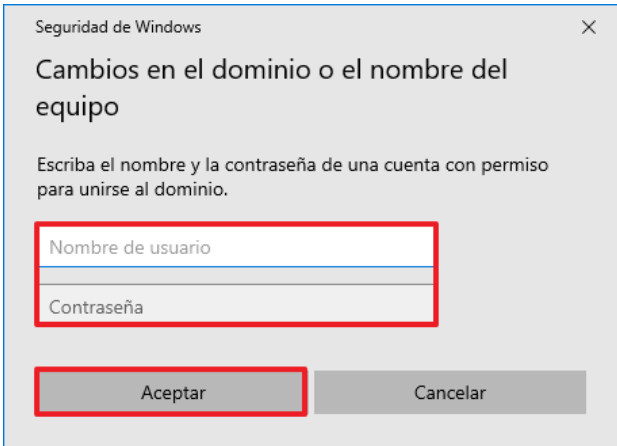
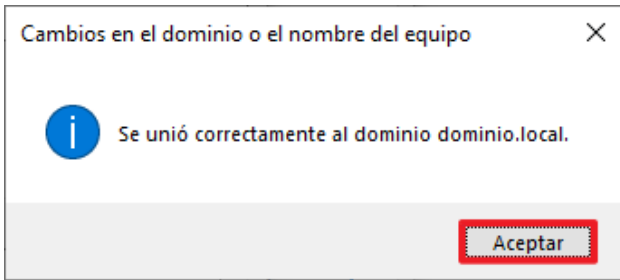
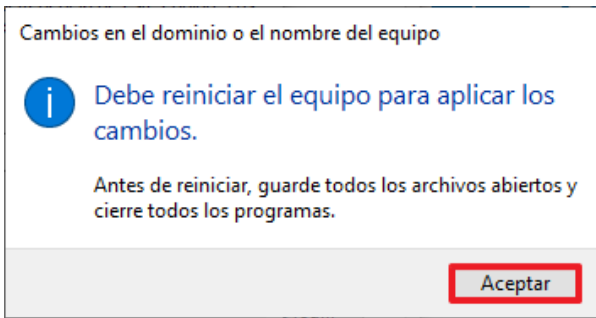
Paso	Descripción
150.	En la ventana “Propiedades de Ethernet” de las diferentes conexiones de red, desmarque si están marcados todos los elementos excepto "Cliente para redes Microsoft", “Uso compartido de archivos e impresoras para redes Microsoft” y “Protocolo de Internet versión 4 (TCP/IPv4)” como se muestra en la siguiente figura.  Nota: Recuerde hacer uso de la barra lateral para mostrar y deshabilitar todos los elementos.
151.	Pulse el botón "Aceptar", para cerrar la ventana guardando los cambios. Nota: Si no lo hizo antes, configure correctamente los parámetros de red (Protocolo de Internet versión 4), especialmente la dirección IP del equipo, de la puerta de enlace predeterminada y del servidor de DNS, ya sean fijas o para obtener automáticamente por DHCP, de modo que el equipo pueda posteriormente contactar con un controlador del dominio al que se unirá. 

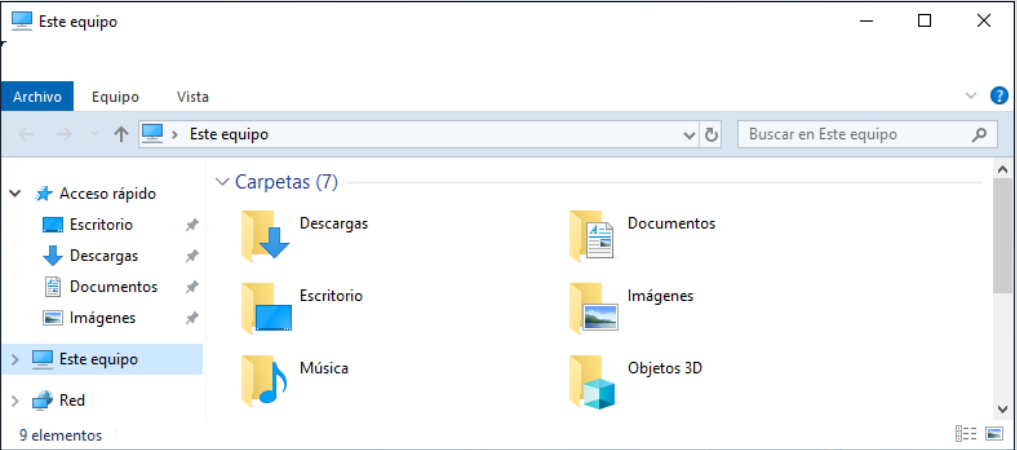
Paso	Descripción
152.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 4 – firewall.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: A pesar de que en pasos anteriores se configuró la directiva de Firewall a través del "Administrador de directivas de grupo" y a través de la política "CCN-STIC-599A19 Windows 10 - Equipos", en este punto se realiza localmente la importación de algunas directivas específicas de Windows 10 que no son compatibles con el "Firewall de Windows con seguridad avanzada de Windows Server 2016. De modo que las reglas de entrada y salida queden correcta y completamente configuradas.
153.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 

Paso	Descripción
154.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 5a – Deshabilita appx - LTSC.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 
155.	De nuevo, pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comandos. 
156.	A continuación, se unirá el equipo al dominio. Para ello, en la barra de tareas, pulse sobre "Inicio" con el botón derecho y seleccione "Explorador de archivos". 

Paso	Descripción
157.	En el “Explorador de archivos” pulse con el botón derecho del ratón sobre “Este equipo” y seleccione “Propiedades”. 
158.	Localice en la ventana “Ver información básica acerca del equipo” el apartado “Configuración de nombre, dominio y grupo de trabajo del equipo” y pulse sobre “Cambiar configuración”. 

Paso	Descripción
159.	En “Propiedades del sistema”, en la pestaña “Nombre de equipo”, pulse sobre “Cambiar”. 
160.	Marque la opción “Dominio”, introduzca el nombre del dominio y pulse “Aceptar”.  Nota: En el ejemplo, el dominio se denomina “dominio.local”.

Paso	Descripción
161.	Introduzca credenciales de administrador del dominio cuando el sistema se lo solicite y pulse “Aceptar” 
162.	Pulse “Aceptar” en el mensaje de confirmación de unión al dominio. 
163.	El sistema deberá reiniciar para guardar los cambios. Pulse “Aceptar” en la ventana de “Cambios en el dominio o el nombre de equipo”. 
164.	Pulse “Cerrar” en “Propiedades del sistema” y “Reiniciar ahora” para que se reinicie el equipo y hagan efecto los cambios.

Paso	Descripción
165.	Una vez haya reiniciado el sistema, inicie sesión con una cuenta con privilegios de administración en el dominio. Nota: Es posible que en el primer inicio de sesión después de unir el equipo a dominio, el sistema operativo contenga errores visuales en el explorador de archivos. Si es el caso, reinicie el equipo nuevamente. 
166.	Deberá aplicar este momento la guía CCN-STIC-520 – Internet Explorer 11. Para ello, lleve a cabo la implementación del Anexo A, del paso 1 al 51. No es necesario que continúe con el resto de pasos. El resto de pasos de dicho anexo instalaría Internet Explorer 11 en el cliente y esto no es necesario ya que Internet Explorer 11 es el navegador existente en Windows 10. Nota: Las GPO que se han implementado a través de la presente guía no incluyen plantillas administrativas de Internet Explorer. Por tanto, para poder hacer uso seguro de Internet Explorer 11 será necesario aplicar, adicionalmente, la guía CCN-STIC-520 – Internet Explorer 11.
167.	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 Microsoft Windows 10 Enterprise LTSC (versión 1809), que el equipo es un cliente miembro de un dominio Windows, que en los controladores del dominio al que pertenece se ha aplicado la configuración expuesta en la guía CCN-STIC-570A (controladores Microsoft Windows Server 2016), y que en el equipo cliente se ha aplicado la configuración expuesta en la presente guía.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador del dominio, con una cuenta de usuario que tenga permisos de administración en el dominio. En esa primera fase se realizarán las comprobaciones comunes a todos los equipos cliente Windows 10 (versión 1809) miembros del dominio.

Posteriormente, deberá realizar una serie de comprobaciones en el propio equipo cliente miembro del dominio. Para ello, necesitará ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario del dominio que sea administrador local del servidor y que sea miembro del grupo global "Usuarios de shells". Por ejemplo, los usuarios del grupo "Admins. del dominio" cumplirán ambas condiciones.

Para poder verificar que la configuración de usuario, además de la configuración de equipo, está siendo aplicada correctamente en el equipo cliente Windows 10, necesitará que el usuario con el que realice las comprobaciones resida, aunque sea temporalmente, en la siguiente unidad organizativa de Active Directory.

"<Nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10"

Nota: 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).

1. COMPROBACIONES EN SERVIDOR CONTROLADOR DEL DOMINIO

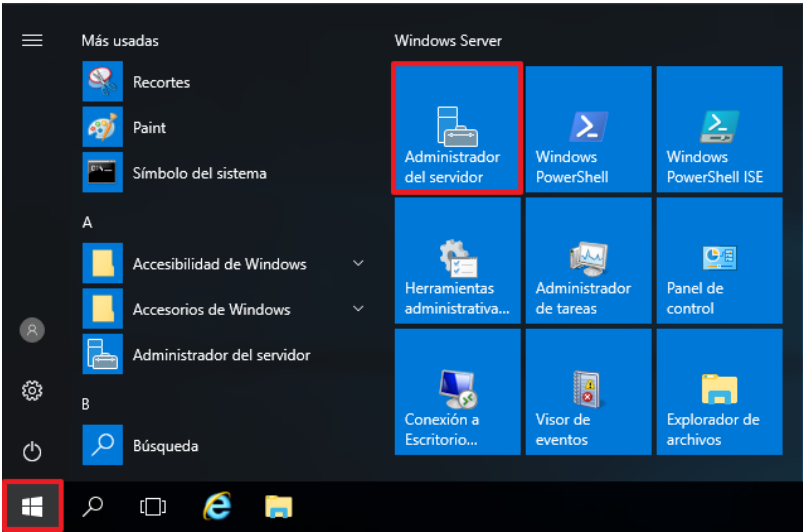
Para realizar algunas de las comprobaciones necesitará ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán en el controlador de dominio son las siguientes:

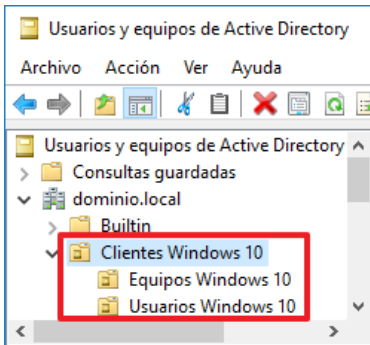
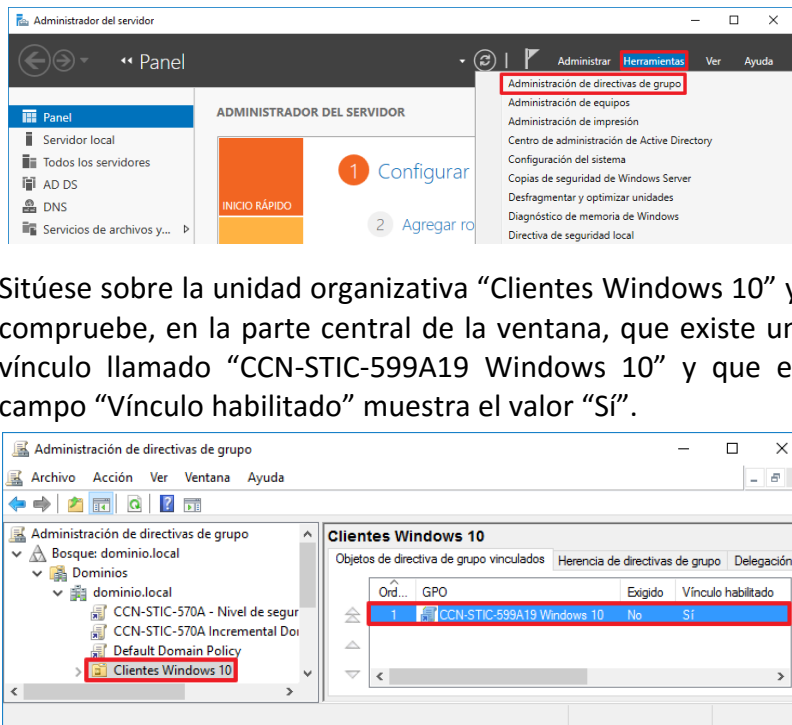
- Administrador del servidor
- Servicios de dominio de Active Directory
- Administración de directivas de grupo
- Editor de administración de directivas de grupo
- Usuarios y equipos de Active Directory

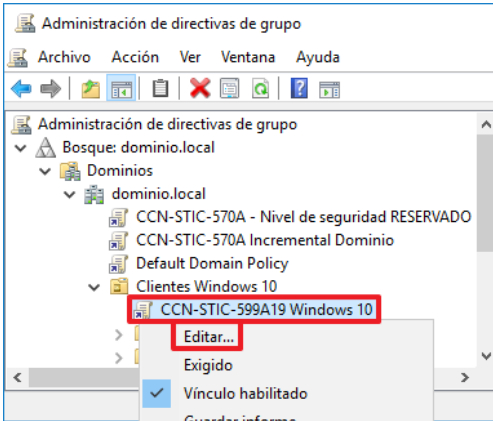
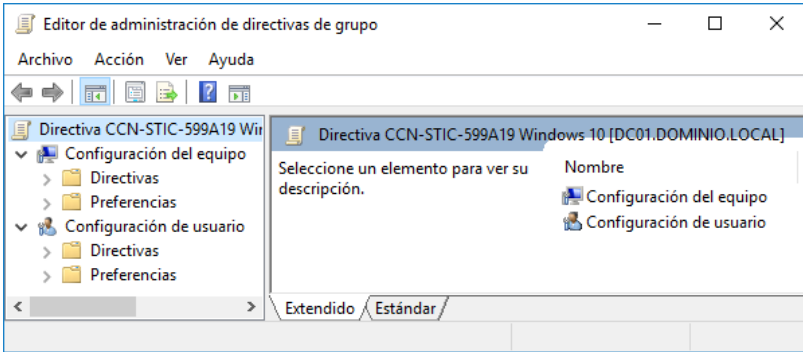
Ejecute los siguientes pasos en un controlador del dominio al que pertenece el equipo a comprobar:

Nota: Las configuraciones y capturas se han realizado a partir de un controlador de dominio Microsoft Windows Server 2016 al que se le ha aplicado la guía CCN-STIC-570A. Salvo que se especifique, los procedimientos y comprobaciones no varían con respecto a la guía CCN-STIC-560A.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio		Inicie sesión en el servidor, utilizando una cuenta de usuario perteneciente al grupo de administradores del dominio ("Admins. del dominio").

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que están creadas las unidades organizativas necesarias		Ejecute el "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Introduzca las credenciales de un usuario con permisos de administración del dominio, pulse sobre el menú superior en "Herramientas" y seleccione "Usuarios y equipos de Active Directory". 

Comprobación	OK/NOK	Cómo hacerlo
		Despliegue los objetos y compruebe que bajo el objeto con el nombre del dominio existe una unidad organizativa llamada "Clientes Windows 10" y bajo ésta dos unidades organizativas, al mismo nivel, llamadas "Equipos Windows 10" y "Usuarios Windows 10", como se muestra en la siguiente figura.  Nota: Si en su entorno las unidades organizativas elegidas para albergar las configuraciones de equipos cliente miembro Windows 10 fueran otras, deberá sustituir en esta lista de comprobación todas las referencias a dichas unidades organizativas por referencias a las unidades organizativas de su entorno.
3. Verifique que está creada y asignada correctamente la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando, de nuevo, la herramienta "Administrador del servidor" seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo".  Sitúese sobre la unidad organizativa "Clientes Windows 10" y compruebe, en la parte central de la ventana, que existe un vínculo llamado "CCN-STIC-599A19 Windows 10" y que el campo "Vínculo habilitado" muestra el valor "Sí".

Comprobación	OK/NOK	Cómo hacerlo
4. Abra la directiva GPO "CCN-STIC-599A19 Windows 10" en el editor de administración de directivas de grupo		Marque con el botón derecho el vínculo de la GPO "CCN-STIC-599A19 Windows 10" situado en el siguiente contenedor de la herramienta "Administrador del servidor": "Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>" En el menú contextual que aparecerá, seleccione la opción "Editar...", como se muestra en la figura.  Con ello se abrirá el Editor de administración de directivas de grupo, mostrando la configuración de la GPO "CCN-STIC-599A19 Windows 10".  En los próximos pasos y hasta que se indique lo contrario, verificará la configuración de este GPO utilizando esta ventana del editor de administración de directivas de grupo
5. Verifique los valores de la directiva de auditoría cuenta de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de las directivas de auditoría: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → 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	
6. Verifique los valores de Asignación de derechos de usuario de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de las directivas de asignación de derechos de usuario: Nota: En las cuentas de dominio, resaltadas con fondo gris en la siguiente tabla, aparecerá su nombre de dominio en lugar de "DOMINIO". Además, tenga en cuenta que tanto la cuenta Administrador como la cuenta Invitado estarán renombradas, y aparecerán con su nuevo nombre en el editor. "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → 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		DOMINIO\Auditores, 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		

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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	
Denegar el acceso a este equipo desde la red		Invitados, ANONYMOUS LOGON, DOMINIO\acCdCmN570	
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)	
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)	
Realizar tareas de mantenimiento del volumen		Administradores	

Comprobación	OK/NOK	Cómo hacerlo
Directiva		Valor
Reemplazar un símbolo (token) de nivel de proceso		Servicio de red, SERVICIO LOCAL
Restaurar archivos y directorios		Administradores
Tener acceso a este equipo desde la red		Administradores, Usuarios
Tomar posesión de archivos y otros objetos		Administradores
7. Verifique los valores de Opciones de seguridad de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de las opciones de seguridad: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad"
Directiva		Valor
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)

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos		Habilitada	
Acceso a redes: rutas del Registro accesibles remotamente		System ¹ \CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\ServerApplications, Software\Microsoft\Windows NT\CurrentVersion	
Acceso a redes: rutas y subrutas del Registro accesibles remotamente		System ² \CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, 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: 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	

¹ En este caso "System" hace referencia a HKEY_LOCAL_MACHINE\System, y "Software" a HKEY_LOCAL_MACHINE\Software.

² 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: 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: (NtfsDisable8dot3NameCreatio n) 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: (TcpMaxConnectResponseRetr ansmissions) 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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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)	
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 con ellas	
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) <i>Equivale a:</i> <i>Usuarios autenticados: Permitir Acceso local y Acceso remoto</i>	
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) <i>Equivale a:</i> <i>Usuarios autenticados: Permitir Ejecución local y Activación local.</i> <i>Administradores: Permitir Ejecución local, Ejecución remota, Activación local y Activación remota.</i>	
Dispositivos: impedir que los usuarios instalen controladores de impresora		Habilitada	
Dispositivos: permitir desacoplamiento sin tener que iniciar sesión		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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: 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: 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: 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	
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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	
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 los valores del registro de eventos de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Registro de eventos: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos"	
	Directiva	Valor	OK/NOK
	Método de retención del registro de la aplicación	Según se necesite	
	Método de retención del registro de seguridad	Según se necesite	
	Método de retención del registro del sistema	Según se necesite	
	Tamaño máximo del registro de la aplicación	32768 kilobytes	
	Tamaño máximo del registro de seguridad	163840 kilobytes	
	Tamaño máximo del registro del sistema	32768 kilobytes	
9. Verifique los valores de Grupos restringidos de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Grupos restringidos"	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Usuarios avanzados	Vacío (este grupo no debe contener miembros)	
		Nota: En lugar del nombre puede aparecer el identificador numérico "*S-1-5-32-547" .		
		Usuarios de escritorio remoto	Vacío (este grupo no debe contener miembros)	
10.Verifique los valores de los servicios del sistema restringidos de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Servicios del sistema: Nota: 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 del editor de administración de directivas de grupo 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. "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
Administración de aplicaciones	AppMgmt	Deshabilitado	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 acceso remoto	RasMan	Deshabilitado	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	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		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 de NetBIOS sobre TCP/IP	lmhosts	Automático	Configurado		
Aplicación auxiliar IP	iphlpvc	Deshabilitado	Configurado		
Aplicación del sistema COM+	COMSysApp	Deshabilitado	Configurado		
Archivos sin conexión	CscService	Deshabilitado	Configurado		
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Deshabilitado	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Deshabilitado	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		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Deshabilitado	Configurado		
BranchCache	PeerDistSvc	Deshabilitado	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CaptureService	CaptureService	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Carpetas de trabajo	workfoldersvc	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Deshabilitado	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Deshabilitado	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	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		
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	Deshabilitado	Configurado		
Configuración automática de WWAN	WwanSvc	Deshabilitado	Configurado		
Configuración de Escritorio remoto	SessionEnv	Deshabilitado	Configurado		
ConsentUX	ConsentUxUserSvc	Deshabilitado	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Deshabilitado	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Deshabilitado	Configurado		
Copias de seguridad de Windows	SDRSVC	Deshabilitado	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Desencadenadores de Message Queue Server	MSMQTriggers	Deshabilitado	Configurado		
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado		
Detección SSDP	SSDPSRV	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		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
dmwappushsvc	dmwappushservice	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		
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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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	Deshabilitado	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		
OpenSSH SSH Server	sshd	Deshabilitado	Configurado		
Optimización de entrega	DoSvc	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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	Manual	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	wcncsvc	Deshabilitado	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Deshabilitado	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Deshabilitado	Configurado		
Servicio auxiliar de host para aplicaciones	AppHostSvc	Deshabilitado	Configurado		
Servicio AVCTP	BthAvctpSvc	Deshabilitado	Configurado		
Servicio biométrico de Windows	WbioSrv	Deshabilitado	Configurado		
Servicio Cifrado de unidad BitLocker	BDESVC	Deshabilitado	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	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 administración de Windows	WManSvc	Deshabilitado	Configurado		
Servicio de administración IIS	IISADMIN	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	wlpcsvc	Deshabilitado	Configurado		
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado		
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado		
Servicio de cierre de invitado de Hyper-V	vmicshutdow	Deshabilitado	Configurado		
Servicio de cliente de protección de host	HgClientService	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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 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	
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	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de instalación de dispositivos	DeviceInstall	Manual	Configurado		
Servicio de instalación de Microsoft Store	InstallService	Deshabilitado	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 Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	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 Protección contra amenazas avanzada de Windows Defender	Sense	Deshabilitado	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Deshabilitado	Configurado		
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado		
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Deshabilitado	Configurado		
Servicio de publicación World Wide Web	W3SVC	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 host	hns	Deshabilitado	Configurado		
Servicio de red de Xbox Live	XboxNetApiSvc	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		
Servicio de usuario de difusión y GameDVR	BcastDVRUserService	Deshabilitado	Configurado		
Servicio de usuario de notificaciones de inserción de Windows	WpnUserService	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de usuario del portapapeles	cbdhsvc	Deshabilitado	Configurado		
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Deshabilitado	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Deshabilitado	Configurado		
Servicio de Windows Defender	WinDefend	Deshabilitado	Configurado		
Servicio de Windows Insider	wisvc	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 FrameServer de la Cámara de Windows	FrameServer	Deshabilitado	Configurado		
Servicio FTP de Microsoft	ftpsvc	Deshabilitado	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	Deshabilitado	Configurado		
Servicio MultiPoint	Wms	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio telefónico	PhoneSvc	Deshabilitado	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Deshabilitado	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Deshabilitado	Configurado		
Servicios simples de TCP/IP	simptcp	Deshabilitado	Configurado		
Servidor	LanmanServer	Deshabilitado	Configurado		
Servidor de roles de DS	DsRoleSvc	Deshabilitado	Configurado		
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		
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	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		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	wuauerv	Deshabilitado	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Deshabilitado	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	
11.Verifique los valores de Registro de la directiva "CCN-STIC-599A19 Windows 10"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Registro: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro"			
	Directiva	Valor	OK/NOK	
	MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	Administradores: Control Total SYSTEM: Control Total Usuarios: Leer		
	MACHINE\SYSTEM\CurrentControlSet\Enum	Administradores: Control Total Usuarios autenticados: Leer		

Comprobación	OK/NOK	Cómo hacerlo		
12.Verifique los valores de Sistema de archivos de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Sistema de archivos: Nota: Para verificar los permisos de cada fichero o carpeta deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos"		
Archivo		Usuario	Permiso	OK/NOK
%Public%		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%SystemDrive%\		Administradores	Control Total	
		CREATOR OWNER	Permisos especiales ³	
		SYSTEM	Control Total	
		Usuarios	Leer	
%SystemDrive%\Users\Default		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%SystemRoot%\regedit.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\Registration		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%SystemRoot%\security		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\arp.exe		Administradores	Control Total	
		SYSTEM	Control Total	

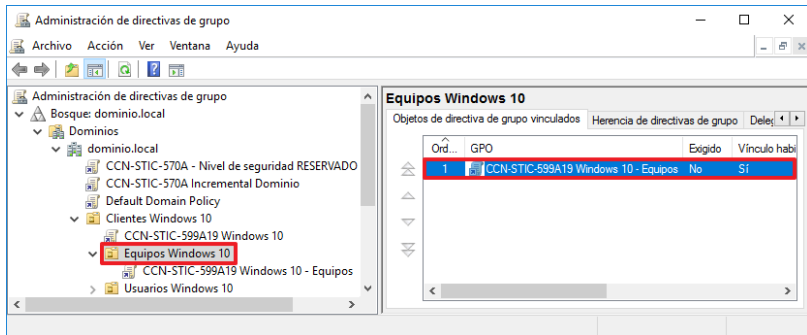
³ Los permisos especiales que se establecerán para el creador de los objetos %SystemDrive% serán de Control Total pero aplicados a "Sólo subcarpetas y archivos" en lugar de aplicarlos a "Esta carpeta, subcarpeta y archivos".

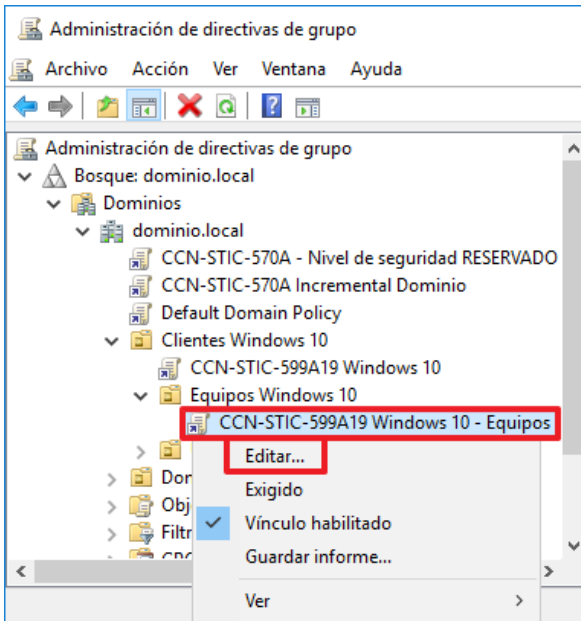
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\at.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\azuresettingsyncprovider.dll	Administradores	Control Total		
%SystemRoot%\system32\bash.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\cacls.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\chatapis.dll	Administradores	Control Total		
%SystemRoot%\system32\clip.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%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\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		
%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		

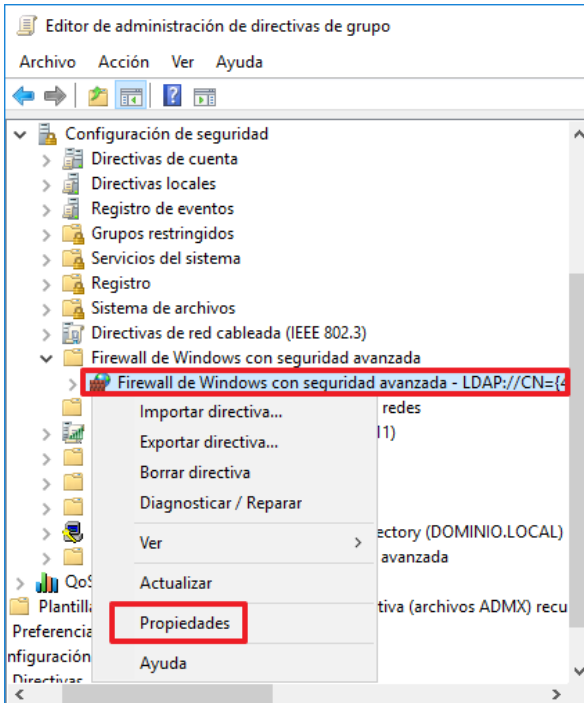
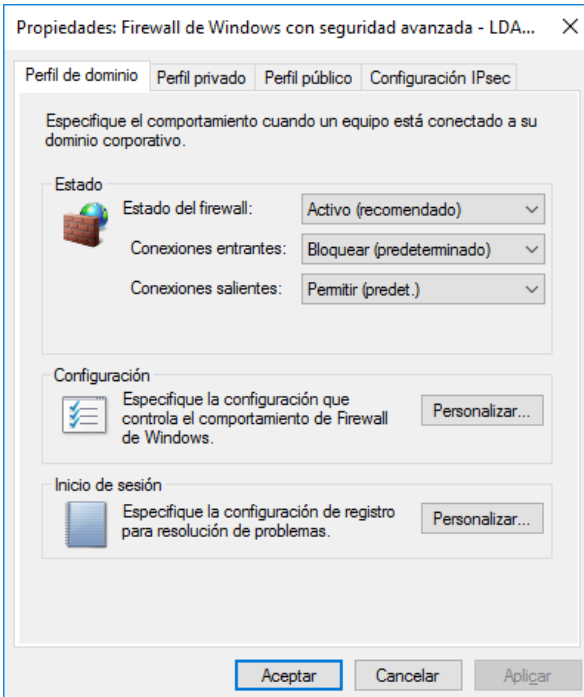
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\nfsadmin.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nslookup.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\phonecallhistoryapis.dll		Administradores	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\rasctnm.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	
%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\telnet.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\tftp.exe		Administradores	Control Total	
		SYSTEM	Control Total	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%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	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%\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	Leer y Ejecutar, Listar el contenido de la carpeta, Leer		
%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		

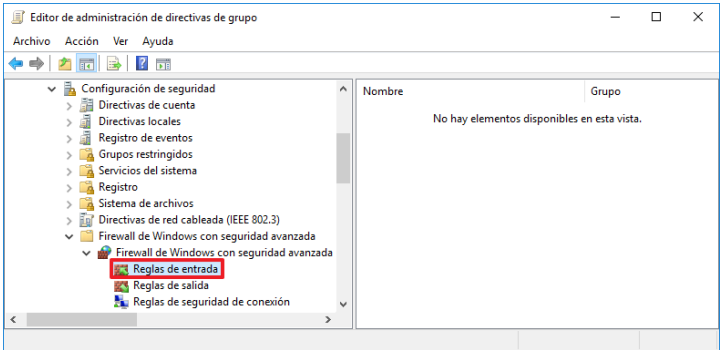
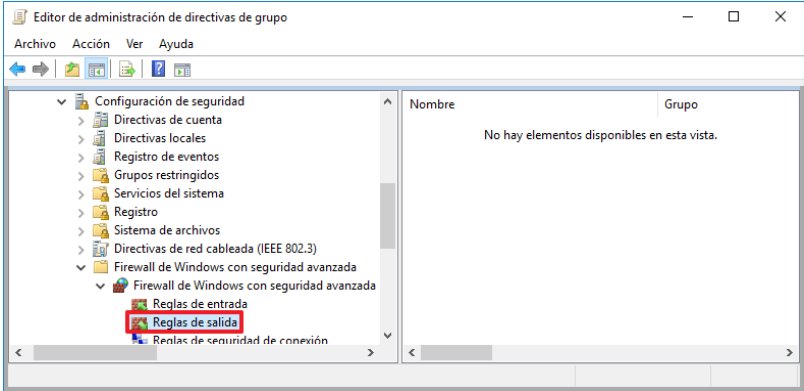
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\ipconfig.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\syswow64\net.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\syswow64\netstat.exe		Administradores	Control 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	
%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	

Comprobación		OK/NOK	Cómo hacerlo										
Archivo			Usuario	Permiso	OK/NOK								
%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									
%SystemRoot%\syswow64\wscript.exe			Administradores	Control Total									
			SYSTEM	Control Total									
%SystemRoot%\syswow64\xcopy.exe			Administradores	Control Total									
			SYSTEM	Control Total									
13.Finalice la comprobación de la directiva “CCN-STIC-599A19 Windows 10”			Cierre la ventana del "Editor de administración de directivas de grupo" que tenía abierta con la directiva "CCN-STIC-599A19 Windows 10"										
14.Verifique que está creada y asignada correctamente la directiva “CCN-STIC-599A19 Windows 10 - Equipos”			De nuevo en la consola de “Administración de directivas de grupo” diríjase a la siguiente unidad organizativa: Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10", y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que existe un vínculo llamado "CCN-STIC-599A19 Windows 10 - Equipos". <table><thead><tr><th>Ord...</th><th>GPO</th><th>Exigido</th><th>Vínculo habi</th></tr></thead><tbody><tr><td>1</td><td>CCN-STIC-599A19 Windows 10 - Equipos</td><td>No</td><td>Sí</td></tr></tbody></table> Compruebe también en el mismo sitio que el campo "Vínculo habilitado" muestra "Sí" para la GPO "CCN-STIC-599A19 Windows 10 - Equipos".			Ord...	GPO	Exigido	Vínculo habi	1	CCN-STIC-599A19 Windows 10 - Equipos	No	Sí
Ord...	GPO	Exigido	Vínculo habi										
1	CCN-STIC-599A19 Windows 10 - Equipos	No	Sí										

Comprobación	OK/NOK	Cómo hacerlo
15. Abra la directiva de equipos cliente miembro Windows 10 (CCN-STIC-599A19 Windows 10 - Equipos) en el editor de administración de directivas de grupo		Marque con el botón derecho el vínculo de la GPO "CCN-STIC-599A19 Windows 10 - Equipos" situado en el siguiente contenedor: "Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10" En el menú contextual que aparecerá, seleccione la opción "Editar...", como se muestra en la figura. 
16. Verifique la configuración general de Firewall de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los valores que se indicarán a continuación en la siguiente ubicación. "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada - LDAP://CN={SID}, CN=POLICIES, CN=SYSTEM, DC=<DOMINIO>, DC=LOCAL"

Comprobación	OK/NOK	Cómo hacerlo
		Abra la ventana de propiedades de dicho contenedor: márkuelo con el botón derecho del ratón y elija la opción "Propiedades" del menú contextual que aparecerá.  La siguiente figura muestra la ventana de propiedades, concretamente con la pestaña "Perfil de dominio" activa.  En la pestaña "Perfil de dominio", comprobar que los valores configurados son los siguientes:

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Estado del firewall	Activo (recomendado)	
		Conexiones entrantes	Bloquear (predeterminado)	
		Conexiones salientes	Permitir (predet.)	
		En la misma pestaña, marque el botón "Personalizar..." dentro del apartado "Configuración" para abrir la ventana "Personalizar la configuración de Perfil de dominio", como la que se muestra en la figura.		
		Personalizar la configuración de Perfil de dominio Especifique la configuración para controlar el comportamiento de Firewall de Windows con seguridad avanzada. Configuración del firewall Muestra notificaciones al usuario cuando se bloquea la recepción de conexiones entrantes para un programa. Mostrar una notificación: No Respuesta de unidifusión Permitir respuesta de unidifusión para multidifusión o difusión del tráfico de red. Permitir respuesta de unidifusión: Sí (predeterminado) Combinación de reglas Permite combinar las reglas creadas por administradores locales con reglas distribuidas con la directiva de grupo. Esta configuración solo se puede aplicar con la directiva de grupo. Aplicar reglas de firewall local: No Aplicar reglas de seguridad de conexión local: No Aceptar Cancelar		
		En esta ventana de configuración, compruebe que los valores configurados son los siguientes:		
		Directiva	Valor	OK/NOK
		Mostrar una notificación	No	
		Permitir respuesta de unidifusión	Sí (predeterminado)	
		Aplicar reglas de firewall local	No	
		Aplicar reglas de seguridad de conexión local	No	
		Repita, para cada uno de los otros dos perfiles: "Perfil privado" y "Perfil público", todas las comprobaciones de este paso recién realizadas sobre el "Perfil de dominio". La configuración debe ser idéntica.		

Comprobación	OK/NOK	Cómo hacerlo
17. Verifique las Reglas de entrada de la configuración de Firewall de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada - LDAP://CN={SID}, CN=POLICIES, CN=SYSTEM, DC=<DOMINIO>, DC=LOCAL \ Reglas de entrada" Seleccione dicho contenedor, y en la parte central de la ventana compruebe que no existe ninguna regla. 
18. Verifique las Reglas de salida de la configuración de Firewall de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de: "Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada - LDAP://CN={SID}, CN=POLICIES, CN=SYSTEM, DC=<DOMINIO>, DC=LOCAL → Reglas de salida" Seleccione dicho contenedor, y en la parte central de la ventana compruebe que no existe ninguna regla. 

Comprobación	OK/NOK	Cómo hacerlo		
19. Verifique los valores de "Administración de derechos digitales de Windows Media" de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
20. Verifique los valores del cliente WinRM de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
21. Verifique los valores del servicio WinRM de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
22. Verifique los valores para agregar características de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10"		
	Directiva		Valor	OK/NOK
	Impedir que el asistente se ejecute		Habilitada	
23. Verifique los valores del almacén digital de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Almacén digital"		
	Directiva		Valor	OK/NOK
	No permitir que se ejecute el Almacén digital		Habilitada	
24. Verifique los valores del análisis de confiabilidad de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Análisis de confiabilidad de Windows"		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar proveedores de WMI de confiabilidad	Habilitada	
25. Verifique los valores de Windows Ink de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
26. Verifique los valores de asistencia en línea de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Asistencia en línea"		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitada	
27. Verifique los valores de biometría de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Biometría"		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
28. Verifique los valores de búsqueda de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
		Impedir que los clientes soliciten el índice de forma remota	Habilitada	
29. Verifique los valores de cámara de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cámara"		
		Directiva	Valor	OK/NOK
		Permitir el uso de la cámara	Deshabilitada	
30. Verifique los valores del centro de movilidad de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows"		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	
31. Verifique los valores del centro de seguridad de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Centro de seguridad"		
		Directiva	Valor	OK/NOK
		Activar el Centro de seguridad (solo equipos de dominio)	Deshabilitada	
32. Verifique los valores de la compatibilidad de aplicaciones de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
33. Verifique los valores de la configuración de conectar de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
34. Verifique los valores de la configuración de presentación de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Configuración de presentación"		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
35. Verifique los valores de Contenido de la nube de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
36. Verifique los valores de las directivas de reproducción automática de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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 la ejecución automática	Habilitada, (No ejecutar ningún comando de ejecución automática)	
		Evitar que reproducción automática recuerde las elecciones del usuario	Habilitada	
37. Verifique los valores de las directivas del explorador de Archivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
38. Verifique los valores de las directivas de las versiones anteriores del explorador de Archivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
39. Verifique los valores de las directivas del explorador de juegos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
40. Verifique los valores de las fuentes RSS de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Fuentes RSS"		
		Directiva	Valor	OK/NOK
		Desactivar la descarga de información sobre juegos	Habilitada	

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	
41. Verifique los valores de la grabación y difusión de juegos de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
42. Verifique los valores de la grabadora de sonidos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos"		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute la grabadora de sonidos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
43. Verifique los valores del grupo en el hogar de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
44. Verifique los valores de paquete de aplicación de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
45. Verifique los valores del informe de errores de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	Habilitada	
		No enviar datos adicionales	Habilitada	
46. Verifique los valores de la interfaz de usuario de credenciales de la directiva "CCN-STIC-599A19 Windows 10-Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	Habilitada	
47. Verifique los valores de Mapas de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
48. Verifique los valores de MDM de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → MDM"		
		Directiva	Valor	OK/NOK
		Deshabilitar la inscripción de MDM	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
49. Verifique los valores de Mensajería de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Mensajería"		
		Directiva	Valor	OK/NOK
		Permitir la sincronización en la nube del servicio de mensajería	Deshabilitada	
50. Verifique los valores de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → NetMeeting"		
		Directiva	Valor	OK/NOK
		Deshabilitar el uso compartido de escritorio remoto	Habilitada	
51. Verifique los valores de las opciones de One Drive de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive"		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
52. Verifique los valores de las opciones de inicio de sesión de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
53. Verifique los valores de la plataforma de protección de software de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Plataforma de protección de software"		
		Directiva	Valor	OK/NOK
		Controlar la reactivación de dispositivos comerciales	Habilitada	
		Desactivar validación AVS en línea del cliente KMS	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
54. Verifique los valores de Privacidad de aplicación de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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 (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 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 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)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows se sincronicen con dispositivos	Habilitada (Forzar denegación)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitada (Forzar denegación)	
55. Verifique los valores del Programa para la mejora de la experiencia de usuario de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
56. Verifique los valores de Recopilación de datos y versiones preliminares de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Recopilación de datos y versiones preliminares"		
		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])	

Comprobación	OK/NOK	Cómo hacerlo		
57. Verifique los valores del cliente de conexión a escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
58. Verifique los valores de las conexiones de Host de sesión de Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
59. Verifique los valores de la redirección de dispositivos o recursos de Host de sesión de Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
60. Verifique los valores de la seguridad de Host de sesión de Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Seguridad"		
		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	
61. Verifique los valores del Shell remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Shell Remoto de Windows"		

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	
62. Verifique los valores para Sincronizar la configuración de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Sincronizar la configuración"		
		Directiva	Valor	OK/NOK
		No sincronizar	Habilitada, (Permitir a los usuarios activar la sincronización: Deshabilitado)	
63. Verifique los valores de Accesorios de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tablet PC → Accesorios"		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute Windows Journal	Habilitada	
64. Verifique los valores de Tarjeta inteligente de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
65. Verifique los valores de la tienda de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tienda"		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitada	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitada	
66. Verifique los valores de ubicación y sensores de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores"		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
67. Verifique los valores de Servicio de localización de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
68. Verifique los valores de virtualización de la experiencia del usuario de Microsoft de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
69. Verifique los valores de Windows Hello de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Hello para empresas"		
		Directiva	Valor	OK/NOK
		Usa Windows Hello para empresas	Deshabilitada	
		Usar biometría	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
70. Verifique los valores de Windows Installer de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
71. Verifique los valores de Windows Mail de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Mail"		
		Directiva	Valor	OK/NOK
		Turn off the communities features	Habilitada	
		Turn off Windows Mail application	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
72. Verifique los valores de Windows Messenger de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
73. Verifique los valores de Windows Update de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update"		
		Directiva	Valor	OK/NOK
		Configurar Actualizaciones automáticas	Deshabilitada	
74. Verifique los valores de Impresoras de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Impresoras"		
		Directiva	Valor	OK/NOK
		Ejecutar controladores de impresión en procesos aislados	Habilitada	
		Permitir que se publiquen impresoras	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
75. Verifique los valores de Notificaciones de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Menú inicio y barra de tareas → Notificaciones"		
		Directiva	Valor	OK/NOK
		Desactivar el uso de la red para notificaciones	Habilitada	
76. Verifique los valores de Panel de control de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Panel de control"		
		Directiva	Valor	OK/NOK
		Permitir recomendaciones en línea	Deshabilitada	
77. Verifique los valores de Configuración regional y de idioma de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
78. Verifique los valores de Personalización de escritura a mano de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano"		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitada	
79. Verifique los valores de Personalización de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Panel de control → Personalización"		
		Directiva	Valor	OK/NOK
		Evitar la activación de la cámara de la pantalla de bloqueo	Habilitada	
80. Verifique los valores del administrador de conexiones de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
81. Verifique los valores de archivos sin conexión de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Archivos sin conexión"		
		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	
82. Verifique los valores de BranchCache de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → BranchCache"		
		Directiva	Valor	OK/NOK
		Activar BranchCache	Deshabilitada	
83. Verifique los valores del perfil de firewall de dominio de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Conexiones de Red → Firewall de Windows Defender → Perfil de dominio"		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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\LogFiles\Firewall\pfirewall.log) (Límite de tamaño: 4096 KB)	
		Firewall de Windows Defender: Proteger todas las conexiones de red	Habilitada	
84. Verifique los valores del perfil de firewall estándar de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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\LogFiles\Firewall\pfirewall.log) (Límite de tamaño: 4096 KB)	
		Firewall de Windows Defender: Proteger todas las conexiones de red	Habilitada	
85. Verifique los valores de las tecnologías de transición a IPv6 de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Configuración de TCPIP → Tecnologías de transición IPv6"		
		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		
86. Verifique los valores de la detección de topologías a nivel de vínculo de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
87. Verifique los valores de la estación de trabajo Lanman de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Estación de trabajo Lanman"		
		Directiva	Valor	OK/NOK
		Habilitar inicios de sesión de invitado no seguros	Deshabilitada	
88. Verifique los valores de Fuentes de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Fuentes"		
		Directiva	Valor	OK/NOK
		Habilitar Proveedores de fuentes	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
89. Verifique los valores de Proyección inalámbrica de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Proyección inalámbrica"		
		Directiva	Valor	OK/NOK
		Requerir emparejamiento de PIN	Habilitada	
90. Verifique los valores de Configuración WLAN de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
91. Verifique los valores de Acceso a datos móviles de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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)	

Comprobación	OK/NOK	Cómo hacerlo		
92. Verifique los valores de Configuración de la interfaz de usuario de WWAN de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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)	
93. Verifique los valores de los servicios de redes de igual a igual de Microsoft de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
94. Verifique los valores del servidor Lanman de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Servidor Lanman"		

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)	
95. Verifique los valores de Windows Connect Now de la directiva “CCN-STIC-599A19 Windows 10 – Equipos”		Utilizando la herramienta “Editor de administración de directivas de grupo”, verifique que la directiva “CCN-STIC-599A19 Windows 10 – Equipos” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Windows Connect Now”		
		Directiva	Valor	OK/NOK
		Prohibir el acceso de los asistentes de Windows Connect Now	Habilitada	
96. Verifique los valores de Acceso de almacenamiento extraíble de la directiva “CCN-STIC-599A19 Windows 10 – Equipos”		Utilizando la herramienta “Editor de administración de directivas de grupo”, verifique que la directiva “CCN-STIC-599A19 Windows 10 – Equipos” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Acceso de almacenamiento extraíble”		
		Directiva	Valor	OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Habilitada	
97. Verifique los valores de la administración de comunicaciones de Internet de la directiva “CCN-STIC-599A19 Windows 10 – Equipos”		Utilizando la herramienta “Editor de administración de directivas de grupo”, verifique que la directiva “CCN-STIC-599A19 Windows 10 – Equipos” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet”		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Restringir comunicaciones de Internet	Habilitada	
98. Verifique los valores de la configuración de comunicaciones de Internet de la directiva "CCN-STIC-599A19 Windows 10 – Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 – Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
		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	
99. Verifique los valores de App-V de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → App-V"		
		Directiva	Valor	OK/NOK
		Habilitar el cliente de App-V	Deshabilitada	
100. Verifique los valores de asistencia remota de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Asistencia Remota"		
		Directiva	Valor	OK/NOK
		Configurar Asistencia remota solicitada	Deshabilitada	
		Configurar Ofrecer Asistencia remota	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
101.Verifique los valores de directiva de grupo de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Directiva de grupo"		
		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	Deshabilitada	
		Vinculación de teléfono y PC en este dispositivo	Deshabilitada	
102.Verifique los valores de directiva del sistema operativo de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir la carga de actividades del usuario	Deshabilitada	
103.Verifique los valores de inicio de sesión de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
104.Verifique los valores de instalación de dispositivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Instalación de dispositivos"		
		Directiva	Valor	OK/NOK
		Permitir acceso remoto a la interfaz Plug and Play	Deshabilitada	

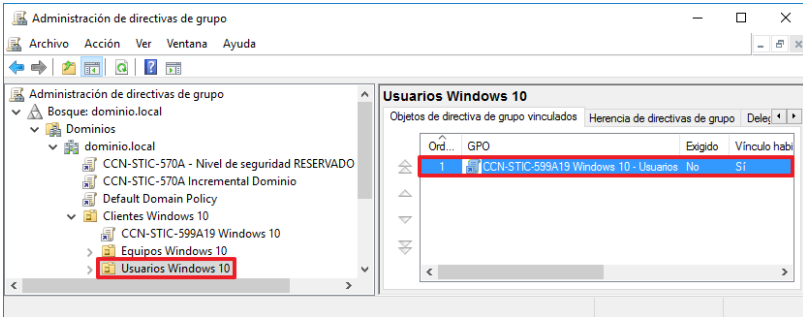
Comprobación	OK/NOK	Cómo hacerlo		
105.Verifique los valores de restricciones de instalación de dispositivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos"		
		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)	
106.Verifique los valores de la llamada a procedimiento remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos	Deshabilitada	
		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Llamada a procedimiento remoto"		
		Directiva	Valor	OK/NOK
		Habilitar la autenticación de clientes del Asignador de extremos de RPC	Habilitada	
		Restringir clientes de RPC no autenticados	Habilitada (Autenticado)	

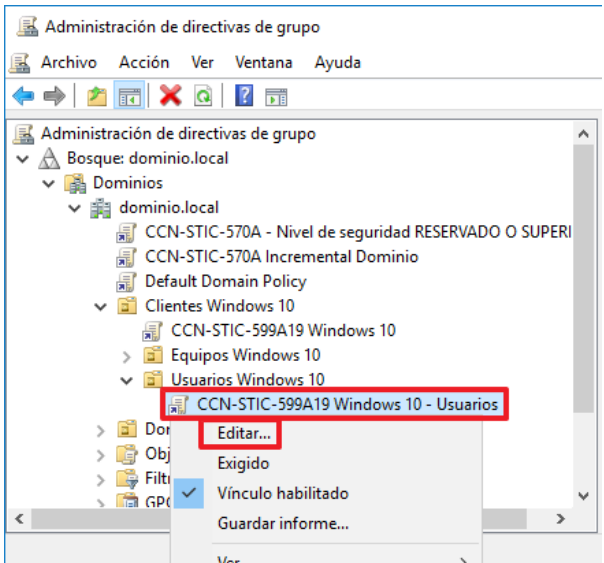
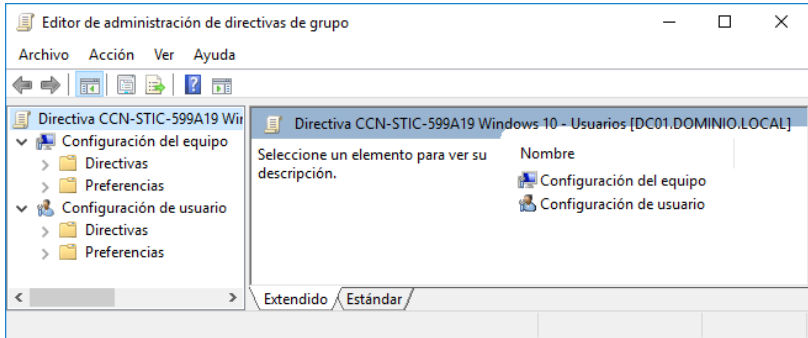
Comprobación	OK/NOK	Cómo hacerlo		
107.Verifique los valores de Net Logon de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Net Logon"		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada	
108.Verifique los valores de Perfiles de usuario de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Perfiles de Usuario"		
		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	
109.Verifique los valores de Servicios de configuración regional de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Servicios de configuración regional"		
		Directiva	Valor	OK/NOK
		Denegar el cambio de ubicación geográfica	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
110.Verifique los valores de Herramienta de diagnóstico de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Solución de problemas y diagnósticos → Herramienta de diagnóstico para soporte técnico de Microsoft"		
		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	
111.Verifique los valores de Preferencias de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Preferencias → Configuración de Windows → Registro"		
		Directiva	Valor	OK/NOK
		SMB1	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters Tipo: REG_DWORD Valor: 00000000 (0)	

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva	Valor	OK/NOK
	HiberbootEnabled	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Power Tipo: REG_DWORD Valor: 00000000 (0)	
	AllowTelemetry	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection Tipo: REG_DWORD Valor: 00000001	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\MessagingService Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\NgcCtnrSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\NgcSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\OneSyncSvc Tipo: REG_DWORD Valor: 00000004	

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva	Valor	OK/NOK
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ PimIndexMaintenanceSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ Sense Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ SgrmBroker Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ UnistoreSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ UserDataSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ WpnUserService Tipo: REG_DWORD Valor: 00000004	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\EntAppSvc Tipo: REG_DWORD Valor: 00000004	
		Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\PrintWorkflowUserSvc Tipo: REG_DWORD Valor: 00000004	Start
112.Finalice la comprobación de la directiva CCN-STIC-599A19 Windows 10 - Equipos		Cierre la ventana del "Editor de administración de directivas de grupo" que tenía abierta con la directiva de dominio "CCN-STIC-599A19 Windows 10 - Equipos"		
113.Verifique que está creada y asignada correctamente la directiva (GPO) de usuarios ("CCN-STIC-599A19 Windows 10 - Usuarios")		De nuevo en la consola de "Administración de directivas de grupo" diríjase a la siguiente unidad organizativa: Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10" y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que existe un vínculo llamado "CCN-STIC-599A19 Windows 10 - Usuarios".  Compruebe también en el mismo sitio que el campo "Vínculo habilitado" muestra "Sí" para la GPO "CCN-STIC-599A19 Windows 10 - Usuarios".		

Comprobación	OK/NOK	Cómo hacerlo
114. Abra la directiva (GPO) de usuarios (CCN-STIC-599A19 Windows 10 - Usuarios) en el editor de administración de directivas de grupo		Marque con el botón derecho el vínculo de la GPO "CCN-STIC-599A19 Windows 10 - Usuarios" situado en el siguiente contenedor: "Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10" En el menú contextual que aparecerá, seleccione la opción "Editar...", como se muestra en la figura.  Con ello se abrirá el Editor de administración de directivas de grupo, mostrando la configuración de la GPO "CCN-STIC-599A19 Windows 10 - Usuarios".  En los próximos pasos, hasta que se indique lo contrario, verificará la configuración de este GPO utilizando esta ventana del editor de administración de directivas de grupo

Comprobación	OK/NOK	Cómo hacerlo		
115.Verifique los valores de Carpetas compartidas de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Carpetas compartidas"		
		Directiva	Valor	OK/NOK
		Permitir publicación de carpetas compartidas	Deshabilitada	
		Permitir publicación de raíces DFS	Deshabilitada	
116.Verifique los valores del administrador de datos adjuntos de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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		
117.Verifique los valores para Agregar características a Windows 10 de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10"		
		Directiva	Valor	OK/NOK
		Impedir que el asistente se ejecute	Habilitada	
118.Verifique los valores del almacén digital de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Almacén digital"		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el Almacén digital	Habilitada	
119.Verifique los valores del centro de movilidad de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows"		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
120.Verifique los valores de la compatibilidad de aplicaciones de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Compatibilidad de aplicaciones"		
		Directiva	Valor	OK/NOK
		Desactivar el Asistente para la compatibilidad de programas	Habilitada	
121.Verifique los valores de la configuración de presentación de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Configuración de presentación"		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
122.Verifique los valores de la configuración de nube de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
123.Verifique los valores de las directivas de reproducción automática de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
124.Verifique los valores del explorador de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Explorador de archivos"		
		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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
125.Verifique los valores de diálogo común para abrir archivos de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
126.Verifique los valores del panel de marcos del explorador de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Explorador de archivos → Panel de marcos del explorador"		
		Directiva	Valor	OK/NOK
		Desactivar el panel de vista previa	Habilitada	
127.Verifique los valores de las versiones anteriores del explorador de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Explorador de archivos → 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	
128.Verifique los valores de las fuentes RSS de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
129.Verifique los valores de la grabadora de sonidos de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos"		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute la grabadora de sonidos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
130.Verifique los valores del informe de errores de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Informe de errores de Windows"		
		Directiva	Valor	OK/NOK
		Deshabilitar el Informe de errores de Windows	Habilitada	
131.Verifique los valores de la interfaz de usuario de credenciales de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Interfaz de usuario de credenciales"		
		Directiva	Valor	OK/NOK
		No mostrar el botón revelar contraseña	Habilitada	
132.Verifique los valores de Microsoft Management Console de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
133.Verifique los valores de los complementos restringidos o permitidos de Microsoft Management Console de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
		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	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	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	
134.Verifique los valores de directiva de grupo de Microsoft Management Console de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
135.Verifique los valores de las extensiones de complemento de directivas de grupo de MMC de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
136.Verifique los valores de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
		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	

Comprobación	OK/NOK	Cómo hacerlo		
137.Verifique los valores de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → NetMeeting → Audio y video"		
		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	
138.Verifique los valores de compartir aplicaciones a través de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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		
139.Verifique los valores de la página de opciones de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → NetMeeting → Página de opciones"		
		Directiva	Valor	OK/NOK
		Deshabilitar el botón Llamada avanzada	Habilitada	
		Ocultar la página General	Habilitada	
140.Verifique los valores de Cliente de conexión a Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
141.Verifique los valores de Accesorios de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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		
142.Verifique los valores de Tienda de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
143.Verifique los valores de ubicación y sensores de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Ubicación y sensores"		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
144.Verifique los valores de uso compartido de red de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Uso compartido de red"		
		Directiva	Valor	OK/NOK
		Impedir que los usuarios compartan archivos dentro de su perfil	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
145.Verifique los valores de virtualización de la experiencia del usuario de Microsoft de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Usuarios → Configuración del equipo → Directivas → 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	
146.Verifique los valores de Windows Mail de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Windows Mail"		
		Directiva	Valor	OK/NOK
		Turn off the communities features	Habilitada	
		Turn off Windows Mail application	Habilitada	
147.Verifique los valores de Windows Messenger de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Windows Messenger"		

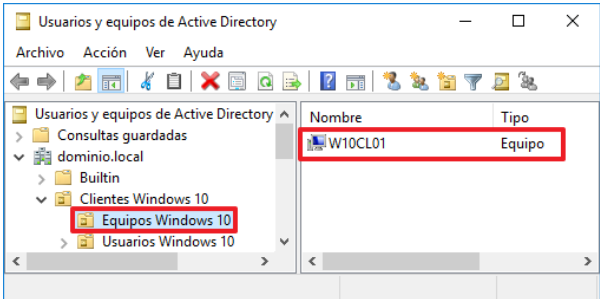
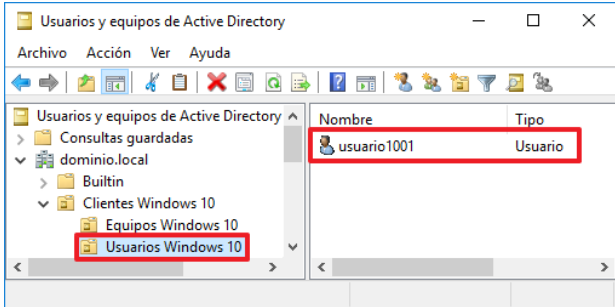
Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		No ejecutar automáticamente Windows Messenger al inicio	Habilitada	
		No permitir que se ejecute Windows Messenger	Habilitada	
148.Verifique los valores de Windows Update de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Windows Update"		
		Directiva	Valor	OK/NOK
		Quitar el acceso a todas las características de Windows Update	Habilitada, (0 – No mostrar ninguna notificación)	
149.Verifique los valores del menú Inicio y barra de tareas de la directiva "CCN-STIC-599A19 Windows 10- Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
150.Verifique los valores del Panel de Control de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Panel de Control"		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Abrir siempre Todos los elementos del Panel de control al abrir el Panel de control	Habilitada	
151.Verifique los valores de las impresoras de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Panel de Control → Impresoras"		
		Directiva	Valor	OK/NOK
		Impedir la adición de impresoras	Habilitada	
		Impedir la eliminación de impresoras	Habilitada	
152.Verifique los valores de personalización del panel de control de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Panel de Control → Programas"		
		Directiva	Valor	OK/NOK
		Ocultar "Características de Windows"	Deshabilitada	
153.Verifique los valores de archivos sin conexión a la red de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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		
154.Verifique los valores de Windows Connect Now de la directiva "CCN-STIC-599A19 Windows 10 Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Red → Windows Connect Now"		
		Directiva	Valor	OK/NOK
		Prohibir el acceso a los asistentes de Windows Connect Now	Habilitada	
155.Verifique los valores de sistema de la directiva "CCN-STIC-599A19 Windows 10 Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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?)	
156.Verifique los valores de acceso de almacenamiento extraíble de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble"		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Deshabilitada	
157.Verifique los valores de administración de comunicaciones de Internet de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Administración de comunicaciones de Internet"		
		Directiva	Valor	OK/NOK
		Restringir comunicación de Internet	Habilitada	
158.Verifique los valores de configuración de comunicaciones de Internet de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	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	
159.Verifique los valores de Ctrl+Alt+Supr de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Opciones de Ctrl+Alt+Supr"		
	Directiva		Valor	OK/NOK
	Quitar Administrador de tareas		Habilitada	
160.Verifique los valores de Servicios de configuración regional de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Servicios de configuración regional"		
	Directiva		Valor	OK/NOK
	Denegar el cambio de ubicación geográfica		Habilitada	
161.Finalice la comprobación de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Cierre la ventana del "Editor de administración de directivas de grupo" que tenía abierta con la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		

Comprobación	OK/NOK	Cómo hacerlo
162.Verifique que el equipo cliente miembro Windows 10 a asegurar se encuentra dentro de la unidad organizativa "Equipos Windows 10"		A través de la herramienta “Usuarios y equipos de Active Directory” mediante el menú “Herramientas” del “Administrador del servidor”, compruebe que el equipo Windows 10 a asegurar se encuentra en la unidad organizativa “Equipos Windows 10” situada en la siguiente ruta: <Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 Verifique que existe dentro de él un objeto de tipo "Equipo" que se corresponde con el equipo cliente miembro cuya configuración se está comprobando (en el ejemplo de la figura siguiente el equipo a comprobar se llama "W10CL01"): 
163.Verifique que la cuenta del usuario o usuarios del cliente miembro Windows 10 a asegurar se encuentran dentro de la unidad organizativa "Usuarios Windows 10"		De nuevo, a través de la herramienta “Usuarios y equipos de Active Directory”, compruebe que el cliente o clientes Windows 10 a asegurar se encuentran en la unidad organizativa “Usuarios Windows 10” situada en la siguiente ruta: <Nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10 Verifique que existe dentro de él un objeto de tipo "Usuario" que se corresponde con el usuario cliente miembro cuya configuración se está comprobando (en el ejemplo de la figura siguiente el usuario a comprobar se llama "usuario1001"). 
164.Finalice las comprobaciones en el controlador de dominio		En este punto ha realizado todas las comprobaciones necesarias en el controlador de dominio. Puede cerrar la sesión que tenía abierta hasta ahora en él.

2. COMPROBACIONES EN EQUIPO CLIENTE WINDOWS 10 ENTERPRISE LTSC

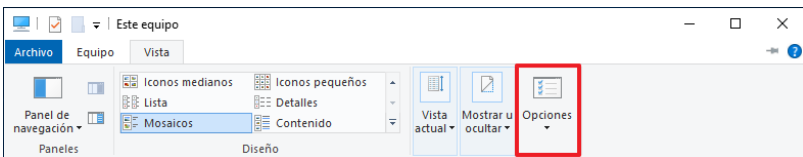
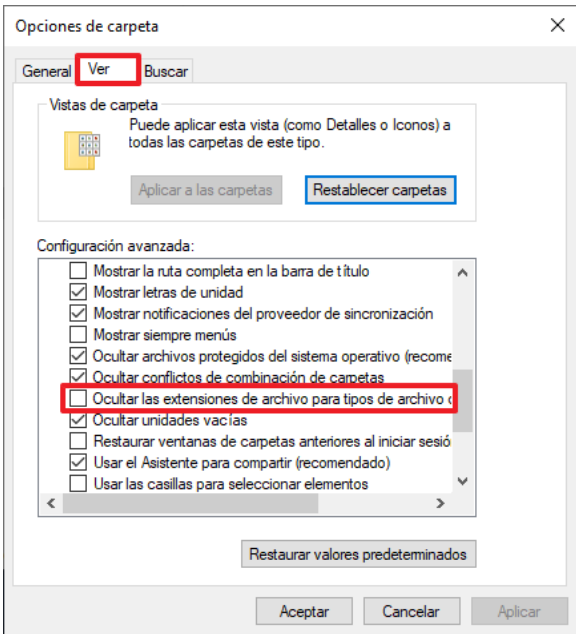
Para realizar algunas de las comprobaciones necesitará ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán en el equipo cliente miembro son las siguientes:

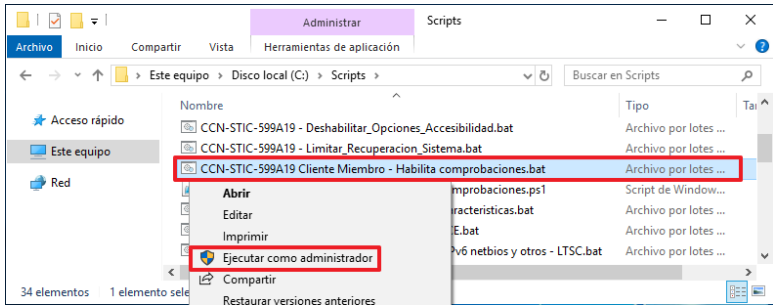
- a) Explorador de Windows (explorer.exe)
- b) PowerShell (powershell.exe)
- c) Conjunto resultante de directivas (rsop.msc)
- d) Panel de control (control.exe)
- e) Varias consolas de administración accesibles desde el panel de control (control.exe)
- f) Consola de administración de Microsoft (mmc.exe)
- g) Editor del registro (regedit.exe)
- h) Programador de tareas (taskschd.msc)

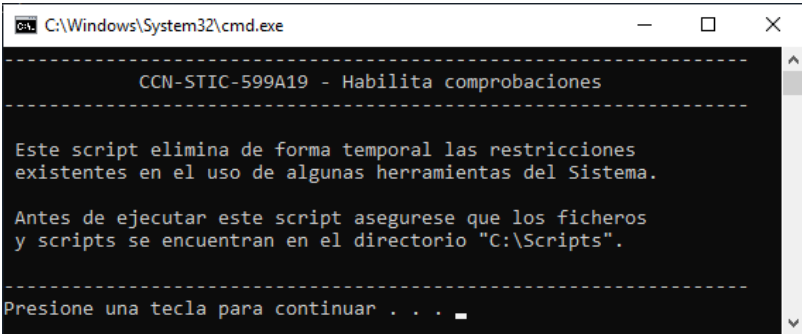
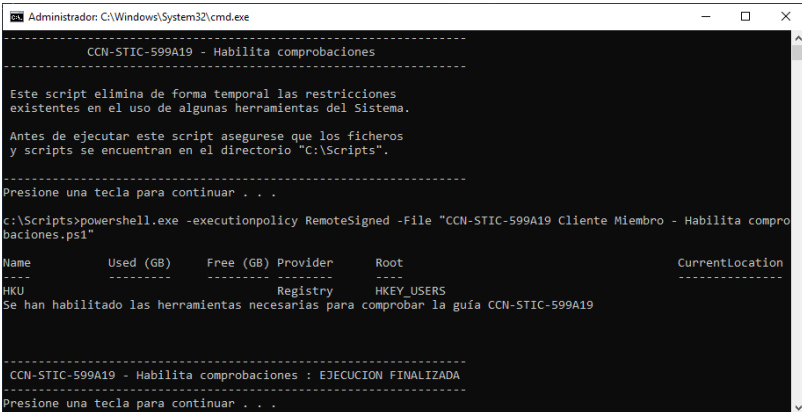
Siguiendo las recomendaciones de seguridad de esta guía, algunas de estas herramientas y consolas de administración estarán inicialmente deshabilitadas. Para poder implementar la lista de comprobación será necesario habilitarlas temporalmente. Para ello se suministra junto con esta guía el script “CCN-STIC-599A19 Cliente Miembro - 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.

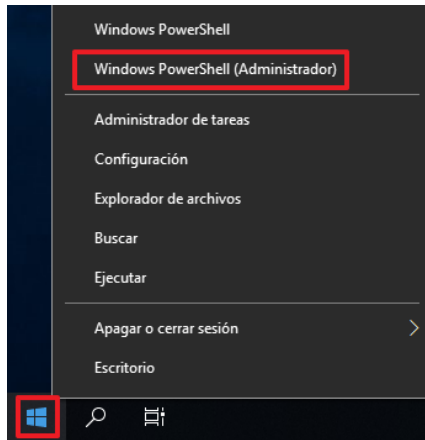
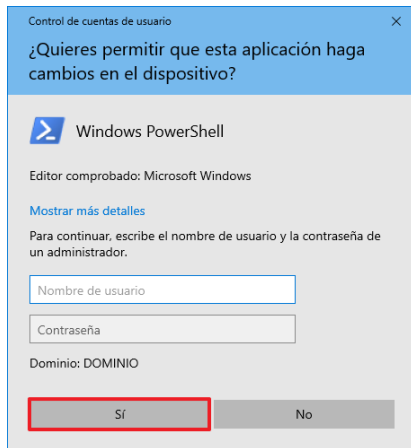
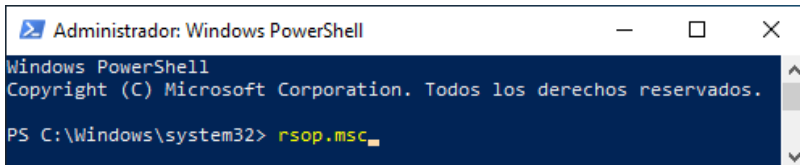
Ejecute los siguientes pasos en el cliente Windows 10 a comprobar:

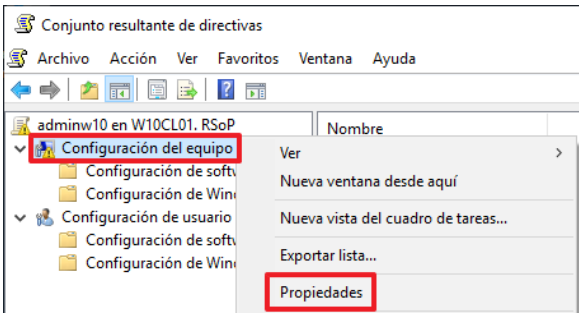
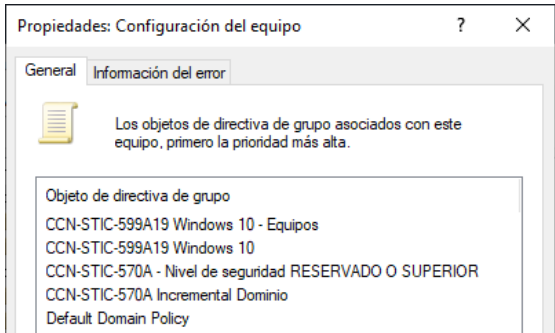
Comprobación	OK/NOK	Cómo hacerlo
165. Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador, con un usuario de la unidad organizativa "Usuarios Windows 10"		Inicie sesión en el equipo que está comprobando con una cuenta de usuario de Windows que esté ubicada en la unidad organizativa "Usuarios Windows 10" de Active Directory y que pertenezca al grupo local "Administradores" (por ejemplo, un miembro del grupo "Admins. del dominio" y al grupo local de dominio "Usuarios de shells). Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.

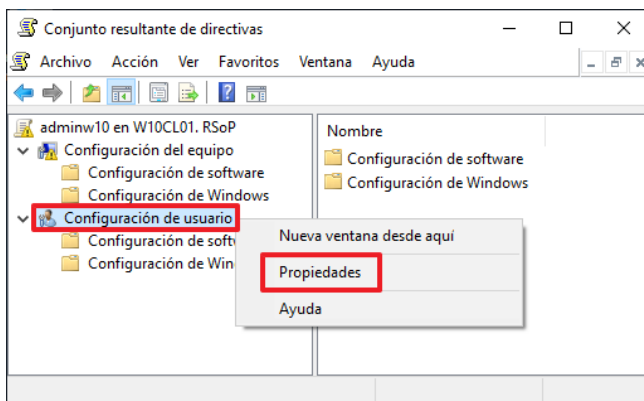
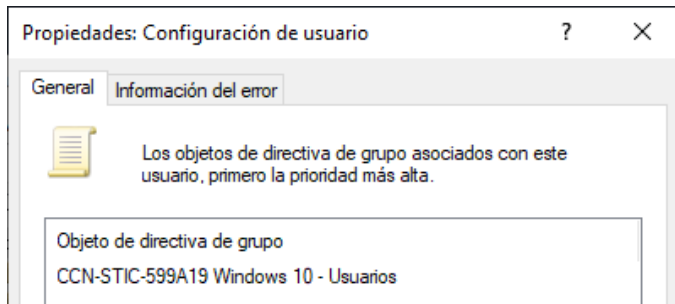
Comprobación	OK/NOK	Cómo hacerlo
166. Configure Explorador de Windows para que muestre las extensiones de los archivos		Por defecto Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador 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 (clic derecho) → Explorador de Windows" En el menú superior pulse sobre “Vista” y seleccione “Opciones”.  Seleccione la pestaña “Ver” y dentro de dicho menú, "Opciones de carpeta...". De la ventana que aparecerá, 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".

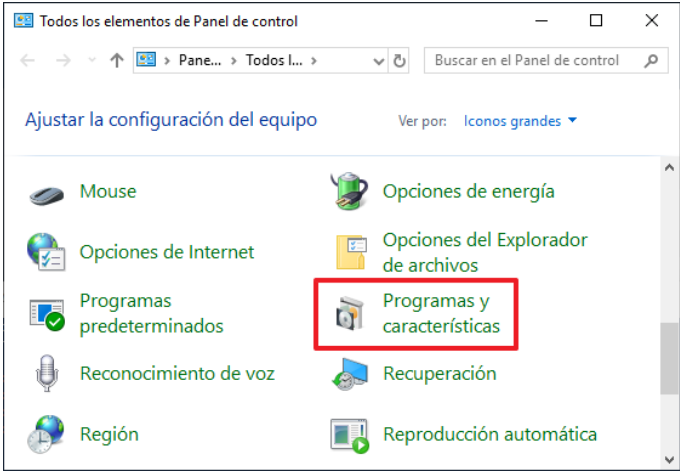
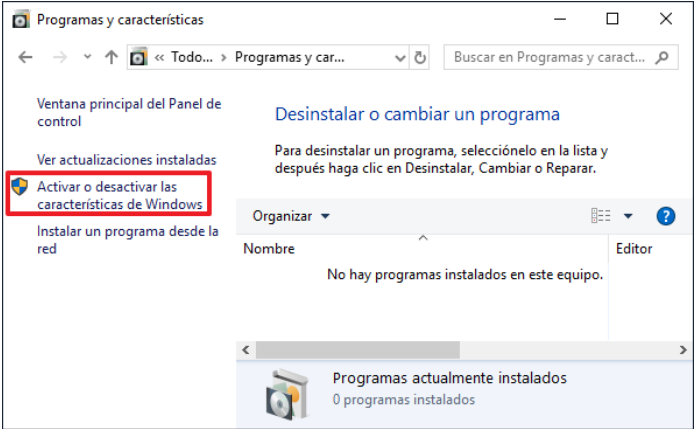
Comprobación	OK/NOK	Cómo hacerlo
167.Cree el directorio "C:\Scripts" y copie en él al menos los ficheros que se indican		Cree el directorio "Scripts" en la unidad "C:" ("C:\Scripts") en el sistema y copie en él al menos los siguientes dos scripts, los cuales están incluidos entre los ficheros que acompañan a esta guía: – CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.ps1 Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".
168.Ejecute el script que habilita temporalmente las consolas de administración restringidas		Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - 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.  Aparecerá la solicitud de credenciales el escritorio seguro, en el cual deberá introducir las credenciales de un usuario administrador y pulse "Sí". Nota: Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

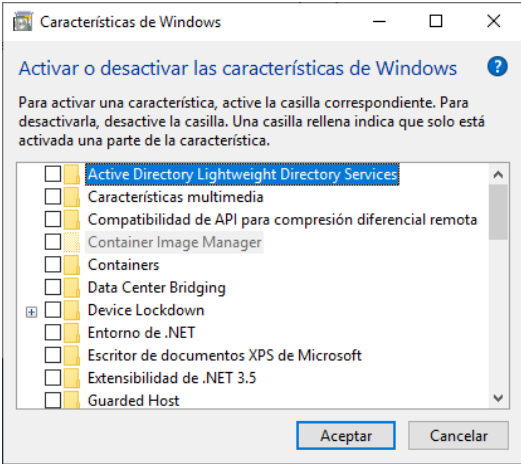
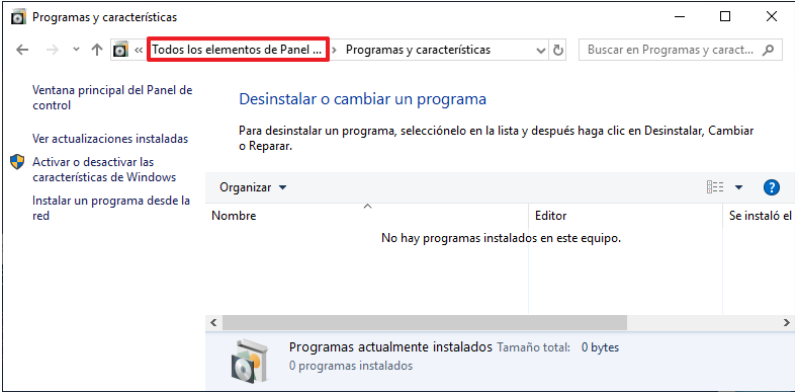
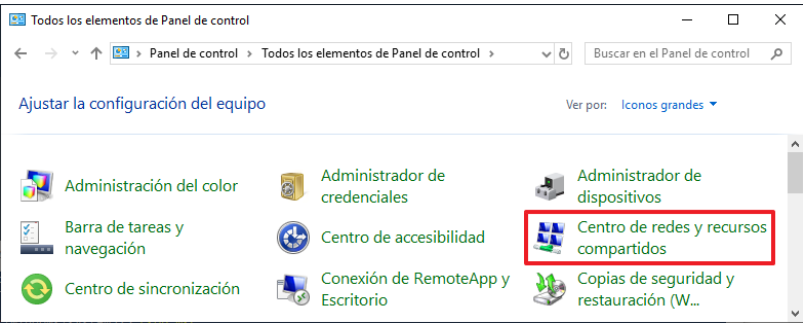
Comprobación	OK/NOK	Cómo hacerlo
169.Habilite temporalmente las consolas de administración restringidas		Aparecerá una consola de comandos con la ejecución del script. Pulse una tecla para continuar.  Cuando termine la ejecución, pulse una tecla para cerrar la ventana de comandos.  Nota: La próxima vez 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 de dominio y, por tanto, se han deshabilitado las comprobaciones. Ante tal eventualidad deberá volver a ejecutar el script “CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat” del mismo modo en que se describe en los pasos anteriores.

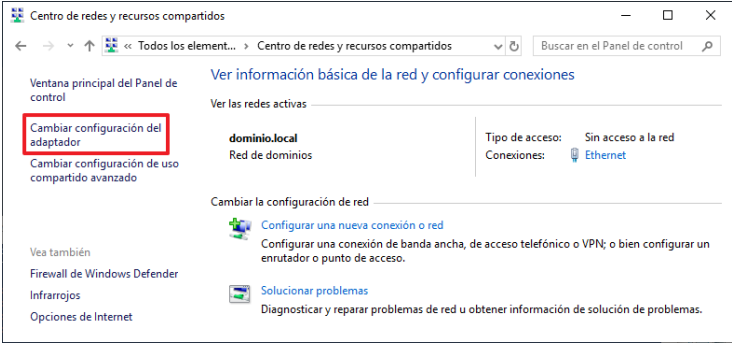
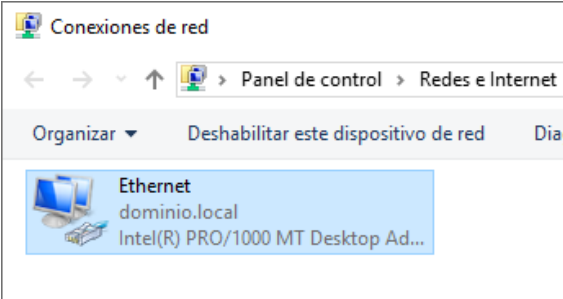
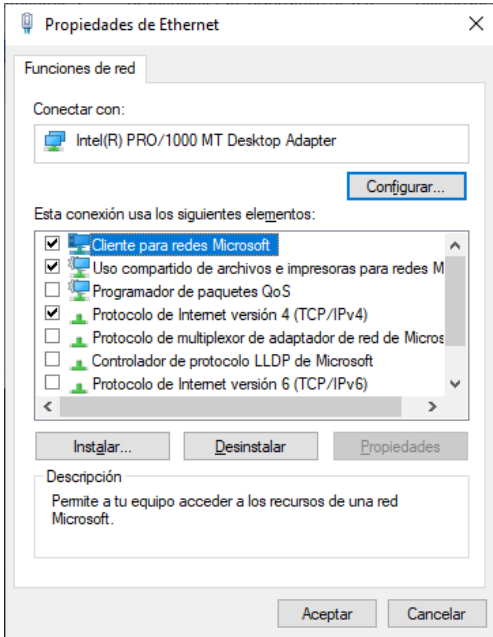
Comprobación	OK/NOK	Cómo hacerlo
170.Lance una ventana de PowerShell con permisos de administrador , para lanzar desde ella en pasos posteriores comandos con permisos de administrador		Haga clic con el botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”.  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.  Tras introducir las credenciales de un usuario administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.
171.Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse “Enter” para abrir la consola de administración "Conjunto resultante de directivas": 

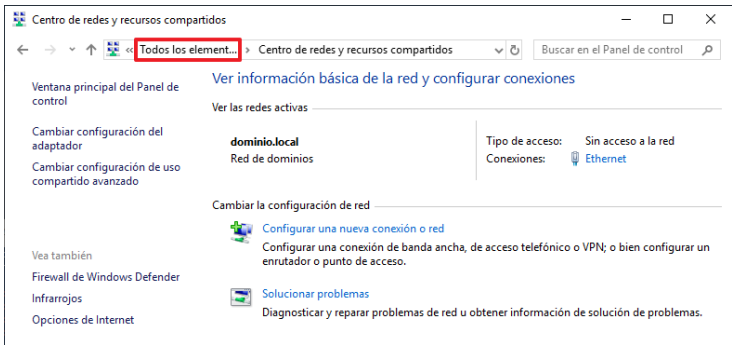
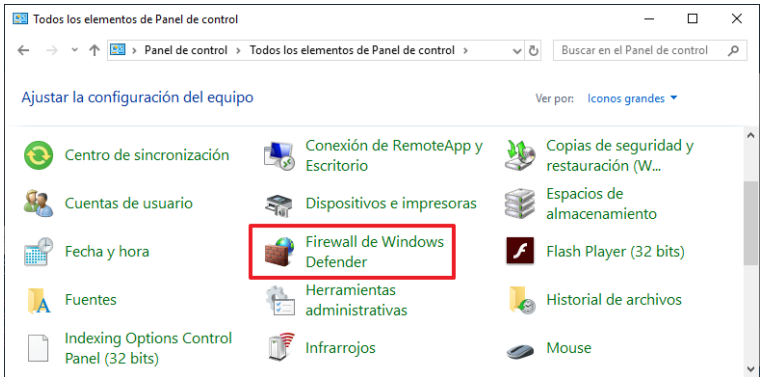
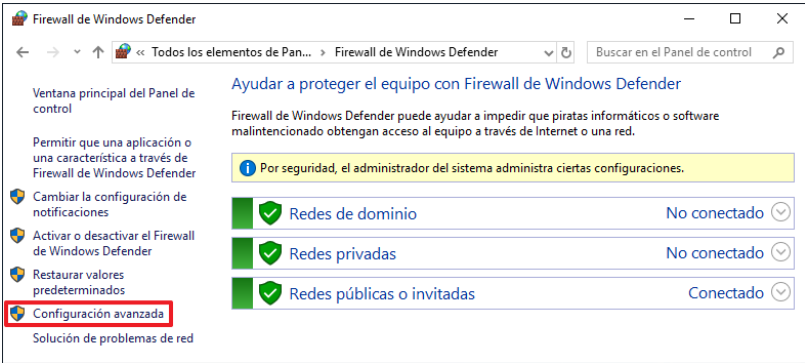
Comprobación	OK/NOK	Cómo hacerlo
172.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 Windows 10" y "CCN-STIC-599A19 Windows 10 - Equipos"		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las dos políticas deberán aparecer y "CCN-STIC-599A19 Windows 10 – Equipos" deberá estar situada encima de "CCN-STIC-599A19 Windows 10", tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al usuario del equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 Windows 10 - Equipos" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.
Parámetro		OK/NOK
CCN-STIC-599A19 Windows 10 - Equipos		
CCN-STIC-599A19 Windows 10		
CCN-STIC-570A - Nivel de seguridad RESERVADO O SUPERIOR		
Nota: Esta GPO dependerá del nivel de clasificación implementado en su organización.		
CCN-STIC-570A Incremental Dominio		
Default Domain Policy		

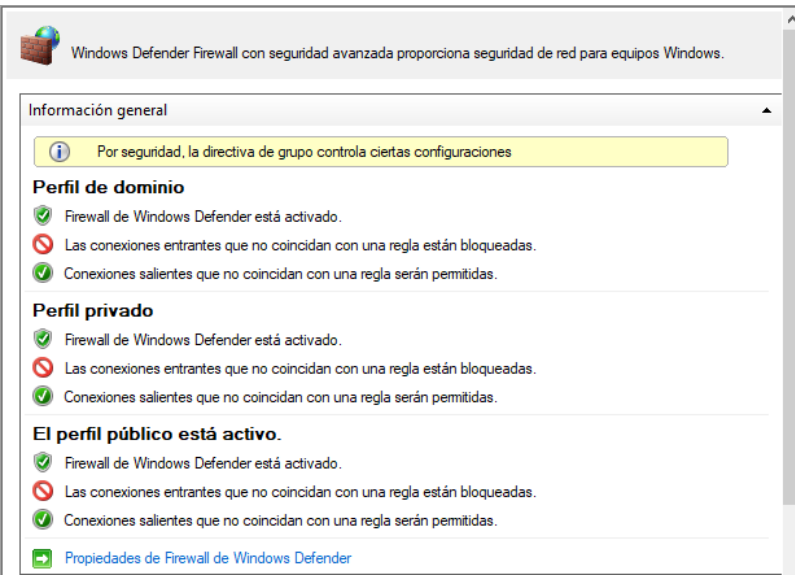
Comprobación	OK/NOK	Cómo hacerlo
		Cierre la ventana de “Propiedades” pero no cierre aún la consola de administración “Conjunto resultante de directivas”.
173.Verifique que el equipo ha recibido correctamente la directiva de grupo "CCN-STIC-599A19 Windows 10 - Usuarios"		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración de Usuario", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", deberá aparecer la política “CCN-STIC-599A19 Windows 10 – Usuarios”, tal y como se muestra en la siguiente figura.  Nota: Si el usuario que se está utilizando no está alojado en la unidad organizativa “Usuarios Windows 10”, la lista aparecerá vacía y, por tanto, este usuario no estará heredando dichas políticas. Puede mover a dicho usuario a la unidad organizativa correspondiente mediante la herramienta “Usuarios y equipos de Active Directory” o, en su lugar, utilizar un usuario que esté alojado en dicha unidad organizativa y que tenga privilegios de administración local del equipo Windows 10 en el que se están realizando las comprobaciones.
		Parámetro OK/NOK
		CCN-STIC-599A19 Windows 10 - Usuarios

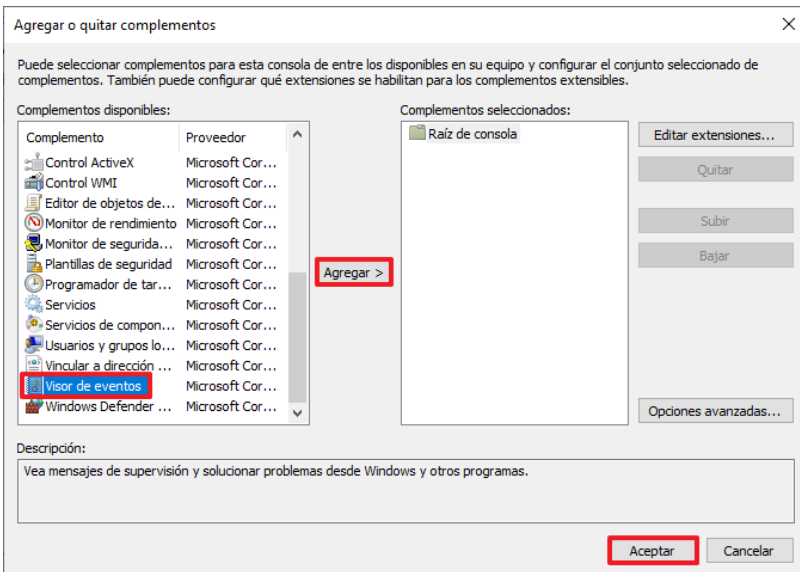
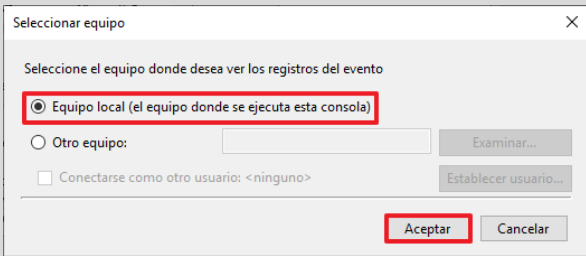
Comprobación	OK/NOK	Cómo hacerlo
		Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al usuario del equipo que está comprobando. Deberá asegurarse de que al menos el objeto “CCN-STIC-599A19 Windows 10 – Usuarios” está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización. Cierre la ventana de propiedades y cierre también la consola de administración "Conjunto resultante de directivas"
174.Verifique que no hay características opcionales de Windows habilitadas		Desde la ventana de PowerShell con privilegios de administrador, ejecute "control.exe" para abrir el panel de control, y seleccione la opción "Programas y características".  Dentro de la ventana que aparecerá, seleccione la opción "Activar o desactivar las características de Windows". 

Comprobación	OK/NOK	Cómo hacerlo
		En la ventana de control de cuentas de usuario, introduzca de nuevo las credenciales de un usuario administrador, accederá 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.
175.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”: 

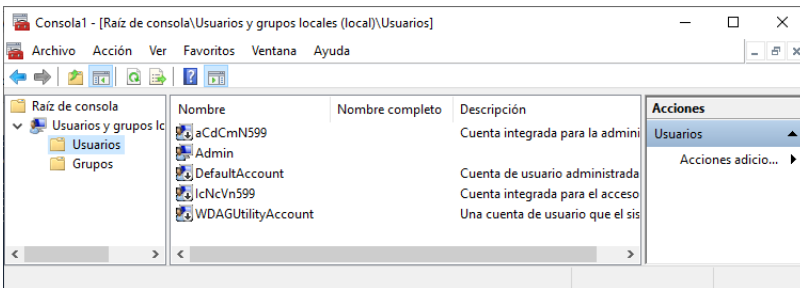
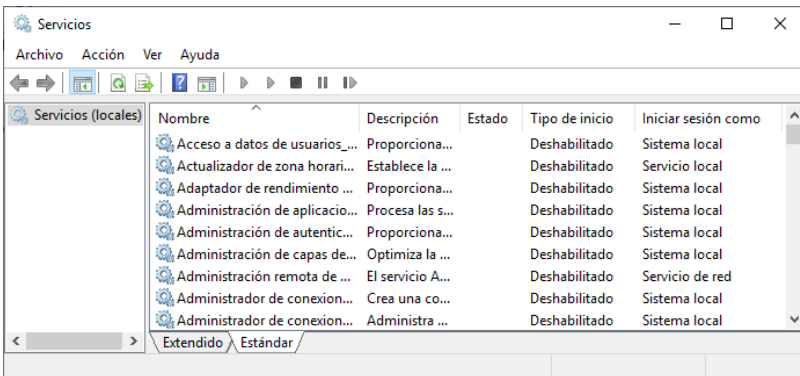
Comprobación	OK/NOK	Cómo hacerlo
		Seleccione “Cambiar configuración del adaptador”:  Aparecerá en la ventana del panel de control la lista de tarjetas de red del sistema:  Para cada tarjeta de red, marque con el botón derecho del ratón el icono de la tarjeta y seleccione la opción "Propiedades" del menú contextual que aparecerá. Tras introducir las credenciales de un usuario administrador de nuevo, aparecerá la ventana de propiedades del adaptador: 

Comprobación	OK/NOK	Cómo hacerlo
		Compruebe que los únicos elementos seleccionados sean "Cliente para redes Microsoft", "Uso compartido de archivos e impresoras para redes Microsoft" y "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.
176.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.  Seleccione "Firewall de Windows Defender" en el "Panel de Control".  Seleccione "Configuración avanzada". 

Comprobación	OK/NOK	Cómo hacerlo																											
		Introduzca credenciales 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. <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>Las conexiones entrantes que no coincidan con una regla están bloqueadas.</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla serán permitidas.</td><td></td></tr> <tr> <td rowspan="3">Perfil privado</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Las conexiones entrantes que no coincidan con una regla están bloqueadas.</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla serán permitidas.</td><td></td></tr> <tr> <td rowspan="3">Perfil público</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Las conexiones entrantes que no coincidan con una regla están bloqueadas.</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla serán permitidas.</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.		Las conexiones entrantes que no coincidan con una regla están bloqueadas.		Conexiones salientes que no coincidan con una regla serán permitidas.		Perfil privado	Firewall de Windows está activado.		Las conexiones entrantes que no coincidan con una regla están bloqueadas.		Conexiones salientes que no coincidan con una regla serán permitidas.		Perfil público	Firewall de Windows está activado.		Las conexiones entrantes que no coincidan con una regla están bloqueadas.		Conexiones salientes que no coincidan con una regla serán permitidas.	
Parámetro		OK/NOK																											
Por seguridad, la directiva de grupo controla ciertas configuraciones																													
Perfil de dominio	Firewall de Windows está activado.																												
	Las conexiones entrantes que no coincidan con una regla están bloqueadas.																												
	Conexiones salientes que no coincidan con una regla serán permitidas.																												
Perfil privado	Firewall de Windows está activado.																												
	Las conexiones entrantes que no coincidan con una regla están bloqueadas.																												
	Conexiones salientes que no coincidan con una regla serán permitidas.																												
Perfil público	Firewall de Windows está activado.																												
	Las conexiones entrantes que no coincidan con una regla están bloqueadas.																												
	Conexiones salientes que no coincidan con una regla serán permitidas.																												

Comprobación	OK/NOK	Cómo hacerlo
177. 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. 
178. 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
179. 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
		Tamaño máximo del registro (KB)	32768
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)
180.Verifique la configuración del registro de eventos de Seguridad		Pulse el botón derecho del ratón sobre el contenedor “Aplicación”, 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
		Tamaño máximo del registro (KB)	163840
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)
181.Verifique la configuración del registro de eventos de Sistema		Pulse el botón derecho del ratón sobre el contenedor “Aplicación”, 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
		Tamaño máximo del registro (KB)	32768
		Cuando alcance el tamaño máx. del reg. de eventos:	Sobrescribir eventos si es necesario (los anteriores primero)
182.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 pasos anteriores.	
183.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	
184.Verifique que se han renombrado los usuarios locales Administrador e Invitado		Adicionalmente, haga doble clic en el resto de los grupos y compruebe que sus miembros corresponden con los usuarios adecuados para su entorno.
		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 deshabilitados como en la siguiente figura.
		
	Usuarios	
		OK/NOK
	aCdCmN599	
	IcNcVn599	
185.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:

Comprobación	OK/NOK	Cómo hacerlo		
		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
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	
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	

Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administrador de conexiones de acceso remoto	RasMan	Deshabilitado	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	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	
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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 de NetBIOS sobre TCP/IP	lmhosts	Automático	Configurado	
Aplicación auxiliar IP	iphlpvc	Deshabilitado	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	
ASP.NET State Service	aspnet_state	Deshabilitado	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	
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Deshabilitado	Configurado	
BranchCache	PeerDistSvc	Deshabilitado	Configurado	
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado	
CaptureService	CaptureService	Deshabilitado	Configurado	
Carpetas de trabajo	workfoldersvc	Deshabilitado	Configurado	
CDPUserSvc	CDPUserSvc	Deshabilitado	Configurado	
Centro de seguridad	wscsvc	Automático	Configurado	
Cliente de directiva de grupo	gpsvc	Automático	Configurado	
Cliente de seguimiento de vínculos distribuidos	TrkWks	Deshabilitado	Configurado	
Cliente DHCP	Dhcp	Automático	Configurado	
Cliente DNS	Dnscache	Automático	Configurado	

Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	Deshabilitado	Configurado	
Configuración automática de WWAN	WwanSvc	Deshabilitado	Configurado	
Configuración de Escritorio remoto	SessionEnv	Deshabilitado	Configurado	
ConsentUX	ConsentUxUserSvc	Deshabilitado	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Deshabilitado	Configurado	
Control parental	WpcMonSvc	Deshabilitado	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Deshabilitado	Configurado	
Copias de seguridad de Windows	SDRSVC	Deshabilitado	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
Datos de contactos	PimIndexMaintenanceSvc	Deshabilitado	Configurado	
Desencadenadores de Message Queue Server	MSMQTriggers	Deshabilitado	Configurado	
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado	
Detección SSDP	SSDPSRV	Deshabilitado	Configurado	
DevicePicker	DevicePickerUserSvc	Deshabilitado	Configurado	
DevicesFlow	DevicesFlowUserSvc	Deshabilitado	Configurado	
Diagnostic Execution Service	diagsvc	Deshabilitado	Configurado	

Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Deshabilitado	Configurado	
Disco virtual	vds	Manual	Configurado	
Dispositivo host de UPnP	upnphost	Deshabilitado	Configurado	
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado	
dmwappushsvc	dmwappushservice	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	
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	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	

Comprobación		OK/NOK			Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK		
Propagación de certificados	CertPropSvc	Deshabilitado	Configurado			
Protección de software	spssvc	Automático	Configurado			
Protocolo de autenticación extensible	EapHost	Manual	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			
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 auxiliar de host para aplicaciones	AppHostSvc	Deshabilitado	Configurado			
Servicio AVCTP	BthAvctpSvc	Deshabilitado	Configurado			
Servicio biométrico de Windows	WbioSrv	Deshabilitado	Configurado			
Servicio Cifrado de unidad BitLocker	BDESVC	Deshabilitado	Configurado			

Comprobación		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	Deshabilitado	Configurado	
Servicio de administración de radio	RmSvc	Deshabilitado	Configurado	
Servicio de administración de web	WMSVC	Deshabilitado	Configurado	
Servicio de administración de Windows	WManSvc	Deshabilitado	Configurado	
Servicio de administración IIS	IISADMIN	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	wlpcsvc	Deshabilitado	Configurado	
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado	
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado	
Servicio de cierre de invitado de Hyper-V	vmicshutdwn	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	IpplattCfgSvc	Deshabilitado	Configurado	

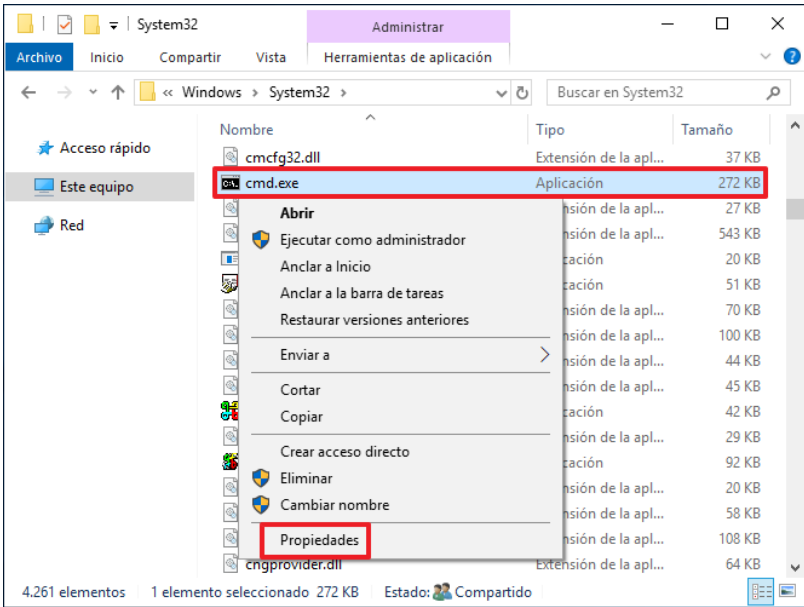
Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de datos del sensor	SensorDataService	Deshabilitado	Configurado	
Servicio de datos espacial	SharedRealitySvc	Deshabilitado	Configurado	
Servicio de detección automática de proxy web WinHTTP	WinHttpAutoProxySvc	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 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	
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	Deshabilitado	Configurado	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Deshabilitado	Configurado	
Servicio de latido de Hyper-V	vmicheartbeat	Deshabilitado	Configurado	

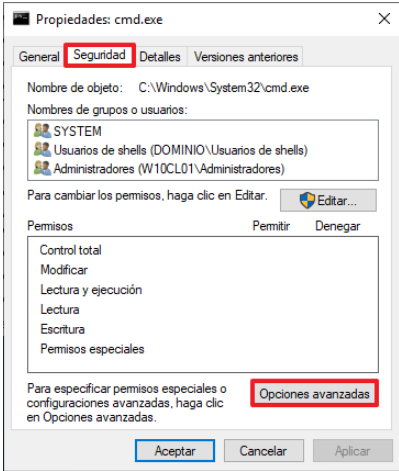
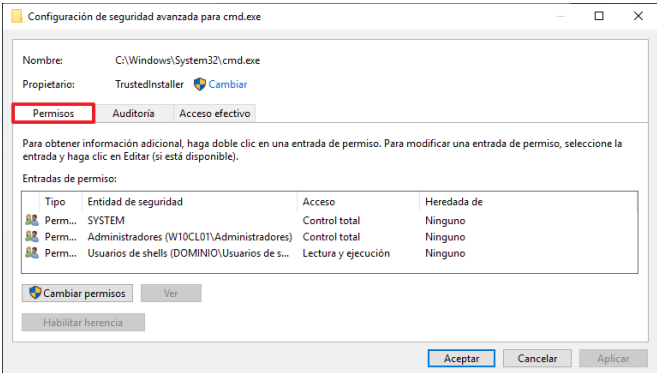
Comprobación		OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de licencia de cliente (ClipSVC)	ClipSVC	Manual	Configurado		
Servicio de lista de redes	netprofm	Manual	Configurado		
Servicio de mejora de visualización	DisplayEnhancementService	Deshabilitado	Configurado		
Servicio de monitor de infrarrojos	irmon	Deshabilitado	Configurado		
Servicio de notificación de eventos de sistema	SENS	Automático	Configurado		
Servicio de Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	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 Protección contra amenazas avanzada de Windows Defender	Sense	Deshabilitado	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Deshabilitado	Configurado		
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado		
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Deshabilitado	Configurado		
Servicio de publicación World Wide Web	W3SVC	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 host	hns	Deshabilitado	Configurado		
Servicio de red de Xbox Live	XboxNetApiSvc	Deshabilitado	Configurado		

Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	

Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado	
Servicio de virtualización de red	nvagent	Deshabilitado	Configurado	
Servicio de Windows Defender	WinDefend	Deshabilitado	Configurado	
Servicio de Windows Insider	wisvc	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 FrameServer de la Cámara de Windows	FrameServer	Deshabilitado	Configurado	
Servicio FTP de Microsoft	ftpsvc	Deshabilitado	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	Deshabilitado	Configurado	
Servicio MultiPoint	Wms	Deshabilitado	Configurado	
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Deshabilitado	Configurado	
Servicio PushToInstall de Windows	PushToInstall	Deshabilitado	Configurado	

Comprobación		Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standard.collector.service	Deshabilitado	Configurado	
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado	
Servicio SNMP	SNMP	Deshabilitado	Configurado	
Servicio telefónico	PhoneSvc	Deshabilitado	Configurado	
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado	
Servicio WAS (Windows Process Activation Service)	WAS	Deshabilitado	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Deshabilitado	Configurado	
Servicios simples de TCP/IP	simptcp	Deshabilitado	Configurado	
Servidor	LanmanServer	Deshabilitado	Configurado	
Servidor de roles de DS	DsRoleSvc	Deshabilitado	Configurado	
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	
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
186.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: 		

Comprobación	OK/NOK	Cómo hacerlo																
		En la ventana de “Propiedades”, seleccione la pestaña “Seguridad” y pulse sobre “Opciones Avanzadas”.  Nota: En el caso de estar usando un usuario perteneciente a la unidad organizativa “Usuarios Windows 10” éste no podrá ver la pestaña seguridad por lo que deberá utilizar un usuario que este fuera de dicha unidad organizativa. Así mismo, es posible que requiera de permisos adicionales para poder visualizar los permisos de los diferentes ficheros. En la pestaña “Permisos” de la ventana “Configuración avanzada de <archivo a comprobar>” observe los permisos y compárelos con la siguiente tabla:  <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>SYSTEM</td><td>Control total</td><td>Ninguno</td></tr><tr><td>Perm...</td><td>Administradores (W10CL01\Administradores)</td><td>Control total</td><td>Ninguno</td></tr><tr><td>Perm...</td><td>Usuarios de shells (DOMINIO\Usuarios de s...</td><td>Lectura y ejecución</td><td>Ninguno</td></tr></tbody></table> 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. En las cuentas de dominio, resaltadas con fondo gris en la siguiente tabla, aparecerá el nombre de su dominio en lugar de "DOMINIO". Además, 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”.	Tipo	Entidad de seguridad	Acceso	Heredada de	Perm...	SYSTEM	Control total	Ninguno	Perm...	Administradores (W10CL01\Administradores)	Control total	Ninguno	Perm...	Usuarios de shells (DOMINIO\Usuarios de s...	Lectura y ejecución	Ninguno
Tipo	Entidad de seguridad	Acceso	Heredada de															
Perm...	SYSTEM	Control total	Ninguno															
Perm...	Administradores (W10CL01\Administradores)	Control total	Ninguno															
Perm...	Usuarios de shells (DOMINIO\Usuarios de s...	Lectura y ejecución	Ninguno															

Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%ProgramFiles%\NetMeeting	Administrador	Control total	
	System	Control total	
%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	
%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	
	Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\repair	Administradores	Control Total	
	SYSTEM	Control Total	
%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\cacls.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\clip.exe	Administradores	Control Total	
	SYSTEM	Control Total	

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".

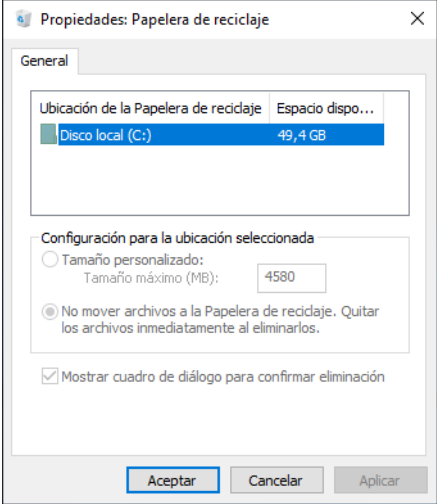
Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\cmd.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\cscript.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\debug.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\edit.com	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\edlin.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\hostname.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\ipconfig.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\nbtstat.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\net.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\netstat.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\nslookup.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\ntbackup.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\ping.exe	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\rasctrm.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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo	Usuario	Permiso	OK/NOK	
%SystemRoot%\system32\rasmans.dll	Administradores	Control Total		
%SystemRoot%\system32\rasmontr.dll	Administradores	Control Total		
%SystemRoot%\system32\rasmxs.dll	Administradores	Control Total		
%SystemRoot%\system32\rasphone.exe	Administradores	Control Total		
%SystemRoot%\system32\rasppp.dll	Administradores	Control Total		
%SystemRoot%\system32\rasrad.dll	Administradores	Control Total		
%SystemRoot%\system32\rasser.dll	Administradores	Control Total		
%SystemRoot%\system32\rastapi.dll	Administradores	Control Total		
%SystemRoot%\system32\rastls.dll	Administradores	Control Total		
%SystemRoot%\system32\rcp.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\regedt32.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\regsvr32.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\rexec.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\route.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\rsh.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\sysedit.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\telnet.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\WindowsPowerShell\v1.0\PowerShell.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%\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\winmsd.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\wscript.exe	Administradores	Control Total	
	SYSTEM	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	
%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	

Comprobación		OK/NOK	Cómo hacerlo	
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\raschap.dll		Administradores	Control Total	
%SystemRoot%\syswow64\rasctrnm.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	
%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	
187. Compruebe las entradas en el registro		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:		

Comprobación	OK/NOK		Cómo hacerlo
	Clave		Valor
	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\tcpip6\Parameters\DisabledComponents		ffffff (0xffffffff)
	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\LaunchTo		1
	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsHistory		1
	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsMenu		1
	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClearRecentDocsOnExit		1
	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecycleFiles		1
	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ConfirmFileDelete		1
188. 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		OK/NOK
	Microsoft\XblGameSave\XblGameSaveTask		
	Microsoft\Windows\Maps\MapsToastTask		
	Microsoft\Windows\HelloFace\FODCleanupTask		
	Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser		

Comprobación	OK/NOK	Cómo hacerlo
189.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.	
190.Borre el directorio "C:\Scripts"		Borre el directorio "C:\Scripts" con todo su contenido.
191.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. Nota: Si movió temporalmente un usuario administrador en Active Directory a la unidad organizativa "Usuarios Windows 10" para realizar los pasos de la lista de comprobación en el equipo que está comprobando, devuelva dicho usuario a su ubicación original a través de la herramienta "Usuarios y equipos de Active Directory" en el controlador de dominio.

ANEXO B.2. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO B.2.1. 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), miembro 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 el siguiente enlace:

<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 hecho 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 miembro de un dominio, con sistema operativo Windows 10 versión 1809, 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 adicionales a cumplir tras 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.

Algunas de las acciones descritas en esta guía deberán llevarse a cabo en un controlador de dominio al que pertenezca el equipo cliente y otras en el propio equipo cliente.

3. REQUISITOS HARDWARE Y SOFTWARE

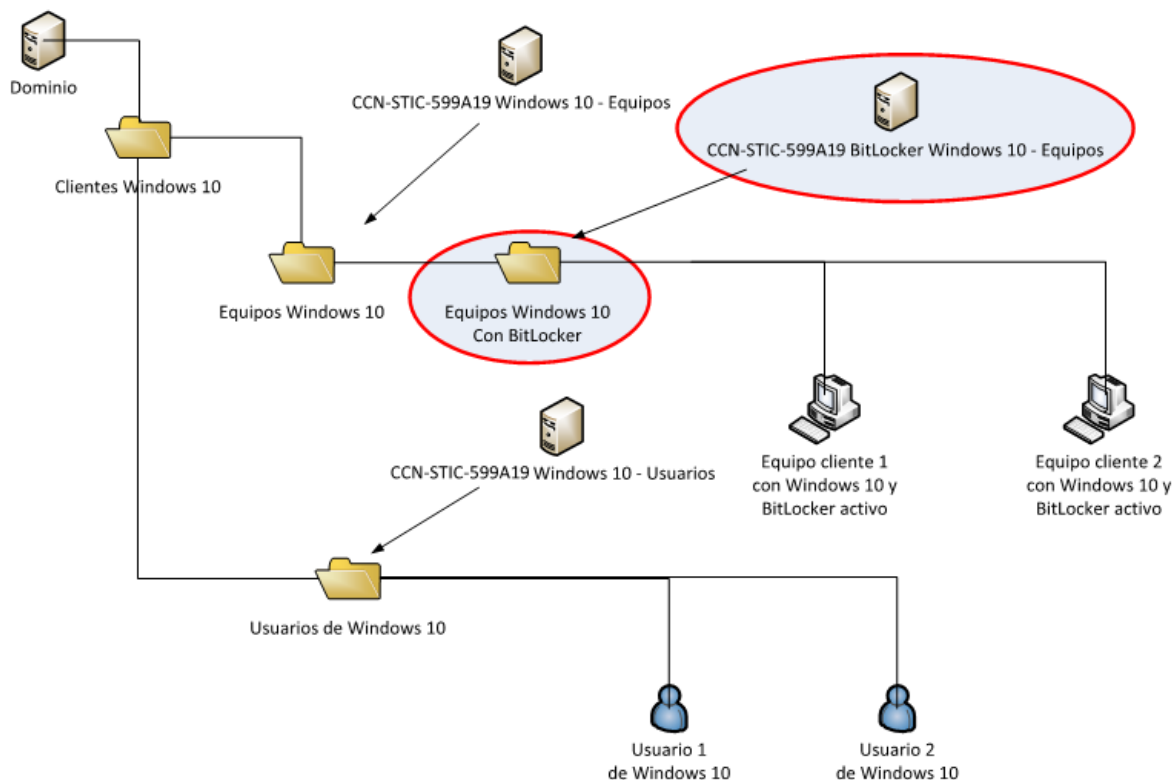
La implementación del cifrado de unidad BitLocker tiene los siguientes requisitos de hardware y software:

- a) Un equipo que cumpla los requisitos mínimos para Windows 10 (BitLocker no está disponible en la edición Windows 10 Home).
- 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.

4. OBJETO DE DIRECTIVA DE GRUPO (GPO)

En este apartado se documentan las configuraciones de un objeto de directiva de grupo específico para el cifrado de disco con BitLocker. Esta GPO se deberá aplicar de forma incremental sobre el equipo, complementando las configuraciones definidas en las otras GPOs definidas en esta guía. El orden de aplicación deberá ser tal que las configuraciones definidas en esta GPO específica de BitLocker tengan prioridad sobre las definidas en las otras GPOs de esta guía.

Para aplicar correctamente las configuraciones de esta GPO, que se llamará "CCN-STIC-599A19 BitLocker Windows 10 - Equipos", se creará en Active Directory una nueva unidad organizativa que se llamará "Equipos Windows 10 con BitLocker", específica para equipos Windows 10 con BitLocker, dentro de la unidad organizativa "Equipos Windows 10", como muestra la siguiente figura.



La configuración sólo afectará a la parte de "Configuración del Equipo" de la GPO. No será necesario definir ninguna configuración adicional en la parte de "Configuración de Usuario".

4.1. SERVICIOS DEL SISTEMA

La implementación del cifrado de unidad BitLocker para esta guía, requiere que se configuren los servicios del sistema mostrados en la siguiente tabla de la manera en que en ella se indica.

La configuración de estos servicios se puede realizar en un objeto de directiva de grupo (GPO), utilizando la consola de administración "Editor de administración de directivas de grupo", en la siguiente ubicación:

"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"

Servicio	Inicio	Permiso
Servicio Cifrado de unidad BitLocker (BDESVC)	Automático	Configurado
Detección de hardware Shell (shellhwdetection)	Automático	Configurado

4.2. PLANTILLAS ADMINISTRATIVAS (EQUIPO)

A continuación, se describen los valores relacionados con la configuración de “Cifrado de unidad BitLocker”, que se establecen dentro del apartado "Plantillas Administrativas", dentro de la sección "Configuración de equipo", de una GPO.

Las siguientes tablas indican la GPO, sus valores y una descripción. Estos valores se establecen en las ubicaciones indicadas al comienzo de cada tabla.

“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker”

Servicio	Inicio	Permiso
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	Permite configurar el algoritmo y la intensidad del cifrado que se usan en el Cifrado de unidad BitLocker.
Impedir la sobreescritura de memoria al reiniciar	Deshabilitada	Los secretos de BitLocker se quitan de la memoria al reiniciarse el equipo.

“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades de datos extraíbles”

Servicio	Inicio	Permiso
Controlar el uso de BitLocker en unidades extraíbles	Deshabilitada	Si deshabilita esta configuración de directiva, los usuarios no podrán usar BitLocker en unidades de datos extraíbles.

“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades del sistema operativo”

Servicio	Inicio	Permiso
Configurar longitud mínima de PIN para el inicio	Habilitada, 8	Esta configuración de directiva le permite configurar una longitud mínima para un PIN de inicio del Módulo de plataforma segura (TPM). Se aplica al activar BitLocker. El PIN de inicio debe tener una longitud mínima de 4 dígitos y una longitud máxima de 20 dígitos.

Servicio	Inicio	Permiso
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	Si habilita esta configuración de directiva antes de activar BitLocker, puede configurar los componentes de arranque que el TPM validará antes de desbloquear el acceso a la unidad del sistema operativo cifrada mediante BitLocker. Si cualquiera de estos componentes cambia mientras la protección del BitLocker permanece activa, el TPM no liberará la clave de cifrado para desbloquear la unidad; en su lugar, el equipo mostrará la consola de recuperación de BitLocker y solicitará que se proporcione la contraseña de recuperación o la clave de recuperación para desbloquear la unidad.
Permitir los PIN mejorados para el inicio	Habilitada	Los PIN de inicio mejorados permiten el uso de caracteres en mayúsculas y minúsculas, símbolos, números y espacios. Nota: No todos los equipos admiten los PIN mejorados en el entorno previo al arranque. Se recomienda que los usuarios realicen una comprobación del sistema al instalar BitLocker.
Requerir autenticación adicional al iniciar	Habilitada, Requerir PIN de inicio con TPM (no permitir los demás)	Esta configuración de directiva le permite configurar si BitLocker requiere autenticación adicional cada vez que se inicia el equipo y si se usa BitLocker con un Módulo de plataforma segura (TPM).

5. GUIA PASO A PASO – BITLOCKER

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

Antes de empezar se deberá tener en cuenta los siguientes requisitos:

- Un equipo que cumpla los requisitos mínimos para Windows 10 (BitLocker no está disponible en la edición Windows 10 Home).
- Un microchip TPM, versión 1.2 o superior, activado.
- BIOS compatible con TCG (Trusted Computing Group).

- d) Una partición de disco para la unidad del sistema. En Windows 10, si cuenta con una sola partición de disco para la unidad del sistema operativo, BitLocker preparará automáticamente la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema para usarla para 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.

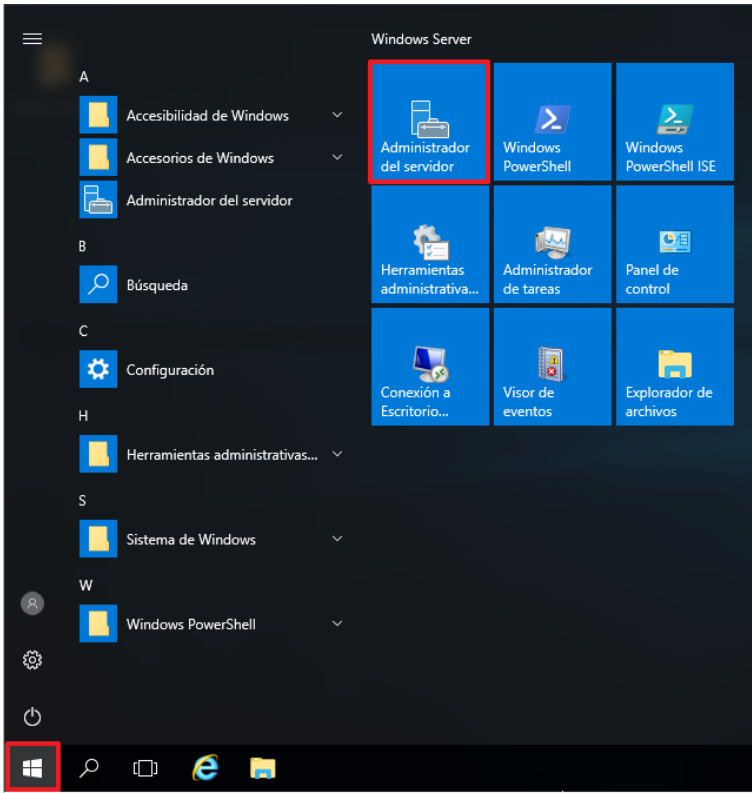
- e) Una unidad flash USB para almacenar claves de inicio y recuperación.
- f) Una configuración BIOS para iniciar primero desde el disco duro, no las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como una clave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

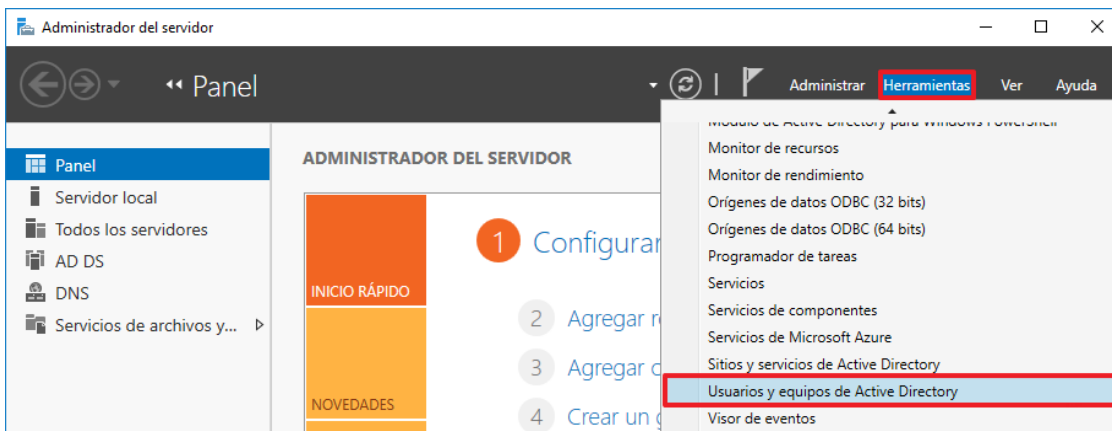
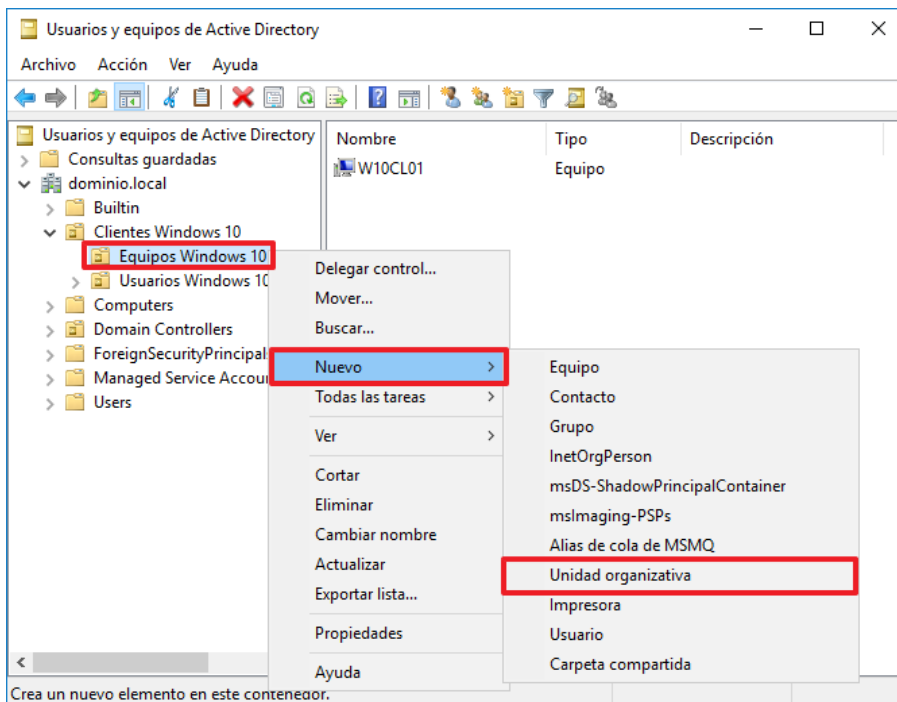
Nota: Tenga en cuenta que el acceso a las impresoras puede estar deshabilitado, debido a la aplicación de la configuración de seguridad implementada. Recuerde que antes de realizar este paso a paso necesitará de una unidad para almacenar las claves necesarias por lo que deberá aplicar la configuración para utilizar el dispositivo de almacenamiento descrito en el “ANEXO B.2.2 DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19”.

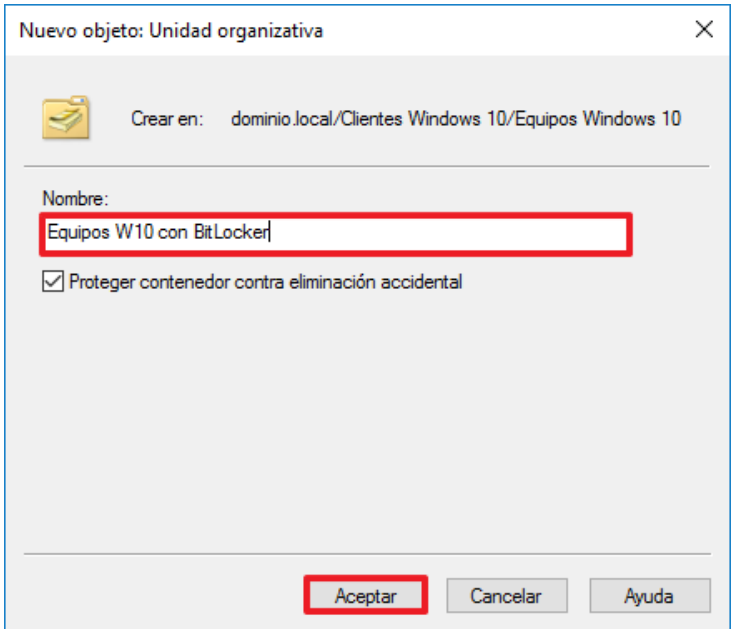
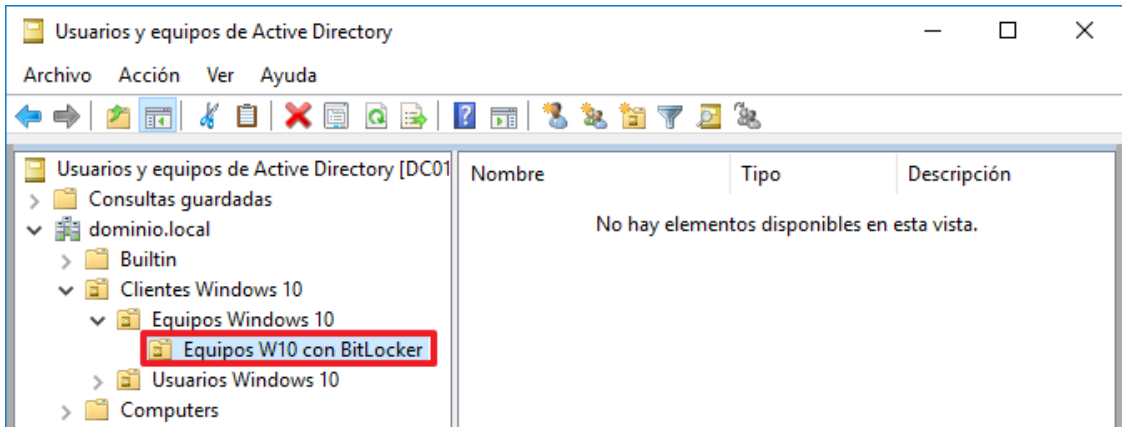
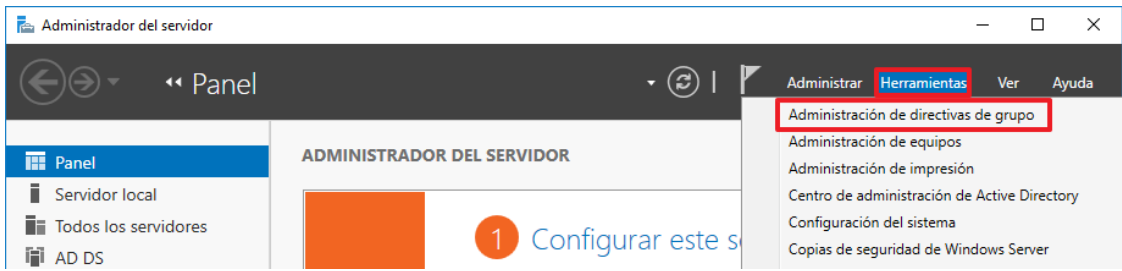
El primer conjunto de acciones deberá realizarlos en un controlador de dominio del dominio al que pertenece el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se configure BitLocker en el primer equipo cliente Windows 10 miembro de dominio, ya que crear la unidad organizativa necesaria e incorporar las configuraciones recomendadas en esta guía en un objeto de directiva de grupo, sólo es necesario realizarlo la primera vez.

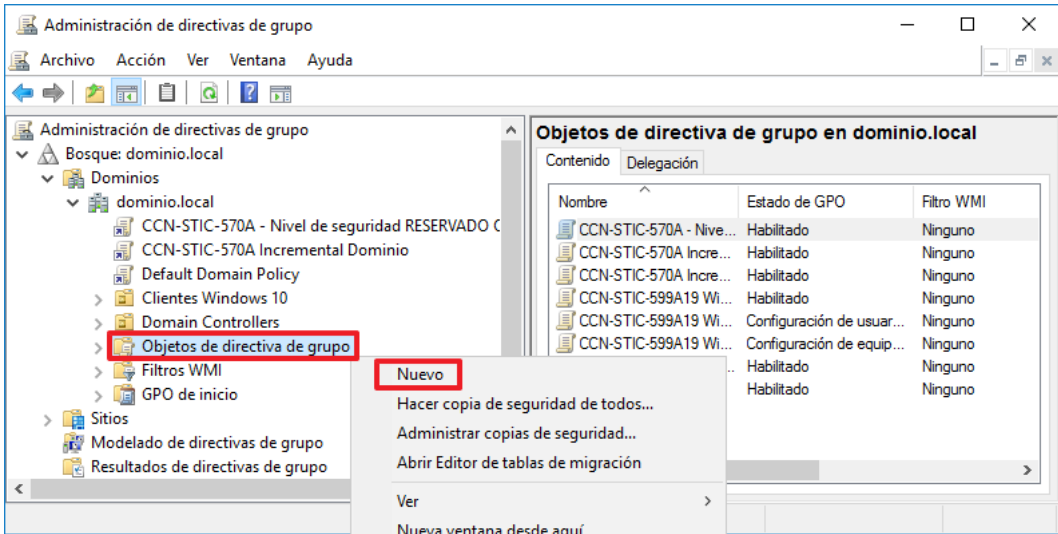
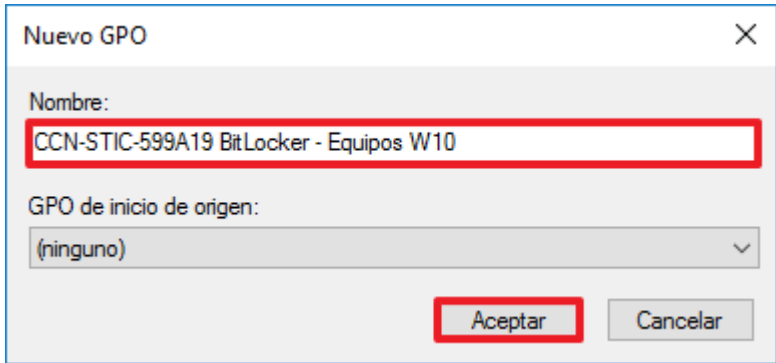
Para la configuración de BitLocker en el resto de clientes Windows 10, miembros del mismo dominio, deberá saltar estos pasos e ir directamente al paso 34, ya que esos clientes compartirán la configuración establecida en este punto y automáticamente recibirán las configuraciones al incluirse en la Unidad Organizativa "Equipos W10 con BitLocker".

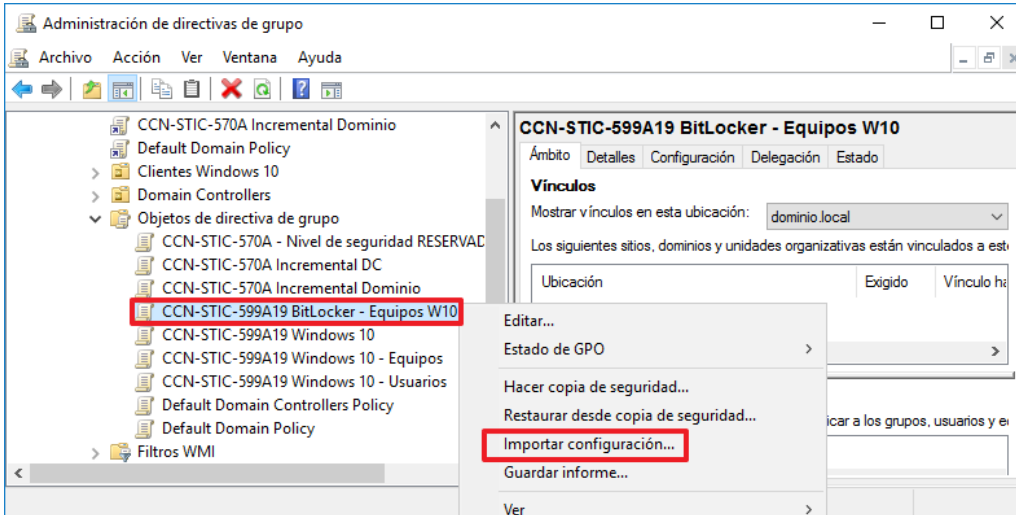
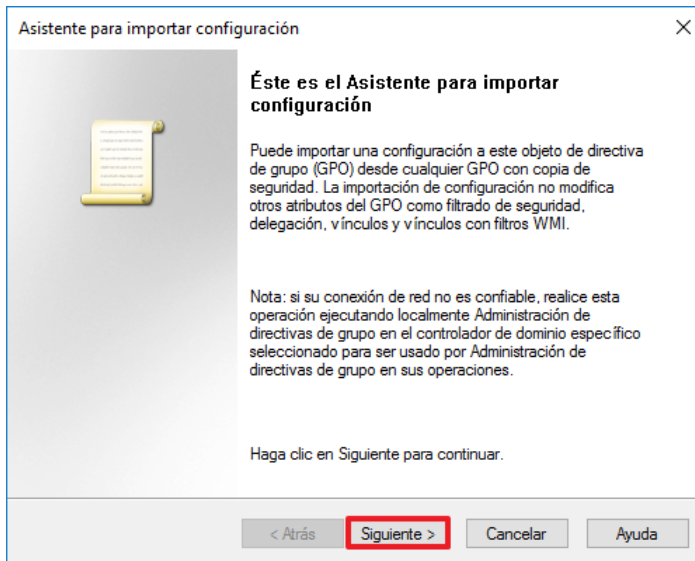
Nota: Esta guía paso a paso para la configuración de BitLocker, asume que a los servidores controladores del dominio al que pertenece el equipo cliente en el que se va a configurar BitLocker, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A IMPLEMENTACIÓN DE SEGURIDAD SOBRE MICROSOFT WINDOWS SERVER 2016, y que al propio cliente Windows 10 miembro del dominio se le ha aplicado la configuración de seguridad recomendada en la presente guía. Así mismo, si se va a emplear el navegador Internet Explorer 11, será necesario haber implementado la guía CCN-STIC-520 – Internet Explorer 11. Si no es así, aplique primero dichas guías a los controladores de dominio y al equipo cliente, antes de continuar con la configuración de BitLocker.

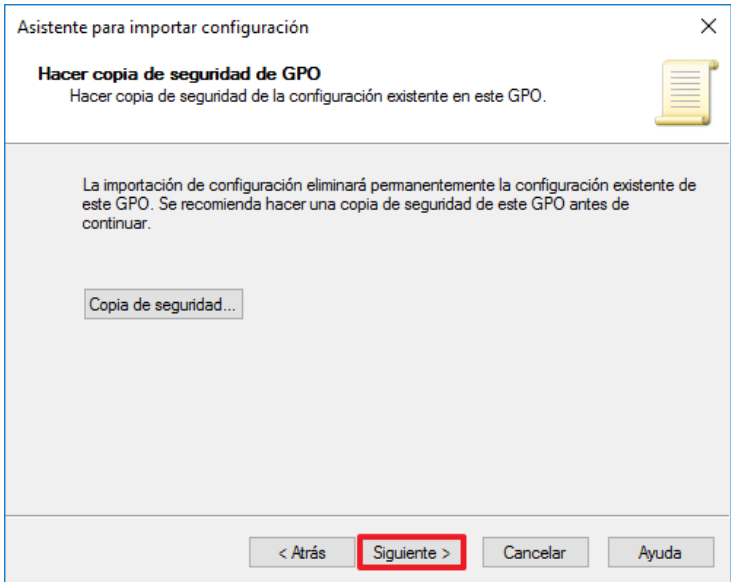
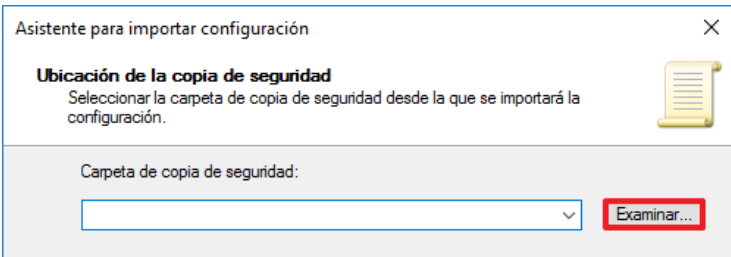
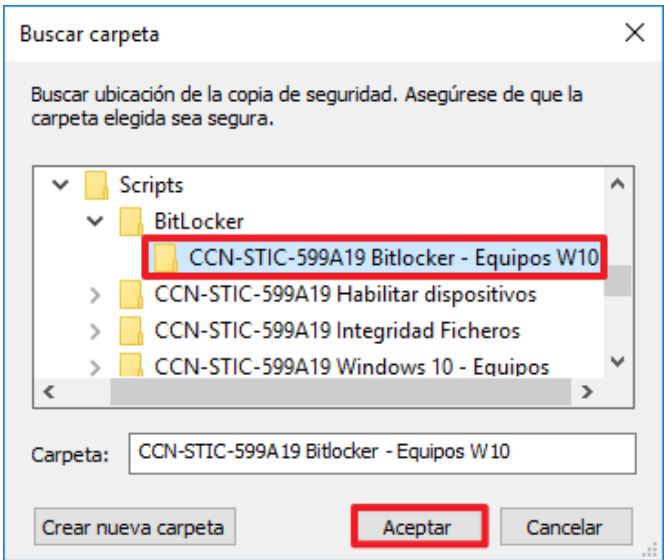
Paso	Descripción
1.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\\"
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio. Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". 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.	Asegúrese de que al menos el siguiente directorio haya sido copiado al directorio "C:\Scripts\BitLocker" del controlador de dominio. – CCN-STIC-599A19 – BitLocker Equipos W10
5.	Cree la unidad organizativa "Equipos W10 con BitLocker". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente del menú inicio. 
	Nota: El sistema le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio.

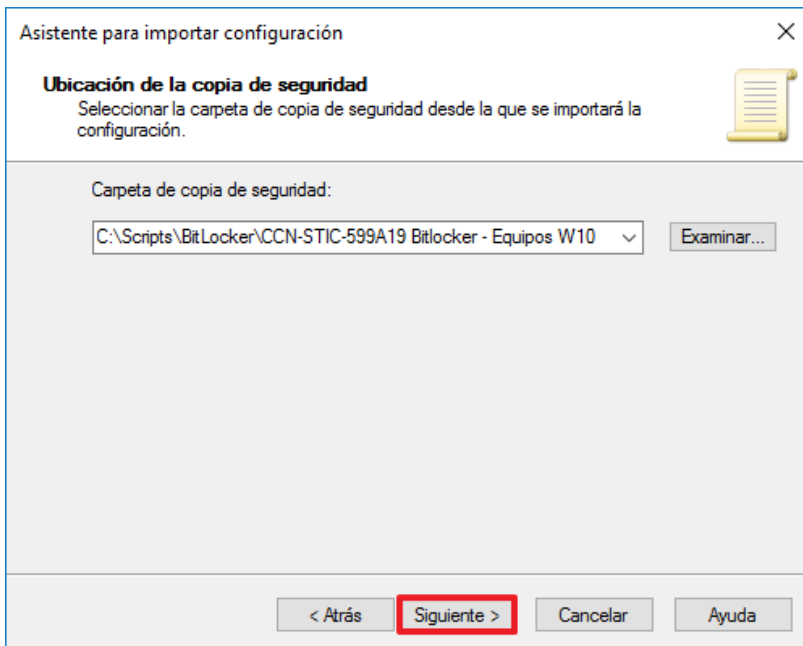
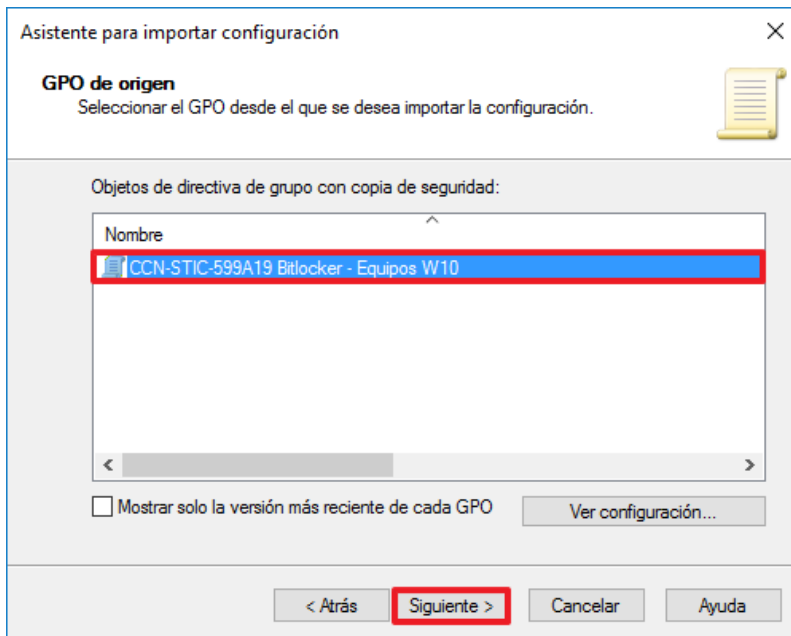
Paso	Descripción
6.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual que se ha desplegado “Usuarios y equipos de Active Directory”. 
7.	En la consola “Usuarios y equipos de Active Directory” sitúese sobre la unidad organizativa “Equipos Windows 10” y, pulsando con el botón derecho del ratón, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá, como se muestra en la siguiente figura. 

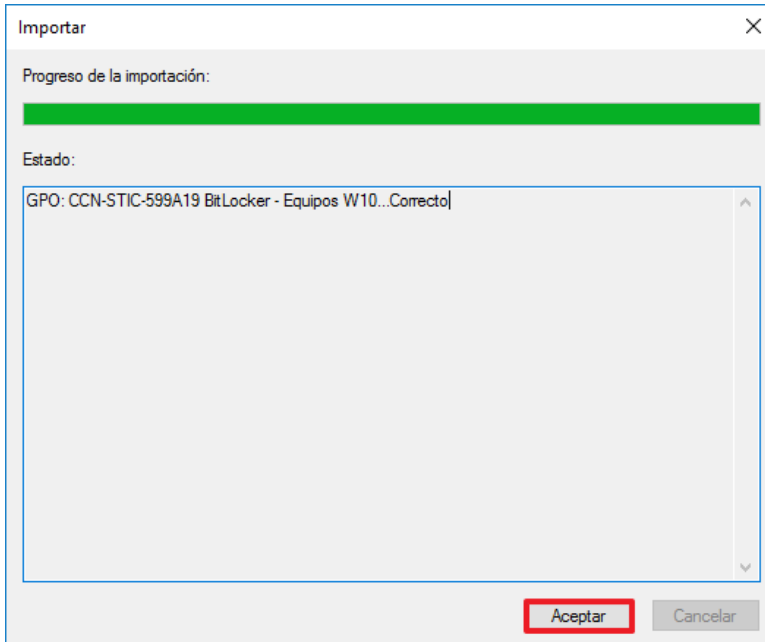
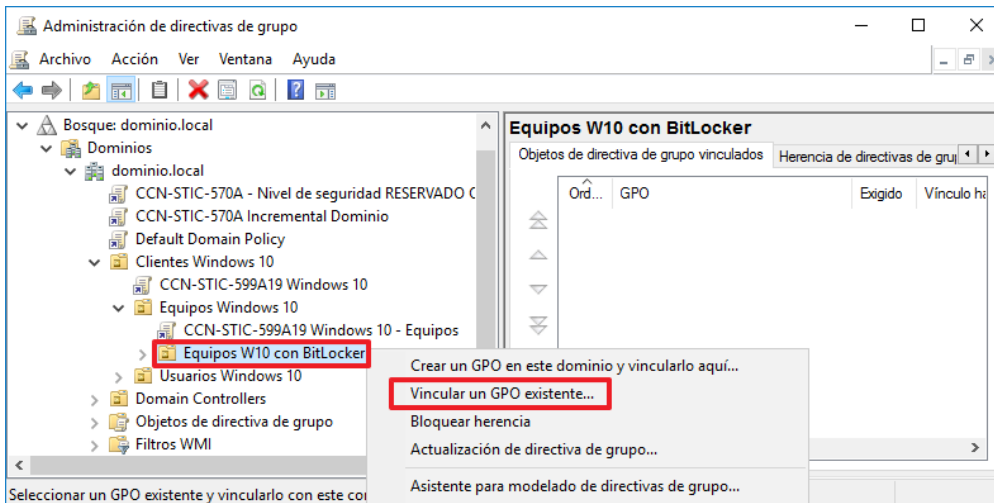
Paso	Descripción
8.	Asigne el nombre "Equipos W10 con BitLocker" a la nueva unidad organizativa, rellenando con este nombre el campo "Nombre:" del cuadro de diálogo que aparecerá y deje marcada la opción "Proteger contenedor contra eliminación accidental". A continuación, pulse "Aceptar". 
9.	Compruebe que la nueva unidad organizativa aparece colgando de "Equipos Windows 10" como se muestra en la siguiente figura. 
10.	De nuevo, utilizando la herramienta "Administrador del servidor", Seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 

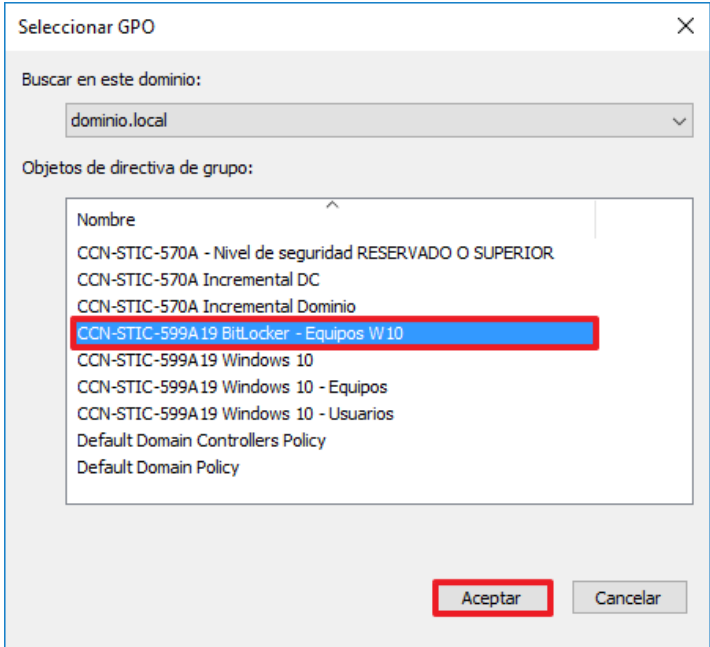
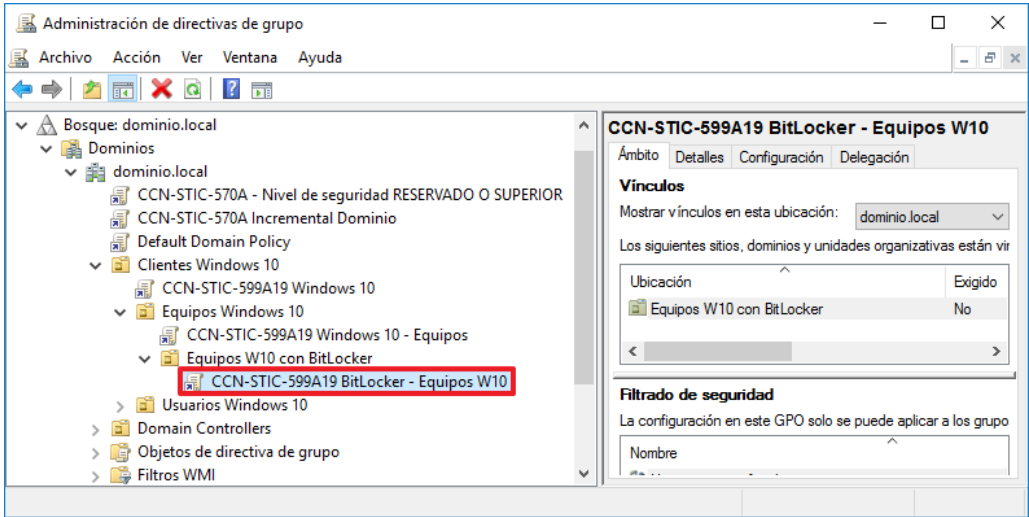
Paso	Descripción
11.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>" A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPO correspondientes. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).
12.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" con el botón derecho y elija la opción "Nuevo" del menú contextual que aparecerá. 
13.	Asigne el siguiente nombre "CCN-STIC-599A19 BitLocker – Equipos W10" a la nueva GPO y pulse “Aceptar”. 

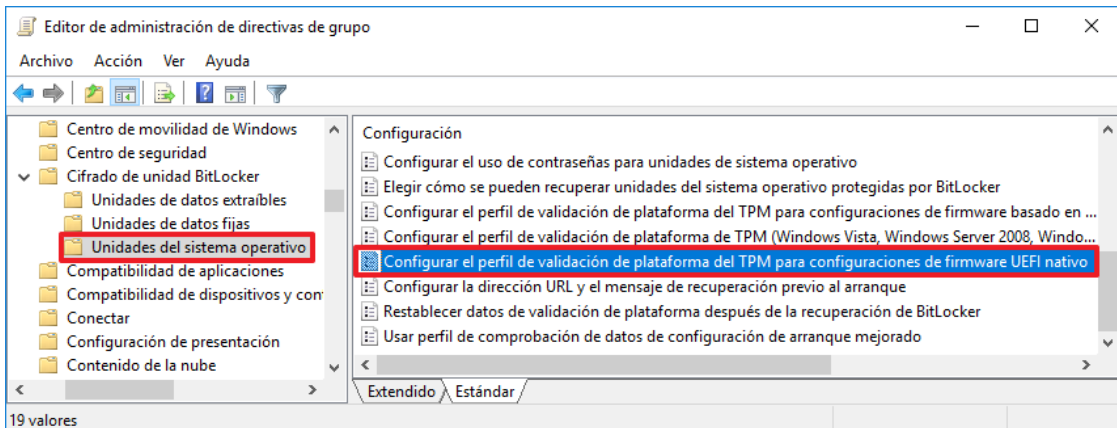
Paso	Descripción
14.	Seleccione la GPO recién creada, "CCN-STIC-599A19 BitLocker – Equipos W10" y, marcando con el botón derecho en ella, elija la opción "Importar configuración..." en el menú contextual que aparecerá. 
15.	En el "Asistente para importar configuración" pulse "Siguiente >". 

Paso	Descripción
16.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiete >" en la ventana "Hacer copia de seguridad de GPO". 
17.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 
18.	Localice la carpeta "CCN-STIC-599A19 Bitlocker – Equipos W10" y pulse "Aceptar". 

Paso	Descripción
19.	Pulse “Siguiente >” para continuar. 
20.	En “GPO de origen” pulse “Siguiente >”. 
21.	En “Examinar copia de seguridad” pulse “Siguiente >”.
22.	Pulse “Finalizar” para realizar la importación.

Paso	Descripción
23.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 
24.	Utilizando de nuevo la herramienta de “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 

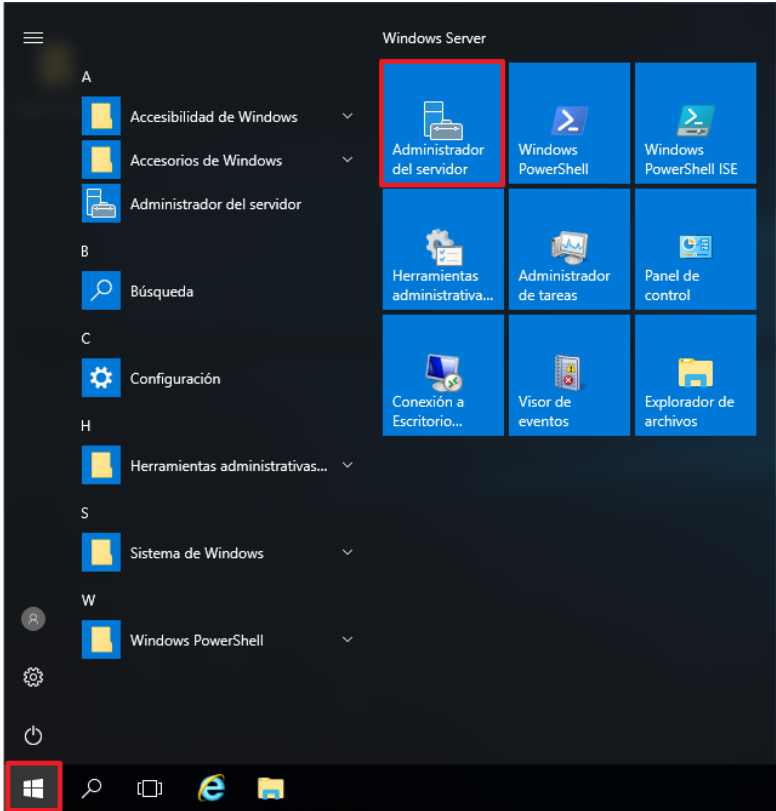
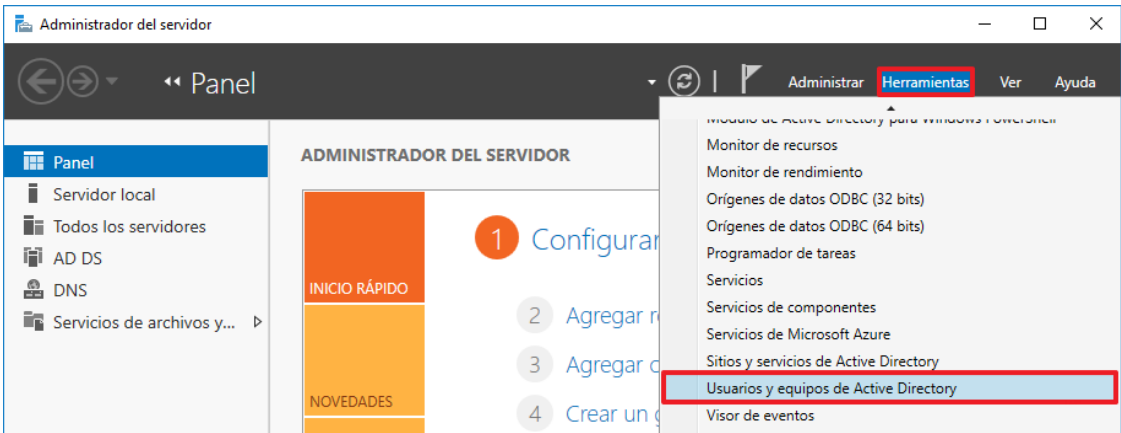
Paso	Descripción
25.	Seleccione “CCN-STIC-599A19 BitLocker – Equipos W10 - Equipos” de la lista y pulse “Aceptar”. 
26.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Equipos W10 con BitLocker”. 

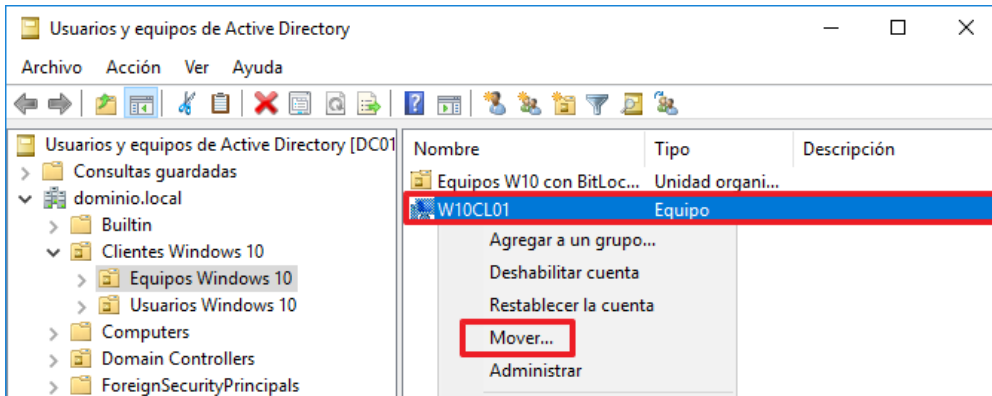
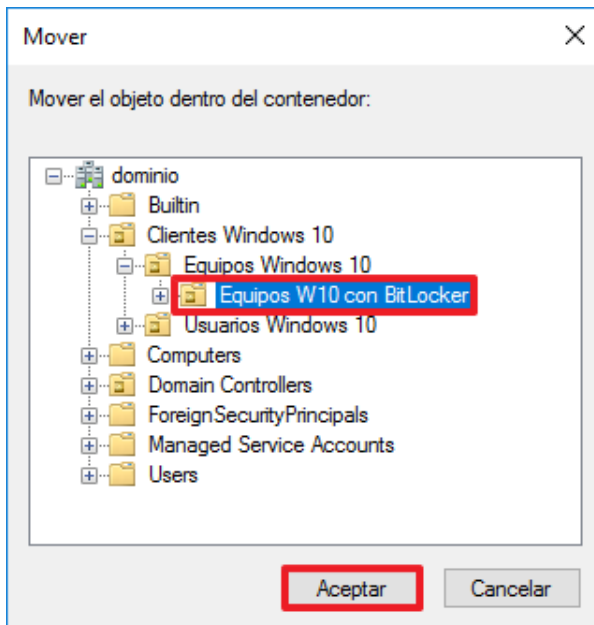
Paso	Descripción
27.	La configuración importada en la GPO desde la copia de seguridad establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si dispone de equipos con firmware UEFI nativo, deberá habilitar y configurar la directiva “Directiva CCN-STIC-599A19 BitLocker – Equipos W10 → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo → Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo” de la GPO configurada en este apartado.  The screenshot shows the Group Policy Editor window. In the left-hand navigation pane, the tree structure is expanded to 'Unidades del sistema operativo' (Operating System Drives), which is highlighted with a red box. In the right-hand pane, the list of policies is shown, and the policy 'Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo' is selected and highlighted with a red box. The policy is currently set to 'Extendido' (Extended).

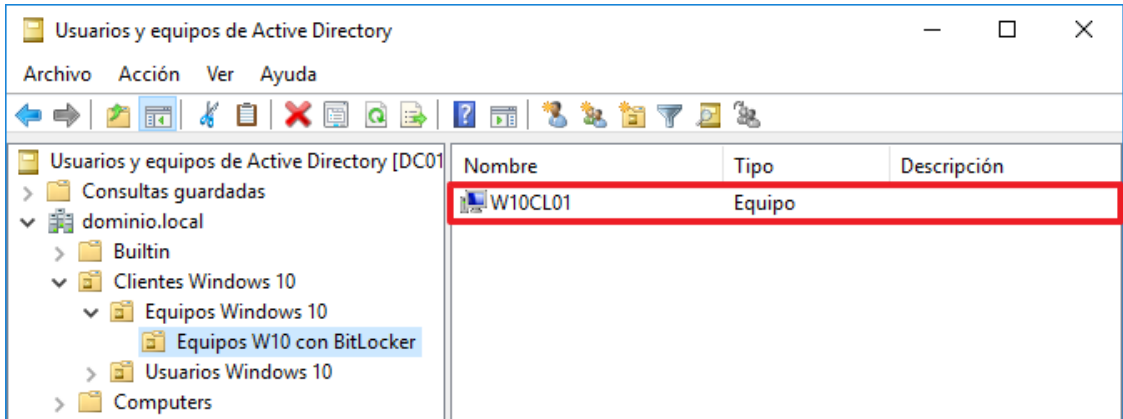
En este punto, la unidad organizativa "Equipos W10 con BitLocker" y la GPO "CCN-STIC-599A19 BitLocker - Equipos W10" están ya configuradas correctamente en Active Directory y la configuración de este último se aplicará automáticamente al equipo cliente Windows 10 miembro del dominio en el que está configurando BitLocker, y a los futuros equipos cliente Windows 10 miembros del dominio en los que también lo configure.

Los siguientes pasos deberá realizarlos en un controlador de dominio del dominio al que pertenece el equipo que está asegurando, y deberá realizarlos cada vez que necesite configurar BitLocker en un nuevo equipo cliente Windows 10 miembro del dominio, ya que se trata de trasladar, en Active Directory, la cuenta de equipo del equipo en el que está configurando BitLocker, a la unidad organizativa "Equipos W10 con BitLocker".

Paso	Descripción
28.	Inicie sesión en un servidor controlador de dominio del dominio al que pertenece el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.

Paso	Descripción
29.	Traslade, en Active Directory, la cuenta de equipo del equipo en el que está configurando BitLocker, desde su ubicación actual hasta su nueva ubicación: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker" Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
30.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Usuarios y equipos de Active Directory". 

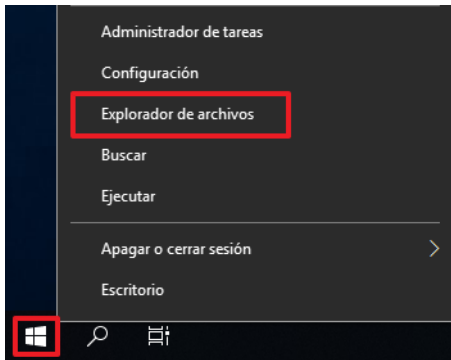
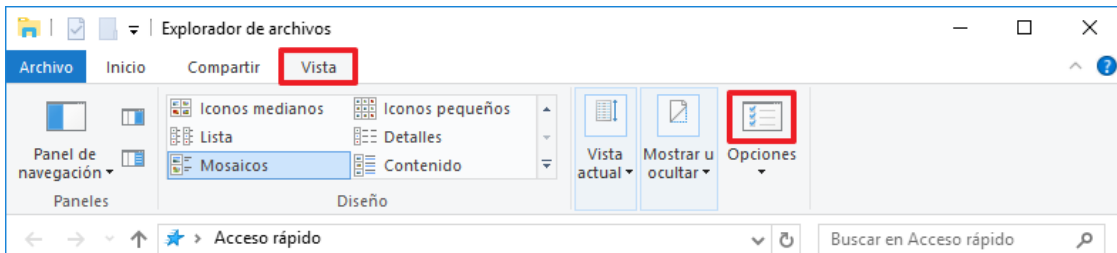
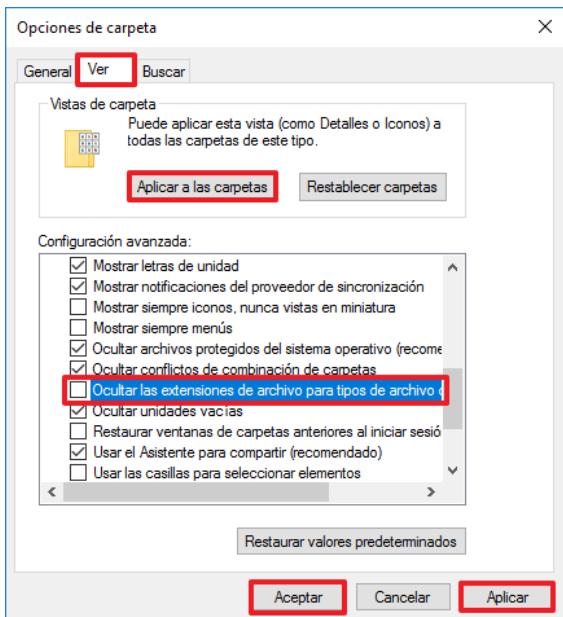
Paso	Descripción
31.	Seleccione entonces, en la parte central de la ventana, la cuenta del equipo a trasladar con el botón derecho del ratón y seleccione la opción "Mover..." del menú contextual que aparecerá, como se muestra en la siguiente figura.  Nota: En este ejemplo el nombre del equipo en el que se está configurando BitLocker se supone que es "W10CL01"
32.	En el cuadro de diálogo que aparecerá, titulado "Mover", seleccione el contenedor destino en la siguiente ruta: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker" Pulse "Aceptar" para cerrar la ventana. 

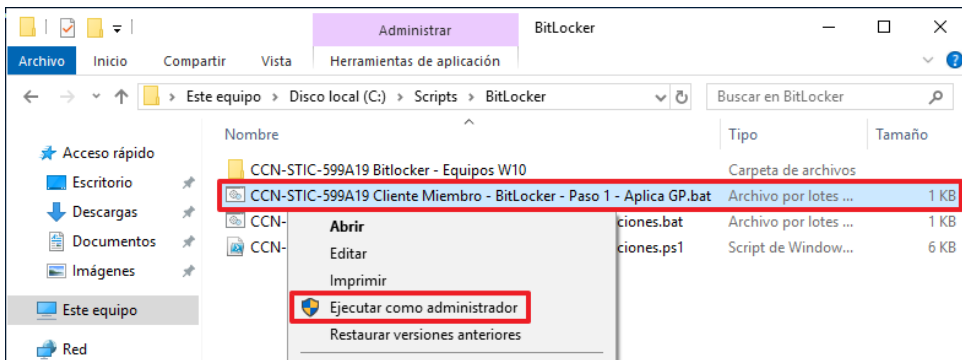
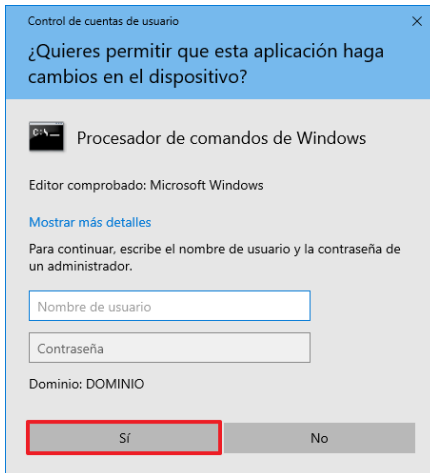
Paso	Descripción
33.	Finalmente, seleccione y expanda el siguiente contenedor: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker" Compruebe que, efectivamente, la cuenta del equipo ahora se encuentra en él: 

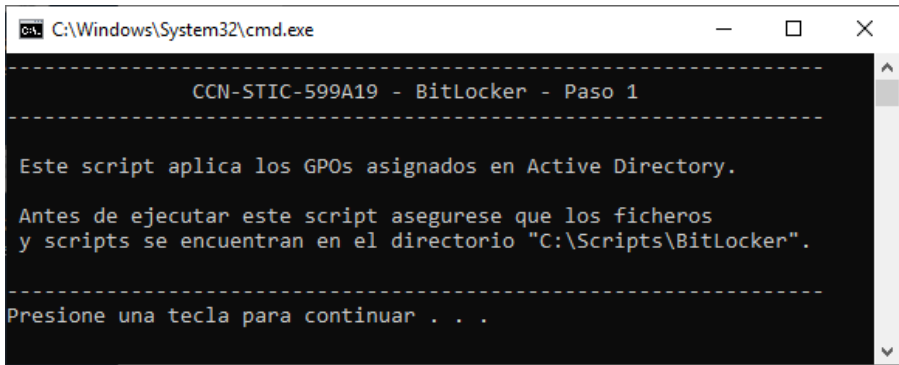
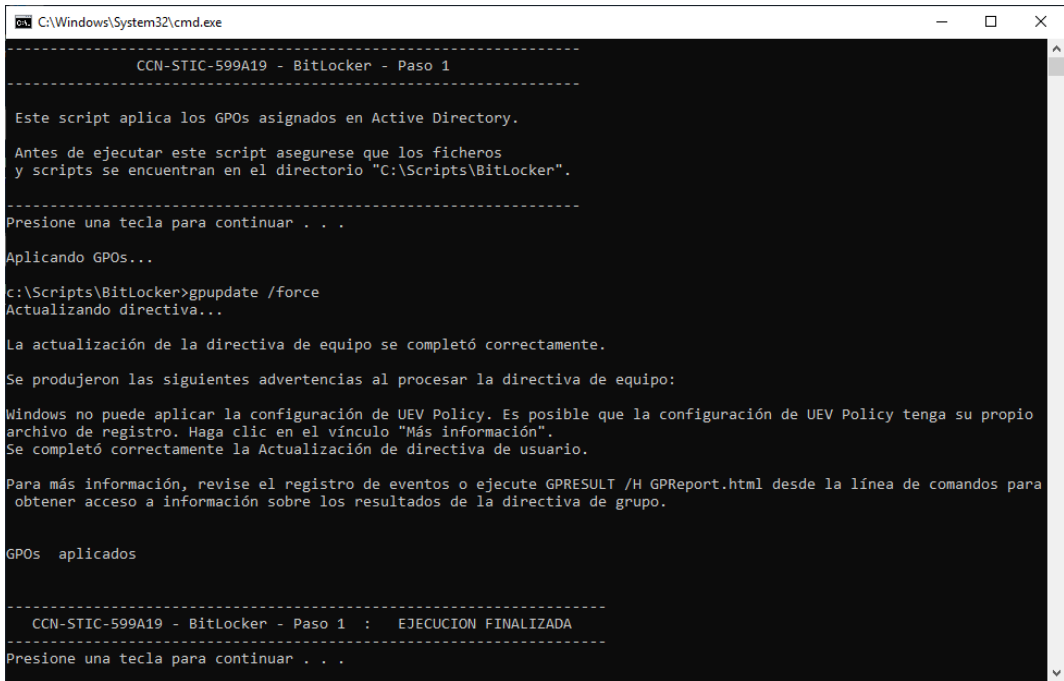
Al estar alojada la cuenta de equipo en este contenedor de Active Directory, el equipo Windows 10 miembro del dominio recibirá la configuración de equipo recomendada en esta guía para equipos con BitLocker además de los parámetros de configuración, recomendados también en esta guía, para el resto de clientes Windows 10.

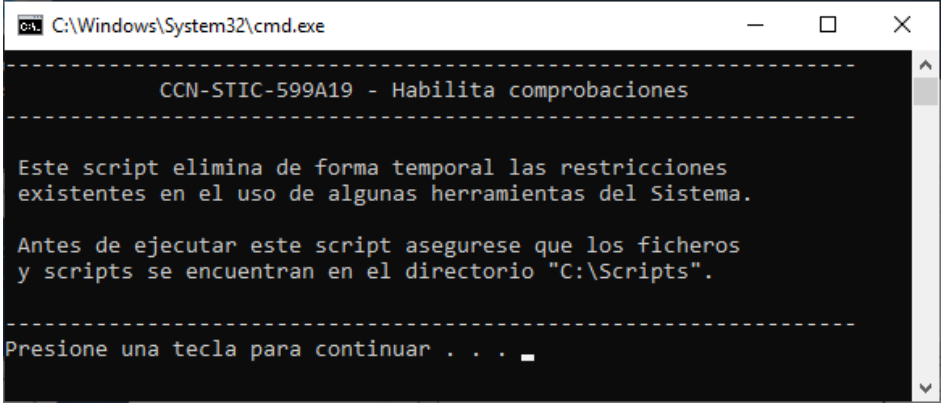
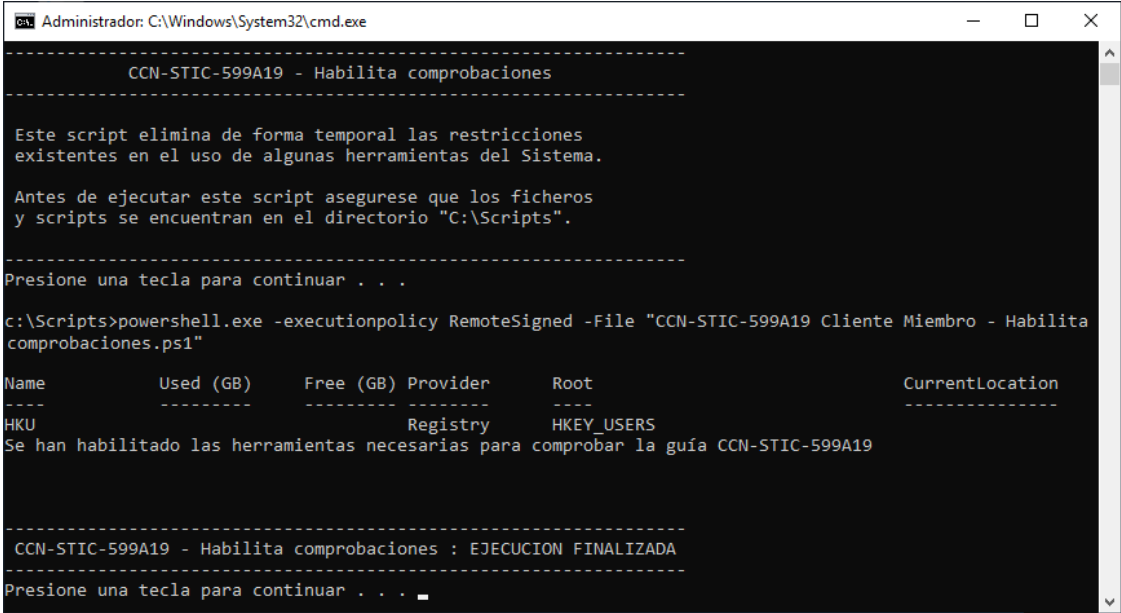
Una vez preparados la unidad organizativa "Equipos W10 con BitLocker" y la GPO "CCN-STIC-599A19 BitLocker - Equipos W10", y ubicada en Active Directory la cuenta de equipo del equipo en el que se está configurando BitLocker, realice los siguientes pasos en el equipo cliente en el que está configurando BitLocker para activar BitLocker con la configuración recomendada en esta guía.

Paso	Descripción
34.	Inicie sesión en el equipo cliente en el que está configurando BitLocker (en adelante simplemente "Equipo Cliente") con una cuenta de usuario de Windows que esté ubicada en la unidad organizativa "Usuarios Windows 10" de Active Directory y que pertenezca al grupo local "Administradores" (por ejemplo, un miembro del grupo "Admins. del dominio" y al grupo local de dominio "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.
35.	Si no existe ya, cree el directorio "Scripts" en la unidad "C:\".
36.	Copie los ficheros asociados a esta guía, incluyendo el subdirectorio "Bitlocker" con todo su contenido, en el directorio "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". 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
37.	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”. 
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, por último, pulse “Aceptar”. 

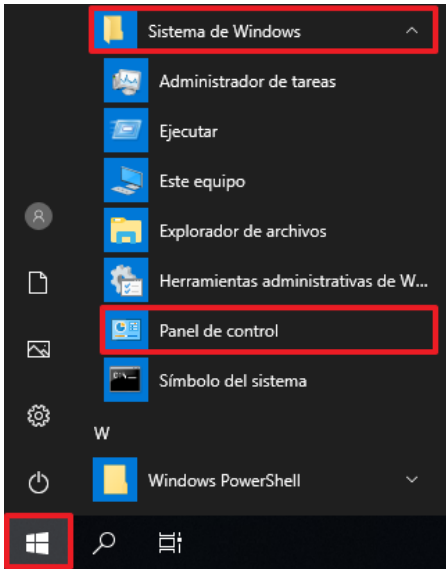
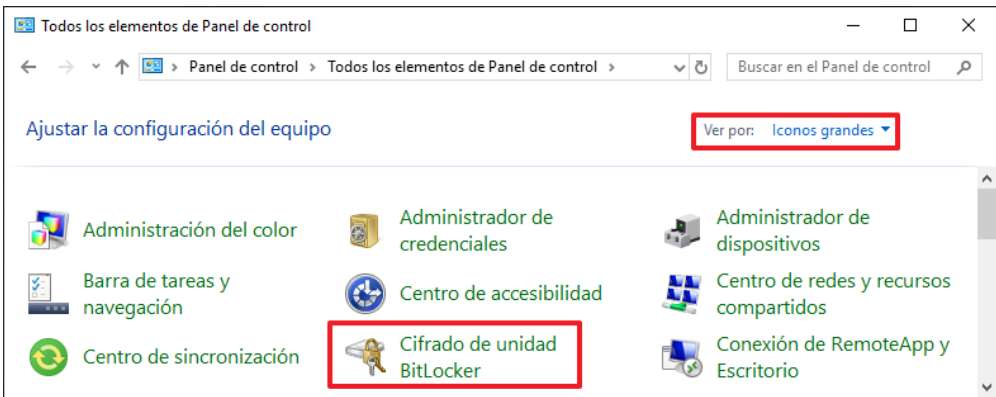
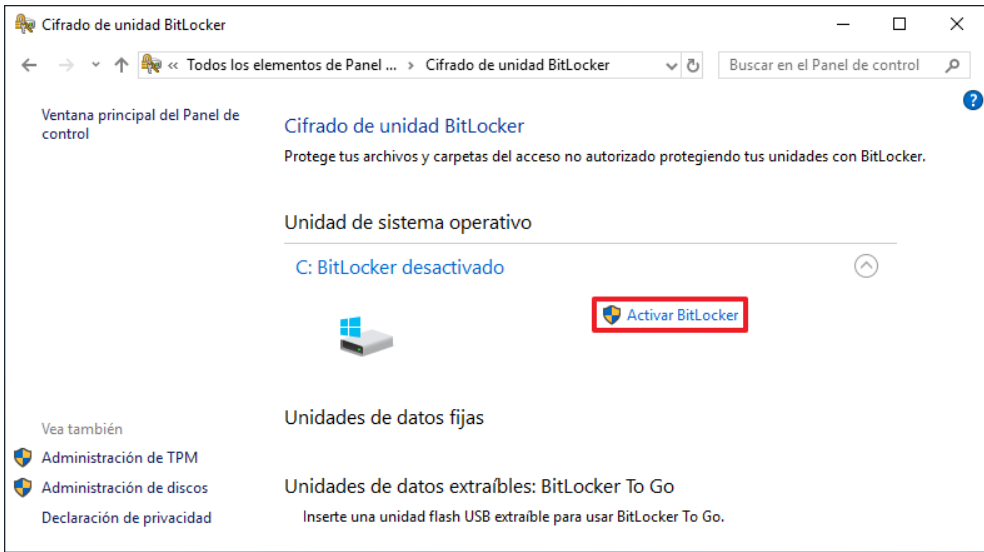
Paso	Descripción
40.	Compruebe que en el directorio “C:\Scripts” se encuentran al menos los siguientes directorios y ficheros: – BitLocker (Directorio) Dentro del directorio “BitLocker” deben estar los siguientes directorios y ficheros: – CCN-STIC-599A19 BitLocker - Equipos W10 (<i>directorio</i>) – CCN-STIC-599A19 Cliente Miembro - BitLocker - Paso 1 - Aplica GP.bat – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.ps1
41.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script " CCN-STIC-599A19 Cliente Miembro – BitLocker Paso 1 – Aplica GP.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
42.	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”. 

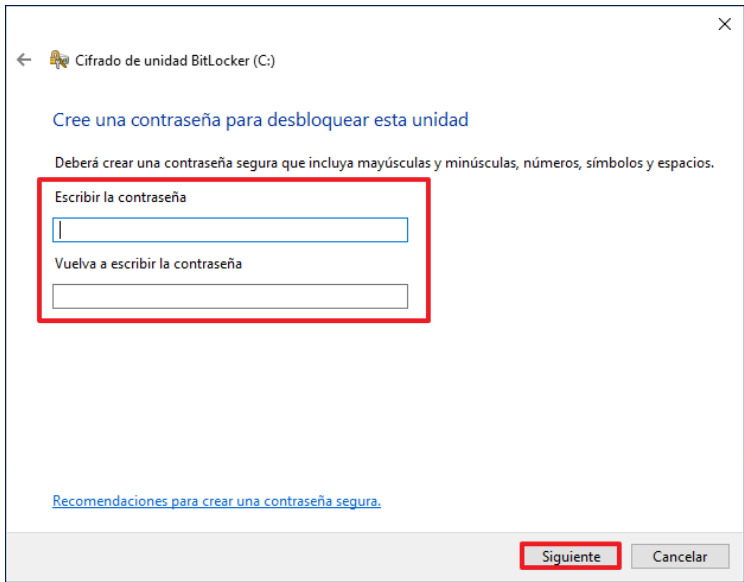
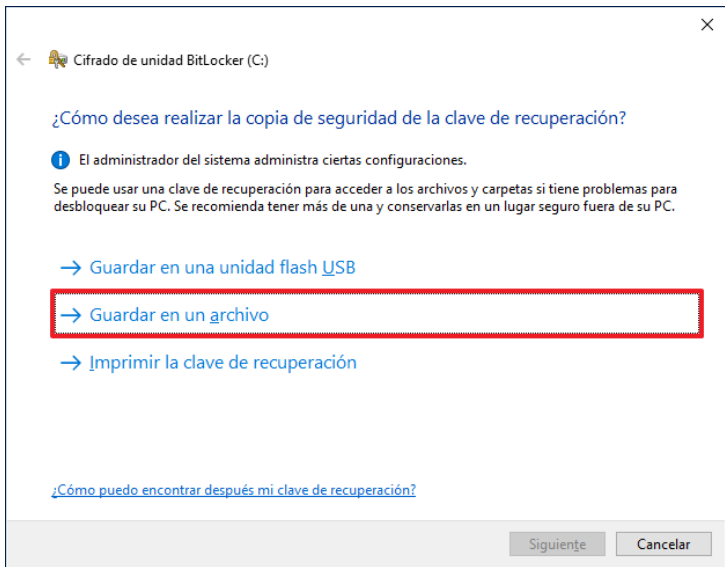
Paso	Descripción
43.	Este script aplica las GPO definidas en Active Directory y que aplican al equipo y usuario actuales. Las GPO se aplican periódicamente de forma automática, pero de esta forma se asegura la configuración definida en las GPO de Active Directory, incluido el añadido para la configuración de BitLocker, haya sido aplicada al equipo antes de que se realicen el resto de pasos. Pulse una tecla para continuar. 
44.	Se actualizarán las directivas de equipo. La pantalla podrá mostrar una serie de advertencias relativas a la aplicación de las directivas. Estas advertencias se deben a un servicio deshabilitado, pero puede ignorarlas ya que la política ha aplicado correctamente. Pulse una tecla para continuar y cerrar la ventana. 

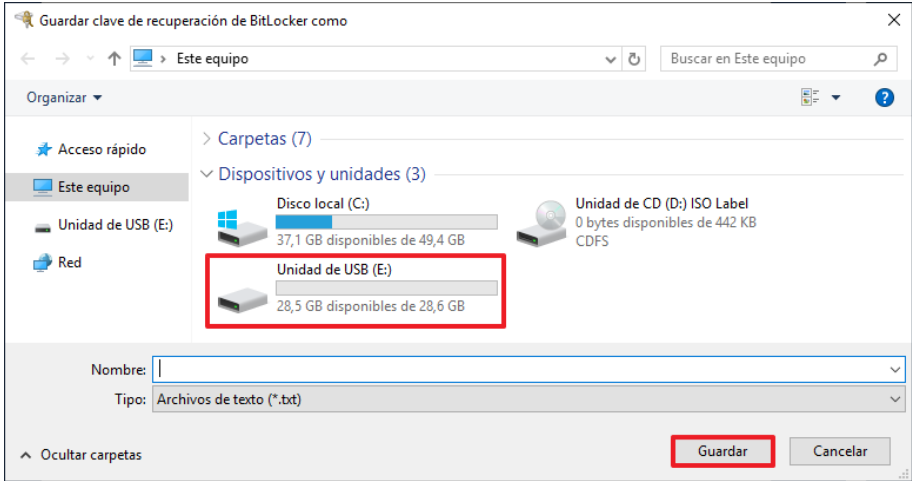
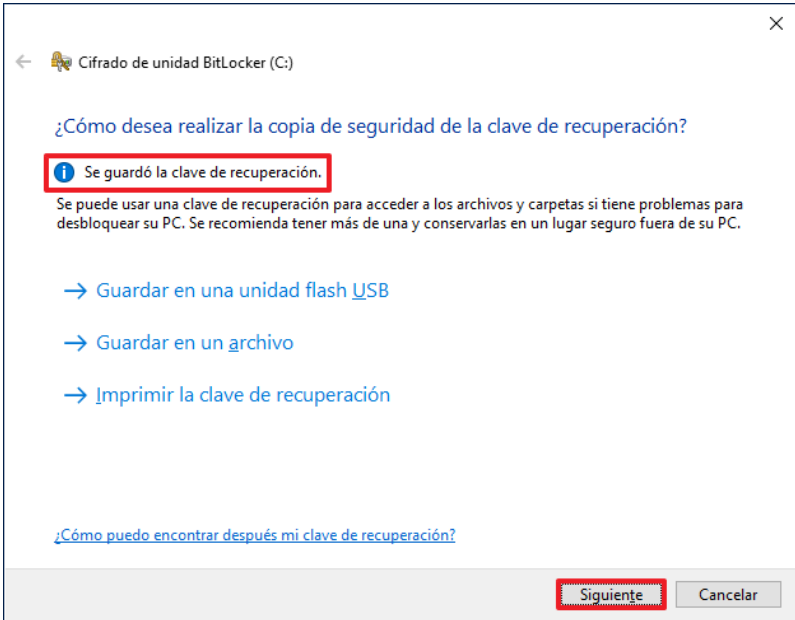
Paso	Descripción
45.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.bat" desde el directorio "C:\Scripts\Bitlocker". Este paso será necesario para habilitar temporalmente características necesarias para continuar con los pasos siguientes. Pulse una tecla para continuar.  Nota: El sistema le solicitará elevación de privilegios.
46.	Pulse una tecla de nuevo para finalizar el proceso. 

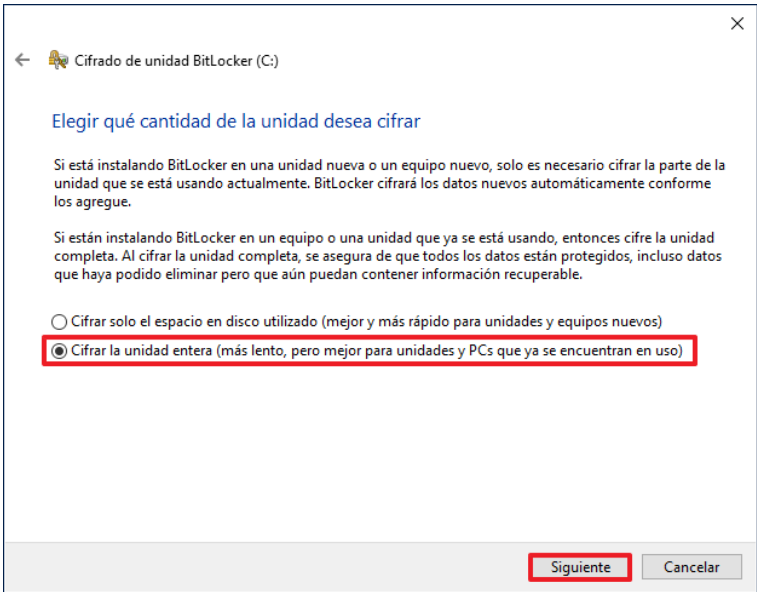
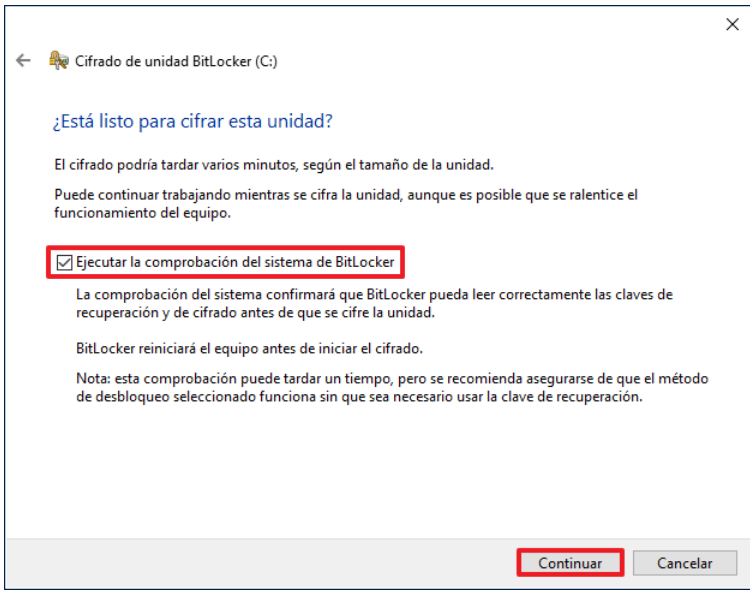
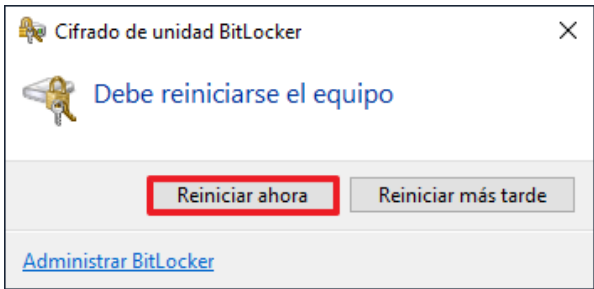
Los siguientes pasos describen el procedimiento para activar el cifrado de unidad BitLocker con contraseña.

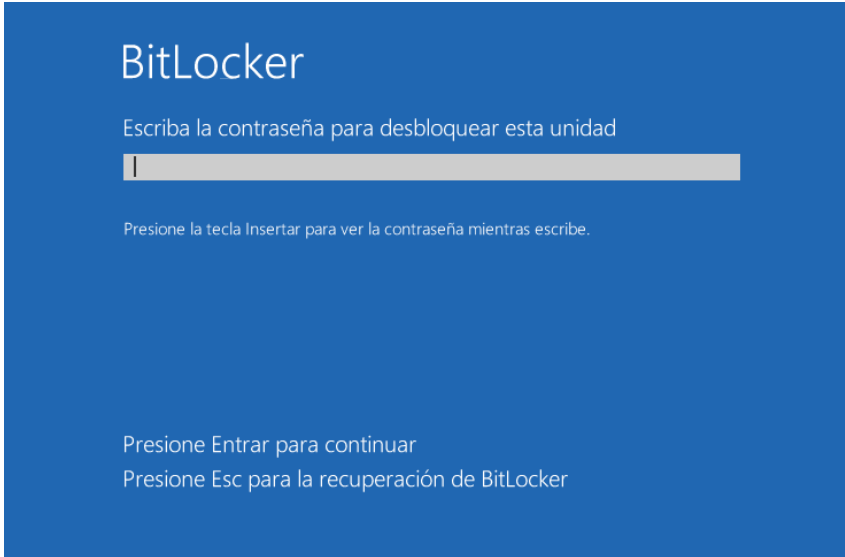
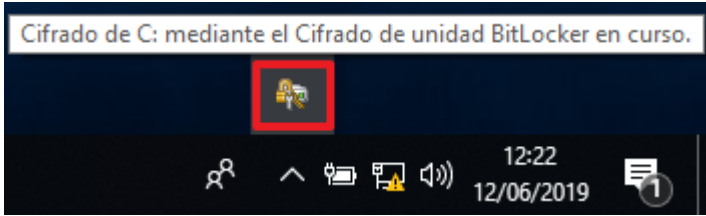
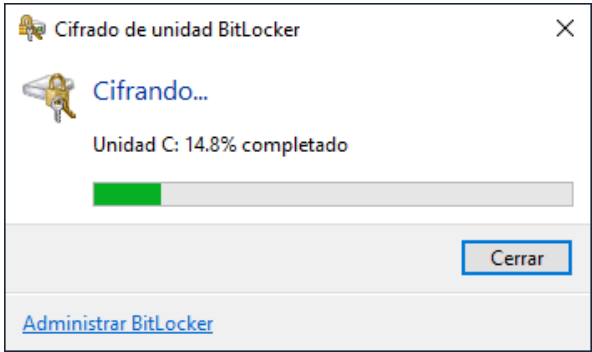
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números.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

Paso	Descripción
47.	Abra el panel de control desde “Inicio → Sistema de Windows → Panel de control”. 
48.	Establezca la vista en “Iconos grandes” y pulse en “Cifrado de unidad BitLocker”. 
49.	Pulse sobre “Activar Bitlocker” como se indica en la siguiente figura. 

Paso	Descripción
50.	El sistema le solicitará elevación de privilegios. Introduzca credenciales de administrador en la ventana “Control de cuentas de usuario”.
51.	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.
52.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
53.	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 almacenada sobre la misma unidad que se está cifrando ni en otra unidad que este cifrada.
54.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

Paso	Descripción
55.	Elija la opción de “Cifrar la unidad entera” y pulse “Siguiente”. 
56.	Marque la opción "Ejecutar la comprobación del sistema de BitLocker" y pulse el botón "Continuar". 
57.	Reinicie el equipo para continuar con el proceso de cifrado de la unidad. 

Paso	Descripción
58.	Al reiniciar, el sistema le pedirá la contraseña de cifrado de unidad BitLocker. Introduzca la contraseña y pulse “Enter” para continuar.  The image shows the BitLocker password prompt screen. It has a blue background with the text 'BitLocker' at the top. Below it, it says 'Escriba la contraseña para desbloquear esta unidad' (Enter the password to unlock this drive). There is a text input field with a cursor. Below the input field, it says 'Presione la tecla Insertar para ver la contraseña mientras escribe.' (Press the Insert key to see the password while you type). At the bottom, it says 'Presione Entrar para continuar' (Press Enter to continue) and 'Presione Esc para la recuperación de BitLocker' (Press Esc for BitLocker recovery).
59.	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:  The image shows a Windows taskbar notification for BitLocker encryption. The notification bar is dark blue with the text 'Cifrado de C: mediante el Cifrado de unidad BitLocker en curso.' (C: drive encryption using BitLocker drive encryption in progress). Below the text is a small icon of a key and a shield. The taskbar also shows the system clock as 12:22 on 12/06/2019 and a notification icon with a '1'.
60.	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.  The image shows a BitLocker encryption progress window. The window title is 'Cifrado de unidad BitLocker'. It has a close button (X) in the top right corner. The window contains a key icon and the text 'Cifrando...' (Encrypting...). Below that, it says 'Unidad C: 14.8% completado' (Unit C: 14.8% completed). There is a progress bar with a green segment representing the progress. At the bottom right, there is a 'Cerrar' (Close) button. At the bottom left, there is a link 'Administrar BitLocker' (Manage BitLocker). Continúe con los siguientes pasos, aunque no haya finalizado este proceso de cifrado inicial del disco.

Paso	Descripción
61.	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.
62.	Eliminé el directorio “C:\Scripts”. Nota: Todos los volúmenes NTFS del Sistema deberán de 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

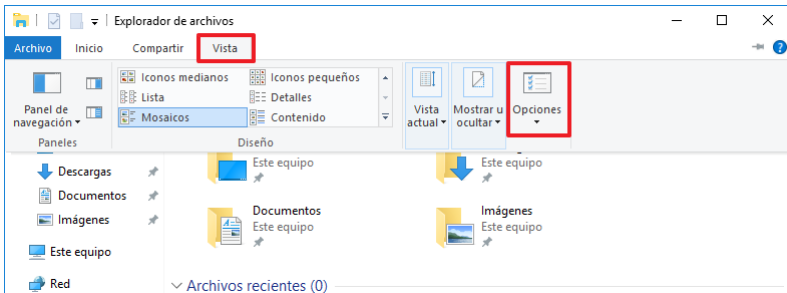
6. LISTA DE COMPROBACIÓN – BITLOCKER

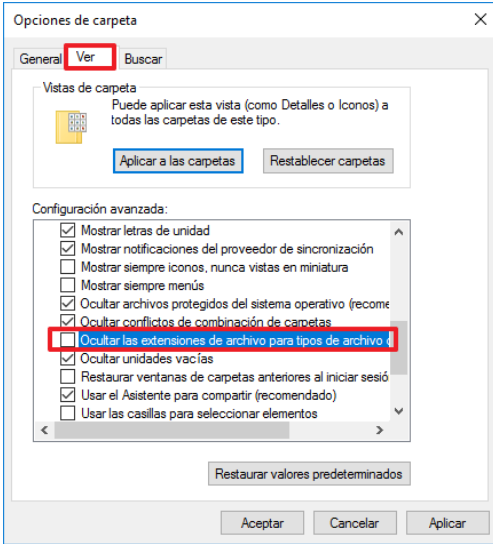
Este anexo se ha diseñado para ayudar a los operadores a verificar que se ha implementado el cifrado de unidad BitLocker en un equipo cliente Windows 10 versión 1809 miembro de un dominio. La lista de comprobación deberá ejecutarse iniciando sesión en el equipo propio cliente con la cuenta de un usuario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

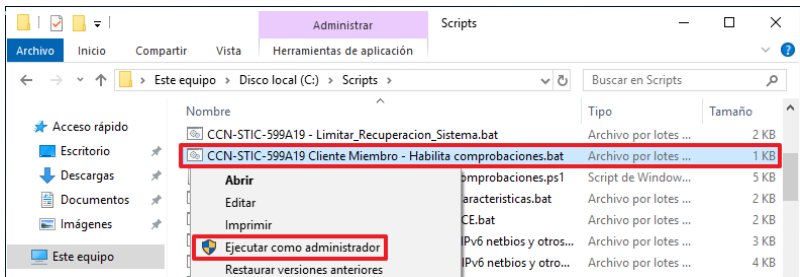
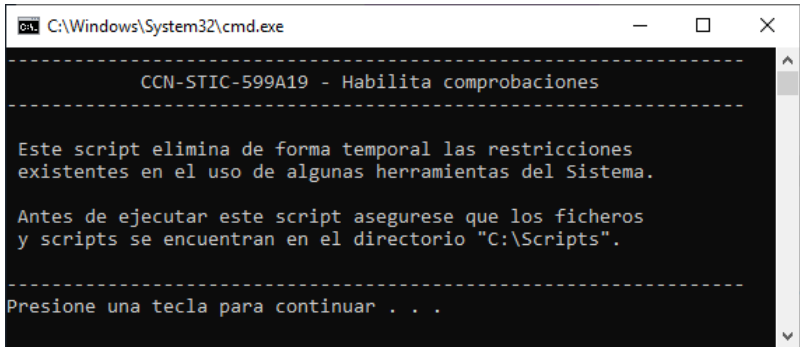
Nota: No podrá utilizar la cuenta integrada de administrador porque esta se encontrará deshabilitada, debido a la aplicación de la configuración de seguridad.

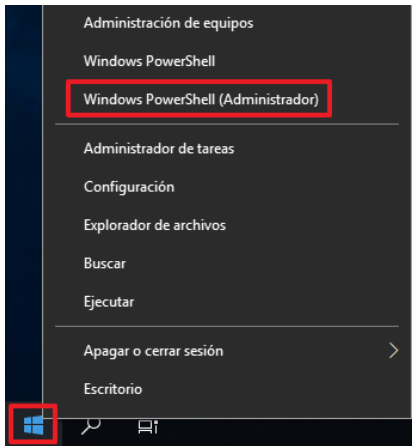
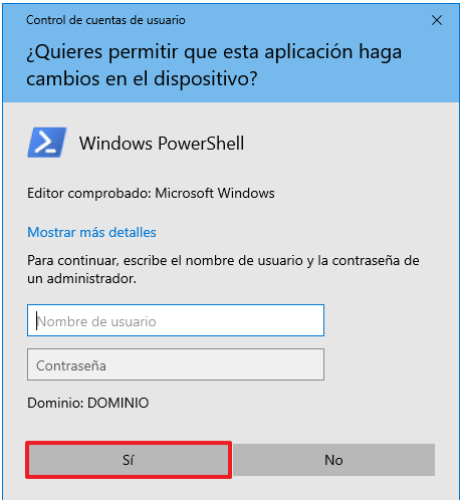
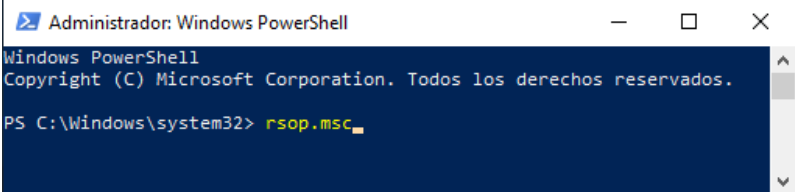
Para realizar algunas de las comprobaciones será necesario ejecutar diferentes consolas de administración y herramientas del sistema. Estas herramientas estarán disponibles si no se ha prohibido la utilización de las mismas. Uno de los primeros pasos, por tanto, consistirá en habilitar temporalmente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

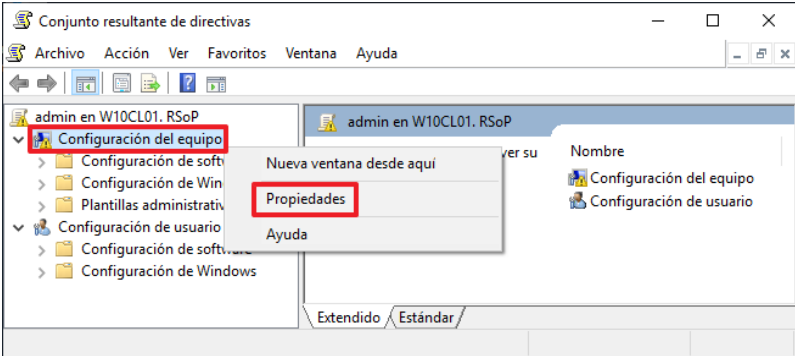
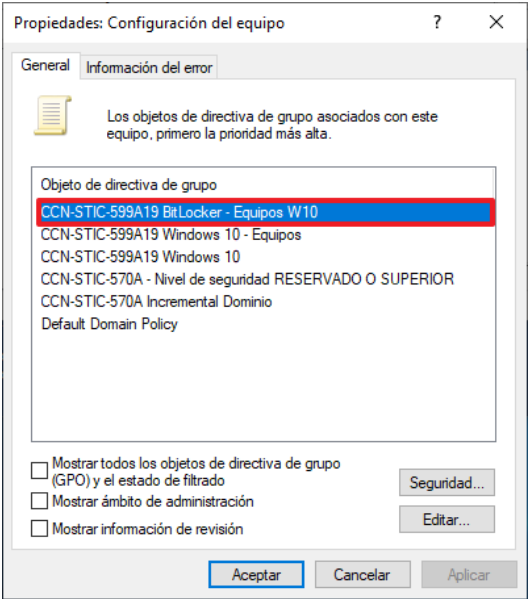
- Explorador de Windows (explorer.exe)
- Windows PowerShell (PowerShell.exe)
- Conjunto resultante de directivas (rsop.msc)
- Panel de control (control.exe)
- Administración de servicios (services.msc)

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 de Windows que esté ubicada en la unidad organizativa "Usuarios Windows 10" de Active Directory y que pertenezca al grupo local "Administradores" (por ejemplo, un miembro del grupo "Admins. del dominio") y al grupo local de dominio "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.
2. Configure 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 (clic derecho) → Explorador de Windows" En el menú superior pulse sobre "Vista" y seleccione "Opciones". 

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione la pestaña “Ver” y dentro de dicho menú, “Opciones de carpeta...”. De la ventana que aparecerá, 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”.
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:” y copie en él al menos los siguientes dos scripts, los cuales están incluidos entre los ficheros que acompañan a esta guía: – CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.ps1 Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”. Aunque en el subdirectorio “Bitlocker” de los ficheros que acompañan a esta guía existen también unos ficheros similares, para esta lista de comprobación bastará con utilizar los scripts indicados, directamente en el directorio “C:\Scripts”.

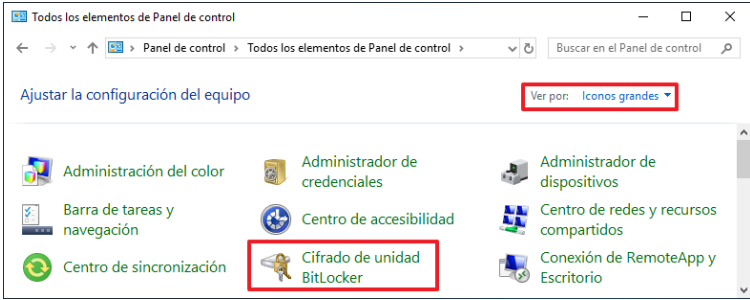
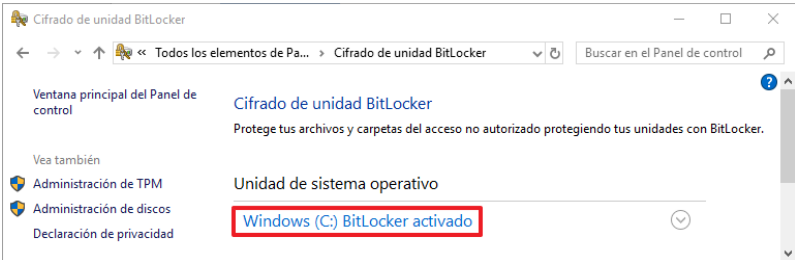
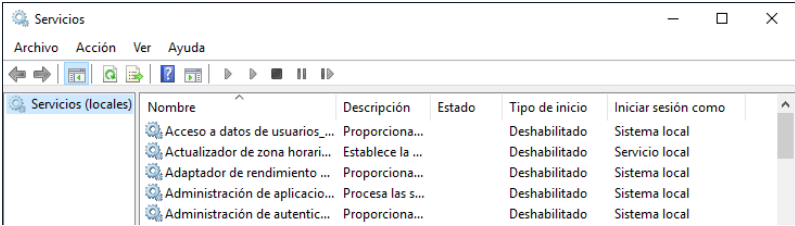
Comprobación	OK/NOK	Cómo hacerlo
4. Ejecute el script que habilita temporalmente las consolas de administración restringidas		Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat". Para ello, visualice la 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 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 administrador y pulse "Sí".
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.

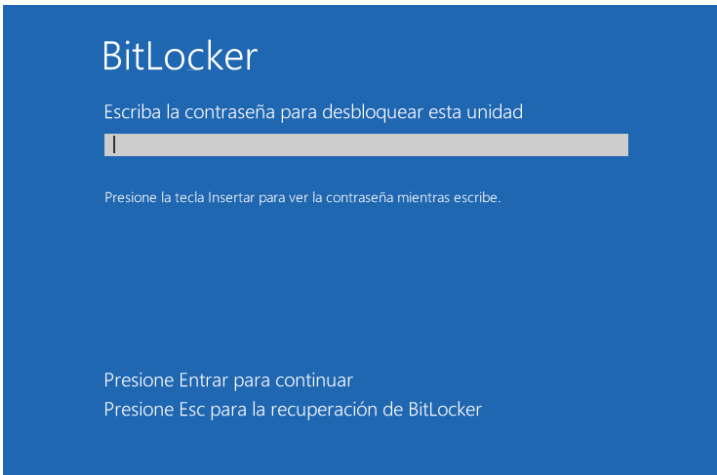
Comprobación	OK/NOK	Cómo hacerlo
6. Lance una ventana de PowerShell con permisos de administrador, para lanzar desde ella en pasos posteriores comandos con permisos de administrador		Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”.  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.  Tras introducir las credenciales de un usuario administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.
7. Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse “Enter” para abrir la consola de administración "Conjunto resultante de directivas". 

Comprobación	OK/NOK	Cómo hacerlo
8. Verifique que el equipo ha recibido correctamente la directiva de grupo "CCN-STIC-599A19 Bitlocker – Equipos W10"		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", la política deberá aparecer y "CCN-STIC-599A19 Bitlocker – Equipos W10" deberá estar situada encima del resto de directivas, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al usuario del equipo que está comprobando. Deberá asegurarse de que al menos el objeto " CCN-STIC-599A19 Bitlocker – Equipos W10" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

Comprobación	OK/NOK	Cómo hacerlo		
	Parámetro			OK/NOK
	CCN-STIC-599A19 Bitlocker – Equipos W10			
	CCN-STIC-599A19 Windows 10 - Equipos			
	CCN-STIC-599A19 Windows 10			
	CCN-STIC-570A Incremental Dominio			
	Default Domain Policy			
		Cierre la ventana de “Propiedades” pero no cierre aún la consola de administración “Conjunto resultante de directivas”.		
9. Compruebe que se han aplicado los valores correctos de directivas de grupo relativos a los servicios del sistema.	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 de equipo → Configuración de Windows → Configuración de seguridad → Servicios del sistema"			
	Servicio		Tipo de inicio	OK/NOK
	Servicio Cifrado de unidad BitLocker (bdesvc)		Automático	
	Detección de hardware Shell (shellhwdetection)		Automático	
10. Verifique la configuración 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		
11.Verifique la configuración 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	
12.Verifique la configuración 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
		Ya puede cerrar la consola de administración Conjunto resultante de directivas.
13. 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".
14. 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
		Servicio Cifrado de unidad BitLocker (bdesvc)	Automático
		Detección de hardware Shell (shellhwdetection)	Automático
		Cierre la consola de administración de servicios.	
15. Borre el directorio "C:\Scripts"		Borre el directorio "C:\Scripts" con todo su contenido.	
16. Reinicie el equipo		Reinicie el equipo para comprobar que BitLocker solicita el código PIN para acceder a la unidad de sistema.	
17. Compruebe que el sistema tiene configurado cifrado de unidad BitLocker con la opción de PIN de arranque.		Al reiniciarse el equipo, compruebe que el sistema requiere que se introduzca el PIN para desbloquear la unidad, como se muestra en la siguiente figura. 	
18. 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.2.2. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19

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-599A19.

Para permitir el uso de dispositivos USB en equipos a los que se les ha aplicado la guía CCN-STIC-599A19, será necesaria la creación de una unidad organizativa a la que pertenecerán todos aquellos equipos en los que se hará uso de dispositivos USB y, sobre ese grupo creado, se aplicará una política de grupo mediante un controlador de dominio del dominio al que pertenecen dichos equipos.

Este anexo muestra, en su primer apartado, la configuración de los diferentes elementos que modifica, a través de GPOs, la política creada y denominada “CCN-STIC-599A19 – Habilitar dispositivos”. Así mismo, muestra una guía paso a paso con la operativa a seguir para poder implementar dicha política en los equipos deseados.

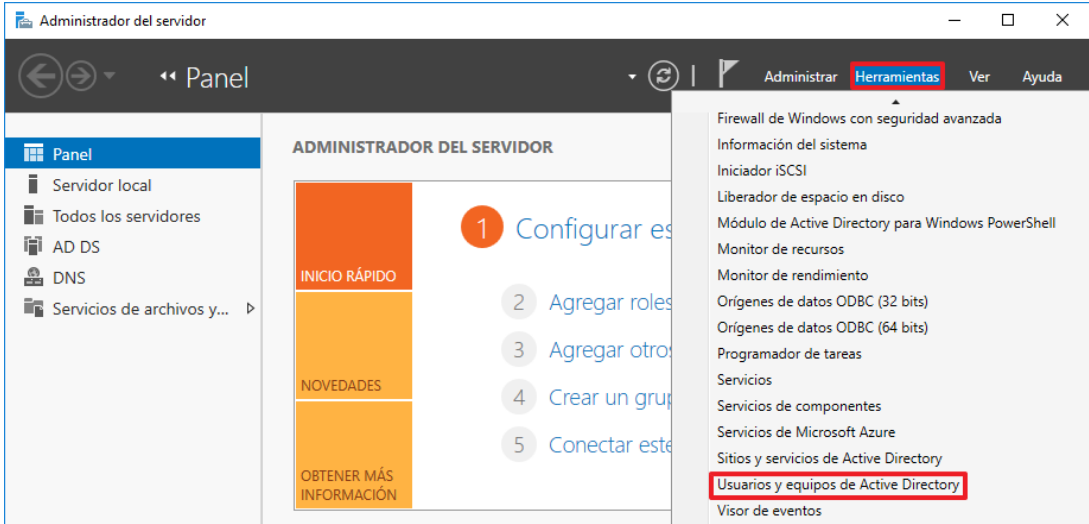
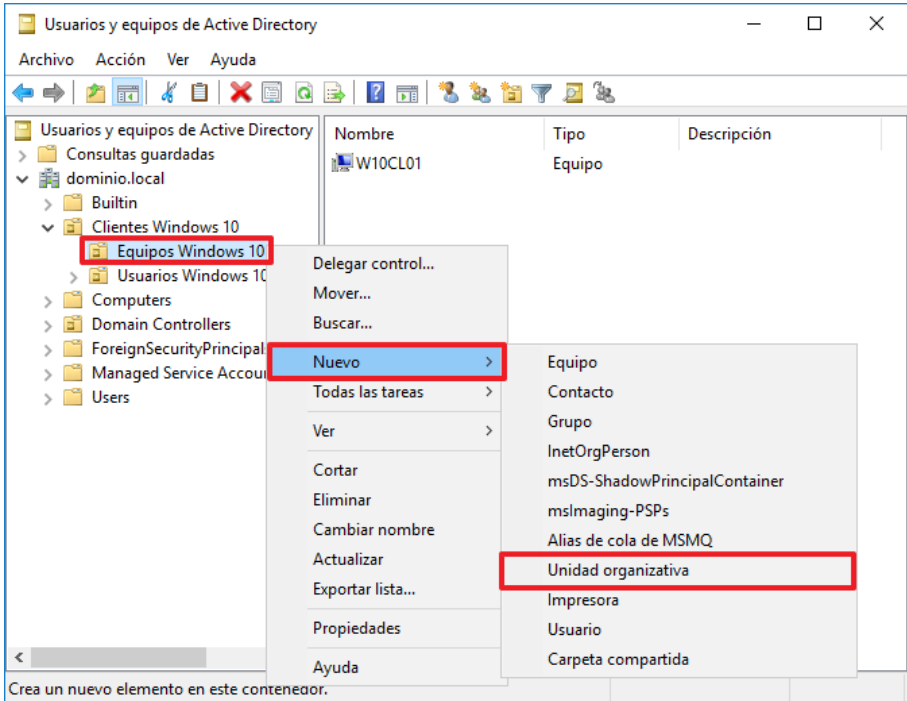
En los puntos posteriores se muestran dos procedimientos para habilitar el uso de dispositivos USB. Los métodos para permitir el uso de dispositivos conectados mediante USB son los siguientes:

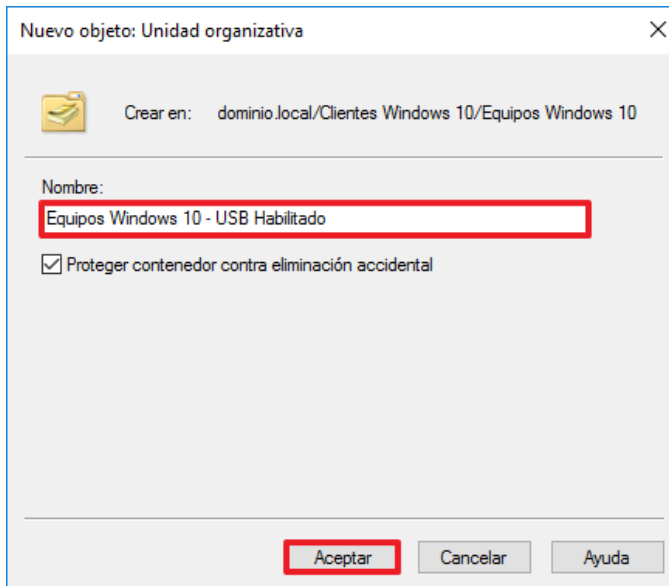
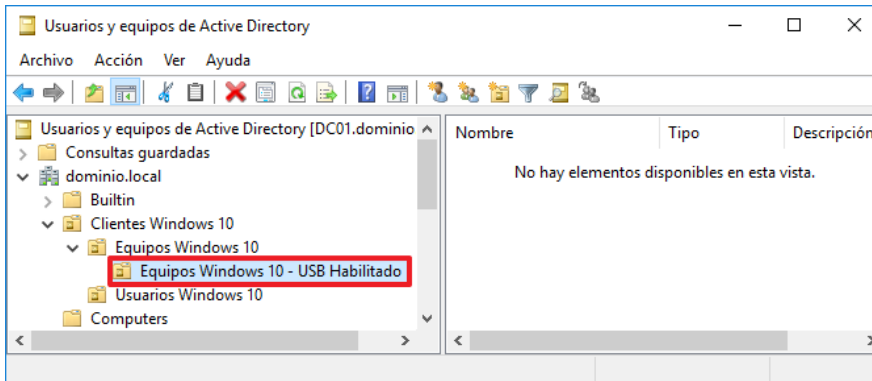
- a) Instalación de controladores mediante el uso de un usuario administrador de la máquina.
- b) Filtrado de USB mediante el uso de los identificadores de dispositivo USB.

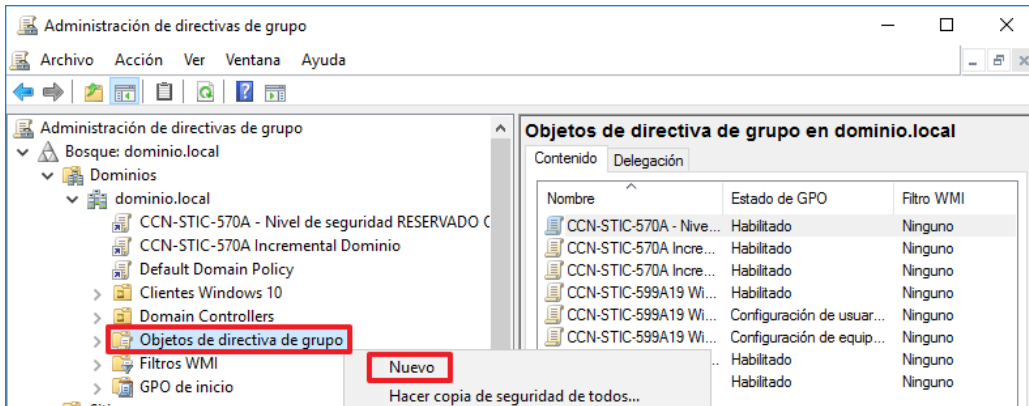
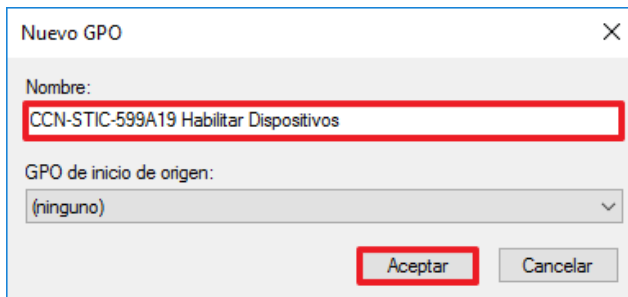
1. PREPARACIÓN DEL DIRECTORIO ACTIVO

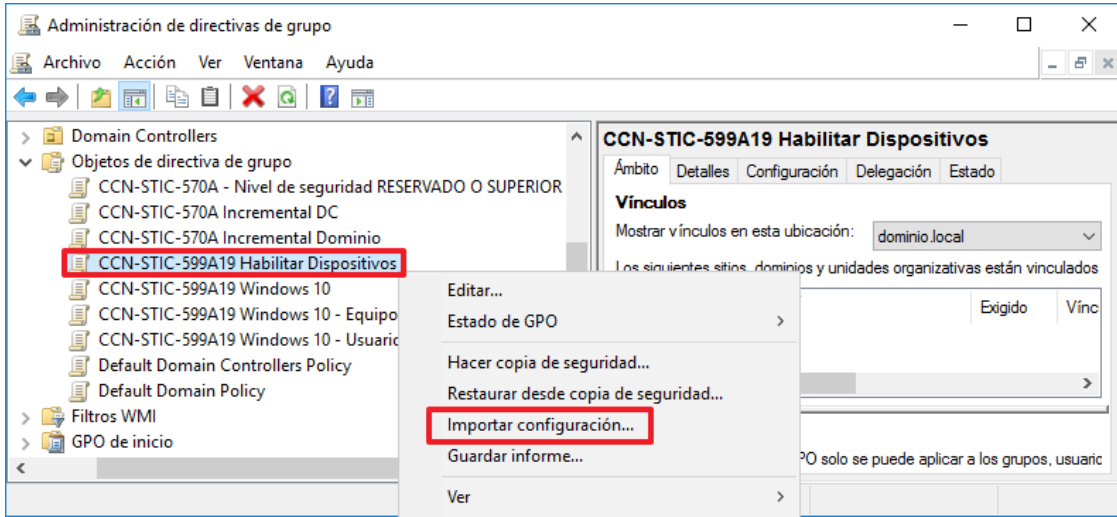
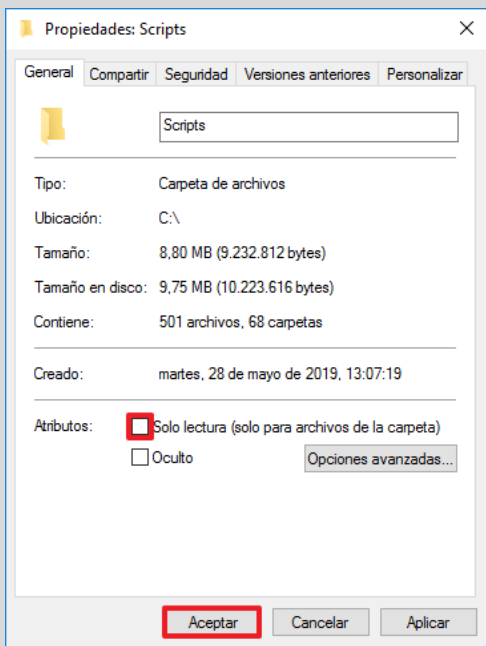
Como paso previo a la configuración de los dispositivos USB, es necesario preparar el directorio activo. Esta preparación se realiza a través de los siguientes pasos.

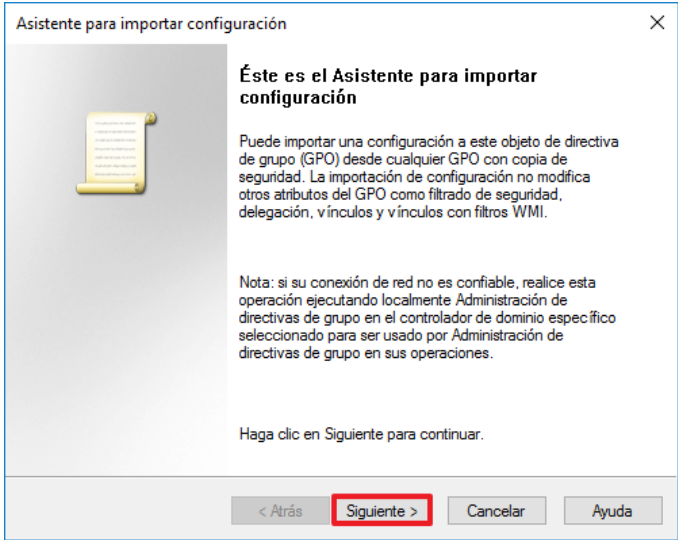
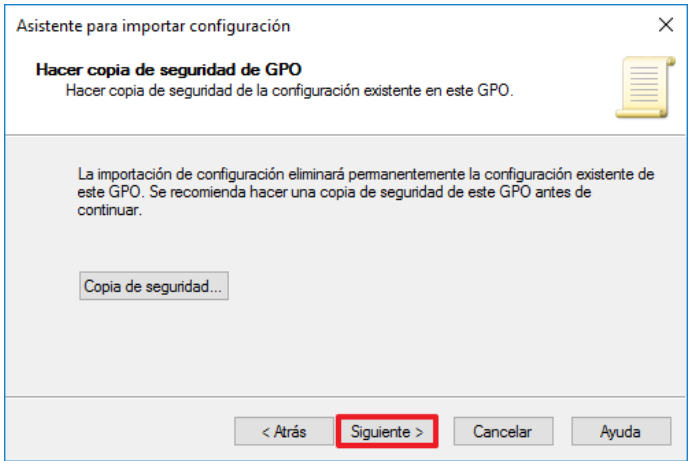
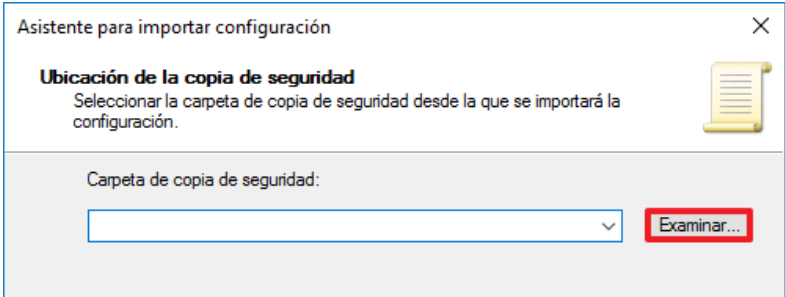
Paso	Descripción
1.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie el siguiente directorio y su contenido a “C:\Scripts” en el controlador de dominio: – CCN-STIC-599A19 Habilitar Dispositivos (directorio)
	Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”.
4.	Cree la unidad organizativa "Equipos Windows 10 – USB habilitado". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.

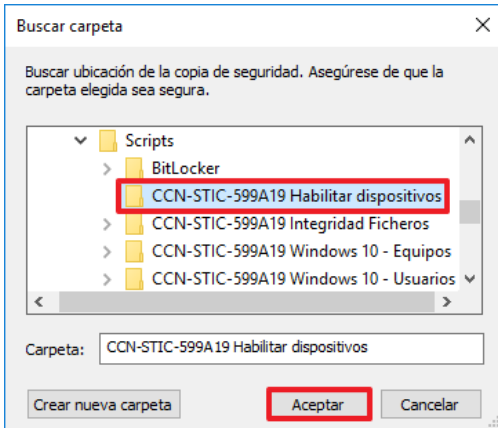
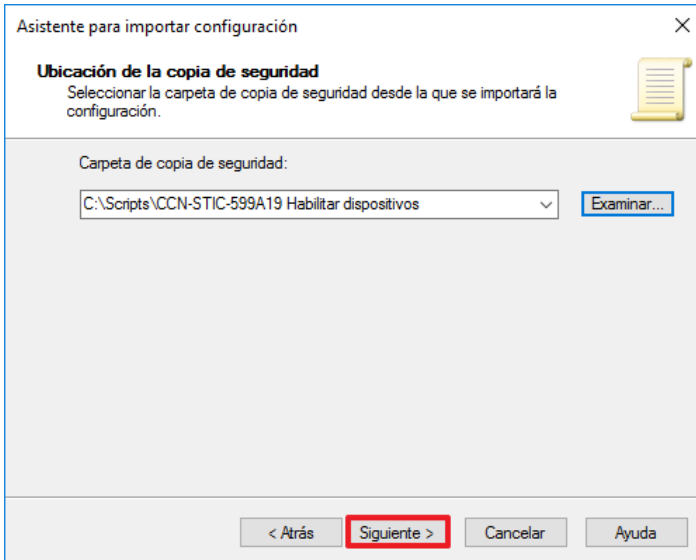
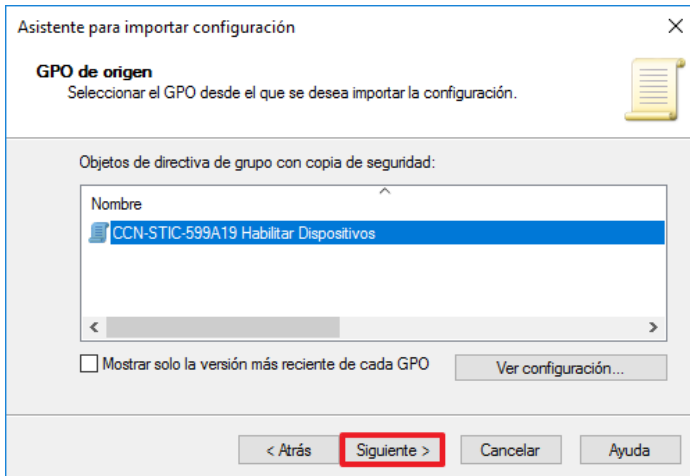
Paso	Descripción
5.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Usuarios y equipos de Active Directory”. 
6.	En la consola de “Usuarios y equipos de Active Directory” sitúese sobre el objeto “Equipos Windows 10” a través de la ruta "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10". Pulsando con el botón derecho del ratón, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá.  Nota: En el ejemplo, el dominio se denomina “dominio.local”.

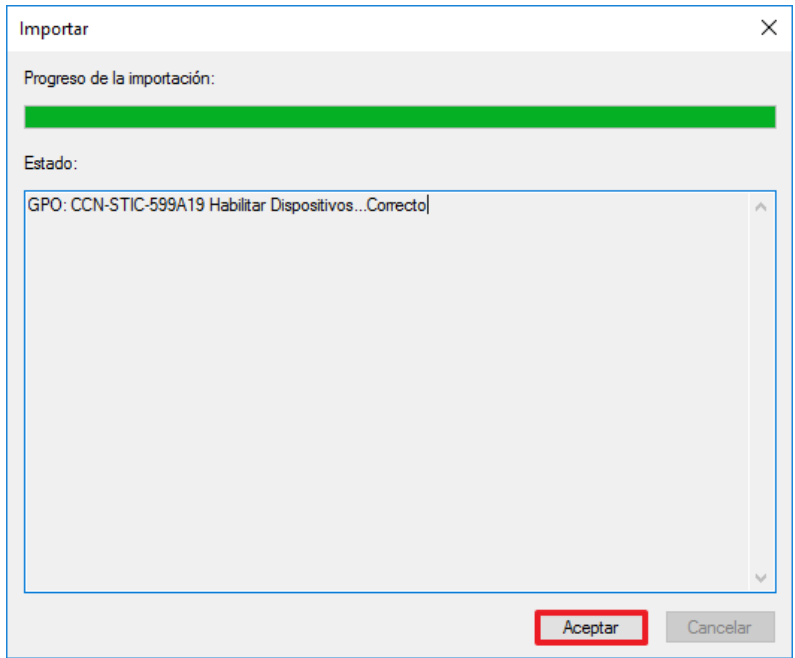
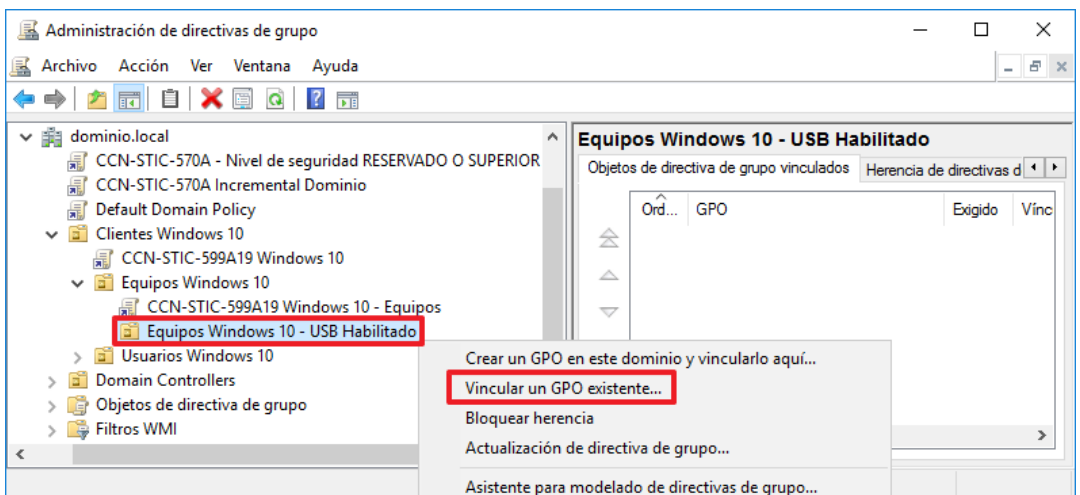
Paso	Descripción
7.	Asigne el nombre "Equipos Windows 10 – USB habilitado" a la nueva unidad organizativa, rellenando con este nombre el campo "Nombre:" del cuadro de diálogo que aparecerá y deje marcada la opción "Proteger contenedor contra eliminación accidental". A continuación, pulse "Aceptar". 
8.	Al pulsar el botón Aceptar, la nueva unidad organizativa, "Equipos Windows 10 – USB habilitado" aparecerá colgando de "Equipos Windows 10", como se muestra en la siguiente figura. 
9.	De nuevo, utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 

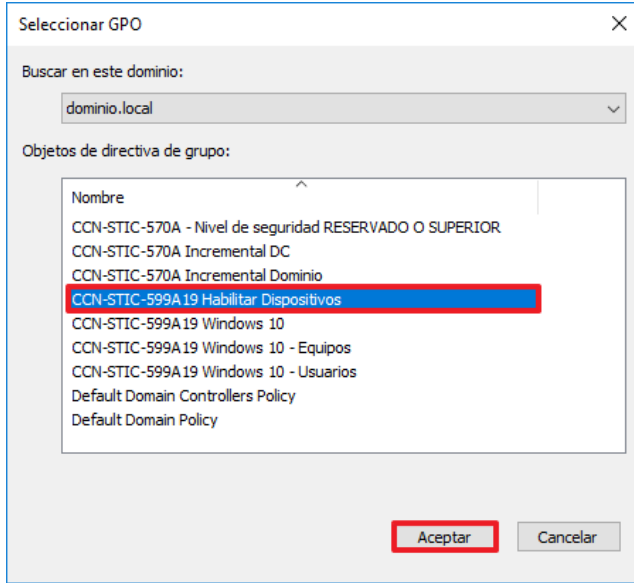
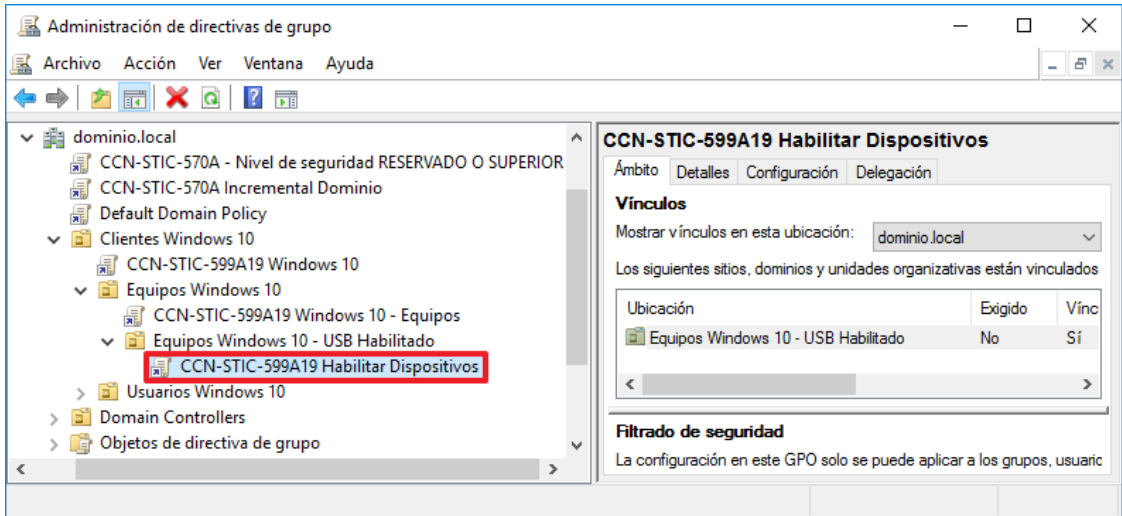
Paso	Descripción
10.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>" A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar la GPO correspondiente.
11.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" con el botón derecho y elija la opción "Nuevo" del menú contextual que aparecerá.  Nota: La GPO que se va a crear y parametrizar en los siguientes pasos deberá vincularse a las unidades organizativas correspondientes a Windows 10 versión 1809. Es importante no mezclar equipos, usuarios o GPOs de Windows 10 versión 1809 con equipos, usuarios o GPOs de Windows 10 versión 1607 (a los cuales les debe aplicar la guía CCN-STIC-599A18, y no la presente guía).
12.	Asigne el siguiente nombre "CCN-STIC-599A19 Habilitar Dispositivos" al nuevo GPO y pulse “Aceptar”. 

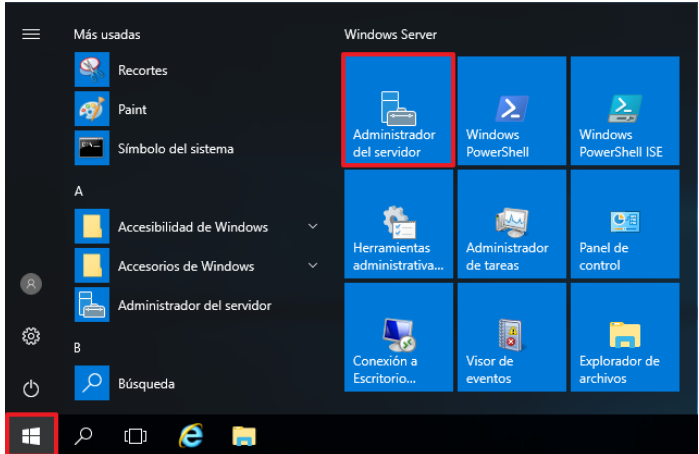
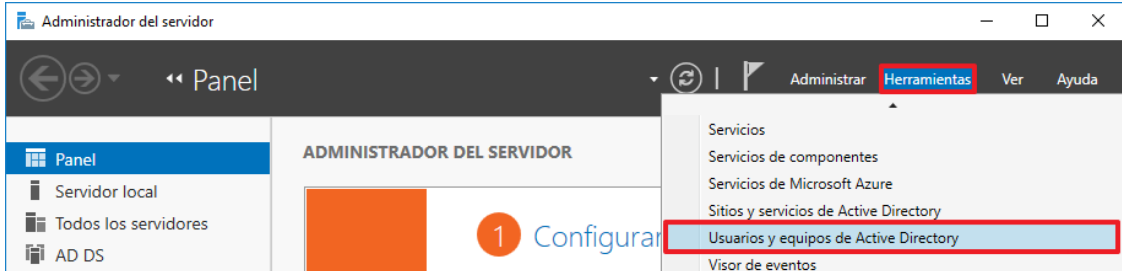
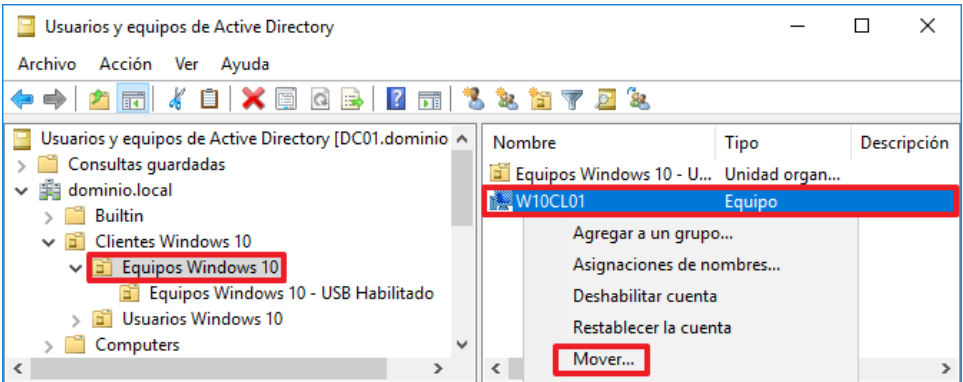
Paso	Descripción
13.	Seleccione la GPO recién creada, "CCN-STIC-599A19 Windows 10" con el botón derecho y elija la opción "Importar configuración..." en el menú contextual que aparecerá.  Nota: Asegúrese de que los archivos alojados en "C:\Scripts" no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

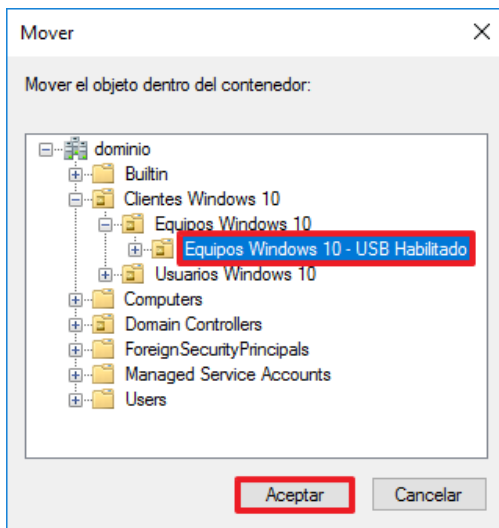
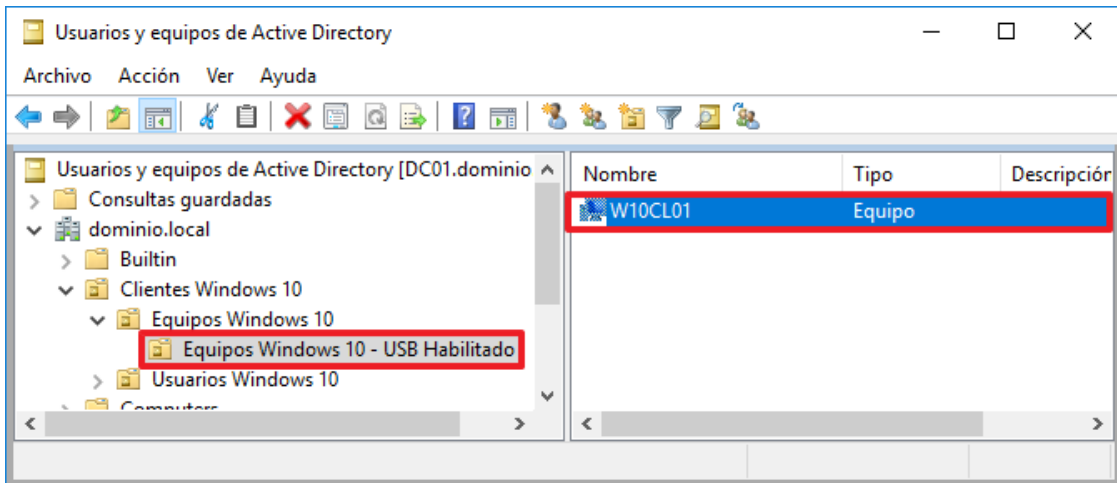
Paso	Descripción
14.	En el “Asistente para importar configuración” pulse “Siguiente >”. 
15.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana “Hacer copia de seguridad de GPO”. 
16.	En “Ubicación de la copia de seguridad” pulse sobre el botón “Examinar...”. 

Paso	Descripción
17.	Localice la carpeta “CCN-STIC-599A19 Habilitar dispositivos” y pulse “Aceptar”. 
18.	Pulse “Siguiente >” para continuar. 
19.	En “GPO de origen” pulse “Siguiente >”. 
20.	En “Examinar copia de seguridad” pulse “Siguiente >”.

Paso	Descripción
21.	Pulse “Finalizar” para realizar la importación.
22.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 
23.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 – USB habilitado” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
24.	Seleccione “CCN-STIC-599A19 Habilitar dispositivos” de la lista y pulse “Aceptar”. 
25.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Equipos Windows 10 – USB habilitado”. 

Paso	Descripción
26.	Traslade, en Active Directory, la cuenta de equipo del equipo en el que necesita hacer uso de un dispositivo externo USB, desde su ubicación actual hasta su nueva ubicación: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 – USB habilitado" Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
27.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Usuarios y equipos de Active Directory". 
28.	Seleccione entonces, en la parte central de la ventana, la cuenta del equipo a trasladar y, marcando con el botón derecho del ratón, seleccione la opción "Mover..." del menú contextual que aparecerá, como se muestra en la siguiente figura.  Nota: En este ejemplo el nombre del equipo en el que se está permitiendo el uso de dispositivos USB se supone que es "W10CL01".

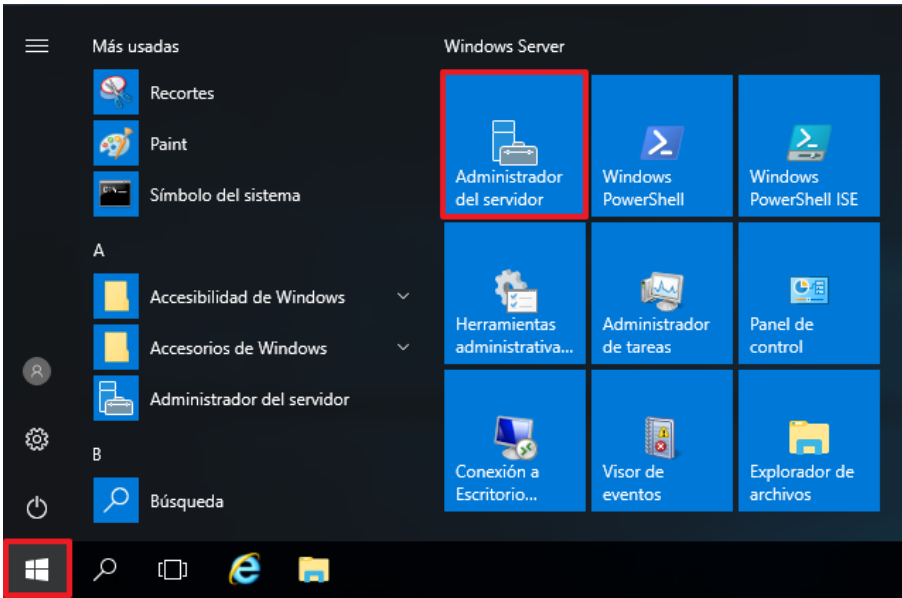
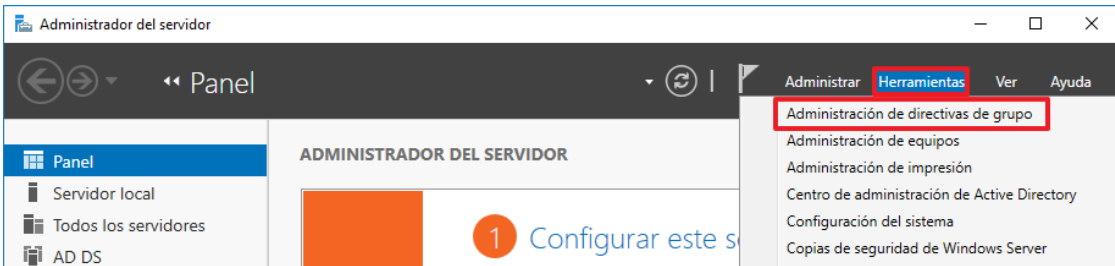
Paso	Descripción
29.	En el cuadro de diálogo que aparecerá, titulado "Mover", seleccione el contenedor destino en la ruta "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 – USB habilitado". Pulse "Aceptar" para cerrar la ventana. 
30.	Finalmente, seleccione y expanda el contenedor siguiente: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 USB habilitado" Compruebe que, efectivamente, la cuenta del equipo ahora se encuentra en él. 
31.	Borre la carpeta "C:\Scripts".

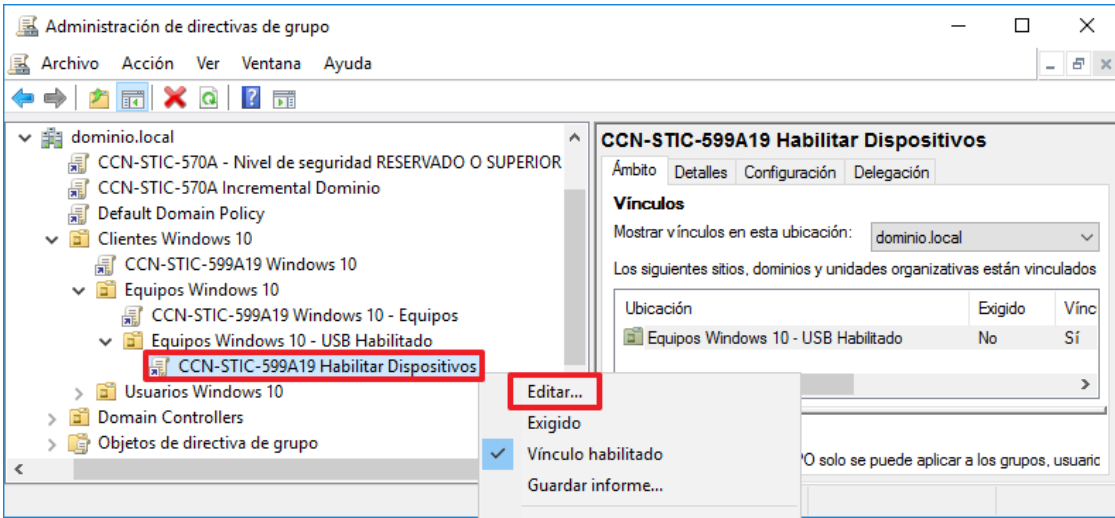
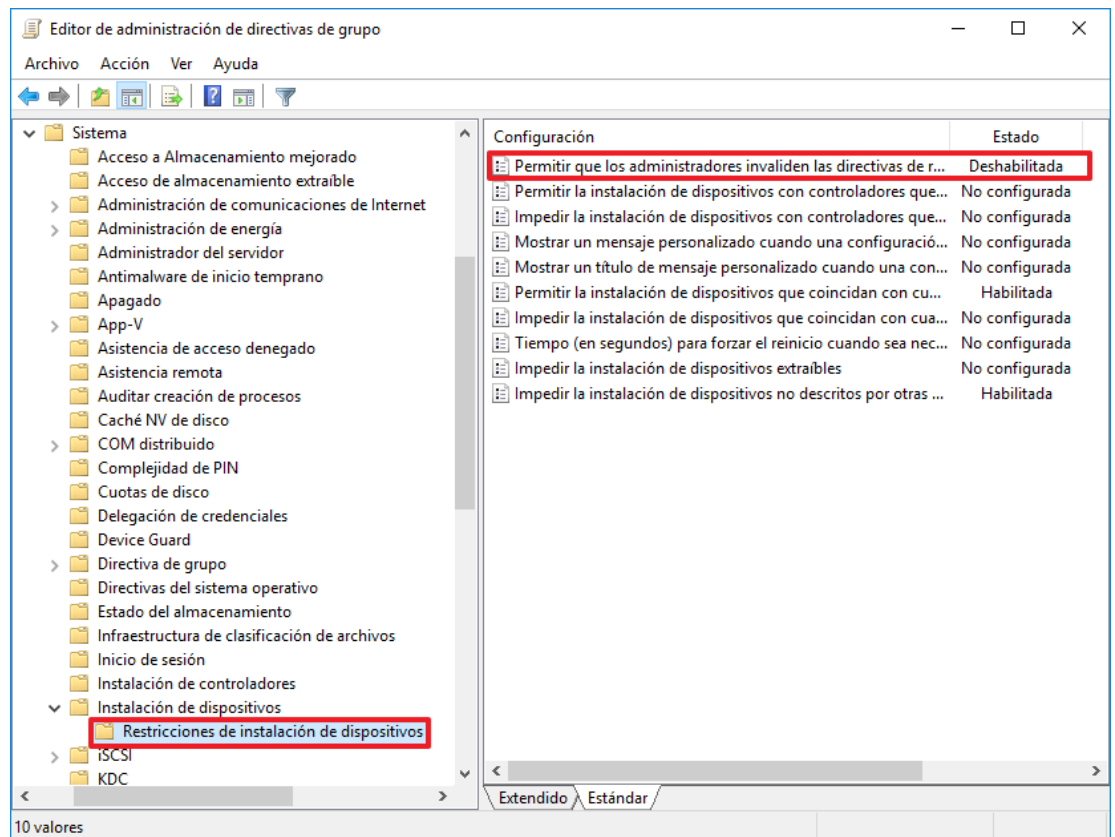
2. ADMINISTRAR USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES

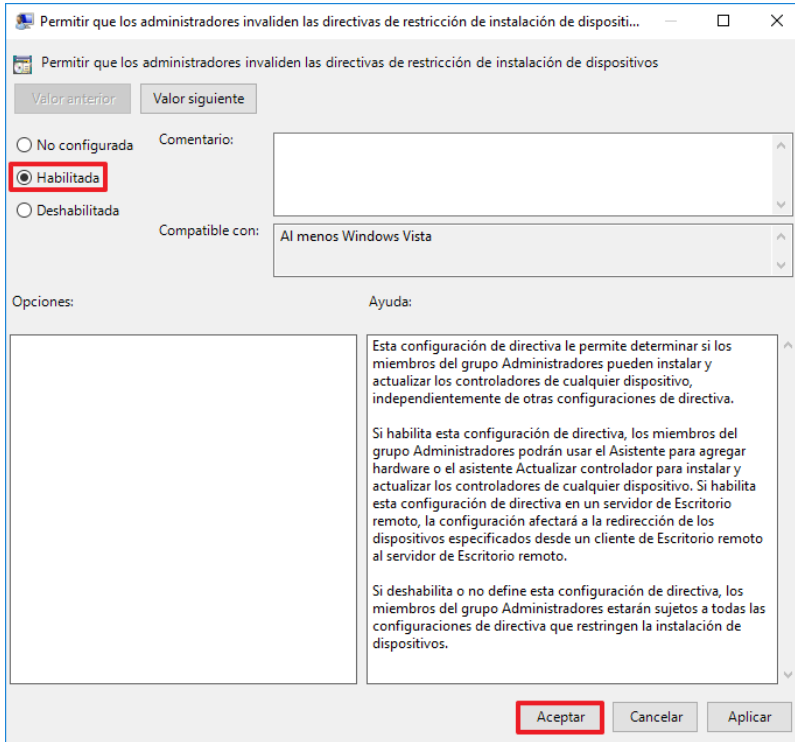
Este punto describe el proceso para instalar y desinstalar el controlador de un dispositivo USB a través de una cuenta que posea privilegios de administrador local de la máquina.

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.

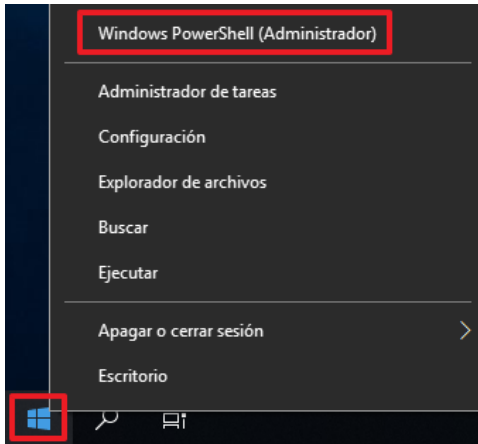
2.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB

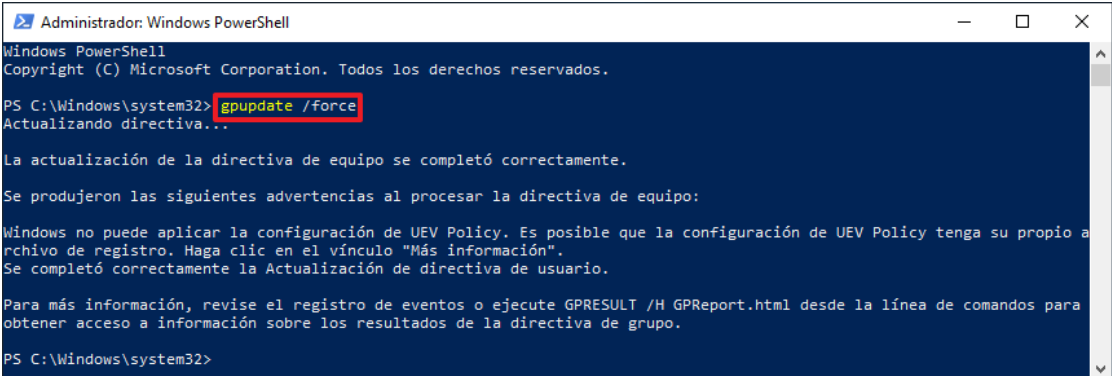
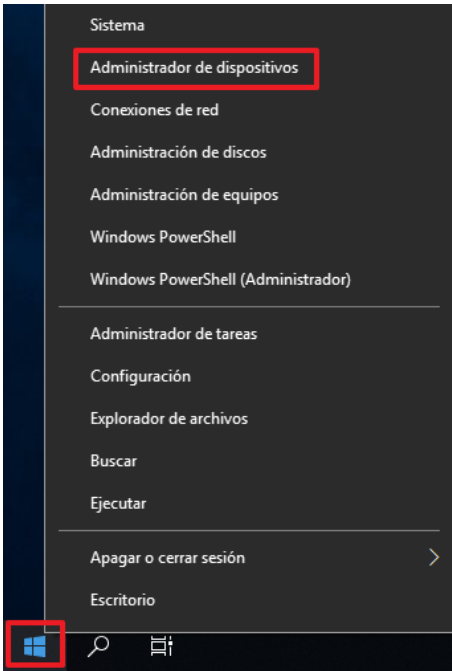
Paso	Descripción
32.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
33.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios.
34.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 

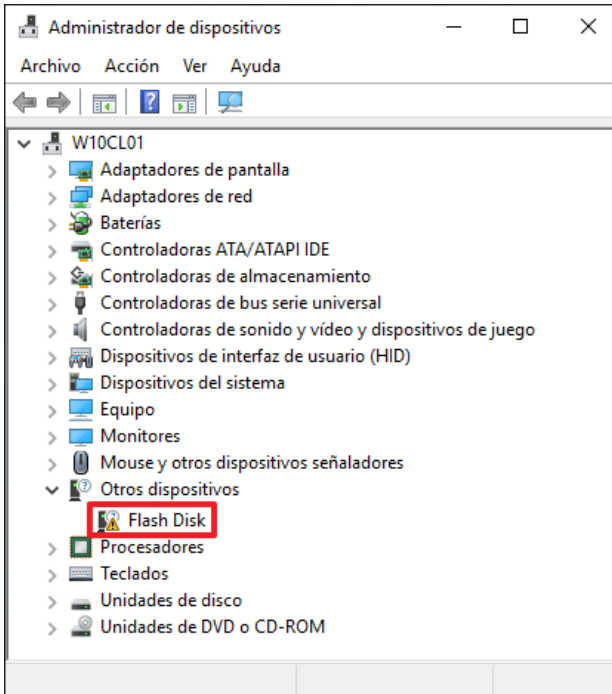
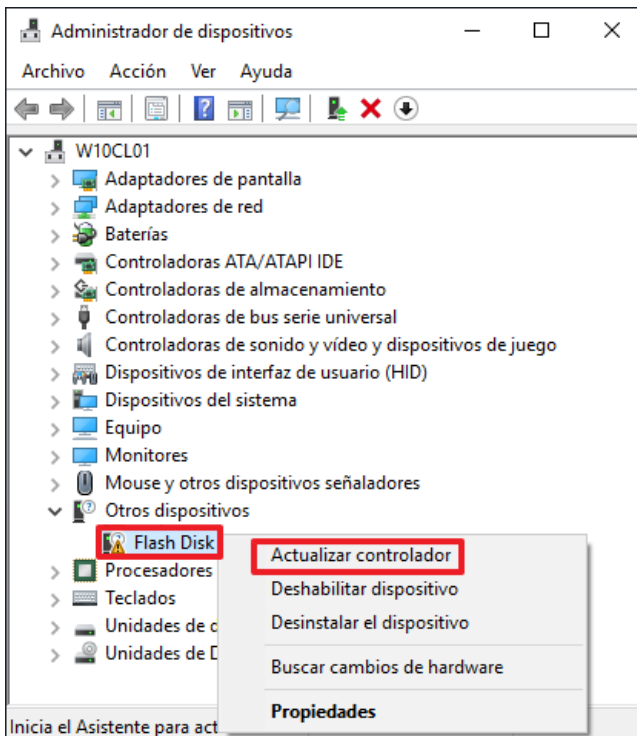
Paso	Descripción
35.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
36.	En el apartado “Objetos de directiva de grupo” seleccione la GPO creada anteriormente, “CCN-STIC-599A19 Habilitar dispositivos”, con el botón derecho y seleccione la opción del menú contextual “Editar...”. 
37.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

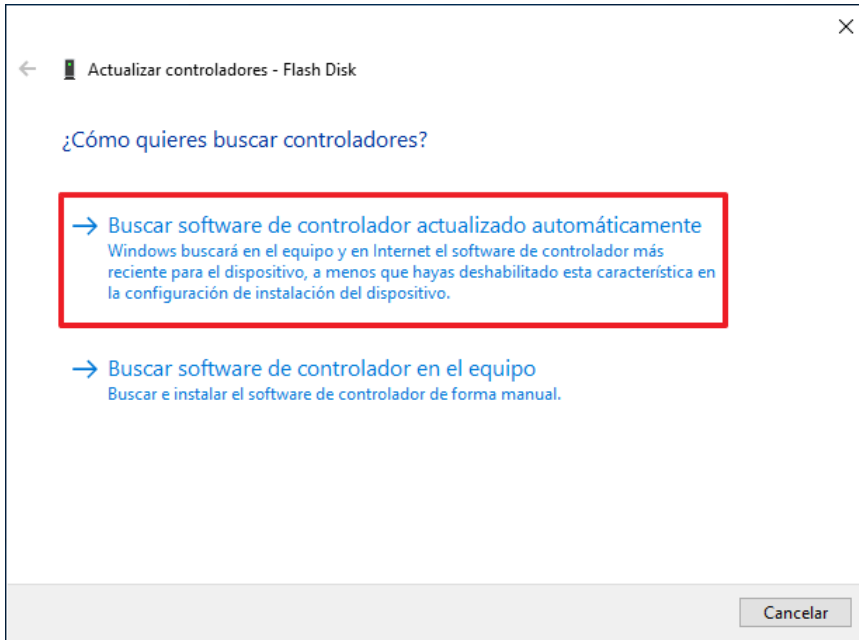
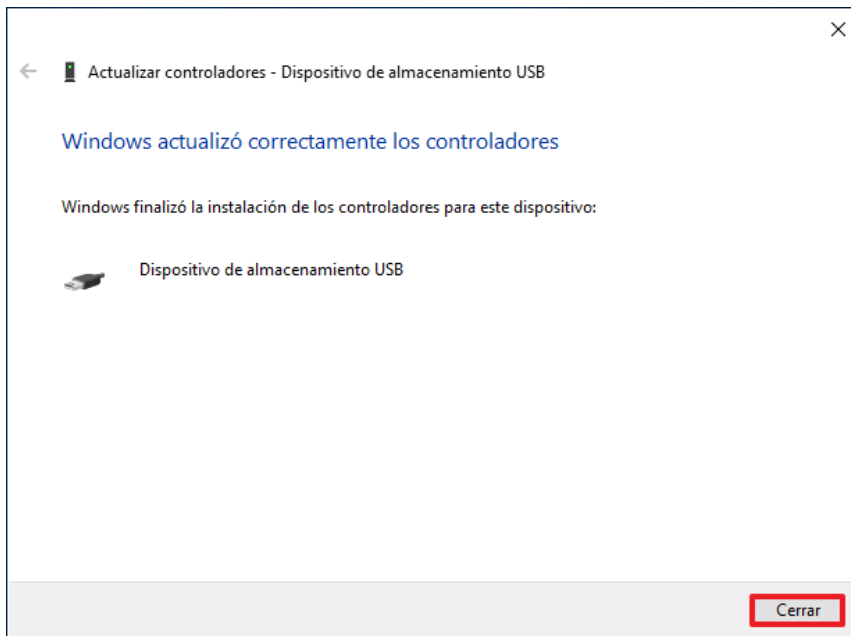
Paso	Descripción
38.	Haga doble clic sobre la directiva “Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos” y configúrela para que su estado sea “Habilitada”. A continuación pulse “Aceptar”. 

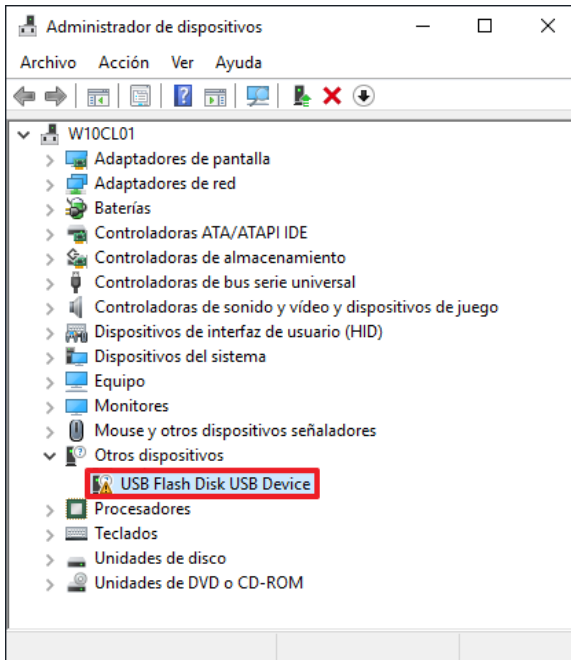
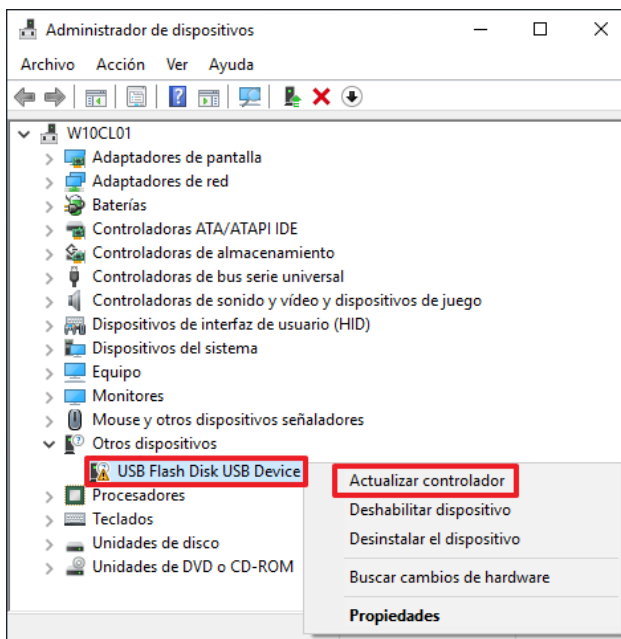
Los pasos definidos a continuación deberá realizarlos sobre un equipo Windows 10 perteneciente al dominio sobre el que se está habilitando el uso de dispositivos USB.

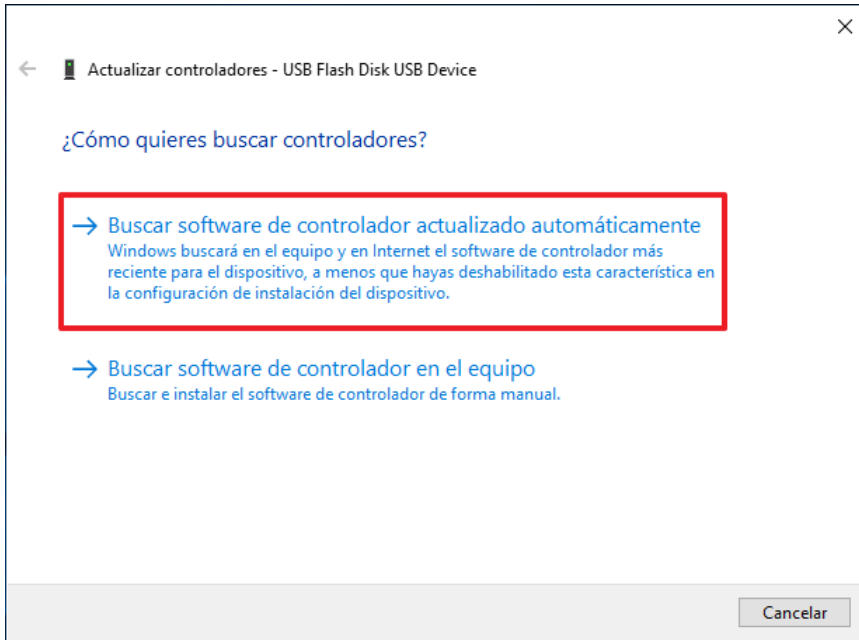
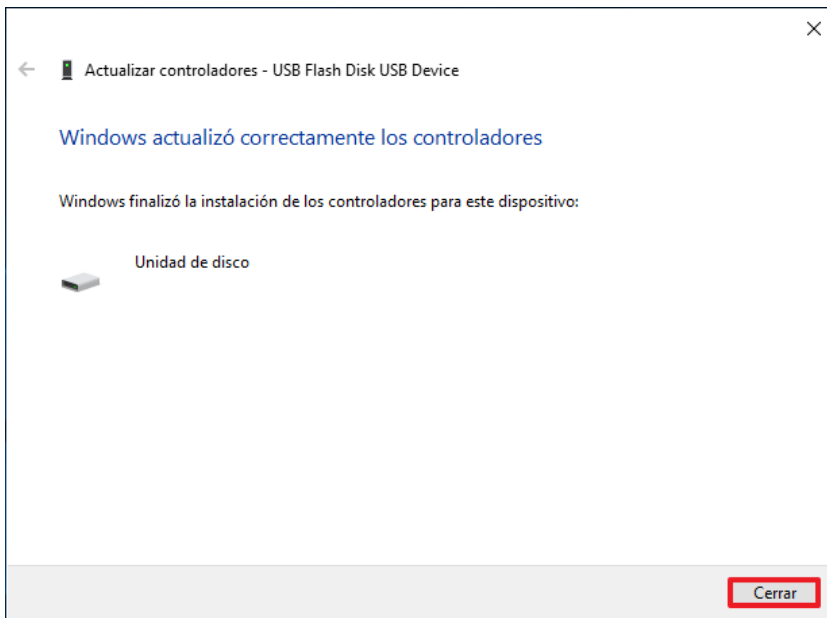
Paso	Descripción
39.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
40.	Deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 

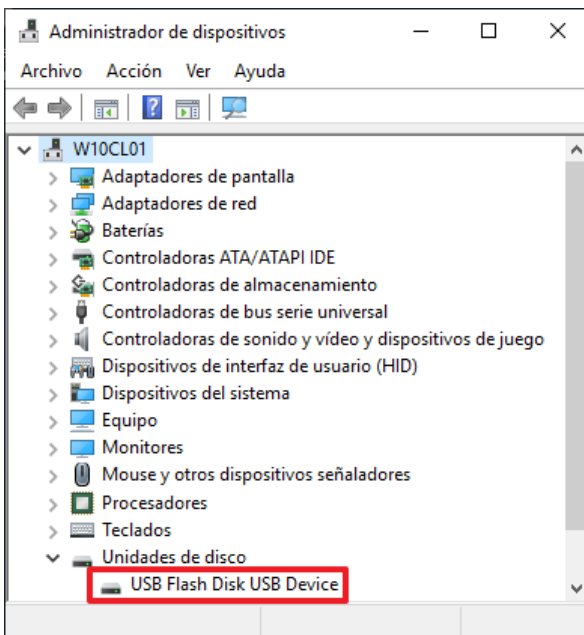
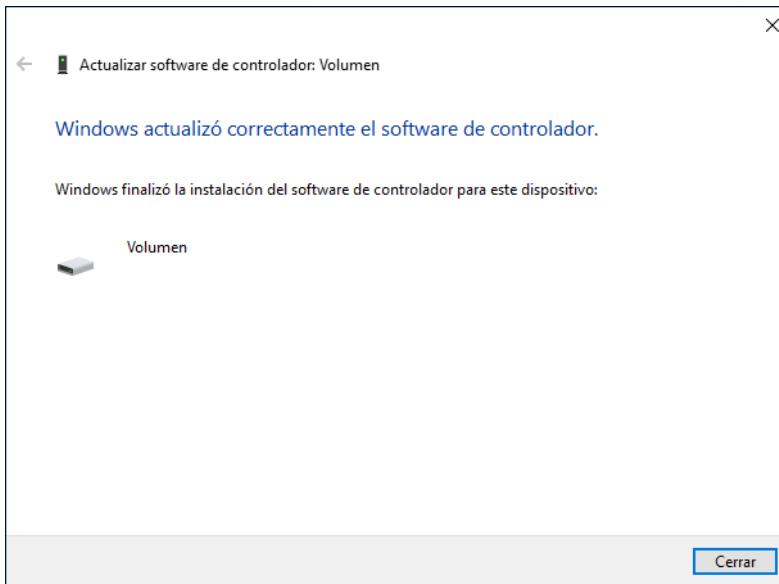
Paso	Descripción
41.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar.
42.	Ejecute el comando “gpupdate /force” y espere a que finalice. 
43.	Para iniciar la instalación 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 que pertenezca al grupo “Admins. del dominio”.
44.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

Paso	Descripción
45.	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”.
46.	Haga clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 

Paso	Descripción
47.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 
48.	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.

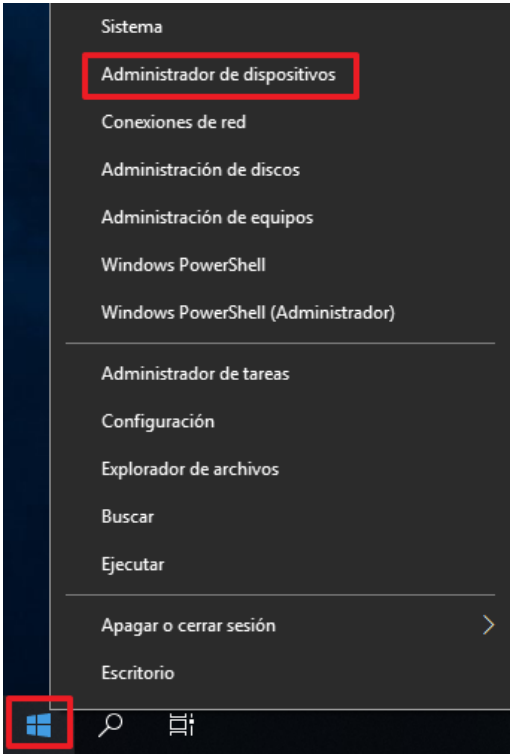
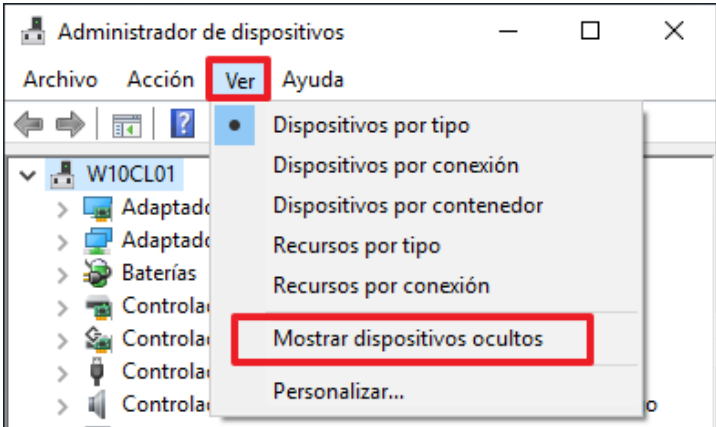
Paso	Descripción
49.	Tras la instalación de los controladores el sistema reconocerá el dispositivo. Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: En este ejemplo se utiliza el dispositivo denominado “USB 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”.
50.	Haga de nuevo clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 

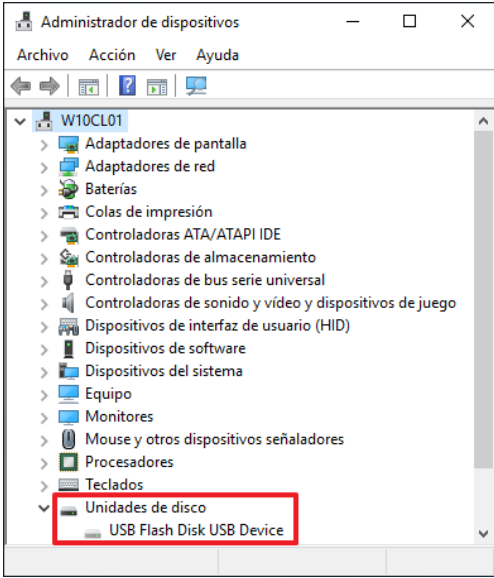
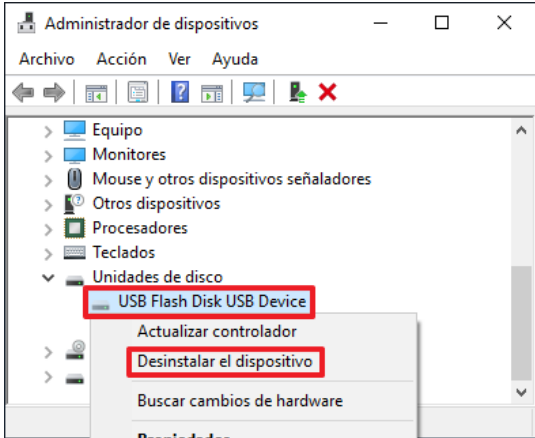
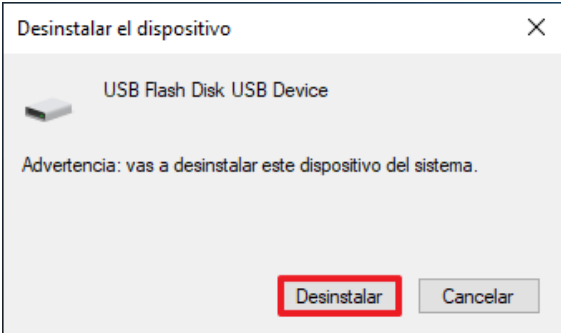
Paso	Descripción
51.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 
52.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  Nota: Deberá repetir estos pasos hasta que su dispositivo de almacenamiento aparezca en el apartado “Unidades de disco”.

Paso	Descripción
53.	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”.
54.	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. 
55.	El dispositivo está listo para ser utilizado.

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

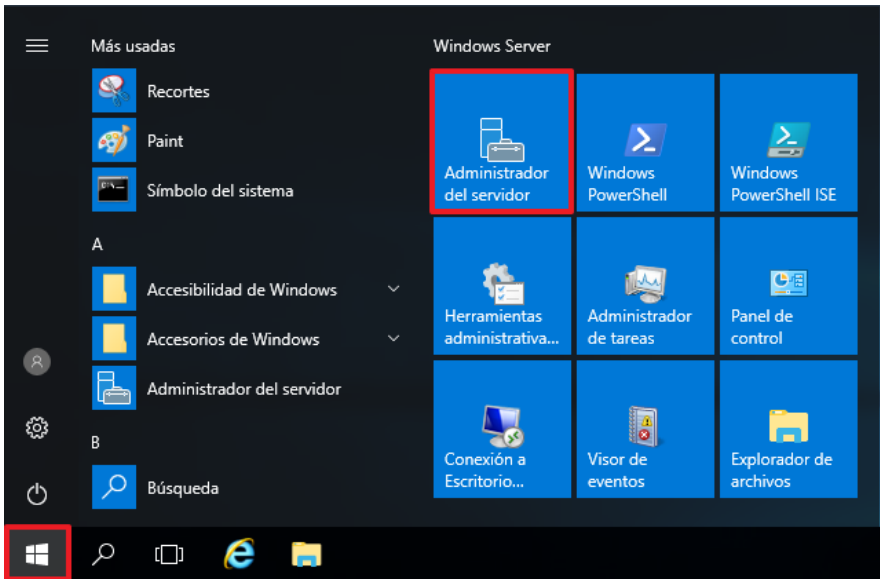
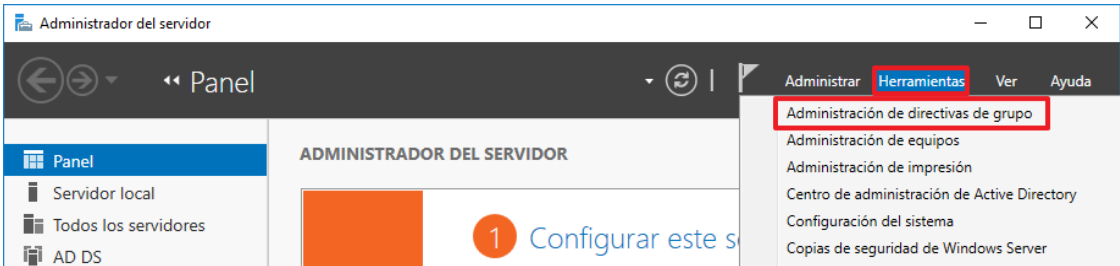
Tras la instalación del dispositivo y su posterior uso será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

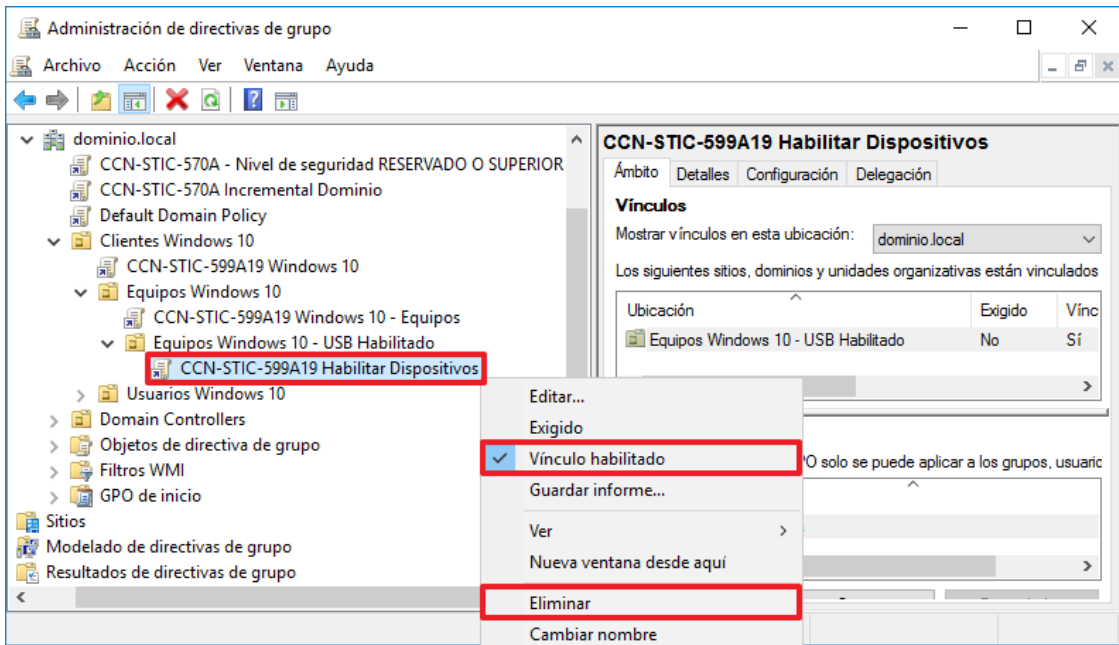
Paso	Descripción
56.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
57.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
58.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

Paso	Descripción
59.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 
60.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
61.	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.

Ejecute los siguientes pasos en el equipo controlador de dominio al que pertenece el equipo Windows 10 sobre el que se está deshabilitando el uso de dispositivos USB.

Nota: El siguiente procedimiento desvincula la GPO “CCN-STIC-599A19 Habilitar dispositivos”. Si no desea desvincular la GPO, no realice los siguientes pasos.

Paso	Descripción
62.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
63.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios.
64.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior “Herramientas” y pulse “Administración de directivas de grupo”. 
65.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta: "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"

Paso	Descripción
66.	Sobre la unidad organizativa creada para habilitar el uso de dispositivos USB “Equipos Windows 10 – USB habilitado” seleccione la GPO vinculada “CCN-STIC-599A19 Habilitar dispositivos” con el botón derecho y desmarque la opción “Vínculo habilitado” o seleccione “Eliminar”. 
67.	Con esto quedará desvinculada la GPO de la unidad organizativa y se volverá al estado anterior de bloqueo de dispositivos USB.

3. 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.

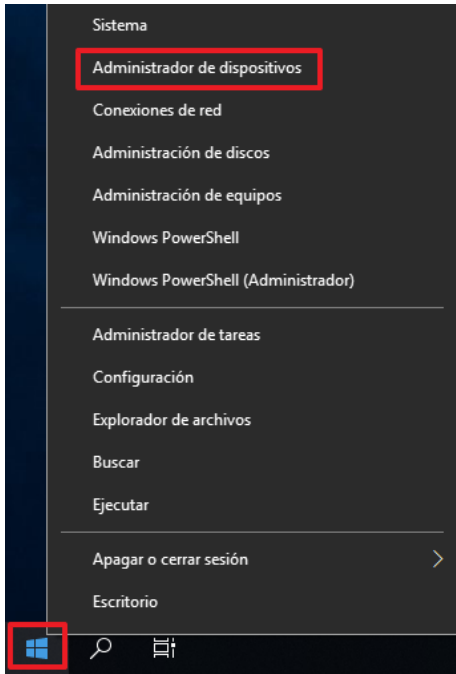
3.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

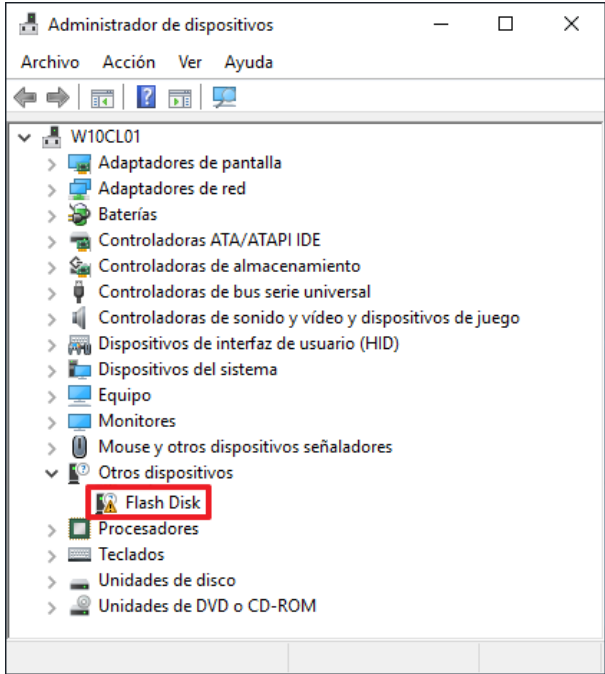
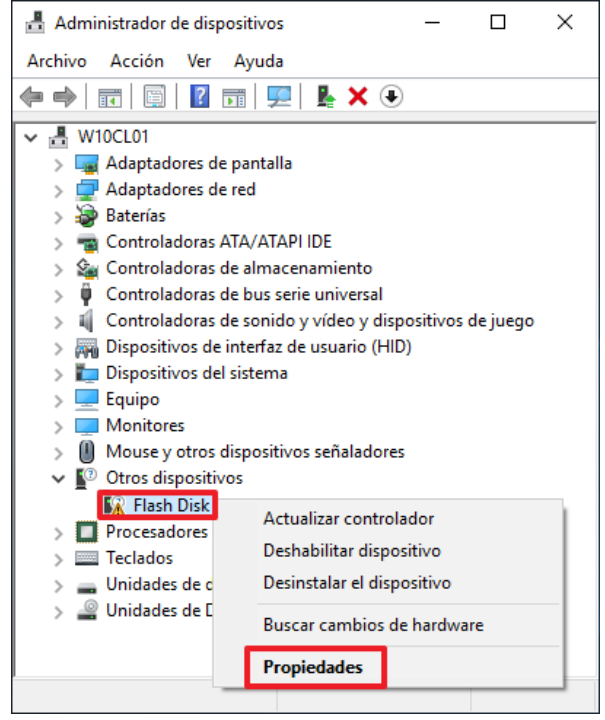
Este punto describe el proceso para permitir el uso un dispositivo mediante el filtrado por su identificador. Cuando el filtro esté realizado, los controladores del dispositivo se instalarán de manera automática y el dispositivo podrá ser utilizado.

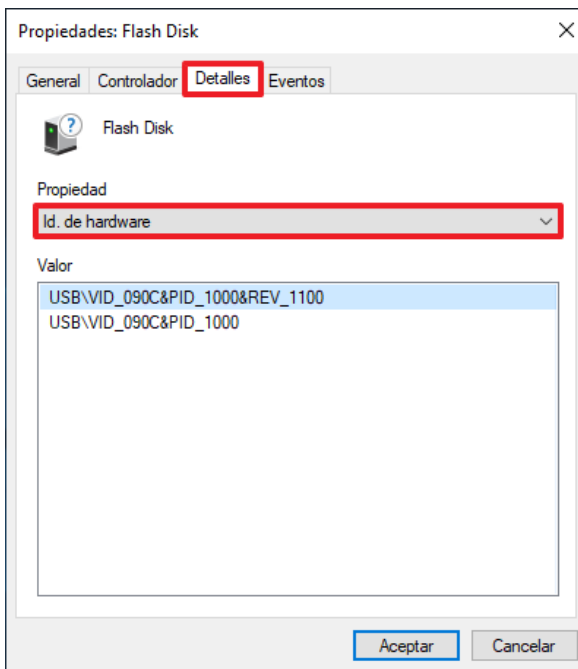
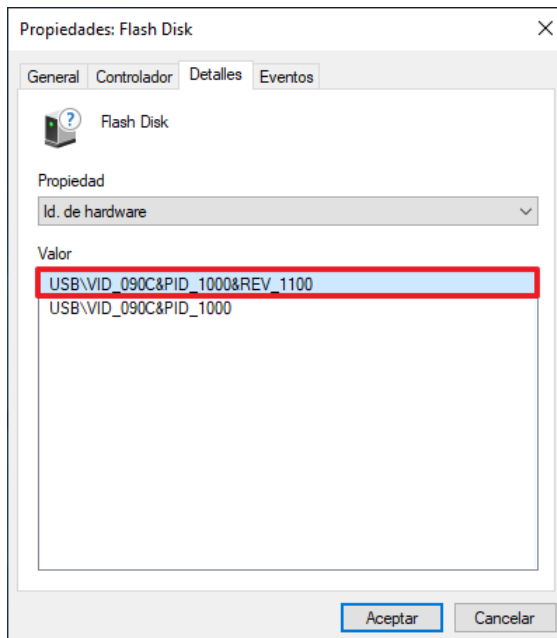
Tras la finalización de su uso, los controladores del dispositivo serán desinstalados tanto si el dispositivo se encuentra conectado al equipo como si no.

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.

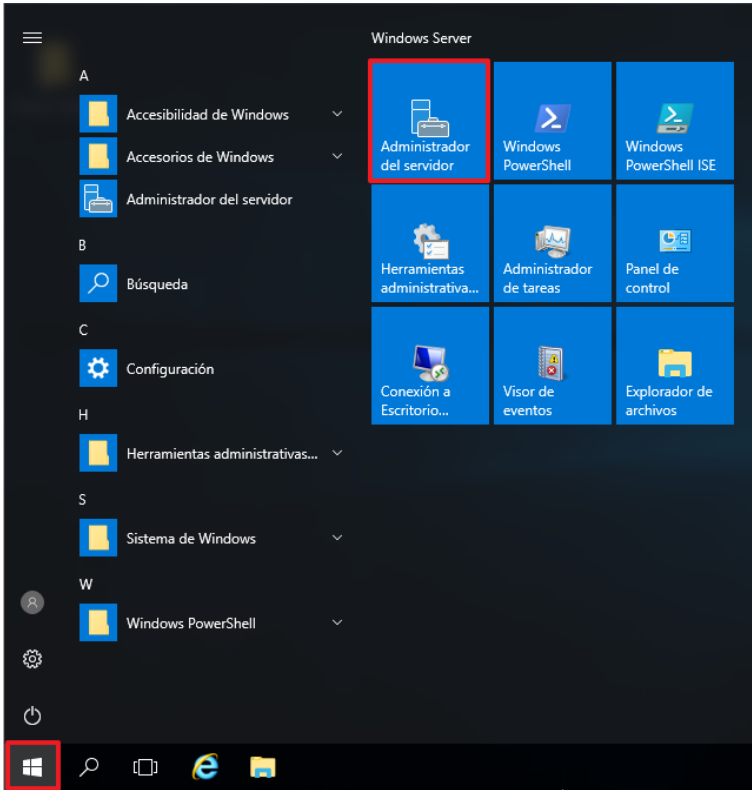
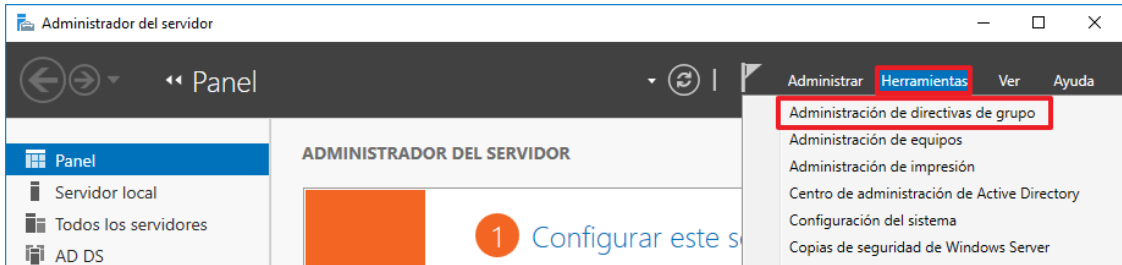
Tras el uso de los dispositivos se procederá a eliminar los identificadores de la lista configurada, y a desinstalar los controladores para evitar el uso de éstos.

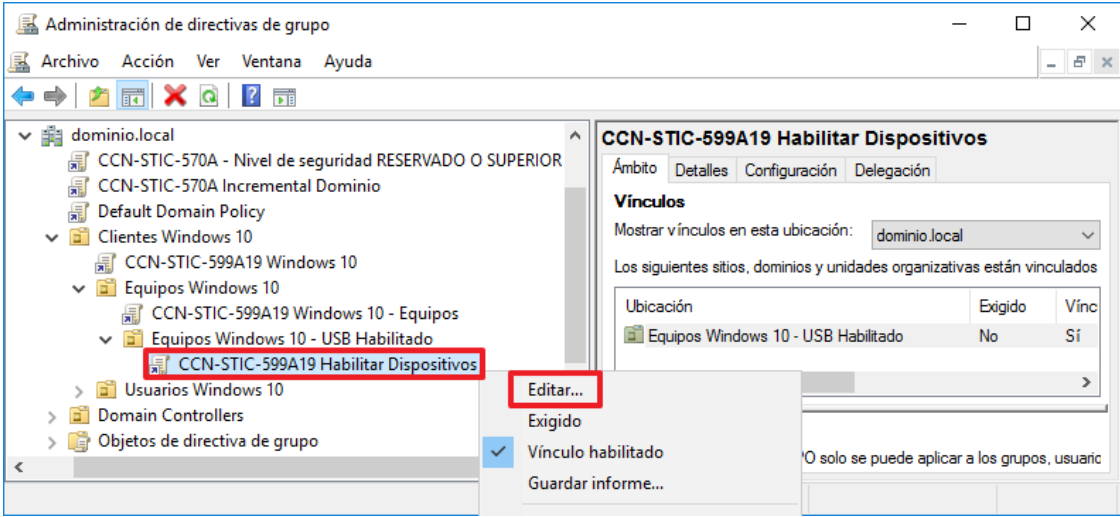
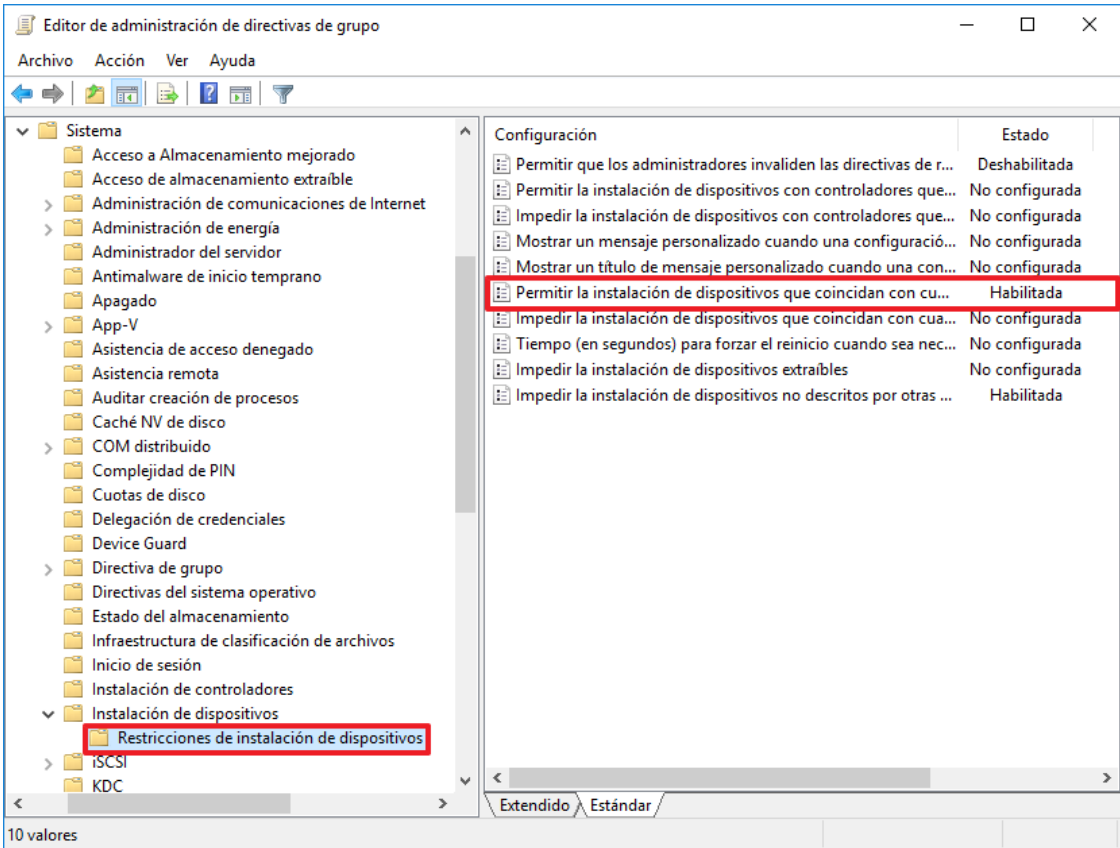
Paso	Descripción
68.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
69.	Para iniciar la instalación de un dispositivo USB deberá conectarlo en el equipo. Nota: Es necesario tener en consideración que la instalación de los dispositivos USB debe realizarse de manera manual y por un usuario que pertenezca al grupo “Admins. del dominio”.
70.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

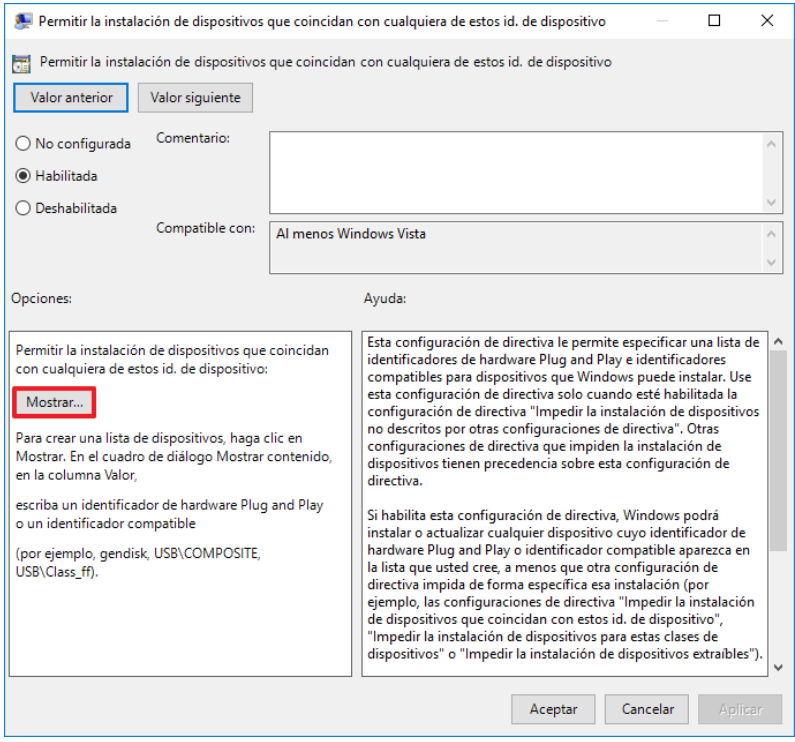
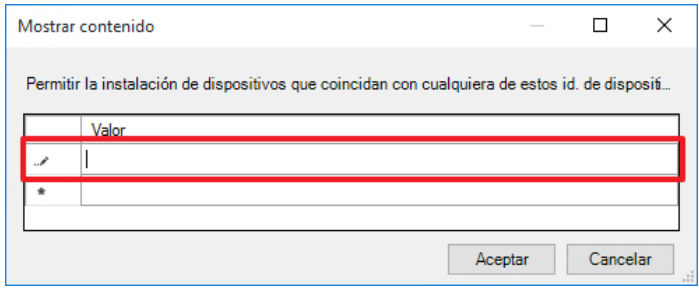
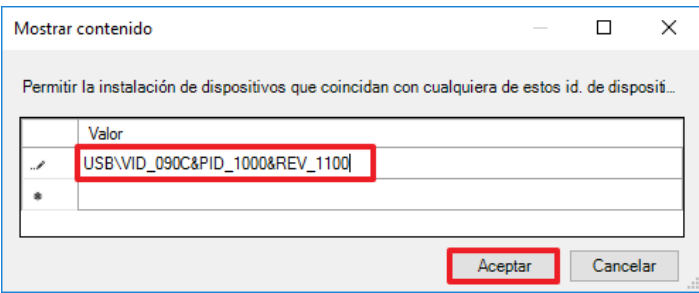
Paso	Descripción
71.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre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

Paso	Descripción
73.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Id. de hardware”. 
74.	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.

Realice los siguientes pasos en el controlador de dominio del dominio al que pertenece el equipo Windows 10 que está asegurando para permitir el uso de dispositivos USB.

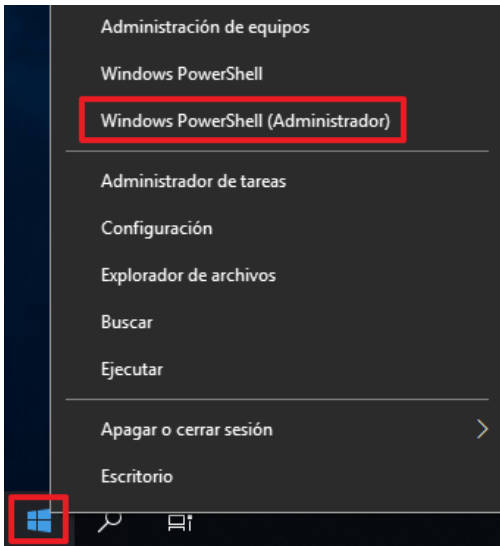
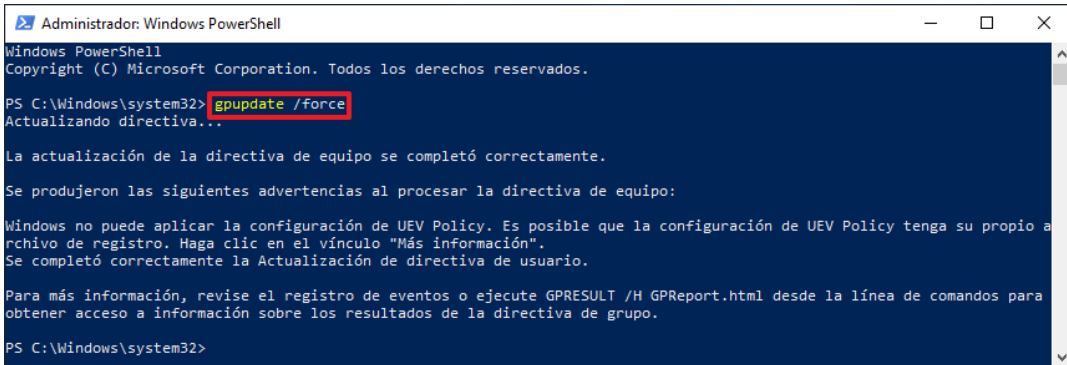
Paso	Descripción
75.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
76.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
77.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
78.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta: "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"

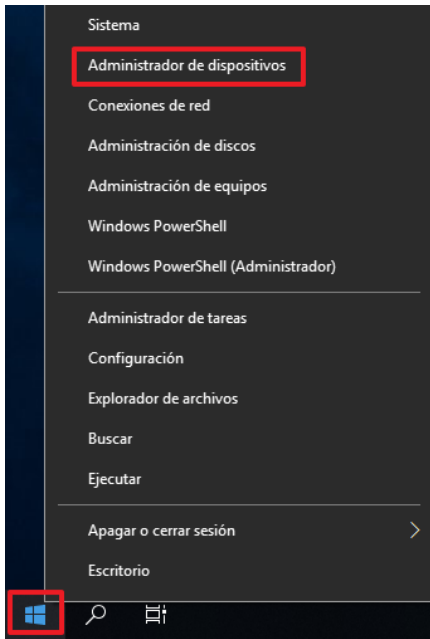
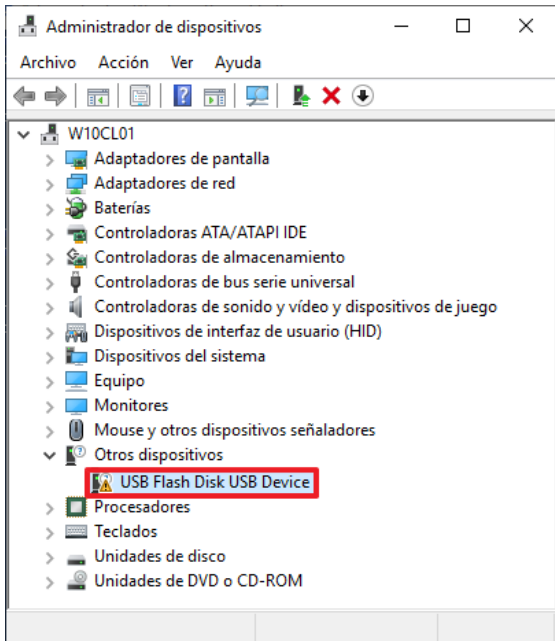
Paso	Descripción
79.	En el apartado “Objetos de directiva de grupo” seleccione la GPO creada anteriormente con el botón derecho y seleccione la opción del menú contextual “Editar”. 
80.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

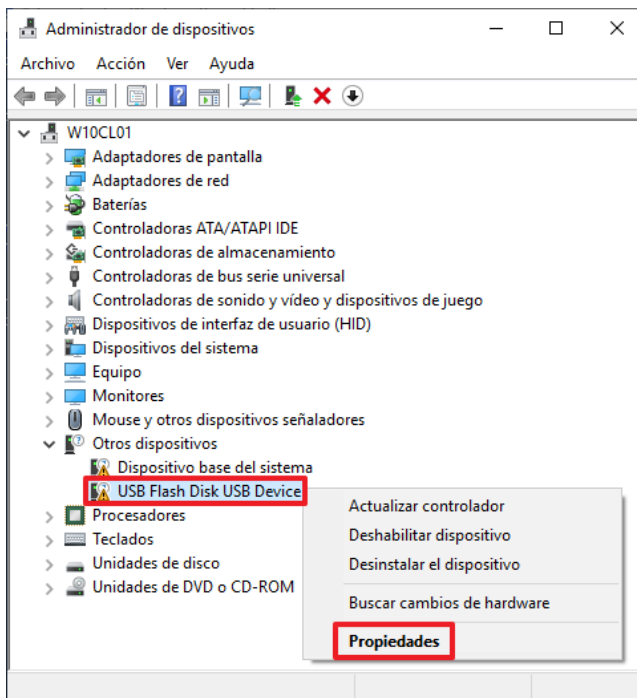
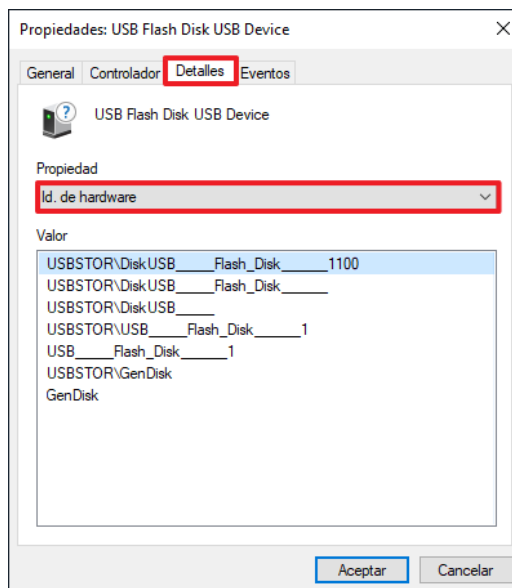
Paso	Descripción
81.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar...”. 
82.	En la ventana emergente “Mostrar contenido” haga 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.
83.	Verifique el identificador introducido y pulse “Aceptar” para continuar. 

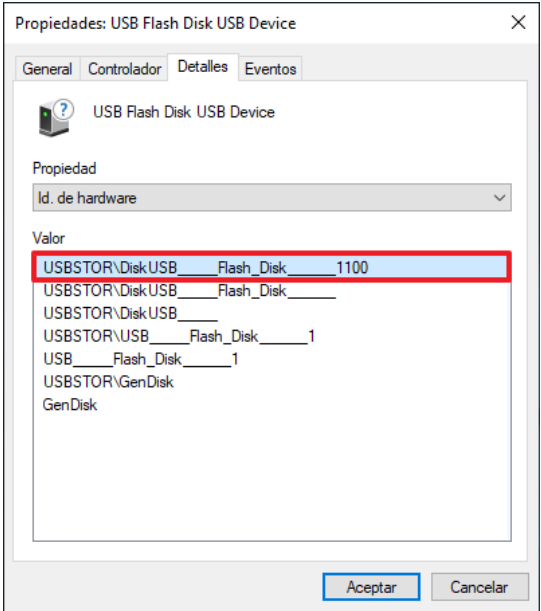
Paso	Descripción
84.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.
85.	Sin cerrar el “Editor de directivas de grupo local”, continúe con el siguiente paso.

Ejecute los siguientes pasos dentro del equipo cliente Windows 10 sobre el que está habilitando el uso de dispositivos USB.

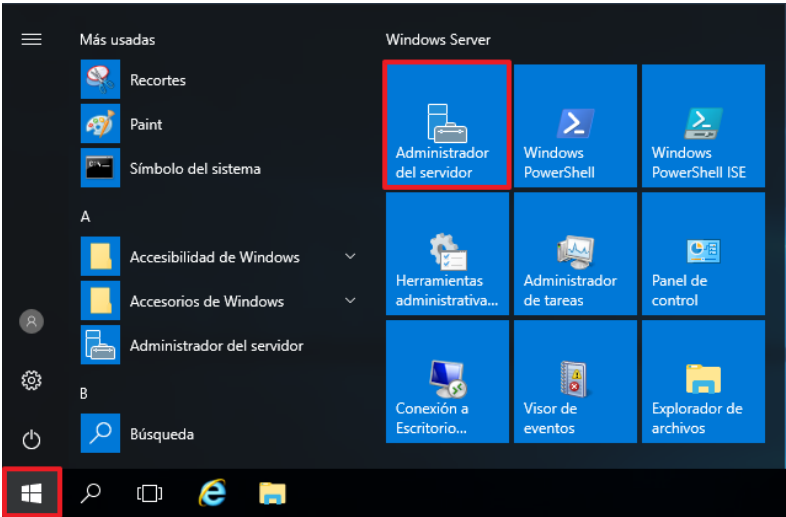
Paso	Descripción
86.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
87.	Deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 
88.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca la credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar.
89.	Ejecute el comando “gpupdate /force” y espere a que finalice. 

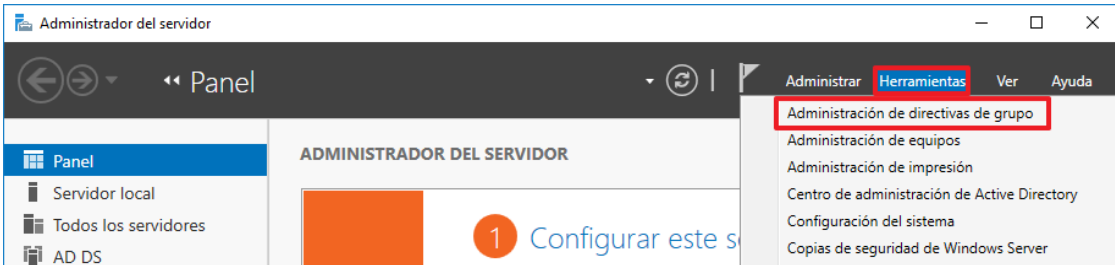
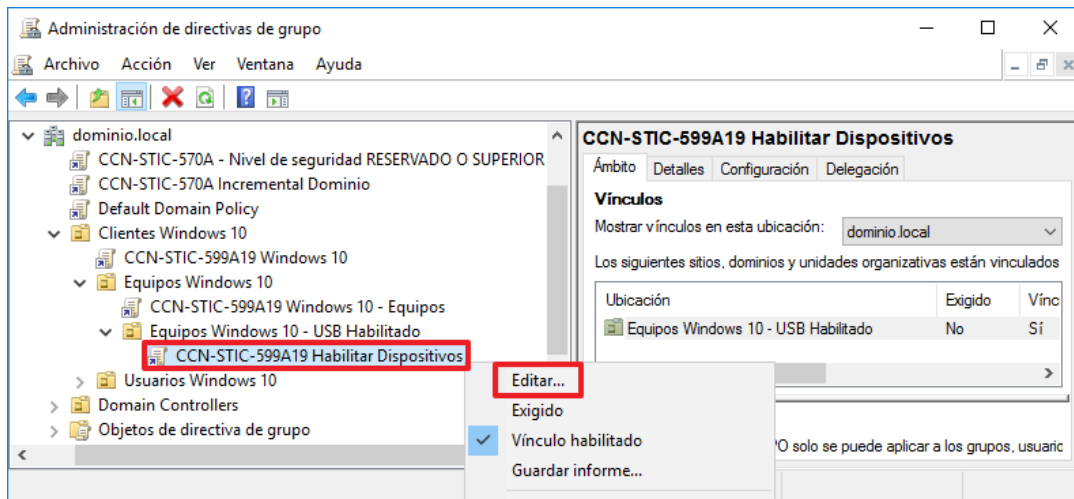
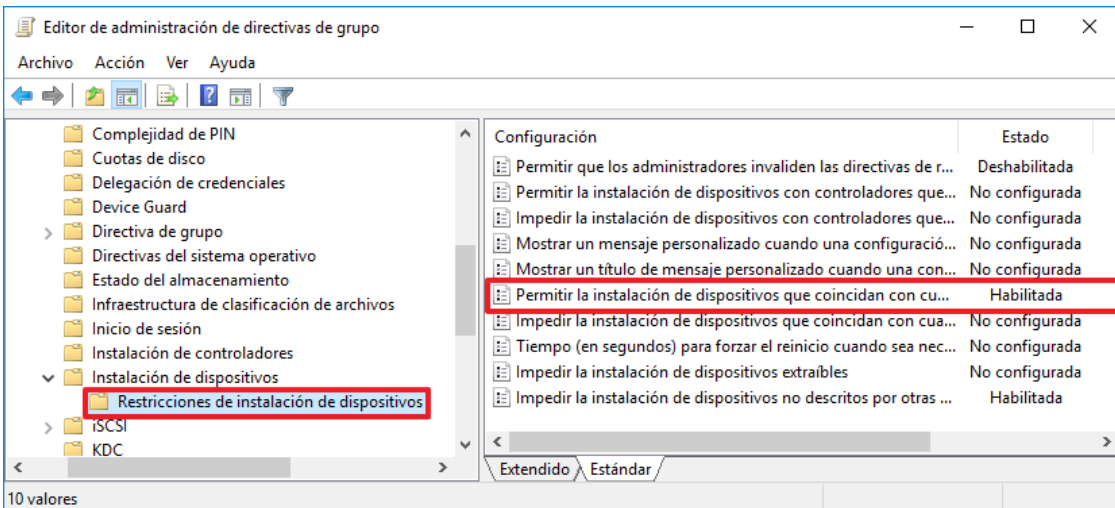
Paso	Descripción
90.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
91.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: En este ejemplo se utiliza el dispositivo denominado “Flash Disk USB Device”. El nombre ha cambiado porque el equipo ha reconocido el identificador introducido en pasos anteriores.

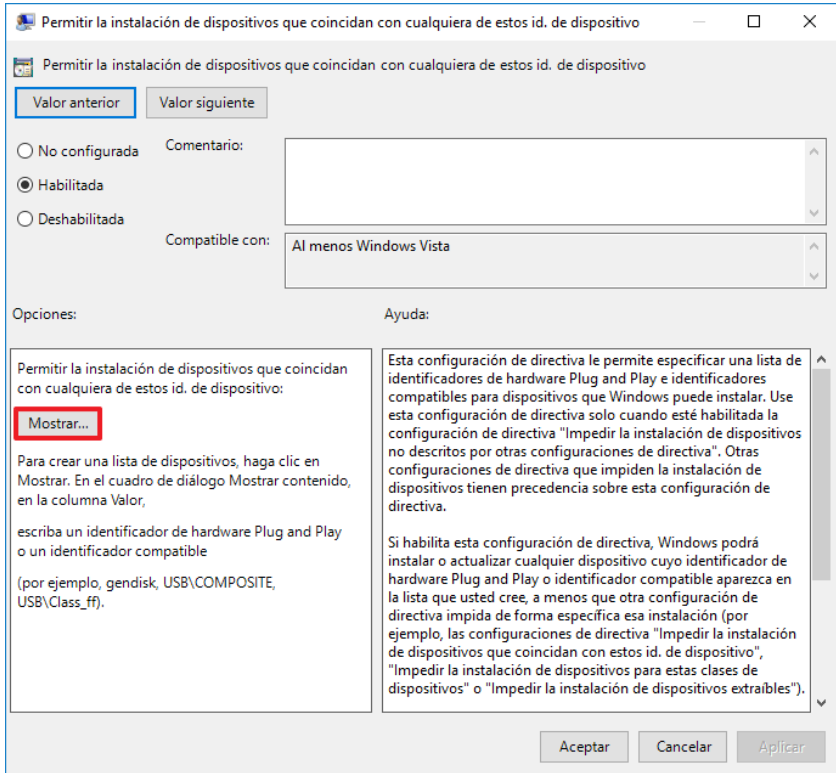
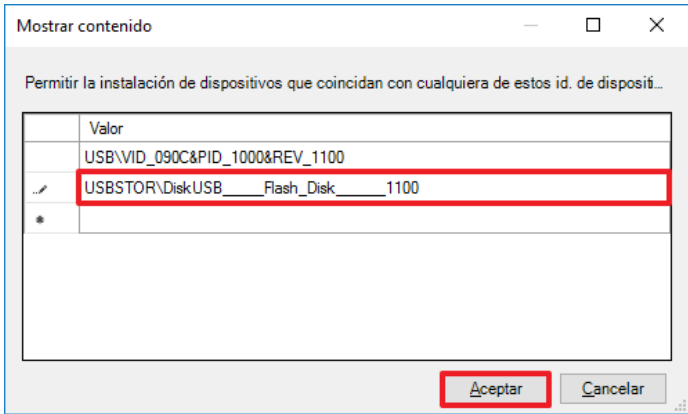
Paso	Descripción
92.	Seleccione dicho dispositivo con el botón derecho y pulse sobre la opción “Propiedades”.  Nota: Espere a que el dispositivo sea reconocido por el equipo. En caso de no ser así, extraiga y vuelva a conectar el dispositivo para que éste sea reconocido. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.
93.	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.

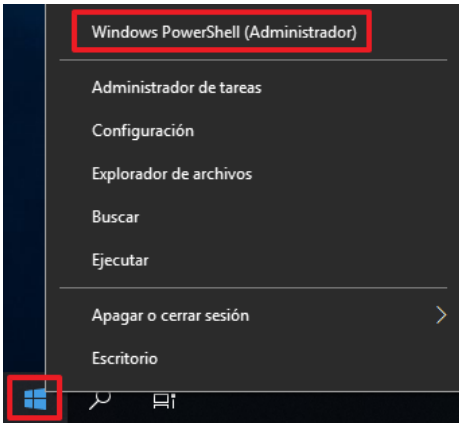
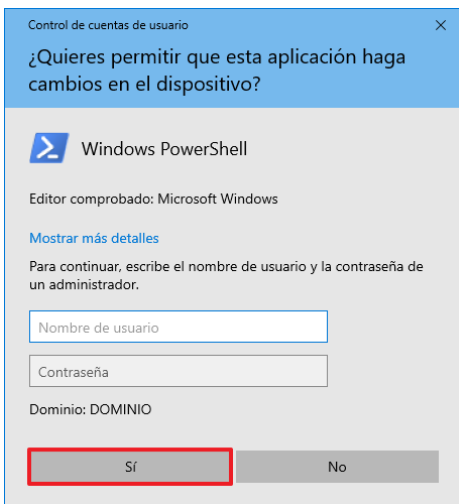
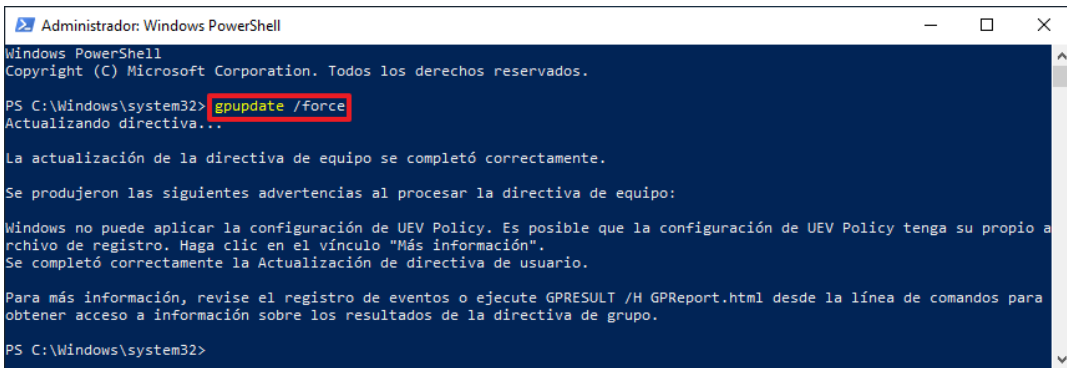
Paso	Descripción
94.	Seleccione el identificador que se encuentre en primer lugar y anótelo para poder introducirlo más adelante.  Nota: Independientemente del numero de identificadores existentes deberá seleccionar siempre aquél que se encuentre en primera posición.

Realice los siguientes pasos en el controlador de dominio del dominio al que pertenece el equipo Windows 10 que está asegurando para permitir el uso de dispositivos USB.

Paso	Descripción
95.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
96.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

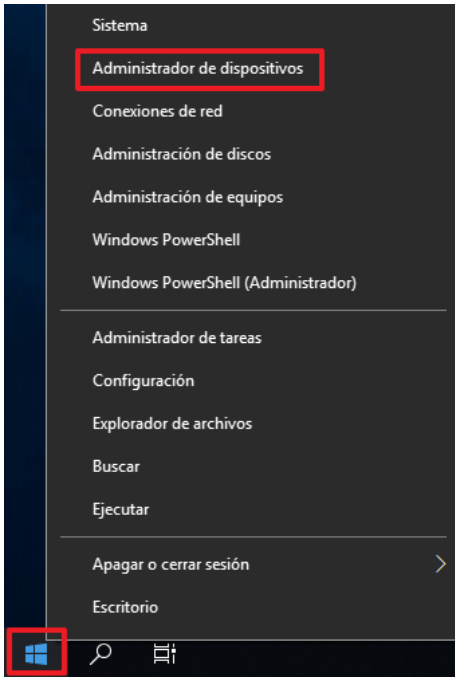
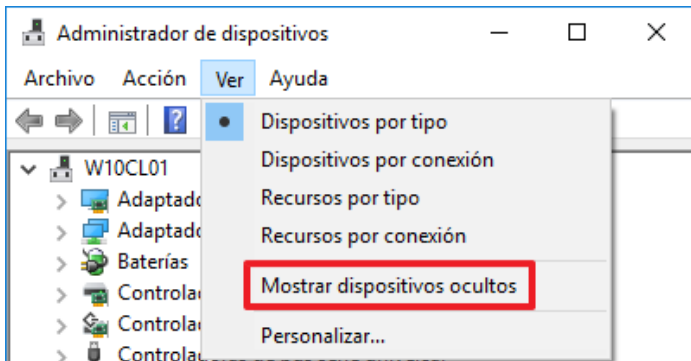
Paso	Descripción
97.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
98.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
99.	En el apartado "Objetos de directiva de grupo" seleccione la GPO creada anteriormente con el botón derecho y seleccione la opción del menú contextual "Editar". 
100.	Despliegue el nodo "Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos". 

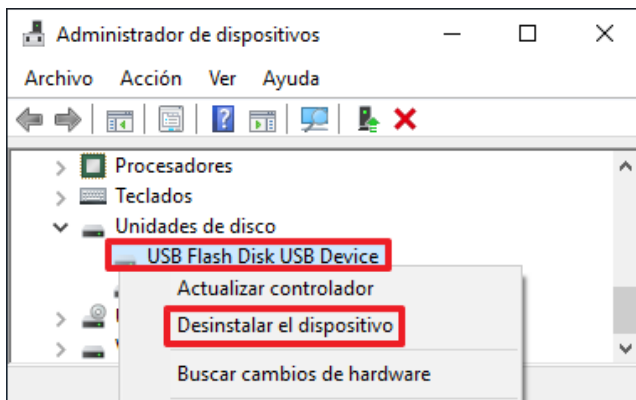
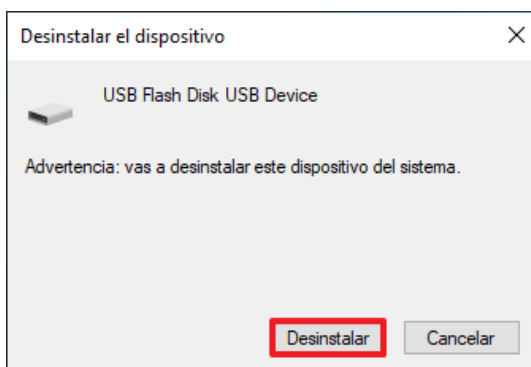
Paso	Descripción
101.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar...”. 
102.	En la ventana “Mostrar contenido” haga doble clic sobre la segunda línea para poder escribir. Introduzca entonces el identificador de USB copiado anteriormente. Pulse “Aceptar” para continuar. 
103.	Deberá repetir este proceso hasta que no se muestren nuevos identificadores en la propiedad “ID. de Hardware” del dispositivo que esta 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”.

Paso	Descripción
104.	Deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 
105.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca la credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar. 
106.	Ejecute el comando “gpupdate /force” y espere a que finalice. 
107.	A partir de este momento el dispositivo estará listo para su uso.

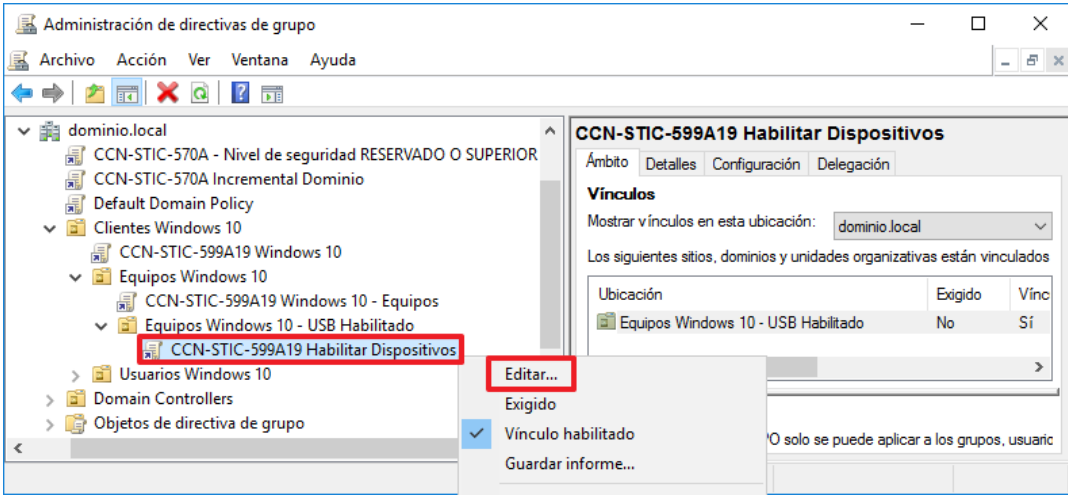
3.2. IMPEDIR EL USO DE DISPOSITIVOS USB

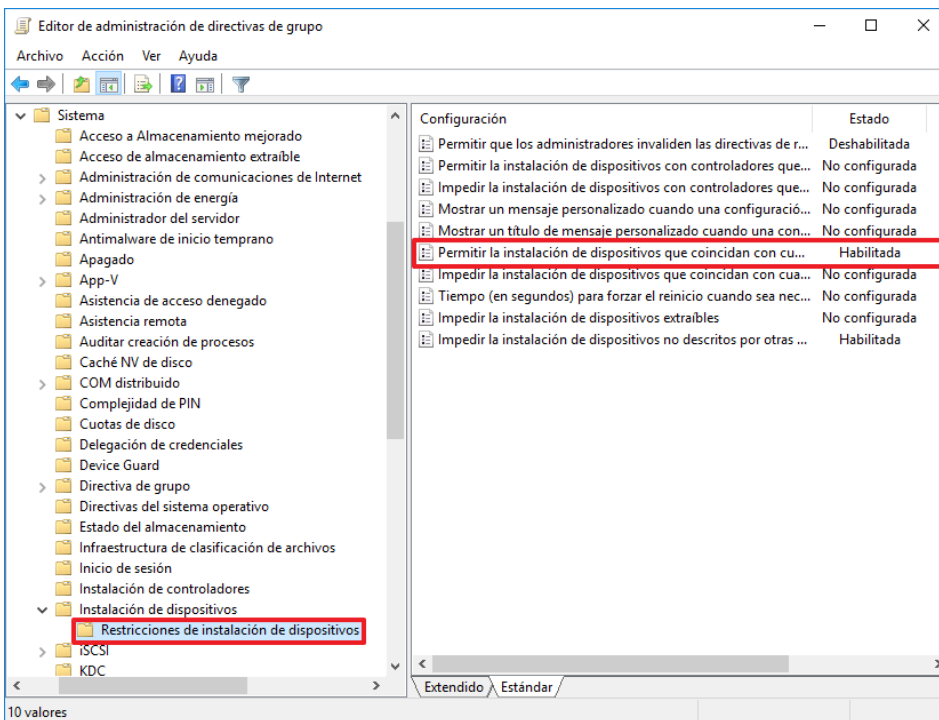
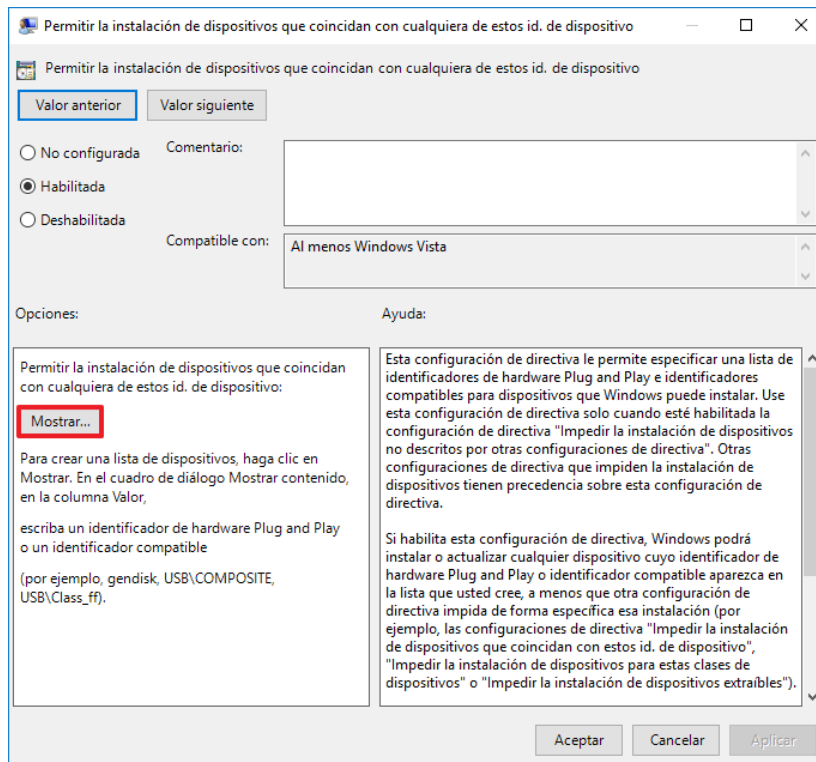
Tras la instalación del dispositivo y su posterior uso, será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

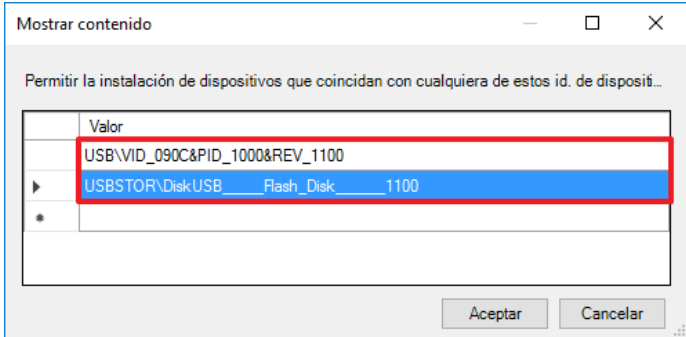
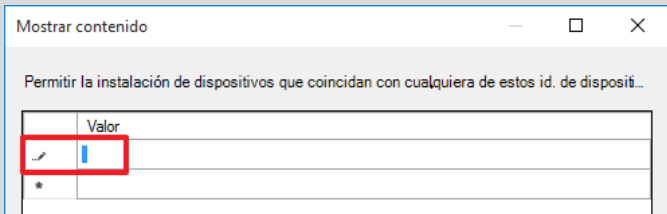
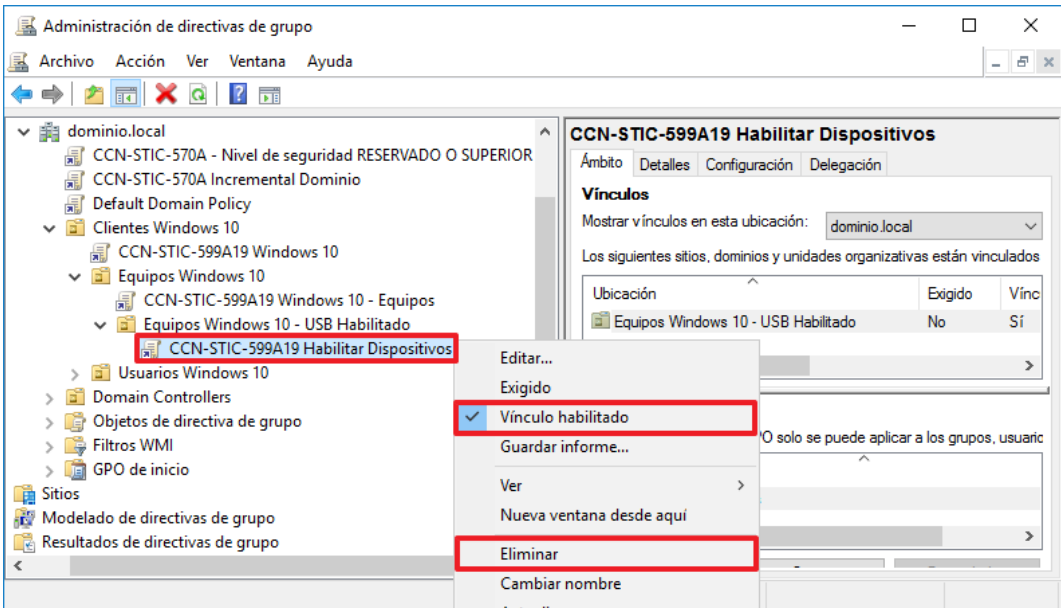
Paso	Descripción
108.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
109.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
110.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

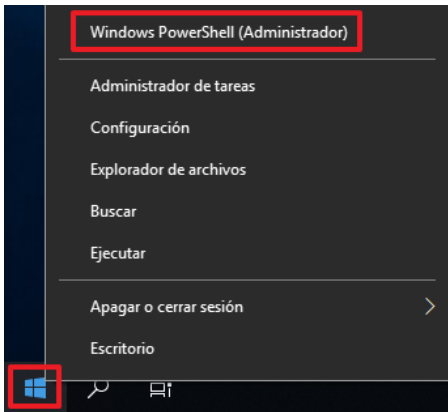
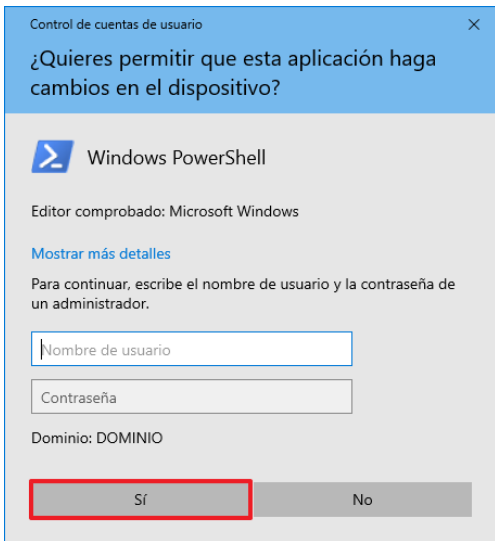
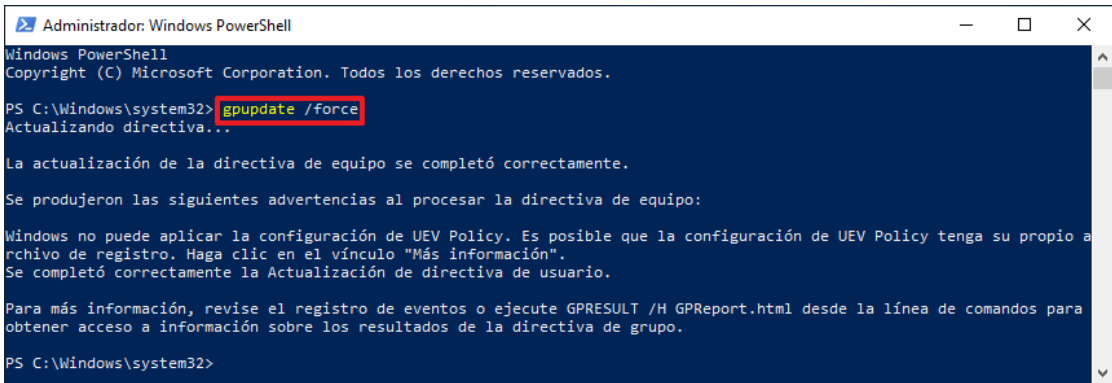
Paso	Descripción
111.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 
112.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
113.	Pulse “Desinstalar” ante 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.

Ejecute los siguientes pasos en el equipo controlador del dominio al que pertenece el equipo Windows 10 sobre el que se está deshabilitando el uso de dispositivos USB.

Paso	Descripción
114.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
115.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. Nota: El sistema le solicitará elevación de privilegios.
116.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
117.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
118.	En el apartado "Objetos de directiva de grupo" seleccione la GPO creada anteriormente con el botón derecho y seleccione la opción del menú contextual "Editar...". 

Paso	Descripción
119.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 
120.	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...”. 

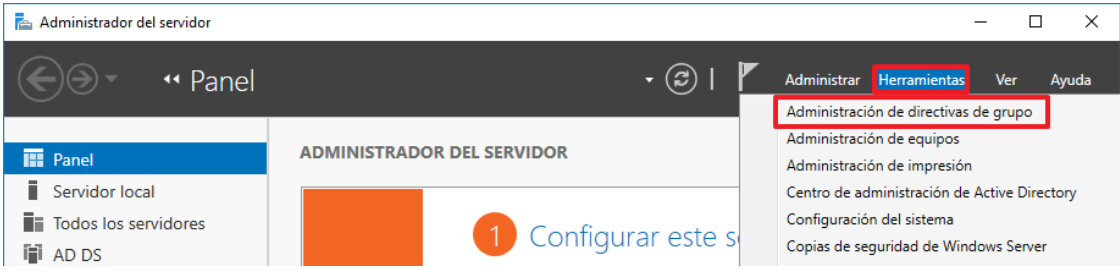
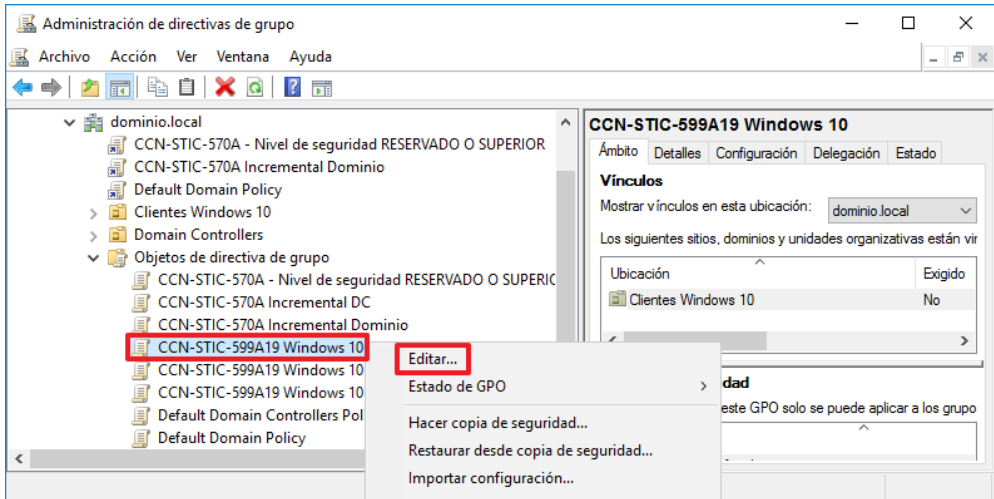
Paso	Descripción
121.	Elimine los identificadores correspondientes a los dispositivos sobre los cuales ya no se desea su uso.  Nota: En caso de eliminar todas las líneas debe dejarse al menos una línea con un espacio en blanco para poder cerrar la configuración de la directiva. En caso contrario se mostrará un error. 
122.	Sobre la unidad organizativa creada para habilitar el uso de dispositivos USB “Equipos Windows 10 – USB habilitado” seleccione la GPO vinculada “CCN-STIC-599A19 Habilitar dispositivos” con el botón derecho y desmarque la opción “Vínculo habilitado” o seleccione “Eliminar”.  Nota: Este paso no será necesario si desea seguir permitiendo algún dispositivo USB en los equipos. En ese caso solo deberá eliminar los ID que pertenezcan a los USB que desea bloquear en los equipos.

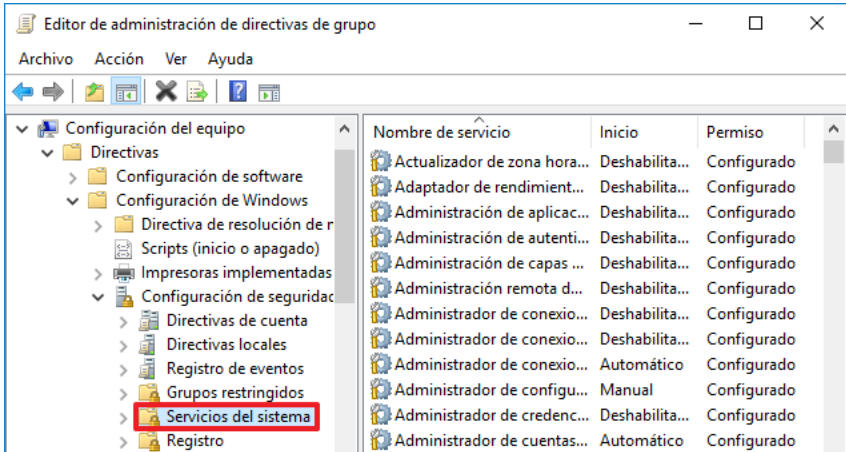
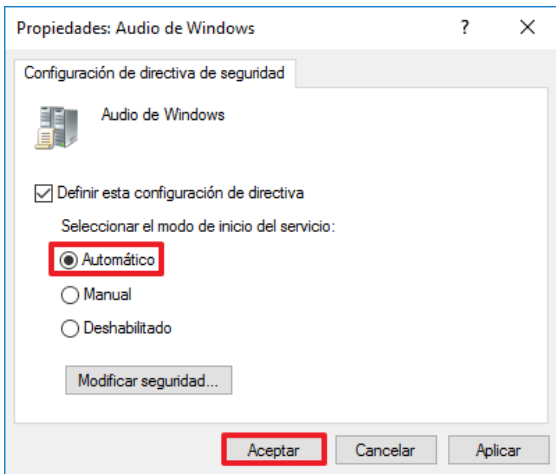
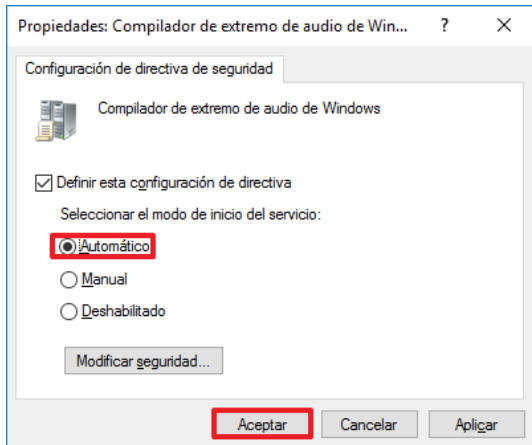
Paso	Descripción
123.	Por último, deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 
124.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar. 
125.	Ejecute el comando “gpupdate /force” y espere a que finalice. 

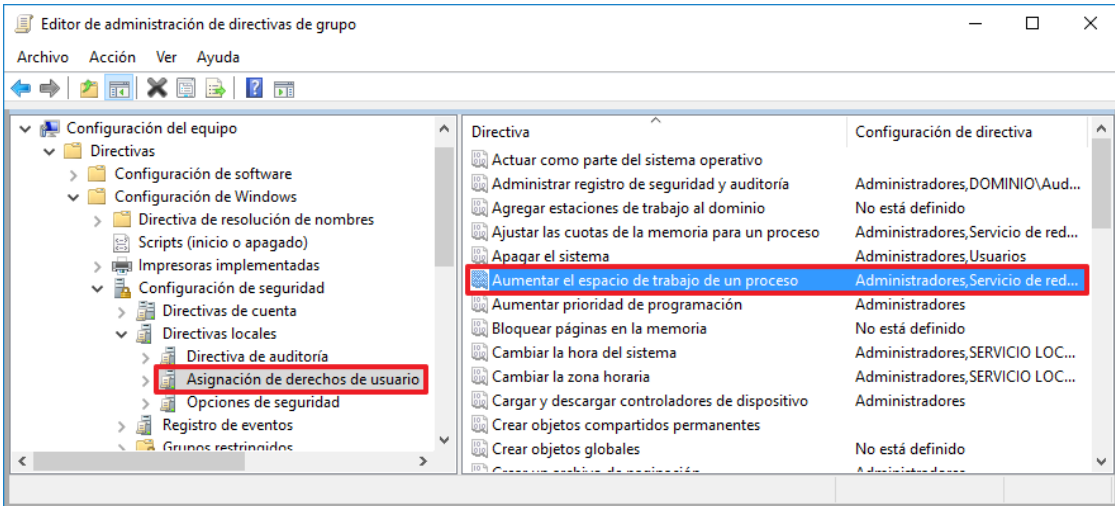
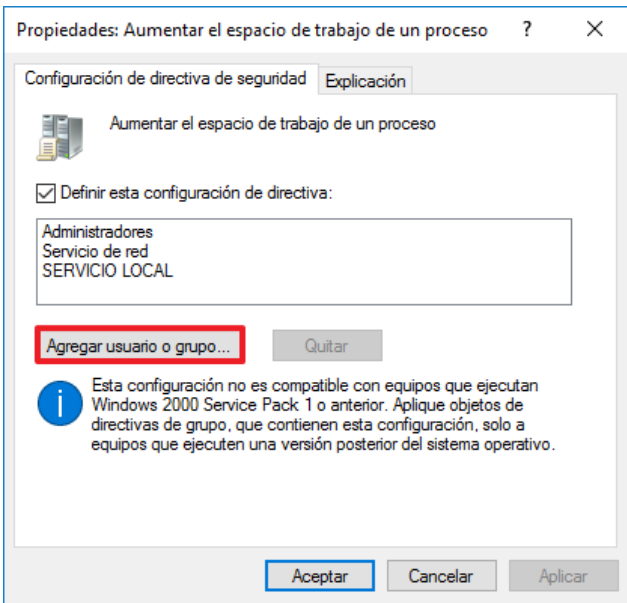
ANEXO B.2.3. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19

A continuación, se indican los pasos a realizar para modificar la plantilla de seguridad a aplicar sobre equipos Windows 10, miembros del dominio, con el objetivo de habilitar el sonido del sistema. Para habilitar el sonido en los equipos, se deberá actualizar el objeto de directiva de grupo “CCN-STIC-599A19 Windows 10” siguiendo la configuración que se indica a continuación.

Nota: En caso de que solamente fuera necesario activar el sonido en algunos de los equipos, en lugar de modificar la directiva “CCN-STIC-599A19 Windows 10”, sería posible establecer una nueva directiva denominada, por ejemplo, “CCN-STIC-599A19 Windows 10 con sonido”. Crear así mismo una unidad organizativa específica llamada, por ejemplo, Clientes Windows 10 con sonido y, de una forma similar a los pasos efectuados en el anexo anterior, modificar la directiva vacía con los pasos siguientes y, vincular y mover equipos a la unidad organizativa que ha creado con esta finalidad.

Paso	Descripción
126.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar el sonido.
127.	Utilizando la herramienta "Administrador del servidor", Seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 
128.	En la consola “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo"
129.	Localice la directiva “CCN-STIC-599A19 Windows 10”, selecciónela con el botón derecho del ratón y pulse sobre “Editar...”. 

Paso	Descripción
130.	Edite los servicios de sistema mediante la siguiente ruta: "Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema" 
131.	Haga doble clic sobre el servicio "Audio de Windows", seleccione el modo de inicio "Automático" y pulse "Aceptar". 
132.	Repita el mismo proceso con el servicio "Compilador de extremo de audio de Windows". 

Paso	Descripción
133.	De nuevo en el “Editor de administración de directivas de grupo”, acceda al apartado “Asignación de derechos de usuario” mediante la siguiente ruta: "Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuarios"
134.	Haga doble clic sobre la directiva “Aumentar el espacio de trabajo de un proceso”. 
135.	En la ventana de “Propiedades: Aumentar el espacio de trabajo de un proceso” compruebe que al menos uno de estos dos elementos aparece en la lista y, de no ser así, añádalo mediante el botón “Agregar usuario o grupo...”: – Usuarios – SERVICIO LOCAL 

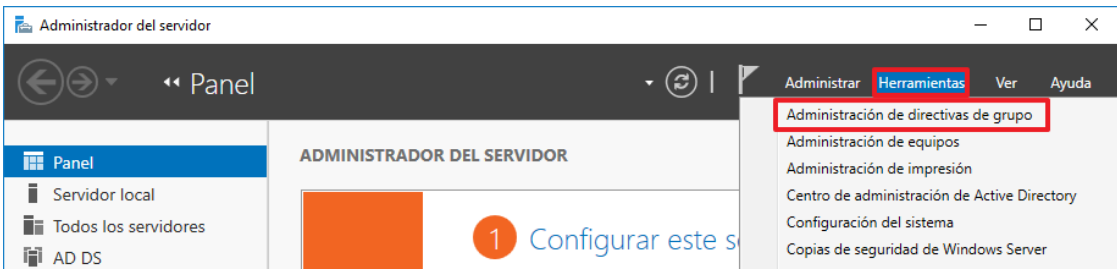
ANEXO B.2.4. CONFIGURACIÓN PARA USO DE NESSUS

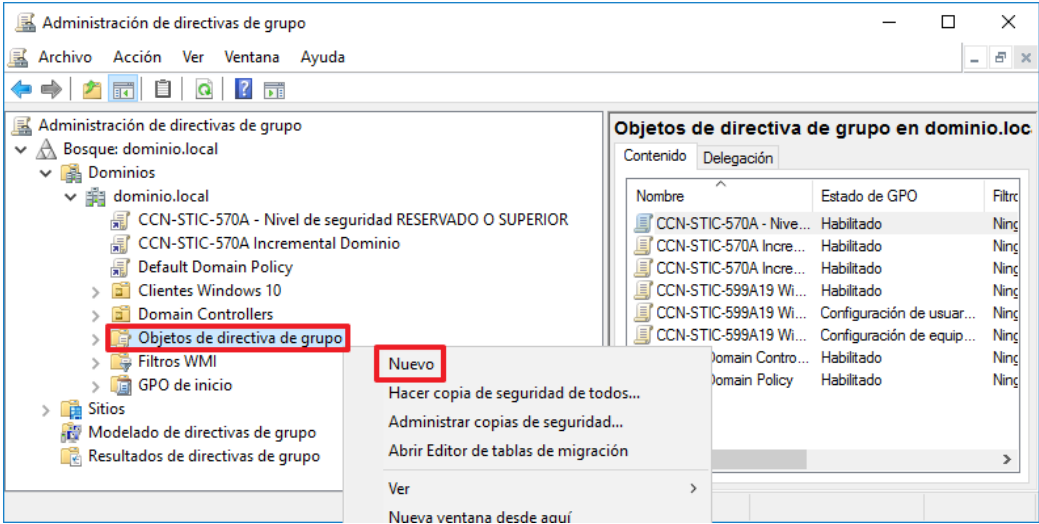
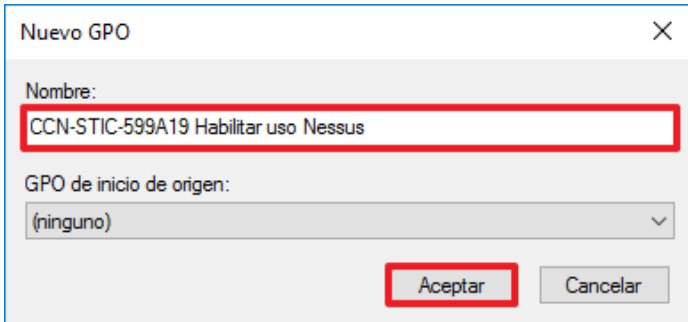
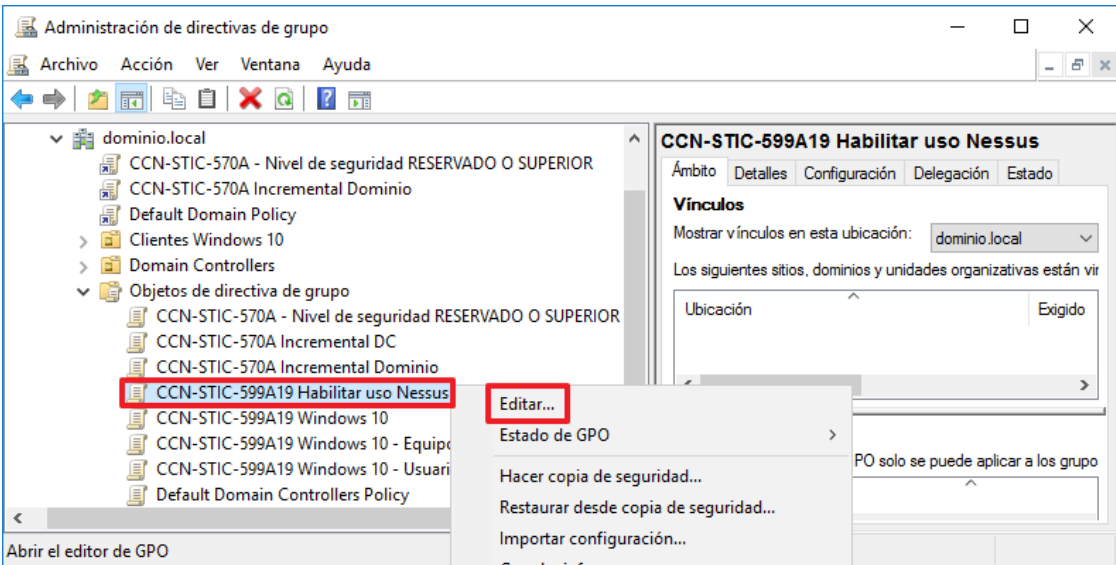
Este anexo ha sido diseñado con el objetivo de establecer la configuración necesaria para que se permita realizar un escáner de vulnerabilidades sobre los equipos Windows 10 haciendo uso de la aplicación Nessus (escáner de vulnerabilidades), localizada en una ubicación remota en la red.

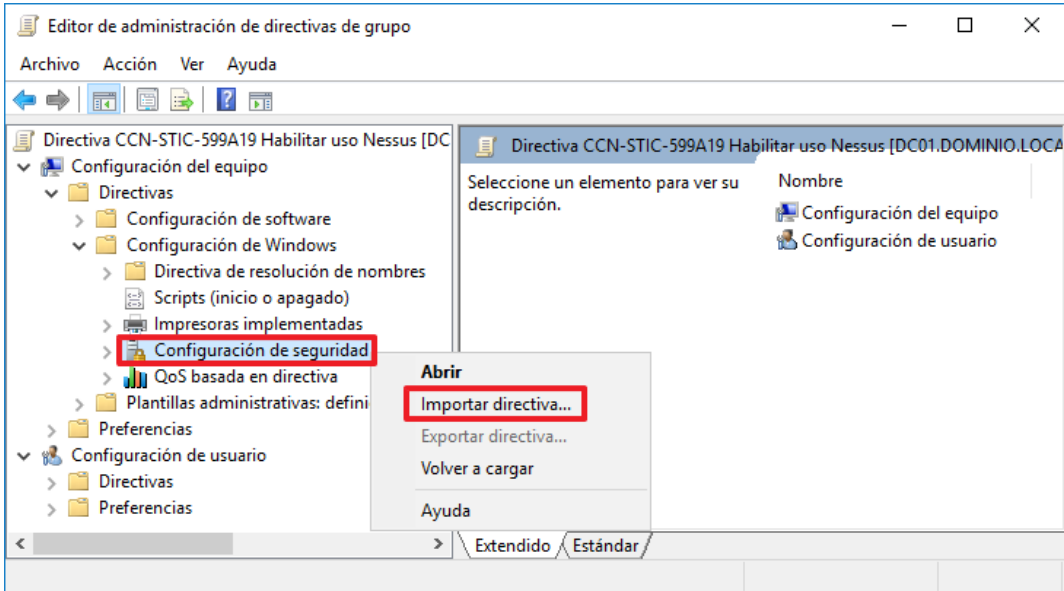
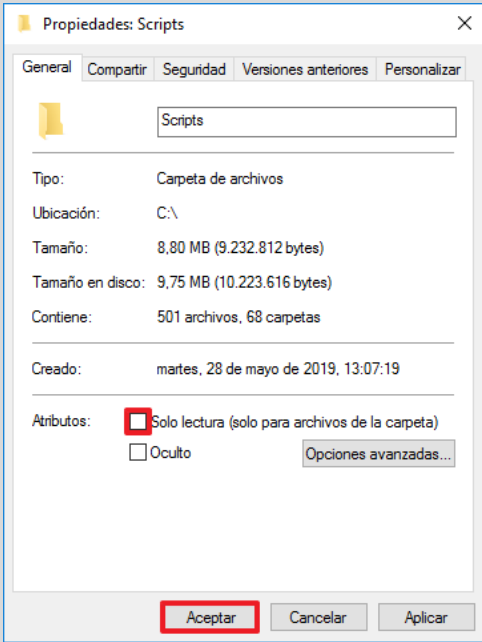
Es necesario resaltar que para permitir el uso de la herramienta Nessus, es necesario aplicar una configuración específica que habilita la comunicación NTLM, el uso compartido de archivos e impresoras en los adaptadores de red e iniciar el servicio “Servidor” durante la ejecución del escáner de vulnerabilidades.

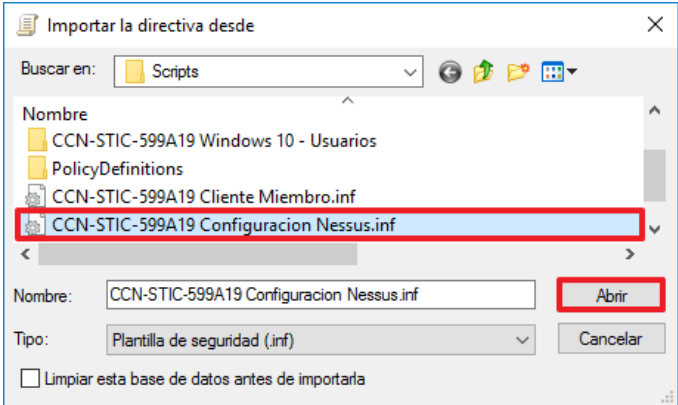
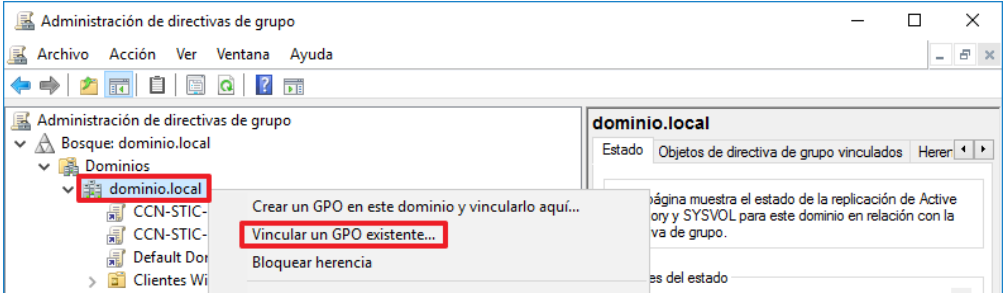
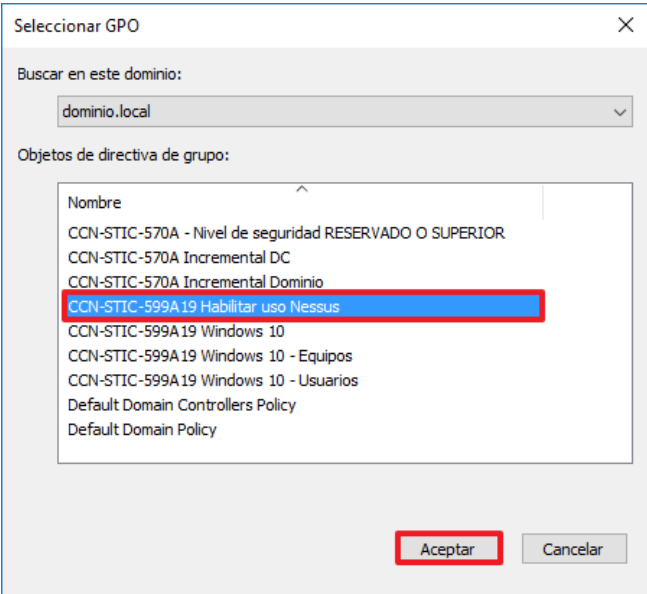
Nota: Dependiendo de la configuración de su equipo, es posible que la configuración que se lleva a cabo en los siguientes pasos ya se encuentre habilitada.

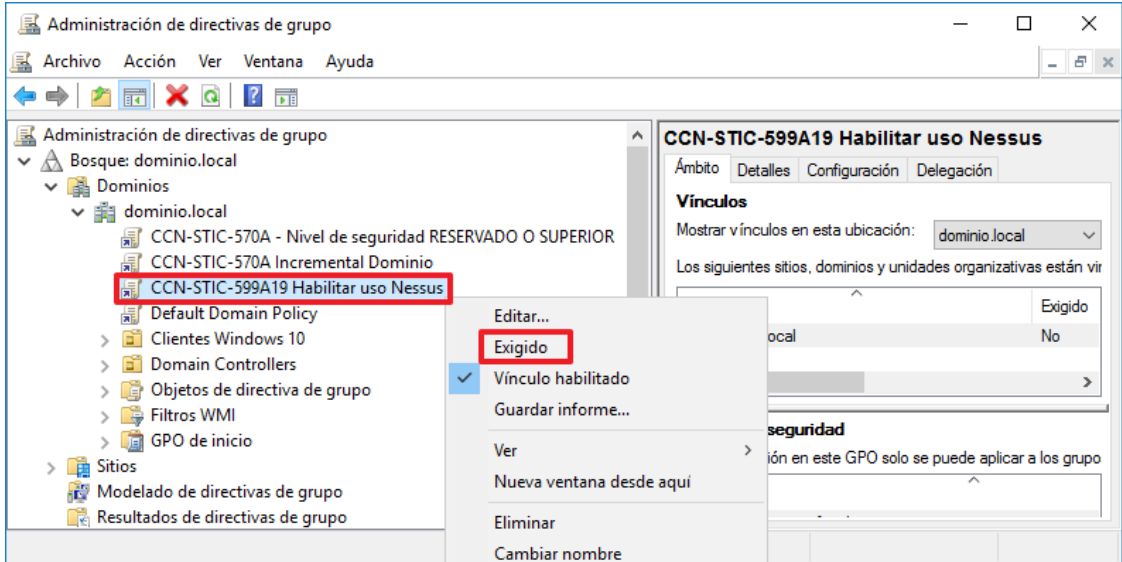
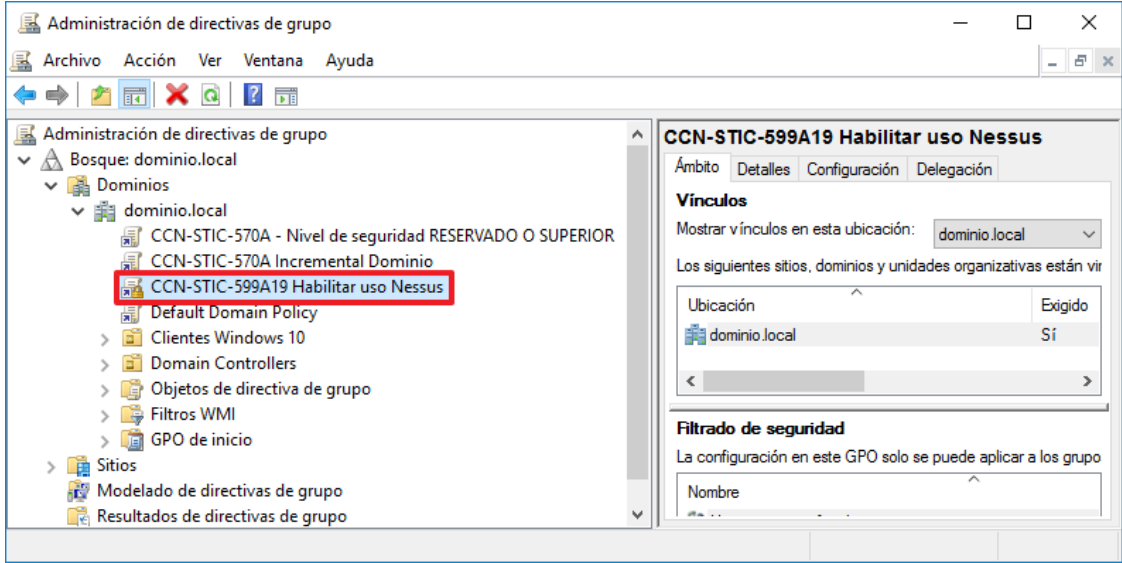
1. HABILITAR AUTENTICACIÓN PARA USO DE NESSUS

Paso	Descripción
1.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar la configuración para el uso de Nessus.
2.	Cree el directorio C:\Scripts.
3.	Copie los ficheros y directorios asociados a esta guía en el directorio “C:\Scripts” y asegúrese de que existen al menos los siguientes ficheros: CCN-STIC-599A19 – Configuración Nessus.inf Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”.
4.	Utilizando la herramienta “Administrador del servidor”, seleccione en el menú superior “Herramientas” y pulse sobre “Administración de directivas de grupo”. 
5.	En la consola “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo"

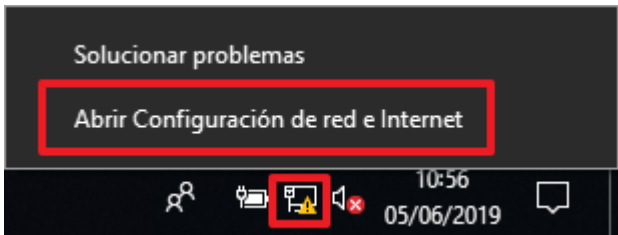
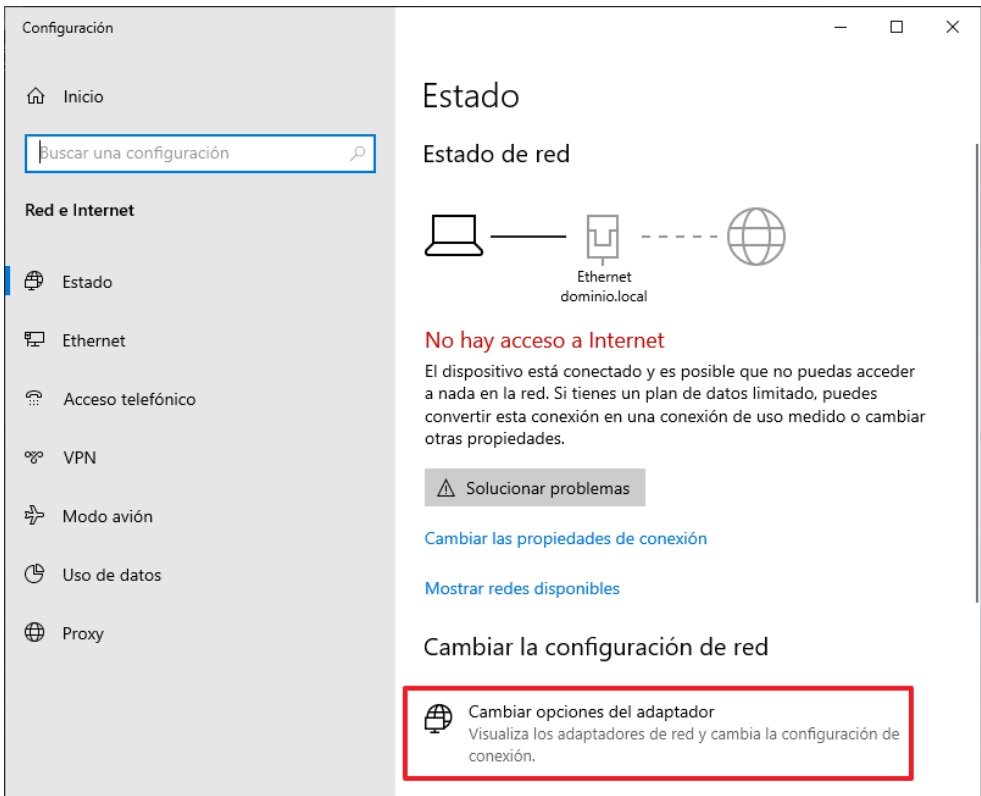
Paso	Descripción
6.	Pulse con el botón derecho sobre “Objetos de directiva de grupo” y seleccione la opción del menú contextual “Nuevo”. 
7.	Establezca el nombre para la GPO “CCN-STIC-599A19 Habilitar uso Nessus” y pulse “Aceptar” para continuar. 
8.	Haga clic derecho sobre la GPO recién creada y pulse sobre la opción del menú contextual “Editar...”. 

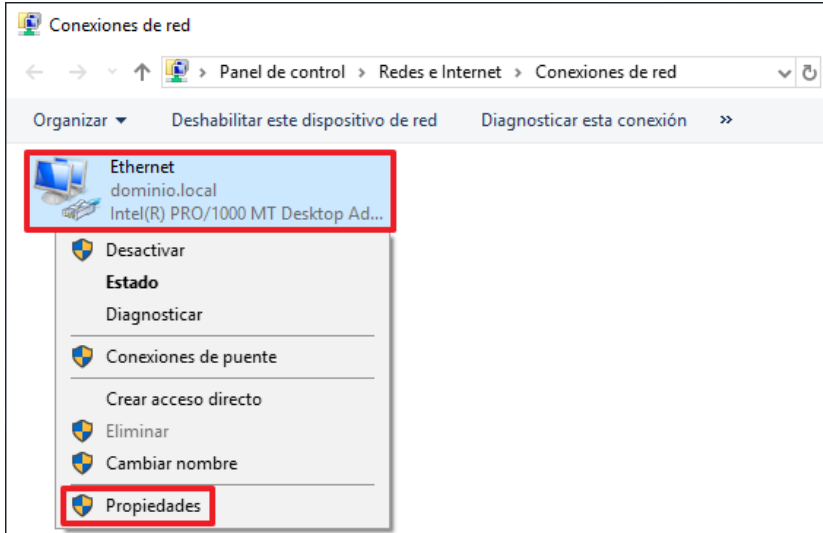
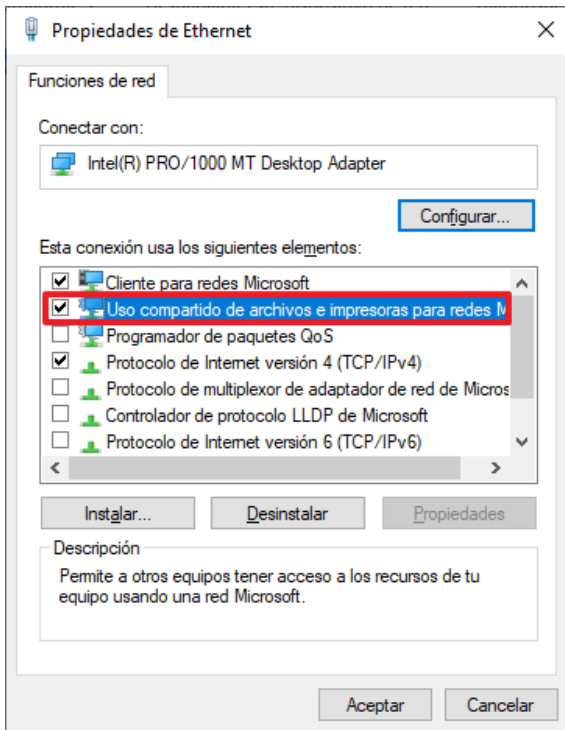
Paso	Descripción
9.	Despliegue la GPO hasta acceder al siguiente nodo: “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad” Haga clic derecho sobre “Configuración de seguridad” y seleccione la opción del menú contextual “Importar directiva...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts” no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

Paso	Descripción
10.	Identifique el fichero “CCN-STIC-599A19 Configuración Nessus.inf” en el directorio “C:\Scripts” y pulse sobre el botón “Abrir”. 
11.	Con esto habrá quedada configurada la GPO para el uso de Nessus. Cierre el “Editor de administración de directivas de grupo”.
12.	A continuación sobre la raíz del dominio haga clic derecho y seleccione la opción del menú contextual “Vincular un GPO existente...”. 
13.	Seleccione la GPO denominada “CCN-STIC-599A19 Habilitar uso Nessus” y pulse “Aceptar”. 

Paso	Descripción
14.	Por último haga clic derecho sobre la GPO recién vinculada y seleccione la opción del menú contextual “Exigido”.  Nota: Deberá tener en consideración la posibilidad de que en su organización existan más GPOs configuradas con el valor “Exigido”. Ante esta casuística, la aplicación de la GPO varía teniendo preferencia la GPO de dominio sobre la de las Unidades Organizativas (UO). En caso de necesitar solo auditar ciertos equipos deberá crear un grupo al que se añadirán todos los equipos a auditar incluyendo de manera obligatoria a los servidores controladores de dominio. Tras esto deberá añadir dicho grupo en el filtrado de seguridad de la GPO de manera que únicamente a los equipos miembros del grupo les sea de aplicación dicha GPO.
15.	Asegúrese que la GPO esta en estado “exigida” para que se aplique siempre en primer lugar. 

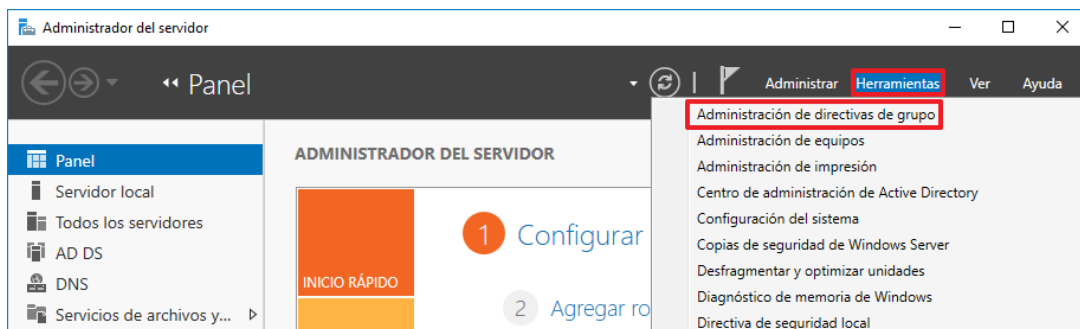
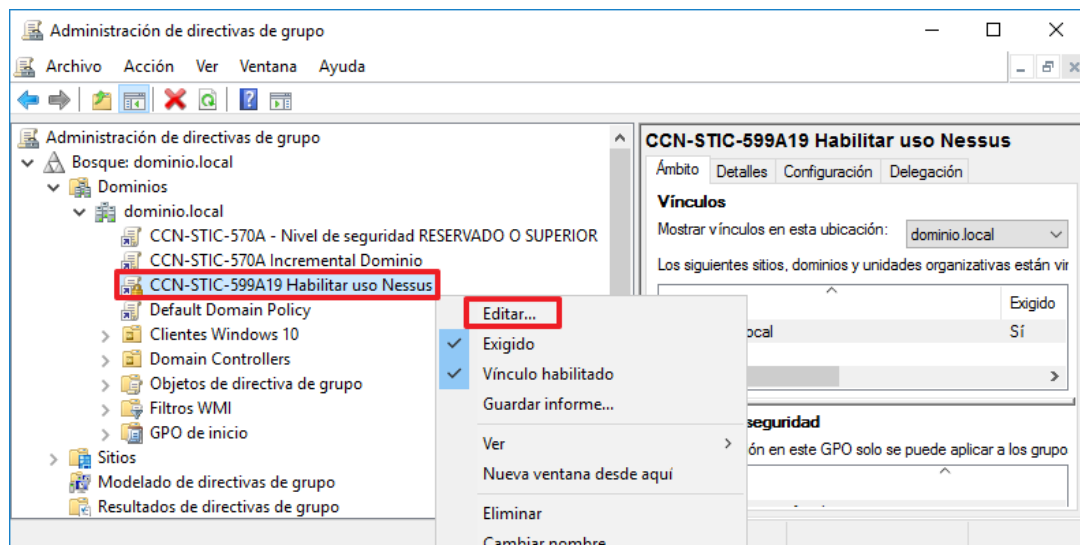
En este momento queda configurado el dominio para permitir el uso de Nessus. Los pasos realizados a continuación se deben hacer en cada equipo que se desea analizar con la herramienta Nessus.

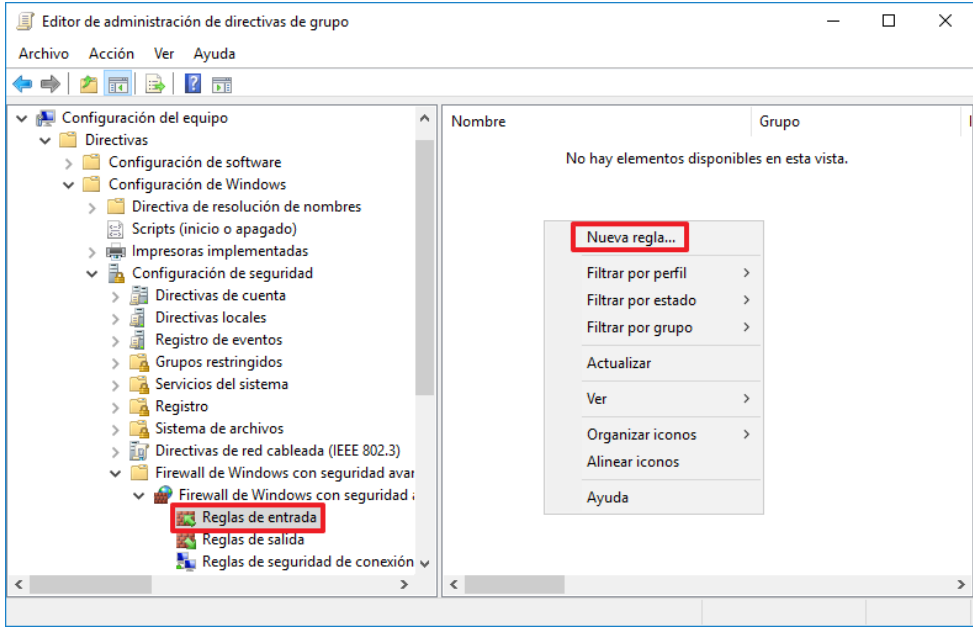
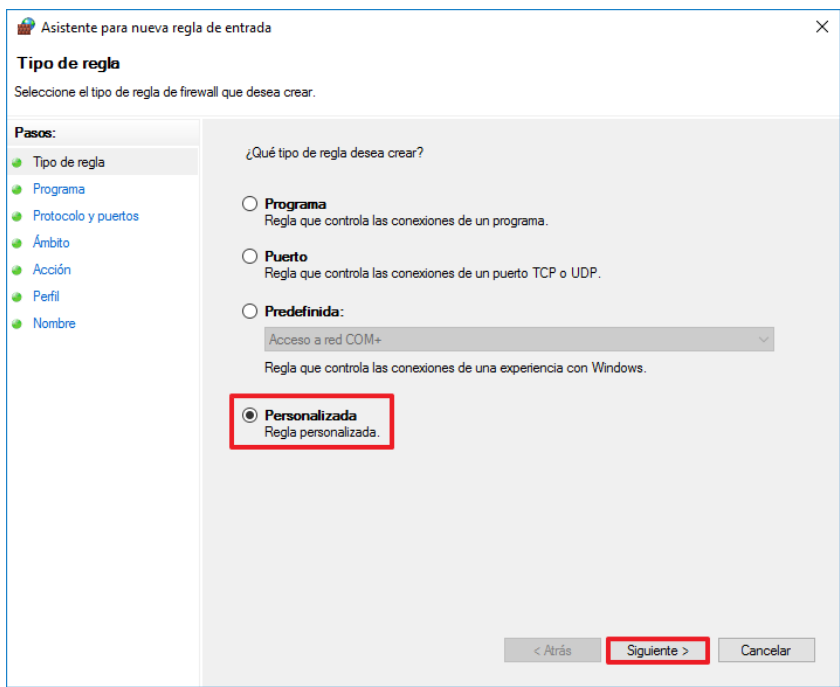
Paso	Descripción
16.	Inicie sesión en el equipo cliente sobre el que se desea permitir el análisis con la herramienta Nessus.
17.	Debe iniciar sesión con un usuario que posea permisos de administración del dominio.
18.	Seleccione el icono correspondiente a la red en la parte inferior derecha con el botón derecho del ratón y seleccione la opción “Abrir Configuración de red e Internet”. 
19.	En la ventana de configuración, seleccione la opción “Cambiar opciones del adaptador”. 

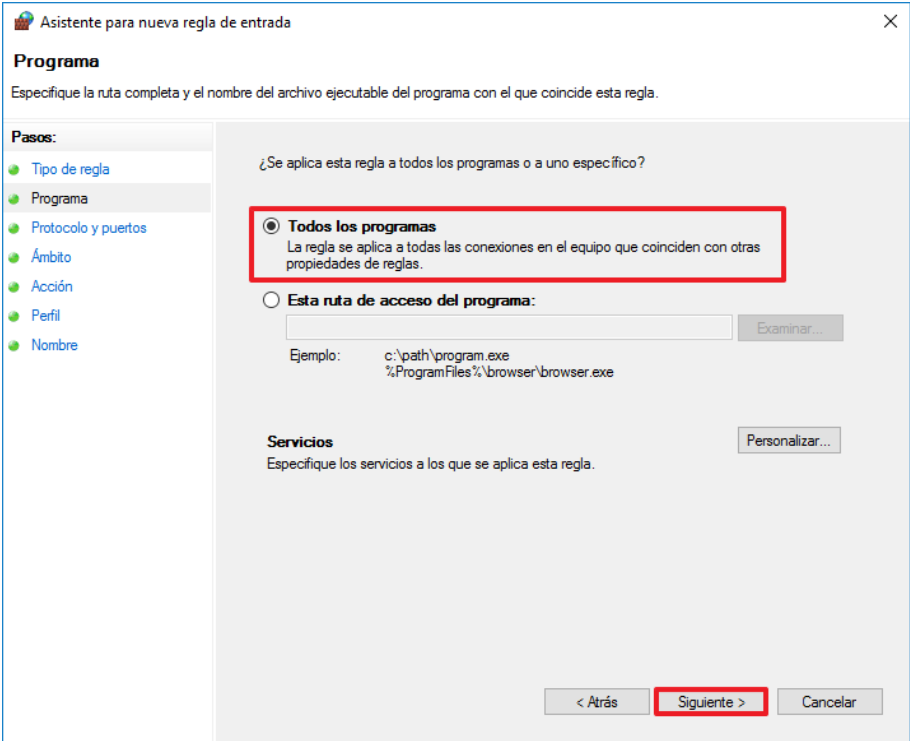
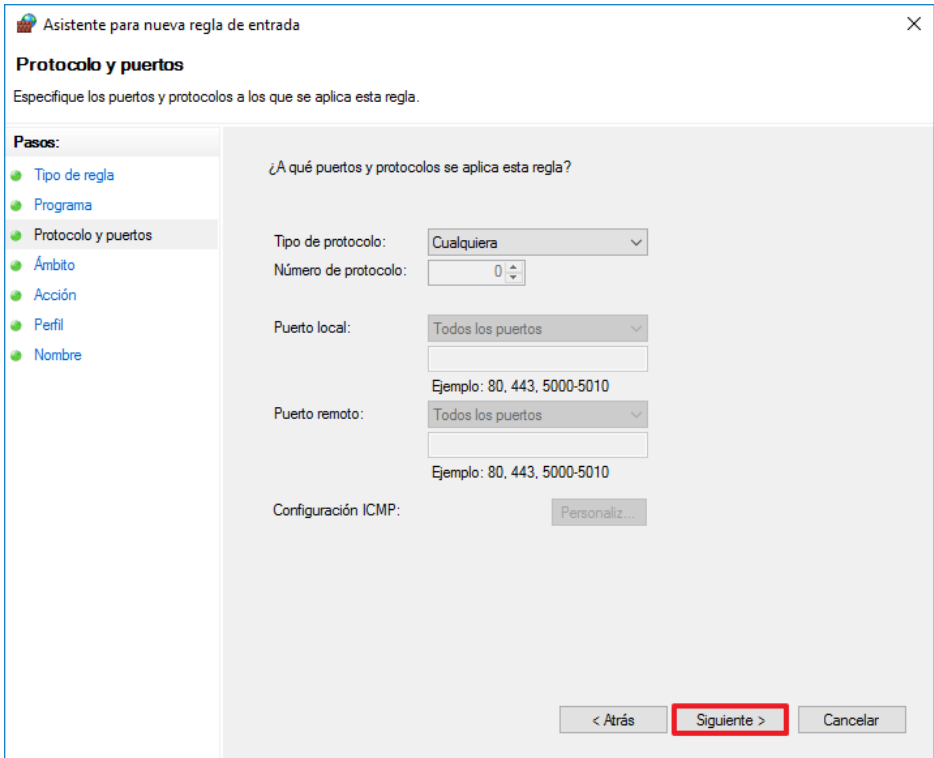
Paso	Descripción
20.	Seleccione con el botón derecho el adaptador de red correspondiente y seleccione la opción del menú contextual “Propiedades”. 
21.	El Control de cuentas de usuario le pedirá la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración del dominio.
22.	Asegurése que esta marcada la opción “Uso compartido de archivos e impresoras para redes Microsoft”. En caso contrario márkuela y cierre todas las ventanas. 
23.	Elimine el directorio “C:\Scripts” del equipo controlador de dominio.
24.	Para finalizar reinicie el equipo o ejecute “gpupdate /force” en la línea de comandos para que se aplique la GPO configurada anteriormente.

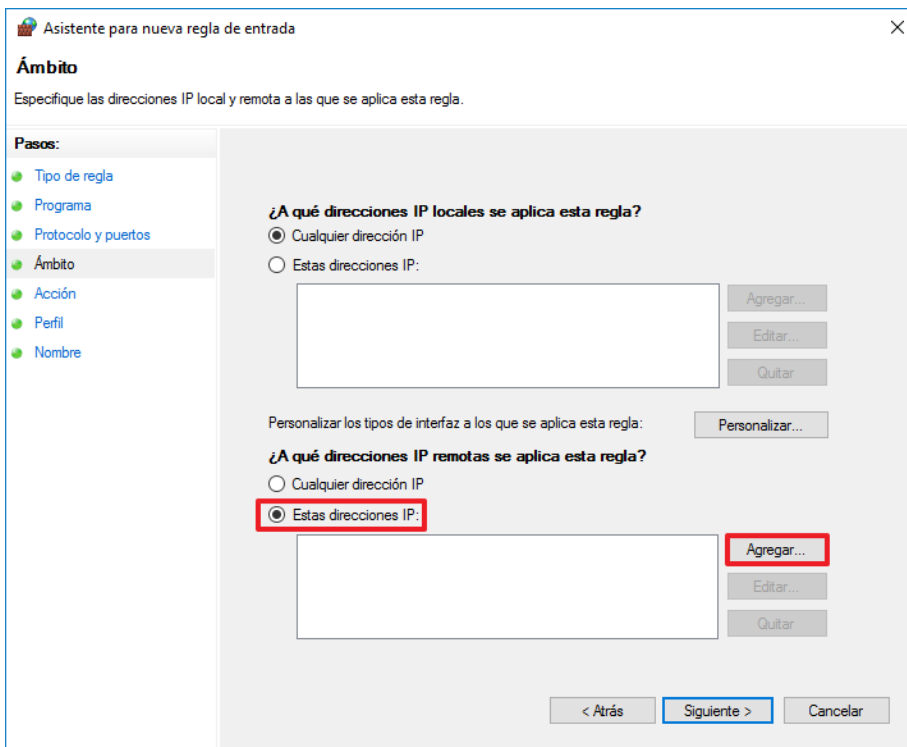
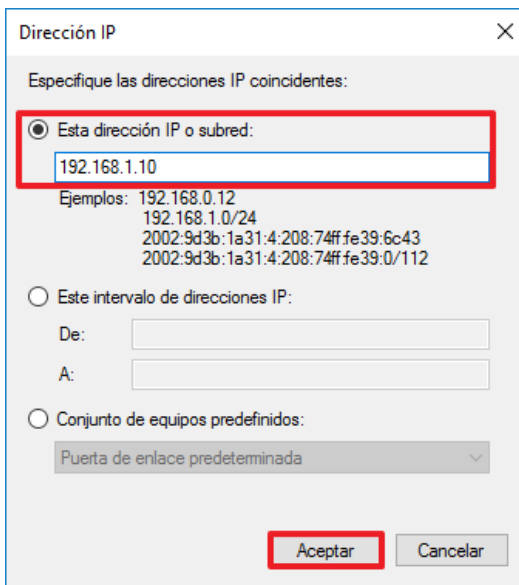
2. PERMITIR COMUNICACIÓN EN EL FIREWALL

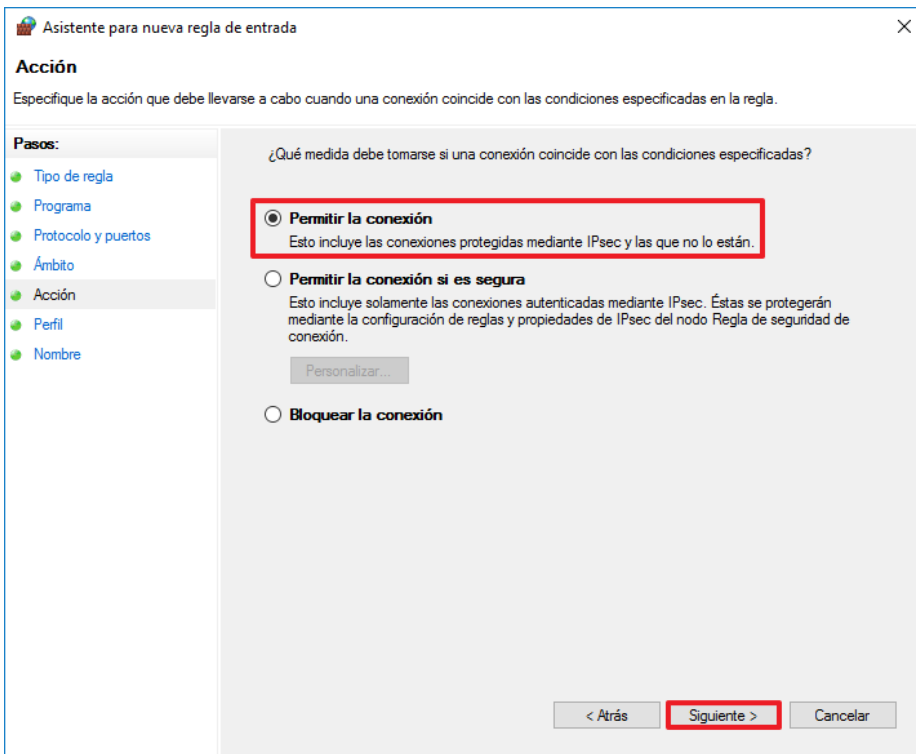
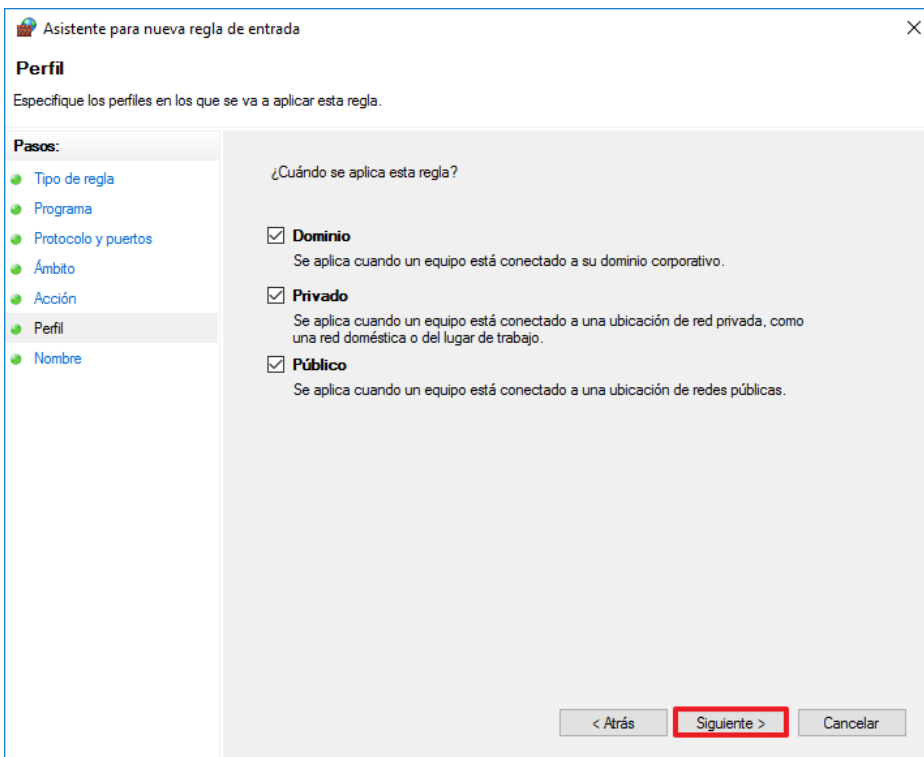
El siguiente procedimiento establece los pasos necesarios para permitir una comunicación total a través del firewall entre el equipo donde se encuentra instalada la aplicación Nessus, y el equipo que se analiza.

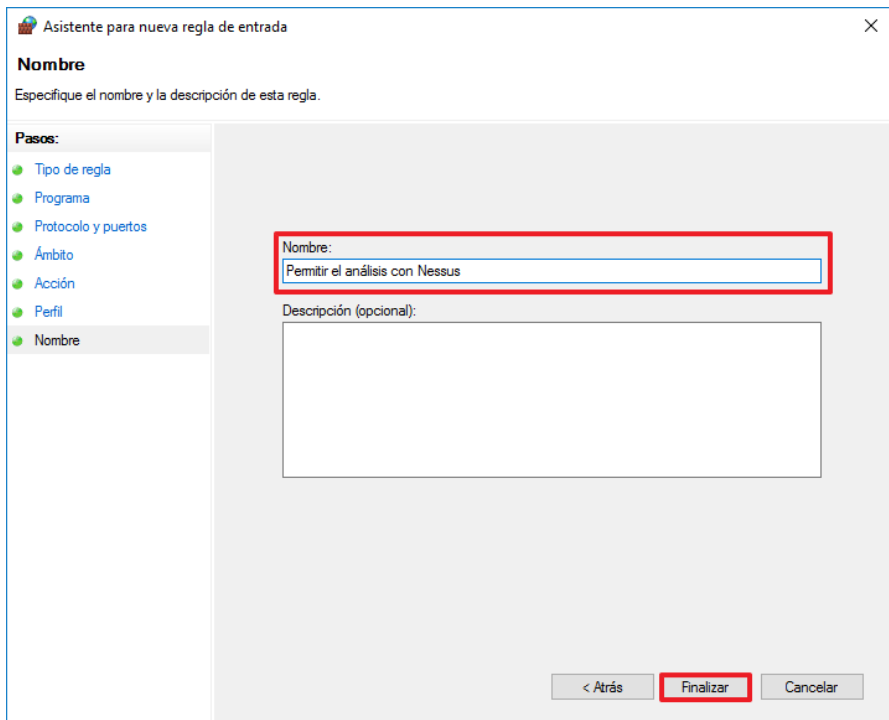
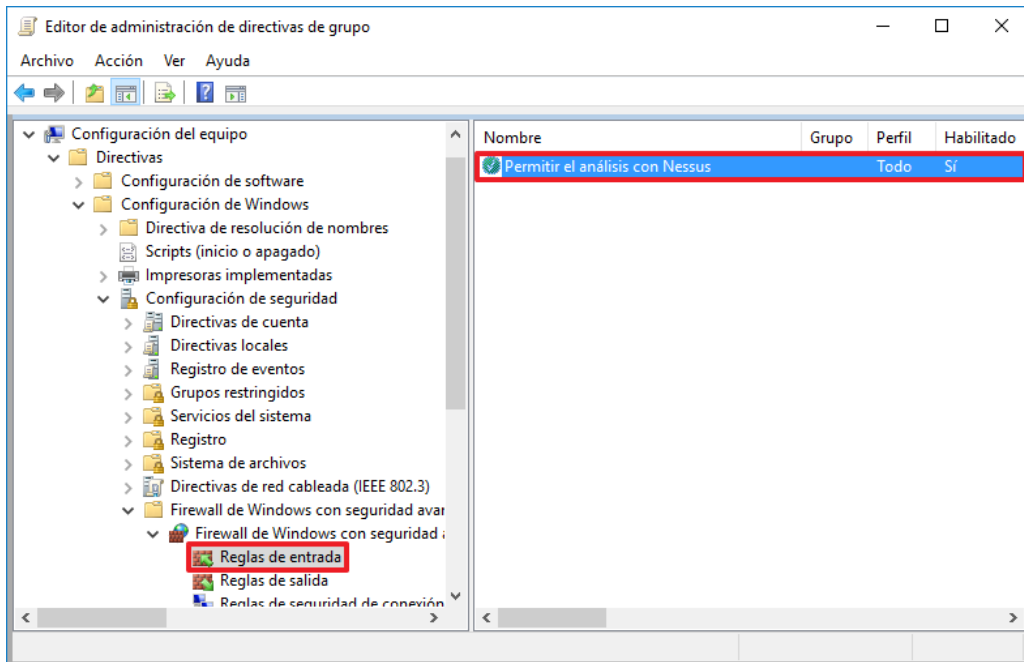
Paso	Descripción
25.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar la configuración para el uso de Nessus.
26.	Utilizando la herramienta "Administrador del servidor", Seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 
27.	En la consola "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta: "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo"
28.	Sobre la GPO configurada en pasos anteriores, "CCN-STIC-599A19 Habilitar uso Nessus", pulse con el botón derecho y seleccione la opción del menú contextual "Editar". 

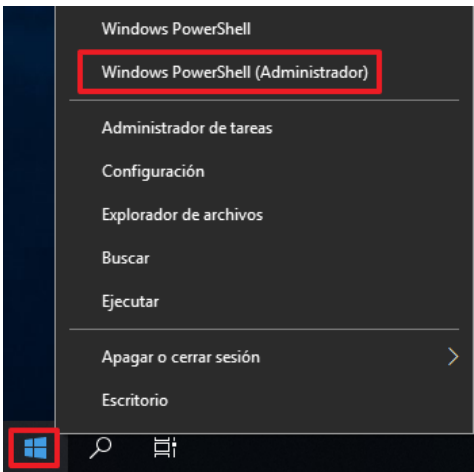
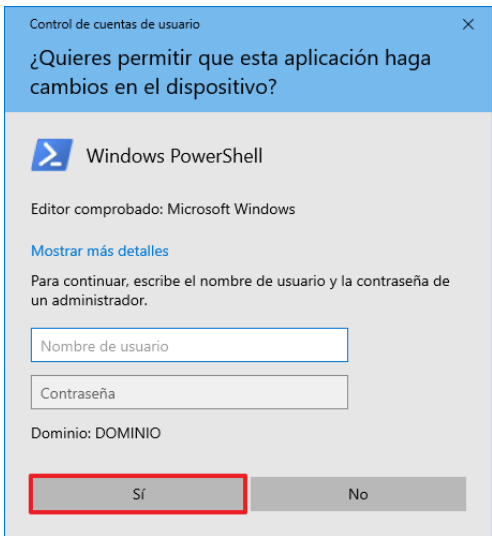
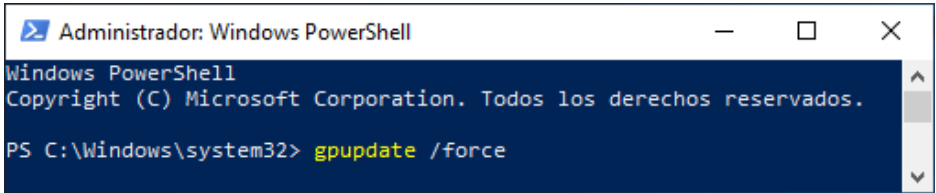
Paso	Descripción
29.	Despliegue la GPO hasta acceder al siguiente nodo: “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con Seguridad Avanzada → Firewall de Windows con Seguridad Avanzada → Reglas de entrada” Haga clic derecho sobre un espacio en blanco y seleccione la opción del menú contextual “Nueva regla...”. 
30.	En el apartado “Tipo de regla” seleccione tipo de regla “Personalizada” y pulse “Siguiente >”. 

Paso	Descripción
31.	En el apartado “Programa” seleccione la opción “Todos los programas” y pulse “Siguiente >”. 
32.	En el apartado “Protocolo y puertos” seleccione la opción “Cualquiera” y pulse “Siguiente >” para continuar. 

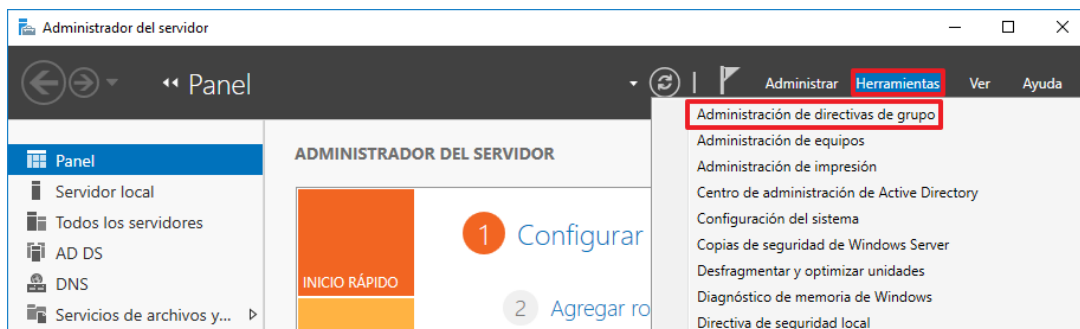
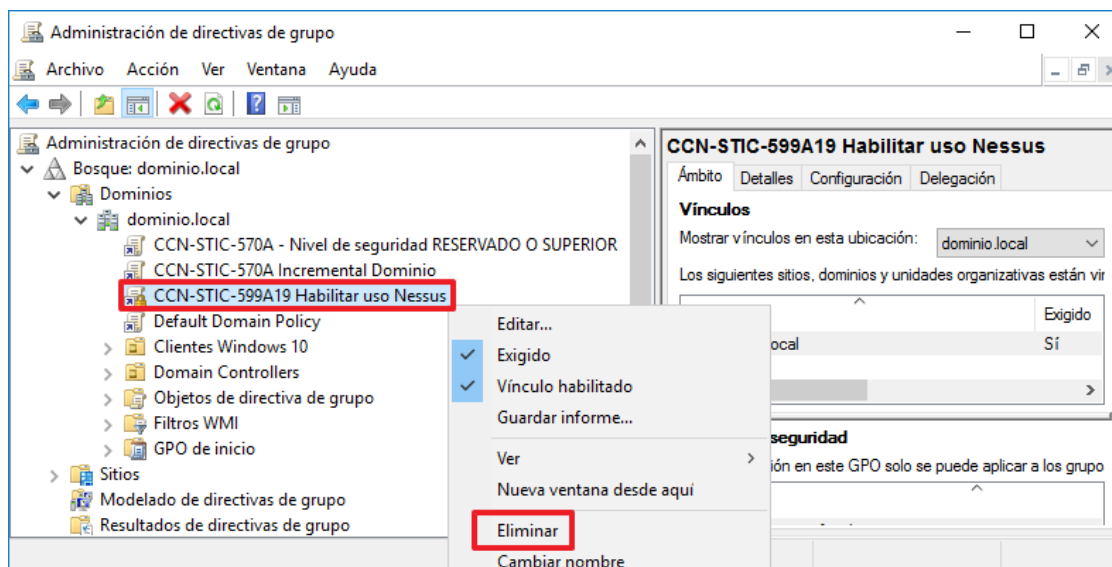
Paso	Descripción
33.	En la ventana “Ámbito”, seleccione en el apartado de IP remotas la opción “Estas direcciones IP:” y a continuación pulse sobre “Agregar...”. 
34.	Seleccione la opción “Esta dirección IP o subred:” y establezca la dirección IP desde donde se va a ejecutar la herramienta Nessus. Pulse “Aceptar” para continuar.  Nota: En este ejemplo, la herramienta Nessus se ejecuta desde la dirección IP “192.168.1.10”.
35.	Pulse “Siguiente >” una vez haya configurado las IP necesarias.

Paso	Descripción
36.	En el apartado “Acción” marque la opción “Permitir la conexión” y pulse “Siguiente >”. 
37.	Pulse “Siguiente >” en el apartado “Perfil”.  Nota: Dependiendo de la configuración de red podrá adaptar este paso y seleccionar el tipo de perfil. Aún así no será necesario realizar ninguna configuración.

Paso	Descripción								
38.	Por último, establezca un nombre para la regla y pulse sobre el botón “Finalizar”. 								
39.	Verifique que ha sido creada la regla de entrada.  <table><tr><th>Nombre</th><th>Grupo</th><th>Perfil</th><th>Habilitado</th></tr><tr><td>Permitir el análisis con Nessus</td><td></td><td>Todo</td><td>Sí</td></tr></table>	Nombre	Grupo	Perfil	Habilitado	Permitir el análisis con Nessus		Todo	Sí
Nombre	Grupo	Perfil	Habilitado						
Permitir el análisis con Nessus		Todo	Sí						

Paso	Descripción
40.	Por último deberá forzar la aplicación de políticas en todos los equipos a analizar al igual que en los equipos controladores de dominio. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en “Inicio → Windows PowerShell (Administrador)”. 
41.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca la credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar. 
42.	Ejecute el comando “gpupdate /force” y espere a que finalice. 

3. ELIMINACIÓN DE LA CONFIGURACIÓN PARA EL USO DE NESSUS

Paso	Descripción
43.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar la configuración para el uso de Nessus.
44.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 
45.	En la consola "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> Elimine la GPO para permitir el análisis con Nessus haciendo clic derecho sobre ella y seleccionando la opción del menú contextual "Eliminar". 

ANEXO B.2.5. 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”.

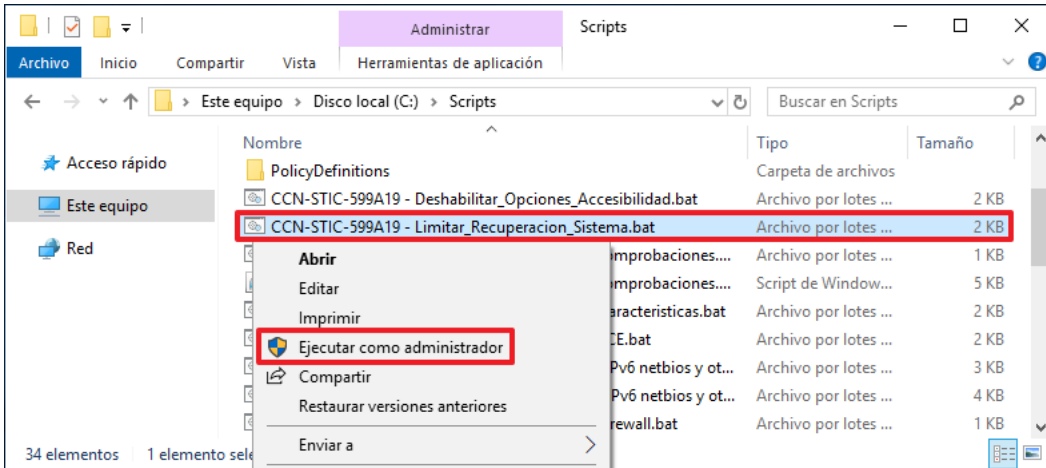
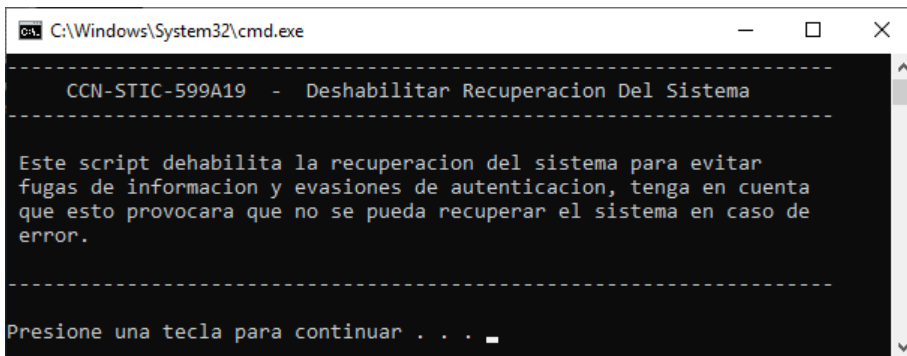
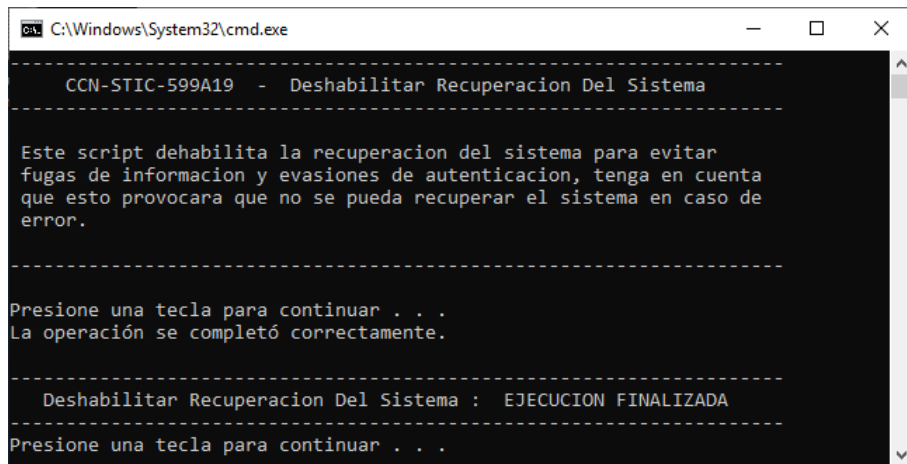
Las medidas a aplicar podrán ser:

- 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.

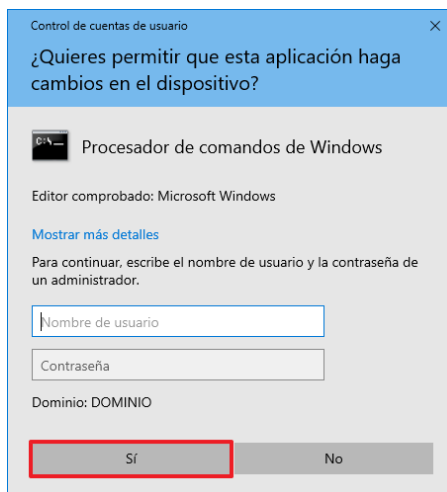
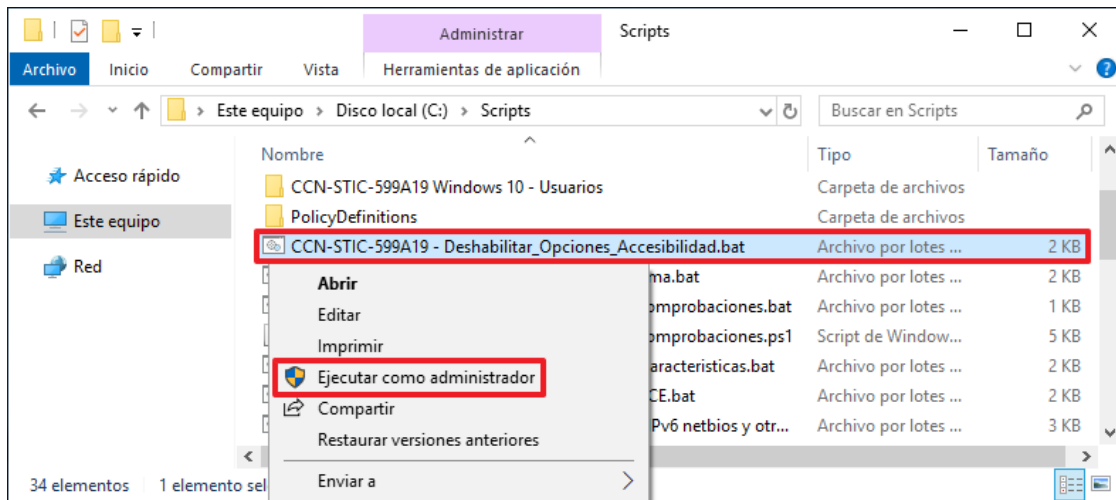
Paso	Descripción
1.	Inicie sesión en el equipo cliente Windows 10 con una cuenta con permisos de administrador del dominio.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.

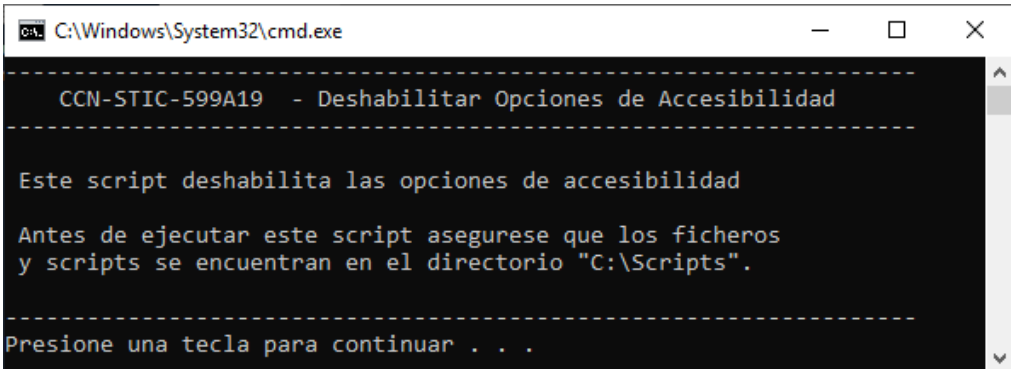
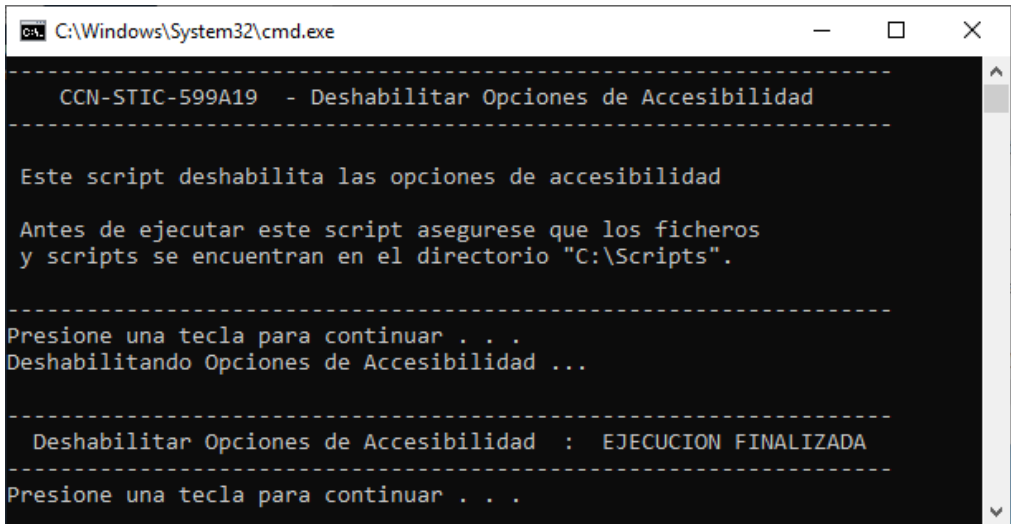
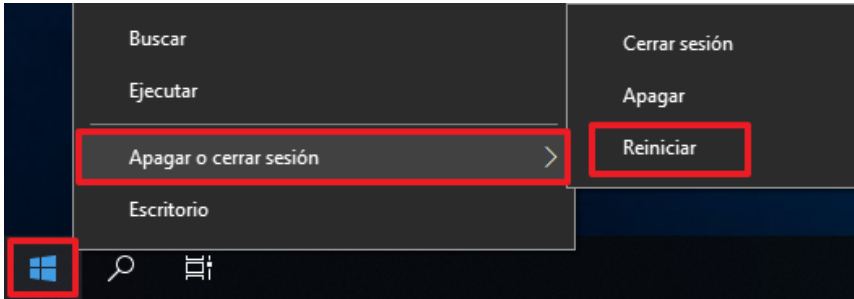
Paso	Descripción
3.	Localice el archivo “CCN-STIC-599A19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”. 
4.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente 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.

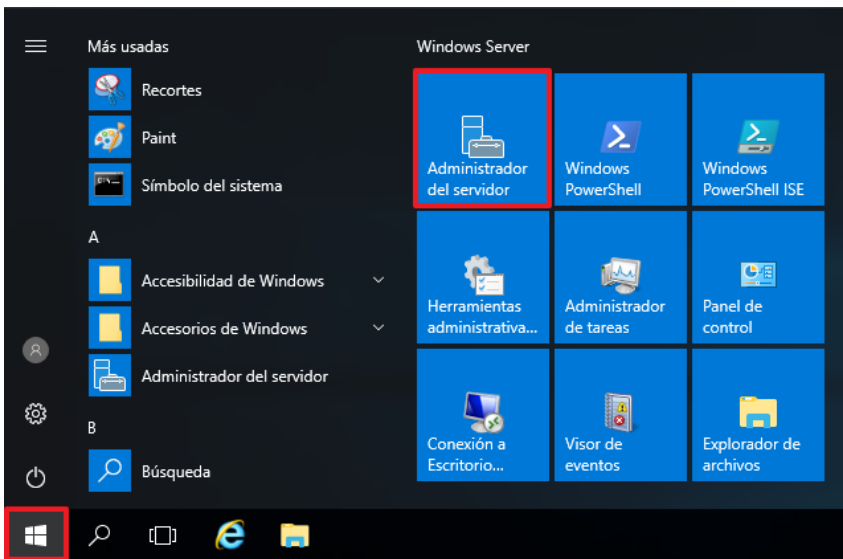
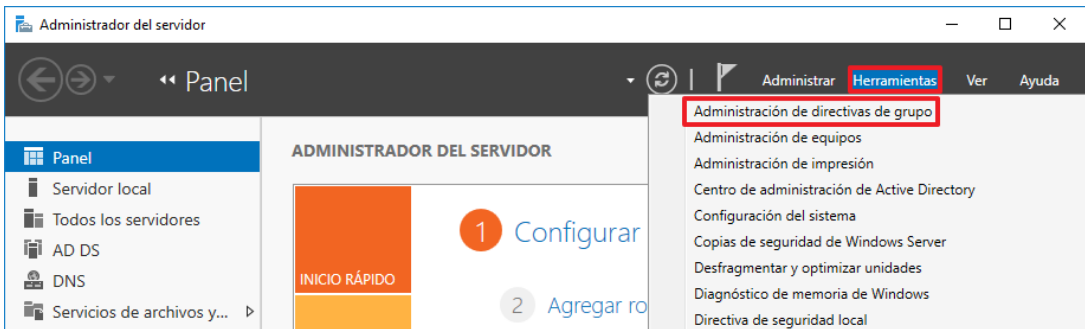
Paso	Descripción
1.	Inicie sesión en el equipo cliente Windows 10 con una cuenta con permisos de administrador del dominio.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
3.	Localice el archivo “CCN-STIC-599A19 – Deshabilitar_Opciones_Accesibilidad.bat” 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”.

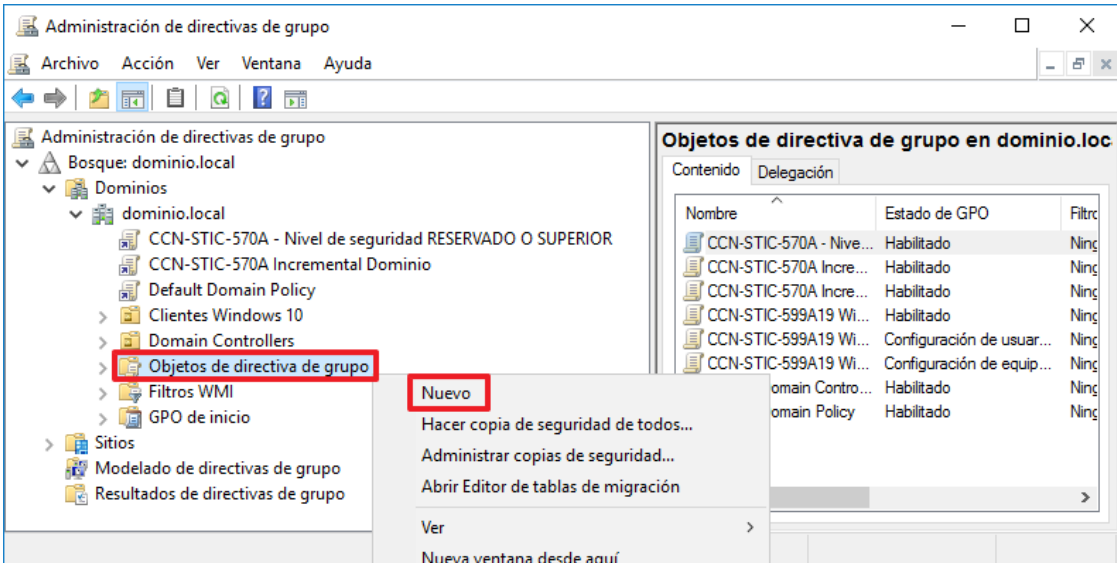
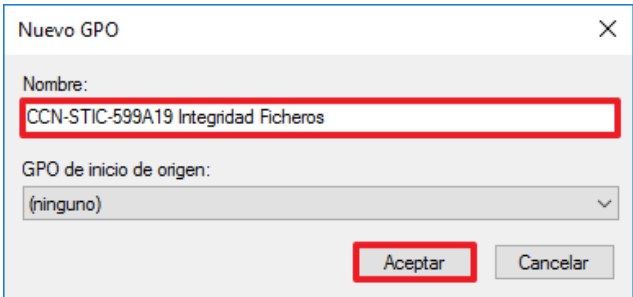
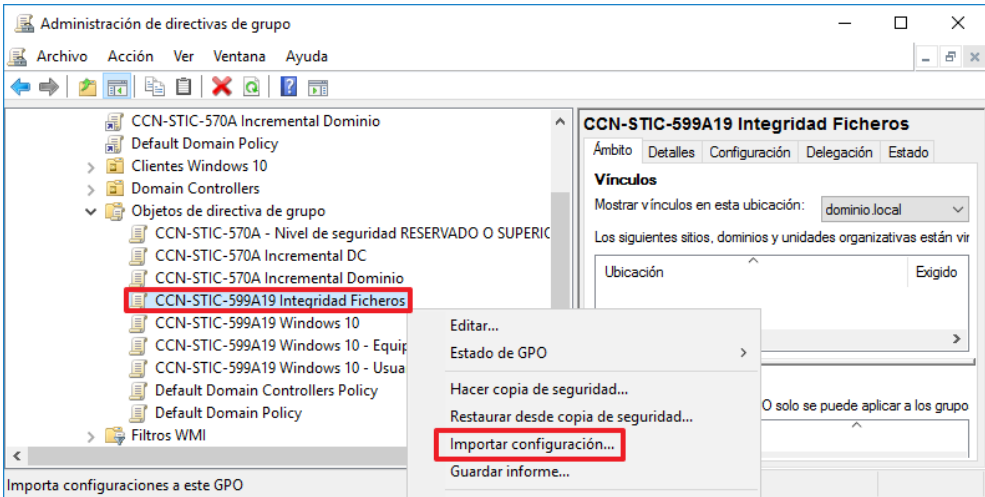


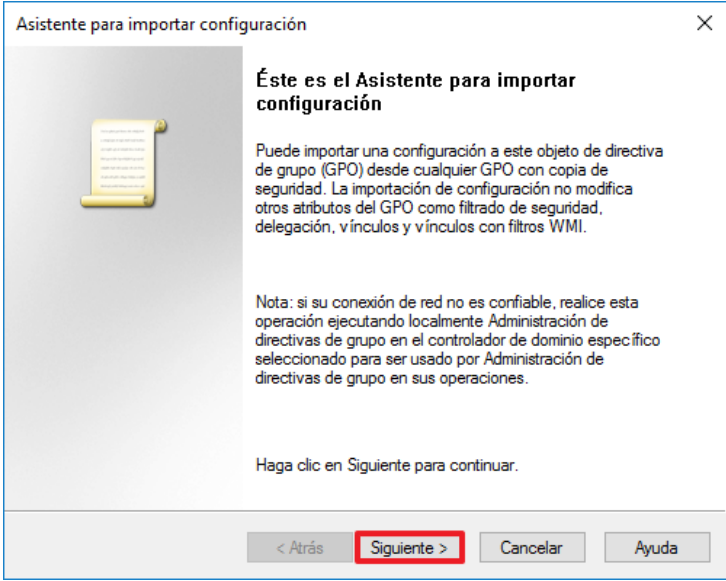
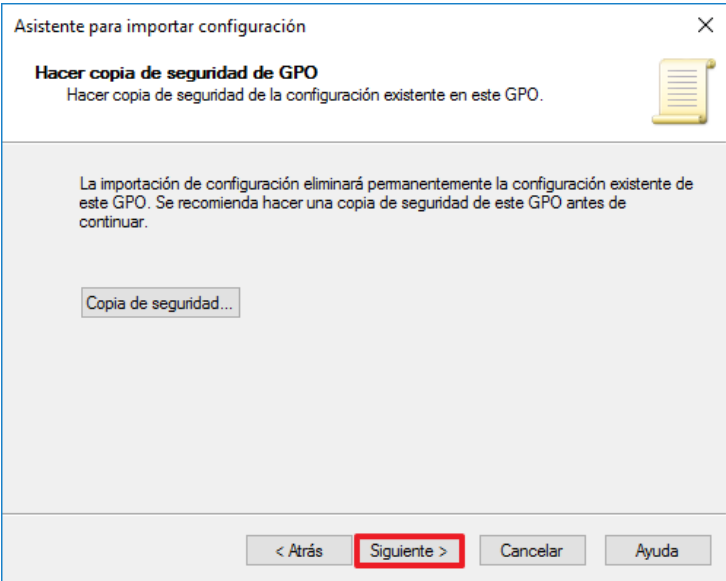
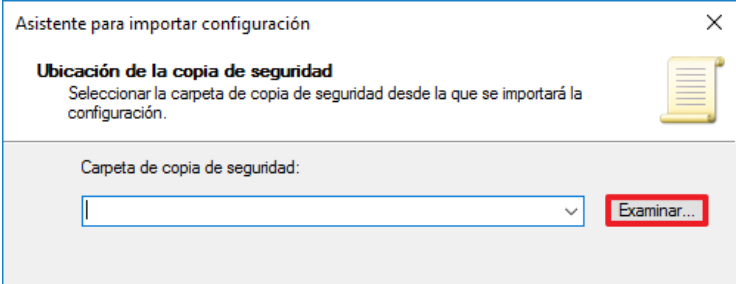
Paso	Descripción
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comando 
7.	Por último, deberá reiniciar 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”.

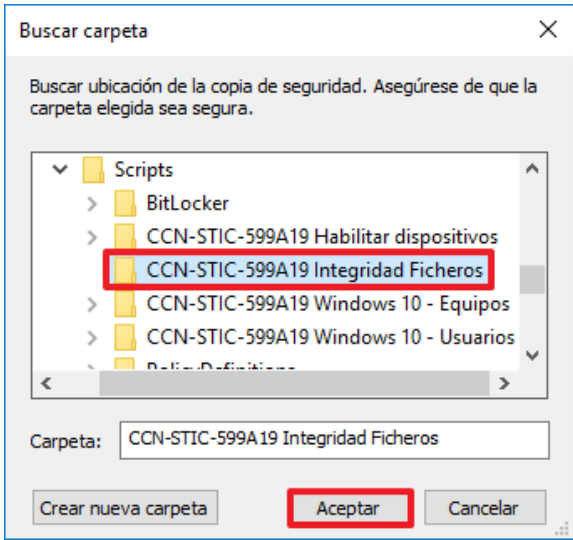
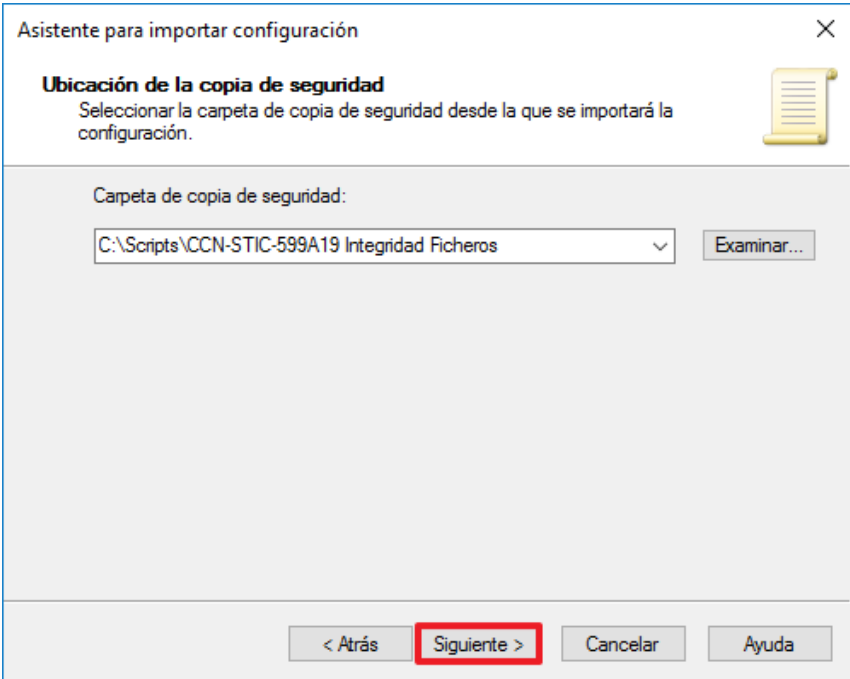
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

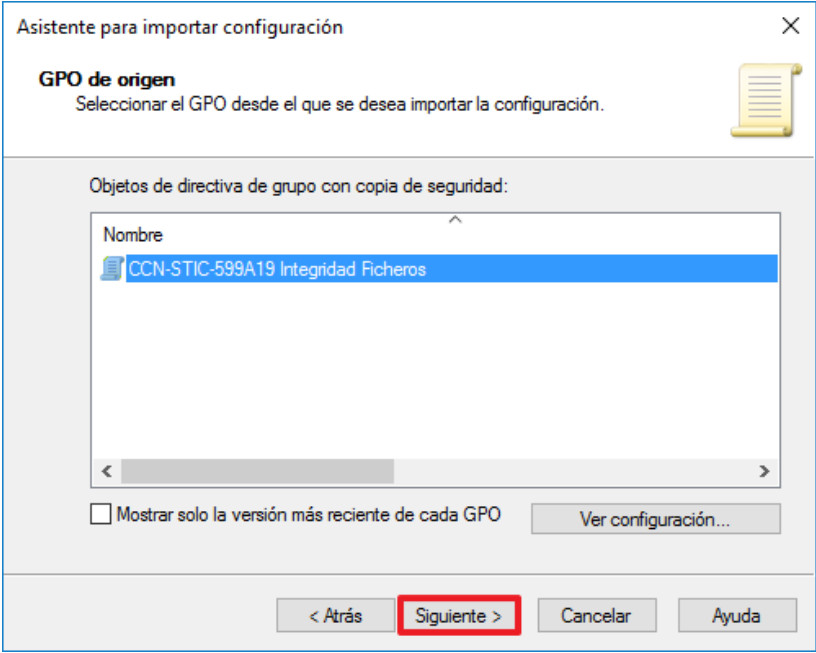
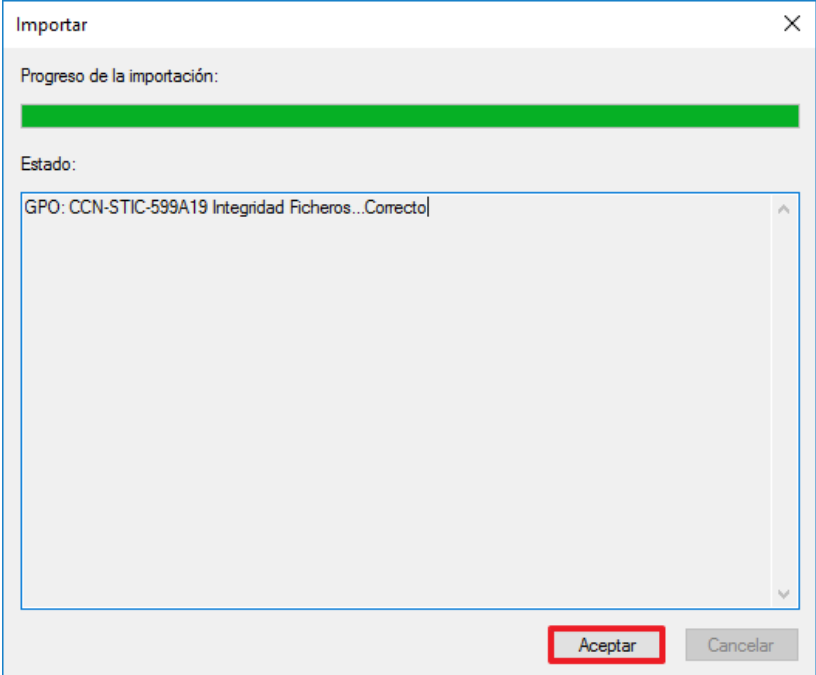
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

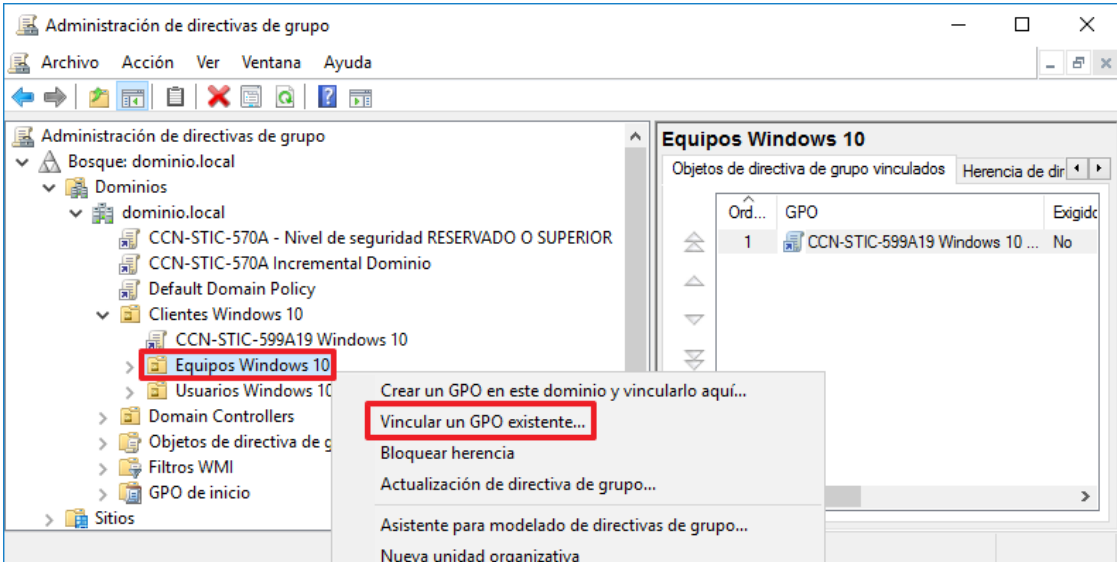
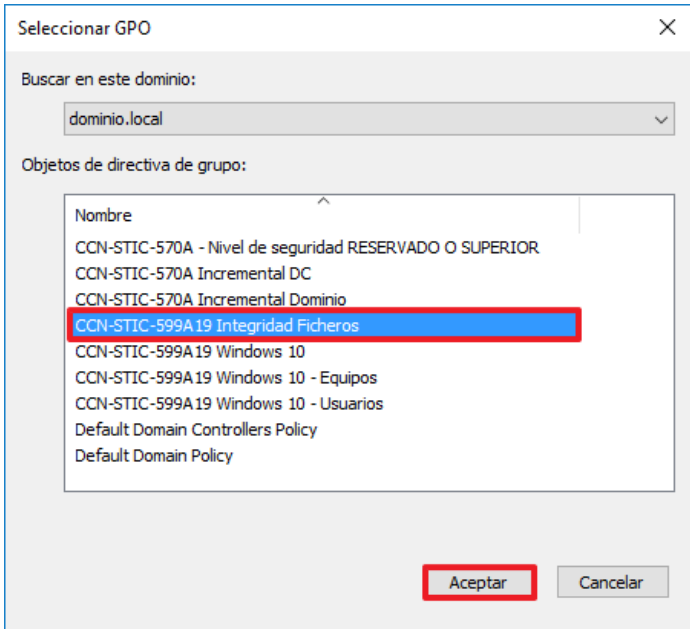
Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio al que pertenecen los equipos cliente que van a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Copie los ficheros que acompañan a esta guía en el directorio "C:\Scripts".
3.	Inicie el "Administrador del servidor" desde el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios.
4.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Administración de directivas de grupo". 
5.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"

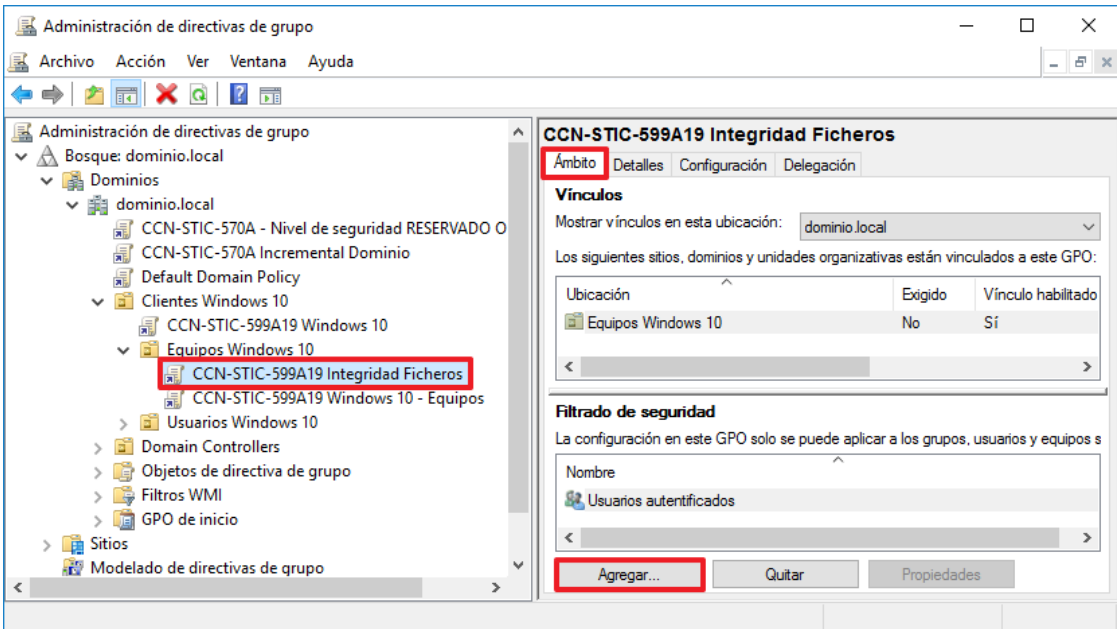
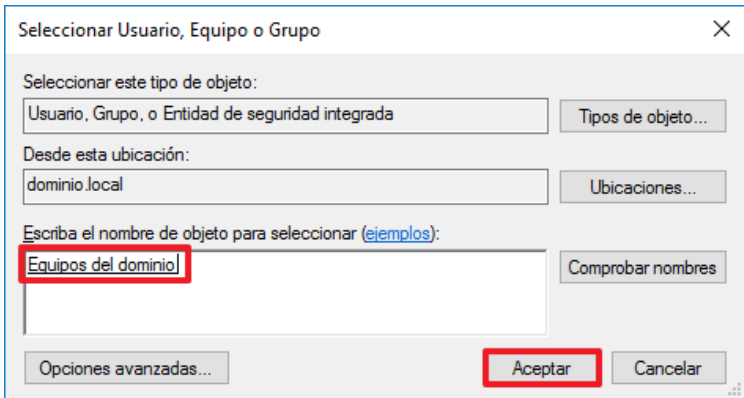
Paso	Descripción
6.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" y, marcando con el botón derecho sobre él, elija la opción "Nuevo" del menú contextual que aparecerá. 
7.	Asigne el siguiente nombre "CCN-STIC-599A19 Integridad Ficheros" a la nueva GPO y pulse "Aceptar". 
8.	Seleccione la GPO recién creada, "CCN-STIC-599A19 Integridad Ficheros" con el botón derecho y pulse sobre la opción "Importar configuración..." en el menú contextual que aparecerá. 

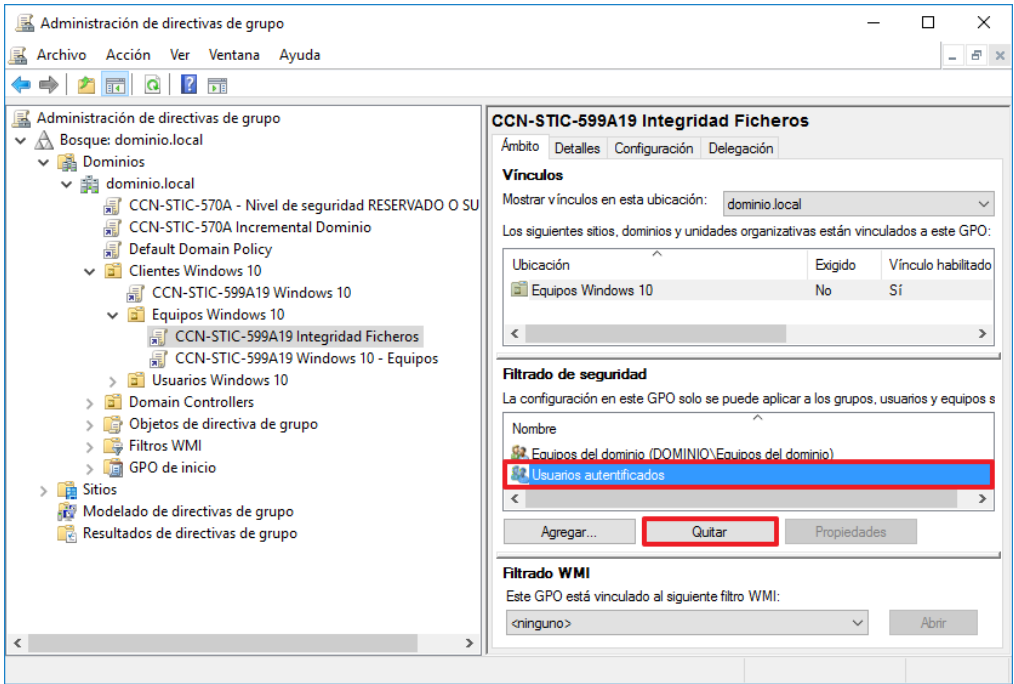
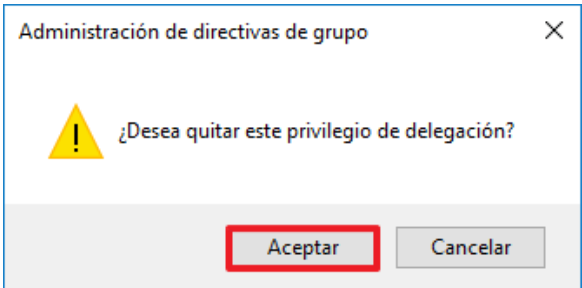
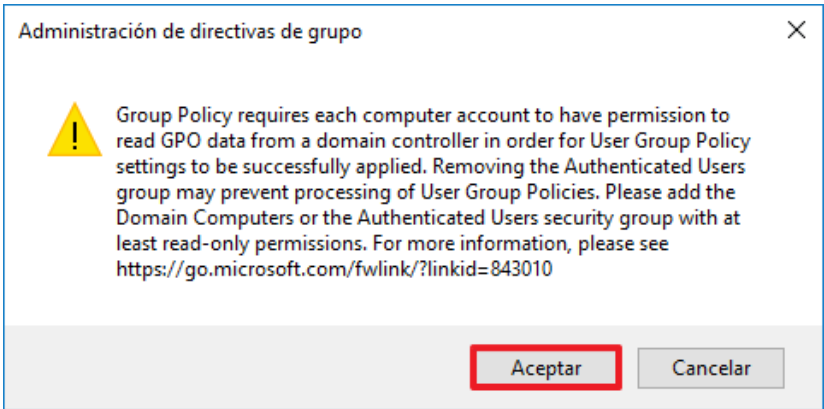
Paso	Descripción
9.	En el “Asistente para importar configuración” pulse “Siguiente >”. 
10.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana “Hacer copia de seguridad de GPO”. 
11.	En “Ubicación de la copia de seguridad” pulse sobre el botón “Examinar...”. 

Paso	Descripción
12.	Localice la carpeta “CCN-STIC-599A19 Integridad Ficheros” en el directorio “C:\Scripts” y pulse “Aceptar”. 
13.	Pulse “Siguiente >” para continuar. 

Paso	Descripción
14.	En “GPO de origen” pulse “Siguiente >”. 
15.	En “Examinar copia de seguridad” pulse “Siguiente >”.
16.	Pulse “Finalizar” para realizar la importación.
17.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 

Paso	Descripción
18.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
19.	Seleccione “CCN-STIC-599A19 Integridad Ficheros” de la lista y pulse “Aceptar”. 

Paso	Descripción
20.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” seleccione la unidad organizativa “Equipos Windows 10” y a continuación la GPO que acaba de vincular. En el panel de la derecha seleccione la pestaña “Ámbito” y en el apartado “Filtrado de seguridad” seleccione “Agregar...”. 
21.	En la ventana emergente introduzca el nombre “Equipos del dominio” y pulse en sobre “Aceptar” 

Paso	Descripción
22.	A continuación, en el apartado “Filtrado de seguridad” seleccione el grupo “Usuarios autenticados” y pulse sobre “Quitar”. 
23.	Pulse “Aceptar” ante la advertencia emergente “¿Desea quitar este privilegio de delegación?”. 
24.	Pulse “Aceptar” ante la ventana emergente. 
25.	Elimine el directorio “C:\Scripts”.

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

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 sus versiones PRO y 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, versiones contempladas 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.

El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.

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 MS WINDOWS 10” 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.

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 entornos de 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 recién 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. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 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 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.

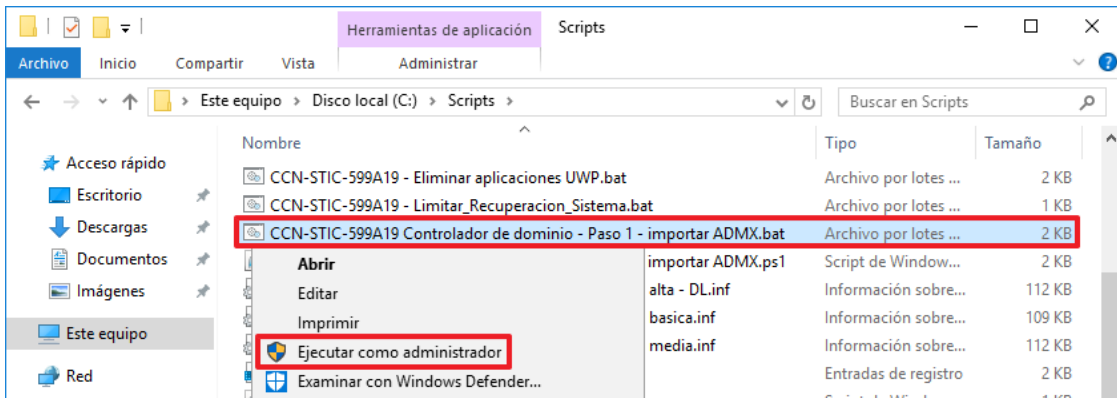
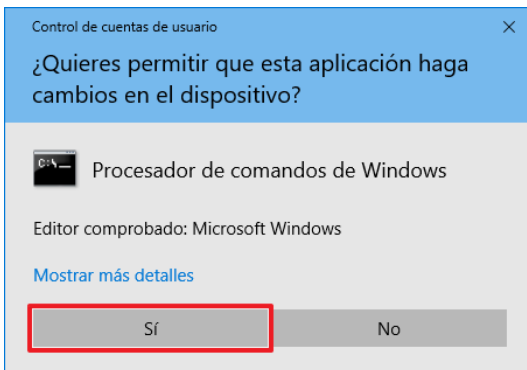
1. PREPARACIÓN DEL DOMINIO

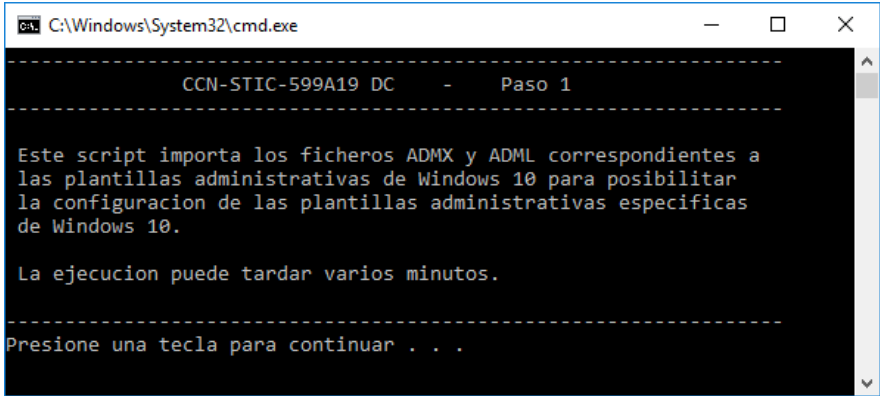
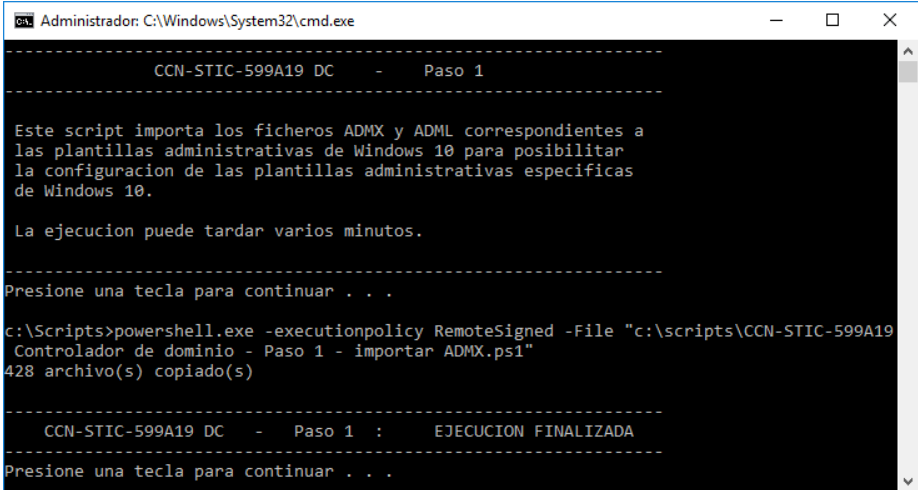
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

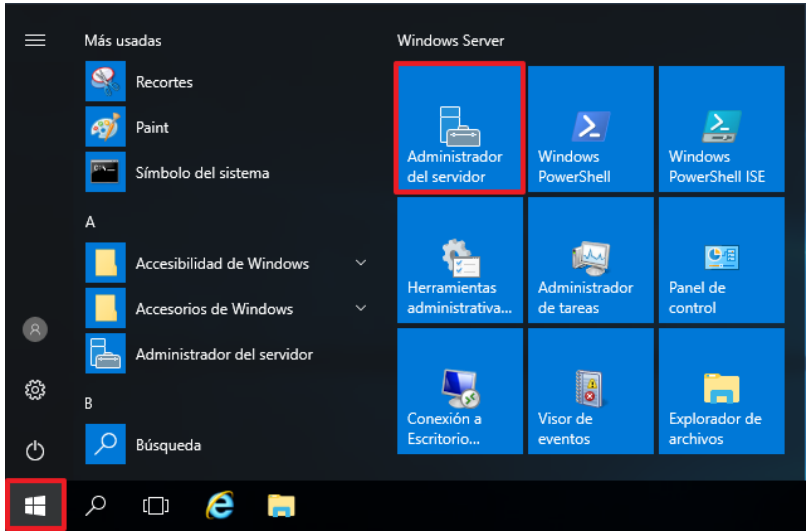
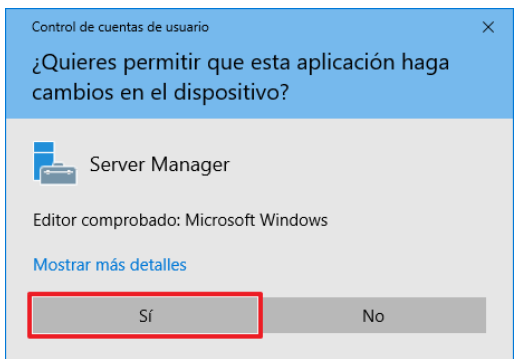
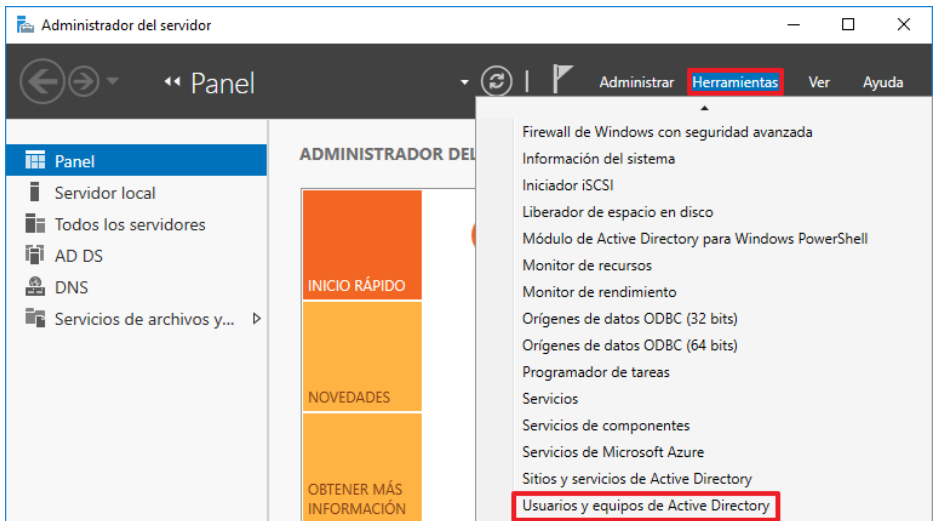
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Si no es así, aplique la guía correspondiente al controlador de dominio, antes de continuar con la aplicación de ésta.

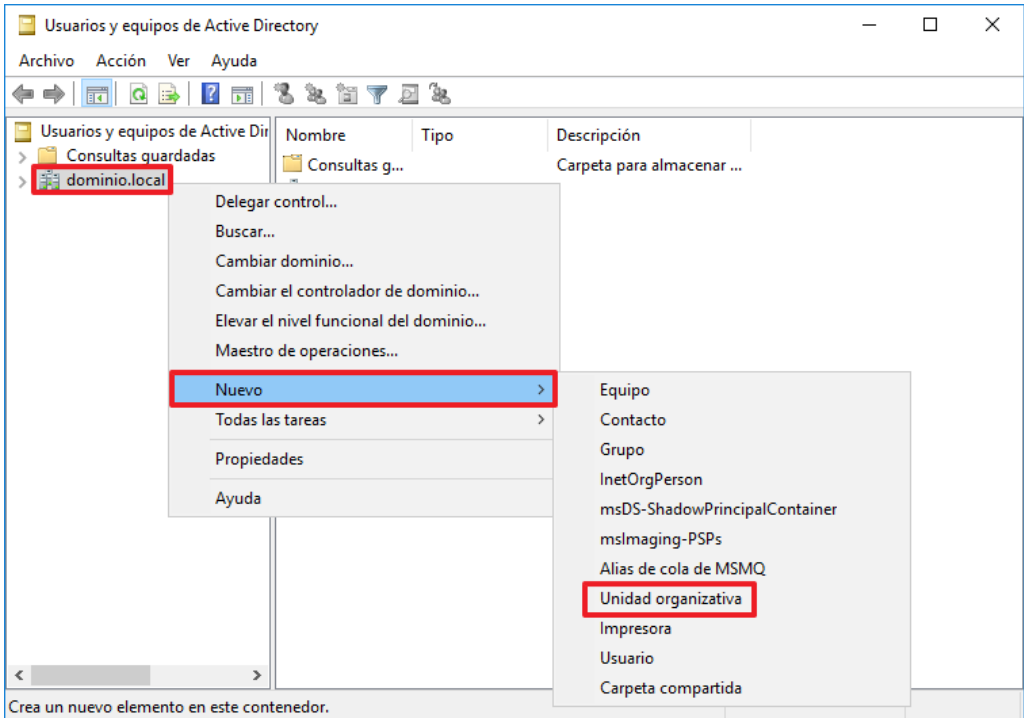
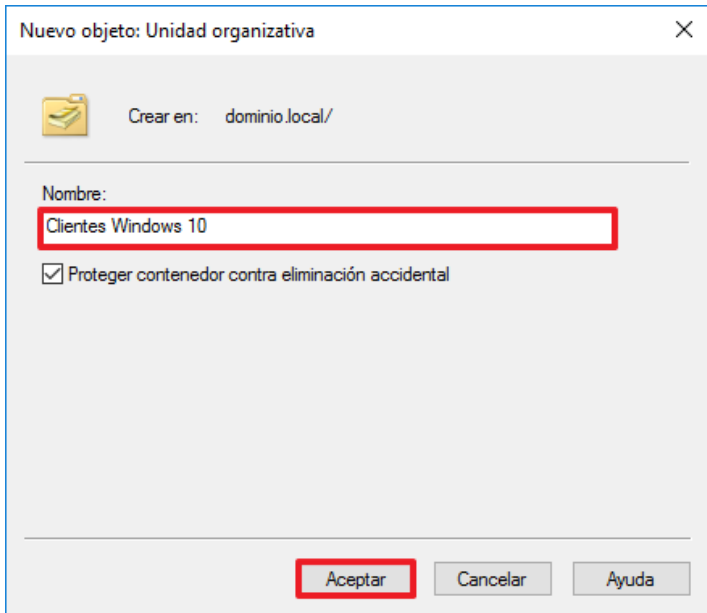
En el ejemplo, las configuraciones y capturas de pantalla han sido realizadas sobre un controlador de dominio al que se le ha instalado Windows Server 2016 y aplicado la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016.

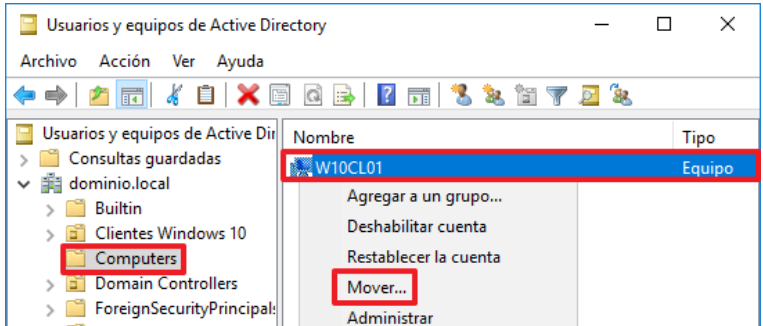
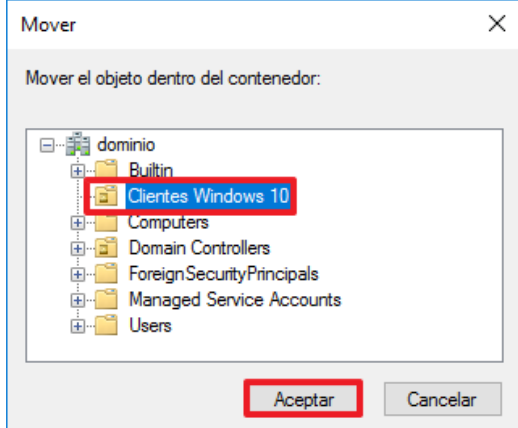
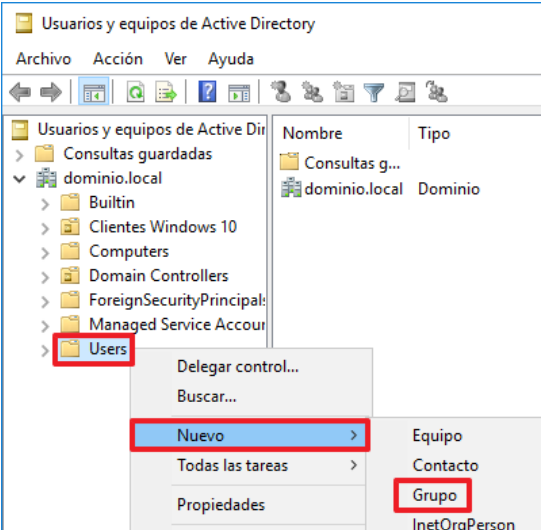
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio.
Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".	

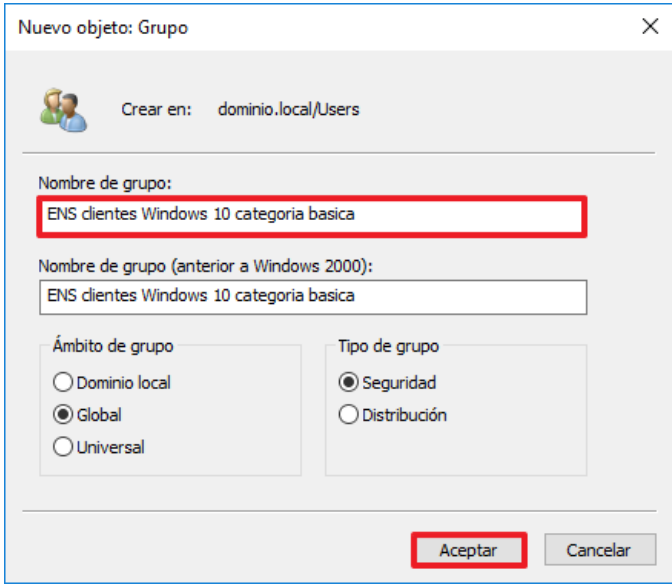
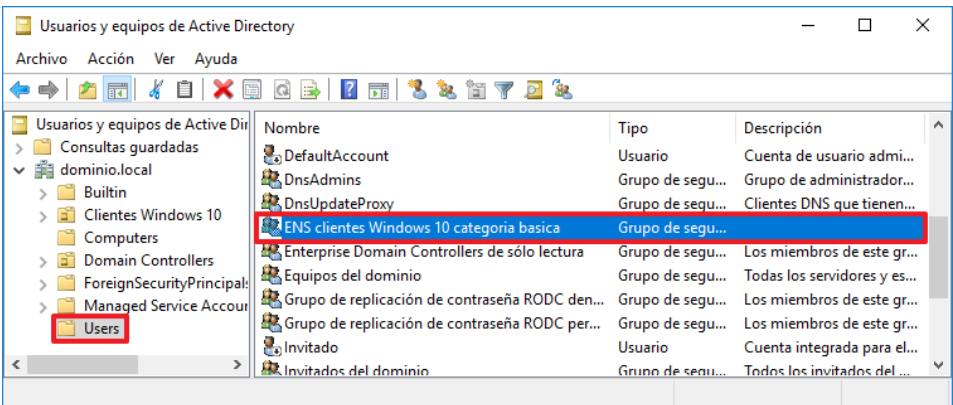
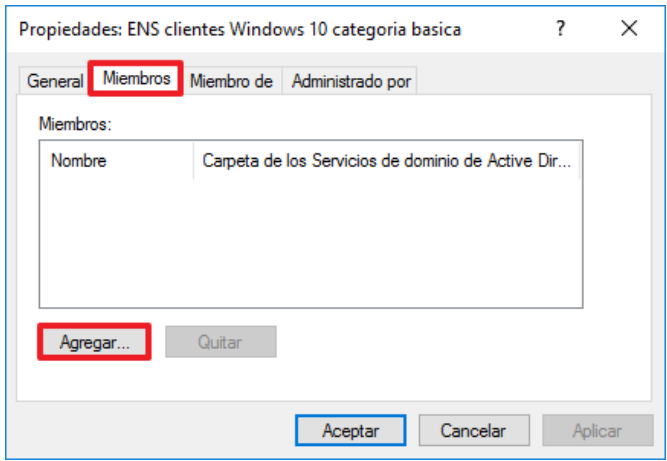
Paso	Descripción
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-599A19 ENS clientes categoria alta - DL (directorio) – CCN-STIC-599A19 ENS clientes categoria media (directorio) – CCN-STIC-599A19 ENS clientes categoria basica (directorio) – CCN-STIC-599A19 ENS Incremental portátiles categoria alta - DL - Bitlocker (directorio) – CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL.inf – CCN-STIC-599A19 ENS Incremental clientes categoria media.inf – CCN-STIC-599A19 ENS Incremental clientes categoria basica.inf – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1 – PolicyDefinitions - (directorio)
6.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
7.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar. 

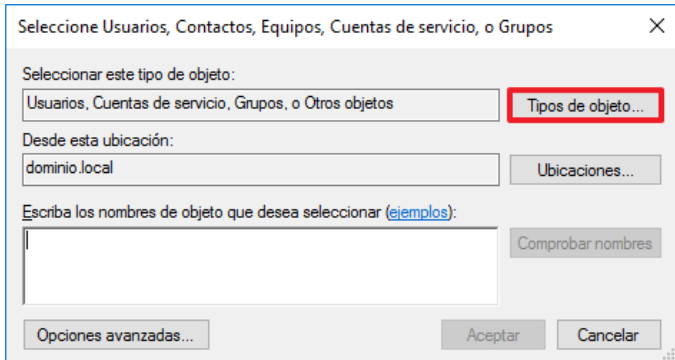
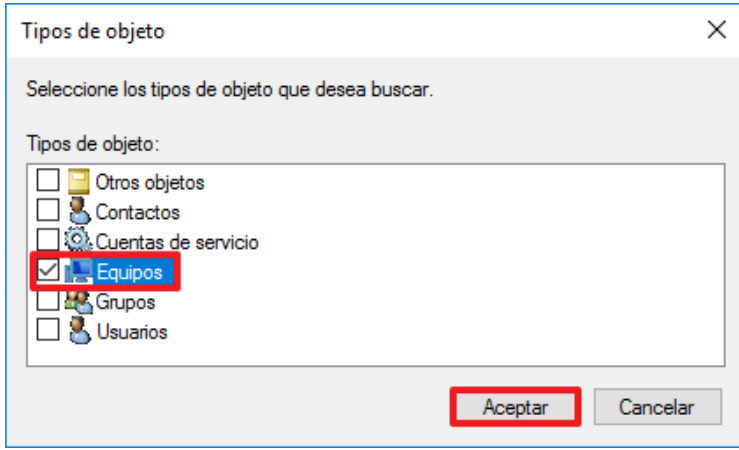
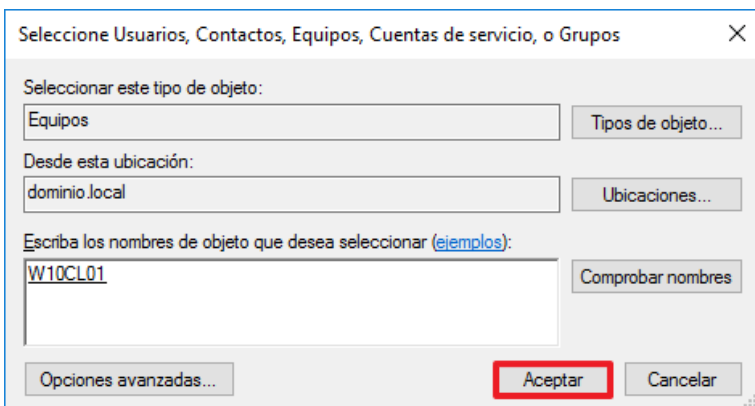
Paso	Descripción
8.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
9.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 
10.	Copie el fichero “CCN-STIC-599A19 ENS incremental clientes categoria basica.inf”, almacenado en la carpeta “C:\Scripts”, al directorio “C:\Windows\Security\Templates” del Controlador de Dominio. Nota: Los siguientes pasos describen el procedimiento para crear un grupo de seguridad donde agregar los puestos de trabajo que le sean de aplicación la categoría básica de seguridad según los criterios definidos del ENS. En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá también crear el grupo debido a que la política deberá aplicarse a nivel de dominio y se asignará exclusivamente a los puestos de trabajo por la pertenencia a este grupo. Si todos los equipos de la organización presentan la misma categoría básica no hace falta la creación de dicho grupo y puede saltar al paso 27. Si por el contrario van a existir puestos de trabajo Windows 10 con categorías media o alta, deberá crear dicho grupo de tal forma que la aplicación de políticas de seguridad en función de los categorías se aplique atendiendo a los criterios de pertenencia a grupo.

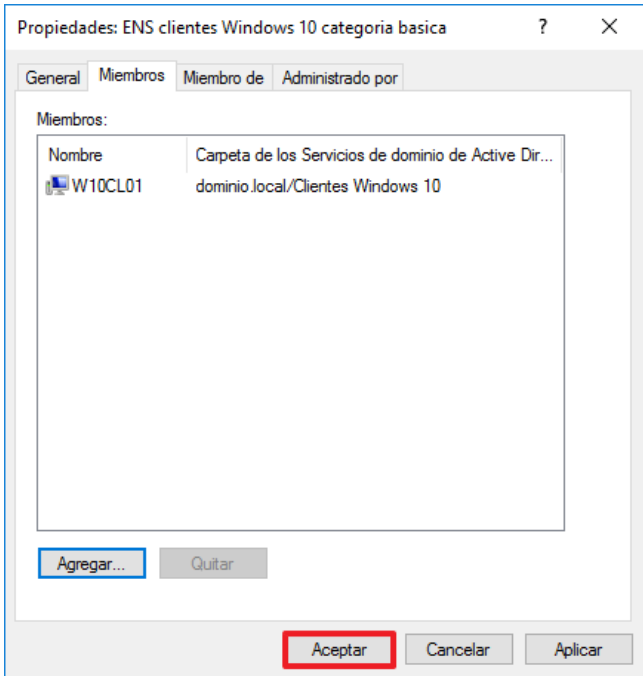
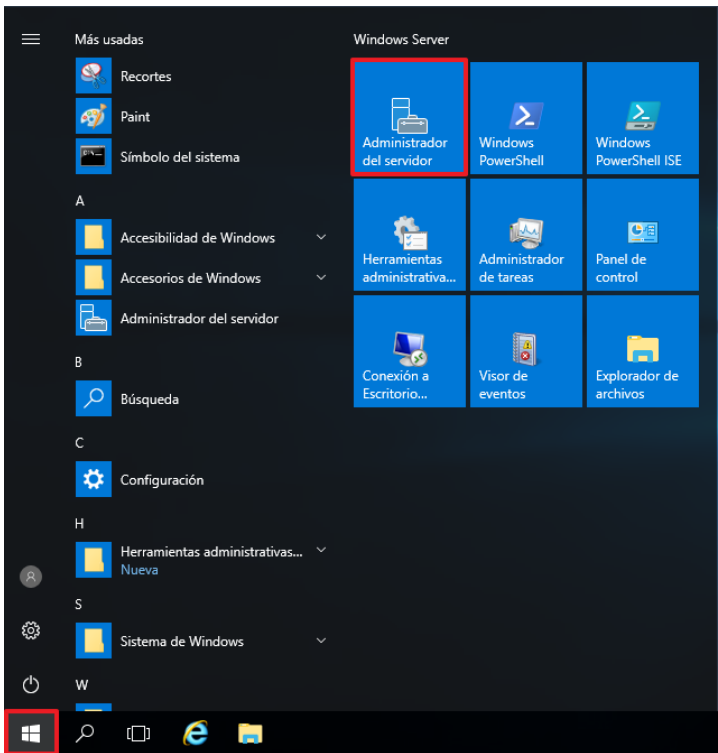
Paso	Descripción
11.	Inicie la herramienta de “Usuarios y equipos de Active Directory”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
12.	Pulse sobre el botón “Sí” para confirmar la operación. 
13.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 

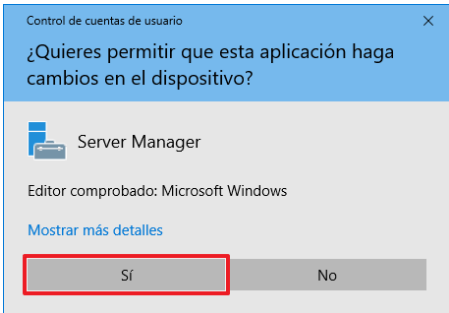
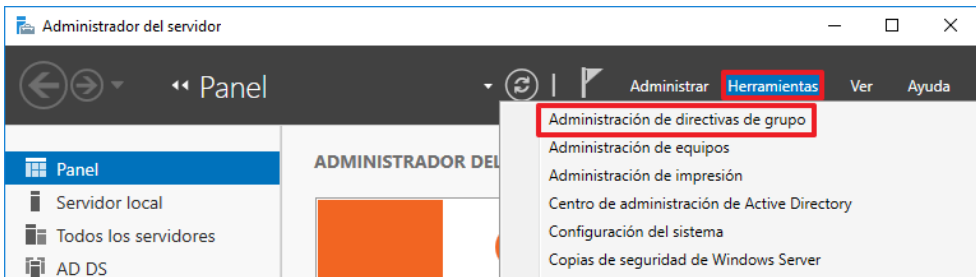
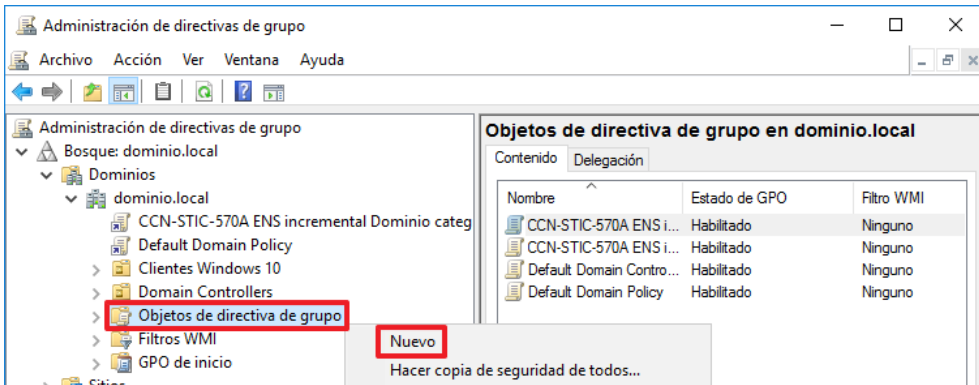
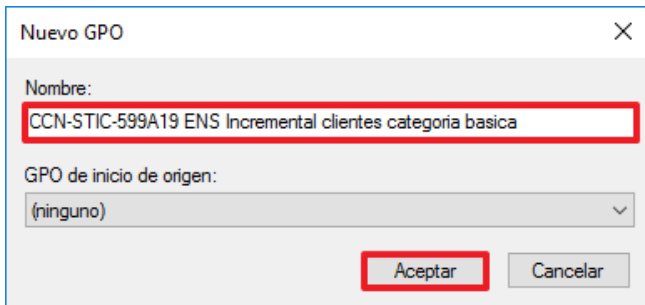
Paso	Descripción
14.	Pulse con el botón derecho sobre el dominio y seleccione “Nuevo → Unidad organizativa”. 
15.	Establezca el nombre para la unidad organizativa con los clientes Windows 10 y pulse “Aceptar”. 

Paso	Descripción
16.	Vaya a las unidades organizativas donde se encuentren los clientes que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover...” en cada uno de ellos.  Nota: En este ejemplo se encuentra bajo la unidad organizativa “Computers”.
17.	Seleccione la unidad organizativa “Clientes Windows 10” creada anteriormente y pulse “Aceptar”. 
18.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

Paso	Descripción
19.	Introduzca como nombre “ENS clientes Windows 10 categoria basica”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio. 
20.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
21.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar...”. 

Paso	Descripción
22.	Pulse el botón de “Tipos de objeto...”. 
23.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
24.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad básica y pulse “Aceptar” para agregar la selección.  Nota: No agregue servidores a este grupo.

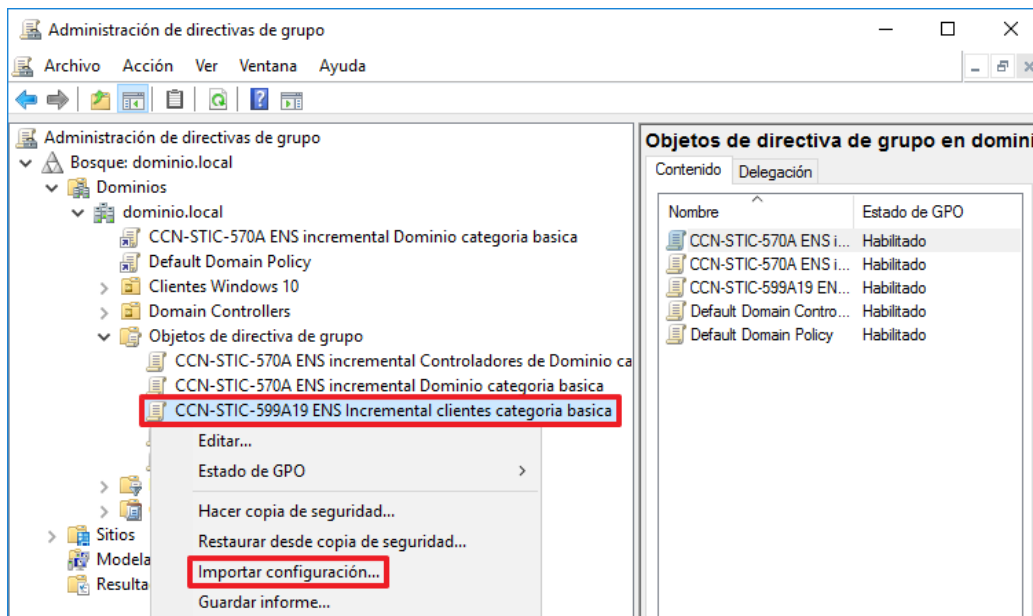
Paso	Descripción
25.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
26.	Cierre la herramienta “Usuarios y equipos e Directorio Activo”.
27.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

Paso	Descripción
28.	Pulse sobre el botón “Sí” para confirmar la operación. 
29.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
30.	Despliegue los contenedores pertenecientes a su dominio y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
31.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón “Aceptar”. 

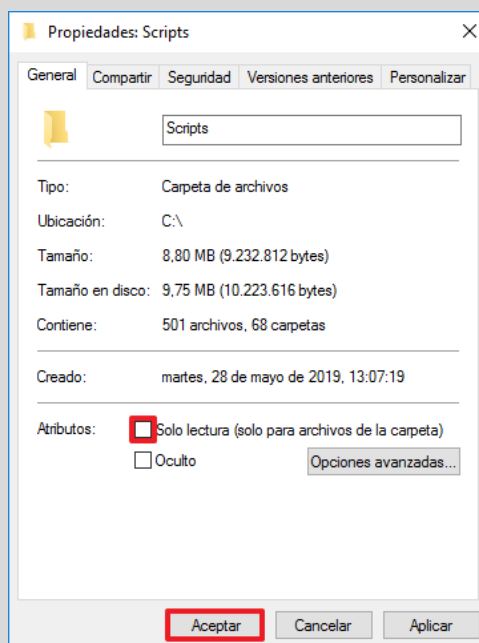
Paso

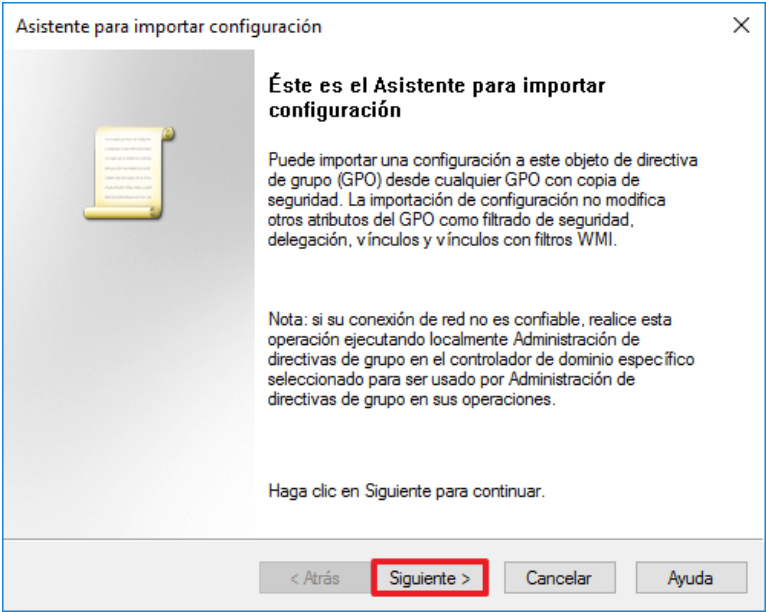
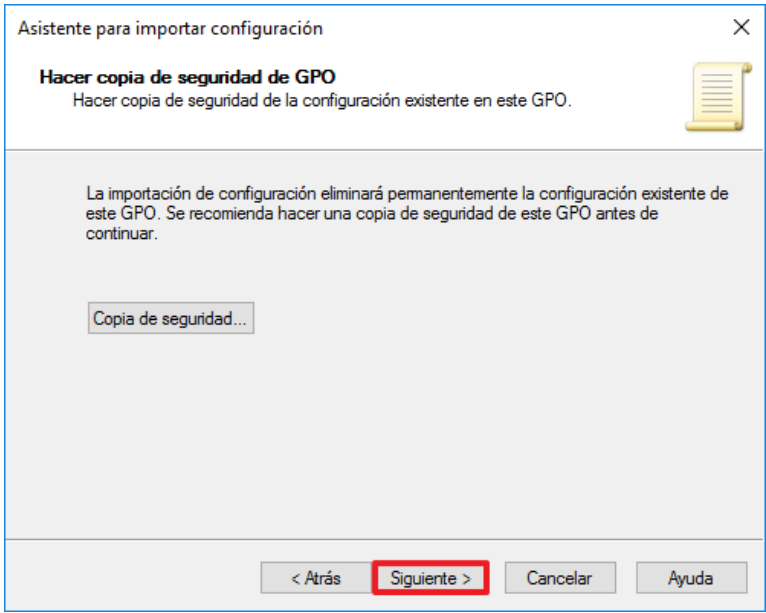
Descripción

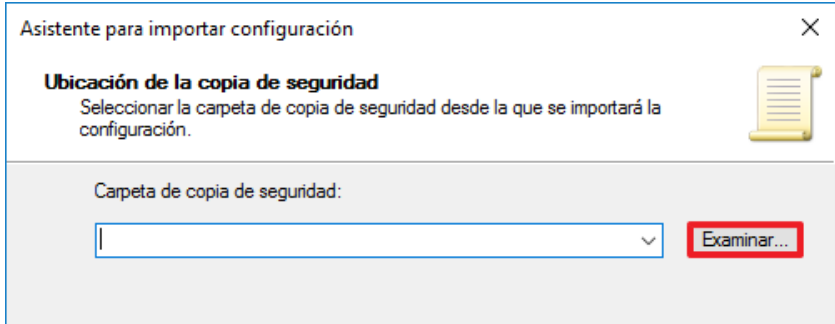
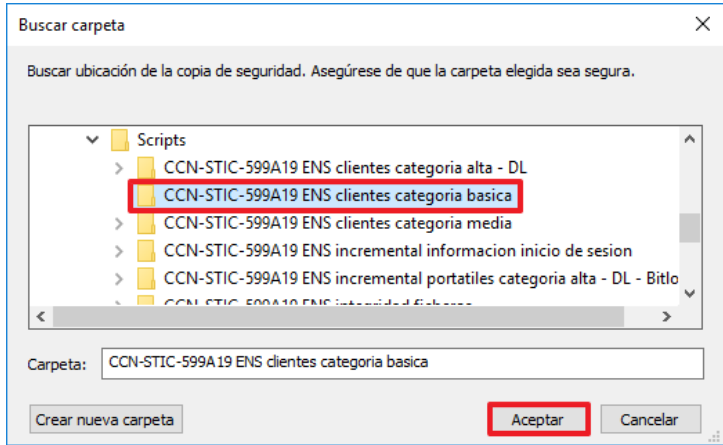
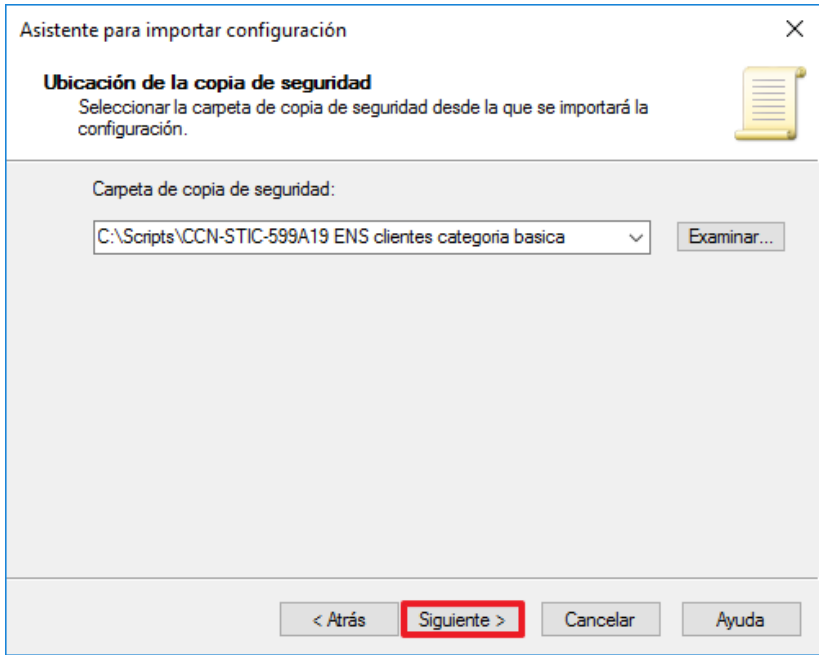
32. La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política con el botón derecho del ratón y seleccione la opción “Importar configuración...”.

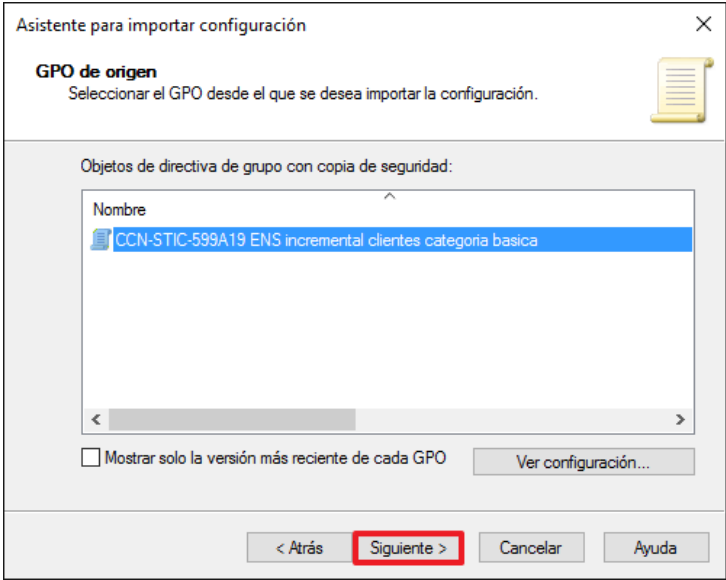
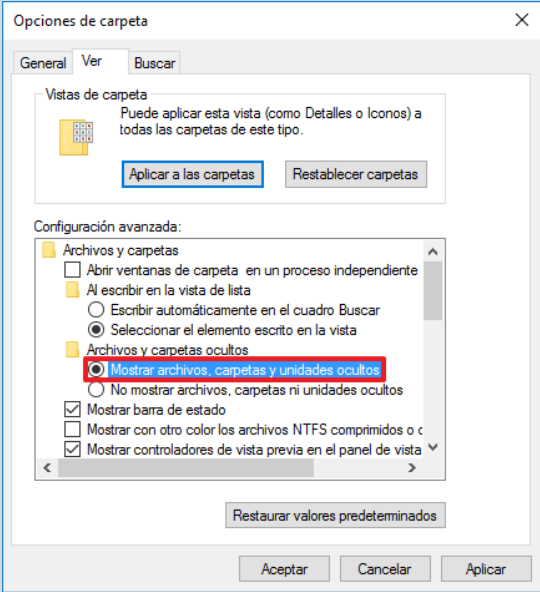


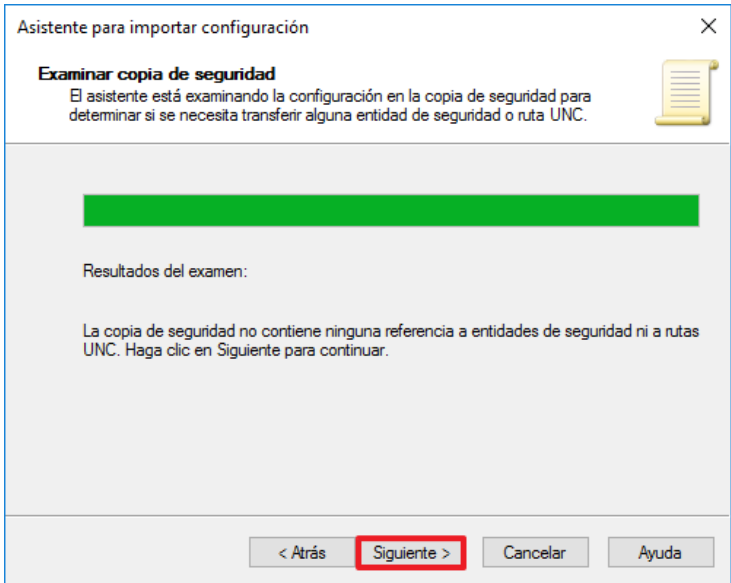
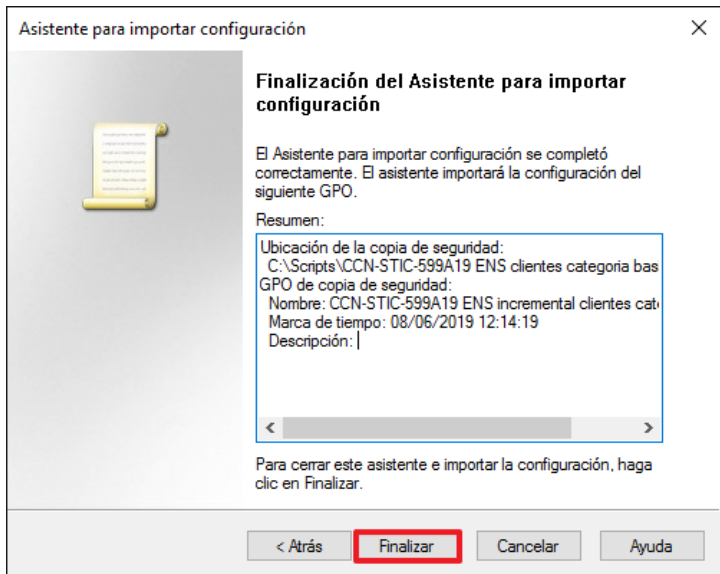
Nota: Asegúrese de que los archivos alojados en “C:\Scripts”, así como los archivos dentro de sus subcarpetas, no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro.

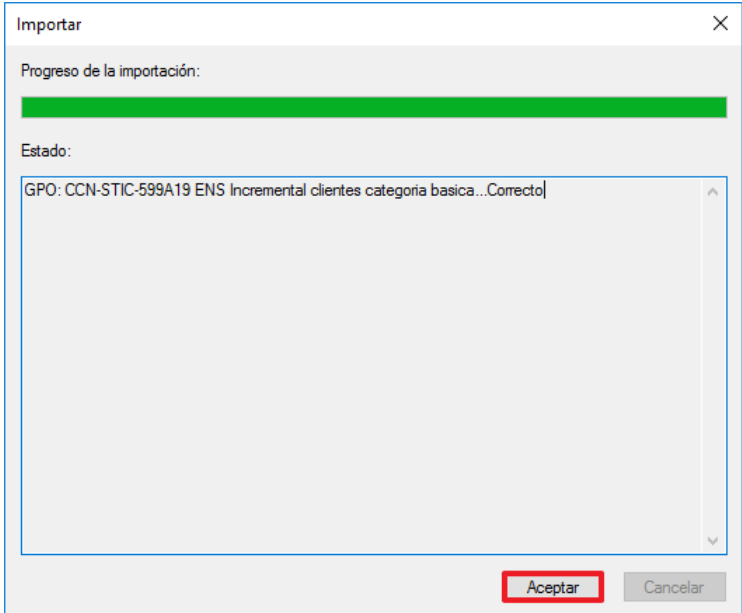
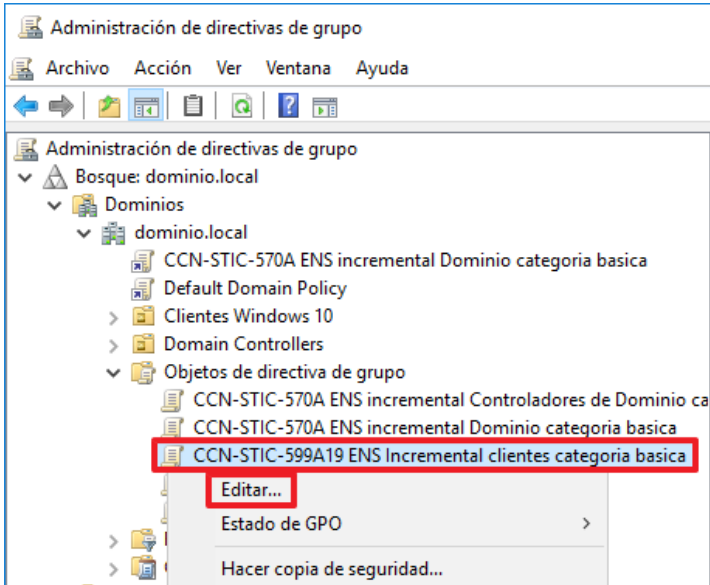


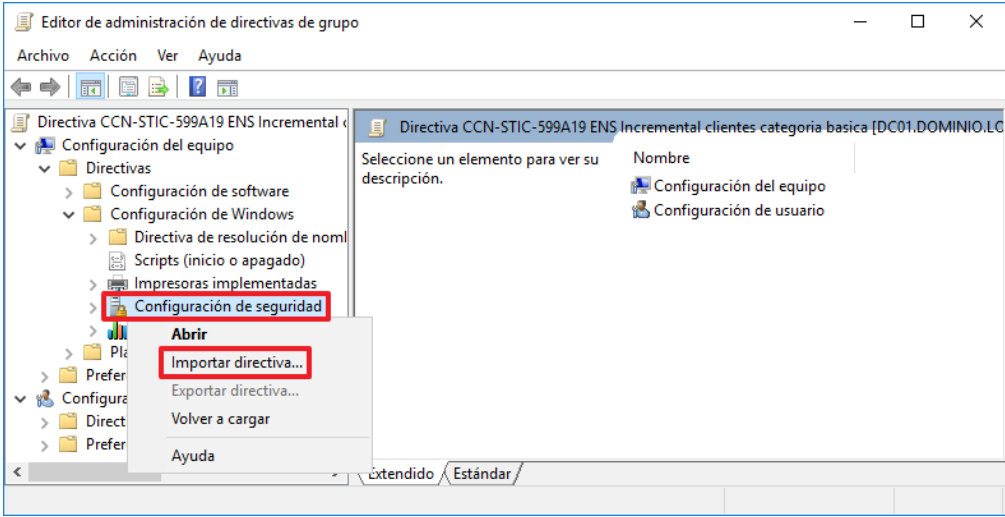
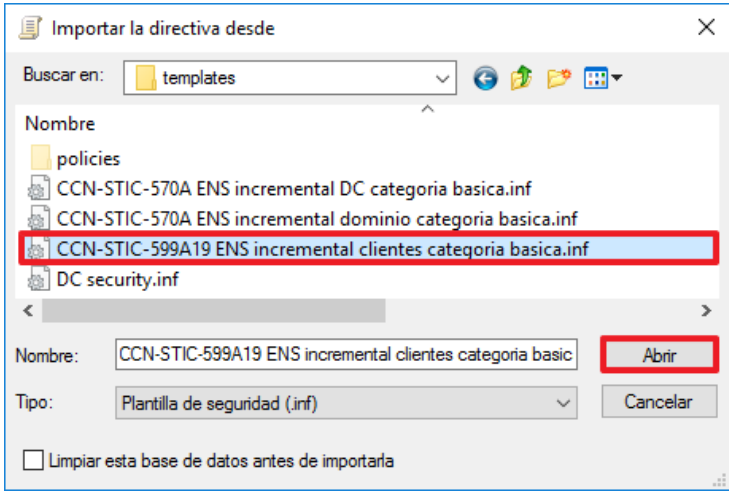
Paso	Descripción
33.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
34.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

Paso	Descripción
35.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
36.	Seleccione la carpeta “CCN-STIC-599A19 ENS clientes categoria basica” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
37.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

Paso	Descripción
38.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón “Siguiente >”. 
	Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
39.	En la pantalla de examen, pulse el botón “Siguiente >”. 
40.	Para completar el asistente pulse el botón “Finalizar”. 

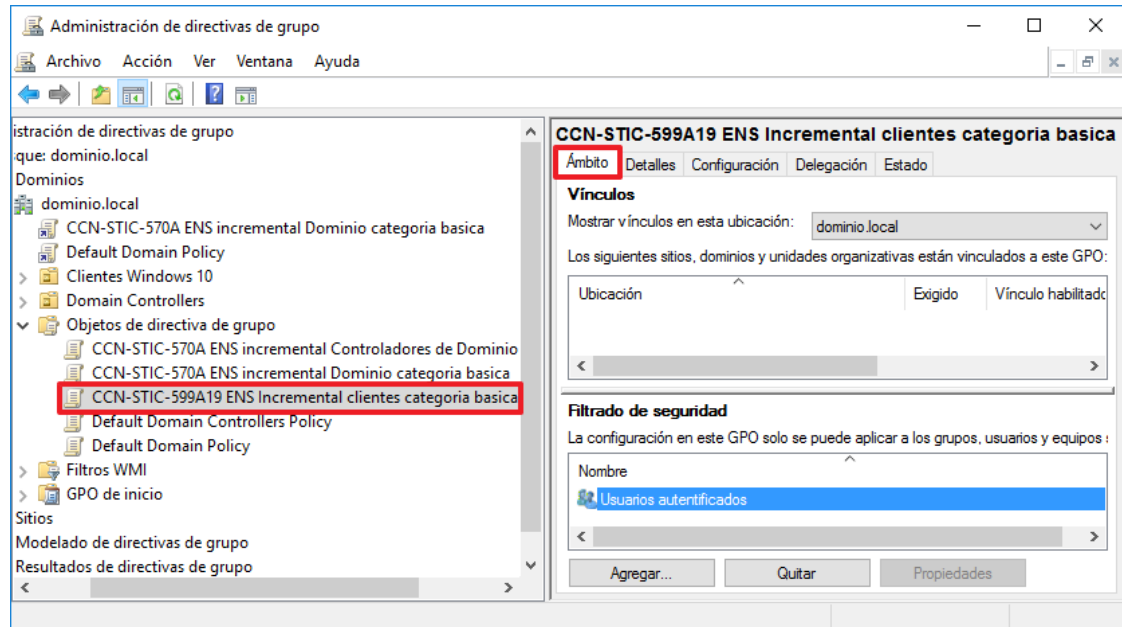
Paso	Descripción
41.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración. 
42.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
43.	Una vez pulsada la opción “Editar...” se abre una ventana de “Editor de administración de directivas de grupo”. Despliegue el objeto de directiva de grupo y sitúe el cursor sobre el nodo Configuración de seguridad. “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”

Paso	Descripción
44.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva...”. 
45.	Seleccione el fichero “CCN-STIC-599A19 ENS incremental clientes categoria basica.inf” ubicado en la ruta “C:\Windows\Security\Templates”. Pulse el botón “Abrir”. 
46.	Cierre la política una vez se haya realizado la importación de la configuración de seguridad. Nota: Los siguientes pasos describen el procedimiento para asignar la política al grupo de seguridad creado en los pasos 11 a 26. Si usted creó el grupo, puesto que va a tener aplicadas diferentes categorías de seguridad en la organización para los puestos de trabajo, siga con el siguiente paso. Si no creó dicho grupo, diríjase al paso 52.

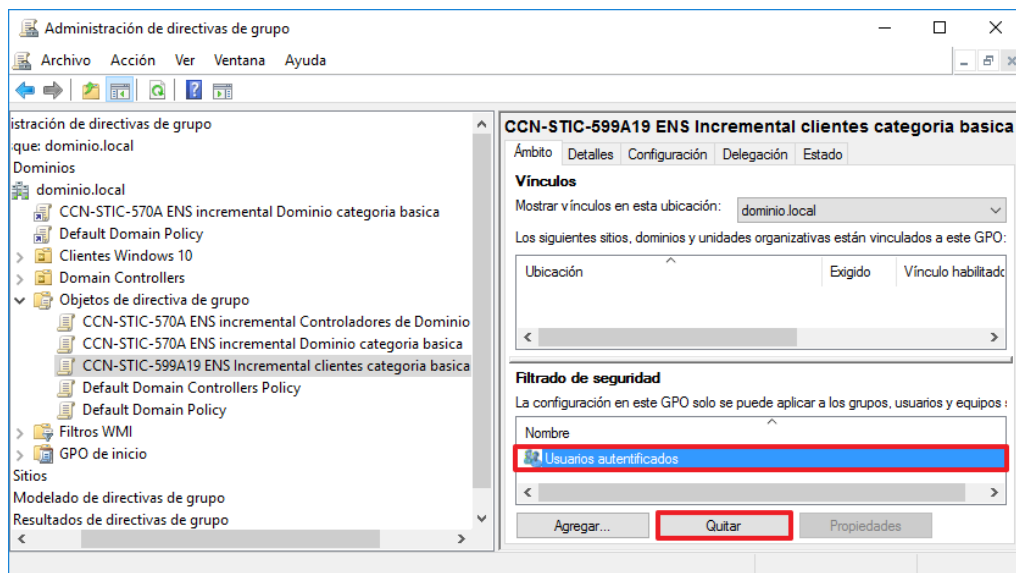
Paso

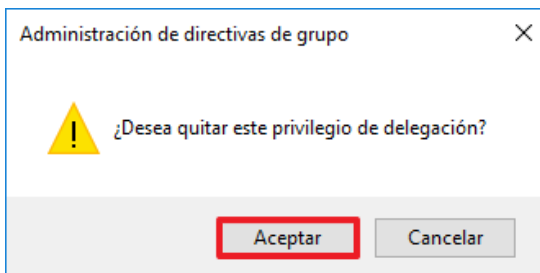
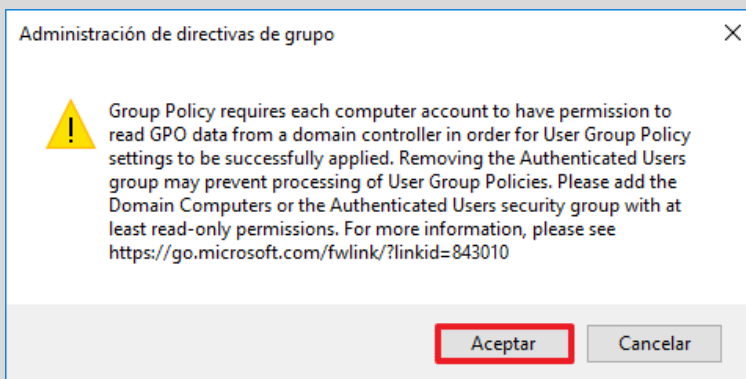
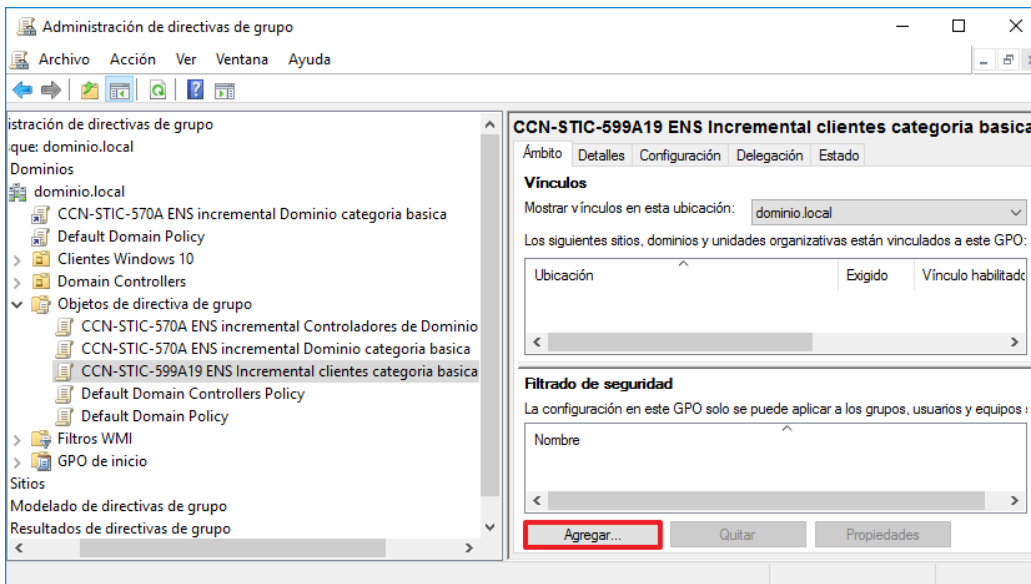
Descripción

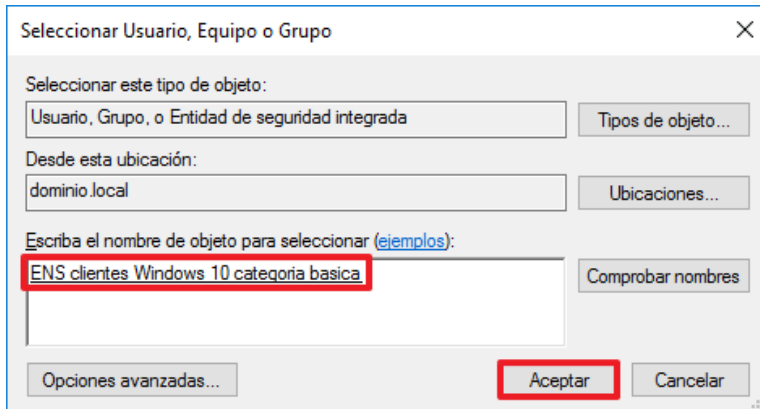
47. Vuelva a la herramienta “Administración de directivas de grupo” y seleccione la nueva GPO configurada. Vaya a las opciones de ámbito que se encuentran en el panel derecho.



48. En el apartado “Filtrado de seguridad”, seleccione “Usuarios autenticados” y pulse el botón “Quitar”.



Paso	Descripción
49.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 
50.	Pulse ahora sobre el botón “Agregar...”. 

Paso	Descripción
51.	Introduzca como nombre “ENS clientes Windows 10 categoría básica”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
52.	La política se encuentra ya creada correctamente. No obstante, no se aplicará hasta más adelante, una vez haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente Anexo.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA BÁSICA

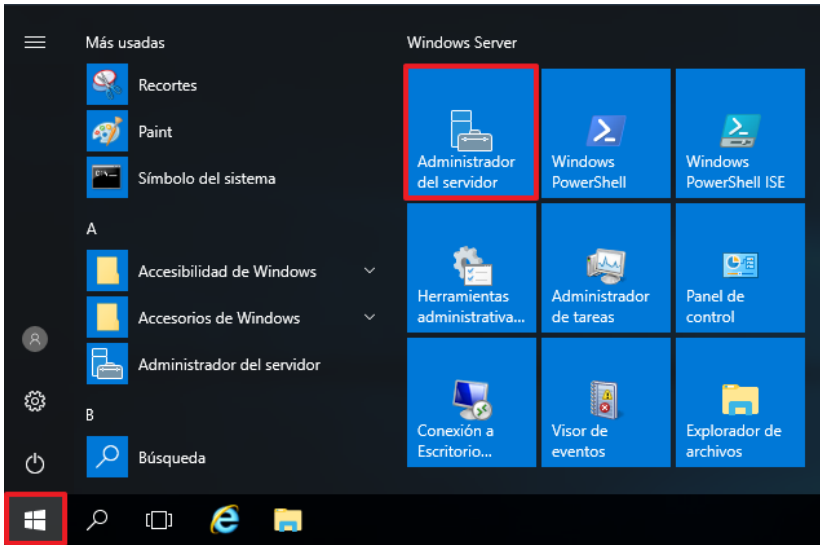
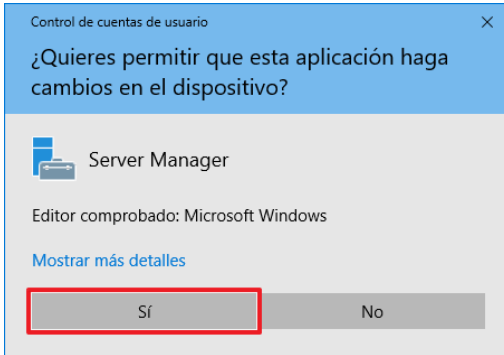
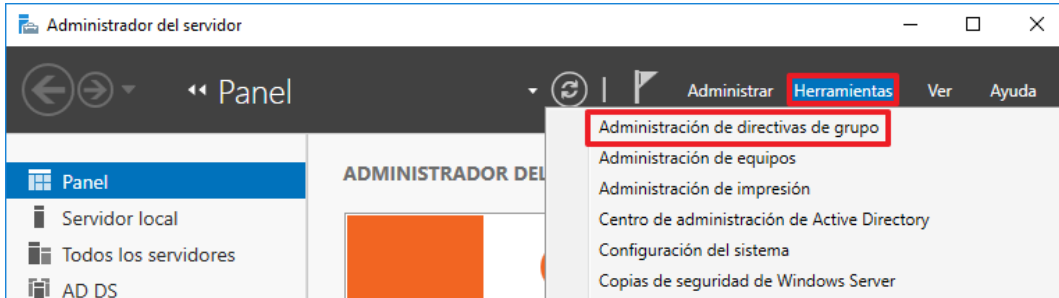
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y por lo tanto deben valorarse con respecto a la aplicación de la presente configuración. La plantilla de seguridad que se ha configurado tiene en consideración los puntos tratados en el Esquema Nacional de seguridad para la categoría básica. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina, como por ejemplo lo relativo al uso de privilegios.

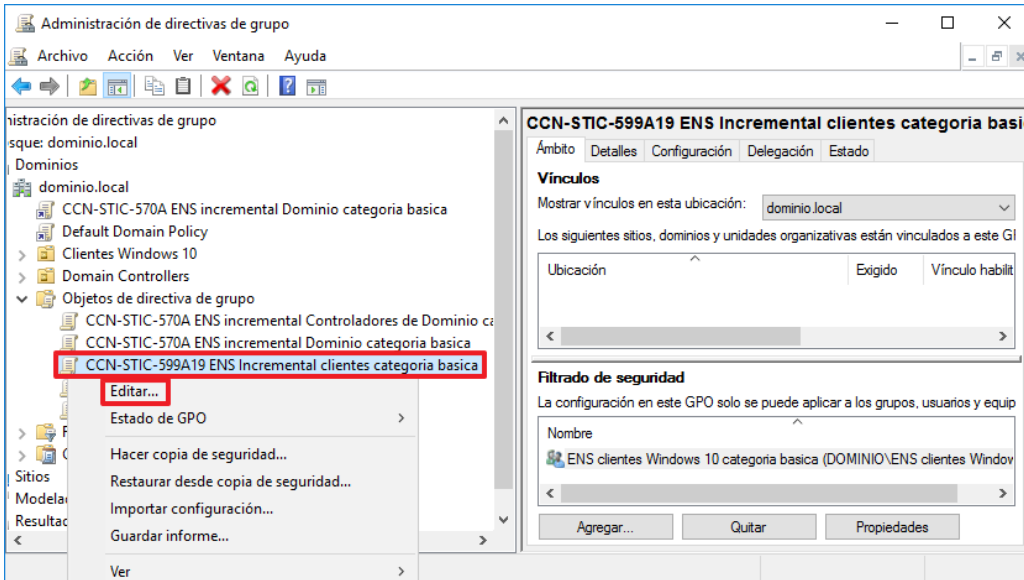
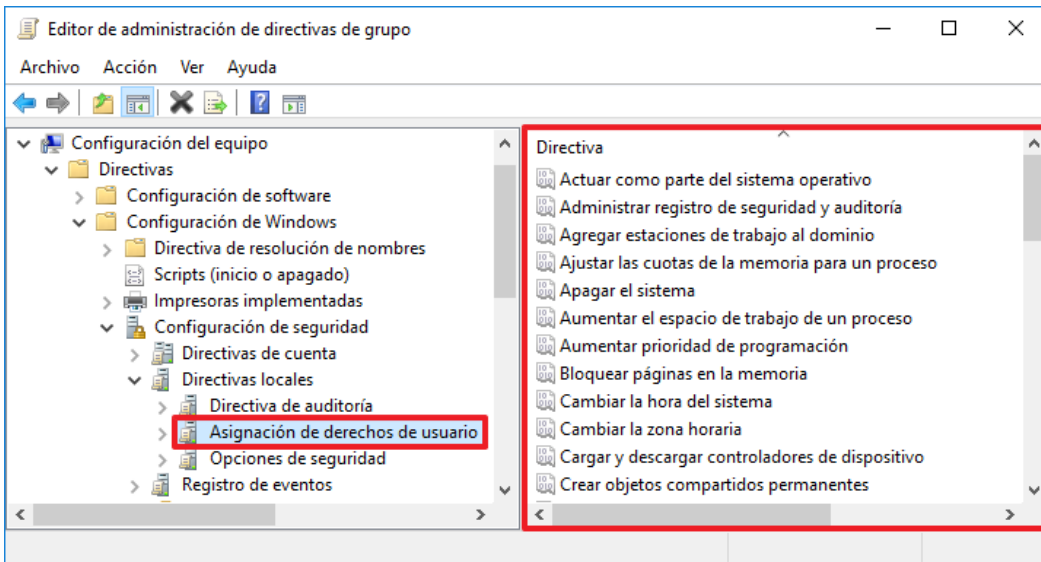
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

Los objetos de políticas de grupo para puestos de trabajo especifican unos derechos de usuario siguiendo planteamientos de seguridad y siguiendo los principios de mínimos privilegios 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 el objeto de política creado en el punto previo.

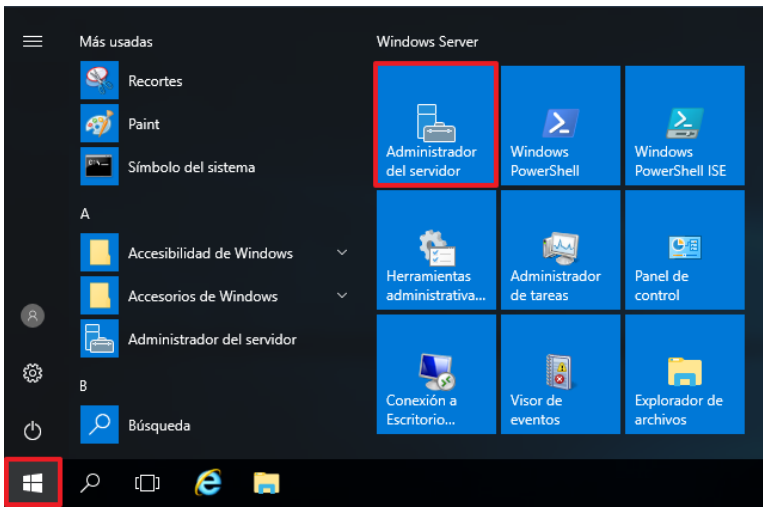
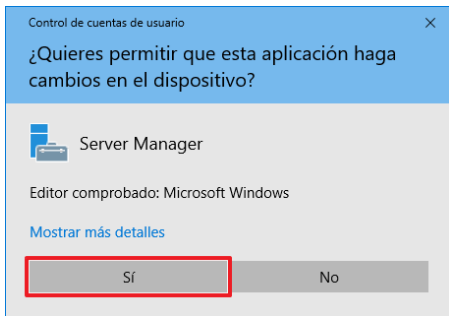
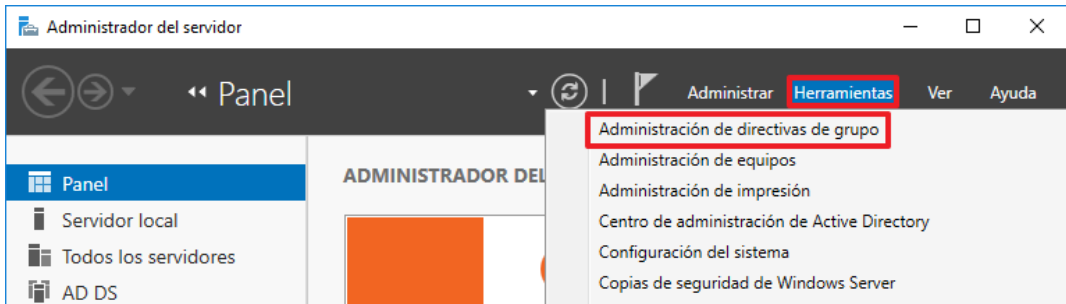
2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

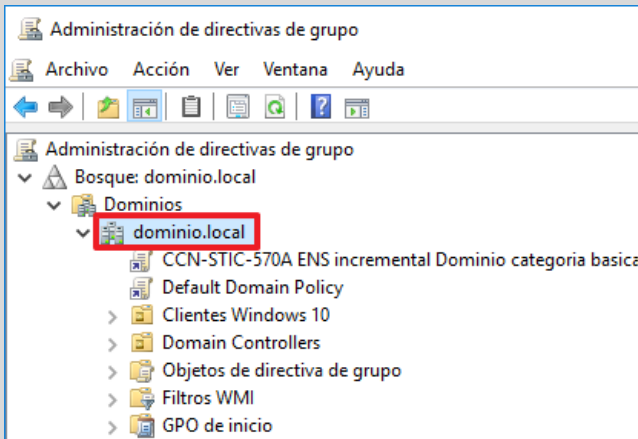
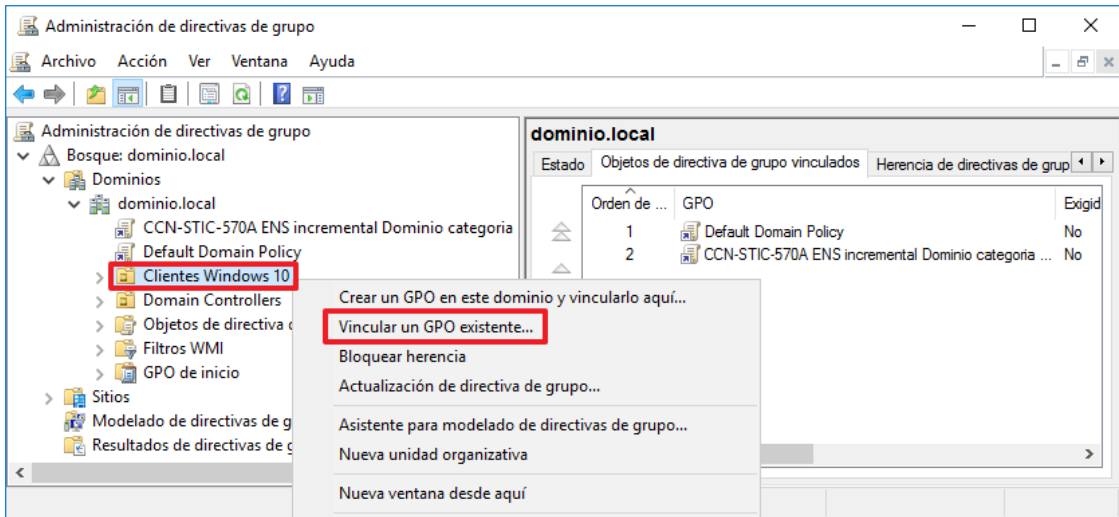
Paso	Descripción
53.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
54.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
55.	Edite la política de grupo correspondiente. Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
56.	Pulse sobre el botón “Sí” para confirmar la operación. 
57.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 

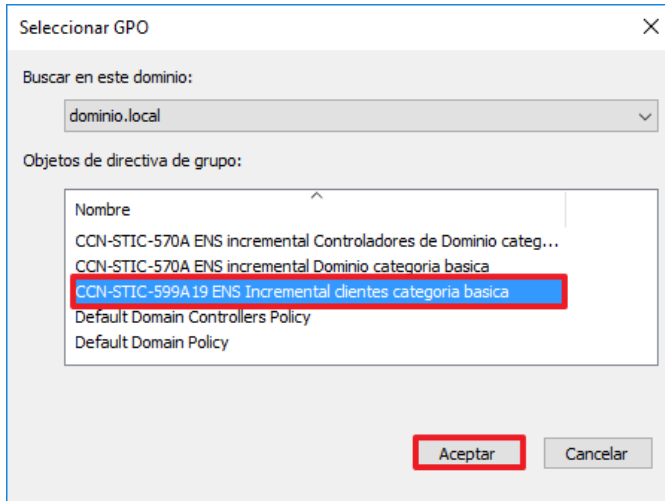
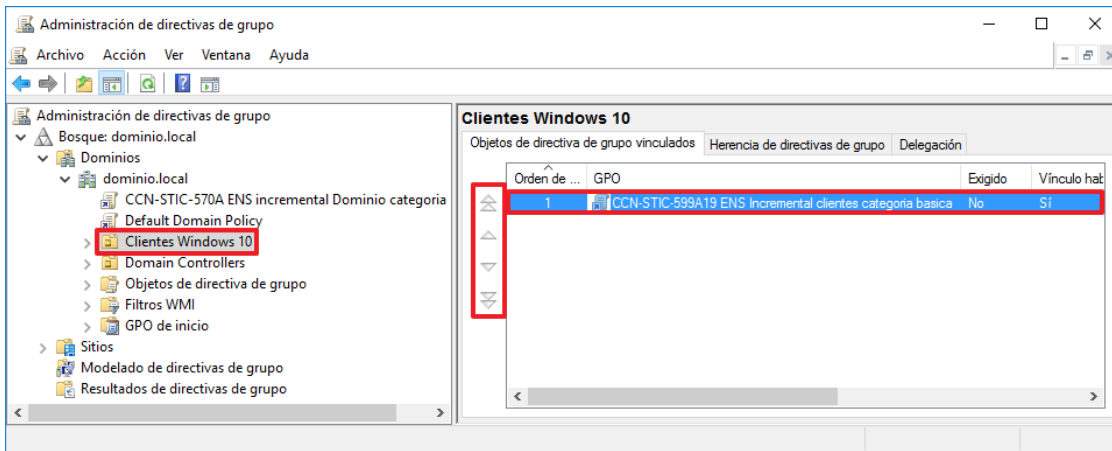
Paso	Descripción
58.	Seleccione la política creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
59.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana del editor de administración de directivas de grupo.

3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, una vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
62.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
63.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
64.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
65.	Pulse sobre el botón "Sí" para confirmar la operación. 
66.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo". 

Paso	Descripción
67.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es “dominio.local”.
68.	Identifique las ubicaciones donde se encuentran los Clientes Windows 10 que les son de aplicación las condiciones de seguridad de categoría básica, según estipula el ENS. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” lugar donde se encuentran ubicados los clientes existentes en este escenario. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 
69.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
70.	Seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón “Aceptar”. 
71.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria basica” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dicha Unidad Organizativa. 
72.	Cierre la herramienta “Administración de directivas de grupo”.
73.	Elimine la carpeta “C:\Scripts”.
74.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Es posible que bajo determinadas condiciones pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado Microsoft propone como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

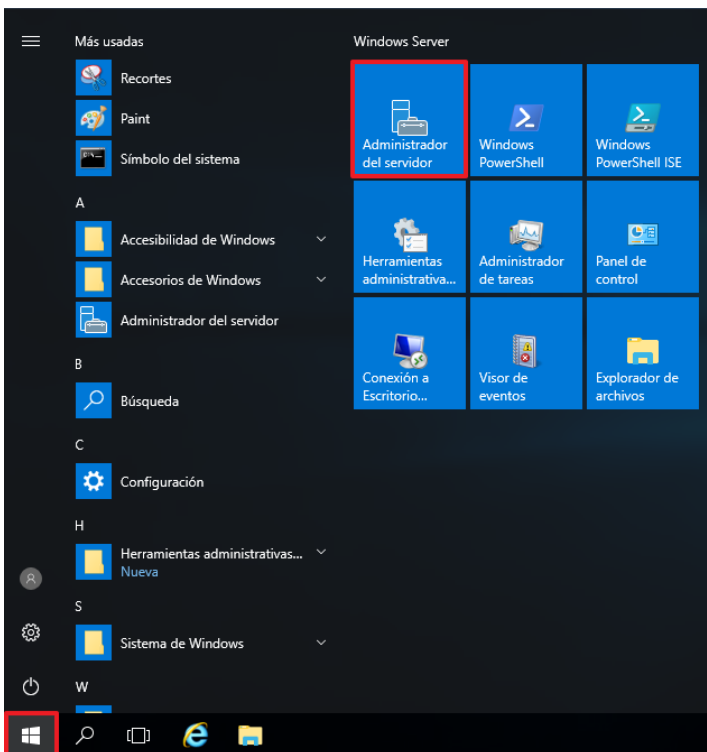
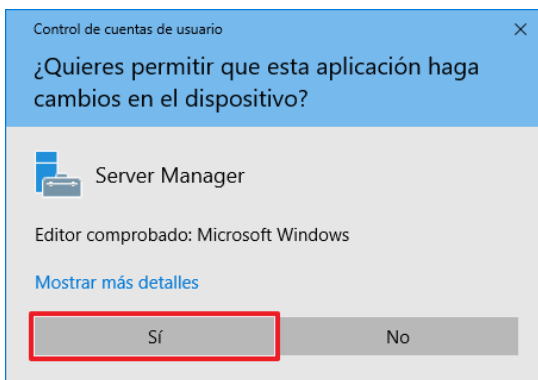
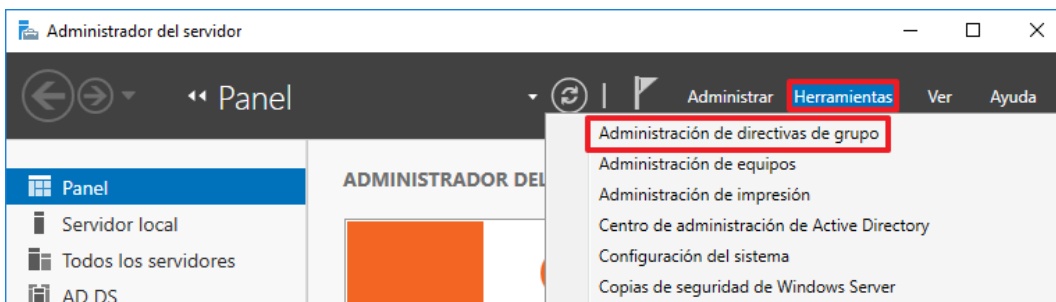
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría básica, aunque con los criterios más laxos de los aplicables.

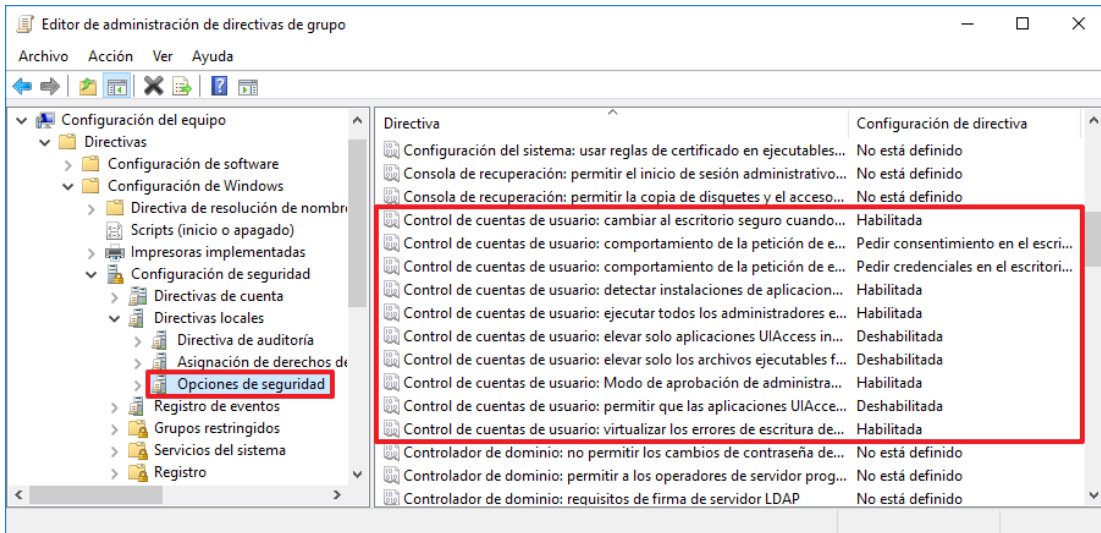
No obstante, y ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría básica por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación a los clientes que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

4.1. CONTROL DE CUENTAS DE USUARIO

Paso	Descripción
75.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
76.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
77.	Identifique los puestos de trabajo que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS clientes Windows 10 categoria basica”. En el caso de que no haya tenido que crear dicho grupo siga al paso siguiente.
78.	Cree un nuevo grupo de forma similar al ya creado, siguiendo los pasos 11 a 26 del presente Anexo.

Paso	Descripción
79.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
80.	Pulse sobre el botón "Sí" para confirmar la operación. 
81.	Seleccione la pestaña "Administración de directivas de grupo" 

Paso	Descripción
82.	Cree una nueva política de grupo con un nombre diferente (p.e. “CCN-STIC-599A19 ENS incremental clientes categoria basica incidencias UAC”) que será asignable a los clientes Windows 10 con una categoría básica e incidencias de funcionalidad del UAC. Siga para ello los pasos 27 a 46. Incluya al nuevo grupo de puestos de trabajo creado anteriormente en lugar del grupo “ENS clientes Windows 10 categoria basica”.
83.	Edite el nuevo objeto de GPO “CCN-STIC-599A19 ENS incremental clientes categoria basica incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar...” del menú contextual.
84.	Despliegue la política y sitúese en la siguiente ruta: Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad
85.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
86.	Realice las modificaciones oportunas.
87.	Cierre la política.
88.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se efectúa cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Debe tener en consideración que, si ha alterado la política de control de cuentas y esta es menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Deberá evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presenten funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

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 GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

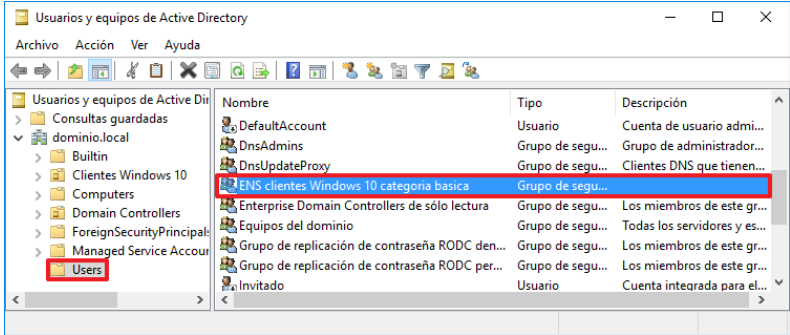
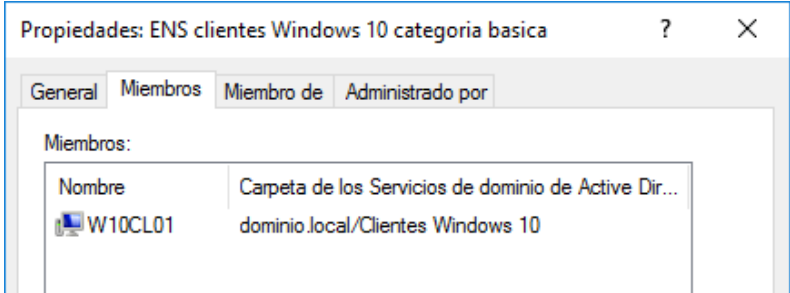
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

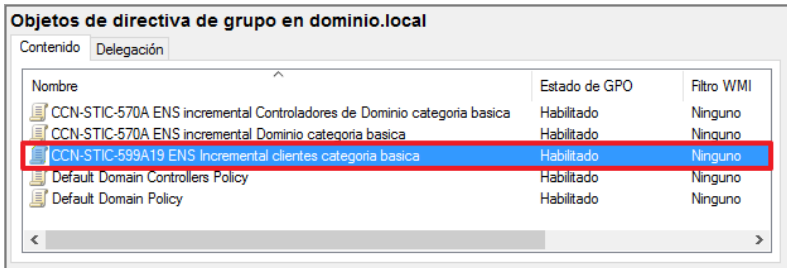
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

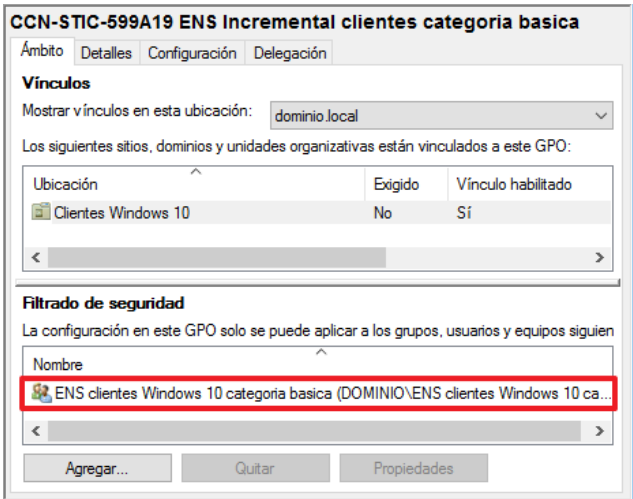
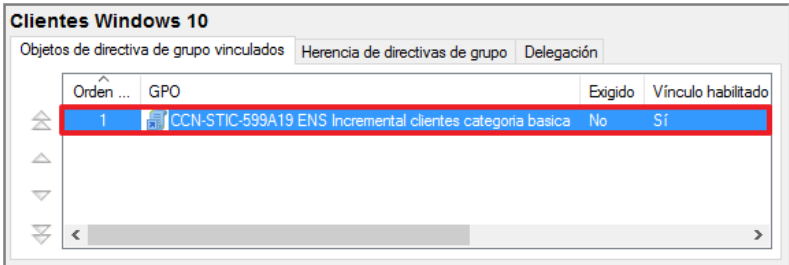
También deberá ejecutar una parte del análisis en los clientes Windows 10 a los que se les haya aplicado la configuración de seguridad de categoría básica. En éstos deberá ejecutar la siguiente aplicación.

- a) Conjunto resultante de directivas (rsop.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creado el grupo “ENS clientes Windows 10 categoria basica” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory” desde: “Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory”

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione el contenedor “Users”, situada en “[Su dominio] → Users” y a continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS clientes Windows 10 categoria basica”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.
3. Verifique que los clientes que han sido catalogados como de categoría de seguridad básica, siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS clientes Windows 10 categoria basica”.		Pulse doble clic sobre el grupo “ENS clientes Windows 10 categoria basica” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los clientes que corresponden a esta categoría de seguridad aparecen en el listado.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” ha sido creado y está habilitado.		Ejecute la herramienta “Administrador de directivas de grupo” desde: “Menú inicio → Herramientas administrativas → Administrador de directivas de grupo” Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo” Verifique que está creado el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” y que en la columna “Estado de la GPO” figura como habilitado. 
	Directiva	Estado
	CCN-STIC-599A19 ENS incremental clientes categoria basica	Habilitado
5. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” tiene definido el Ámbito al grupo “ENS clientes Windows 10 categoria basica”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo”

Comprobación	OK/NOK	Cómo hacerlo
		Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS clientes Windows 10 categoría básica”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.
6. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría básica” es aplicado a todos aquellos equipos Windows 10 que le son de aplicación las condiciones de categoría básica.		Evalúe que la política de seguridad es aplicada en un orden superior a otras políticas aplicables a los puestos de trabajo en todas aquellas ubicaciones donde se encuentren clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría básica. En el árbol de la izquierda, seleccione la ubicación donde se encuentren los clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría básica: 

Comprobación	OK/NOK	Cómo hacerlo		
7. Verifique la directiva de contraseñas en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Pulse el botón derecho del ratón y seleccione la opción “Editar...”. Se abrirá el editor de directivas de grupo. Deberá navegar sobre los elementos del árbol de directorios para verificar las distintas configuraciones. Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directiva de cuentas → Directiva de contraseñas”		
		Directiva	Valor	OK/NOK
		Exigir historial de contraseñas	24	
		Longitud mínima de la contraseña	8	
		Vigencia máxima de la contraseña	90	
		Vigencia mínima de la contraseña	2	
8. Verifique la directiva de bloqueo de cuenta en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directiva de cuentas → Directiva de bloqueo de cuenta”		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	30	
		Restablecer el bloqueo de cuenta después de	30	
		Umbral del bloqueo de cuenta	8	

Comprobación	OK/NOK	Cómo hacerlo		
9. Verifique las directivas de auditoría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
10. Verifique la asignación de derechos de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	BUILTIN\Administradores	

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

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Generar auditorías de seguridad	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Generar perfiles de un solo proceso	BUILTIN\Administradores
		Generar perfiles del rendimiento del sistema	BUILTIN\Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	
		Hacer copias de seguridad de archivos y directorios	BUILTIN\Administradores
		Iniciar sesión como proceso por lotes	
		Iniciar sesión como servicio	
		Modificar la etiqueta de un objeto	
		Modificar valores de entorno firmware	BUILTIN\Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	
		Omitir comprobación de recorrido	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores, NT AUTHORITY\Usuarios autenticados
		Permitir el inicio de sesión local	BUILTIN\Administradores BUILTIN\Usuarios
		Permitir inicio de sesión a través de Servicios de Escritorio remoto	
		Realizar tareas de mantenimiento del volumen	BUILTIN\Administradores
		Reemplazar un símbolo (token) de nivel de proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Restaurar archivos y directorios	BUILTIN\Administradores

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Tener acceso a este equipo desde la red	BUILTIN\Administradores, BUILTIN\Usuarios	
		Tomar posesión de archivos y otros objetos	BUILTIN\Administradores	
11.Verifique las opciones de seguridad en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesible anónimamente		
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitado	
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitado	
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitado	
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitado	
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitado	
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado	
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado	
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en Modo de aprobación de administrador	Pedir consentimiento o 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	Habilitado
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitado
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitado
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitado
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitado
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitado
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitado
		Cuentas: estado de la cuenta de invitado	Deshabilitado
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitado
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		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	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitado
		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	Habilitado
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitado
		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)	Habilitado
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitado
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitado
		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	Habilitado
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
12.Verifique los servicios del sistema definidos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema” Nota: 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 para cada servicio. En la ventana del editor de administración de directivas de grupo 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	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Manual	Configurado		
BranchCache	PeerDistSvc	Manual	Configurado		
Captura SNMP	SNMPTRAP	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Manual	Configurado		
Copias de seguridad de Windows	SDRSVC	Manual	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
Motor de filtrado de base	BFE	Automático	Configurado		
Net Logon	Netlogon	Automático	Configurado		
Notificaciones del servicio de token de Windows	c2wts	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
Registro de eventos de Windows	EventLog	Automático	Configurado	
Registro remoto	RemoteRegistry	Deshabilitado	Configurado	
Registros y alertas de rendimiento	pla	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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	WbioSvc	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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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	vmicshuttdown	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		
Servicio de enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Manual	Configurado		
Servicio de experiencia de idioma	LxpSvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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.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		

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	
13.Verifique los valores del sistema de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos” Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".	
Archivo	Usuario	Permiso	OK/NOK
%ProgramFiles%\Netmeeting	Administradores	Control total	
	System	Control total	
%Public%\	Administradores	Control total	
	System	Control total	
	Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\tftp.exe		Administradores	Control total	
		System	Control total	
		Administradores	Control total	
		System	Control total	
14.Verifique la directiva de almacén digital en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva		OK/NOK
		Valor		OK/NOK
		No permitir que se ejecute el almacén digital		Habilitado
15.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva		OK/NOK
		Valor		OK/NOK
		Desactivar la ayuda activa		Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
16.Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Buscar”		
		Directiva	Valor	OK/NOK
		No buscar en Internet o mostrar resultados de Internet en Search	Habilitada	
17.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
18.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
19.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
20.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
21.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

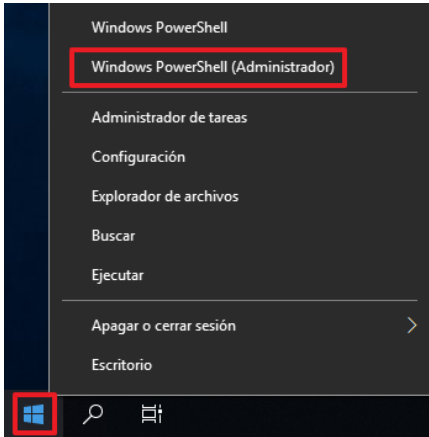
Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Impedir que se eliminen datos del sitio de favoritos		Deshabilitado	
	Impedir que se eliminen los archivos temporales de Internet		Deshabilitado	
	Impedir que se eliminen los datos de filtrado InPrivate		Deshabilitado	
	Impedir que se eliminen 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	
22.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”			
	Directiva		Valor	OK/NOK
	Configurar SmartScreen de Windows Defender		Deshabilitado	
23.Verifique las directivas de OneDrive en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive”			

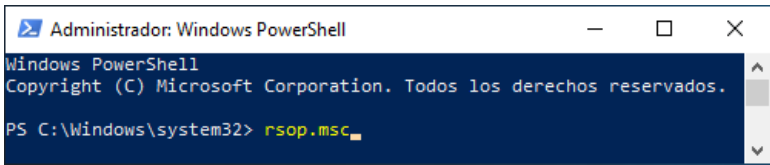
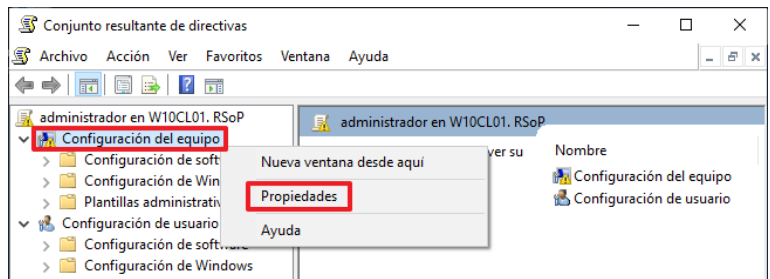
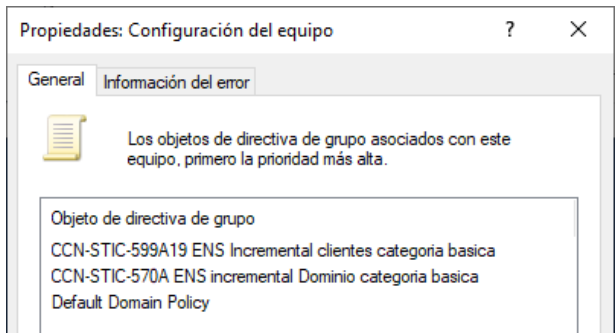
Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado
24.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows →Privacidad de la aplicación”	
		Directiva	Valor
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la cámara	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 accedan a la información de la cuenta	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	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 controlen las radios	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)
25.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		Habilitado	
	Permitir telemetría		Habilitado	
26.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
27.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
	Directiva		Valor	OK/NOK
	Configurar SmartScreen de Windows Defender		Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
28.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitado	
		Desactivar sensores	Habilitado	
		Desactivar ubicación	Habilitado	
29.Verifique la directiva de Windows Update en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	

Comprobación	OK/NOK	Cómo hacerlo		
30.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria basica”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
31.Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador.		Inicie sesión en el equipo cliente que está comprobando con una cuenta de usuario de Windows con permisos de administrador.		
32.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. 		

Comprobación	OK/NOK	Cómo hacerlo
33.Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse "Enter" para abrir la consola de administración "Conjunto resultante de directivas": 
34.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 ENS incremental clientes categoria basica".		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkuelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las políticas deberán aparecer y "CCN-STIC-599A19 ENS incremental clientes categoria basica" deberá estar situada encima de la GPO que se establece a nivel de dominio, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 ENS incremental clientes categoria basica" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

ANEXO C.2. CATEGORÍA MEDIA

ANEXO C.2.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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.

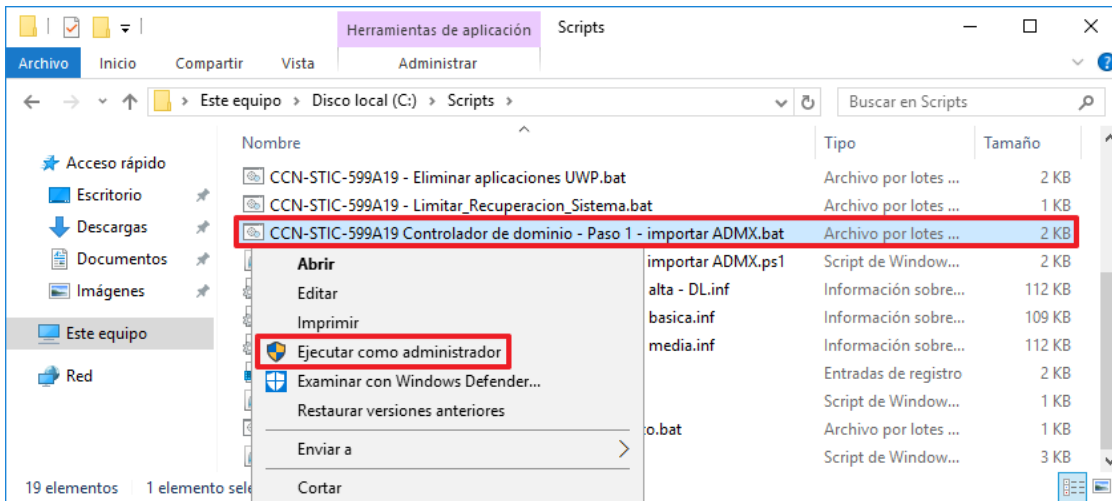
1. PREPARACIÓN DEL DOMINIO

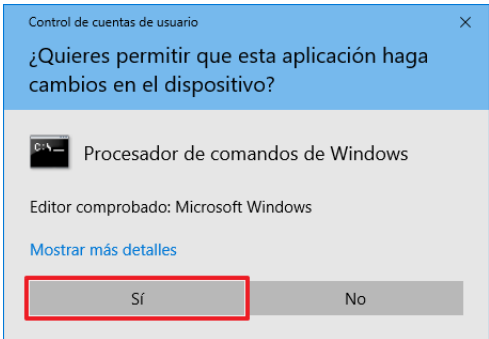
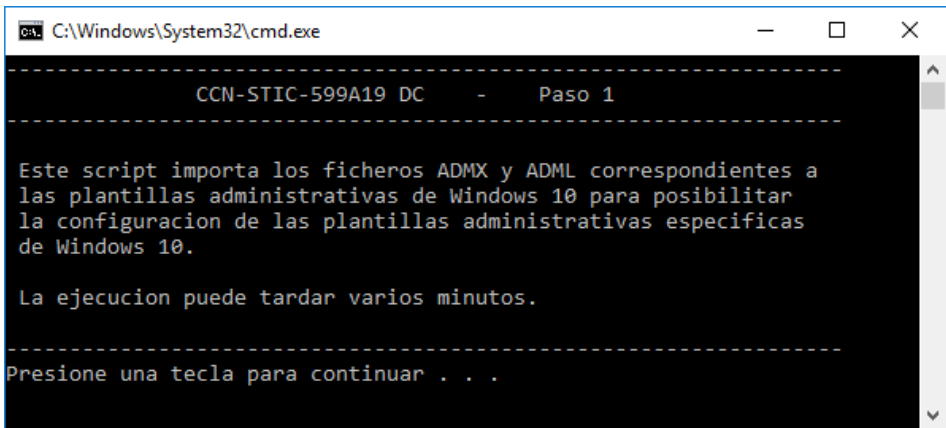
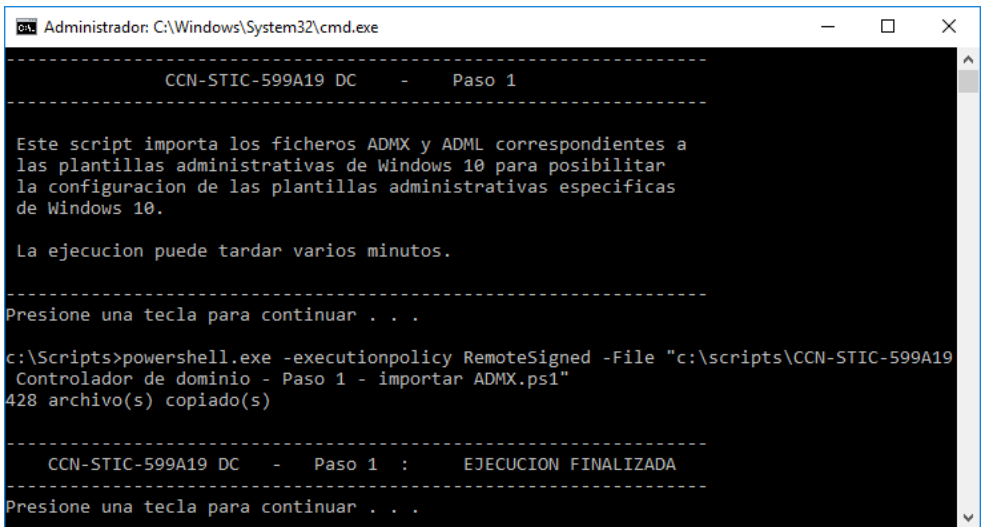
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

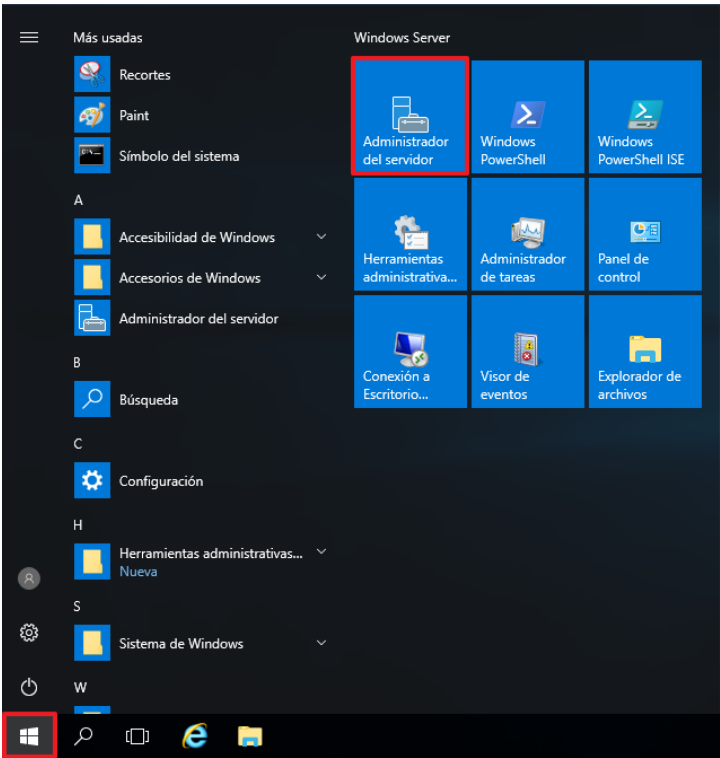
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Si no es así, aplique la guía correspondiente al controlador de dominio, antes de continuar con la aplicación de ésta.

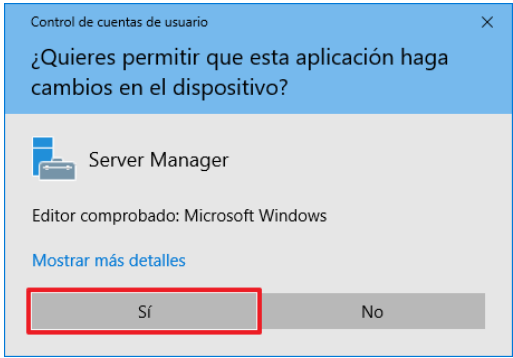
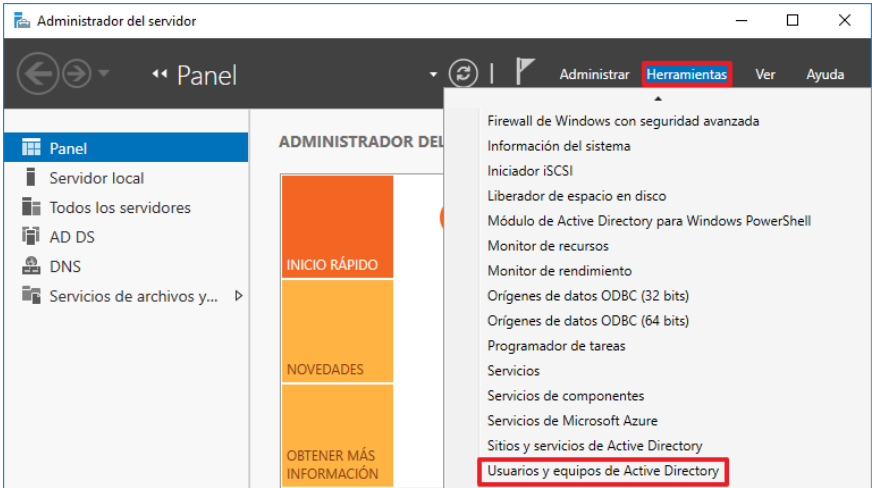
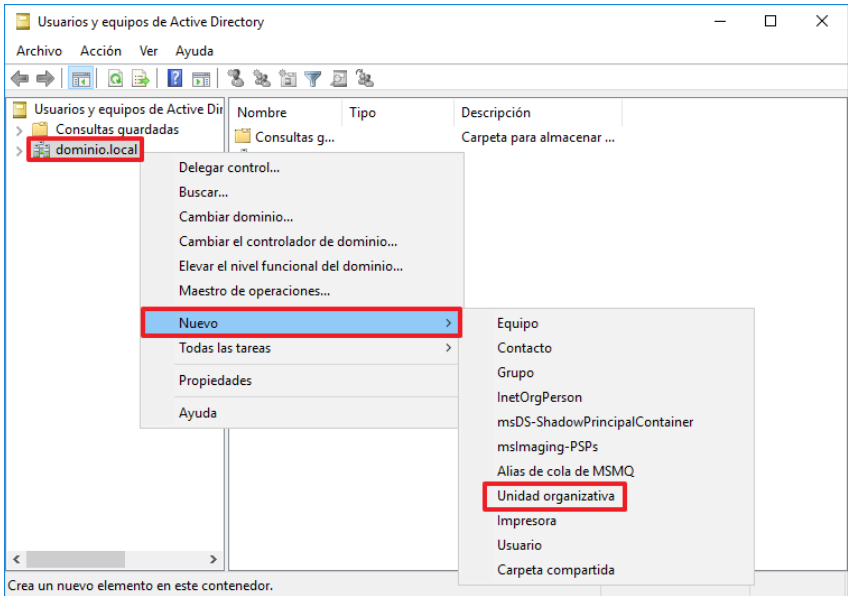
En el ejemplo, las configuraciones y capturas de pantalla han sido realizadas sobre un controlador de dominio al que se le ha instalado Windows Server 2016 y aplicado la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016.

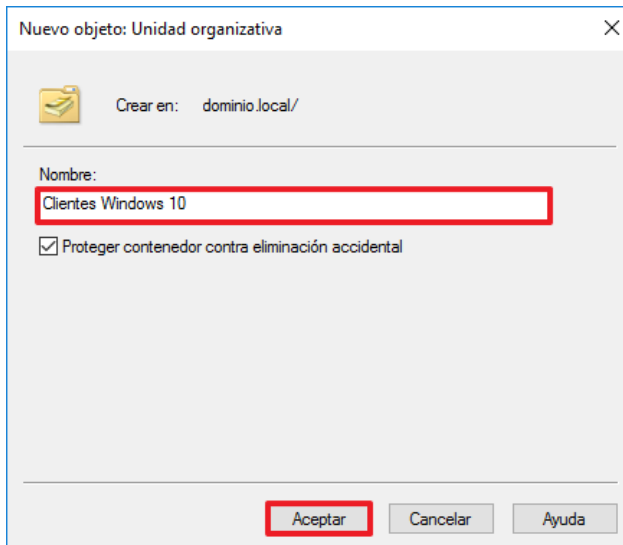
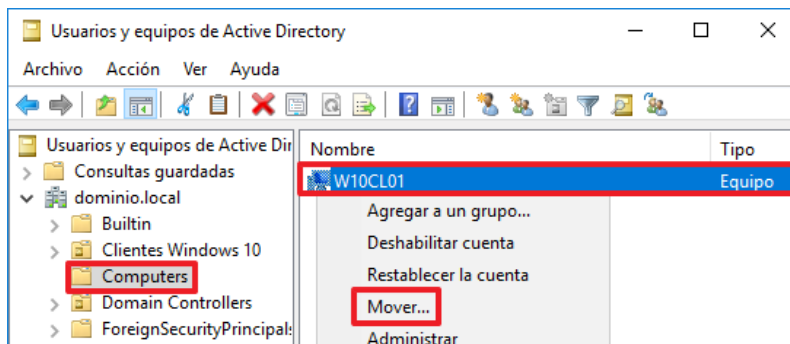
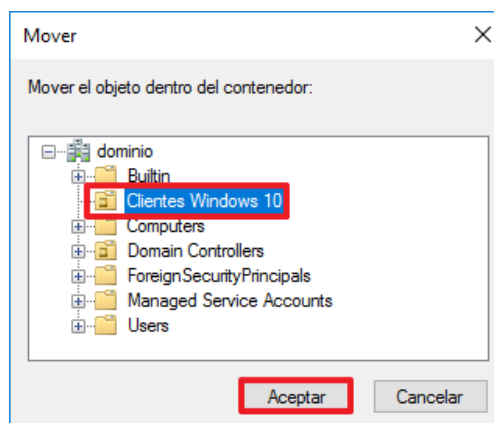
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio.
Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".	

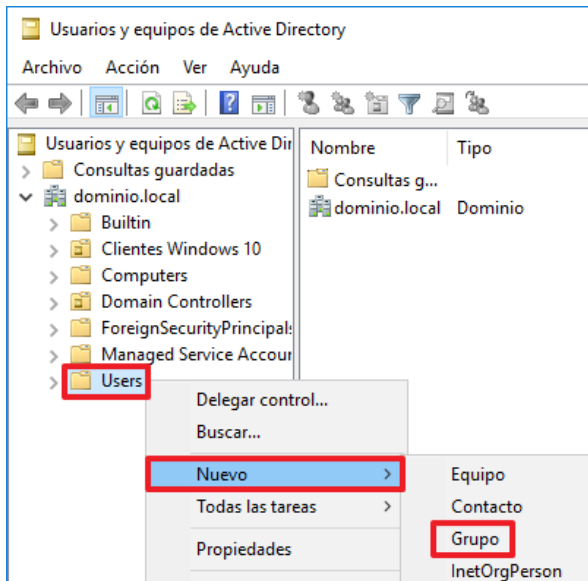
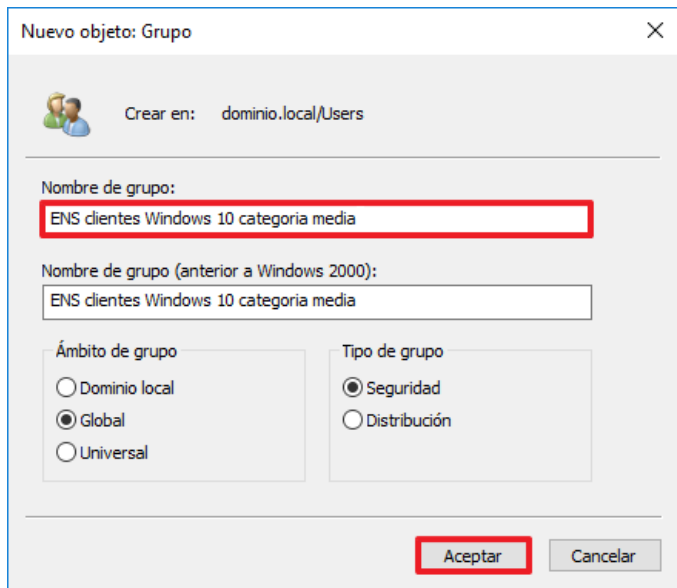
Paso	Descripción
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-599A19 ENS clientes categoria alta - DL (directorio) – CCN-STIC-599A19 ENS clientes categoria media (directorio) – CCN-STIC-599A19 ENS clientes categoria basica (directorio) – CCN-STIC-599A19 ENS Incremental portátiles categoria alta - DL - Bitlocker (directorio) – CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL.inf – CCN-STIC-599A19 ENS Incremental clientes categoria media.inf – CCN-STIC-599A19 ENS Incremental clientes categoria basica.inf – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1 – PolicyDefinitions - (directorio)
6.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

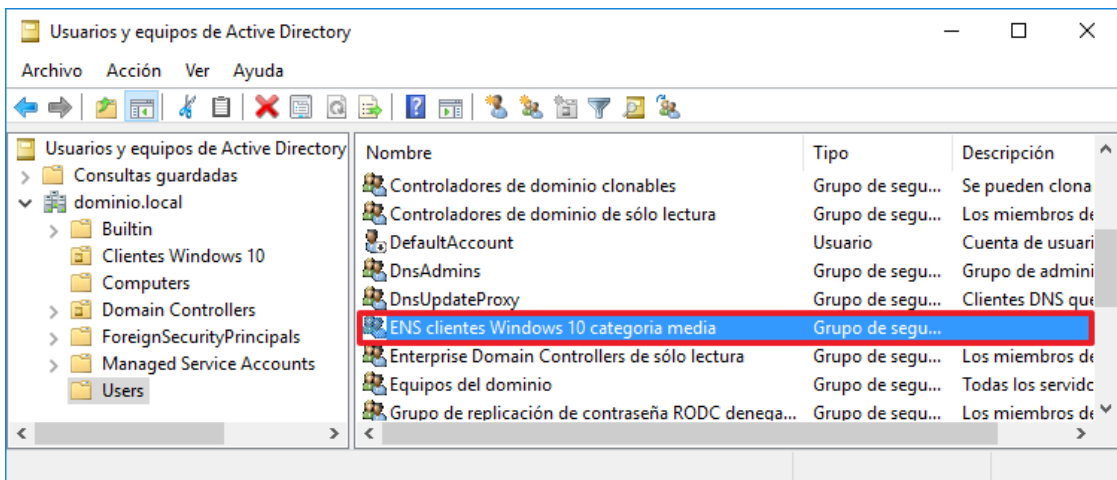
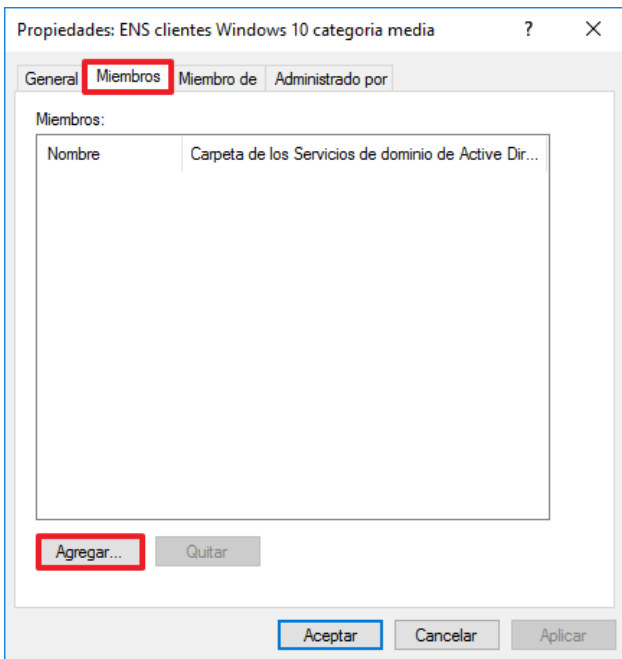
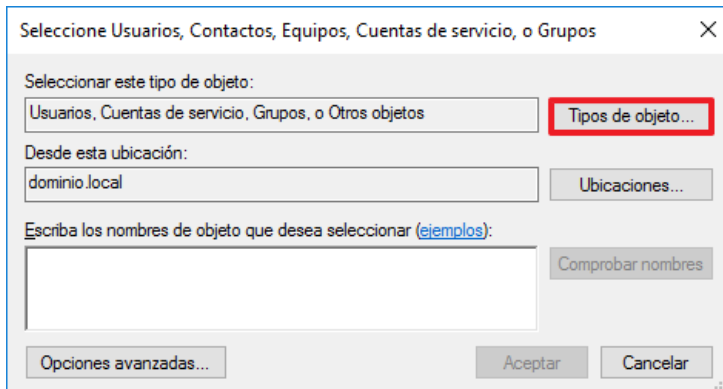
Paso	Descripción
7.	El sistema solicitará elevación de privilegios. Pulse sobre el botón “Sí” para confirmar la operación. 
8.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
9.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 

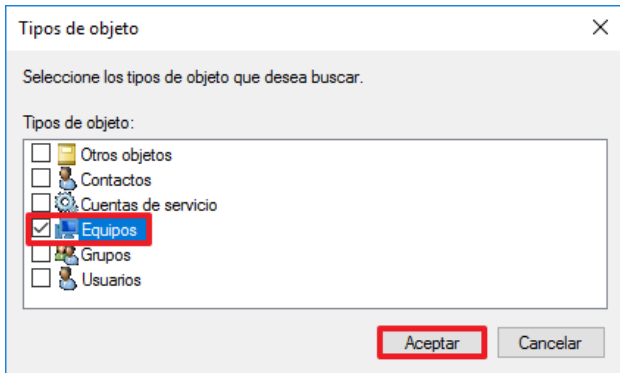
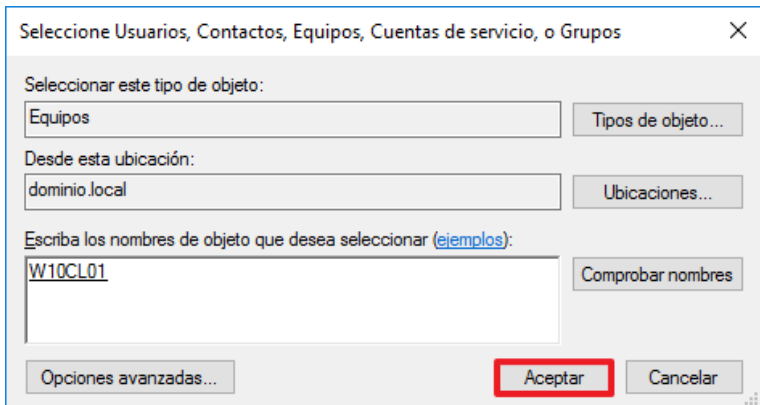
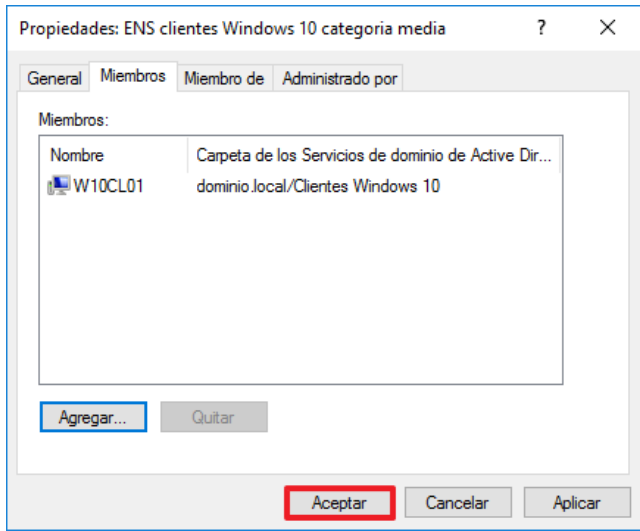
Paso	Descripción
10.	Copie el fichero “CCN-STIC-599A19 ENS incremental clientes categoria media.inf”, almacenado en la carpeta “C:\Scripts”, al directorio “C:\Windows\Security\Templates” del Controlador de Dominio. Nota: Los siguientes pasos describen el procedimiento para crear un grupo de seguridad donde agregar los puestos de trabajo que le sean de aplicación la categoría media de seguridad según los criterios definidos del ENS. En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá también crear el grupo debido a que la política deberá aplicarse a nivel de dominio y se asignará exclusivamente a los puestos de trabajo por la pertenencia a este grupo. Si todos los equipos de la organización presentan la misma categoría media no hace falta la creación de dicho grupo y puede saltar al paso 27. Si por el contrario van a existir puestos de trabajo Windows 10 con categorías básica o alta, deberá crear dicho grupo de tal forma que la aplicación de políticas de seguridad en función de las categorías se aplique atendiendo a los criterios de pertenencia a grupo.
11.	Inicie la herramienta de “Usuarios y equipos de Active Directory”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

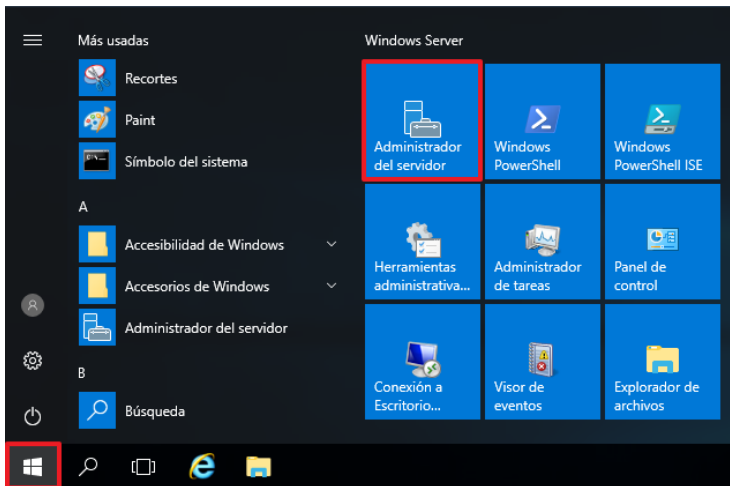
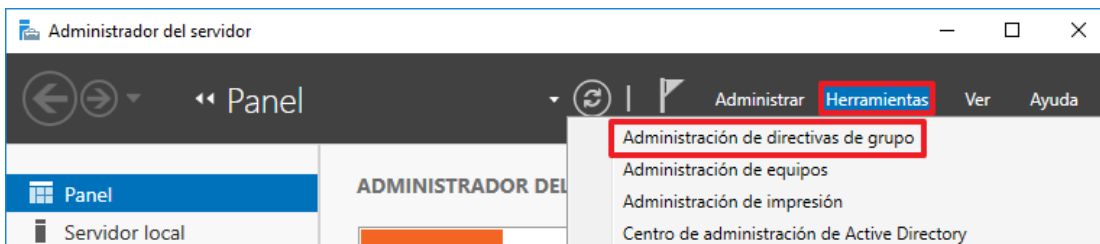
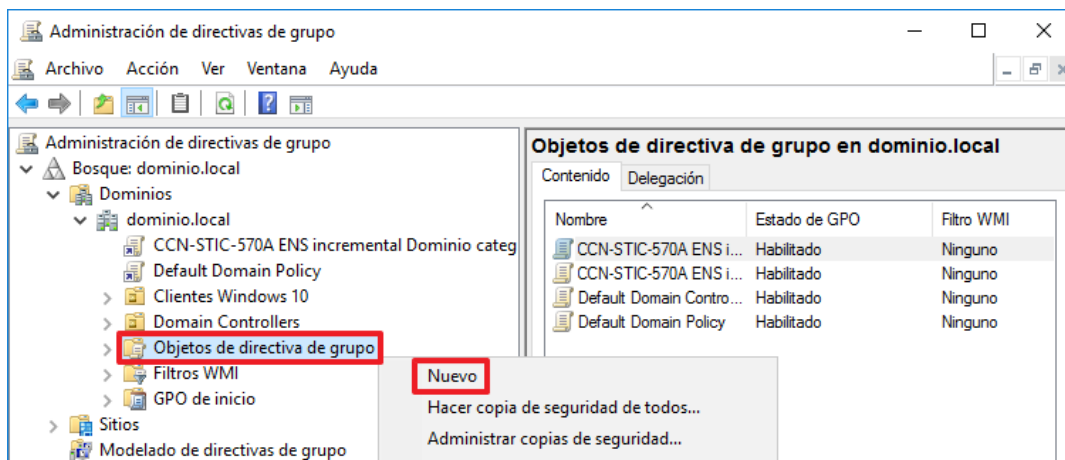
Paso	Descripción
12.	Pulse sobre el botón “Sí” para confirmar la operación. 
13.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
14.	Pulse con el botón derecho sobre el dominio y seleccione “Nuevo → Unidad organizativa”. 

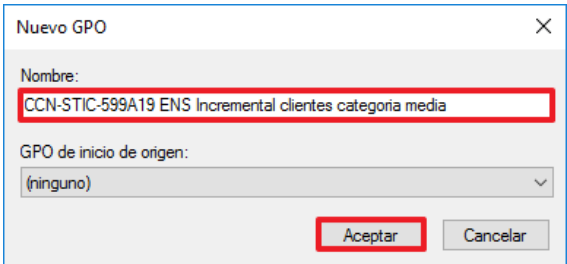
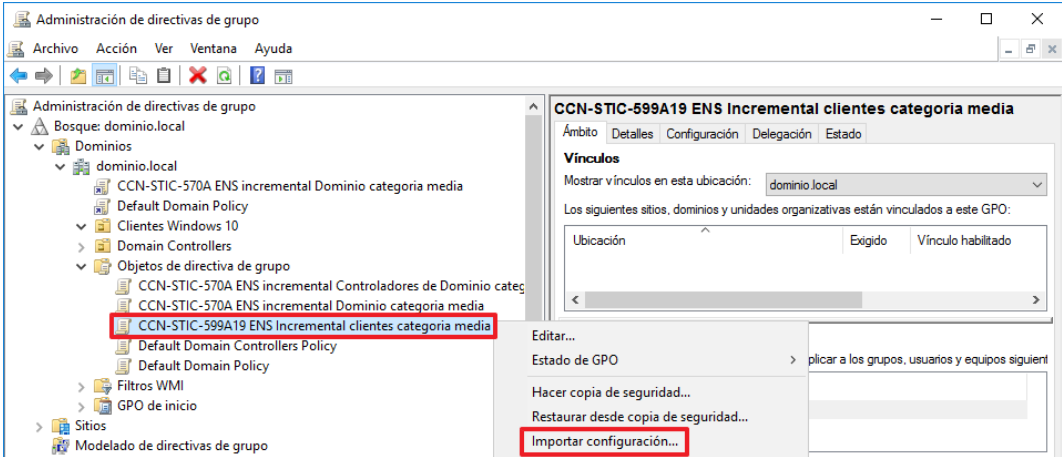
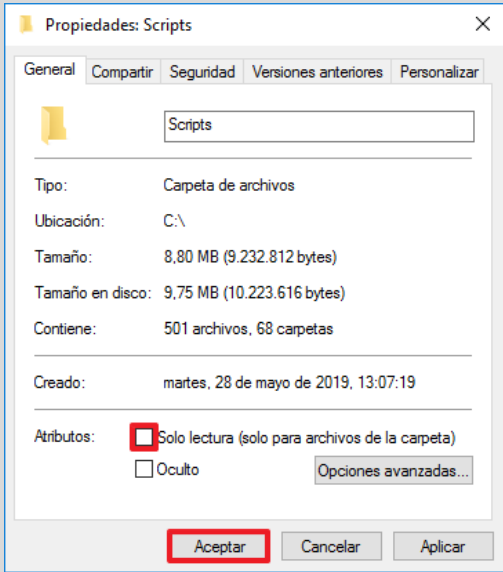
Paso	Descripción
15.	Establezca el nombre para la unidad organizativa con los clientes Windows 10 y pulse “Aceptar”. 
16.	Vaya a las unidades organizativas donde se encuentren los clientes que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover...” en cada uno de ellos.  Nota: En este ejemplo se encuentra bajo la unidad organizativa “Computers”.
17.	Seleccione la unidad organizativa “Clientes Windows 10” creada anteriormente y pulse “Aceptar”. 

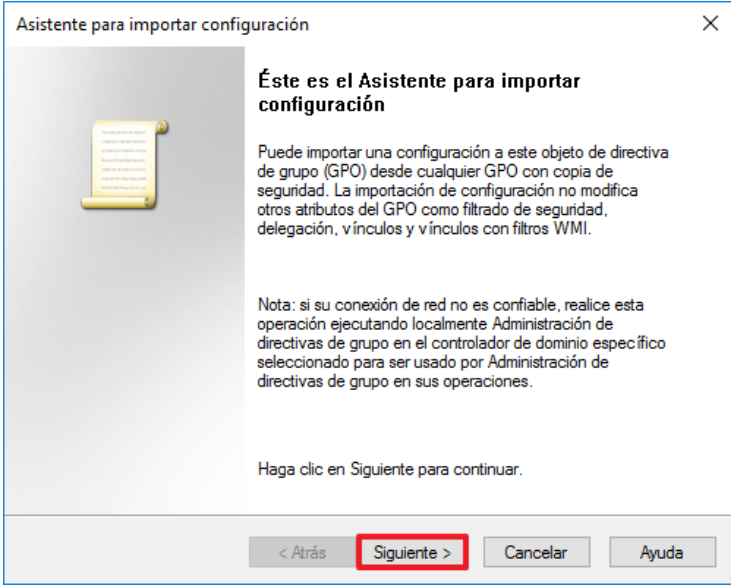
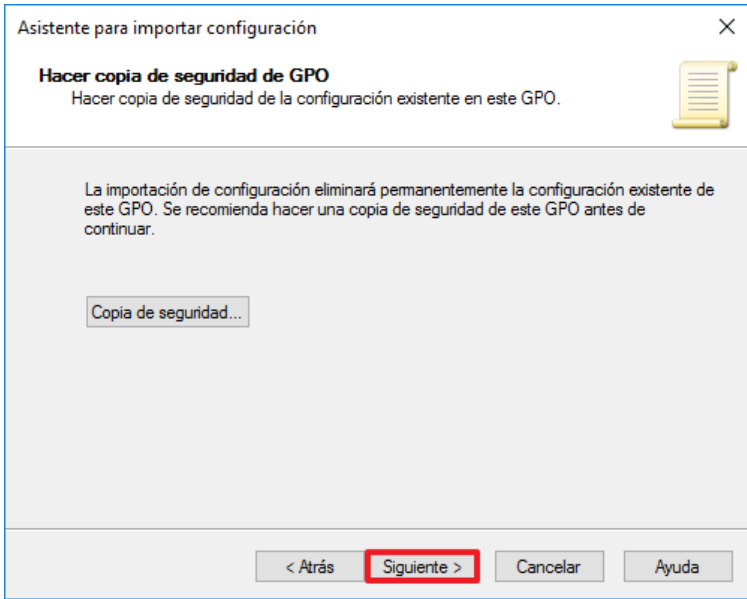
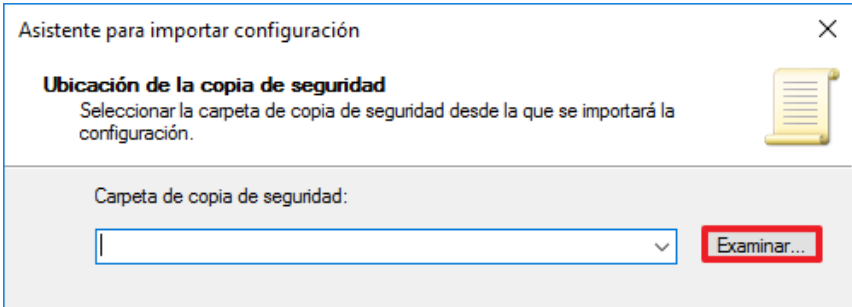
Paso	Descripción
18.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
19.	Introduzca como nombre “ENS clientes Windows 10 categoria media”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio. 

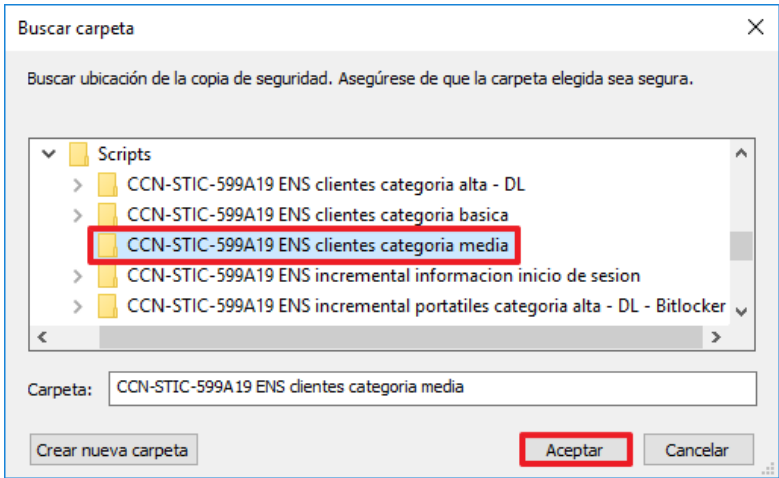
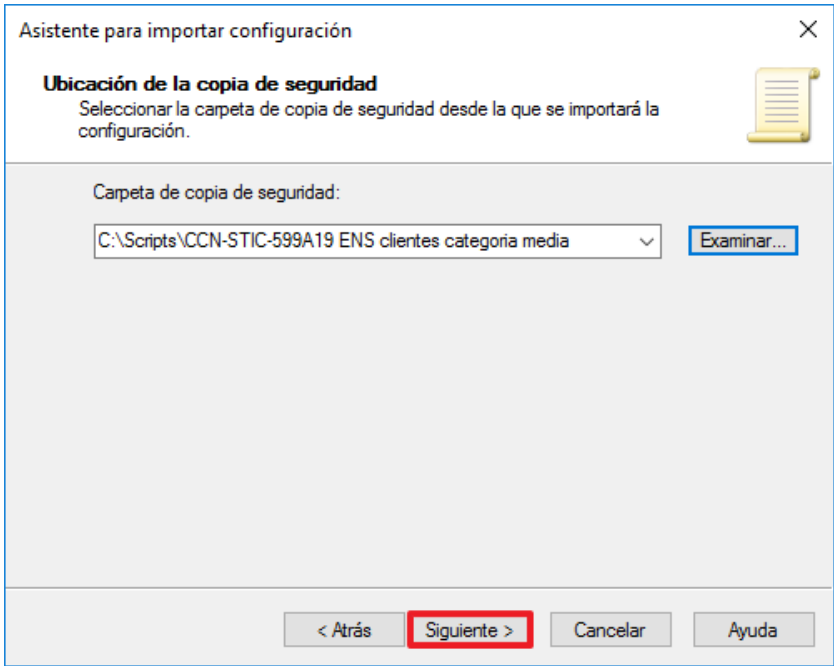
Paso	Descripción
20.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
21.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar...”. 
22.	Pulse el botón de “Tipos de objeto...”. 

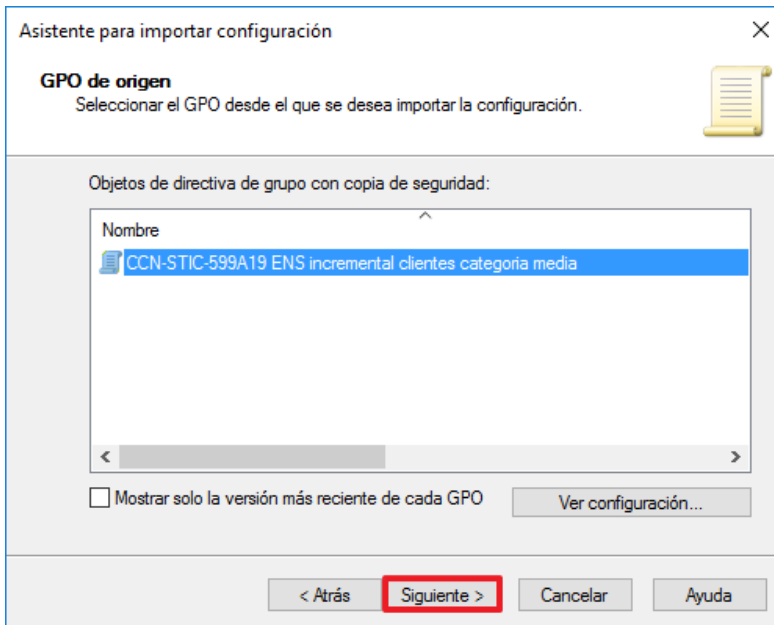
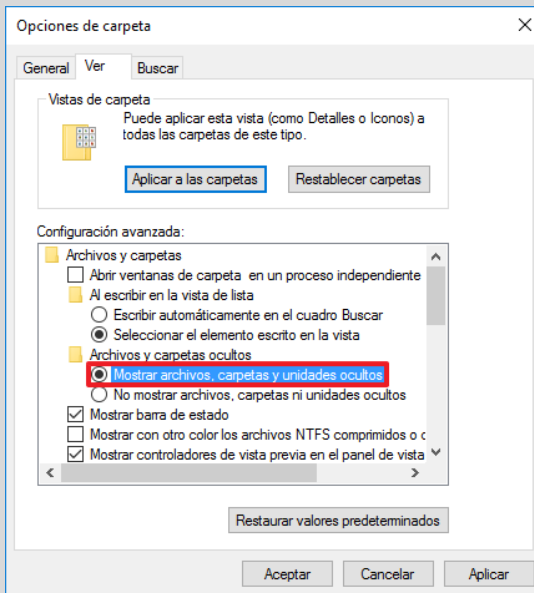
Paso	Descripción
23.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
24.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad media y pulse “Aceptar” para agregar la selección.  Nota: No agregue servidores a este grupo.
25.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
26.	Cierre la herramienta “Usuarios y equipos e Directorio Activo”.

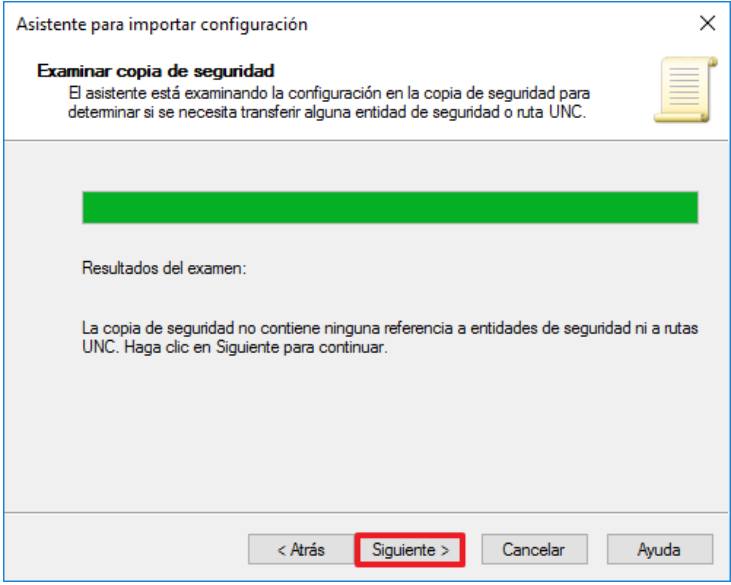
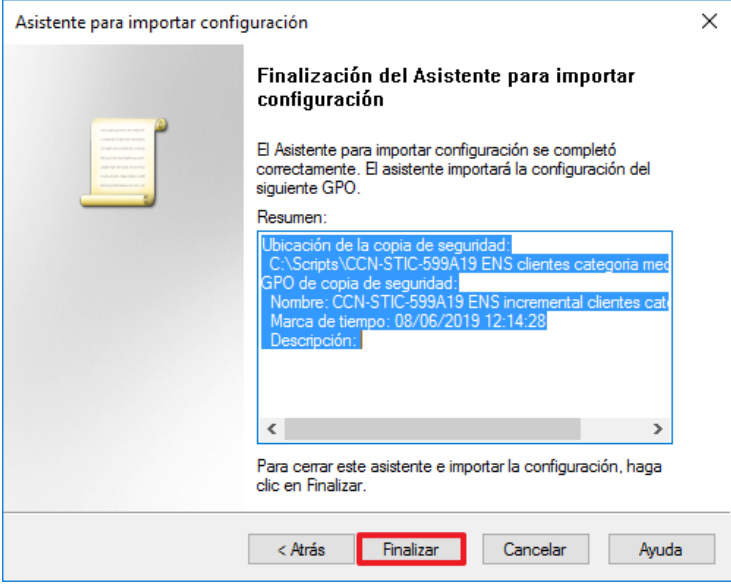
Paso	Descripción
27.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
28.	Pulse sobre el botón "Sí" para confirmar la operación.
29.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo". 
30.	Despliegue los contenedores pertenecientes a su dominio y sitúese sobre la carpeta "Objetos de directiva de grupo". Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción "Nuevo". 

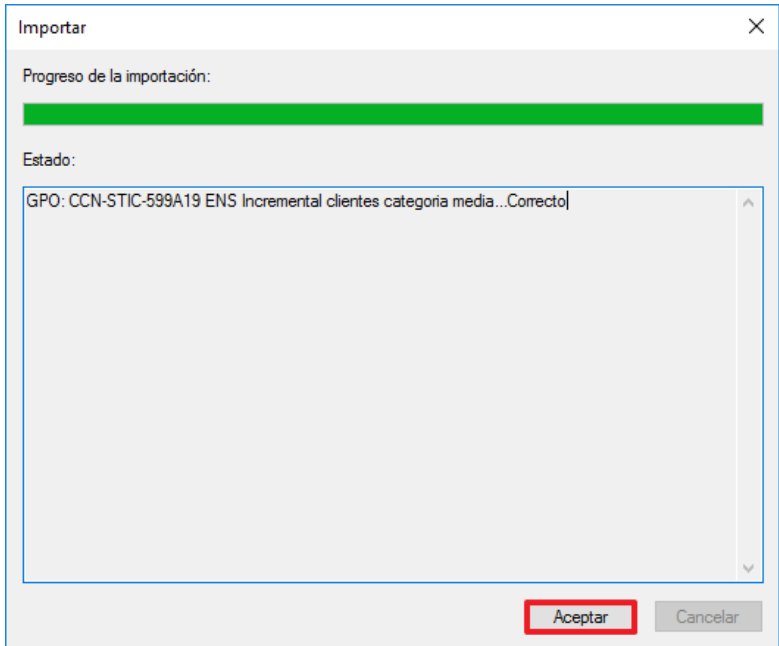
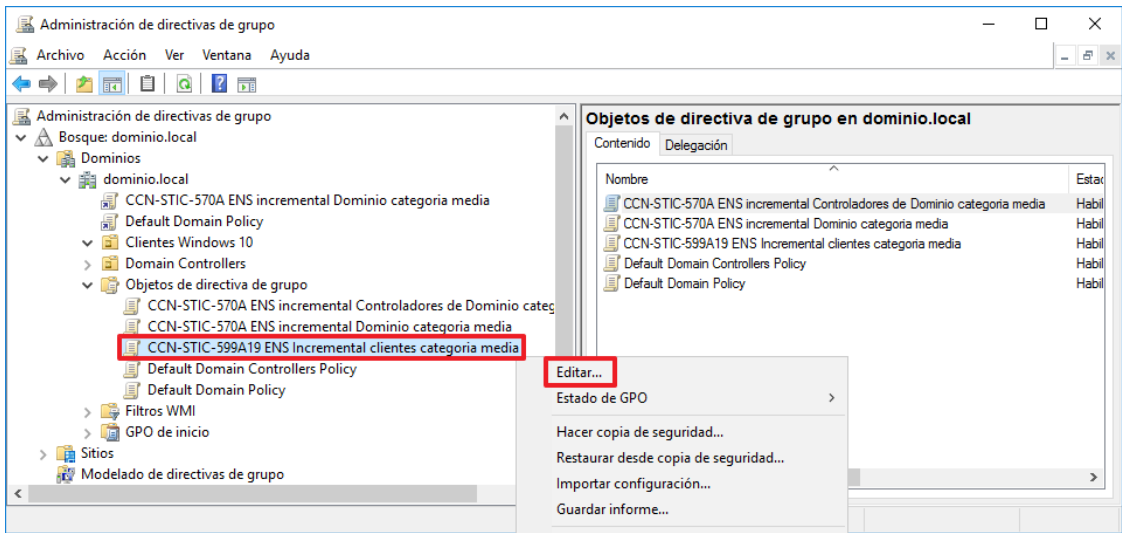
Paso	Descripción
31.	Introduzca como nombre “CCN-STIC-599A19 ENS Incremental clientes categoria media” y pulse el botón “Aceptar”. 
32.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política con el botón derecho del ratón y seleccione la opción “Importar configuración...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts”, así como los archivos dentro de sus subcarpetas, no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

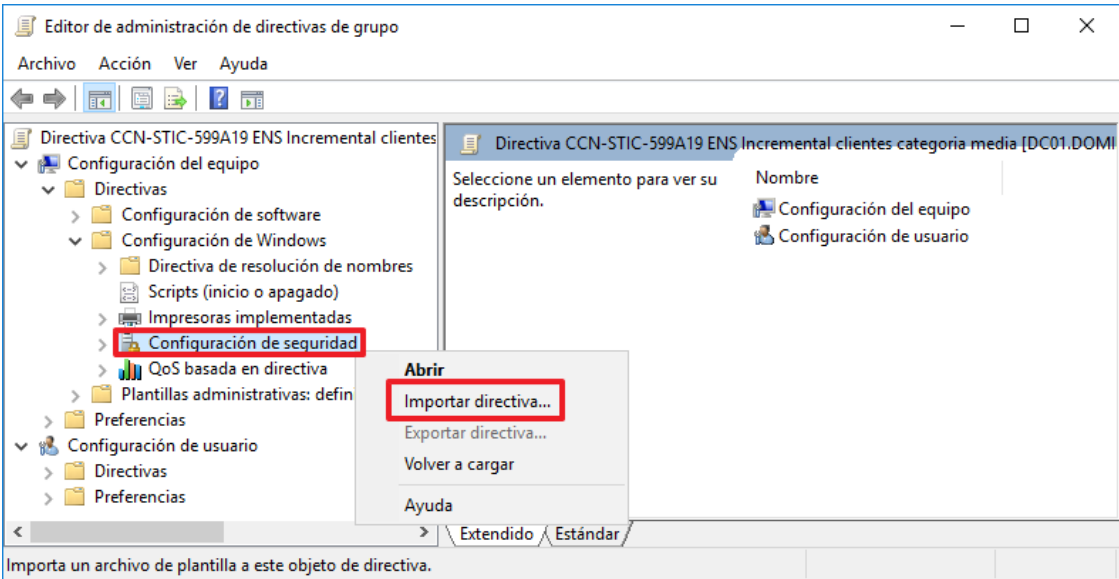
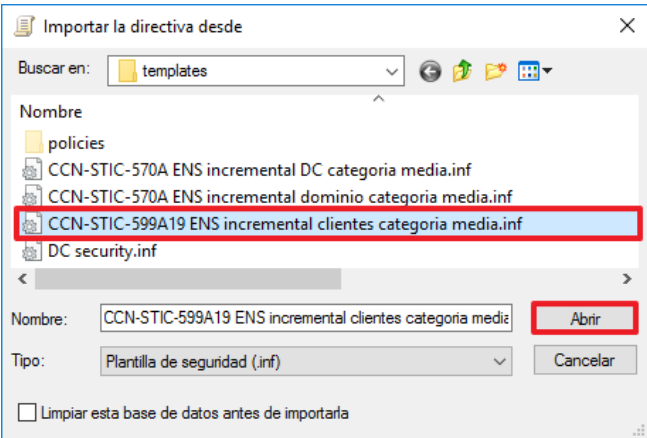
Paso	Descripción
33.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
34.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 
35.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 

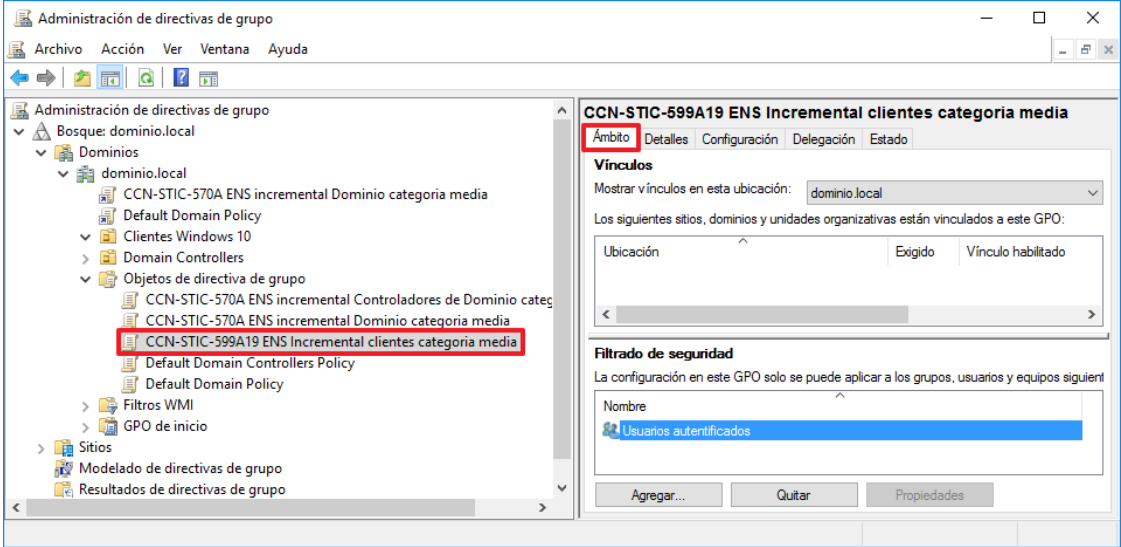
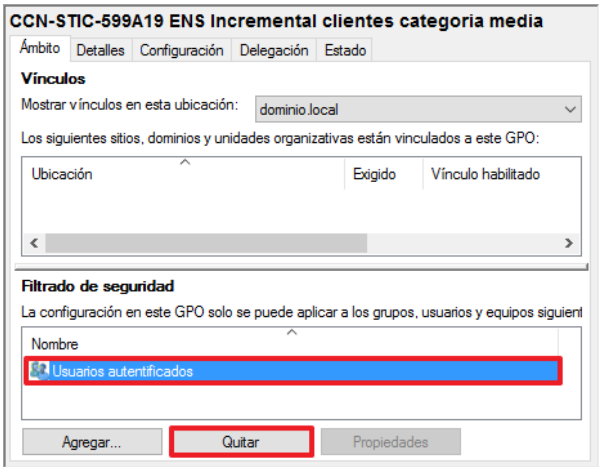
Paso	Descripción
36.	Seleccione la carpeta “CCN-STIC-599A19 ENS clientes categoria media” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
37.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

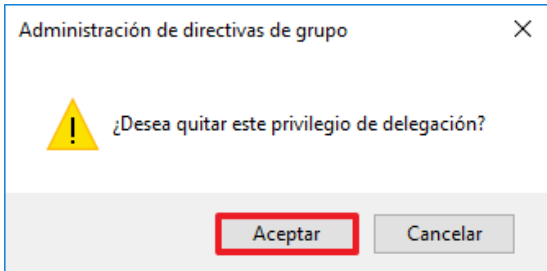
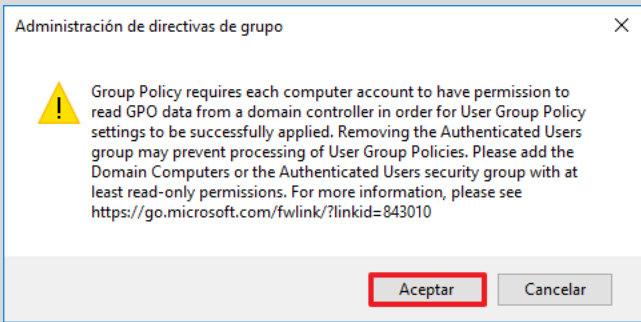
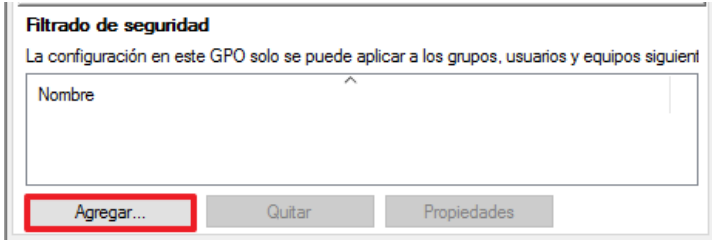
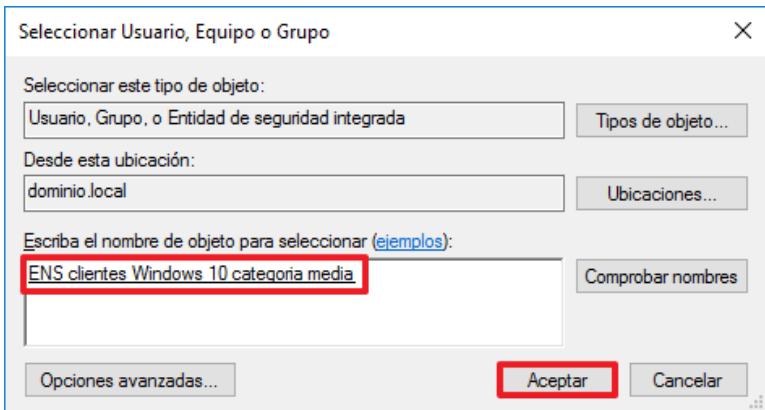
Paso	Descripción
38.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental puestos de trabajo medio” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
39.	En la pantalla de examen, pulse el botón “Siguiente >”. 
40.	Para completar el asistente pulse el botón “Finalizar”. 

Paso	Descripción
41.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración. 
42.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
43.	Una vez pulsada la opción “Editar...” se abre una ventana de “Editor de administración de directivas de grupo”. Despliegue el objeto de directiva de grupo y sitúe el cursor sobre el nodo Configuración de seguridad. “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”

Paso	Descripción
44.	Pulse con el botón derecho en “Configuración de seguridad” y seleccione la opción “Importar directiva...”. 
45.	Seleccione el fichero “CCN-STIC-599A19 ENS incremental clientes categoria media.inf” ubicado en la ruta “C:\Windows\Security\Templates”. Pulse el botón “Abrir”. 
46.	Cierre la política una vez se haya realizado la importación de la configuración de seguridad. Nota: Los siguientes pasos describen el procedimiento para asignar la política al grupo de seguridad creado en los pasos 18 a 25. Si usted creó el grupo, puesto que va a tener aplicadas diferentes categorías de seguridad en la organización para los puestos de trabajo, siga con el siguiente paso. Si no creo dicho grupo, diríjase al paso 52.

Paso	Descripción
47.	Vuelva a la “Administración de directivas de grupo” y seleccione la nueva política de grupo configurada. Vaya a las opciones de ámbito que se encuentran en el panel derecho. 
48.	En el apartado “Filtrado de seguridad”, seleccione “Usuarios autenticados” y pulse el botón “Quitar”. 

Paso	Descripción
49.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 
50.	Pulse ahora sobre el botón “Agregar...”. 
51.	Introduzca como nombre “ENS clientes Windows 10 categoría media”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse “Aceptar”. 
52.	La política se encuentra ya creada correctamente. No obstante, no se aplicará hasta más adelante, una vez haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente Anexo.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA MEDIA

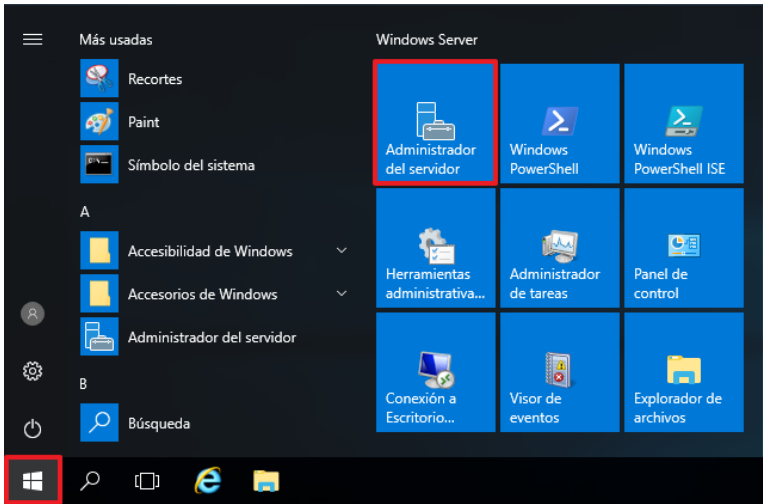
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y por lo tanto deben valorarse con respecto a la aplicación de la presente configuración. La plantilla de seguridad que se ha configurado tiene en consideración los puntos tratados en el Esquema Nacional de seguridad para la categoría media. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina, como por ejemplo lo relativo al uso de privilegios.

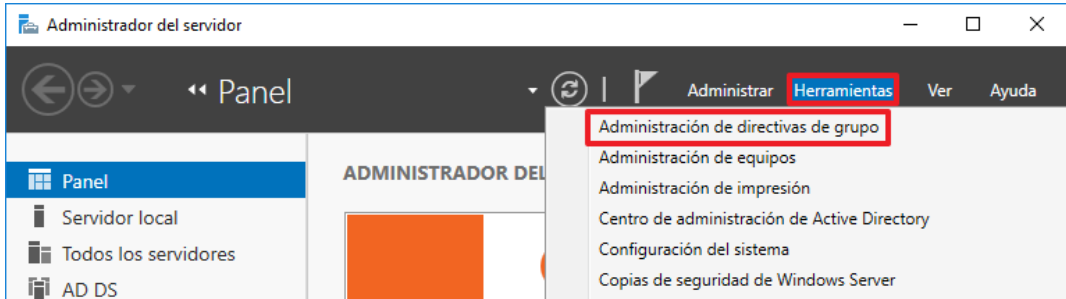
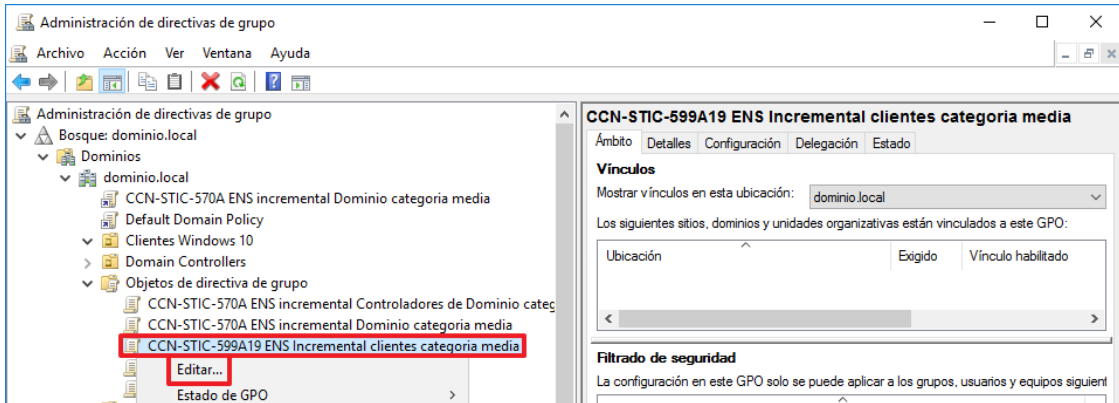
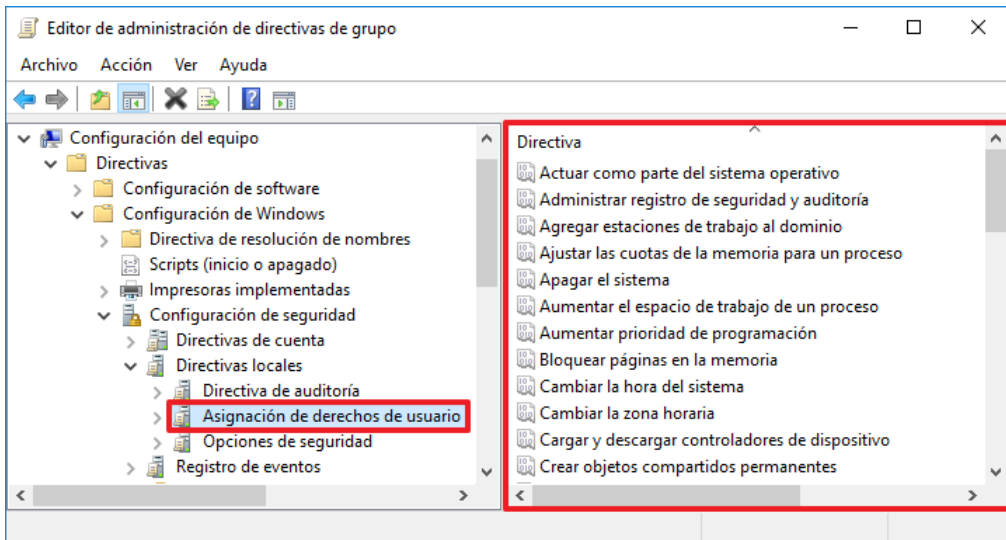
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

Los objetos de políticas de grupo para puestos de trabajo especifican unos derechos de usuario siguiendo planteamientos de seguridad siguiendo los principios de mínimos privilegios 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 el objeto de política creado en el punto previo.

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

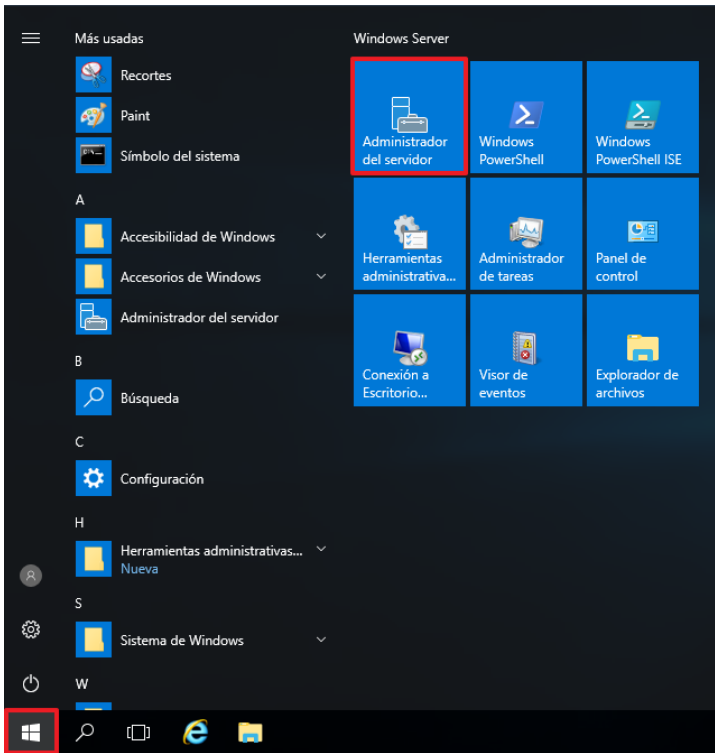
Paso	Descripción
53.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
54.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
55.	Edite la política de grupo correspondiente. Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

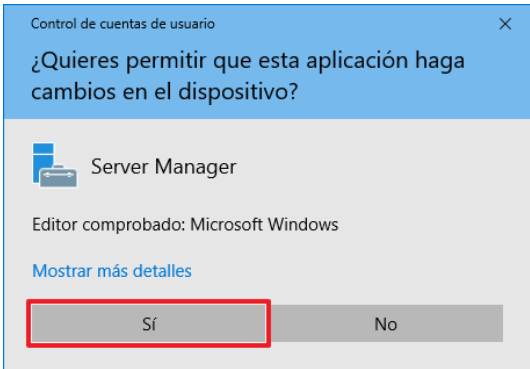
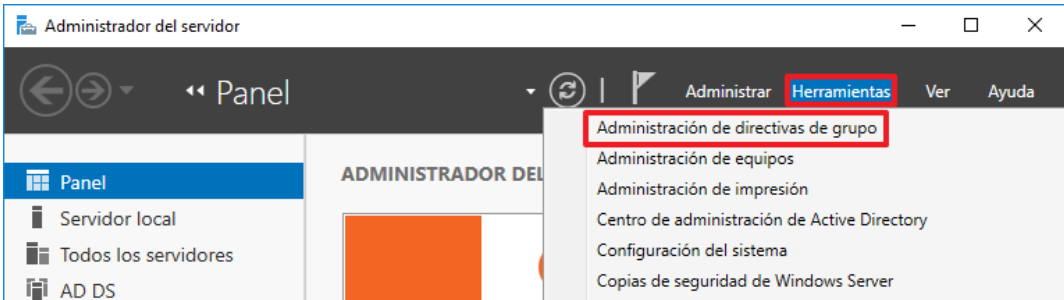
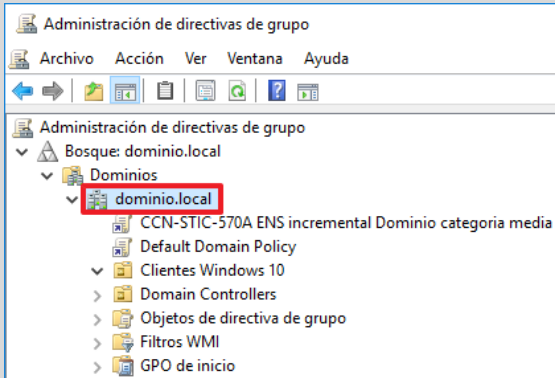
Paso	Descripción
56.	Pulse sobre el botón “Sí” para confirmar la operación.
57.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
58.	Seleccione la política creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
59.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 

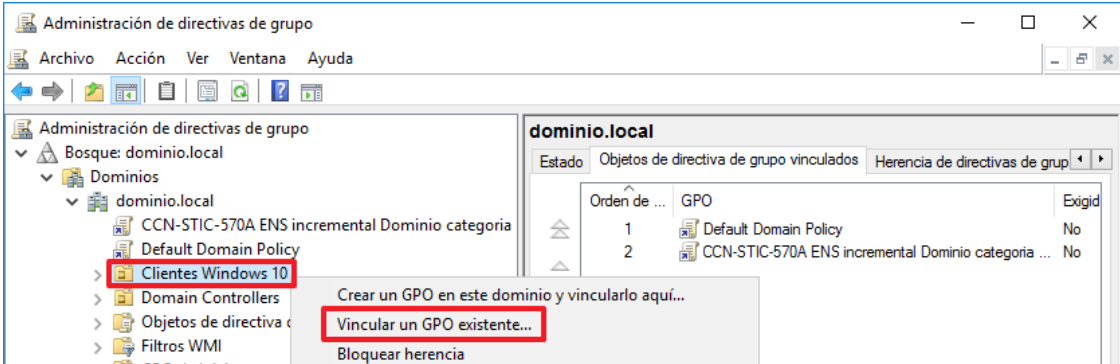
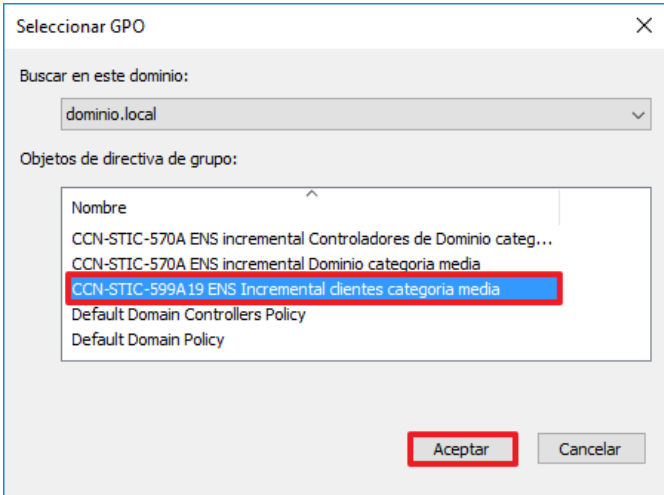
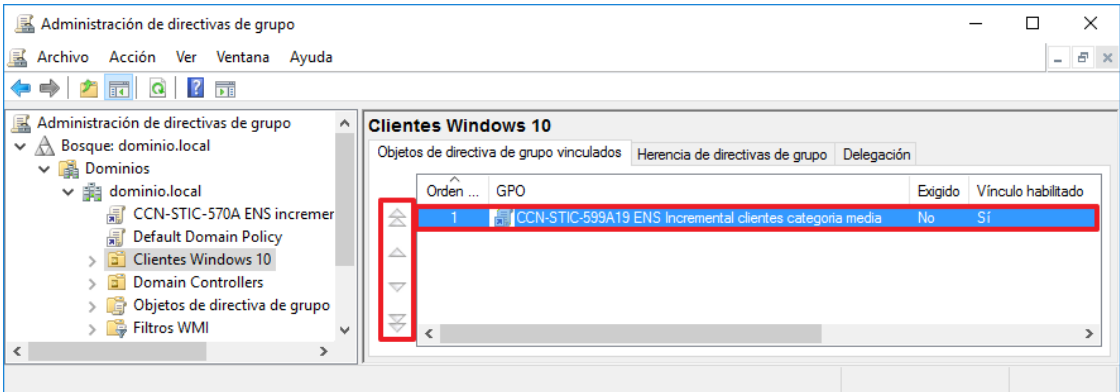
Paso	Descripción
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana del editor de administración de directivas de grupo.

3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, una vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
62.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
63.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
64.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

Paso	Descripción
65.	Pulse sobre el botón “Sí” para confirmar la operación. 
66.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
67.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es “dominio.local”.
68.	Identifique las ubicaciones donde se encuentran los Clientes Windows 10 que les son de aplicación las condiciones de seguridad de categoría media, según estipula el ENS. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC ENS incremental clientes categoria media”. En el ejemplo se aplicará sobre la OU “Clientes Windows 10” lugar donde se encuentran ubicados los clientes existentes en este escenario. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 

Paso	Descripción
69.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y seleccione la opción “Vincular un GPO existente...”. 
70.	Seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria media” y pulse el botón “Aceptar”. 
71.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria media” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dichas Unidades Organizativas. 
72.	Cierre la herramienta “Administración de directivas de grupo”.

Paso	Descripción
73.	Elimine la carpeta “C:\Scripts”.
74.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Tenga en consideración que la edición “Pro” de Windows 10 no permite realizar un bloqueo de la Tienda a través de directivas de grupo por lo que deberá hacer uso de AppLocker para realizar el bloqueo de uso. Consulte el documento de seguridad codificado como “CCN-STIC-869 AppLocker en el ENS”.

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Es posible que bajo determinadas condiciones pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

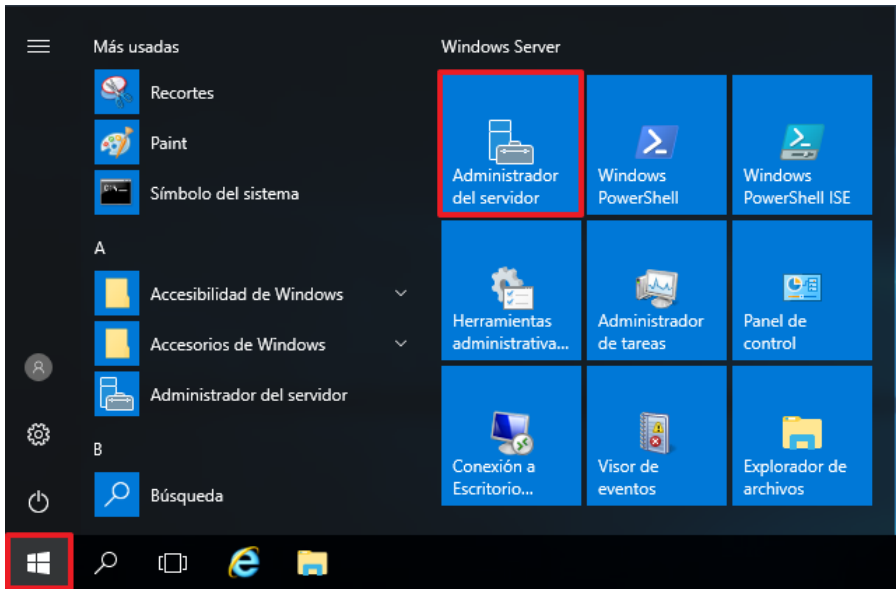
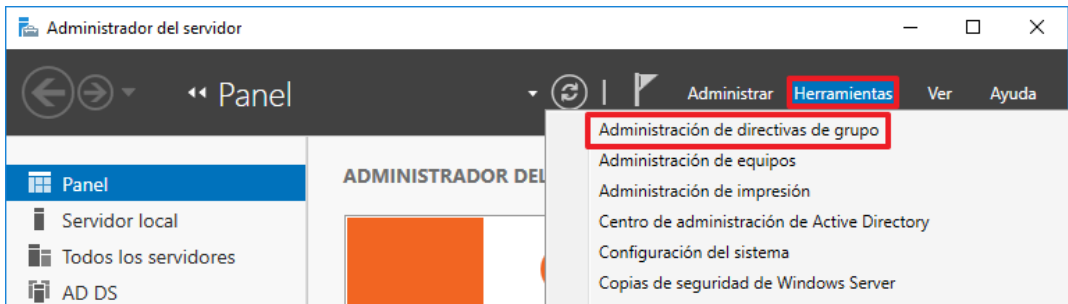
El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado Microsoft propone como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

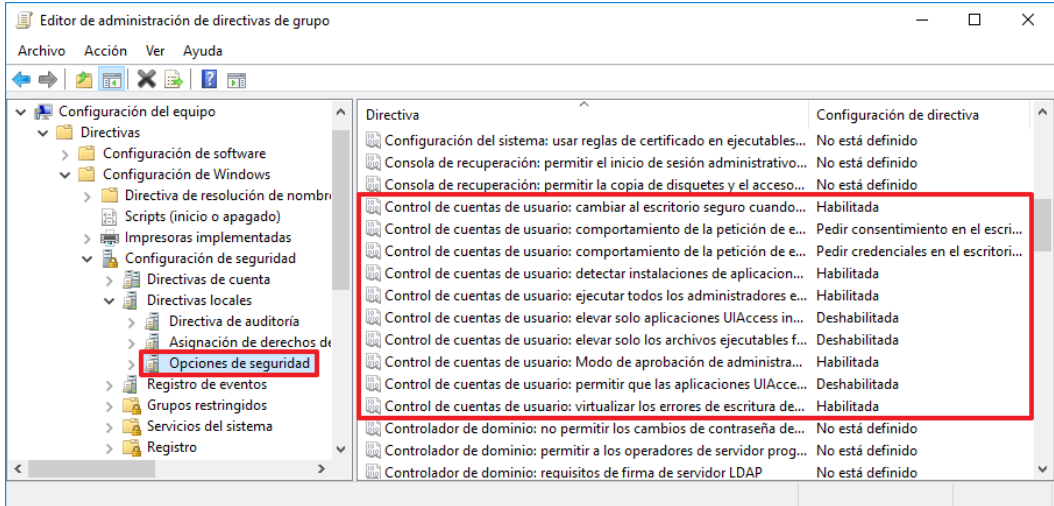
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría media, aunque con los criterios más laxos de los aplicables.

No obstante, y ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría media por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación en los clientes que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

4.1. CONTROL DE CUENTAS DE USUARIO

Paso	Descripción
75.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
76.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
77.	Identifique los puestos de trabajo que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS clientes Windows 10 categoría media”. En el caso de que no haya tenido que crear dicho grupo siga al paso siguiente.
78.	Cree un nuevo grupo de forma similar al ya creado, siguiendo los pasos 18 a 25 del presente Anexo.
79.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
80.	Pulse sobre el botón “Sí” para confirmar la operación.
81.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 

Paso	Descripción
82.	Cree una nueva política de grupo con un nombre diferente (p.e. “CCN-STIC-599A19 ENS incremental clientes categoria media incidencias UAC”) que será asignable a los clientes Windows 10 con una categoría media e incidencias de funcionalidad del UAC. Siga para ello los pasos 27 a 46. Incluya al nuevo grupo de puestos de trabajo creados en lugar del grupo “ENS clientes Windows 10 categoria media” creado en el proceso previo.
83.	Edite el nuevo objeto de GPO “CCN-STIC-599A19 ENS incremental clientes categoria media incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar...” del menú contextual.
84.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”
85.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
86.	Realice las modificaciones oportunas.
87.	Cierre la política.
88.	Para que la nueva política sea efectiva necesita reiniciar los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Debe tener en consideración que, si ha alterado la política de control de cuentas y esta es menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presenten funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

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 GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

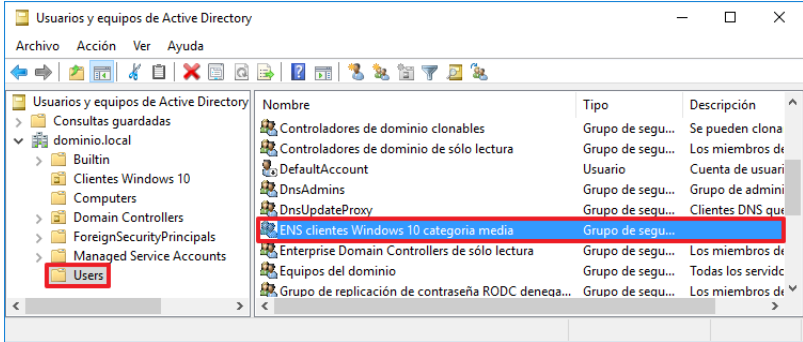
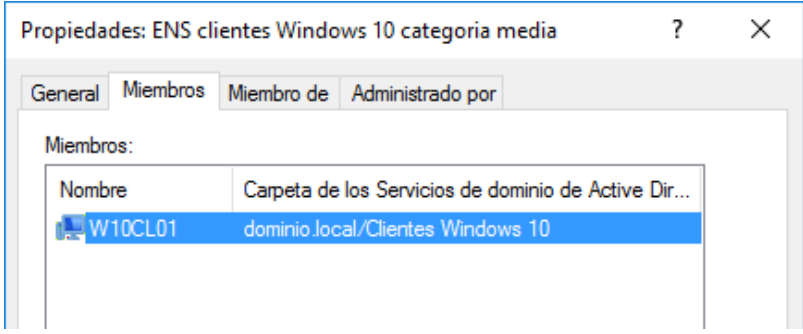
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

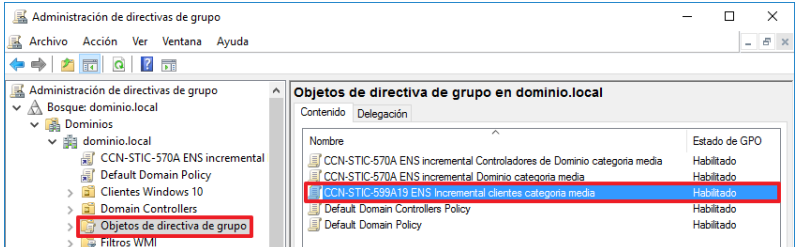
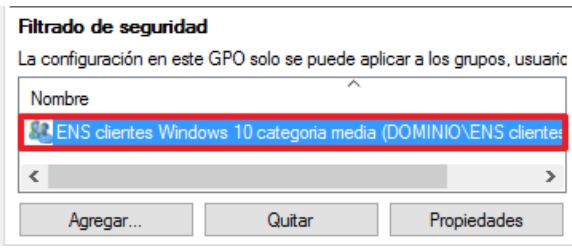
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

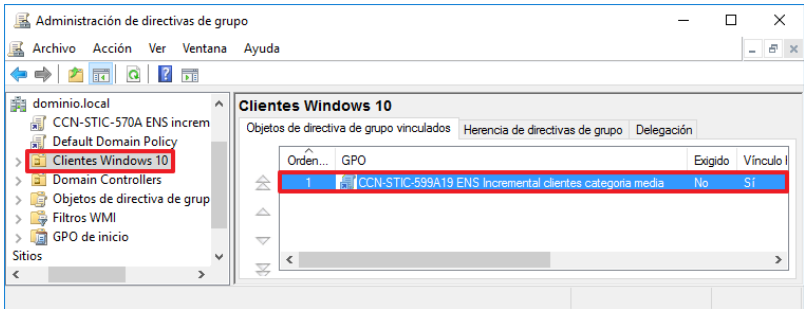
También deberá ejecutar una parte del análisis en los clientes Windows 10 a los que se les haya aplicado la configuración de seguridad de categoría media. En éstos deberá ejecutar la siguiente aplicación.

- a) Conjunto resultante de directivas (rsop.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creado el grupo “ENS clientes Windows 10 categoría media” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory” desde: “Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory”

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione el contenedor “Users”, situada en “[Su dominio] → Users” y a continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS clientes Windows 10 categoria media”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.
3. Verifique que los clientes que han sido catalogados como de categoría de seguridad media, siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS clientes Windows 10 categoria media”.		Pulse doble clic sobre el grupo “ENS clientes Windows 10 categoria media” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los clientes que corresponden a esta categoría de seguridad aparecen en el listado.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.

Comprobación	OK/NOK	Cómo hacerlo						
4. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” ha sido creado y está habilitado.		Ejecute la herramienta “Administrador de directivas de grupo” desde: “Menú inicio → Herramientas administrativas → Administrador de directivas de grupo” Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo” Verifique que está creado el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” y que en la columna “Estado de la GPO” figura como habilitado.  <table border="1"> <thead> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>CCN-STIC-599A19 ENS incremental clientes categoria media</td><td>Habilitado</td><td></td></tr> </tbody> </table>	Directiva	Valor	OK/NOK	CCN-STIC-599A19 ENS incremental clientes categoria media	Habilitado	
Directiva	Valor	OK/NOK						
CCN-STIC-599A19 ENS incremental clientes categoria media	Habilitado							
5. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” tiene definido el Ámbito al grupo “ENS clientes Windows 10 categoría media”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS clientes Windows 10 categoría media”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers” y la GPO se aplica a nivel de dominio.						

Comprobación	OK/NOK	Cómo hacerlo															
6. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” es aplicado a todos aquellos equipos Windows 10 que le son de aplicación las condiciones de categoría media.		Evalúe que la política de seguridad es aplicada en un orden superior a otras políticas aplicables a los puestos de trabajo en todas aquellas ubicaciones donde se encuentren clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría media. En el árbol de la izquierda, seleccione la ubicación donde se encuentren los clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría media: 															
7. Verifique la directiva de contraseñas en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Pulse el botón derecho del ratón y seleccione la opción “Editar...”. Se abrirá el editor de directivas de grupo. Deberá navegar sobre los elementos del árbol de directorios para verificar las distintas configuraciones. Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas” <table border="1"> <thead> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Exigir historial de contraseñas</td><td>24</td><td></td></tr> <tr> <td>Longitud mínima de la contraseña</td><td>10</td><td></td></tr> <tr> <td>Vigencia máxima de la contraseña</td><td>60</td><td></td></tr> <tr> <td>Vigencia mínima de la contraseña</td><td>2</td><td></td></tr> </tbody> </table>	Directiva	Valor	OK/NOK	Exigir historial de contraseñas	24		Longitud mínima de la contraseña	10		Vigencia máxima de la contraseña	60		Vigencia mínima de la contraseña	2	
Directiva	Valor	OK/NOK															
Exigir historial de contraseñas	24																
Longitud mínima de la contraseña	10																
Vigencia máxima de la contraseña	60																
Vigencia mínima de la contraseña	2																

Comprobación	OK/NOK	Cómo hacerlo		
8. Verifique la directiva de bloqueo de cuenta en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de bloqueo de cuenta”		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	60	
		Restablecer el bloqueo de cuenta después de	30	
		Umbral del bloqueo de cuenta	8	
9. Verifique las directivas de auditoría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
10.Verifique la asignación de derechos de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	BUILTIN\Administradores	
		Ajustar las cuotas de la memoria para un proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores	
		Apagar el sistema	BUILTIN\Usuarios, BUILTIN\Administradores	
		Aumentar el espacio de trabajo de un proceso	BUILTIN\Usuarios, NT AUTHORITY\SERVICIO LOCAL, BUILTIN\Administradores	
		Aumentar prioridad de programación	BUILTIN\Administradores	
		Cambiar la hora del sistema	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cambiar la zona horaria	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cargar y descargar controladores de dispositivo	BUILTIN\Administradores	
		Crear objetos compartidos permanentes		
		Crear un archivo de paginación	BUILTIN\Administradores	
		Crear un objeto símbolo (token)		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Crear vínculos simbólicos	BUILTIN\Administradores
		Denegar el acceso a este equipo desde la red	BUILTIN\Invitados, NT AUTHORITY\ANONYMOUS LOGON
		Denegar el inicio de sesión como servicio	BUILTIN\Invitados
		Denegar el inicio de sesión como trabajo por lotes	BUILTIN\Invitados
		Denegar el inicio de sesión local	BUILTIN\Invitados
		Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos
		Depurar programas	BUILTIN\Administradores
		Forzar cierre desde un sistema remoto	BUILTIN\Administradores
		Generar auditorías de seguridad	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red
		Generar perfiles de un solo proceso	BUILTIN\Administradores
		Generar perfiles del rendimiento del sistema	BUILTIN\Administradores
		Habilitar confianza con el equipo y las cuentas de usuario para delegación	
		Hacer copias de seguridad de archivos y directorios	BUILTIN\Administradores
		Iniciar sesión como proceso por lotes	
		Iniciar sesión como servicio	
		Modificar la etiqueta de un objeto	
		Modificar valores de entorno firmware	BUILTIN\Administradores
		Obtener acceso al administrador de credenciales como un llamador de confianza	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Omitir comprobación de recorrido	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores, NT AUTHORITY\Usuarios autenticados	
		Permitir el inicio de sesión local	BUILTIN\Usuarios, BUILTIN\Administradores	
		Permitir inicio de sesión a través de Servicios de Escritorio remoto		
		Realizar tareas de mantenimiento del volumen	BUILTIN\Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red	
		Restaurar archivos y directorios	BUILTIN\Administradores	
		Tener acceso a este equipo desde la red	BUILTIN\Usuarios, BUILTIN\Administradores	
		Tomar posesión de archivos y otros objetos	BUILTIN\Administradores	
11.Verifique las opciones de seguridad en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	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 enumeraciones anónimas de cuentas SAM	Habilitado
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitado
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitado
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitado
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitado
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitado
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitado
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitado
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitado
		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

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		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	Habilitado
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitado
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Deshabilitado
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitado
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitado
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitado
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitado
		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.
		Cuentas: estado de la cuenta de invitado	Deshabilitado
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitado
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitado
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitado
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		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	Habilitado
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitado
		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	Habilitado
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitado
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitado
		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)	Habilitado
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitado
		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	Habilitado
		Seguridad de red: requisitos de firma de cliente LDAP	Negociar firma
		Servidor de red Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado
		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
12.Verifique el registro de eventos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro de seguridad	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro del sistema	Habilitado	
13.Verifique los servicios del sistema definidos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema” Nota: 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 para cada servicio. En la ventana del editor de administración de directivas de grupo 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	
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	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	
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	
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
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
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
CDPUserService	CDPUserService	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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
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
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
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	Wecevc	Manual	Configurado

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	
Redirector de puerto en modo usuario de Servicios de Escritorio remoto	UmRdpService	Manual	Configurado	
Registrador de configuración de Windows Connect Now	wcncsvc	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	
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
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
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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
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
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
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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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	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
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Manual	Configurado
Servicio PushToInstall de Windows	PushToInstall	Manual	Configurado

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	
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	
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	

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
14.Verifique los valores del sistema de archivos en el objeto de directiva de grupo "CCN-STIC-599A19 ENS incremental clientes categoria media".		Seleccione el siguiente nodo. "Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos" Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".	
Archivo	Usuario	Permiso	OK/NOK
%ProgramFiles%\Netmeeting	Administradores	Control total	
	SYSTEM	Control total	
%Public%\	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\rasctrs.dll		Administradores	Control total	
%SystemRoot%\system32\rasctrs.ini		Administradores	Control total	
%SystemRoot%\system32\rasdiag.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\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	
15.Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
16.Verifique la directiva de almacén digital en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Almacén digital”		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el almacén digital	Habilitado	
17.Verifique la directiva de Antivirus en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitado	
18.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	
19.Verifique las directivas de biometría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
20.Verifique la directiva de inicio de sesión de red en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
21.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
22.Verifique las directivas de reproducción automática en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar reproducción automática	Habilitado (Todas las unidades)	
		Establece el comportamiento predeterminado para la ejecución automática	Habilitado (No ejecutar ningún comando de ejecución automática)	

Comprobación	OK/NOK	Cómo hacerlo		
23.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar Windows SmartScreen de Windows defender	Habilitado (Advertir e impedir la omisión)	
24.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
25.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
26.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de Internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
27.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
28.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
29.Verifique las directivas de OneDrive en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	
30.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”		
		Directiva	Valor	OK/NOK

Comprobación	OK/NOK	Cómo hacerlo		
		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	Deshabilitado	
31.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitado (Solo HTTP (0))	
32.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	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 accedan a la información de diagnóstico sobre otras aplicaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la información de la cuenta	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	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 controlen las radios	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)

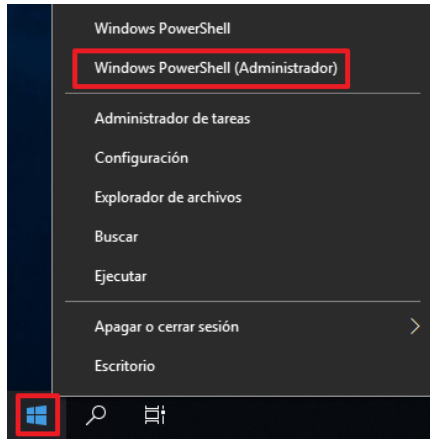
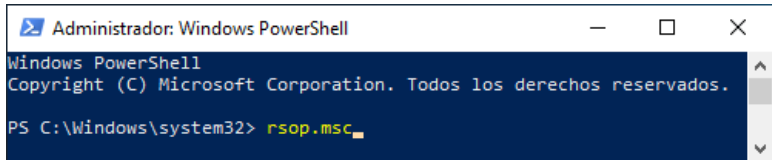
Comprobación	OK/NOK	Cómo hacerlo		
33.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Recopilación de datos a versiones preliminares”		
		Directiva	Valor	OK/NOK
		No volver a mostrar notificaciones de comentarios	Habilitado	
		Permitir telemetría	Habilitado	
34.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”		
		Directiva	Valor	OK/NOK
		Permitir acceso a Shell remoto	Deshabilitado	

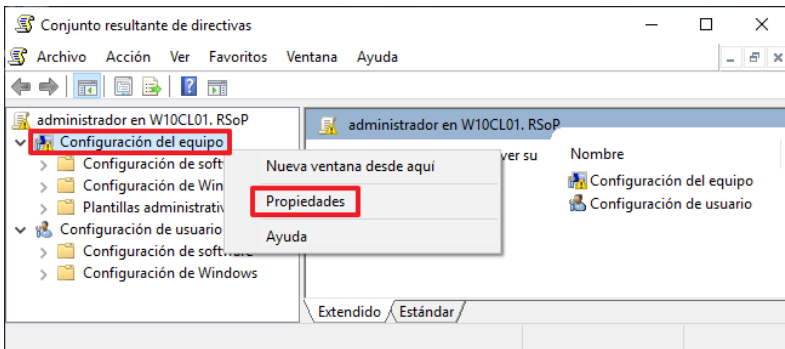
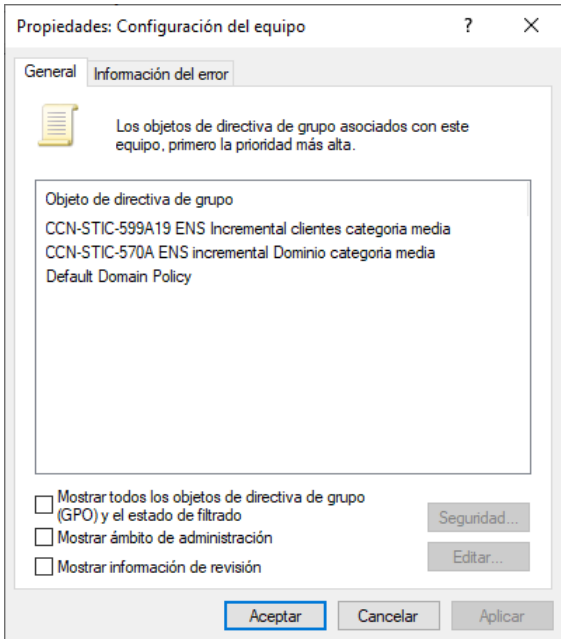
Comprobación	OK/NOK	Cómo hacerlo		
35.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Explorador”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Habilitado (Advertir e impedir la omisión)	
36.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
37.Verifique la directiva de Tienda en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	Desactivar la aplicación Store		Habilitado	
	Deshabilita todas las aplicaciones de Microsoft Store		Deshabilitado	
38.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Ubicación y Sensores”		
	Directiva		Valor	OK/NOK
	Desactivar scripting de ubicación		Habilitado	
	Desactivar sensores		Habilitado	
	Desactivar ubicación		Habilitado	
39.Verifique la directiva de Windows Update en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
	Directiva		Valor	OK/NOK
	Administrar preliminares		Habilitado (Deshabilitar preliminares)	

Comprobación	OK/NOK	Cómo hacerlo		
40.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano”		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitado	
41.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoría media”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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 la 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	
42.Verifique la directiva de Net Logon en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Net Logon”			
	Directiva		Valor	OK/NOK
	Permitir algoritmos de criptografía compatibles con Windows NT 4.0		Deshabilitado	
43.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental clientes categoria media”.	Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Perfiles de usuario”			

Comprobación	OK/NOK	Cómo hacerlo		
		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)	
		Desactivar el identificador de publicidad	Habilitado	
44. Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador.		Inicie sesión en el equipo cliente que está comprobando con una cuenta de usuario de Windows con permisos de administrador.		
45. 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. 		
46. Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse "Enter" para abrir la consola de administración "Conjunto resultante de directivas": 		

Comprobación	OK/NOK	Cómo hacerlo
47.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 ENS incremental clientes categoria media".		En la consola de administración "Conjunto resultante de directivas, seleccione el contenedor "Configuración del equipo", márkuelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las políticas deberán aparecer y "CCN-STIC-599A19 ENS incremental clientes categoria media" deberá estar situada encima de la GPO que se establece a nivel de dominio, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 ENS incremental clientes categoria media" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

ANEXO C.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO C.3.1. GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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.

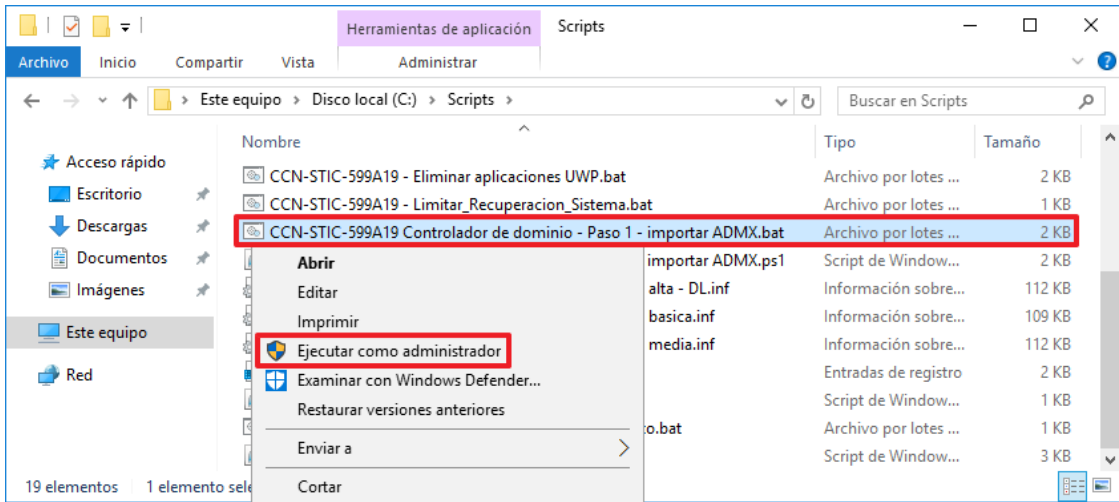
1. PREPARACIÓN DEL DOMINIO

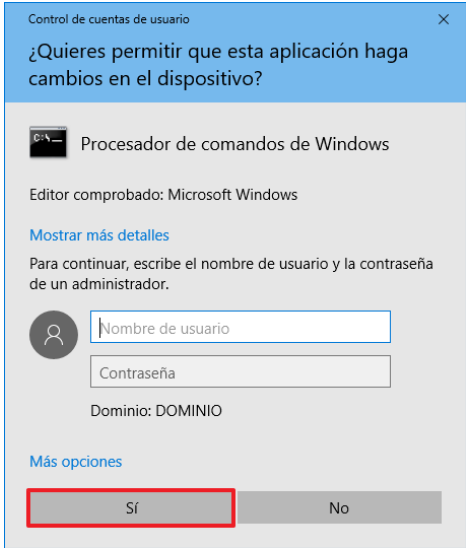
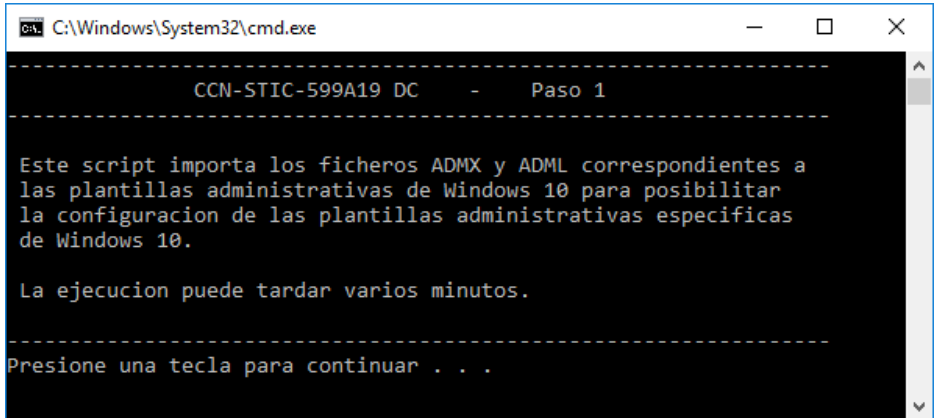
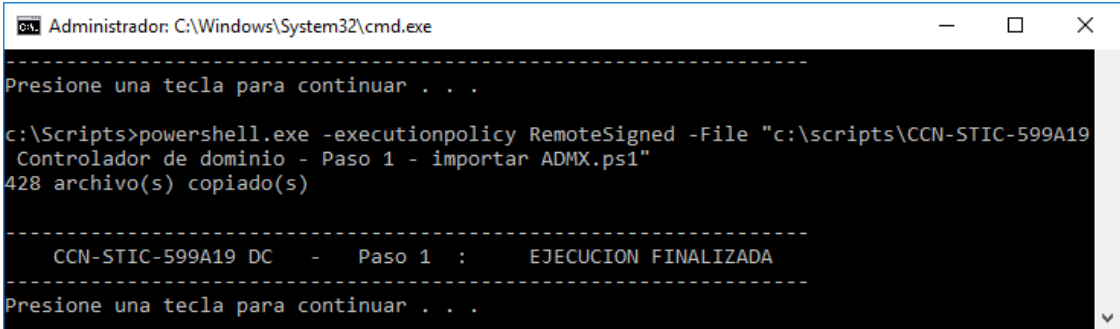
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

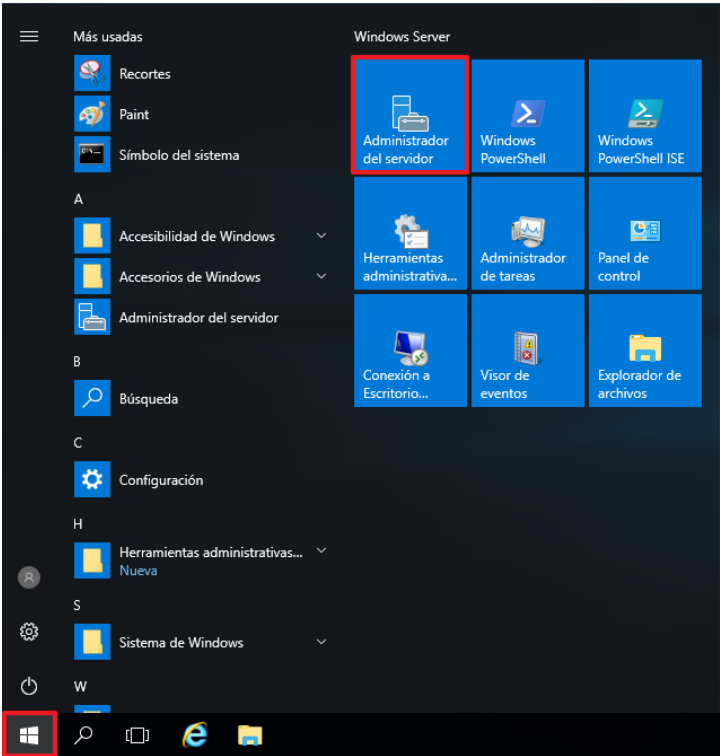
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Si no es así, aplique la guía correspondiente al controlador de dominio, antes de continuar con la aplicación de ésta.

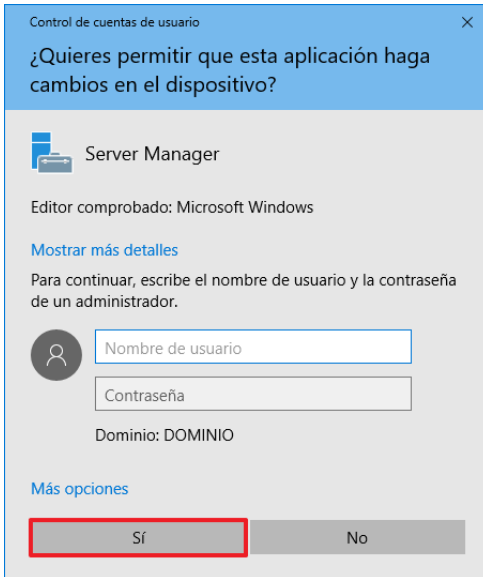
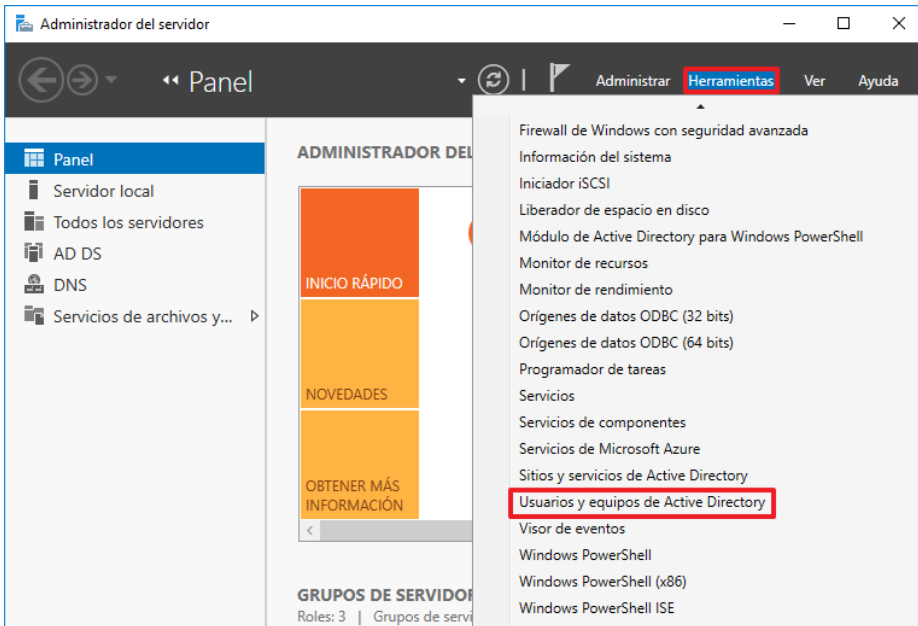
En el ejemplo, las configuraciones y capturas de pantalla han sido realizadas sobre un controlador de dominio al que se le ha instalado Windows Server 2016 y aplicado la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016.

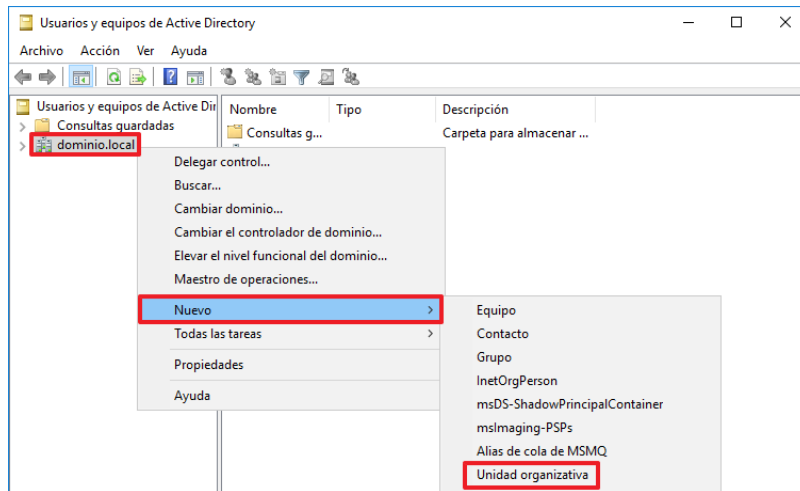
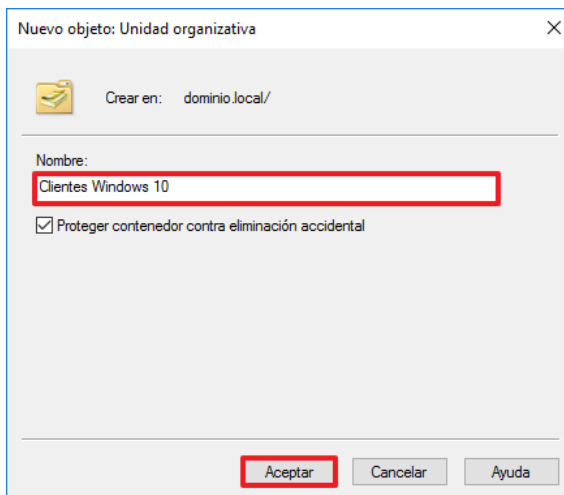
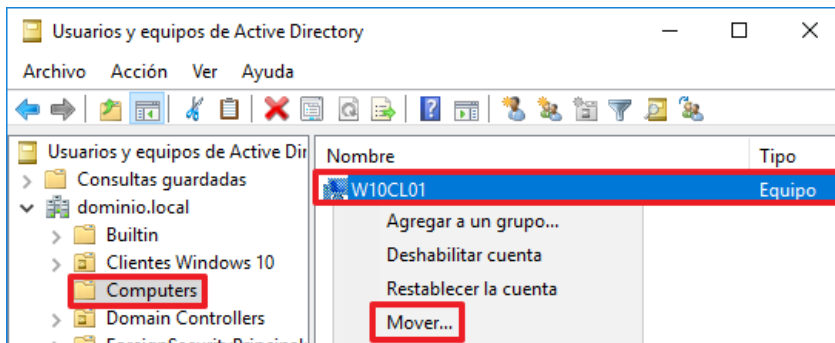
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.

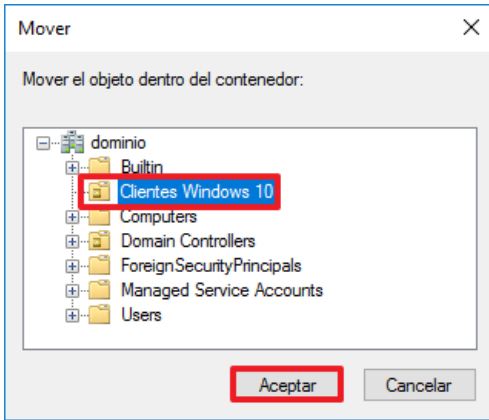
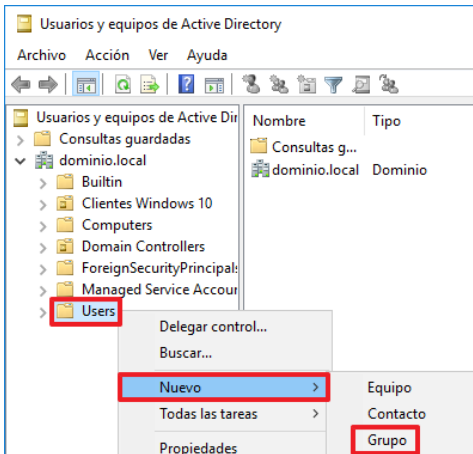
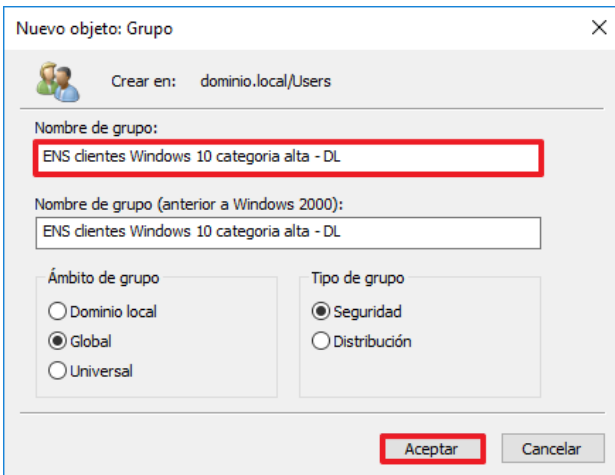
Paso	Descripción
4.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio. Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".
5.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-599A19 ENS clientes categoria alta - DL (directorio) – CCN-STIC-599A19 ENS clientes categoria media (directorio) – CCN-STIC-599A19 ENS clientes categoria basica (directorio) – CCN-STIC-599A19 ENS Incremental portátiles categoria alta - DL - Bitlocker (directorio) – CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL.inf – CCN-STIC-599A19 ENS Incremental clientes categoria media.inf – CCN-STIC-599A19 ENS Incremental clientes categoria basica.inf – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1 – PolicyDefinitions - (directorio)
6.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

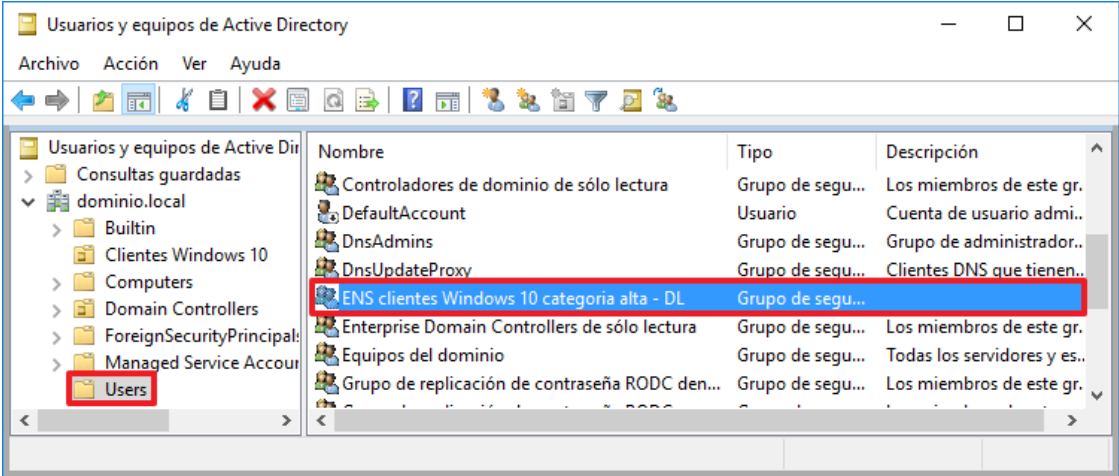
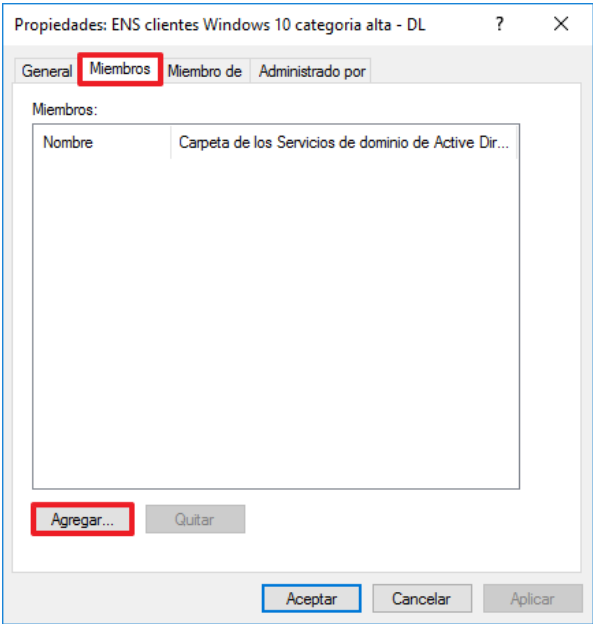
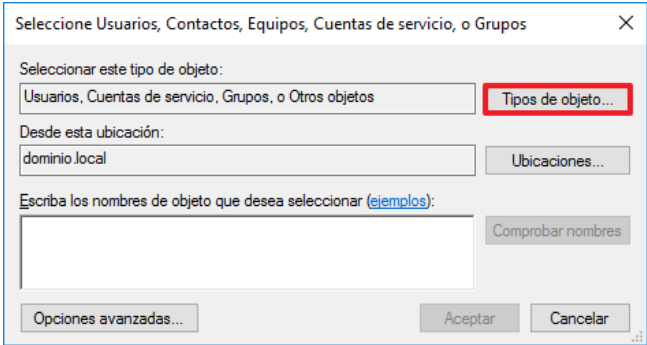
Paso	Descripción
7.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
8.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
9.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 

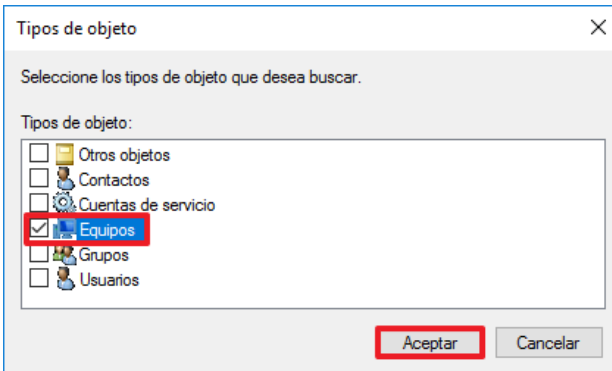
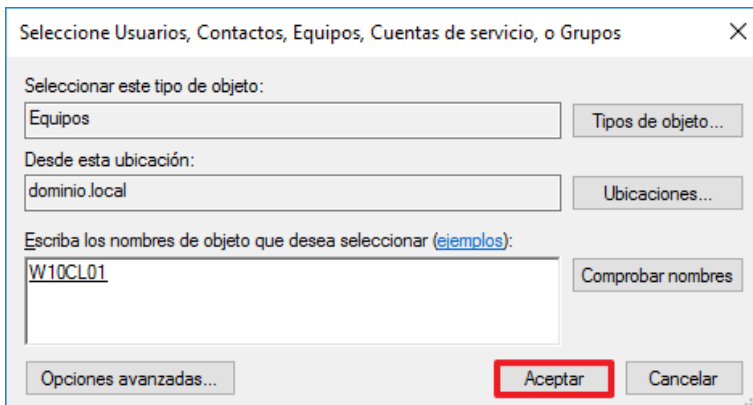
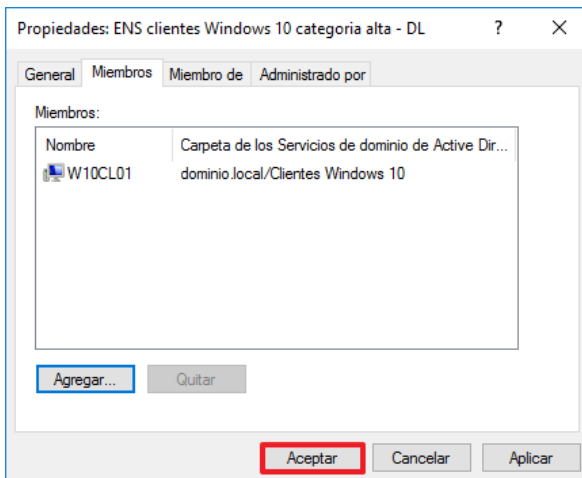
Paso	Descripción
10.	Copie el fichero “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL.inf”, almacenado en la carpeta “C:\Scripts”, al directorio “C:\Windows\Security\Templates” del Controlador de Dominio. Nota: Los siguientes pasos describen el procedimiento para crear un grupo de seguridad donde agregar los puestos de trabajo que le sean de aplicación la categoría media de seguridad según los criterios definidos del ENS. En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá también crear el grupo debido a que la política deberá aplicarse a nivel de dominio y se asignará exclusivamente a los puestos de trabajo por la pertenencia a este grupo. Si todos los equipos de la organización presentan la misma categoría media no hace falta la creación de dicho grupo y puede saltar al paso 27. Si por el contrario van a existir puestos de trabajo Windows 10 con categorías básica o media, deberá crear dicho grupo de tal forma que la aplicación de políticas de seguridad en función de las categorías se aplique atendiendo a los criterios de pertenencia a grupo.
11.	Inicie la herramienta de “Usuarios y equipos de Active Directory”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

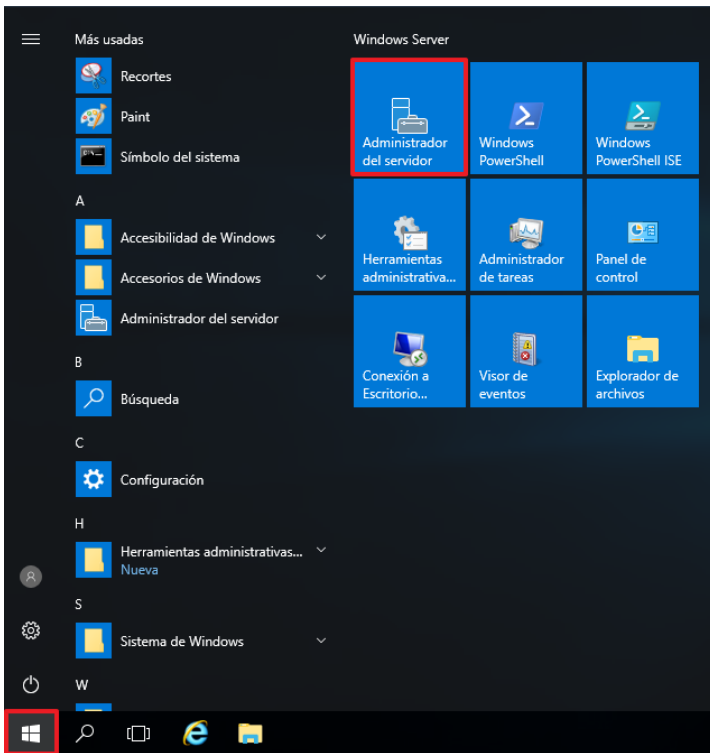
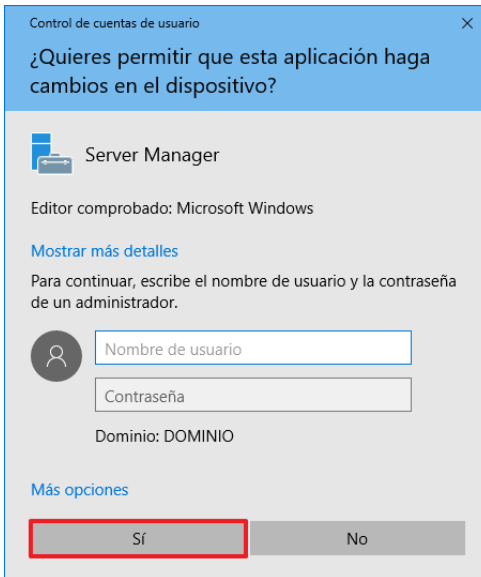
Paso	Descripción
12.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
13.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 

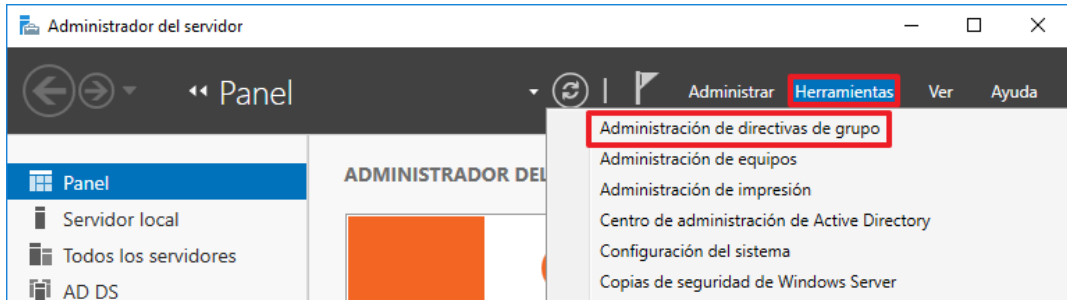
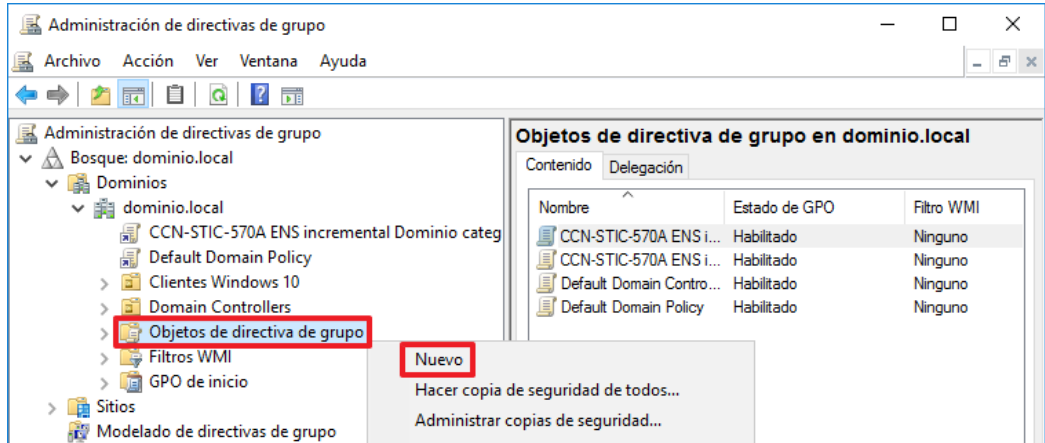
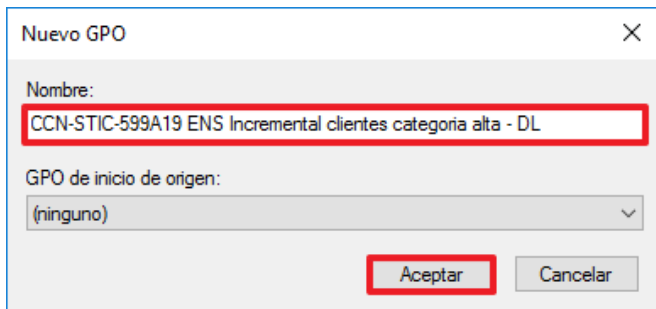
Paso	Descripción
14.	Pulse son el botón derecho sobre el dominio y seleccione “Nuevo → Unidad organizativa”. 
15.	Establezca el nombre para la unidad organizativa con los clientes Windows 10 y pulse “Aceptar”. 
16.	Vaya a las unidades organizativas donde se encuentren los clientes que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover...” en cada uno de ellos.  Nota: En este ejemplo se encuentra bajo la unidad organizativa “Computers”.

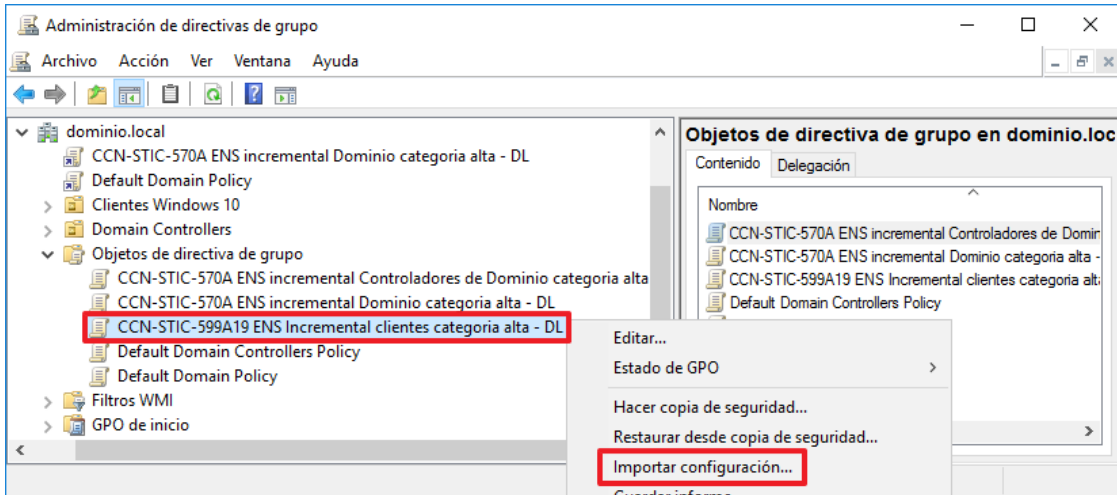
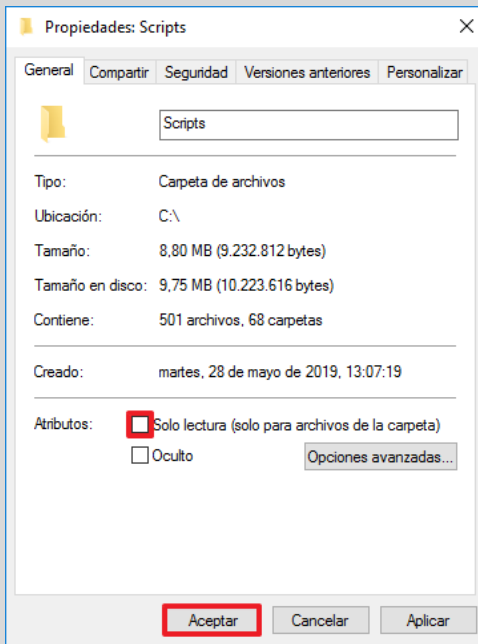
Paso	Descripción
17.	Seleccione la unidad organizativa “Clientes Windows 10” creada anteriormente y pulse “Aceptar”. 
18.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
19.	Introduzca como nombre “ENS clientes Windows 10 categoría media - DL”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio. 

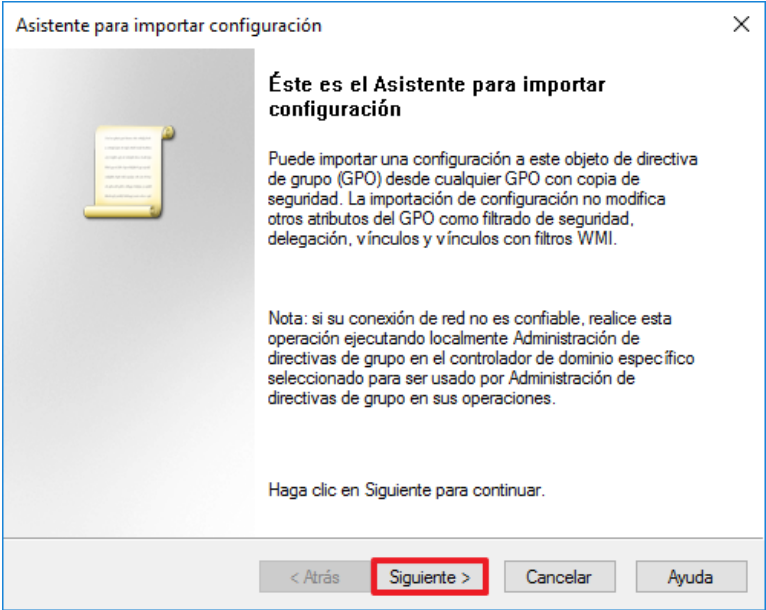
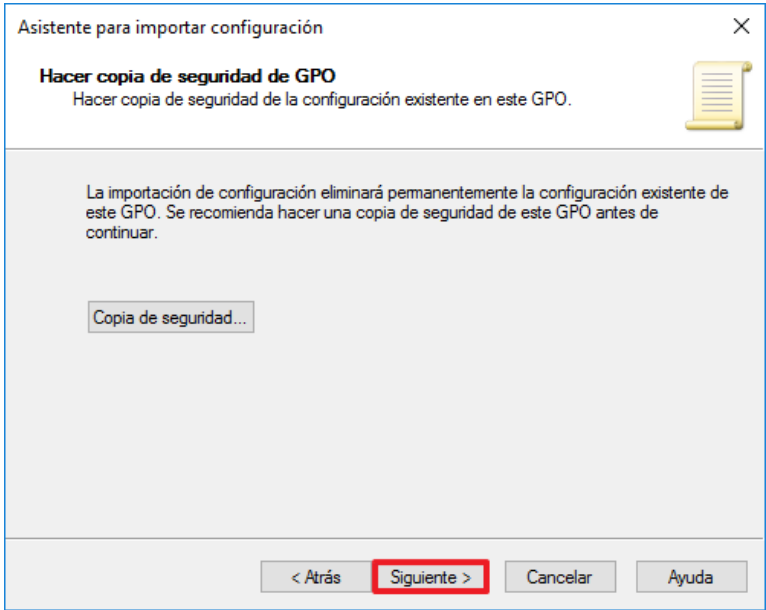
Paso	Descripción
20.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
21.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar...”. 
22.	Pulse el botón de “Tipos de objeto...”. 

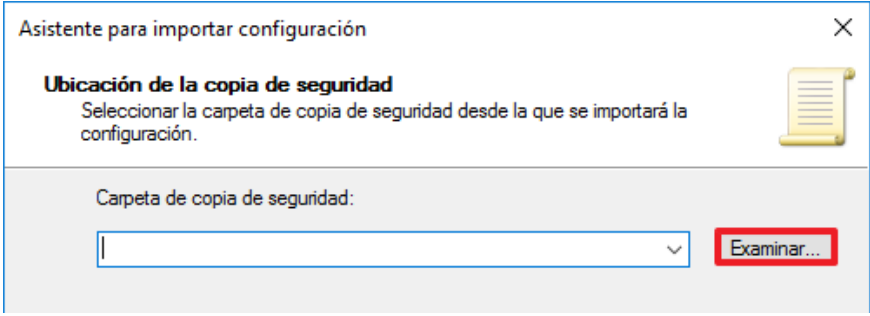
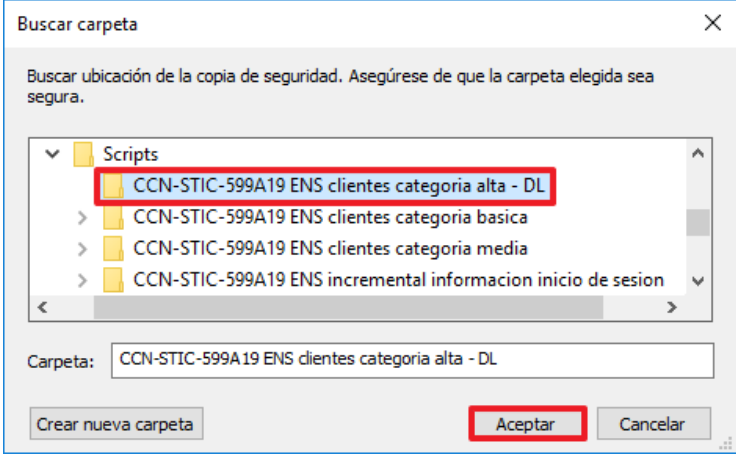
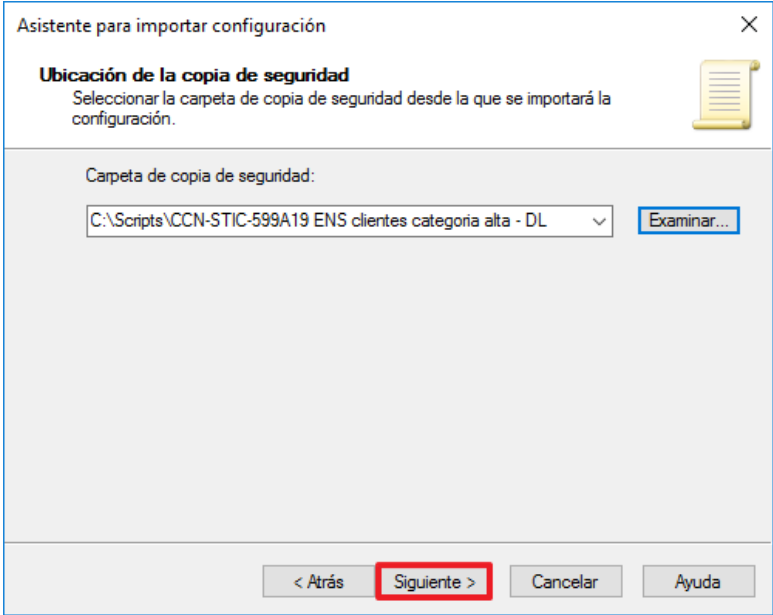
Paso	Descripción
23.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
24.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad alta / Difusión Limitada y pulse “Aceptar” para agregar la selección.  Nota: No agregue servidores a este grupo.
25.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
26.	Cierre la herramienta “Usuarios y equipos e Directorio Activo”.

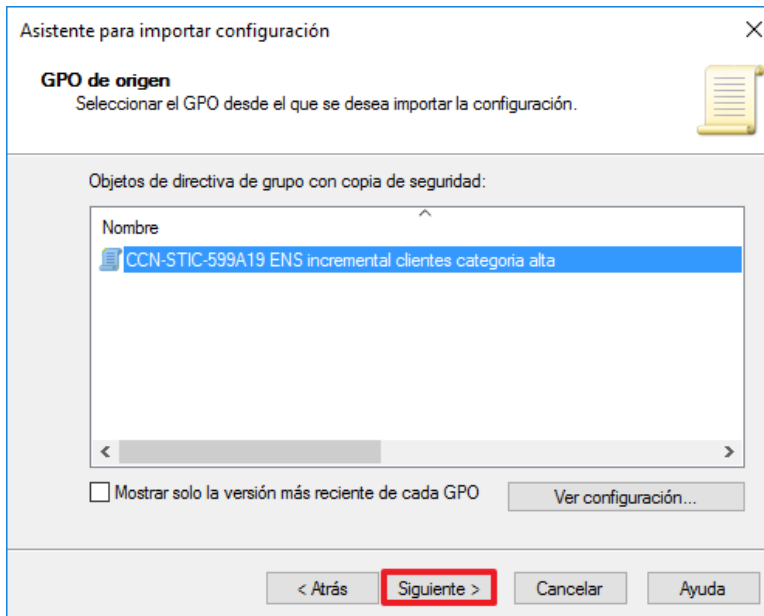
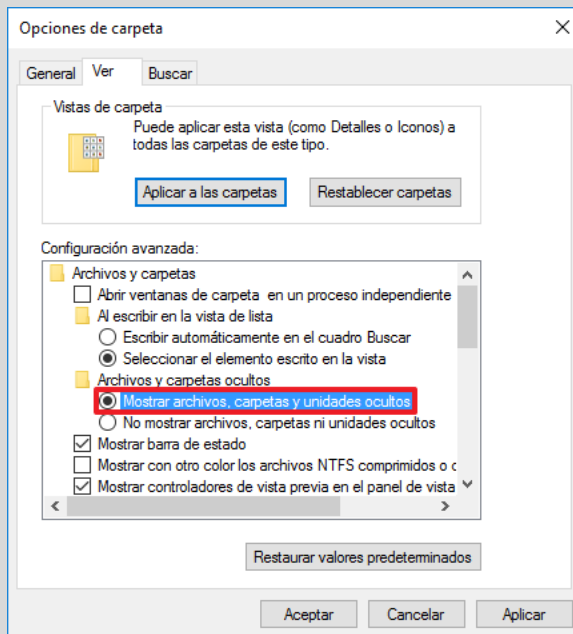
Paso	Descripción
27.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
28.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 

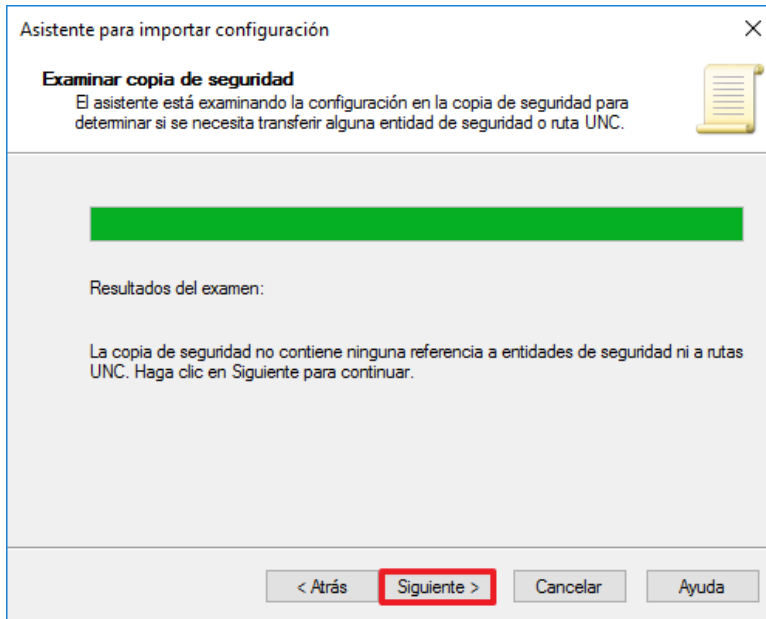
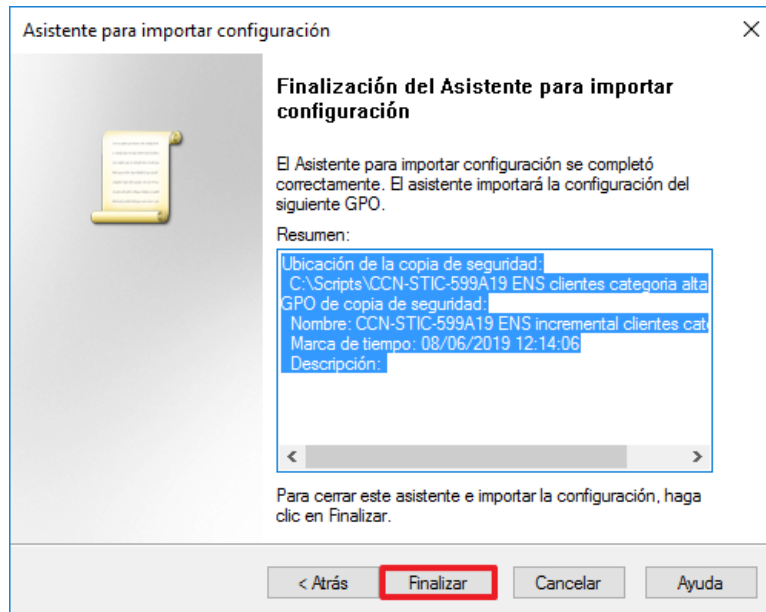
Paso	Descripción															
29.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 															
30.	Despliegue los contenedores pertenecientes a su dominio y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”.  <table><thead><tr><th>Nombre</th><th>Estado de GPO</th><th>Filtro WMI</th></tr></thead><tbody><tr><td>CCN-STIC-570A ENS incremental Dominio categ</td><td>Habilitado</td><td>Ninguno</td></tr><tr><td>CCN-STIC-570A ENS i...</td><td>Habilitado</td><td>Ninguno</td></tr><tr><td>Default Domain Contro...</td><td>Habilitado</td><td>Ninguno</td></tr><tr><td>Default Domain Policy</td><td>Habilitado</td><td>Ninguno</td></tr></tbody></table>	Nombre	Estado de GPO	Filtro WMI	CCN-STIC-570A ENS incremental Dominio categ	Habilitado	Ninguno	CCN-STIC-570A ENS i...	Habilitado	Ninguno	Default Domain Contro...	Habilitado	Ninguno	Default Domain Policy	Habilitado	Ninguno
Nombre	Estado de GPO	Filtro WMI														
CCN-STIC-570A ENS incremental Dominio categ	Habilitado	Ninguno														
CCN-STIC-570A ENS i...	Habilitado	Ninguno														
Default Domain Contro...	Habilitado	Ninguno														
Default Domain Policy	Habilitado	Ninguno														
31.	Introduzca como nombre “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” y pulse el botón “Aceptar”. 															

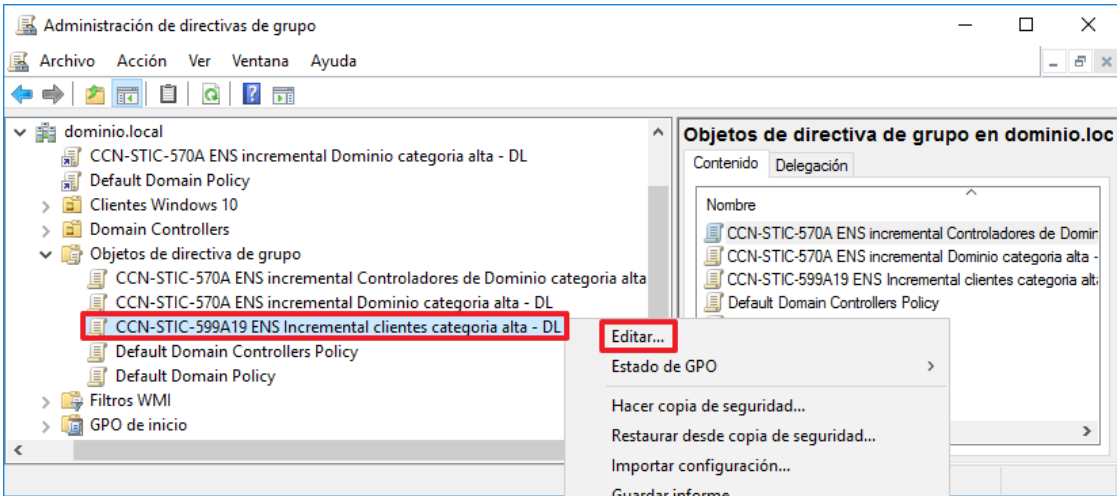
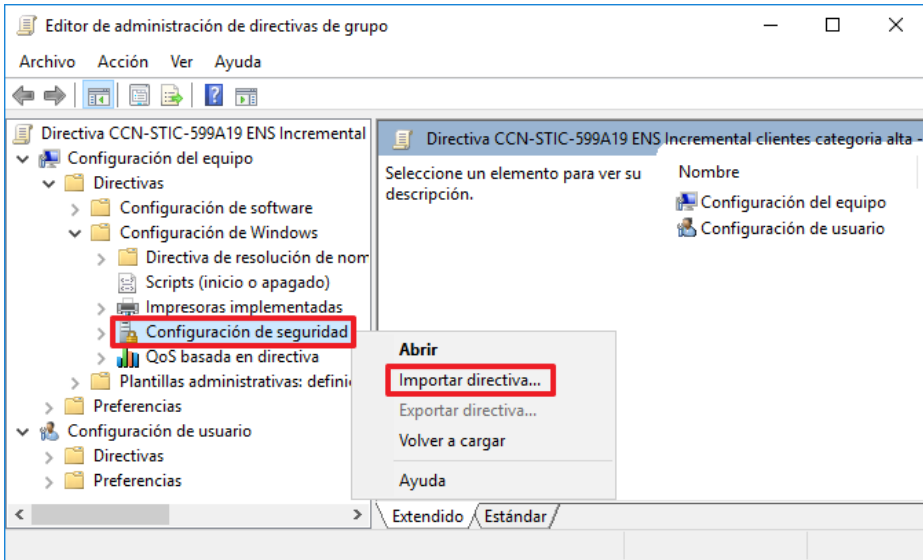
Paso	Descripción
32.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política con el botón derecho del ratón y seleccione la opción “Importar configuración...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts”, así como los archivos dentro de sus subcarpetas, no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

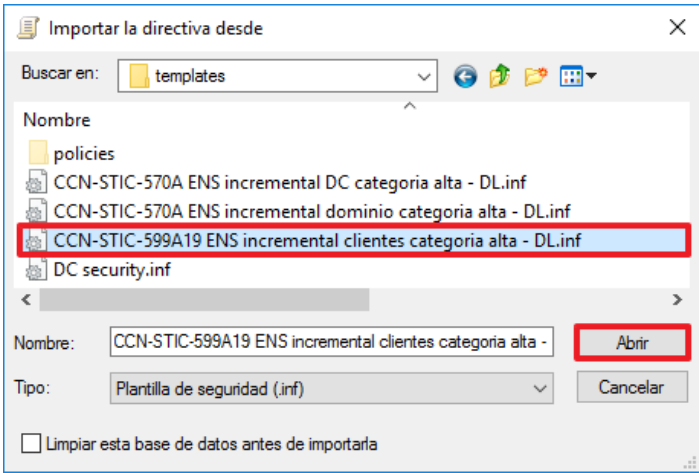
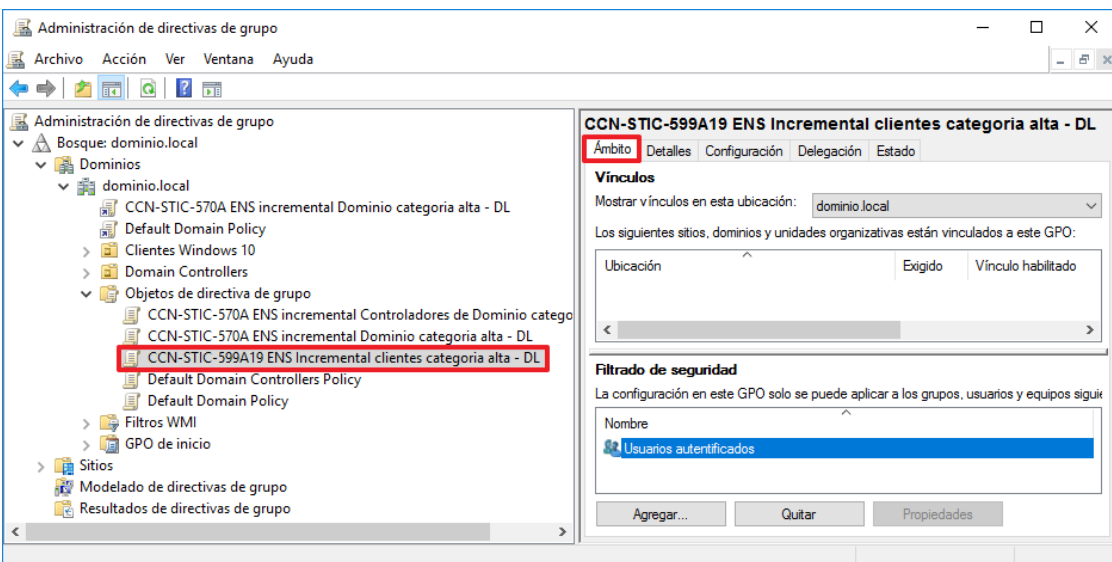
Paso	Descripción
33.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
34.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

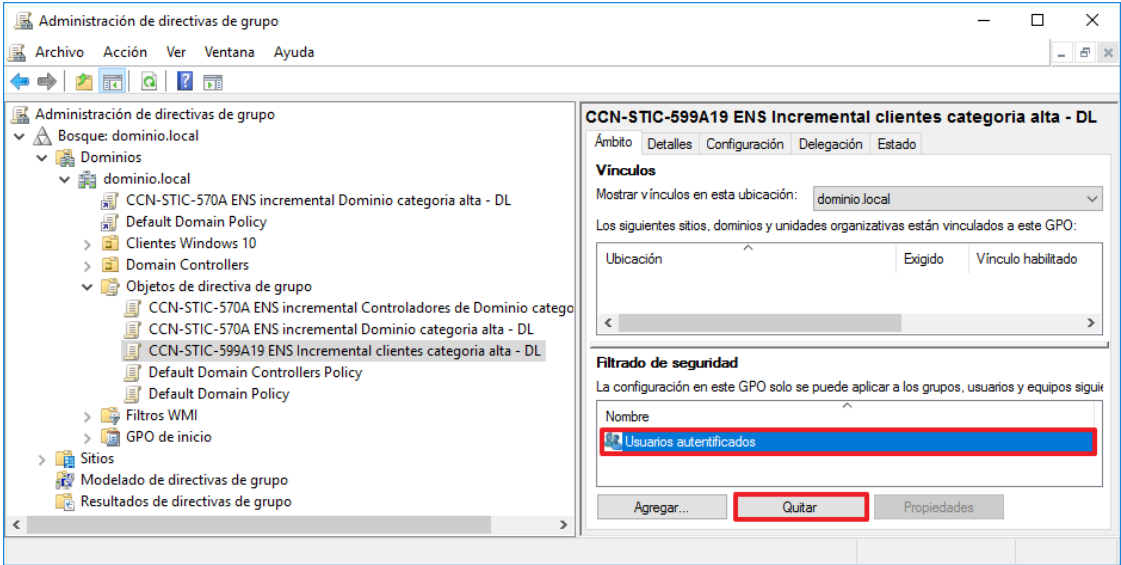
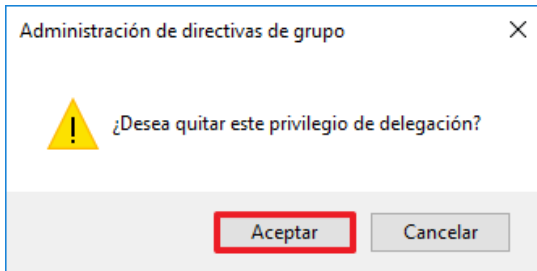
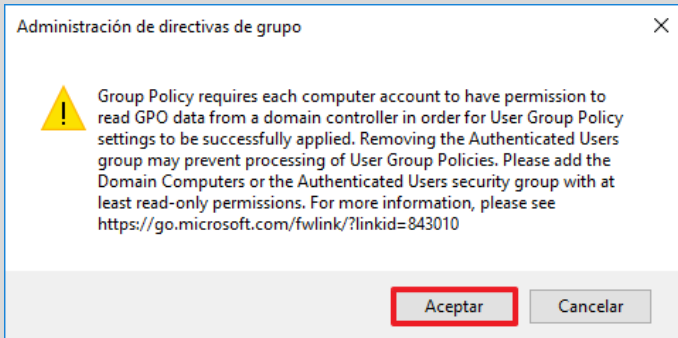
Paso	Descripción
35.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
36.	Seleccione la carpeta “CCN-STIC-599A19 ENS clientes categoria alta - DL” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
37.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

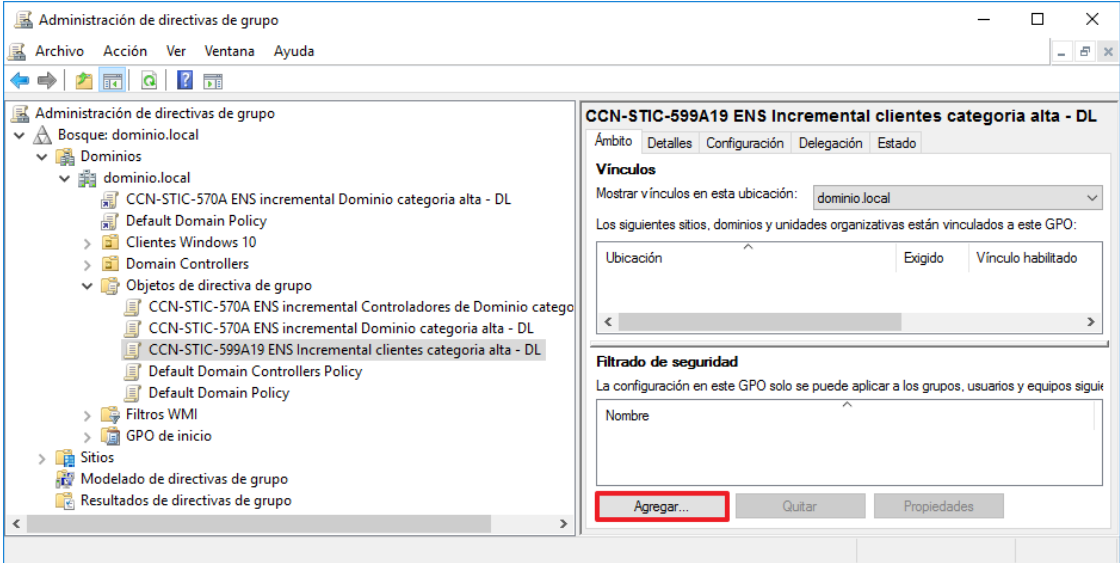
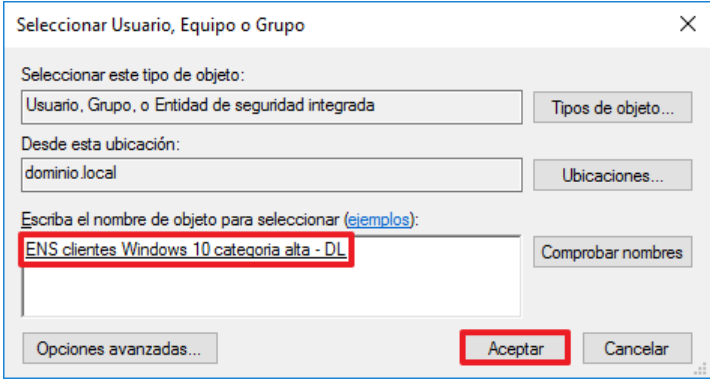
Paso	Descripción
38.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental clientes categoria alta – DL” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
39.	En la pantalla de examen, pulse el botón “Siguiente >”. 
40.	Para completar el asistente pulse el botón “Finalizar”. 
41.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.

Paso	Descripción
42.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
43.	Una vez pulsada la opción “Editar...” se abre una ventana de “Editor de administración de directivas de grupo”. Despliegue el objeto de directiva de grupo y sitúe el cursor sobre el nodo Configuración de seguridad. “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”
44.	Pulse con el botón derecho en configuración de seguridad y seleccione la opción “Importar directiva...”. 

Paso	Descripción
45.	Seleccione el fichero “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL.inf” ubicado en la ruta “C:\Windows\Security\Templates” y pulse el botón “Abrir”. 
46.	Cierre la política una vez se haya realizado la importación de la configuración de seguridad. Nota: Los siguientes pasos describen el procedimiento para asignar la política al grupo de seguridad creado en los pasos 18 a 25. Si usted creó el grupo puesto que va a tener aplicadas diferentes categorías de seguridad en la organización para los puestos de trabajo, siga con el siguiente paso. Si no creo dicho grupo, diríjase al paso 52.
47.	Seleccione la nueva política de grupo configurada y vaya a las opciones de ámbito que se encuentran en el panel derecho. 

Paso	Descripción
48.	En el apartado “Filtrado de seguridad”, seleccione “Usuarios autenticados” y pulse el botón “Quitar”. 
49.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
50.	Pulse ahora sobre el botón “Agregar...”. 
51.	Introduzca como nombre “ENS clientes Windows 10 categoria alta - DL”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse el botón “Aceptar”. 
52.	La política se encuentra ya creada correctamente. No obstante, no se aplicarán hasta más adelante, una vez que haya tenido en cuenta y aplicado todas las consideraciones adicionales que se mostrarán en el siguiente punto del presente Anexo.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

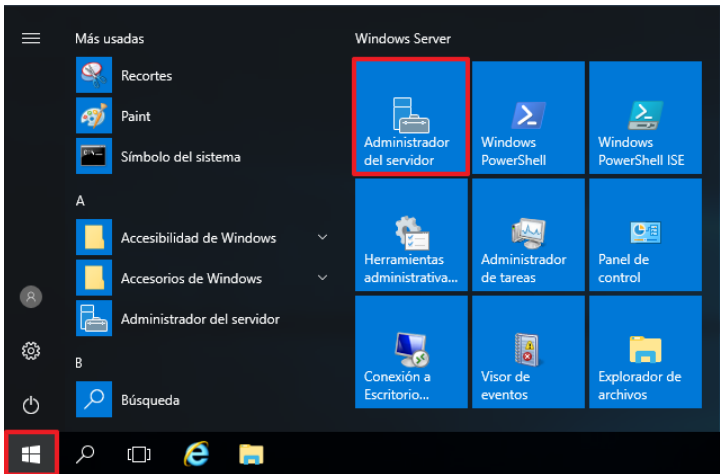
El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y por lo tanto deben valorarse con respecto a la aplicación de la presente configuración. La plantilla de seguridad que se ha configurado tiene en consideración los puntos tratados en el Esquema Nacional de seguridad para la categoría alta / Difusión Limitada. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina, como por ejemplo lo relativo al uso de privilegios.

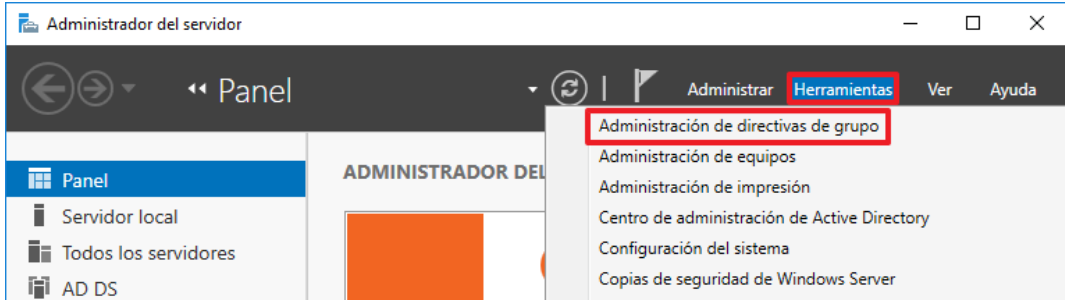
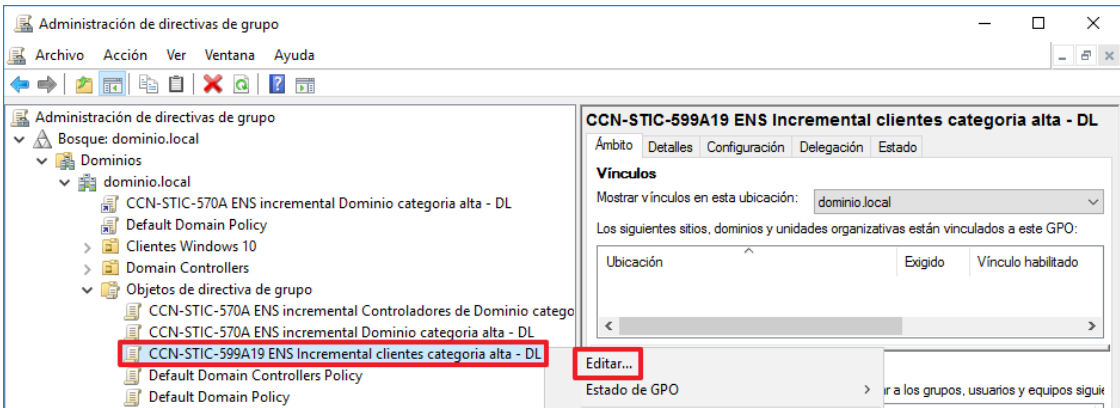
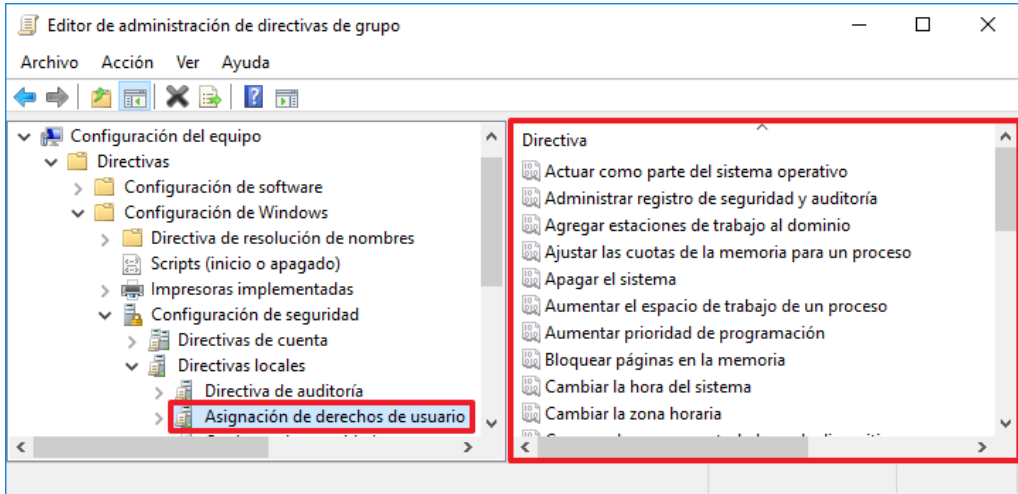
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

Los objetos de políticas de grupo para puestos de trabajo especifican unos derechos de usuario siguiendo planteamientos de seguridad siguiendo los principios de mínimos privilegios 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 el objeto de política creado en el punto previo.

2.1. ASIGNACIÓN DE DERECHOS DE USUARIO

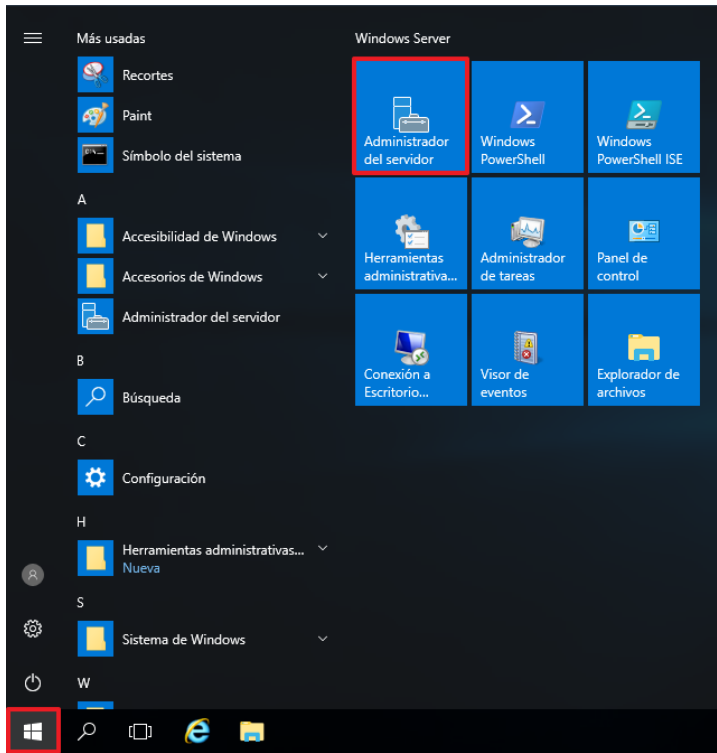
Paso	Descripción
53.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
54.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
55.	Edite la política de grupo correspondiente. Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

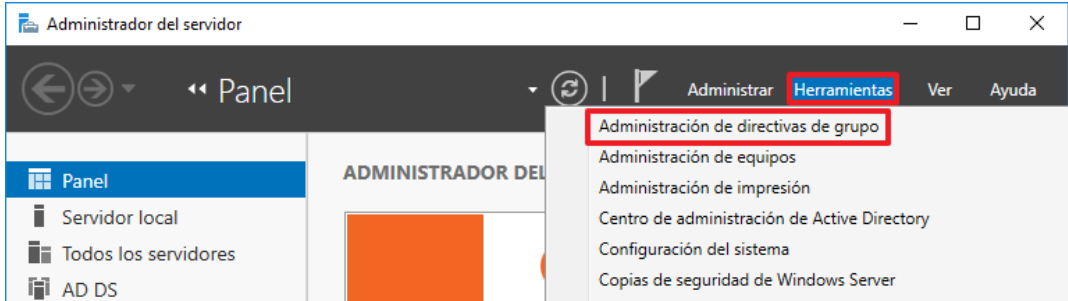
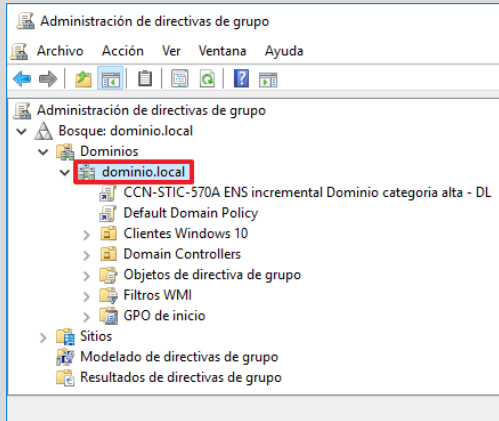
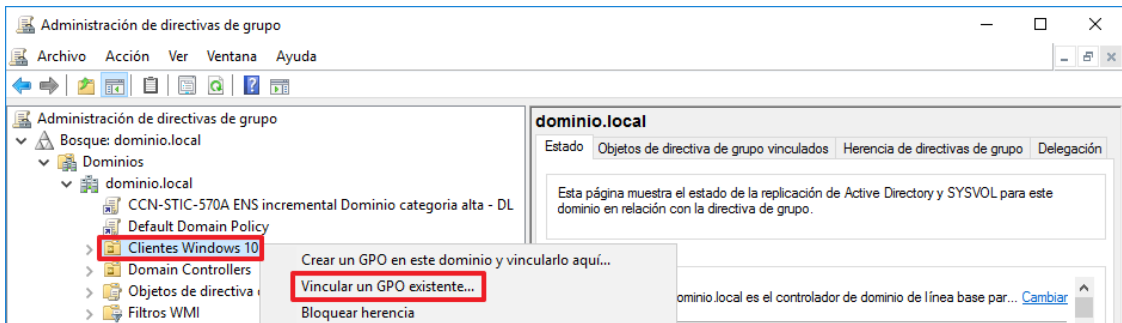
Paso	Descripción
56.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio.
57.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
58.	Seleccione la política creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
59.	Despliegue la política y sitúese en la siguiente ruta: “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario” 

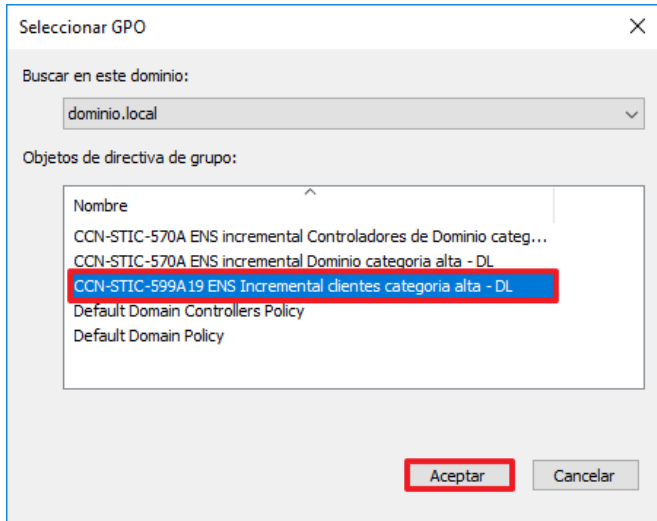
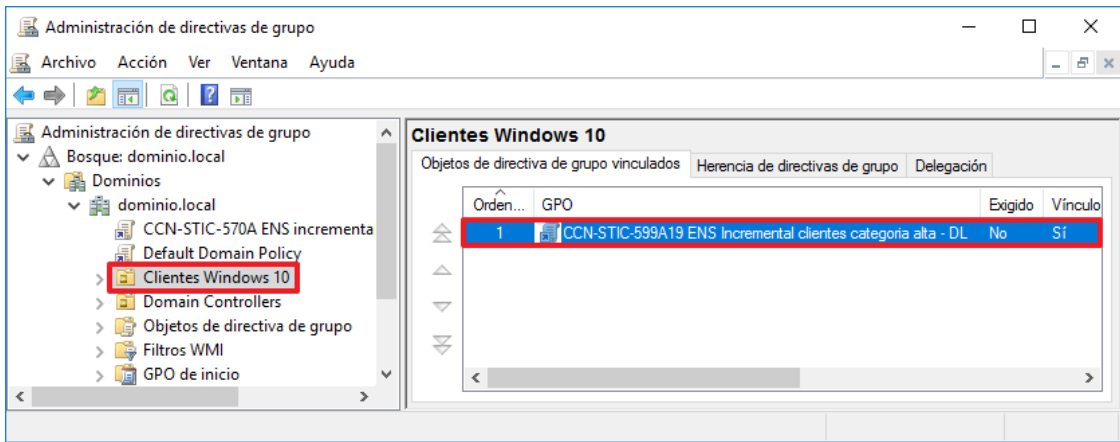
Paso	Descripción
60.	Modifique las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales.
61.	Guarde la configuración cerrando la ventana del editor de administración de directivas de grupo.

3. IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD

El presente punto establece la aplicación de las políticas de seguridad, una vez que se han tenido en consideración las condiciones definidas en el punto previo.

Paso	Descripción
62.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
63.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
64.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
65.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio.

Paso	Descripción
66.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
67.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es “dominio.local”.
68.	Identifique las ubicaciones donde se encuentran los Clientes Windows 10 que les son de aplicación las condiciones de seguridad de categoría alta, según estipula el ENS. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” que es donde se encuentran ubicados los clientes existentes en este escenario. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminada de “computers” y no los ha movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 
69.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente y seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción								
70.	Seleccione la política “CCN-STIC-599A19 ENS Incremental categoria alta - DL” y pulse el botón “Aceptar”. 								
71.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental clientes categoria alta - DL” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dichas Unidades Organizativas.  <table><thead><tr><th>Orden...</th><th>GPO</th><th>Exigido</th><th>Vínculo</th></tr></thead><tbody><tr><td>1</td><td>CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL</td><td>No</td><td>Sí</td></tr></tbody></table>	Orden...	GPO	Exigido	Vínculo	1	CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL	No	Sí
Orden...	GPO	Exigido	Vínculo						
1	CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL	No	Sí						
72.	Cierre la herramienta “Administración de directivas de grupo”.								
73.	Elimine la carpeta “C:\scripts”.								
74.	Para que la nueva política sea efectiva necesita reiniciar el o los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Tenga en consideración que la edición “Pro” de Windows 10 no permite realizar un bloqueo de la Tienda a través de directivas de grupo por lo que deberá hacer uso de AppLocker para realizar el bloqueo de uso. Consulte el documento de seguridad codificado como “CCN-STIC-869 AppLocker en el ENS”.								

4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD

Las configuraciones planteadas a través de la presente guía han sido ampliamente probadas en entornos de operativa Microsoft. No obstante, no se han podido probar todas las condiciones existentes, ni con las peculiaridades de cada organización. Es posible que bajo determinadas condiciones pudieran suceder algunas incidencias que se describen a continuación, así como su resolución.

Debe tenerse en consideración que la resolución consiste en rebajar algunos de los mecanismos de seguridad descritos en la presente guía. Por lo tanto, deberá tener en consideración la problemática y ofrecer una solución que permita recuperar el estado de seguridad deseado y recomendado por la presente guía.

El control de cuentas de usuario surge en Windows Vista como respuesta para limitar las acciones de los administradores cuando actuaban con cuentas privilegiadas ante acciones que no requieren dicho privilegio. En sistemas previos a Windows Vista, un administrador que había iniciado una sesión actuaba siempre con los máximos privilegios, independientemente de que estuviera abriendo un fichero ofimático o estuviera navegando por internet. Puesto que el riesgo era bastante elevado Microsoft propone como solución UAC con objeto de advertir a los administradores cuando una acción requería privilegio para actuar.

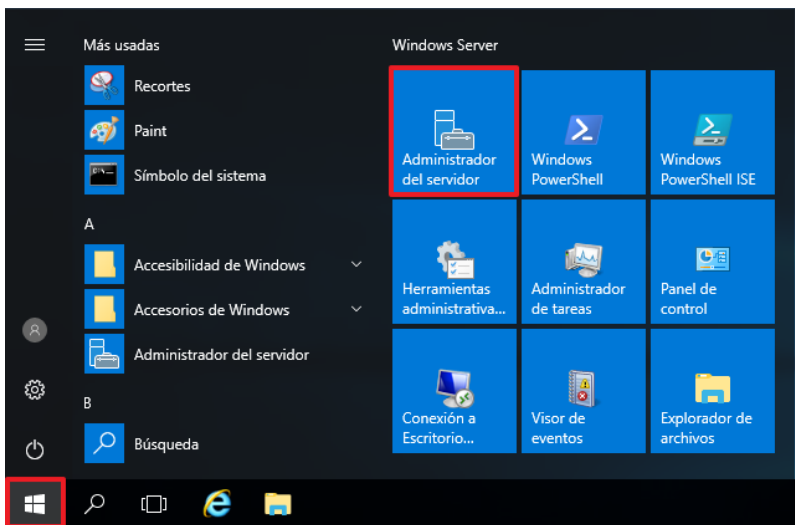
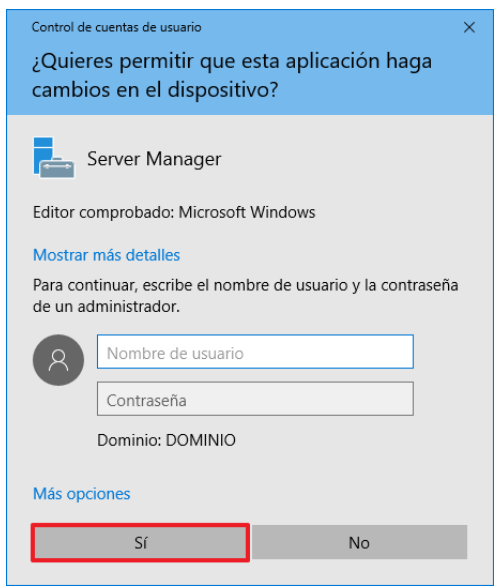
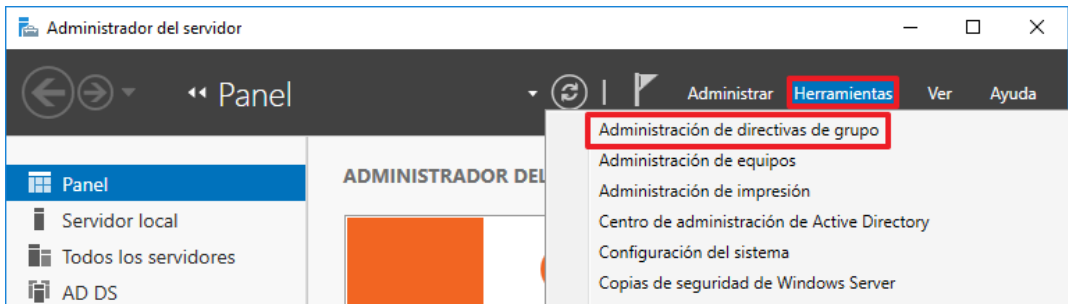
Siguiendo el principio de menor privilegio y menor exposición, la presente guía habilita las condiciones de funcionalidad de UAC para la categoría alta.

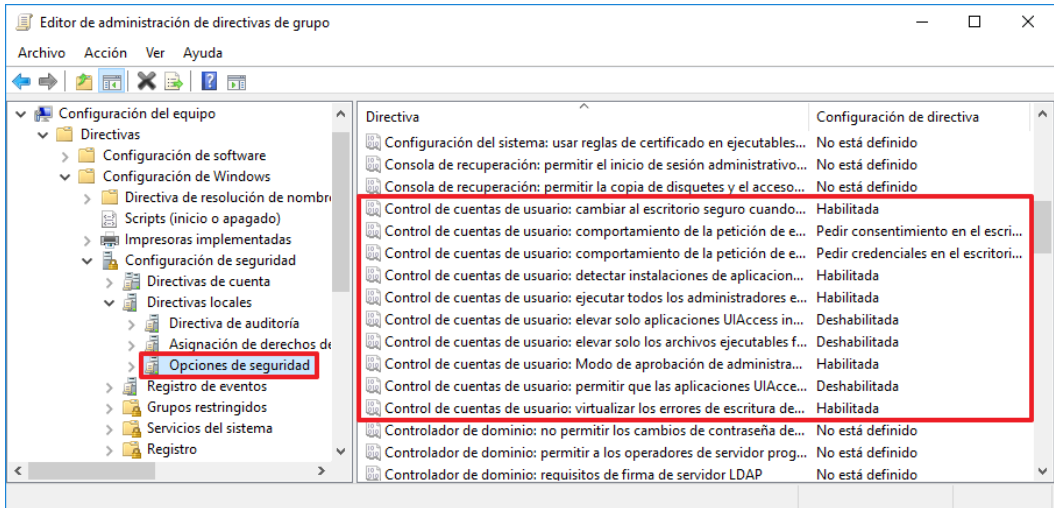
No obstante, y ante aplicaciones o servicios antiguos pudieran darse fallos de funcionalidad en los mismos requiriendo que se realicen análisis o la modificación en la configuración de UAC predeterminada para la categoría alta por la presente guía.

Los siguientes pasos definen los procedimientos para la creación de una nueva política de seguridad de aplicación en los clientes que pudieran presentar incidencias con una nueva política de seguridad para el UAC.

4.1. CONTROL DE CUENTAS USUARIO

Paso	Descripción
75.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
76.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
77.	Identifique los puestos de trabajo que tienen problemas para la ejecución de aplicaciones y servicios y quítelos como miembros del grupo “ENS clientes Windows 10 categoría alta - DL”. En el caso de que no haya tenido que crear dicho grupo siga al paso siguiente.
78.	Cree un nuevo grupo de forma similar al ya creado, siguiendo los pasos 18 a 25 del presente Anexo.

Paso	Descripción
79.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
80.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio. 
81.	Seleccione la pestaña "Administración de directivas de grupo". 

Paso	Descripción
82.	Cree una nueva política de grupo con un nombre diferente (p.e. “CCN-STIC-599A19 ENS incremental clientes categoria alta – DL - incidencias UAC”) que será asignable a los clientes Windows 10 con una categoría alta e incidencias de funcionalidad del UAC. Siga para ello los pasos 27 a 46. Incluya al nuevo grupo de puestos de trabajo creados en lugar del grupo “ENS clientes Windows 10 categoria alta - DL” creado en el proceso previo.
83.	Edite el nuevo objeto de GPO “CCN-STIC-599A19 ENS incremental clientes categoria alta – DL - incidencias UAC”. Para ello seleccione dicha política y seleccione la opción “Editar...” del menú contextual.
84.	Despliegue la política y sitúese en la siguiente ruta. “Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”
85.	Identifique las directivas relativas a “Control de cuenta de usuario”. 
86.	Realice las modificaciones oportunas.
87.	Cierre la política.
88.	Para que la nueva política sea efectiva necesita reiniciar el o los clientes correspondientes. Esto es debido a que la aplicación se basa en la membresía a un grupo. Adquirir la condición del miembro del grupo se realiza cuando se inicia sesión en el dominio, cuestión que se produce cuando el equipo se reinicia. Nota: Debe tener en consideración que, si ha alterado la política de control de cuentas y esta es menos rigurosa que la propuesta en la configuración deseada de esta guía, se encuentra por debajo de los requerimientos de seguridad actuales. Debería evaluar los problemas ocasionados por las aplicaciones y servicios e intentar adaptarlos a configuraciones válidas. Es factible que si los servicios y/o aplicaciones no presenten funcionalidad con UAC presenten riesgos de seguridad notables y se esté exponiendo de forma significativa la infraestructura de la organización.

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 GUÍA PASO A PASO DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN 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 con implementación de seguridad de categoría alta del ENS / Difusión Limitada.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

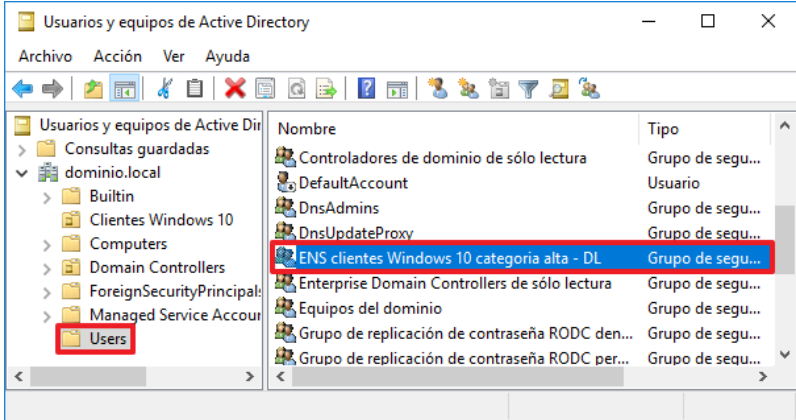
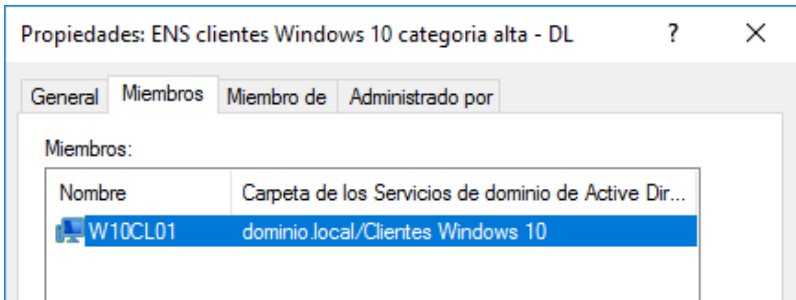
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador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

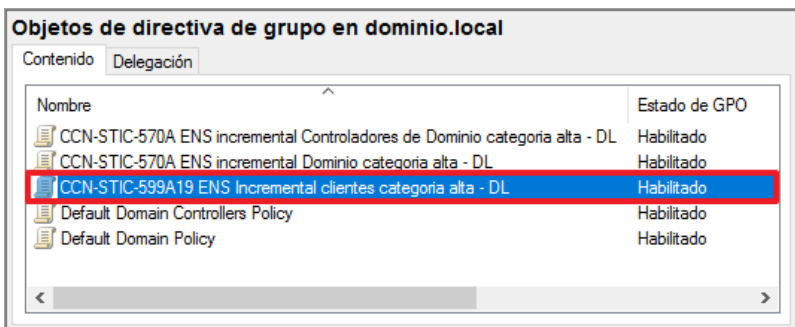
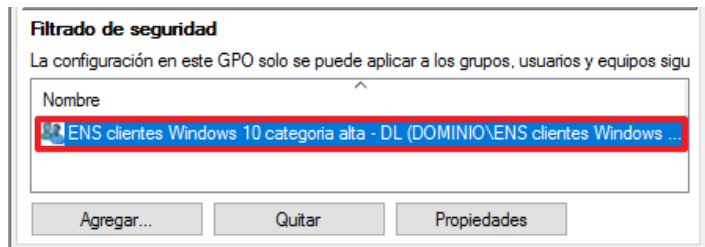
- a) Usuarios y equipos de Active Directory (dsa.msc).
- b) Administrador de directivas de grupo (gpmc.msc).
- c) Editor de objetos de directiva de grupo (gpedit.msc).

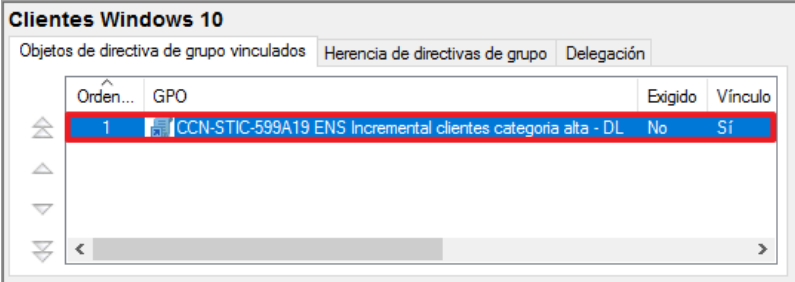
También deberá ejecutar una parte del análisis en los clientes Windows 10 a los que se les haya aplicado la configuración de seguridad de categoría alta – Difusión Limitada. En éstos deberá ejecutar la siguiente aplicación.

- a) Conjunto resultante de directivas (rsop.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creado el grupo “ENS clientes Windows 10 categoría alta - DL” dentro del contenedor “Users”.		Ejecute la herramienta “Usuarios y equipos de Active Directory” desde: “Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory”

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione el contenedor “Users”, situada en “[Su dominio] → Users” y a continuación, en el panel de la derecha, verifique que está creado el objeto denominado “ENS clientes Windows 10 categoría alta - DL”.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers”.
3. Verifique que los clientes que han sido catalogados como de categoría de seguridad alta, siguiendo los criterios definidos en el ENS, son miembros del grupo “ENS clientes Windows 10 categoría alta”.		Pulse doble clic sobre el grupo “ENS clientes Windows 10 categoría alta - DL” situado en el panel de la derecha y seleccione la pestaña “Miembros” para verificar que los clientes que corresponden a esta categoría de seguridad aparecen en el listado.  Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers”.

Comprobación	OK/NOK	Cómo hacerlo		
4. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” ha sido creado y está habilitado.		Ejecute la herramienta “Administrador de directivas de grupo” desde: “Menú inicio → Herramientas administrativas → Administrador de directivas de grupo” Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo” Verifique que está creado el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” y que en la columna “Estado de la GPO” figura como habilitado. 		
		Directiva	Estado	OK/NOK
		CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL	Habilitado	
5. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” tiene definido el Ámbito al grupo “ENS clientes Windows 10 categoria alta - DL”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo “ENS clientes Windows 10 categoria alta - DL”. 		
		Nota: Esta comprobación es necesaria realizarla en el caso de que haya generado este grupo debido a que tiene la necesidad de aplicación de diferentes categorías de seguridad o bien los equipos se encuentran ubicados en la carpeta del Directorio Activo “Computers”.		

Comprobación	OK/NOK	Cómo hacerlo															
6. Verifique que el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” es aplicado a todos aquellos equipos Windows 10 que le son de aplicación las condiciones de categoría alta.		Evalúe que la política de seguridad es aplicada en un orden superior a otras políticas aplicables a los puestos de trabajo en todas aquellas ubicaciones donde se encuentren clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría alta – Difusión Limitada. En el árbol de la izquierda, seleccione la ubicación donde se encuentren los clientes del dominio Windows 10 al que le son de aplicación, las condiciones de seguridad de categoría alta – Difusión Limitada: 															
7. Verifique la directiva de contraseñas en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL”.		En el árbol de la izquierda, seleccione el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL” desde: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo” Pulse el botón derecho del ratón y seleccione la opción “Editar...”. Se abrirá el editor de directivas de grupo. Deberá navegar sobre los elementos del árbol de directorios para verificar las distintas configuraciones. Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de contraseñas”															
		<table> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> <tr> <td>Exigir historial de contraseñas</td><td>24</td><td></td></tr> <tr> <td>Longitud mínima de la contraseña</td><td>12</td><td></td></tr> <tr> <td>Vigencia máxima de la contraseña</td><td>45</td><td></td></tr> <tr> <td>Vigencia mínima de la contraseña</td><td>2</td><td></td></tr> </table>	Directiva	Valor	OK/NOK	Exigir historial de contraseñas	24		Longitud mínima de la contraseña	12		Vigencia máxima de la contraseña	45		Vigencia mínima de la contraseña	2	
Directiva	Valor	OK/NOK															
Exigir historial de contraseñas	24																
Longitud mínima de la contraseña	12																
Vigencia máxima de la contraseña	45																
Vigencia mínima de la contraseña	2																

Comprobación	OK/NOK	Cómo hacerlo		
8. Verifique la directiva de bloqueo de cuenta en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas de cuenta → Directiva de bloqueo de cuenta”		
		Directiva	Valor	OK/NOK
		Duración del bloqueo de cuenta	0	
		Restablecer el bloqueo de cuenta después de	30	
		Umbral del bloqueo de cuenta	8	
9. Verifique las directivas de auditoría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
10.Verifique la asignación de derechos de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	BUILTIN\Administradores	
		Ajustar las cuotas de la memoria para un proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores	
		Apagar el sistema	BUILTIN\Usuarios, BUILTIN\Administradores	
		Aumentar el espacio de trabajo de un proceso	BUILTIN\Usuarios, NT AUTHORITY\SERVICIO LOCAL, BUILTIN\Administradores	
		Aumentar prioridad de programación	BUILTIN\Administradores	
		Cambiar la hora del sistema	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cambiar la zona horaria	BUILTIN\Administradores NT AUTHORITY\SERVICIO LOCAL	
		Cargar y descargar controladores de dispositivo	BUILTIN\Administradores	
		Crear objetos compartidos permanentes		
		Crear un archivo de paginación	BUILTIN\Administradores	
		Crear un objeto símbolo (token)		
		Crear vínculos simbólicos	BUILTIN\Administradores	

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva	Valor	OK/NOK
	Denegar el acceso a este equipo desde la red	BUILTIN\Invitados, NT AUTHORITY\ANONYMOUS LOGON	
	Denegar el inicio de sesión como servicio	BUILTIN\Invitados	
	Denegar el inicio de sesión como trabajo por lotes	BUILTIN\Invitados	
	Denegar el inicio de sesión local	BUILTIN\Invitados	
	Denegar inicio de sesión a través de Servicios de Escritorio remoto	Todos	
	Depurar programas	BUILTIN\Administradores	
	Forzar cierre desde un sistema remoto	BUILTIN\Administradores	
	Generar auditorías de seguridad	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red	
	Generar perfiles de un solo proceso	BUILTIN\Administradores	
	Generar perfiles del rendimiento del sistema	BUILTIN\Administradores	
	Habilitar confianza con el equipo y las cuentas de usuario para delegación		
	Hacer copias de seguridad de archivos y directorios	BUILTIN\Administradores	
	Iniciar sesión como proceso por lotes		
	Iniciar sesión como servicio		
	Modificar la etiqueta de un objeto		
	Modificar valores de entorno firmware	BUILTIN\Administradores	
	Obtener acceso al administrador de credenciales como un llamador de confianza		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Omitir comprobación de recorrido	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red, BUILTIN\Administradores, NT AUTHORITY\Usuarios autenticados	
		Permitir el inicio de sesión local	BUILTIN\Usuarios, BUILTIN\Administradores	
		Permitir inicio de sesión a través de Servicios de Escritorio remoto		
		Realizar tareas de mantenimiento del volumen	BUILTIN\Administradores	
		Reemplazar un símbolo (token) de nivel de proceso	NT AUTHORITY\SERVICIO LOCAL, NT AUTHORITY\Servicio de red	
		Restaurar archivos y directorios	BUILTIN\Administradores	
		Tener acceso a este equipo desde la red	BUILTIN\Usuarios, BUILTIN\Administradores	
		Tomar posesión de archivos y otros objetos	BUILTIN\Administradores	
11.Verifique las opciones de seguridad en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad		
		Directiva	Valor	OK/NOK
		Acceso a redes: canalizaciones con nombre accesibles anónimamente		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	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	Habilitado
		Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitado
		Acceso a redes: no permitir enumeraciones anónimas de cuentas y recursos compartidos SAM	Habilitado
		Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos	Deshabilitado
		Acceso a redes: restringir acceso anónimo a canalizaciones con nombre y recursos compartidos	Habilitado
		Acceso de red: permitir traducción SID/nombre anónima	Deshabilitado
		Apagado: borrar el archivo de paginación de la memoria virtual	Habilitado
		Auditoría: apagar el sistema de inmediato si no se pueden registrar las auditorías de seguridad	Habilitado
		Auditoría: auditar el acceso de objetos globales del sistema	Habilitado
		Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
		Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado
		Consola de recuperación: permitir el inicio de sesión administrativo automático	Deshabilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Consola de recuperación: permitir la copia de disquetes y el acceso a todas las unidades y carpetas	Deshabilitado
		Control de cuentas de usuario: cambiar al escritorio seguro cuando se pida confirmación de elevación	Habilitado
		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	Habilitado
		Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador	Habilitado
		Control de cuentas de usuario: elevar sólo aplicaciones UIAccess instaladas en ubicaciones seguras	Habilitado
		Control de cuentas de usuario: elevar sólo los archivos ejecutables firmados y validados	Deshabilitado
		Control de cuentas de usuario: Modo de aprobación de administrador para la cuenta predefinida Administrador	Habilitado
		Control de cuentas de usuario: permitir que las aplicaciones UIAccess pidan confirmación de elevación sin usar el escritorio seguro	Deshabilitado
		Control de cuentas de usuario: virtualizar los errores de escritura de archivo y de Registro en diferentes ubicaciones por usuario	Habilitado
		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.

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash	Habilitado
		Cuentas: estado de la cuenta de invitado	Deshabilitado
		Cuentas: limitar el uso de cuentas locales con contraseña en blanco sólo para iniciar sesión en la consola	Habilitado
		Dispositivos: permitir desacoplamiento sin tener que iniciar sesión	Deshabilitado
		Dispositivos: restringir el acceso a disquetes sólo al usuario con sesión iniciada localmente	Habilitado
		Dispositivos: restringir el acceso al CD-ROM sólo al usuario con sesión iniciada localmente	Habilitado
		Inicio de sesión interactivo: comportamiento de extracción de tarjeta inteligente	Bloquear estación de trabajo
		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	Habilitado
		Inicio de sesión interactivo: no requerir Ctrl+Alt+Supr	Deshabilitado
		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	Deshabilitado
		Miembro de dominio: cifrar digitalmente datos de un canal seguro (cuando sea posible)	Habilitado
		Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor
		Miembro de dominio: deshabilitar los cambios de contraseña de cuentas de equipo	Deshabilitado
		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)	Habilitado
		Miembro de dominio: requerir clave de sesión segura (Windows 2000 o posterior)	Habilitado
		Objetos de sistema: reforzar los permisos predeterminados de los objetos internos del sistema (por ejemplo, vínculos simbólicos)	Habilitado
		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	Habilitado
		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 Microsoft: desconectar a los clientes cuando expire el tiempo de inicio de sesión	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
		Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
12.Verifique el registro de eventos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos”		
		Directiva	Valor	OK/NOK
		Evitar que el grupo de invitados locales tenga acceso al registro de aplicaciones	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro de seguridad	Habilitado	
		Evitar que el grupo de invitados locales tenga acceso al registro del sistema	Habilitado	
		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”		
13.Verifique los servicios del sistema definidos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Nota: 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 para cada servicio. En la ventana del editor de administración de directivas de grupo 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	
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	
Administrador de identidad de redes de mismo nivel	p2pimsvc	Manual	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	
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	
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	

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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	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
Control parental	WpcMonSvc	Deshabilitado	Configurado

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
GraphicsPerfSvc	GraphicsPerfSvc	Manual	Configurado
Hora de Windows	W32Time	Manual	Configurado
Host de proveedor de detección de función	fdPHost	Manual	Configurado

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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	Wecevc	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
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	vmicshuttdown	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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
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

Comprobación	OK/NOK	Cómo hacerlo	
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso
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
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

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	
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	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
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
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
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
14.Verifique los valores del sistema de archivos en el objeto de directiva de grupo "CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL".		Seleccione el siguiente nodo. "Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de Archivos" Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción "Propiedades" del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".	

Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%ProgramFiles%\Netmeeting	Administradores	Control total	
	SYSTEM	Control total	
%Public%\	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%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\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	

Comprobación	OK/NOK	Cómo hacerlo		
15.Verifique la directiva de administración de derechos digitales de Windows Media en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	
16.Verifique la directiva de almacén digital en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
17.Verifique la directiva de Antivirus en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Antivirus de Windows Defender”		
		Directiva	Valor	OK/NOK
		Desactivar Antivirus de Windows Defender	Habilitado	
18.Verifique la directiva de asistencia en línea en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Asistencia en línea”		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitado	
19.Verifique las directivas de biometría en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Biometría”		

Comprobación	OK/NOK	Cómo hacerlo		
		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	
20.Verifique las directivas de búsqueda en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	Deshabilitado	
21.Verifique las directivas de contenido en la nube en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
22.Verifique las directivas de reproducción automática en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Directivas de reproducción automática”		
		Directiva	Valor	OK/NOK
		Desactivar reproducción automática	Habilitado (Todas las unidades)	
		Establece el comportamiento predeterminado para la ejecución automática	Habilitado (No ejecutar ningún comando de ejecución automática)	
23.Verifique las directivas de Explorador de archivos en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Explorador de archivos”		
		Directiva	Valor	OK/NOK
		Configurar Windows SmartScreen de Windows defender	Habilitado (Advertir e impedir la omisión)	

Comprobación	OK/NOK	Cómo hacerlo		
24.Verifique las directivas de informe de errores de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Informe de errores de Windows”		
		Directiva	Valor	OK/NOK
		Deshabilitar el informe de errores de Windows	Habilitado	
		No enviar datos adicionales	Habilitado	
25.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
26.Verifique las directivas de Internet Explorer en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Internet Explorer → Configuración de Internet → Autocompletar”		
		Directiva	Valor	OK/NOK
		Desactivar las sugerencias de direcciones URL	Habilitado	
27.Verifique las directivas de Eliminar el historial de exploración en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
28.Verifique las directivas de Microsoft Edge en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Microsoft Edge”		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
29.Verifique las directivas de OneDrive en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive”		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos.	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo		
30.Verifique las directivas de inicio de sesión de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	Deshabilitado	
31.Verifique las directivas de optimización de entrega en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Optimización de entrega”		
		Directiva	Valor	OK/NOK
		Modo de descarga	Habilitado (Solo HTTP (0))	

Comprobación	OK/NOK	Cómo hacerlo		
32.Verifique la directiva de privacidad de la aplicación en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Privacidad de la aplicación”		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la cámara	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 accedan a la información de la cuenta	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a la ubicación	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las notificaciones	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a las tareas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan a los mensajes	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al calendario	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al correo electrónico	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al historial de llamadas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows accedan al micrófono	Habilitado (Forzar denegación)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Permitir que las aplicaciones de Windows accedan al movimiento	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows controlen las radios	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows realicen llamadas telefónicas	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se comuniquen con dispositivos desemparejados	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows se ejecuten en el fondo	Habilitado (Forzar denegación)	
		Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitado (Forzar denegación)	
33.Verifique las directivas de recopilación de datos a versiones preliminares en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

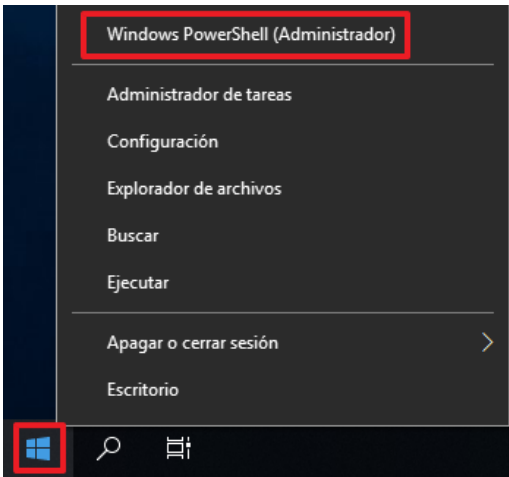
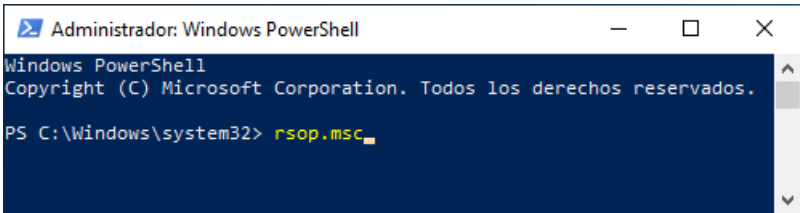
Comprobación	OK/NOK	Cómo hacerlo		
34.Verifique la directiva de Shell remoto de Windows en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Shell remoto de Windows”		
		Directiva	Valor	OK/NOK
		Permitir acceso a Shell remoto	Deshabilitado	
35.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
36.Verifique la directiva de Smart Screen en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Smart Screen de Windows Defender → Microsoft Edge”		
		Directiva	Valor	OK/NOK

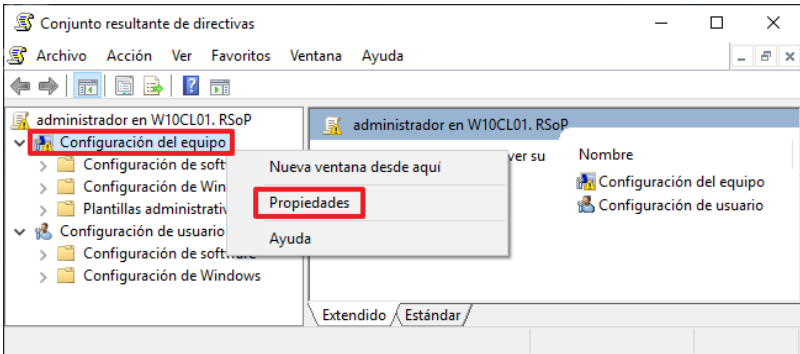
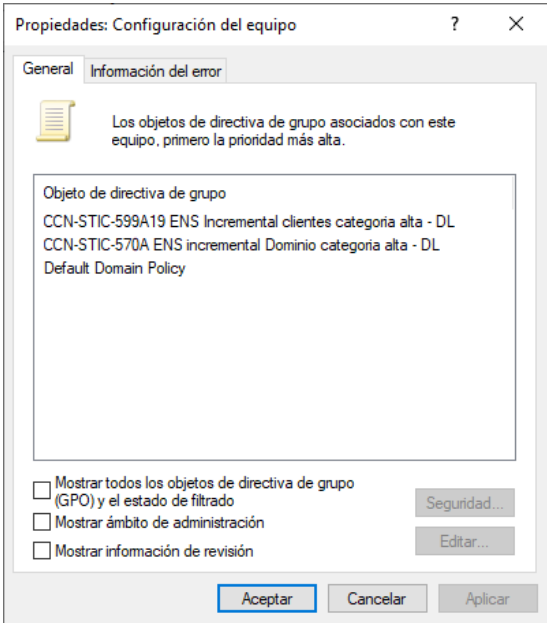
Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar SmartScreen de Windows Defender	Deshabilitado	
37.Verifique la directiva de Tienda en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tienda”		
		Directiva	Valor	OK/NOK
		Desactivar la aplicación Store	Habilitado	
		Deshabilita todas las aplicaciones de Microsoft Store	Deshabilitado	
38.Verifique la directiva de Ubicación y sensores en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
39.Verifique la directiva de Windows Update en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update → Actualización de Windows para empresas”		
		Directiva	Valor	OK/NOK
		Administrar preliminares	Habilitado (Deshabilitar preliminares)	
40.Verifique la directiva de personalización de escritura a mano en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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		
41.Verifique la directiva de comunicaciones de Internet en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
42.Verifique la directiva de Net Logon en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Plantillas Administrativas → Sistema → Net Logon”		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitado	
43.Verifique la directiva de perfiles de usuario en el objeto de directiva de grupo “CCN-STIC-599A19 ENS Incremental clientes categoría alta - DL”.		Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → 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)	
		Desactivar el identificador de publicidad	Habilitado	

Comprobación	OK/NOK	Cómo hacerlo
44. Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador.		Inicie sesión en el equipo cliente que está comprobando con una cuenta de usuario de Windows con permisos de administrador.
45. 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. 
46. Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse "Enter" para abrir la consola de administración "Conjunto resultante de directivas": 

Comprobación	OK/NOK	Cómo hacerlo
47.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL".		En la consola de administración "Conjunto resultante de directivas, seleccione el contenedor "Configuración del equipo", márkuelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las políticas deberán aparecer y "CCN-STIC-599A19 ENS incremental clientes categoria alta - DL" deberá estar situada encima de la GPO que se establece a nivel de dominio, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

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). Dentro de la solución se integra la característica de MBAM (Administración y supervisión de Microsoft BitLocker) que va a permitir centralizar la administración de BitLocker, así como una gestión eficiente de las claves de recuperación. Para más información sobre MBAM, puede consultar la siguiente URL:

<https://technet.microsoft.com/en-us/itpro/mdop/mbam-v25/about-mbam-25-sp1>

La implementación de BitLocker requiere de unos requisitos específicos 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 de la 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 sin darse cuenta. Una vez que la unidad está preparada, debe reiniciarse el equipo.

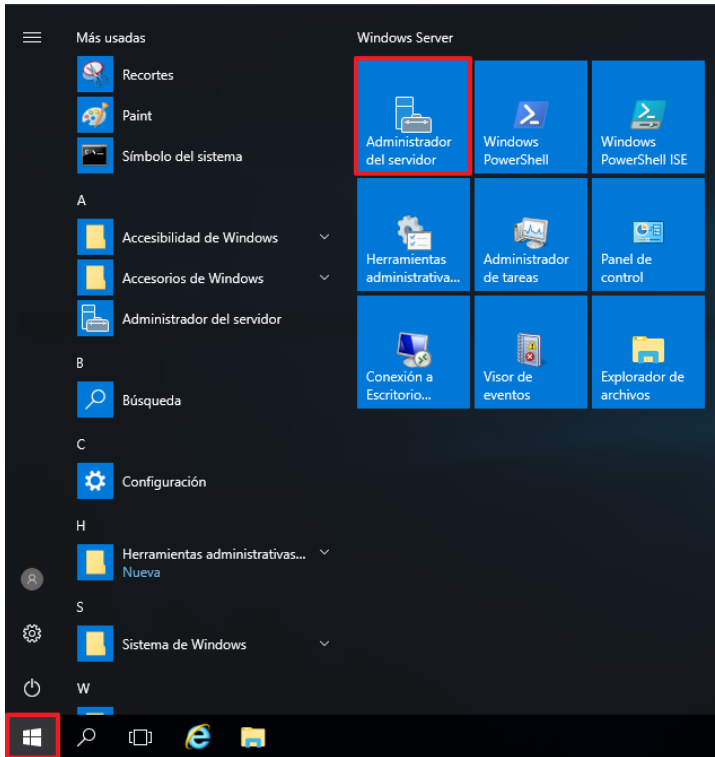
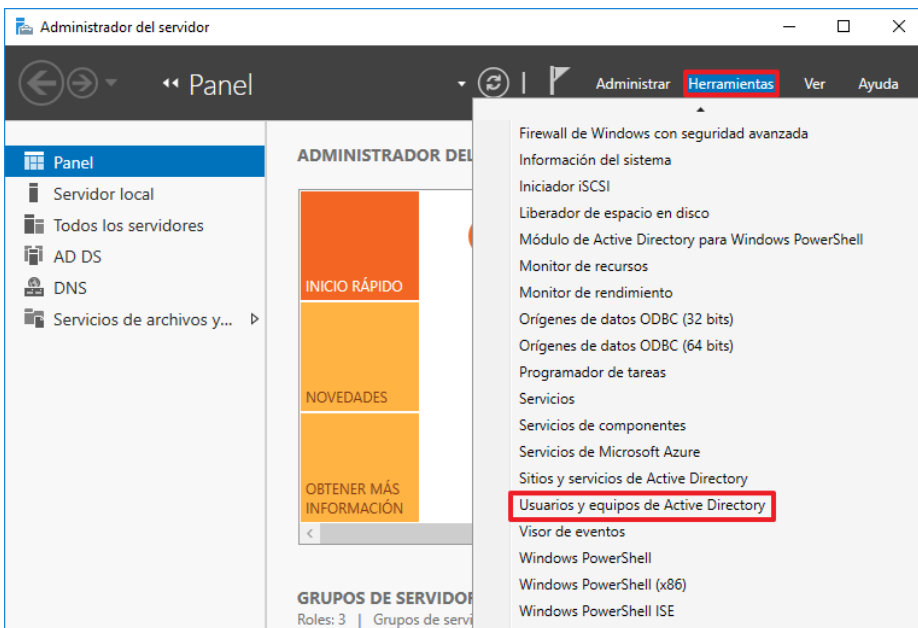
No obstante, si se ha realizado una instalación por defecto de Windows 10, el programa de instalación ya habrá creado durante la instalación las dos particiones de disco necesarias para activar BitLocker.

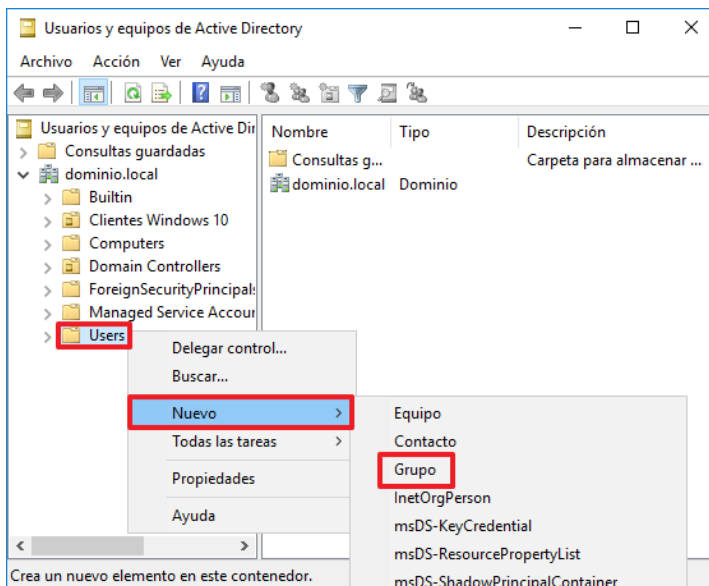
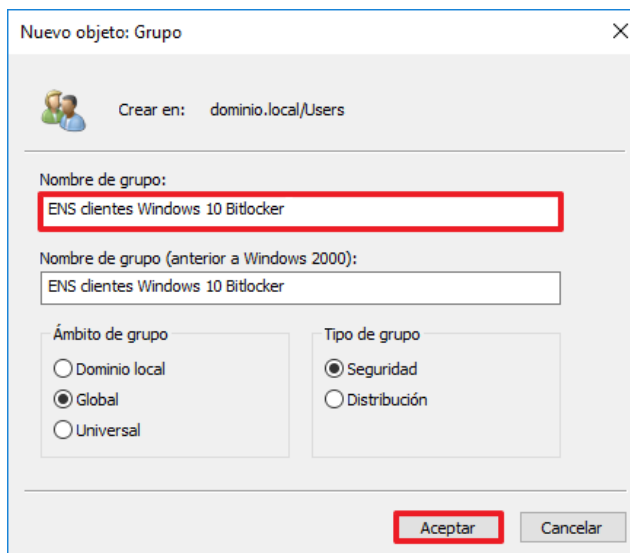
- a) Una unidad flash USB para almacenar claves de inicio y recuperación.
- b) Una configuración BIOS para iniciar primero desde el disco duro, no desde las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como la clave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

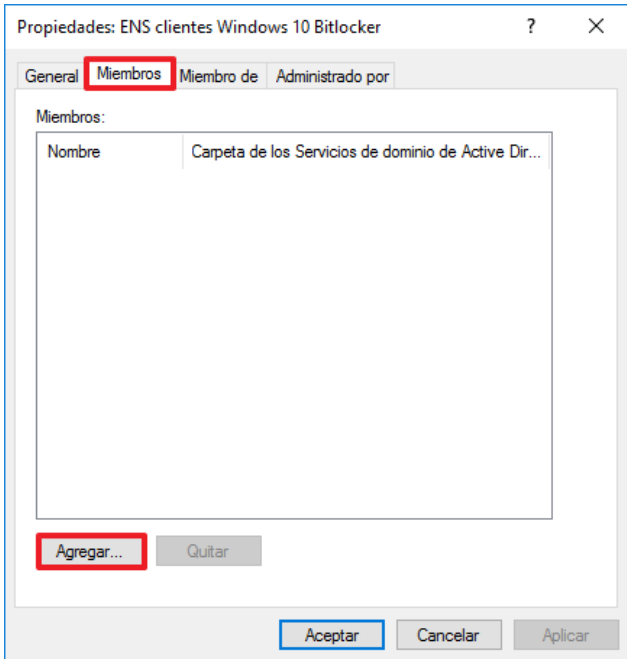
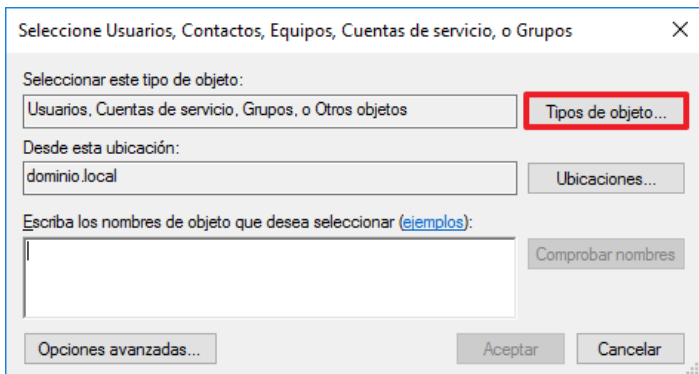
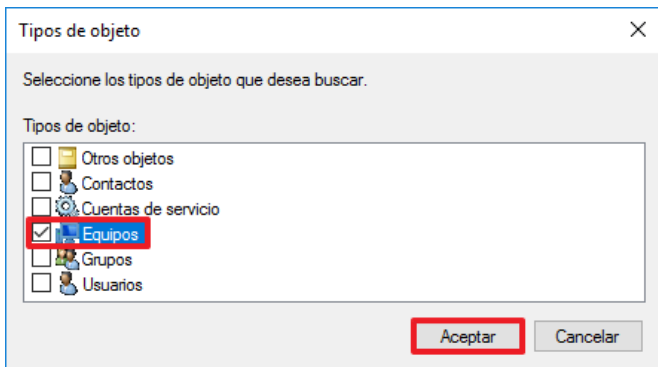
1. PREPARACIÓN DE DOMINIO

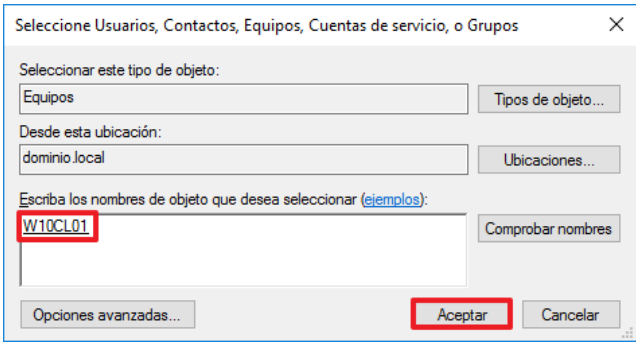
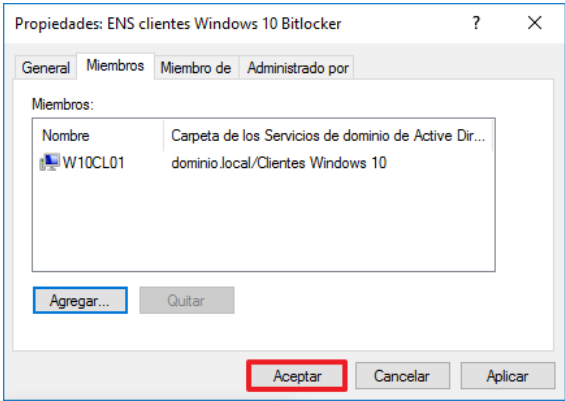
La implementación de BitLocker se basará en la aplicación de una política de seguridad aplicada sobre un grupo de equipos determinados. Para ello deberán seguirse los siguientes pasos.

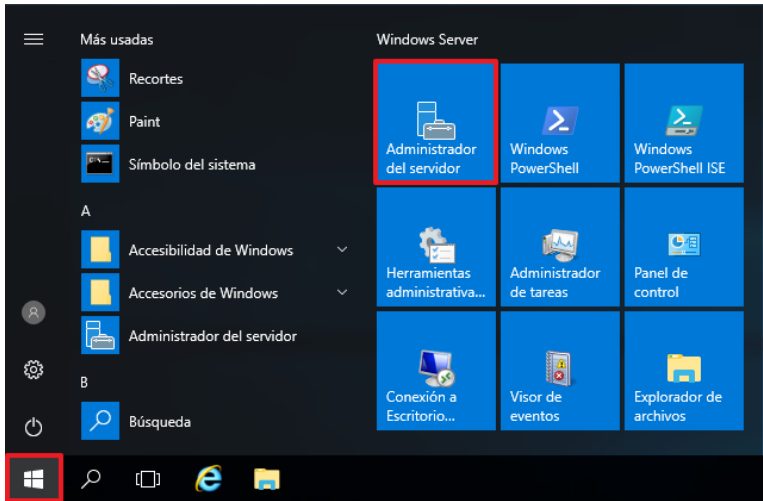
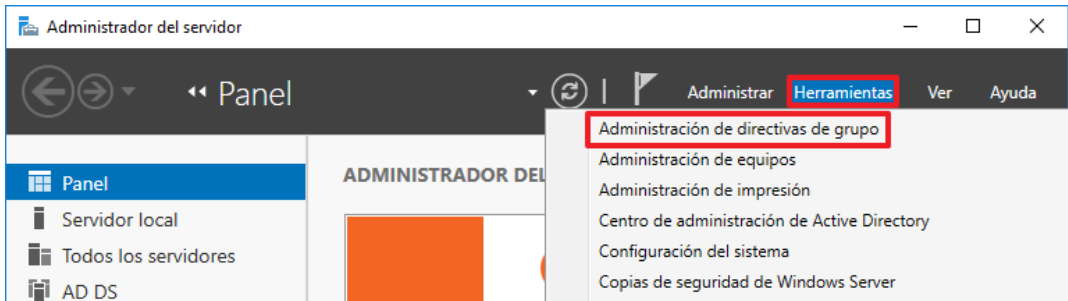
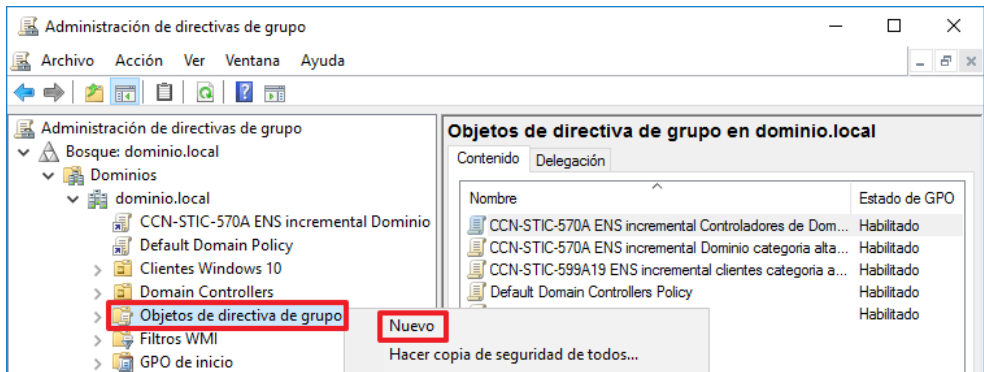
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Cree el directorio "Scripts" en la unidad C:\.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".

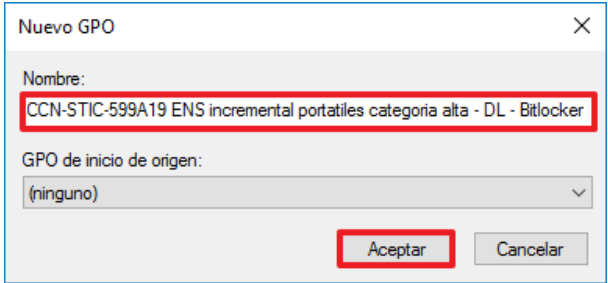
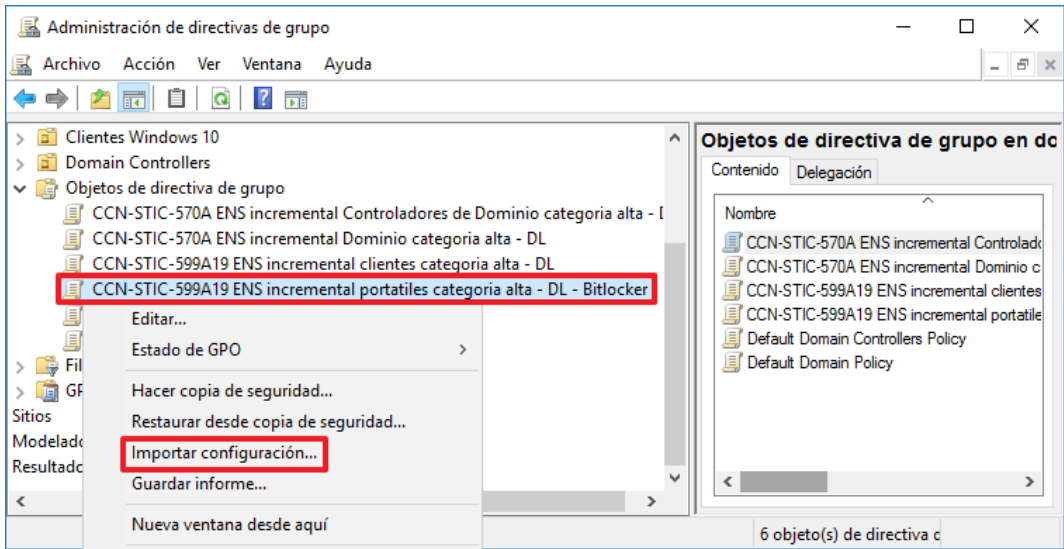
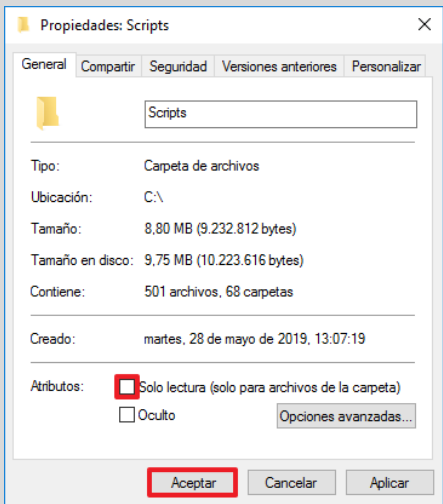
Paso	Descripción
5.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
6.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 

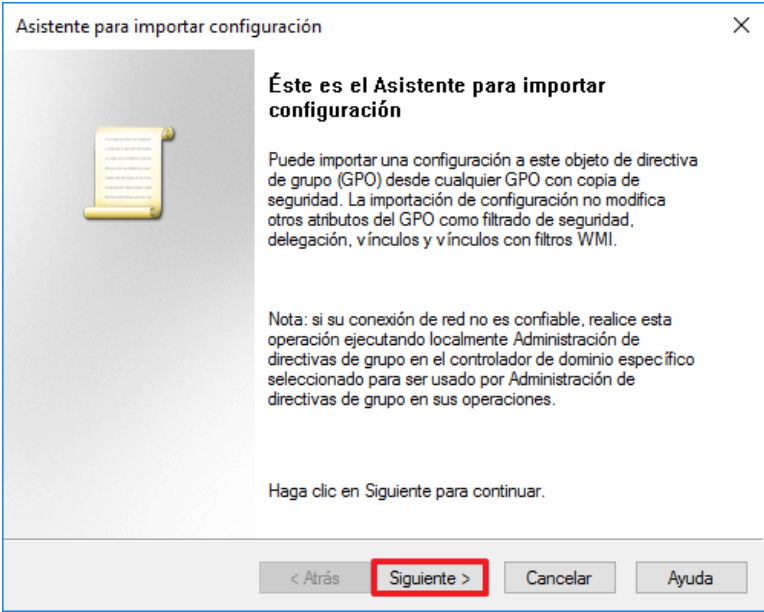
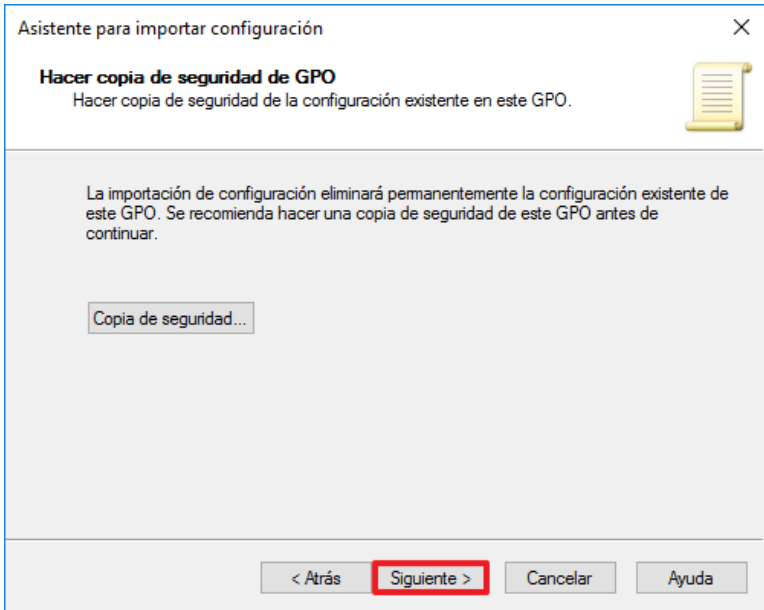
Paso	Descripción
7.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
8.	Introduzca como nombre “ENS clientes Windows 10 BitLocker”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes miembros del dominio sobre los que se vaya a realizar implementación de BitLocker. 
9.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.

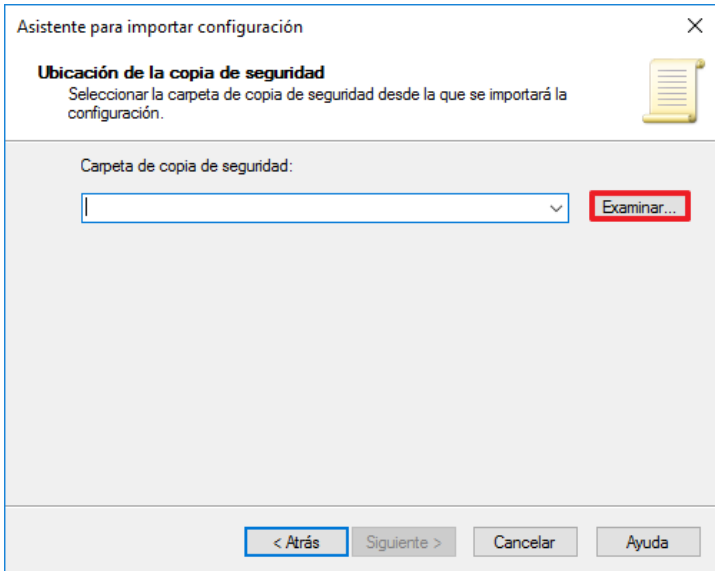
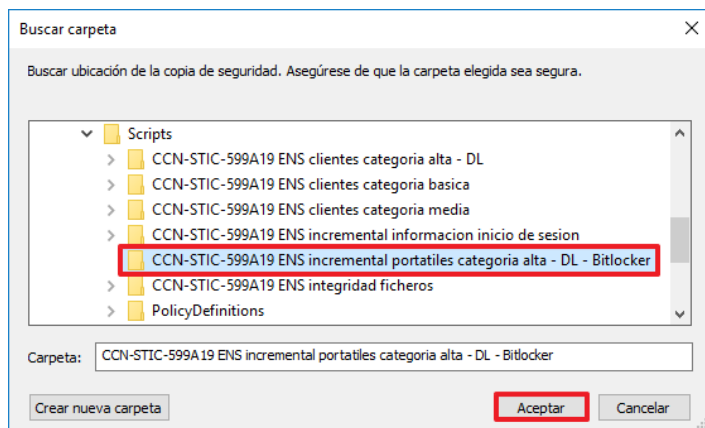
Paso	Descripción
10.	Pulse el botón “Agregar...”. 
11.	Pulse el botón “Tipos de objeto...”. 
12.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

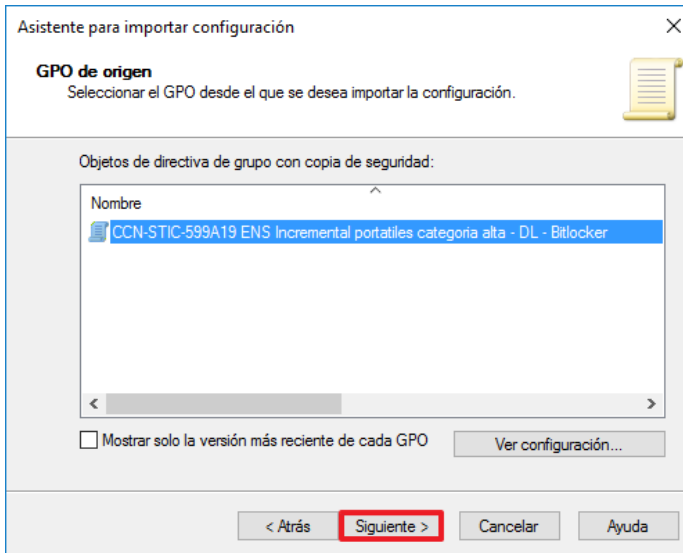
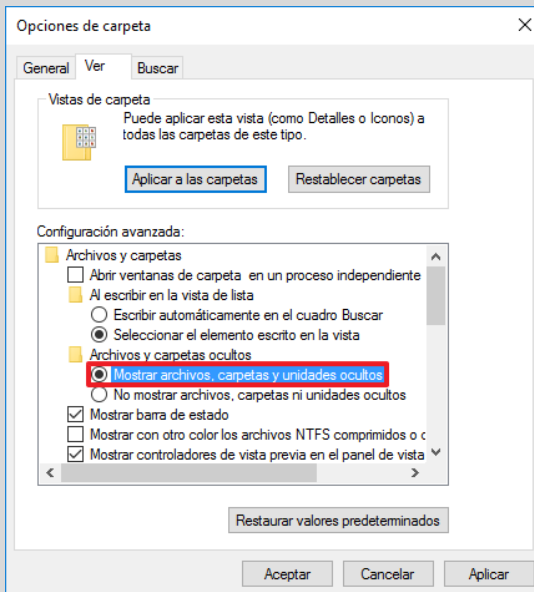
Paso	Descripción
13.	Introduzca el nombre o utilice las opciones avanzadas para agregar aquellos portátiles que manejen datos de categoría alta / Difusión Limitada para los que debe garantizarse la confidencialidad o bien aquellos equipos que desee proteger mediante el cifrado de unidad BitLocker.  Nota: No agregue servidores a este grupo.
14.	Pulse el botón “Aceptar” para agregar la selección.
15.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.

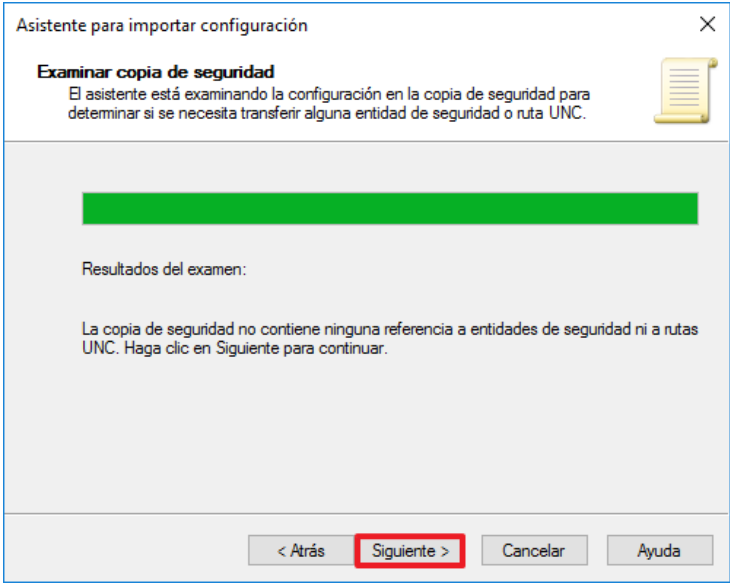
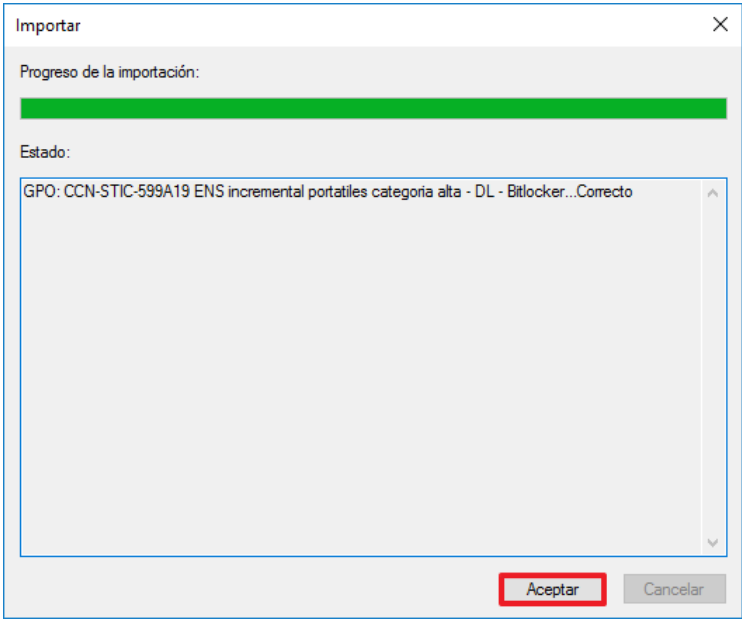
Paso	Descripción
17.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
18.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas de grupo" 
19.	Despliegue los contenedores y sitúese sobre la carpeta "Objetos de directiva de grupo".
20.	Pulse con el botón derecho del ratón sobre dicho contenedor y seleccione la opción "Nuevo". 

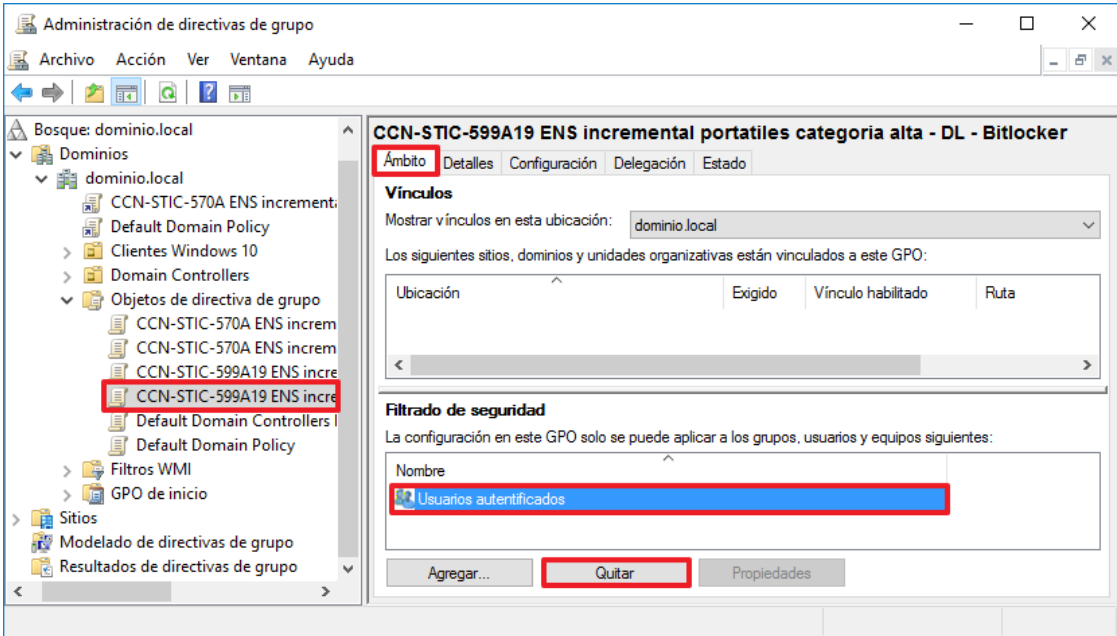
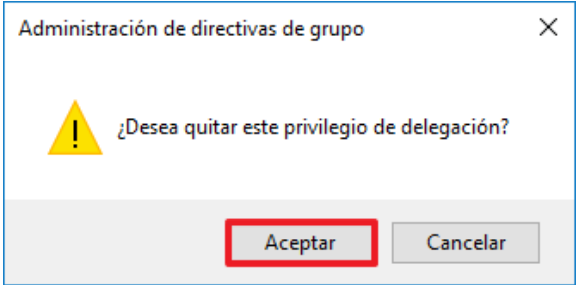
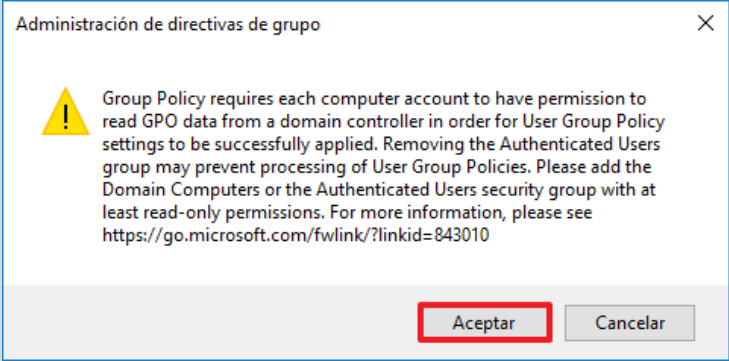
Paso	Descripción
21.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental portátiles categoría alta – DL - BitLocker” y pulse el botón “Aceptar”. 
22.	La nueva política requiere una configuración de plantillas administrativas. Para ello seleccione la política, pulse con el botón derecho del ratón sobre la misma y seleccione la opción “Importar configuración...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts” no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

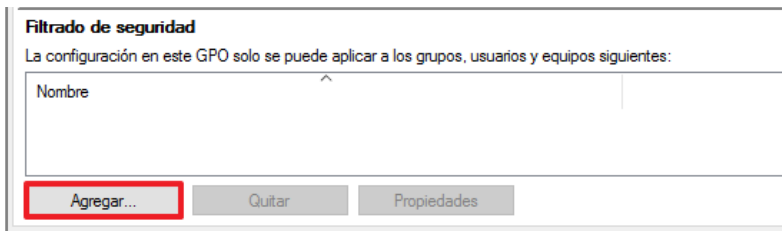
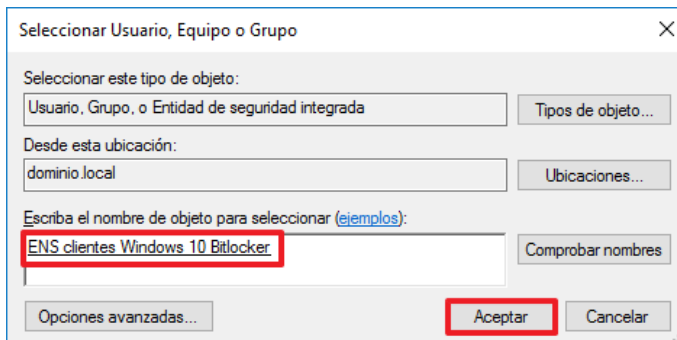
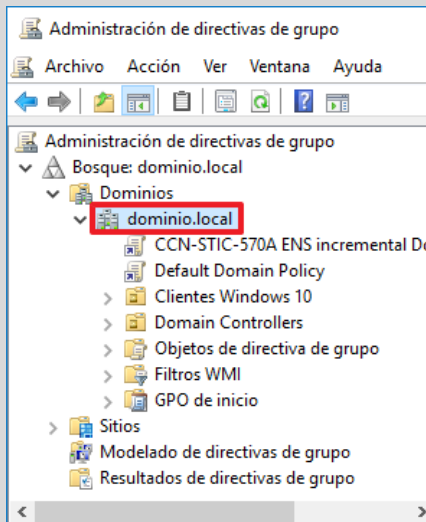
Paso	Descripción
23.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 
24.	En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía. 

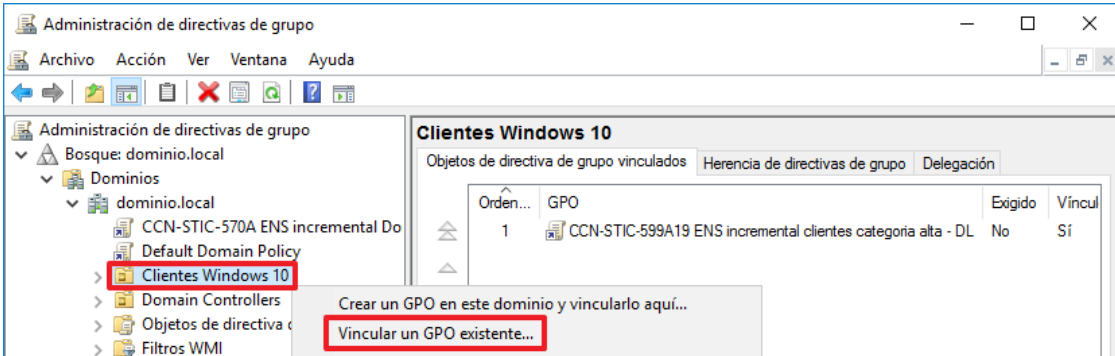
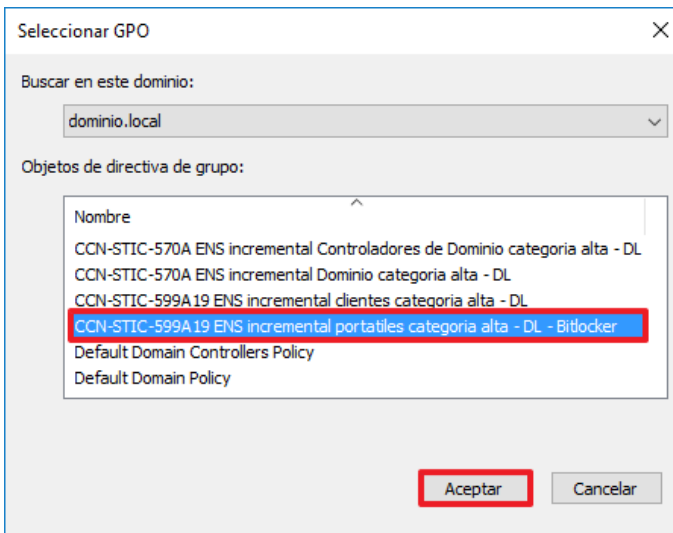
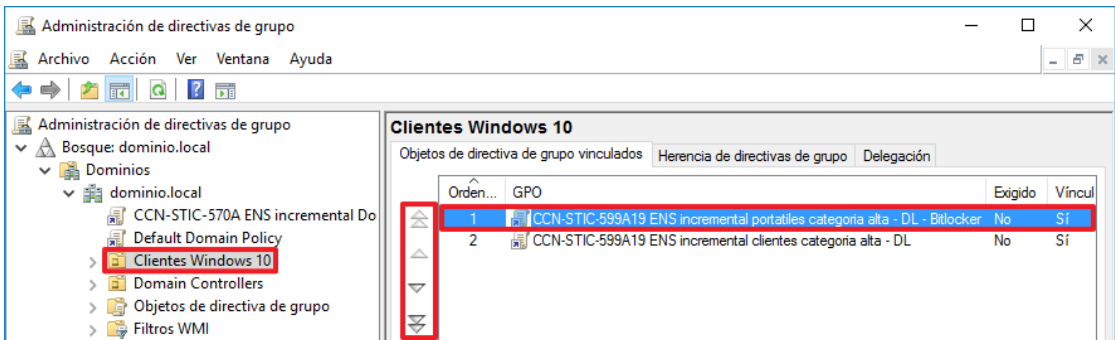
Paso	Descripción
25.	En la ventana “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 
26.	Seleccione la carpeta “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”. 
27.	Pulse el botón “Siguiete >” cuando haya sido seleccionada la carpeta correspondiente.

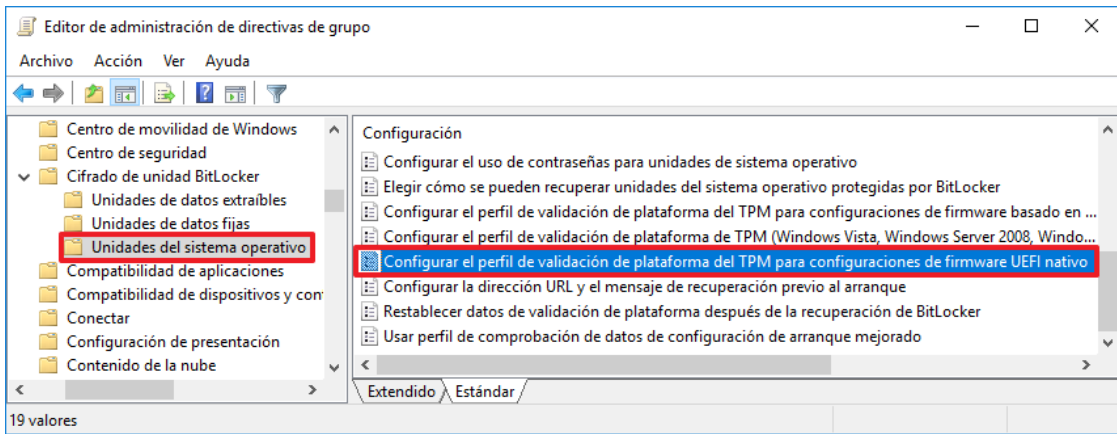
Paso	Descripción
28.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker” y pulse el botón “Siguiente >”.  Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el “fichero manifest.xml”. Este es un fichero oculto y por lo tanto debe mostrar en opciones de carpeta, la opción “Mostrar archivos, carpetas y unidades ocultos”. 

Paso	Descripción
29.	En la pantalla de examen, pulse el botón “Siguiente >”. 
30.	Para completar el asistente pulse el botón “Finalizar”.
31.	Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración. 

Paso	Descripción
32.	En el apartado “Filtrado de seguridad” del objeto de directiva de grupo “CCN-STIC-599A19 ENS incremental portátiles categoria alta – DL - BitLocker”, seleccione la pestaña “Ámbito”, marque “Usuarios autenticados” y pulse el botón “Quitar”. 
33.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
34.	Una vez quitado, pulse el botón “Agregar...”. 
35.	Introduzca como nombre “ENS clientes Windows 10 BitLocker”. Este grupo corresponde con el generado en pasos previos. A continuación, pulse “Aceptar”. 
36.	Identifique las ubicaciones donde se encuentran los portátiles Windows 10 donde desea realizar la aplicación del cifrado de unidad BitLocker. Sobre cada una de esas ubicaciones asigne el objeto de política de grupo “CCN-STIC ENS incremental portátiles alto BitLocker”. En el ejemplo se aplicará sobre la UO “Clientes Windows 10” lugar donde se encuentran ubicados los clientes existentes en este entorno. Nota: En el caso de que sus puestos de trabajo se encuentren en la ubicación predeterminadas de “computers” y no los haya movido a una Unidad Organizativa, deberá asignar la política a nivel del dominio. 

Paso	Descripción
37.	Pulse con el botón derecho del ratón sobre la unidad organizativa correspondiente, en el ejemplo “Clientes Windows 10”, y seleccione la opción “Vincular un GPO existente...”. 
38.	Seleccione la política “CCN-STIC-599A19 ENS incremental portátiles categoría alta – DL - BitLocker” y pulse el botón “Aceptar”. 
39.	Una vez agregado, en el panel derecho seleccione la política “CCN-STIC-599A19 ENS incremental portátiles categoría alta - DL - BitLocker” y pulse el botón subir hasta situarla en primer lugar dentro del orden de vínculo, en el caso de que existieran más políticas aplicadas en dichas Unidades Organizativas. 

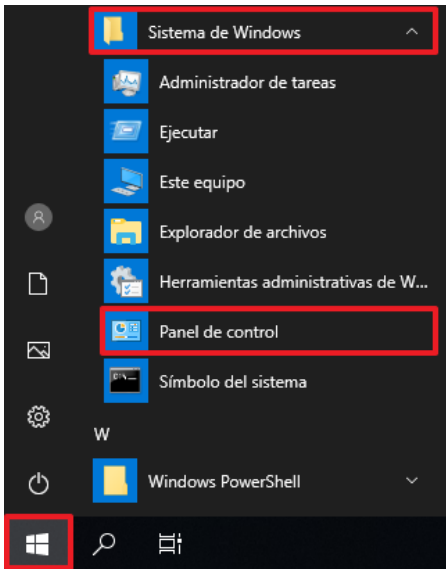
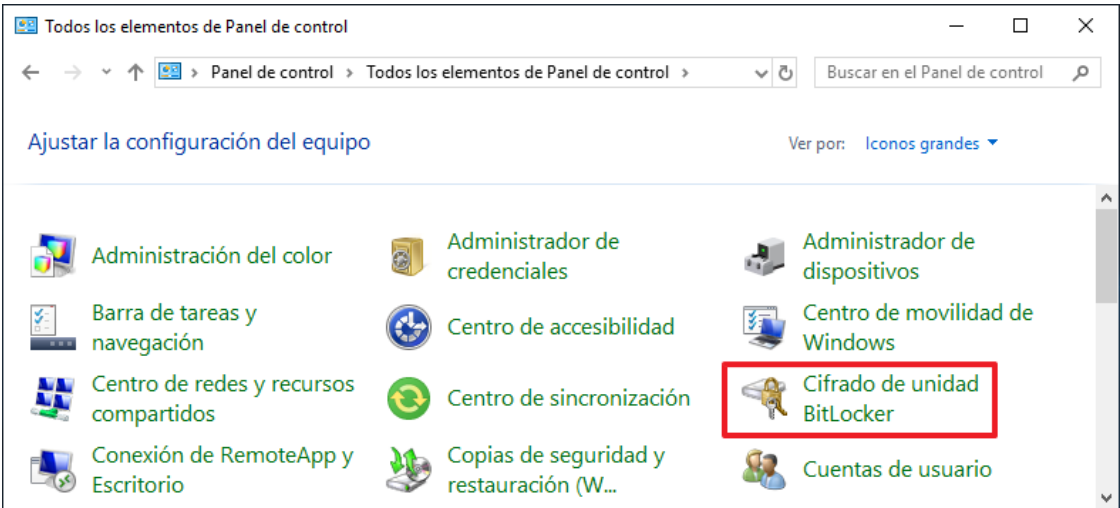
Paso	Descripción
40.	La configuración importada en la GPO desde la copia de seguridad establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si dispone de equipos con firmware UEFI nativo, deberá habilitar y configurar la directiva “Directiva CCN-STIC-599A19 ENS incremental portátiles categoría alta – DL - Bitlocker → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades del sistema operativo → Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo” de la GPO configurada en este apartado. 
41.	Cierre la herramienta “Administración de directivas de grupo”.
42.	Elimine la carpeta “C:\Scripts”.

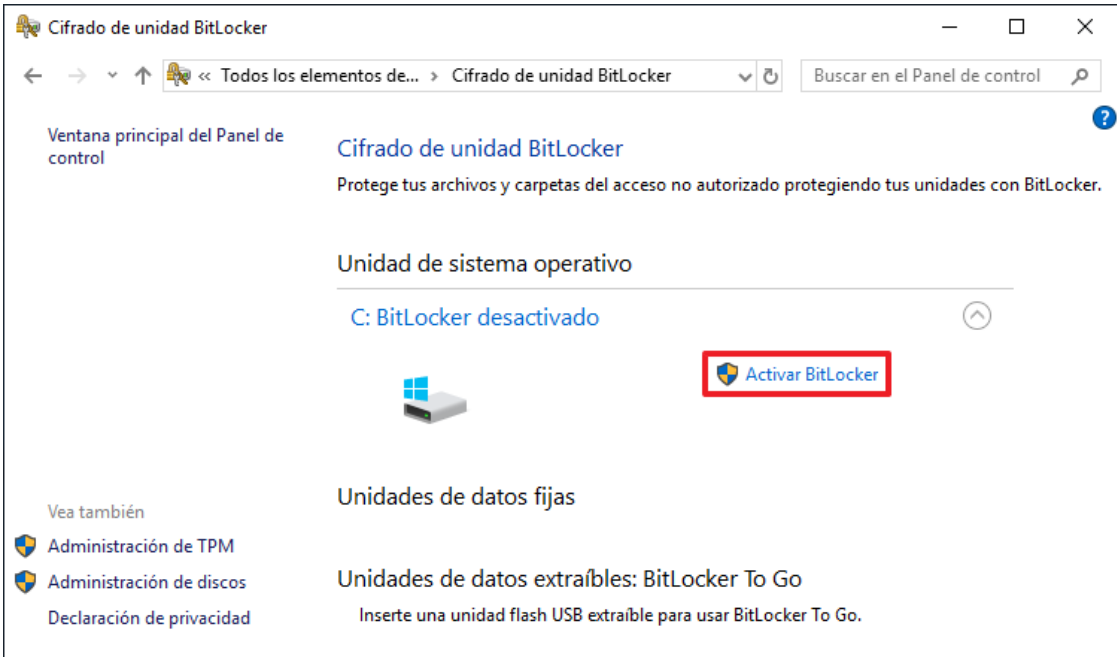
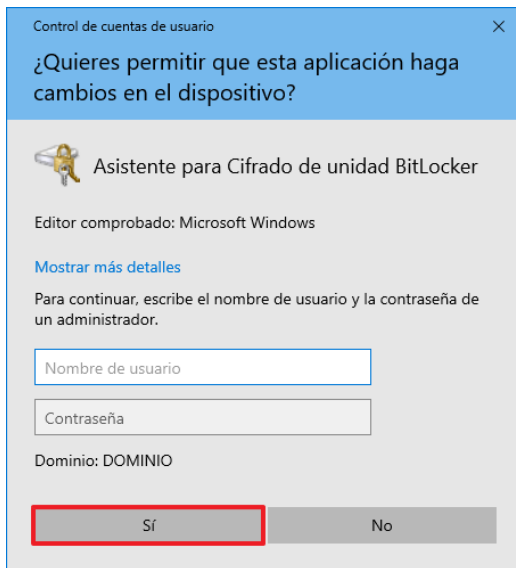
2. CONFIGURACIÓN DE BITLOCKER EN EL PUESTO CLIENTE

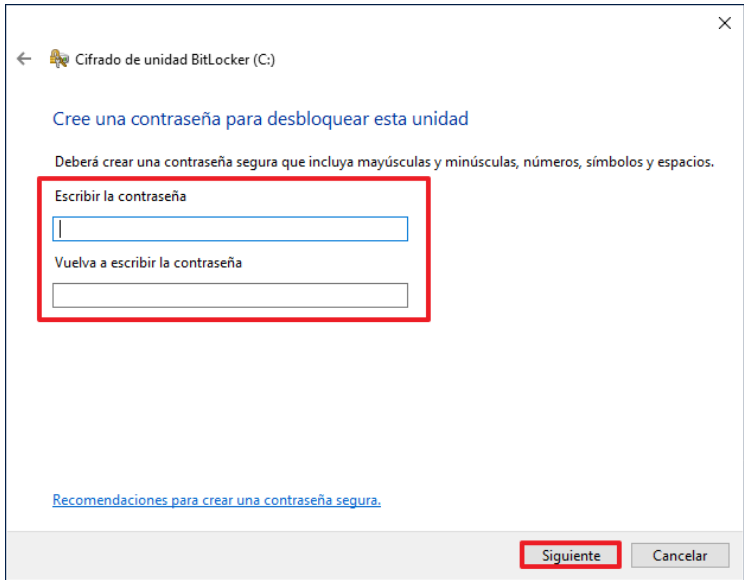
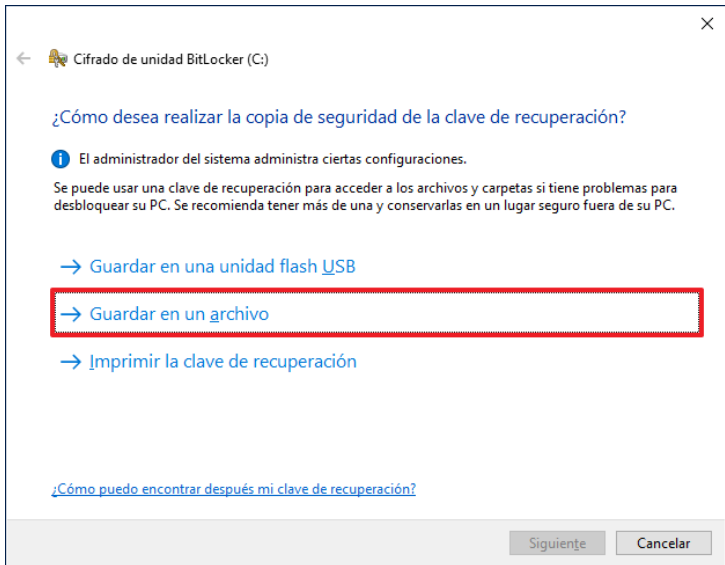
El presente punto establece los pasos que deberá efectuar el operador para realizar la implementación de BitLocker en los clientes, así como la aplicación de una contraseña para el desbloqueo de la unidad.

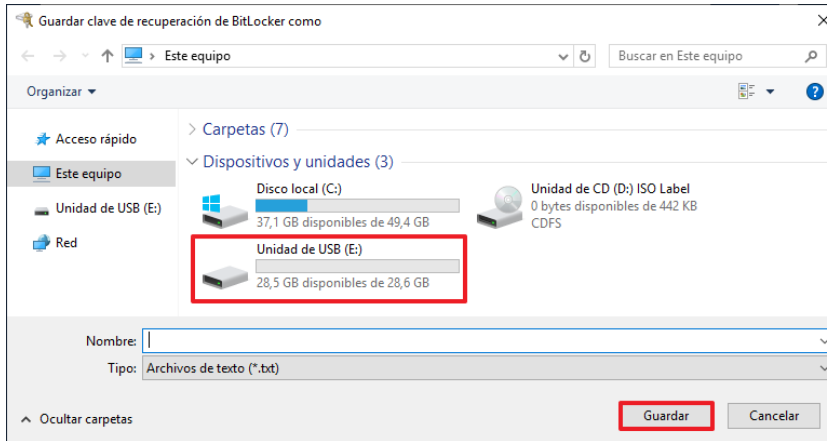
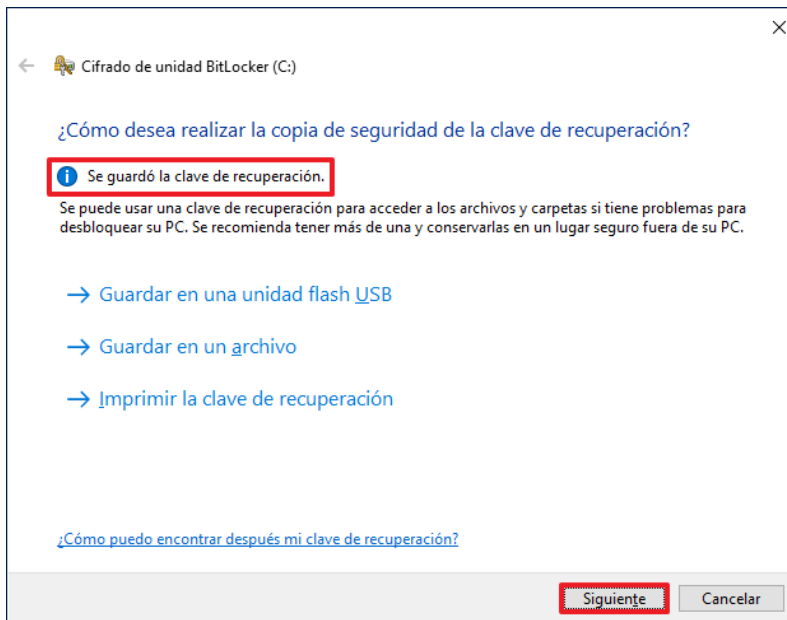
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números.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

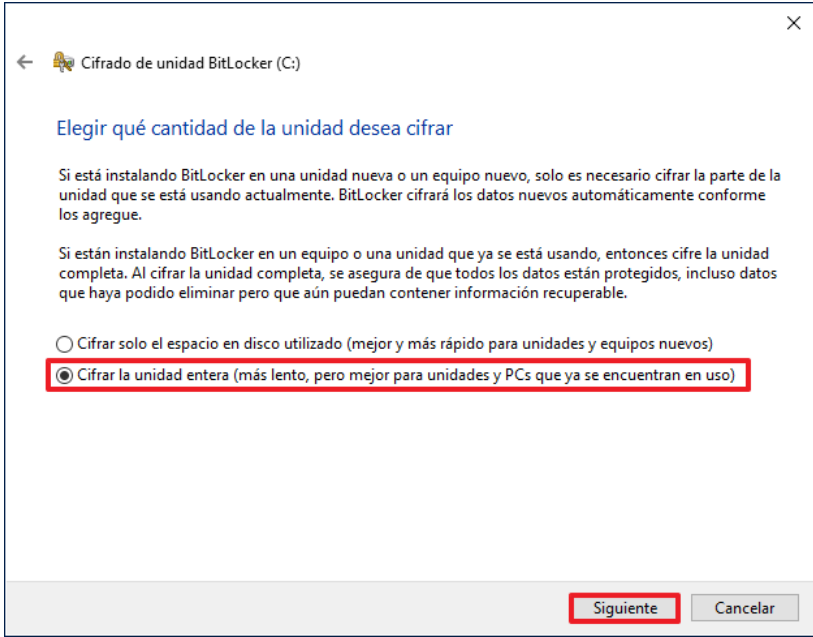
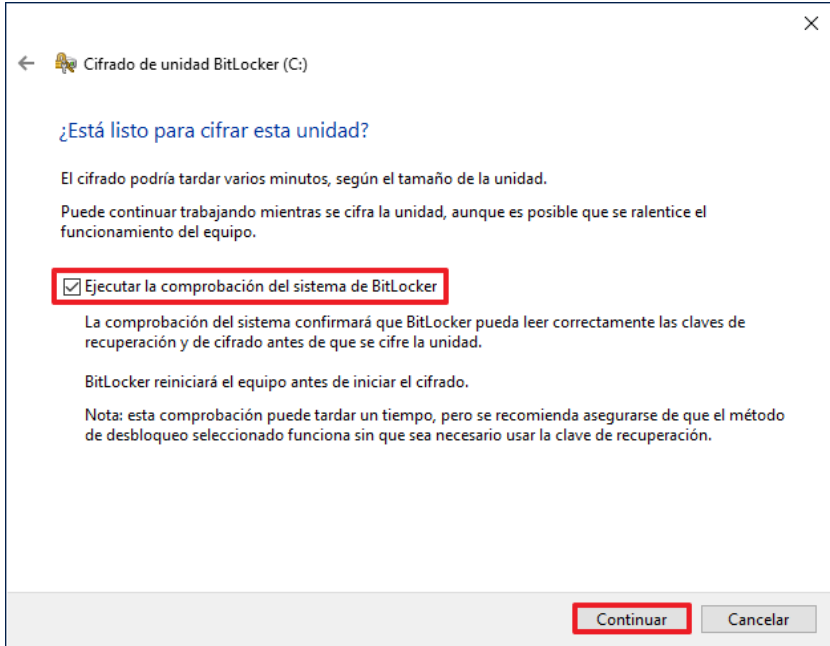
Paso	Descripción
43.	Si el equipo estaba arrancado, inicie sesión en el cliente donde desee realizar implementación del cifrado de BitLocker y reinicie el equipo. Si el equipo estaba apagado y lo ha arrancado siga en el siguiente paso. El reinicio permitirá que el equipo le sea de aplicación la membresía al grupo creado, así como la aplicación de la política de BitLocker.
44.	Inicie sesión en el cliente con un usuario con privilegio de administrador.

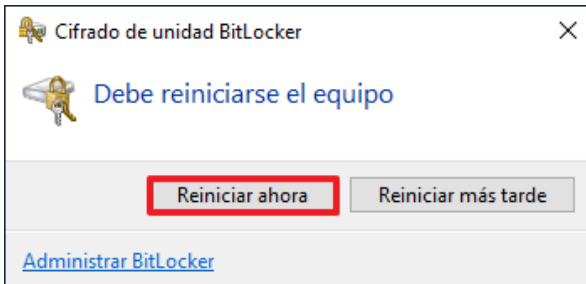
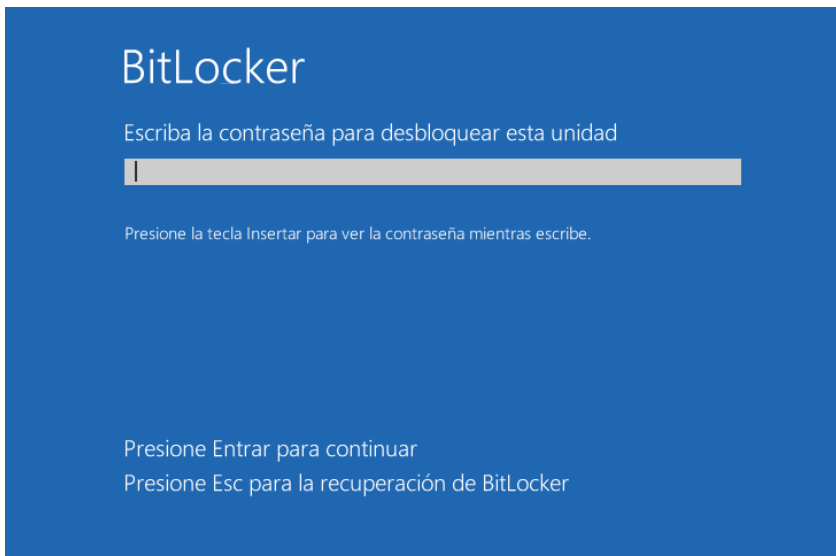
Paso	Descripción
45.	Abra el panel de control desde “Inicio → Sistema de Windows → Panel de control”. 
46.	Seleccione dentro del “Panel de control” el apartado “Cifrado de unidad BitLocker”.  Nota: Tenga en cuenta la visualización del Panel de control. En la parte superior derecha podrá cambiar el modo en que se muestran los iconos.

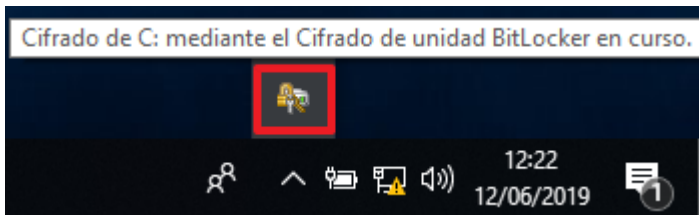
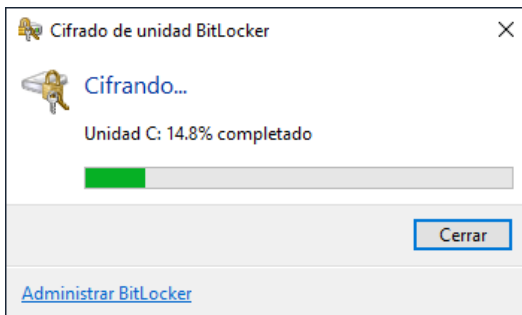
Paso	Descripción
47.	Pulse sobre “Activar BitLocker” como se indica en la siguiente imagen. 
48.	El sistema le solicitará elevación de privilegios. Introduzca credenciales de un usuario con privilegios de administrador en la ventana “Control de cuentas de usuario”. 

Paso	Descripción
49.	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.
50.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
51.	Seleccione la ubicación de la memoria 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.
52.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

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

Paso	Descripción
55.	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 45 a 55, pero en este último paso pulse sobre la opción “Reiniciar más tarde” y reinicie el equipo manualmente mediante la ruta “Inicio → “Iniciar/Apagar””. 
56.	Al reiniciar, el sistema le pedirá la contraseña de cifrado de unidad BitLocker. Introduzca la contraseña y pulse “Enter” para continuar. 

Paso	Descripción
57.	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.  Si marca con el ratón en él, o sobre 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.
58.	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.

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 del cortafuegos con seguridad avanzada con objeto de ofrecer mecanismos de protección adicionales a los clientes Windows 10. 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 una política de firewall dependerá de si los clientes presentan servicios o aplicaciones que necesitan la conexión remota desde otros sistemas, por ejemplo, si la organización emplea algún sistema para realizar tareas de soporte o asistencia remota. A partir de Windows Vista, Microsoft proporciona un servicio de cortafuegos con seguridad avanzada. Este 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: pública, privada o dominio.

De forma predeterminada el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local. No obstante, existe la posibilidad de realizar un control centralizado a través de la aplicación de objetos de políticas de grupo. Esta opción proporciona dos condiciones fundamentales:

- a) Mejorar las condiciones de seguridad, al establecer las mismas por parte de los administradores de dominio, sin que una alteración de tipo local afecte a dicha configuración.
- b) Centralizar la administración de tal forma que exista un único punto de control.

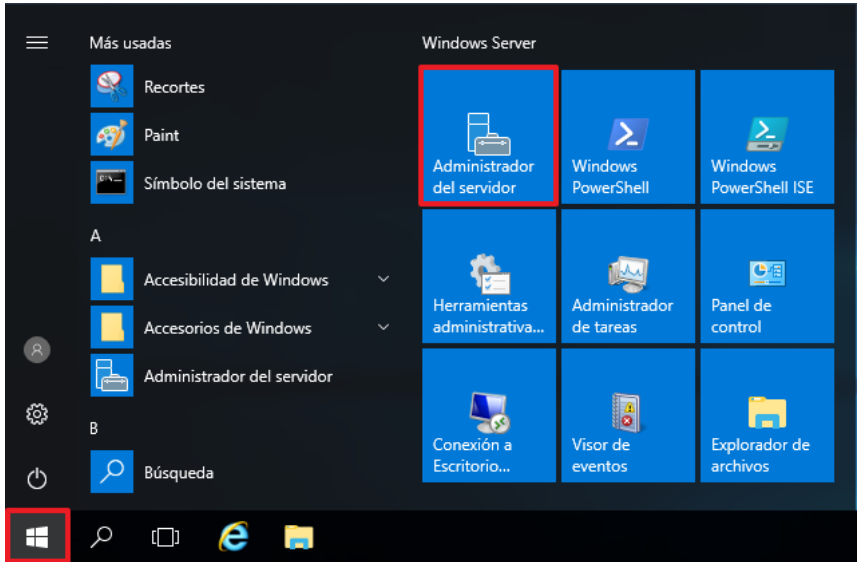
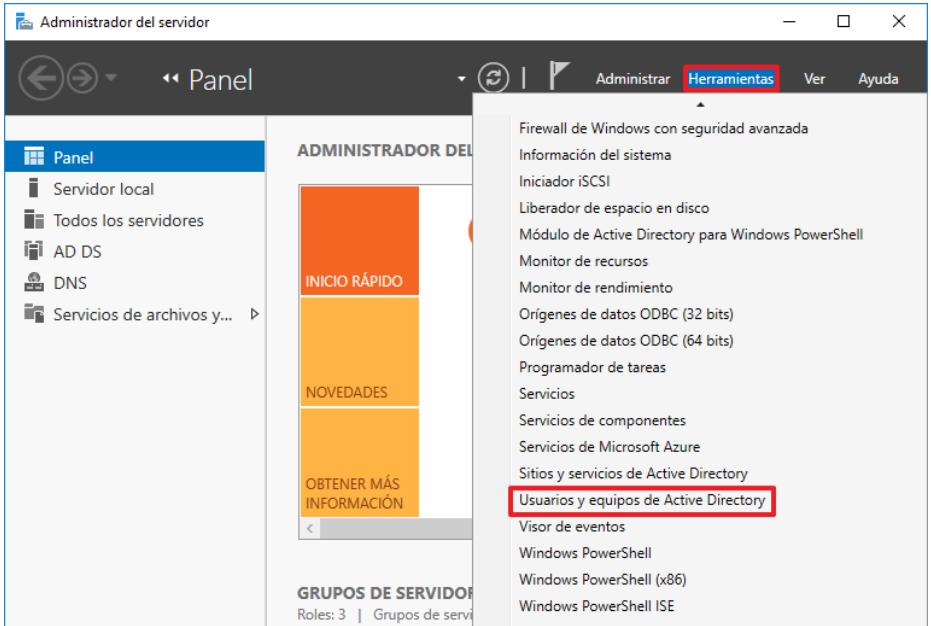
No obstante, este mecanismo de administración centralizado exige por parte de los administradores un control elevado y tener claro la creación y aplicación de diferentes políticas de seguridad en función de las necesidades demandadas por los servicios.

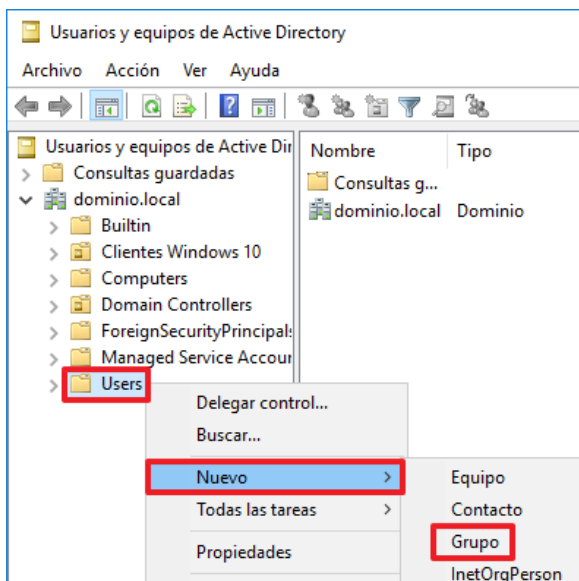
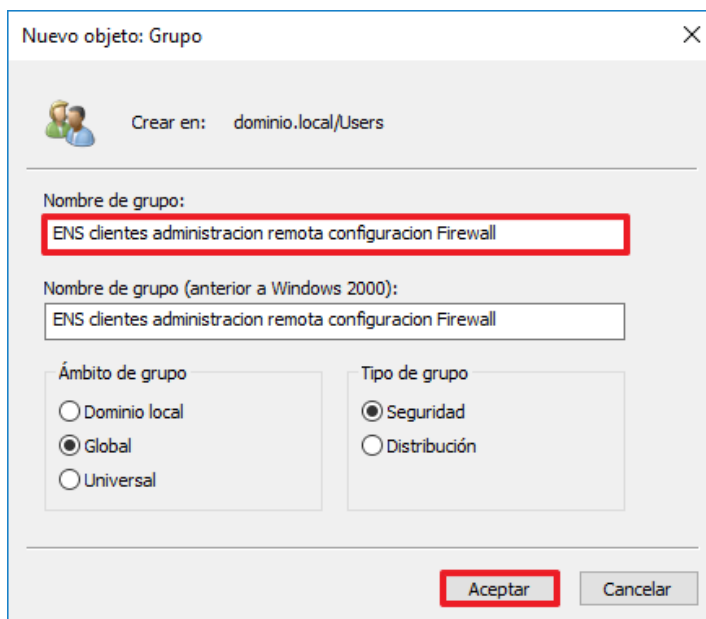
En este Anexo se darán recomendaciones necesarias para la creación y gestión de GPO para la administración centralizada de la seguridad del cortafuegos. Como en los Anexos previos, los operadores deberán realizar pruebas en entornos de preproducción antes de realizar una implementación en el entorno de producción.

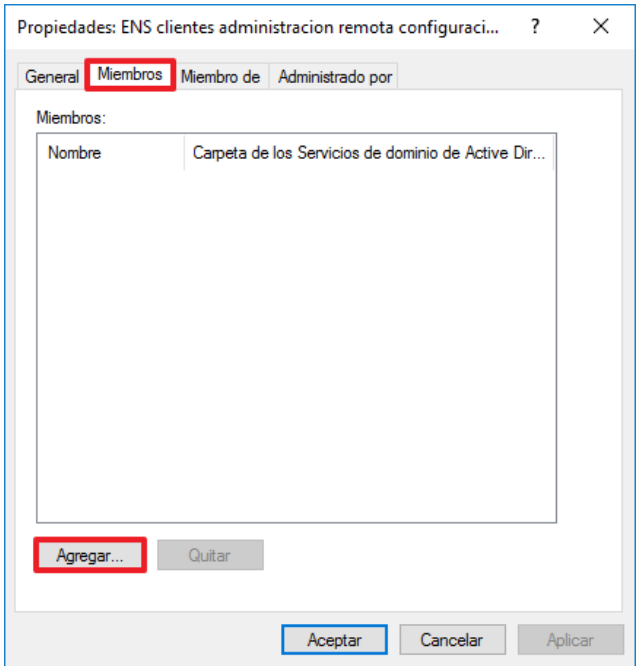
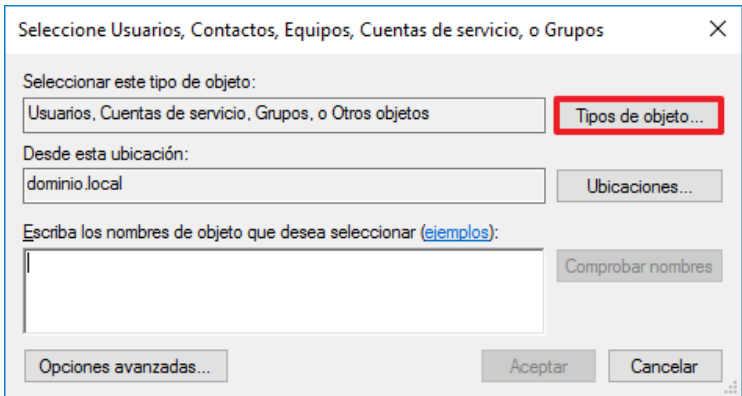
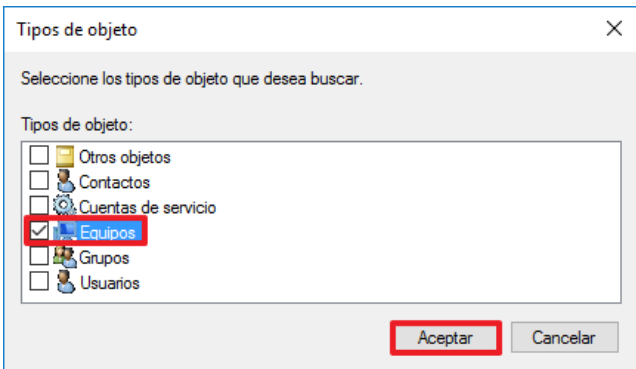
1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

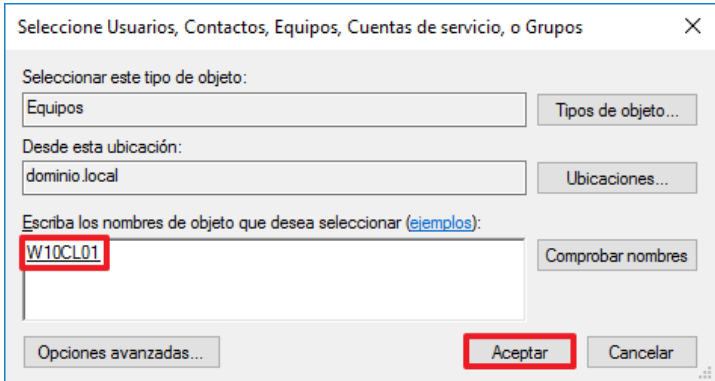
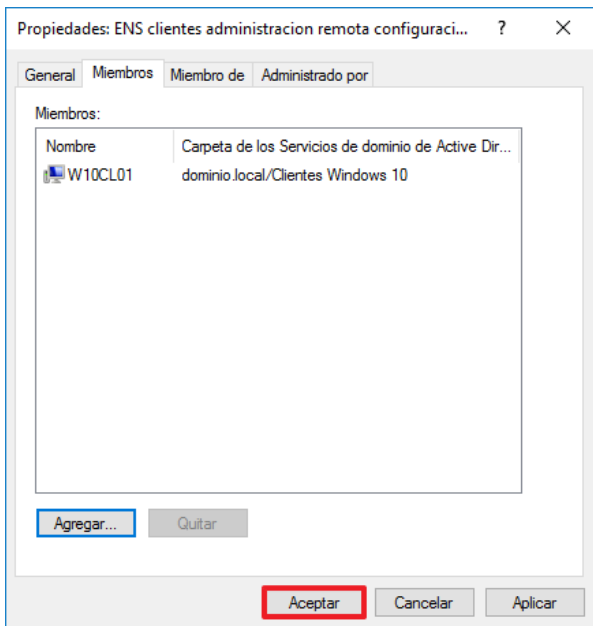
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos que permita la apertura de puertos para la realización de soporte remoto mediante el empleo de RDP (protocolo de escritorio remoto).

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
4.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Usuarios y equipos de Active Directory". 

Paso	Descripción
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
6.	Introduzca como nombre “ENS clientes administracion remota configuracion Firewall”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad en el cortafuegos.  Nota: Recuerde que este paso a paso es un ejemplo de cómo configurar un objeto de política de grupo para aplicar sobre un conjunto de clientes determinados con motivo de aplicarles una configuración específica. El presente ejemplo se basa en la agrupación de clientes sobre los que se va a realizar administración remota.
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.

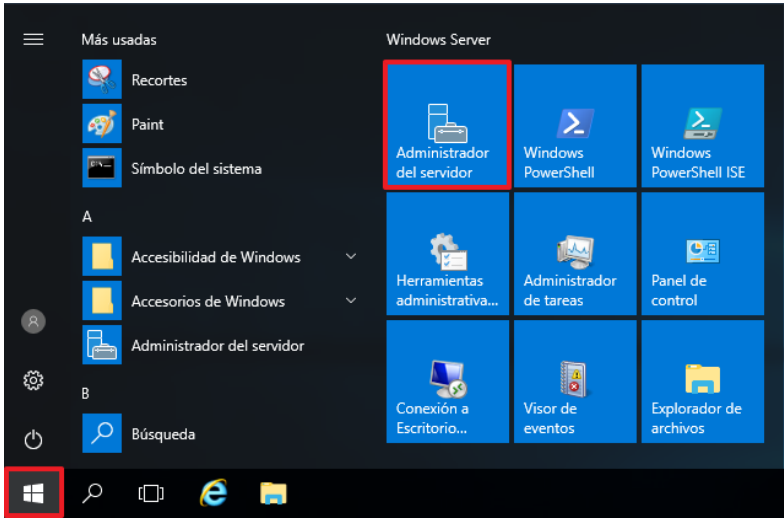
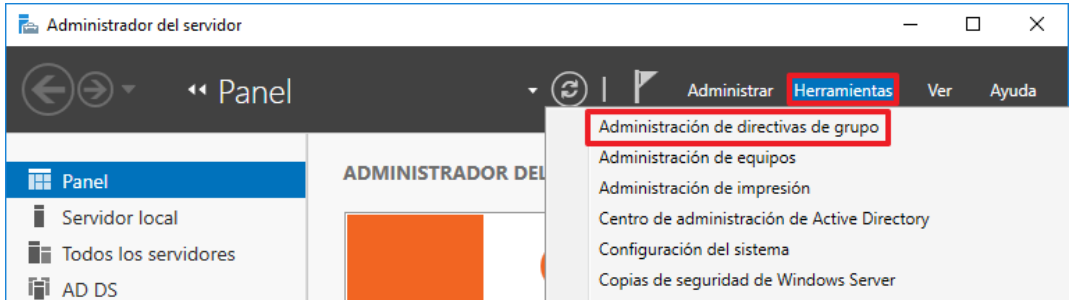
Paso	Descripción
8.	Pulse el botón “Agregar...”. 
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

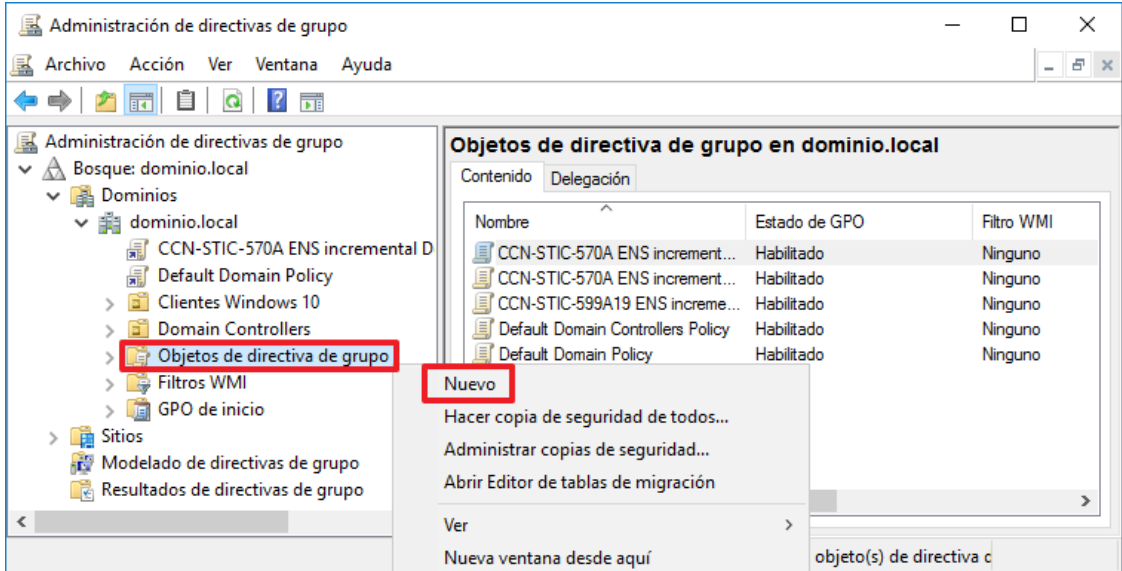
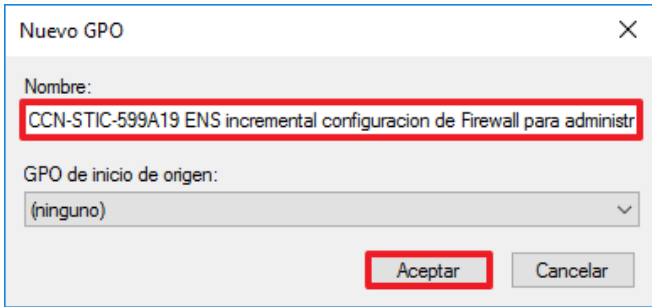
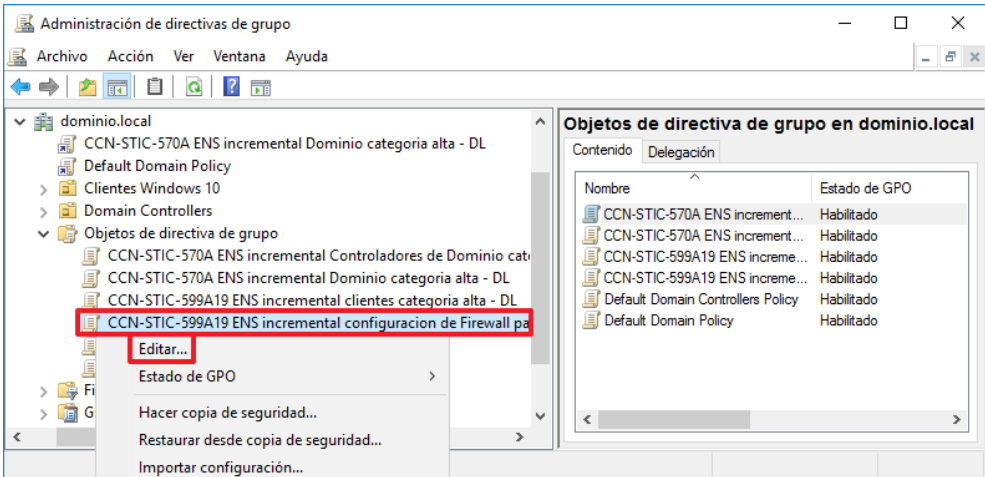
Paso	Descripción
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos equipos que cumplan las condiciones de aplicación de la GPO para la configuración del firewall. En este caso clientes sobre los que se vayan a efectuar tareas de administración remota con el protocolo RDP. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo. 
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”. Nota: El grupo creado, aunque en el ejemplo se va a emplear para la configuración del cortafuegos, se podría emplear para la aplicación de una configuración de seguridad aplicable a través de GPO diferente del resto de servidores de la organización.

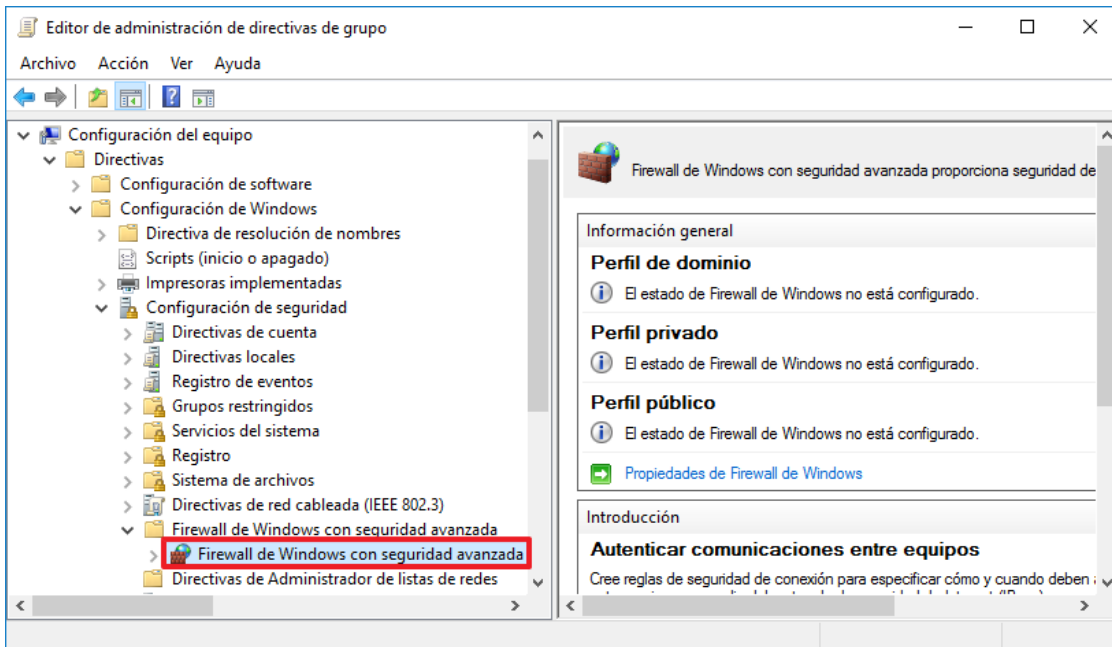
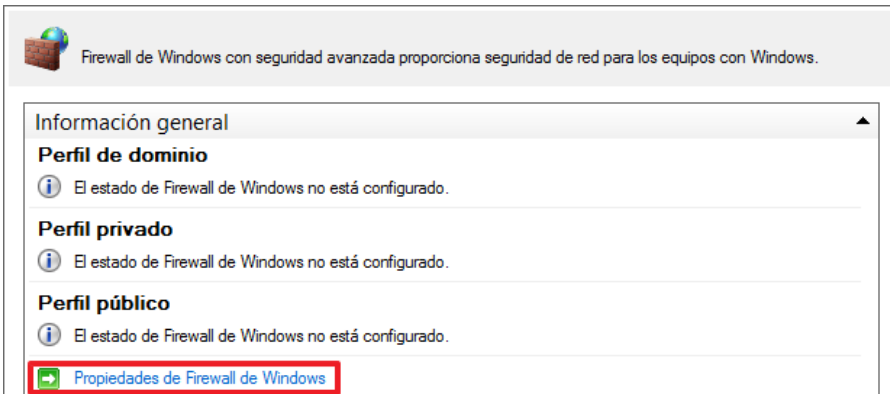
2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CORTAFUEGOS

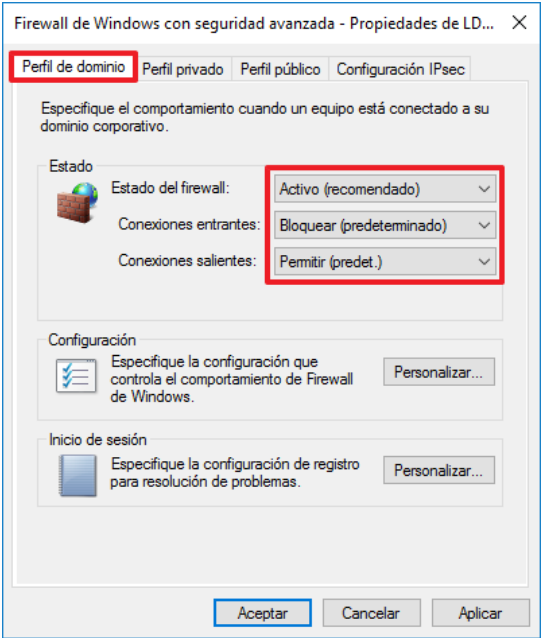
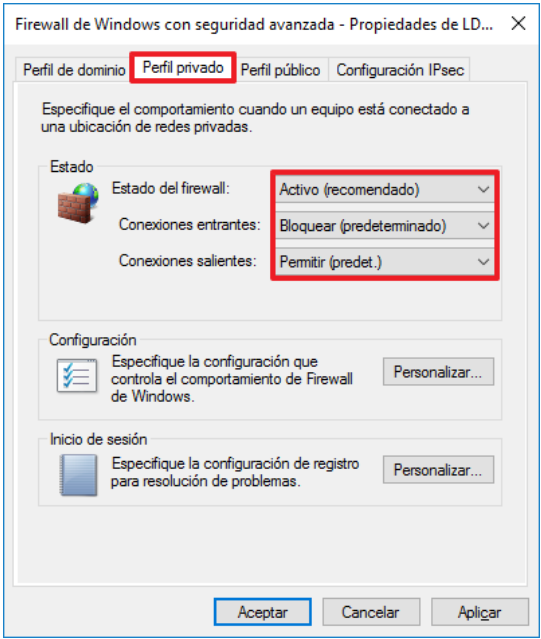
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política de cortafuegos. Deberá tomar en consideración las necesidades de qué puertos y/o aplicaciones o servicios son necesarios permitir para el conjunto de equipos clientes Windows 10.

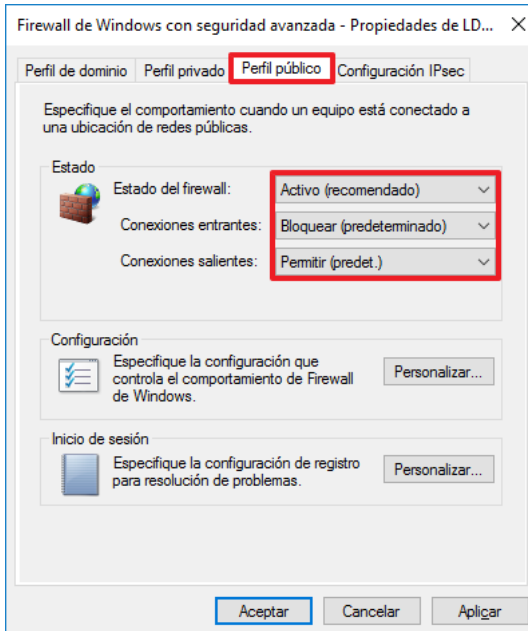
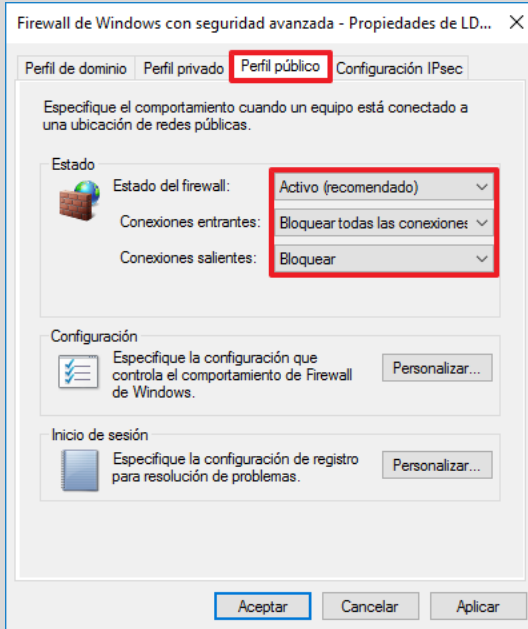
Nota: En el presente ejemplo se va a crear una política de grupo para la aplicación de política de cortafuegos para un conjunto de clientes a los que se va a permitir conexión para administración remota mediante RDP.

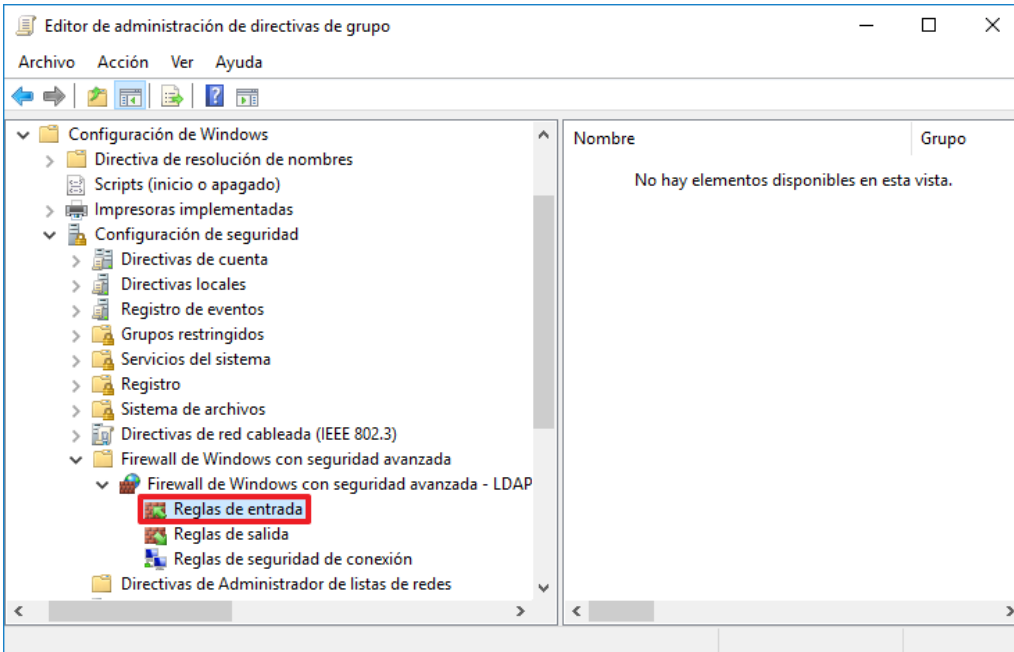
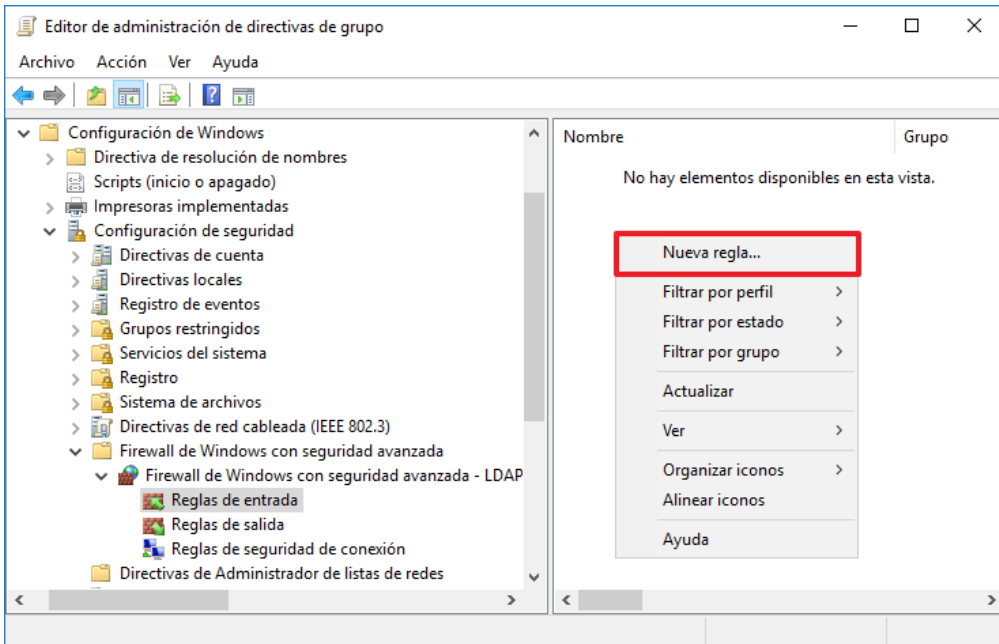
Paso	Descripción
14.	Inicie sesión en un servidor Controlador de Dominio del dominio.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
17.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas grupo". 
18.	Despliegue los contenedores y sitúese sobre la carpeta "Objetos de directiva de grupo".

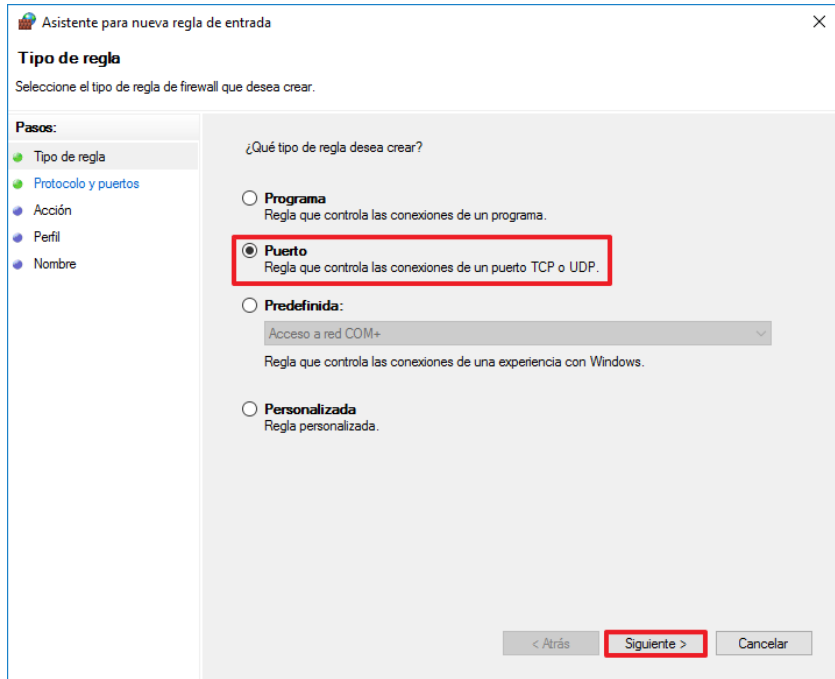
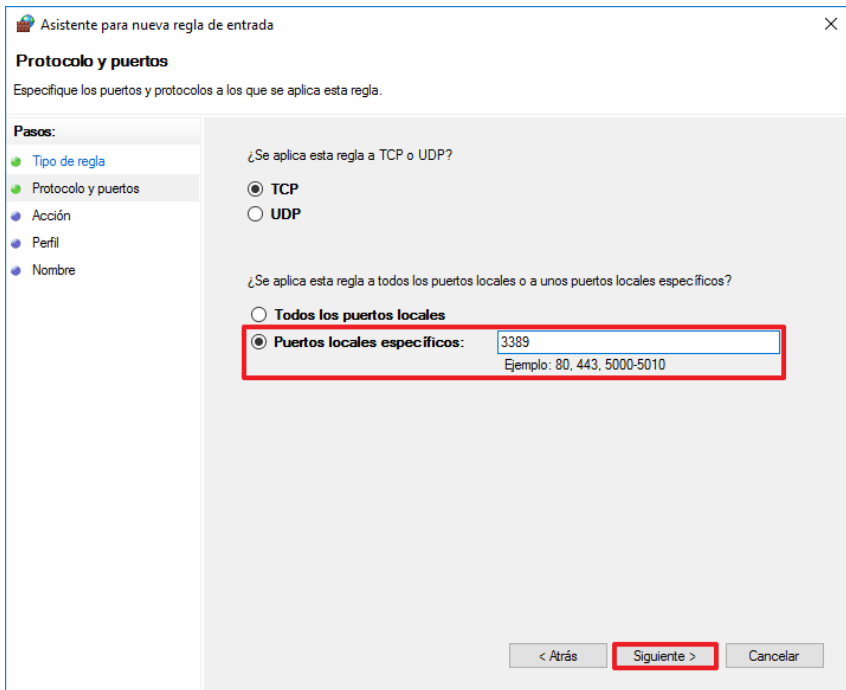
Paso	Descripción
19.	Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
20.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental configuracion de Firewall para administracion remota de cliente” y pulse el botón “Aceptar”. 
21.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 

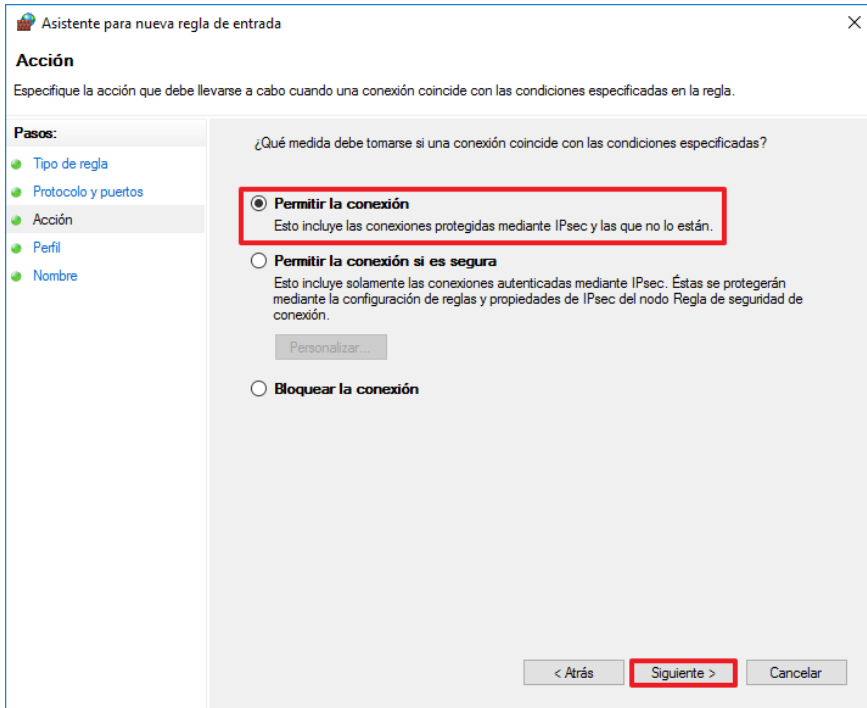
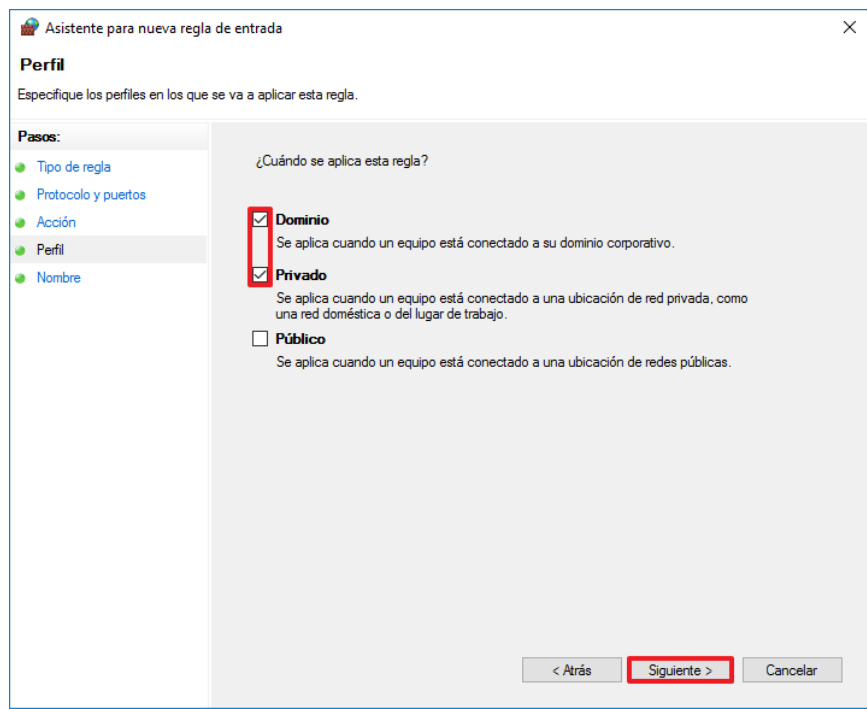
Paso	Descripción
22.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada – LDAP://CN=...  The screenshot shows the 'Editor de administración de directivas de grupo' window. The left pane displays a tree view under 'Configuración del equipo' > 'Directivas' > 'Configuración de Windows' > 'Configuración de seguridad'. The item 'Firewall de Windows con seguridad avanzada' is selected and highlighted with a red rectangle. The right pane shows the 'Firewall de Windows con seguridad avanzada' properties, with the 'Propiedades de Firewall de Windows' link highlighted in red.
23.	Pulse sobre las “Propiedades de Firewall de Windows” que aparece en el panel derecho.  The screenshot shows the 'Firewall de Windows con seguridad avanzada' window. The 'Información general' tab is selected. Under the 'Perfil de dominio', 'Perfil privado', and 'Perfil público' sections, the status is 'El estado de Firewall de Windows no está configurado.' The 'Propiedades de Firewall de Windows' link at the bottom is highlighted with a red rectangle.

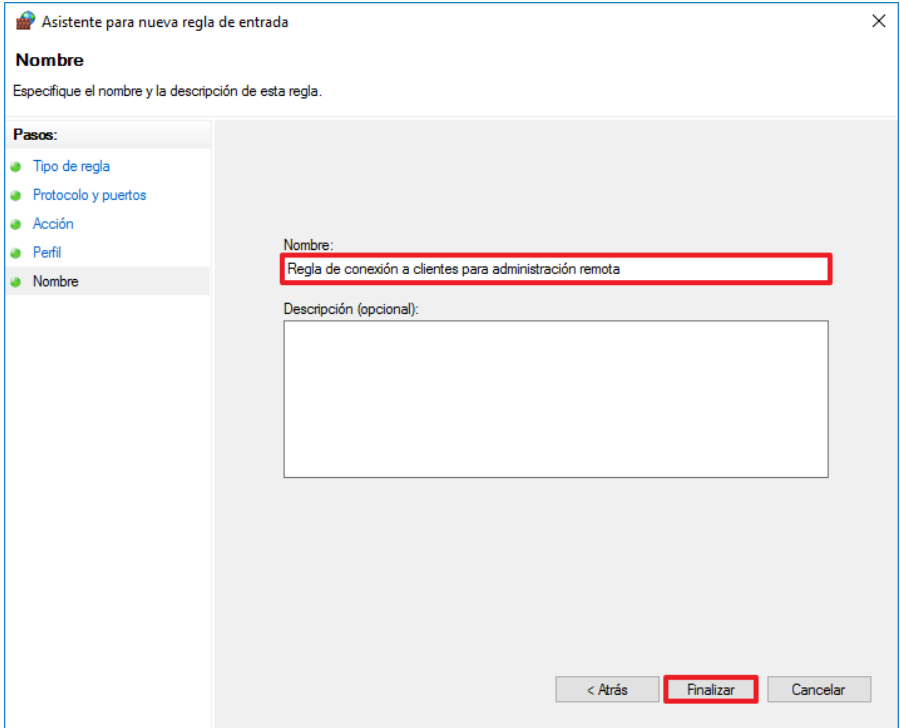
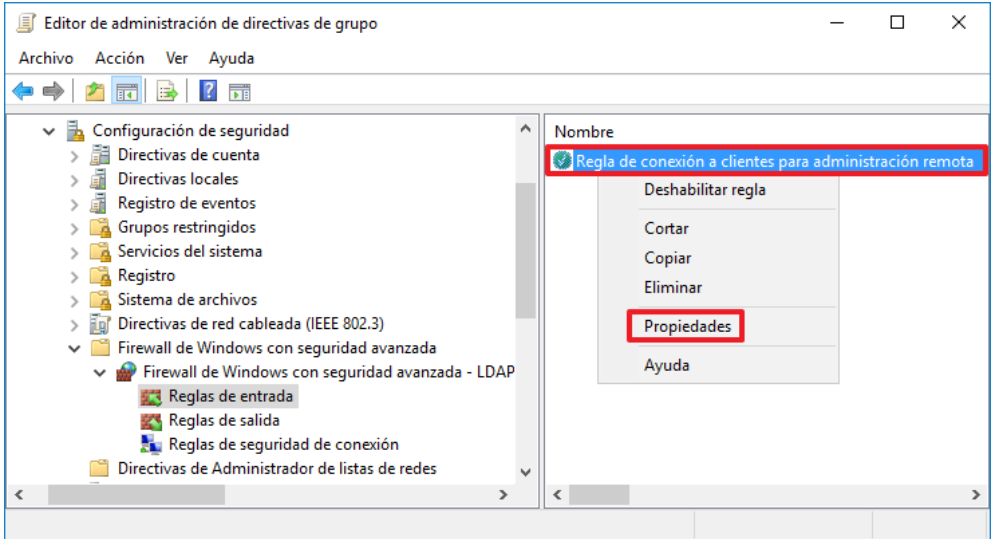
Paso	Descripción
24.	La primera de las pestañas, “Perfil de dominio”, configúrela como aparece en la siguiente imagen. 
25.	A continuación, vaya a la pestaña “Perfil privado” y configúrela tal y como aparece en la siguiente imagen. 

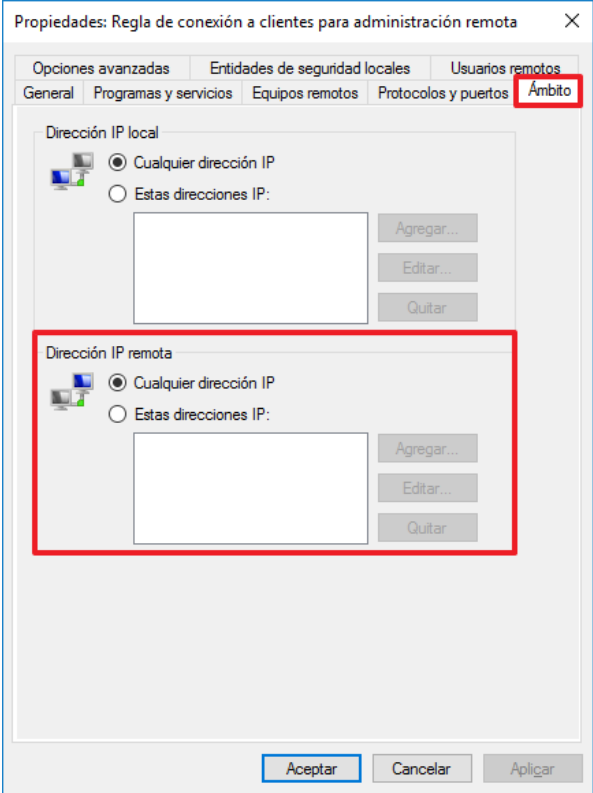
Paso	Descripción
26.	Vaya posteriormente a la pestaña “Perfil público” y establezca la configuración que aparece en la siguiente imagen.  Nota: En el caso de que los clientes estuvieran categorizados como alta, sería recomendable que el perfil público quedara configurado como aparece en la siguiente imagen. 
27.	Pulse el botón “Aceptar” para guardar los cambios introducidos en los diferentes perfiles.

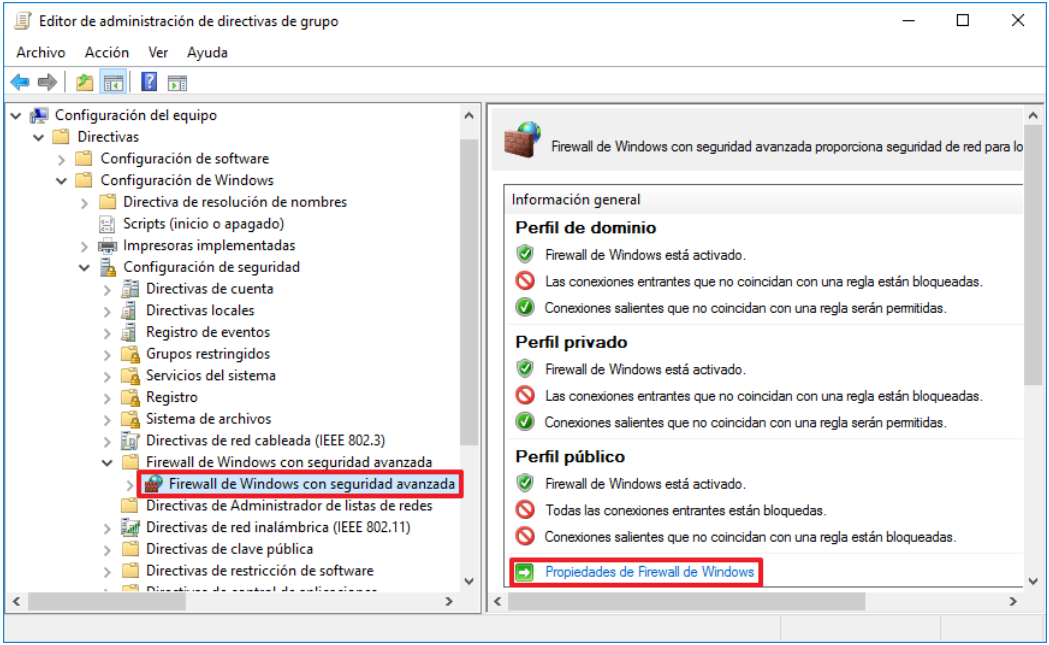
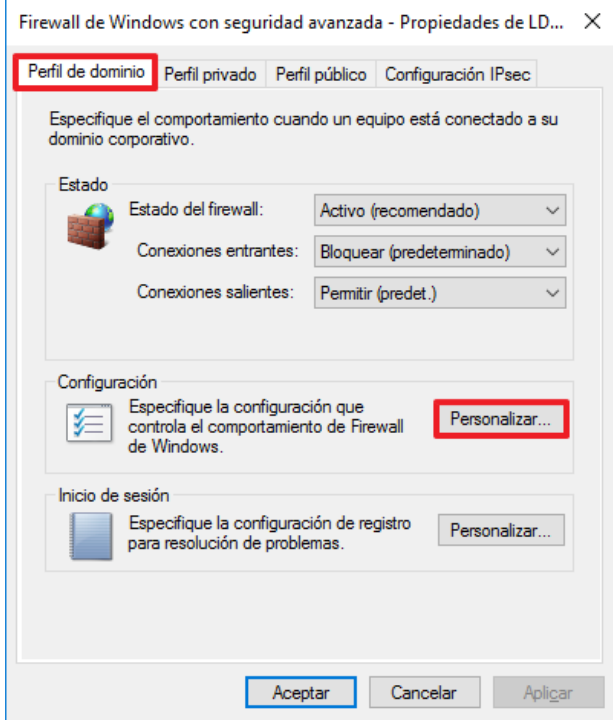
Paso	Descripción
28.	Despliegue el Firewall con seguridad avanzada y vaya al apartado “Reglas de entrada”. 
29.	Pulse con el botón derecho sobre un espacio en blanco en el panel derecho y seleccione la opción “Nueva regla...”. 

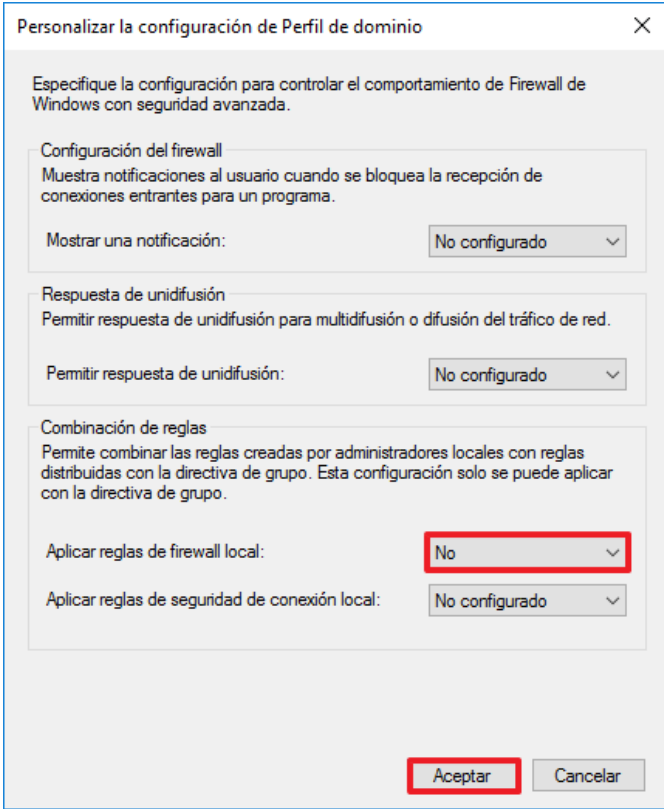
Paso	Descripción
30.	En el inicio del asistente seleccione la opción de “Puerto” y pulse el botón “Siguiete >”. 
31.	Seleccione la opción “Puertos locales específicos” e introduzca los puertos necesarios. Pulse el botón “Siguiete >”.  Nota: Para este ejemplo se utiliza el puerto “3389”.

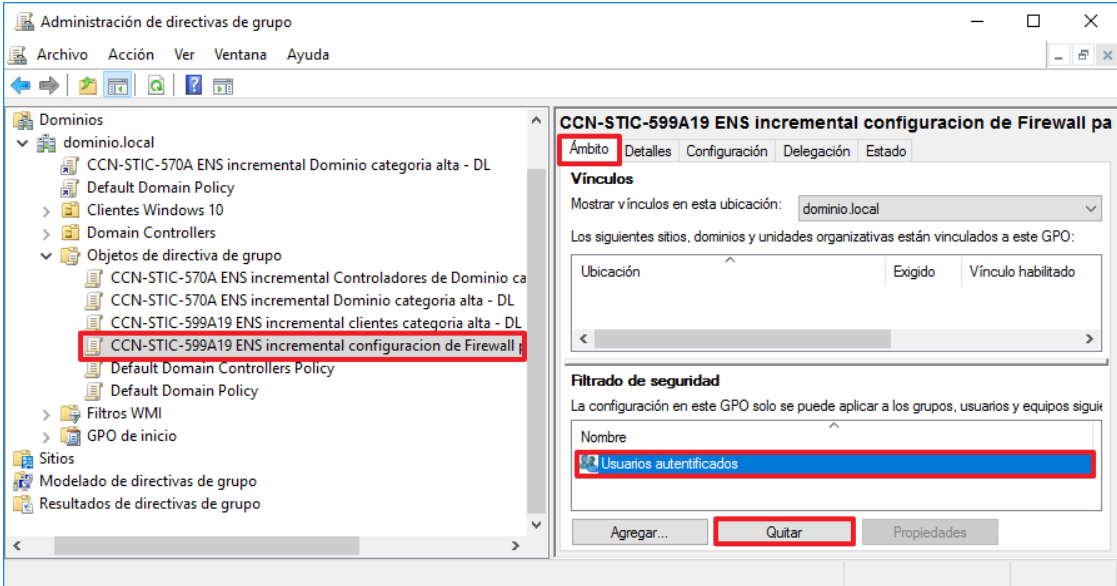
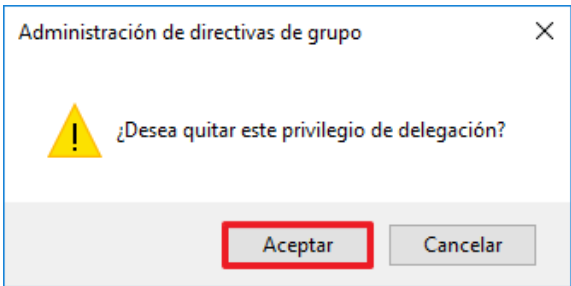
Paso	Descripción
32.	En la pantalla “Acción”, mantenga la configuración y pulse el botón “Siguiente >”. 
33.	En “Perfil”, marque los perfiles “Dominio” y “Privado” y desmarque el perfil “Público”. Pulse el botón “Siguiente >”. 

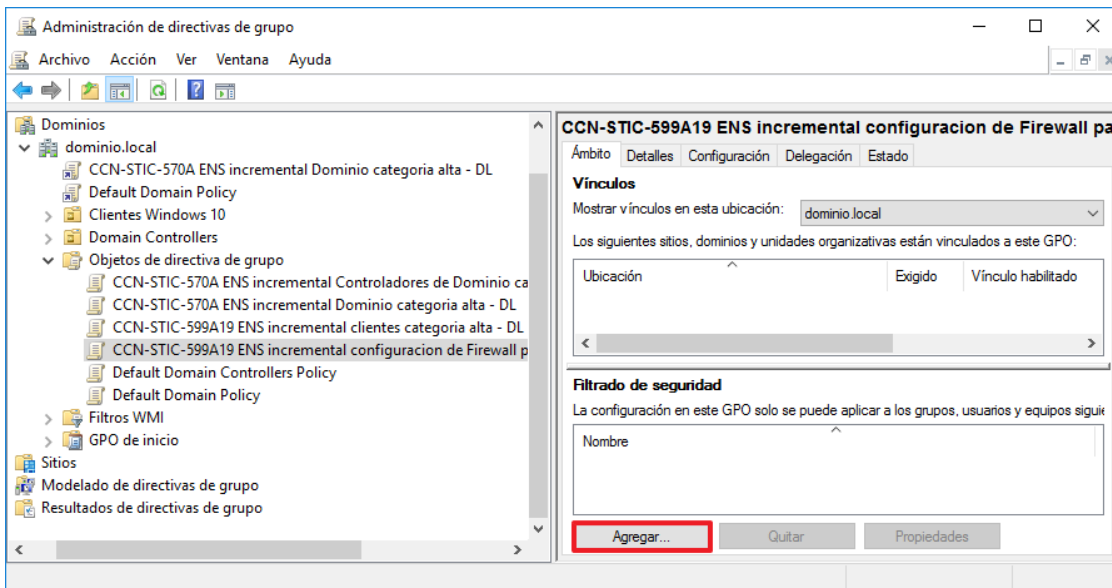
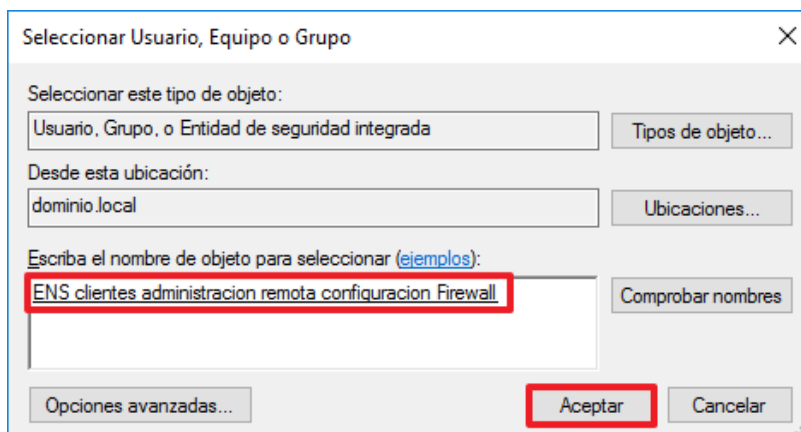
Paso	Descripción
34.	Asigne un nombre a la nueva regla de entrada que está creando y pulse el botón “Finalizar”.  Nota: En este ejemplo se asigna el nombre “Regla de conexión a clientes para administración remota”.
35.	La nueva regla ya se encuentra creada. Puede editarla pulsando con el botón derecho del ratón sobre la misma y seleccionando la opción “Propiedades”. 

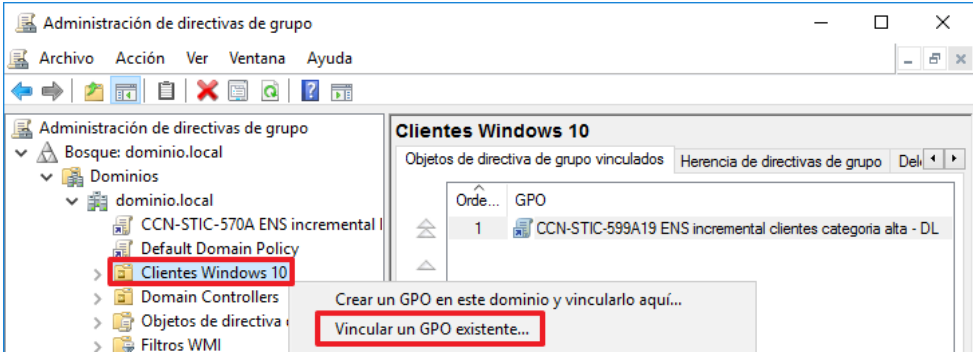
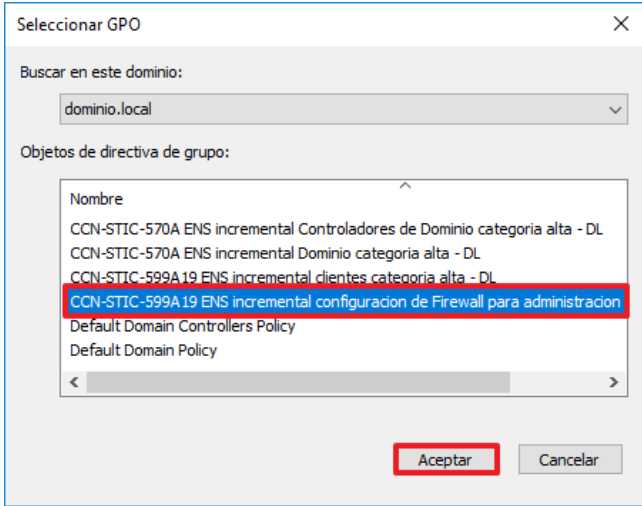
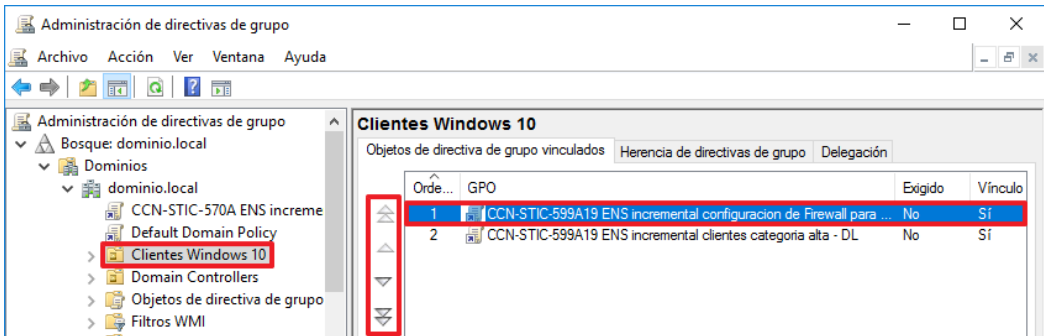
Paso	Descripción
36.	Se podría, por ejemplo, limitar las IP remotas o rangos de redes que podrían conectarse a los clientes para la administración remota, por ejemplo, si el personal de soporte o los administradores emplean una red concreta, direcciones IP fijas o bien asignada por asociación de MAC. De forma predetermina se admite cualquier IP, pero podría establecerse un límite a las mismas. 
37.	Una vez creada las reglas de entrada para los puertos del servicio de administración remota, debería determinarse si existe la necesidad de abrir otros puertos. Por ejemplo, si hay algún servicio en escucha en los clientes por ejemplo para la recolección de eventos. Deberá crear tantas reglas como sean necesarias en función de la necesidad de los clientes.
38.	En el caso de que los servicios fueran de categoría básica o media, deberá cerrarse la política y continuar en el paso 45. En el caso de que la categoría fuera alta / Difusión Limitada, deberá continuar con los siguientes pasos.

Paso	Descripción
39.	Seleccione nuevamente “Firewall con seguridad avanzada – LDAP://CN...” y seleccione la opción del panel derecho “Propiedades de Firewall de Windows”. 
40.	En la pestaña de dominio pulse el botón “Personalizar” del apartado “Configuración”. 

Paso	Descripción
41.	En “Combinación de reglas” configure la opción “Aplicar reglas de firewall local”. Seleccione “No” y pulse el botón “Aceptar”. 
42.	Haga lo mismo para los perfiles “Privado” y “Público”.
43.	Una vez modificado los tres perfiles pulse el botón “Aceptar”. Esto impedirá que la configuración de cortafuegos que se realice localmente tenga alguna validez. Solo será de aplicación la configuración del dominio. Nota: Tenga en cuenta este hecho para agregar reglas que se estuvieran aplicando localmente en los clientes al objeto GPO que se está creando”.
44.	Cierre la política creada.
45.	Una vez creada la política, ésta deberá asignarse al grupo creado en pasos anteriores, del presente Anexo. Para ello seleccione la política recién creada y vaya al panel derecho de su configuración en la herramienta “Administración de directivas de grupo”.

Paso	Descripción
46.	En la pestaña “Ámbito” seleccione el grupo “Usuarios autenticados” y pulse el botón “Quitar”. 
47.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
48.	A continuación, pulse el botón “Agregar...”. 
49.	Introduzca el nombre del grupo creado en el primer paso del presente Anexo y pulse el botón “Aceptar”. 
50.	Solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.

Paso	Descripción
51.	Seleccione la Unida Organizativa y pulsando con el botón derecho haga uso de la opción “Vincular un GPO existente...”. 
52.	En la pantalla de selección, marque la GPO creada previamente y pulse “Aceptar”. 
53.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el panel derecho. 
54.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.
55.	Deberá crear tantos objetos GPO como fueran necesarias, siendo asignados a los clientes Windows 10.

ANEXO C.4.2. CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA MS WINDOWS 10

1. CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO

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 GPO. 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 ésta con Microsoft para el mantenimiento de sus equipos.

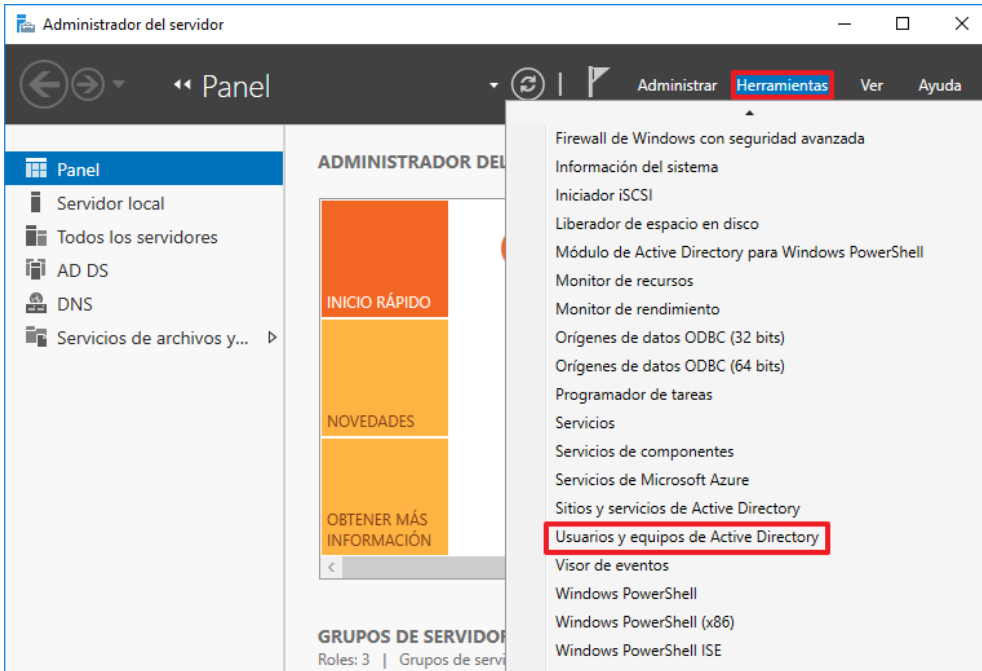
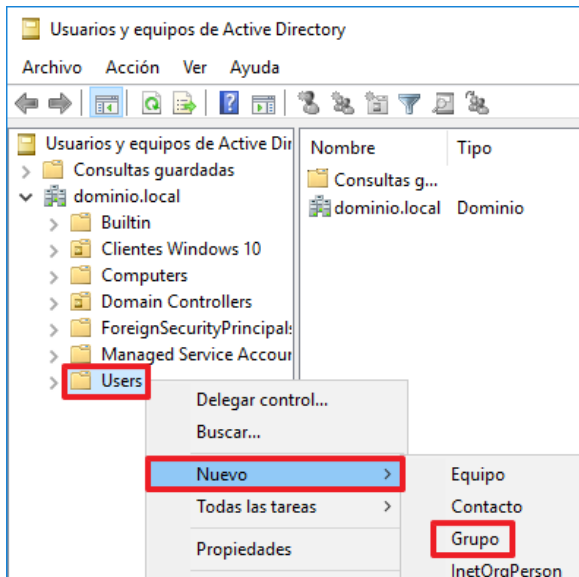
Debe tener en consideración que determinados componentes tales como Windows Defender ATP, podrían llegar a requerir al menos un nivel de telemetría de tipo básico.

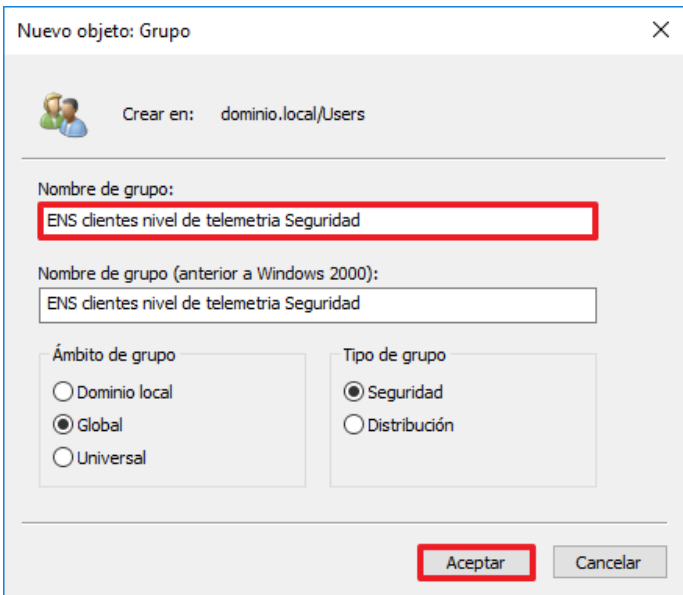
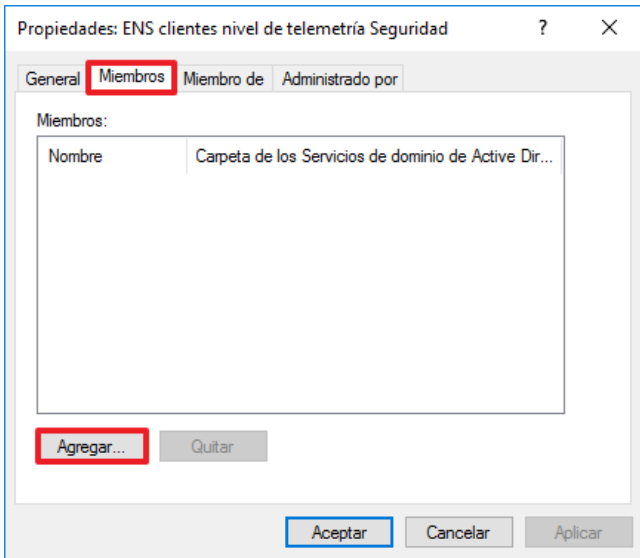
1.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

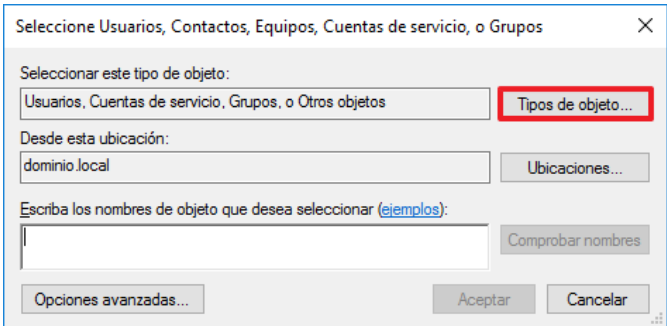
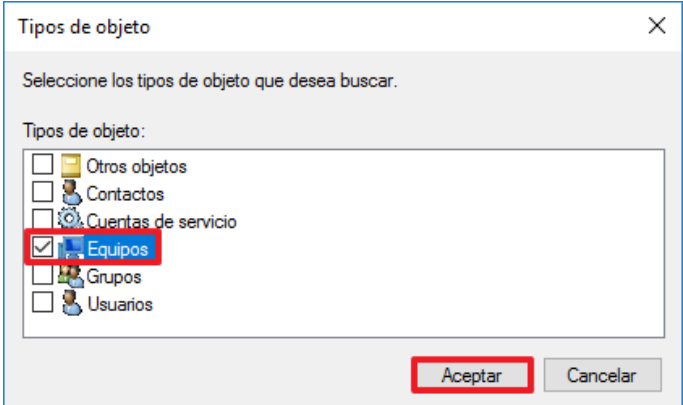
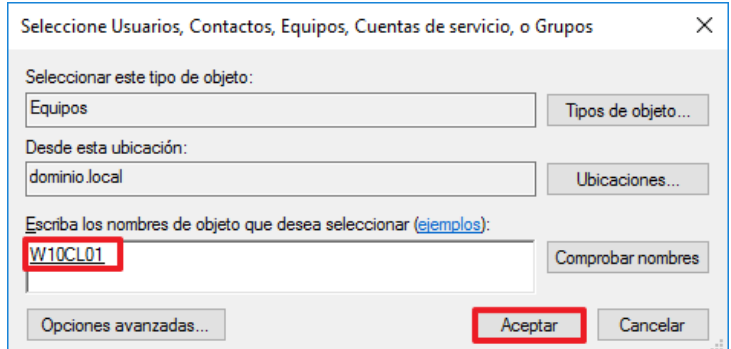
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

Nota: En el presente ejemplo se va a crear una política de grupo para la configuración del valor de telemetría que permita a la organización adaptar sus equipos a las exigencias establecidas por el ENS. Se van a mostrar las distintas posibilidades de configuración para dicho valor. En caso de precisar de distintos niveles de telemetría, sería conveniente crear un grupo para cada uno de estos niveles.

Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

Paso	Descripción
4.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

Paso	Descripción
6.	Introduzca como nombre “ENS clientes nivel de telemetría Seguridad”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO que implementen el nivel de telemetría estipulado para dicho grupo.  Nota: Recuerde que este paso a paso es un ejemplo de cómo configurar un objeto de política de grupo para aplicar sobre un conjunto de clientes determinados con motivo de aplicarles una configuración específica. Una sugerencia para los nombres de grupo en caso de precisar distintos niveles de telemetría sería incluir el nivel que se va a estipular para cada grupo. En este caso al establecer un nivel de telemetría de “Seguridad” el nombre a aplicar será “ENS clientes nivel de telemetría Seguridad”.
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.
8.	Pulse el botón “Agregar...”. 

Paso	Descripción
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos servidores miembro que cumplan las condiciones de aplicación de la GPO para los distintos niveles de telemetría. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”. Nota: El grupo creado, aunque en el ejemplo se va a emplear para la configuración del nivel para la telemetría, se podría emplear para la aplicación de una configuración de seguridad aplicable a través de GPO diferente del resto de servidores de la organización.

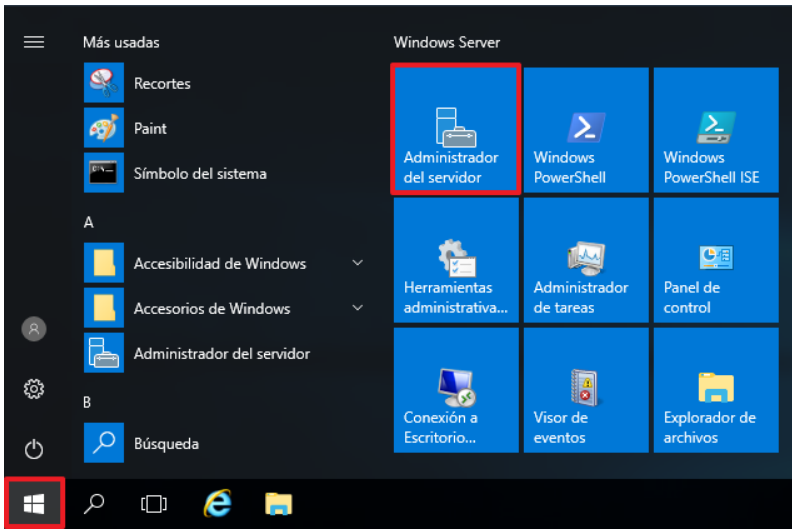
1.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA DE CONFIGURACIÓN DEL VALOR DE TELEMETRÍA

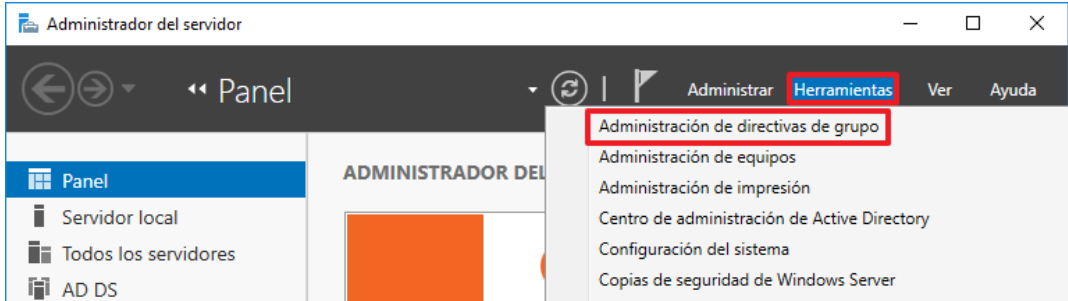
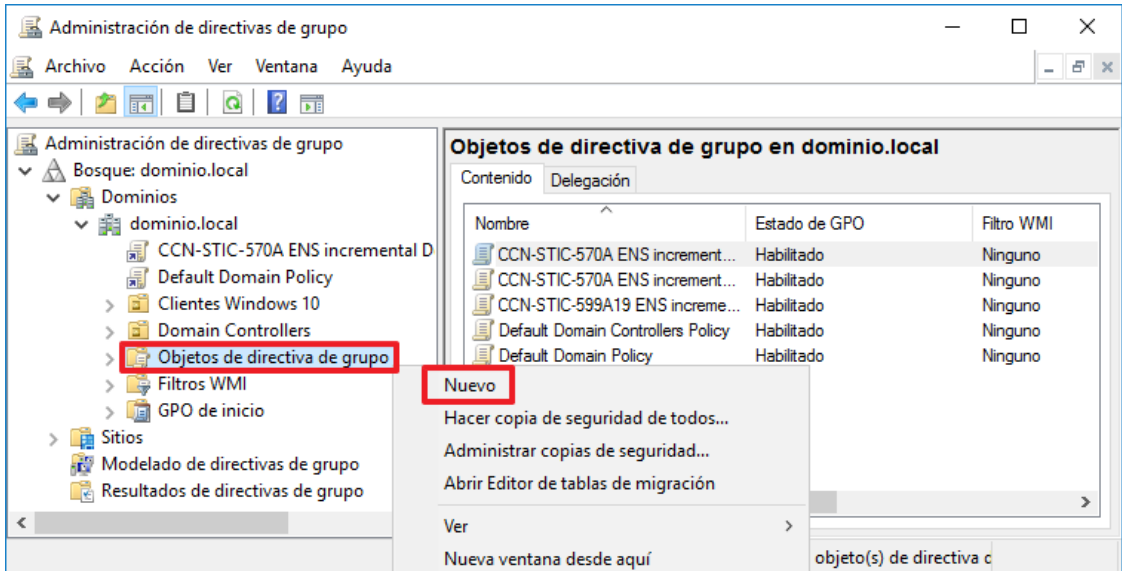
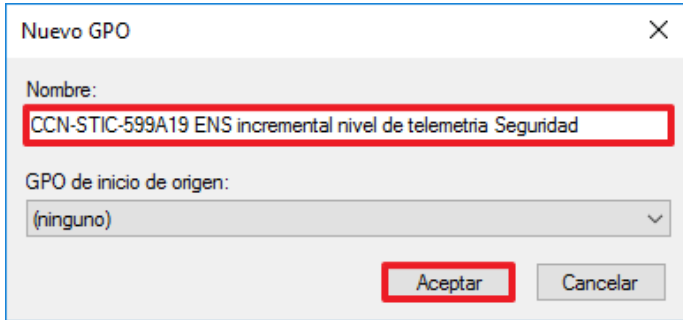
El comportamiento de la telemetría difiere dependiendo de la edición utilizada de Windows 10, Enterprise o Pro. En el caso de la edición Enterprise la telemetría puede establecerse hasta de un valor 0 (Seguridad) mientras que en la edición Pro en el caso de establecer un valor 0, esta será tomada por parte del sistema operativo como un valor 1 (Básico) no siendo posible la configuración en valor 0 (Seguridad) en las ediciones Pro de Windows 10.

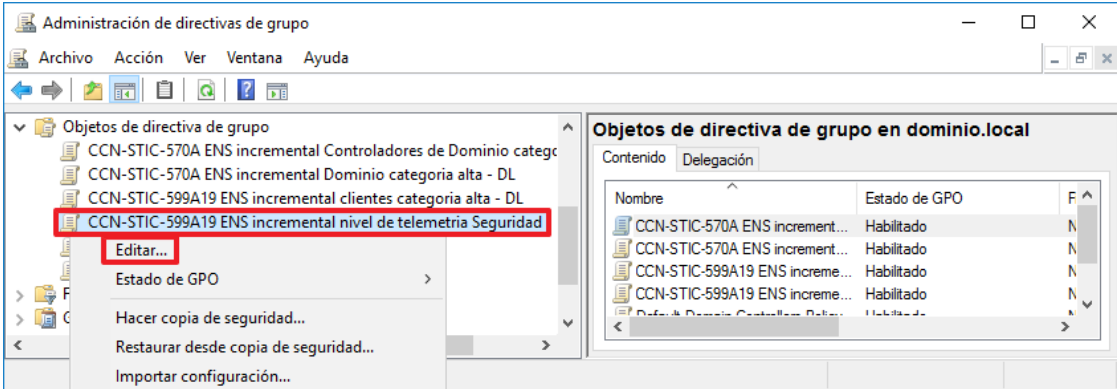
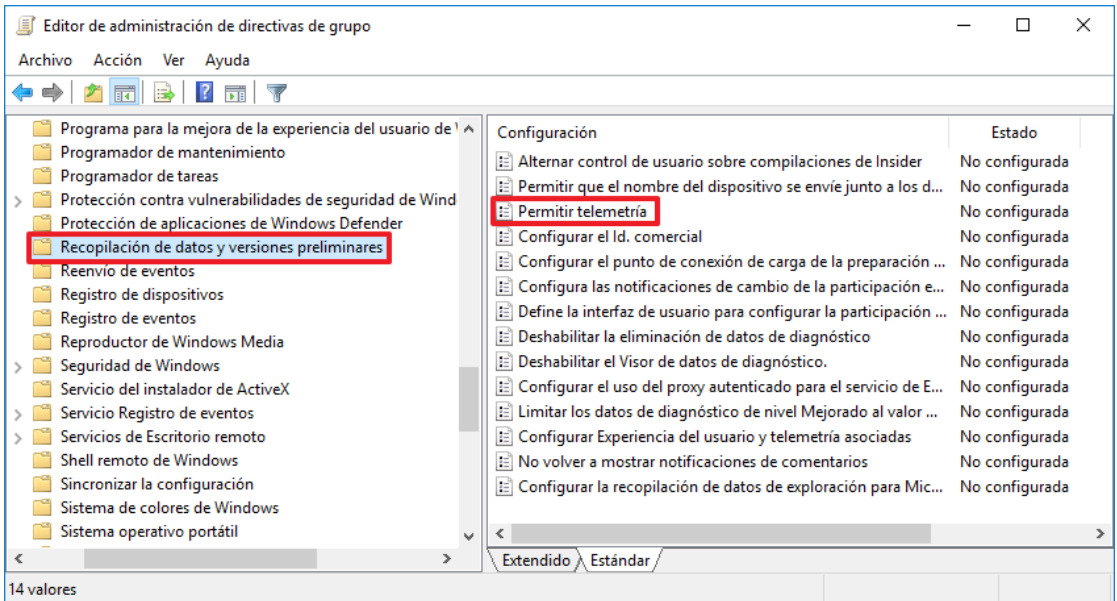
Nota: Establecer un valor de telemetría 0 supone el no funcionamiento de otras directivas como puede ser la aplicación de diferentes opciones de mantenimiento por lo que deberá tener muy en consideración esta casuística.

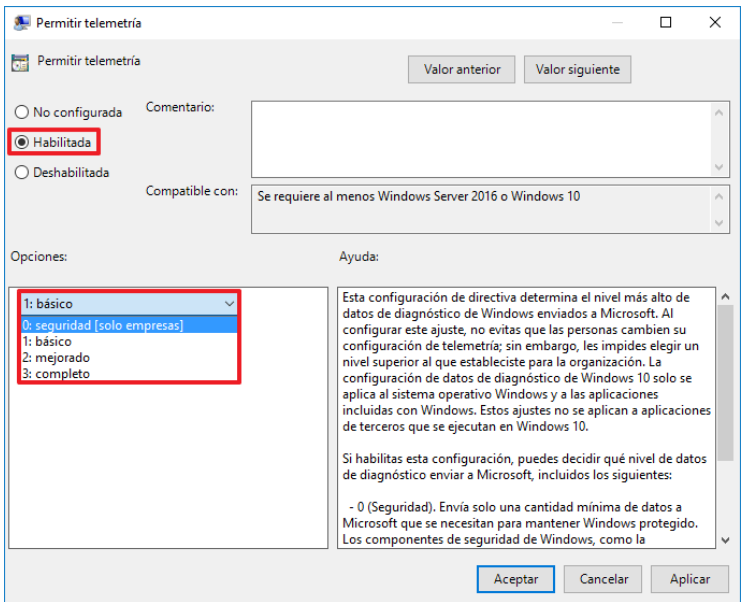
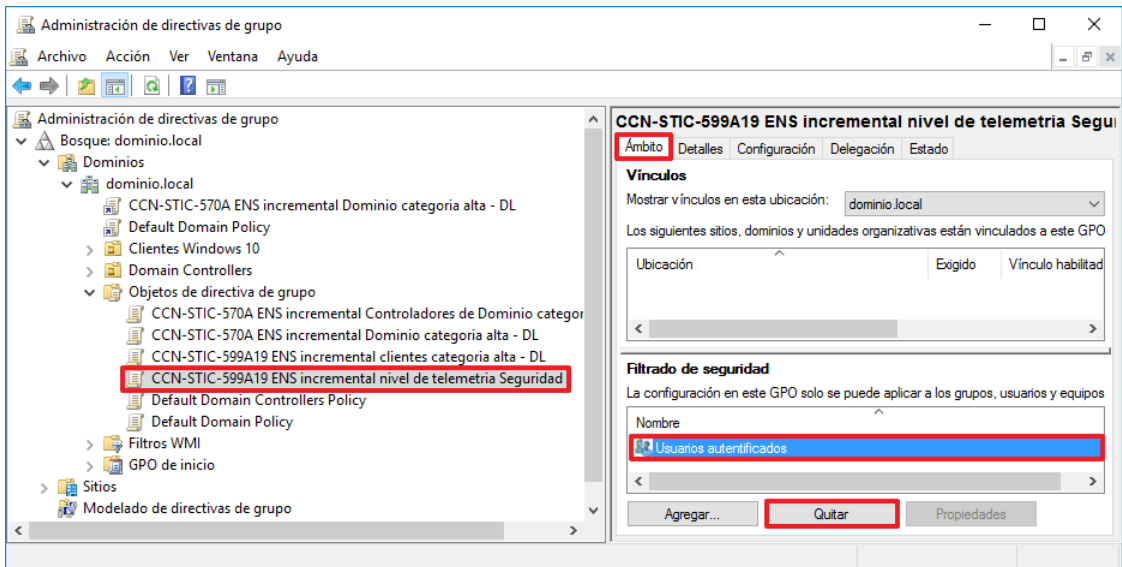
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política de configuración de valor de telemetría.

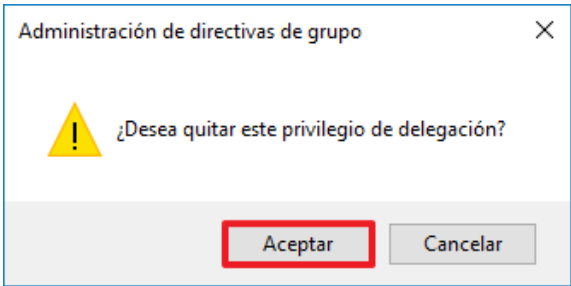
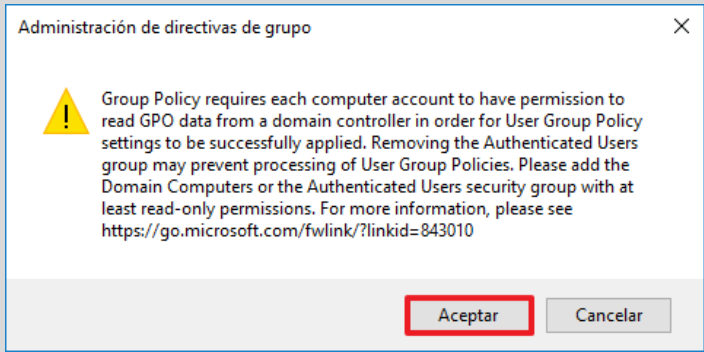
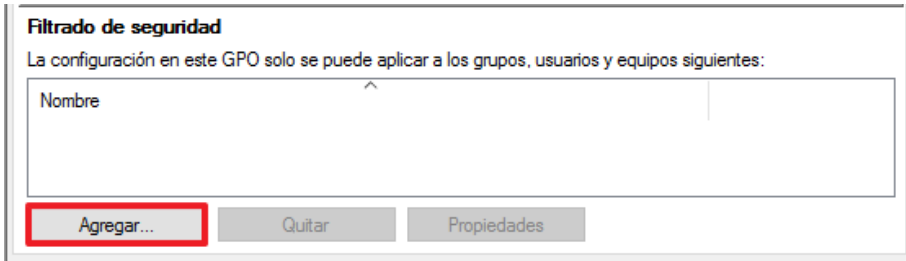
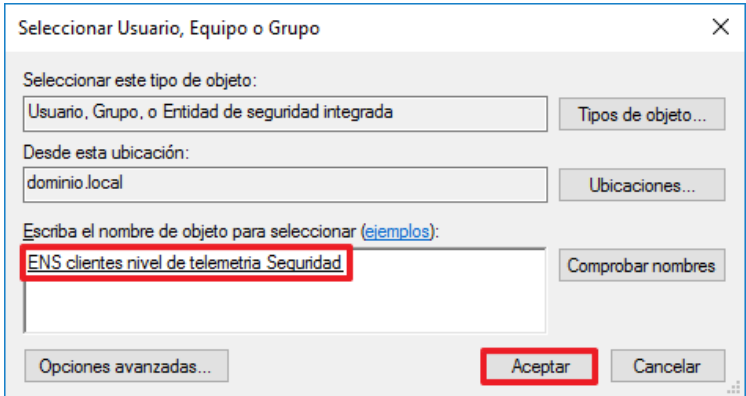
A continuación, se va a mostrar el procedimiento para modificar el valor de telemetría acorde a las necesidades de la organización. Deberá tomar en consideración que determinadas funcionalidades del sistema, como Windows Defender ATP, podrían requerir un mínimo de nivel de telemetría. Consulte la información del fabricante para establecer el nivel de telemetría más adecuado para su organización.

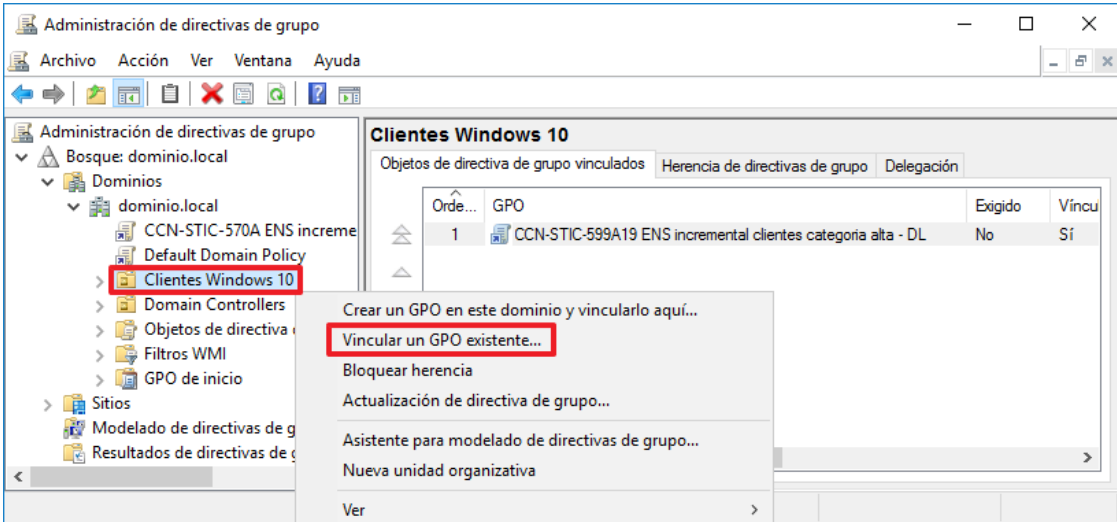
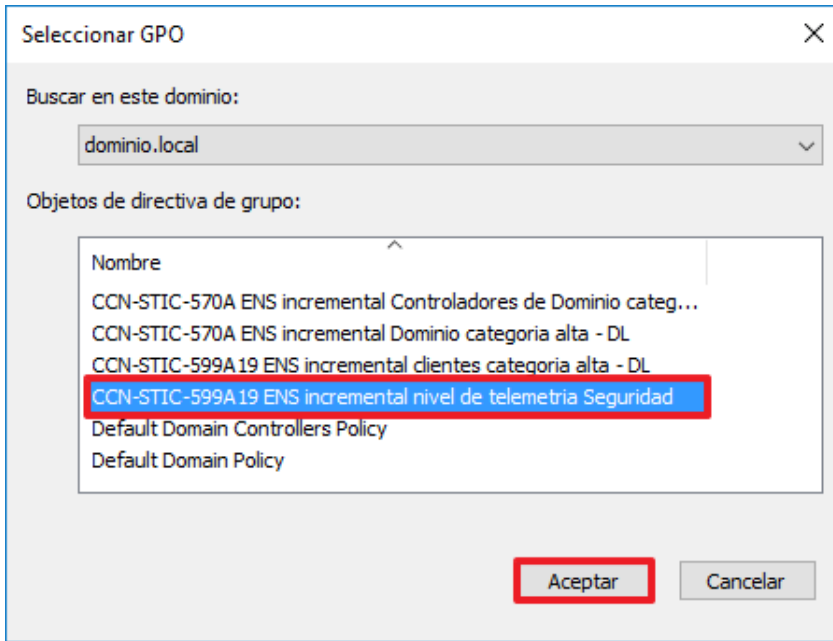
Paso	Descripción
14.	Inicie sesión en un servidor Controlador de Dominio del dominio.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

Paso	Descripción
17.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas grupo”. 
18.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
19.	Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
20.	Introduzca como nombre “CCN-STIC-599A19 ENS incremental nivel de telemetria Seguridad” y pulse el botón “Aceptar”. 

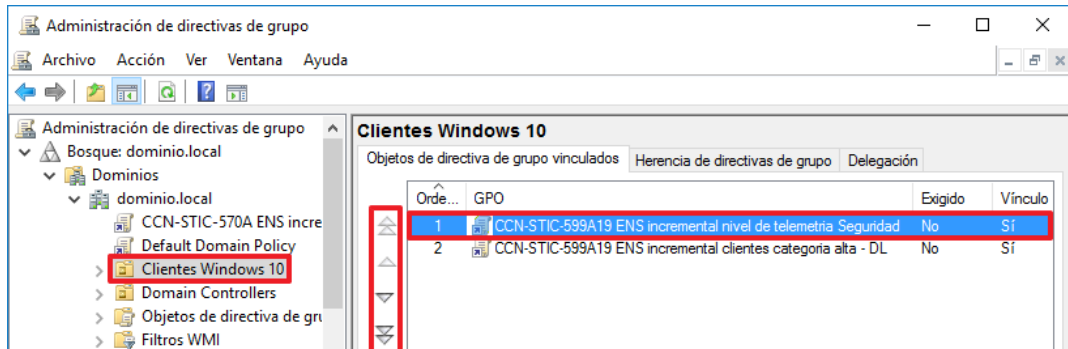
Paso	Descripción
21.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar...”. 
22.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. Configuración de equipo → Directivas → Plantillas administrativas → Componentes de Windows → Recopilación de datos y versiones preliminares 
23.	En el panel derecho haga doble clic sobre “Permitir telemetría”. Se abrirá una ventana con la administración de la configuración para el valor de nivel de telemetría.

Paso	Descripción
24.	En la ventana emergente pulse sobre “Habilitada”. En este punto encontrará un desplegable en el que se muestran los diferentes niveles que se le puede otorgar al componente de telemetría acorde a las necesidades de la organización. Establezca el valor de telemetría en función de las necesidades de su organización. 
25.	Una vez definido el valor de telemetría en el desplegable sólo quedaría guardar la configuración pulsando el botón “Aceptar”.
26.	Cierre el editor de políticas.
27.	Una vez editada la política, esta deberá asignarse al grupo creado en pasos anteriores del presente Anexo. Para ello seleccione la política recién creada y vaya al panel derecho de su configuración.
28.	En la pestaña “Ámbito” seleccione el grupo “Usuarios autenticados” y pulse el botón “Quitar”. 

Paso	Descripción
29.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 
30.	A continuación, pulse el botón “Agregar...”. 
31.	Introduzca el nombre del grupo creado en el primer paso del presente Anexo y pulse el botón “Aceptar”. 

Paso	Descripción
32.	Solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.
33.	Seleccione la Unida Organizativa y pulsando con el botón derecho sobre ella seleccione la opción “Vincular un GPO existente...”. 
34.	En la pantalla de selección, marque la GPO creada previamente y pulse “Aceptar”. 
35.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.

Paso	Descripción
36.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el cuadro de la derecha.



The screenshot shows the 'Administración de directivas de grupo' window. On the left, the tree view shows 'dominio.local' > 'Clientes Windows 10' highlighted with a red box. On the right, the 'Objetos de directiva de grupo vinculados' tab shows a list of GPOs. The first GPO, 'CCN-STIC-599A19 ENS incremental nivel de telemetría Seguridad', is highlighted with a red box and is being moved to the top of the list using the up arrow icon.

Orden	GPO	Exigido	Vínculo
1	CCN-STIC-599A19 ENS incremental nivel de telemetría Seguridad	No	Sí
2	CCN-STIC-599A19 ENS incremental clientes categoría alta - DL	No	Sí

2. CONFIGURACIÓN DE OPCIÓN DE MANTENIMIENTO PARA WINDOWS 10

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 rama 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 rama semianual, tal y como se determina en el siguiente paso a paso.

Adicionalmente para que se puedan realizar pruebas anticipadas que permitan evaluar los cambios que provocan las actualizaciones de Windows 10, sería aconsejable establecer un grupo de control de equipos en modo rama semianual (dirigida), a efectos de que éstos reciban las actualizaciones de funcionalidades dentro del ciclo tempranos. Esto permitirá anticipar problemas de funcionalidad en dichos equipos, antes de que el despliegue de las actualizaciones se realice sobre toda la organización.

Debe tomar en consideración que la configuración establecida mediante GPO establece la opción de mantenimiento en modo rama semianual. Establecer determinados sistemas en modo rama semianual (dirigida) le permite anticipar que consecuencias tendrán las nuevas actualizaciones con respecto a los equipos de su organización.

El siguiente paso a paso establece los siguientes elementos:

- Configuración del objeto GPO de Windows 10 en modo rama semianual para la opción de mantenimiento.
- Creación de un grupo de equipos que tendrán establecido la opción de mantenimiento en modo rama semianual (dirigida).
- Asignación de una GPO a dicho grupo de equipos para configurarlos en la opción de mantenimiento en modo rama semianual (dirigida).

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 rama semianual (dirigida).

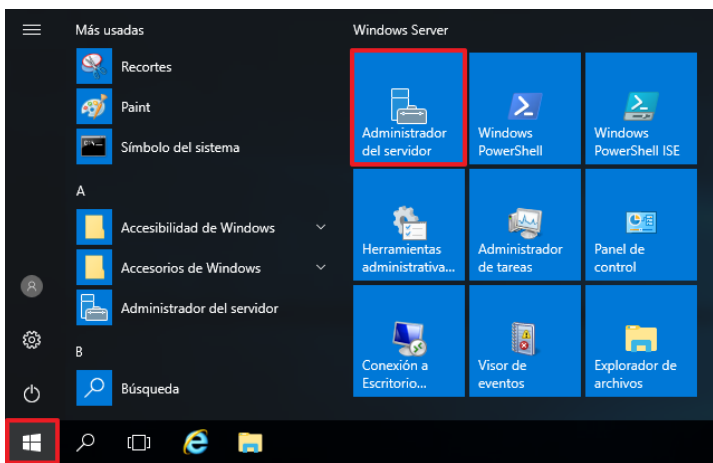
Nota: Tenga en cuenta la nueva nomenclatura adoptada por Microsoft para las opciones de mantenimiento del sistema operativo Windows 10:

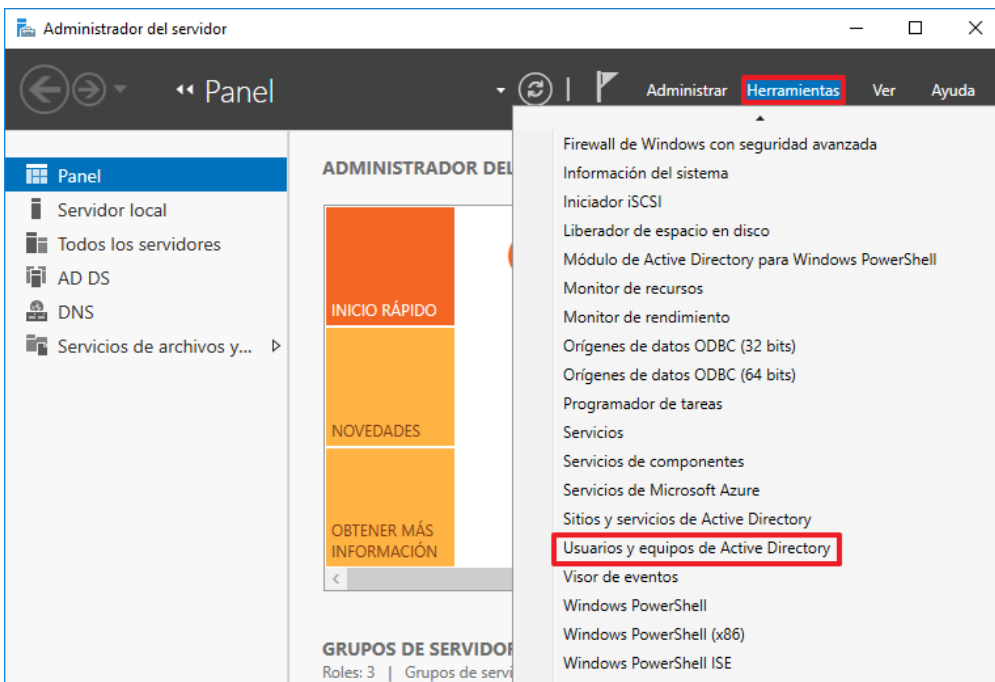
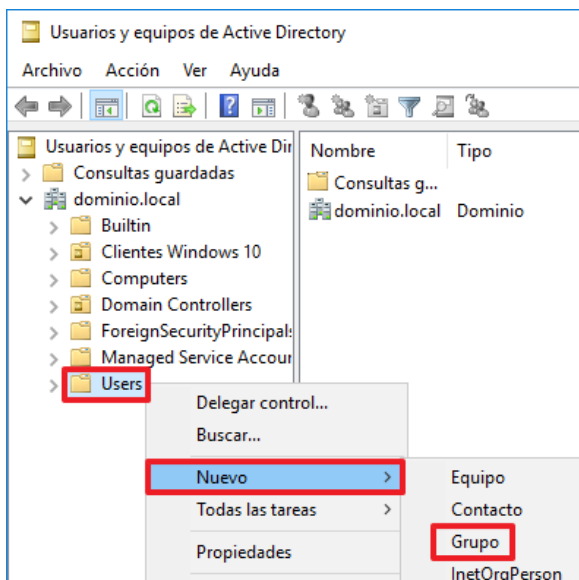
- CB: rama semianual (dirigida).
- CBB: rama semianual.
- Canal de mantenimiento a largo plazo (LTSC): canal de mantenimiento a largo plazo (LTSC).

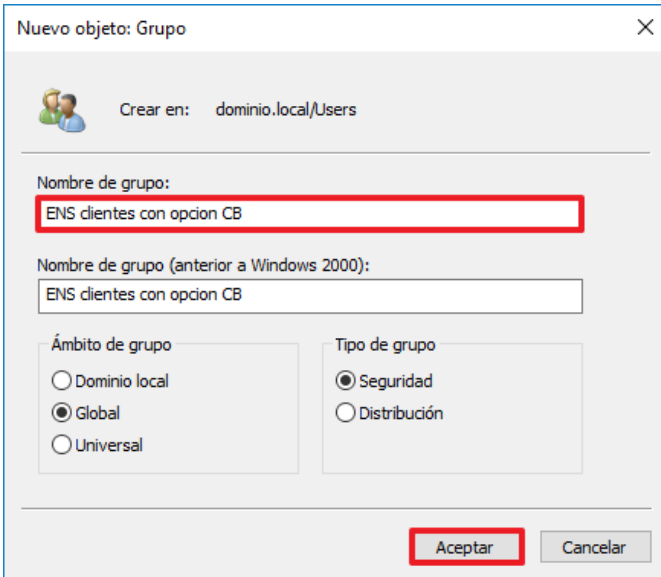
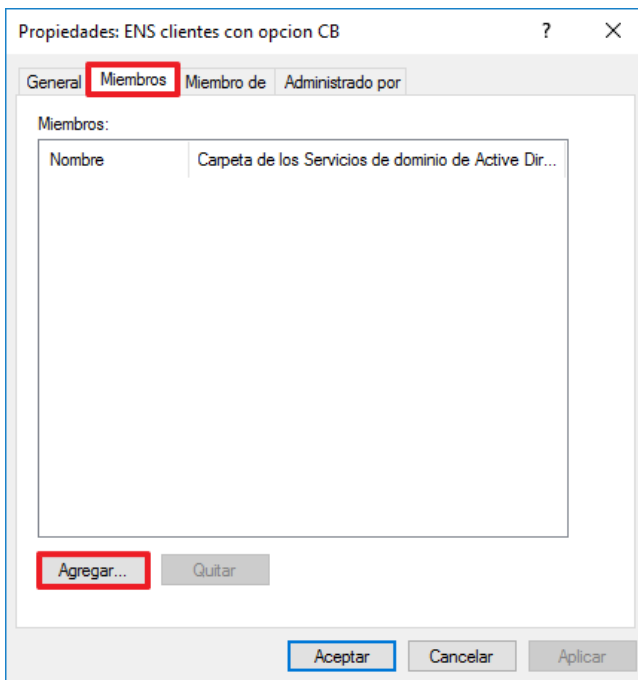
2.1. CREACIÓN DE GRUPO PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

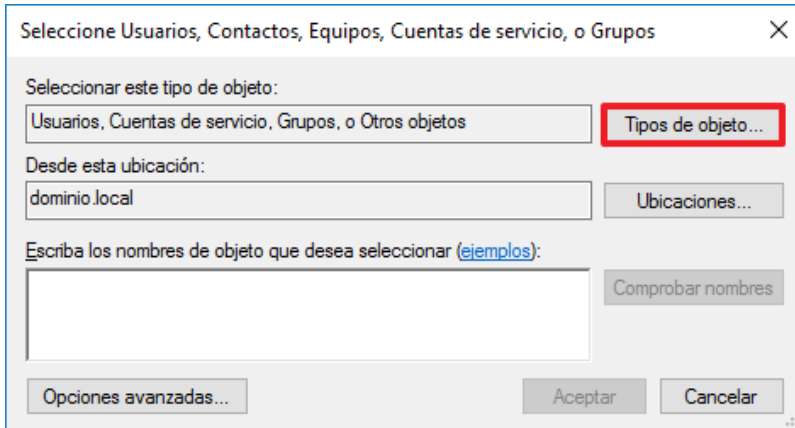
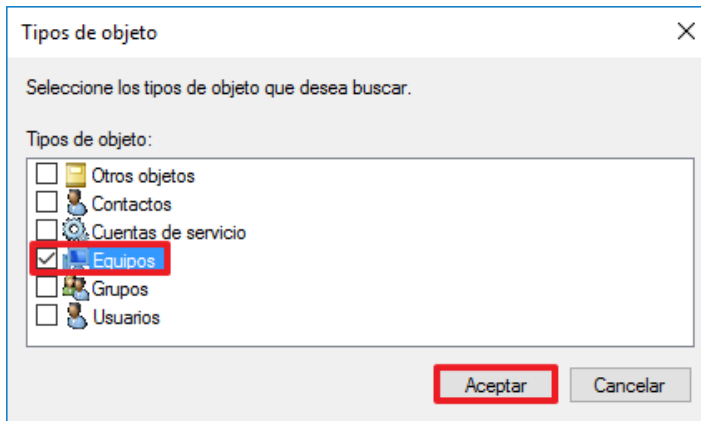
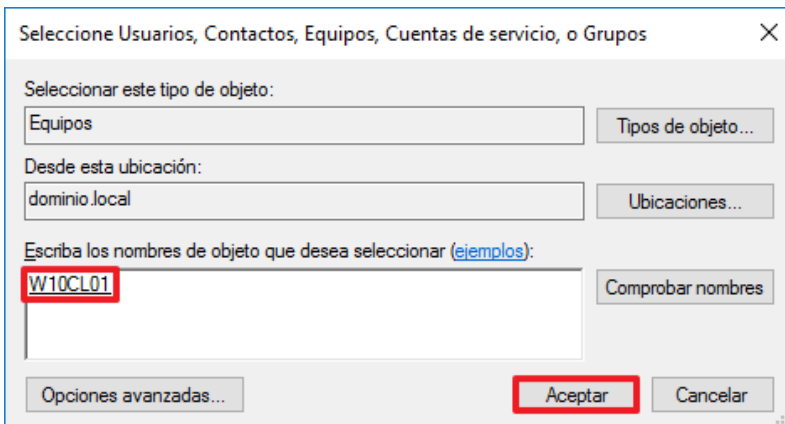
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

Nota: En el presente ejemplo se va a crear una política de grupo para establecer determinados puestos de trabajo en la opción CB, rama semianual (dirigida).

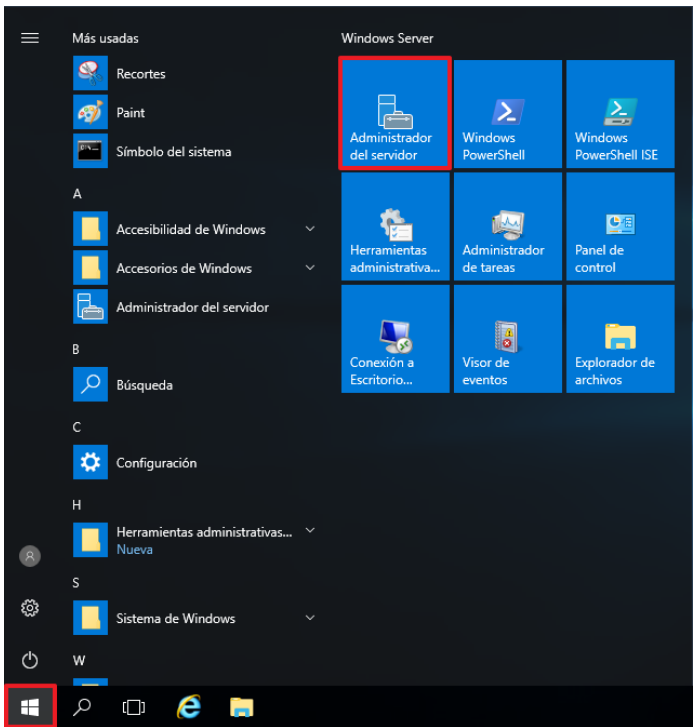
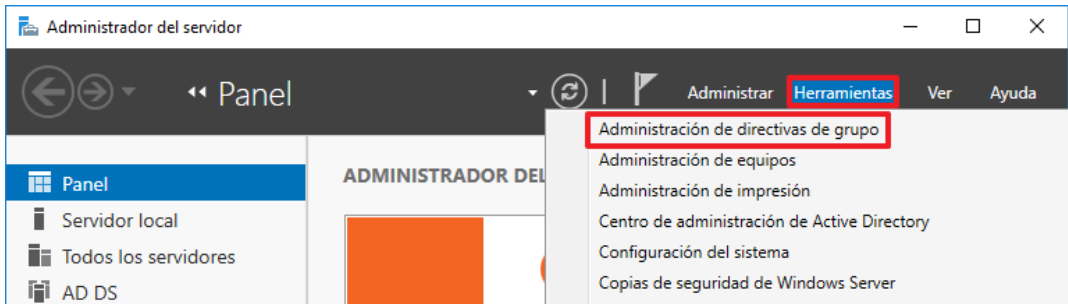
Paso	Descripción
1.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar esta operativa de configuración de la opción de mantenimiento en modo rama semianual (dirigida).
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

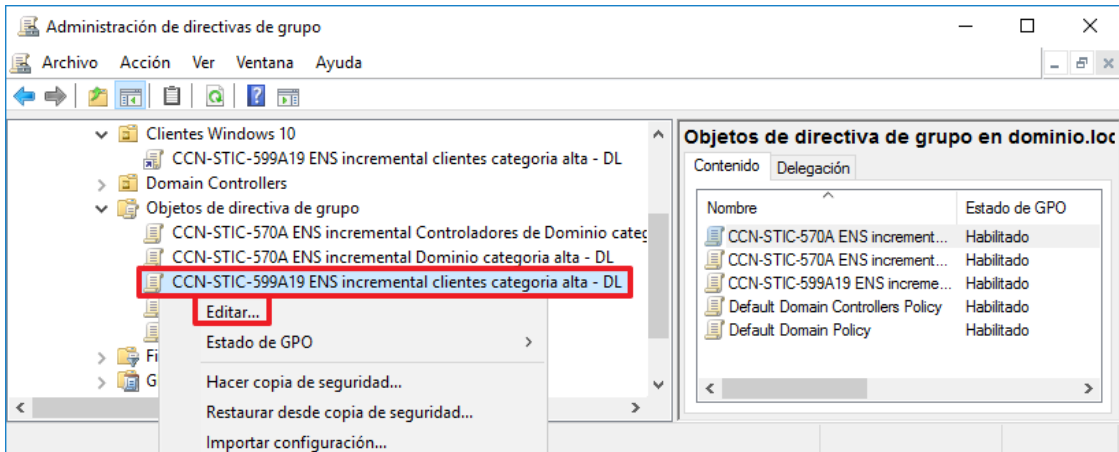
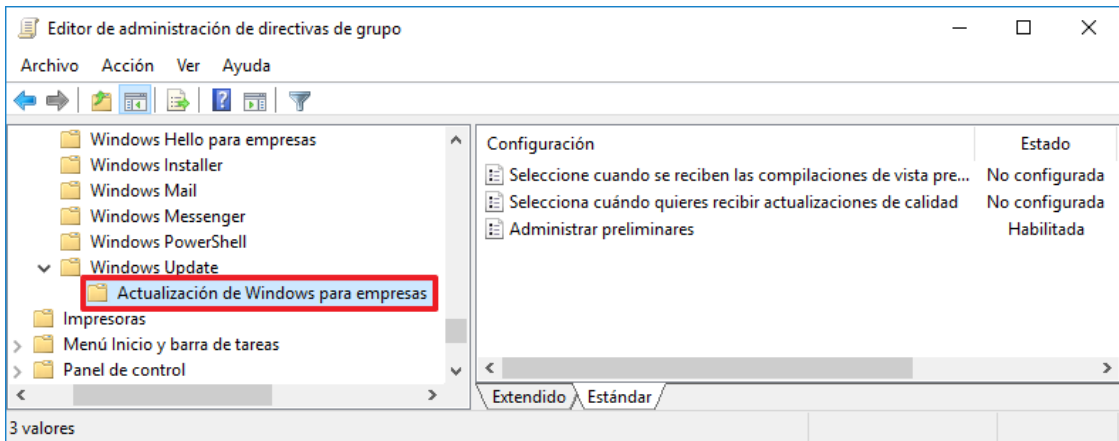
Paso	Descripción
4.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

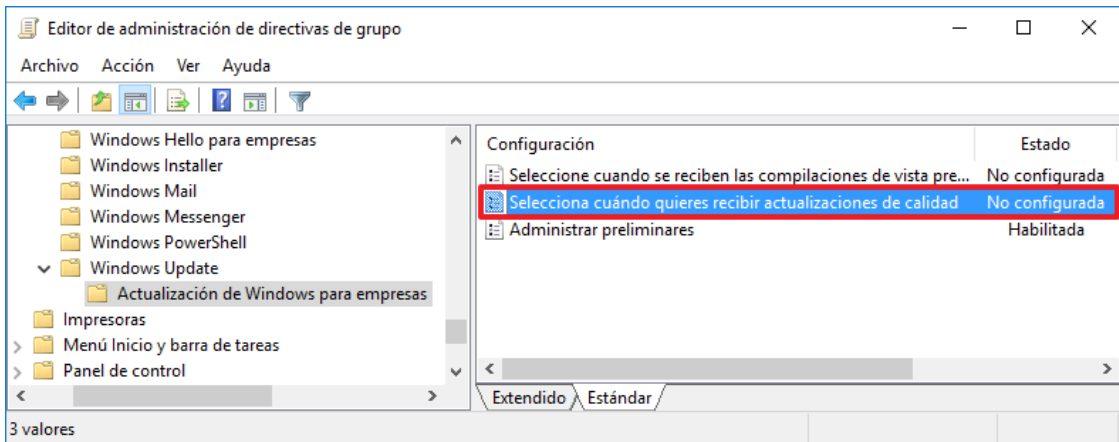
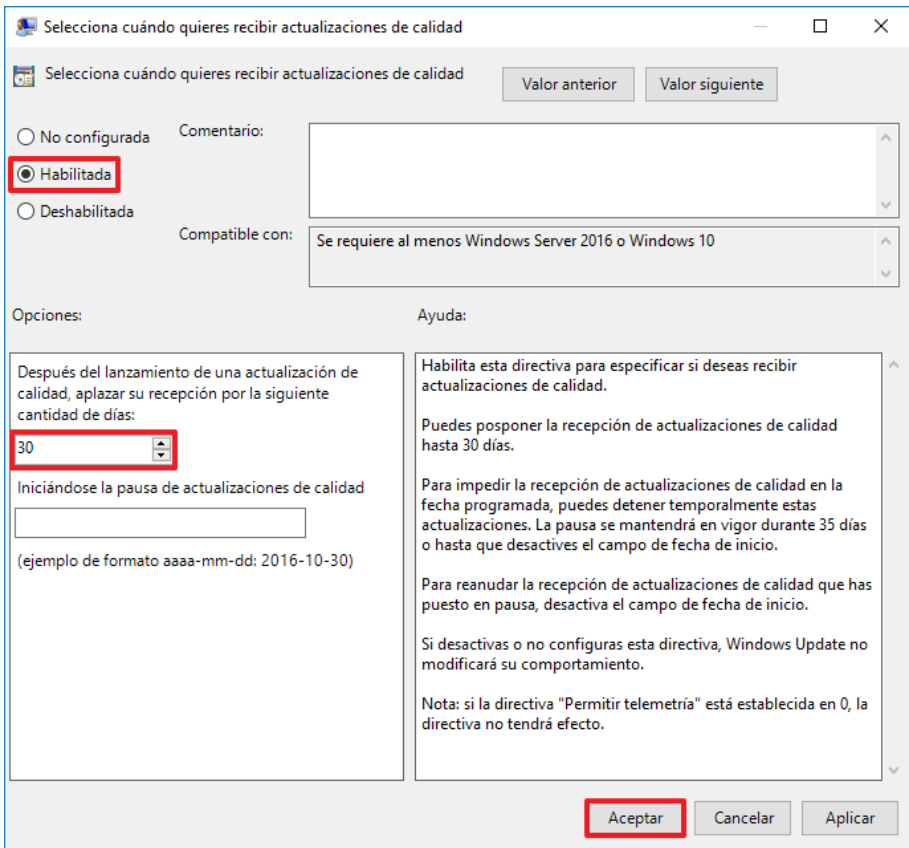
Paso	Descripción
6.	Introduzca como nombre “ENS clientes con opcion CB”. No modifique el resto de opciones y pulse el botón “Aceptar”. 
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.
8.	Pulse el botón “Agregar...”. 

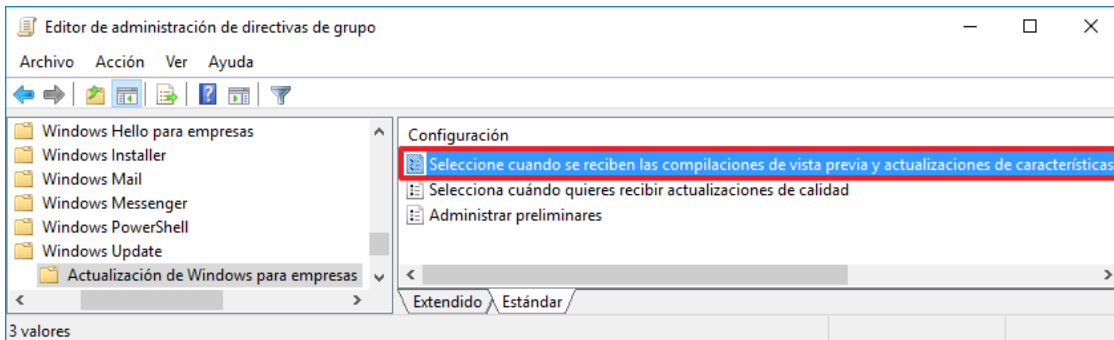
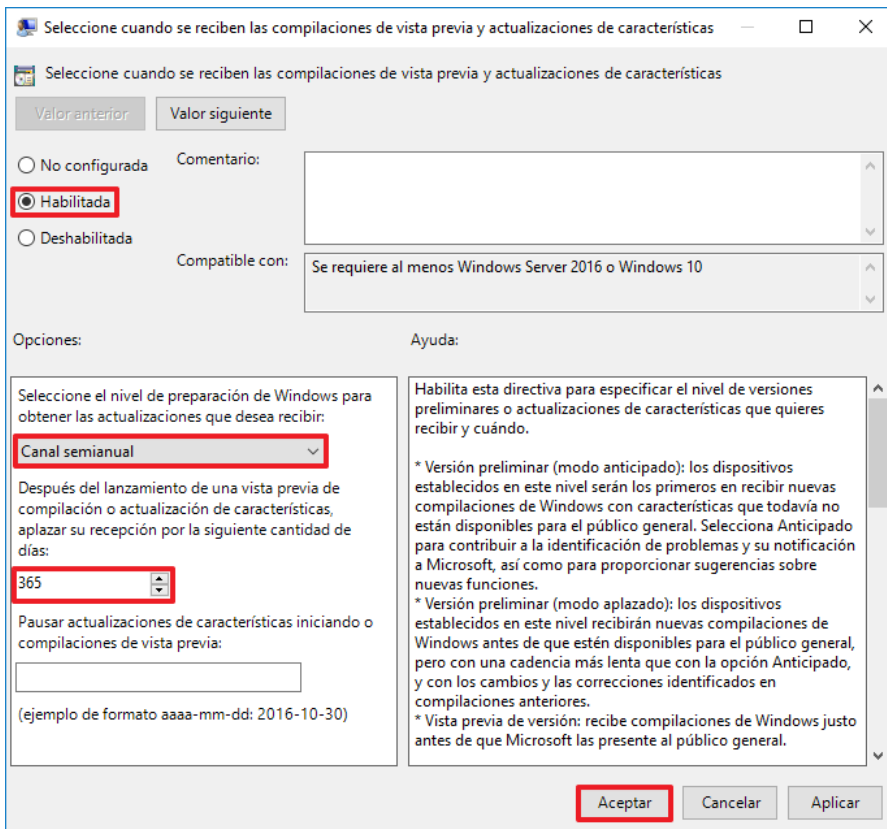
Paso	Descripción
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que cumplan las condiciones de aplicación de la GPO para que estos equipos reciban las nuevas características y funcionalidades de Windows 10 antes que el resto de equipos. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”.

2.2. CONFIGURACIÓN DE LA GPO DE MICROSOFT WINDOWS 10 PARA ESTABLECER LA OPCIÓN DE MANTENIMIENTO EN MODOS RAMA SEMIANUAL PARA LOS EQUIPOS DE LA ORGANIZACIÓN

Paso	Descripción
14.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar esta operativa de configuración de la opción de mantenimiento en modo rama semianual.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
17.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas grupo". 

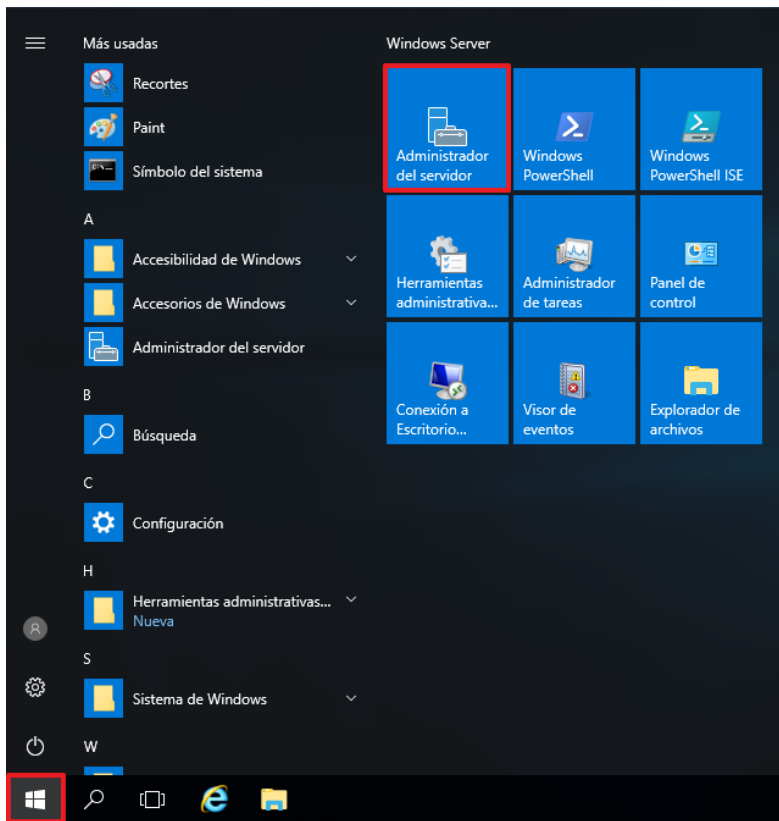
Paso	Descripción								
18.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”, Dentro de ella seleccione y edite las GPO que contienen la configuración de equipos Microsoft Windows 10 para el cumplimiento del ENS. Es factible que su organización tenga diferentes políticas para distintos equipos, realice dicho proceso para cada una de ellas.  Nota: En el presente ejemplo se va a modificar el objeto GPO asignado a puestos de trabajo de categoría alta/Difusión Limitada. Modifique los objetos GPO de puestos de trabajo MS Windows 10 acorde a la configuración de su organización.								
19.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. “Configuración de equipo → Directivas → Plantillas administrativas: Definiciones de directiva → Componentes de Windows → Windows Update → Actualización de Windows para empresas”  <table border="1"> <thead> <tr> <th>Configuración</th> <th>Estado</th> </tr> </thead> <tbody> <tr> <td>Seleccione cuando se reciben las compilaciones de vista pre...</td> <td>No configurada</td> </tr> <tr> <td>Selecciona cuándo quieres recibir actualizaciones de calidad</td> <td>No configurada</td> </tr> <tr> <td>Administrar preliminares</td> <td>Habilitada</td> </tr> </tbody> </table>	Configuración	Estado	Seleccione cuando se reciben las compilaciones de vista pre...	No configurada	Selecciona cuándo quieres recibir actualizaciones de calidad	No configurada	Administrar preliminares	Habilitada
Configuración	Estado								
Seleccione cuando se reciben las compilaciones de vista pre...	No configurada								
Selecciona cuándo quieres recibir actualizaciones de calidad	No configurada								
Administrar preliminares	Habilitada								

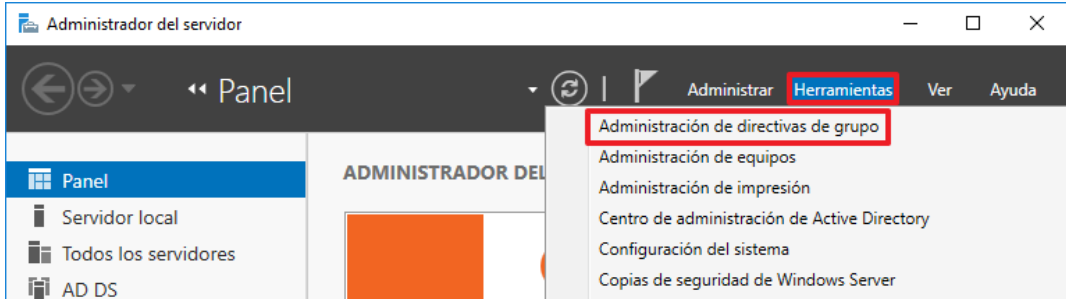
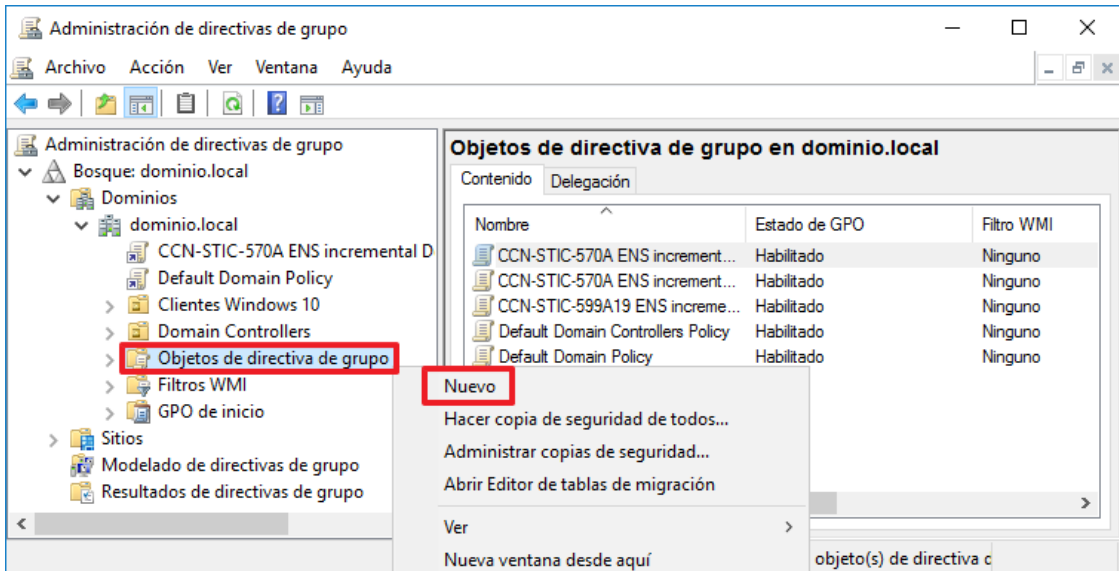
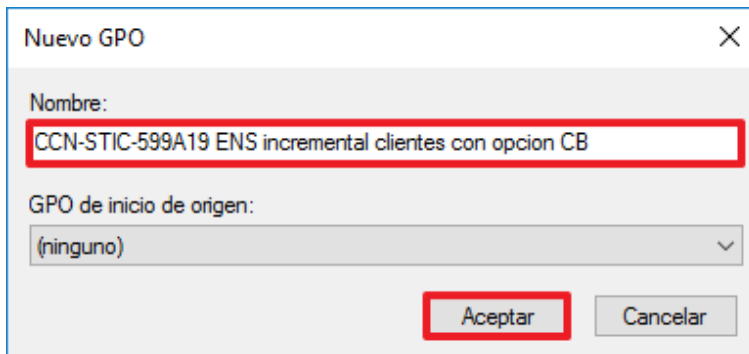
Paso	Descripción
20.	Edite la directiva “Selecciona cuándo quieres recibir actualizaciones de calidad” haciendo doble clic sobre ella. 
21.	Establezca la configuración en “Habilitada” en introduzca los valores de duración, tal y como se muestra en la siguiente imagen. Pulse “Aceptar” para finalizar. 

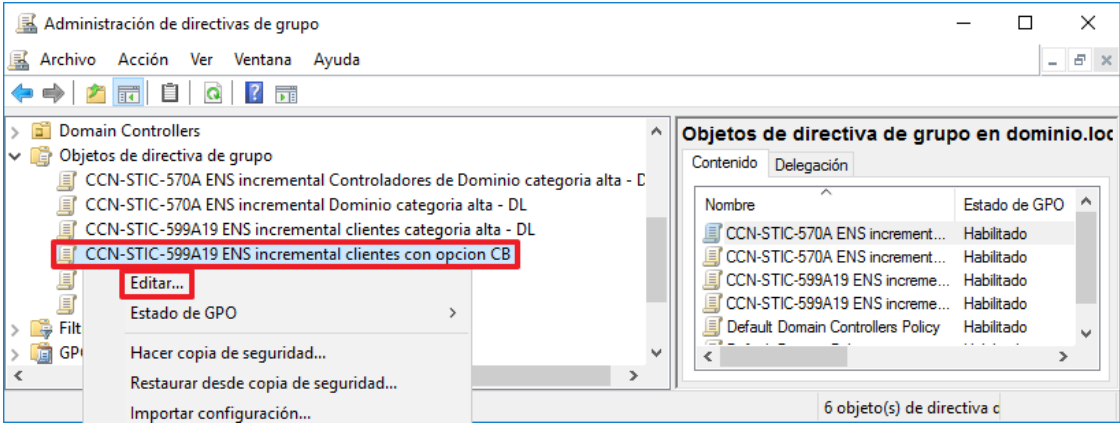
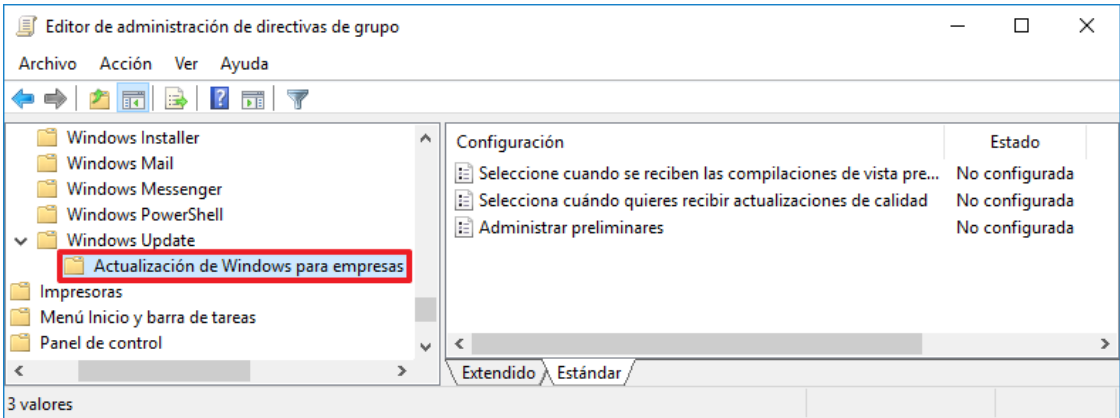
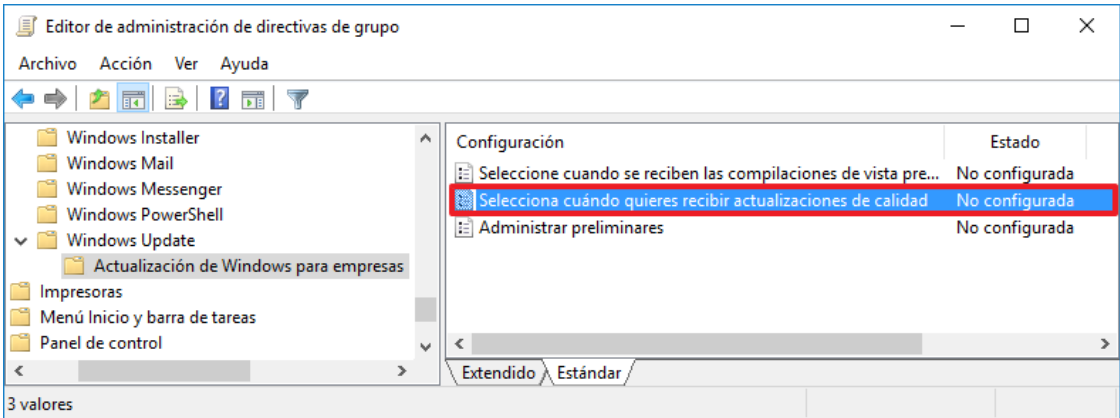
Paso	Descripción
22.	A continuación, edite la directiva “Seleccione cuando se reciben las compilaciones de vista previa y actualizaciones de características” haciendo doble clic sobre ella. 
23.	Establezca la configuración en “Habilitada” en introduzca los valores, tal y como se muestra en la siguiente imagen. Pulse “Aceptar” para finalizar.  Nota: Tenga en consideración que si estableció un valor de telemetría “0” en el punto “ANEXO C.4.2 CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA MS WINDOWS 10, CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO” estas configuraciones no tendrán efecto.
24.	Cuando haya configurado los valores, pulse el botón “Aceptar” para guardar los cambios.
25.	Cierre la política de grupo modificada.
26.	Cierre la herramienta “Administración de directivas de grupo”.

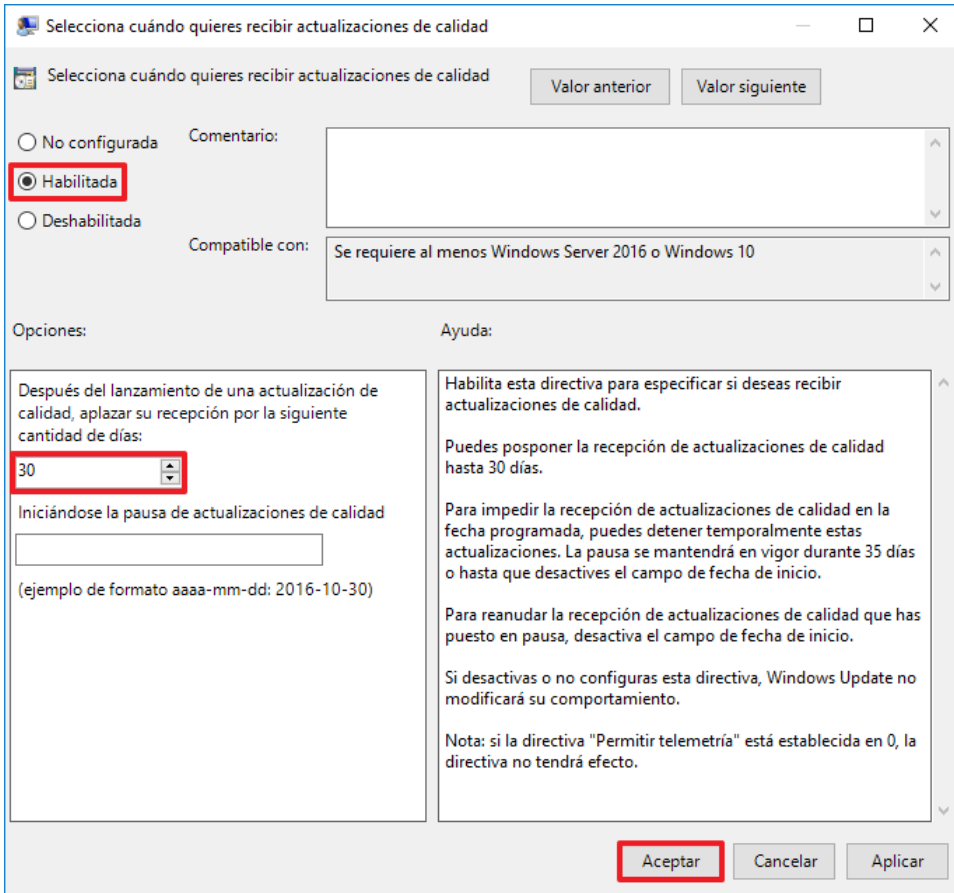
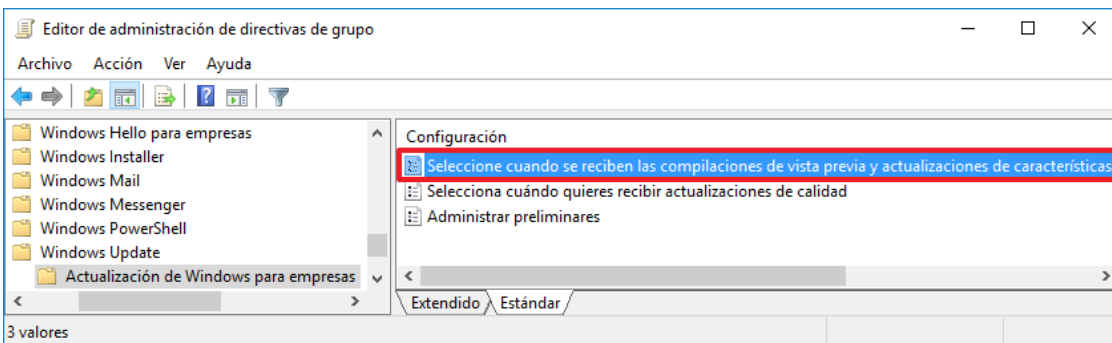
2.3. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA QUE CONFIGURE LA OPCIÓN DE MANTENIMIENTO EN MODO RAMA SEMIANUAL (DIRIGIDA) EN LOS EQUIPOS DE CONTROL

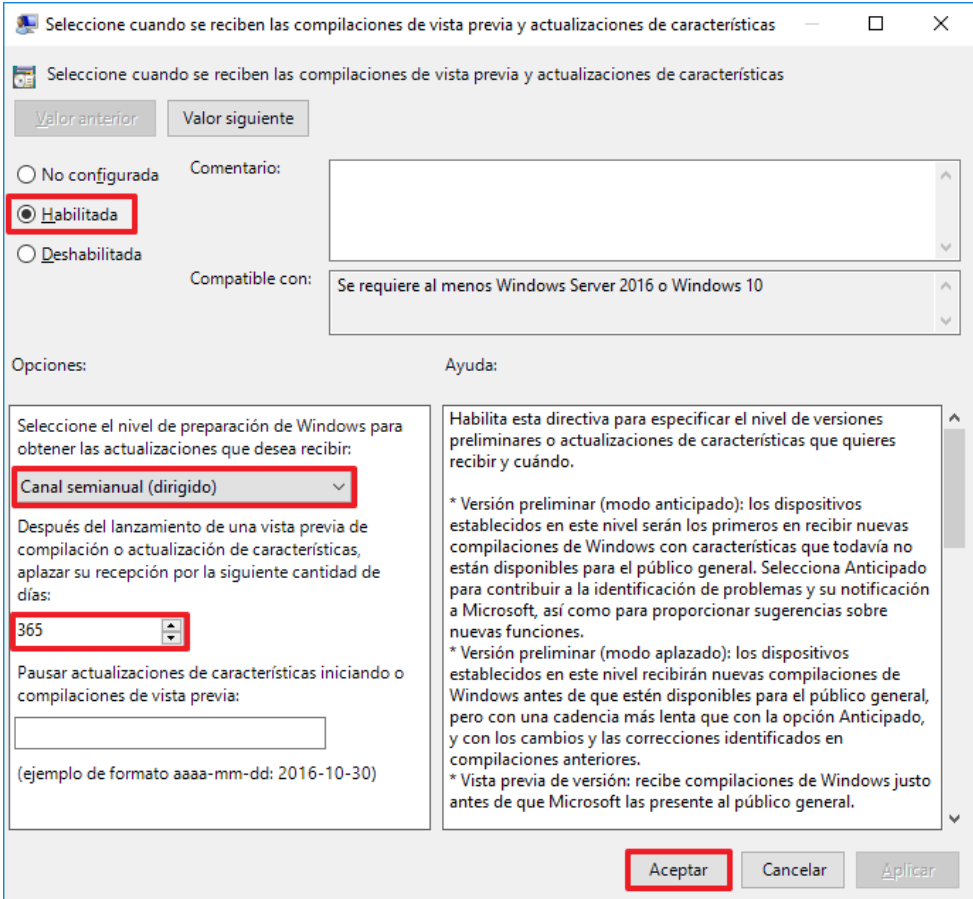
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política para establecer la opción de mantenimiento en modo rama semianual (dirigida). Estos equipos recibirán las nuevas características y funcionalidades de Windows 10 antes que el resto de equipos de la infraestructura.

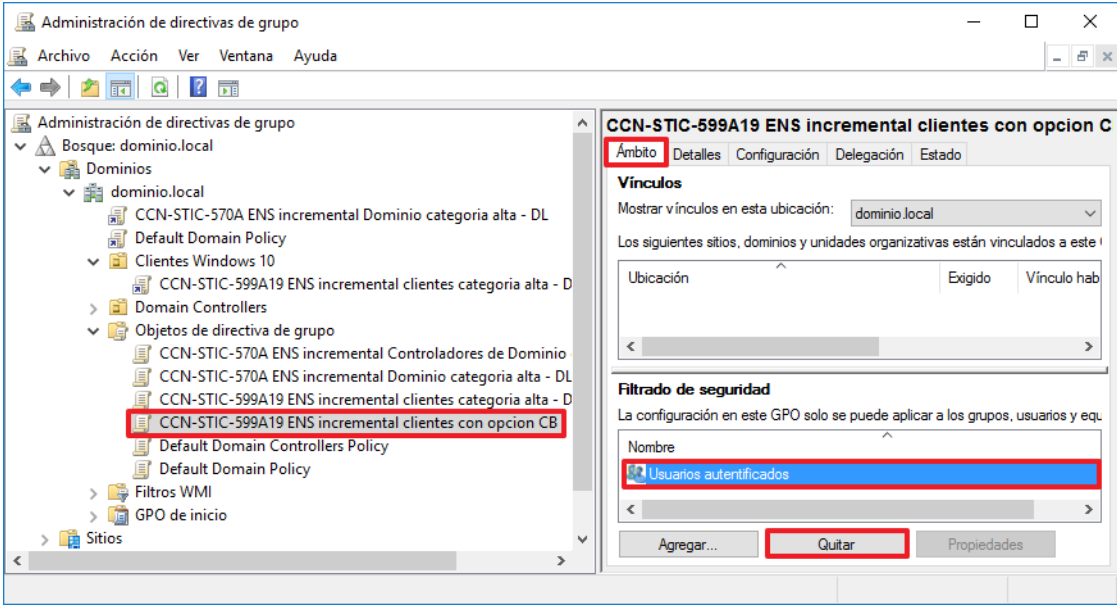
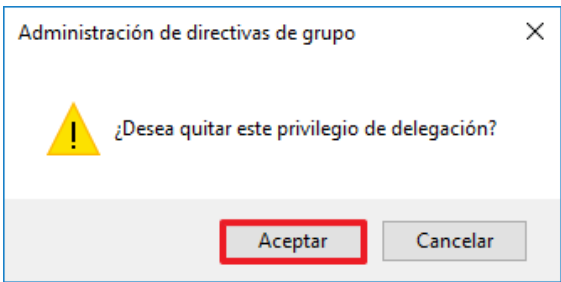
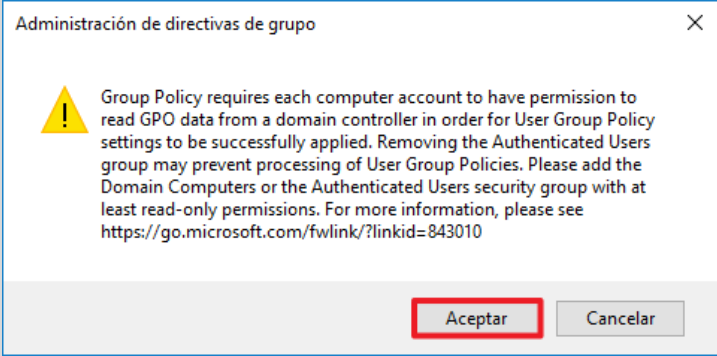
Paso	Descripción
27.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar esta operativa de configuración de la opción de mantenimiento en modo rama semianual (dirigida).
28.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
29.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

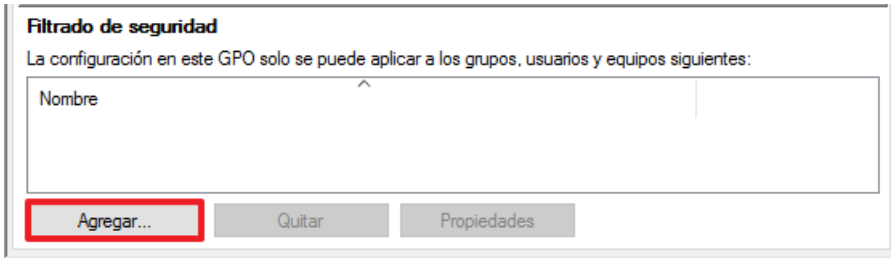
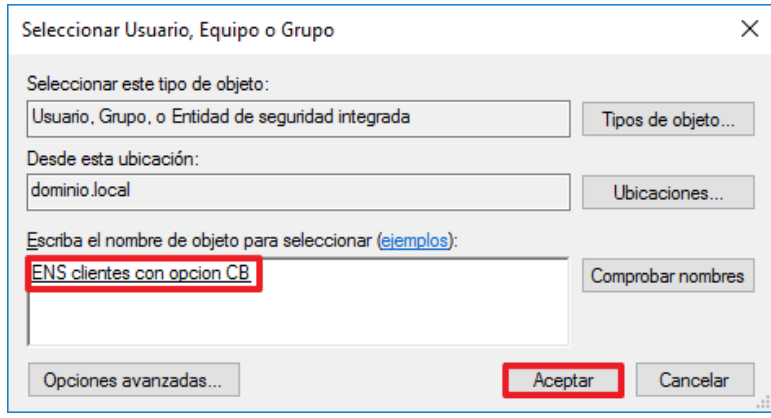
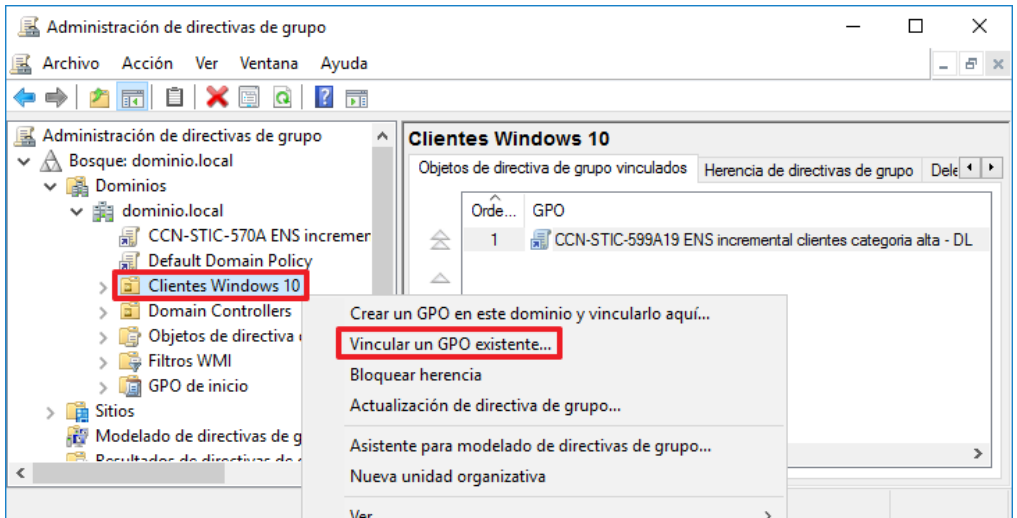
Paso	Descripción
30.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas grupo” 
31.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo” y cree una nueva GPO pulsando con botón derecho y seleccionando la opción “Nuevo”. 
32.	Establezca el nombre “CCN-STIC-599A19 ENS incremental clientes con opcion CB”. Pulse “Aceptar” y continúe con el siguiente paso. 

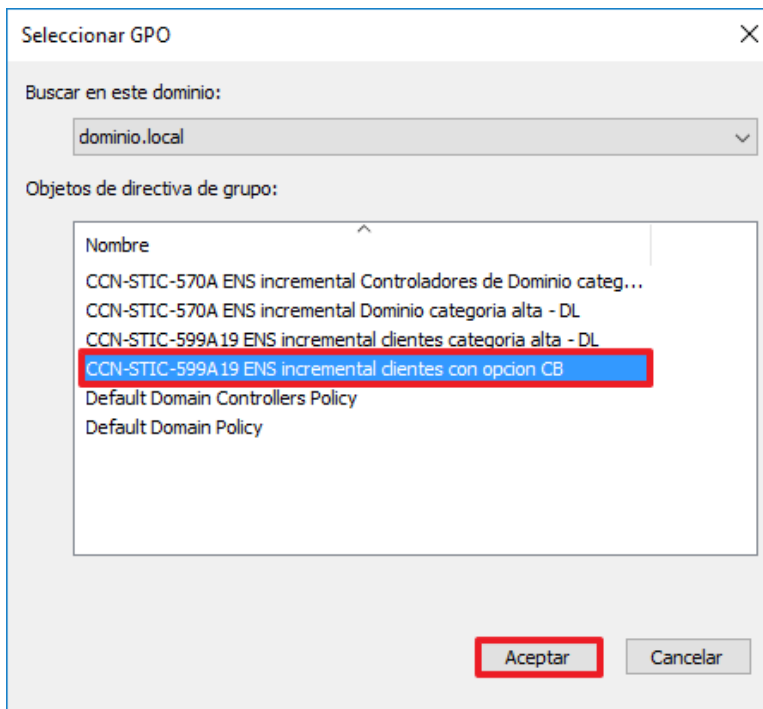
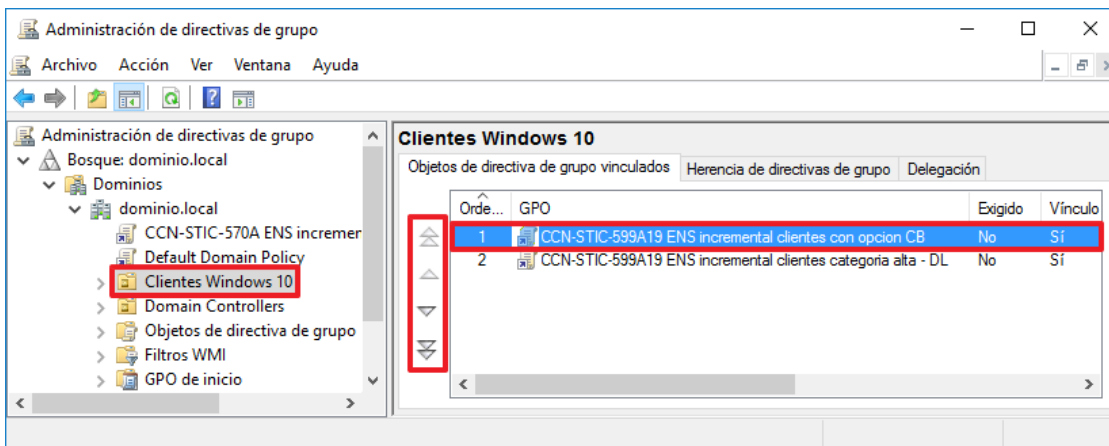
Paso	Descripción
33.	Tras esto modifique la política que acaba de crear, pulse botón derecho sobre la misma y seleccione la opción “Editar...”. 
34.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. “Configuración de equipo → Directivas → Plantillas administrativas: Definiciones de directiva → Componentes de Windows → Windows Update → Actualización de Windows para empresas” 
35.	Edite la directiva “Selecciona cuando quieres recibir actualizaciones de calidad” haciendo doble clic sobre ella. 

Paso	Descripción
36.	Establezca la configuración en “Habilitada” en introduzca los valores de duración, tal y como se muestra en la siguiente imagen. Pulse “Aceptar” para finalizar. 
37.	A continuación, edite la directiva “Seleccione cuando se reciben las compilaciones de vista previa y actualizaciones de características” haciendo doble clic sobre ella. 

Paso	Descripción
38.	Establezca la configuración en “Habilitada” en introduzca los valores, tal y como se muestra en la siguiente imagen. Pulse “Aceptar” para finalizar.  Nota: Tenga en consideración que si estableció un valor de telemetría “0” en el punto “ANEXO C.4.2 CONFIGURACIONES ADICIONALES DE SEGURIDAD PARA MS WINDOWS 10, CONFIGURACIÓN DE VALOR DE TELEMETRÍA PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO” estas configuraciones no tendrán efecto.
39.	Pulse el botón “Aceptar” para guardar los cambios.
40.	Cierre la política modificada.

Paso	Descripción
41.	Seleccione la GPO que acaba de crear. Dentro de la pestaña “Ámbito” seleccione “Usuarios autenticados” y pulse el botón “Quitar”. 
42.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
43.	Pulse ahora sobre el botón “Agregar...”. 
44.	Seleccione el grupo creado en el punto anterior, “ENS clientes con opcion CB”, y pulse “Aceptar”. 
45.	Ya solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.
46.	Seleccione la Unida Organizativa y pulsando con el botón derecho sobre ella haga uso de la opción “Vincular un GPO existente...”. 

Paso	Descripción
47.	En la pantalla de selección, marque la GPO creada previamente y pulse el botón “Aceptar”. 
48.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el panel derecho. 
49.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.

3. INFORMACIÓN ACERCA DEL ÚLTIMO INICIO DE SESIÓN

Dentro del ENS, a partir de la aplicación de su categoría media, es necesario informar al usuario de cuándo fue la última vez que inicio sesión. Hasta ahora, para realizar dicha tarea se hacía uso del inicio interactivo que posee Microsoft Windows de base utilizando las GPO y más concretamente la directiva denominada “Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario”.

La directiva establece la visualización de una fecha y hora concreta en la que el usuario se validó correctamente por última vez. Del mismo modo, indica que en caso de no estar disponible el controlador de dominio no podrá ser posible iniciar sesión en la máquina y no se podrá autenticar.

Debido a esta problemática la cual afecta sobre todo a equipos que suelen estar fuera de las organizaciones, se plantea a continuación una solución para llevar a cabo la tarea de informar al usuario de cuándo fue la última vez que inicio sesión correctamente.

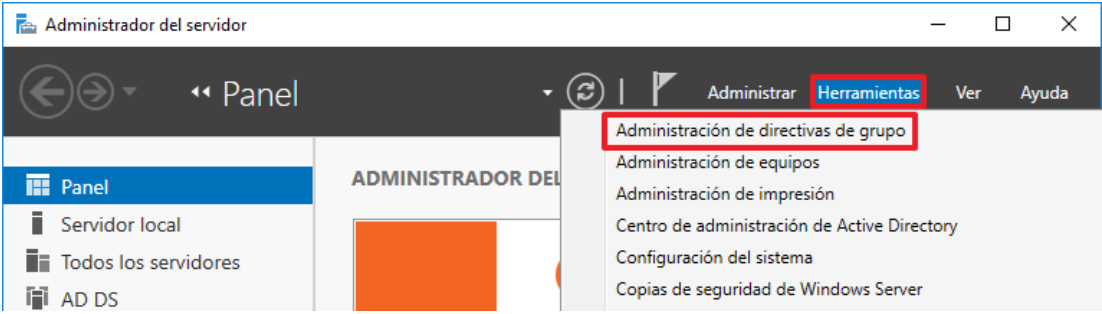
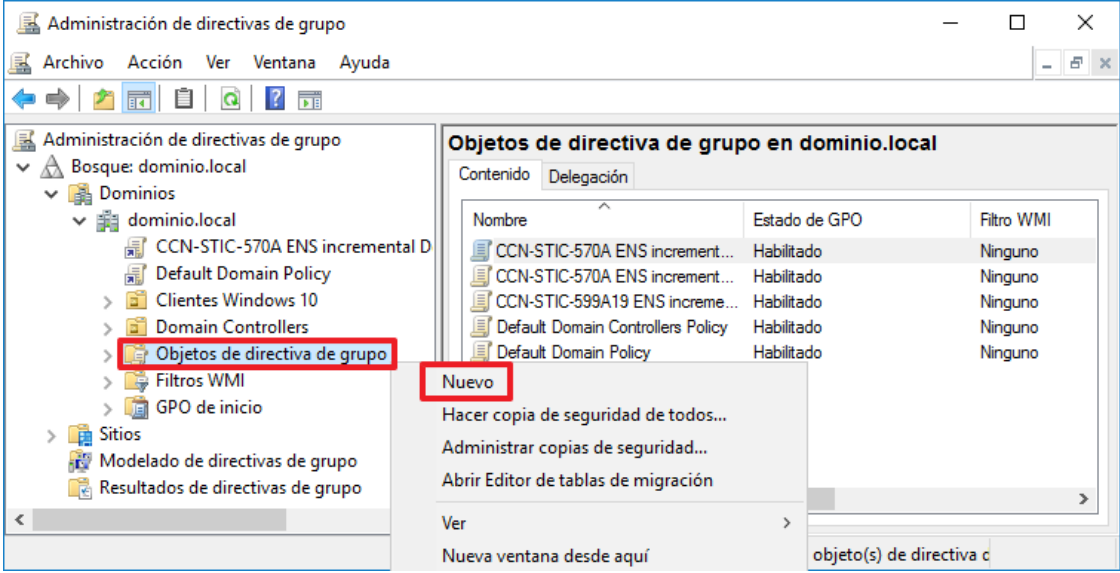
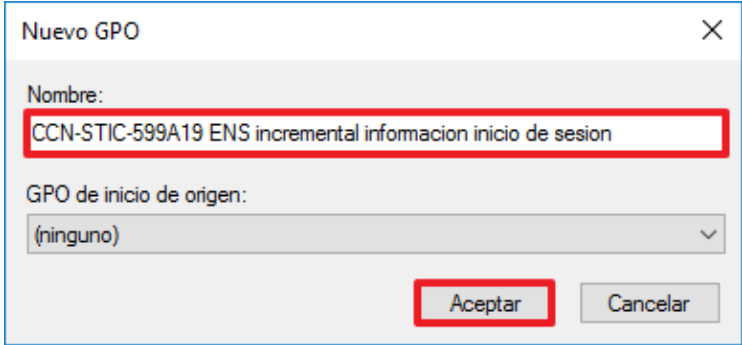
Para realizar dicha tarea se va a hacer uso de una tarea programada que ejecuta un script que muestra el último inicio de sesión correcto del usuario que es almacenado en un atributo del usuario.

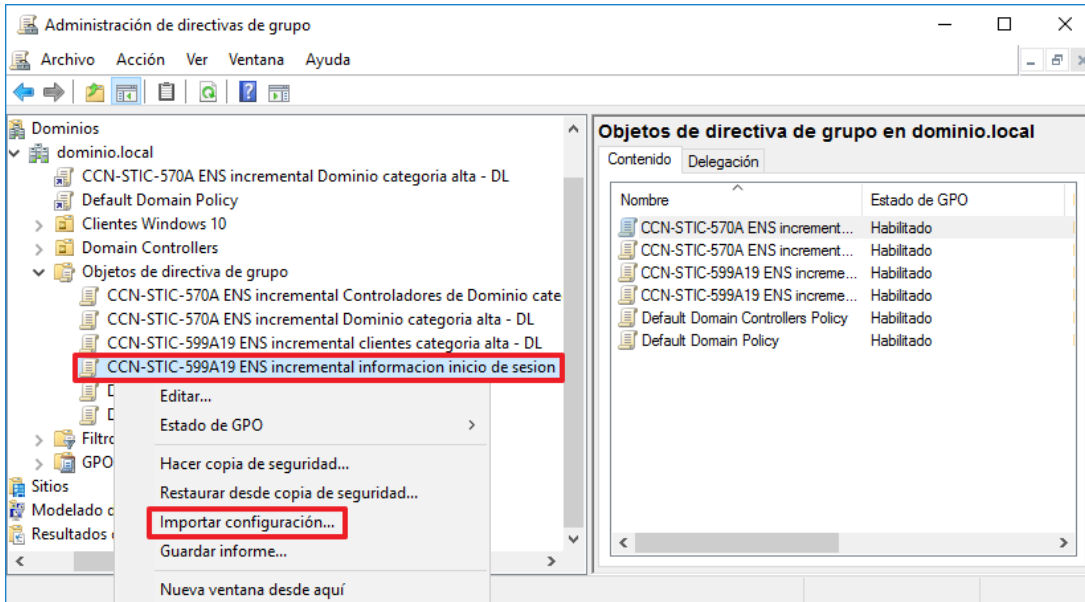
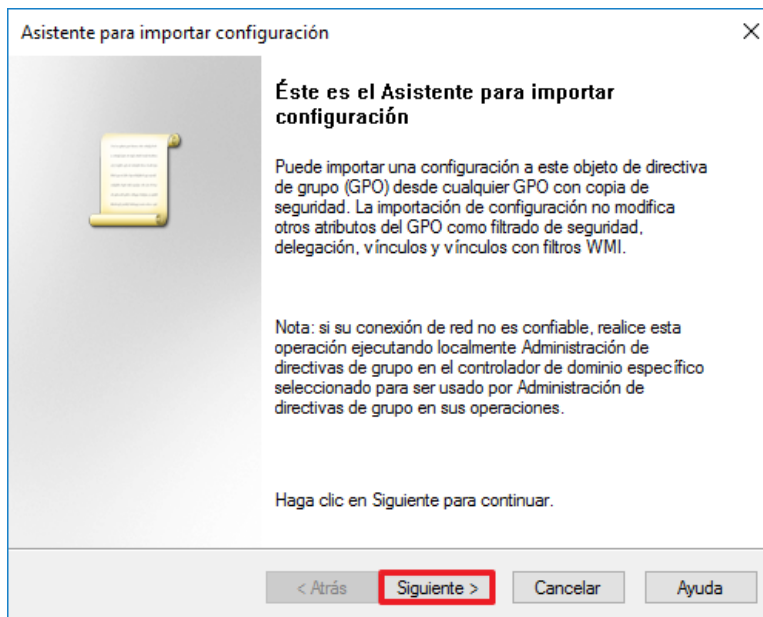
Nota: Puede hacer uso del siguiente enlace para conocer los atributos: [https://msdn.microsoft.com/en-us/library/ms675090\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms675090(v=vs.85).aspx).

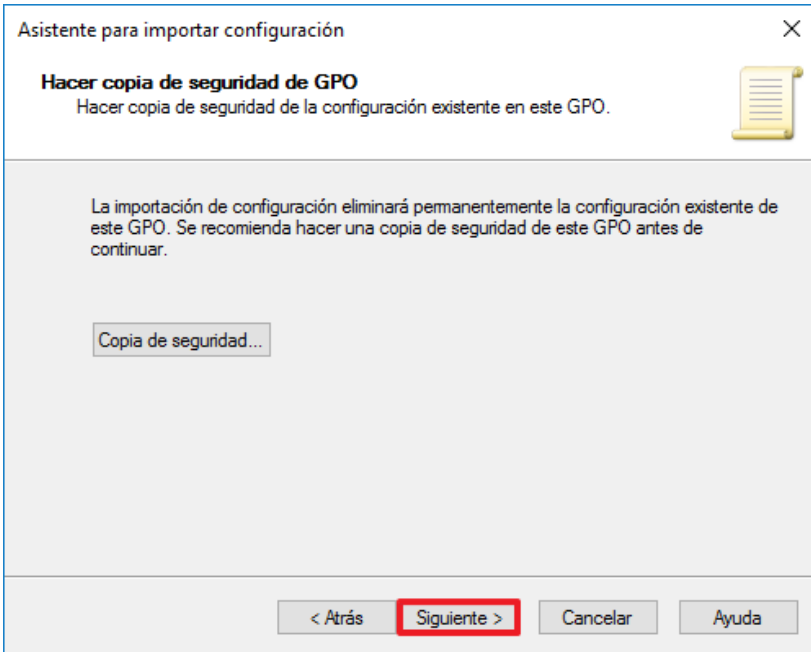
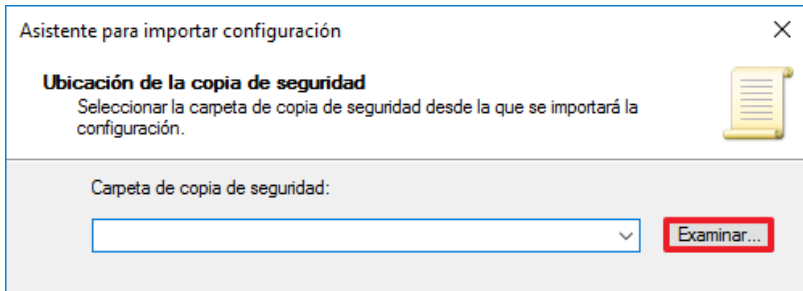
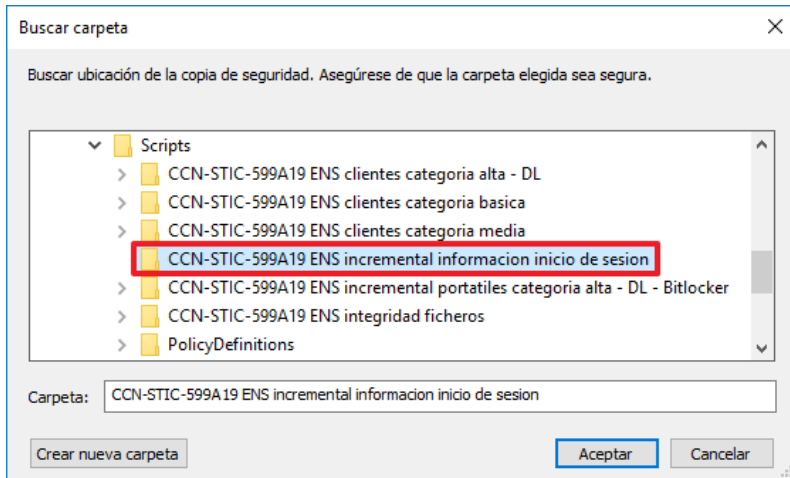
3.1. CREACIÓN DE TAREA PROGRAMADA

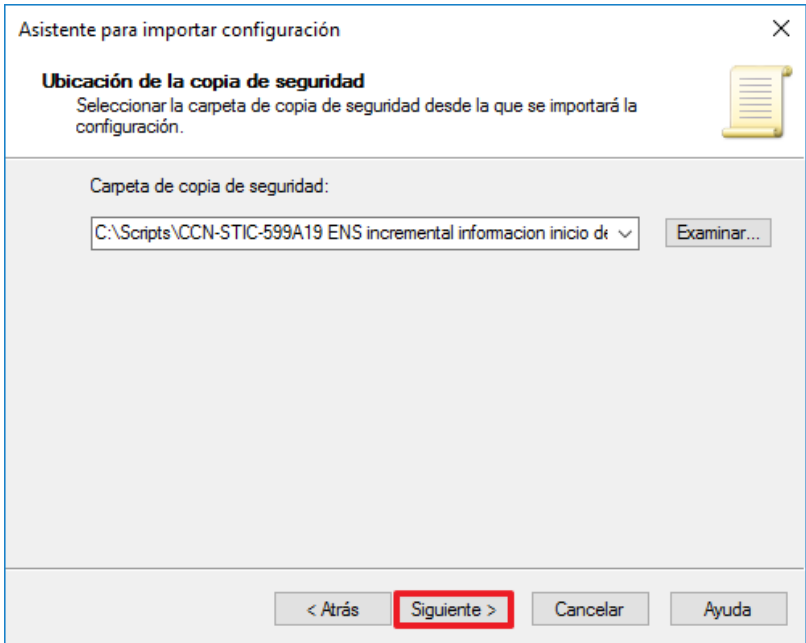
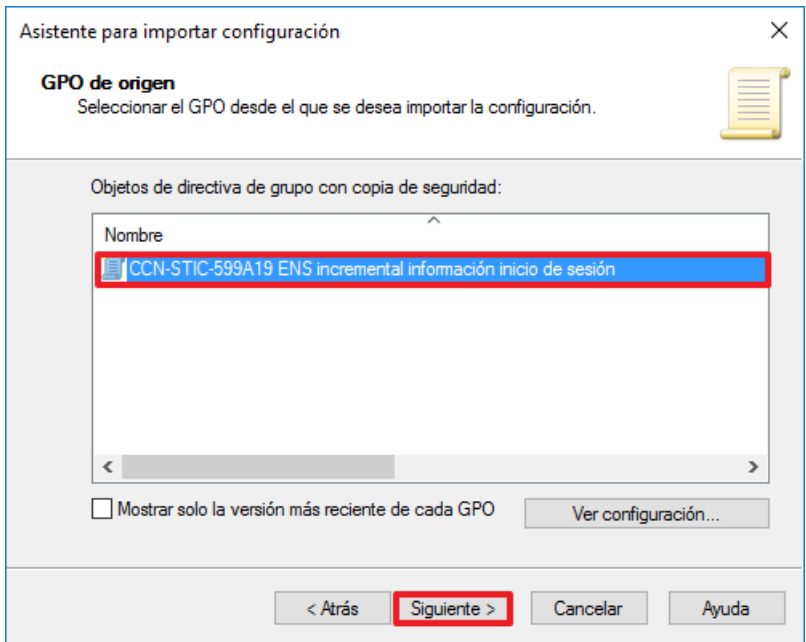
Este apartado permite implementar una tarea programada en los equipos para que los usuarios puedan visualizar el último inicio de sesión correcto mediante la ejecución de un script.

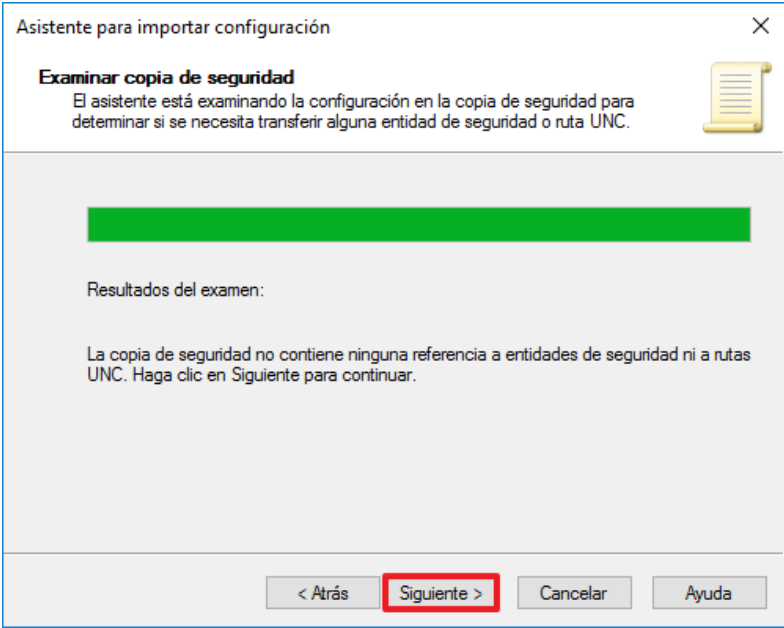
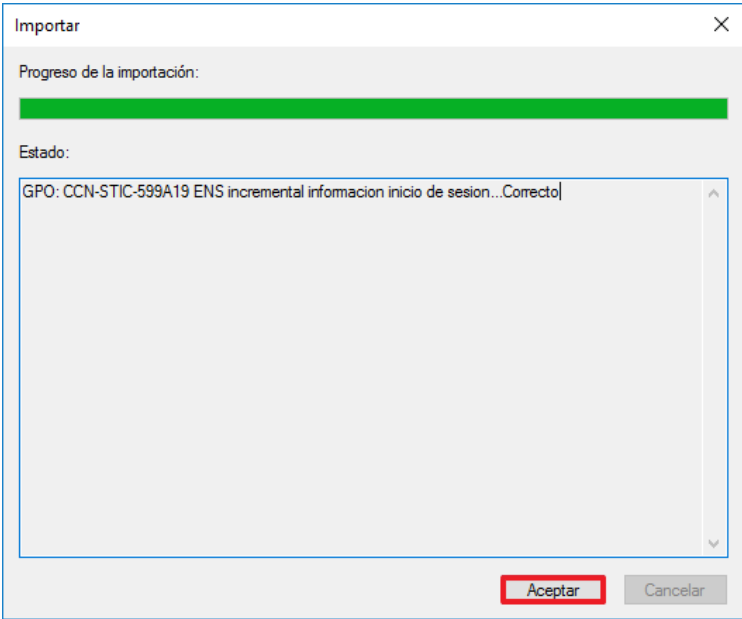
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios del ENS.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Copie los script y plantillas que acompañan a esta guía al directorio “C:\Scripts”.
4.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.
5.	Eleve privilegios para iniciar el “Administrador del servidor”.
Nota: Dependiendo de la categoría de seguridad aplicado deberá confirmar la operación o bien introducir las credenciales de un usuario con privilegios de administrador del dominio.	

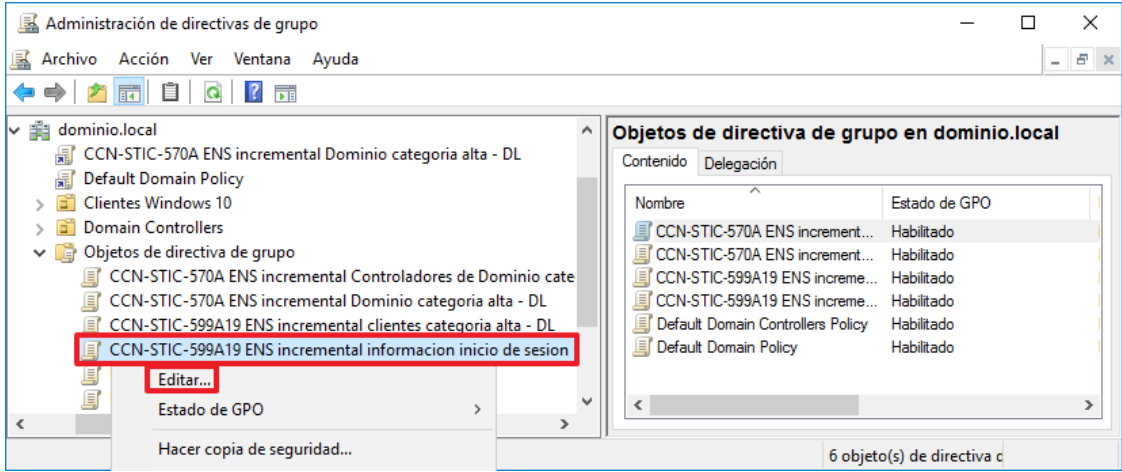
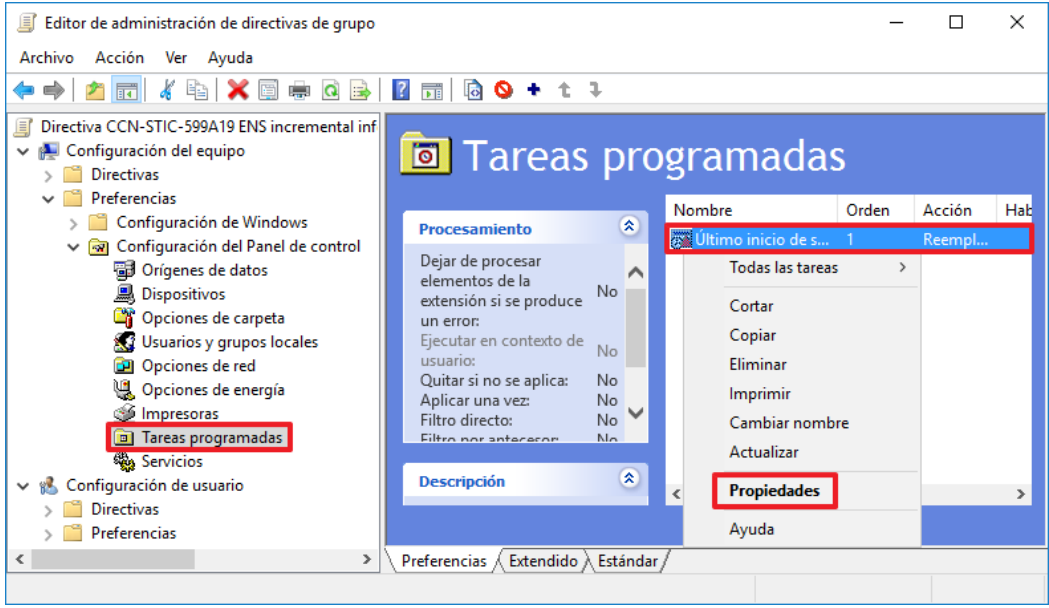
Paso	Descripción
6.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas de grupo”. 
7.	Despliegue el bloque y posicione sobre su dominio, en el ejemplo es “dominio.local”.
8.	Seleccione el nodo “Objetos de directiva de grupo” con el botón derecho y seleccione la opción del menú contextual “Nuevo”. 
9.	Asigne el nombre para la GPO “CCN-STIC-599A19 ENS incremental informacion inicio de sesion” y pulse “Aceptar”. 

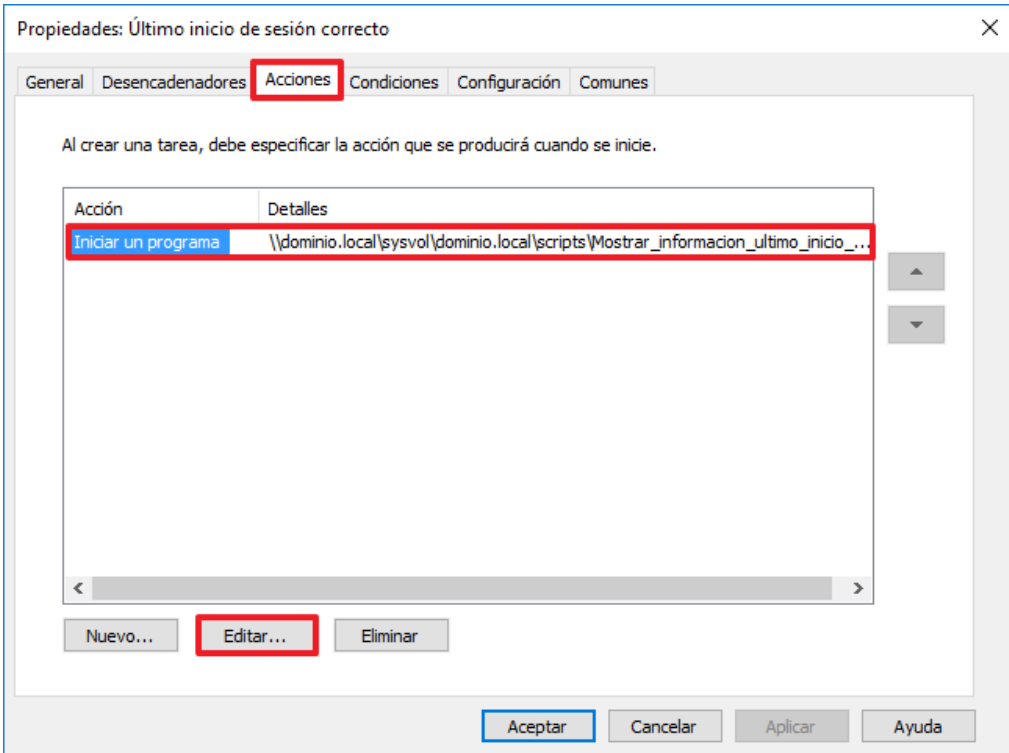
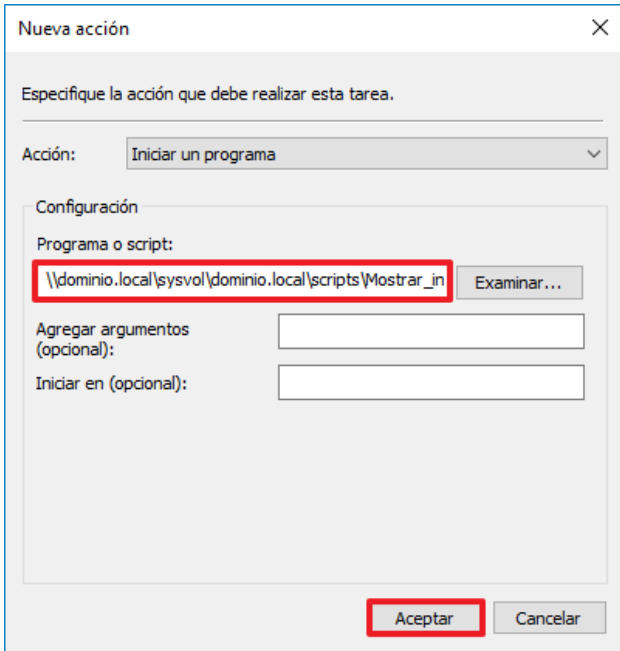
Paso	Descripción
10.	Seleccione con el botón derecho la GPO recién creada y pulse sobre la opción del menú contextual “Importar configuración...”. 
11.	En el “Asistente para importar configuración” pulse “Siguiente >”. 

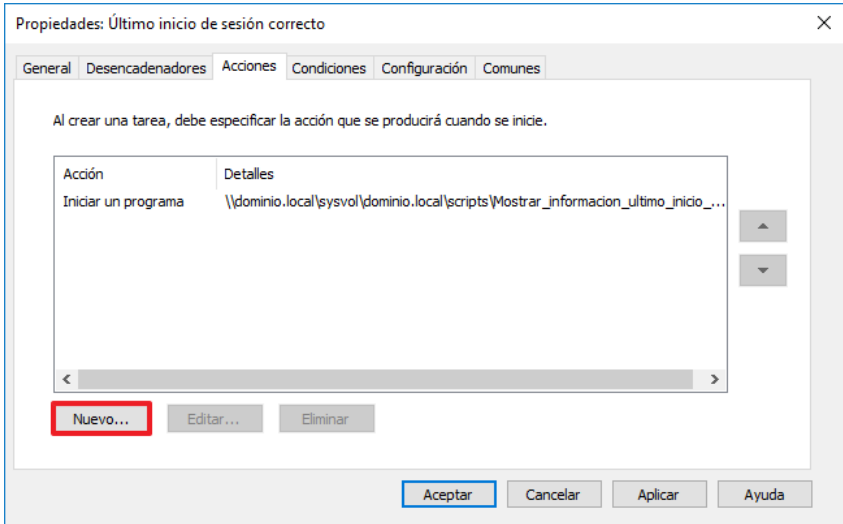
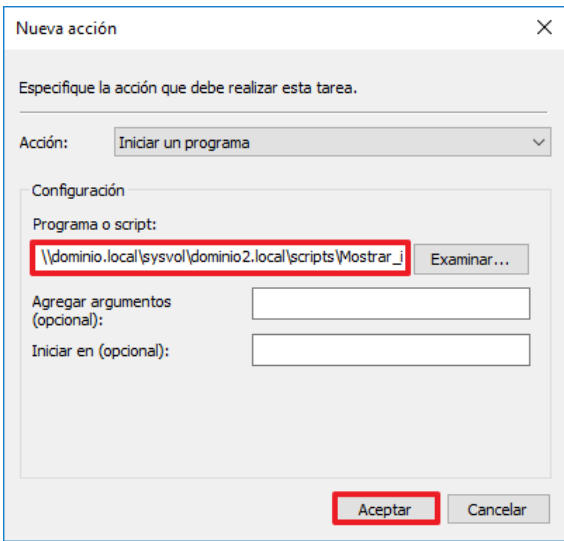
Paso	Descripción
12.	En apartado “Hacer copia de seguridad de GPO” pulse de nuevo “Siguiente >”. 
13.	En “Ubicación de copia de seguridad” pulse sobre “Examinar...”. 
14.	Navegue a la ubicación “C:\Scripts” y seleccione la carpeta “CCN-STIC-599A19 ENS incremental informacion inicio de sesion”. Pulse “Aceptar” para continuar. 

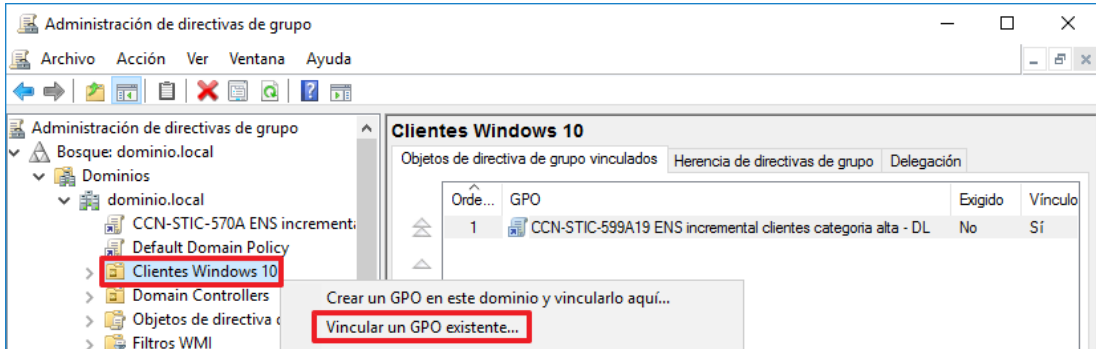
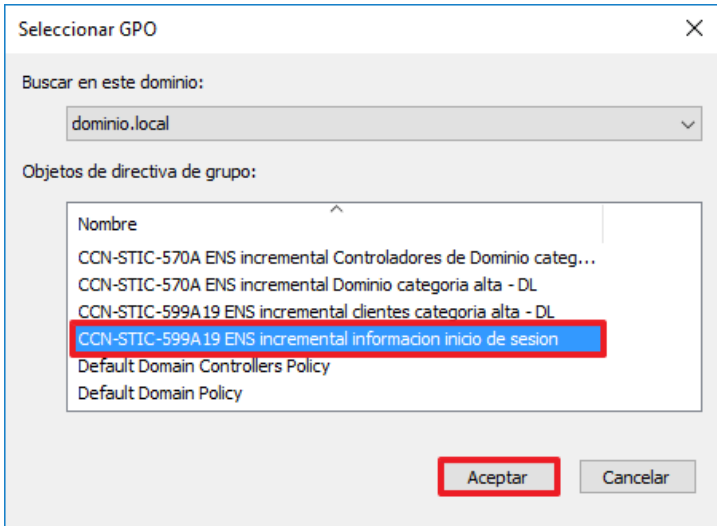
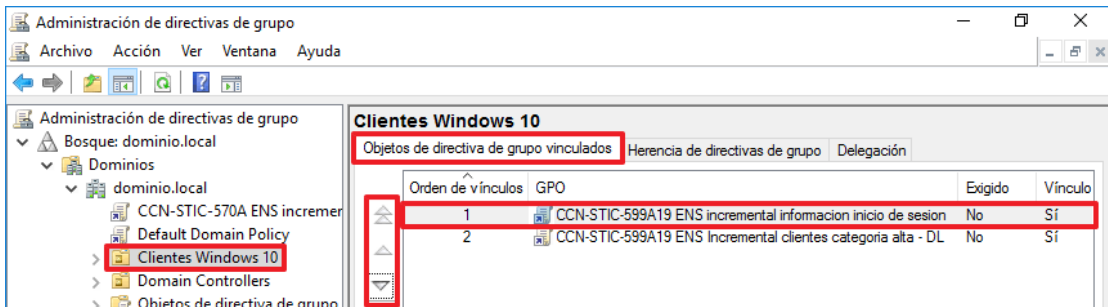
Paso	Descripción
15.	Pulse “Siguiente >” para seguir con la importación de seguridad. 
16.	Pulse de nuevo “Siguiente >” en el apartado “GPO de origen”. 

Paso	Descripción
17.	En el apartado “Examinar copia de seguridad” pulse “Siguiente >”. 
18.	Pulse “Finalizar” para terminar de importar la copia de seguridad.
19.	Pulse “Aceptar” para continuar. 

Paso	Descripción
20.	Seleccione de nuevo la GPO recién creada con el botón derecho y seleccione la opción del menú contextual “Editar...”. 
21.	Despliegue en el editor de administración de directivas de grupo el nodo “Configuración de equipo → Preferencias → Configuración del Panel de control → Tareas programadas”.
22.	Seleccione con el botón derecho la tarea programada existente y seleccione “Propiedades”. 
23.	En la ventana emergente selecciones la pestaña “Acciones”.

Paso	Descripción
24.	A continuación, seleccione la línea existente y pulse sobre “Editar...”. 
25.	En la ventana emergente edite el apartado “Programa o script:” añadiendo la información de su organización.  Nota: En el ejemplo se utiliza el dominio denominado “dominio.local”. Deberá adaptar estos nombres a los utilizados en su organización teniendo en consideración la ruta del dominio y/o subdominio utilizado.

Paso	Descripción
26.	En caso de necesitar esta tarea en otros dominios o subdominios del bosque deberá, en la ventana “Propiedades:”, dentro de la pestaña “Acciones” seleccionar la opción “Nuevo...”. 
27.	En la ventana “Nueva acción” indique la ruta del dominio o subdominio deseado. Pulse “Aceptar” para continuar.  Nota: En este ejemplo se utiliza el subdominio “dominio2.local”. Adapte los nombres a las necesidades de su organización.
28.	Repita la operativa por cada dominio o subdominio en el que necesite la ejecución del script. Solo será necesario editar la ruta al dominio ya que la carpeta “sysvol” y “scripts” se crean por defecto en los sistemas en una implementación de Active Directory.
29.	Pulse “Aceptar” para finalizar la configuración de la tarea programada y cierre el editor de administración de directivas de grupo.
30.	Identifique ahora las unidades organizativas sobre las que se está aplicando seguridad según criterios del ENS.

Paso	Descripción
31.	Seleccione la unidad organizativa sobre la que desee aplicar la GPO recién configurada con el botón derecho y seleccione la opción del menú contextual “Vincular GPO existente...”.  Nota: En este ejemplo se utiliza la unidad organizativa “Clientes Windows 10”. Deberá adaptar estos pasos a las necesidades de su organización.
32.	Seleccione la GPO “CCN-STIC-599A19 incremental informacion inicio de sesion”. 
33.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la primera posición del orden de vínculos en la pestaña de “Objetos de directiva de grupo vinculados”. 

3.2. DELEGACIÓN DE PERMISOS DE ESCRITURA SOBRE ATRIBUTO DE USUARIO

Debido a la necesidad de almacenar la información del último inicio de sesión en un atributo propio de cada usuario es necesario delegar el permiso sobre cada usuario para que pueda modificar el valor de dicho atributo.

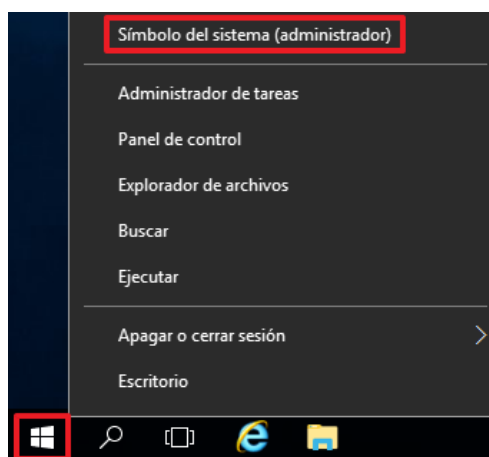
Durante esta implementación se utiliza el atributo “groupsTolgnore”. Este atributo no es utilizado habitualmente por lo que es idóneo para realizar dicha tarea. No obstante, si su organización hace uso de este atributo, deberá determinar qué atributo utilizar dentro de su organización y adaptar los scripts en consecuencia.

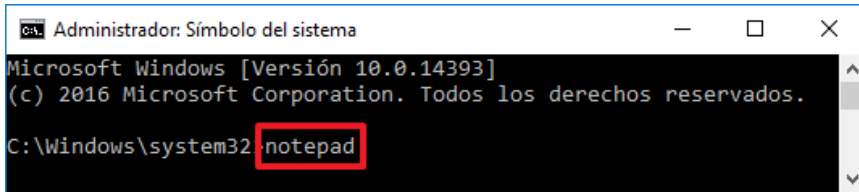
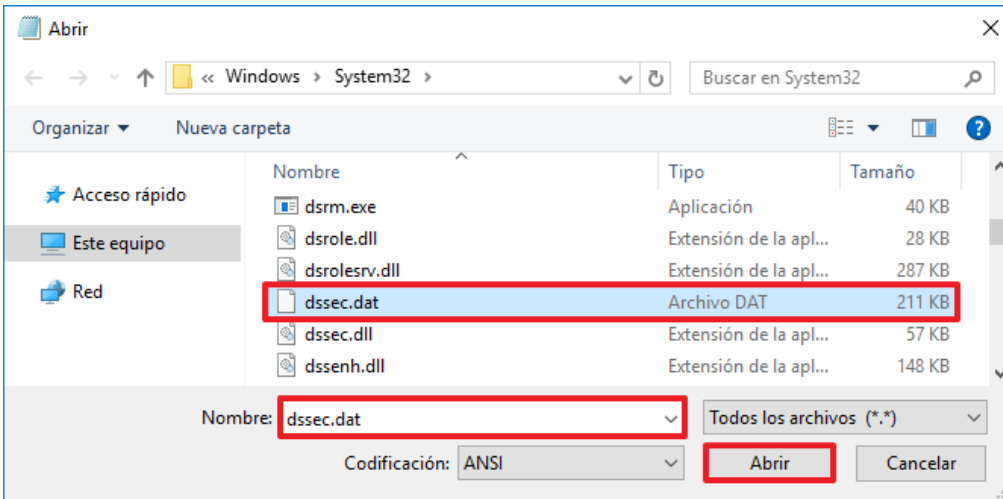
Nota: Deberá modificar el atributo utilizado para almacenar dicha información teniendo en cuenta los siguientes condicionantes:

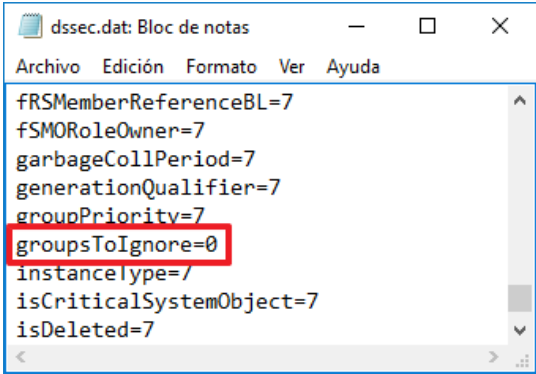
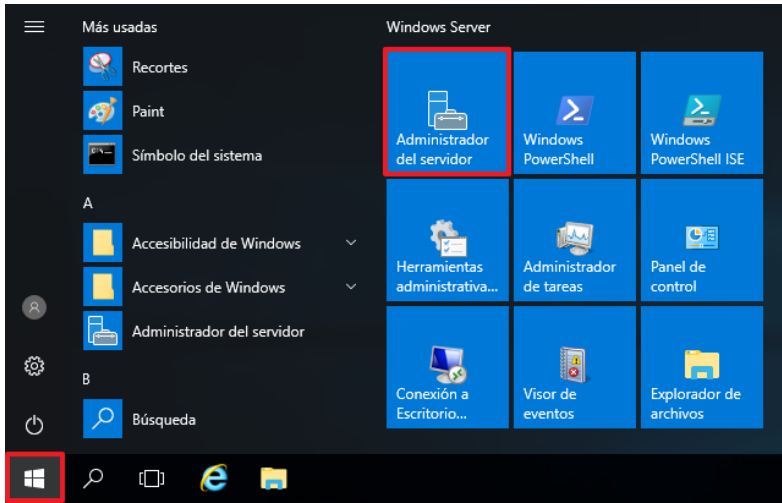
- El atributo no está en uso actualmente.
- El atributo ya no se utiliza/está obsoleto (véase un atributo de Windows NT por ejemplo).
- El atributo debe poder almacenar una cadena de caracteres.
- El atributo puede ser modificado por el propio usuario (de lo contrario deberá delegar el permiso de escritura sobre el atributo).
- Tener previsión de que el atributo utilizado no va a ser modificado por el sistema.

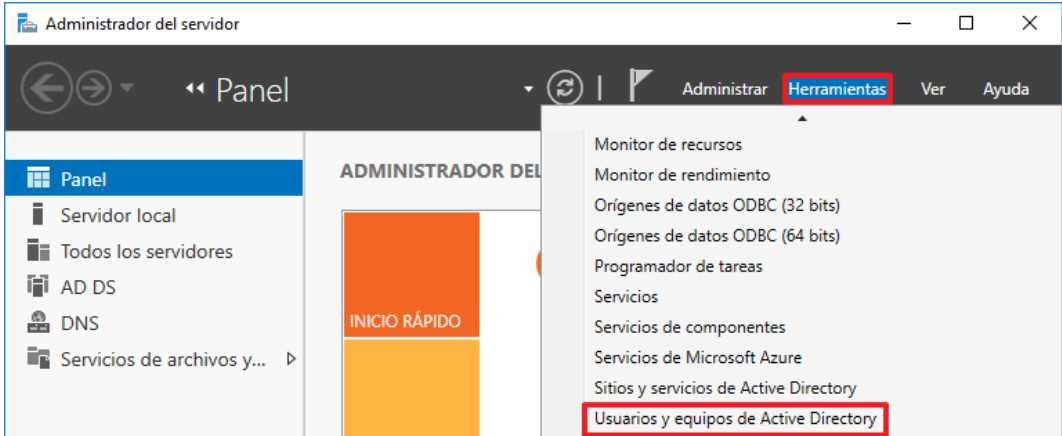
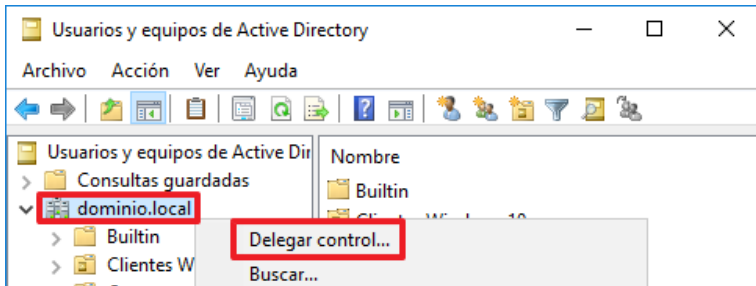
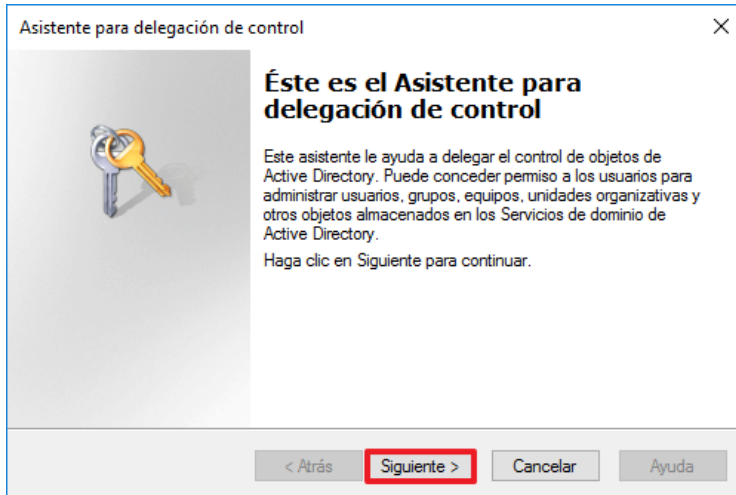
Los pasos que se definen a continuación pueden no ser necesarios en caso de que vaya a utilizarse un atributo diferente al indicado durante este paso a paso. Deberá determinar el atributo deseado y comprobar sus permisos y disponibilidad.

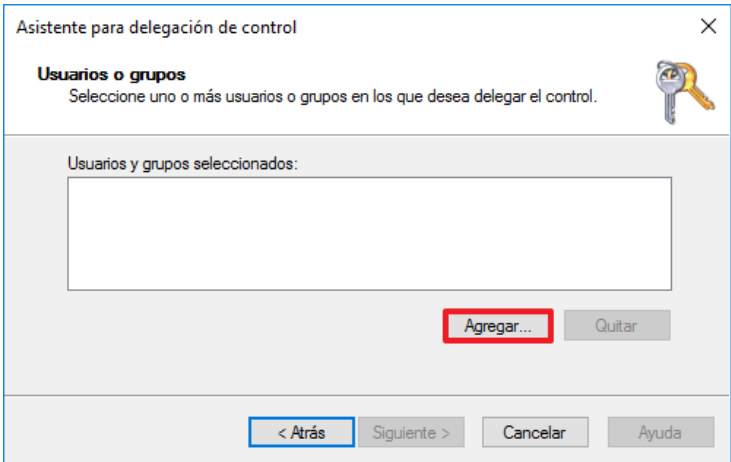
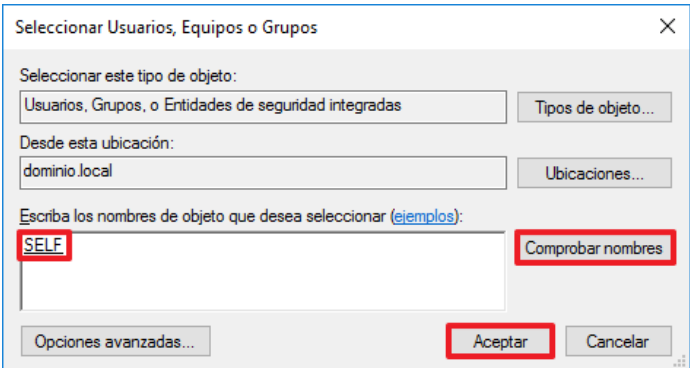
Paso	Descripción
34.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
35.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
36.	Ejecute una consola de comandos como un usuario administrador. Para ello pulse con el botón derecho sobre “Inicio” y seleccione la opción “Símbolo del sistema (administrador)”.

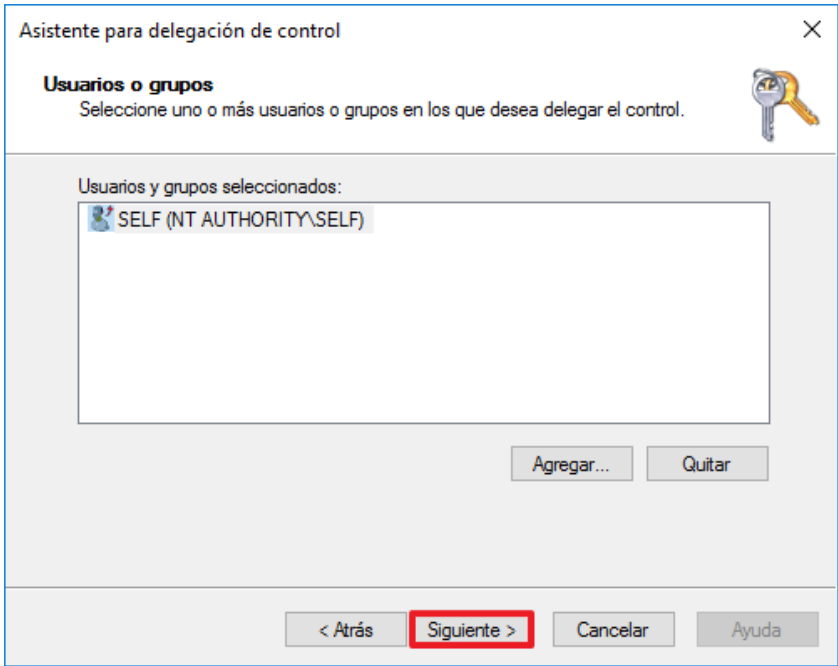
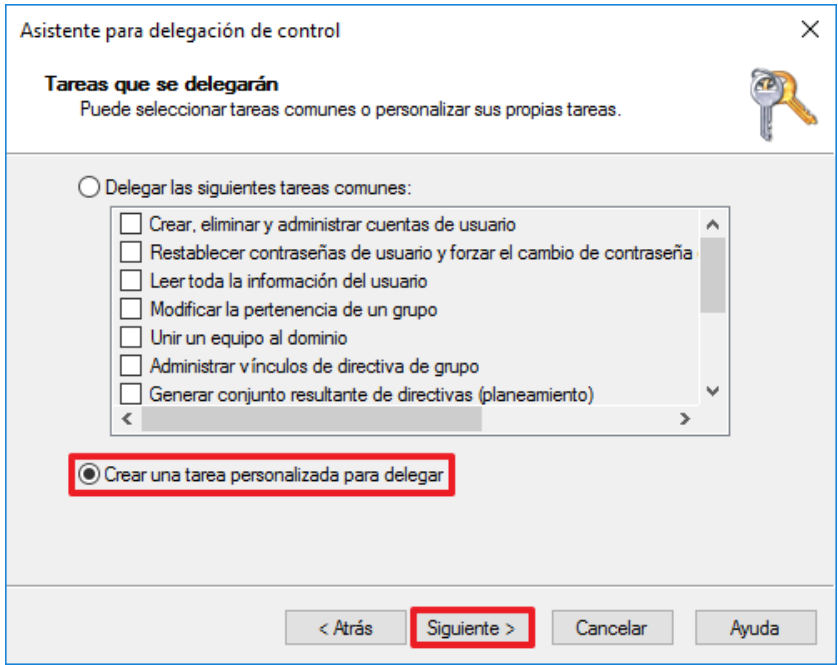


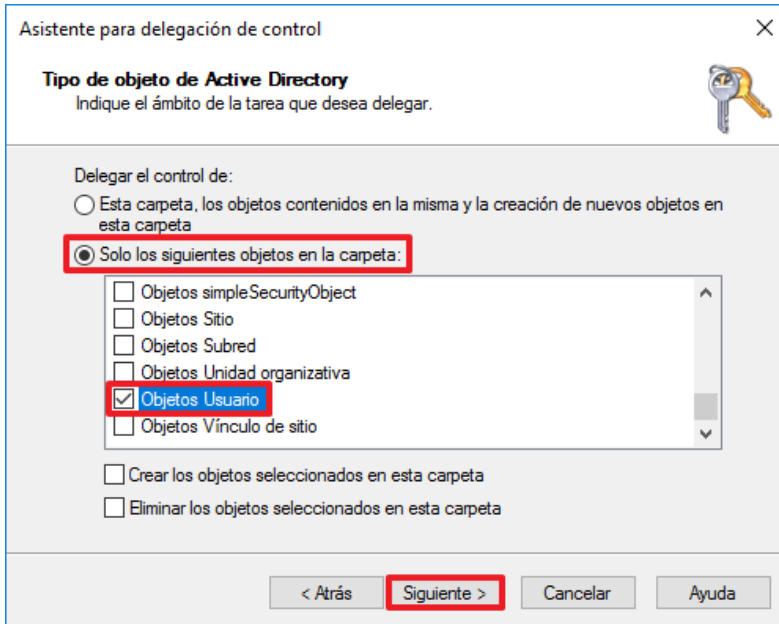
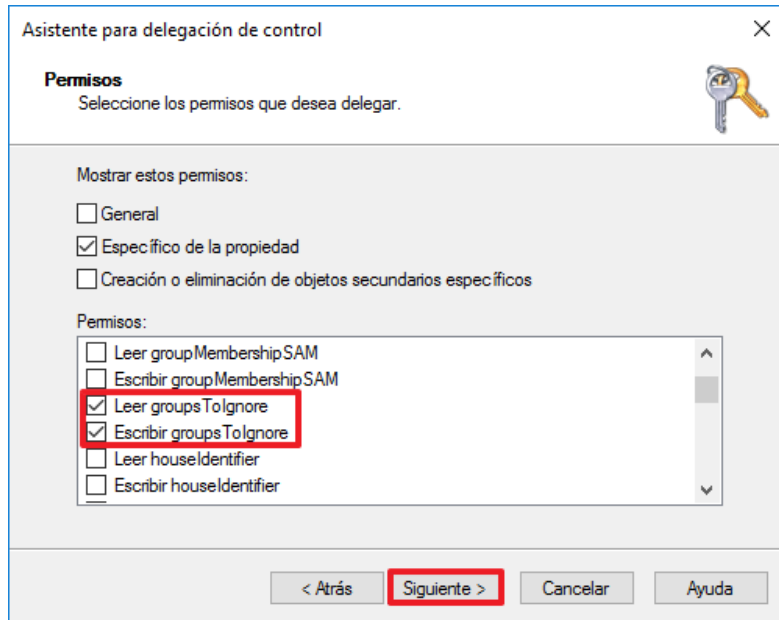
Paso	Descripción
37.	Eleve privilegios para poder acceder a la consola. Nota: Dependiendo de la categoría de seguridad aplicada sobre el sistema deberá elevar privilegios simplemente o bien introducir las credenciales de un usuario con permisos de administrador del dominio.
38.	En la consola escriba “notepad”. 
39.	Abra el fichero denominado “dssec.dat” ubicado en “%SYSTEMROOT%\System32”. Introduzca el nombre “dssec.dat” y pulse el botón “Abrir”.  Nota: Este fichero debe ser editado como administrador para que pueda ser guardado en la ubicación.

Paso	Descripción
40.	En el apartado “[User]” del fichero localice el atributo “groupsToIgnore” y establezca su valor en “0”. Utilice la ruta “Edición → Buscar” para localizar el atributo.  Nota: Tenga en consideración que pueden existir más atributos con el mismo nombre dentro del fichero, pero ubicados en distintos apartados, como pueda ser el apartado “[computer]”. Asegúrese de que modifica el atributo en el apartado “[User]”.
41.	Guarde la configuración realizada desde la ruta “Archivo → Guardar”.
42.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
43.	Eleve privilegios para iniciar el “Administrador del servidor”. Nota: Dependiendo de la categoría de seguridad aplicada deberá confirmar la operación o bien introducir las credenciales de un usuario con privilegios de administrador del dominio.

Paso	Descripción
44.	Inicie la herramienta “Usuarios y equipos de Active Directory” en el apartado “Herramientas”. 
45.	Seleccione con el botón derecho sobre el dominio en uso y pulse sobre la opción del menú contextual “Delegar control...”. 
46.	En el “Asistente para delegación de control” pulse “Siguiente >”. 

Paso	Descripción
47.	Pulse el botón “Agregar...”. 
48.	En la ventana emergente introduzca el usuario “SELF”, pulse sobre “Comprobar nombres” y pulse sobre “Aceptar” para continuar. 

Paso	Descripción
49.	Pulse “Siguiente >” para continuar con la configuración de delegación. 
50.	Seleccione la opción “Crear una tarea personalizada para delegar” y pulse “Siguiente >”. 

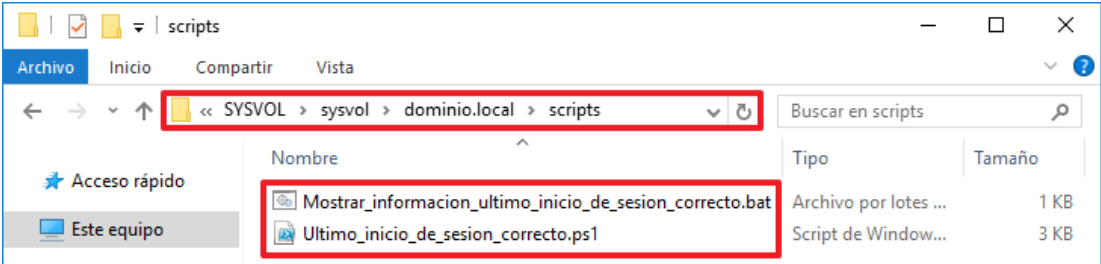
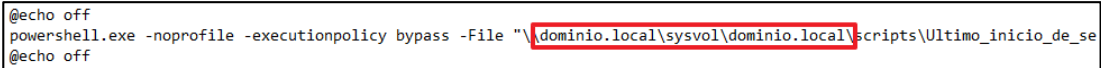
Paso	Descripción
51.	A continuación, marque la opción “Solo los siguientes objetos en la carpeta:” y marque el objeto “Objetos Usuario”. Pulse “Siguiente >” para continuar. 
52.	En el apartado permisos seleccione la opción “Específico de la propiedad” y marque los permisos “Leer groupsTolgnore” y “Escribir groupsTolgnore”. Pulse “Siguiente >” para continuar. 
53.	Pulse “Finalizar” para completar la delegación de control.

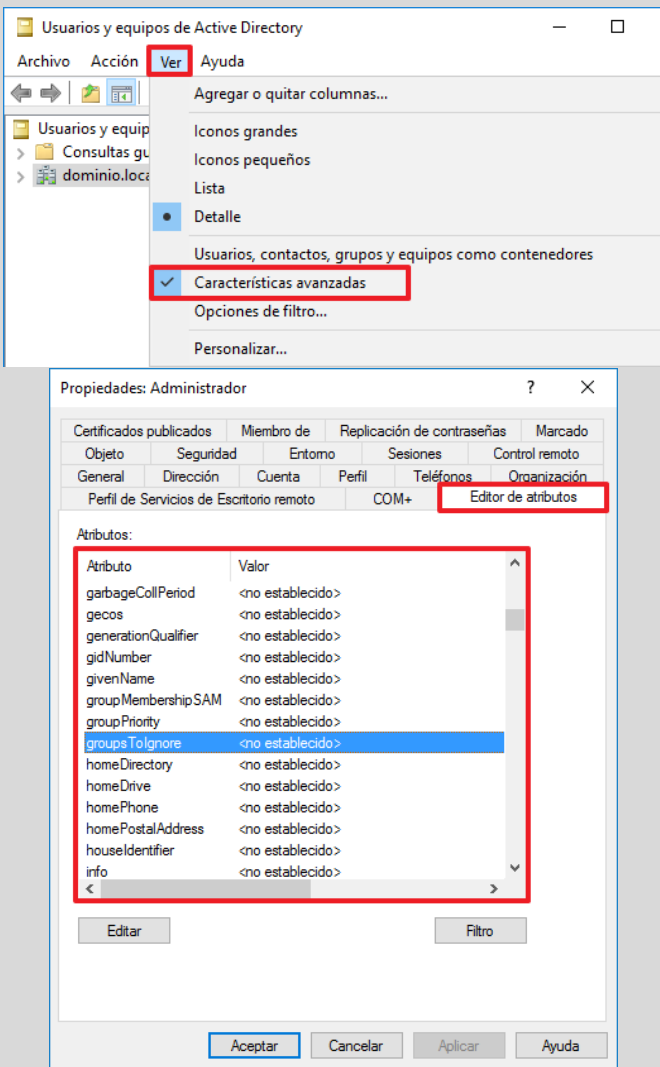
En este punto, cuando un usuario inicie sesión por primera vez no tendrá almacenada información de sesión, pero el siguiente inicio ya mostrará la información (fecha y hora) del último inicio de sesión realizado correctamente.

3.3. CONFIGURACIÓN DE SCRIPTS PARA MOSTRAR LA INFORMACIÓN DE INICIO DE SESIÓN

En este momento existe una GPO configurada y asociada a una unidad organizativa. Esta GPO crea una tarea programada en cada equipo que esté asociado a esta GPO, y ejecuta un script que muestra el ultimo inicio de sesión correcto que ha realizado el usuario.

Los pasos definidos a continuación establecen la configuración a realizar para que el script se ejecute al inicio de cada sesión de usuario. Este script no ha sido diseñado para que se ejecute como script de inicio de sesión ya que estos están deshabilitados por otras directivas.

Paso	Descripción
54.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.
55.	Pulse con botón derecho en el menú de inicio y seleccione el “Explorador de archivos”.
56.	Copie los siguientes ficheros al directorio “%SYSTEMROOT%\SYSVOL\sysvol\nombre_de_su_dominio\scripts”: – “Mostrar_informacion_ultimo_inicio_de_sesion_correcto.bat” – “Ultimo_inicio_de_sesion_correcto.ps1  Nota: Adapte esta ruta a la configuración que posea su organización. En el ejemplo está establecida la ruta por defecto del directorio “sysvol\dominio.local\scripts”. Deberá tener en consideración la replicación de estos ficheros en los diferentes dominio y subdominios que posea su organización para que estos ejecutados. El sistema le solicitará elevación de privilegios.
57.	Edite el fichero “Mostrar_informacion_ultimo_inicio_de_sesion_correcto.bat” y modifique el nombre del dominio para que coincida con el de su organización.  Nota: En este ejemplo se utiliza el nombre de dominio “dominio.local” y la ruta por defecto “\\sysvol\dominio.local\scripts”. Deberá editar esta ruta para que se adapte al nombre de su organización.

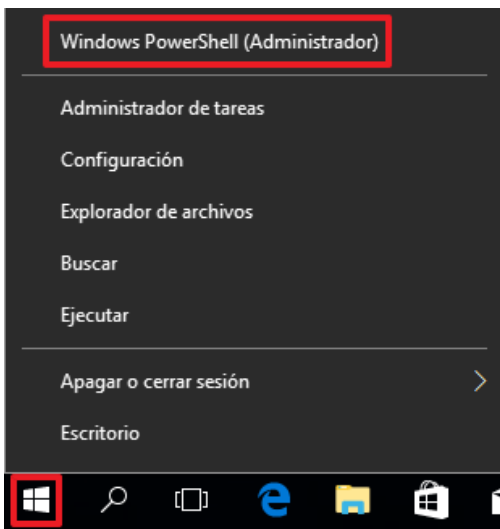
Paso	Descripción
58.	A continuación, edite el fichero “Ultimo_inicio_de_sesion_correcto.ps1”. Este script hace uso de los atributos del usuario para almacenar la información del último inicio de sesión tal y como se muestra en la imagen. <pre> \$objs = @() \$ErrorActionPreference = 'SilentlyContinue' \$ADProperty = 'groupstoignore' </pre> Nota: Para este ejemplo se ha utilizado el atributo de usuario “groupsToIgnore”. Para determinar que atributo es modificado puede hacer uso del siguiente enlace: https://msdn.microsoft.com/en-us/library/ms675090(v=vs.85).aspx. Podrá comprobar los atributos en uso dentro de la herramienta “Usuarios y Equipos de Active Directory” existente en el controlador de dominio, visualizando las “Características avanzadas”. Seleccione la que más se adecúe a las necesidades de su organización. 

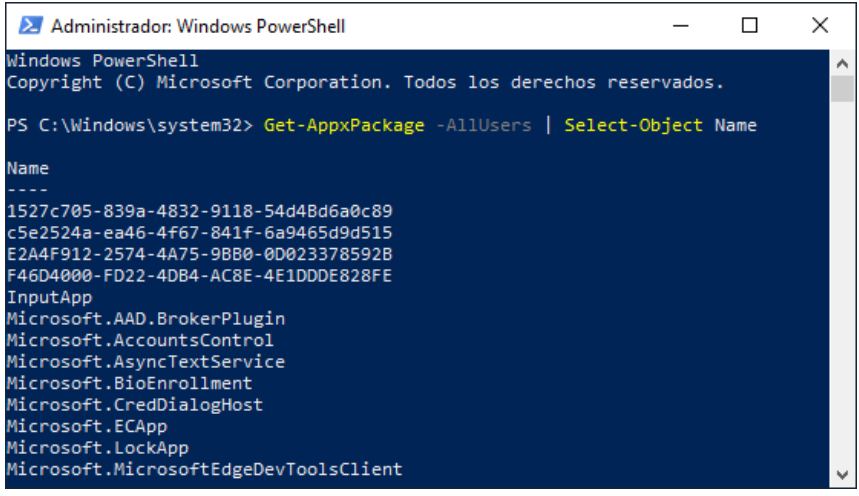
4. DESINSTALACIÓN DE APPS (UWP) EN WINDOWS 10

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 de inicio, funcionan como una App. Existen algunas de ellas que no se pueden desinstalar mediante este método como es el caso de Edge.

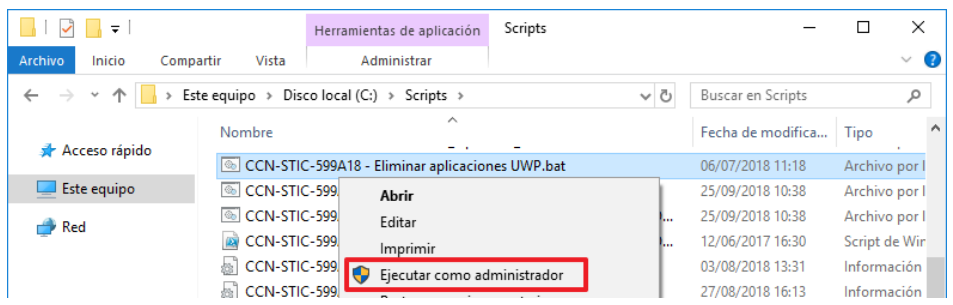
Existen dos tipos de aplicaciones. Aquellas nativas al sistema que se instalan junto con Windows 10 y aquellas que están preparadas para su ejecución (AppxProvisioned). El siguiente proceso describe la desinstalación de ambos tipos de Appx.

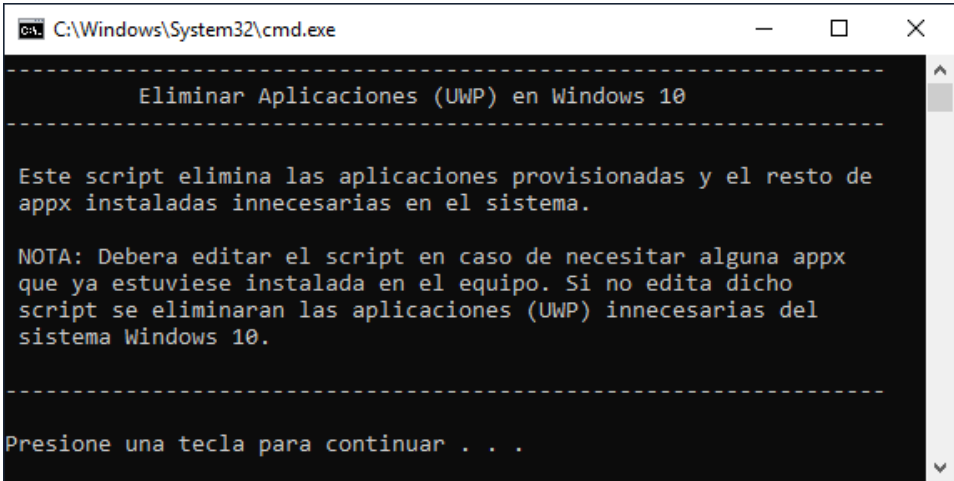
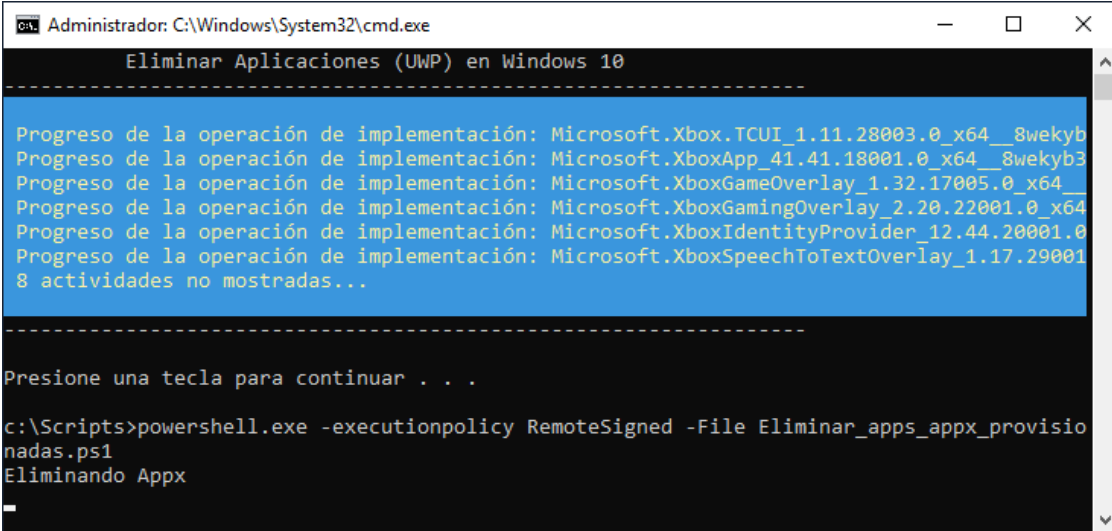
4.1. IDENTIFICACIÓN DE APPX INSTALADAS

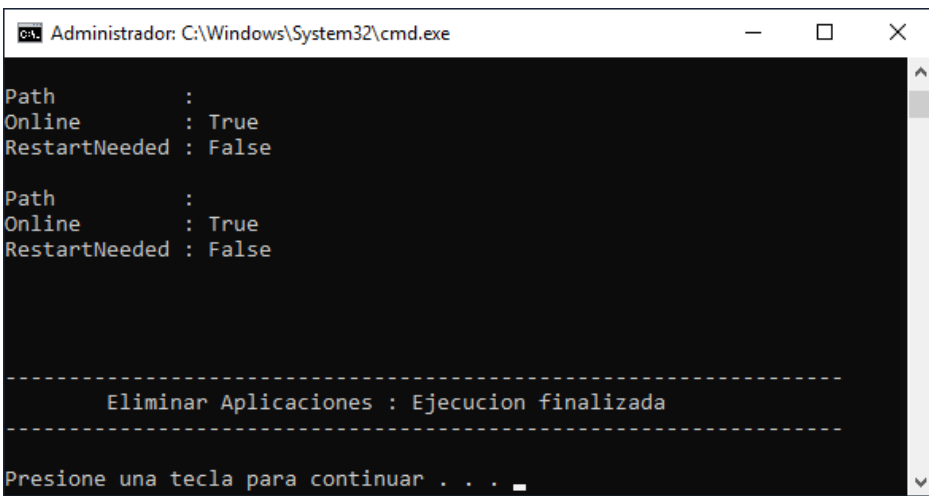
Paso	Descripción
1.	Inicie sesión en un equipo cliente en el cual desee eliminar las Appx precargadas.
2.	El primer paso a la hora de decidir que Appx se van a desinstalar, sería conocer cuáles son las que se encuentran instaladas.
3.	Ejecute una consola de “PowerShell” con permisos de administrador. Para ello pulse con el botón derecho sobre “Inicio” y seleccione “Windows PowerShell (Administrador)”.  Nota: Si apareciese “Símbolo del sistema Administrador” es debido a que se han cambiado las opciones de personalización del menú “Inicio” y deberá buscar la aplicación Powershell.
4.	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
5.	Ejecute la siguiente sintaxis para listar las aplicaciones instaladas y pulse “Enter”. Get-AppxPackage –Allusers Select-Object Name” 
6.	Con esto tendrá un listado de las Appx preinstaladas en su sistema.

4.2. ELIMINACIÓN DE APPX PROVISIONADAS E INSTALADAS

Paso	Descripción
7.	Inicie sesión en un equipo cliente con una cuenta con privilegios de administrador.
8.	Cree el directorio “Scripts” en “C:\”
9.	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-599A19 - Eliminar aplicaciones UWP.bat – Eliminar_apps_appx_provisionadas.ps1 Nota: Tenga en consideración la posibilidad de hacer llegar los siguientes ficheros a toda la organización a través de los métodos establecidos en la misma, pero siempre teniendo en cuenta que la ejecución de los scripts debe realizarse desde “C:\Scripts” si no se modifica el script en cuestión.
10.	Acceda al directorio “C:\Script”. Pulse con el botón derecho el fichero “CCN-STIC-599A19 - Eliminar aplicaciones UWP.bat” y seleccione la opción “Ejecutar como administrador” del menú contextual que aparecerá. 

Paso	Descripción
11.	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.
12.	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 especificar un listado de aplicaciones que desea desinstalar de forma que aquellas que sean necesarias no se desinstalen. Con este scripts se desinstalan todas las aplicaciones UWP innecesarias de Windows.
13.	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. 

Paso	Descripción
14.	Pulse una tecla cuando finalice el script. 
15.	A partir de este momento no se dispone de aplicaciones UWP innecesarias. Elimine el directorio "C:\Script" y todo su contenido.

5. ACTIVACIÓN DE TIENDA DE WINDOWS PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO

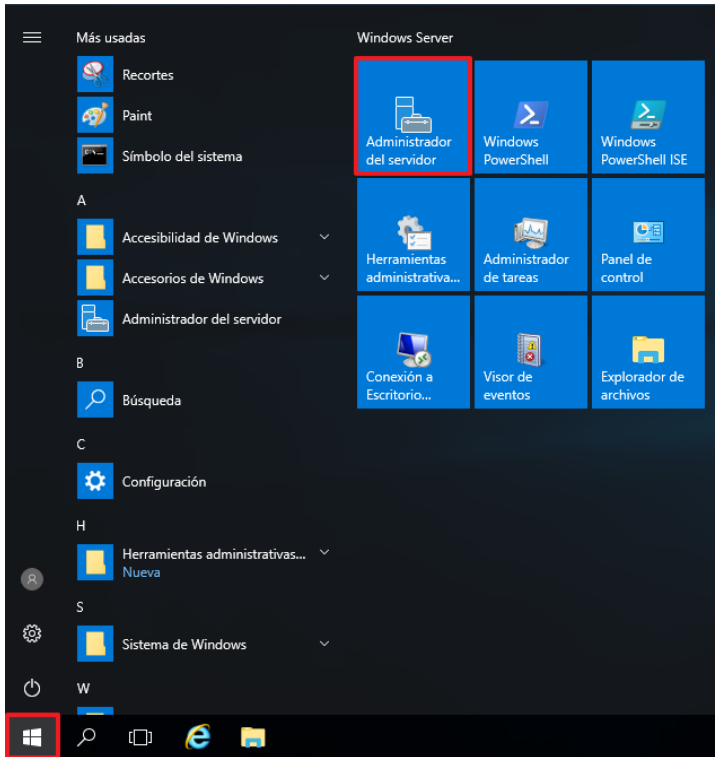
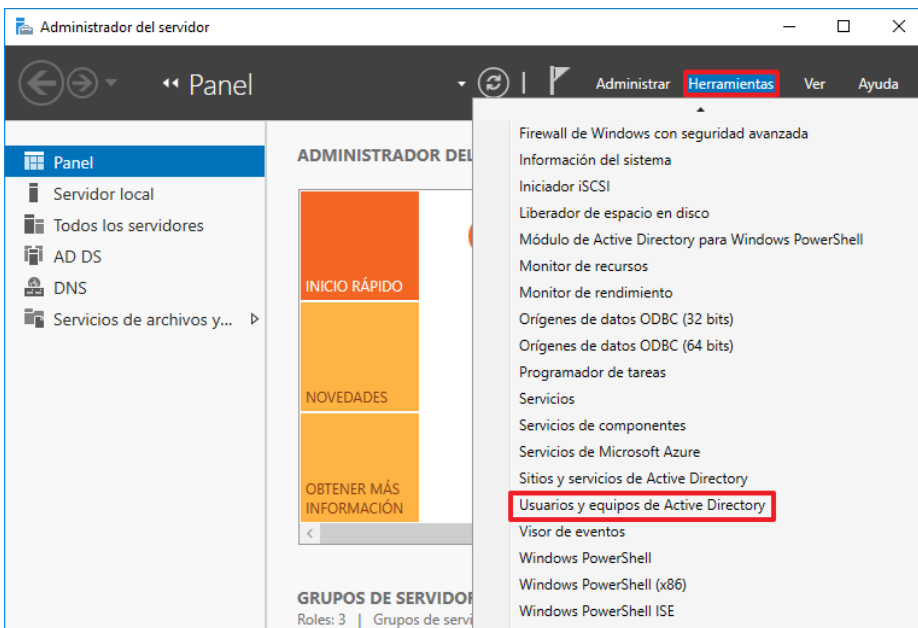
En este punto se va a tratar la posibilidad de activación del servicio de Tienda de Microsoft por necesidades propias de la entidad.

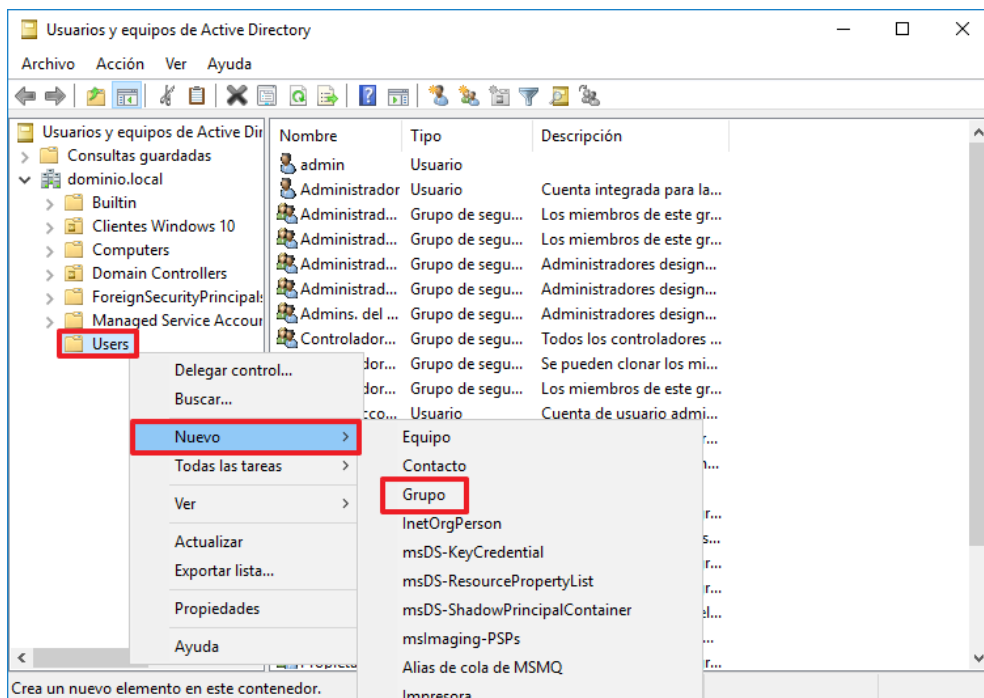
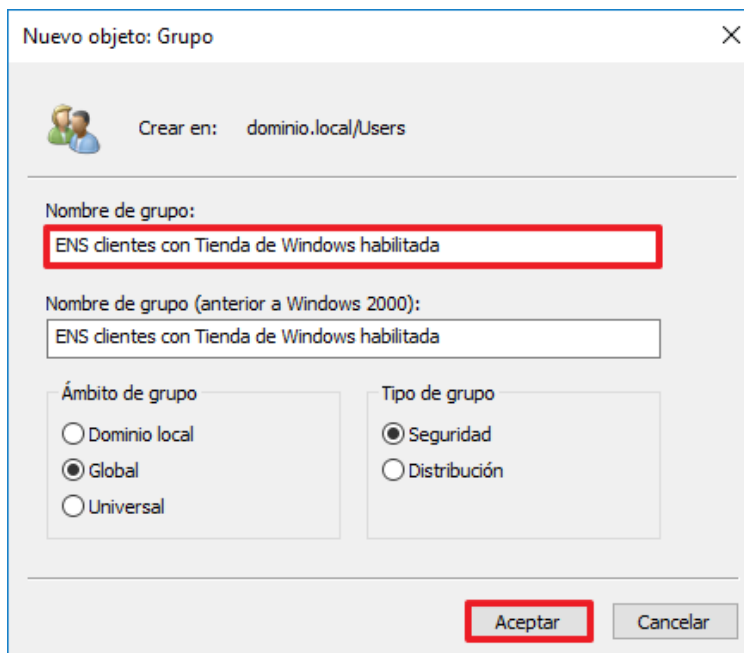
5.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

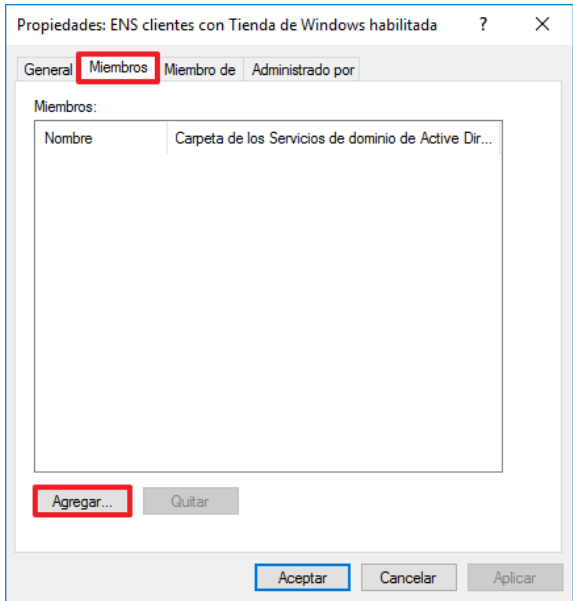
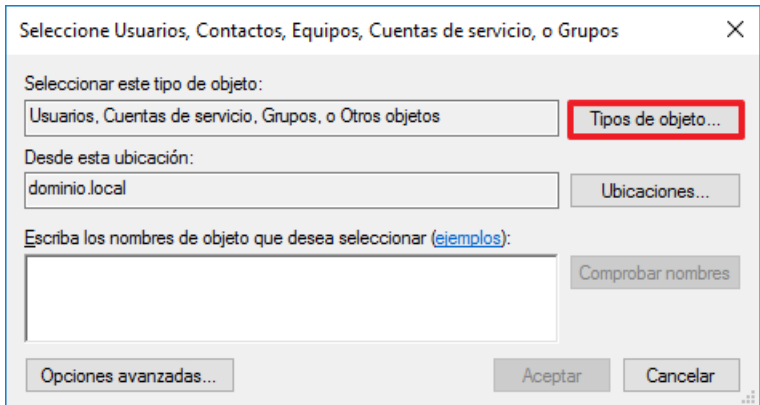
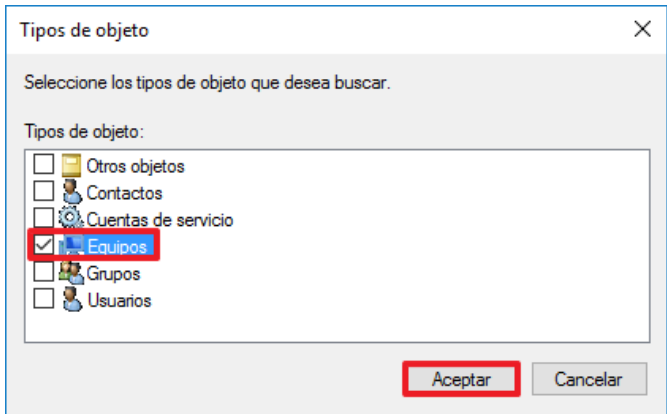
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

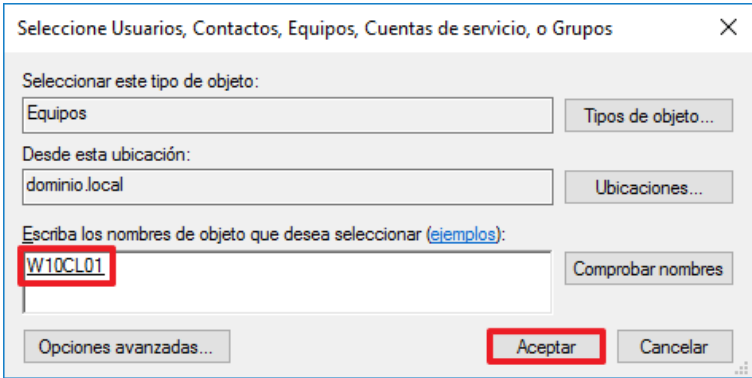
Nota: En el presente ejemplo se va a crear una política de grupo para habilitar el servicio de Tienda de Windows en los puestos que les sea de necesidad. Tenga en consideración que la edición "Pro" de Windows 10 no permite realizar un bloqueo de la Tienda a través de directivas de grupo por lo que deberá hacer uso de AppLocker para realizar el bloqueo de uso. Consulte el documento de seguridad codificado como "CCN-STIC-869 AppLocker en el ENS".

Paso	Descripción
1.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar la operativa de activación del servicio de Tienda de Windows.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
4.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Usuarios y equipos de Active Directory". 

Paso	Descripción
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 
6.	Introduzca como nombre “ENS clientes con Tienda de Windows habilitada”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO que habiliten el servicio de Tienda de Windows. 
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.

Paso	Descripción
8.	Pulse el botón “Agregar...”. 
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 

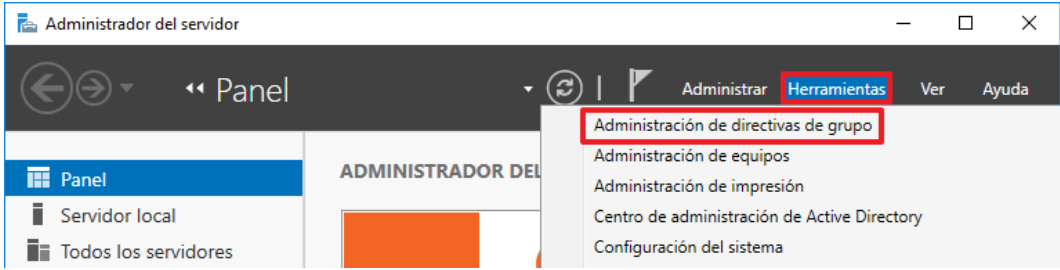
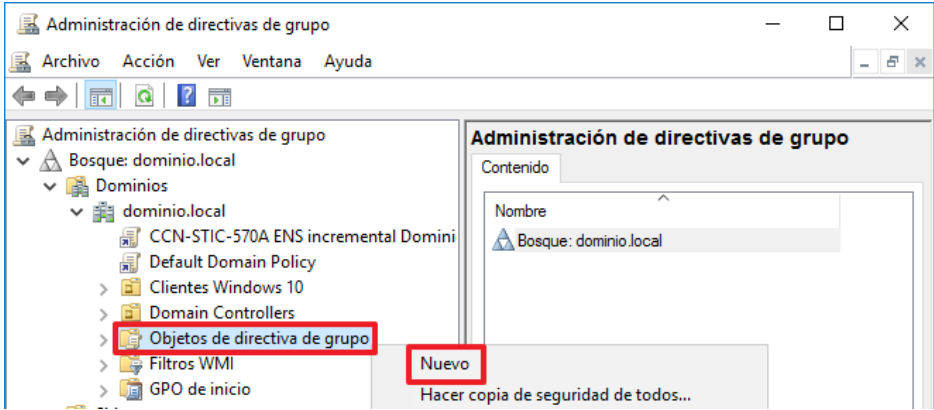
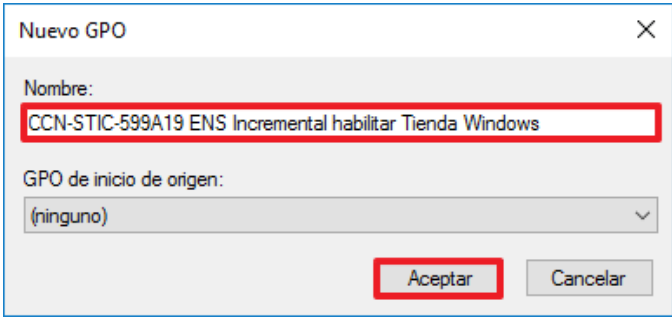
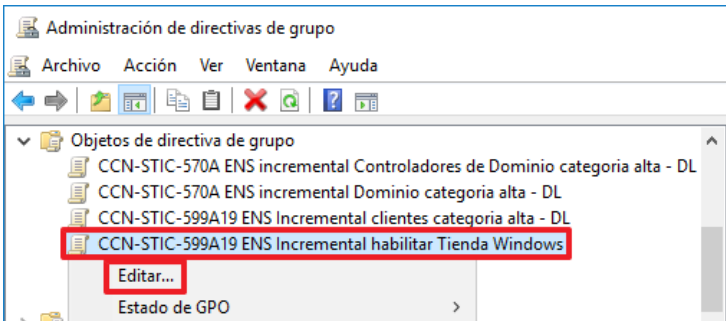
Paso	Descripción
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que cumplan las condiciones de aplicación de la GPO para habilitar la Tienda de Windows. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”.

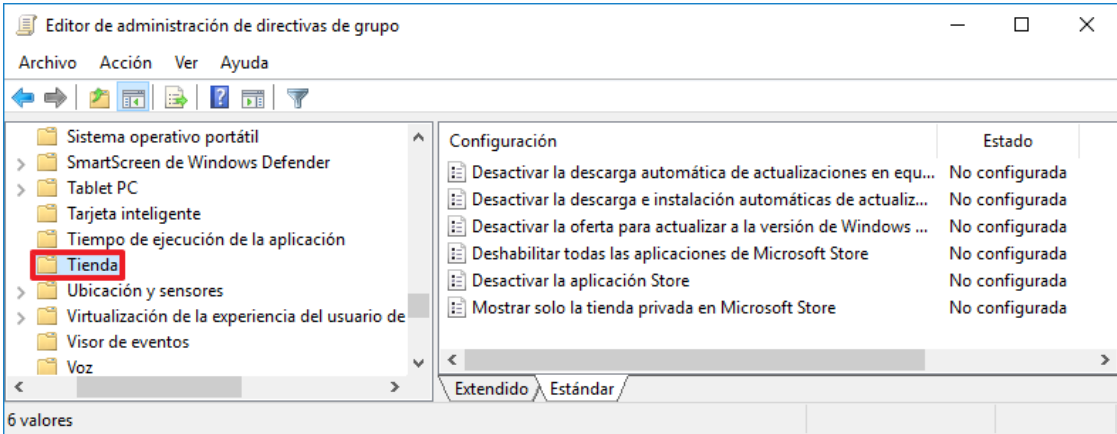
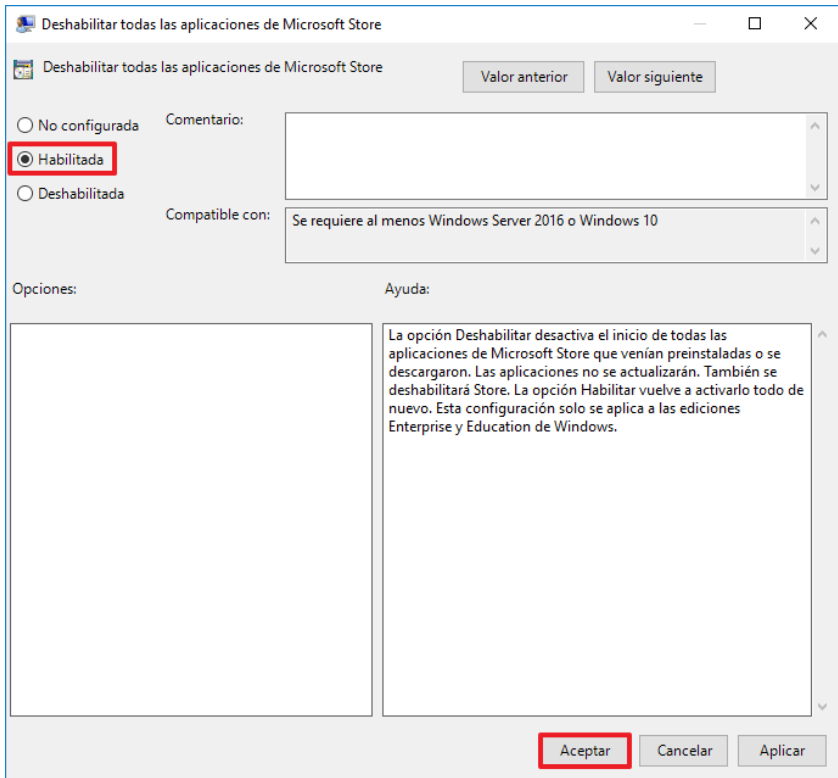
5.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA QUE HABILITE EL SERVICIO DE TIENDA DE WINDOWS

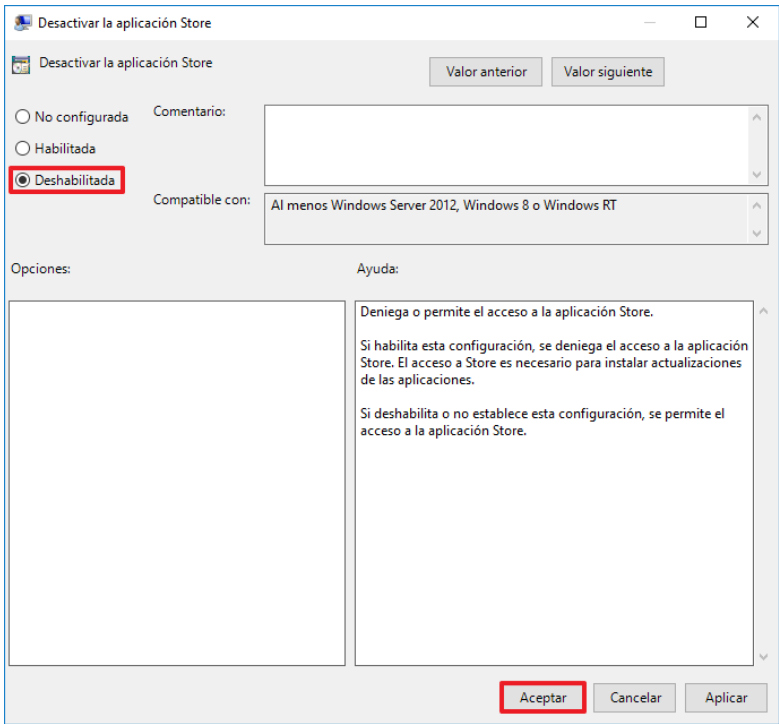
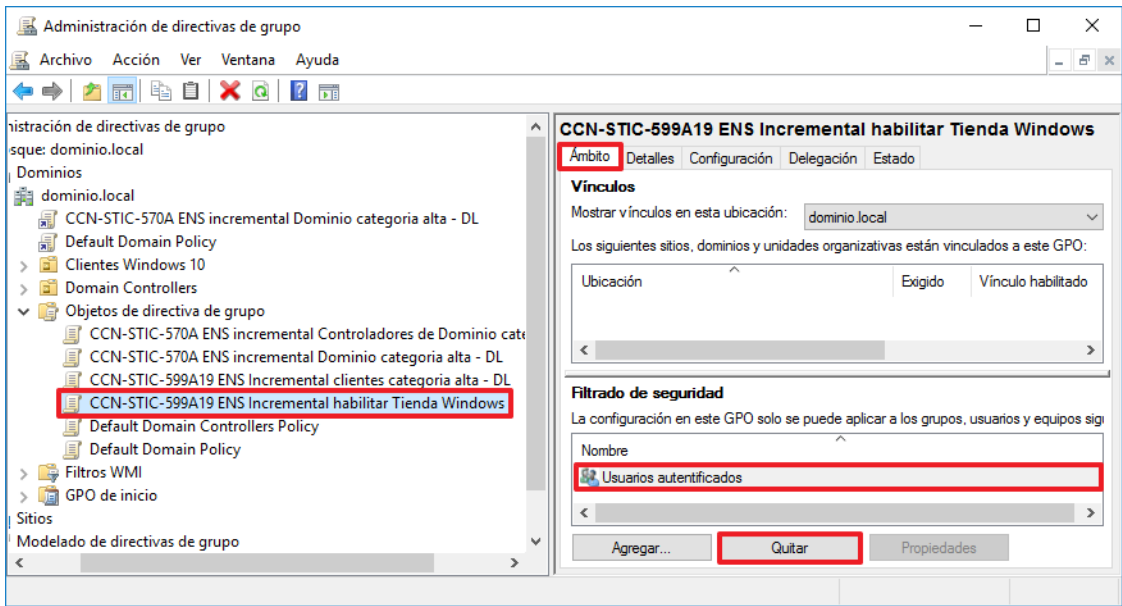
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política para habilitar el servicio de Tienda de Windows.

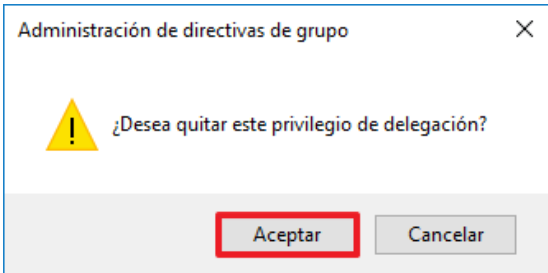
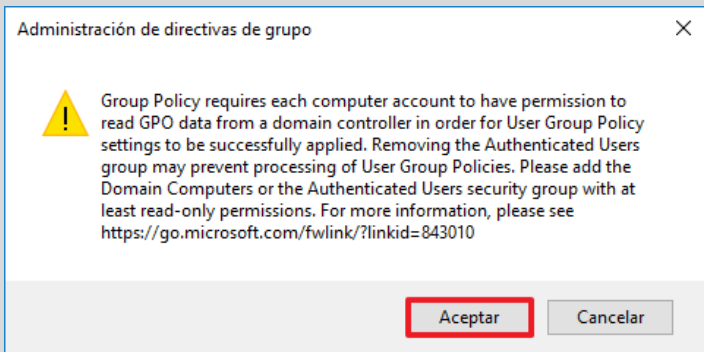
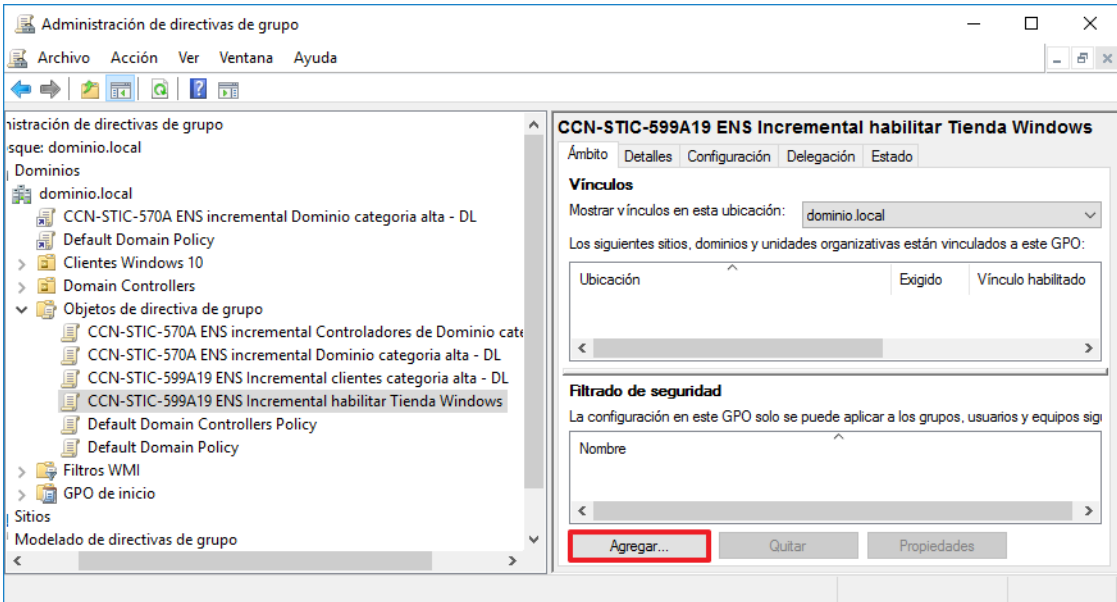
Nota: En el presente ejemplo se va a crear una política de grupo para habilitar el servicio de Tienda de Windows para un conjunto de clientes a los que les sea de necesidad el uso de dicho servicio.

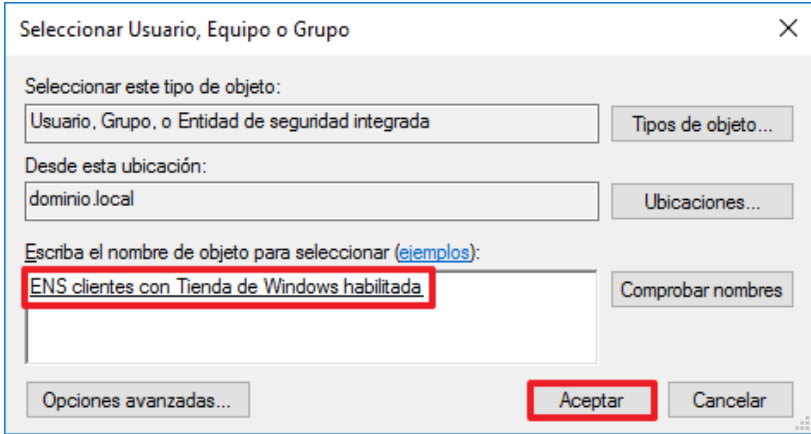
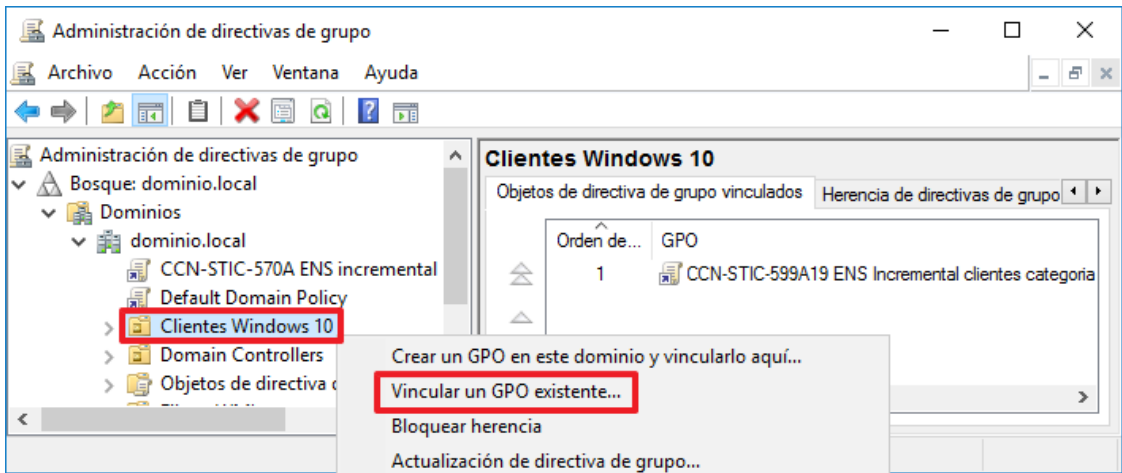
Paso	Descripción
14.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar la operativa de activación del servicio de Tienda de Windows.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

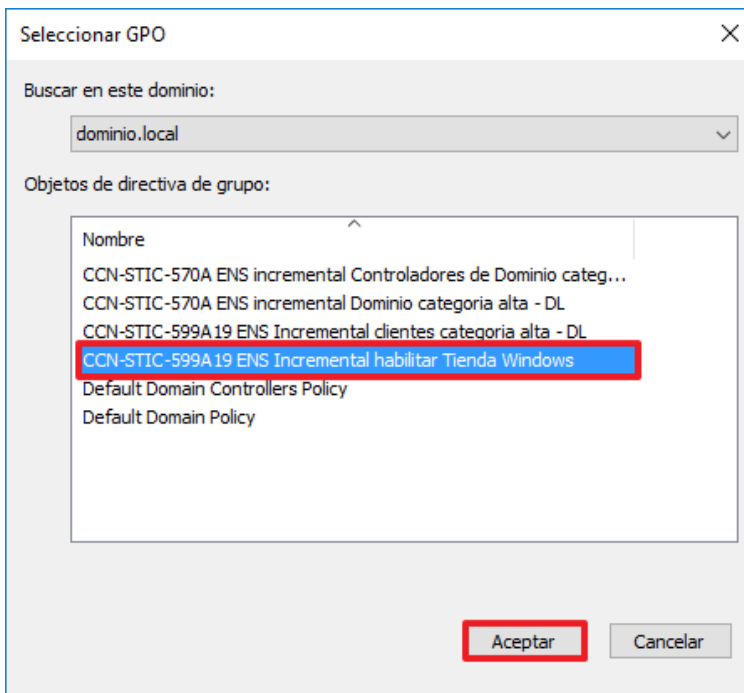
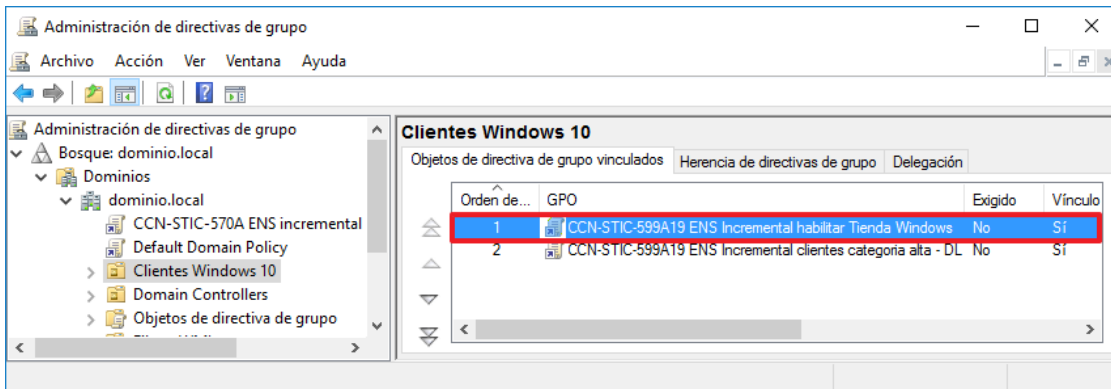
Paso	Descripción
17.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Administración de directivas grupo” 
18.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione “Nuevo”. 
19.	Introduzca como nombre “CCN-STIC-599A19 ENS Incremental habilitar Tienda Windows” y pulse el botón “Aceptar”. 
20.	Pulse botón derecho sobre la política que acaba de crear y seleccione “Editar...”. 

Paso	Descripción
21.	Sitúese en la siguiente ruta, perteneciente a la misma GPO. “Configuración de equipo → Directivas → Plantillas administrativas → Componentes de Windows → Tienda” 
22.	En la columna de la derecha haga doble clic sobre la directiva “Deshabilitar todas las aplicaciones de la Microsoft Store” y defina su estado en “Habilitada”. Pulse “Aceptar” para finalizar. 
23.	Ahora se va a activar la aplicación de la Tienda de Windows mediante la directiva “Desactivar la aplicación Store” ubicada en la misma ruta.

Paso	Descripción
24.	Seleccione la directiva mencionada anteriormente y ante la ventana emergente configure las opciones como se muestra en la imagen. Para finalizar el proceso pulse “Aceptar”. 
25.	Cierre el editor de administración de directivas de grupo.
26.	Seleccione ahora la GPO que acaba de configurar. Ubíquese en la pestaña “Ámbito”, seleccione el grupo “Usuarios autenticados” y pulse el botón “Quitar”. 

Paso	Descripción
27.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 
28.	Pulse ahora sobre el botón “Agregar...”. 

Paso	Descripción
29.	Seleccione el grupo creado en el punto anterior “ENS clientes con Tienda de Windows habilitada” y pulse “Aceptar”. 
30.	Ya solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.
31.	Seleccione la Unida Organizativa y pulsando con el botón derecho haga uso de la opción “Vincular un GPO existente...”. 

Paso	Descripción
32.	En la pantalla de selección, marque la GPO creada previamente y pulse el botón “Aceptar”. 
33.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el cuadro de la derecha. 
34.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.

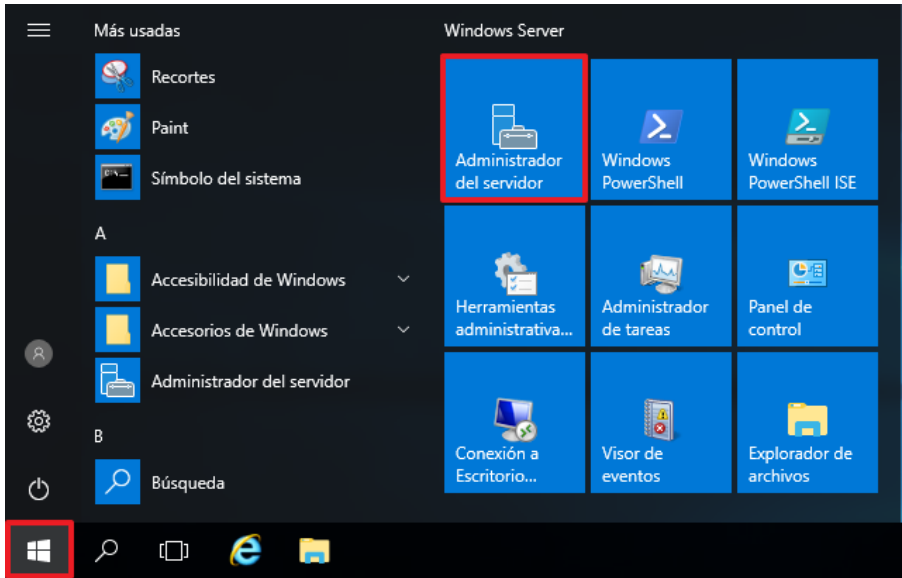
6. ACTIVACIÓN DE MICROSOFT ONEDRIVE PARA CLIENTES WINDOWS 10 MIEMBROS DE UN DOMINIO

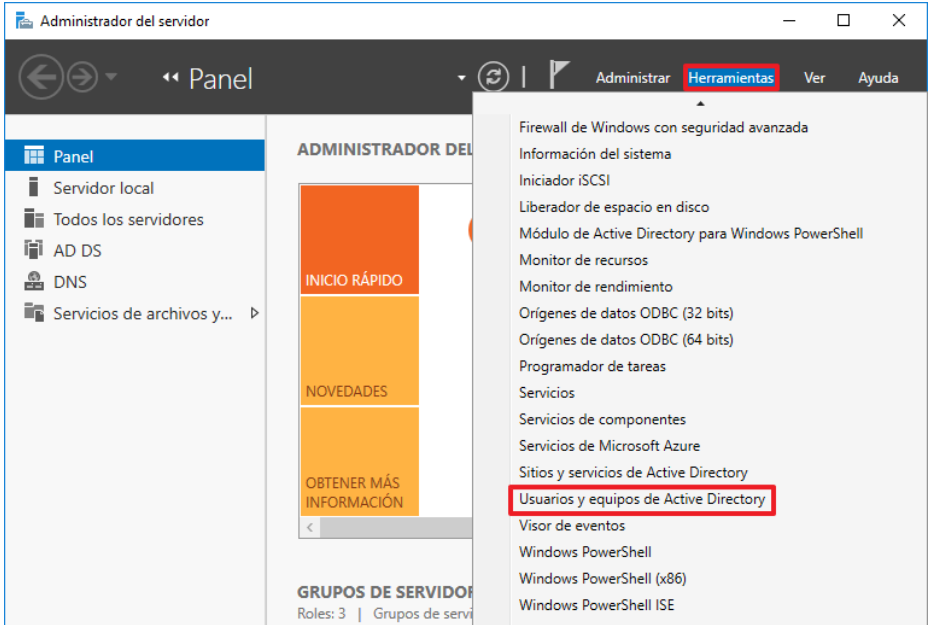
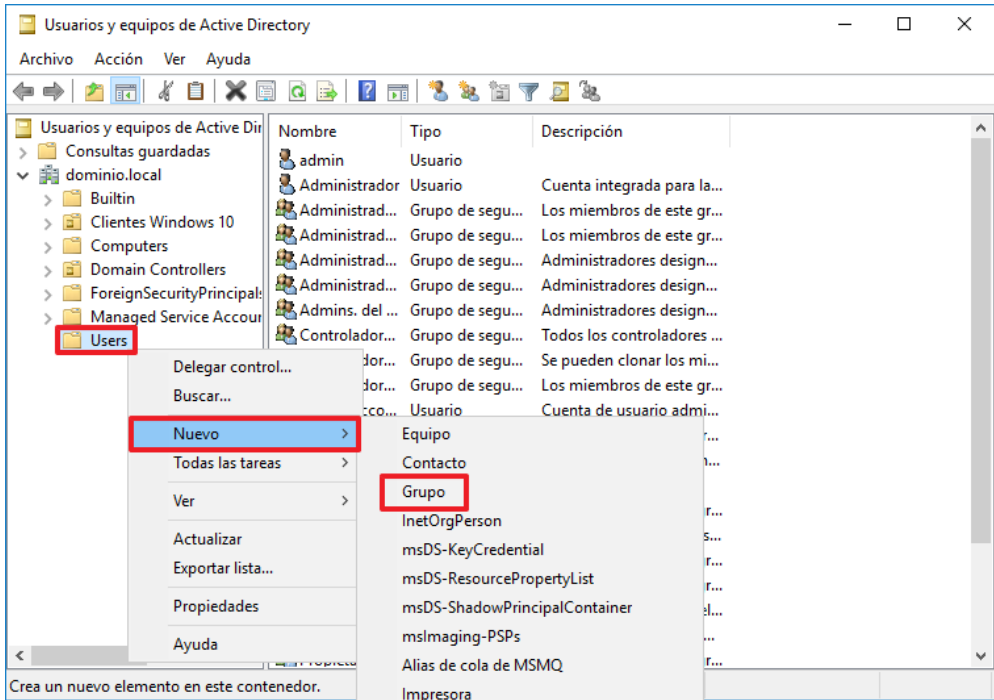
En este anexo se va a tratar la posibilidad de activación del servicio de Microsoft OneDrive por necesidades propias de la entidad.

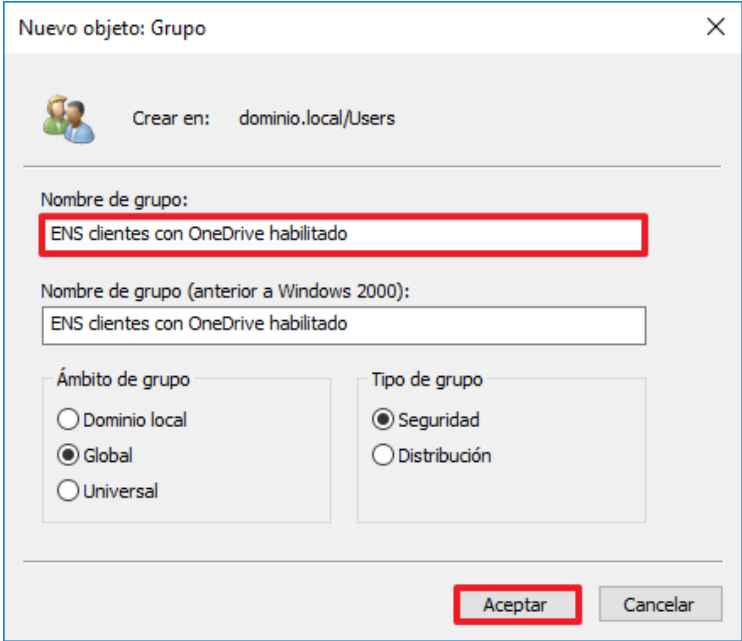
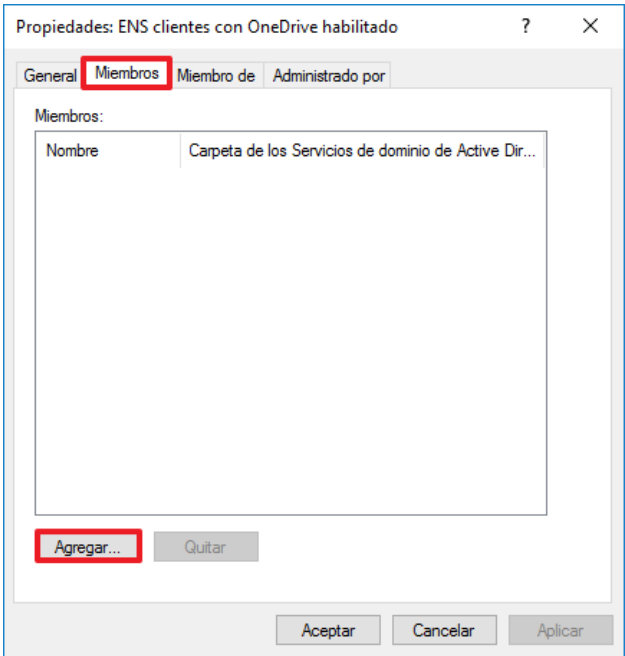
6.1. CREACIÓN DE GRUPOS PARA LA ASIGNACIÓN DE OBJETOS DE POLÍTICA DE GRUPO

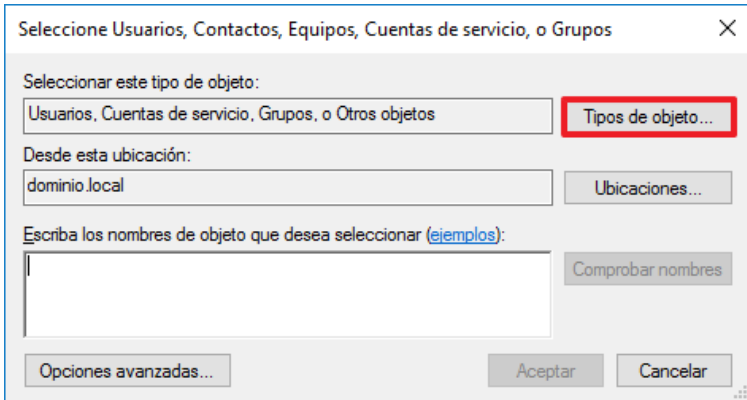
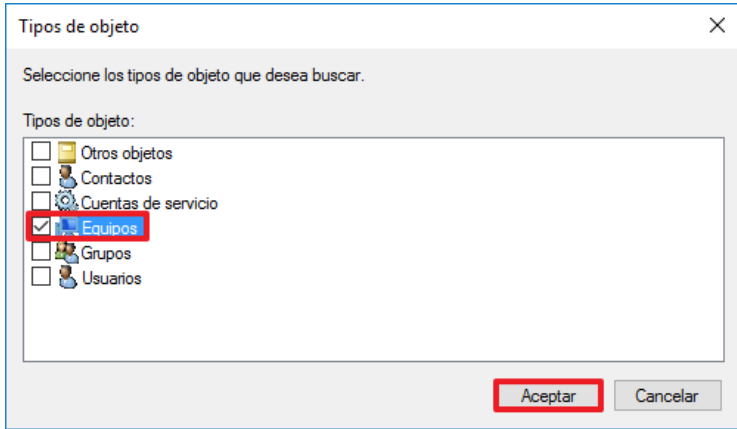
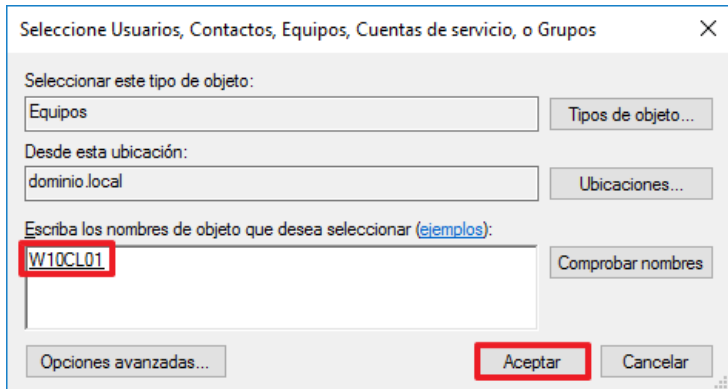
Motivado por el hecho de la posibilidad de aplicar diferentes configuraciones a los puestos de trabajo de una organización en base a sus necesidades, podrán aplicarse diferentes objetos GPO filtrados por grupos de equipos. Para realizar dicho filtrado será necesaria la creación de forma previa de los grupos de equipos necesarios en el Directorio Activo. En este sentido se considera conveniente agrupar los puestos de trabajo en base a los servicios y puertos que necesiten tener abiertos.

Nota: En el presente ejemplo se va a crear una política de grupo para habilitar el servicio de Microsoft OneDrive en los puestos que les sea de necesidad.

Paso	Descripción
1.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar la operativa de activación del servicio de Microsoft OneDrive.
2.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
3.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.

Paso	Descripción
4.	Seleccione el apartado “Herramientas” y a continuación la pestaña “Usuarios y equipos de Active Directory”. 
5.	Despliegue el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo → Grupo”. 

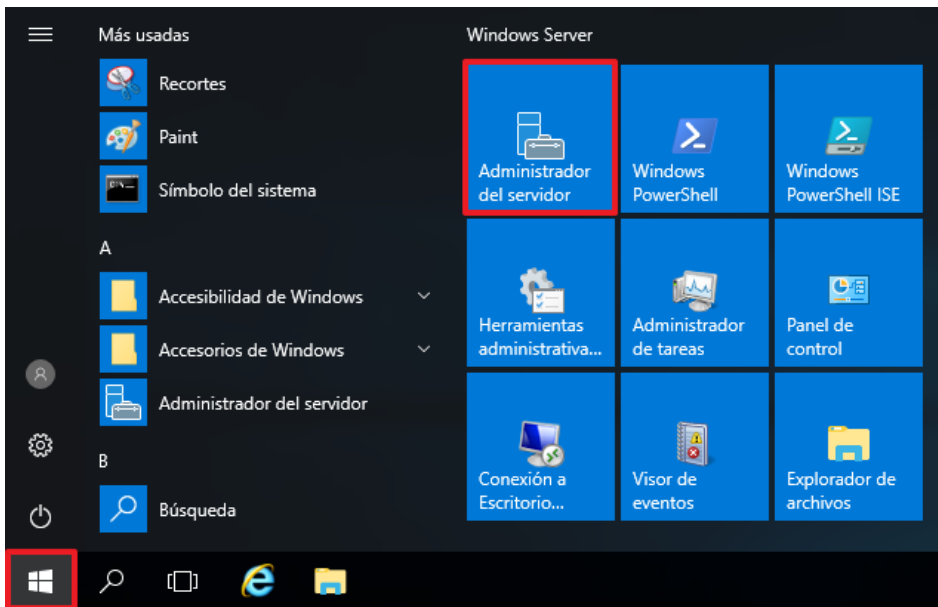
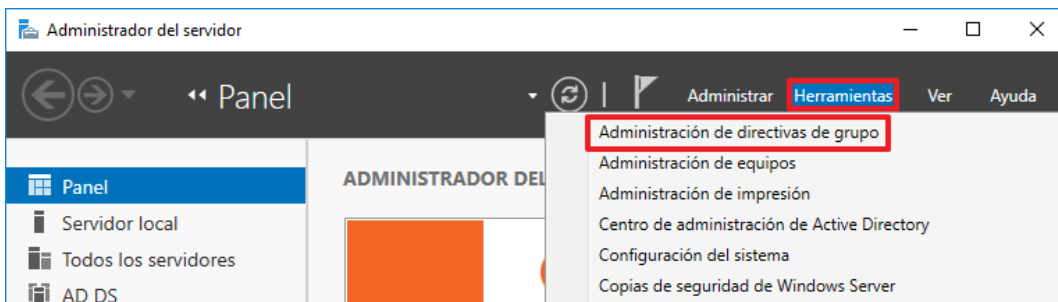
Paso	Descripción
6.	Introduzca como nombre “ENS clientes con OneDrive habilitado”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO que habiliten el servicio de OneDrive. 
7.	Abra el nuevo grupo creado y vaya a la pestaña “Miembros”.
8.	Pulse el botón “Agregar...”. 

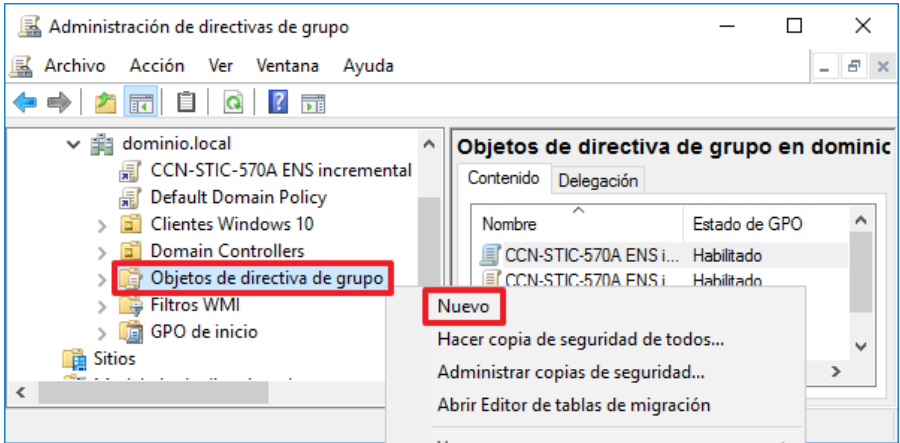
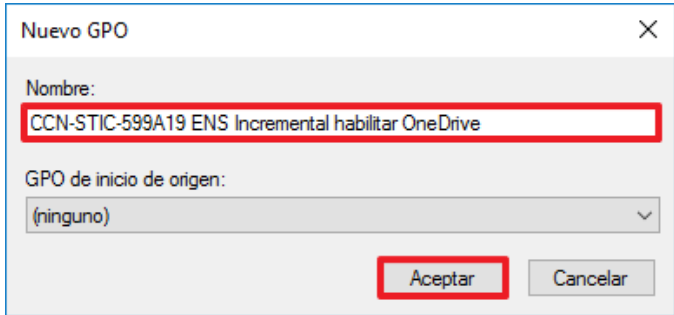
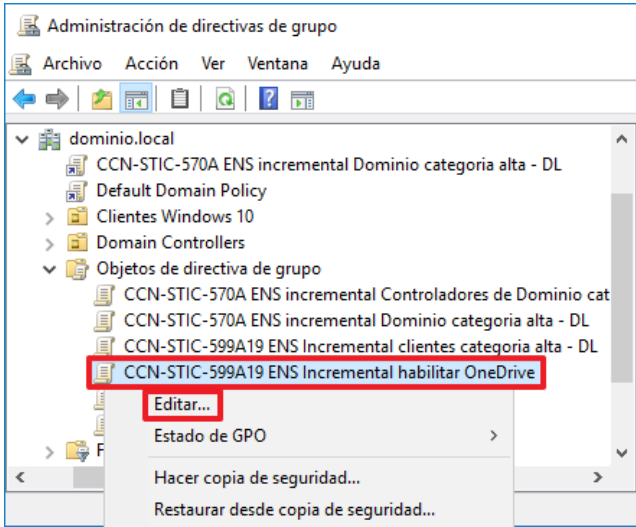
Paso	Descripción
9.	Pulse el botón “Tipos de objeto...”. 
10.	Marque el tipo de objeto “Equipos” y desmarque el resto. Pulse el botón “Aceptar”. 
11.	Introduzca el nombre de los clientes o utilice las opciones avanzadas para agregar todos aquellos clientes que cumplan las condiciones de aplicación de la GPO para habilitar OneDrive. Pulse el botón “Aceptar” para agregar la selección. 
12.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo.
13.	Cierre la herramienta “Usuarios y equipos de Active Directory”.

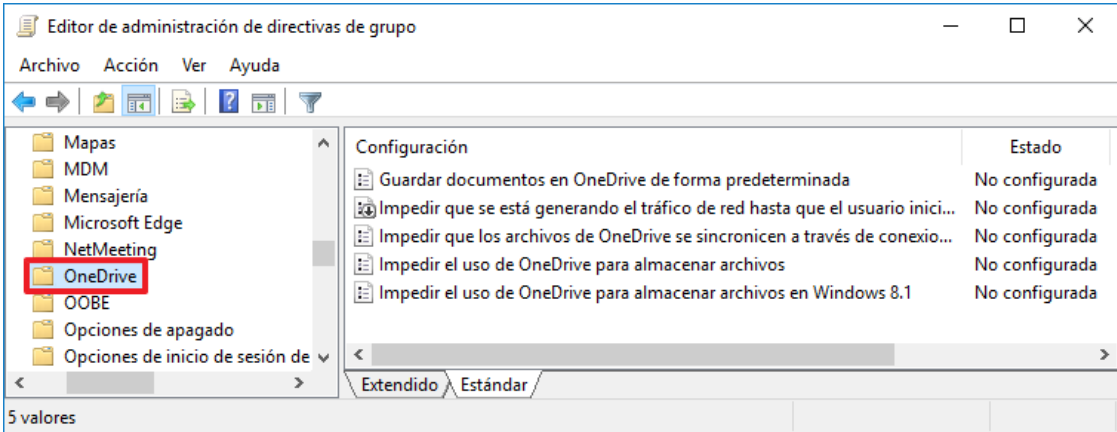
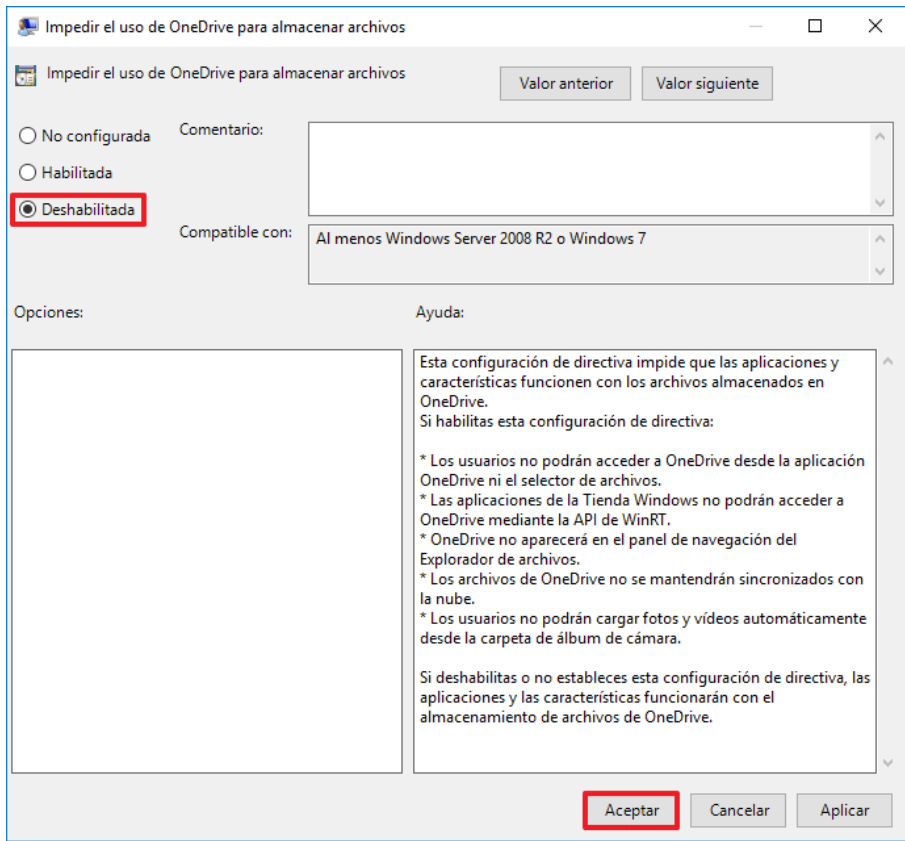
6.2. CREACIÓN Y ASIGNACIÓN DE LAS GPO PARA LA APLICACIÓN DE UNA POLÍTICA QUE HABILITE ONEDRIVE DE MICROSOFT

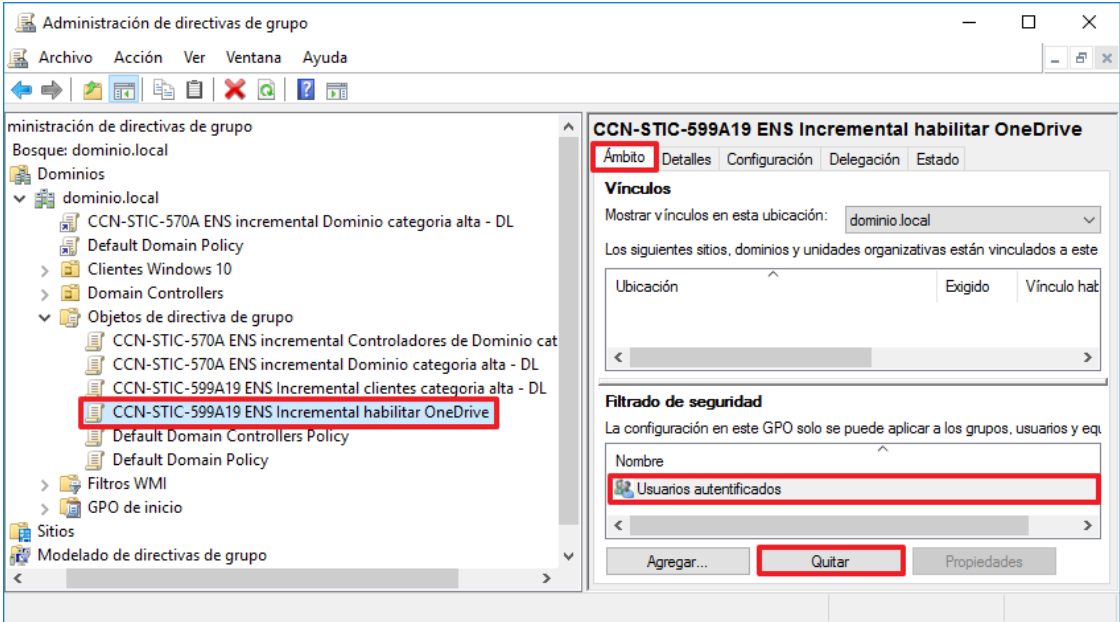
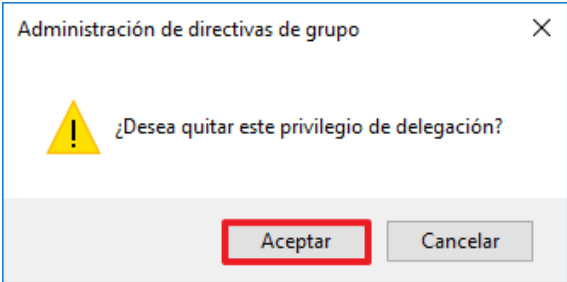
Una vez creado el grupo correspondiente, se procederá a crear y asignar la política para habilitar el servicio de Microsoft OneDrive.

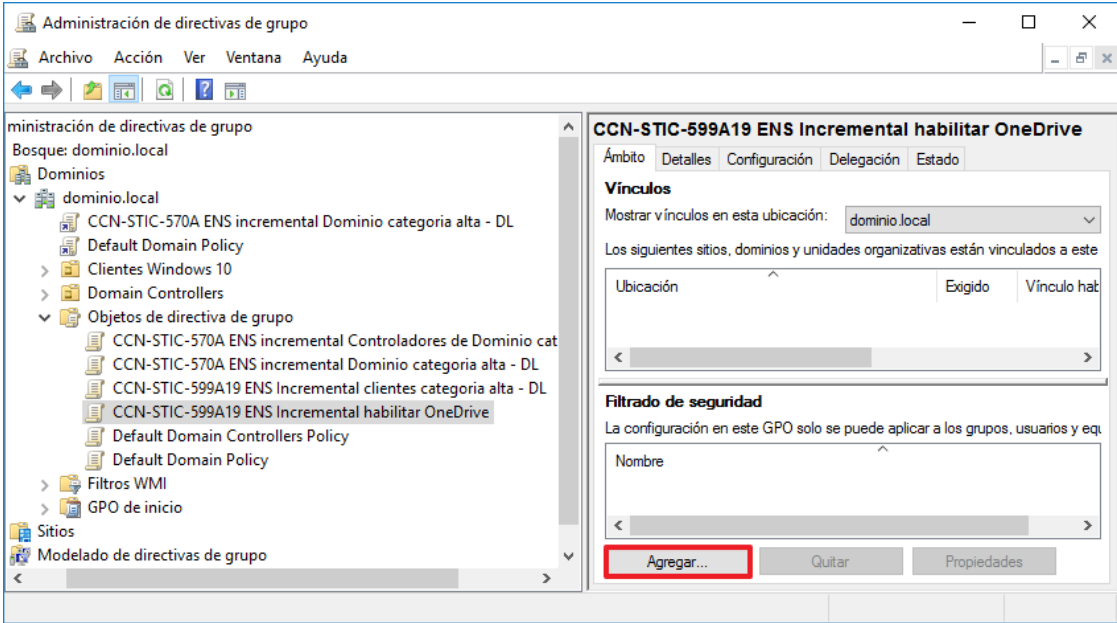
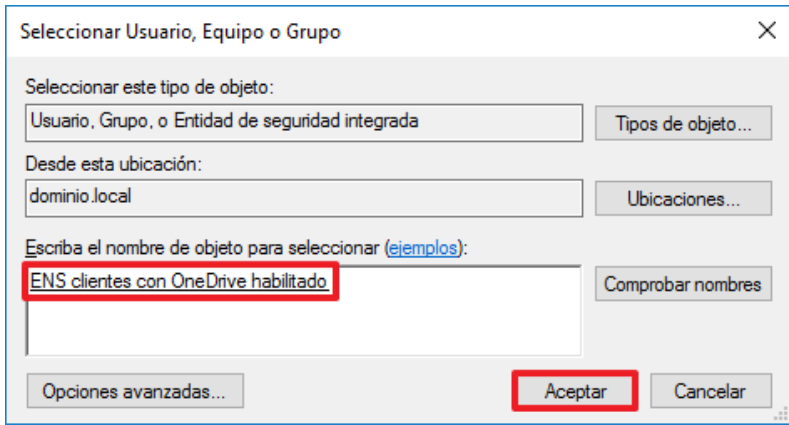
Nota: En el presente ejemplo se va a crear una política de grupo para habilitar Microsoft OneDrive para un conjunto de clientes a los que les sea de necesidad el uso de dicho servicio.

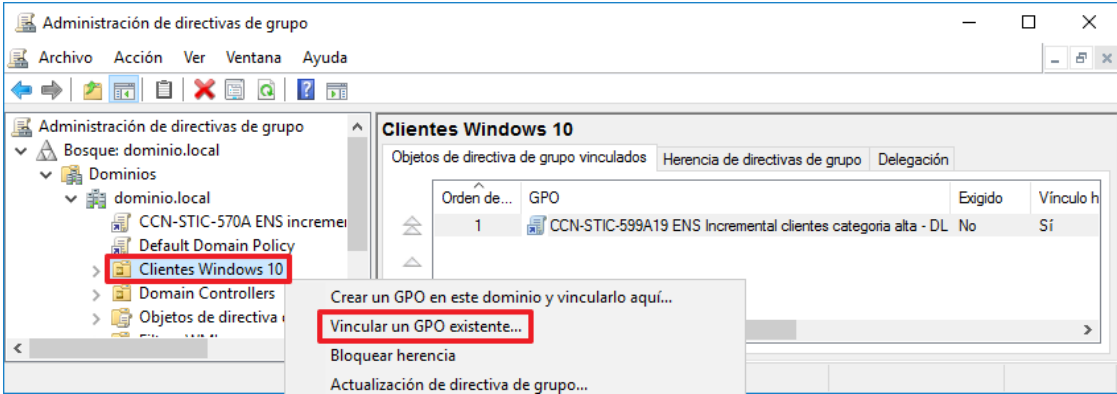
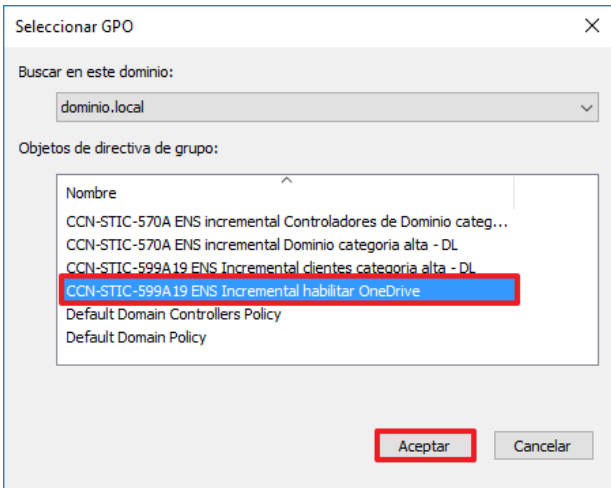
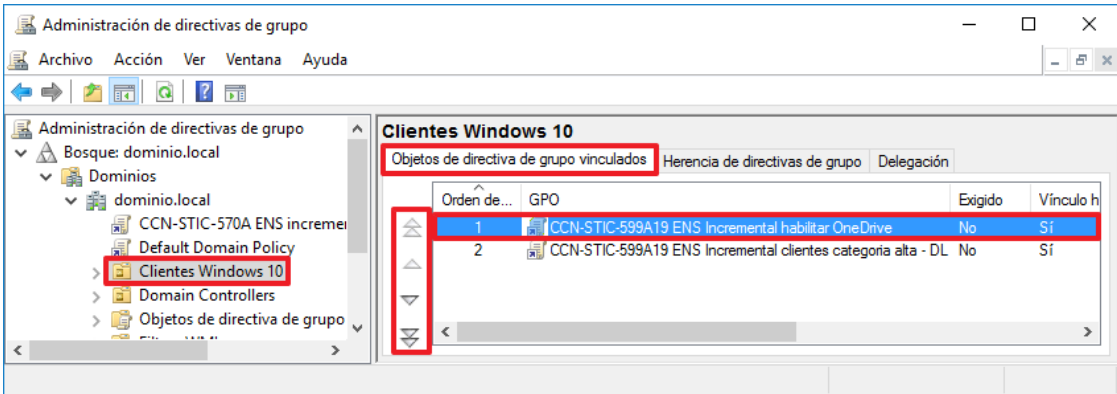
Paso	Descripción
14.	Inicie sesión en el controlador de dominio al cual pertenecen los equipos a los que se le va a aplicar la operativa de activación del servicio OneDrive.
15.	Debe iniciar sesión con una cuenta que sea Administrador del Dominio.
16.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios. Dependiendo de la categoría de seguridad de su sistema, se le solicitará confirmar la operación, o introducir las credenciales de un usuario con privilegios de administración.
17.	Seleccione el apartado "Herramientas" y a continuación la pestaña "Administración de directivas grupo". 

Paso	Descripción
18.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción “Nuevo”. 
19.	Introduzca como nombre “CCN-STIC-599A19 ENS Incremental habilitar OneDrive” y pulse el botón “Aceptar”. 
20.	Edite la política que acaba de crear, para ello pulse con el botón derecho del ratón sobre la misma y seleccione la opción “Editar...”. 

Paso	Descripción
21.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. “Configuración de equipo → Directivas → Plantillas administrativas → Componentes de Windows → OneDrive” 
22.	En el panel derecho haga doble clic sobre la directiva “Impedir el uso de OneDrive para almacenar archivos”. Establezca su configuración en “Deshabilitada” y pulse “Aceptar”. 

Paso	Descripción
23.	A continuación, seleccione la GPO que acaba de crear. Ubíquese en la pestaña ámbito, seleccione el grupo “Usuarios autenticados” y pulse el botón “Quitar”. 
24.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 

Paso	Descripción
25.	Pulse ahora sobre el botón “Agregar...”. 
26.	Seleccione el grupo creado en el punto anterior “ENS clientes con OneDrive habilitado” y pulse “Aceptar”. 
27.	Ya solo queda realizar la asignación de la política. Para ello identifique el lugar dentro del Directorio Activo donde se ubican estos clientes y asigne allí la política. Si los clientes se ubicaran en diferentes Unidades Organizativas, puede buscar un lugar común desde donde cuelguen las diferentes ubicaciones o bien asignar la GPO en cada una de las Unidades Organizativas. En el ejemplo los clientes se encuentran ubicados en la Unidad Organizativa “Clientes Windows 10”.

Paso	Descripción
28.	Seleccione la Unida Organizativa y pulsando con el botón derecho haga uso de la opción “Vincular un GPO existente...”. 
29.	En la pantalla de selección, marque la GPO creada previamente y pulse “Aceptar”. 
30.	Si existen más directivas asociadas a la misma unidad organizativa, es necesario desplazar la creada en este punto hasta la parte alta de las directivas en el cuadro de la derecha. 
31.	El nuevo GPO ya estará creado y asignado correctamente al grupo de clientes que le corresponde.

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:

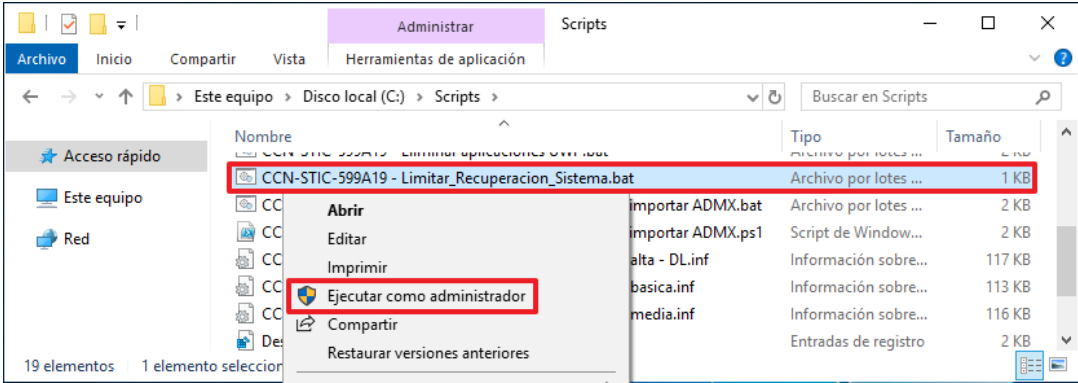
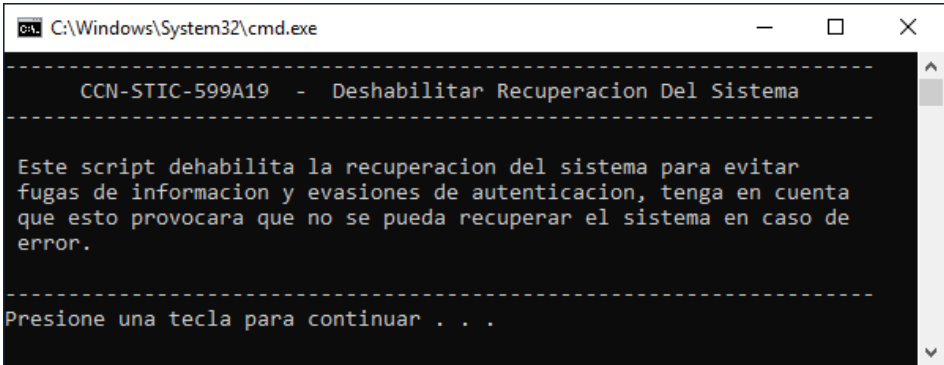
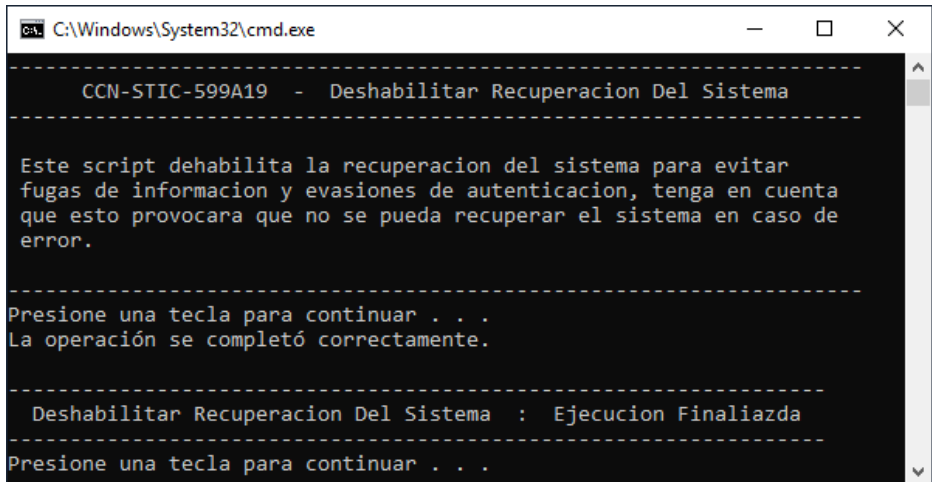
- Cifrado del sistema de archivos. Utilizar BitLocker u otro sistema de cifrado autorizado para evitar el acceso a la información almacenada y, por tanto, evitar su modificación ya que requiere de la introducción de un PIN o contraseña en el arranque del equipo, o en el momento de acceder a los datos. 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.

7.1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

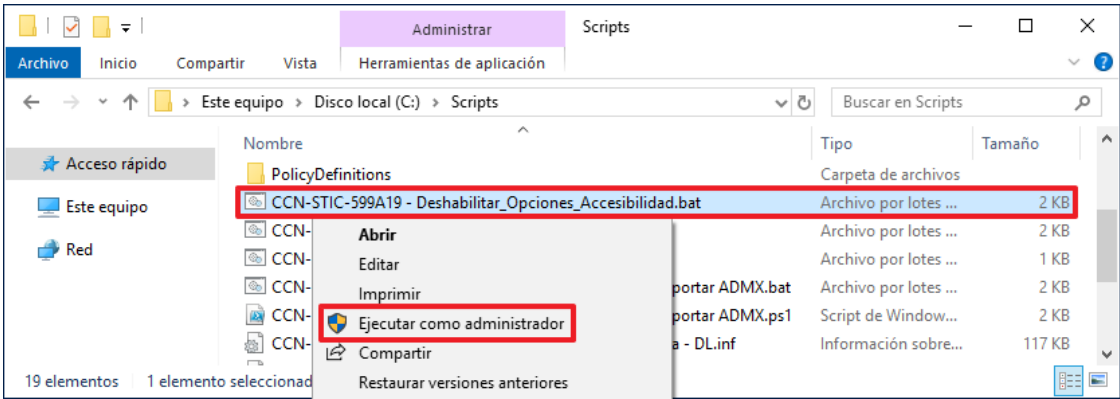
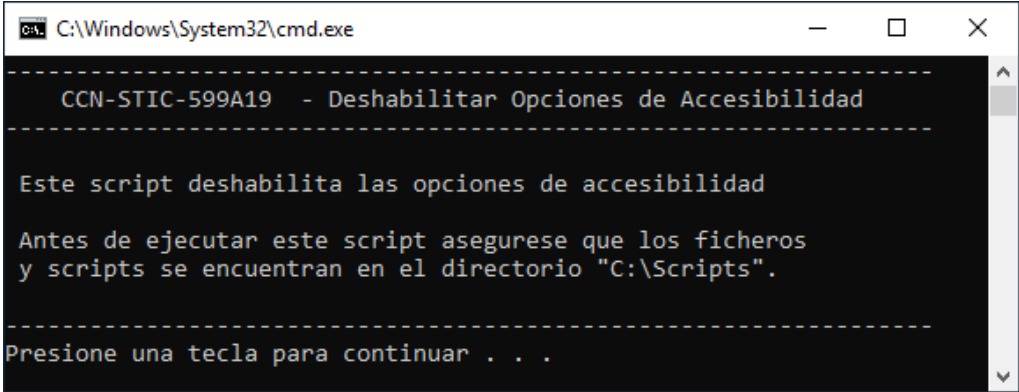
A continuación, se indican los pasos a realizar para deshabilitar la funcionalidad de recuperación del sistema.

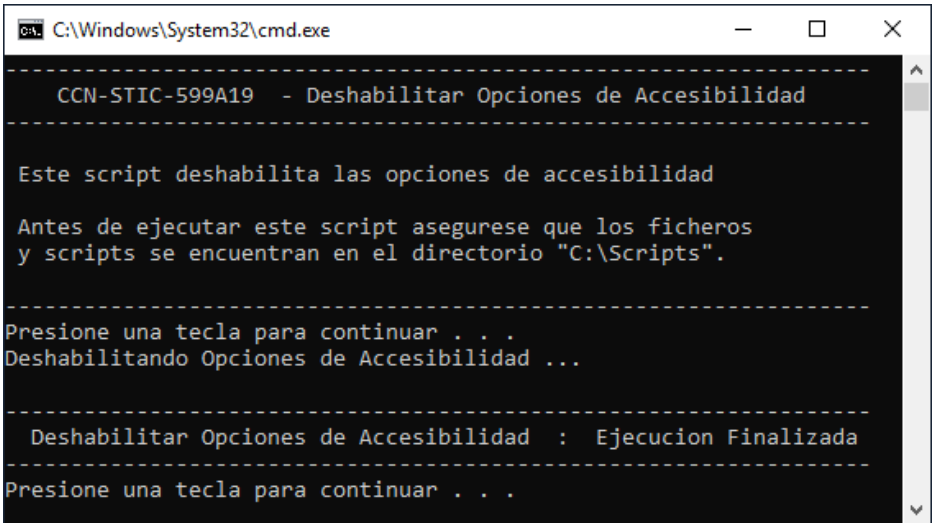
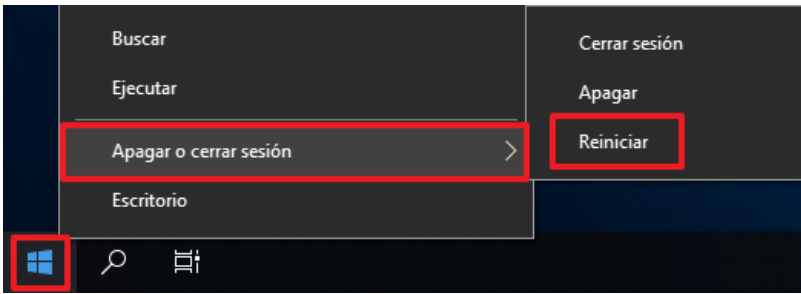
Paso	Descripción
1.	Inicie sesión en el equipo con una cuenta con permisos de administrador del dominio.

Paso	Descripción
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-599A19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.  Nota: El sistema le solicitará elevación de privilegios.
4.	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. 
5.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana. 
6.	Elimine el directorio “C:\Scripts”.

7.2. DESHABILITAR LAS OPCIONES DE ACCESIBILIDAD

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

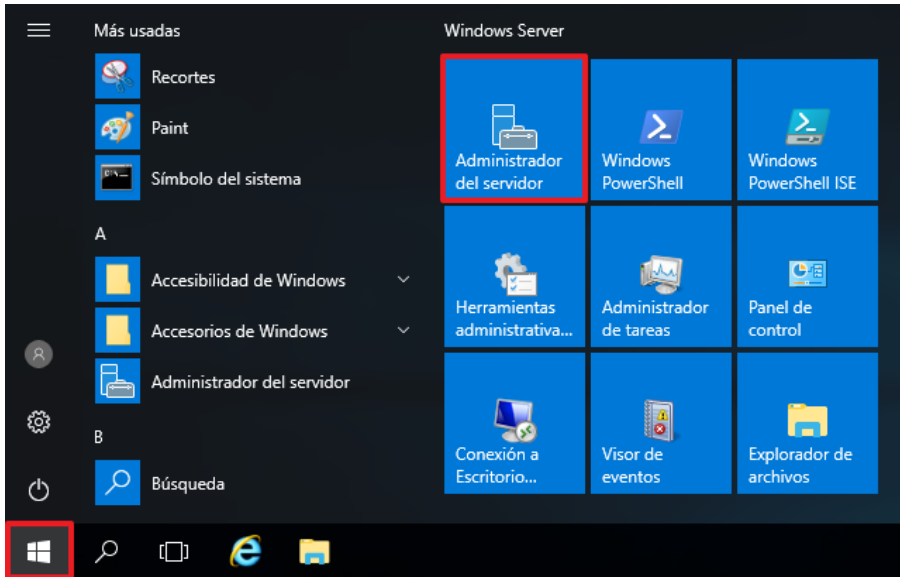
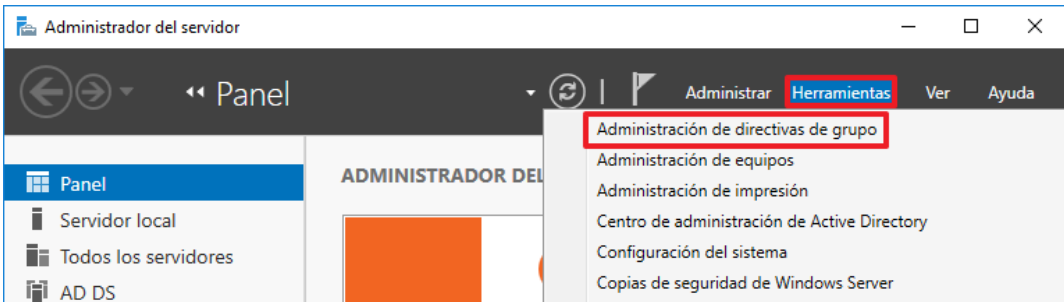
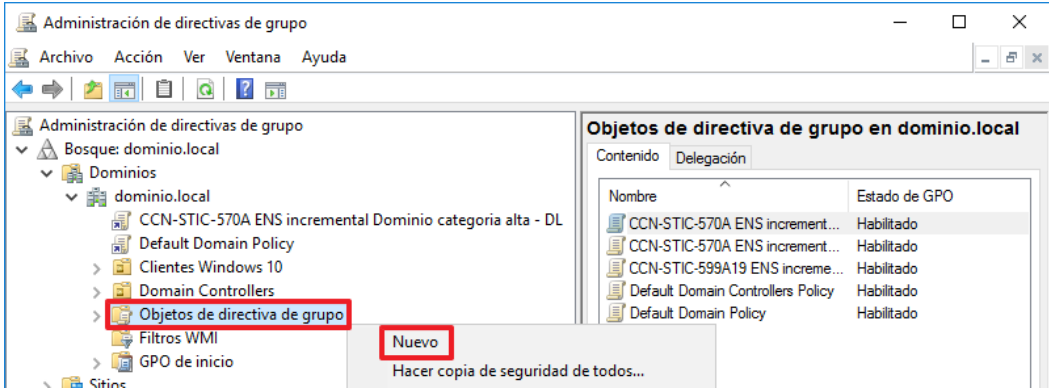
Paso	Descripción
7.	Inicie sesión en el equipo con una cuenta con permisos de administrador del dominio.
8.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
9.	Localice el archivo “CCN-STIC-599A19 – Deshabilitar_Opciones_Accesibilidad.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”.  Nota: El sistema le solicitará elevación de privilegios.
10.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 

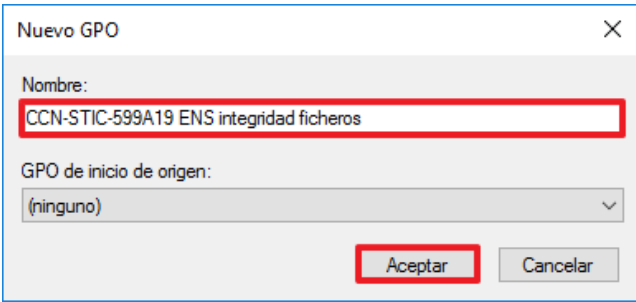
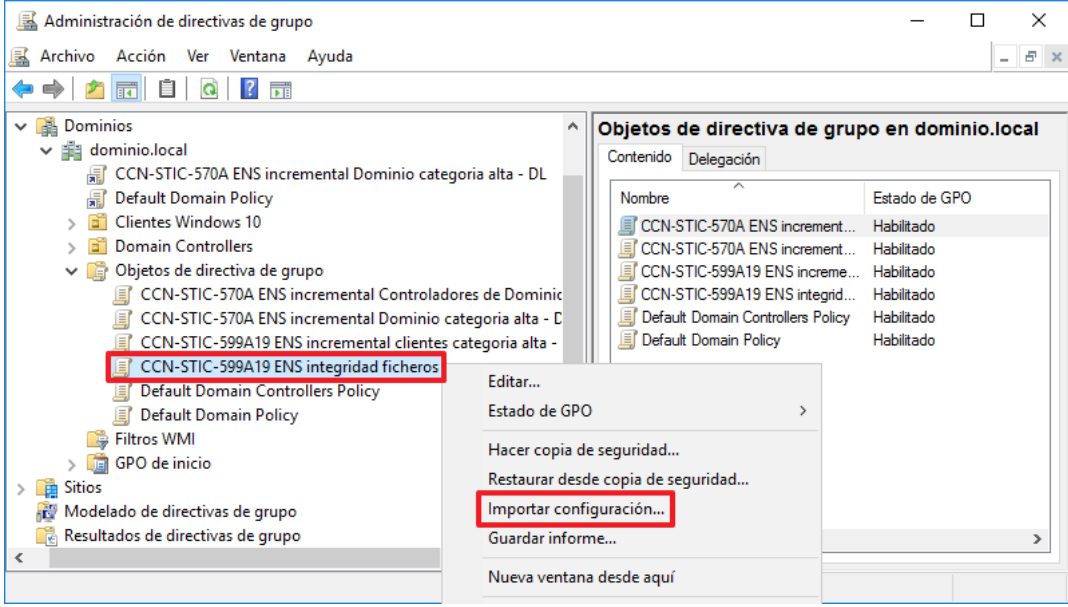
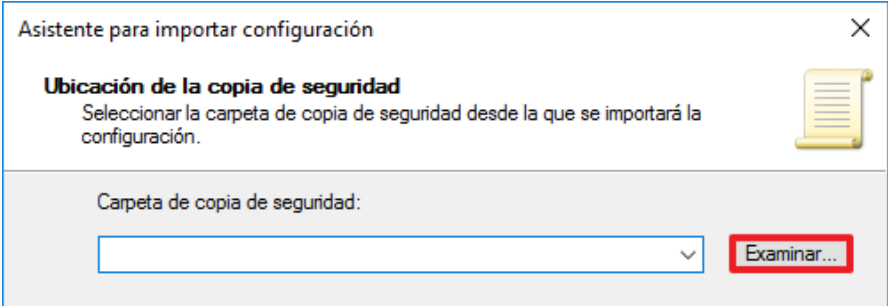
Paso	Descripción
11.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comando 
12.	Por último, deberá reiniciar el sistema para que los cambios sean aplicados. Para ello haga clic derecho en el botón de “Inicio” y seleccione “Apagar o cerrar sesión → Reiniciar”. 
13.	Elimine el directorio “C:\Scripts”.

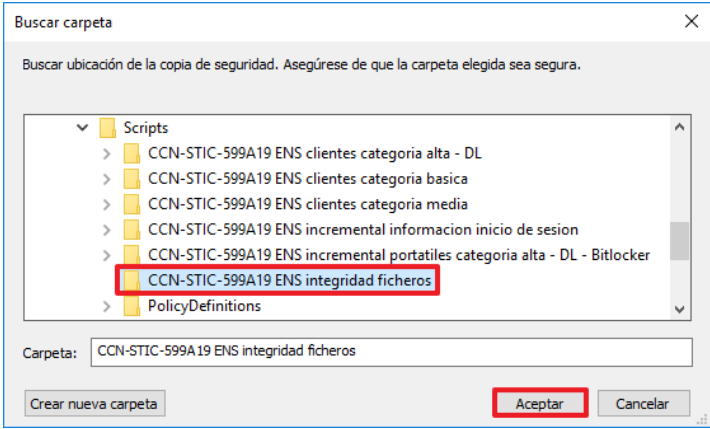
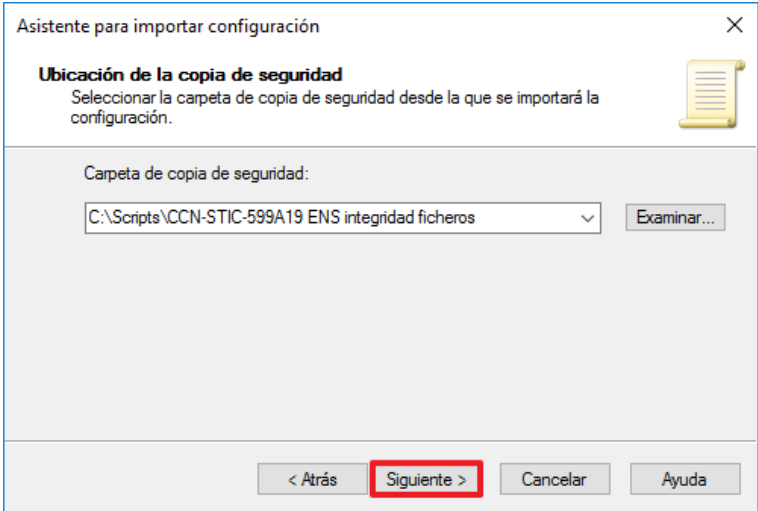
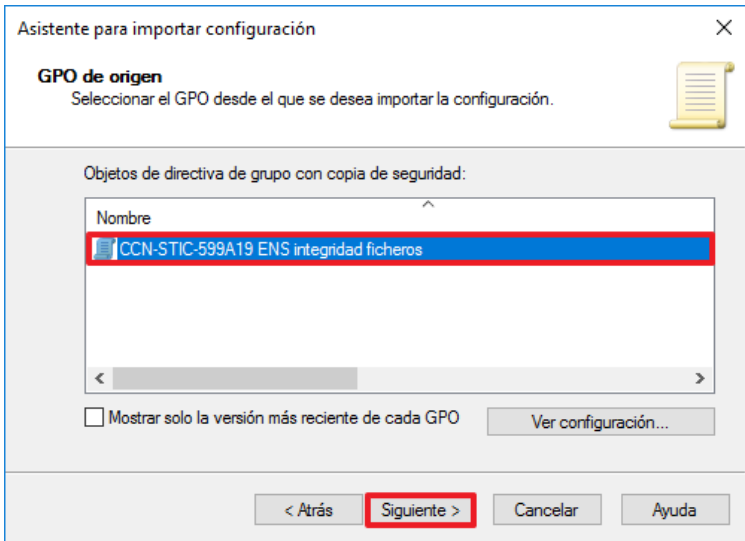
7.3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

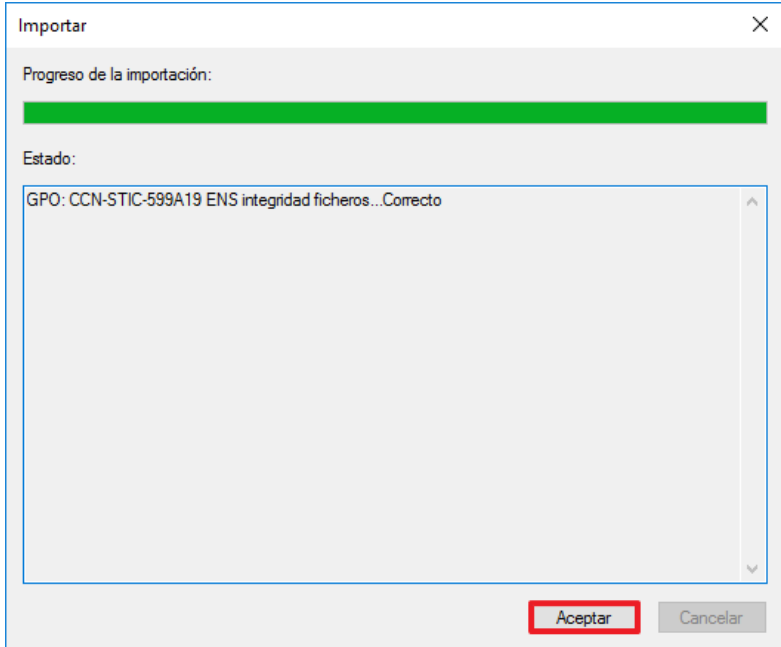
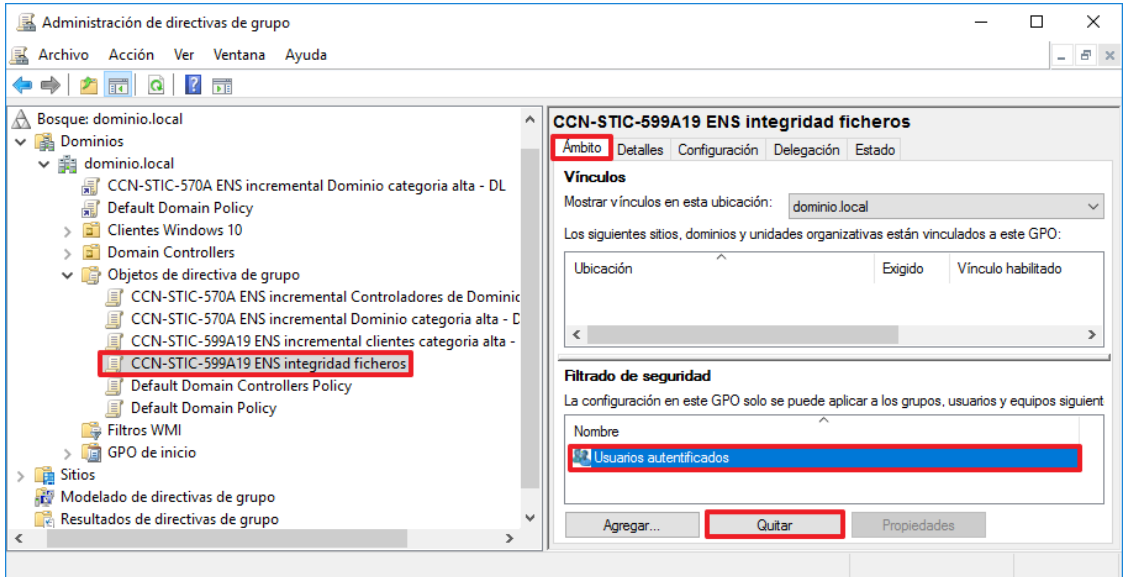
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

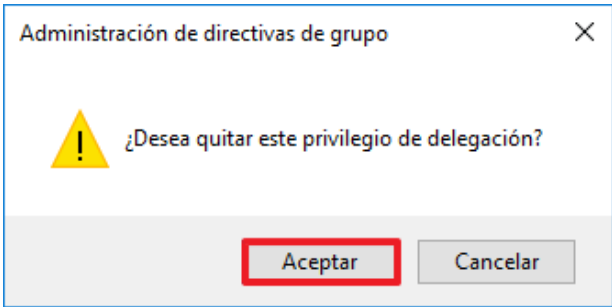
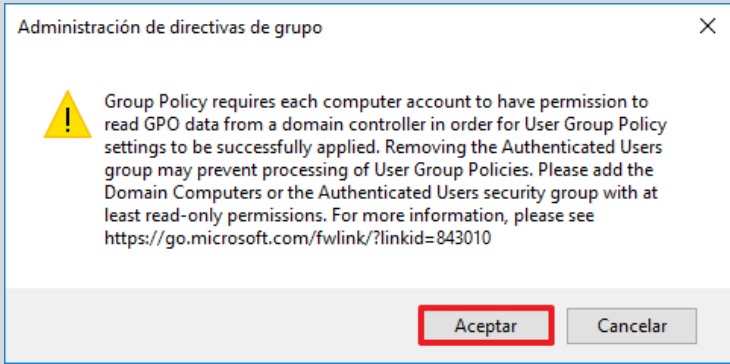
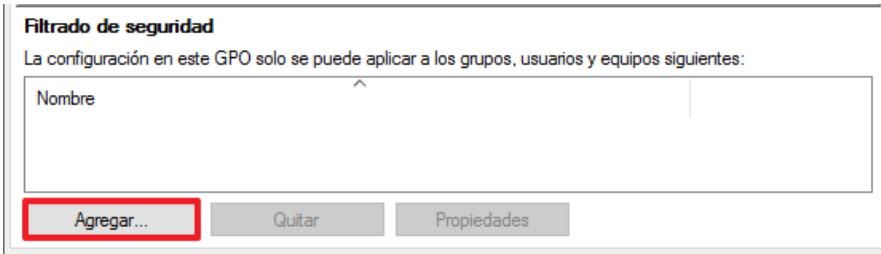
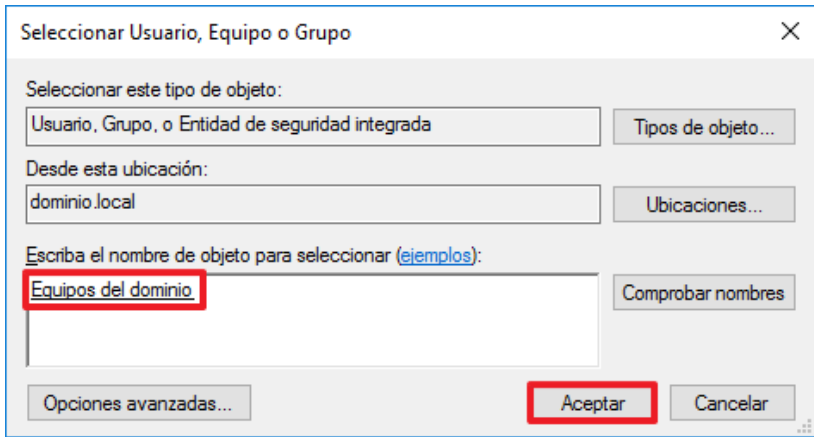
Paso	Descripción
14.	Inicie sesión en el servidor controlador de dominio al que pertenecen los equipos cliente que van a asegurar, con una cuenta con derechos de administración en el dominio.
15.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.

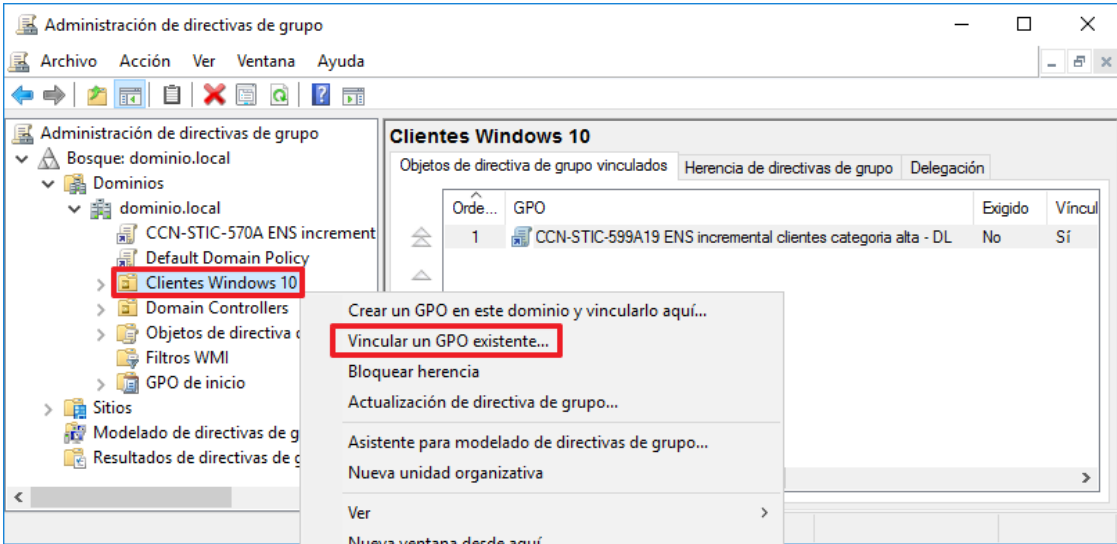
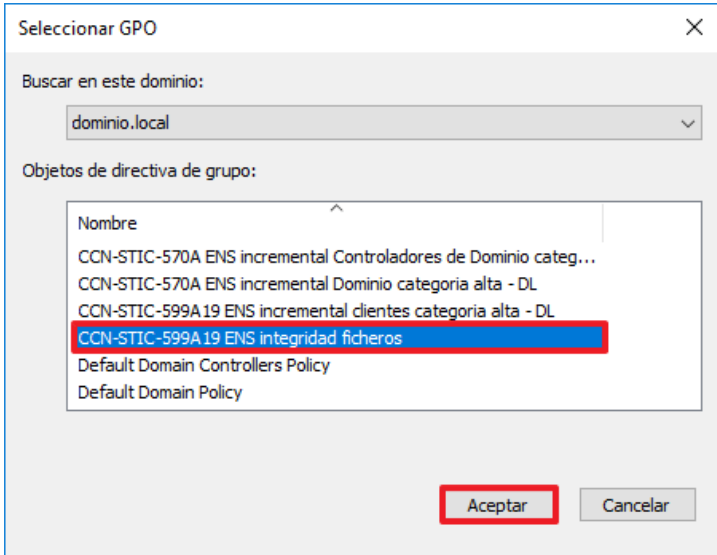
Paso	Descripción
16.	Inicie el “Administrador del servidor” desde el icono correspondiente en el menú de inicio. 
17.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Administración de directivas de grupo”. 
18.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
19.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" y, marcando con el botón derecho sobre él, elija la opción "Nuevo" del menú contextual que aparecerá. 

Paso	Descripción
20.	Asigne el siguiente nombre "CCN-STIC-599A19 integridad ficheros" a la nueva GPO y pulse "Aceptar". 
21.	Seleccione la GPO recién creada, "CCN-STIC-599A19 integridad ficheros" con el botón derecho y pulse sobre la opción "Importar configuración..." en el menú contextual que aparecerá. 
22.	En el "Asistente para importar configuración" pulse "Siguiente >".
23.	En apartado "Hacer copia de seguridad de GPO" pulse de nuevo "Siguiente >".
24.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 

Paso	Descripción
25.	Localice la carpeta “CCN-STIC-599A19 ENS Integridad Ficheros” en el directorio “C:\Scripts” y pulse “Aceptar”. 
26.	Pulse “Siguiente >” para continuar. 
27.	En “GPO de origen” pulse “Siguiente >”. 

Paso	Descripción
28.	En el apartado “Examinar copia de seguridad” pulse “Siguiente >”.
29.	Pulse “Finalizar” para terminar de importar la copia de seguridad.
30.	Pulse “Aceptar” para continuar. 
31.	Seleccione la nueva política de grupo configurada y vaya a las opciones de ámbito que se encuentran en el panel derecho. Seleccione el grupo “Usuarios autenticados” y pulse sobre el botón “Quitar”. 

Paso	Descripción
32.	Pulse el botón “Aceptar” ante el mensaje de advertencia “¿Desea quitar este privilegio de delegación?”.  Nota: En caso de aparecer la siguiente advertencia pulse de nuevo sobre “Aceptar”. 
33.	Pulse ahora sobre el botón “Agregar...”. 
34.	Introduzca como nombre “Equipos del dominio”. A continuación, pulse el botón “Aceptar”. 

Paso	Descripción
35.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
36.	Seleccione “CCN-STIC-599A19 integridad ficheros” de la lista y pulse “Aceptar”. 
37.	Elimine el directorio “C:\Scripts”.

ANEXO D. CONFIGURACIÓN SEGURA DE MICROSOFT WINDOWS 10 PRO/ENTERPRISE EN REDES CLASIFICADAS COMO CLIENTE MIEMBRO DE DOMINIO

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 anexo 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 (versión 1809) sin opción de mantenimiento LTSC 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-599A19” 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 (versión contemplada en este anexo) en su versión 1809 sin opción de mantenimiento LTSC. 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 mediante GPO. En el anexo para la versión Pro/Enterprise, además de la configuración descrita anteriormente, se limita por la aplicación de la presente guía.

- 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 sin opción de mantenimiento LTSC 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.

Internet Explorer 11 será securizado según los mecanismos definidos en la guía CCN-STIC-520, tal y como se indicará en el correspondiente paso a paso. Las políticas y configuraciones de dicha guía se aplican junto con las de la presente durante los pasos que aseguran el equipo cliente Microsoft Windows 10.

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.

ANEXO D.1. IMPLEMENTACIÓN SEGURA DE WINDOWS 10 PRO/ENTERPRISE COMO CLIENTE MIEMBRO DE DOMINIO

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 (versión 1809) sin opción de mantenimiento LTSC miembro de un dominio de Windows.

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.2.1 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.
- j) Deberá disponer de la guía CCN-STIC-520 – INTERNET EXPLORER 11 para aplicarla durante los pasos finales de la presente sección.

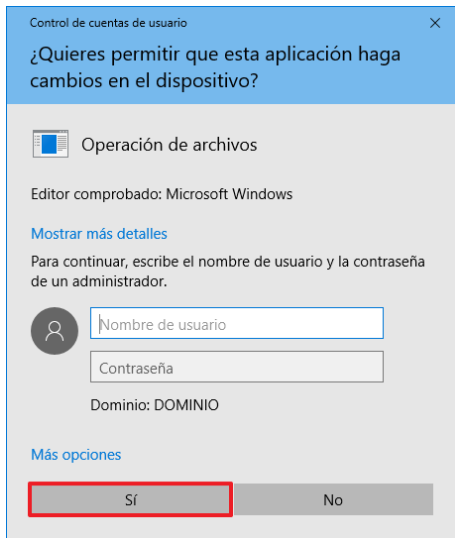
El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación. No se proporciona un fichero de respuestas automáticas, como se hacía en otras guías para versiones anteriores de Windows, porque la instalación por defecto de Microsoft 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.

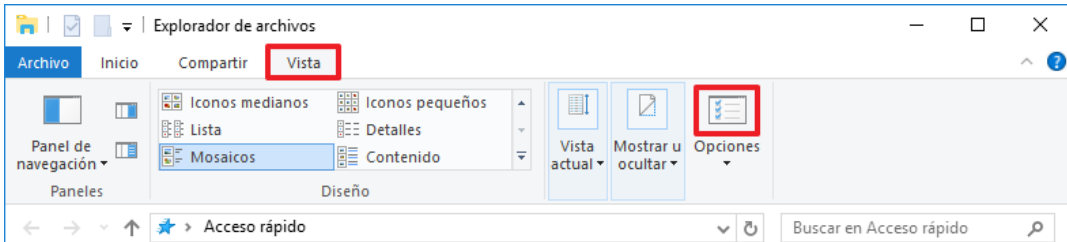
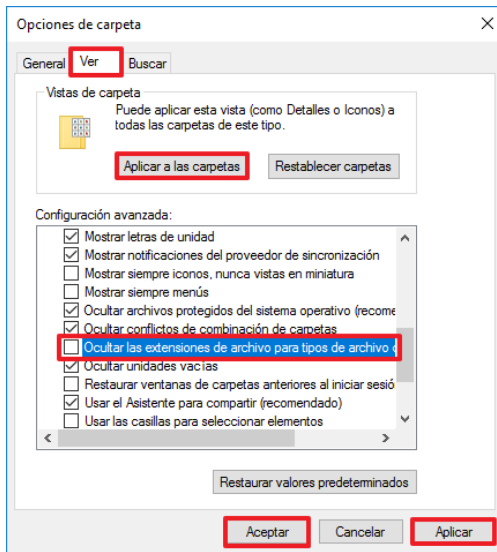
1. PREPARACIÓN DEL DOMINIO

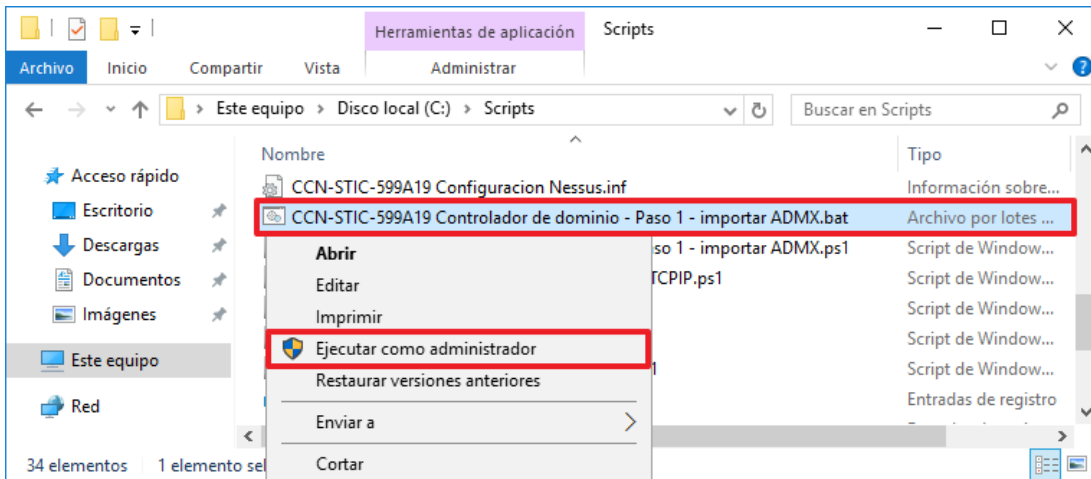
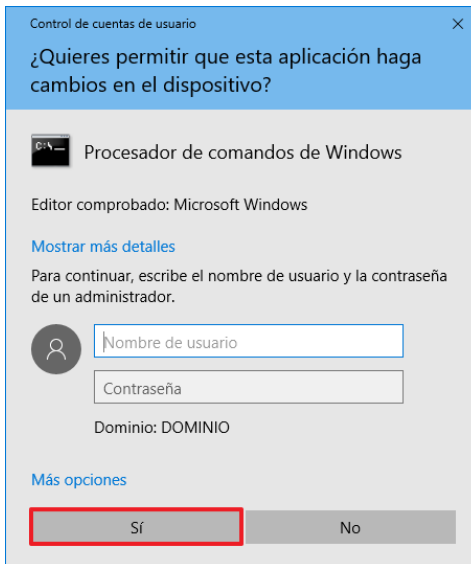
Los pasos que se describen a continuación deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer cliente Windows 10 miembro de dominio, ya que crear las unidades organizativas e incorporar las configuraciones recomendadas en esta guía en objetos de directiva de grupo, sólo es necesario realizarlo una única vez.

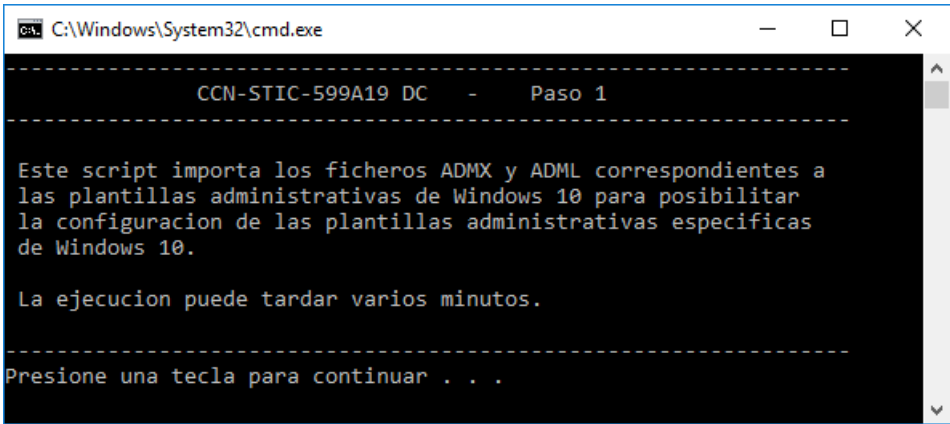
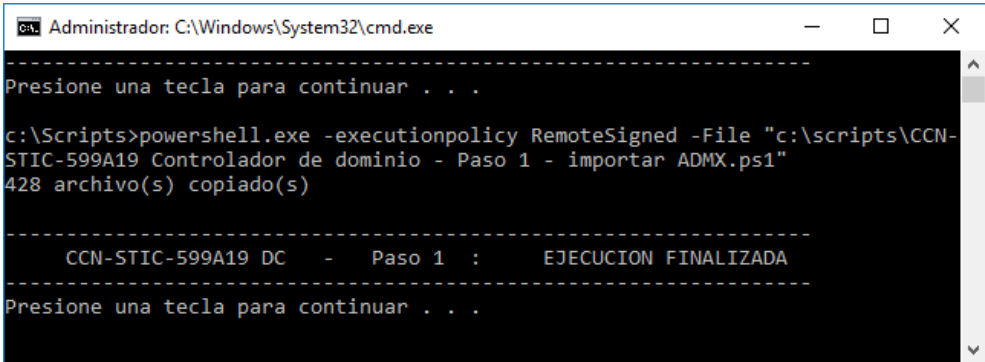
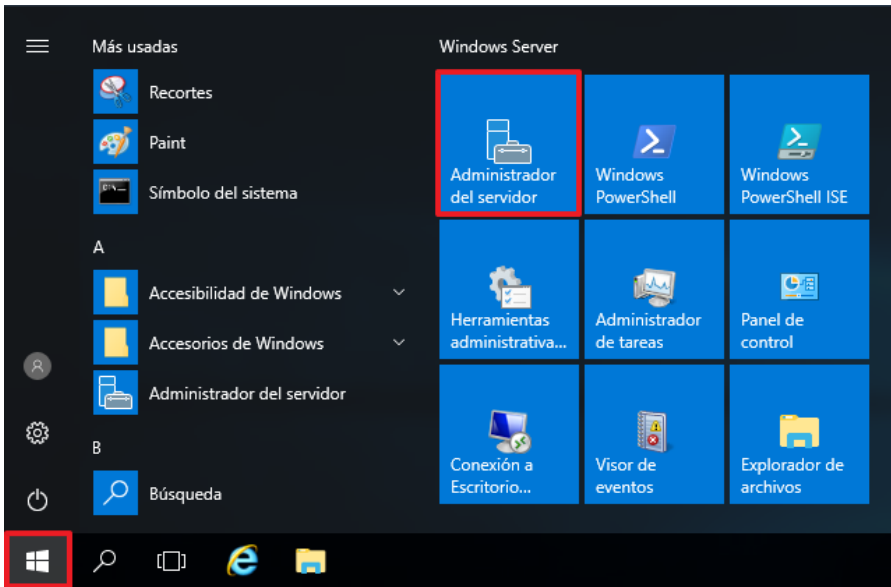
Para el resto de clientes Windows 10 miembros del mismo dominio deberá saltar estos pasos e ir directamente al paso 85, ya que esos clientes compartirán la configuración establecida en este punto y, de forma automática, recibirán las configuraciones de dominio y las relativas a la Unidad Organizativa "Clientes Windows 10 - Equipos".

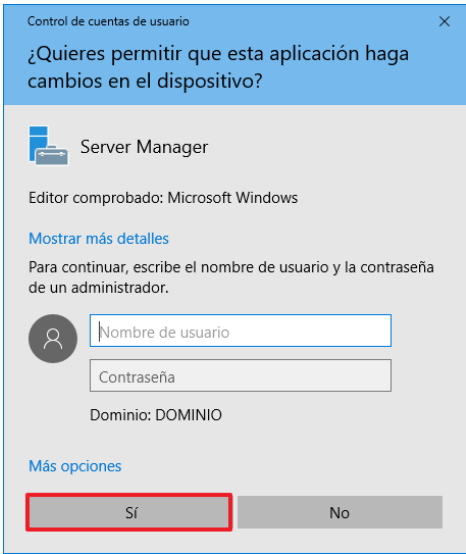
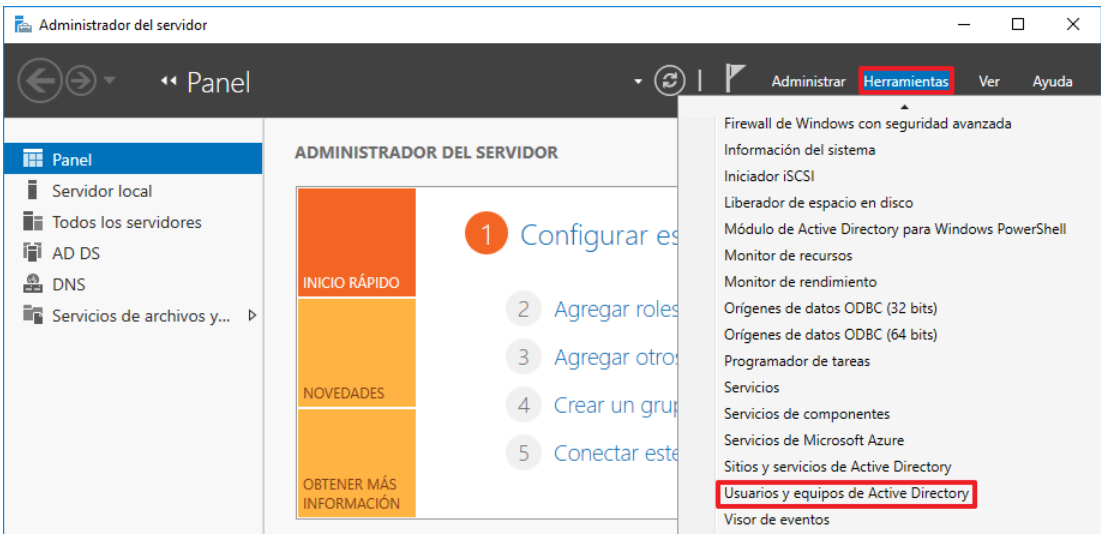
Nota: Esta guía asume que a los servidores controladores del dominio al que va a pertenecer el equipo cliente que está asegurando, se les ha aplicado la configuración descrita en la guía “CCN-STIC-570A WINDOWS SERVER 2016 CONTROLADOR DE DOMINIO”. Si no es así, aplique la guía correspondiente a los controladores de dominio, antes de continuar con la aplicación de ésta.

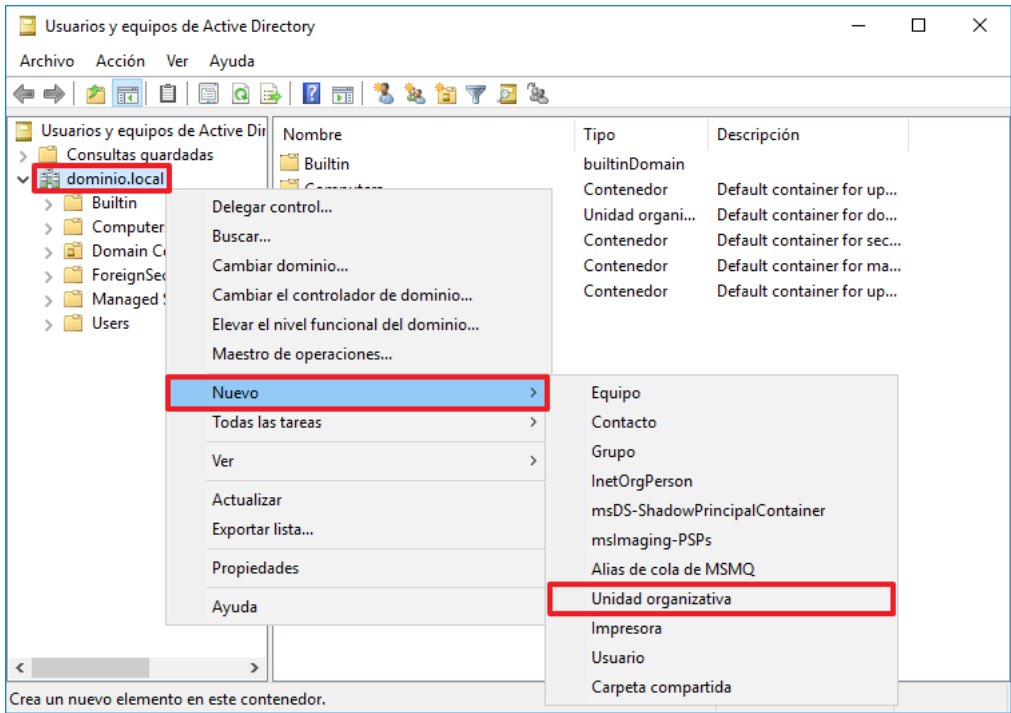
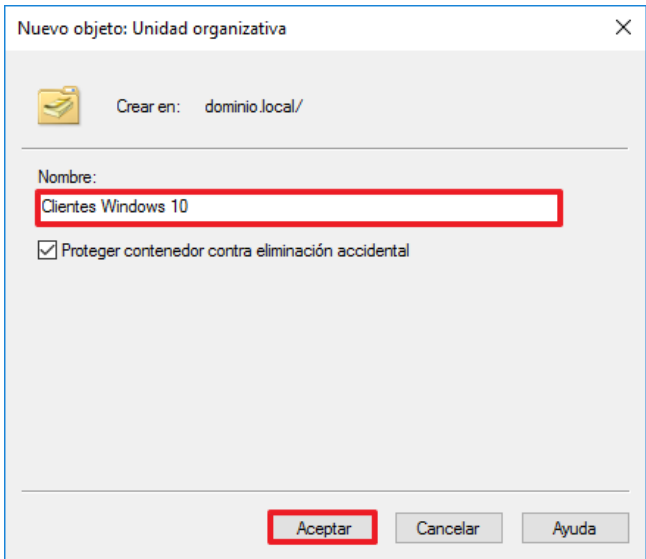
Paso	Descripción
1.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. El sistema le solicitará elevación de privilegios, introduzca las credenciales de un usuario con permisos de administrador. 

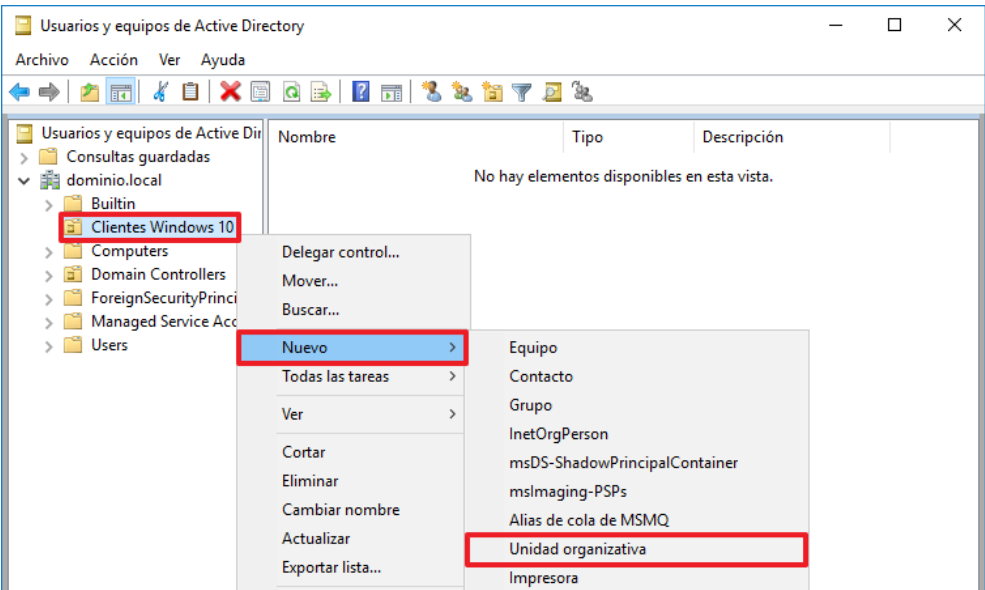
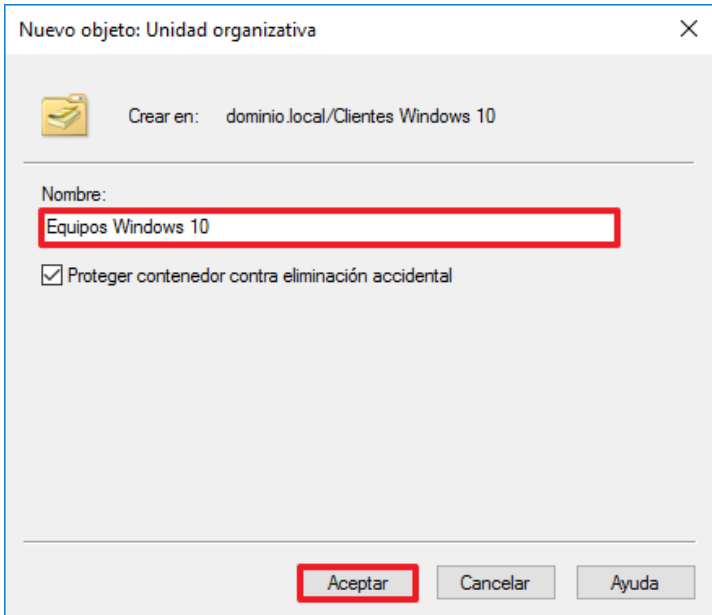
Paso	Descripción
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio. El sistema le solicitará elevación de privilegios. Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". Los scripts asumen que su 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.	Asegúrese de que al menos los siguientes directorios y ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-599A19 Windows 10 - Equipos (directorio) – CCN-STIC-599A19 Windows 10 - Usuarios (directorio) – CCN-STIC-599A19 Cliente Miembro.inf – CCN-STIC-599A19 Cliente Miembro.wfw – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.bat – CCN-STIC-599A19 Controlador de dominio – Paso 1 – importar ADMX.ps1
5.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 
6.	En "Opciones de carpeta" sitúese en la pestaña "Ver" y en el campo "Configuración avanzada" localice y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos". Pulse primero sobre el botón "Aplicar", después sobre "Aplicar a las carpetas" (Pulse "Sí" ante el mensaje de confirmación) y, por último, pulse "Aceptar". 

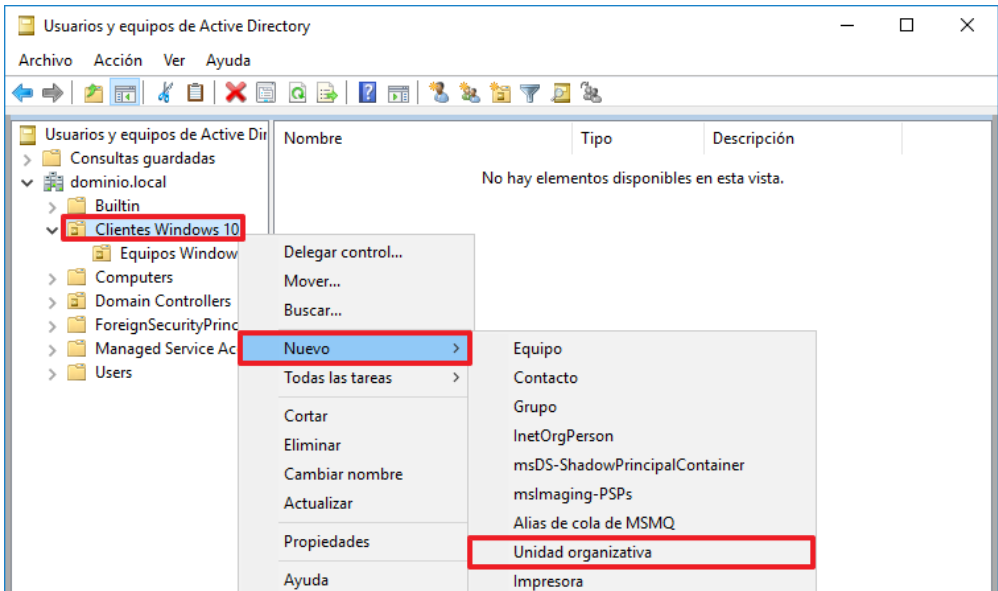
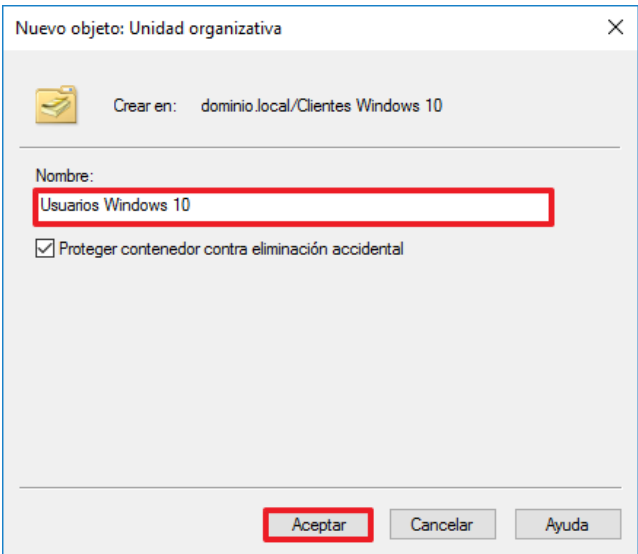
Paso	Descripción
7.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Controlador de dominio - Paso 1 – importar ADMX.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
8.	El sistema solicitará elevación de privilegios. Introduzca las credenciales de una cuenta con permisos de administración de dominio y administración de esquema. 

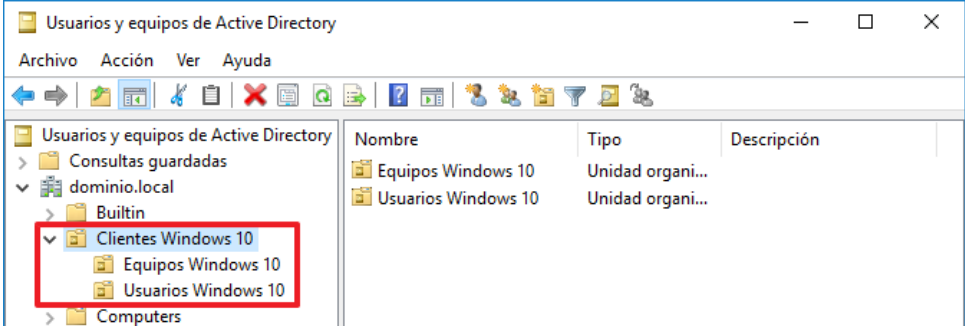
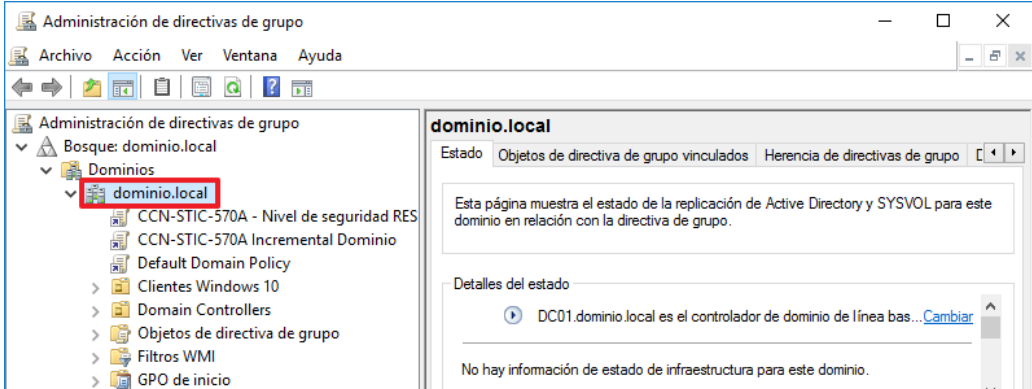
Paso	Descripción
9.	Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Windows 10 en el controlador de dominio.  Nota: La ejecución puede durar bastante tiempo, no cierre la ventana hasta que finalice el proceso.
10.	Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana. 
11.	Cree la unidad organizativa "Clientes Windows 10". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

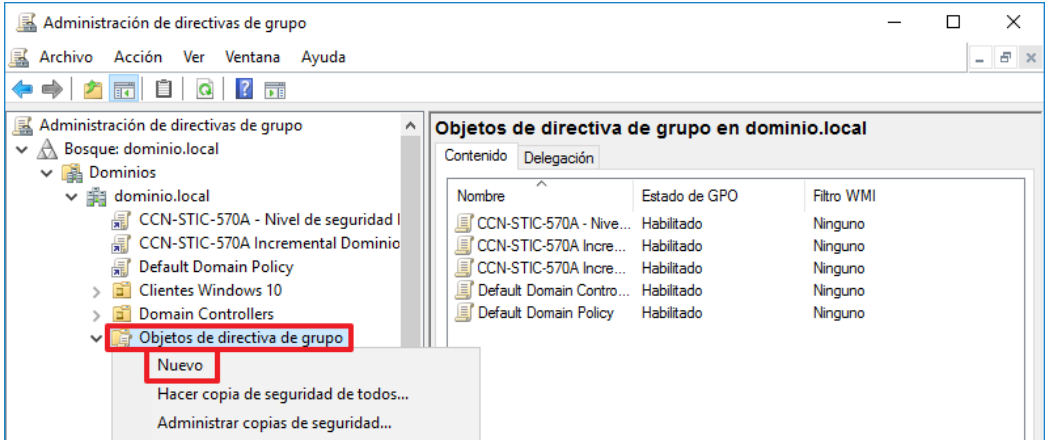
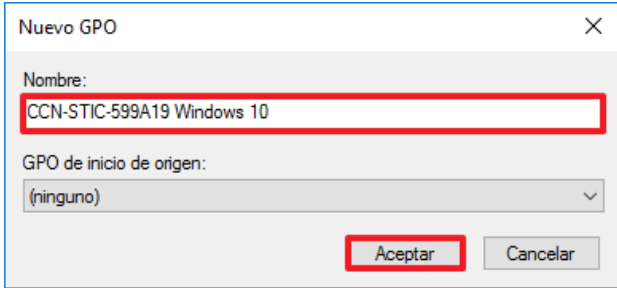
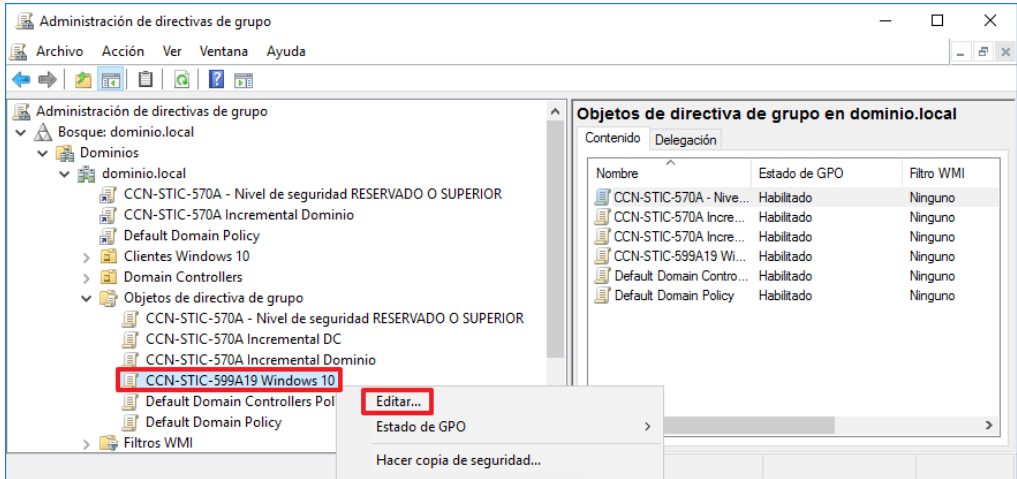
Paso	Descripción
12.	El sistema le solicitará elevación de privilegios. Introduzca las credenciales de un administrador del dominio. 
13.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Usuarios y equipos de Active Directory”. 

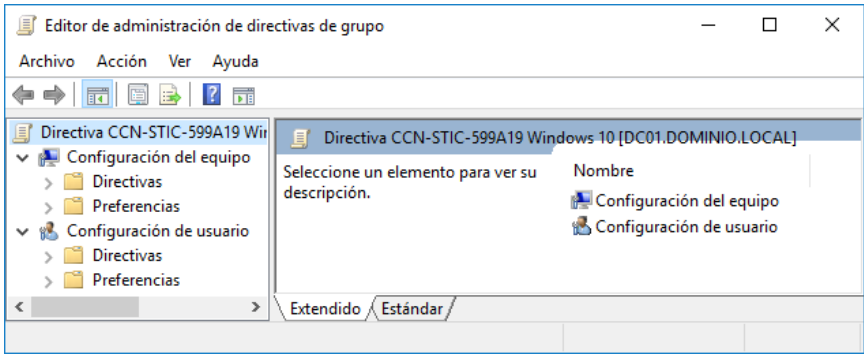
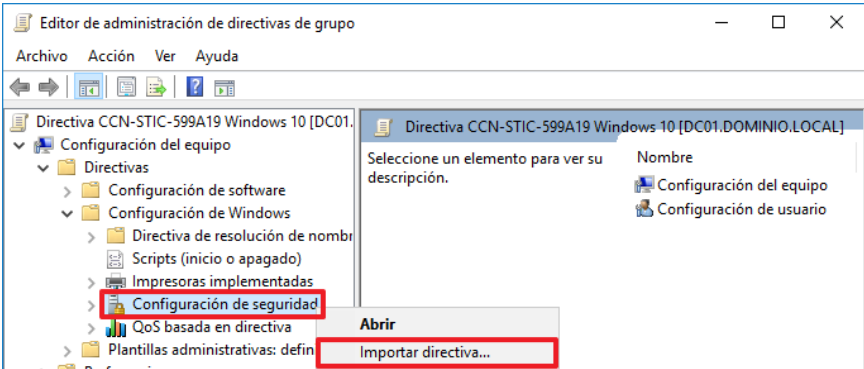
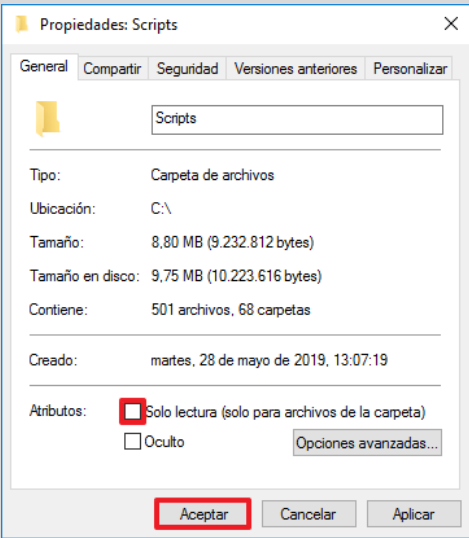
Paso	Descripción
14.	En la consola “Usuarios y equipos de Active Directory” sitúese sobre el objeto con el nombre del dominio y, pulsando con el botón derecho del ratón sobre él, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá, como se muestra en la siguiente figura.  Nota: En el ejemplo, el dominio se denomina “dominio.local”.
15.	Asigne el nombre "Clientes Windows 10" a la nueva unidad organizativa, y deje marcada la opción "Proteger contenedor contra eliminación accidental". A continuación, pulse “Aceptar”. 

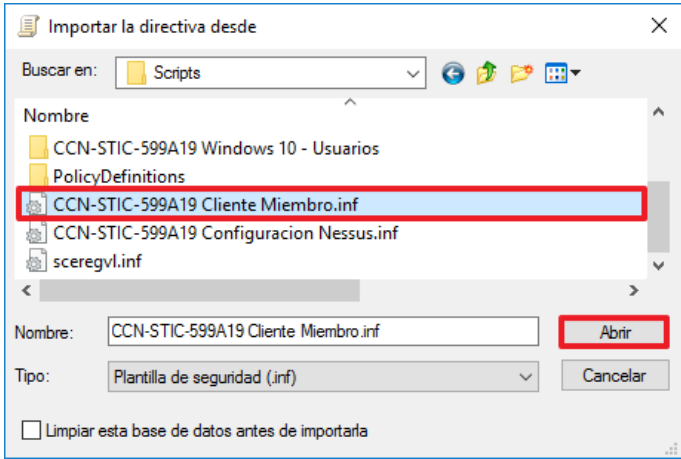
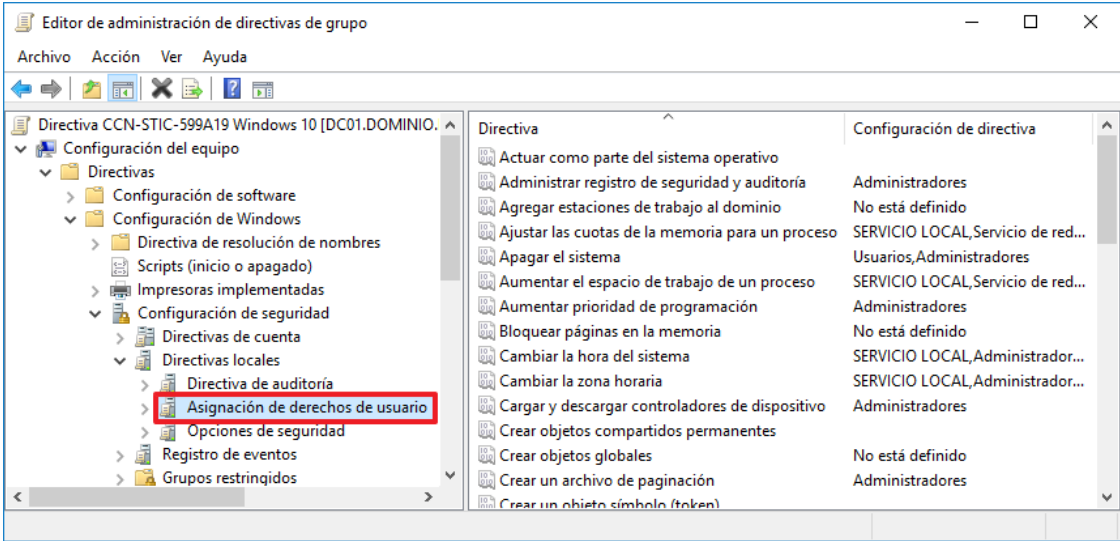
Paso	Descripción
16.	A continuación, cree las unidades organizativas "Equipos Windows 10" y "Usuarios Windows 10" colgando de la unidad organizativa que acaba de crear en el paso anterior, "Clientes Windows 10". Para ello, y utilizando de nuevo la herramienta "Usuarios y equipos de Active Directory", expanda y seleccione el siguiente contenedor: "<Nombre de su dominio> → Clientes Windows 10" Marcándolo con el botón derecho del ratón, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá. 
17.	Asigne el nombre "Equipos Windows 10", mantenga marcado "Proteger contenedor contra eliminación accidental" y pulse "Aceptar". 

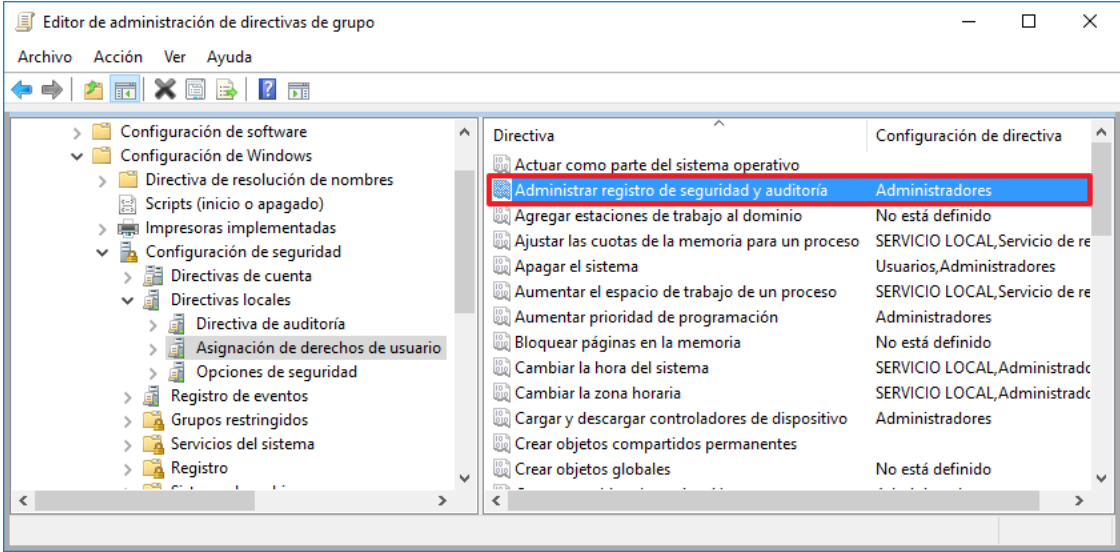
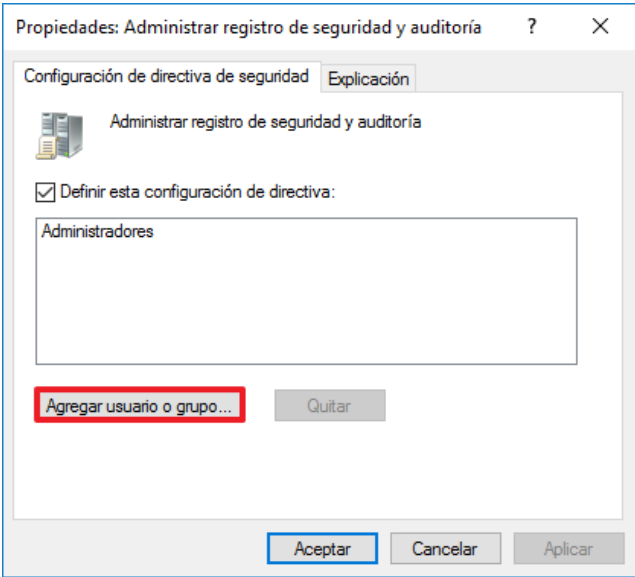
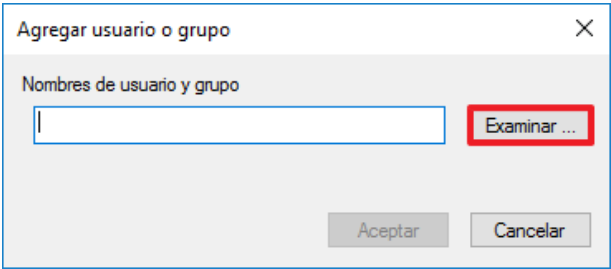
Paso	Descripción
18.	Del mismo modo, vuelva a seleccionar el contenedor “Clientes Windows 10” a través de la ruta “<Nombre de su dominio> → Clientes Windows 10”. Marcándolo con el botón derecho del ratón, seleccione la opción “Nuevo → Unidad organizativa” del menú contextual. 
19.	Asigne el nombre “Usuarios Windows 10” y pulse “Aceptar”. 

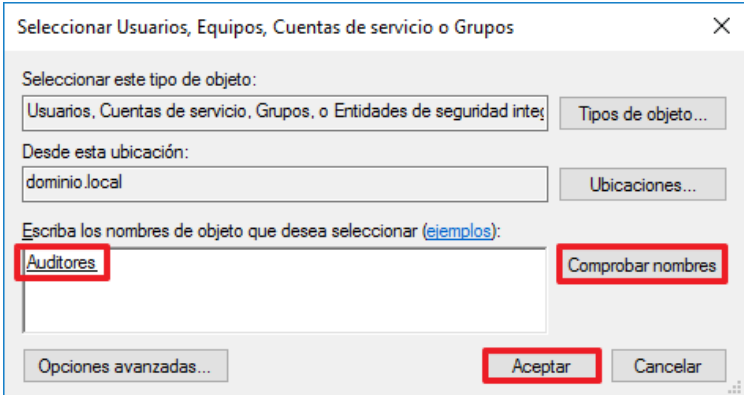
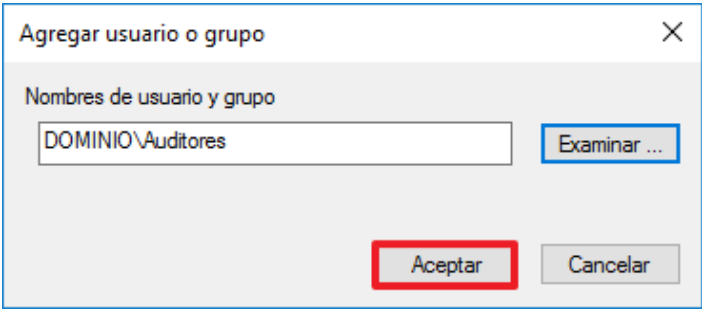
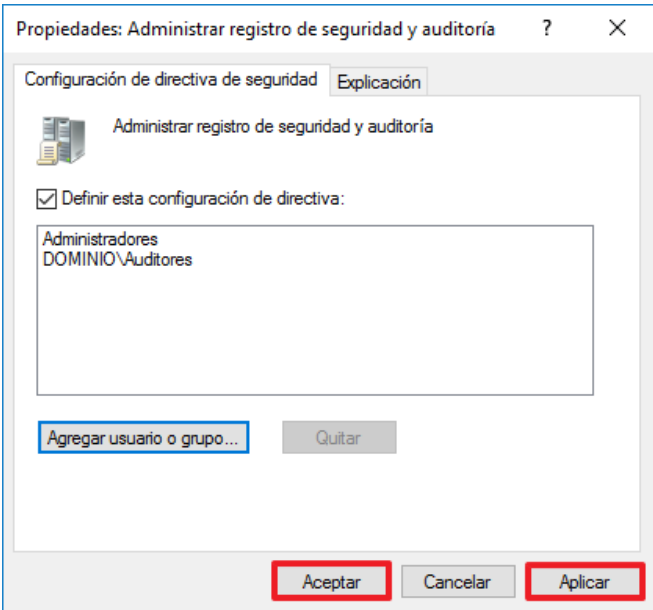
Paso	Descripción
20.	Al finalizar, las nuevas unidades organizativas, "Equipos Windows 10" y "Usuarios Windows 10", aparecerán colgando de "Clientes Windows 10", como se muestra en la siguiente figura.  Nota: Es importante, sobre todo en entornos en que haya clientes Windows 10 con la versión 1607 contemplada en la guía "CCN-STIC-599A18" conviviendo con los clientes Windows 10 con la versión 1809 contemplada en la presente guía, que se diferencien los equipos y usuarios de cada sistema.
21.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.
22.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Administración de directivas de grupo". 
23.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la ruta "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>". A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPO correspondientes. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>). 

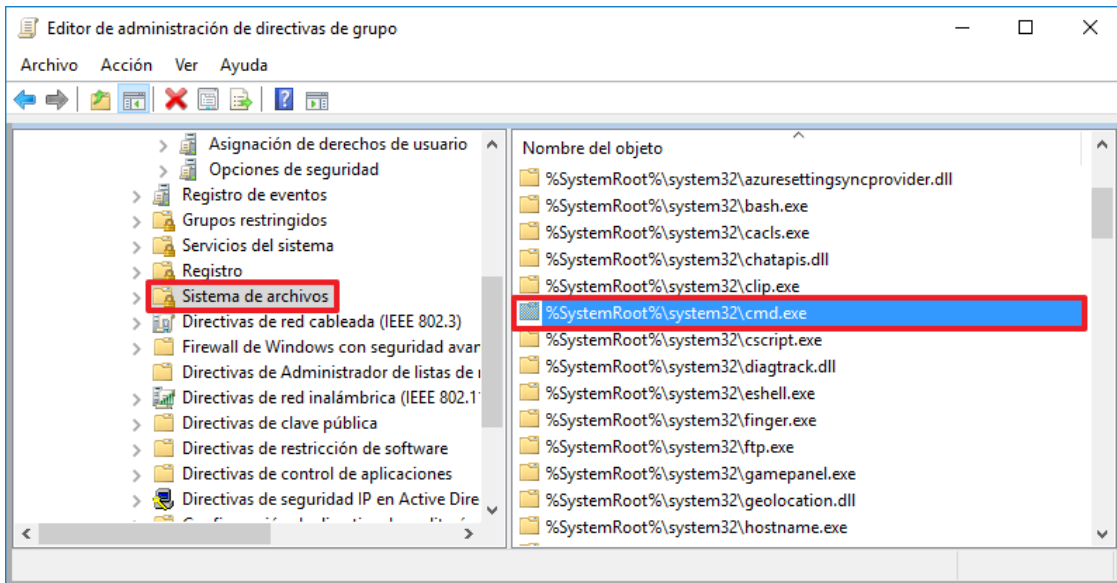
Paso	Descripción
24.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" y, marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá.  Nota: Las GPO que se van a crear y parametrizar en los siguientes pasos deberán vincularse a las unidades organizativas correspondientes a Windows 10 versión 1809 contempladas en la presente guía. Es importante no mezclar equipos, usuarios o GPO de Windows 10 1809 con equipos, usuarios o GPO de Windows 10 1607 (a los cuales les debe aplicar la guía CCN-STIC-599A18, y no la presente guía).
25.	Asigne el siguiente nombre "CCN-STIC-599A19 Windows 10" a la nueva GPO y pulse "Aceptar". 
26.	Seleccione la GPO recién creada, "CCN-STIC-599A19 Windows 10" con el botón derecho y elija la opción "Editar" en el menú contextual que aparecerá. 

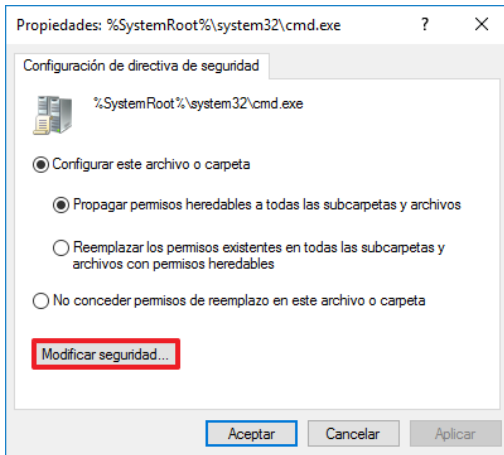
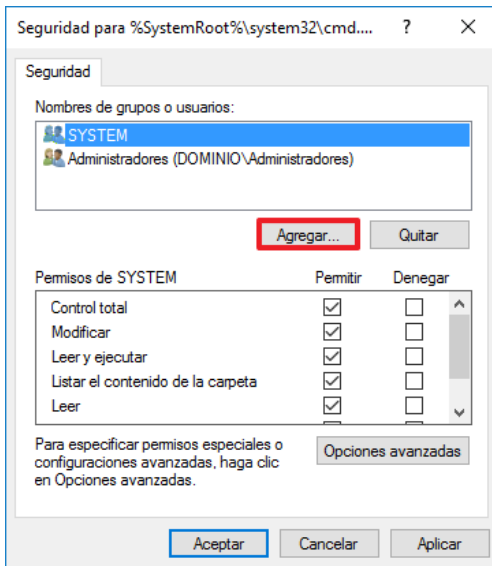
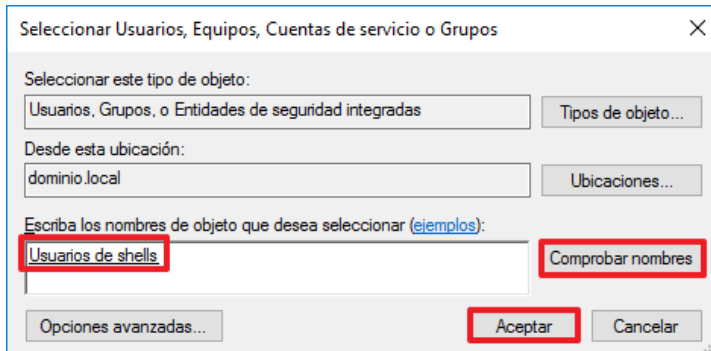
Paso	Descripción
27.	Con ello se abrirá una ventana del editor de administración de directivas de grupo, en la cual se podrá editar el contenido de la GPO. 
28.	En dicha ventana del editor de administración de directivas de grupo, seleccione el nodo "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad". Marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá.  Nota: Asegúrese de que los archivos alojados en "C:\Scripts" no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

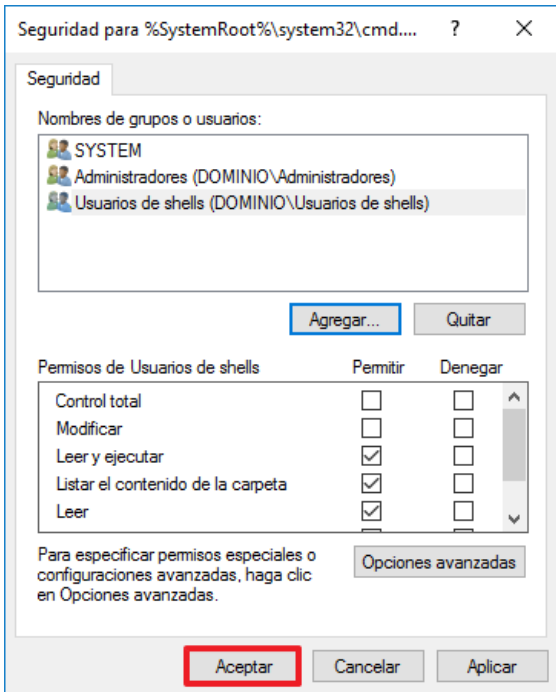
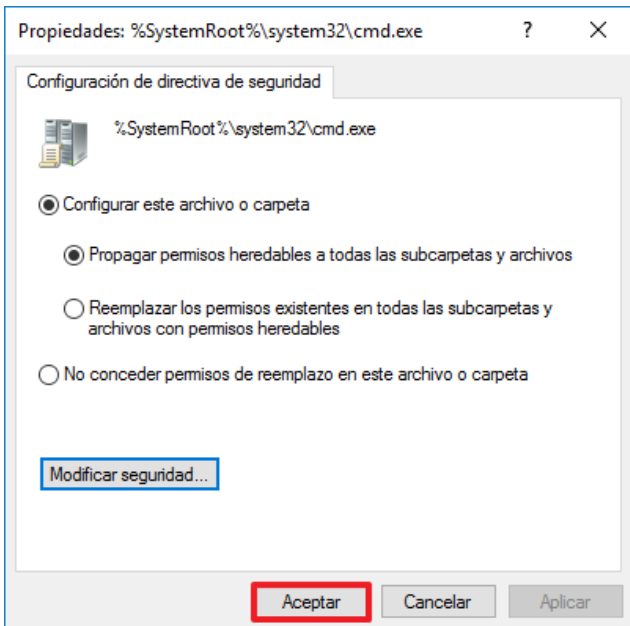
Paso	Descripción
29.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Scripts\CCN-STIC-599A19 Cliente Miembro.inf" y pulse el botón "Abrir". Con eso habrá quedado importada la plantilla en la GPO. No cierre aún el "Editor de directivas de grupo" y continúe con el siguiente paso. 
30.	Utilizando de nuevo el "Editor de administración de directivas de grupo", abierto anteriormente, seleccione "Asignación de derechos de usuarios" a través de la siguiente ruta: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario" 

Paso	Descripción
31.	Haga doble clic sobre la directiva “Administrar registro de seguridad y auditoría”. 
32.	Pulse sobre “Agregar usuario o grupo...” en la ventana emergente. 
33.	Pulse sobre “Examinar”. 

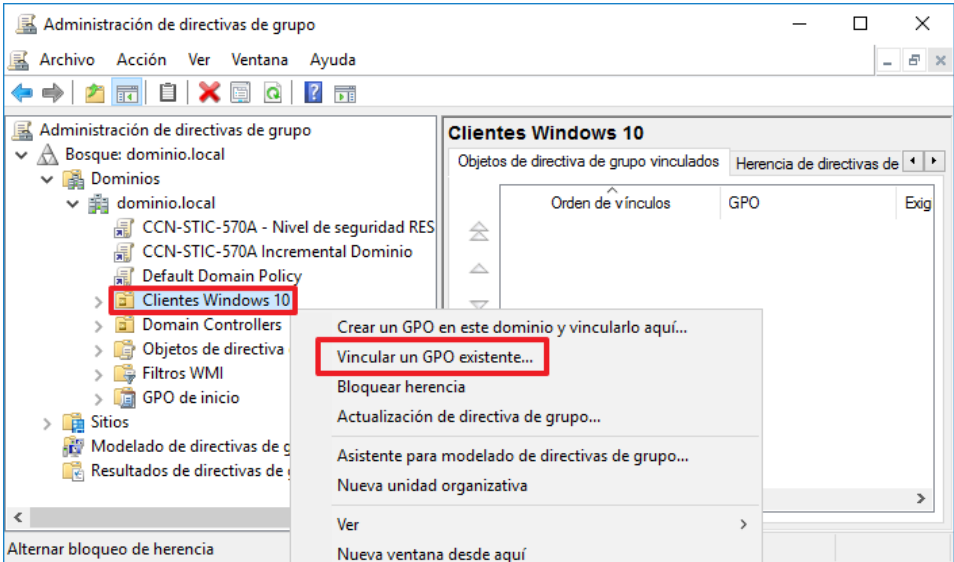
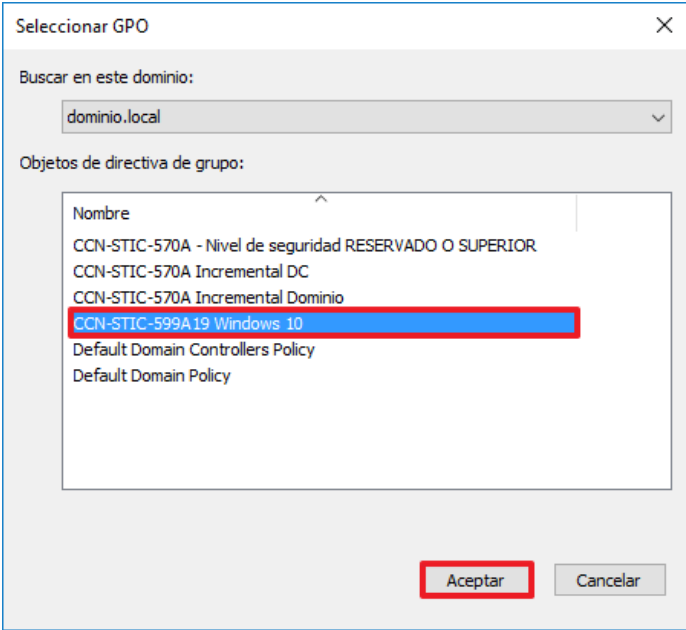
Paso	Descripción
34.	Introduzca el grupo de seguridad “Auditores”, pulse en “Comprobar nombre” y “Aceptar”.  Nota: El grupo "Auditores" ya debe existir en el dominio si se aplicó correctamente la guía CCN-STIC-570A a los controladores de dominio. Si no existe, revise la aplicación de dicha guía. Recuerde también que la cuenta Administrador (administrador integrado del dominio) puede haber sido renombrada por la aplicación de dicha guía.
35.	Pulse “Aceptar”. 
36.	Por último, pulse “Aplicar” y “Aceptar” para confirmar los cambios. 

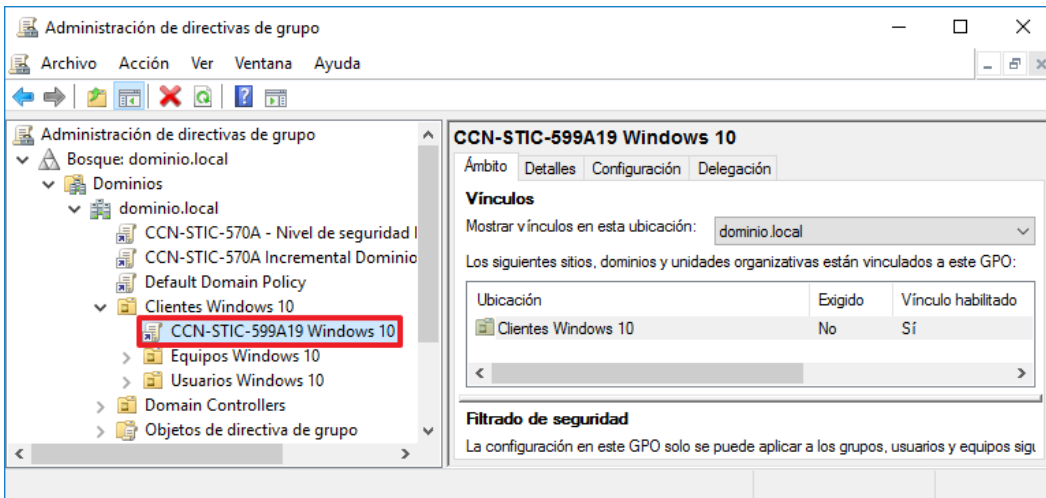
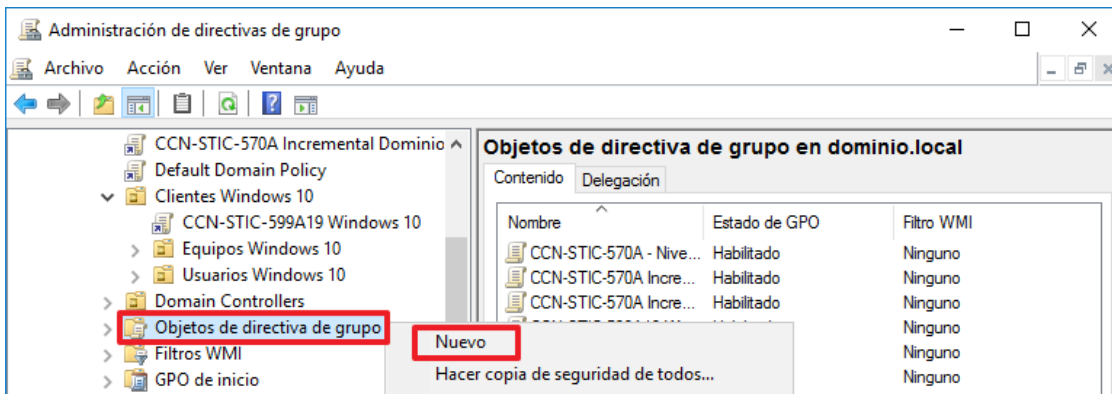
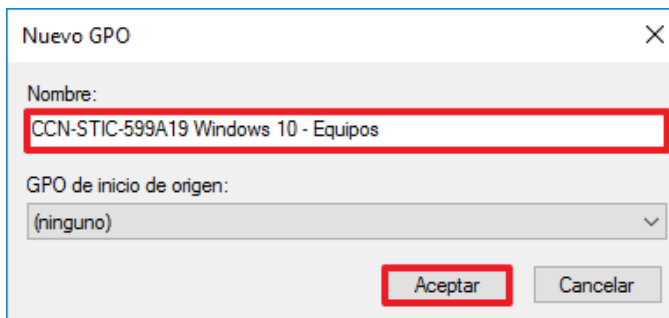
Paso	Descripción									
37.	Repita el proceso con los valores indicados en la siguiente tabla. Concretamente, deberá añadir los usuarios y grupos de seguridad marcados en gris. <table><tr><th>Directiva</th><th>Valor</th><th>Descripción</th></tr><tr><td>Administrar registro de seguridad y auditoría</td><td>Auditores, Administradores</td><td>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.</td></tr><tr><td>Denegar el acceso a este equipo desde la red</td><td>Invitados, ANONYMOUS LOGON, Administrador</td><td>Este permiso determina a qué usuarios se les impide acceder a un ordenador desde la red</td></tr></table>	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
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								
38.	De manera análoga a lo realizado en el paso anterior, despliegue el nodo “Sistema de archivos” mediante la ruta “Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos”.									
39.	Haga doble clic sobre el objeto “%SystemRoot%\system32\cmd.exe”. 									

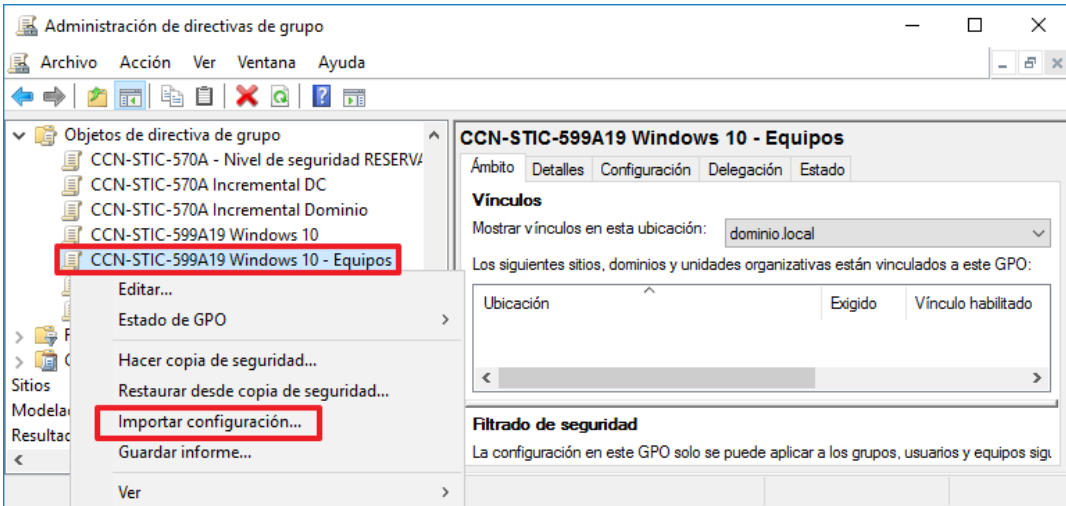
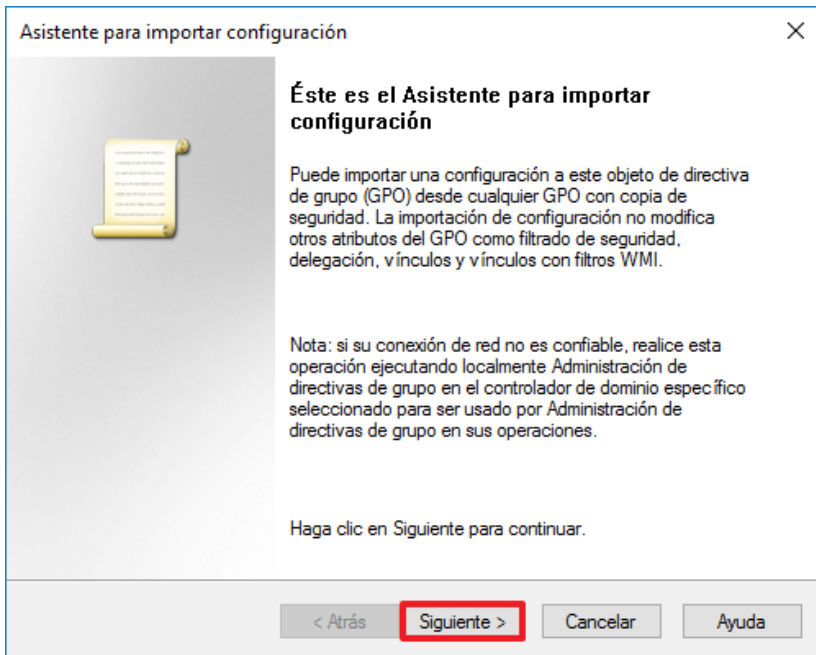
Paso	Descripción
40.	Pulse en “Modificar seguridad...”. 
41.	Pulse “Agregar...” para añadir el grupo de seguridad que tendrá permisos para ejecutar la consola de comandos. 
42.	Introduzca el grupo de seguridad “Usuarios de shells”, pulse “Comprobar nombre” y “Aceptar”.  Nota: El grupo "Usuarios de shells" ya debe existir en el dominio si se aplicó correctamente la guía CCN-STIC-570A al controlador de dominio. Si no existe, revise la aplicación de dicha guía.

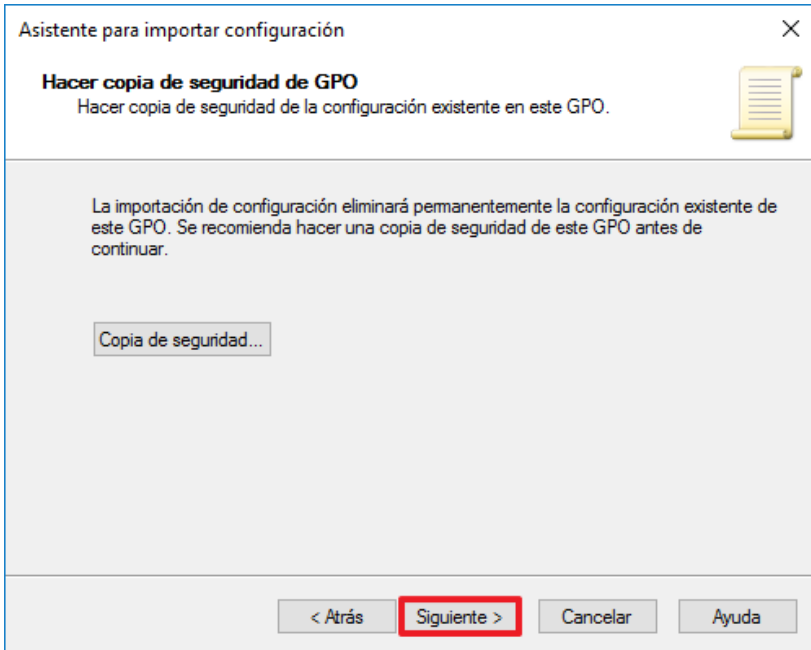
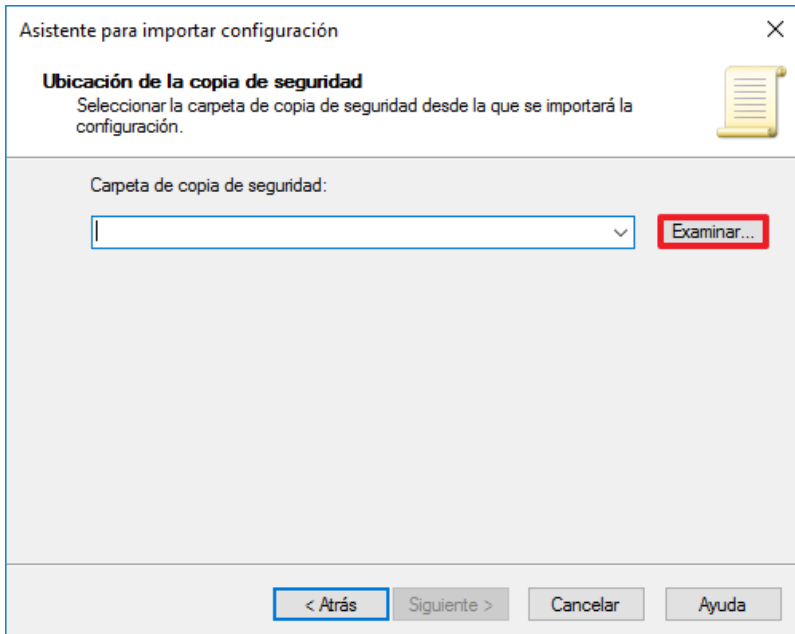
Paso	Descripción
43.	Pulse “Aceptar” sin modificar los permisos asignados por defecto. 
44.	Pulse nuevamente en “Aceptar” para confirmar cambios. 

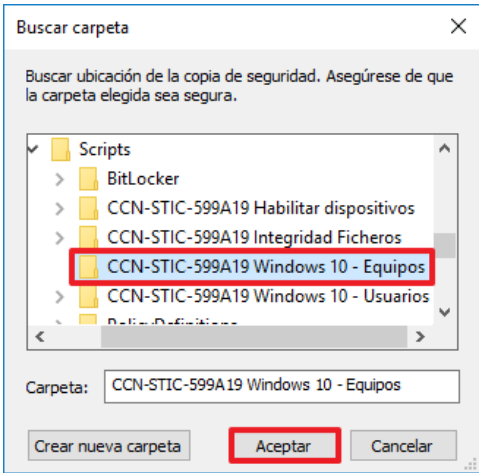
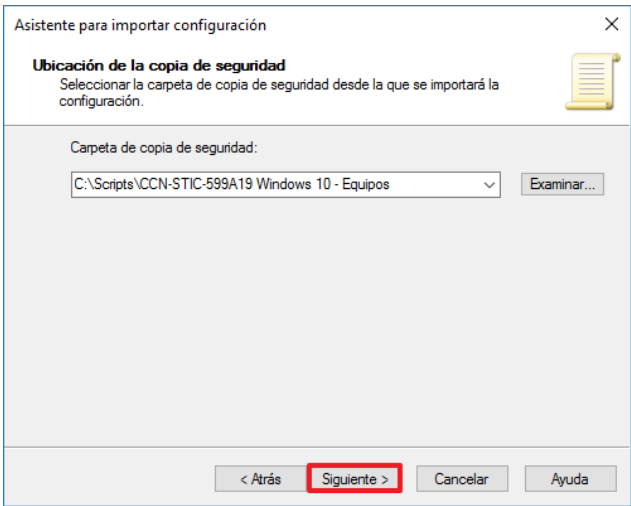
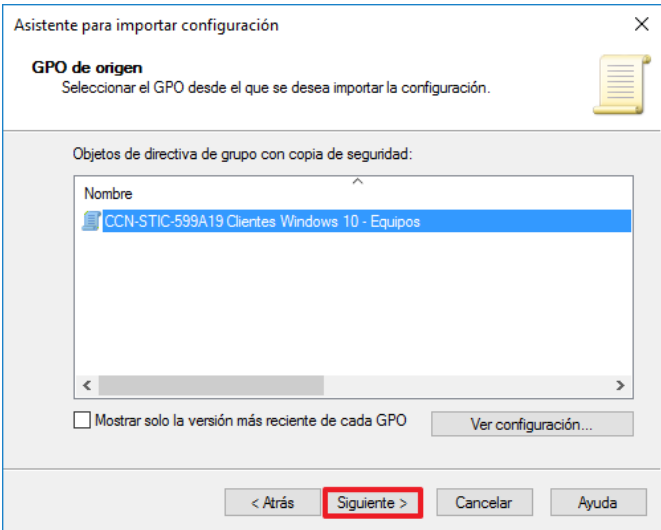
Paso	Descripción		
45.	Repita el proceso con los valores indicados en la siguiente tabla. Concretamente, deberá añadir los usuarios y grupos de seguridad marcados en gris.		
	Archivo o carpeta	Usuarios/Grupos	Permisos
	%SystemRoot%\system32\ cmd.exe	Administradores	Control Total
		SYSTEM	Control Total
		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
	%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
46.	A continuación, cierre el “Editor de administración de directivas de grupo”.		

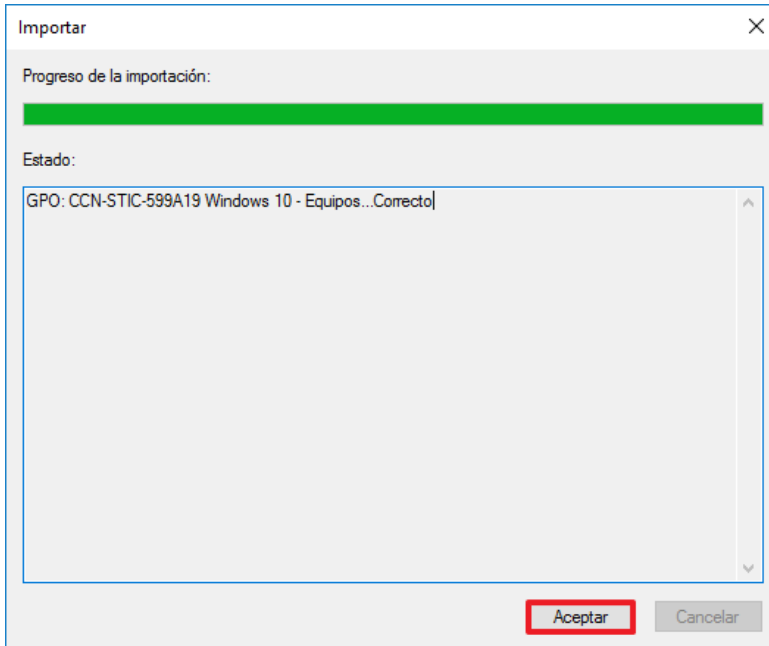
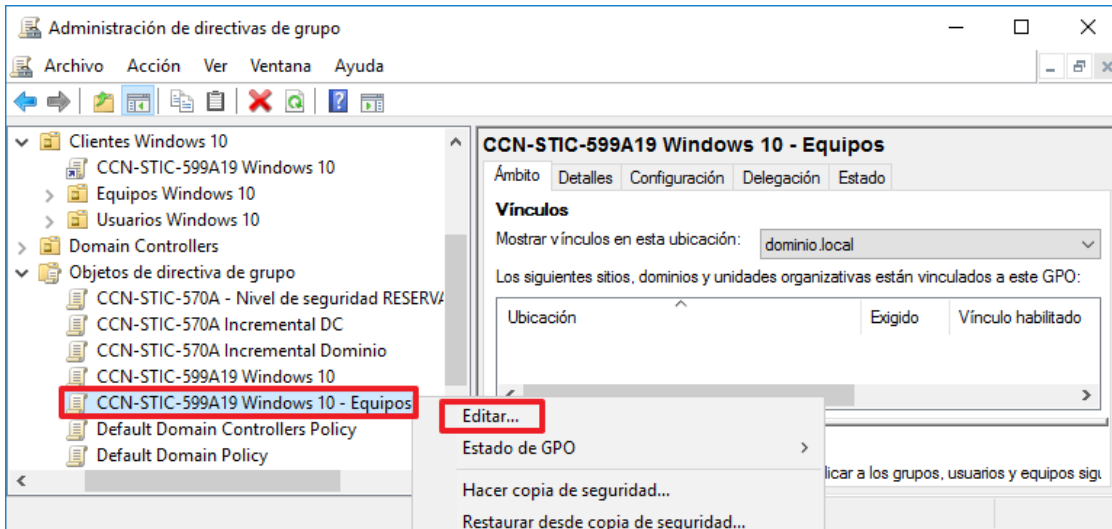
Paso	Descripción
47.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Clientes Windows 10” a través de la ruta “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10”. Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
48.	Seleccione “CCN-STIC-599A19 Windows 10” de la lista y pulse “Aceptar”. 

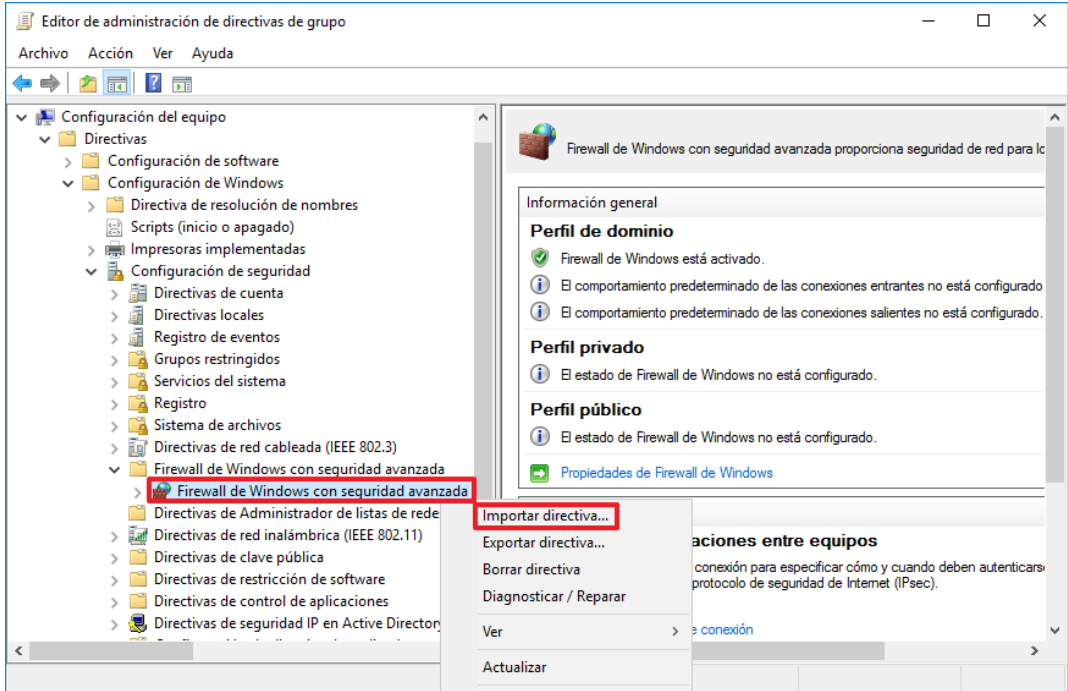
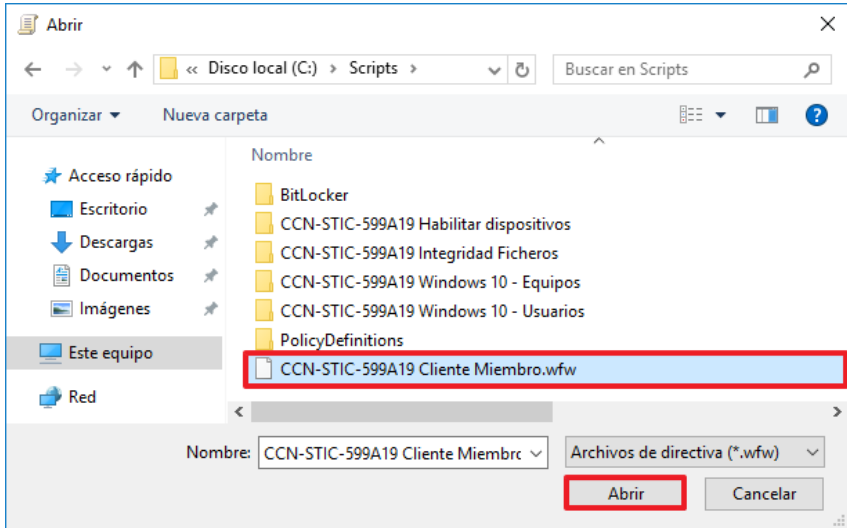
Paso	Descripción
49.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa "Clientes Windows 10". 
50.	De nuevo, en la consola "Administración de directivas de grupo", expanda y seleccione el contenedor "Objetos de directiva de grupo" mediante la ruta "Características → Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo". Pulsando el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
51.	Asigne el nombre "CCN-STIC-599A19 Windows 10 - Equipos" a la nueva GPO y pulse "Aceptar". 

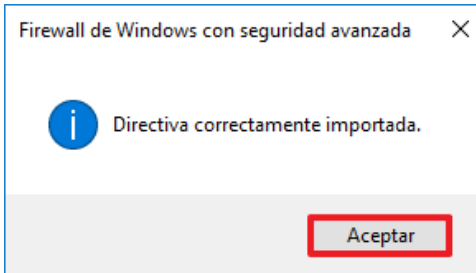
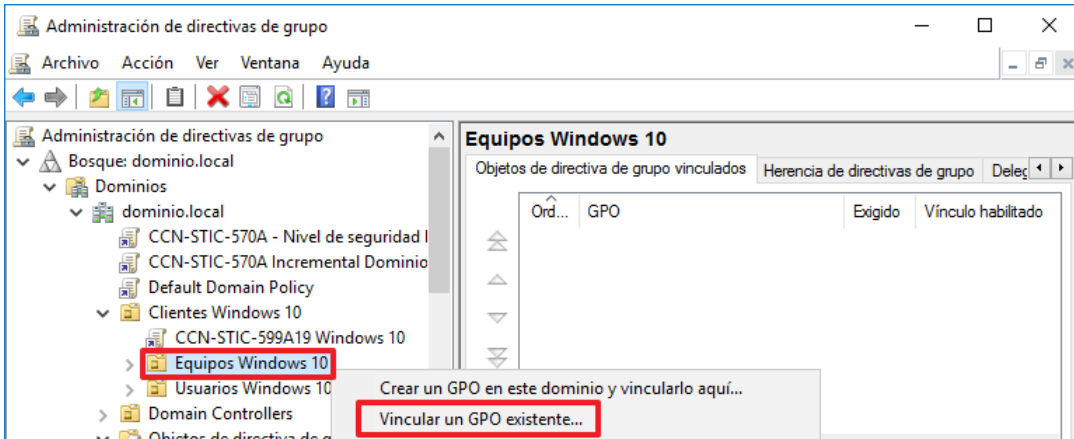
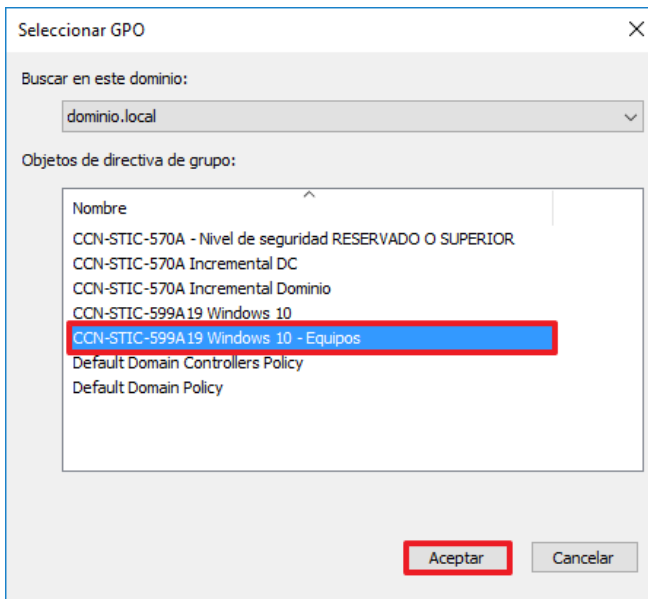
Paso	Descripción
52.	Seleccione la GPO recién creada, “CCN-STIC-599A19 Windows 10 - Equipos” con el botón derecho y elija la opción "Importar configuración..." en el menú contextual que aparecerá. 
53.	En el “Asistente para importar configuración” pulse “Siguiente >”. 

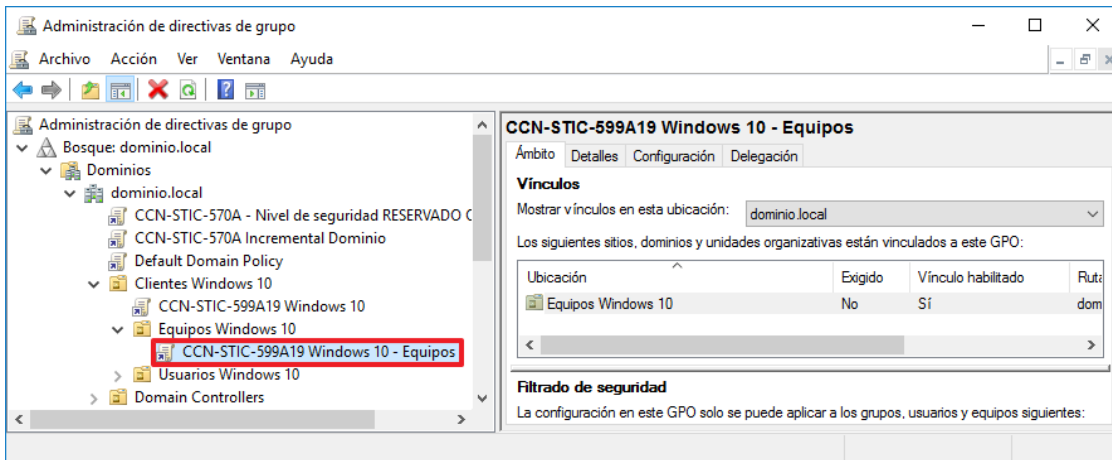
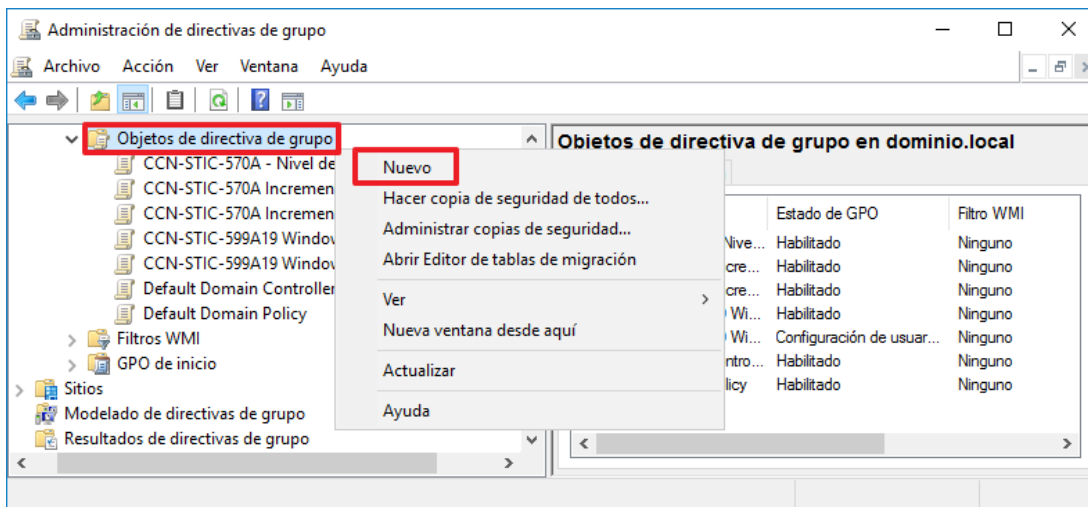
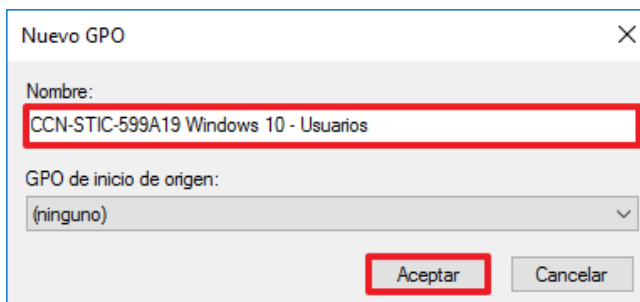
Paso	Descripción
54.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana "Hacer copia de seguridad de GPO". 
55.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 

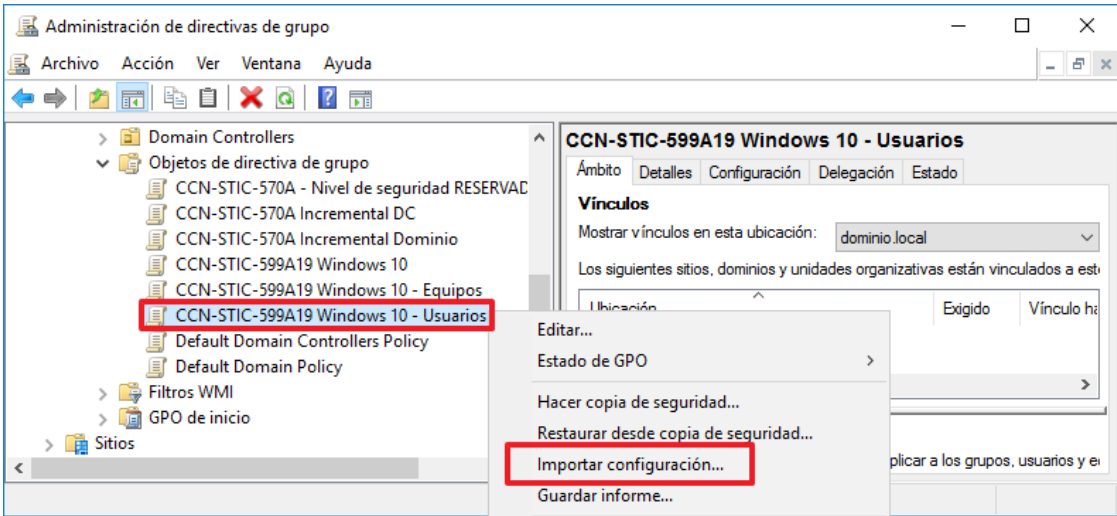
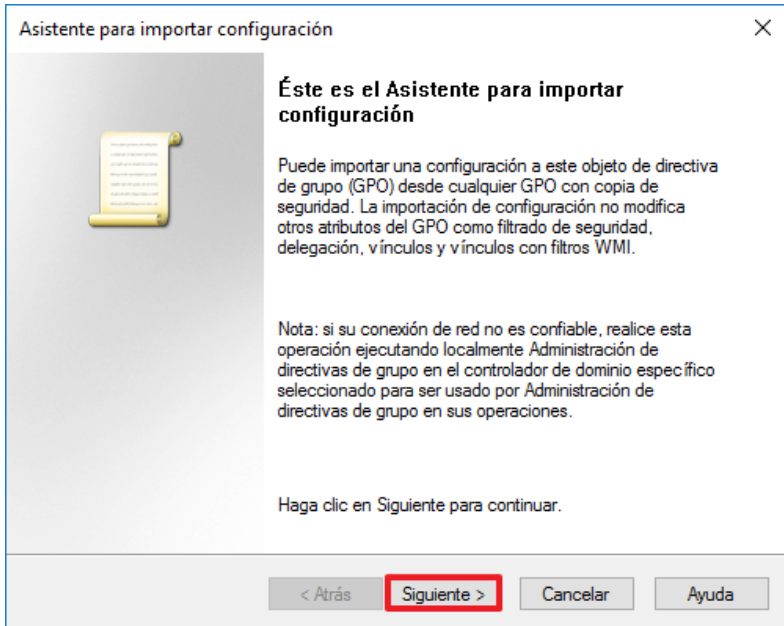
Paso	Descripción
56.	Localice la carpeta “CCN-STIC-599A19 Windows 10- Equipos” dentro de “C:\Scripts” y pulse “Aceptar”. 
57.	Pulse “Siguiente >” para continuar. 
58.	En “GPO de origen” pulse “Siguiente >”. 

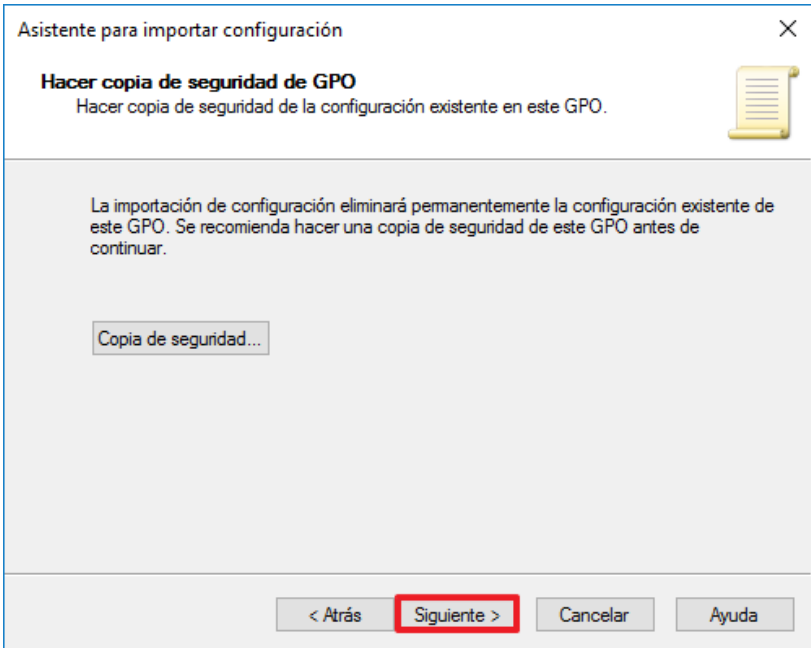
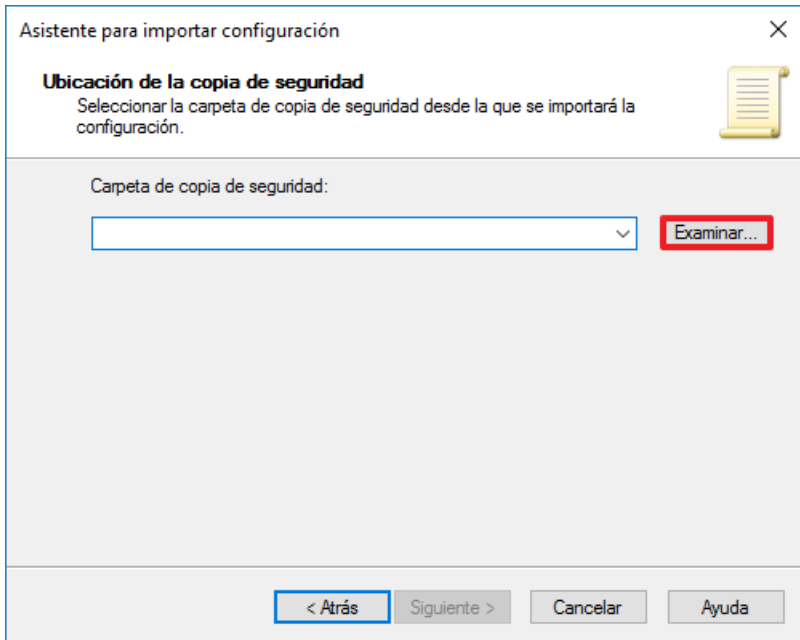
Paso	Descripción
59.	En “Examinar copia de seguridad” pulse “Siguiente >”.
60.	Pulse “Finalizar” para realizar la importación.
61.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 
62.	Seleccione de nuevo la GPO con el botón derecho y pulse sobre la opción del menú contextual “Editar”. 
63.	Despliegue el nodo “Firewall de Windows con seguridad avanzada” a través de la ruta “Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada”

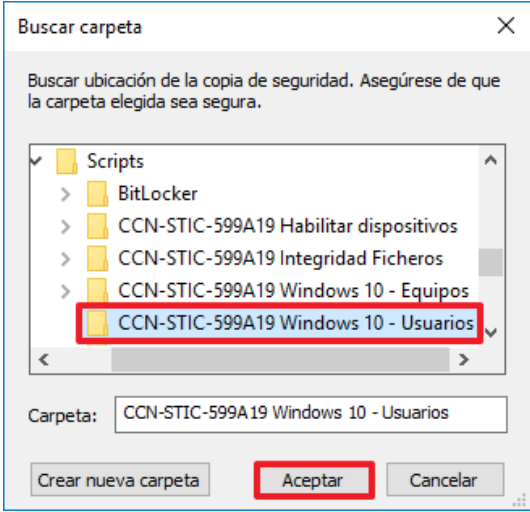
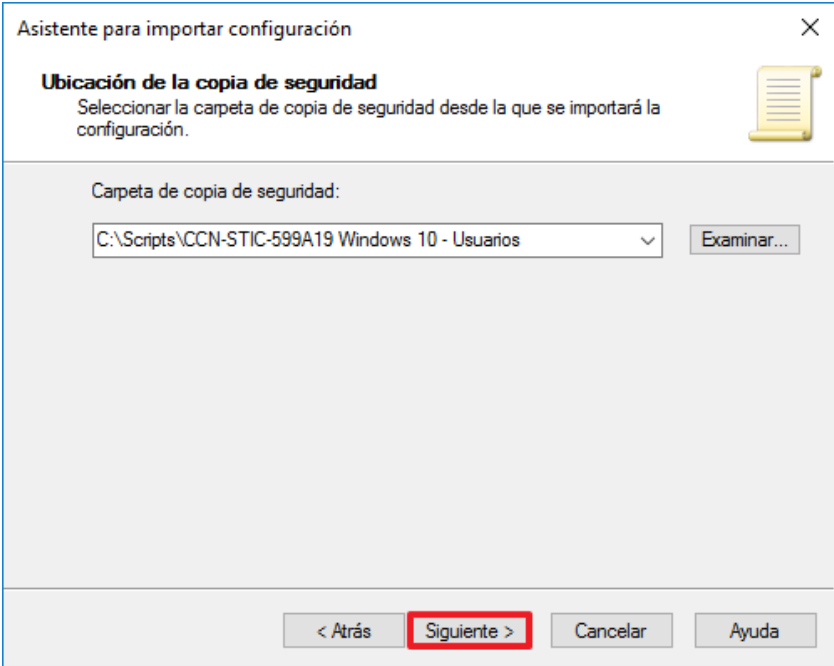
Paso	Descripción
64.	Pulse con el botón derecho sobre “Firewall de Windows con seguridad avanzada” y seleccione la opción del menú contextual “Importar directiva...”. 
65.	Pulse “S” ante el mensaje de advertencia emergente y seleccione el fichero “CCN-STIC-599A19 Cliente Miembro.wfw” ubicado en el directorio “C:\Scripts”. Pulse sobre “Abrir” para cargar el fichero. 

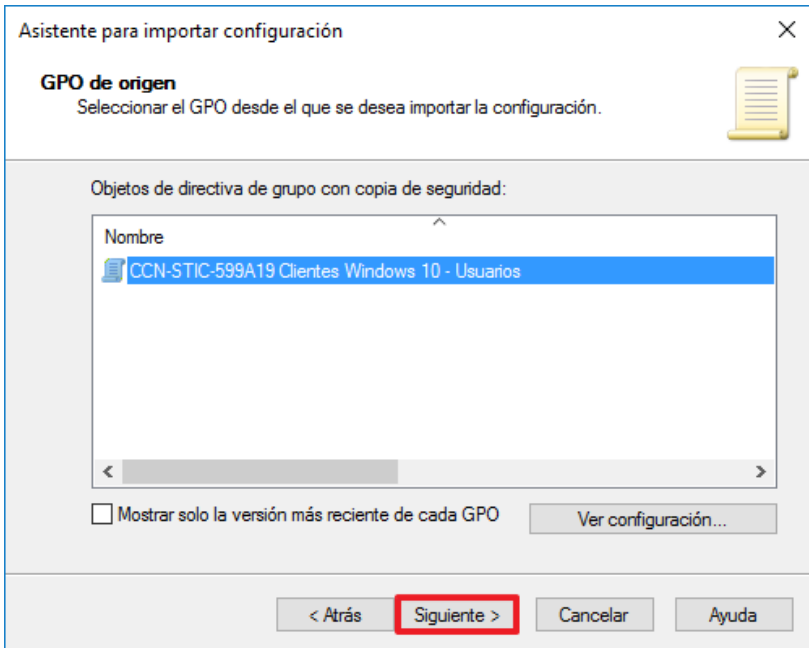
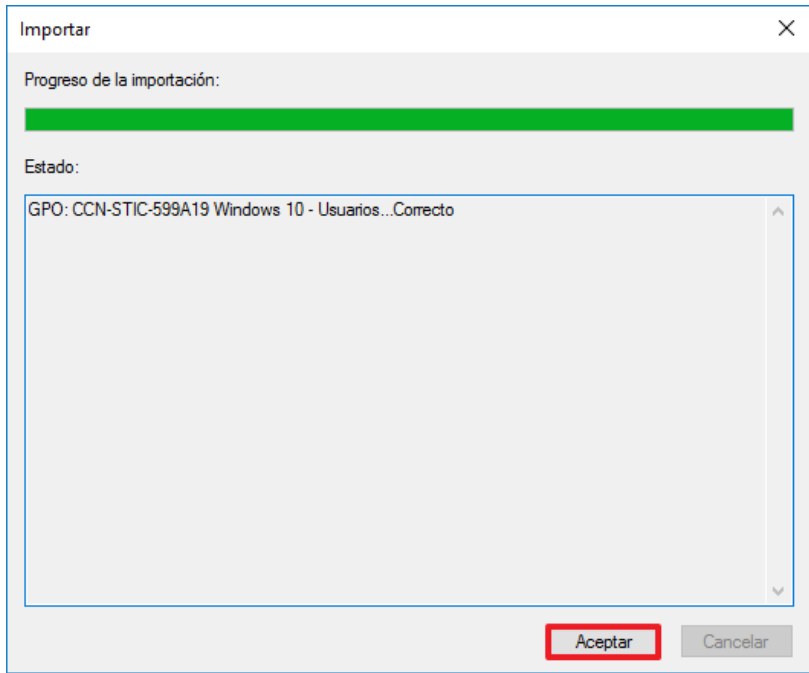
Paso	Descripción
66.	Pulse sobre “Aceptar” en el mensaje emergente y cierre el “Editor de administración de directivas de grupo”. 
67.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la ruta “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10”. Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
68.	Seleccione “CCN-STIC-599A19 Windows 10 - Equipos” de la lista y pulse “Aceptar”. 

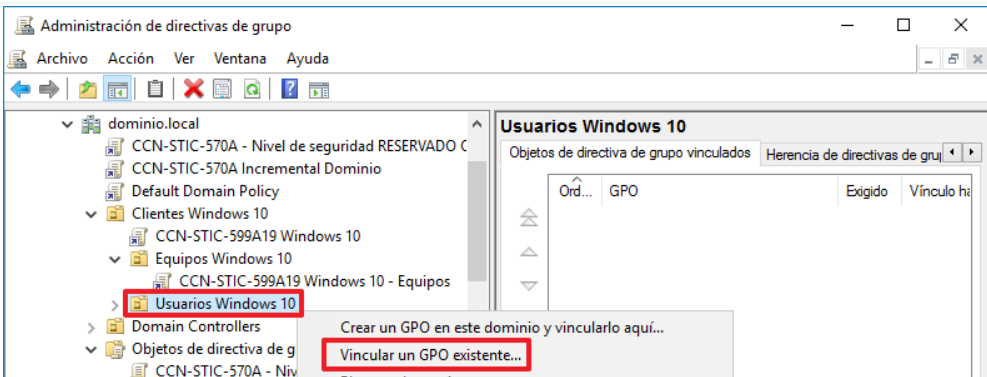
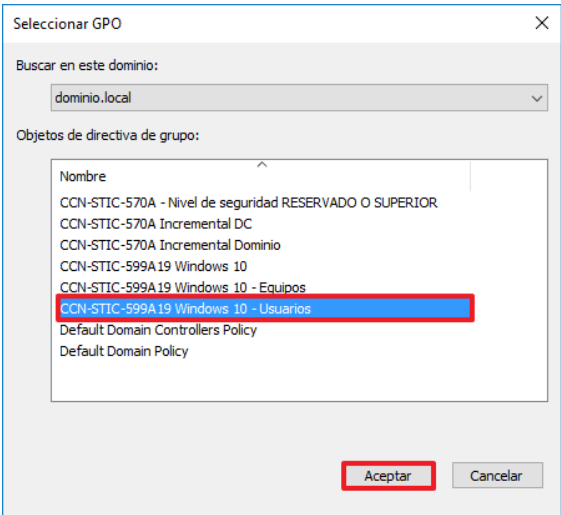
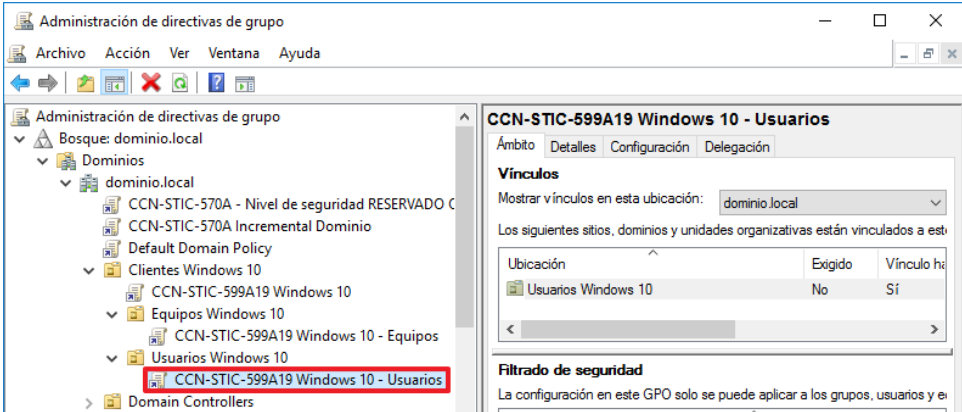
Paso	Descripción
69.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa "Equipos Windows 10". 
70.	De nuevo, en la consola "Administración de directivas de grupo", expanda y seleccione el contenedor "Objetos de directiva de grupo" mediante la siguiente ruta. "Administración de directivas de grupo → Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo" Pulsando el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
71.	Asigne el nombre "CCN-STIC-599A19 Windows 10 – Usuarios" a la nueva GPO y pulse "Aceptar". 

Paso	Descripción
72.	Seleccione la GPO recién creada, “CCN-STIC-599A19 Windows 10 - Usuarios” con el botón derecho y elija la opción “Importar configuración...” en el menú contextual. 
73.	En el “Asistente para importar configuración” pulse “Siguiente >”. 

Paso	Descripción
74.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana "Hacer copia de seguridad de GPO". 
75.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 

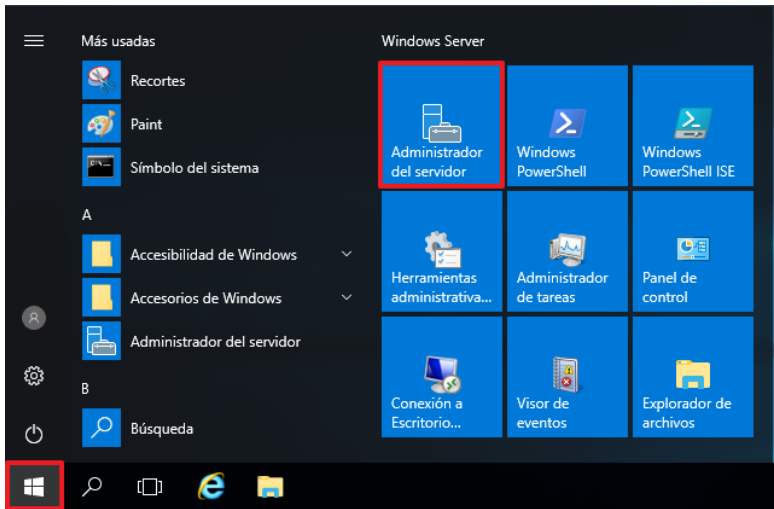
Paso	Descripción
76.	Localice la carpeta “CCN-STIC-599A19 Windows 10- Usuarios” y pulse “Aceptar”. 
77.	Pulse “Siguiente >” para continuar. 

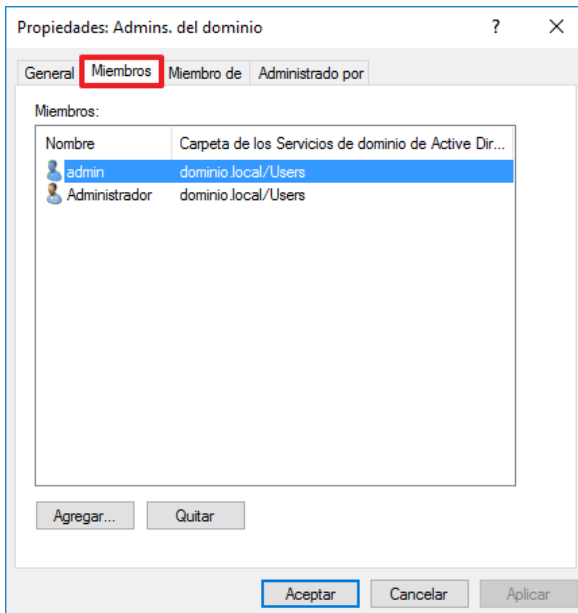
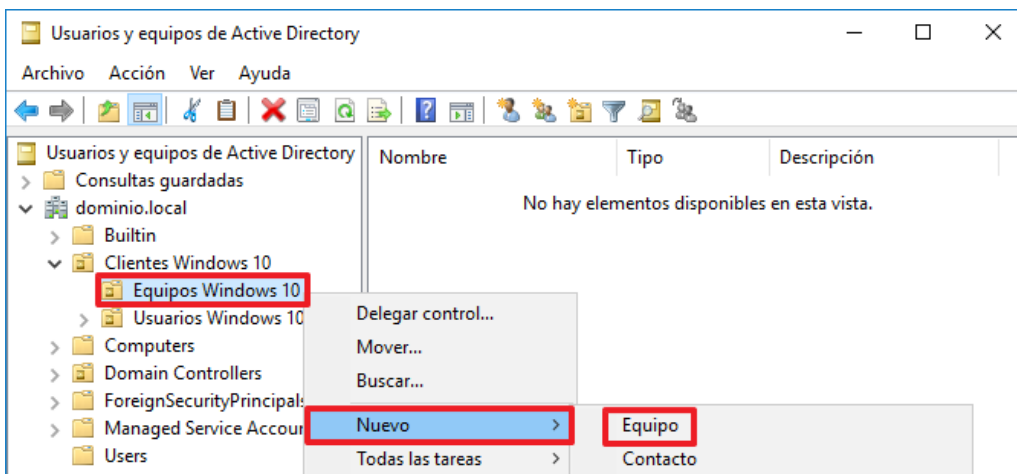
Paso	Descripción
78.	En “GPO de origen” pulse “Siguiente >”. 
79.	En “Examinar copia de seguridad” pulse “Siguiente >”.
80.	Pulse “Finalizar” para realizar la importación.
81.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 

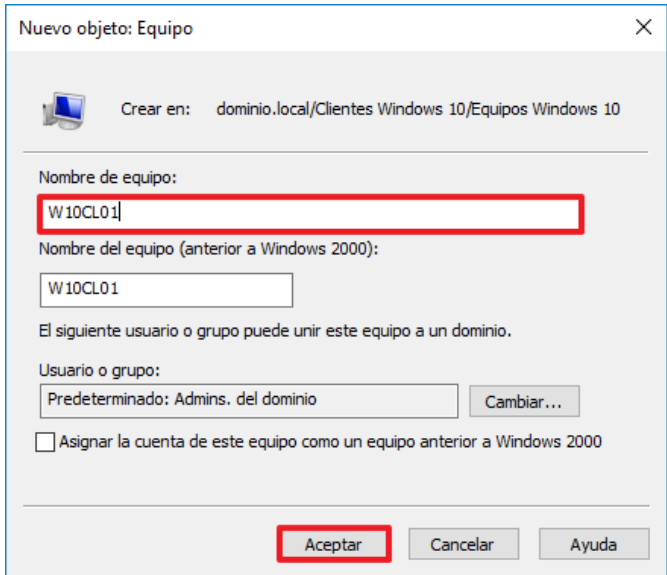
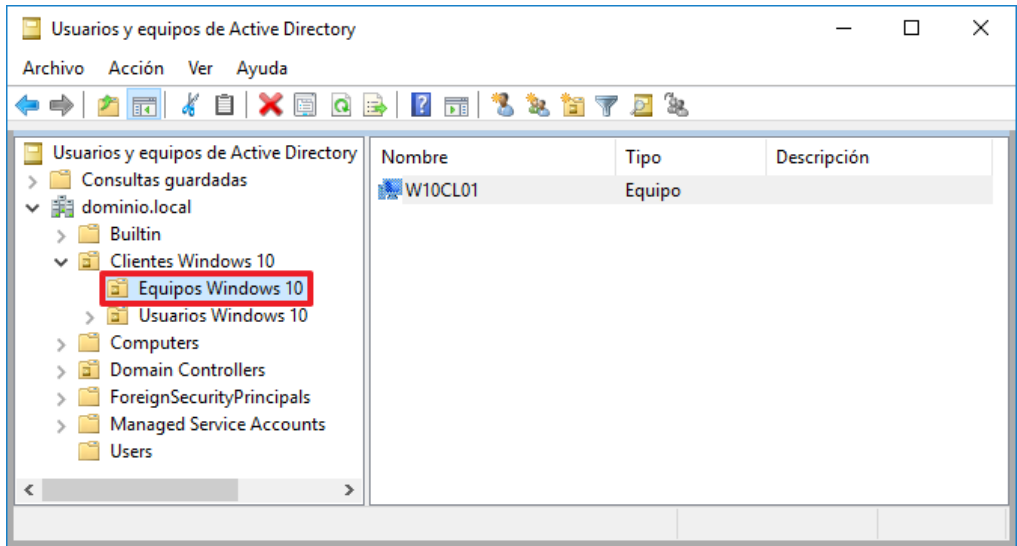
Paso	Descripción
82.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Usuarios Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
83.	Seleccione “CCN-STIC-599A19 Windows 10 - Usuarios” de la lista y pulse “Aceptar”. 
84.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Usuarios Windows 10”. 

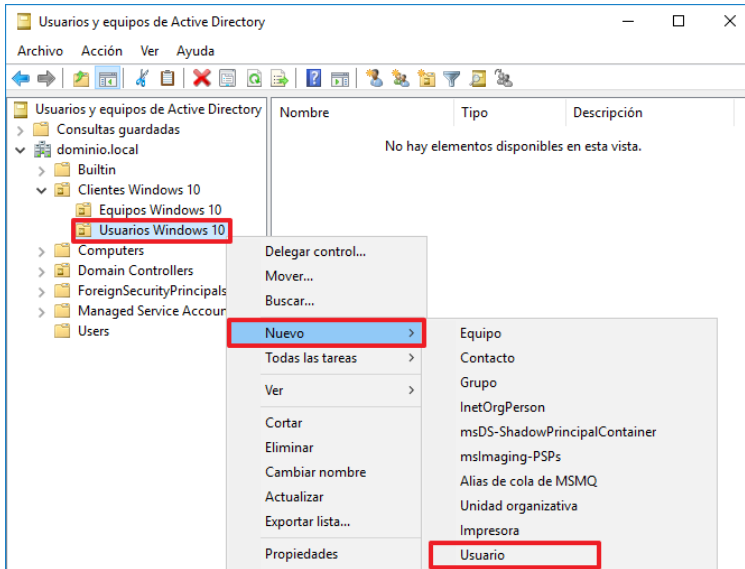
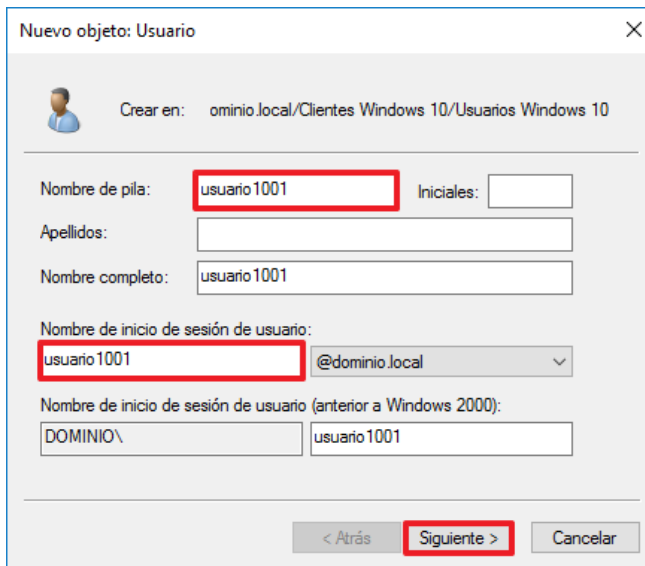
En este punto, las unidades organizativas y las GPO necesarias están ya configuradas correctamente en Active Directory y su configuración se aplicará automáticamente tanto al equipo cliente Microsoft Windows 10 miembro del dominio que está asegurando como a los futuros equipos cliente Microsoft Windows 10 que se añadan.

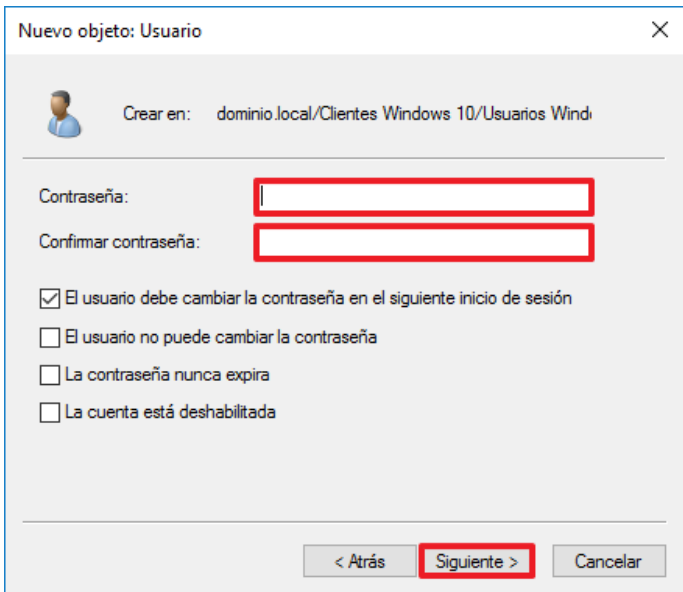
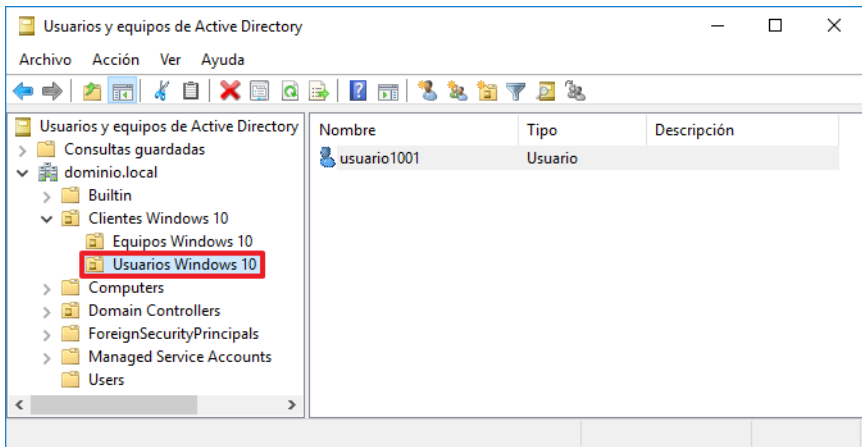
Los siguientes pasos deberá realizarlos en un controlador de dominio del dominio al que va a pertenecer el equipo que está asegurando, además, deberá realizarlos cada vez que necesite asegurar un nuevo equipo cliente Windows 10, ya que se trata de preparar en Active Directory una cuenta de equipo para el equipo que está asegurando y que va a unir al dominio.

Paso	Descripción
85.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo que va a asegurar. Deberá iniciar sesión con una cuenta que pertenezca al grupo “Admins. del dominio”.
86.	Asegúrese, antes de continuar, de que los grupos "Administradores" y "Usuarios de shells" contienen los usuarios adecuados para su entorno. Para ello, acceda a la herramienta “Administrador del servidor” mediante el icono correspondiente en el menú de inicio. 
87.	En el menú superior haga clic sobre “Herramientas” y seleccione “Usuarios y equipos de Active Directory”. 

Paso	Descripción
88.	Diríjase al contenedor “Users” mediante la ruta “<Nombre de su dominio> → Users”. Haciendo doble clic sobre estos grupos podrá comprobar sus propiedades. En la pestaña “Miembros” podrá ver qué grupos o usuarios pertenecen a dicho grupo. 
89.	De nuevo en la consola “Usuarios y equipos de Active Directory”, cree una cuenta de equipo con el nombre del equipo que va a incluir en el dominio bajo la unidad organizativa "Equipos Windows 10". Para ello, expanda y seleccione el contenedor “Equipos Windows 10” mediante la siguiente ruta: “<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10” Haga clic con el botón derecho del ratón sobre la unidad organizativa y seleccione la opción “Nuevo → Equipo” del menú contextual que aparecerá. 

Paso	Descripción
90.	En el cuadro de diálogo que aparecerá, titulado "Nuevo objeto: Equipo", introduzca en el campo "Nombre de equipo:" el nombre del equipo que va a unir al dominio y pulse "Aceptar".  Nota: El campo "Nombre del equipo (anterior a Windows 2000):" se rellenará de forma automática, aun así, no marque la opción "Asignar la cuenta de este equipo como un equipo anterior a Windows 2000". En el ejemplo, se utiliza el equipo con nombre "W10CL01".
91.	La nueva cuenta de equipo aparecerá dentro del contenedor "Equipos Windows 10".  Nota: Al estar alojada la cuenta de equipo en este contenedor de Active Directory, el equipo Windows 10 miembro del dominio recibirá la configuración de equipo recomendada en esta guía para equipos clientes Windows 10.

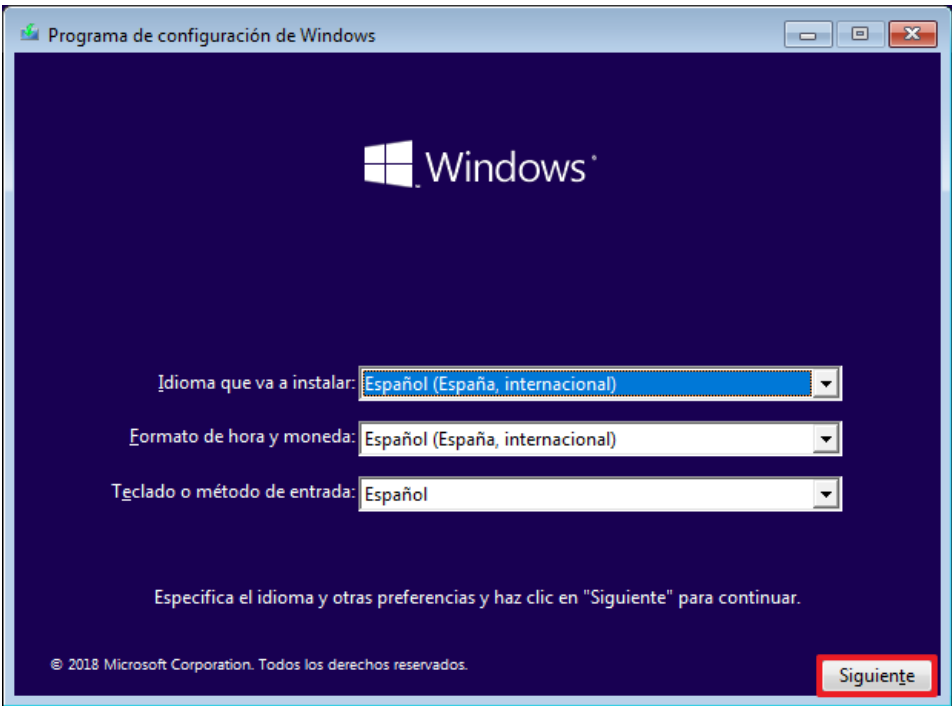
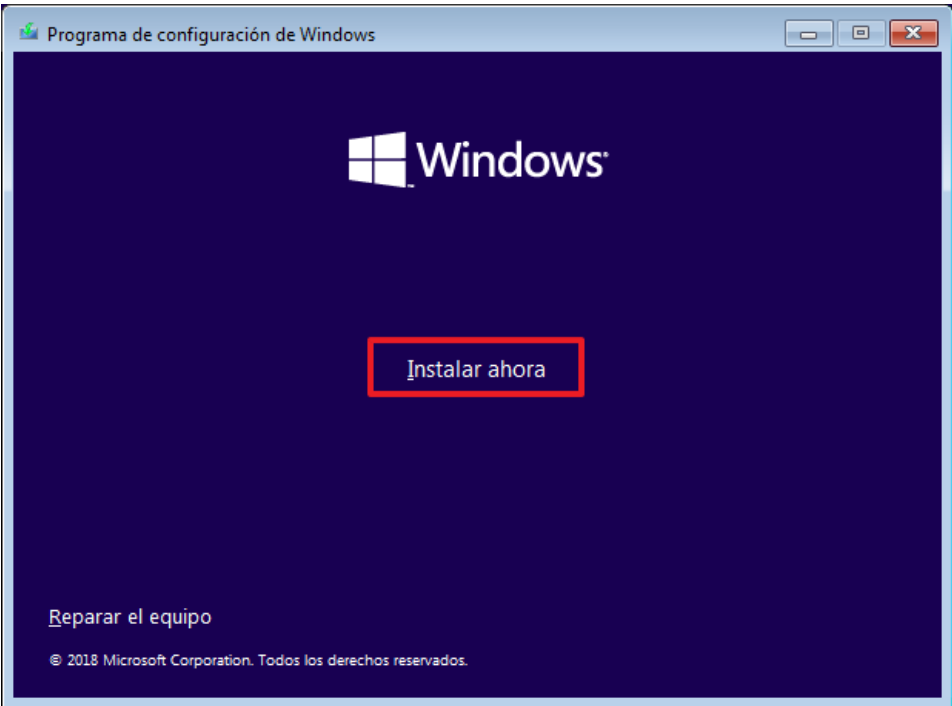
Paso	Descripción
92.	El siguiente paso consiste en crear a cuenta del usuario que vaya a utilizar el equipo cliente que está asegurando, bajo la unidad organizativa “Usuarios Windows 10”. Para ello y utilizando, de nuevo, la consola “Usuarios y equipos de Active Directory”. Para ello, expanda y seleccione el contenedor “Usuarios Windows 10” mediante la siguiente ruta "<Nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10". Haga clic con el botón derecho del ratón sobre la unidad organizativa y seleccione la opción "Nuevo → Usuario" del menú contextual que aparecerá. 
93.	En el cuadro de diálogo "Nuevo objeto: Usuario", introduzca en el campo “Nombre de pila” y “Nombre de inicio de sesión de usuario:” el nombre que tendrá en el nuevo usuario, El sistema rellenará automáticamente el campo “Nombre completo”. A continuación, pulse “Siguiente >” para continuar.  Nota: En el ejemplo, se utiliza "usuario1001" como nombre del nuevo usuario. Elija un nombre de usuario siguiendo los criterios que sean apropiados para su entorno, y rellene o deje en blanco el resto de datos según sea oportuno para su entorno.

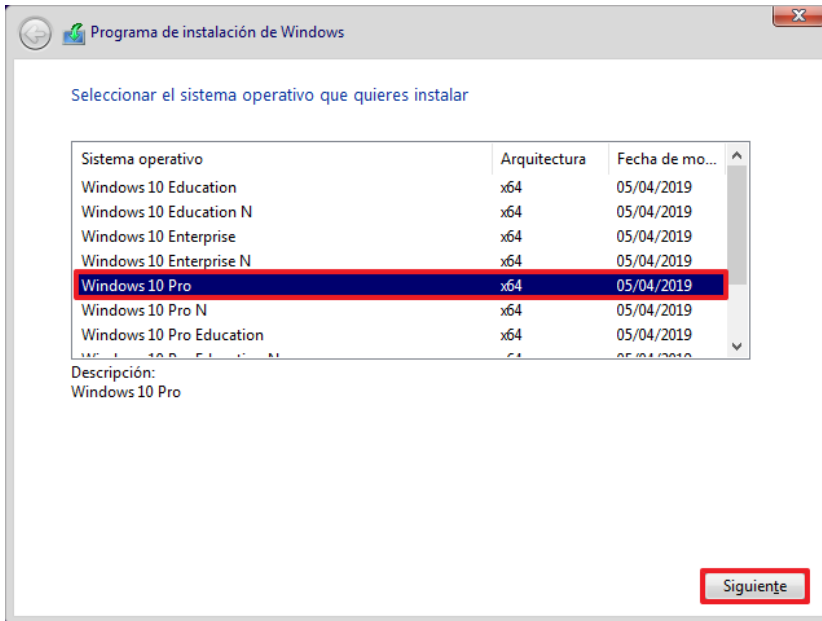
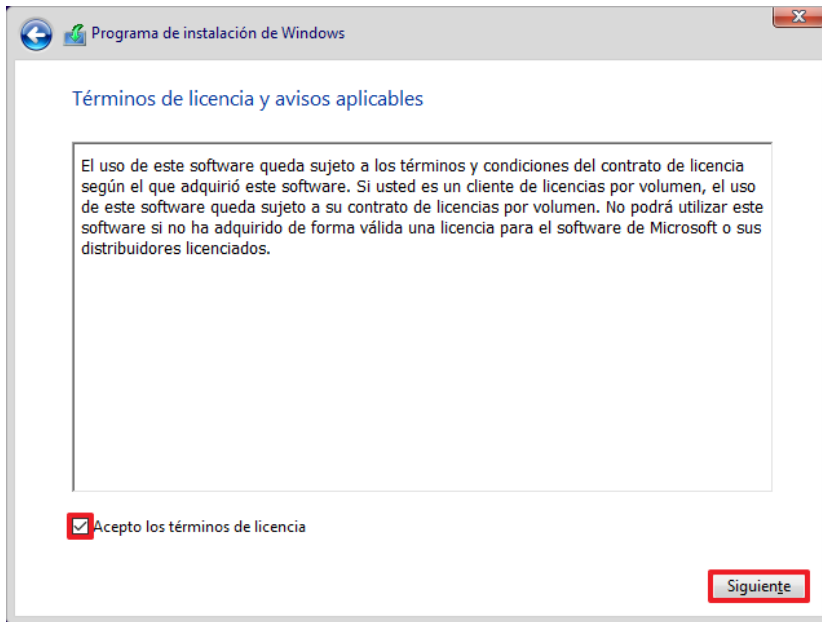
Paso	Descripción
94.	Asigne una contraseña segura al usuario y marque las opciones que sean oportunas para su entorno y pulse “Siguiente >”. 
95.	Pulse “Finalizar” para cerrar la ventana “Nuevo objeto: Usuario”. La cuenta de usuario aparecerá dentro del contenedor "Usuarios Windows 10". 

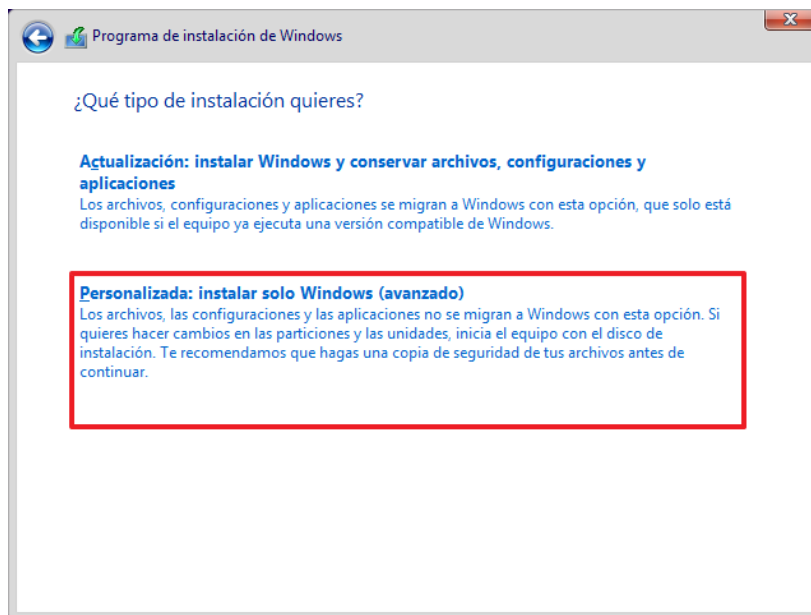
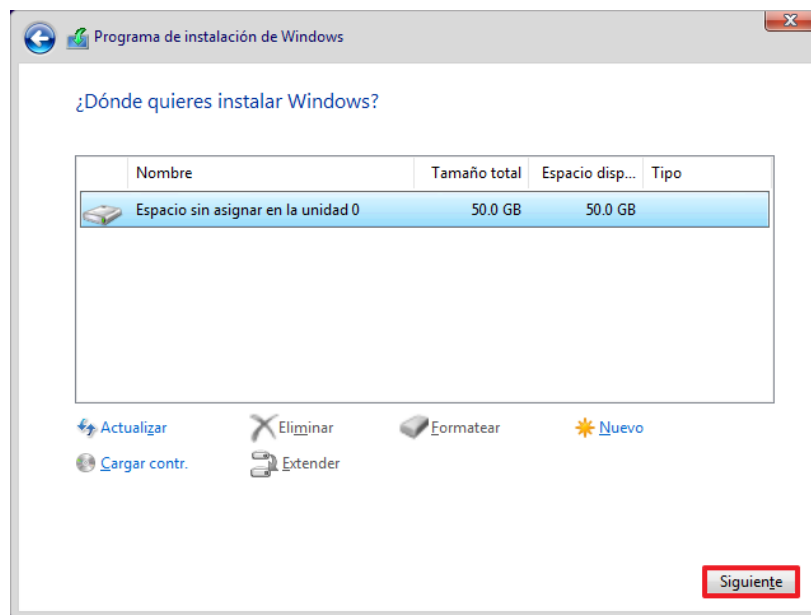
2. INSTALACIÓN Y PREPARACIÓN MS WINDOWS 10

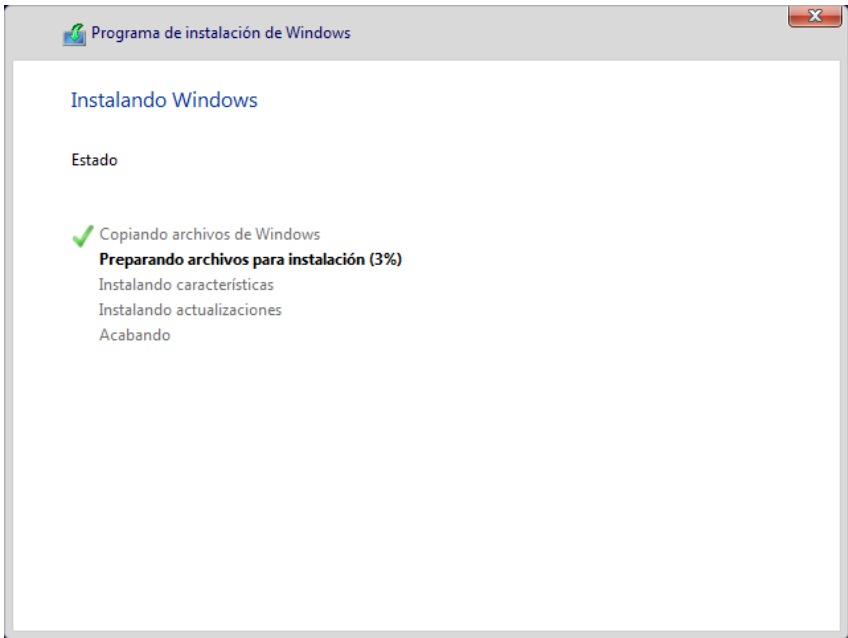
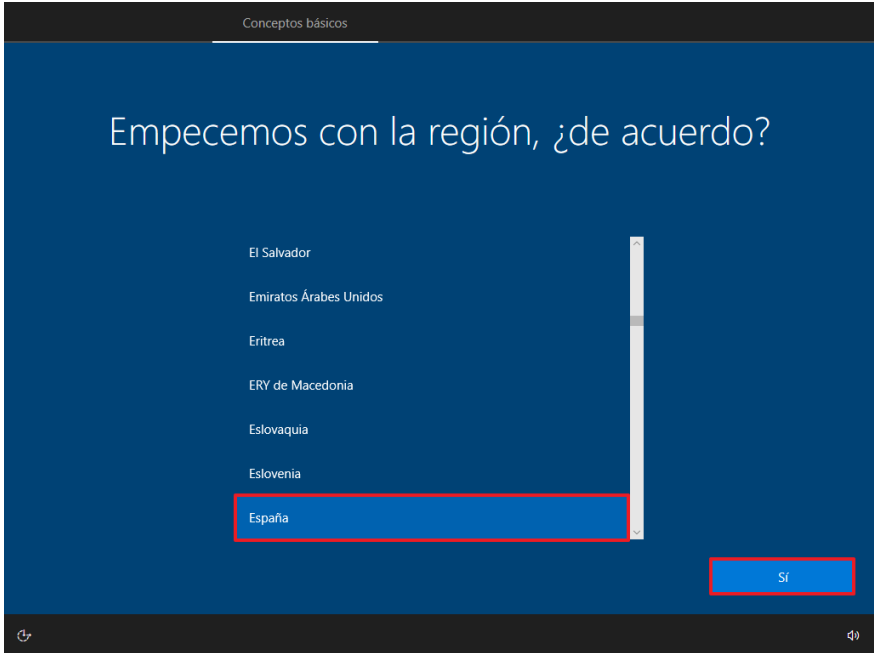
Los pasos que se describen a continuación deberá realizarlos en la máquina donde se instalará y configurará el equipo puesto cliente con sistema operativo Microsoft Windows 10 (versión 1809) Pro/Enterprise sin opción de mantenimiento LTSC.

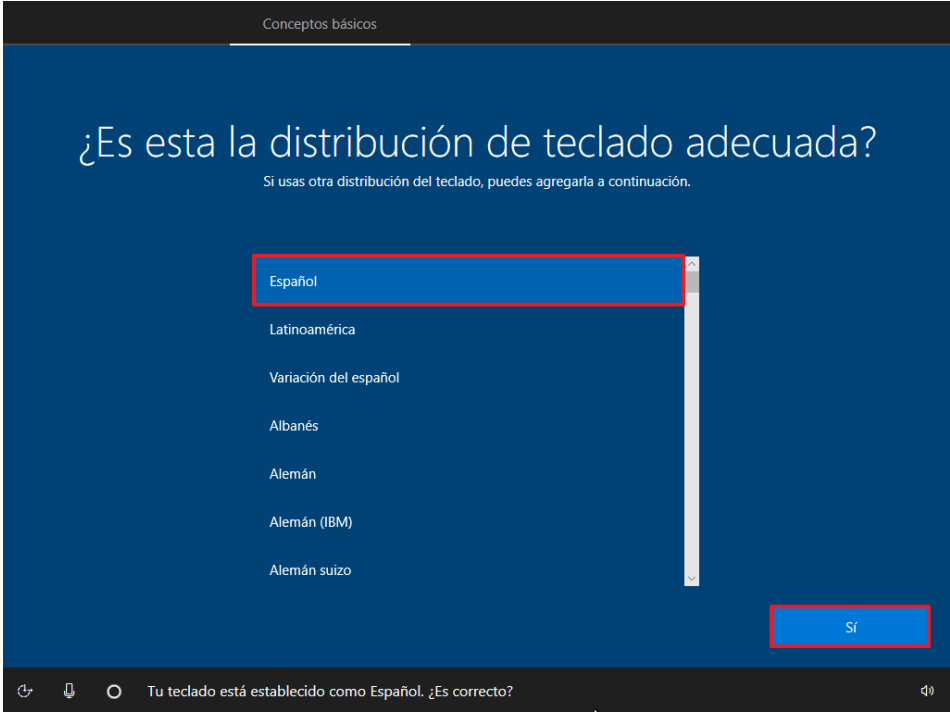
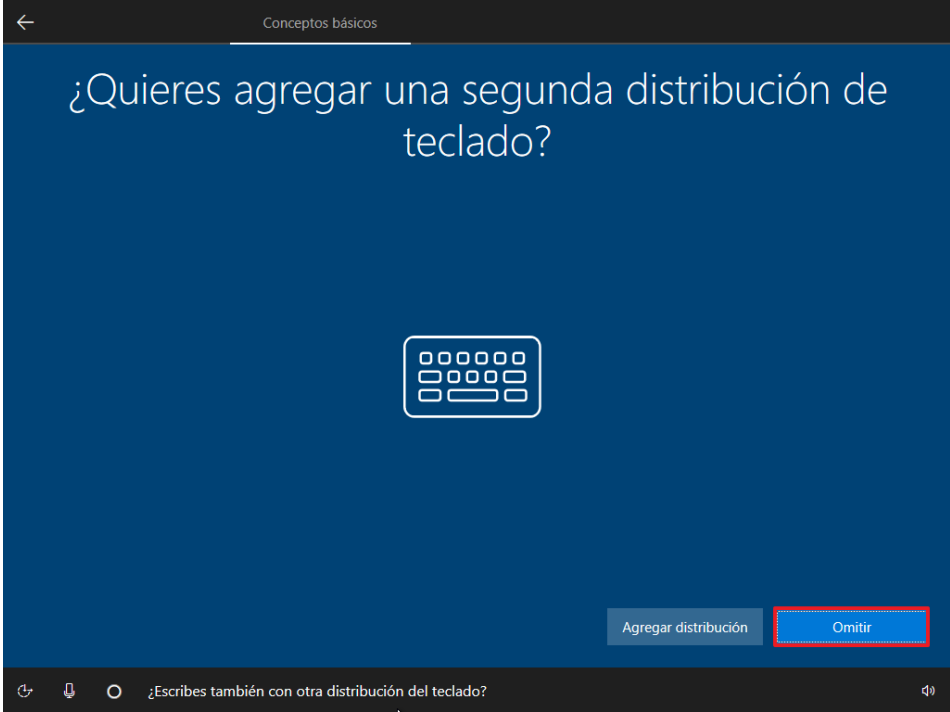
Paso	Descripción
96.	Introduzca el dispositivo USB o DVD de Microsoft Windows 10 PRO y, si fuera necesario, reinicie la máquina para iniciar la instalación del sistema. Nota: En este ejemplo se utiliza la versión Pro, también está admitida la versión Enterprise. Utilice la más adecuada para su organización.

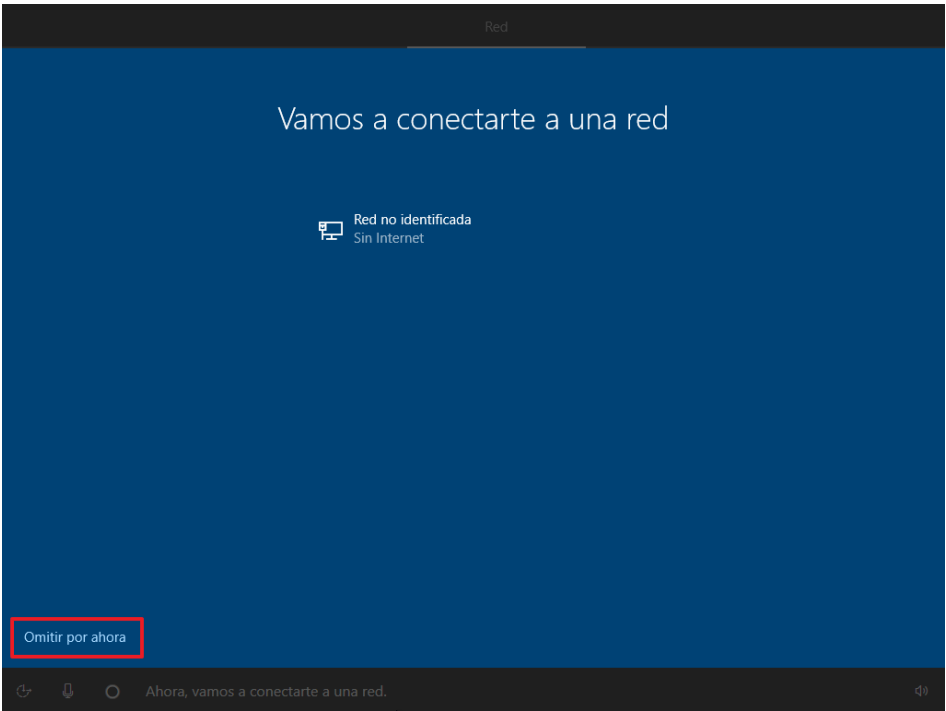
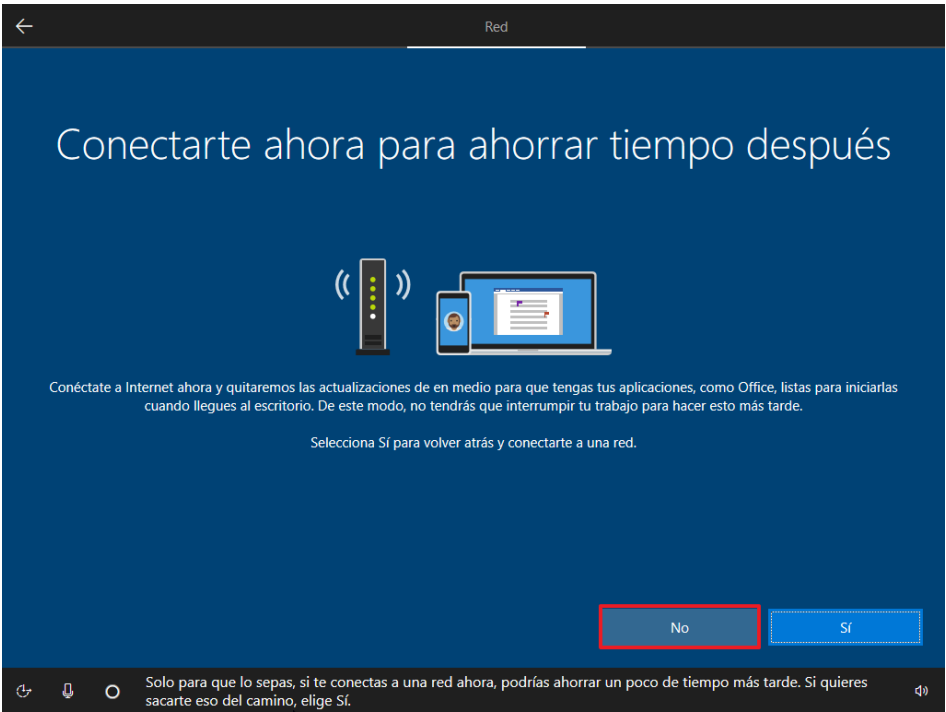
Paso	Descripción
97.	Cuando aparezca el mensaje Presionar una tecla para arrancar desde el DVD, pulse una tecla. Si el equipo no se inicia desde DVD revise los parámetros de la BIOS.
98.	Cuando se le indique en pantalla, seleccione el idioma y la configuración de teclado (español). Pulse “Siguiente” para continuar. 
99.	Pulse sobre “Instalar ahora”. 

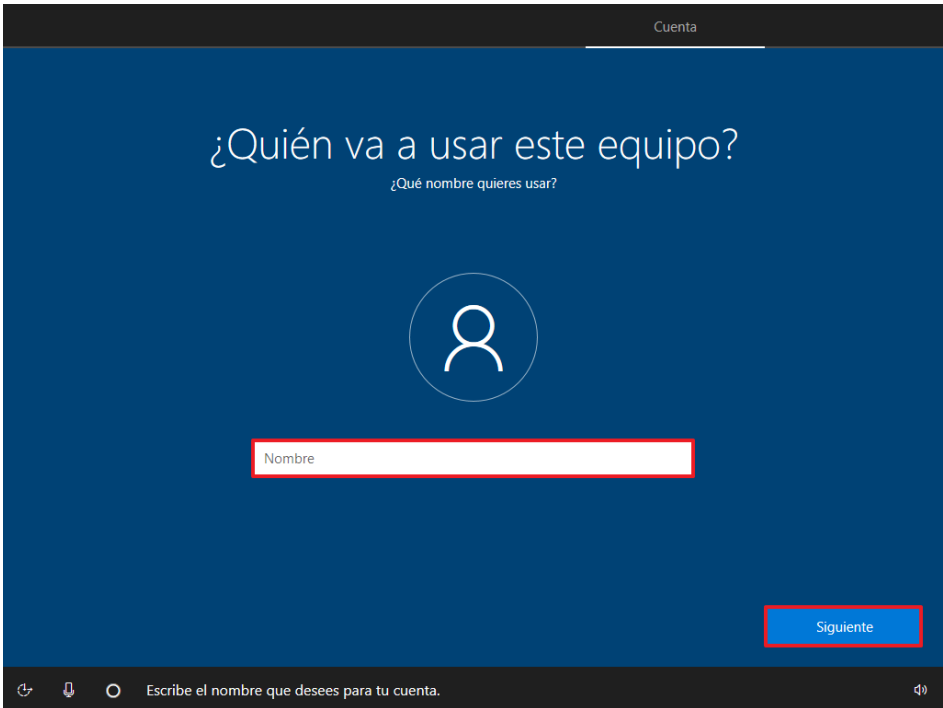
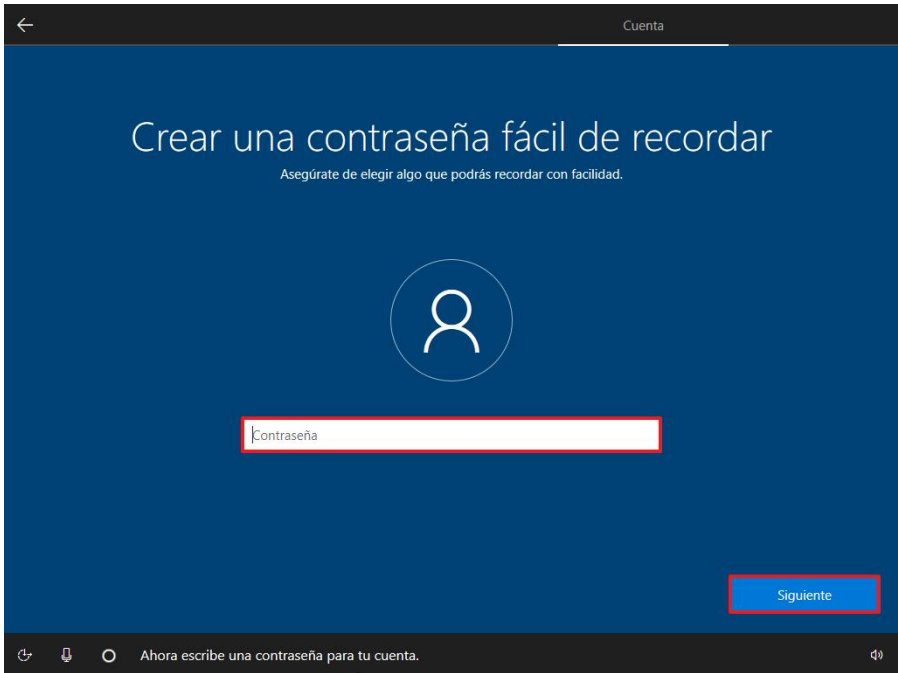
Paso	Descripción
100.	Seleccione la opción “Windows 10 PRO”.  The screenshot shows the 'Programa de instalación de Windows' window. It displays a list of operating systems with columns for 'Sistema operativo', 'Arquitectura', and 'Fecha de mo...'. The 'Windows 10 Pro' option is highlighted in blue. Below the list, there is a 'Descripción:' section showing 'Windows 10 Pro'. A 'Siguiente' button is visible at the bottom right.
101.	Marque la opción “Acepto los términos de licencia” y pulse “Siguiente”.  The screenshot shows the 'Programa de instalación de Windows' window. It displays the 'Términos de licencia y avisos aplicables' section. The text states: 'El uso de este software queda sujeto a los términos y condiciones del contrato de licencia según el que adquirió este software. Si usted es un cliente de licencias por volumen, el uso de este software queda sujeto a su contrato de licencias por volumen. No podrá utilizar este software si no ha adquirido de forma válida una licencia para el software de Microsoft o sus distribuidores licenciados.' Below the text, the 'Acepto los términos de licencia' checkbox is checked. A 'Siguiente' button is visible at the bottom right.

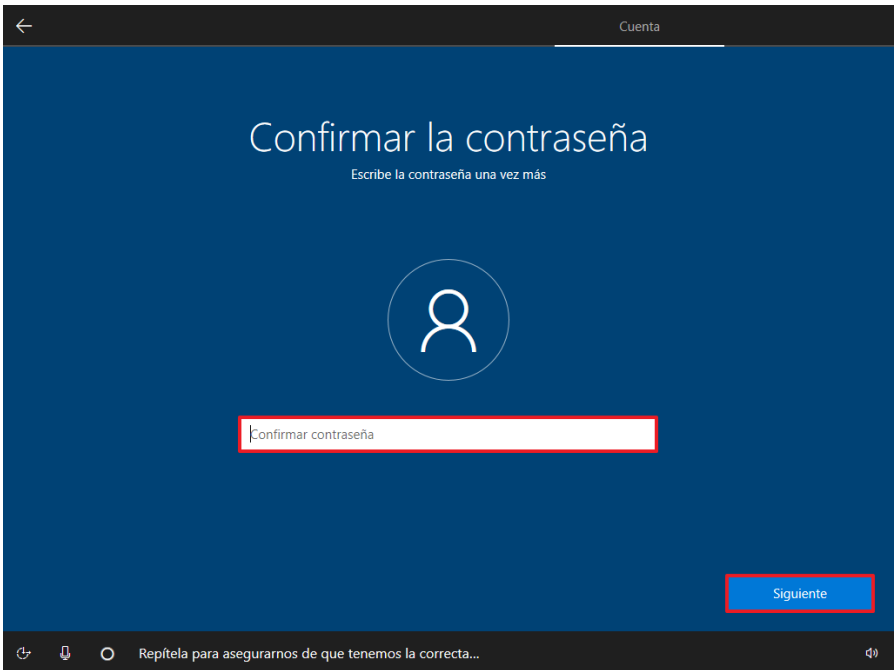
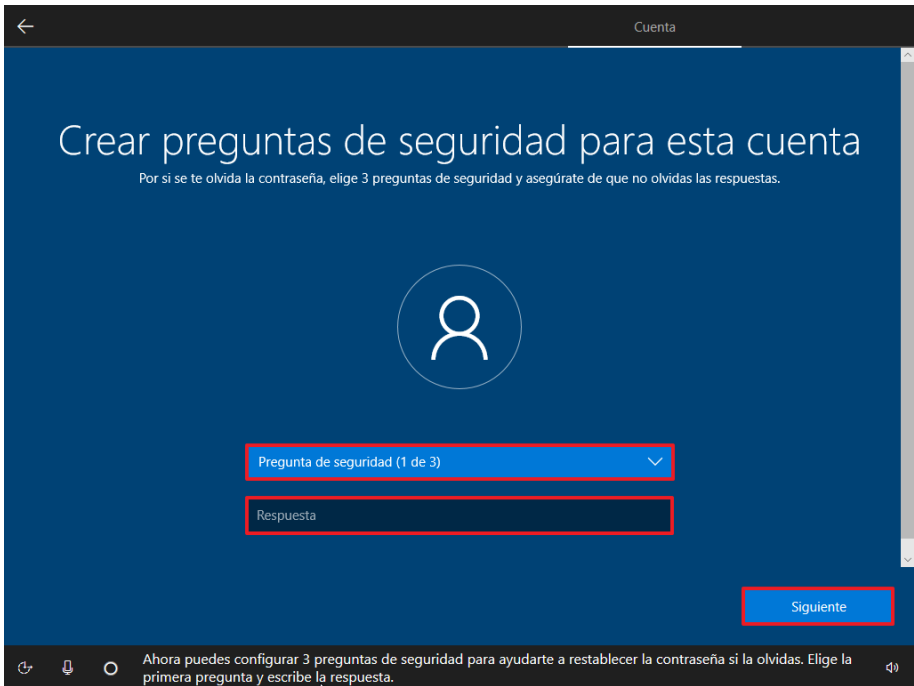
Paso	Descripción
102.	Seleccione la opción tipo de instalación “Personalizada: instalar solo Windows (avanzada)”. 
103.	Seleccione el disco en el que se realizará la instalación y pulse “Siguiente”. 
Nota: En caso de necesitar establecer particiones o formatear particiones o discos, es en este momento 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	

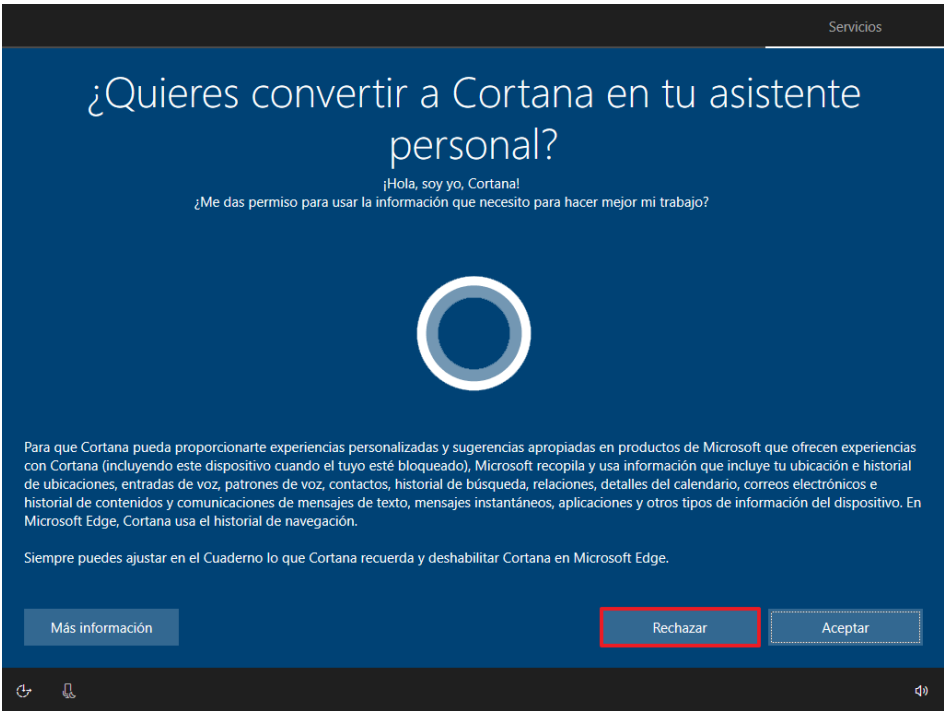
Paso	Descripción
104.	Comenzará la instalación en este momento. Este proceso durará varios minutos dependiendo de las prestaciones del dispositivo sobre el que se instale Microsoft Windows 10 y, posiblemente, requerirá reiniciar en varias ocasiones. Espere a que aparezca la ventana “Conceptos básicos” y continúe con el siguiente paso. 
105.	En la ventana “Conceptos básicos” seleccione la región “España” y pulse “Sí”. 

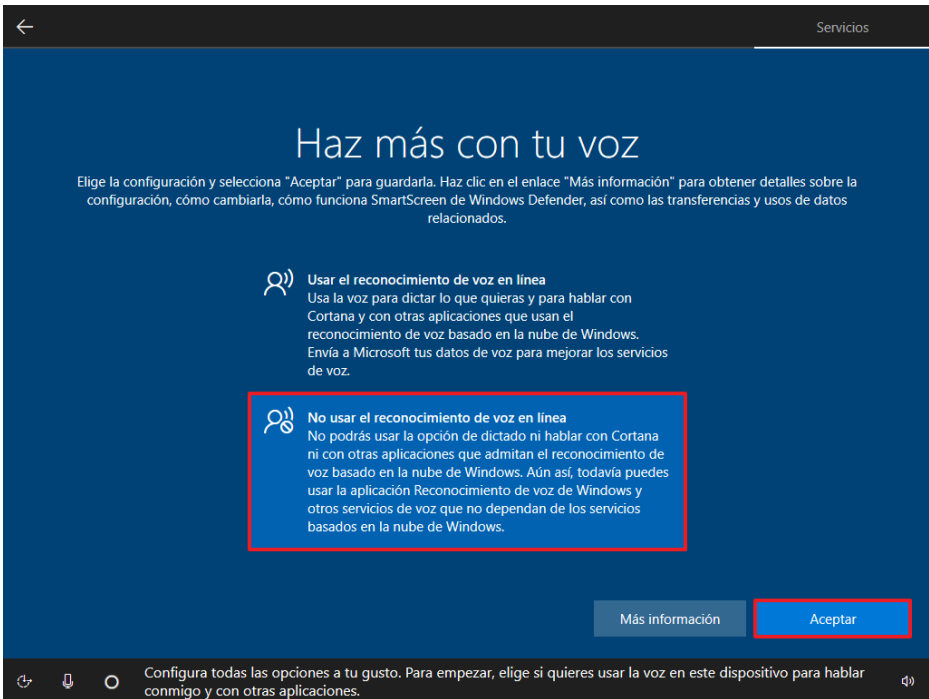
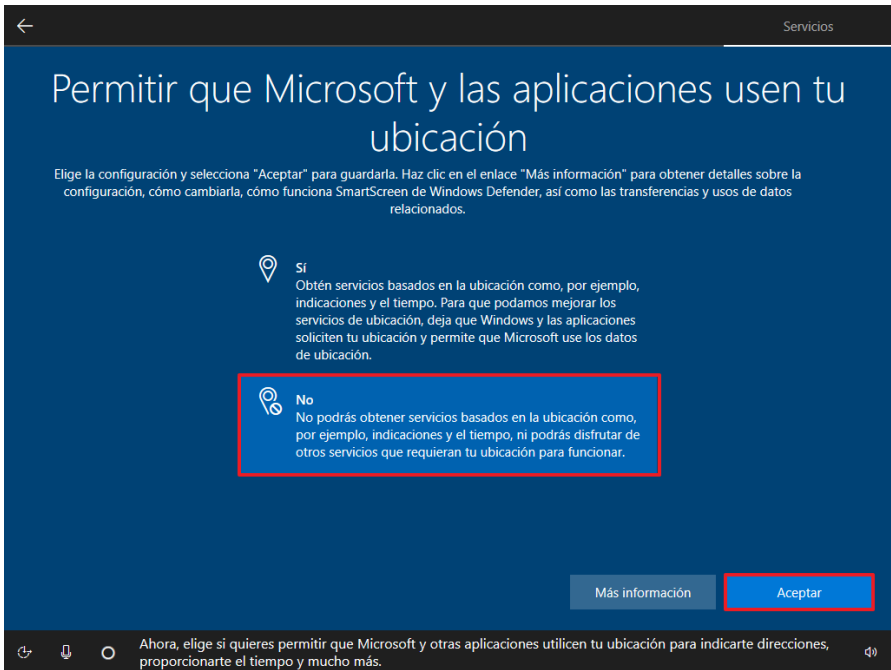
Paso	Descripción
106.	Seleccione la distribución de teclado “Español” y pulse “Sí” para continuar. 
107.	Pulse “Omitir” para no agregar una segunda distribución de teclado. 

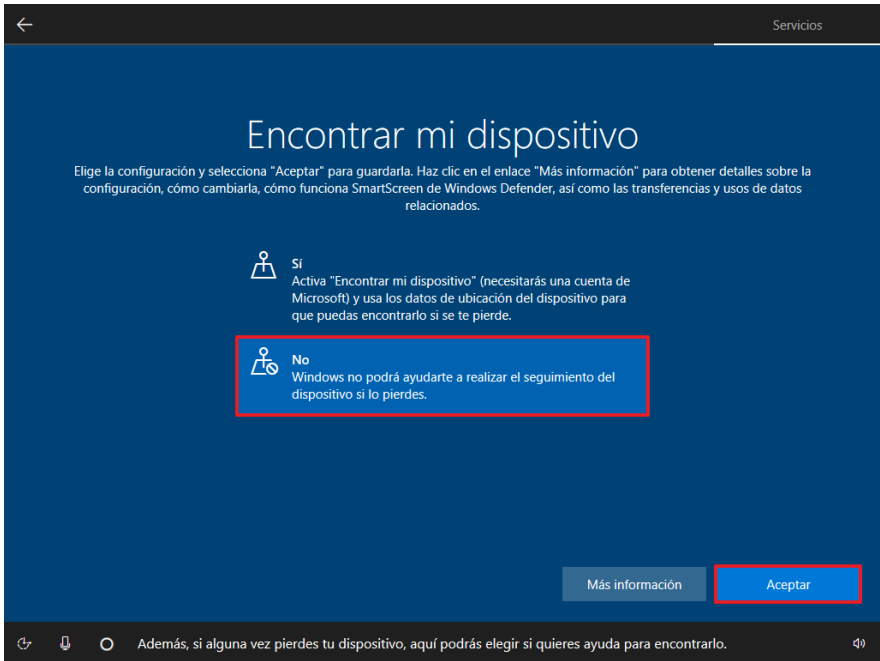
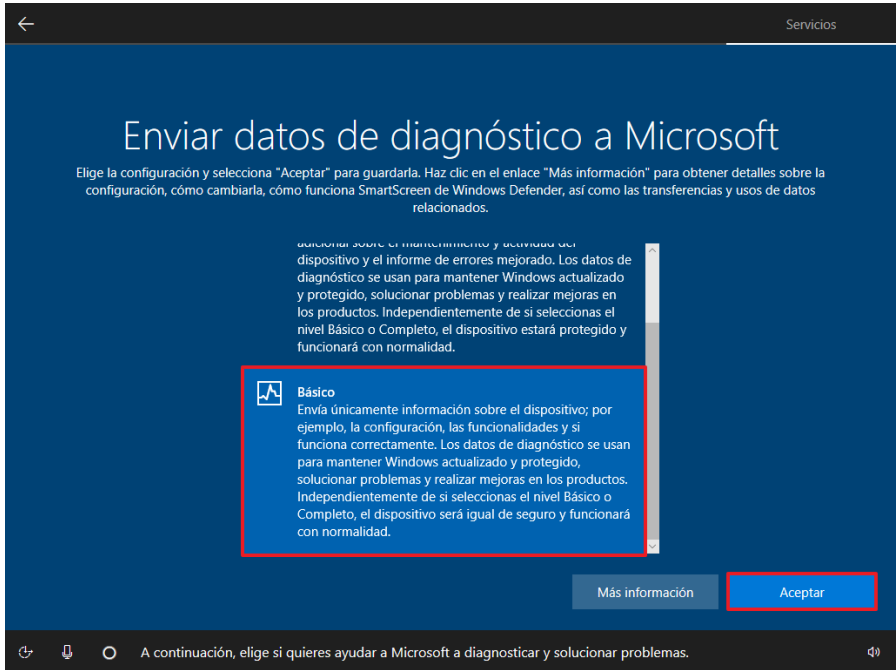
Paso	Descripción
108.	En el apartado de red seleccione la opción “Omitir por ahora”. La configuración de red se establecerá más adelante. 
109.	Pulse “No” para continuar. 

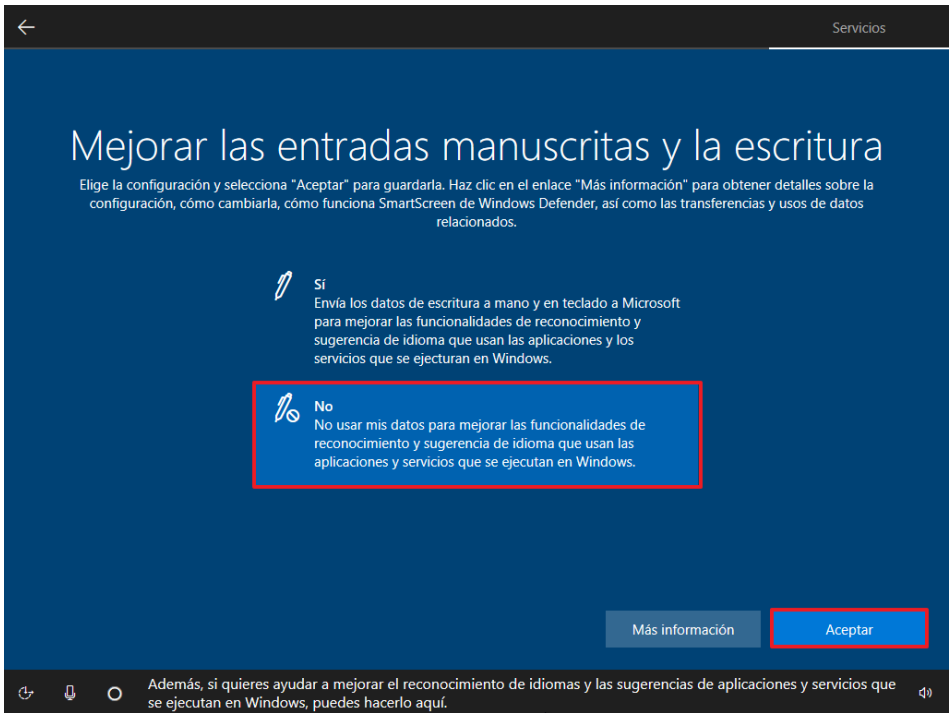
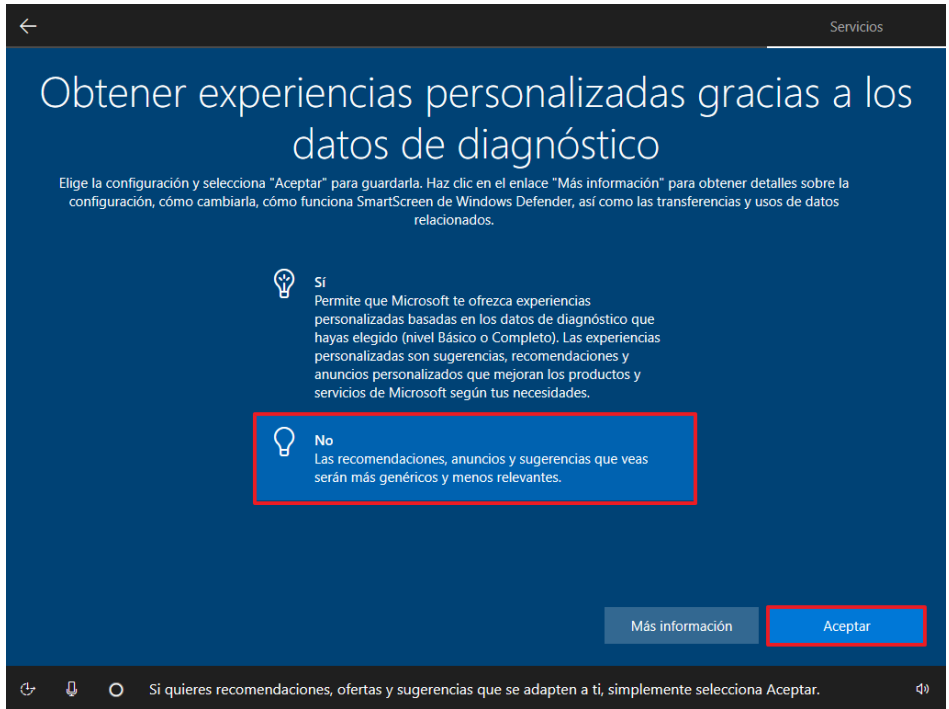
Paso	Descripción
110.	En la ventana “Cuenta”, introduzca un nombre de usuario (por ejemplo "Admin") que se creará con permisos de administrador local. Pulse “Siguiente” para continuar.  Nota: Deberá elegir un nombre de usuario adecuado para su entorno. Los nombres aquí indicados sólo se proporcionan a modo de ejemplo.
111.	Introduzca una contraseña para el usuario administrador local y pulse “Siguiente”. 

Paso	Descripción
112.	Introduzca nuevamente la contraseña y pulse “Siguiente”. 
113.	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.

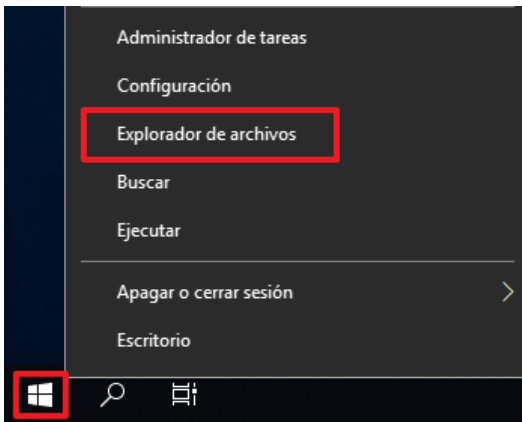
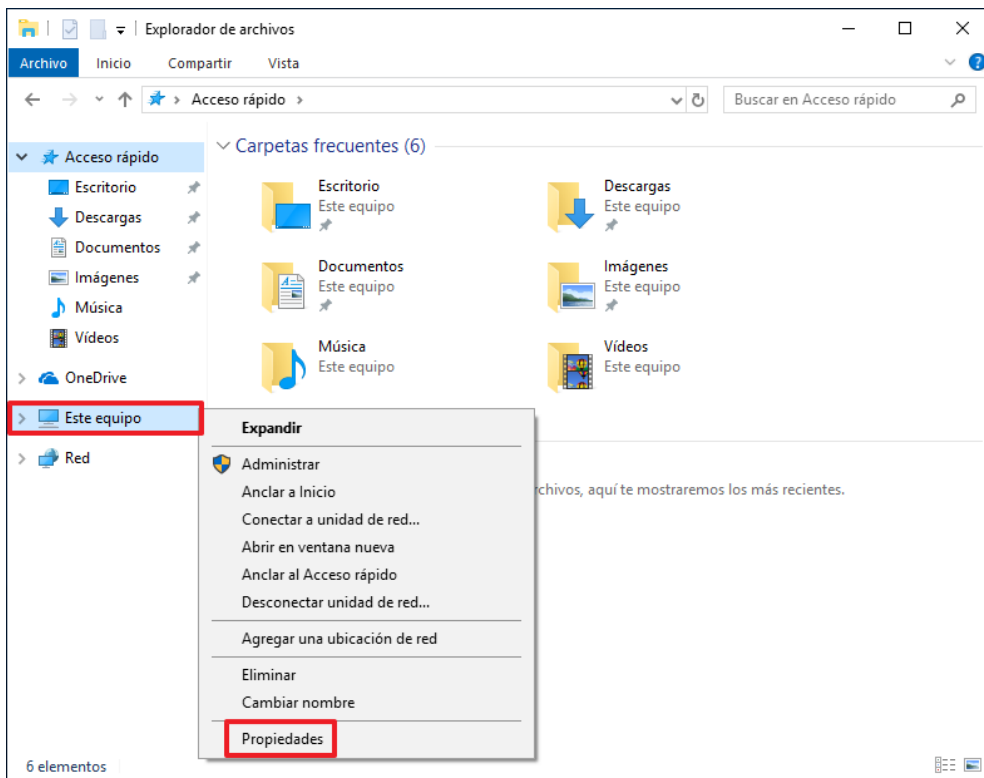
Paso	Descripción
114.	Pulse “Rechazar” para no dar permisos al asistente personal “Cortana” para que recopile información. 
115.	Pulse “No” para desactivar el historial de actividad. 

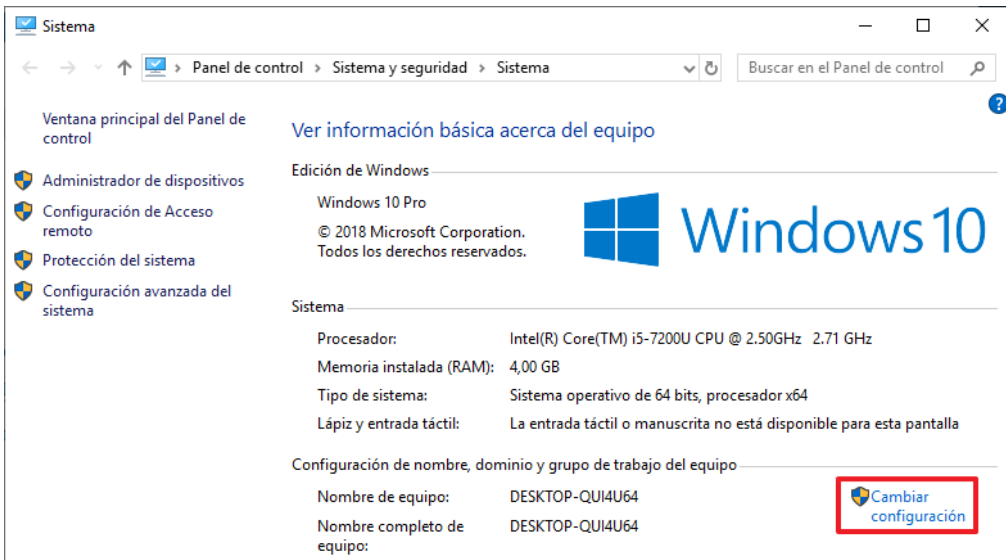
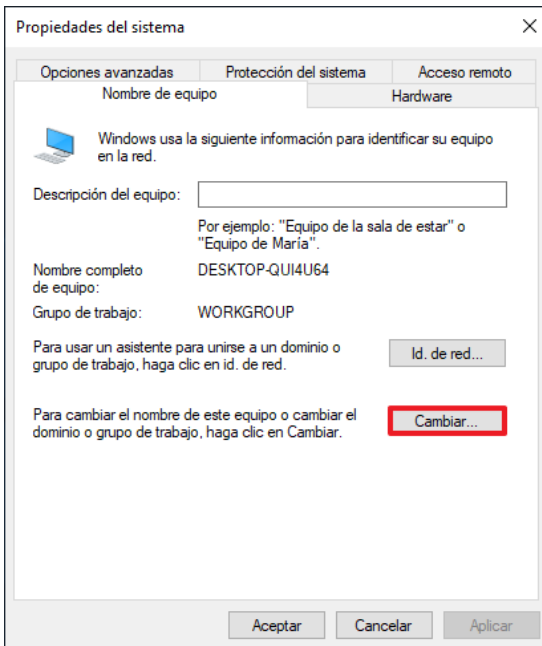
Paso	Descripción
116.	Seleccione “No” para no usar el reconocimiento de voz en línea y pulse “Aceptar”. 
117.	Seleccione “No” para impedir que las aplicaciones usen la ubicación y pulse “Aceptar”. 

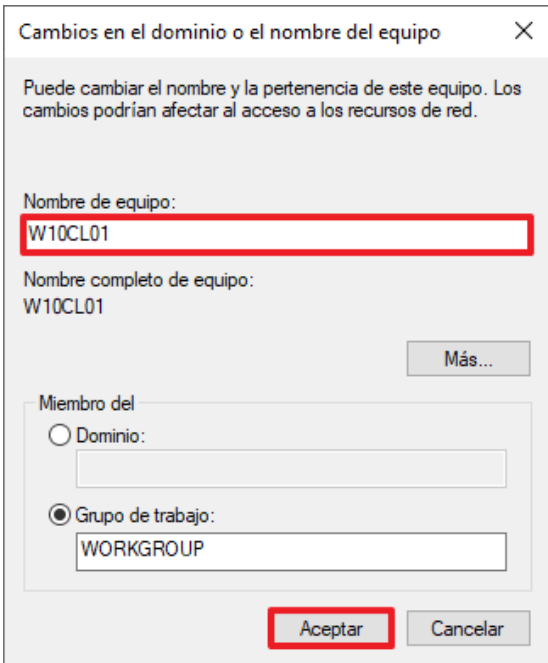
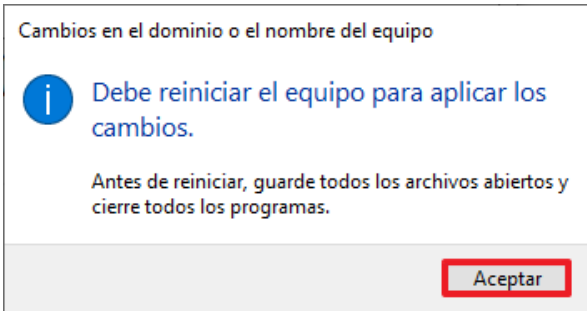
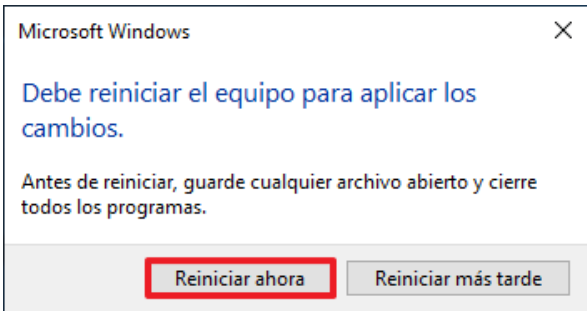
Paso	Descripción
118.	Seleccione “No” para desactivar la funcionalidad de “Encontrar mi dispositivo”. Pulse “Aceptar” para continuar. 
119.	Seleccione la opción “Básico” y pulse “Aceptar”.  Nota: Más adelante se impedirá toda comunicación con los servidores de Windows y se desactiva la telemetría.

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

Paso	Descripción
122.	Seleccione “No” para impedir que las aplicaciones usen el identificador de publicidad. Pulse “Aceptar” para continuar.
123.	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
124.	En la barra de tareas, pulse con el botón derecho sobre “Inicio” y seleccione “Explorador de archivos”. 
125.	En el “Explorador de archivos” pulse con el botón derecho del ratón sobre “Este equipo” y seleccione “Propiedades”. 

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

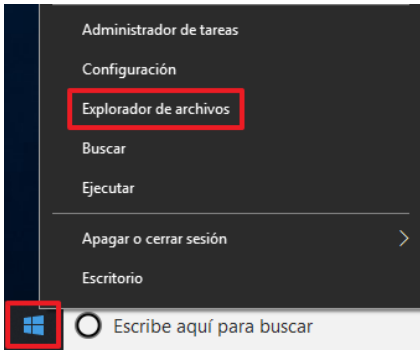
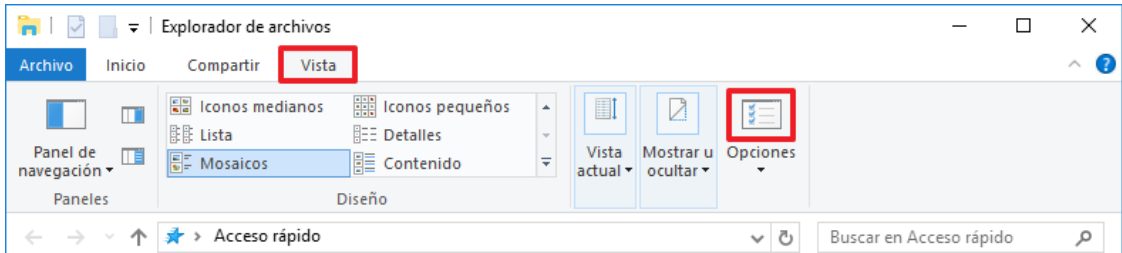
Paso	Descripción
128.	Establezca un nombre de equipo y pulse “Aceptar”.  Nota: En el ejemplo, el equipo se denomina “W10CL01”. Deberá ser el mismo nombre que le asignó en la unidad organizativa “Equipos Windows 10” del controlador de dominio, que le asignó durante la realización del apartado “1 PREPARACIÓN DEL DOMINIO”.
129.	El sistema deberá reiniciar para guardar los cambios. Pulse “Aceptar” en la ventana de “Cambios en el dominio o el nombre de equipo”. 
130.	Pulse sobre “Cerrar” en “Propiedades del sistema” y “Reiniciar ahora” para que se reinicie el equipo y hagan efecto los cambios. 

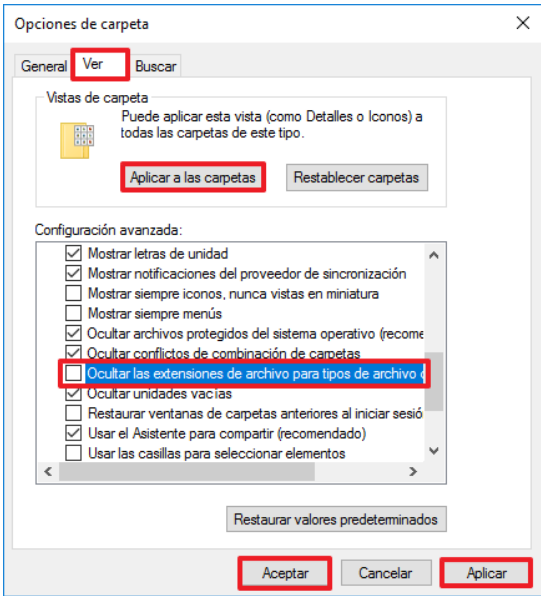
3. CONFIGURACIÓN DE SEGURIDAD MS WINDOWS 10

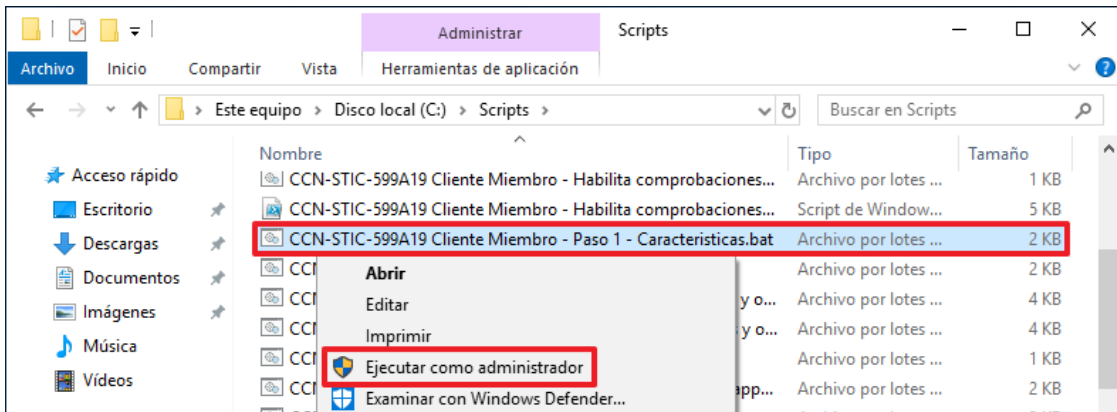
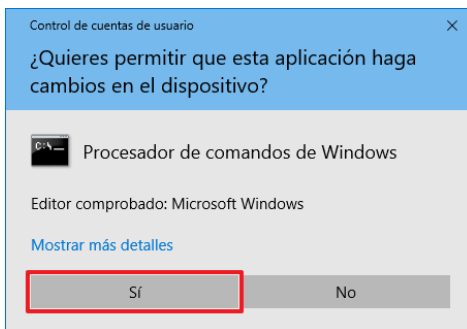
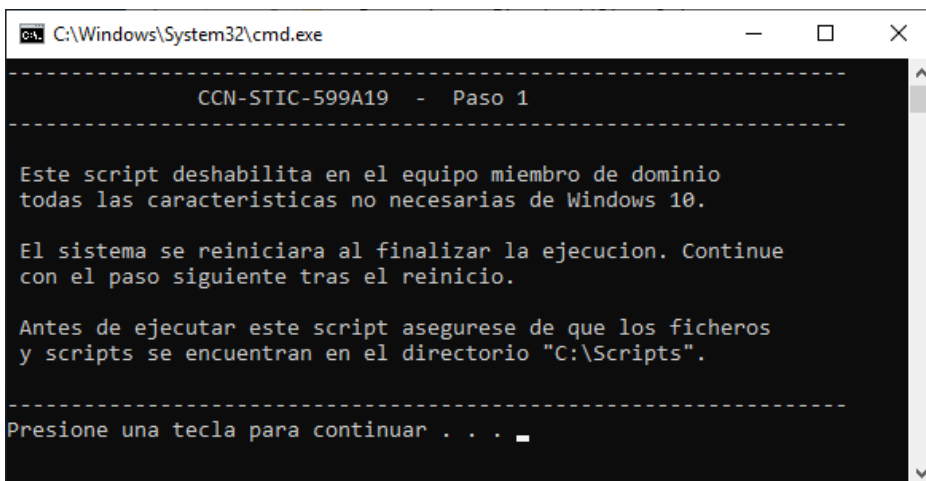
Con el sistema operativo instalado, se procederá a configurar el equipo.

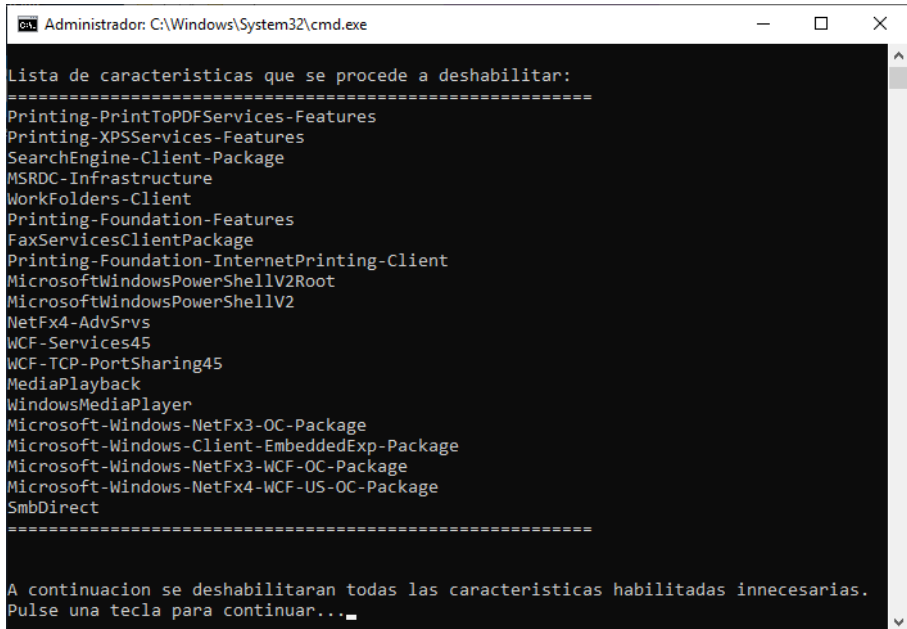
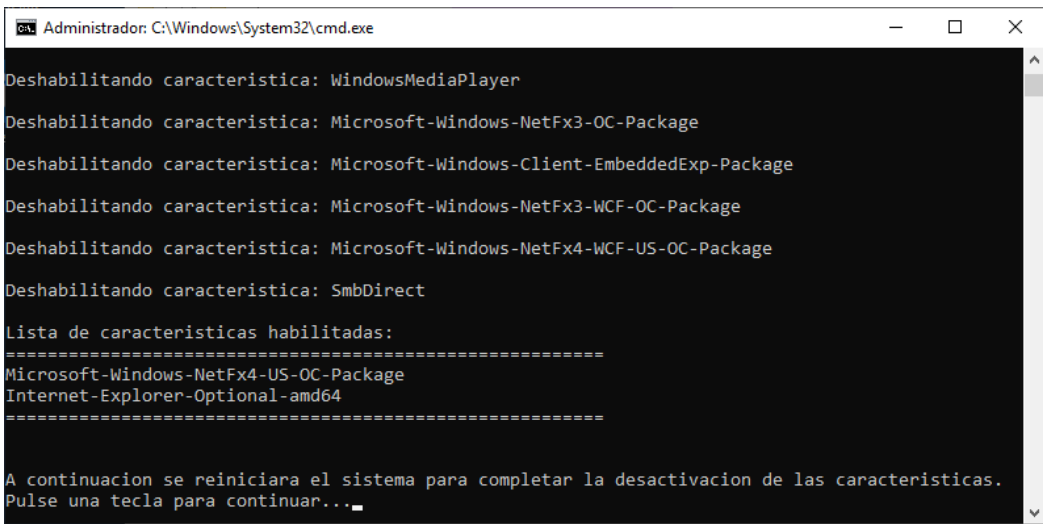
Nota: En este punto es conveniente recordar que, aunque en esta guía paso a paso no se dedica ningún apartado concreto a ello, será necesario instalar las actualizaciones de seguridad disponibles y realizar la activación de Windows en el equipo.

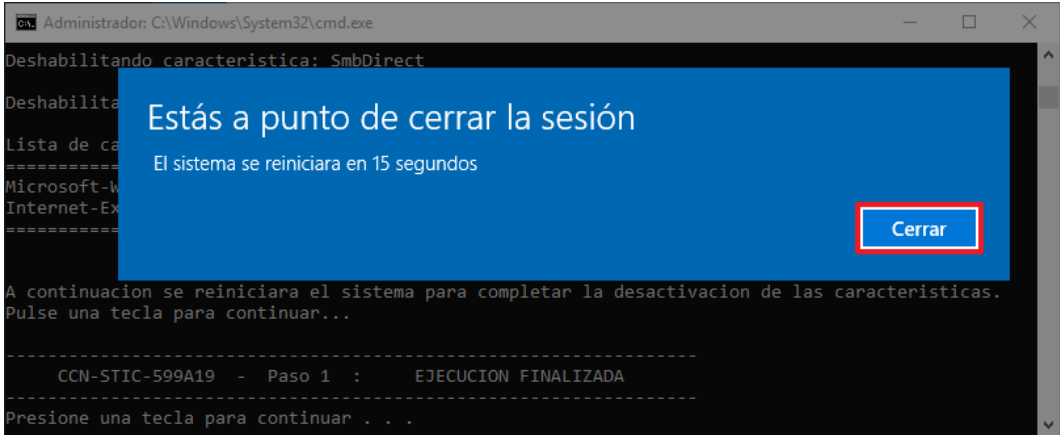
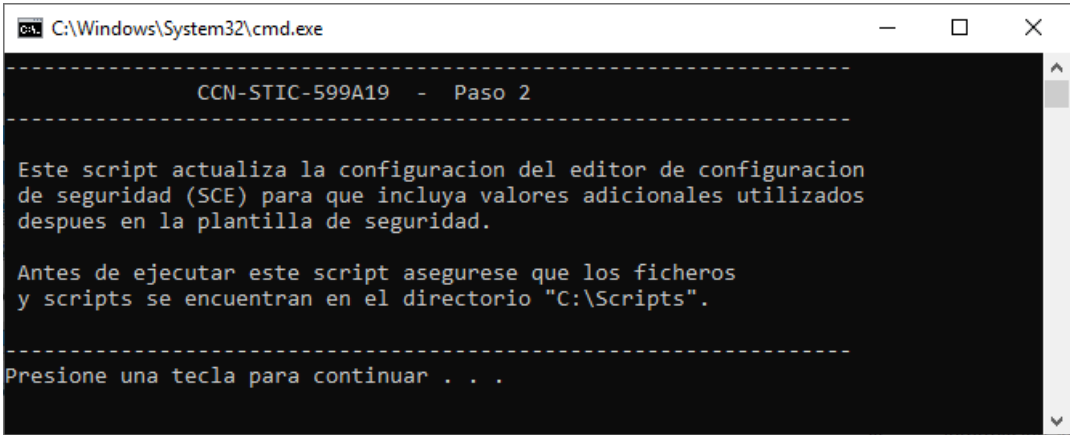
Una vez preparadas las unidades organizativas "Equipos Windows 10" y "Usuarios Windows 10", y creada en Active Directory la cuenta de equipo para el equipo que está asegurando, y para el usuario que lo utilizará, según se ha descrito en pasos anteriores, realice los siguientes pasos en el equipo cliente que está asegurando, para unirlo al dominio y aplicarle la configuración recomendada en esta guía.

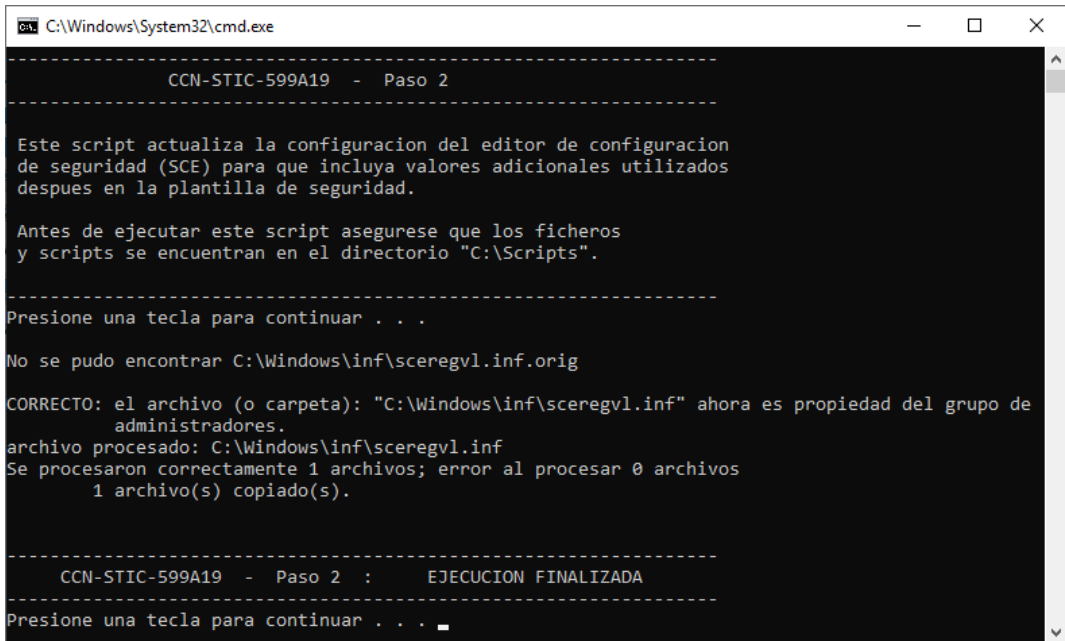
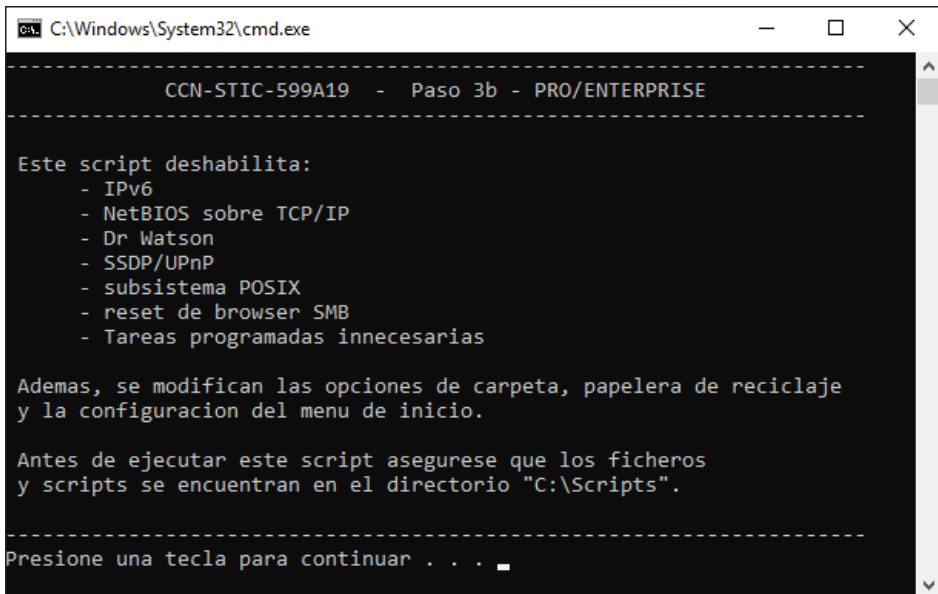
Paso	Descripción
131.	Inicie sesión en el equipo Windows 10 que está asegurando, con una cuenta con permisos de administrador local (por ejemplo "admin", si ese fue el nombre de usuario administrador que proporcionó durante la instalación).
132.	Cree el directorio "Scripts" en la unidad "C:\".
133.	Copie los ficheros asociados a esta guía en el directorio "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". 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.
134.	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". 
135.	En el "Explorador de archivos" pulse sobre la pestaña "Vista" del menú superior y seleccione el icono de "Opciones". 

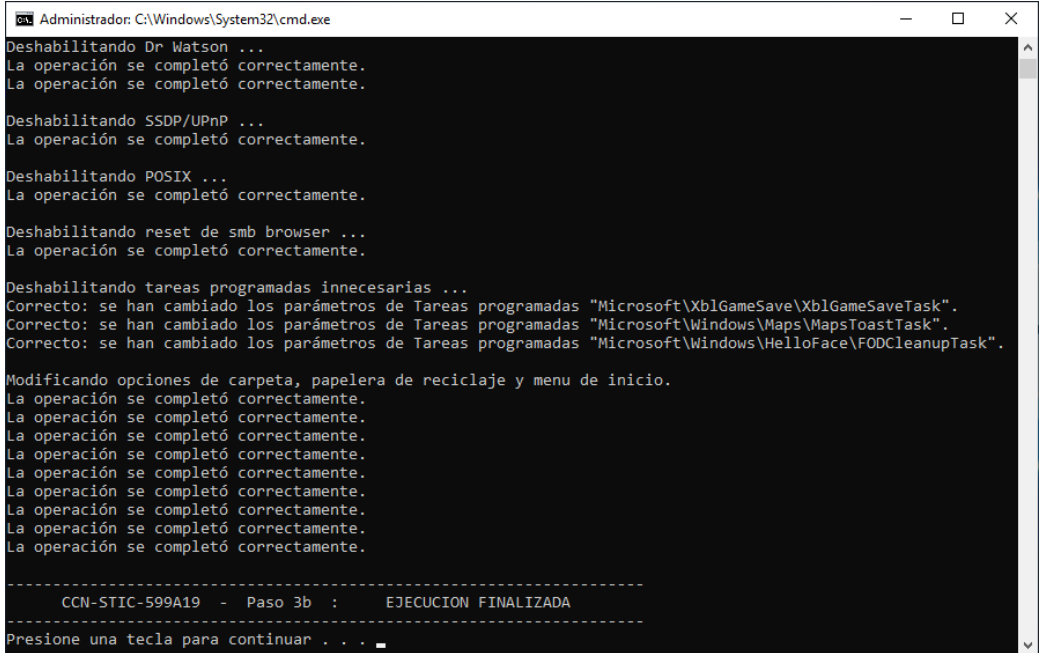
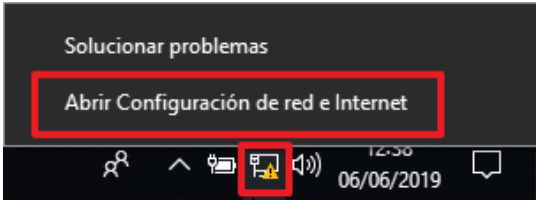
Paso	Descripción
136.	En “Opciones de carpeta” sitúese en la pestaña “Ver” y en el campo “Configuración avanzada” localice y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. Pulse primero sobre el botón “Aplicar”, después sobre “Aplicar a las carpetas” (Pulse “Sí” ante el mensaje de confirmación) y, por último, pulse “Aceptar”. 
137.	Compruebe que en el directorio “C:\Scripts” se encuentran al menos los siguientes directorios y ficheros: – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.ps1 – CCN-STIC-599A19 Cliente Miembro - Paso 1 - Caracteristicas.bat – CCN-STIC-599A19 Cliente Miembro - Paso 2 - SCE.bat – CCN-STIC-599A19 Cliente Miembro - Paso 3b - IPv6 netbios y otros - PRO.bat – CCN-STIC-599A19 Cliente Miembro - Paso 4 - Firewall.bat – CCN-STIC-599A19 Cliente Miembro - Paso 5b - Deshabilita Appx - PRO.bat – CCN-STIC-599A19 Cliente Miembro.wfw – CCN-STIC-599A19_Deshabilita_NetBIOS_sobre_TCPIP.ps1 – CCN-STIC-599A19_Desinstala_Appx_LTSC.ps1 – CCN-STIC-599A19_Desinstala_caracteristicas.ps1 – CCN-STIC-599A19_No_IPv6.reg – drwatson.reg – posix.reg – refusereset.reg – scereglv.inf – ssdp.reg – Start_Layout.xml

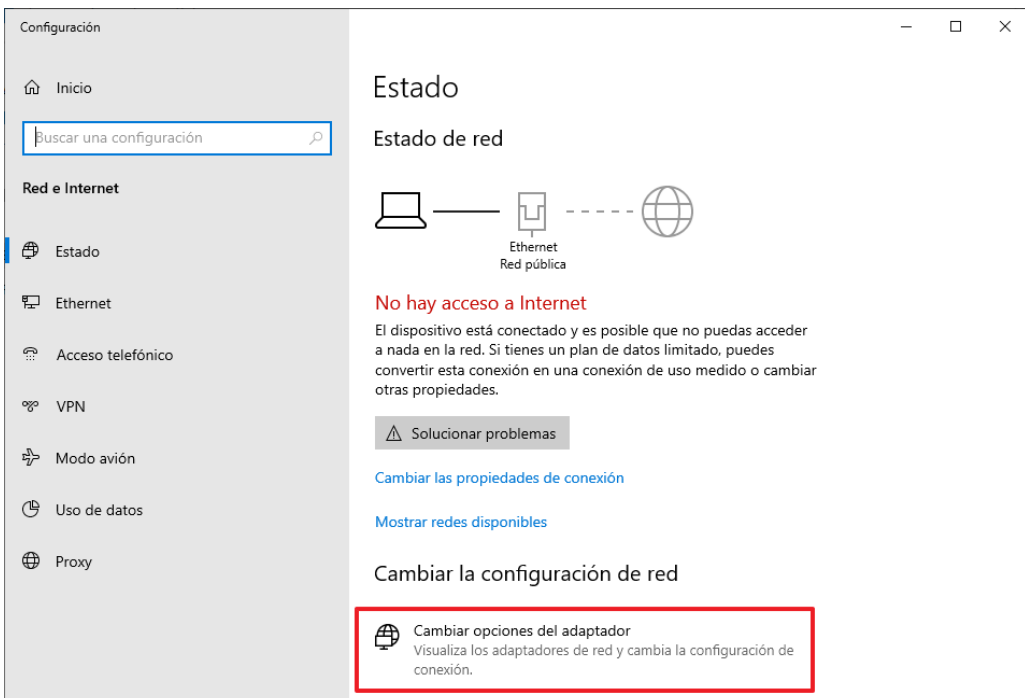
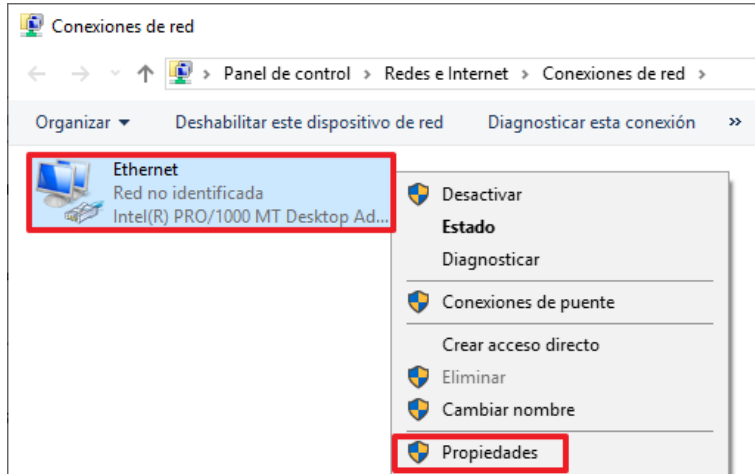
Paso	Descripción
138.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 1 - Características.bat". Para ello, visualice la carpeta "C:\Scripts" en el explorador de Windows, marque con el botón derecho el script y seleccione la opción "Ejecutar como administrador" del menú contextual.  Nota: Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
139.	Pulse "Sí" en la ventana de "Control de cuentas de usuario". 
140.	Este script deshabilitará todas las características opcionales que se encuentren habilitadas en el equipo. Pulse una tecla para continuar el proceso. 

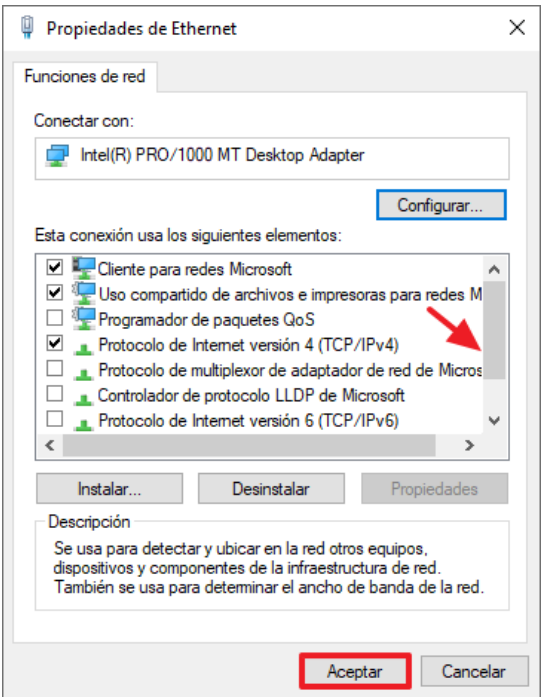
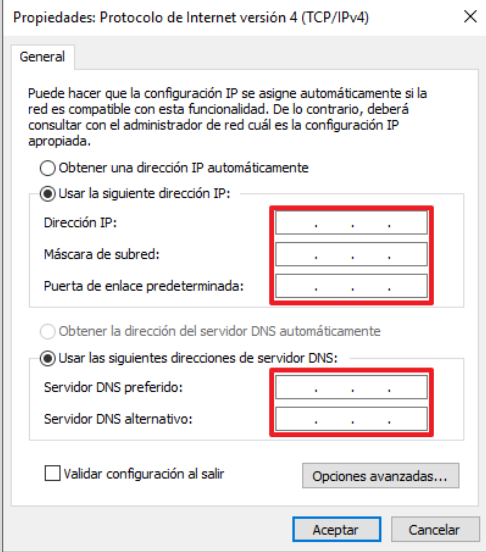
Paso	Descripción
141.	El sistema mostrará una lista de las características instaladas que no son necesarias y que deberán ser eliminadas. Pulse una tecla para continuar con el proceso de eliminación de las características. 
142.	Una vez desinstaladas las características innecesarias compruebe que únicamente 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.

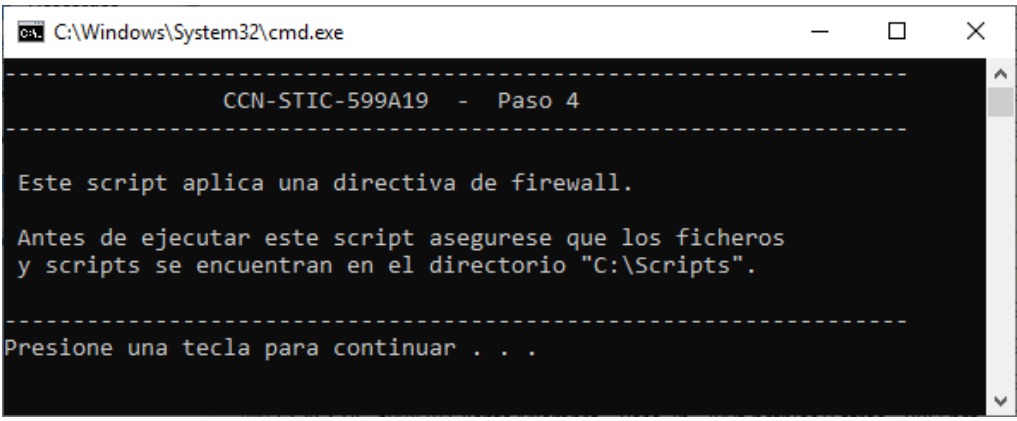
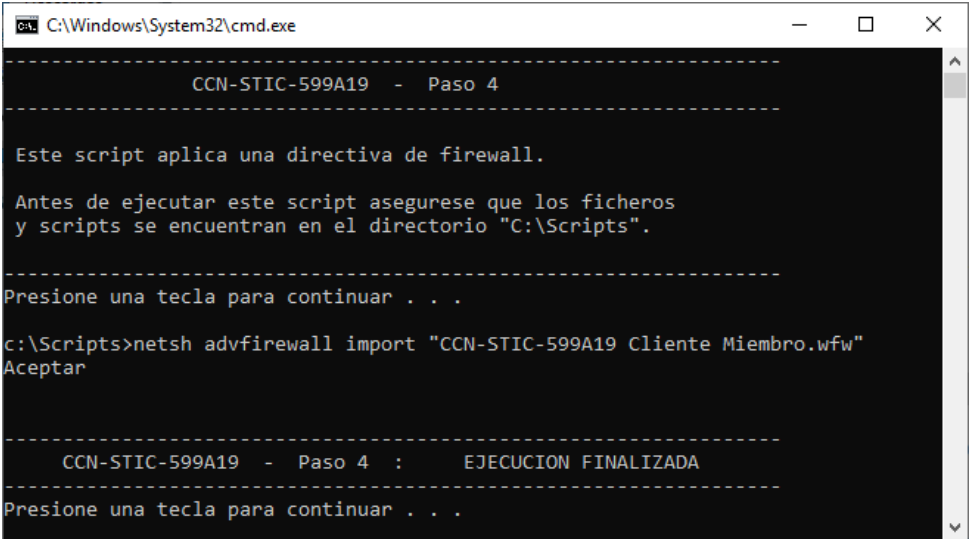
Paso	Descripción
143.	Será necesario que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. Al finalizar la ejecución, se reiniciará automáticamente el sistema. Pulse “Cerrar” en el mensaje de confirmación y cuando el sistema se inicie, continúe con el siguiente paso. 
144.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - 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. 

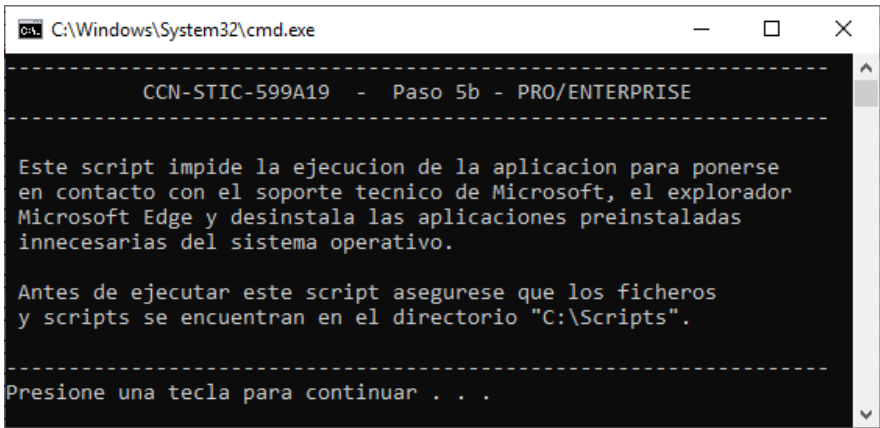
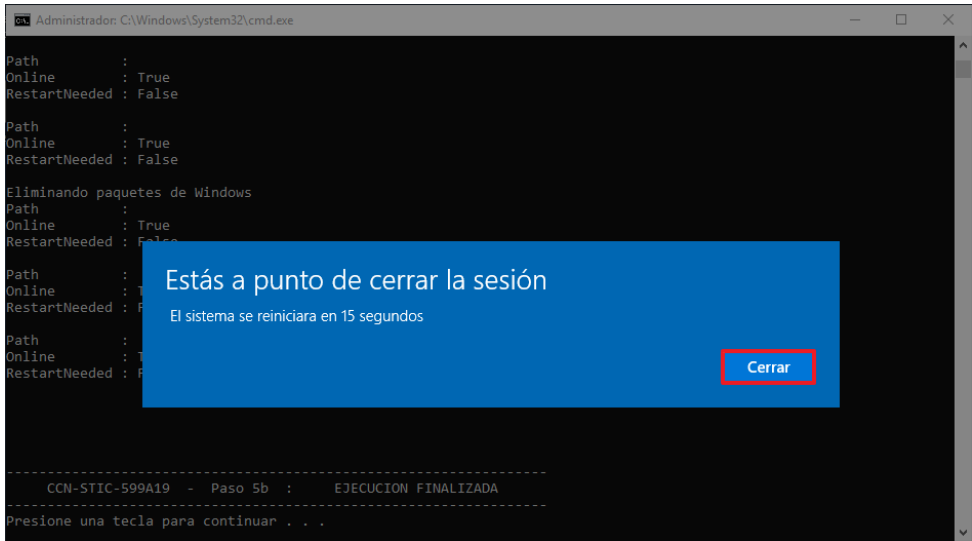
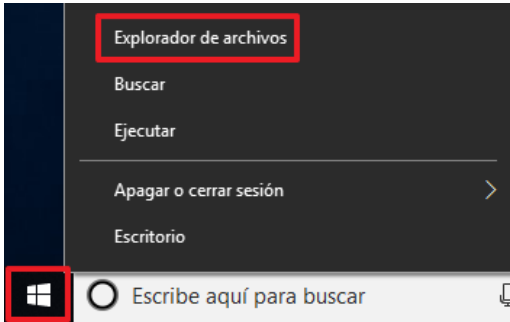
Paso	Descripción
145.	Pulse una tecla de nuevo para finalizar el proceso.  Nota: Este script actualiza la configuración de SCE (editor de configuración de seguridad) para que incluya valores adicionales. Si sale el aviso "No se pudo encontrar "C:\Windows\inf\sceregvl.inf.orig", este aviso se puede ignorar. Sólo se debe a que no se encontró una copia de seguridad anterior del fichero "sceregvl.inf". No representa ningún problema y se puede continuar con el siguiente paso.
146.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 3b – Ipv6 netbios y otros - PRO.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 

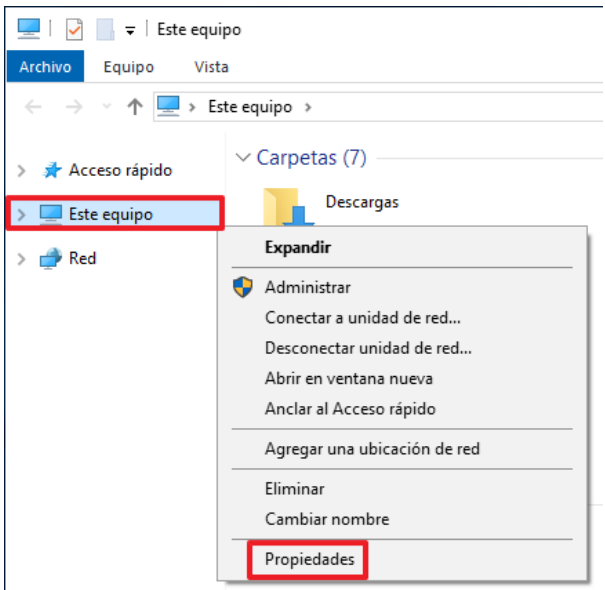
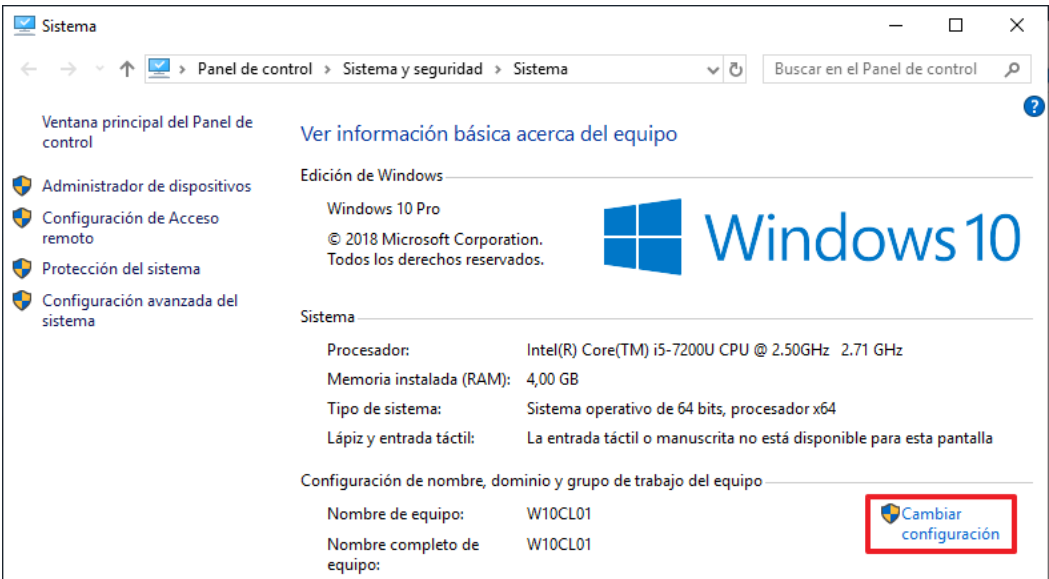
Paso	Descripción
147.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 
148.	A continuación, en la barra de tareas, localice el icono de conexiones de red y pulsando con el botón derecho del ratón sobre él seleccione “Abrir Configuración de red e Internet”. 

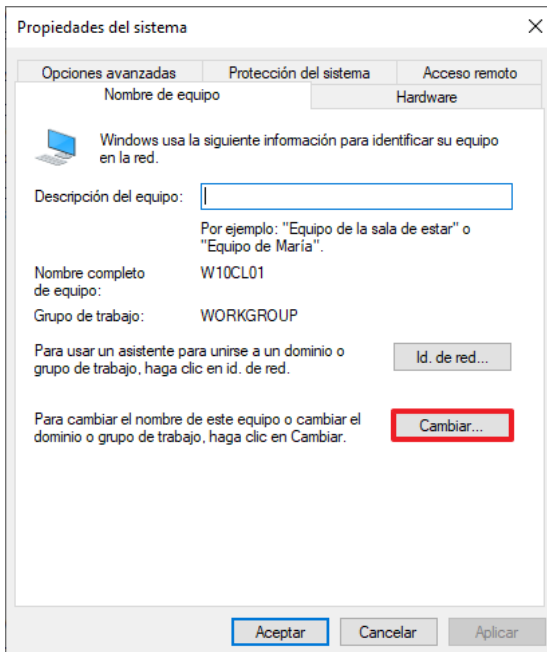
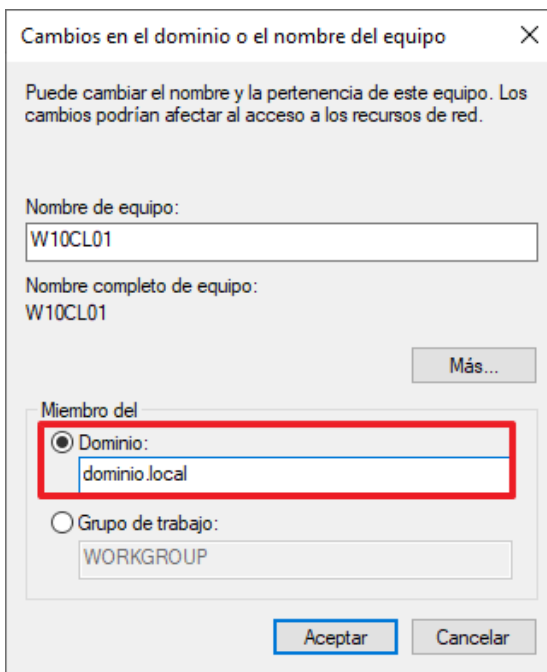
Paso	Descripción
149.	En la ventana de configuración seleccione la opción “Cambiar opciones del adaptador”. 
150.	Pulse con el botón derecho sobre el adaptador de red y seleccione “Propiedades”. 

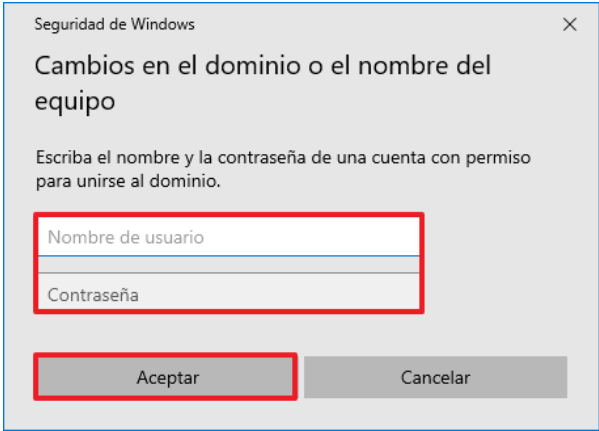
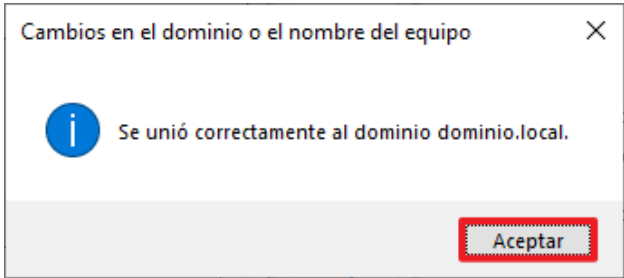
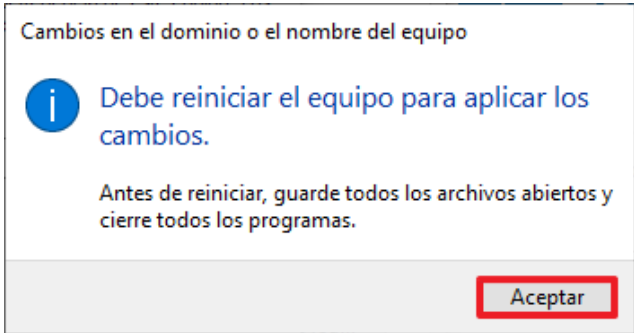
Paso	Descripción
151.	En la ventana “Propiedades de Ethernet” de las diferentes conexiones de red, desmarque si están marcados todos los elementos excepto "Cliente para redes Microsoft", “Uso compartido de archivos e impresoras para redes Microsoft” y “Protocolo de Internet versión 4 (TCP/IPv4)” como se muestra en la siguiente figura.  Nota: Recuerde hacer uso de la barra lateral para mostrar y deshabilitar todos los elementos.
152.	Pulse el botón "Aceptar", para cerrar la ventana guardando los cambios. Nota: Si no lo hizo antes, configure correctamente los parámetros de red (Protocolo de Internet versión 4), especialmente la dirección IP del equipo, de la puerta de enlace predeterminada y del servidor de DNS, ya sean fijas o para obtener automáticamente por DHCP, de modo que el equipo pueda posteriormente contactar con un controlador del dominio al que se unirá. 

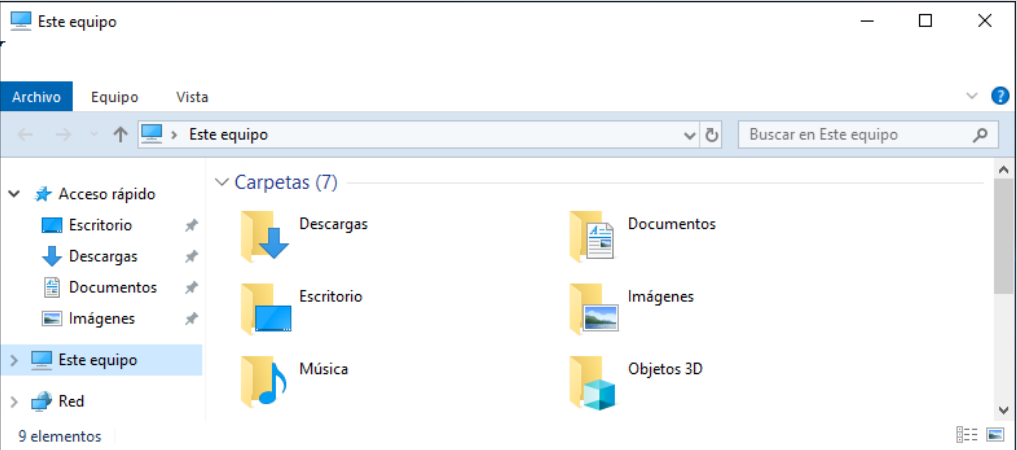
Paso	Descripción
153.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 4 – firewall.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso.  Nota: A pesar de que en pasos anteriores se configuró la directiva de Firewall a través del "Administrador de directivas de grupo" y a través de la política "CCN-STIC-599A19 Windows 10 - Equipos", en este punto se realiza localmente la importación de algunas directivas específicas de Windows 10 que no son compatibles con el "Firewall de Windows con seguridad avanzada de Windows Server 2016. De modo que las reglas de entrada y salida queden correcta y completamente configuradas.
154.	Una vez finalizado el proceso pulse, de nuevo, una tecla para continuar. 

Paso	Descripción
155.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Paso 5b – Deshabilita appx - PRO.bat" y, una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. 
156.	El sistema se reiniciará al finalizar la ejecución del script. Pulse “Cerrar” en la ventana emergente. 
157.	A continuación, se unirá el equipo al dominio. Para ello inicie sesión en el equipo, en la barra de tareas, pulse sobre “Inicio” con el botón derecho y seleccione “Explorador de archivos”. 

Paso	Descripción
158.	En el “Explorador de archivos” pulse con el botón derecho del ratón sobre “Este equipo” y seleccione “Propiedades”. 
159.	Localice en la ventana “Ver información básica acerca del equipo” el apartado “Configuración de nombre, dominio y grupo de trabajo del equipo” y pulse sobre “Cambiar configuración” 

Paso	Descripción
160.	En “Propiedades del sistema”, en la pestaña “Nombre de equipo”, pulse sobre “Cambiar”. 
161.	Marque la opción “Dominio”, introduzca el nombre del dominio y pulse “Aceptar”.  Nota: En el ejemplo, el dominio se denomina “dominio.local”.

Paso	Descripción
162.	Introduzca credenciales de administrador del dominio cuando el sistema se lo solicite y pulse “Aceptar” 
163.	Pulse “Aceptar” en el mensaje de confirmación de unión al dominio. 
164.	El sistema deberá reiniciar para guardar los cambios. Pulse “Aceptar” en la ventana de “Cambios en el dominio o el nombre de equipo”. 
165.	Pulse “Cerrar” en “Propiedades del sistema” y “Reiniciar ahora” para que se reinicie el equipo y hagan efecto los cambios.

Paso	Descripción
166.	Una vez haya reiniciado el sistema, inicie sesión con una cuenta con privilegios de administración en el dominio. Nota: Es posible que en el primer inicio de sesión de un usuario en el equipo securizado, el sistema operativo contenga errores visuales en el explorador de archivos. Si es el caso, reinicie el equipo nuevamente. 
167.	Deberá aplicar este momento la guía CCN-STIC-520 – Internet Explorer 11. Para ello, lleve a cabo la implementación del Anexo A, del paso 1 al 51. No es necesario que continúe con el resto de pasos. El resto de pasos de dicho anexo instalaría Internet Explorer 11 en el cliente y esto no es necesario ya que Internet Explorer 11 es el navegador existente en Windows 10. Nota: Tenga en cuenta que se ha restringido el acceso a la aplicación Microsoft Edge, por lo que no hay ningún navegador predeterminado establecido. Deberá establecer Internet Explorer como navegador predeterminado por cada usuario en el equipo que está securizando. Las GPO que se han implementado a través de la presente guía no incluyen plantillas administrativas de Internet Explorer. Por tanto, para poder hacer uso seguro de Internet Explorer 11 será necesario aplicar, adicionalmente, la guía CCN-STIC-520 – Internet Explorer 11.
168.	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 Microsoft Windows 10 Pro/Enterprise (versión 1809) sin opción de mantenimiento LTSC, que el equipo es un cliente miembro de un dominio Windows, que en los controladores del dominio al que pertenece se ha aplicado la configuración expuesta en la guía CCN-STIC-570A (controladores Microsoft Windows Server 2016), y que en el equipo cliente se ha aplicado la configuración expuesta en la presente guía.

Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador del dominio, con una cuenta de usuario que tenga permisos de administración en el dominio. En esa primera fase se realizarán las comprobaciones comunes a todos los equipos cliente Windows 10 (versión 1809) miembros del dominio.

Posteriormente, deberá realizar una serie de comprobaciones en el propio equipo cliente miembro del dominio. Para ello, necesitará ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario del dominio que sea administrador local del servidor y que sea miembro del grupo global "Usuarios de shells". Por ejemplo, los usuarios del grupo "Admins. del dominio" cumplirán ambas condiciones.

Para poder verificar que la configuración de usuario, además de la configuración de equipo, está siendo aplicada correctamente en el equipo cliente Windows 10, necesitará que el usuario con el que realice las comprobaciones resida, aunque sea temporalmente, en la siguiente unidad organizativa de Active Directory.

"<Nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10"

Nota: 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).

1. COMPROBACIONES EN SERVIDOR CONTROLADOR DEL DOMINIO

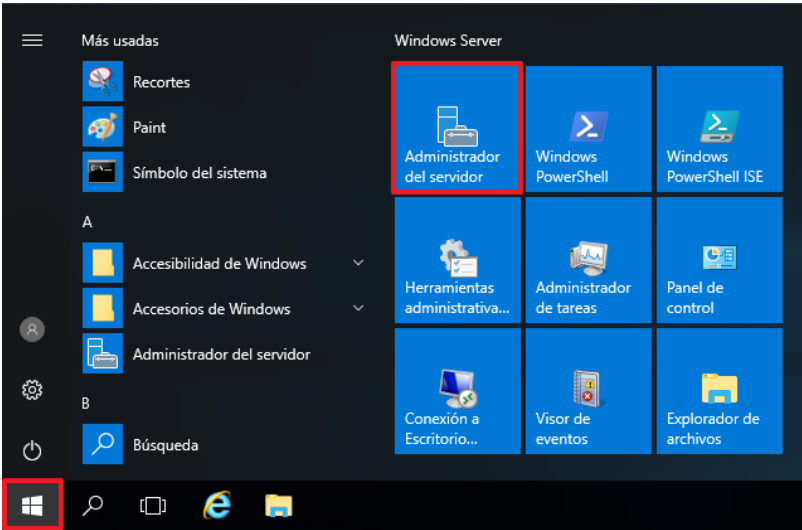
Para realizar algunas de las comprobaciones necesitará ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán en el controlador de dominio son las siguientes:

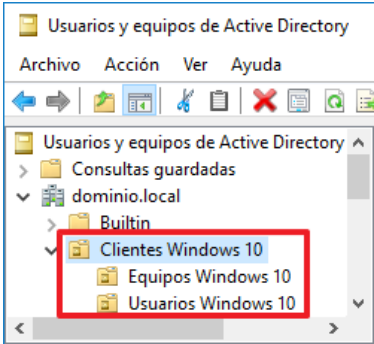
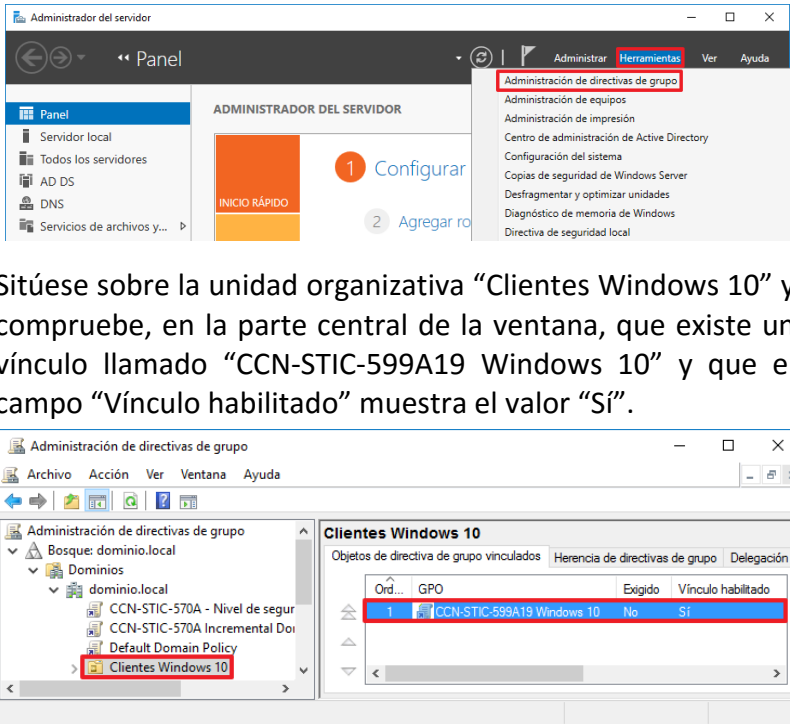
- a) Administrador del servidor
- b) Servicios de dominio de Active Directory
- c) Administración de directivas de grupo
- d) Editor de administración de directivas de grupo
- e) Usuarios y equipos de Active Directory

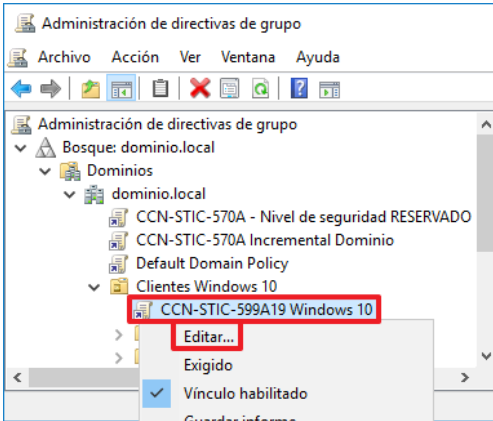
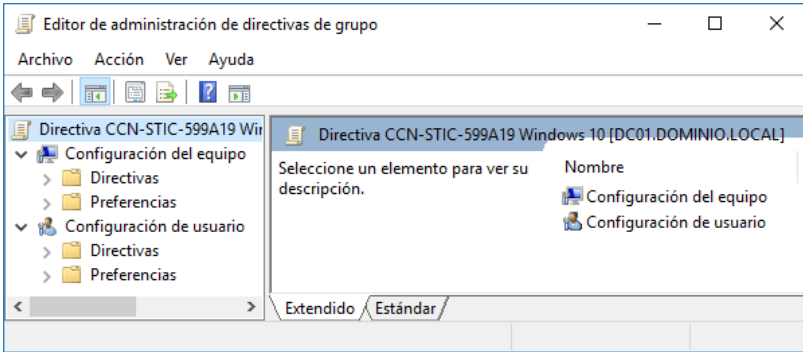
Ejecute los siguientes pasos en un controlador del dominio al que pertenece el equipo a comprobar:

Nota: Las configuraciones y capturas se han realizado a partir de un controlador de dominio Microsoft Windows Server 2016 al que se le ha aplicado la guía CCN-STIC-570A. Salvo que se especifique, los procedimientos y comprobaciones no varían con respecto a la guía CCN-STIC-560A.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio		Inicie sesión en el servidor, utilizando una cuenta de usuario perteneciente al grupo de administradores del dominio ("Admins. del dominio").

Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que están creadas las unidades organizativas necesarias		Ejecute el "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Introduzca las credenciales de un usuario con permisos de administración del dominio, pulse sobre el menú superior en "Herramientas" y seleccione "Usuarios y equipos de Active Directory". 

Comprobación	OK/NOK	Cómo hacerlo
		Despliegue los objetos y compruebe que bajo el objeto con el nombre del dominio existe una unidad organizativa llamada "Clientes Windows 10" y bajo ésta dos unidades organizativas, al mismo nivel, llamadas "Equipos Windows 10" y "Usuarios Windows 10", como se muestra en la siguiente figura.  Nota: Si en su entorno las unidades organizativas elegidas para albergar las configuraciones de equipos cliente miembro Windows 10 fueran otras, deberá sustituir en esta lista de comprobación todas las referencias a dichas unidades organizativas por referencias a las unidades organizativas de su entorno.
3. Verifique que está creada y asignada correctamente la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando, de nuevo, la herramienta "Administrador del servidor" seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo".  Sitúese sobre la unidad organizativa "Clientes Windows 10" y compruebe, en la parte central de la ventana, que existe un vínculo llamado "CCN-STIC-599A19 Windows 10" y que el campo "Vínculo habilitado" muestra el valor "Sí".

Comprobación	OK/NOK	Cómo hacerlo
4. Abra la directiva GPO "CCN-STIC-599A19 Windows 10" en el editor de administración de directivas de grupo		Marque con el botón derecho el vínculo de la GPO "CCN-STIC-599A19 Windows 10" situado en el siguiente contenedor de la herramienta "Administrador del servidor": "Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>" En el menú contextual que aparecerá, seleccione la opción "Editar...", como se muestra en la figura.  Con ello se abrirá el Editor de administración de directivas de grupo, mostrando la configuración de la GPO "CCN-STIC-599A19 Windows 10".  En los próximos pasos y hasta que se indique lo contrario, verificará la configuración de este GPO utilizando esta ventana del editor de administración de directivas de grupo
5. Verifique los valores de la directiva de auditoría cuenta de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) CCN-STIC-599A19 Windows 10 tiene los siguientes valores dentro de las directivas de auditoría: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → 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
6. Verifique los valores de Asignación de derechos de usuario de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de las directivas de asignación de derechos de usuario: Nota: En las cuentas de dominio, resaltadas con fondo gris en la siguiente tabla, aparecerá su nombre de dominio en lugar de "DOMINIO". Además, tenga en cuenta que tanto la cuenta Administrador como la cuenta Invitado estarán renombradas, y aparecerán con su nuevo nombre en el editor. "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → 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		DOMINIO\Auditores, 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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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	
Tener acceso a este equipo desde la red		Administradores, Usuarios	
Tomar posesión de archivos y otros objetos		Administradores	
7. Verifique los valores de Opciones de seguridad de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de las opciones de seguridad: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → 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 ⁵ \CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\ServerApplications, Software\Microsoft\Windows NT\CurrentVersion	
Acceso a redes: rutas y subrutas del Registro accesibles remotamente		System ⁶ \CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, 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: 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	

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
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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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)	
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 con ellas	
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) <i>Equivale a:</i> <i>Usuarios autenticados: Permitir Acceso local y Acceso remoto</i>	
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) <i>Equivale a:</i> <i>Usuarios autenticados: Permitir Ejecución local y Activación local.</i> <i>Administradores: Permitir Ejecución local, Ejecución remota, Activación local y Activación remota.</i>	
Dispositivos: impedir que los usuarios instalen controladores de impresora		Habilitada	
Dispositivos: permitir desacoplamiento sin tener que iniciar sesión		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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: 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: 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	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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: 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	
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem		Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo	
Directiva		Valor	OK/NOK
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	
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 los valores del registro de eventos de la directiva (GPO) CCN-STIC-599A19 Windows 10		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Registro de eventos: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro de eventos"	
		Directiva	Valor
		Método de retención del registro de la aplicación	Según se necesite
		Método de retención del registro de seguridad	Según se necesite
		Método de retención del registro del sistema	Según se necesite
		Tamaño máximo del registro de la aplicación	32768 kilobytes
		Tamaño máximo del registro de seguridad	163840 kilobytes
		Tamaño máximo del registro del sistema	32768 kilobytes
9. Verifique los valores de Grupos restringidos de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Grupos restringidos"	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Usuarios avanzados	Vacío (este grupo no debe contener miembros)	
		Nota: En lugar del nombre puede aparecer el identificador numérico "*S-1-5-32-547" .		
		Usuarios de escritorio remoto	Vacío (este grupo no debe contener miembros)	
10. Verifique los valores de los servicios del sistema restringidos de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Servicios del sistema: Nota: 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 del editor de administración de directivas de grupo 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. "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
Administración de aplicaciones	AppMgmt	Deshabilitado	Configurado	
Administración de autenticación de Xbox Live	XblAuthManager	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 acceso remoto	RasMan	Deshabilitado	Configurado		
Administrador de conexiones de Windows	Wcmsvc	Automático	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		
Agente de conexión de red	NcbService	Manual	Configurado		
Agente de detección en segundo plano de DevQuery	DevQueryBroker	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 de NetBIOS sobre TCP/IP	lmhosts	Automático	Configurado		
Aplicación auxiliar IP	iphlpvc	Deshabilitado	Configurado		
Aplicación del sistema COM+	COMSysApp	Deshabilitado	Configurado		
Archivos sin conexión	CscService	Deshabilitado	Configurado		
Asignador de detección de topologías de nivel de vínculo	lltdsvc	Deshabilitado	Configurado		
Asignador de extremos de RPC	RpcEptMapper	Automático	Configurado		
Asistente para la conectividad de red	NcaSvc	Manual	Configurado		
ASP.NET State Service	aspnet_state	Deshabilitado	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		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Deshabilitado	Configurado		
BranchCache	PeerDistSvc	Deshabilitado	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CaptureService	CaptureService	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Carpetas de trabajo	workfoldersvc	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Deshabilitado	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Deshabilitado	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	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		
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	Deshabilitado	Configurado		
Configuración automática de WWAN	WwanSvc	Deshabilitado	Configurado		
Configuración de Escritorio remoto	SessionEnv	Deshabilitado	Configurado		
ConsentUX	ConsentUxUserSvc	Deshabilitado	Configurado		
Contenedor de Microsoft Passport	NgcCtnrSvc	Deshabilitado	Configurado		
Control parental	WpcMonSvc	Deshabilitado	Configurado		
Coordinador de transacciones distribuidas	MSDTC	Deshabilitado	Configurado		
Copias de seguridad de Windows	SDRSVC	Deshabilitado	Configurado		
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado		
Datos de contactos	PimIndexMaintenanceSvc	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Desencadenadores de Message Queue Server	MSMQTriggers	Deshabilitado	Configurado		
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado		
Detección SSDP	SSDPSRV	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		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
dmwappushsvc	dmwappushservice	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		
Hora de Windows	W32Time	Automático	Configurado		
Host de proveedor de detección de función	fdPHost	Deshabilitado	Configurado		
Host de sistema de diagnóstico	WdiSystemHost	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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	Deshabilitado	Configurado		
OpenSSH Authentication Agent	ssh-agent	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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	Manual	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	wcncsvc	Deshabilitado	Configurado		
Registro de eventos de Windows	EventLog	Automático	Configurado		
Registro remoto	RemoteRegistry	Deshabilitado	Configurado		
Registros y alertas de rendimiento	pla	Deshabilitado	Configurado		
Servicio Administrador de funcionalidad de acceso	camsvc	Manual	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio Asistente para la compatibilidad de programas	PcaSvc	Manual	Configurado	
Servicio AssignedAccessManager	AssignedAccessManagerSvc	Deshabilitado	Configurado	
Servicio auxiliar de host para aplicaciones	AppHostSvc	Deshabilitado	Configurado	
Servicio AVCTP	BthAvctpSvc	Deshabilitado	Configurado	
Servicio biométrico de Windows	WbioSrv	Deshabilitado	Configurado	
Servicio Cifrado de unidad BitLocker	BDESVC	Deshabilitado	Configurado	
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	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 administración de Windows	WManSvc	Deshabilitado	Configurado	
Servicio de administración IIS	IISADMIN	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 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		
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	Deshabilitado	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 Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	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 Protección contra amenazas avanzada de Windows Defender	Sense	Deshabilitado	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Deshabilitado	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	Deshabilitado	Configurado	
Servicio de publicación World Wide Web	W3SVC	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 host	hns	Deshabilitado	Configurado	
Servicio de red de Xbox Live	XboxNetApiSvc	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	

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	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 Windows Defender	WinDefend	Deshabilitado	Configurado		
Servicio de Windows Insider	wisvc	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 FrameServer de la Cámara de Windows	FrameServer	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio FTP de Microsoft	ftpsvc	Deshabilitado	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	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.standard.collector.service	Deshabilitado	Configurado	
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado	
Servicio SNMP	SNMP	Deshabilitado	Configurado	
Servicio telefónico	PhoneSvc	Deshabilitado	Configurado	
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado	
Servicio WAS (Windows Process Activation Service)	WAS	Deshabilitado	Configurado	
Servicios de cifrado	CryptSvc	Automático	Configurado	
Servicios de Escritorio remoto	TermService	Deshabilitado	Configurado	
Servicios simples de TCP/IP	simptcp	Deshabilitado	Configurado	
Servidor	LanmanServer	Deshabilitado	Configurado	
Servidor de roles de DS	DsRoleSvc	Deshabilitado	Configurado	
Shared PC Account Manager	shpamsvc	Deshabilitado	Configurado	
Sincronizar host	OneSyncSvc	Deshabilitado	Configurado	
Sistema de cifrado de archivos (EFS)	EFS	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	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	
11. Verifique los valores de Registro de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Registro: "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Registro"		

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer		Administradores: Control Total SYSTEM: Control Total Usuarios: Leer	
	MACHINE\SYSTEM\CurrentControlSet\Enum		Administradores: Control Total Usuarios autenticados: Leer	
12. Verifique los valores de Sistema de archivos de la directiva "CCN-STIC-599A19 Windows 10"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva (GPO) "CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de Sistema de archivos: Nota: Para verificar los permisos de cada fichero o carpeta deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar". "Directiva CCN-STIC-599A19 Windows 10 → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos"		
Archivo		Usuario	Permiso	OK/NOK
%Public%		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%SystemDrive%\		Administradores	Control Total	
		CREATOR OWNER	Permisos especiales ⁷	
		SYSTEM	Control Total	
		Usuarios	Leer	
%SystemDrive%\Users\Default		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%SystemRoot%\regedit.exe		Administradores	Control Total	
		SYSTEM	Control Total	

⁷ 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".

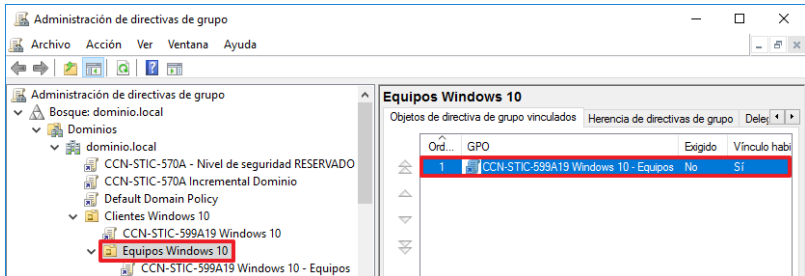
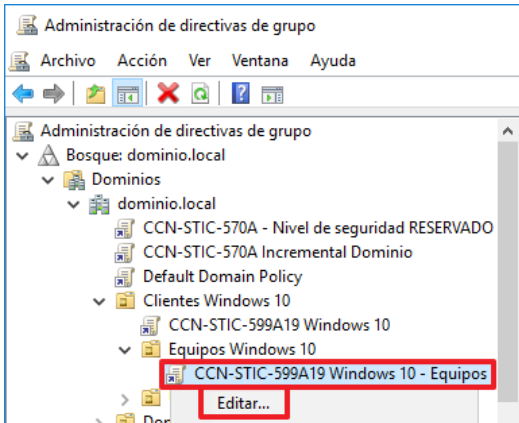
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\Registration	Administradores	Control Total		
	SYSTEM	Control Total		
	Usuarios	Leer y Ejecutar, Listar el contenido de la carpeta, Leer		
%SystemRoot%\security	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\arp.exe	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\clip.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%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\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		
%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		

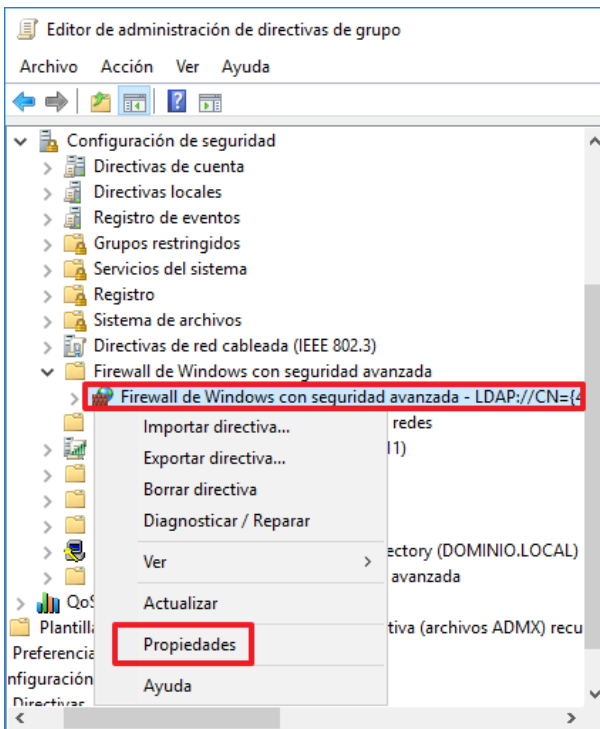
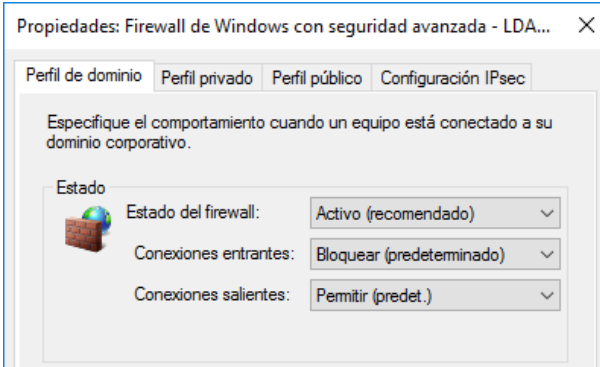
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\nbtstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net1.exe		Administradores	Control Total	
		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	
%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	

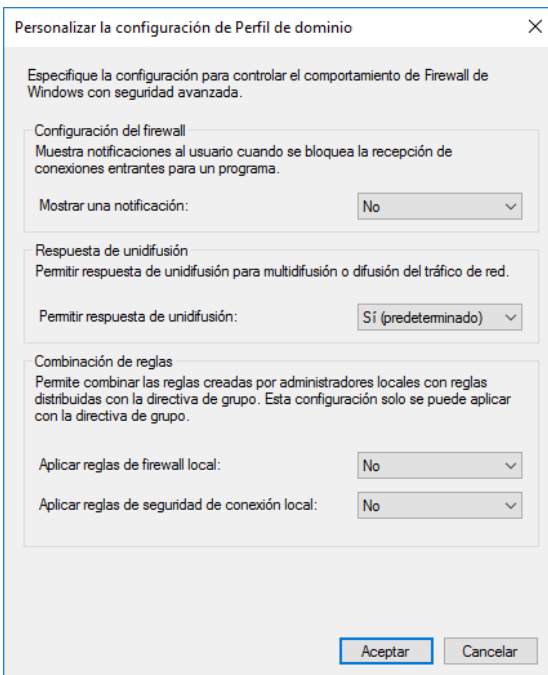
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\secedit.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\syskey.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\telnet.exe		Administradores	Control 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	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%\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	

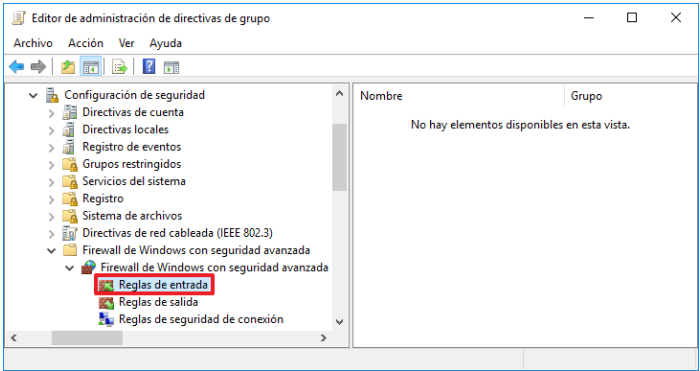
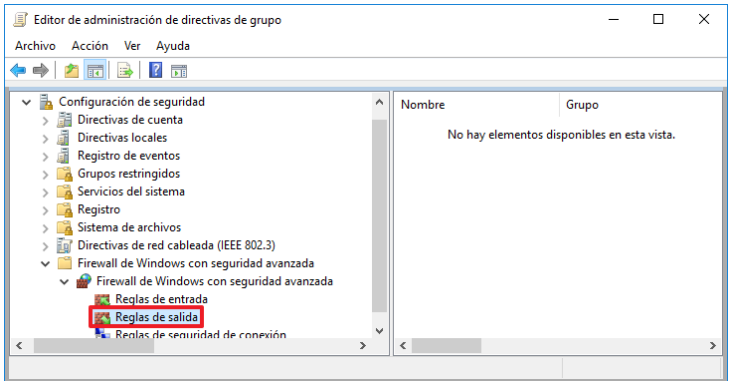
Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\cmd.exe	Administradores	Control Total	
	SYSTEM	Control Total	
	Usuarios de Shells	Leer y Ejecutar, Listar el contenido de la carpeta, Leer	
%SystemRoot%\syswow64\cscript.exe	Administradores	Control Total	
	SYSTEM	Control 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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\runonce.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\secedit.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\syskey.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\tracert.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%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\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\syskey.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\tracert.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%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		
%SystemRoot%\syswow64\wscript.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\syswow64\xcopy.exe	Administradores	Control Total		
	SYSTEM	Control Total		

Comprobación	OK/NOK	Cómo hacerlo
13. Finalice la comprobación de la directiva "CCN-STIC-599A19 Windows 10"		Cierre la ventana del "Editor de administración de directivas de grupo" que tenía abierta con la directiva "CCN-STIC-599A19 Windows 10"
14. Verifique que está creada y asignada correctamente la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		De nuevo en la consola de "Administración de directivas de grupo" diríjase a la siguiente unidad organizativa: Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10", y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que existe un vínculo llamado "CCN-STIC-599A19 Windows 10 - Equipos".  Compruebe también en el mismo sitio que el campo "Vínculo habilitado" muestra "Sí" para la GPO "CCN-STIC-599A19 Windows 10 - Equipos".
15. Abra la directiva de equipos cliente miembro Windows 10 (CCN-STIC-599A19 Windows 10 - Equipos) en el editor de administración de directivas de grupo		Marque con el botón derecho el vínculo de la GPO "CCN-STIC-599A19 Windows 10 - Equipos" situado en el siguiente contenedor: "Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10" En el menú contextual que aparecerá, seleccione la opción "Editar...", como se muestra en la figura. 

Comprobación	OK/NOK	Cómo hacerlo
16. Verifique la configuración general de Firewall de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los valores que se indicarán a continuación en la siguiente ubicación. "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada - LDAP://CN={SID}, CN=POLICIES, CN=SYSTEM, DC=<DOMINIO>, DC=LOCAL" Abra la ventana de propiedades de dicho contenedor: márkelo con el botón derecho del ratón y elija la opción "Propiedades" del menú contextual que aparecerá.  La siguiente figura muestra la ventana de propiedades, concretamente con la pestaña "Perfil de dominio" activa. 

Comprobación	OK/NOK	Cómo hacerlo															
		En la pestaña "Perfil de dominio", comprobar que los valores configurados son los siguientes:															
		<table> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> <tr> <td>Estado del firewall</td><td>Activo (recomendado)</td><td></td></tr> <tr> <td>Conexiones entrantes</td><td>Bloquear (predeterminado)</td><td></td></tr> <tr> <td>Conexiones salientes</td><td>Permitir (predet.)</td><td></td></tr> </table>	Directiva	Valor	OK/NOK	Estado del firewall	Activo (recomendado)		Conexiones entrantes	Bloquear (predeterminado)		Conexiones salientes	Permitir (predet.)				
Directiva	Valor	OK/NOK															
Estado del firewall	Activo (recomendado)																
Conexiones entrantes	Bloquear (predeterminado)																
Conexiones salientes	Permitir (predet.)																
		En la misma pestaña, marque el botón "Personalizar..." dentro del apartado "Configuración" para abrir la ventana "Personalizar la configuración de Perfil de dominio", como la que se muestra en la figura.  En esta ventana de configuración, compruebe que los valores configurados son los siguientes: <table> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> <tr> <td>Mostrar una notificación</td><td>No</td><td></td></tr> <tr> <td>Permitir respuesta de unidifusión</td><td>Sí (predeterminado)</td><td></td></tr> <tr> <td>Aplicar reglas de firewall local</td><td>No</td><td></td></tr> <tr> <td>Aplicar reglas de seguridad de conexión local</td><td>No</td><td></td></tr> </table>	Directiva	Valor	OK/NOK	Mostrar una notificación	No		Permitir respuesta de unidifusión	Sí (predeterminado)		Aplicar reglas de firewall local	No		Aplicar reglas de seguridad de conexión local	No	
Directiva	Valor	OK/NOK															
Mostrar una notificación	No																
Permitir respuesta de unidifusión	Sí (predeterminado)																
Aplicar reglas de firewall local	No																
Aplicar reglas de seguridad de conexión local	No																
		Repita, para cada uno de los otros dos perfiles: "Perfil privado" y "Perfil público", todas las comprobaciones de este paso recién realizadas sobre el "Perfil de dominio". La configuración debe ser idéntica.															

Comprobación	OK/NOK	Cómo hacerlo
17. Verifique las Reglas de entrada de la configuración de Firewall de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada - LDAP://CN={SID}, CN=POLICIES, CN=SYSTEM, DC=<DOMINIO>, DC=LOCAL \ Reglas de entrada" Seleccione dicho contenedor, y en la parte central de la ventana compruebe que no existe ninguna regla. 
18. Verifique las Reglas de salida de la configuración de Firewall de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva CCN-STIC-599A19 Windows 10" tiene los siguientes valores dentro de: "Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con seguridad avanzada → Firewall de Windows con seguridad avanzada - LDAP://CN={SID}, CN=POLICIES, CN=SYSTEM, DC=<DOMINIO>, DC=LOCAL → Reglas de salida" Seleccione dicho contenedor, y en la parte central de la ventana compruebe que no existe ninguna regla. 

Comprobación	OK/NOK	Cómo hacerlo
19. Verifique los valores de "Administración de derechos digitales de Windows Media" de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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
20. Verifique los valores del cliente WinRM de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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
21. Verifique los valores del servicio WinRM de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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
22. Verifique los valores para agregar características de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10"		
	Directiva		Valor
			OK/NOK
	Impedir que el asistente se ejecute		Habilitada
23. Verifique los valores del almacén digital de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Almacén digital"		
	Directiva		Valor
			OK/NOK
	No permitir que se ejecute el Almacén digital		Habilitada
24. Verifique los valores del análisis de confiabilidad de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Análisis de confiabilidad de Windows"		

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Configurar proveedores de WMI de confiabilidad	Habilitada	
25. Verifique los valores de Windows Ink de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
26. Verifique los valores de asistencia en línea de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Asistencia en línea"		
		Directiva	Valor	OK/NOK
		Desactivar la ayuda activa	Habilitada	
27. Verifique los valores de biometría de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Biometría"		
		Directiva	Valor	OK/NOK
		Permitir el uso de biometría	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo
28. Verifique los valores de búsqueda de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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
	Impedir que los clientes soliciten el índice de forma remota	Habilitada
29. Verifique los valores de cámara de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cámara"
	Directiva	Valor OK/NOK
	Permitir el uso de la cámara	Deshabilitada
30. Verifique los valores del centro de movilidad de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows"

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	
31. Verifique los valores del centro de seguridad de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Centro de seguridad"		
		Directiva	Valor	OK/NOK
		Activar el Centro de seguridad (solo equipos de dominio)	Deshabilitada	
32. Verifique los valores de la compatibilidad de aplicaciones de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
33. Verifique los valores de la configuración de conectar de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
34. Verifique los valores de la configuración de presentación de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Configuración de presentación"		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
35. Verifique los valores de Contenido de la nube de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
36. Verifique los valores de las directivas de reproducción automática de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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 la ejecución automática	Habilitada, (No ejecutar ningún comando de ejecución automática)	
		Evitar que reproducción automática recuerde las elecciones del usuario	Habilitada	
37. Verifique los valores de las directivas del explorador de Archivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
38. Verifique los valores de las directivas de las versiones anteriores del explorador de Archivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
39. Verifique los valores de las directivas del explorador de juegos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
40. Verifique los valores de las fuentes RSS de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Fuentes RSS"		
		Directiva	Valor	OK/NOK
		Desactivar la descarga de información sobre juegos	Habilitada	

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	
41. Verifique los valores de la grabación y difusión de juegos de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
42. Verifique los valores de la grabadora de sonidos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos"			
	Directiva		Valor	OK/NOK
	No permitir que se ejecute la grabadora de sonidos		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
43. Verifique los valores del grupo en el hogar de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
44. Verifique los valores de paquete de aplicación de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
45. Verifique los valores del informe de errores de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		Habilitada
46. Verifique los valores de la interfaz de usuario de credenciales de la directiva "CCN-STIC-599A19 Windows 10-Equipos"	No enviar datos adicionales		Habilitada
	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Interfaz de usuario de credenciales"		
	Directiva		Valor
			OK/NOK
	Enumerar las cuentas de administración al realizar una elevación		Deshabilitada
47. Verifique los valores de Mapas de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	No mostrar el botón revelar contraseña		Habilitada
	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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
48. Verifique los valores de MDM de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"	Desactivar la descarga automática y la actualización de datos de mapa		Habilitada
	Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → MDM"		
	Directiva		Valor
			OK/NOK
	Deshabilitar la inscripción de MDM		Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
49. Verifique los valores de Mensajería de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Mensajería"		
		Directiva	Valor	OK/NOK
		Permitir la sincronización en la nube del servicio de mensajería	Deshabilitada	
50. Verifique los valores de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → NetMeeting"		
		Directiva	Valor	OK/NOK
		Deshabilitar el uso compartido de escritorio remoto	Habilitada	
51. Verifique los valores de las opciones de One Drive de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → OneDrive"		
		Directiva	Valor	OK/NOK
		Impedir el uso de OneDrive para almacenar archivos	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo			
52. Verifique los valores de las opciones de inicio de sesión de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
53. Verifique los valores de la plataforma de protección de software de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Plataforma de protección de software"			
		Directiva		Valor	OK/NOK
		Controlar la reactivación de dispositivos comerciales		Habilitada	
		Desactivar validación AVS en línea del cliente KMS		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo
54. Verifique los valores de Privacidad de aplicación de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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 (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 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 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 sincronicen con dispositivos	Habilitada (Forzar denegación)
	Permitir que las aplicaciones de Windows tengan acceso a los contactos	Habilitada (Forzar denegación)

Comprobación	OK/NOK	Cómo hacerlo		
55. Verifique los valores del Programa para la mejora de la experiencia de usuario de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
56. Verifique los valores de Recopilación de datos y versiones preliminares de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Recopilación de datos y versiones preliminares"		
		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])	
57. Verifique los valores del cliente de conexión a escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Cliente de conexión a escritorio remoto"		

Comprobación	OK/NOK	Cómo hacerlo	
		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
58. Verifique los valores de las conexiones de Host de sesión de Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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
59. Verifique los valores de la redirección de dispositivos o recursos de Host de sesión de Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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

Comprobación	OK/NOK	Cómo hacerlo		
60. Verifique los valores de la seguridad de Host de sesión de Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Servicios de Escritorio Remoto → Host de sesión de Escritorio remoto → Seguridad"		
		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	
61. Verifique los valores del Shell remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Shell Remoto de Windows"		
		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	
62. Verifique los valores para Sincronizar la configuración de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Sincronizar la configuración"		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor OK/NOK
		No sincronizar	Habilitada, (Permitir a los usuarios activar la sincronización: Deshabilitado))
63. Verifique los valores de Accesorios de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tablet PC → Accesorios"	
		Directiva	Valor OK/NOK
		No permitir que se ejecute Windows Journal	Habilitada
64. Verifique los valores de Tarjeta inteligente de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Tarjeta inteligente"	
		Directiva	Valor OK/NOK
		Activar servicio Plug and Play de tarjeta inteligente	Deshabilitada
65. Verifique los valores de la tienda de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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		
66. Verifique los valores de ubicación y sensores de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Ubicación y sensores”		
	Directiva		Valor	OK/NOK
	Desactivar scripting de ubicación		Habilitada	
	Desactivar sensores		Habilitada	
	Desactivar ubicación		Habilitada	
67. Verifique los valores de Servicio de localización de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
68. Verifique los valores de virtualización de la experiencia del usuario de Microsoft de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
69. Verifique los valores de Windows Hello de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Hello para empresas"		
		Directiva	Valor	OK/NOK
		Usa Windows Hello para empresas	Deshabilitada	
		Usar biometría	Deshabilitada	
70. Verifique los valores de Windows Installer de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
71. Verifique los valores de Windows Mail de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Mail"		
		Directiva	Valor	OK/NOK
		Turn off Windows Mail application	Habilitada	
		Turn off the communities features	Habilitada	
72. Verifique los valores de Windows Messenger de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
73. Verifique los valores de Windows Update de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Componentes de Windows → Windows Update"		
		Directiva	Valor	OK/NOK
		Configurar Actualizaciones automáticas	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
74. Verifique los valores de Impresoras de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Impresoras"		
		Directiva	Valor	OK/NOK
		Ejecutar controladores de impresión en procesos aislados	Habilitada	
		Permitir que se publiquen impresoras	Deshabilitada	
75. Verifique los valores de Notificaciones de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Menú inicio y barra de tareas → Notificaciones"		
		Directiva	Valor	OK/NOK
		Desactivar el uso de la red para notificaciones	Habilitada	
76. Verifique los valores de Panel de control de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Panel de control"		
		Directiva	Valor	OK/NOK
		Permitir recomendaciones en línea	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
77. Verifique los valores de Configuración regional y de idioma de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
78. Verifique los valores de Personalización de escritura a mano de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Panel de control → Configuración regional y de idioma → Personalización de escritura a mano"		
		Directiva	Valor	OK/NOK
		Desactivar el aprendizaje automático	Habilitada	
79. Verifique los valores de Personalización de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Panel de control → Personalización"		
		Directiva	Valor	OK/NOK
		Evitar la activación de la cámara de la pantalla de bloqueo	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
80. Verifique los valores del administrador de conexiones de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
81. Verifique los valores de archivos sin conexión de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Archivos sin conexión"		
		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	
82. Verifique los valores de BranchCache de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → BranchCache"		
		Directiva	Valor	OK/NOK
		Activar BranchCache	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
83. Verifique los valores del perfil de firewall de dominio de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Conexiones de Red → Firewall de Windows Defender → Perfil de dominio"		
		Directiva	Valor	OK/NOK
	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		
84. Verifique los valores del perfil de firewall estándar de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
85. Verifique los valores de las tecnologías de transición a IPv6 de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Configuración de TCPIP → Tecnologías de transición IPv6"		
	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)	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Estado de Teredo	Habilitada (Estado Deshabilitado)	
86. Verifique los valores de la detección de topologías a nivel de vínculo de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
87. Verifique los valores de la estación de trabajo Lanman de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Estación de trabajo Lanman"		
		Directiva	Valor	OK/NOK
		Habilitar inicios de sesión de invitado no seguros	Deshabilitada	
88. Verifique los valores de Fuentes de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Fuentes"		
		Directiva	Valor	OK/NOK
		Habilitar Proveedores de fuentes	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
89. Verifique los valores de Proyección inalámbrica de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Proyección inalámbrica"		
		Directiva	Valor	OK/NOK
		Requerir emparejamiento de PIN	Habilitada	
90. Verifique los valores de Configuración WLAN de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
91. Verifique los valores de Acceso a datos móviles de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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)	

Comprobación	OK/NOK	Cómo hacerlo		
92. Verifique los valores de Configuración de la interfaz de usuario de WWAN de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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)	
93. Verifique los valores de los servicios de redes de igual a igual de Microsoft de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
94. Verifique los valores del servidor Lanman de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Servidor Lanman"		

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)	
95. Verifique los valores de Windows Connect Now de la directiva “CCN-STIC-599A19 Windows 10 – Equipos”		Utilizando la herramienta “Editor de administración de directivas de grupo”, verifique que la directiva “CCN-STIC-599A19 Windows 10 – Equipos” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Red → Windows Connect Now”		
	Directiva		Valor	OK/NOK
	Prohibir el acceso de los asistentes de Windows Connect Now		Habilitada	
96. Verifique los valores de Acceso de almacenamiento extraíble de la directiva “CCN-STIC-599A19 Windows 10 – Equipos”		Utilizando la herramienta “Editor de administración de directivas de grupo”, verifique que la directiva “CCN-STIC-599A19 Windows 10 – Equipos” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Acceso de almacenamiento extraíble”		
	Directiva		Valor	OK/NOK
	Todas las clases de almacenamiento extraíble: denegar acceso a todo		Habilitada	
97. Verifique los valores de la administración de comunicaciones de Internet de la directiva “CCN-STIC-599A19 Windows 10 – Equipos”		Utilizando la herramienta “Editor de administración de directivas de grupo”, verifique que la directiva “CCN-STIC-599A19 Windows 10 – Equipos” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Administración de comunicaciones de Internet”		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor OK/NOK
		Restringir comunicaciones de Internet	Habilitada
98. Verifique los valores de la configuración de comunicaciones de Internet de la directiva "CCN-STIC-599A19 Windows 10 – Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 – Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Equipos → Configuración del equipo → Directivas → 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 la 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

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
		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	
99. Verifique los valores de App-V de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → App-V"		
		Directiva	Valor	OK/NOK
		Habilitar el cliente de App-V	Deshabilitada	
100. Verifique los valores de asistencia remota de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Asistencia Remota"		
		Directiva	Valor	OK/NOK
		Configurar Asistencia remota solicitada	Deshabilitada	
		Configurar Ofrecer Asistencia remota	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
101.Verifique los valores de directiva de grupo de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Directiva de grupo"		
		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	Deshabilitada	
		Vinculación de teléfono y PC en este dispositivo	Deshabilitada	
102.Verifique los valores de directiva del sistema operativo de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo	
103.Verifique los valores de inicio de sesión de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → 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	
104.Verifique los valores de instalación de dispositivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Instalación de dispositivos"	
	Directiva	Valor	OK/NOK
	Permitir acceso remoto a la interfaz Plug and Play	Deshabilitada	

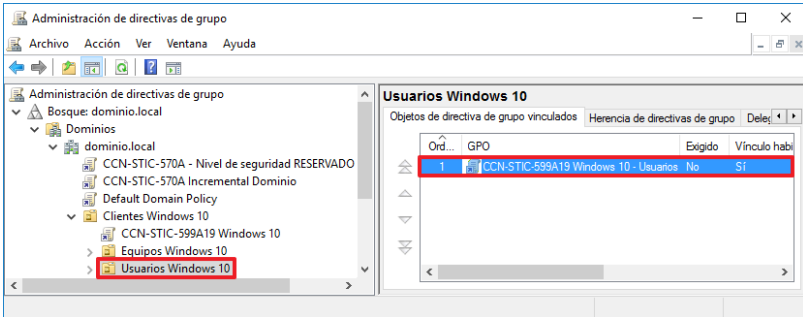
Comprobación	OK/NOK	Cómo hacerlo		
105.Verifique los valores de restricciones de instalación de dispositivos de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”		
		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	
106.Verifique los valores de la llamada a procedimiento remoto de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Llamada a procedimiento remoto”		
		Directiva	Valor	OK/NOK
		Habilitar la autenticación de clientes del Asignador de extremos de RPC	Habilitada	
		Restringir clientes de RPC no autenticados	Habilitada (Autenticado)	

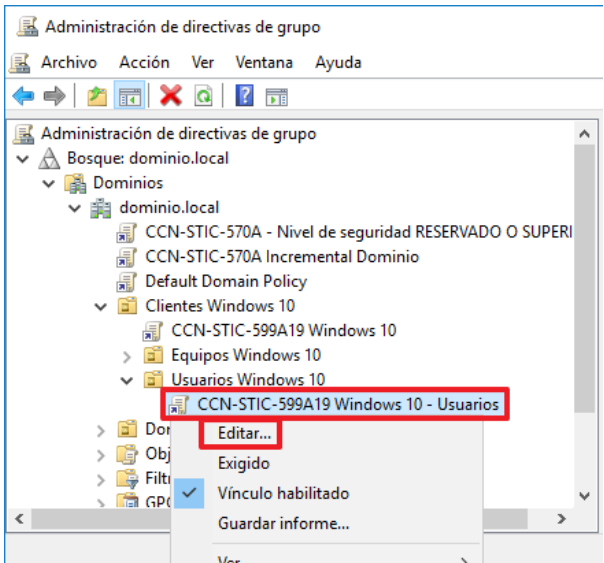
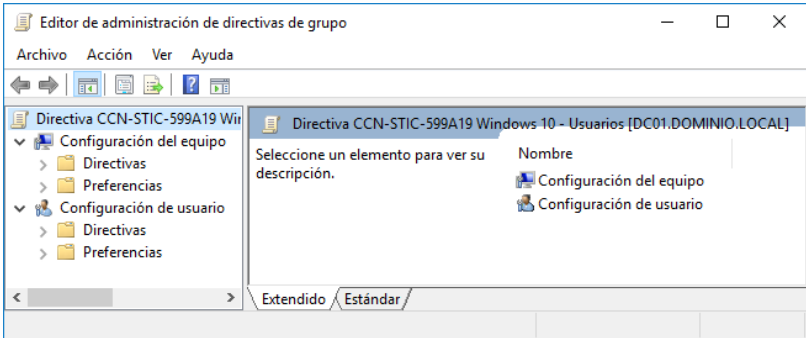
Comprobación	OK/NOK	Cómo hacerlo		
107.Verifique los valores de Net Logon de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Net Logon"		
		Directiva	Valor	OK/NOK
		Permitir algoritmos de criptografía compatibles con Windows NT 4.0	Deshabilitada	
108.Verifique los valores de Perfiles de usuario de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Perfiles de Usuario"		
		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	
109.Verifique los valores de Servicios de configuración regional de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Servicios de configuración regional"		
		Directiva	Valor	OK/NOK
		Denegar el cambio de ubicación geográfica	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
110.Verifique los valores de Herramienta de diagnóstico de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Configuración del equipo → Directivas → Plantillas Administrativas → Sistema → Solución de problemas y diagnósticos → Herramienta de diagnóstico para soporte técnico de Microsoft"		
		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	
111.Verifique los valores de Preferencias de la directiva "CCN-STIC-599A19 Windows 10 - Equipos"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Equipos → Preferencias → Configuración de Windows → Registro"		
		Directiva	Valor	OK/NOK
		SMB1	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters Tipo: REG_DWORD Valor: 00000000 (0)	

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva	Valor	OK/NOK
	HiberbootEnabled	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Power Tipo: REG_DWORD Valor: 00000000 (0)	
	AllowTelemetry	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection Tipo: REG_DWORD Valor: 00000001	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\MessagingService Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\NgcCtnrSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\NgcSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\OneSyncSvc Tipo: REG_DWORD Valor: 00000004	

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva	Valor	OK/NOK
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ PimIndexMaintenanceSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ Sense Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ SgrmBroker Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ UnistoreSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ UserDataSvc Tipo: REG_DWORD Valor: 00000004	
	Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\ WpnUserService Tipo: REG_DWORD Valor: 00000004	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\EntAppSvc Tipo: REG_DWORD Valor: 00000004	
		Start	Acción: Actualización Subárbol: HKEY_LOCAL_MACHINE Clave: SYSTEM\CurrentControlSet\Services\PrintWorkflowUserSvc Tipo: REG_DWORD Valor: 00000004	Start
112.Finalice la comprobación de la directiva CCN-STIC-599A19 Windows 10 - Equipos		Cierre la ventana del "Editor de administración de directivas de grupo" que tenía abierta con la directiva de dominio "CCN-STIC-599A19 Windows 10 - Equipos"		
113.Verifique que está creada y asignada correctamente la directiva (GPO) de usuarios ("CCN-STIC-599A19 Windows 10 - Usuarios")		De nuevo en la consola de "Administración de directivas de grupo" diríjase a la siguiente unidad organizativa: Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10" y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que existe un vínculo llamado "CCN-STIC-599A19 Windows 10 - Usuarios".  Compruebe también en el mismo sitio que el campo "Vínculo habilitado" muestra "Sí" para la GPO "CCN-STIC-599A19 Windows 10 - Usuarios".		

Comprobación	OK/NOK	Cómo hacerlo
114. Abra la directiva (GPO) de usuarios (CCN-STIC-599A19 Windows 10 - Usuarios) en el editor de administración de directivas de grupo		Marque con el botón derecho el vínculo de la GPO "CCN-STIC-599A19 Windows 10 - Usuarios" situado en el siguiente contenedor: "Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10" En el menú contextual que aparecerá, seleccione la opción "Editar...", como se muestra en la figura.  Con ello se abrirá el Editor de administración de directivas de grupo, mostrando la configuración de la GPO "CCN-STIC-599A19 Windows 10 - Usuarios".  En los próximos pasos, hasta que se indique lo contrario, verificará la configuración de este GPO utilizando esta ventana del editor de administración de directivas de grupo

Comprobación	OK/NOK	Cómo hacerlo		
115.Verifique los valores de Carpetas compartidas de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Carpetas compartidas"		
		Directiva	Valor	OK/NOK
		Permitir publicación de carpetas compartidas	Deshabilitada	
		Permitir publicación de raíces DFS	Deshabilitada	
116.Verifique los valores del administrador de datos adjuntos de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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		
117.Verifique los valores para Agregar características a Windows 10 de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Agregar características a Windows 10"		
		Directiva	Valor	OK/NOK
		Impedir que el asistente se ejecute	Habilitada	
118.Verifique los valores del almacén digital de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Almacén digital"		
		Directiva	Valor	OK/NOK
		No permitir que se ejecute el Almacén digital	Habilitada	
119.Verifique los valores del centro de movilidad de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Centro de movilidad de Windows"		
		Directiva	Valor	OK/NOK
		Desactivar Centro de movilidad de Windows	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
120.Verifique los valores de la compatibilidad de aplicaciones de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Compatibilidad de aplicaciones"		
		Directiva	Valor	OK/NOK
		Desactivar el Asistente para la compatibilidad de programas	Habilitada	
121.Verifique los valores de la configuración de presentación de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Configuración de presentación"		
		Directiva	Valor	OK/NOK
		Desactivar la configuración de presentación de Windows	Habilitada	
122.Verifique los valores de la configuración de nube de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
123.Verifique los valores de las directivas de reproducción automática de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
124.Verifique los valores del explorador de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Explorador de archivos"		
		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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
125.Verifique los valores de diálogo común para abrir archivos de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
126.Verifique los valores del panel de marcos del explorador de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Explorador de archivos → Panel de marcos del explorador"		
		Directiva	Valor	OK/NOK
		Desactivar el panel de vista previa	Habilitada	
127.Verifique los valores de las versiones anteriores del explorador de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Explorador de archivos → Versiones anteriores"		

Comprobación	OK/NOK	Cómo hacerlo	
	Directiva		Valor
	Impedir la restauración de versiones anteriores remotas		Habilitada
	Ocultar lista de versiones anteriores para archivos remotos		Habilitada
128.Verifique los valores de las fuentes RSS de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Fuentes RSS"	
	Directiva		Valor
	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
129.Verifique los valores de la grabadora de sonidos de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Grabadora de sonidos"	
	Directiva		Valor
	No permitir que se ejecute la grabadora de sonidos		Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
130.Verifique los valores del informe de errores de Windows de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Informe de errores de Windows"		
		Directiva	Valor	OK/NOK
		Deshabilitar el Informe de errores de Windows	Habilitada	
131.Verifique los valores de la interfaz de usuario de credenciales de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Interfaz de usuario de credenciales"		
		Directiva	Valor	OK/NOK
		No mostrar el botón revelar contraseña	Habilitada	
132.Verifique los valores de Microsoft Management Console de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
133.Verifique los valores de los complementos restringidos o permitidos de Microsoft Management Console de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
	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	

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	Valor	OK/NOK
		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	
134.Verifique los valores de directiva de grupo de Microsoft Management Console de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	

Comprobación	OK/NOK	Cómo hacerlo		
135.Verifique los valores de las extensiones de complemento de directivas de grupo de MMC de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
136.Verifique los valores de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
	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	

Comprobación	OK/NOK	Cómo hacerlo		
137.Verifique los valores de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → NetMeeting → Audio y video"		
		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	
138.Verifique los valores de compartir aplicaciones a través de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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														
139.Verifique los valores de la página de opciones de NetMeeting de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → NetMeeting → Página de opciones"														
		<table><tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Deshabilitar el botón Llamada avanzada</td><td>Habilitada</td><td></td></tr><tr><td>Ocultar la página General</td><td>Habilitada</td><td></td></tr><tr><td>Ocultar la página Seguridad</td><td>Habilitada</td><td></td></tr></table>			Directiva	Valor	OK/NOK	Deshabilitar el botón Llamada avanzada	Habilitada		Ocultar la página General	Habilitada		Ocultar la página Seguridad	Habilitada	
		Directiva	Valor	OK/NOK												
		Deshabilitar el botón Llamada avanzada	Habilitada													
		Ocultar la página General	Habilitada													
Ocultar la página Seguridad	Habilitada															
140.Verifique los valores de Cliente de conexión a Escritorio remoto de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Servicios de Escritorio remoto → Cliente de conexión a Escritorio remoto"														
		<table><tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>No permitir que se guarden las contraseñas</td><td>Habilitada</td><td></td></tr></table>			Directiva	Valor	OK/NOK	No permitir que se guarden las contraseñas	Habilitada							
		Directiva	Valor	OK/NOK												
No permitir que se guarden las contraseñas	Habilitada															
141.Verifique los valores de Accesorios de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Tablet PC → Accesorios"														
		<table><tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>No permitir que se ejecute Windows Journal</td><td>Habilitada</td><td></td></tr></table>			Directiva	Valor	OK/NOK	No permitir que se ejecute Windows Journal	Habilitada							
		Directiva	Valor	OK/NOK												
No permitir que se ejecute Windows Journal	Habilitada															

Comprobación	OK/NOK	Cómo hacerlo		
142.Verifique los valores de Tienda de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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	
143.Verifique los valores de ubicación y sensores de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Ubicación y sensores"		
		Directiva	Valor	OK/NOK
		Desactivar scripting de ubicación	Habilitada	
		Desactivar sensores	Habilitada	
		Desactivar ubicación	Habilitada	
144.Verifique los valores de uso compartido de red de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Uso compartido de red"		
		Directiva	Valor	OK/NOK
		Impedir que los usuarios compartan archivos dentro de su perfil	Habilitada	

Comprobación	OK/NOK	Cómo hacerlo		
145.Verifique los valores de virtualización de la experiencia del usuario de Microsoft de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 - Usuarios → Configuración del equipo → Directivas → 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	
146.Verifique los valores de Windows Mail de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Windows Mail"		
		Directiva	Valor	OK/NOK
		Turn off the communities features	Habilitada	
		Turn off Windows Mail application	Habilitada	
147.Verifique los valores de Windows Messenger de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Windows Messenger"		

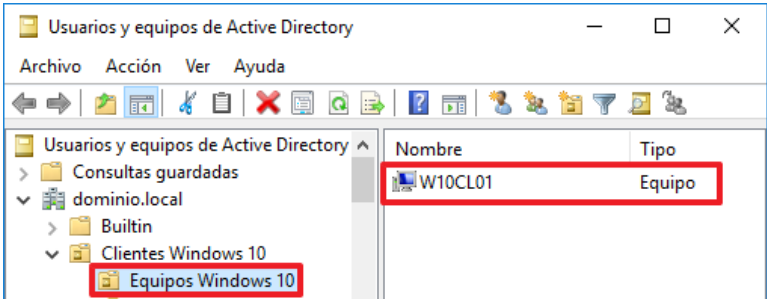
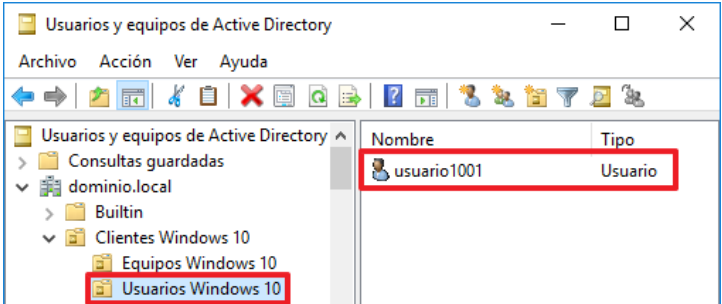
Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor OK/NOK
		No ejecutar automáticamente Windows Messenger al inicio	Habilitada
		No permitir que se ejecute Windows Messenger	Habilitada
148.Verifique los valores de Windows Update de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Componentes de Windows → Windows Update"	
		Directiva	Valor OK/NOK
		Quitar el acceso a todas las características de Windows Update	Habilitada, (0 – No mostrar ninguna notificación)
149.Verifique los valores del menú Inicio y barra de tareas de la directiva "CCN-STIC-599A19 Windows 10-Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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
150.Verifique los valores del Panel de Control de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Panel de Control"	

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor OK/NOK
		Abrir siempre Todos los elementos del Panel de control al abrir el Panel de control	Habilitada
151.Verifique los valores de las impresoras de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Panel de Control → Impresoras"	
		Directiva	Valor OK/NOK
		Impedir la adición de impresoras	Habilitada
		Impedir la eliminación de impresoras	Habilitada
152.Verifique los valores de personalización del panel de control de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Panel de Control → Programas"	
		Directiva	Valor OK/NOK
		Ocultar "Características de Windows"	Deshabilitada
153.Verifique los valores de archivos sin conexión a la red de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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		
154.Verifique los valores de Windows Connect Now de la directiva "CCN-STIC-599A19 Windows 10 Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Red → Windows Connect Now”		
	Directiva		Valor	OK/NOK
	Prohibir el acceso a los asistentes de Windows Connect Now		Habilitada	
155.Verifique los valores de sistema de la directiva "CCN-STIC-599A19 Windows 10 Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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?)	
156.Verifique los valores de acceso de almacenamiento extraíble de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: “Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Acceso de almacenamiento extraíble”		

Comprobación	OK/NOK	Cómo hacerlo	
		Directiva	Valor OK/NOK
		Todas las clases de almacenamiento extraíble: denegar acceso a todo	Deshabilitada
157.Verifique los valores de administración de comunicaciones de Internet de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Administración de comunicaciones de Internet"	
		Directiva	Valor OK/NOK
		Restringir comunicación de Internet	Habilitada
158.Verifique los valores de configuración de comunicaciones de Internet de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → 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

Comprobación	OK/NOK	Cómo hacerlo		
	Directiva		Valor	OK/NOK
	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	
159.Verifique los valores de Ctrl+Alt+Supr de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Usuarios" tiene los valores que se indicarán a continuación en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Opciones de Ctrl+Alt+Supr"		
	Directiva		Valor	OK/NOK
	Quitar Administrador de tareas		Habilitada	
160.Verifique los valores de Servicios de configuración regional de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-599A19 Windows 10 - Equipos" tiene los siguientes valores en la siguiente ubicación: "Directiva CCN-STIC-599A19 Windows 10 – Usuarios → Configuración del usuario → Directivas → Plantillas administrativas → Sistema → Servicios de configuración regional"		
	Directiva		Valor	OK/NOK
	Denegar el cambio de ubicación geográfica		Habilitada	
161.Finalice la comprobación de la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		Cierre la ventana del "Editor de administración de directivas de grupo" que tenía abierta con la directiva "CCN-STIC-599A19 Windows 10 - Usuarios"		

Comprobación	OK/NOK	Cómo hacerlo
162.Verifique que el equipo cliente miembro Windows 10 a asegurar se encuentra dentro de la unidad organizativa "Equipos Windows 10"		A través de la herramienta “Usuarios y equipos de Active Directory” mediante el menú “Herramientas” del “Administrador del servidor”, compruebe que el equipo Windows 10 a asegurar se encuentra en la unidad organizativa “Equipos Windows 10” situada en la siguiente ruta: <Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 Verifique que existe dentro de él un objeto de tipo "Equipo" que se corresponde con el equipo cliente miembro cuya configuración se está comprobando (en el ejemplo de la figura siguiente el equipo a comprobar se llama "W10CL01"): 
163.Verifique que la cuenta del usuario o usuarios del cliente miembro Windows 10 a asegurar se encuentran dentro de la unidad organizativa "Usuarios Windows 10"		De nuevo, a través de la herramienta “Usuarios y equipos de Active Directory”, compruebe que el cliente o clientes Windows 10 a asegurar se encuentran en la unidad organizativa “Usuarios Windows 10” situada en la siguiente ruta: <Nombre de su dominio> → Clientes Windows 10 → Usuarios Windows 10 Verifique que existe dentro de él un objeto de tipo "Usuario" que se corresponde con el usuario cliente miembro cuya configuración se está comprobando (en el ejemplo de la figura siguiente el usuario a comprobar se llama "usuario1001"). 
164.Finalice las comprobaciones en el controlador de dominio		En este punto ha realizado todas las comprobaciones necesarias en el controlador de dominio. Puede cerrar la sesión que tenía abierta hasta ahora en él.

2. COMPROBACIONES EN EQUIPO CLIENTE WINDOWS 10 PRO/ENTERPRISE

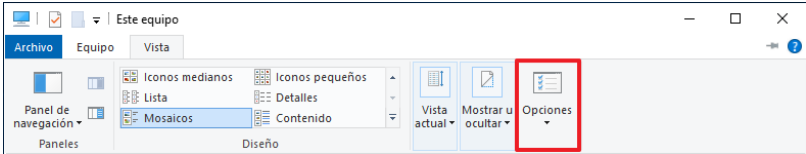
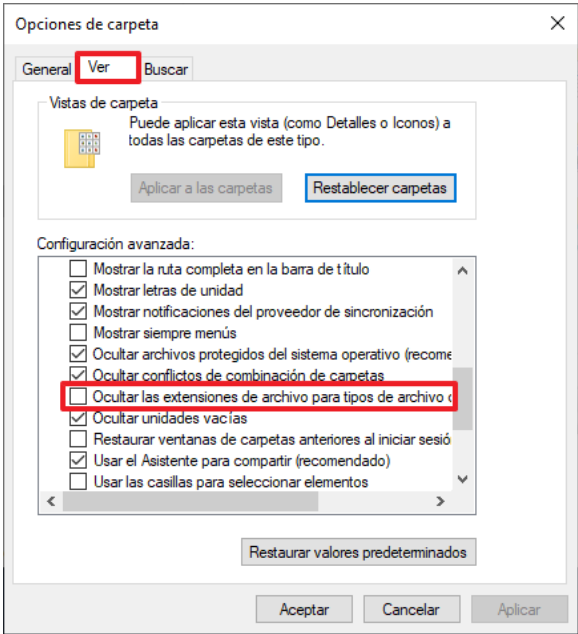
Para realizar algunas de las comprobaciones necesitará ejecutar diferentes consolas de administración y herramientas del sistema. Las consolas y herramientas que se utilizarán en el equipo cliente miembro son las siguientes:

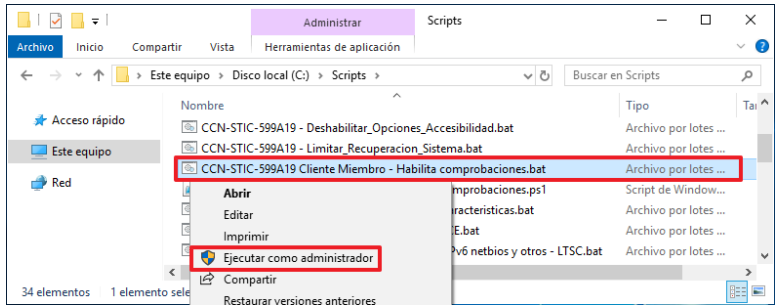
- a) Explorador de Windows (explorer.exe)
- b) PowerShell (powershell.exe)
- c) Conjunto resultante de directivas (rsop.msc)
- d) Panel de control (control.exe)
- e) Varias consolas de administración accesibles desde el panel de control (control.exe)
- f) Consola de administración de Microsoft (mmc.exe)
- g) Editor del registro (regedit.exe)
- h) Programador de tareas (taskschd.msc)

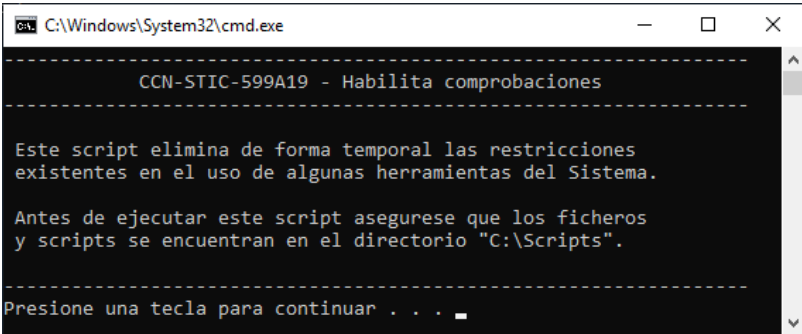
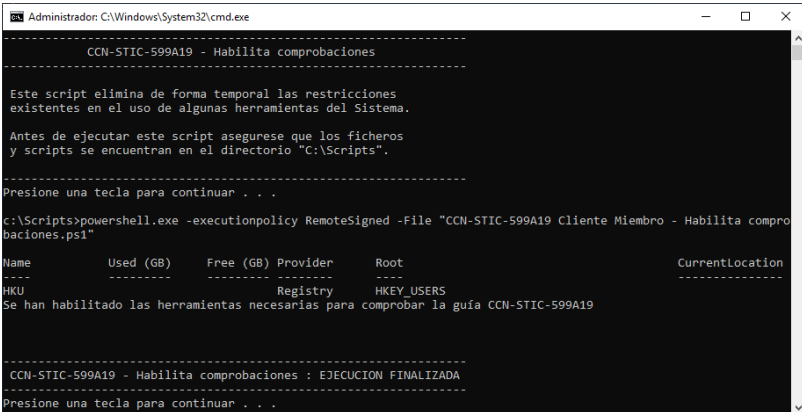
Siguiendo las recomendaciones de seguridad de esta guía, algunas de estas herramientas y consolas de administración estarán inicialmente deshabilitadas. Para poder implementar la lista de comprobación será necesario habilitarlas temporalmente. Para ello se suministra junto con esta guía el script “CCN-STIC-599A19 Cliente Miembro - 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.

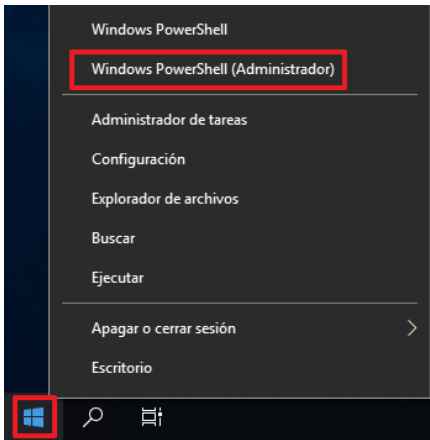
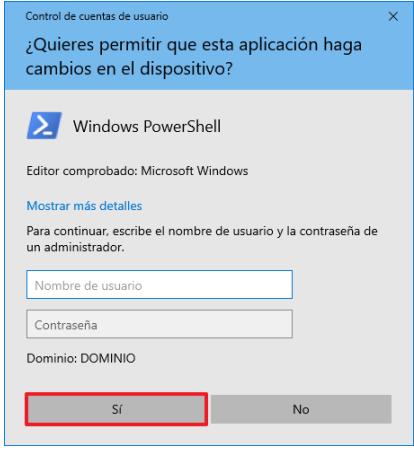
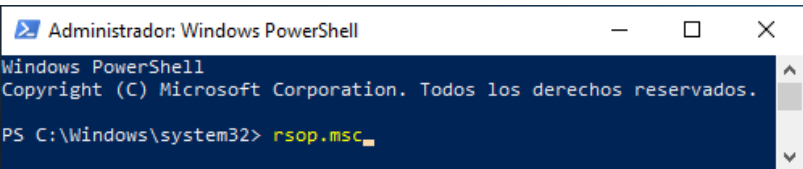
Ejecute los siguientes pasos en el cliente Windows 10 a comprobar:

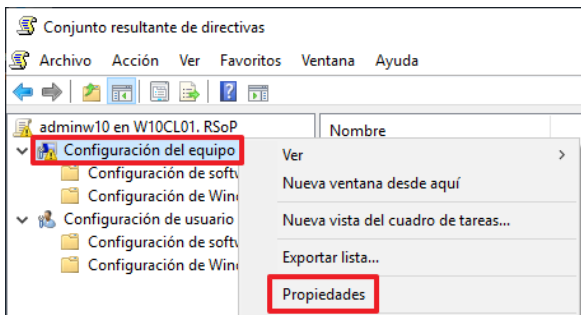
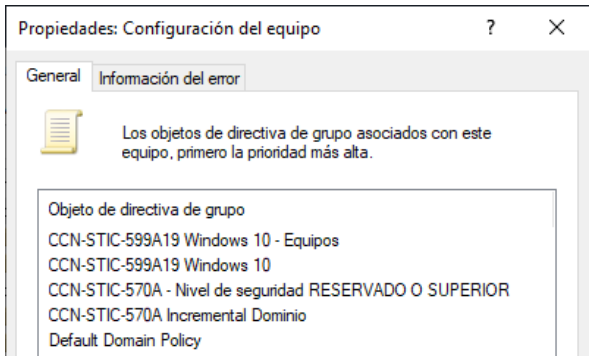
Comprobación	OK/NOK	Cómo hacerlo
165. Inicie sesión en el equipo cliente que está comprobando con privilegios de administrador, con un usuario de la unidad organizativa "Usuarios Windows 10"		Inicie sesión en el equipo que está comprobando con una cuenta de usuario de Windows que esté ubicada en la unidad organizativa "Usuarios Windows 10" de Active Directory y que pertenezca al grupo local "Administradores" (por ejemplo, un miembro del grupo "Admins. del dominio" y al grupo local de dominio "Usuarios de shells). Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.

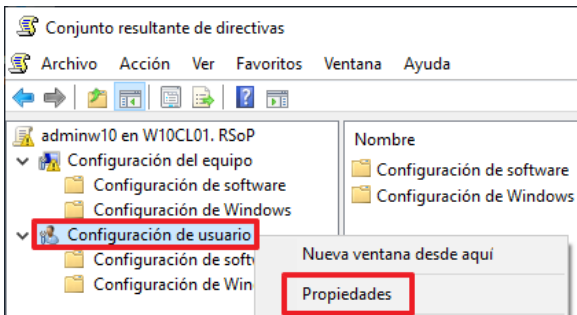
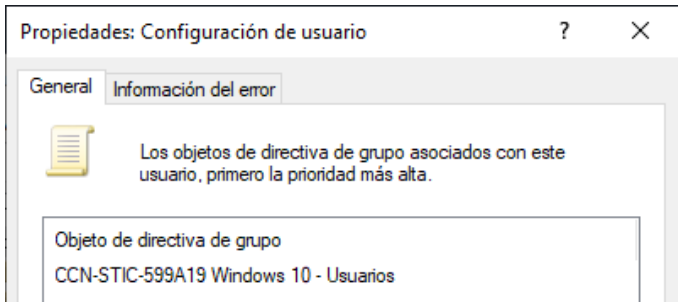
Comprobación	OK/NOK	Cómo hacerlo
166. Configure Explorador de Windows para que muestre las extensiones de los archivos		Por defecto Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador 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 (clic derecho) → Explorador de Windows" En el menú superior pulse sobre “Vista” y seleccione “Opciones”.  Seleccione la pestaña “Ver” y dentro de dicho menú, "Opciones de carpeta...". De la ventana que aparecerá, 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".

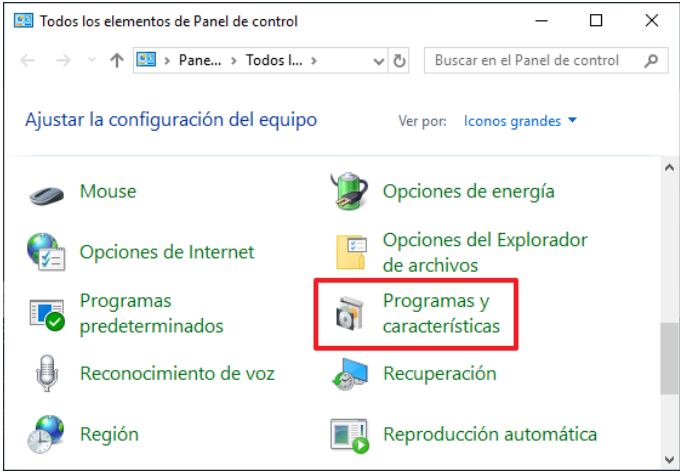
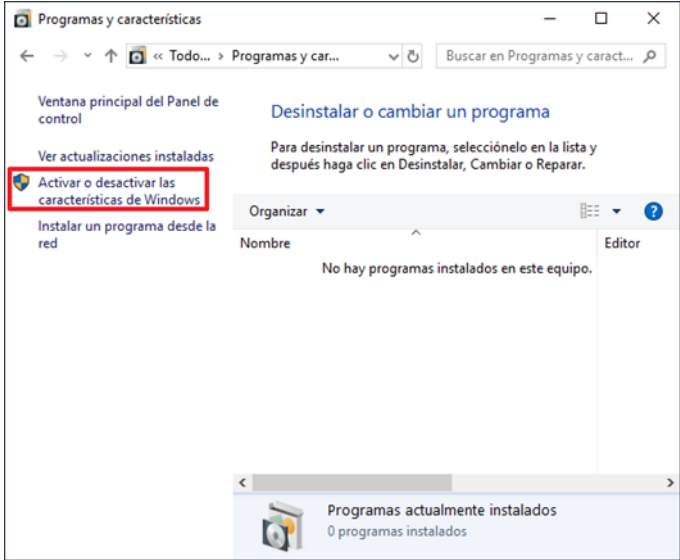
Comprobación	OK/NOK	Cómo hacerlo
167.Cree el directorio "C:\Scripts" y copie en él al menos los ficheros que se indican		Cree el directorio "Scripts" en la unidad "C:" ("C:\Scripts") en el sistema y copie en él al menos los siguientes dos scripts, los cuales están incluidos entre los ficheros que acompañan a esta guía: - CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.bat - CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.ps1 Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19".
168.Ejecute el script que habilita temporalmente las consolas de administración restringidas		Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - 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.  Aparecerá la solicitud de credenciales del escritorio seguro, en el cual deberá introducir las credenciales de un usuario administrador y pulse "Sí". Nota: Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.

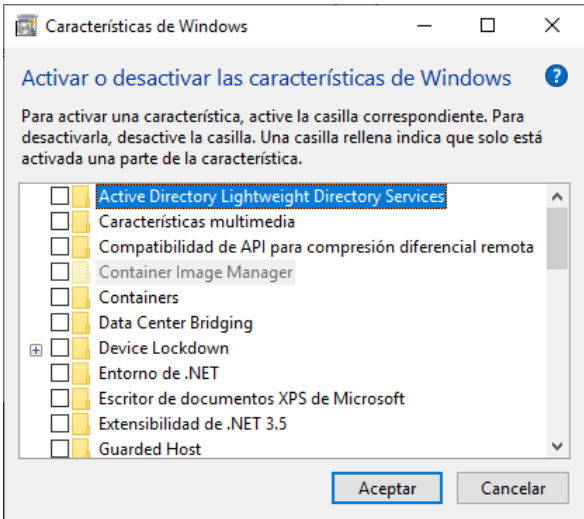
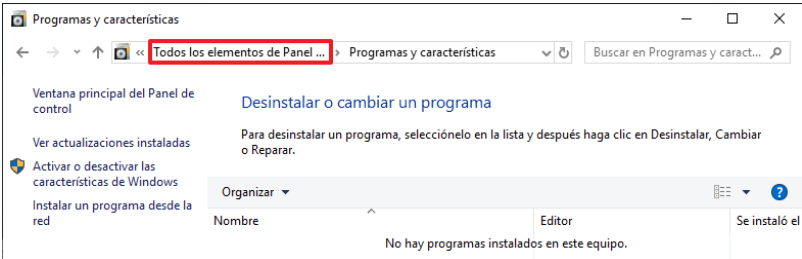
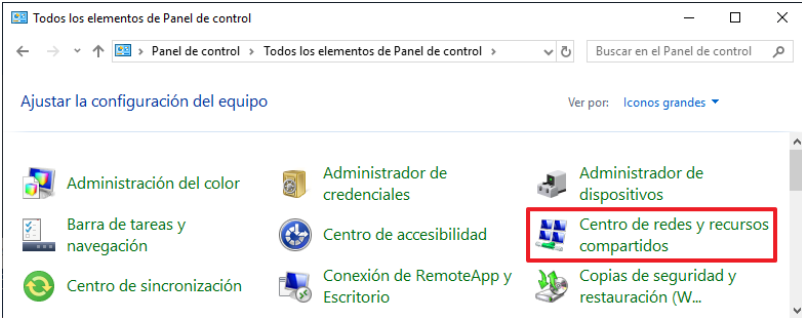
Comprobación	OK/NOK	Cómo hacerlo
169.Habilite temporalmente las consolas de administración restringidas		Aparecerá una consola de comandos con la ejecución del script. Pulse una tecla para continuar.  Cuando termine la ejecución, pulse una tecla para cerrar la ventana de comandos.  Nota: La próxima vez 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 de dominio y, por tanto, se han deshabilitado las comprobaciones. Ante tal eventualidad deberá volver a ejecutar el script “CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat” del mismo modo en que se describe en los pasos anteriores.

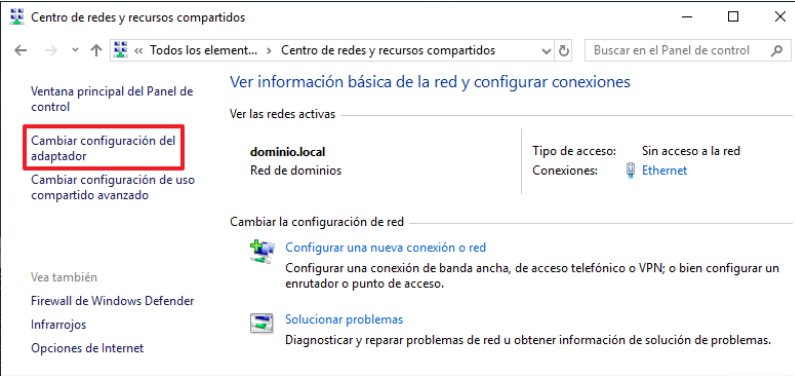
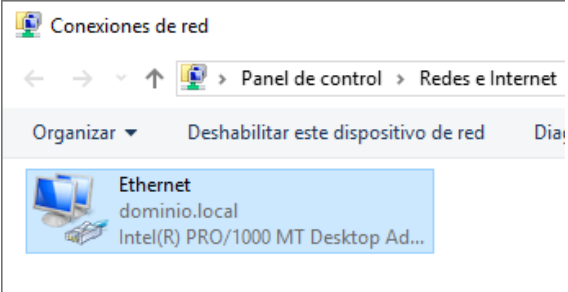
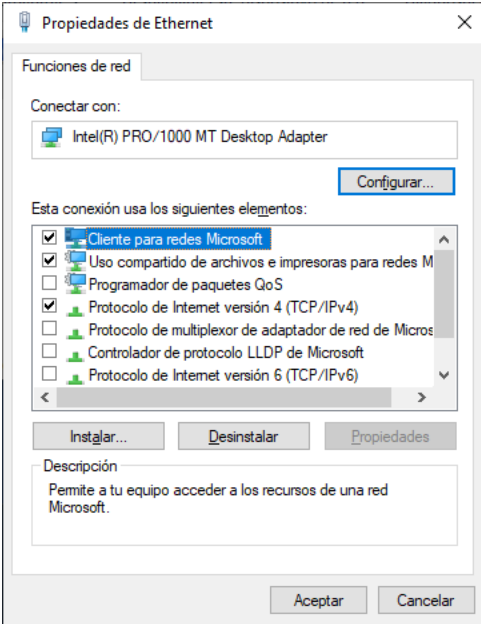
Comprobación	OK/NOK	Cómo hacerlo
170.Lance una ventana de PowerShell con permisos de administrador , para lanzar desde ella en pasos posteriores comandos con permisos de administrador		Haga clic con el botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”.  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.  Tras introducir las credenciales de un usuario administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.
171.Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse “Enter” para abrir la consola de administración "Conjunto resultante de directivas": 

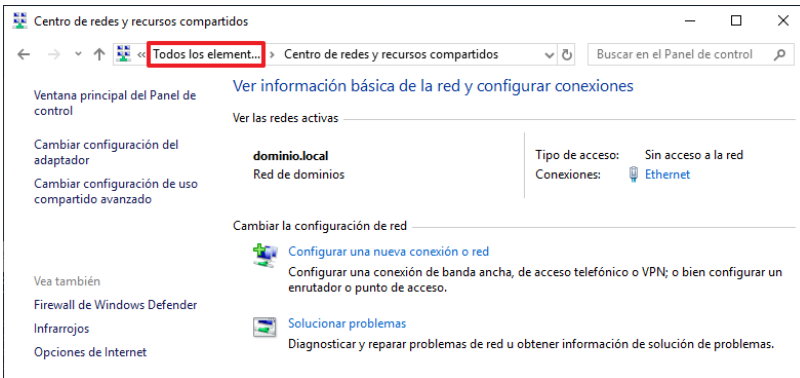
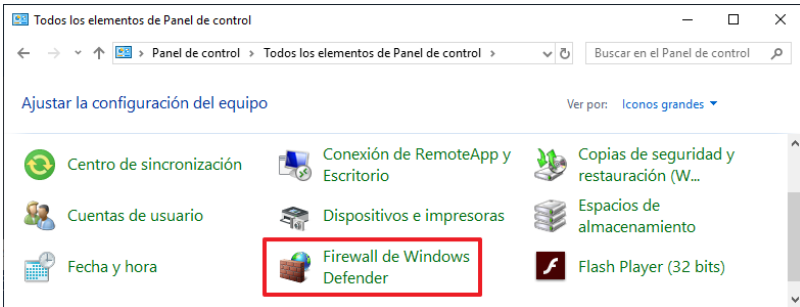
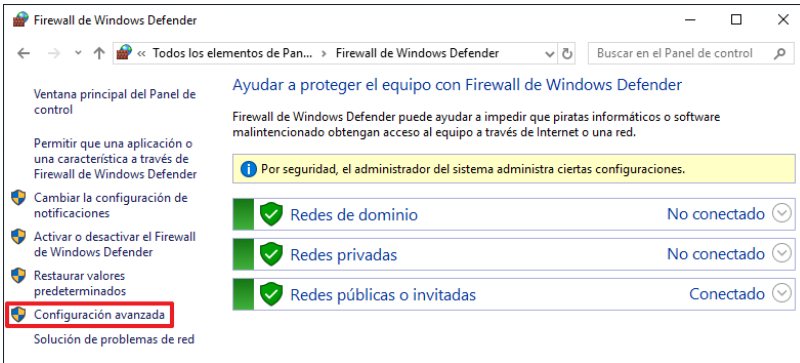
Comprobación	OK/NOK	Cómo hacerlo
172.Verifique que el equipo ha recibido correctamente las directivas de grupo "CCN-STIC-599A19 Windows 10" y "CCN-STIC-599A19 Windows 10 - Equipos"		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", las dos políticas deberán aparecer y "CCN-STIC-599A19 Windows 10 – Equipos" deberá estar situada encima de "CCN-STIC-599A19 Windows 10", tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al usuario del equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 Windows 10 - Equipos" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.
Parámetro		OK/NOK
CCN-STIC-599A19 Windows 10 - Equipos		
CCN-STIC-599A19 Windows 10		
CCN-STIC-570A - Nivel de seguridad RESERVADO O SUPERIOR		
Nota: Esta GPO dependerá del nivel de clasificación implementado en su organización.		
CCN-STIC-570A Incremental Dominio		
Default Domain Policy		

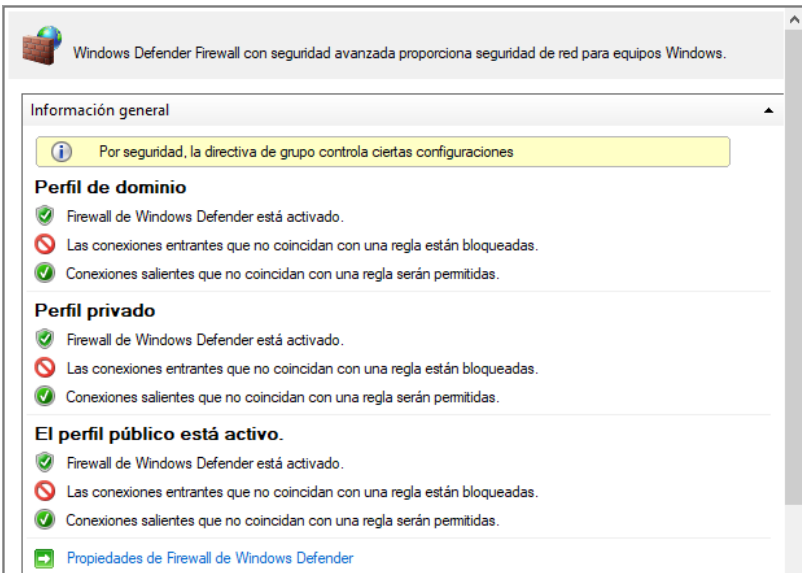
Comprobación	OK/NOK	Cómo hacerlo				
		Cierre la ventana de “Propiedades” pero no cierre aún la consola de administración “Conjunto resultante de directivas”.				
173.Verifique que el equipo ha recibido correctamente la directiva de grupo "CCN-STIC-599A19 Windows 10 - Usuarios"		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración de Usuario", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", deberá aparecer la política “CCN-STIC-599A19 Windows 10 – Usuarios”, tal y como se muestra en la siguiente figura.  Nota: Si el usuario que se está utilizando no está alojado en la unidad organizativa “Usuarios Windows 10”, la lista aparecerá vacía y, por tanto, este usuario no estará heredando dichas políticas. Puede mover a dicho usuario a la unidad organizativa correspondiente mediante la herramienta “Usuarios y equipos de Active Directory” o, en su lugar, utilizar un usuario que esté alojado en dicha unidad organizativa y que tenga privilegios de administración local del equipo Windows 10 en el que se están realizando las comprobaciones.				
		<table><tr><th>Parámetro</th><th>OK/NOK</th></tr><tr><td>CCN-STIC-599A19 Windows 10 - Usuarios</td><td></td></tr></table>	Parámetro	OK/NOK	CCN-STIC-599A19 Windows 10 - Usuarios	
Parámetro	OK/NOK					
CCN-STIC-599A19 Windows 10 - Usuarios						

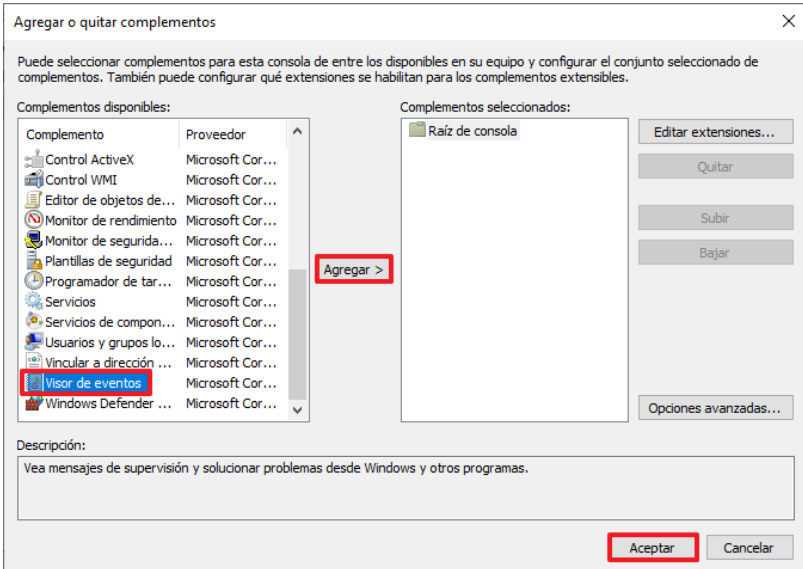
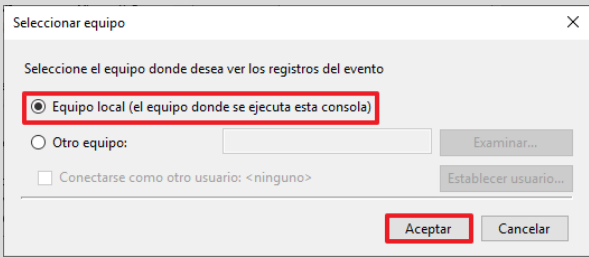
Comprobación	OK/NOK	Cómo hacerlo
		Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al usuario del equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 Windows 10 – Usuarios" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización. Cierre la ventana de propiedades y cierre también la consola de administración "Conjunto resultante de directivas"
174.Verifique que no hay características opcionales de Windows habilitadas		Desde la ventana de PowerShell con privilegios de administrador, ejecute "control.exe" para abrir el panel de control, y seleccione la opción "Programas y características".  Dentro de la ventana que aparecerá, seleccione la opción "Activar o desactivar las características de Windows". 

Comprobación	OK/NOK	Cómo hacerlo
		En la ventana de control de cuentas de usuario, introduzca de nuevo las credenciales de un usuario administrador, accederá 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.
175.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”: 

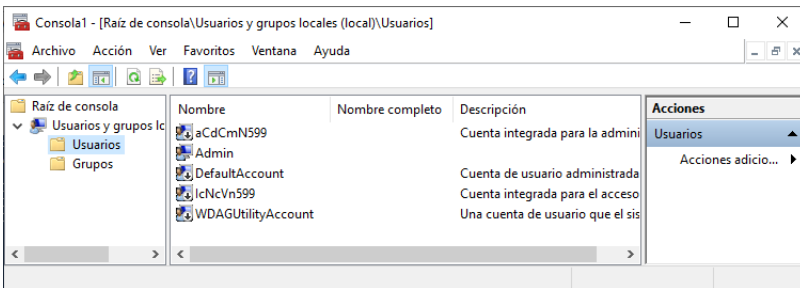
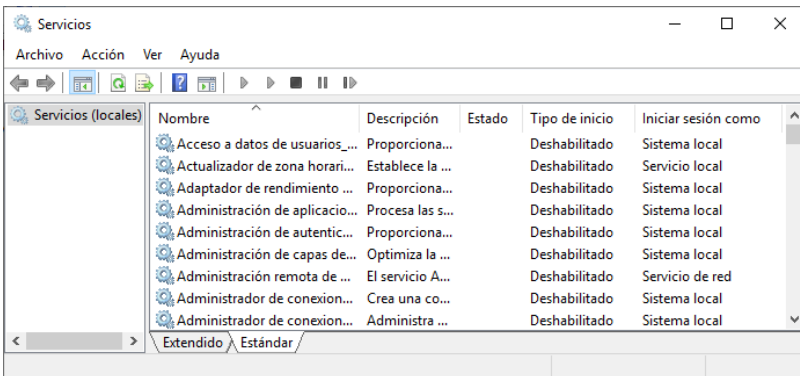
Comprobación	OK/NOK	Cómo hacerlo
		Seleccione “Cambiar configuración del adaptador”:  Aparecerá en la ventana del panel de control la lista de tarjetas de red del sistema:  Para cada tarjeta de red, marque con el botón derecho del ratón el icono de la tarjeta y seleccione la opción "Propiedades" del menú contextual que aparecerá. Tras introducir las credenciales de un usuario administrador de nuevo, aparecerá la ventana de propiedades del adaptador: 

Comprobación	OK/NOK	Cómo hacerlo
		Compruebe que los únicos elementos seleccionados sean "Cliente para redes Microsoft", "Uso compartido de archivos e impresoras para redes Microsoft" y "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.
176.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.  Seleccione "Firewall de Windows Defender" en el "Panel de Control".  Seleccione "Configuración avanzada". 

Comprobación	OK/NOK	Cómo hacerlo																											
		Introduzca credenciales 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. <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>Las conexiones entrantes que no coincidan con una regla están bloqueadas.</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla serán permitidas.</td><td></td></tr> <tr> <td rowspan="3">Perfil privado</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Las conexiones entrantes que no coincidan con una regla están bloqueadas.</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla serán permitidas.</td><td></td></tr> <tr> <td rowspan="3">Perfil público</td><td>Firewall de Windows está activado.</td><td></td></tr> <tr> <td>Las conexiones entrantes que no coincidan con una regla están bloqueadas.</td><td></td></tr> <tr> <td>Conexiones salientes que no coincidan con una regla serán permitidas.</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.		Las conexiones entrantes que no coincidan con una regla están bloqueadas.		Conexiones salientes que no coincidan con una regla serán permitidas.		Perfil privado	Firewall de Windows está activado.		Las conexiones entrantes que no coincidan con una regla están bloqueadas.		Conexiones salientes que no coincidan con una regla serán permitidas.		Perfil público	Firewall de Windows está activado.		Las conexiones entrantes que no coincidan con una regla están bloqueadas.		Conexiones salientes que no coincidan con una regla serán permitidas.	
Parámetro		OK/NOK																											
Por seguridad, la directiva de grupo controla ciertas configuraciones																													
Perfil de dominio	Firewall de Windows está activado.																												
	Las conexiones entrantes que no coincidan con una regla están bloqueadas.																												
	Conexiones salientes que no coincidan con una regla serán permitidas.																												
Perfil privado	Firewall de Windows está activado.																												
	Las conexiones entrantes que no coincidan con una regla están bloqueadas.																												
	Conexiones salientes que no coincidan con una regla serán permitidas.																												
Perfil público	Firewall de Windows está activado.																												
	Las conexiones entrantes que no coincidan con una regla están bloqueadas.																												
	Conexiones salientes que no coincidan con una regla serán permitidas.																												

Comprobación	OK/NOK	Cómo hacerlo
177. 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. 
178. 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
179. 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)	
180.Verifique la configuración del registro de eventos de Seguridad		Pulse el botón derecho del ratón sobre el contenedor “Aplicación”, 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)	
181.Verifique la configuración del registro de eventos de Sistema		Pulse el botón derecho del ratón sobre el contenedor “Aplicación”, 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)	
182.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 pasos anteriores.		
183.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
		Adicionalmente, haga doble clic en el resto de los grupos y compruebe que sus miembros corresponden con los usuarios adecuados para su entorno.
184.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 deshabilitados como en la siguiente figura.
		
	Usuarios	
	OK/NOK	
		aCdCmN599
		IcNcVn599
185.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:

Comprobación	OK/NOK	Cómo hacerlo			
		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	
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		
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		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Administrador de conexiones de acceso remoto	RasMan	Deshabilitado	Configurado	
Administrador de conexiones de Windows	Wcmsvc	Automático	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	
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	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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 de NetBIOS sobre TCP/IP	lmhosts	Automático	Configurado		
Aplicación auxiliar IP	iphlpvc	Deshabilitado	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		
ASP.NET State Service	aspnet_state	Deshabilitado	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		
Ayudante para el inicio de sesión de cuenta Microsoft	wlidsvc	Deshabilitado	Configurado		
BranchCache	PeerDistSvc	Deshabilitado	Configurado		
Captura SNMP	SNMPTRAP	Deshabilitado	Configurado		
CaptureService	CaptureService	Deshabilitado	Configurado		
Carpetas de trabajo	workfoldersvc	Deshabilitado	Configurado		
CDPUserSvc	CDPUserSvc	Deshabilitado	Configurado		
Centro de seguridad	wscsvc	Automático	Configurado		
Cliente de directiva de grupo	gpsvc	Automático	Configurado		
Cliente de seguimiento de vínculos distribuidos	TrkWks	Deshabilitado	Configurado		
Cliente DHCP	Dhcp	Automático	Configurado		
Cliente DNS	Dnscache	Automático	Configurado		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	
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	Deshabilitado	Configurado	
Configuración automática de WWAN	WwanSvc	Deshabilitado	Configurado	
Configuración de Escritorio remoto	SessionEnv	Deshabilitado	Configurado	
ConsentUX	ConsentUxUserSvc	Deshabilitado	Configurado	
Contenedor de Microsoft Passport	NgcCtnrSvc	Deshabilitado	Configurado	
Control parental	WpcMonSvc	Deshabilitado	Configurado	
Coordinador de transacciones distribuidas	MSDTC	Deshabilitado	Configurado	
Copias de seguridad de Windows	SDRSVC	Deshabilitado	Configurado	
CoreMessaging	CoreMessagingRegistrar	Automático	Configurado	
Datos de contactos	PimIndexMaintenanceSvc	Deshabilitado	Configurado	
Desencadenadores de Message Queue Server	MSMQTriggers	Deshabilitado	Configurado	
Detección de hardware shell	ShellHWDetection	Deshabilitado	Configurado	
Detección SSDP	SSDPSRV	Deshabilitado	Configurado	
DevicePicker	DevicePickerUserSvc	Deshabilitado	Configurado	
DevicesFlow	DevicesFlowUserSvc	Deshabilitado	Configurado	
Diagnostic Execution Service	diagsvc	Deshabilitado	Configurado	

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Directiva de extracción de tarjetas inteligentes	SCPolicySvc	Deshabilitado	Configurado		
Disco virtual	vds	Manual	Configurado		
Dispositivo host de UPnP	upnphost	Deshabilitado	Configurado		
DLL de host del Contador de rendimiento	PerfHost	Manual	Configurado		
dmwappushsvc	dmwappushservice	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		
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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
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		
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	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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Programador de tareas	Schedule	Automático	Configurado		
Propagación de certificados	CertPropSvc	Deshabilitado	Configurado		
Protección de software	sppsvc	Automático	Configurado		
Protocolo de autenticación extensible	EapHost	Manual	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		
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 auxiliar de host para aplicaciones	AppHostSvc	Deshabilitado	Configurado		
Servicio AVCTP	BthAvctpSvc	Deshabilitado	Configurado		
Servicio biométrico de Windows	WbioSrv	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio Cifrado de unidad BitLocker	BDESVC	Deshabilitado	Configurado		
Servicio de actualizaciones Orchestrator para Windows Update	UsoSvc	Automático	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 administración de Windows	WManSvc	Deshabilitado	Configurado		
Servicio de administración IIS	IISADMIN	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	wlpcsvc	Deshabilitado	Configurado		
Servicio de asociación de dispositivos	DeviceAssociationService	Manual	Configurado		
Servicio de caché de fuentes de Windows	FontCache	Deshabilitado	Configurado		
Servicio de cierre de invitado de Hyper-V	vmicshutdown	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		

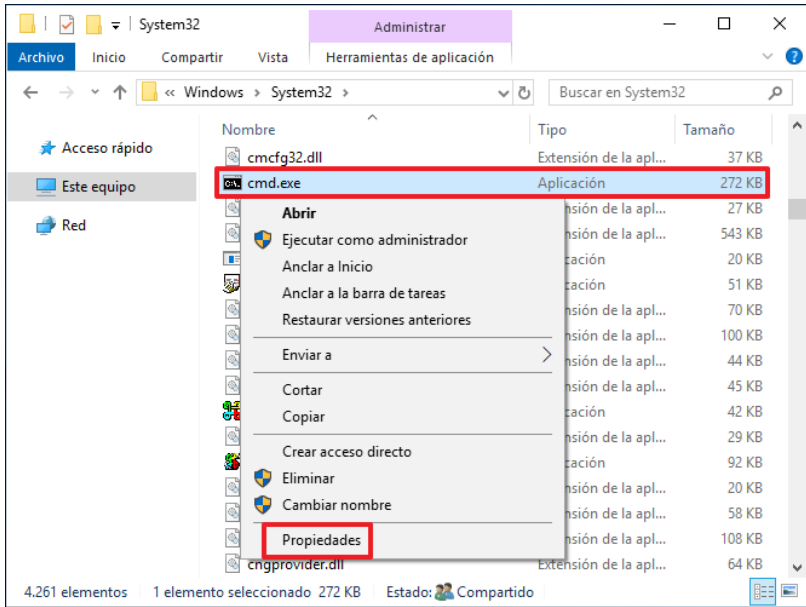
Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
Servicio de configuración de traslación de IP	IpxlatCfgSvc	Deshabilitado	Configurado	
Servicio de datos del sensor	SensorDataService	Deshabilitado	Configurado	
Servicio de datos espacial	SharedRealitySvc	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 enumeración de dispositivos de tarjeta inteligente	ScDeviceEnum	Deshabilitado	Configurado	
Servicio de experiencia de idioma	LxpSvc	Deshabilitado	Configurado	
Servicio de geolocalización	Ifsvc	Deshabilitado	Configurado	
Servicio de historial de archivos	fhsvc	Deshabilitado	Configurado	
Servicio de host HV (Hyper-V)	HvHost	Deshabilitado	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	Deshabilitado	Configurado	

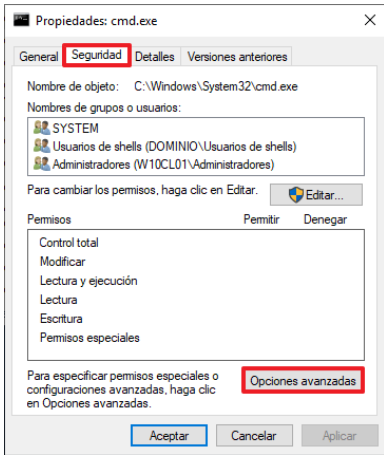
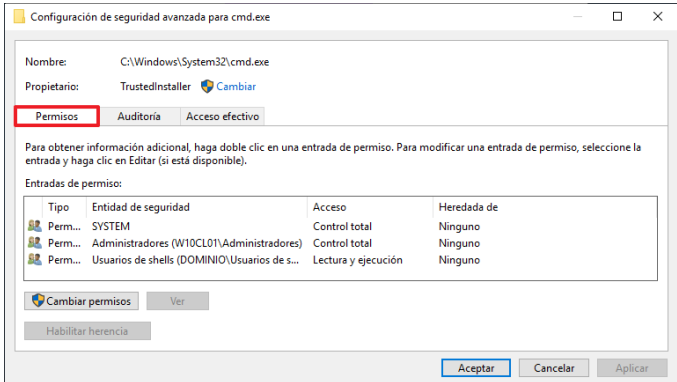
Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de intercambio de datos de Hyper-V	vmickvpexchange	Deshabilitado	Configurado		
Servicio de latido de Hyper-V	vmicheartbeat	Deshabilitado	Configurado		
Servicio de licencia de cliente (ClipSVC)	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 Panel de escritura a mano y teclado táctil	TabletInputService	Deshabilitado	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 Protección contra amenazas avanzada de Windows Defender	Sense	Deshabilitado	Configurado		
Servicio de protocolo de túnel de sockets seguros	SstpSvc	Deshabilitado	Configurado		
Servicio de prueba comercial	RetailDemo	Deshabilitado	Configurado		
Servicio de publicación de nombres de equipo PNRP	PNRPAutoReg	Deshabilitado	Configurado		
Servicio de publicación World Wide Web	W3SVC	Deshabilitado	Configurado		
Servicio de puerta de enlace de audio de Bluetooth	BTAGService	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de puerta de enlace de nivel de aplicación	ALG	Deshabilitado	Configurado		
Servicio de red de host	hns	Deshabilitado	Configurado		
Servicio de red de Xbox Live	XboxNetApiSvc	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		
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		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio de virtualización de Escritorio remoto de Hyper-V	vmicrdv	Deshabilitado	Configurado		
Servicio de virtualización de la experiencia de usuario	UevAgentService	Deshabilitado	Configurado		
Servicio de virtualización de red	nvagent	Deshabilitado	Configurado		
Servicio de Windows Defender	WinDefend	Deshabilitado	Configurado		
Servicio de Windows Insider	wisvc	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 FrameServer de la Cámara de Windows	FrameServer	Deshabilitado	Configurado		
Servicio FTP de Microsoft	ftpsvc	Deshabilitado	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	Deshabilitado	Configurado		
Servicio MultiPoint	Wms	Deshabilitado	Configurado		
Servicio PowerShell Direct de Hyper-V	vmicvmsession	Deshabilitado	Configurado		

Comprobación	OK/NOK	Cómo hacerlo			
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK	
Servicio PushToInstall de Windows	PushToInstall	Deshabilitado	Configurado		
Servicio Recopilador estándar del concentrador de diagnósticos de Microsoft (R)	diagnosticshub.standard.collector.service	Deshabilitado	Configurado		
Servicio Seguridad de Windows	SecurityHealthService	Manual	Configurado		
Servicio SNMP	SNMP	Deshabilitado	Configurado		
Servicio telefónico	PhoneSvc	Deshabilitado	Configurado		
Servicio Volumetric Audio Compositor	VacSvc	Deshabilitado	Configurado		
Servicio WAS (Windows Process Activation Service)	WAS	Deshabilitado	Configurado		
Servicios de cifrado	CryptSvc	Automático	Configurado		
Servicios de Escritorio remoto	TermService	Deshabilitado	Configurado		
Servicios simples de TCP/IP	simptcp	Deshabilitado	Configurado		
Servidor	LanmanServer	Deshabilitado	Configurado		
Servidor de roles de DS	DsRoleSvc	Deshabilitado	Configurado		
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		
SMP de Espacios de almacenamiento de Microsoft	smphost	Manual	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		

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)	Servicio (nombre corto)	Inicio	Permiso	OK/NOK
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	wuauerv	Deshabilitado	Configurado	
Windows Update Medic Service	WaaSMedicSvc	Deshabilitado	Configurado	
Xbox Accessory Management Service	XboxGipSvc	Deshabilitado	Configurado	
186.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: 		

Comprobación	OK/NOK	Cómo hacerlo																
		En la ventana de “Propiedades”, seleccione la pestaña “Seguridad” y pulse sobre “Opciones Avanzadas”.  Nota: En el caso de estar usando un usuario perteneciente a la unidad organizativa “Usuarios Windows 10” éste no podrá ver la pestaña seguridad por lo que deberá utilizar un usuario que este fuera de dicha unidad organizativa. Así mismo, es posible que requiera de permisos adicionales para poder visualizar los permisos de los diferentes ficheros. En la pestaña “Permisos” de la ventana “Configuración avanzada de <archivo a comprobar>” observe los permisos y compárelos con la siguiente tabla:  <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>SYSTEM</td><td>Control total</td><td>Ninguno</td></tr><tr><td>Perm...</td><td>Administradores (W10CL01\Administradores)</td><td>Control total</td><td>Ninguno</td></tr><tr><td>Perm...</td><td>Usuarios de shells (DOMINIO\Usuarios de s...</td><td>Lectura y ejecución</td><td>Ninguno</td></tr></tbody></table> 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. En las cuentas de dominio, resaltadas con fondo gris en la siguiente tabla, aparecerá el nombre de su dominio en lugar de "DOMINIO". Además, 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”.	Tipo	Entidad de seguridad	Acceso	Heredada de	Perm...	SYSTEM	Control total	Ninguno	Perm...	Administradores (W10CL01\Administradores)	Control total	Ninguno	Perm...	Usuarios de shells (DOMINIO\Usuarios de s...	Lectura y ejecución	Ninguno
Tipo	Entidad de seguridad	Acceso	Heredada de															
Perm...	SYSTEM	Control total	Ninguno															
Perm...	Administradores (W10CL01\Administradores)	Control total	Ninguno															
Perm...	Usuarios de shells (DOMINIO\Usuarios de s...	Lectura y ejecución	Ninguno															

Comprobación	OK/NOK	Cómo hacerlo	
Archivo	Usuario	Permiso	OK/NOK
%ProgramFiles%\NetMeeting	Administrador	Control total	
	System	Control total	
%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 ⁸	
	SYSTEM	Control Total	
	Usuarios	Lectura	
%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	
	Usuarios	Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura	
%SystemRoot%\repair	Administradores	Control Total	
	SYSTEM	Control Total	
%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\cacls.exe	Administradores	Control Total	
	SYSTEM	Control Total	
%SystemRoot%\system32\clip.exe	Administradores	Control Total	
	SYSTEM	Control Total	

⁸ 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".

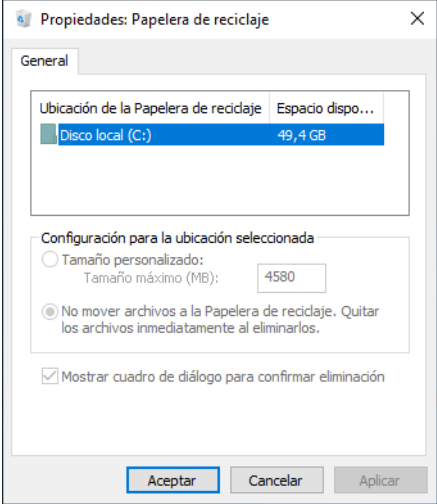
Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\cmd.exe		Administradores	Control Total	
		SYSTEM	Control Total	
		Usuarios de shells	Lectura y ejecución, Lectura	
%SystemRoot%\system32\cscript.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\debug.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\edit.com		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\edlin.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\hostname.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\ipconfig.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nbtstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\net.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\netstat.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\nslookup.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\ntbackup.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\ping.exe		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\rasctrm.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	

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\system32\rasmans.dll		Administradores	Control Total	
%SystemRoot%\system32\rasmontr.dll		Administradores	Control Total	
%SystemRoot%\system32\rasmxs.dll		Administradores	Control Total	
%SystemRoot%\system32\rasphone.exe		Administradores	Control Total	
%SystemRoot%\system32\rasppp.dll		Administradores	Control Total	
%SystemRoot%\system32\rasrad.dll		Administradores	Control Total	
%SystemRoot%\system32\rasser.dll		Administradores	Control Total	
%SystemRoot%\system32\rastapi.dll		Administradores	Control Total	
%SystemRoot%\system32\rastls.dll		Administradores	Control Total	
%SystemRoot%\system32\rcp.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\regedt32.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\regsvr32.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\rexec.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\route.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\rsh.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\sysedit.exe		Administradores	Control Total	
		SYSTEM	Control Total	
%SystemRoot%\system32\telnet.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\WindowsPowerShell\v1.0\PowerShell.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%\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe	Administradores	Control Total		
	SYSTEM	Control Total		
	Usuarios de shells	Lectura y ejecución, Lectura		
%SystemRoot%\system32\winmsd.exe	Administradores	Control Total		
	SYSTEM	Control Total		
%SystemRoot%\system32\wscript.exe	Administradores	Control Total		
	SYSTEM	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		
%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		

Comprobación	OK/NOK	Cómo hacerlo		
Archivo		Usuario	Permiso	OK/NOK
%SystemRoot%\syswow64\raschap.dll		Administradores	Control Total	
%SystemRoot%\syswow64\rasctrnm.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	
%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	
187.Compruebe las entradas en el registro		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:		

Comprobación	OK/NOK	Cómo hacerlo		
		Clave	Valor	OK/NOK
		HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\tcpip6\Parameters\DisabledComponents	ffffff (0xffffffff)	
		HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\LaunchTo	1	
		HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsHistory	1	
		HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecentDocsMenu	1	
		HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClearRecentDocsOnExit	1	
		HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRecycleFiles	1	
		HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ConfirmFileDelete	1	
188.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:		
		Nota: Para ejecutar esta comprobación será necesario que el usuario que va a realizarla no se encuentre en la unidad organizativa “Usuarios Windows 10”.		
		Tarea programada		OK/NOK
		Microsoft\XblGameSave\XblGameSaveTask		
		Microsoft\Windows\Maps\MapsToastTask		
		Microsoft\Windows\HelloFace\FODCleanupTask		
	Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser			

Comprobación	OK/NOK	Cómo hacerlo
189.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.	
190.Borre el directorio "C:\Scripts"		Borre el directorio "C:\Scripts" con todo su contenido.
191.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. Nota: Si movió temporalmente un usuario administrador en Active Directory a la unidad organizativa "Usuarios Windows 10" para realizar los pasos de la lista de comprobación en el equipo que está comprobando, devuelva dicho usuario a su ubicación original a través de la herramienta "Usuarios y equipos de Active Directory" en el controlador de dominio.

ANEXO D.2. TAREAS ADICIONALES DE CONFIGURACIÓN DE SEGURIDAD

ANEXO D.2.1. 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), miembro 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 el siguiente enlace:

<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 hecho 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 miembro de un dominio, con sistema operativo Windows 10 versión 1809, 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 adicionales a cumplir tras 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.

Algunas de las acciones descritas en esta guía deberán llevarse a cabo en un controlador de dominio al que pertenezca el equipo cliente y otras en el propio equipo cliente.

3. REQUISITOS HARDWARE Y SOFTWARE

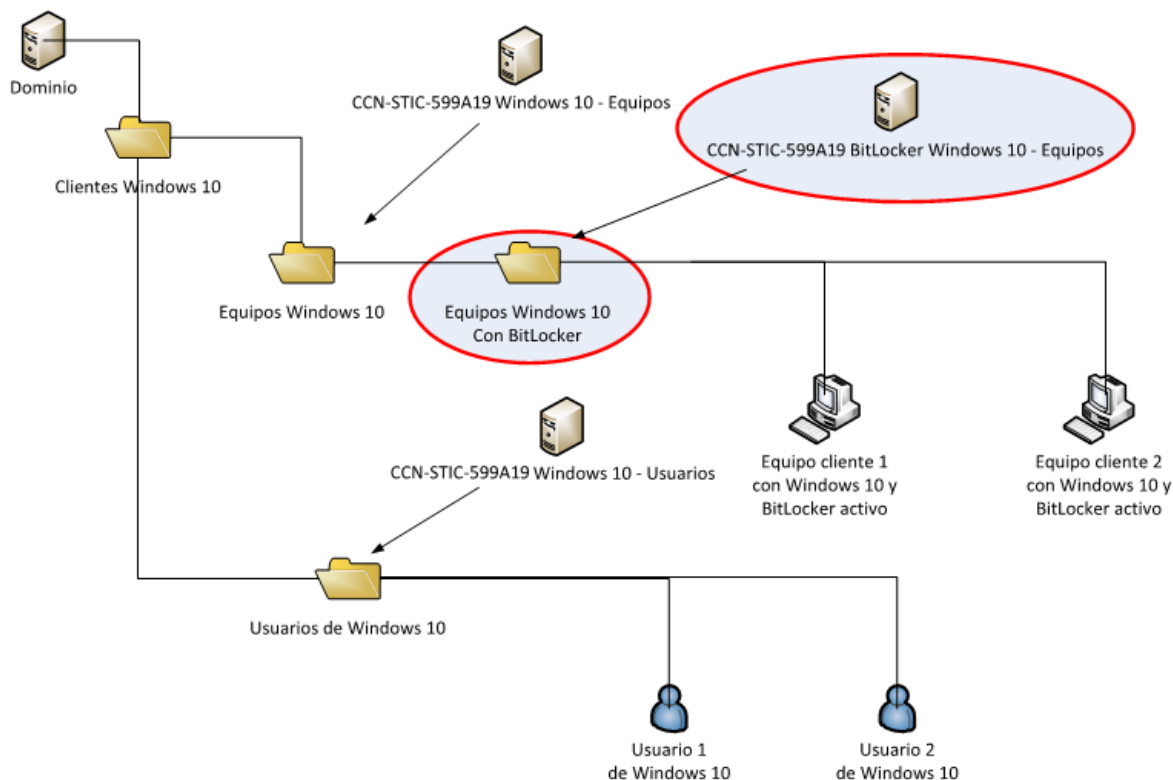
La implementación del cifrado de unidad BitLocker tiene los siguientes requisitos de hardware y software:

- a) Un equipo que cumpla los requisitos mínimos para Windows 10 (BitLocker no está disponible en la edición Windows 10 Home).
- 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.

4. OBJETO DE DIRECTIVA DE GRUPO (GPO)

En este apartado se documentan las configuraciones de un objeto de directiva de grupo específico para el cifrado de disco con BitLocker. Esta GPO se deberá aplicar de forma incremental sobre el equipo, complementando las configuraciones definidas en las otras GPOs definidas en esta guía. El orden de aplicación deberá ser tal que las configuraciones definidas en esta GPO específica de BitLocker tengan prioridad sobre las definidas en las otras GPOs de esta guía.

Para aplicar correctamente las configuraciones de esta GPO, que se llamará "CCN-STIC-599A19 BitLocker Windows 10 - Equipos", se creará en Active Directory una nueva unidad organizativa que se llamará "Equipos Windows 10 con BitLocker", específica para equipos Windows 10 con BitLocker, dentro de la unidad organizativa "Equipos Windows 10", como muestra la siguiente figura.



La configuración sólo afectará a la parte de "Configuración del Equipo" de la GPO. No será necesario definir ninguna configuración adicional en la parte de "Configuración de Usuario".

4.1. SERVICIOS DEL SISTEMA

La implementación del cifrado de unidad BitLocker para esta guía, requiere que se configuren los servicios del sistema mostrados en la siguiente tabla de la manera en que en ella se indica.

La configuración de estos servicios se puede realizar en un objeto de directiva de grupo (GPO), utilizando la consola de administración "Editor de administración de directivas de grupo", en la siguiente ubicación:

"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"

Servicio	Inicio	Permiso
Servicio Cifrado de unidad BitLocker (BDESVC)	Automático	Configurado
Detección de hardware Shell (shellhwdetection)	Automático	Configurado

4.2. PLANTILLAS ADMINISTRATIVAS (EQUIPO)

A continuación, se describen los valores relacionados con la configuración de “Cifrado de unidad BitLocker”, que se establecen dentro del apartado "Plantillas Administrativas", dentro de la sección "Configuración de equipo", de una GPO.

Las siguientes tablas indican la GPO, sus valores y una descripción. Estos valores se establecen en las ubicaciones indicadas al comienzo de cada tabla.

“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker”

Servicio	Inicio	Permiso
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	Permite configurar el algoritmo y la intensidad del cifrado que se usan en el Cifrado de unidad BitLocker.
Impedir la sobreescritura de memoria al reiniciar	Deshabilitada	Los secretos de BitLocker se quitan de la memoria al reiniciarse el equipo.

“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades de datos extraíbles”

Servicio	Inicio	Permiso
Controlar el uso de BitLocker en unidades extraíbles	Deshabilitada	Si deshabilita esta configuración de directiva, los usuarios no podrán usar BitLocker en unidades de datos extraíbles.

“Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker → Unidades del sistema operativo”

Servicio	Inicio	Permiso
Configurar longitud mínima de PIN para el inicio	Habilitada, 8	Esta configuración de directiva le permite configurar una longitud mínima para un PIN de inicio del Módulo de plataforma segura (TPM). Se aplica al activar BitLocker. El PIN de inicio debe tener una longitud mínima de 4 dígitos y una longitud máxima de 20 dígitos.

Servicio	Inicio	Permiso
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	Si habilita esta configuración de directiva antes de activar BitLocker, puede configurar los componentes de arranque que el TPM validará antes de desbloquear el acceso a la unidad del sistema operativo cifrada mediante BitLocker. Si cualquiera de estos componentes cambia mientras la protección del BitLocker permanece activa, el TPM no liberará la clave de cifrado para desbloquear la unidad; en su lugar, el equipo mostrará la consola de recuperación de BitLocker y solicitará que se proporcione la contraseña de recuperación o la clave de recuperación para desbloquear la unidad.
Permitir los PIN mejorados para el inicio	Habilitada	Los PIN de inicio mejorados permiten el uso de caracteres en mayúsculas y minúsculas, símbolos, números y espacios. Nota: No todos los equipos admiten los PIN mejorados en el entorno previo al arranque. Se recomienda que los usuarios realicen una comprobación del sistema al instalar BitLocker.
Requerir autenticación adicional al iniciar	Habilitada, Requerir PIN de inicio con TPM (no permitir los demás)	Esta configuración de directiva le permite configurar si BitLocker requiere autenticación adicional cada vez que se inicia el equipo y si se usa BitLocker con un Módulo de plataforma segura (TPM).

5. GUIA PASO A PASO – BITLOCKER

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

Antes de empezar se deberá tener en cuenta los siguientes requisitos:

- Un equipo que cumpla los requisitos mínimos para Windows 10 (BitLocker no está disponible en la edición Windows 10 Home).
- Un microchip TPM, versión 1.2 o superior, activado.
- BIOS compatible con TCG (Trusted Computing Group).

- d) Una partición de disco para la unidad del sistema. En Windows 10, si cuenta con una sola partición de disco para la unidad del sistema operativo, BitLocker preparará automáticamente la unidad; para ello, reducirá el tamaño de la unidad del sistema operativo y creará una nueva partición del sistema para usarla para 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.

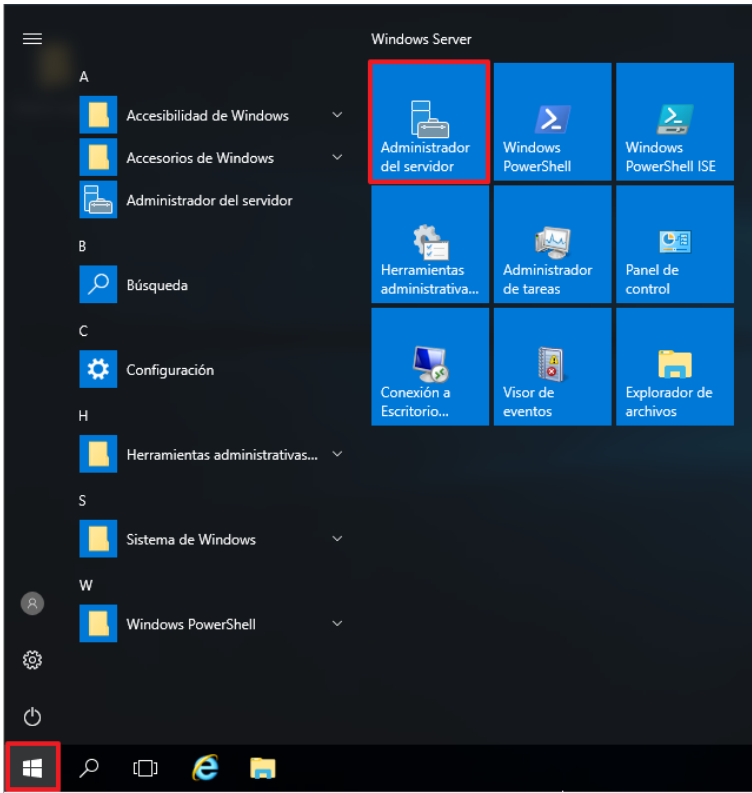
- e) Una unidad flash USB para almacenar claves de inicio y recuperación.
- f) Una configuración BIOS para iniciar primero desde el disco duro, no las unidades USB o CD. No obstante, en cualquier escenario en el que se use una unidad flash USB para proporcionar una clave de BitLocker (como una clave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

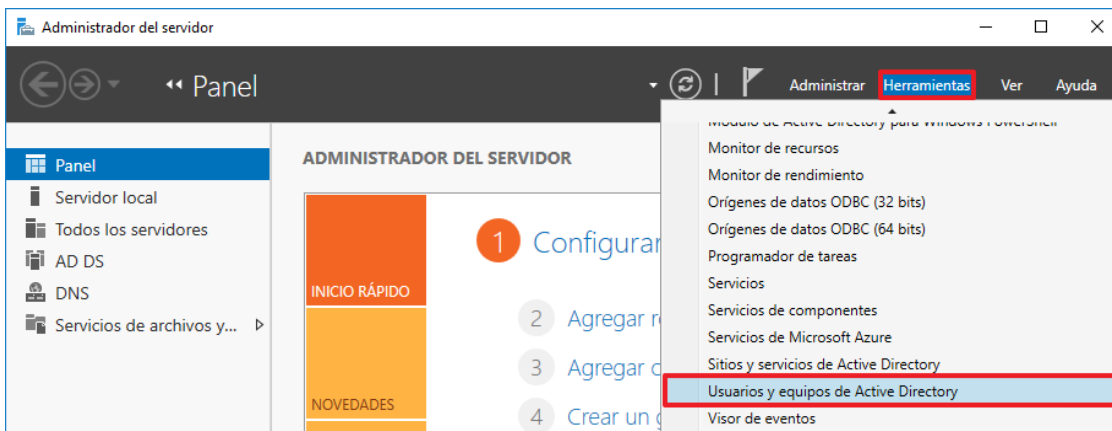
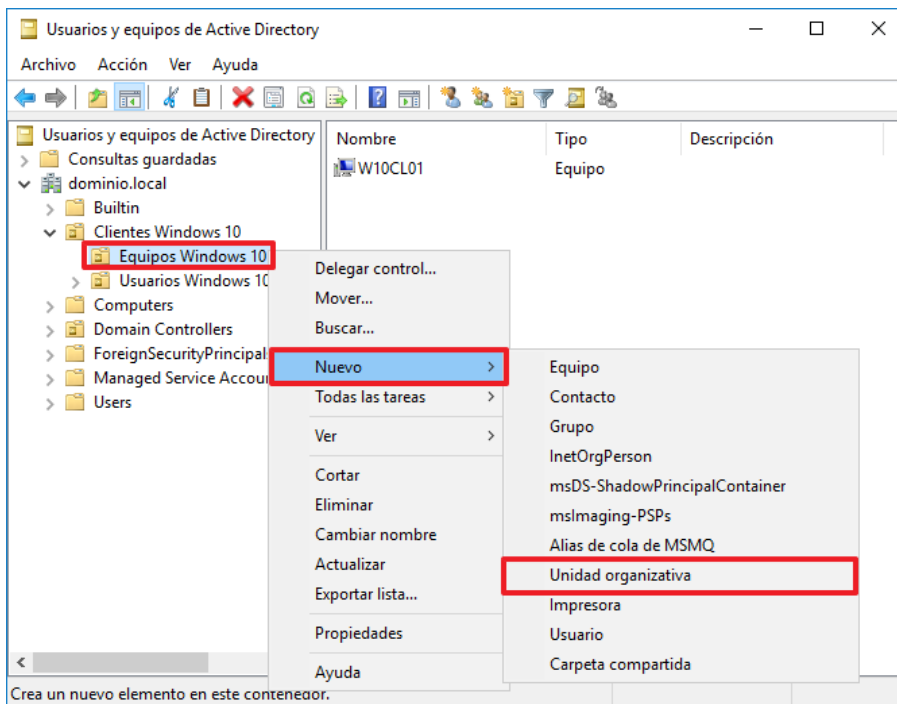
Nota: Tenga en cuenta que el acceso a las impresoras puede estar deshabilitado, debido a la aplicación de la configuración de seguridad implementada. Recuerde que antes de realizar este paso a paso necesitará de una unidad para almacenar las claves necesarias por lo que deberá aplicar la configuración para utilizar el dispositivo de almacenamiento descrito en el “ANEXO D.2.2 DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19”.

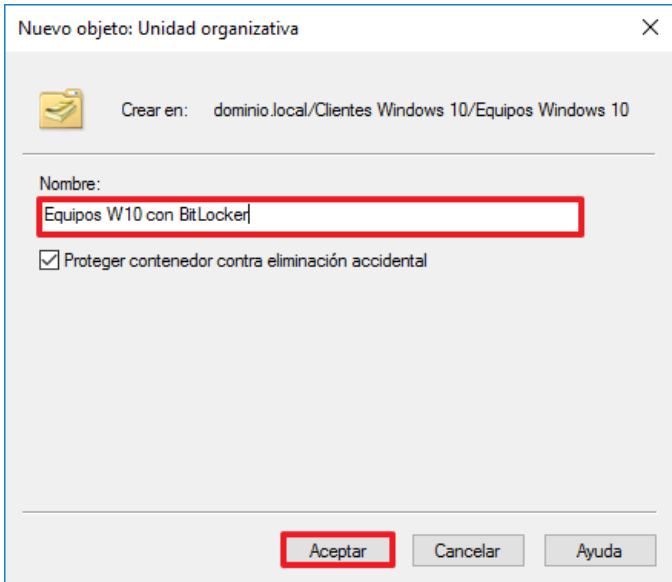
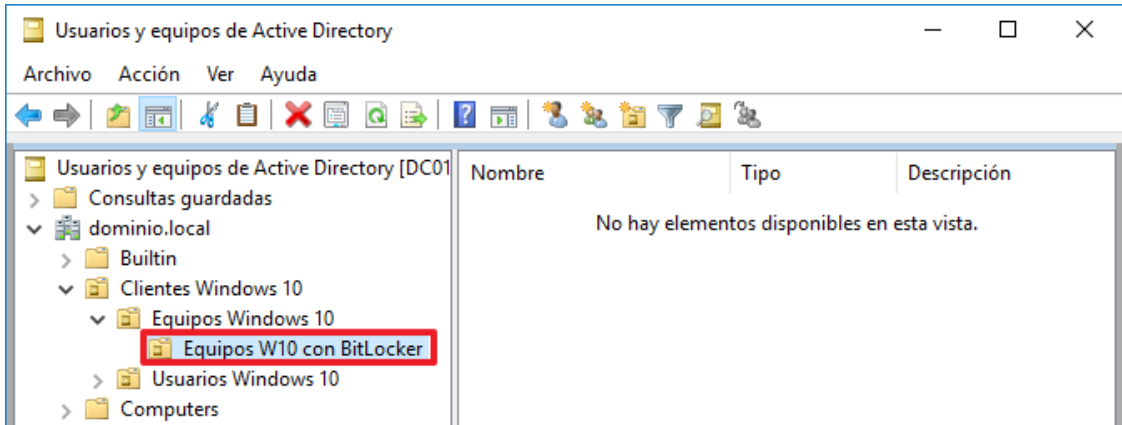
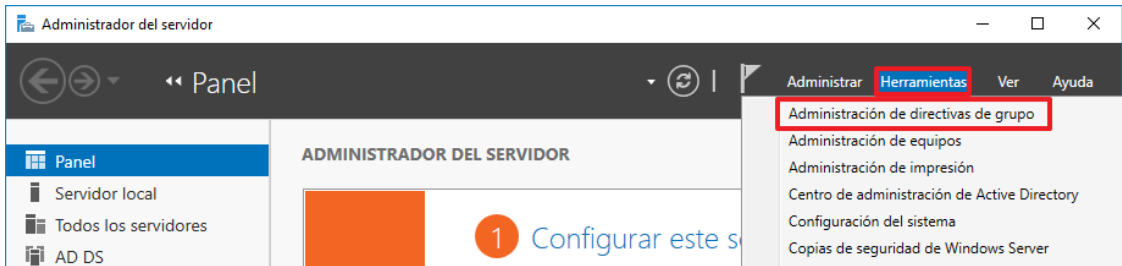
El primer conjunto de acciones deberá realizarlos en un controlador de dominio del dominio al que pertenece el equipo cliente que está asegurando. Estos pasos sólo se realizarán cuando se configure BitLocker en el primer equipo cliente Windows 10 miembro de dominio, ya que crear la unidad organizativa necesaria e incorporar las configuraciones recomendadas en esta guía en un objeto de directiva de grupo, sólo es necesario realizarlo la primera vez.

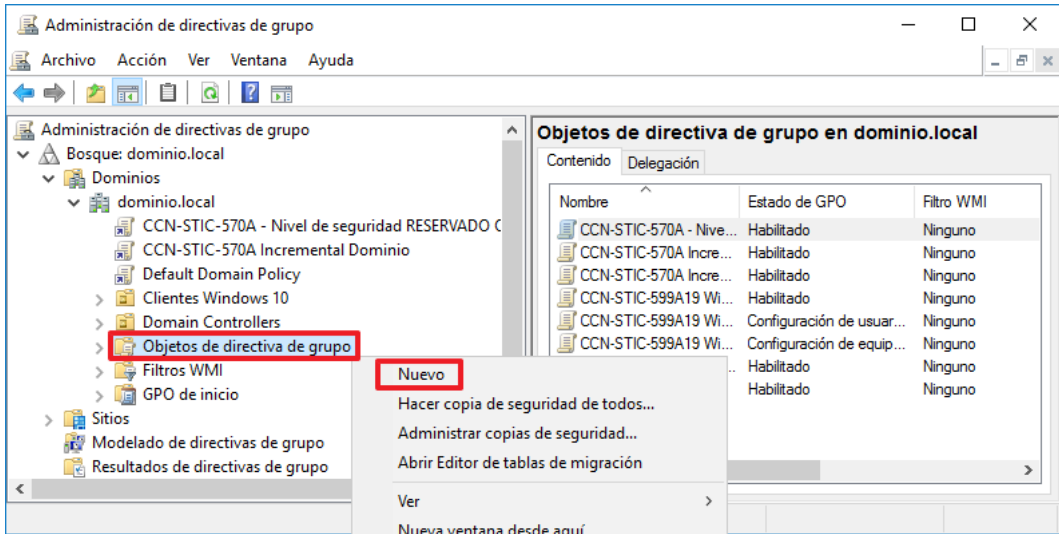
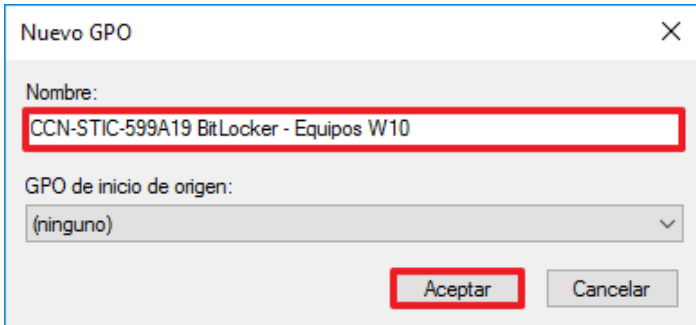
Para la configuración de BitLocker en el resto de clientes Windows 10, miembros del mismo dominio, deberá saltar estos pasos e ir directamente al paso 34, ya que esos clientes compartirán la configuración establecida en este punto y automáticamente recibirán las configuraciones al incluirse en la Unidad Organizativa "Equipos W10 con BitLocker".

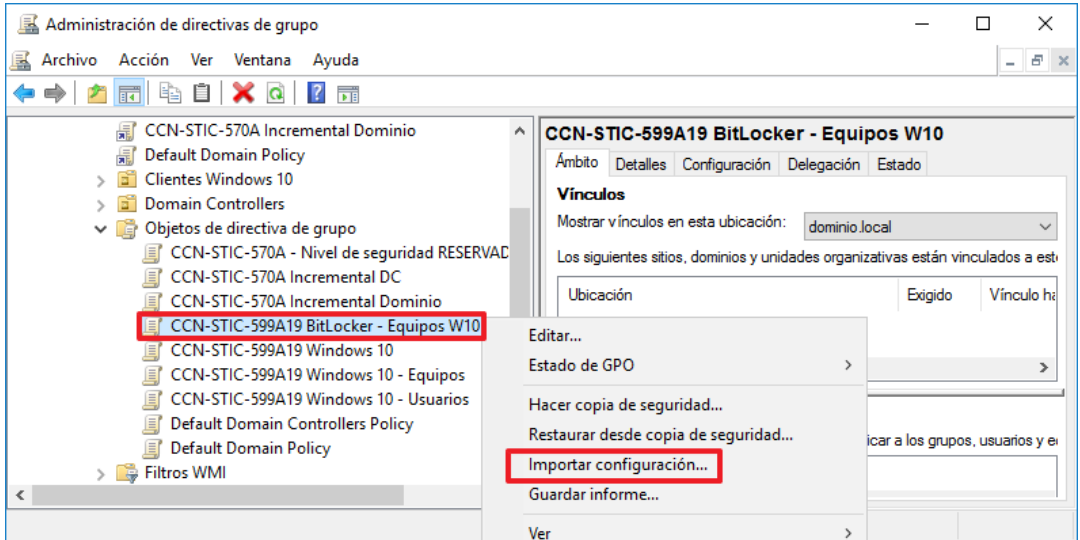
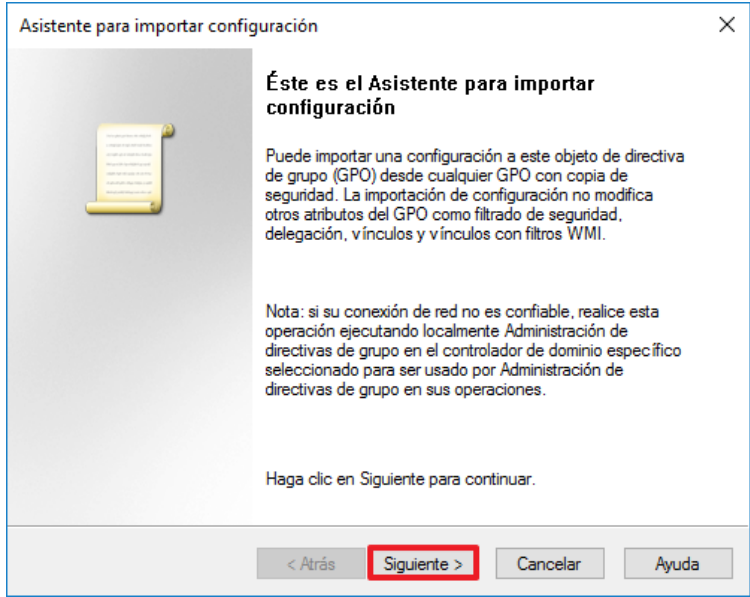
Nota: Esta guía paso a paso para la configuración de BitLocker, asume que a los servidores controladores del dominio al que pertenece el equipo cliente en el que se va a configurar BitLocker, se les ha aplicado la configuración descrita en la guía CCN-STIC-570A IMPLEMENTACIÓN DE SEGURIDAD SOBRE MICROSOFT WINDOWS SERVER 2016, y que al propio cliente Windows 10 miembro del dominio se le ha aplicado la configuración de seguridad recomendada en la presente guía. Así mismo, si se va a emplear el navegador Internet Explorer 11, será necesario haber implementado la guía CCN-STIC-520 – Internet Explorer 11. Si no es así, aplique primero dichas guías a los controladores de dominio y al equipo cliente, antes de continuar con la configuración de BitLocker.

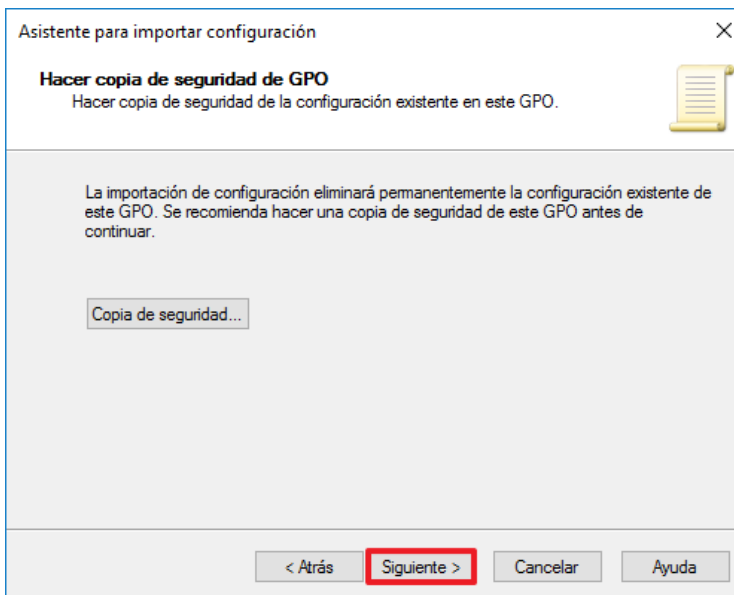
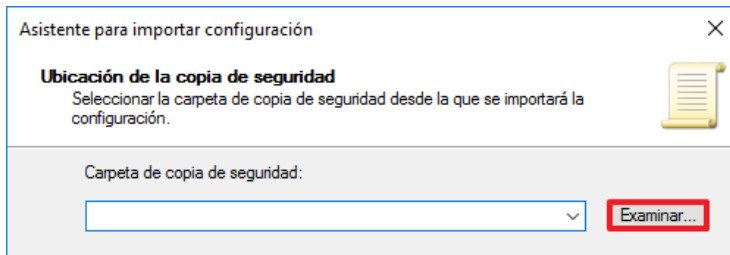
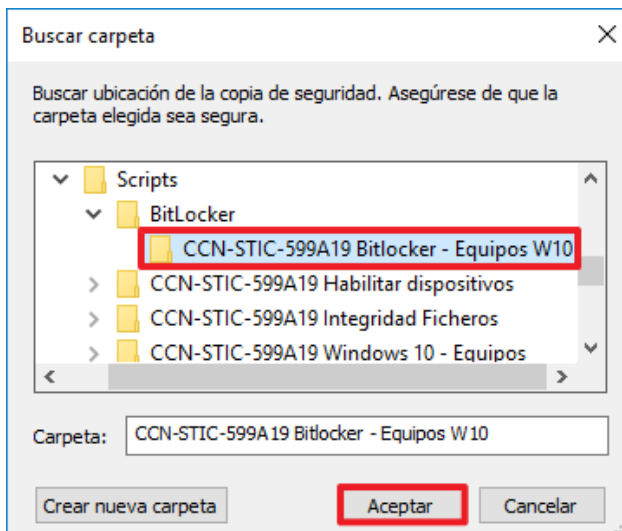
Paso	Descripción
1.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio. Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”. 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.	Asegúrese de que al menos el siguiente directorio haya sido copiado al directorio “C:\Scripts\BitLocker” del controlador de dominio. – CCN-STIC-599A19 – BitLocker Equipos W10
5.	Cree la unidad organizativa "Equipos W10 con BitLocker". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente del menú inicio.  Nota: El sistema le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio.

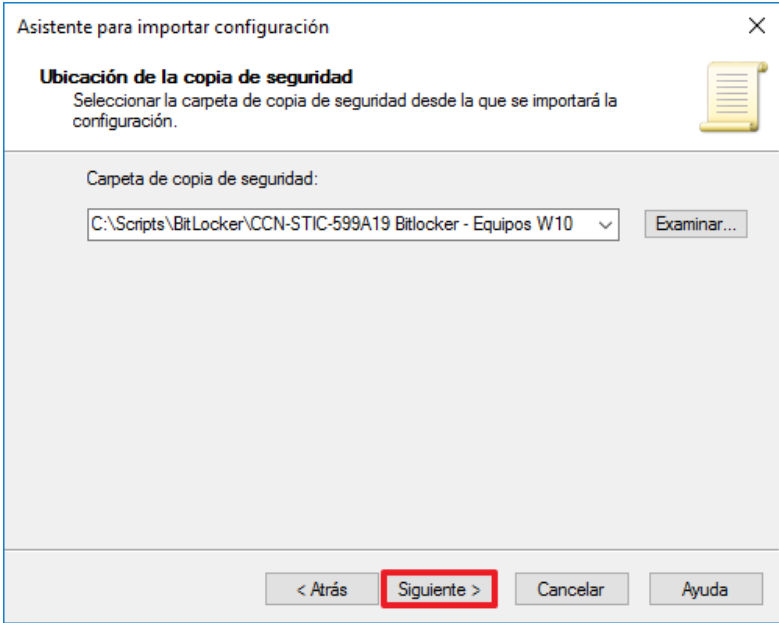
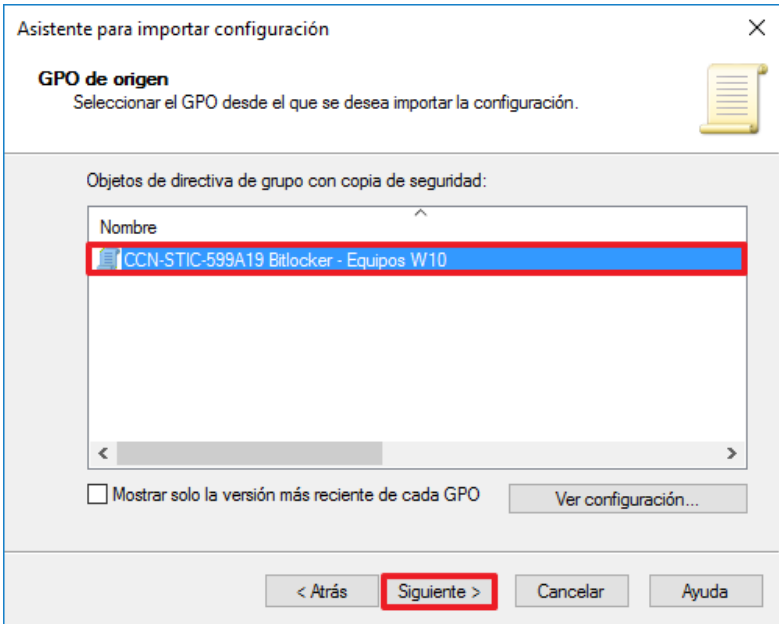
Paso	Descripción
6.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual que se ha desplegado “Usuarios y equipos de Active Directory”. 
7.	En la consola “Usuarios y equipos de Active Directory” sitúese sobre la unidad organizativa “Equipos Windows 10” y, pulsando con el botón derecho del ratón, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá, como se muestra en la siguiente figura. 

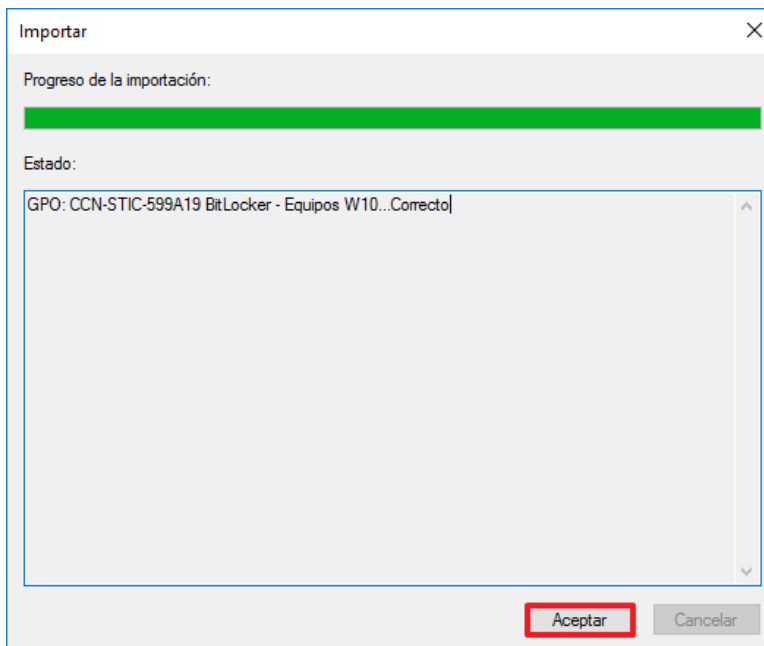
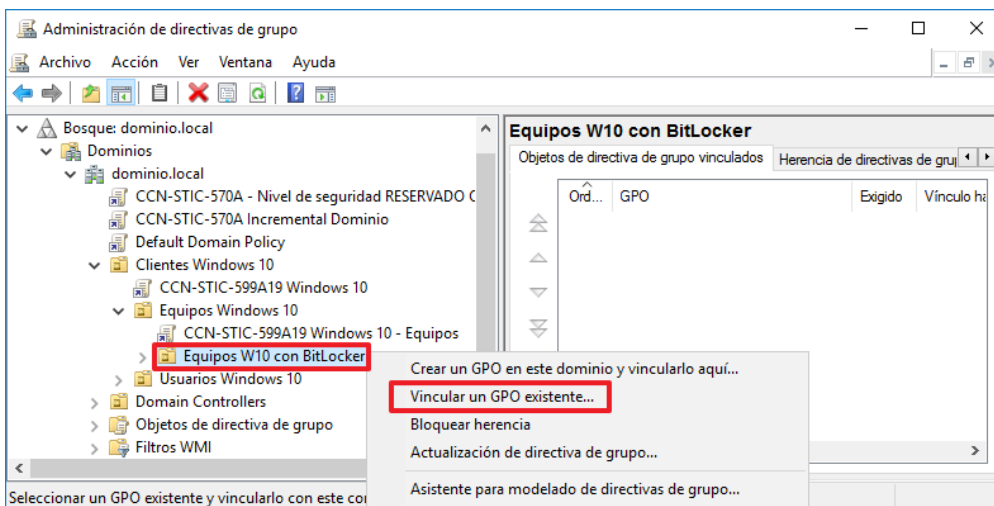
Paso	Descripción
8.	Asigne el nombre "Equipos W10 con BitLocker" a la nueva unidad organizativa, rellenando con este nombre el campo "Nombre:" del cuadro de diálogo que aparecerá y deje marcada la opción "Proteger contenedor contra eliminación accidental". A continuación, pulse "Aceptar". 
9.	Compruebe que la nueva unidad organizativa aparece colgando de "Equipos Windows 10" como se muestra en la siguiente figura. 
10.	De nuevo, utilizando la herramienta "Administrador del servidor", Seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 

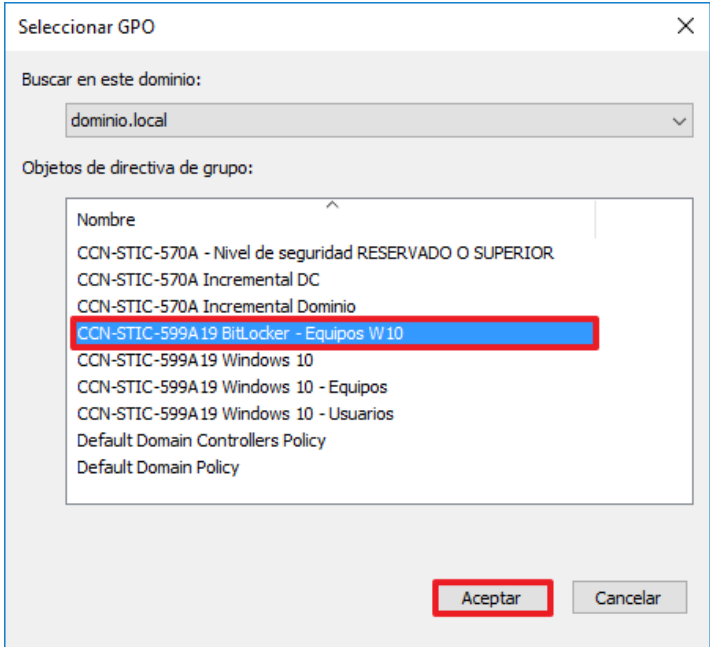
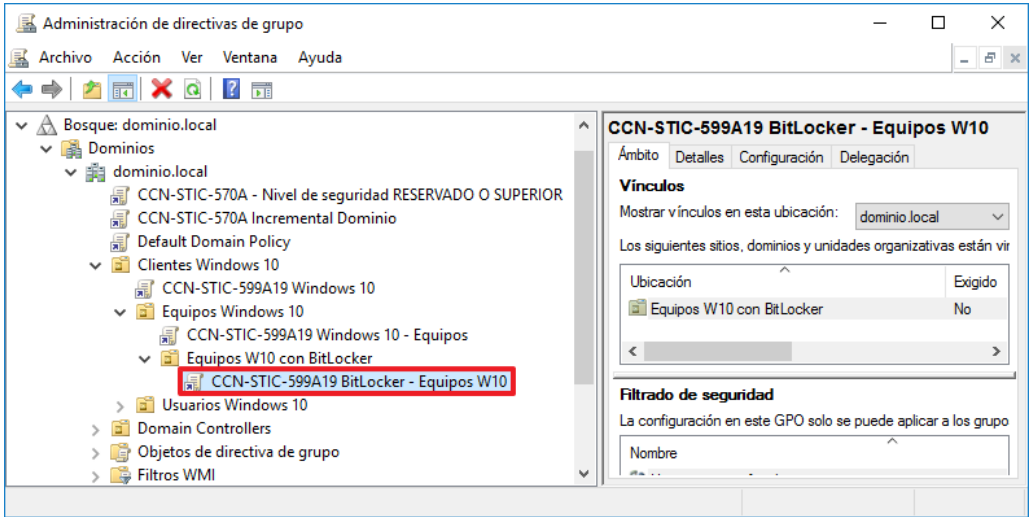
Paso	Descripción
11.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>" A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPO correspondientes. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores de este contenedor recién expandido (<nombre de su dominio>).
12.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" con el botón derecho y elija la opción "Nuevo" del menú contextual que aparecerá. 
13.	Asigne el siguiente nombre "CCN-STIC-599A19 BitLocker – Equipos W10" a la nueva GPO y pulse “Aceptar”. 

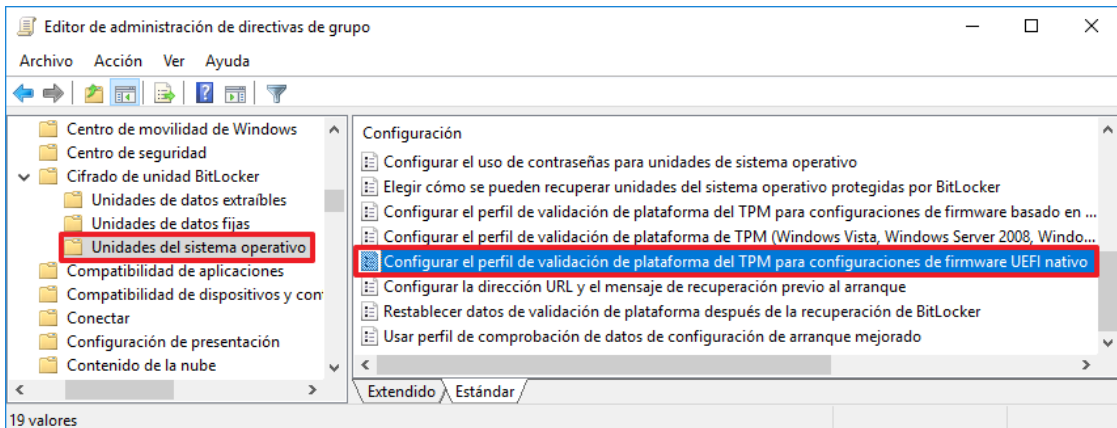
Paso	Descripción
14.	Seleccione la GPO recién creada, "CCN-STIC-599A19 BitLocker – Equipos W10" y, marcando con el botón derecho en ella, elija la opción "Importar configuración..." en el menú contextual que aparecerá. 
15.	En el "Asistente para importar configuración" pulse "Siguiente >". 

Paso	Descripción
16.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiete >" en la ventana "Hacer copia de seguridad de GPO". 
17.	En "Ubicación de la copia de seguridad" pulse sobre el botón "Examinar...". 
18.	Localice la carpeta "CCN-STIC-599A19 Windows 10- Equipos" y pulse "Aceptar". 

Paso	Descripción
19.	Pulse “Siguiente >” para continuar. 
20.	En “GPO de origen” pulse “Siguiente >”. 
21.	En “Examinar copia de seguridad” pulse “Siguiente >”.
22.	Pulse “Finalizar” para realizar la importación.

Paso	Descripción
23.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 
24.	Utilizando de nuevo la herramienta de “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 

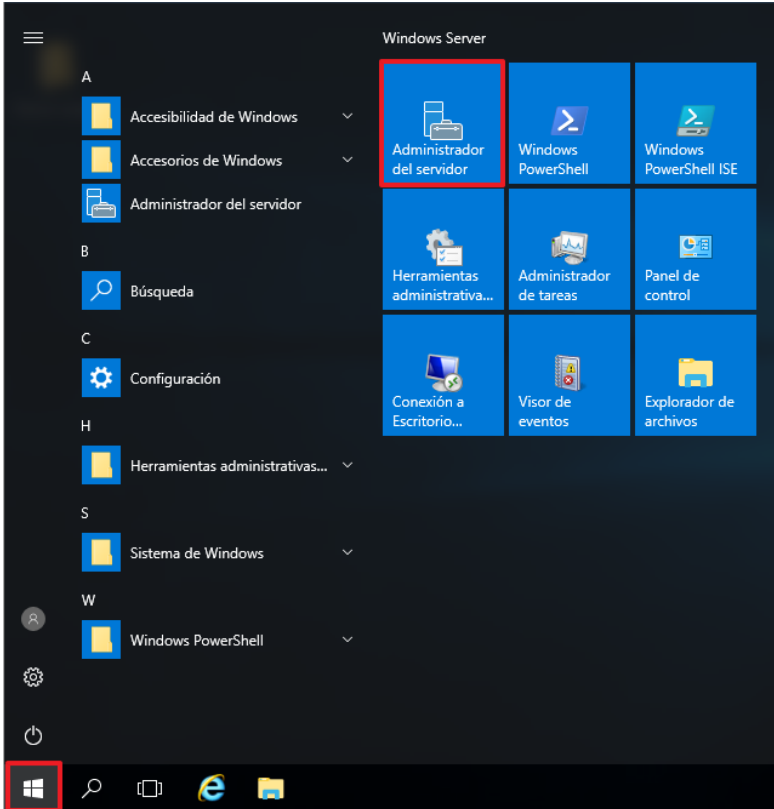
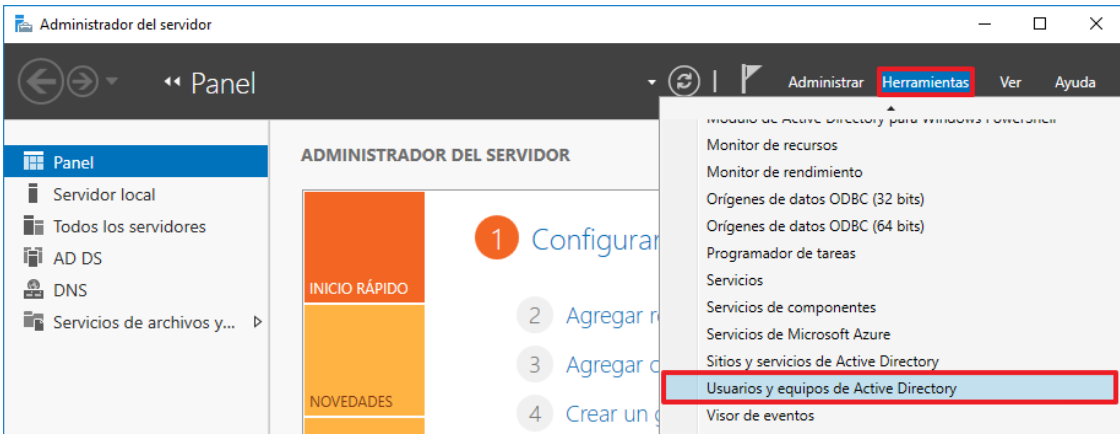
Paso	Descripción
25.	Seleccione “CCN-STIC-599A19 BitLocker – Equipos W10 - Equipos” de la lista y pulse “Aceptar”. 
26.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Equipos W10 con BitLocker”. 

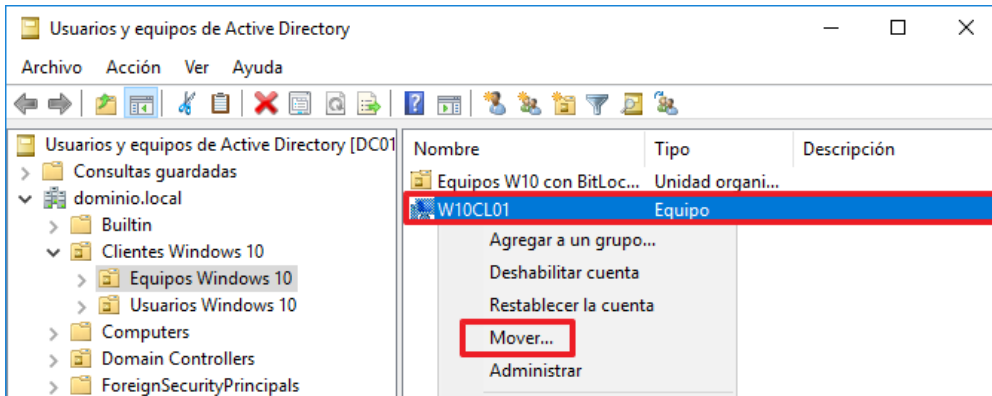
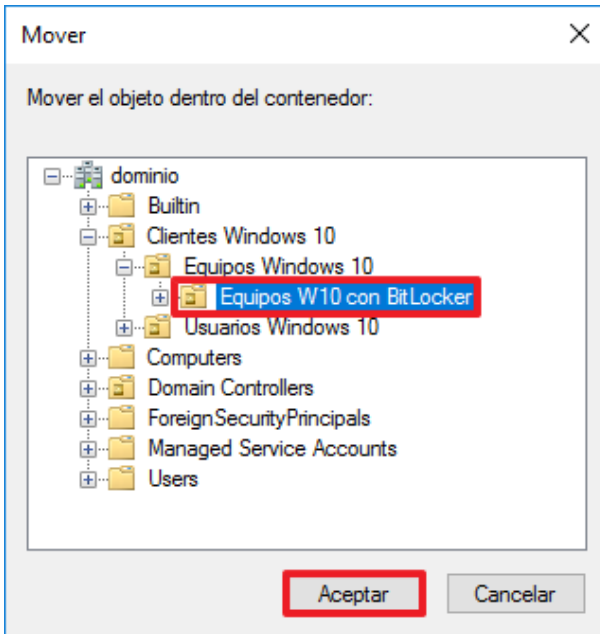
Paso	Descripción
27.	La configuración importada en la GPO desde la copia de seguridad establece la seguridad de BitLocker para firmware basado en BIOS o equipos con firmware UEFI con un módulo de servicio de compatibilidad (CSM) habilitado. Si dispone de equipos con firmware UEFI nativo, deberá habilitar y configurar la directiva “Directiva CCN-STIC-599A19 BitLocker – Equipos W10 → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker Unidades del sistema operativo → Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo” de la GPO configurada en este apartado.  The screenshot shows the Group Policy Editor window. In the left-hand navigation pane, the path is expanded: 'Centro de seguridad' > 'Cifrado de unidad BitLocker' > 'Unidades del sistema operativo'. The 'Unidades del sistema operativo' folder is highlighted with a red box. In the right-hand pane, the list of policies is shown, and the policy 'Configurar el perfil de validación de plataforma del TPM para configuraciones de firmware UEFI nativo' is highlighted with a red box. Below the list, the 'Extendido' tab is selected.

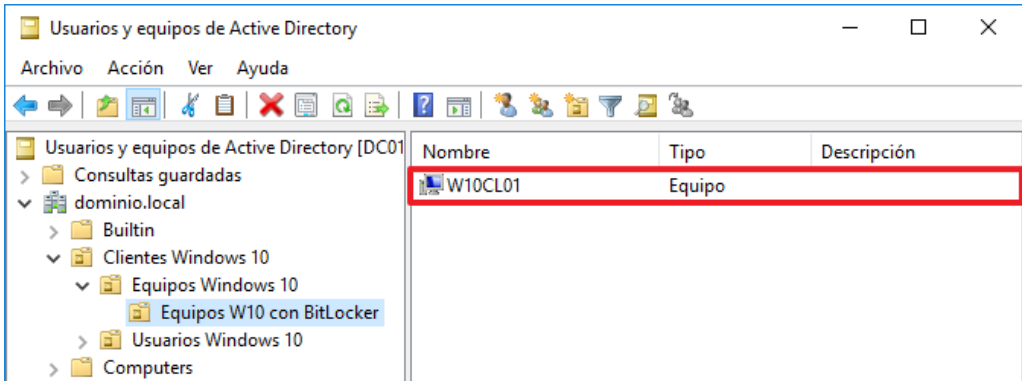
En este punto, la unidad organizativa "Equipos W10 con BitLocker" y la GPO "CCN-STIC-599A19 BitLocker - Equipos W10" están ya configuradas correctamente en Active Directory y la configuración de este último se aplicará automáticamente al equipo cliente Windows 10 miembro del dominio en el que está configurando BitLocker, y a los futuros equipos cliente Windows 10 miembros del dominio en los que también lo configure.

Los siguientes pasos deberá realizarlos en un controlador de dominio del dominio al que pertenece el equipo que está asegurando, y deberá realizarlos cada vez que necesite configurar BitLocker en un nuevo equipo cliente Windows 10 miembro del dominio, ya que se trata de trasladar, en Active Directory, la cuenta de equipo del equipo en el que está configurando BitLocker, a la unidad organizativa "Equipos W10 con BitLocker".

Paso	Descripción
28.	Inicie sesión en un servidor controlador de dominio del dominio al que pertenece el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.

Paso	Descripción
29.	Traslade, en Active Directory, la cuenta de equipo del equipo en el que está configurando BitLocker, desde su ubicación actual hasta su nueva ubicación: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker" Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
30.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Usuarios y equipos de Active Directory". 

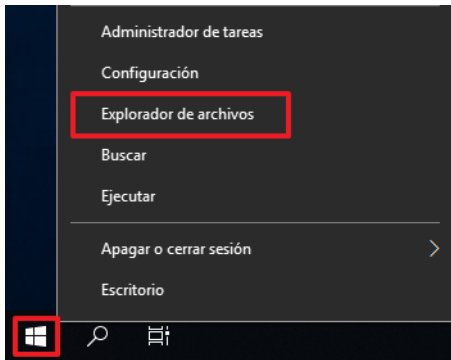
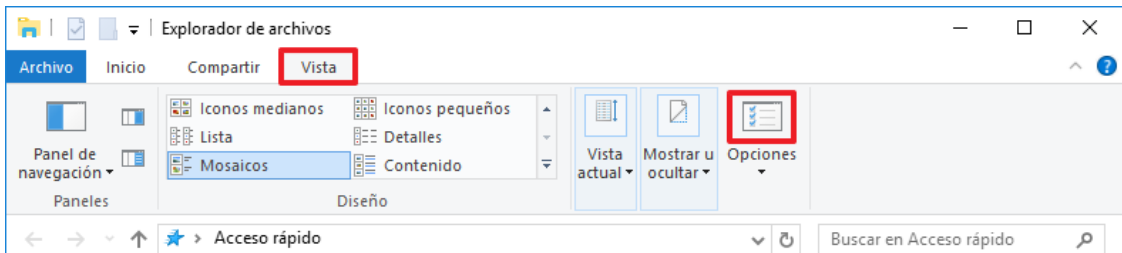
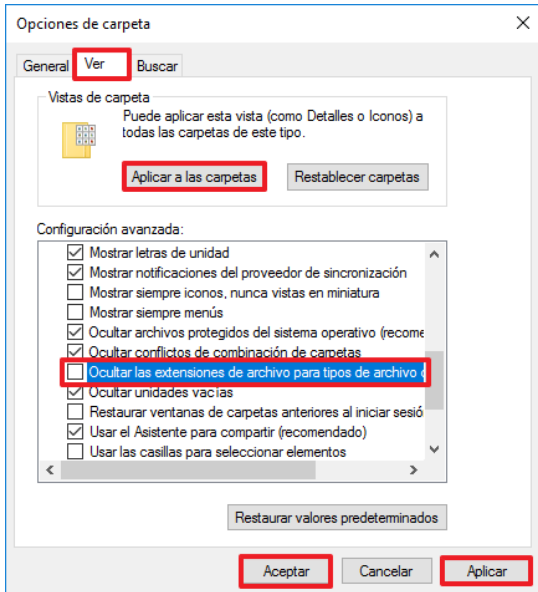
Paso	Descripción
31.	Seleccione entonces, en la parte central de la ventana, la cuenta del equipo a trasladar con el botón derecho del ratón y seleccione la opción "Mover..." del menú contextual que aparecerá, como se muestra en la siguiente figura.  Nota: En este ejemplo el nombre del equipo en el que se está configurando BitLocker se supone que es "W10CL01"
32.	En el cuadro de diálogo que aparecerá, titulado "Mover", seleccione el contenedor destino en la siguiente ruta: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker" Pulse "Aceptar" para cerrar la ventana. 

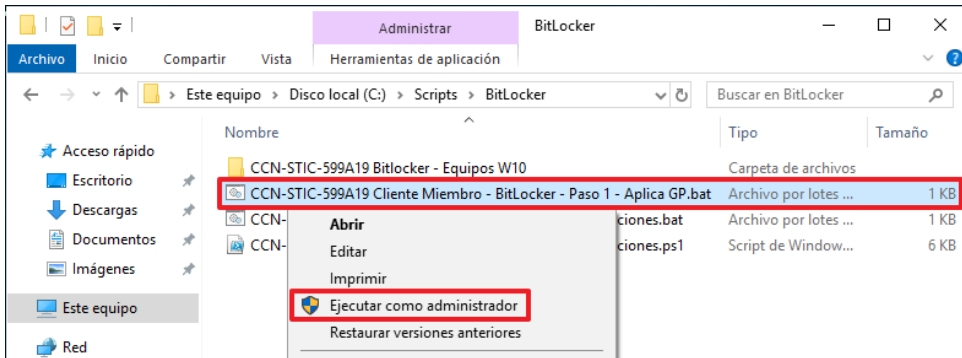
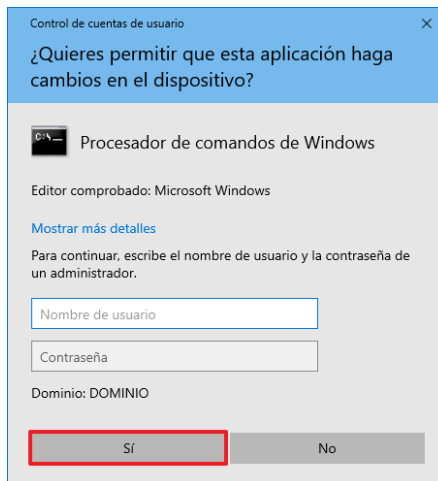
Paso	Descripción
33.	Finalmente, seleccione y expanda el siguiente contenedor: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos W10 con BitLocker" Compruebe que, efectivamente, la cuenta del equipo ahora se encuentra en él: 

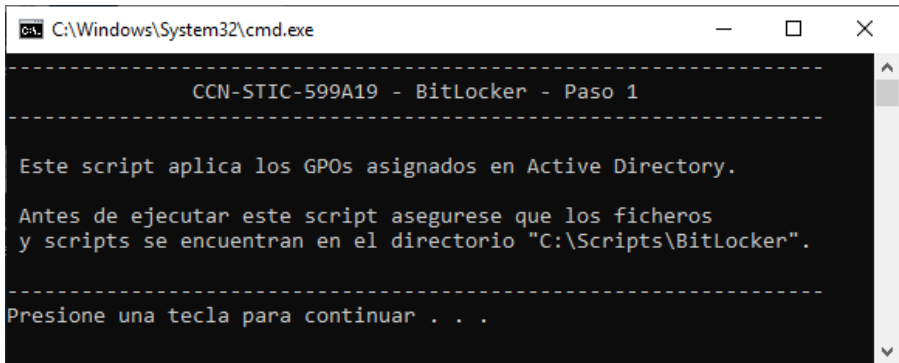
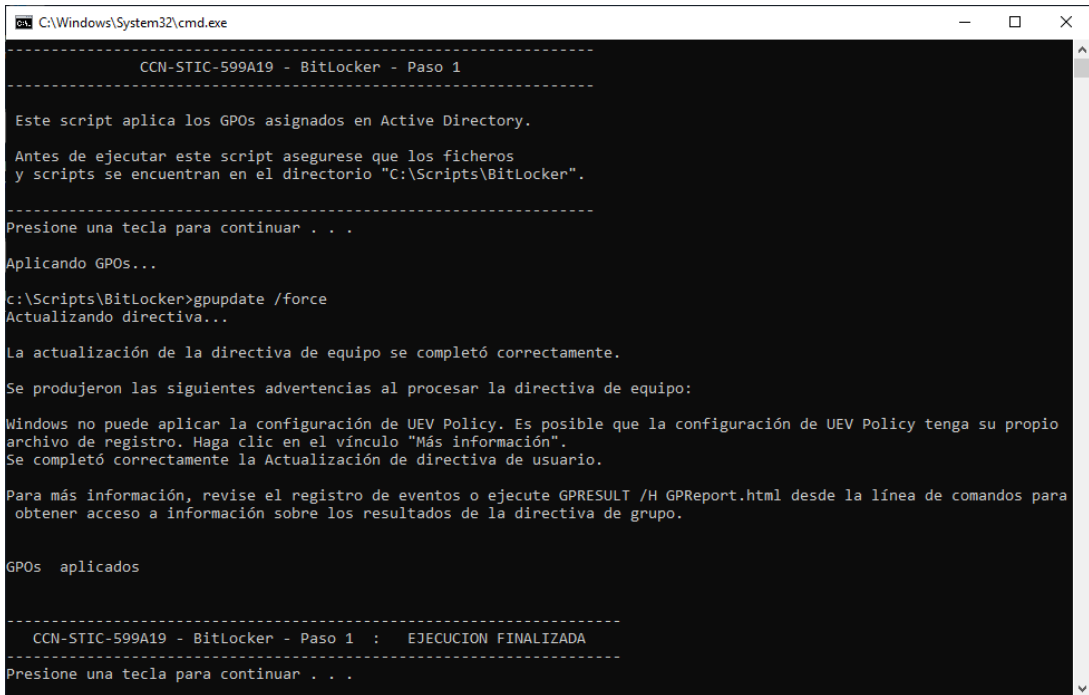
Al estar alojada la cuenta de equipo en este contenedor de Active Directory, el equipo Windows 10 miembro del dominio recibirá la configuración de equipo recomendada en esta guía para equipos con BitLocker además de los parámetros de configuración, recomendados también en esta guía, para el resto de clientes Windows 10.

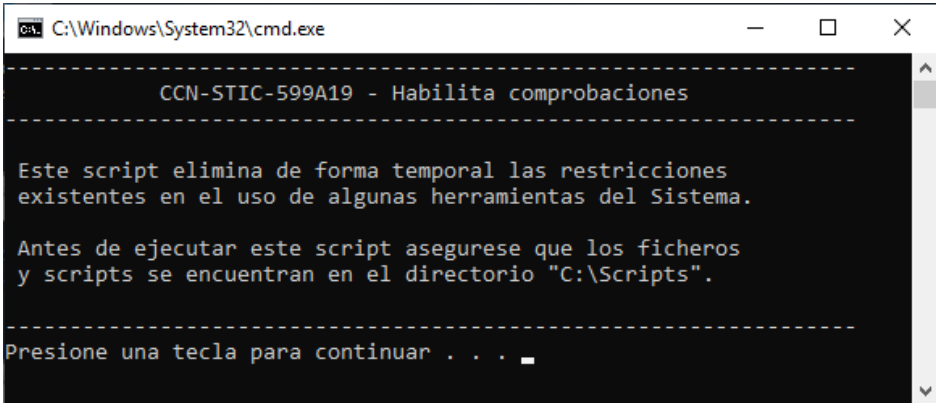
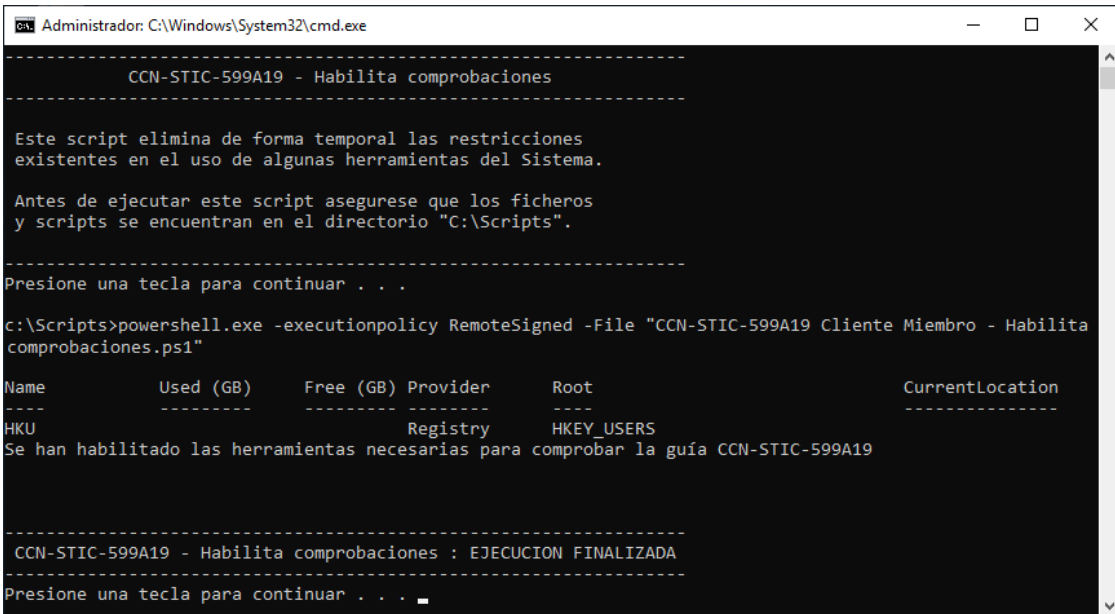
Una vez preparados la unidad organizativa "Equipos W10 con BitLocker" y la GPO "CCN-STIC-599A19 BitLocker - Equipos W10", y ubicada en Active Directory la cuenta de equipo del equipo en el que se está configurando BitLocker, realice los siguientes pasos en el equipo cliente en el que está configurando BitLocker para activar BitLocker con la configuración recomendada en esta guía.

Paso	Descripción
34.	Inicie sesión en el equipo cliente en el que está configurando BitLocker (en adelante simplemente "Equipo Cliente") con una cuenta de usuario de Windows que esté ubicada en la unidad organizativa "Usuarios Windows 10" de Active Directory y que pertenezca al grupo local "Administradores" (por ejemplo, un miembro del grupo "Admins. del dominio" y al grupo local de dominio "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.
35.	Si no existe ya, cree el directorio "Scripts" en la unidad "C:\".
36.	Copie los ficheros asociados a esta guía, incluyendo el subdirectorio "Bitlocker" con todo su contenido, en el directorio "C:\Scripts". Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". 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
37.	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”. 
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, por último, pulse “Aceptar”. 

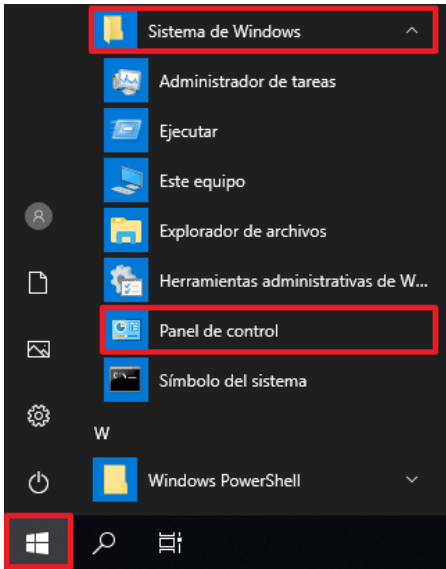
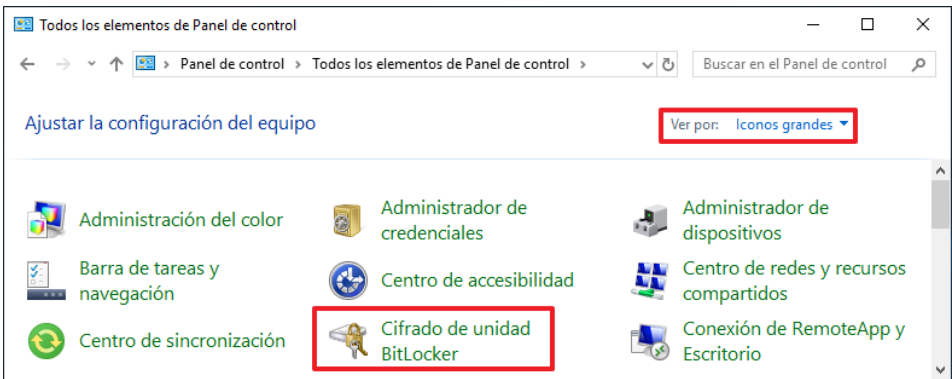
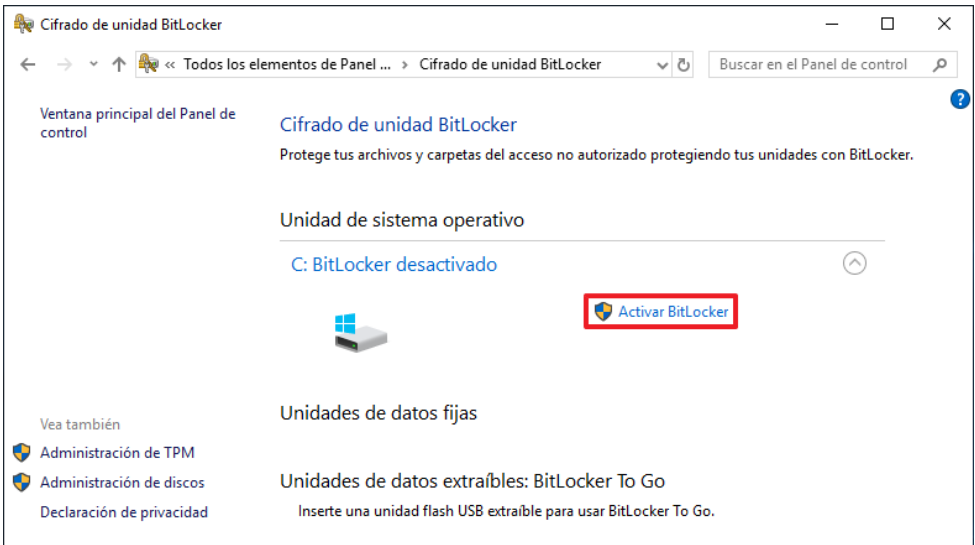
Paso	Descripción
40.	Compruebe que en el directorio “C:\Scripts” se encuentran al menos los siguientes directorios y ficheros: – BitLocker (Directorio) Dentro del directorio “BitLocker” deben estar los siguientes directorios y ficheros: – CCN-STIC-599A19 BitLocker - Equipos W10 (<i>directorio</i>) – CCN-STIC-599A19 Cliente Miembro - BitLocker - Paso 1 - Aplica GP.bat – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.ps1
41.	Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script " CCN-STIC-599A19 Cliente Miembro – BitLocker Paso 1 – Aplica GP.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 administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
42.	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”. 

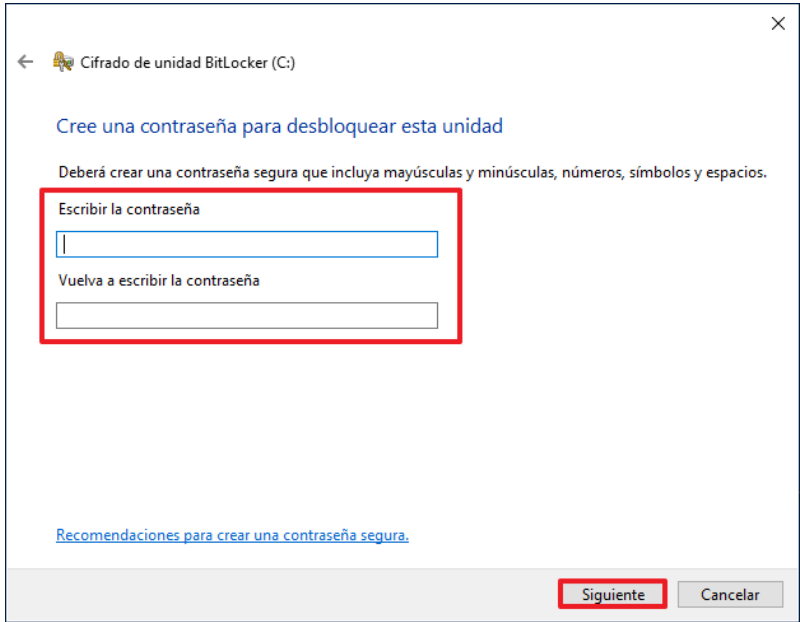
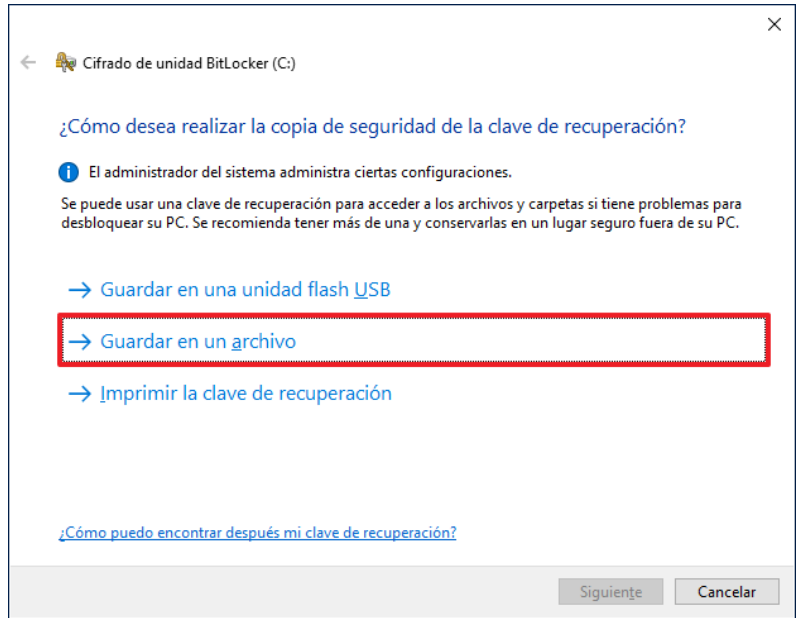
Paso	Descripción
43.	Este script aplica las GPO definidas en Active Directory y que aplican al equipo y usuario actuales. Las GPO se aplican periódicamente de forma automática, pero de esta forma se asegura la configuración definida en las GPO de Active Directory, incluido el añadido para la configuración de BitLocker, haya sido aplicada al equipo antes de que se realicen el resto de pasos. Pulse una tecla para continuar. 
44.	Se actualizarán las directivas de equipo. La pantalla podrá mostrar una serie de advertencias relativas a la aplicación de las directivas. Estas advertencias se deben a un servicio deshabilitado, pero puede ignorarlas ya que la política ha aplicado correctamente. Pulse una tecla para continuar y cerrar la ventana. 

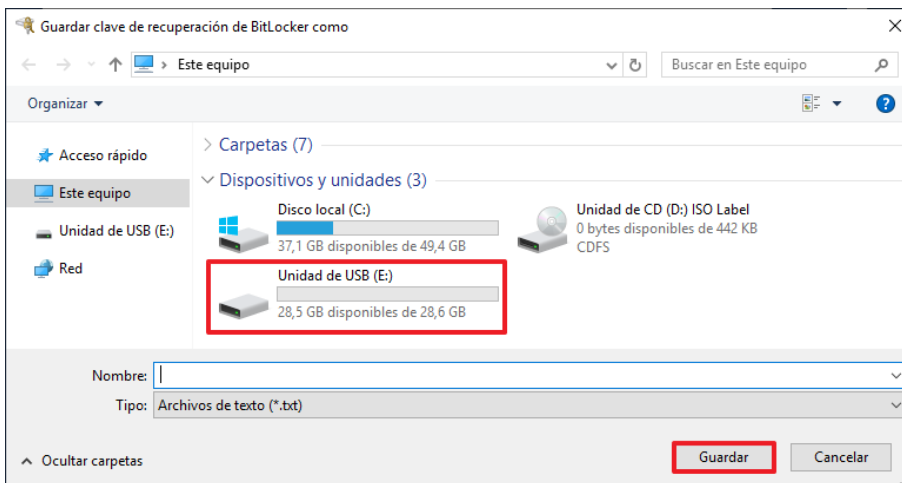
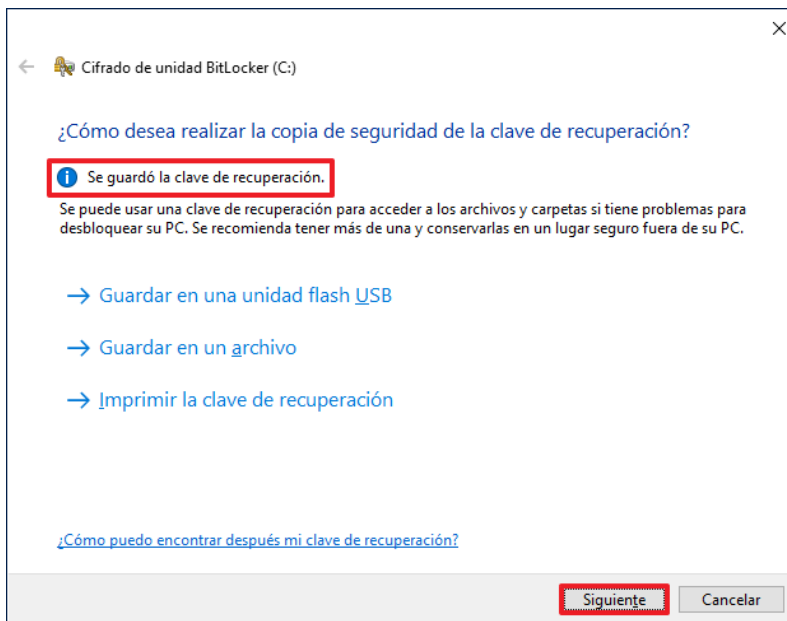
Paso	Descripción
45.	Del mismo modo que en el paso anterior, ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.bat" desde el directorio "C:\Scripts\Bitlocker". Este paso será necesario para habilitar temporalmente características necesarias para continuar con los pasos siguientes. Pulse una tecla para continuar.  Nota: El sistema le solicitará elevación de privilegios.
46.	Pulse una tecla de nuevo para finalizar el proceso. 

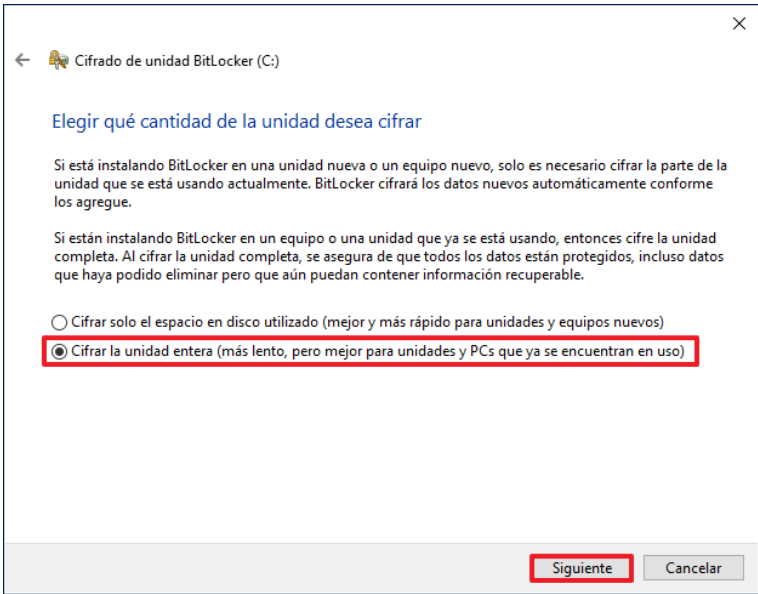
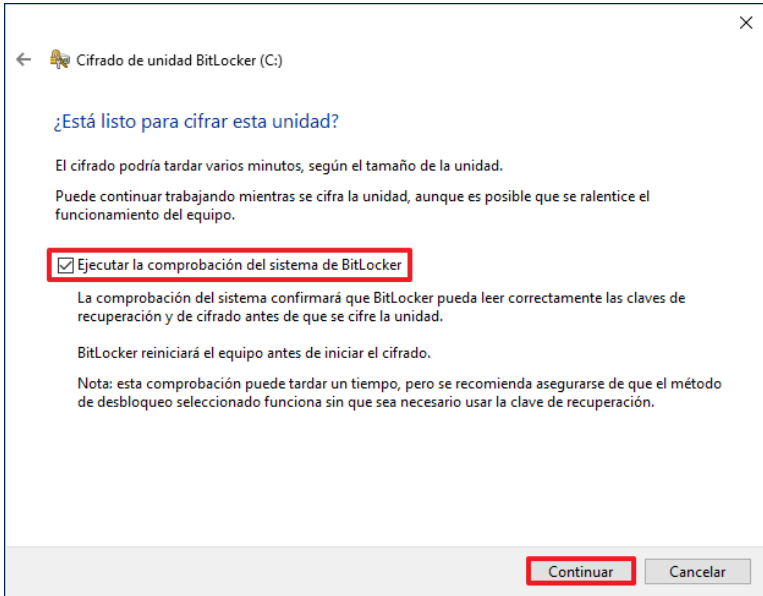
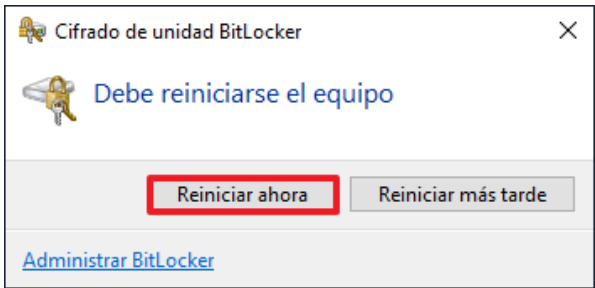
Los siguientes pasos describen el procedimiento para activar el cifrado de unidad BitLocker con PIN (número de identificación personal).

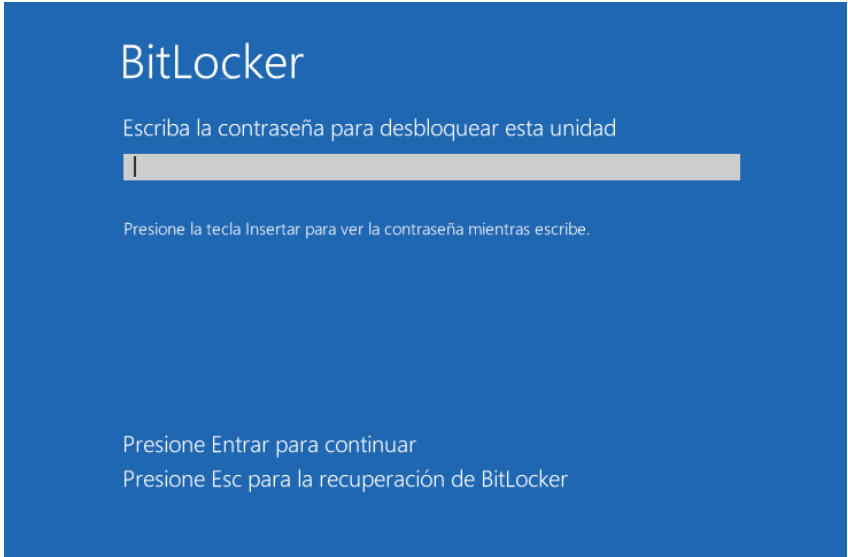
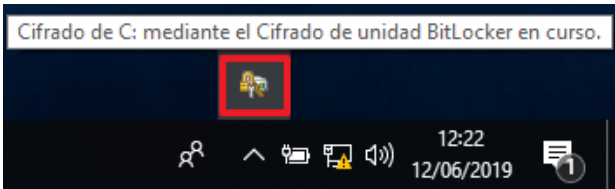
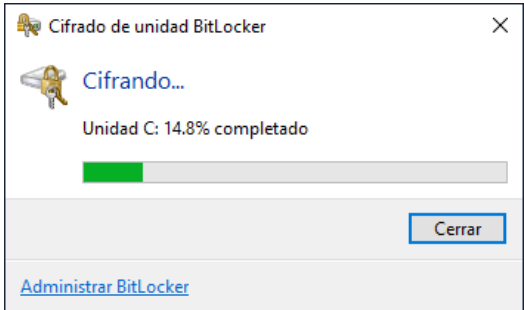
Nota: Aunque a este identificador se le conoce con el nombre de "PIN", del inglés "Personal Identification Number", que significa "número de identificación personal", en realidad en Windows 10 se pueden utilizar identificadores con todo tipo de caracteres, sin necesidad de limitarse únicamente a números.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

Paso	Descripción
47.	Abra el panel de control desde “Inicio → Sistema de Windows → Panel de control”. 
48.	Establezca la vista en “Iconos grandes” y pulse en “Cifrado de unidad BitLocker”. 
49.	Pulse sobre “Activar BitLocker” como se indica en la siguiente figura. 

Paso	Descripción
50.	El sistema le solicitará elevación de privilegios. Introduzca credenciales de administrador en la ventana “Control de cuentas de usuario”.
51.	Introduzca y confirme una contraseña de inicio y pulse “Establecer PIN”.  Nota: Recuerde que puede utilizar entre 8 y 20 caracteres. A mayor longitud, mayor seguridad.
52.	Seleccione “Guardar en un archivo” para guardar una copia de seguridad de la clave de recuperación. 

Paso	Descripción
53.	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.
54.	Pulse “Siguiente” una vez haya guardado la clave de recuperación. 

Paso	Descripción
55.	Elija la opción de “Cifrar la unidad entera” y pulse “Siguiente”. 
56.	Marque la opción "Ejecutar la comprobación del sistema de BitLocker" y pulse el botón "Continuar". 
57.	Reinicie el equipo para continuar con el proceso de cifrado de la unidad. 

Paso	Descripción
58.	Al reiniciar, el sistema le pedirá el PIN de cifrado de unidad BitLocker. Introduzca el PIN y pulse “Enter” para continuar. 
59.	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. 
60.	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.

Paso	Descripción
61.	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.
62.	Eliminé el directorio “C:\Scripts”. Nota: Todos los volúmenes NTFS del Sistema deberán de 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

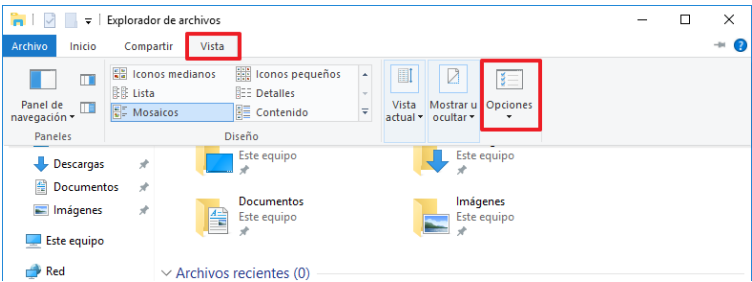
6. LISTA DE COMPROBACIÓN – BITLOCKER

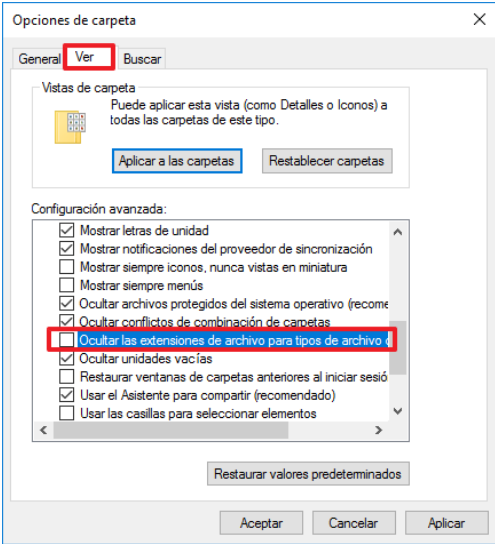
Este anexo se ha diseñado para ayudar a los operadores a verificar que se ha implementado el cifrado de unidad BitLocker en un equipo cliente Windows 10 versión 1809 miembro de un dominio. La lista de comprobación deberá ejecutarse iniciando sesión en el equipo propio cliente con la cuenta de un usuario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

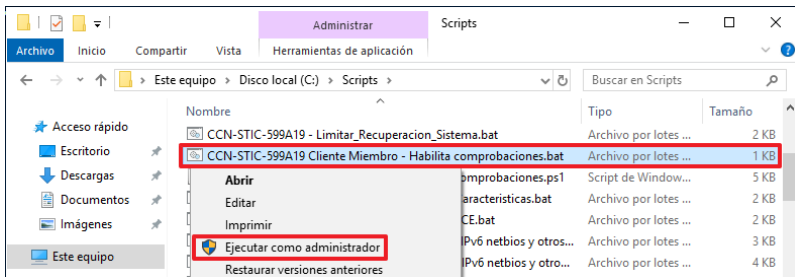
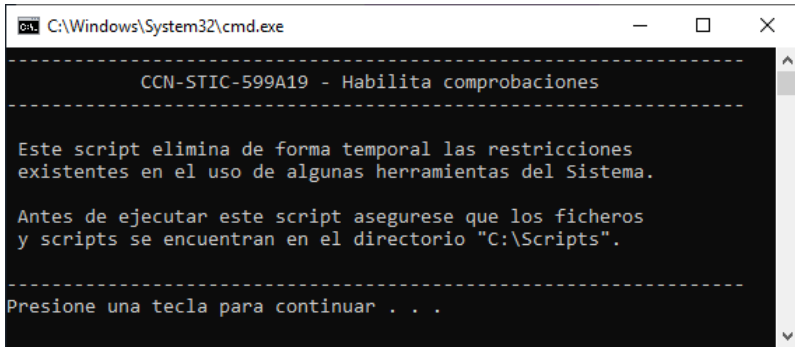
Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada, debido a la aplicación de la configuración de seguridad.

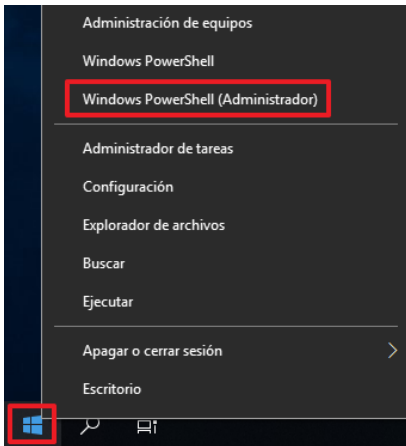
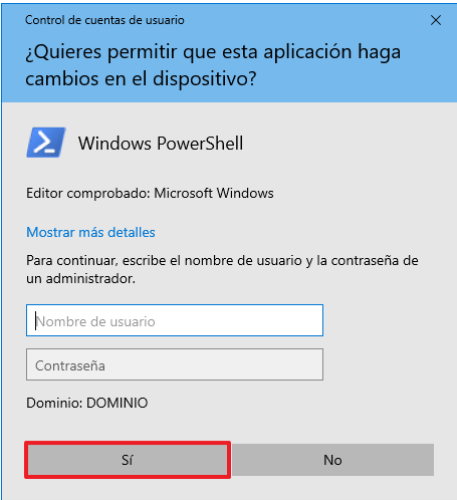
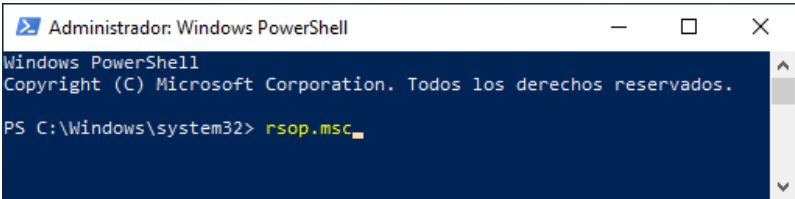
Para realizar algunas de las comprobaciones será necesario ejecutar diferentes consolas de administración y herramientas del sistema. Estas herramientas estarán disponibles si no se ha prohibido la utilización de las mismas. Uno de los primeros pasos, por tanto, consistirá en habilitar temporalmente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

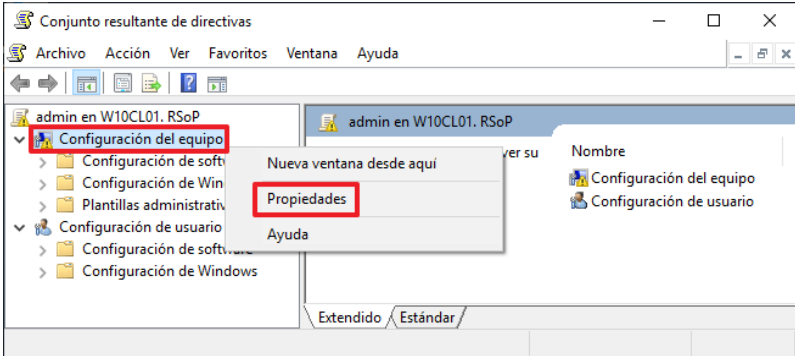
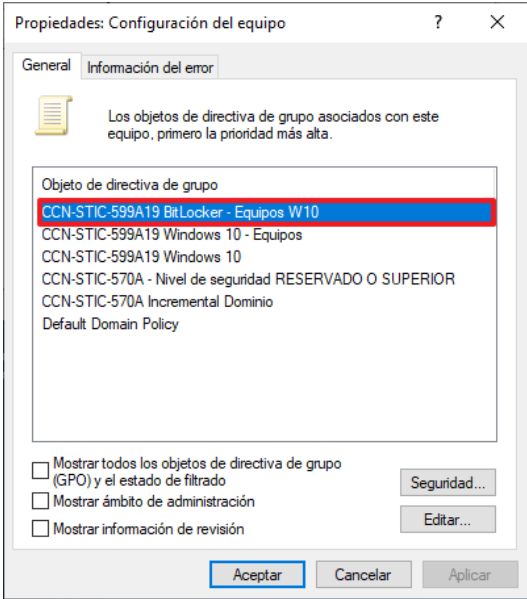
- Explorador de Windows (explorer.exe)
- Windows PowerShell (PowerShell.exe)
- Conjunto resultante de directivas (rsop.msc)
- Panel de control (control.exe)
- Administración de servicios (services.msc)

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 de Windows que esté ubicada en la unidad organizativa "Usuarios Windows 10" de Active Directory y que pertenezca al grupo local "Administradores" (por ejemplo, un miembro del grupo "Admins. del dominio") y al grupo local de dominio "Usuarios de shells". Nota: No podrá utilizar la cuenta integrada de administrador porque ésta se encontrará deshabilitada.
2. Configure 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 (clic derecho) → Explorador de Windows" En el menú superior pulse sobre “Vista” y seleccione “Opciones”. 

Comprobación	OK/NOK	Cómo hacerlo
		Seleccione la pestaña “Ver” y dentro de dicho menú, "Opciones de carpeta...". De la ventana que aparecerá, 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".
3. Cree el directorio "Scripts" en la unidad "C:" y copie en él al menos los ficheros que se indican		Cree el directorio "Scripts" en la unidad "C:" y copie en él al menos los siguientes dos scripts, los cuales están incluidos entre los ficheros que acompañan a esta guía: – CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.bat – CCN-STIC-599A19 Cliente Miembro – Habilita comprobaciones.ps1 Nota: Los recursos asociados a esta guía se encuentran en el directorio "Scripts-599A19". Aunque en el subdirectorio "Bitlocker" de los ficheros que acompañan a esta guía existen también unos ficheros similares, para esta lista de comprobación bastará con utilizar los scripts indicados, directamente en el directorio "C:\Scripts".

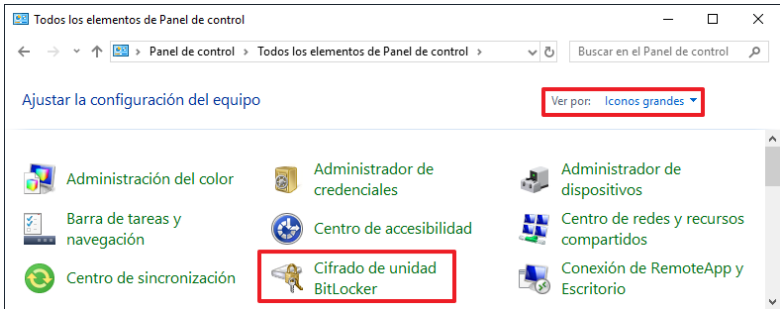
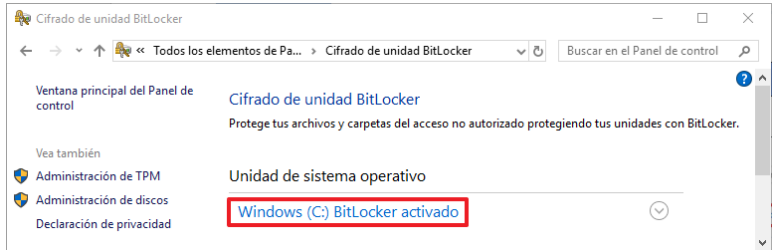
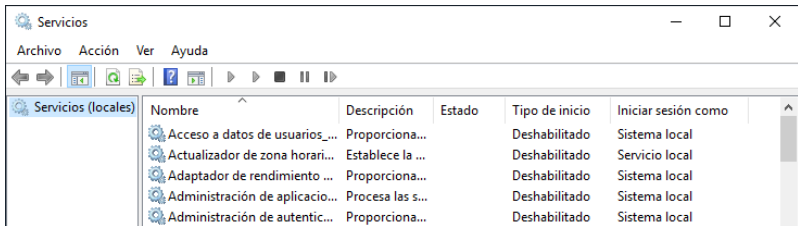
Comprobación	OK/NOK	Cómo hacerlo
4. Ejecute el script que habilita temporalment e las consolas de administración restringidas		Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-599A19 Cliente Miembro - Habilita comprobaciones.bat". Para ello, visualice la 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 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 administrador y pulse "Sí".
5. Habilite temporalment e 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.

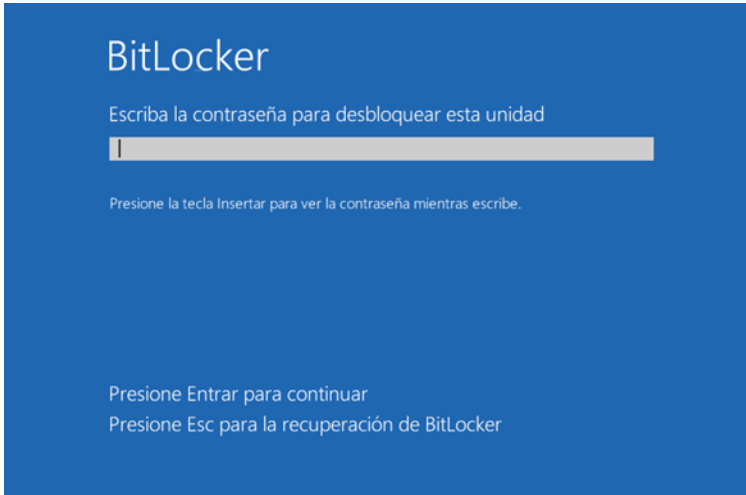
Comprobación	OK/NOK	Cómo hacerlo
6. Lance una ventana de PowerShell con permisos de administrador, para lanzar desde ella en pasos posteriores comandos con permisos de administrador		Haga clic con el botón derecho en el menú de inicio y seleccione “Windows PowerShell (Administrador)”.  El Sistema le solicitará elevación de privilegios a través del control de cuentas de usuario.  Tras introducir las credenciales de un usuario administrador, aparecerá una ventana del intérprete de comandos. Deje esta ventana abierta hasta el final de las comprobaciones.
7. Ejecute la consola de administración "Conjunto resultante de directivas"		Desde la ventana de PowerShell con privilegios de administrador, teclee "rsop.msc" y pulse “Enter” para abrir la consola de administración "Conjunto resultante de directivas". 

Comprobación	OK/NOK	Cómo hacerlo
8. Verifique que el equipo ha recibido correctamente la directiva de grupo "CCN-STIC-599A19 BitLocker – Equipos W10"		En la consola de administración "Conjunto resultante de directivas", seleccione el contenedor "Configuración del equipo", márkelo con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la siguiente figura.  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo", la política deberá aparecer y "CCN-STIC-599A19 BitLocker – Equipos W10" deberá estar situada encima del resto de directivas, tal y como se muestra en la siguiente figura.  Nota: Es posible que, dependiendo de la configuración de su entorno, aparezcan más objetos de directiva de grupo aplicados al usuario del equipo que está comprobando. Deberá asegurarse de que al menos el objeto "CCN-STIC-599A19 BitLocker – Equipos W10" está aplicado y que el orden de aplicación de los distintos objetos de directiva de grupo es el adecuado para su organización.

Comprobación	OK/NOK	Cómo hacerlo		
	Parámetro			OK/NOK
	CCN-STIC-599A19 Bitlocker – Equipos W10			
	CCN-STIC-599A19 Windows 10 - Equipos			
	CCN-STIC-599A19 Windows 10			
	CCN-STIC-570A Incremental Dominio			
	Default Domain Policy			
		Cierre la ventana de “Propiedades” pero no cierre aún la consola de administración “Conjunto resultante de directivas”.		
9. Compruebe que se han aplicado los valores correctos de directivas de grupo relativos a los servicios del sistema.		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 de equipo → Configuración de Windows → Configuración de seguridad → Servicios del sistema"		
	Servicio		Tipo de inicio	OK/NOK
	Servicio Cifrado de unidad BitLocker (bdesvc)		Automático	
	Detección de hardware Shell (shellhwdetection)		Automático	
10. Verifique la configuración 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		
11. Verifique la configuración 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	
12. Verifique la configuración 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
		Ya puede cerrar la consola de administración Conjunto resultante de directivas.
13. 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".
14. 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
		Servicio Cifrado de unidad BitLocker (bdesvc)	Automático
		Detección de hardware Shell (shellhwdetection)	Automático
		Cierre la consola de administración de servicios.	
15. Borre el directorio "C:\Scripts"		Borre el directorio "C:\Scripts" con todo su contenido.	
16. Reinicie el equipo		Reinicie el equipo para comprobar que BitLocker solicita el código PIN para acceder a la unidad de sistema.	
17. Compruebe que el sistema tiene configurado cifrado de unidad BitLocker con la opción de PIN de arranque.		Al reiniciarse el equipo, compruebe que el sistema requiere que se introduzca el PIN para desbloquear la unidad, como se muestra en la siguiente figura. 	
18. 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.2.2. DISPOSITIVOS USB TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19

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-599A19.

Para permitir el uso de dispositivos USB en equipos a los que se les ha aplicado la guía CCN-STIC-599A19, será necesaria la creación de una unidad organizativa a la que pertenecerán todos aquellos equipos en los que se hará uso de dispositivos USB y, sobre ese grupo creado, se aplicará una política de grupo mediante un controlador de dominio del dominio al que pertenecen dichos equipos.

Este anexo muestra, en su primer apartado, la configuración de los diferentes elementos que modifica, a través de GPOs, la política creada y denominada “CCN-STIC-599A19 – Habilitar dispositivos”. Así mismo, muestra una guía paso a paso con la operativa a seguir para poder implementar dicha política en los equipos deseados.

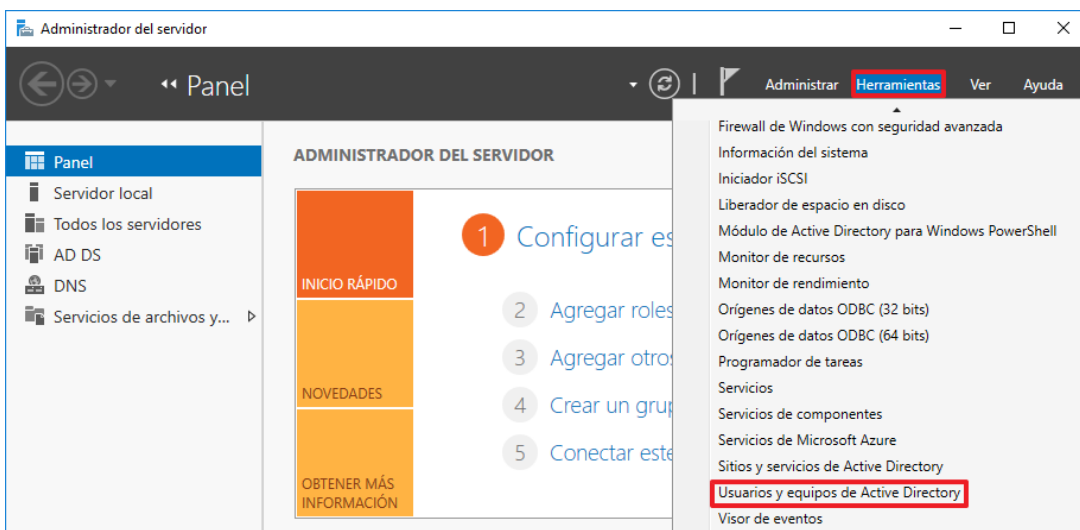
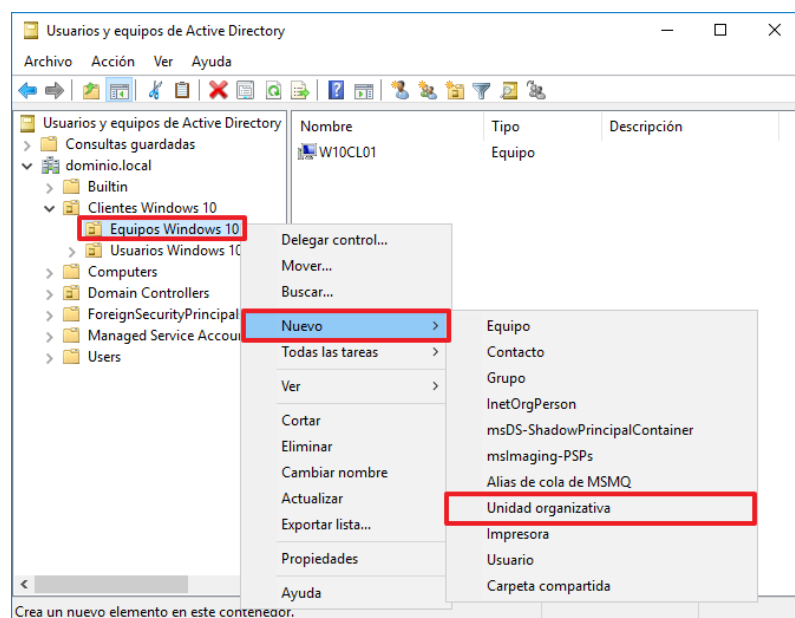
En los puntos posteriores se muestran dos procedimientos para habilitar el uso de dispositivos USB. Los métodos para permitir el uso de dispositivos conectados mediante USB son los siguientes:

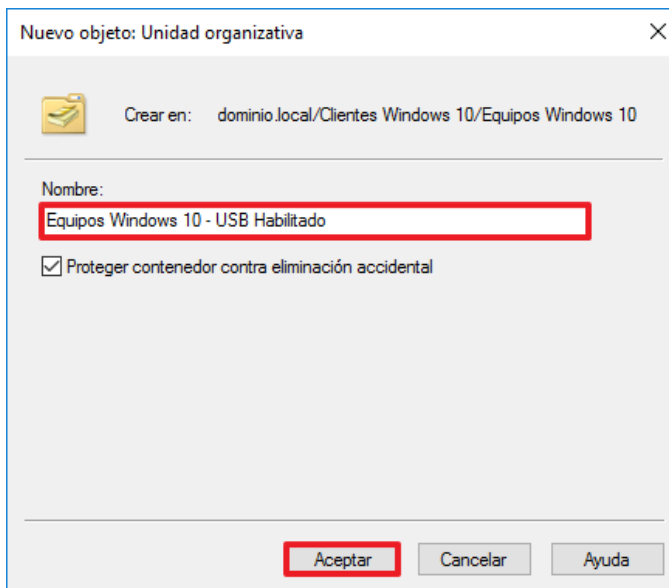
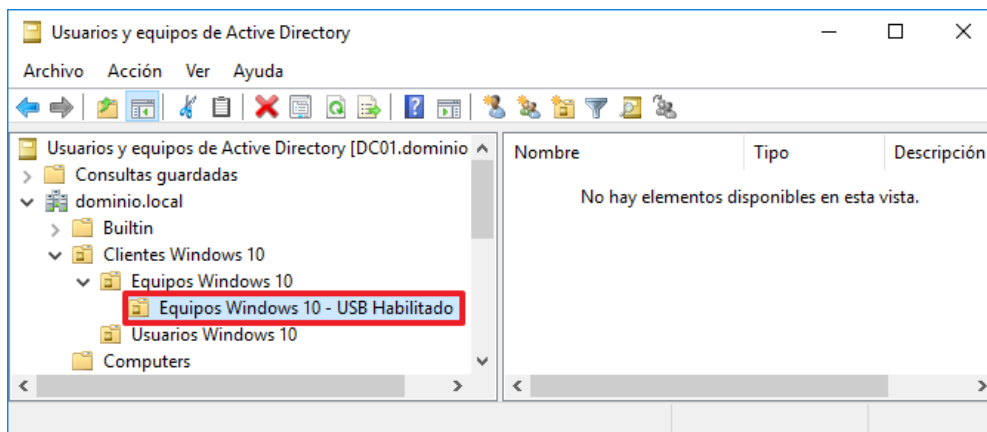
- a) Instalación de controladores mediante el uso de un usuario administrador de la máquina.
- b) Filtrado de USB mediante el uso de los identificadores de dispositivo USB.

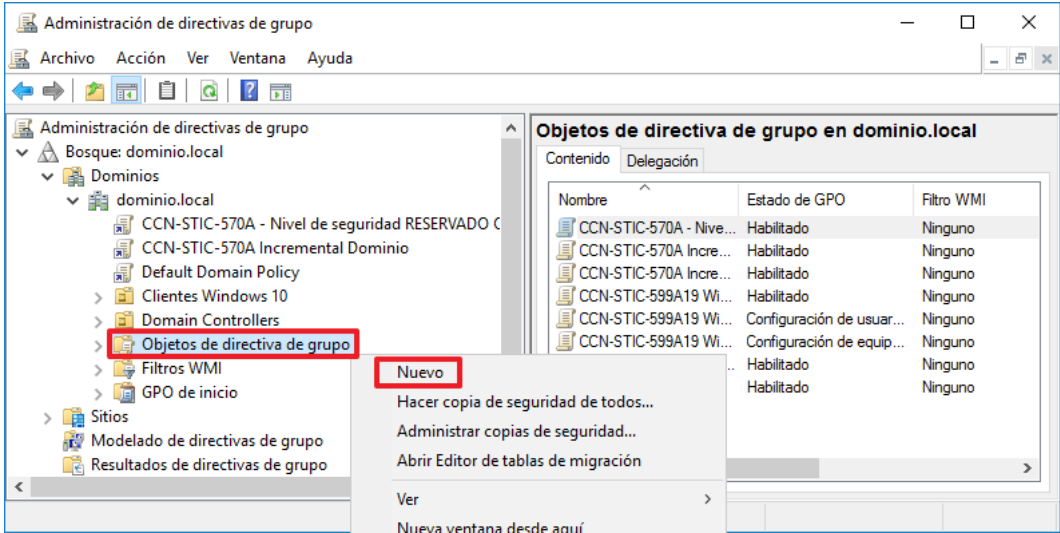
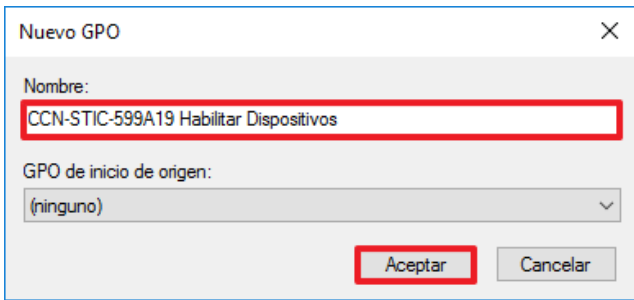
1. PREPARACIÓN DEL DIRECTORIO ACTIVO

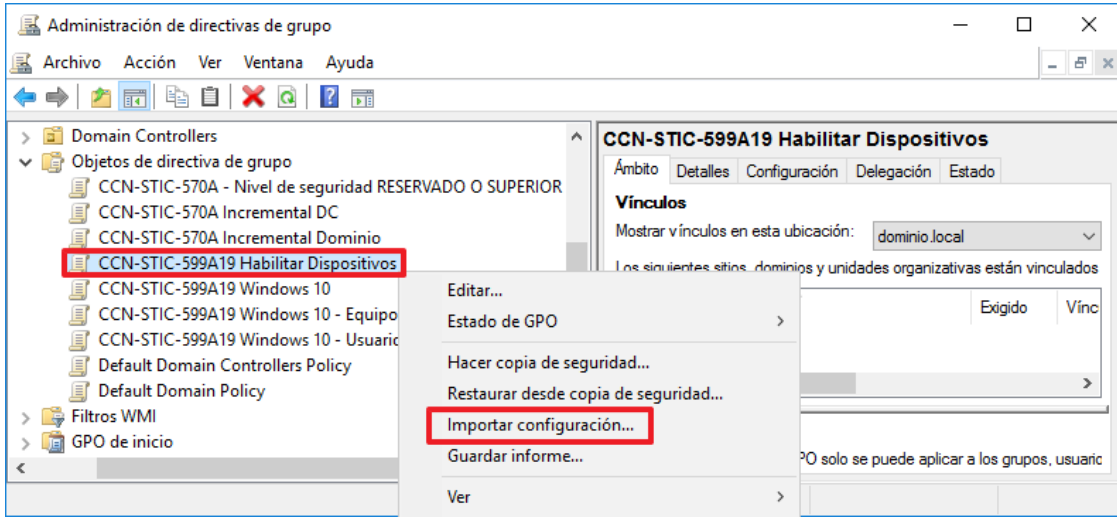
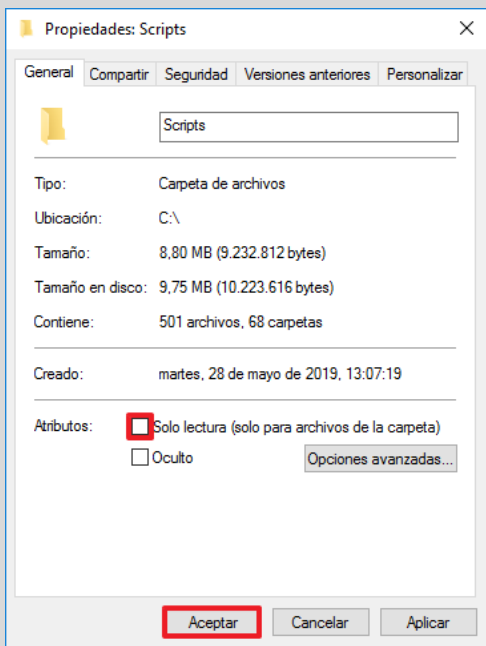
Como paso previo a la configuración de los dispositivos USB, es necesario preparar el directorio activo. Esta preparación se realiza a través de los siguientes pasos.

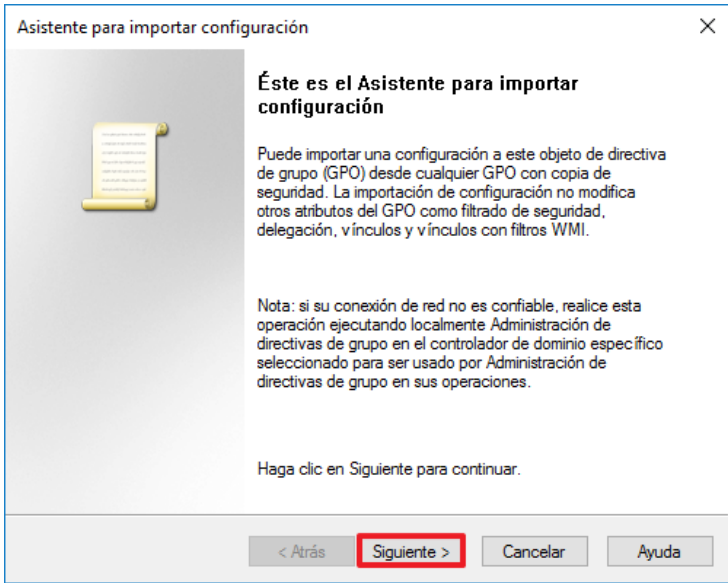
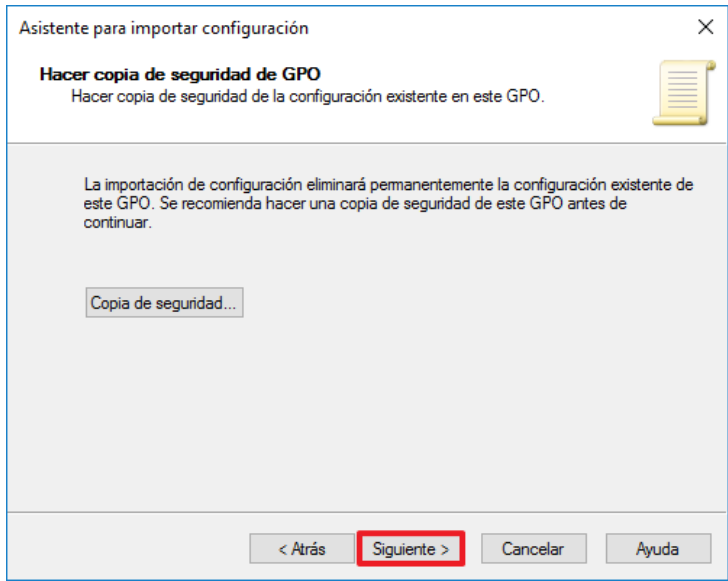
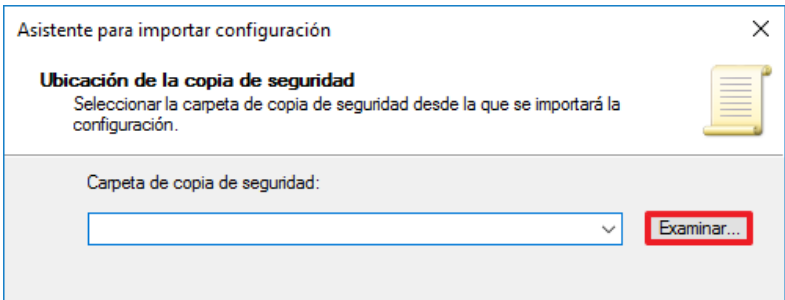
Paso	Descripción
1.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie el siguiente directorio y su contenido a “C:\Scripts” en el controlador de dominio: – CCN-STIC-599A19 Habilitar Dispositivos (directorio)
	Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”.
4.	Cree la unidad organizativa "Equipos Windows 10 – USB habilitado". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.

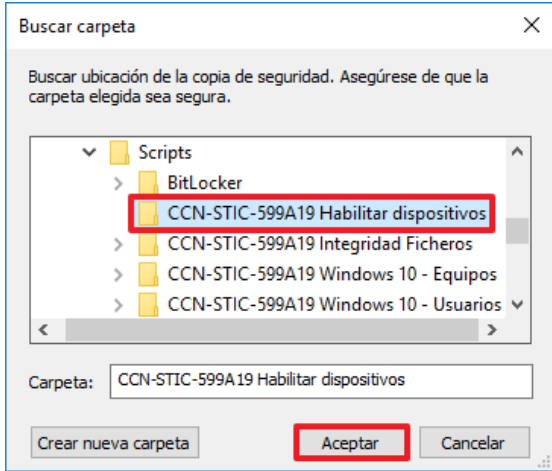
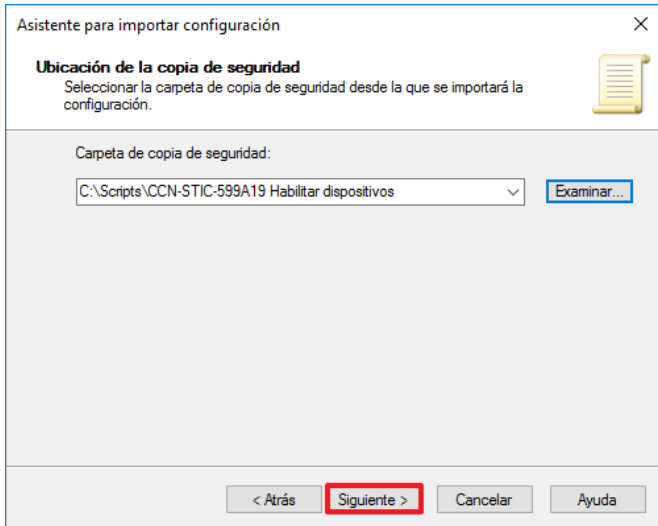
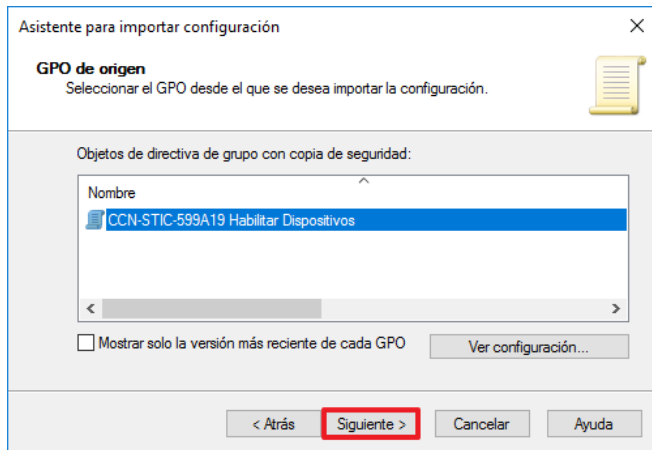
Paso	Descripción
5.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Usuarios y equipos de Active Directory”. 
6.	En la consola de “Usuarios y equipos de Active Directory” sitúese sobre el objeto “Equipos Windows 10” a través de la ruta "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10". Pulsando con el botón derecho del ratón, seleccione la opción "Nuevo → Unidad organizativa" del menú contextual que aparecerá.  Nota: En el ejemplo, el dominio se denomina “dominio.local”.

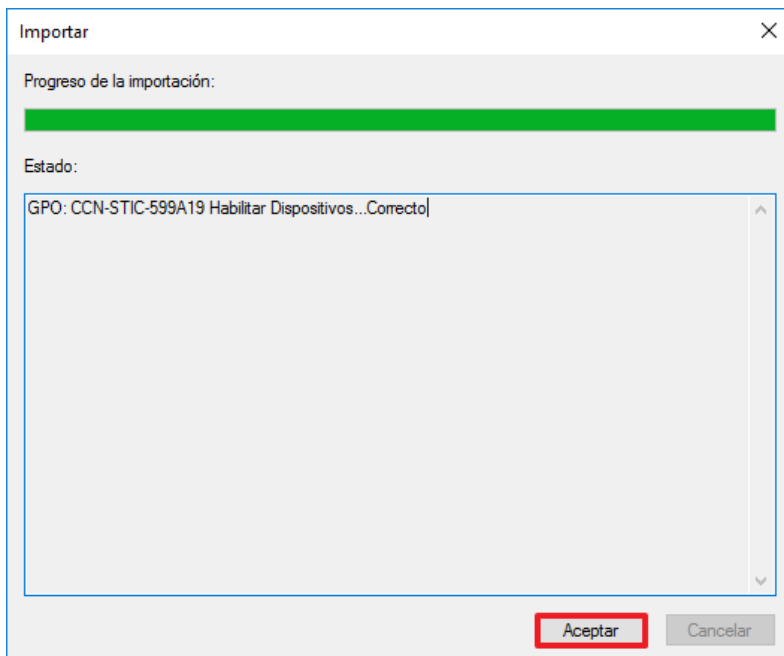
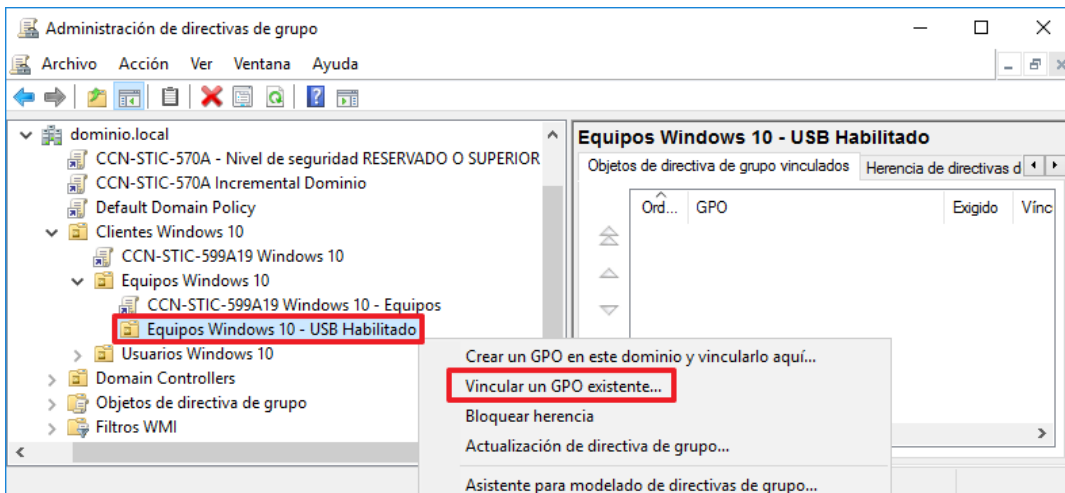
Paso	Descripción
7.	Asigne el nombre "Equipos Windows 10 – USB habilitado" a la nueva unidad organizativa, rellenando con este nombre el campo "Nombre:" del cuadro de diálogo que aparecerá y deje marcada la opción "Proteger contenedor contra eliminación accidental". A continuación, pulse "Aceptar". 
8.	Al pulsar el botón Aceptar, la nueva unidad organizativa, "Equipos Windows 10 – USB habilitado" aparecerá colgando de "Equipos Windows 10", como se muestra en la siguiente figura. 
9.	De nuevo, utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 

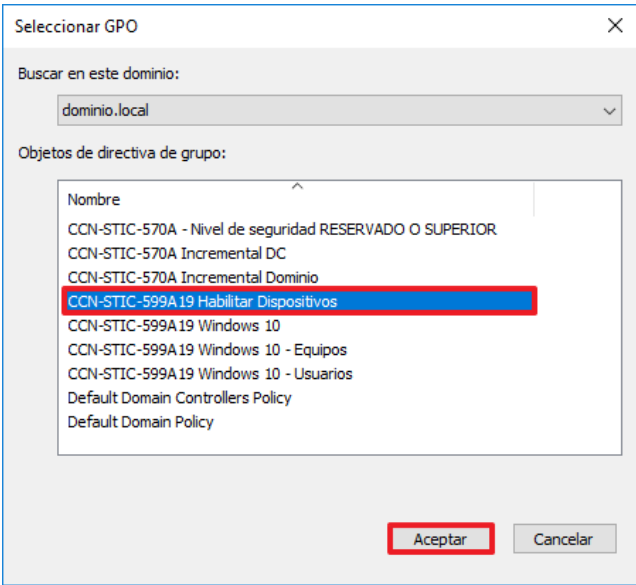
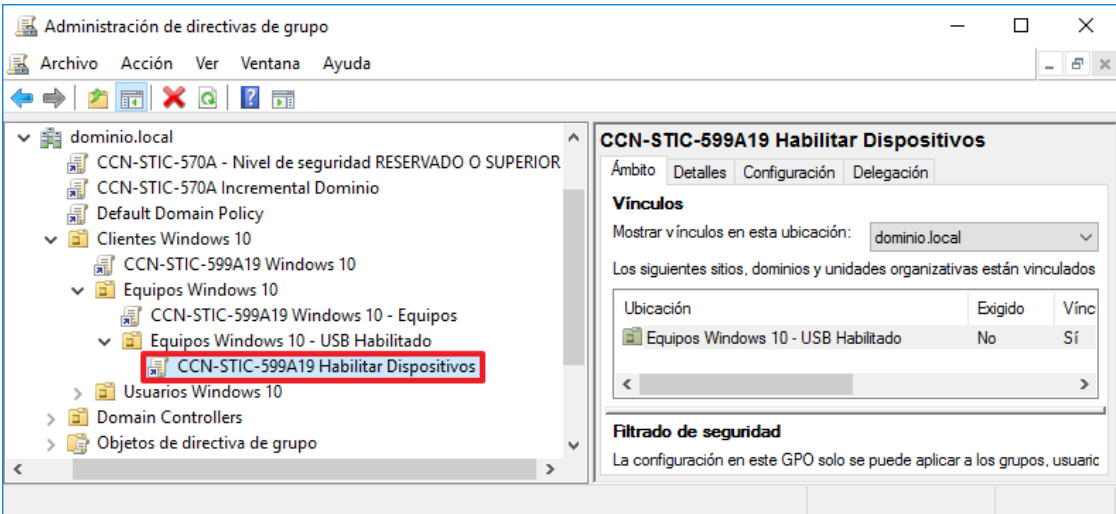
Paso	Descripción
10.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>" A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar la GPO correspondiente.
11.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" con el botón derecho y elija la opción "Nuevo" del menú contextual que aparecerá.  Nota: La GPO que se va a crear y parametrizar en los siguientes pasos deberá vincularse a las unidades organizativas correspondientes a Windows 10 versión 1809. Es importante no mezclar equipos, usuarios o GPOs de Windows 10 versión 1809 con equipos, usuarios o GPOs de Windows 10 versión 1607 (a los cuales les debe aplicar la guía CCN-STIC-599A18, y no la presente guía).
12.	Asigne el siguiente nombre "CCN-STIC-599A19 Habilitar Dispositivos" al nuevo GPO y pulse “Aceptar”. 

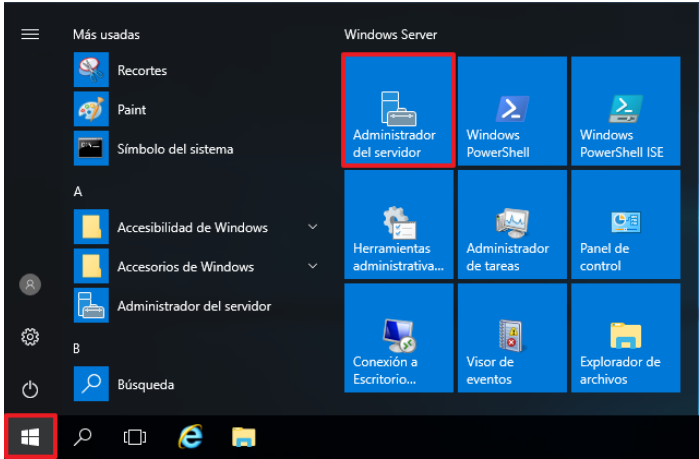
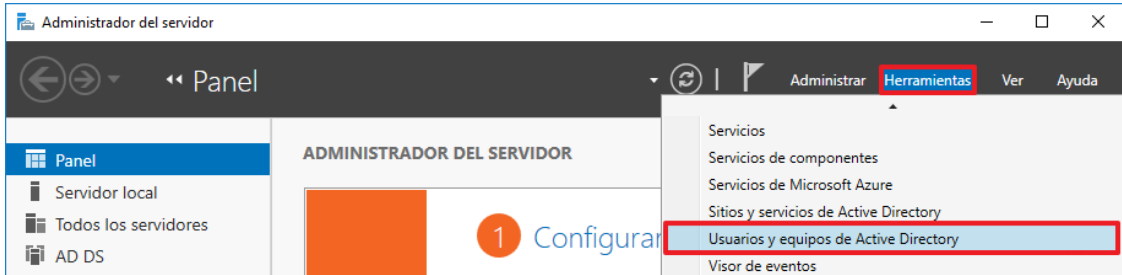
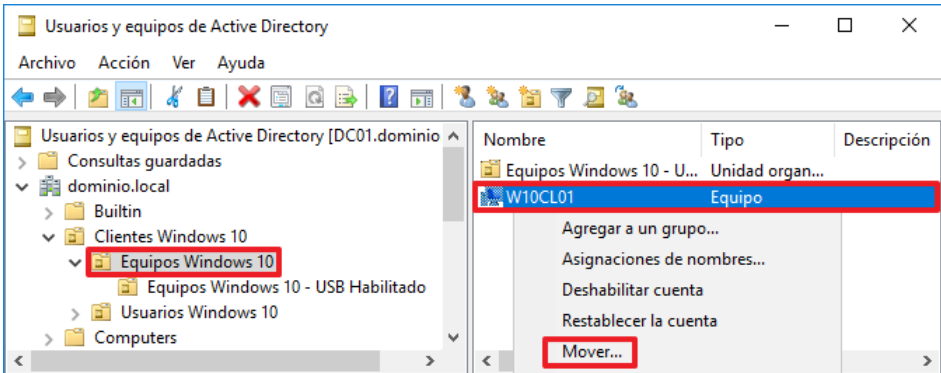
Paso	Descripción
13.	Seleccione la GPO recién creada, "CCN-STIC-599A19 Windows 10" con el botón derecho y elija la opción "Importar configuración..." en el menú contextual que aparecerá.  Nota: Asegúrese de que los archivos alojados en "C:\Scripts" no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

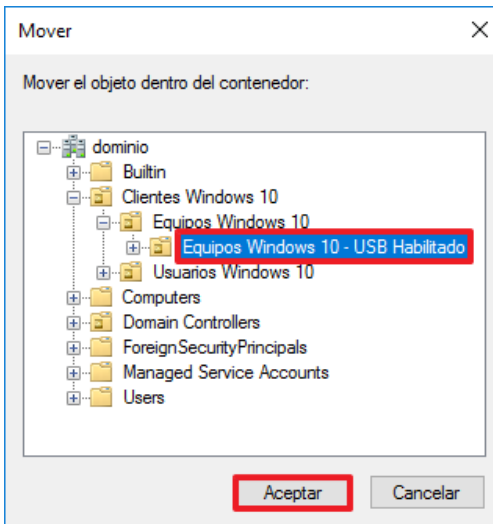
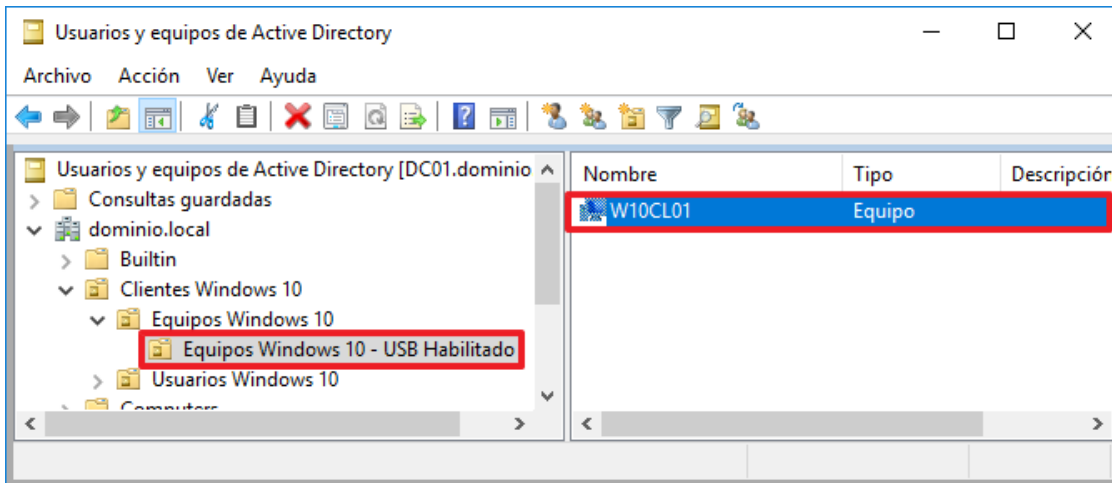
Paso	Descripción
14.	En el “Asistente para importar configuración” pulse “Siguiente >”. 
15.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana “Hacer copia de seguridad de GPO”. 
16.	En “Ubicación de la copia de seguridad” pulse sobre el botón “Examinar...”. 

Paso	Descripción
17.	Localice la carpeta “CCN-STIC-599A19 Habilitar dispositivos” y pulse “Aceptar”. 
18.	Pulse “Siguiente >” para continuar. 
19.	En “GPO de origen” pulse “Siguiente >”. 
20.	En “Examinar copia de seguridad” pulse “Siguiente >”.

Paso	Descripción
21.	Pulse “Finalizar” para realizar la importación.
22.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 
23.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 – USB habilitado” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 

Paso	Descripción
24.	Seleccione “CCN-STIC-599A19 Habilitar dispositivos” de la lista y pulse “Aceptar”. 
25.	Compruebe que la GPO ha quedado correctamente vinculada a la unidad organizativa “Equipos Windows 10 – USB habilitado”. 

Paso	Descripción
26.	Traslade, en Active Directory, la cuenta de equipo del equipo en el que necesita hacer uso de un dispositivo externo USB, desde su ubicación actual hasta su nueva ubicación: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 – USB habilitado" Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
27.	Pulse sobre "Herramientas" en el menú superior y localice, en el menú contextual desplegado "Usuarios y equipos de Active Directory". 
28.	Seleccione entonces, en la parte central de la ventana, la cuenta del equipo a trasladar y, marcando con el botón derecho del ratón, seleccione la opción "Mover..." del menú contextual que aparecerá, como se muestra en la siguiente figura.  Nota: En este ejemplo el nombre del equipo en el que se está permitiendo el uso de dispositivos USB se supone que es "W10CL01".

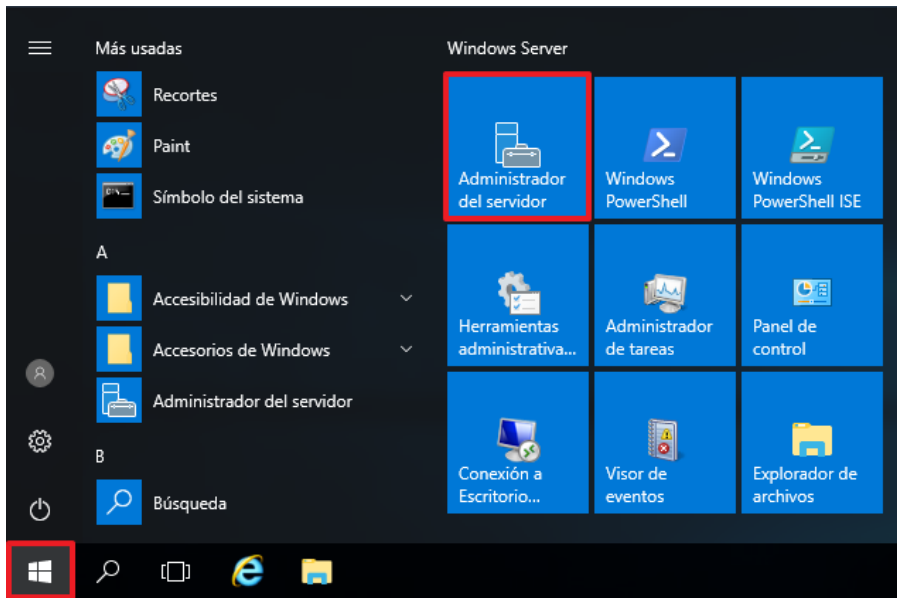
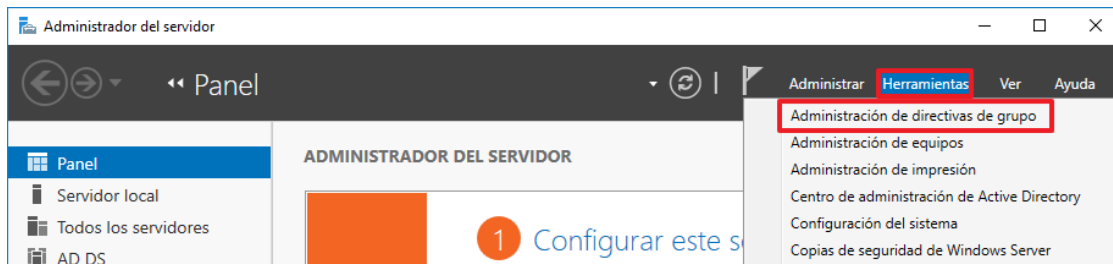
Paso	Descripción
29.	En el cuadro de diálogo que aparecerá, titulado "Mover", seleccione el contenedor destino en la ruta "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 – USB habilitado". Pulse "Aceptar" para cerrar la ventana. 
30.	Finalmente, seleccione y expanda el contenedor siguiente: "<Nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10 → Equipos Windows 10 USB habilitado" Compruebe que, efectivamente, la cuenta del equipo ahora se encuentra en él. 
31.	Borre la carpeta "C:\Scripts".

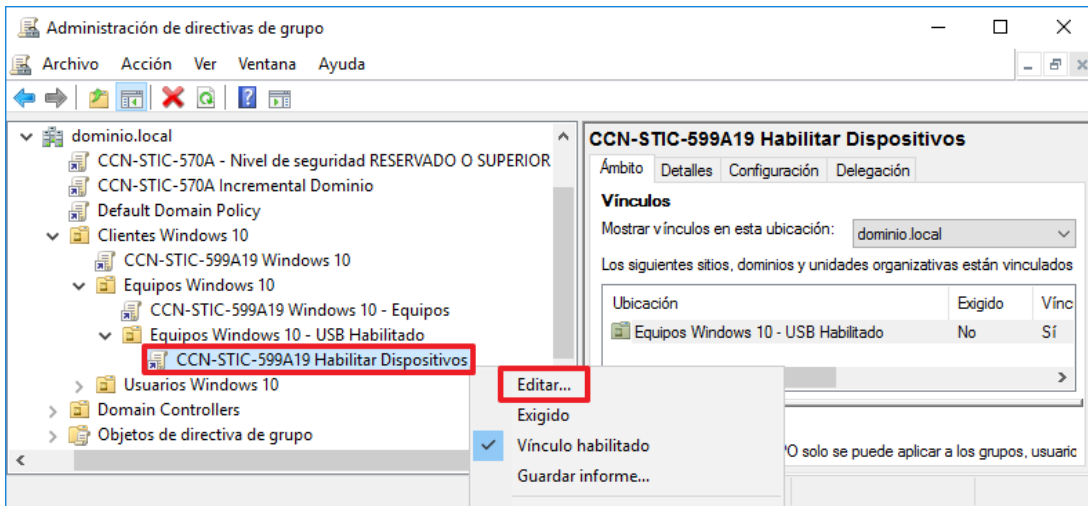
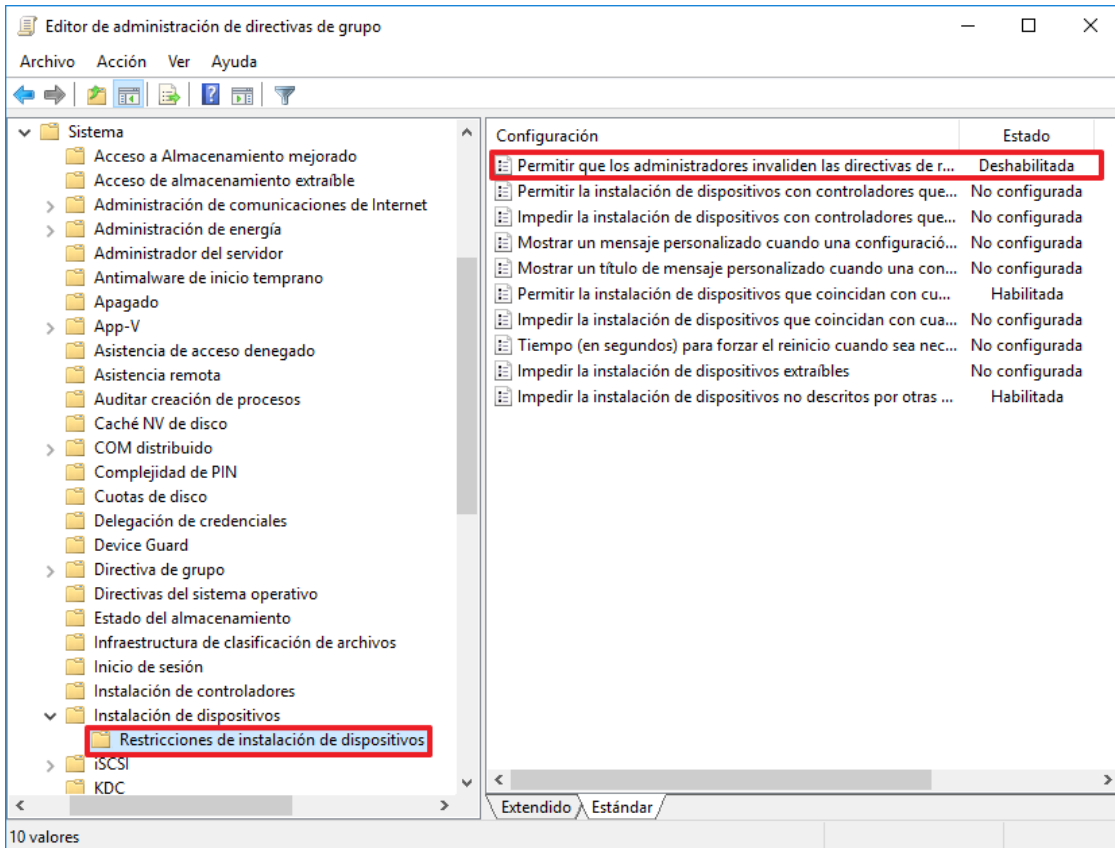
2. ADMINISTRAR USO DE DISPOSITIVOS USB DE ALMACENAMIENTO MEDIANTE LA INSTALACIÓN Y DESINSTALACIÓN DE CONTROLADORES

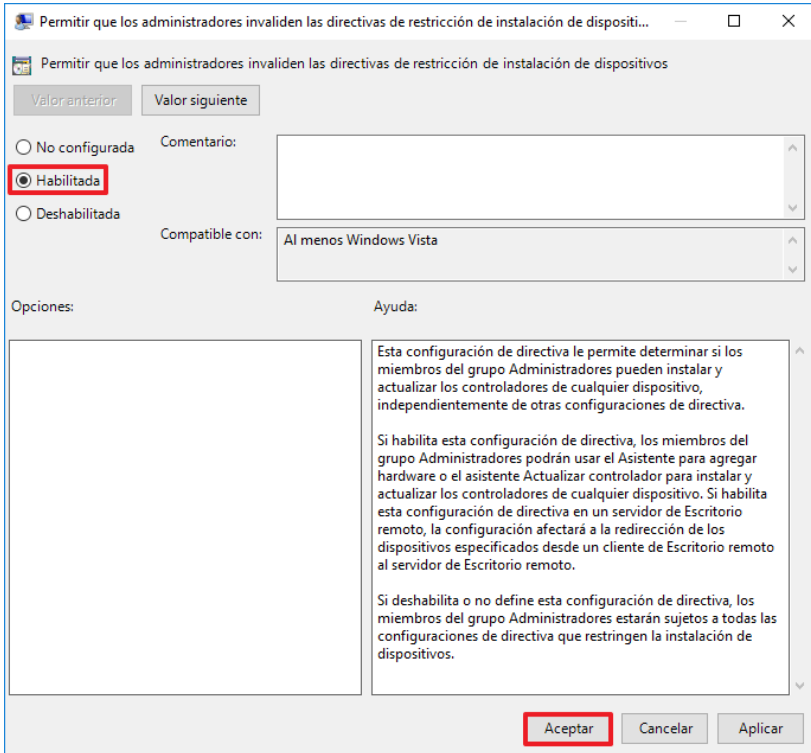
Este punto describe el proceso para instalar y desinstalar el controlador de un dispositivo USB a través de una cuenta que posea privilegios de administrador local de la máquina.

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.

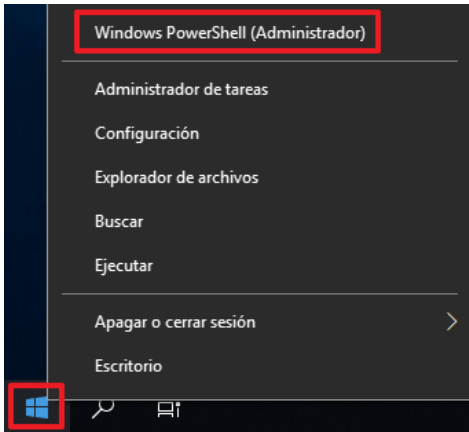
2.1. INSTALACIÓN DE CONTROLADORES PARA HABILITAR DISPOSITIVOS USB

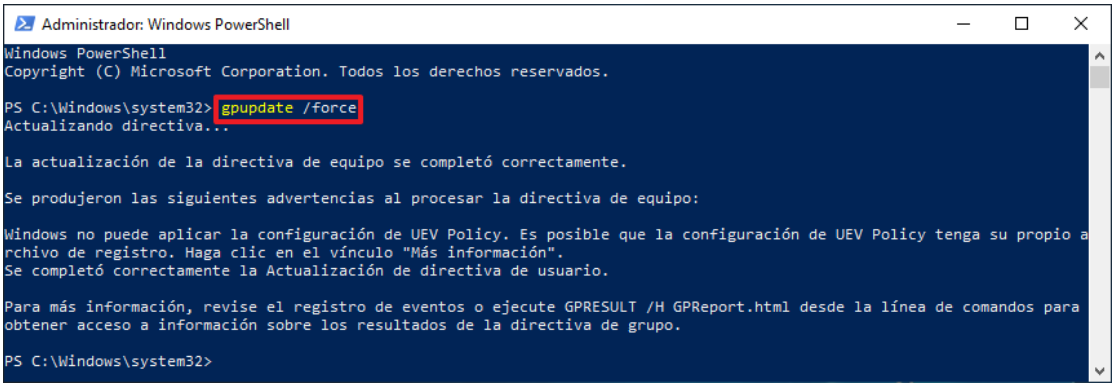
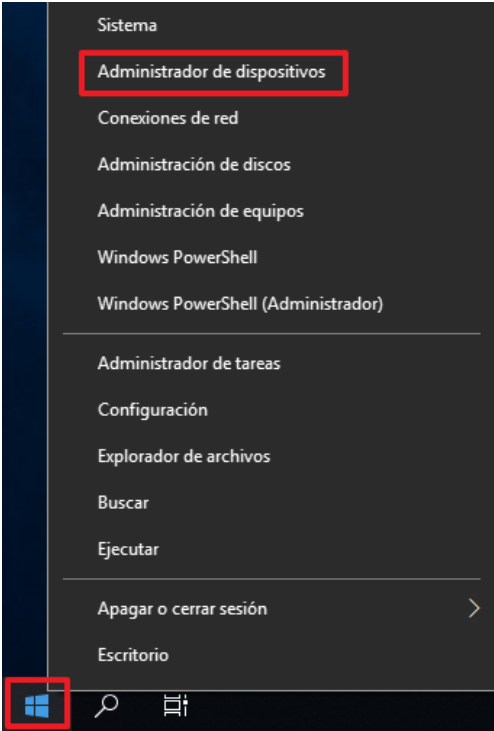
Paso	Descripción
32.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
33.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios.
34.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 

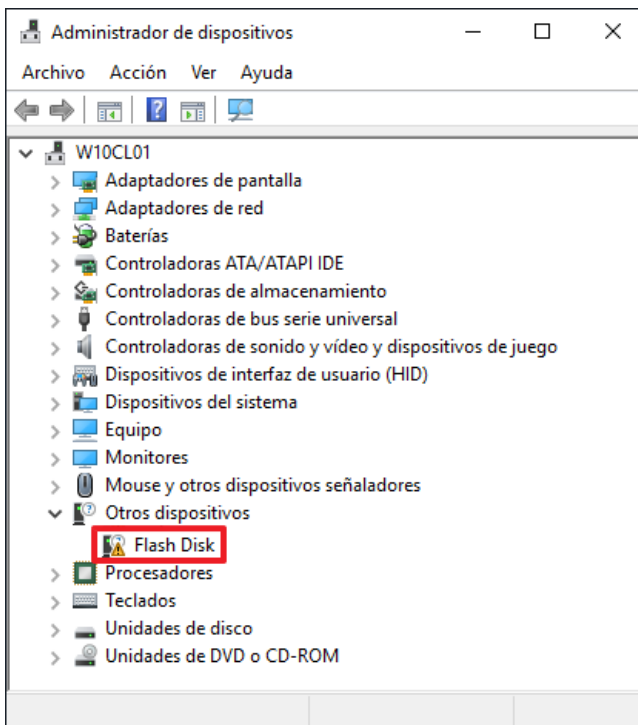
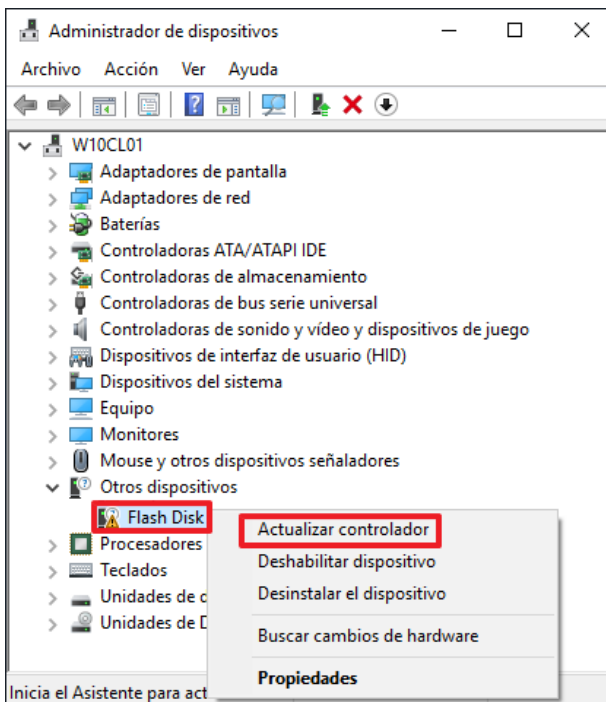
Paso	Descripción
35.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
36.	En el apartado “Objetos de directiva de grupo” seleccione la GPO creada anteriormente, “CCN-STIC-599A19 Habilitar dispositivos”, con el botón derecho y seleccione la opción del menú contextual “Editar...”. 
37.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

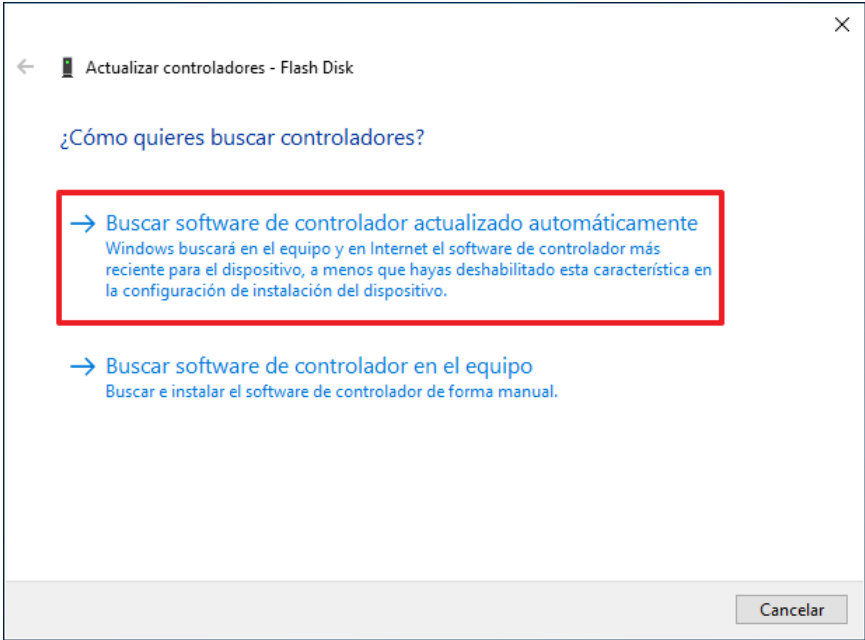
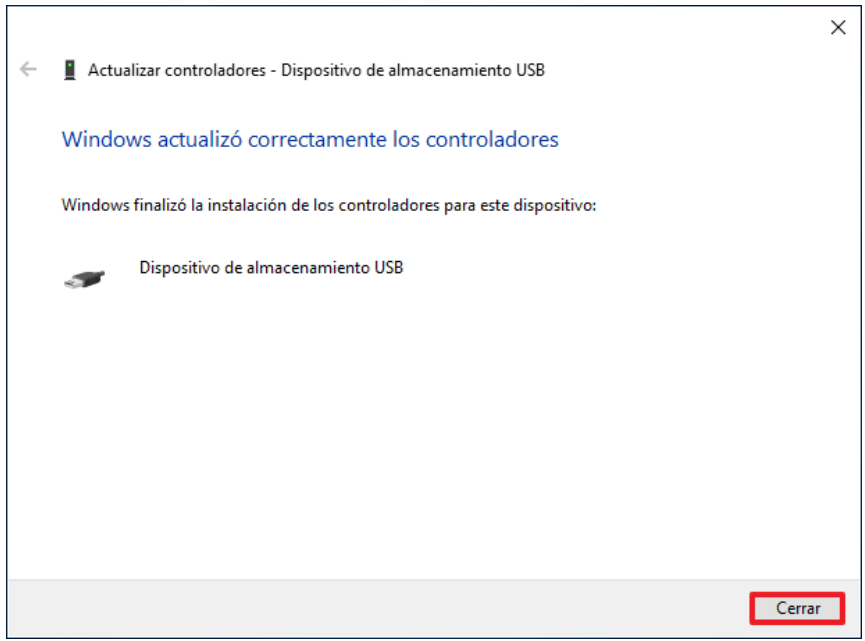
Paso	Descripción
38.	Haga doble clic sobre la directiva “Permitir que los administradores invaliden las directivas de restricción de instalación de dispositivos” y configúrela para que su estado sea “Habilitada”. A continuación pulse “Aceptar”. 

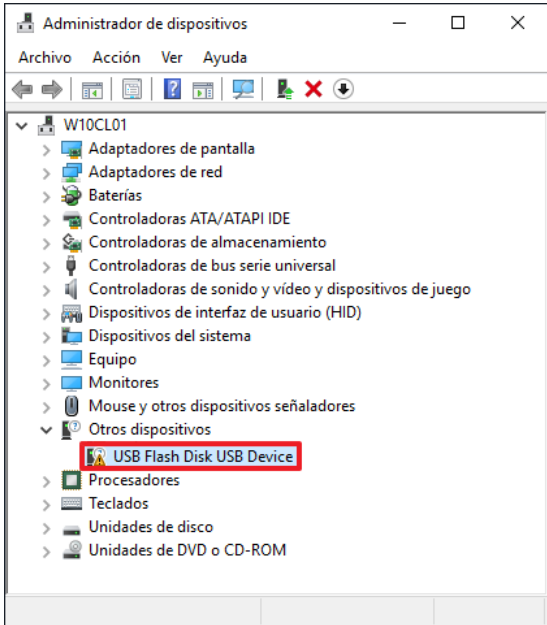
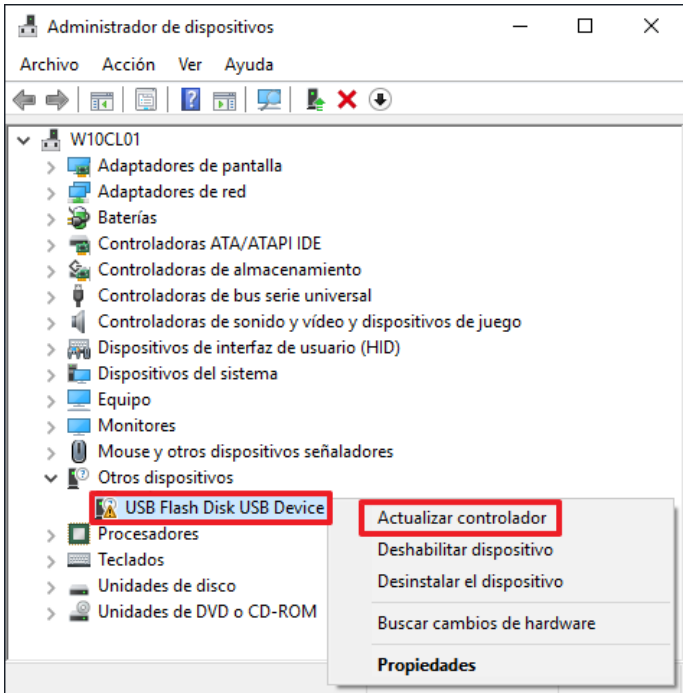
Los pasos definidos a continuación deberá realizarlos sobre un equipo Windows 10 perteneciente al dominio sobre el que se está habilitando el uso de dispositivos USB.

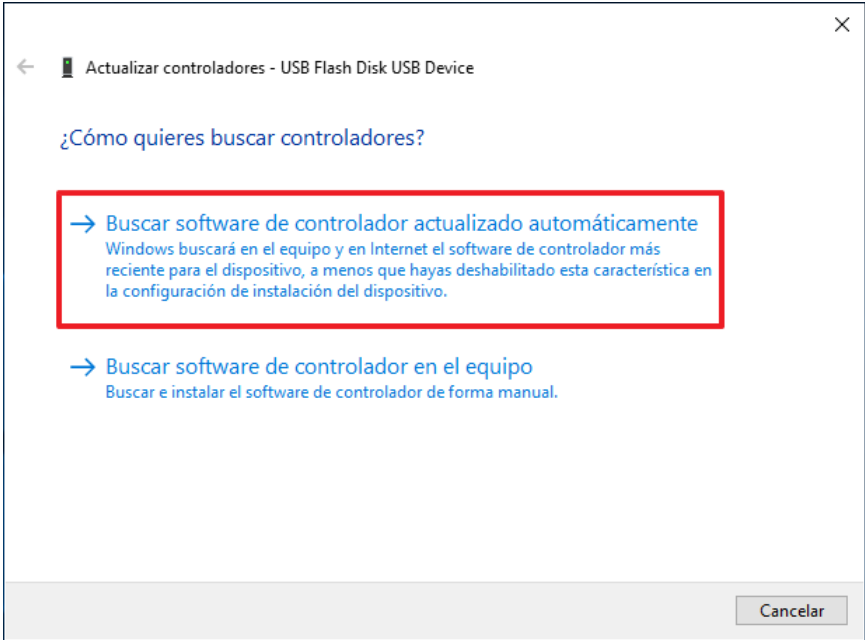
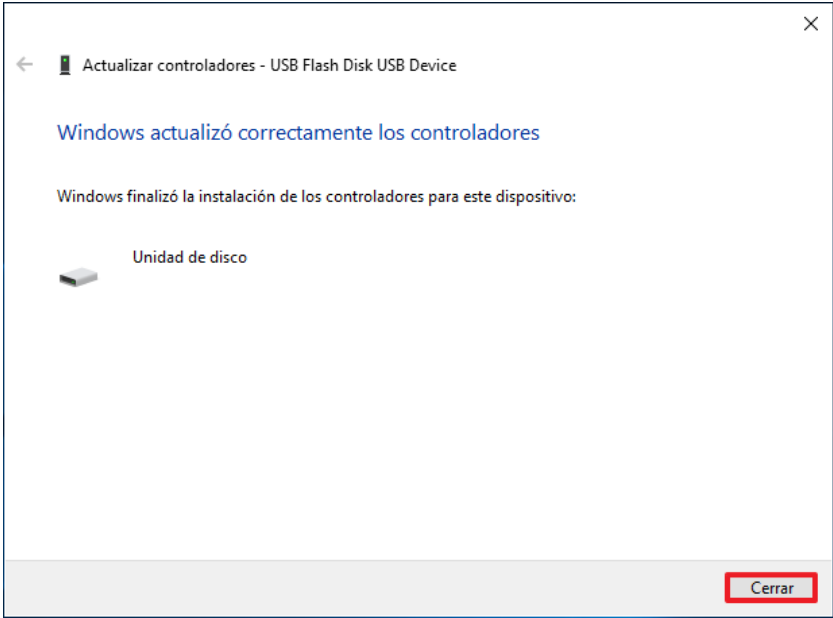
Paso	Descripción
39.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
40.	Deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 

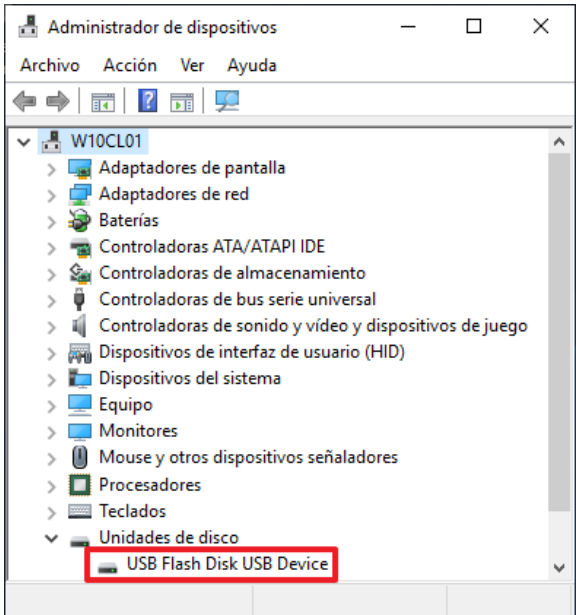
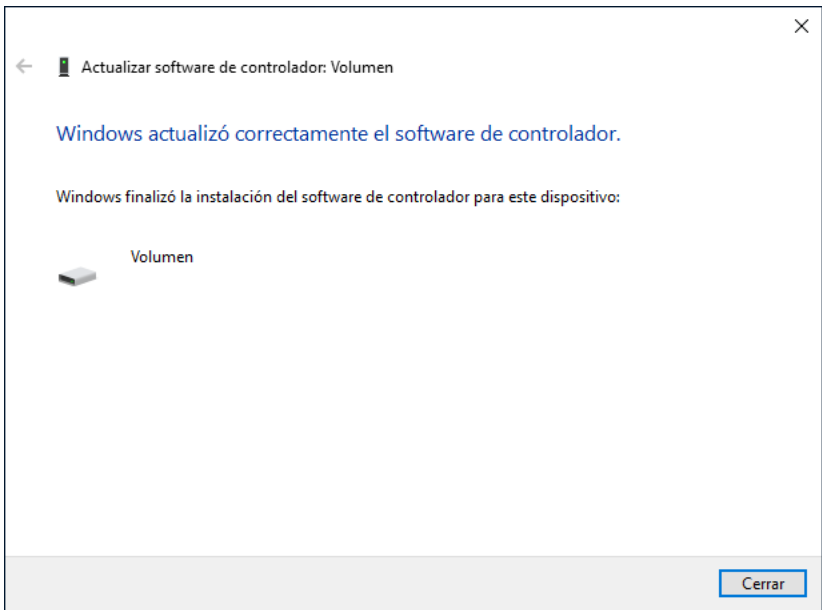
Paso	Descripción
41.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar.
42.	Ejecute el comando “gpupdate /force” y espere a que finalice. 
43.	Para iniciar la instalación 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 que pertenezca al grupo “Admins. del dominio”.
44.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

Paso	Descripción
45.	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”.
46.	Haga clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 

Paso	Descripción
47.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 
48.	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.

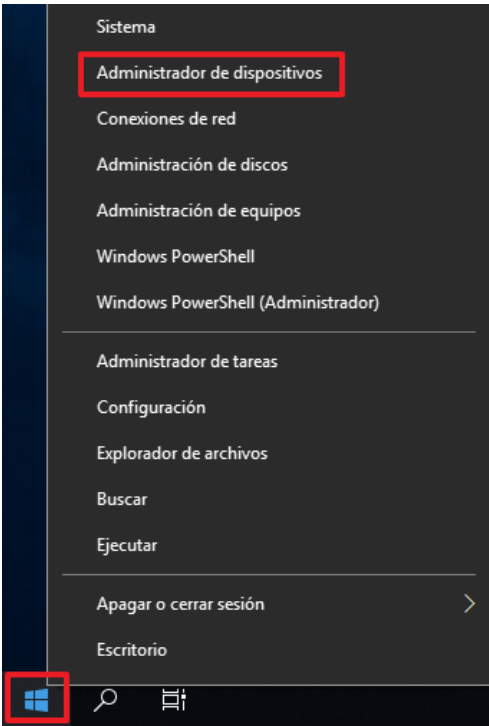
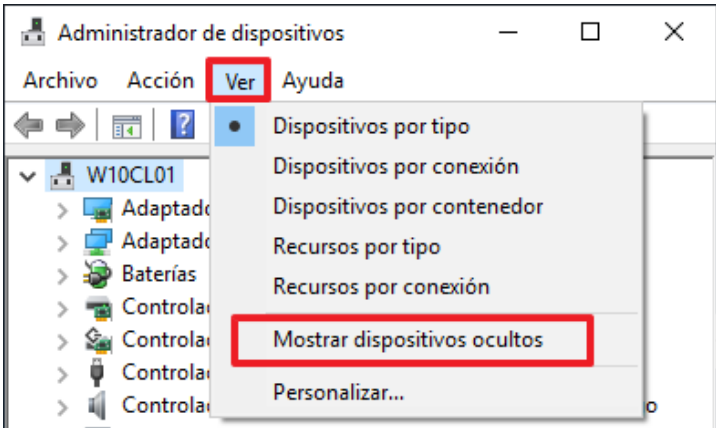
Paso	Descripción
49.	Tras la instalación de los controladores el sistema reconocerá el dispositivo. Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: En este ejemplo se utiliza el dispositivo denominado “USB 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”.
50.	Haga de nuevo clic derecho con el ratón sobre el dispositivo y seleccione la opción del menú contextual “Actualizar controlador”. 

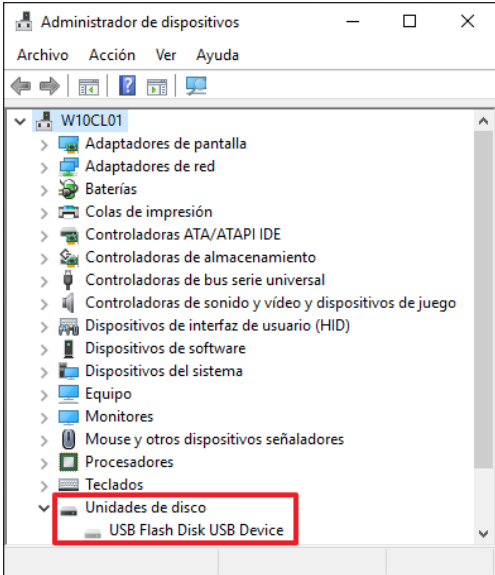
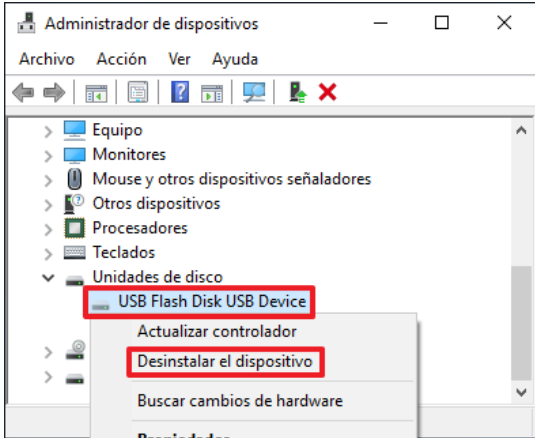
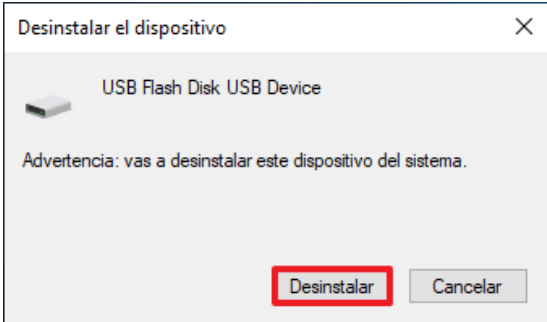
Paso	Descripción
51.	A continuación se iniciará el asistente para instalar del software necesario. Seleccione la opción “Buscar software de controlador actualizado automáticamente”. 
52.	Comenzará la instalación de los controladores automáticamente. Espere a que finalice y pulse “Cerrar” cuando haya finalizado.  Nota: Deberá repetir estos pasos hasta que su dispositivo de almacenamiento aparezca en el apartado “Unidades de disco”.

Paso	Descripción
53.	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”.
54.	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. 
55.	El dispositivo está listo para ser utilizado.

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

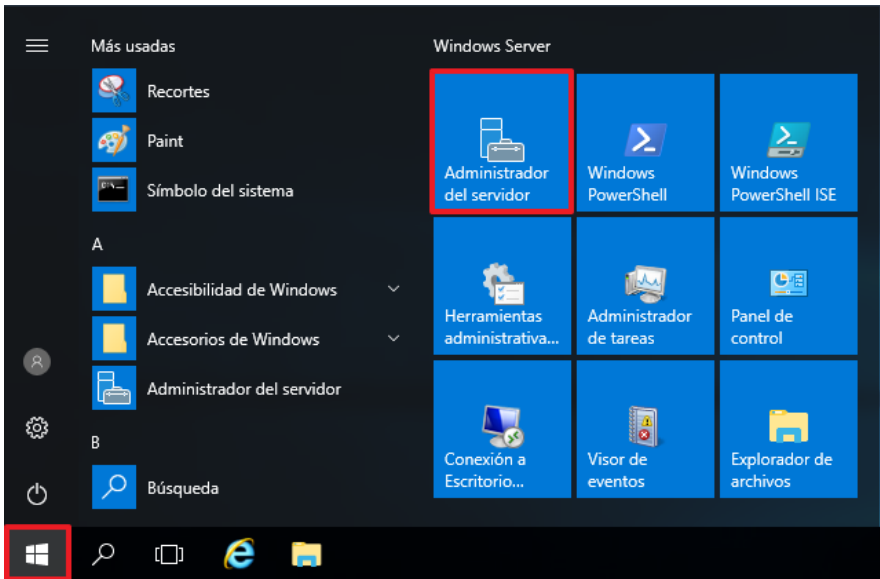
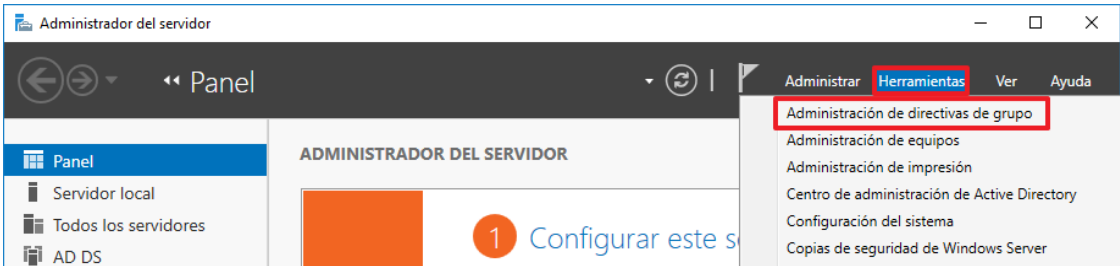
Tras la instalación del dispositivo y su posterior uso será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

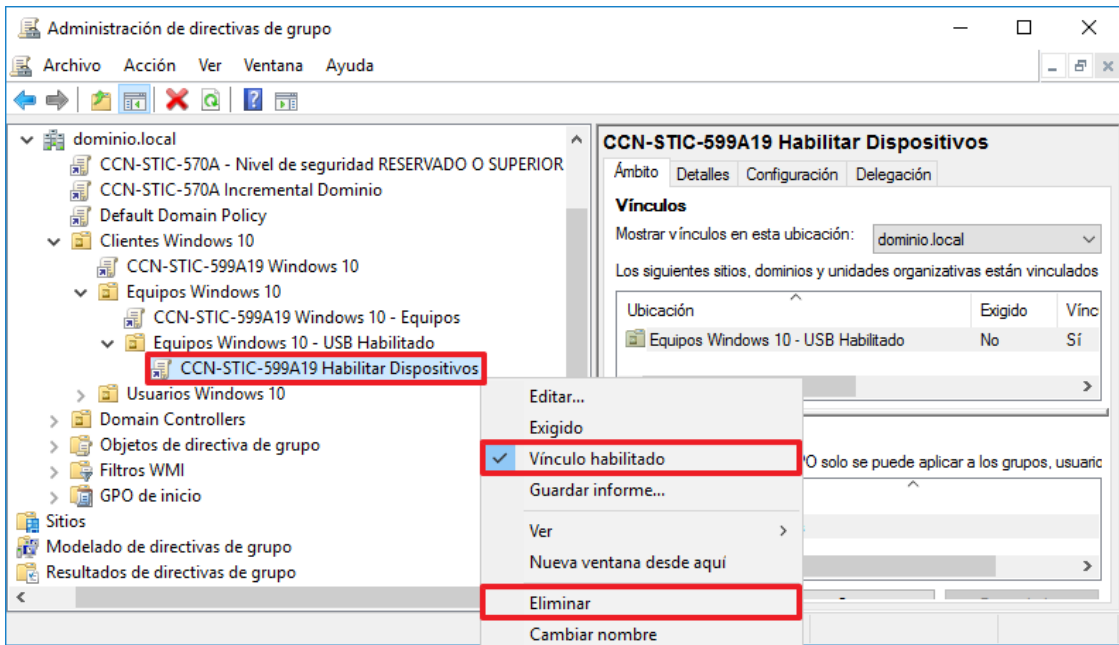
Paso	Descripción
56.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
57.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
58.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

Paso	Descripción
59.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 
60.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
61.	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.

Ejecute los siguientes pasos en el equipo controlador de dominio al que pertenece el equipo Windows 10 sobre el que se está deshabilitando el uso de dispositivos USB.

Nota: El siguiente procedimiento desvincula la GPO “CCN-STIC-599A19 Habilitar dispositivos”. Si no desea desvincular la GPO, no realice los siguientes pasos.

Paso	Descripción
62.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
63.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios.
64.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
65.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta: "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"

Paso	Descripción
66.	Sobre la unidad organizativa creada para habilitar el uso de dispositivos USB “Equipos Windows 10 – USB habilitado” seleccione la GPO vinculada “CCN-STIC-599A19 Habilitar dispositivos” con el botón derecho y desmarque la opción “Vínculo habilitado” o seleccione “Eliminar”. 
67.	Con esto quedará desvinculada la GPO de la unidad organizativa y se volverá al estado anterior de bloqueo de dispositivos USB.

3. 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.

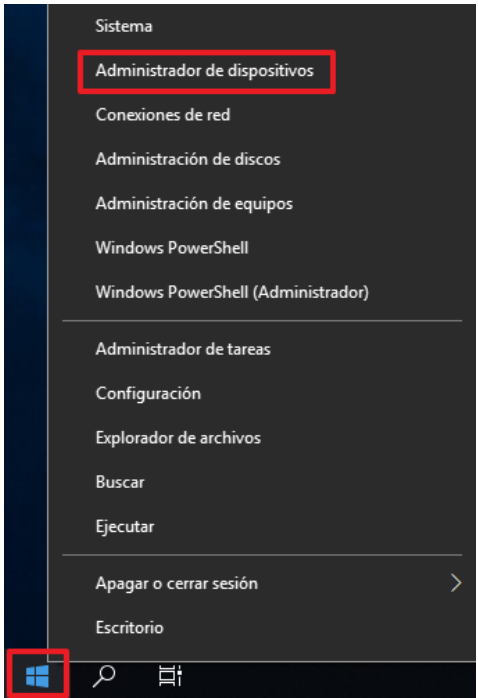
3.1. INSTALACIÓN Y FILTRADO DE DISPOSITIVOS USB MEDIANTE IDENTIFICADOR

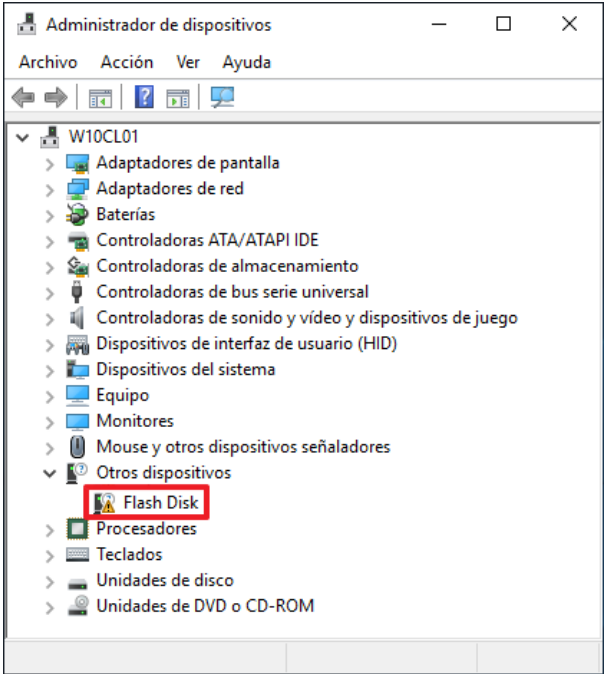
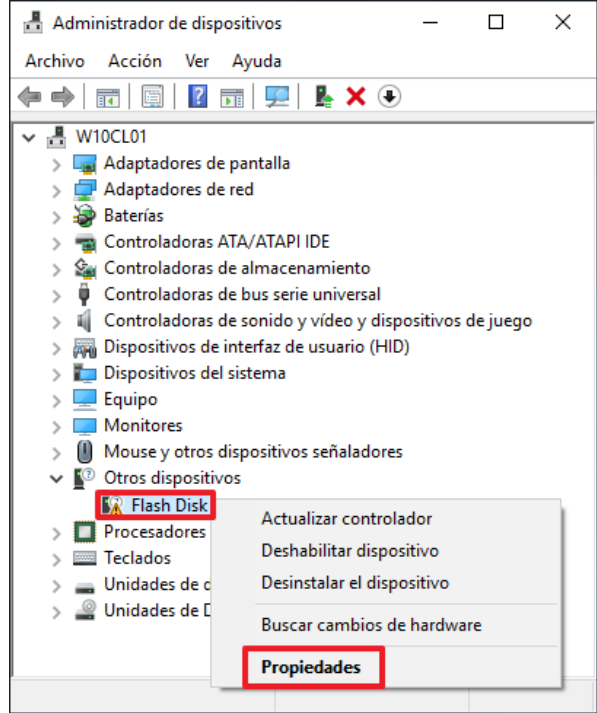
Este punto describe el proceso para permitir el uso un dispositivo mediante el filtrado por su identificador. Cuando el filtro esté realizado, los controladores del dispositivo se instalarán de manera automática y el dispositivo podrá ser utilizado.

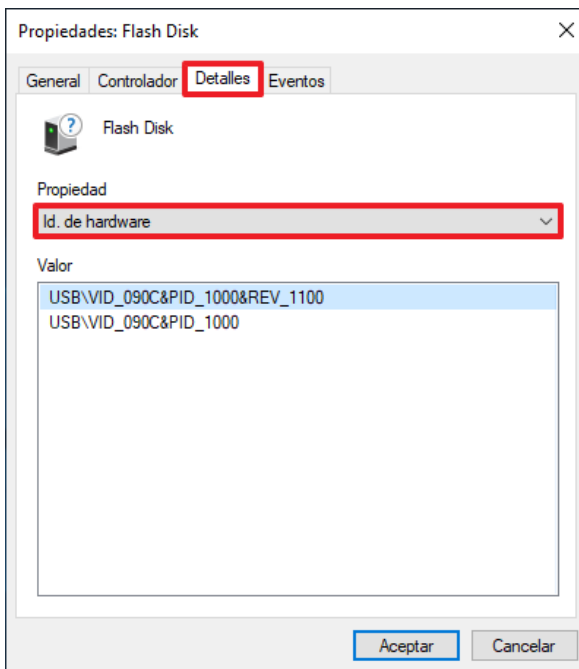
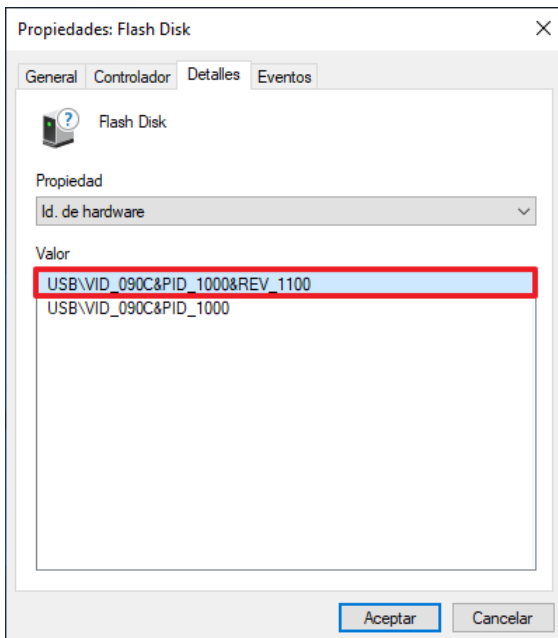
Tras la finalización de su uso, los controladores del dispositivo serán desinstalados tanto si el dispositivo se encuentra conectado al equipo como si no.

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.

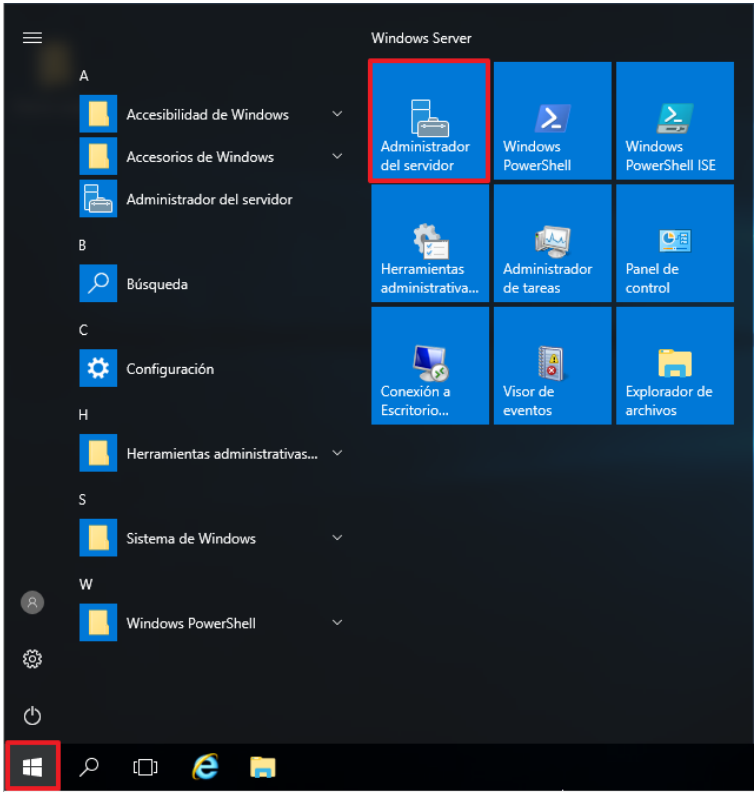
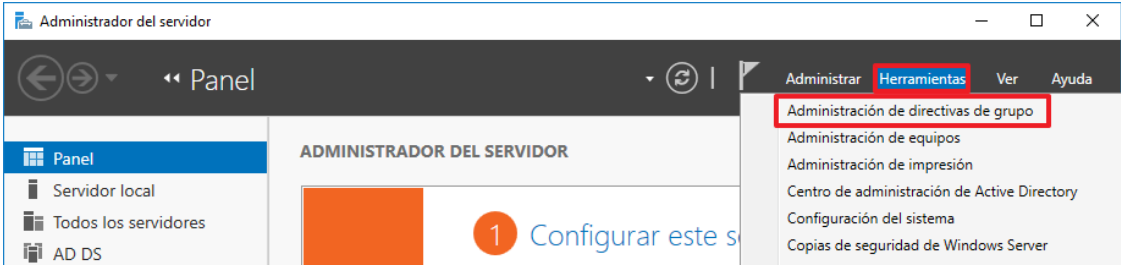
Tras el uso de los dispositivos se procederá a eliminar los identificadores de la lista configurada, y a desinstalar los controladores para evitar el uso de éstos.

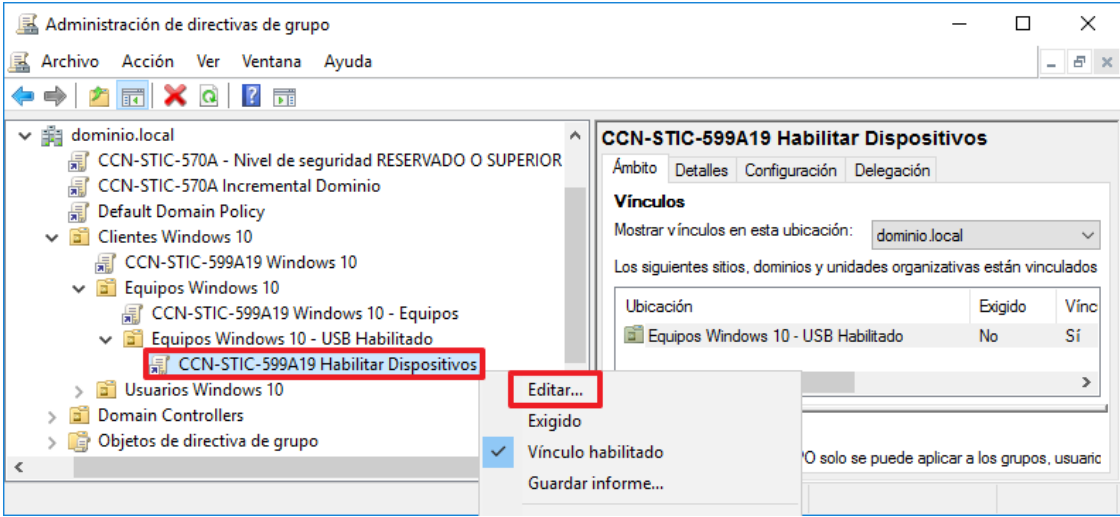
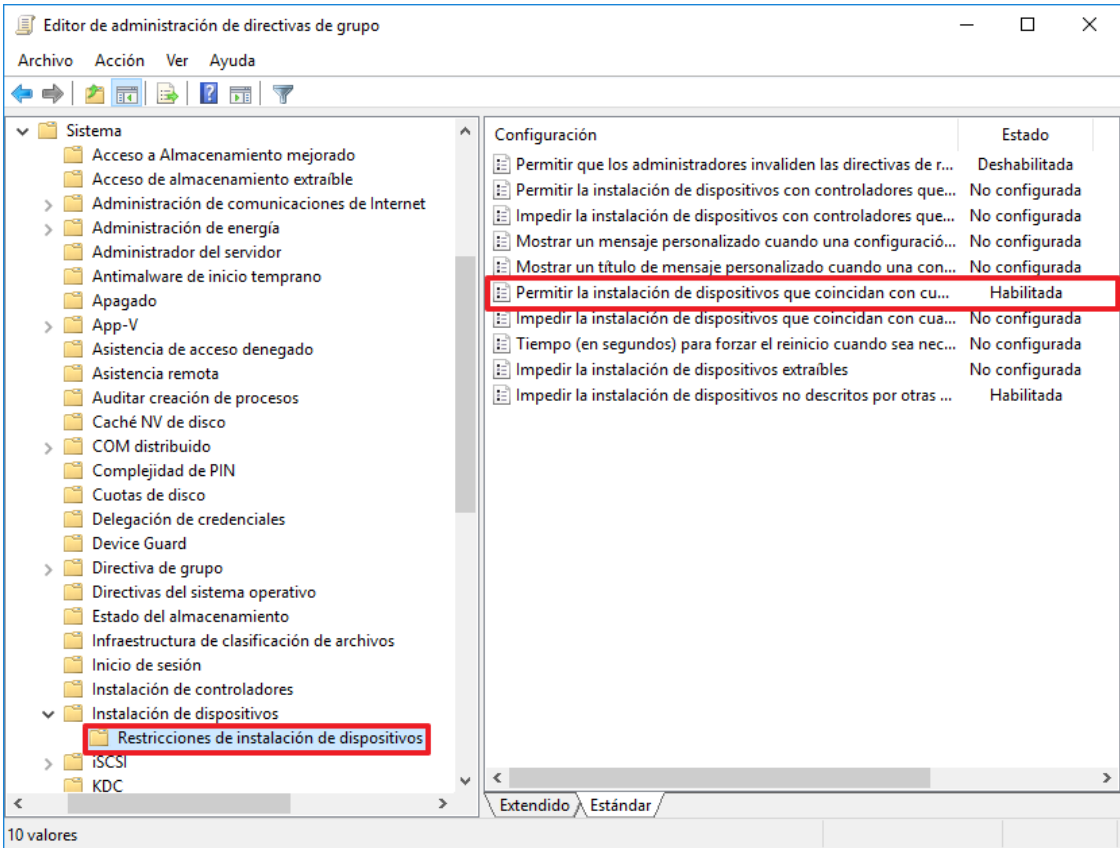
Paso	Descripción
68.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
69.	Para iniciar la instalación de un dispositivo USB deberá conectarlo en el equipo. Nota: Es necesario tener en consideración que la instalación de los dispositivos USB debe realizarse de manera manual y por un usuario que pertenezca al grupo “Admins. del dominio”.
70.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.

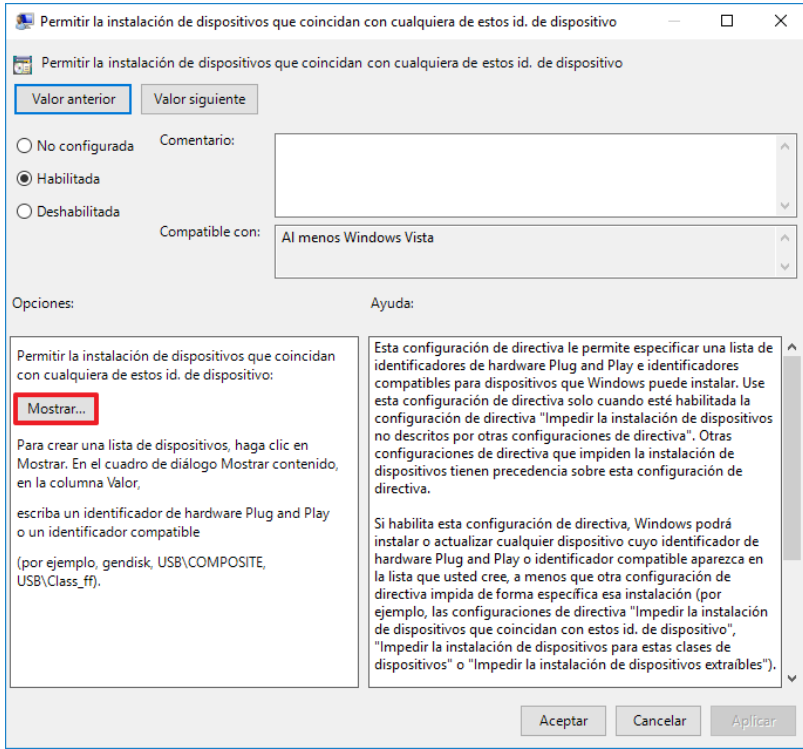
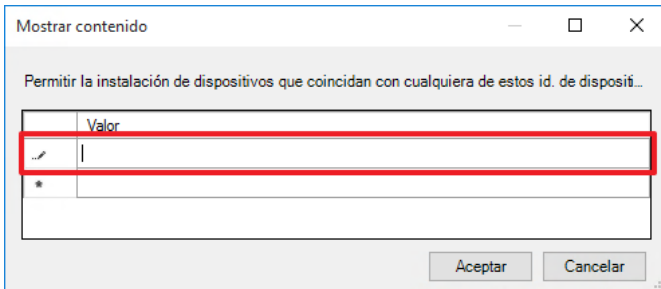
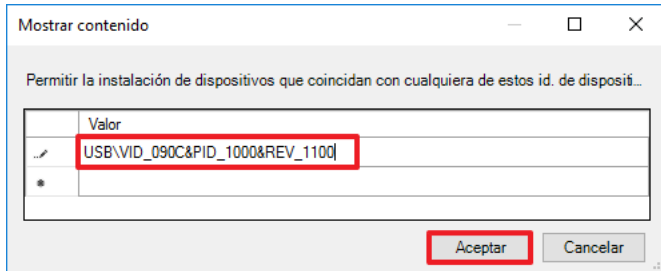
Paso	Descripción
71.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: Debido a la inexistencia de controlador instalado, es posible que el sistema no reconozca el nombre del dispositivo y le asigne el nombre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

Paso	Descripción
73.	Acceda a la pestaña “Detalles”. En el apartado “Propiedad” seleccione “Id. de hardware”.  The screenshot shows the 'Propiedades: Flash Disk' window with the 'Detalles' tab selected. The 'Propiedad' dropdown menu is open, showing 'Id. de hardware' as the selected option. The 'Valor' list below it contains two entries: 'USB\VID_090C&PID_1000&REV_1100' and 'USB\VID_090C&PID_1000'.
74.	Seleccione el identificador que se encuentre en primer lugar y anótelo para poder introducirlo más adelante.  The screenshot shows the same 'Propiedades: Flash Disk' window. The first item in the 'Valor' list, 'USB\VID_090C&PID_1000&REV_1100', is highlighted with a red box. Nota: Independientemente del numero de identificadores existentes, deberá seleccionar siempre aquél que se encuentre en primera posición.

Realice los siguientes pasos en el controlador de dominio del dominio al que pertenece el equipo Windows 10 que está asegurando para permitir el uso de dispositivos USB.

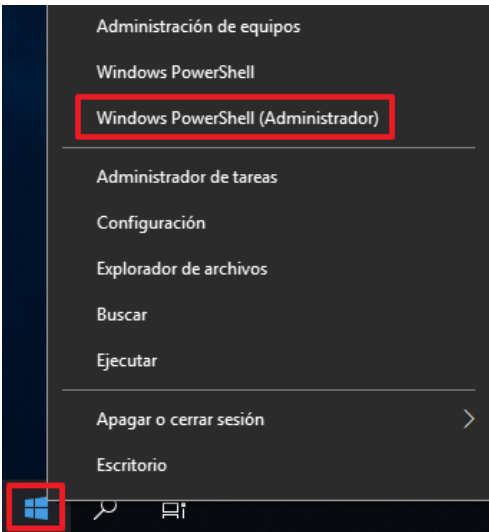
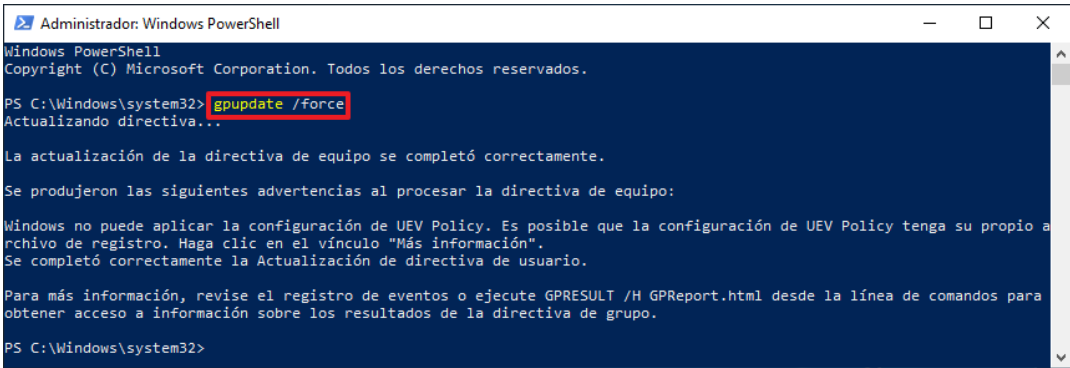
Paso	Descripción
75.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
76.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 
77.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
78.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta: "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"

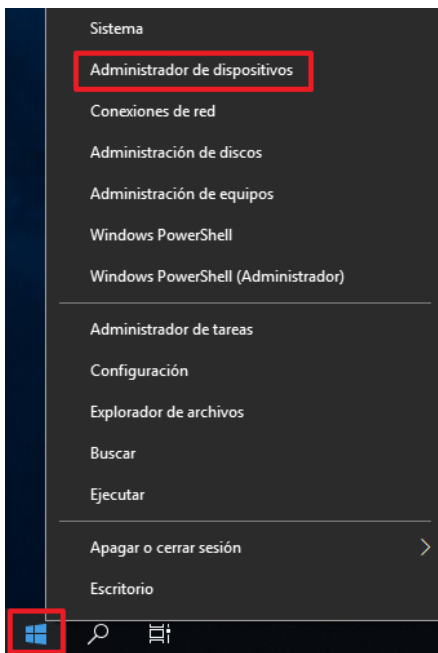
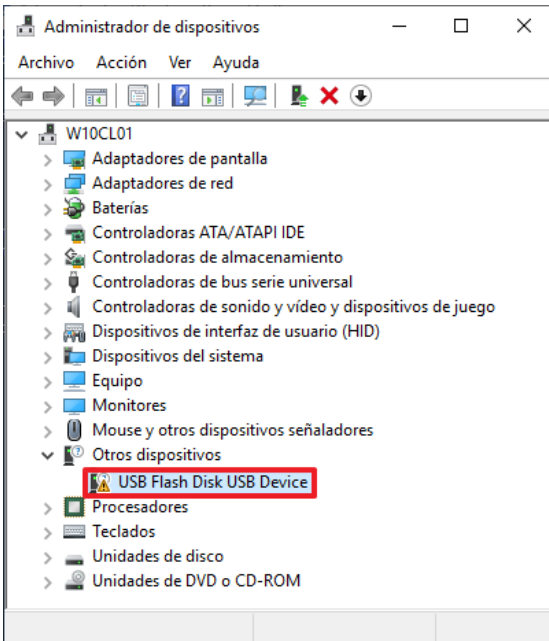
Paso	Descripción
79.	En el apartado “Objetos de directiva de grupo” seleccione la GPO creada anteriormente con el botón derecho y seleccione la opción del menú contextual “Editar”. 
80.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 

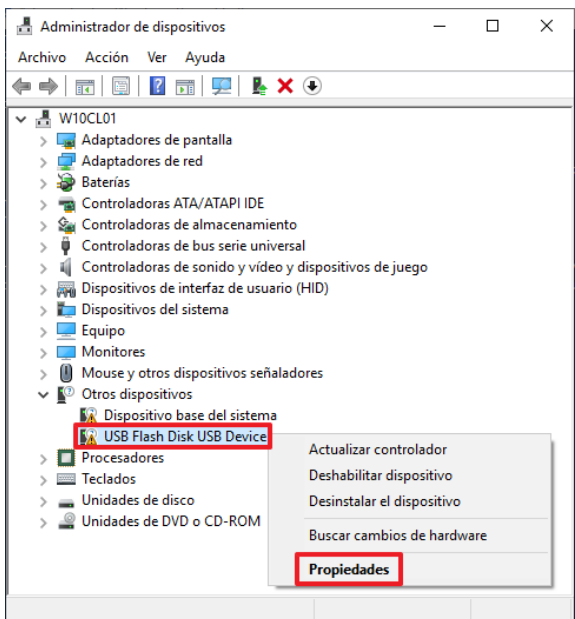
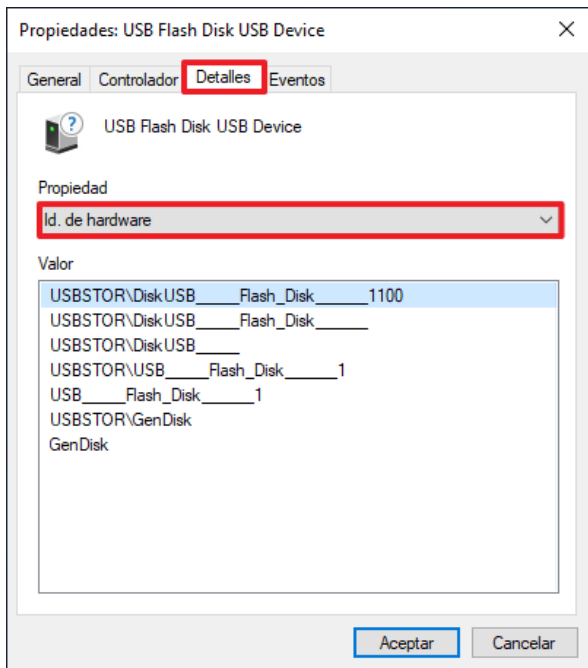
Paso	Descripción
81.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar...”. 
82.	En la ventana emergente “Mostrar contenido” haga 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.
83.	Verifique el identificador introducido y pulse “Aceptar” para continuar. 

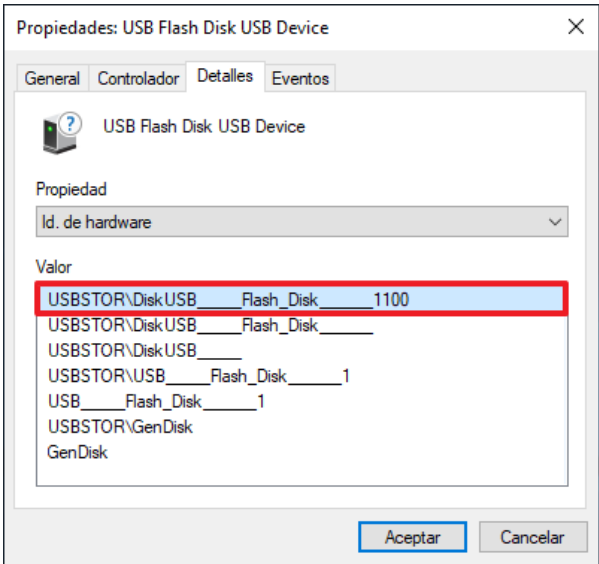
Paso	Descripción
84.	Pulse “Aplicar” en la ventana de la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”.
85.	Sin cerrar el “Editor de directivas de grupo local”, continúe con el siguiente paso.

Ejecute los siguientes pasos dentro del equipo cliente Windows 10 sobre el que está habilitando el uso de dispositivos USB.

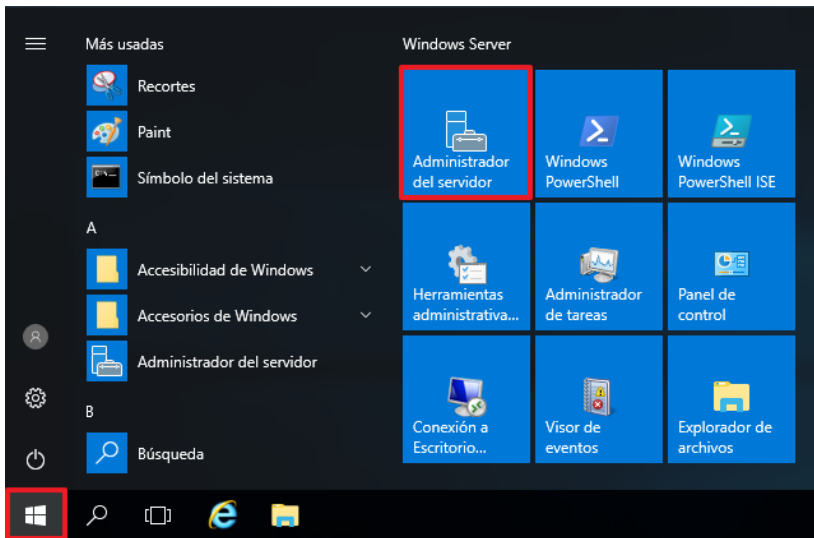
Paso	Descripción
86.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
87.	Deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 
88.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca la credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar.
89.	Ejecute el comando “gpupdate /force” y espere a que finalice. 

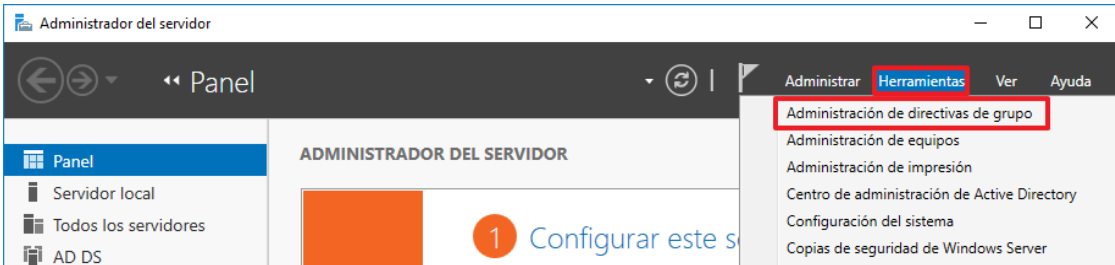
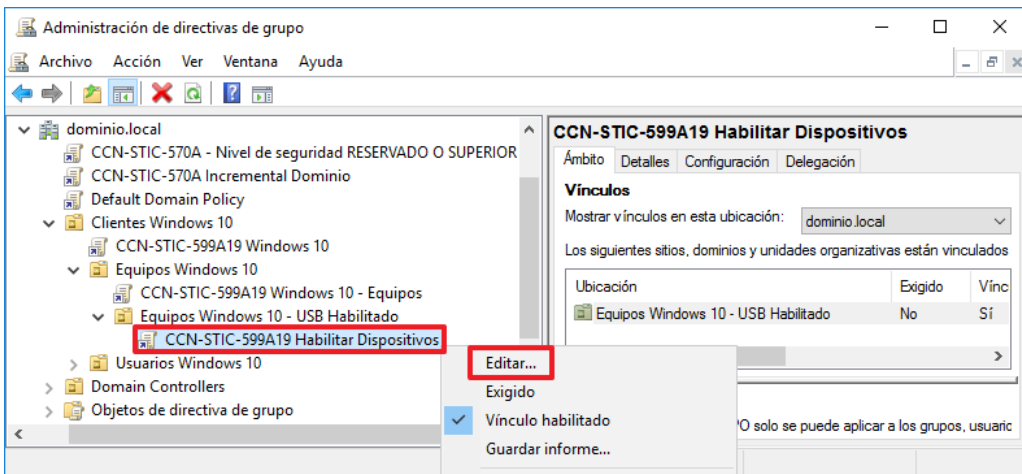
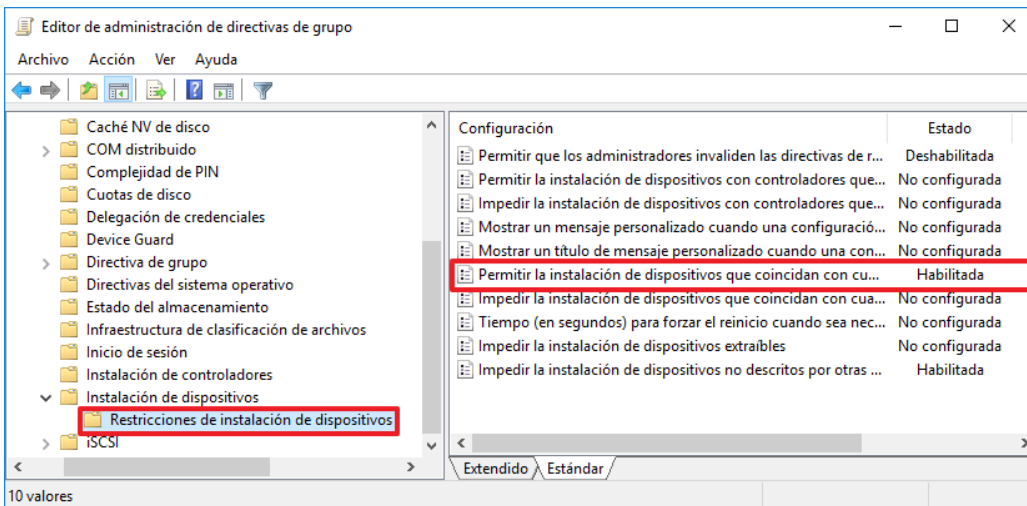
Paso	Descripción
90.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
91.	Despliegue en el “Administrador de dispositivos” el nodo “Otros dispositivos” y localice el dispositivo USB sobre el que desea trabajar.  Nota: En este ejemplo se utiliza el dispositivo denominado “Flash Disk USB Device”. El nombre ha cambiado porque el equipo ha reconocido el identificador introducido en pasos anteriores.

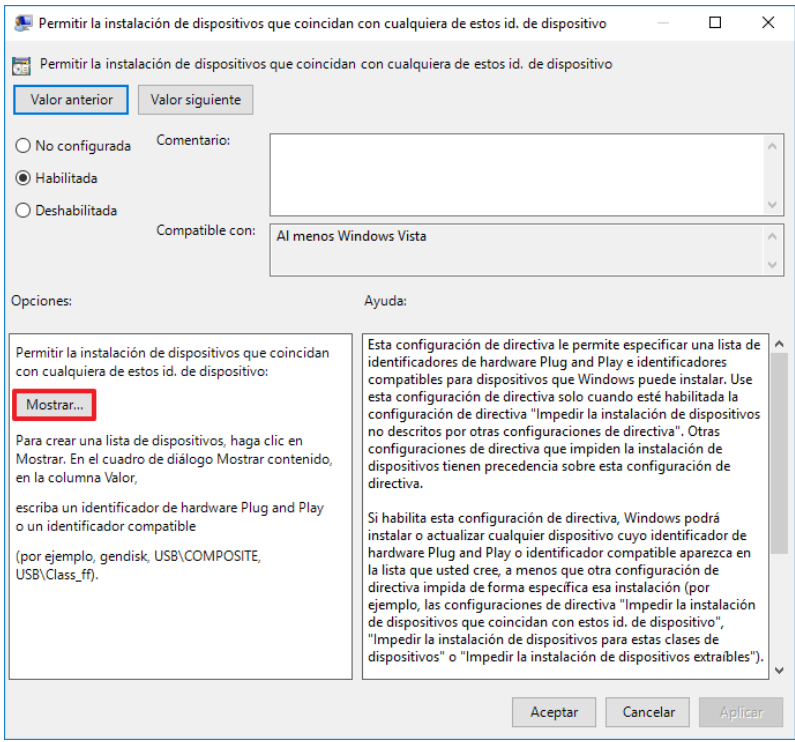
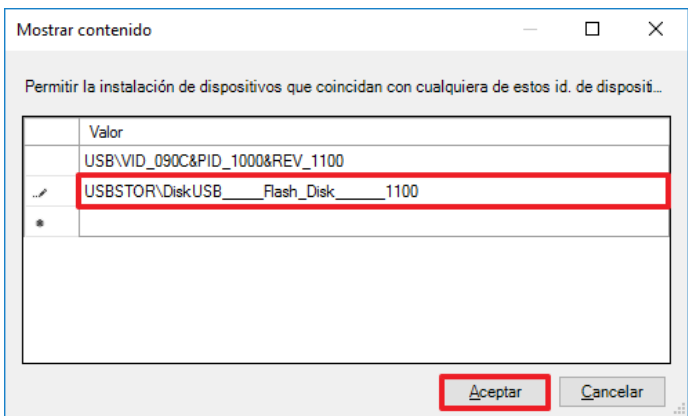
Paso	Descripción
92.	Seleccione dicho dispositivo con el botón derecho y pulse sobre la opción “Propiedades”.  Nota: Espere a que el dispositivo sea reconocido por el equipo. En caso de no ser así, extraiga y vuelva a conectar el dispositivo para que éste sea reconocido. También puede pulsar sobre el menú superior en la ruta “Acción → Buscar cambios de Hardware”.
93.	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.

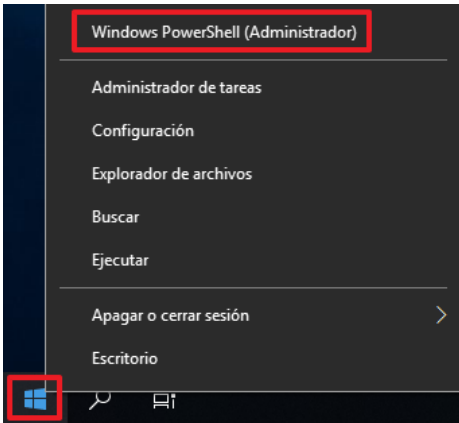
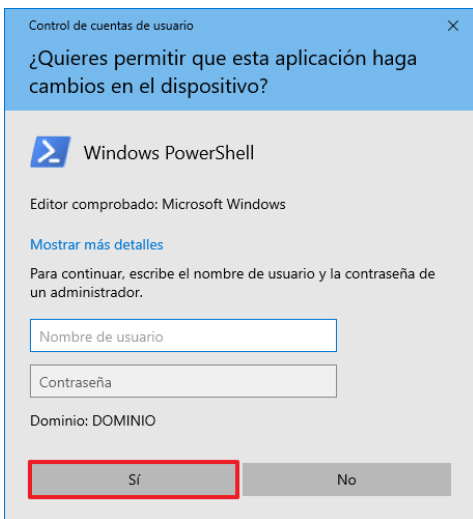
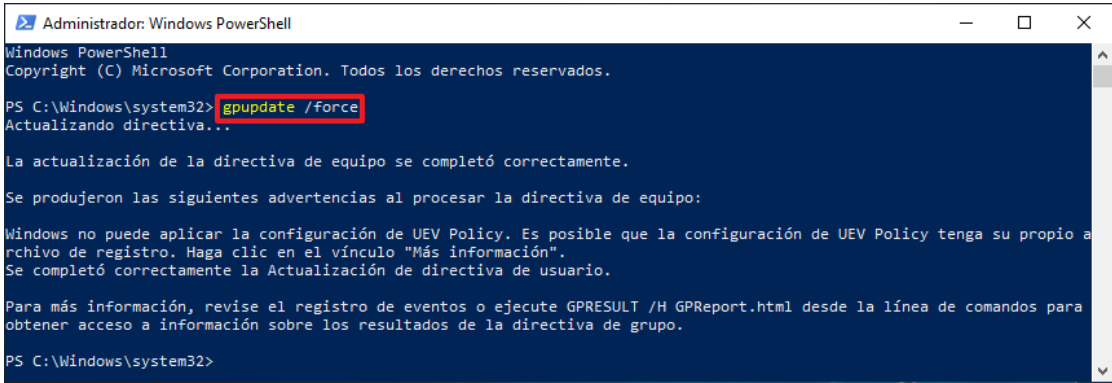
Paso	Descripción
94.	Seleccione el identificador que se encuentre en primer lugar y anótelolo para poder introducirlo más adelante.  Nota: Independientemente del numero de identificadores existentes deberá seleccionar siempre aquél que se encuentre en primera posición.

Realice los siguientes pasos en el controlador de dominio del dominio al que pertenece el equipo Windows 10 que está asegurando para permitir el uso de dispositivos USB.

Paso	Descripción
95.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
96.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. 

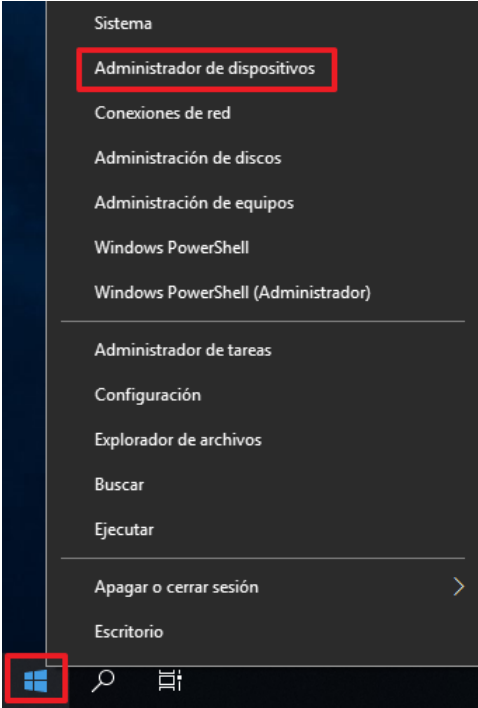
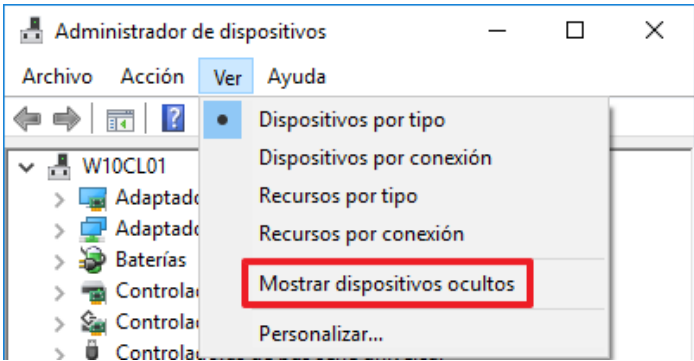
Paso	Descripción
97.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
98.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
99.	En el apartado "Objetos de directiva de grupo" seleccione la GPO creada anteriormente con el botón derecho y seleccione la opción del menú contextual "Editar". 
100.	Despliegue el nodo "Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos". 

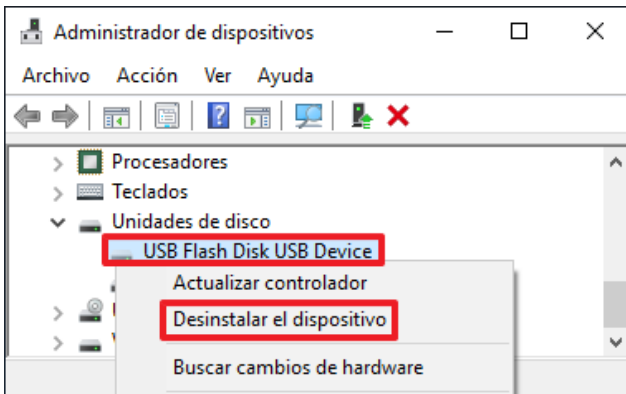
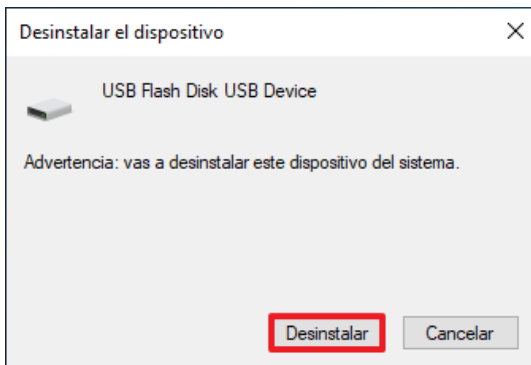
Paso	Descripción
101.	Haga doble clic sobre la directiva “Permitir la instalación de dispositivos que coincidan con cualquiera de estos id. de dispositivo”, la cual debe estar configurada como “Habilitada” y dentro de ella pulse el botón Mostrar...”. 
102.	En la ventana “Mostrar contenido” haga doble clic sobre la segunda línea para poder escribir. Introduzca entonces el identificador de USB copiado anteriormente. Pulse “Aceptar” para continuar. 
103.	Deberá repetir este proceso hasta que no se muestren nuevos identificadores en la propiedad “ID. de Hardware” del dispositivo que esta 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”.

Paso	Descripción
104.	Deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 
105.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca la credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar. 
106.	Ejecute el comando “gpupdate /force” y espere a que finalice. 
107.	A partir de este momento el dispositivo estará listo para su uso.

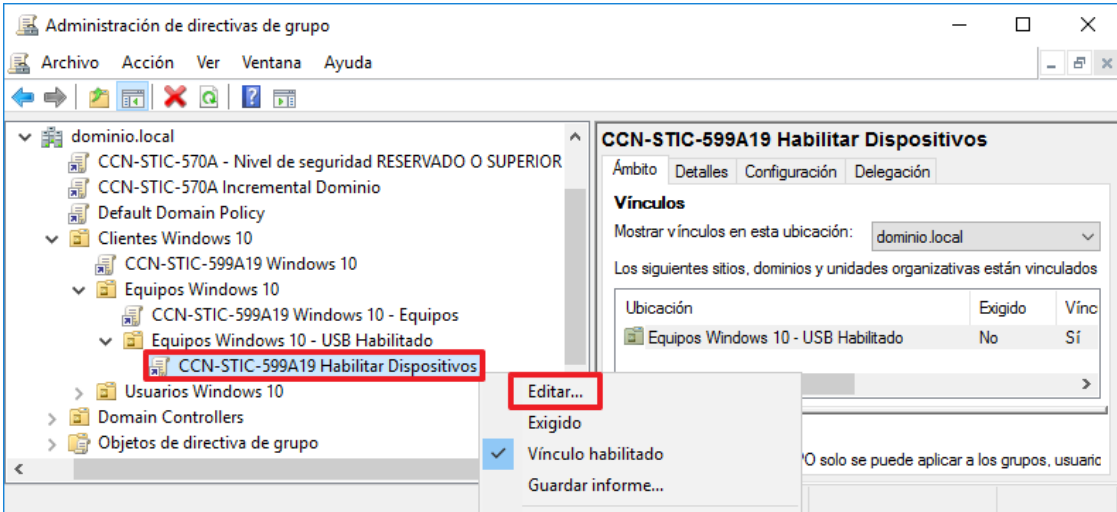
3.2. IMPEDIR EL USO DE DISPOSITIVOS USB

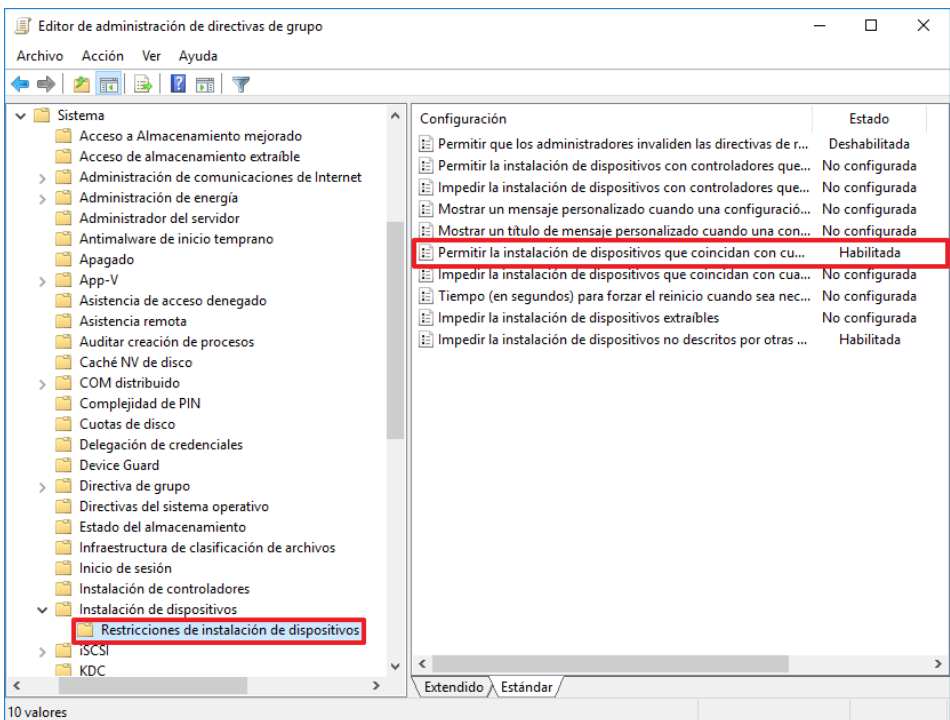
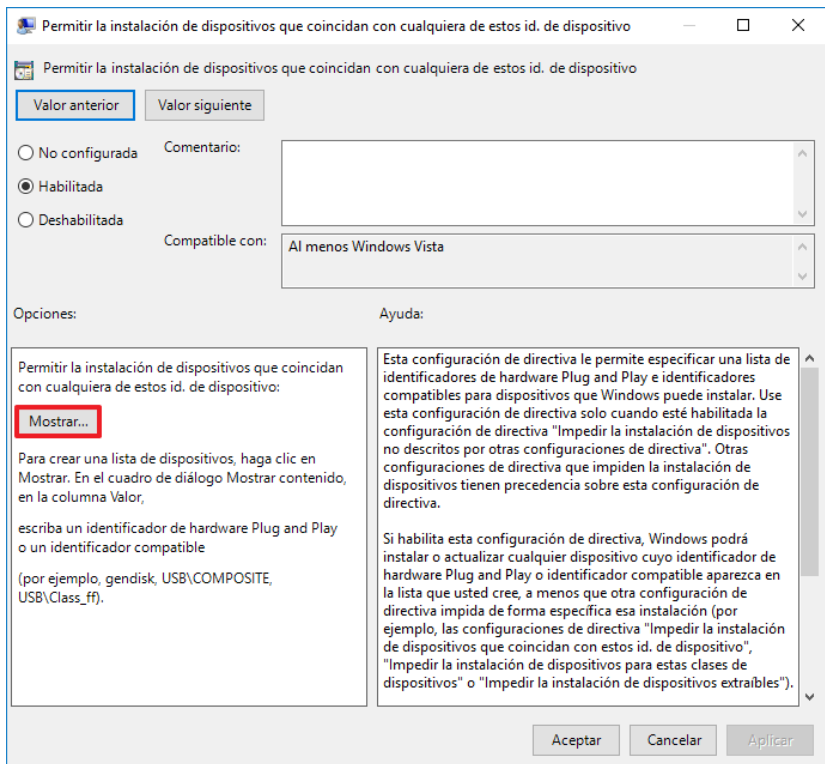
Tras la instalación del dispositivo y su posterior uso, será necesario volver al estado anterior de bloqueo del uso de dispositivos USB. Para ello deberá seguir los siguientes pasos.

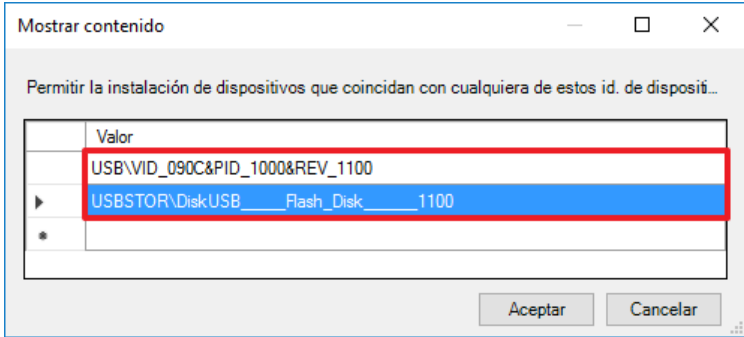
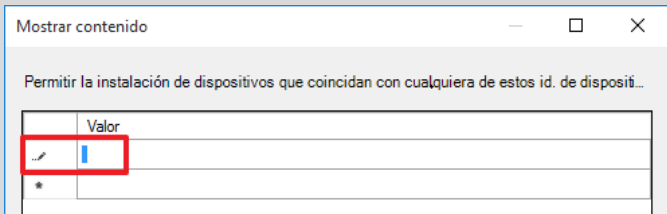
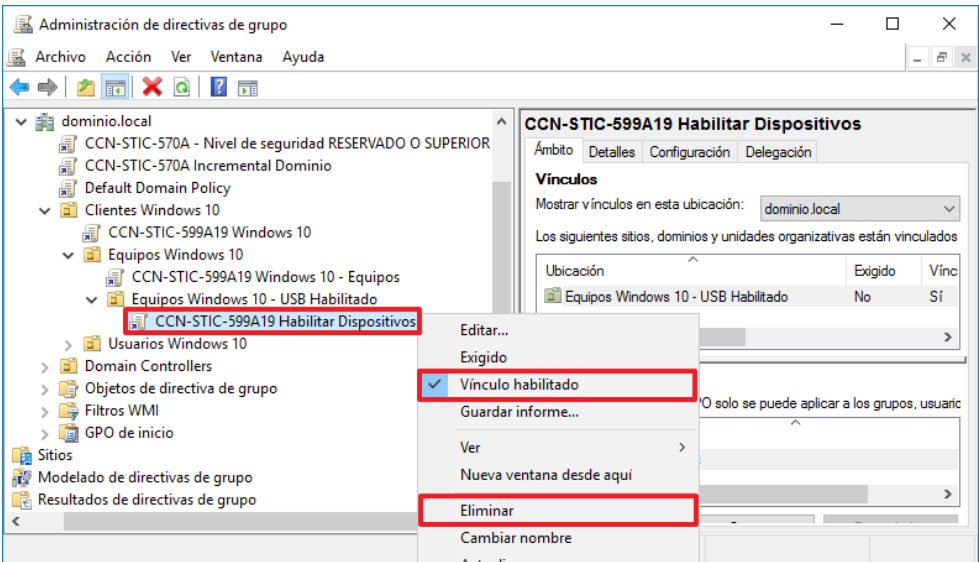
Paso	Descripción
108.	Inicie sesión en el equipo cliente Windows 10 que está asegurando con una cuenta con permisos de administrador del dominio.
109.	Pulse con botón derecho en inicio y seleccione “Administrador de dispositivos”.  Nota: El sistema le solicitará elevación de privilegios.
110.	Seleccione en el “Administrador de dispositivos”, abierto en el paso anterior, la pestaña ver y pulse sobre la opción “Mostrar dispositivos ocultos”. 

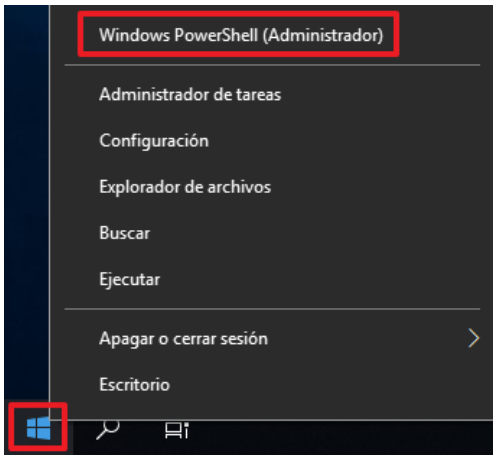
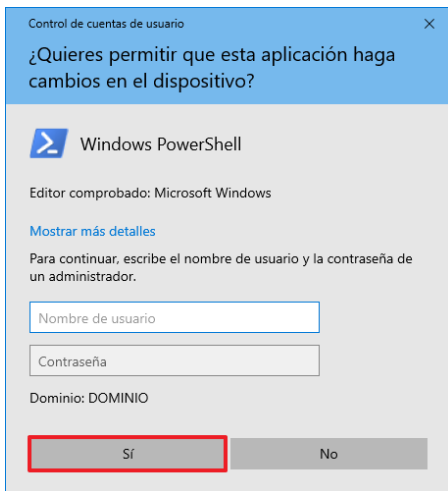
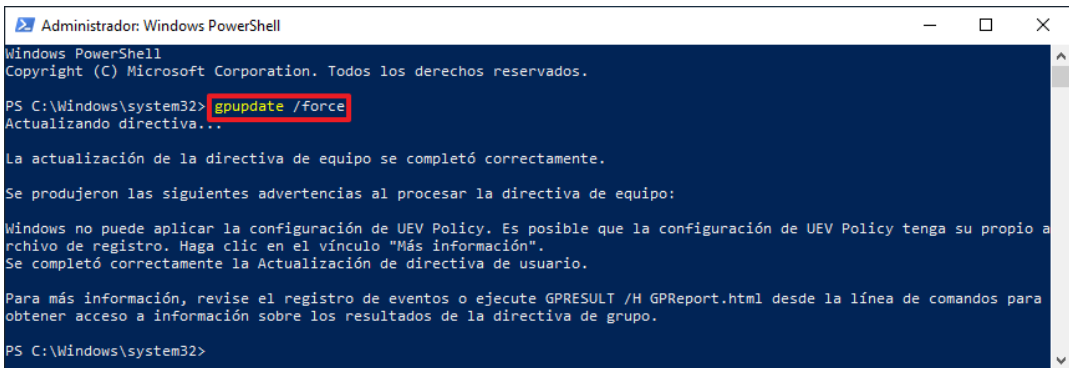
Paso	Descripción
111.	Sitúese en el nodo “Unidades de disco” y localice el dispositivo USB sobre el cual desea desinstalar los controladores. 
112.	Seleccione con el botón derecho el dispositivo USB y pulse sobre la opción del menú contextual “Desinstalar el dispositivo”. 
113.	Pulse “Desinstalar” ante 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.

Ejecute los siguientes pasos en el equipo controlador del dominio al que pertenece el equipo Windows 10 sobre el que se está deshabilitando el uso de dispositivos USB.

Paso	Descripción
114.	Inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el equipo cliente que va a asegurar, con una cuenta con derechos de administración en el dominio.
115.	Inicie la herramienta "Administrador del servidor" mediante el icono correspondiente en el menú de inicio. Nota: El sistema le solicitará elevación de privilegios.
116.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse "Administración de directivas de grupo". 
117.	En la consola de "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"
118.	En el apartado "Objetos de directiva de grupo" seleccione la GPO creada anteriormente con el botón derecho y seleccione la opción del menú contextual "Editar...". 

Paso	Descripción
119.	Despliegue el nodo “Configuración del equipo → Plantillas administrativas → Sistema → Instalación de dispositivos → Restricciones de instalación de dispositivos”. 
120.	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...”. 

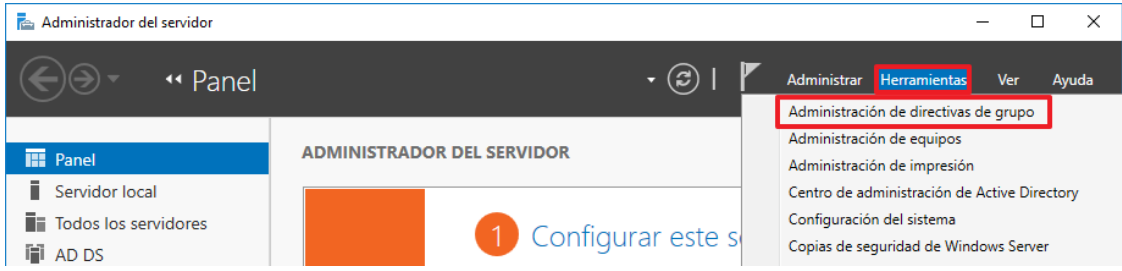
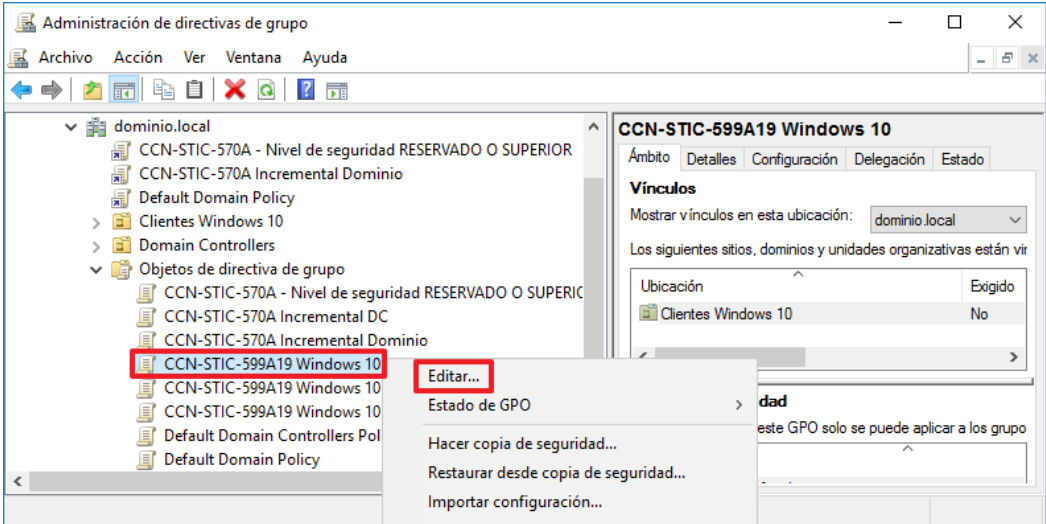
Paso	Descripción
121.	Elimine los identificadores correspondientes a los dispositivos sobre los cuales ya no se desea su uso.  Nota: En caso de eliminar todas las líneas debe dejarse al menos una línea con un espacio en blanco para poder cerrar la configuración de la directiva. En caso contrario se mostrará un error. 
122.	Sobre la unidad organizativa creada para habilitar el uso de dispositivos USB “Equipos Windows 10 – USB habilitado” seleccione la GPO vinculada “CCN-STIC-599A19 Habilitar dispositivos” con el botón derecho y desmarque la opción “Vínculo habilitado” o seleccione “Eliminar”.  Nota: Este paso no será necesario si desea seguir permitiendo algún dispositivo USB en los equipos. En ese caso solo deberá eliminar los ID que pertenezcan a los USB que desea bloquear en los equipos.

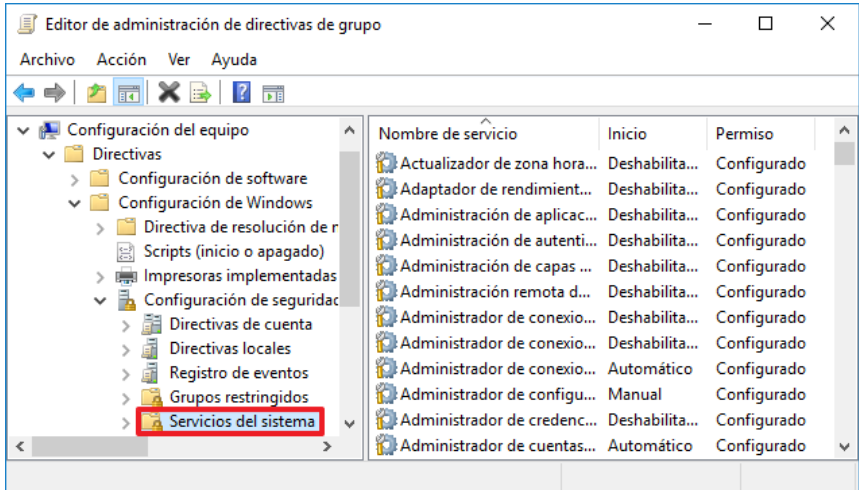
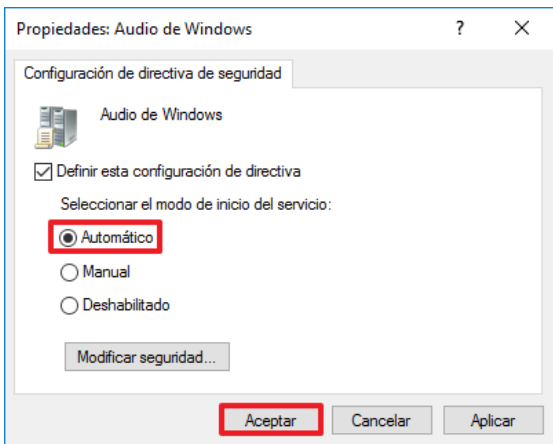
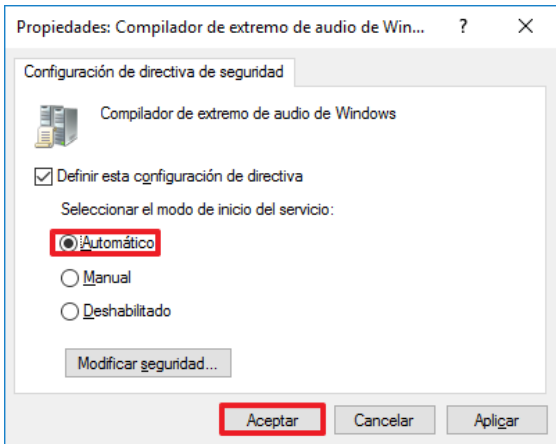
Paso	Descripción
123.	Por último, deberá forzar la aplicación de políticas en todos los equipos. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en inicio y seleccione “Windows PowerShell (Administrador)”. 
124.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador de dominio y pulse “Sí” para continuar. 
125.	Ejecute el comando “gpupdate /force” y espere a que finalice. 

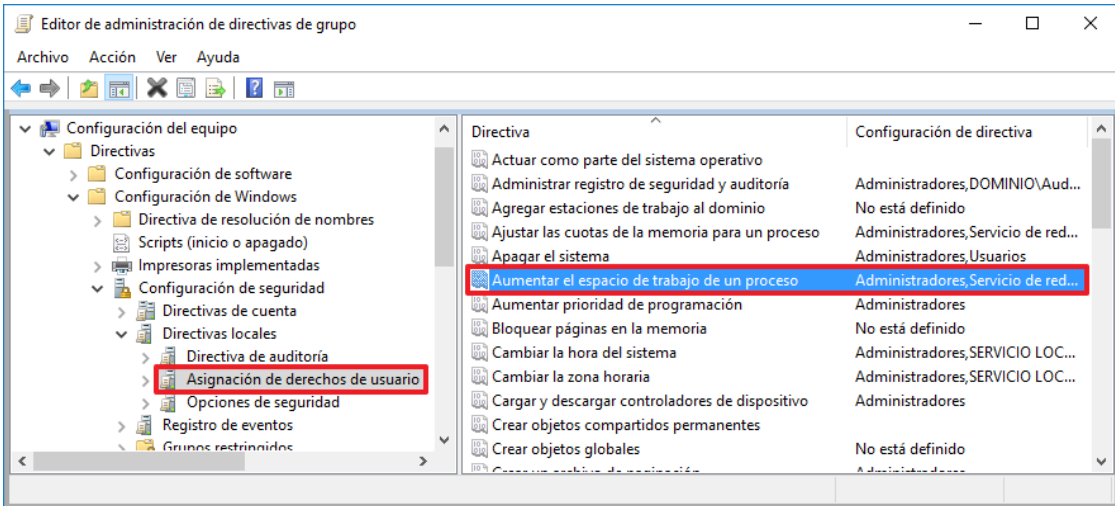
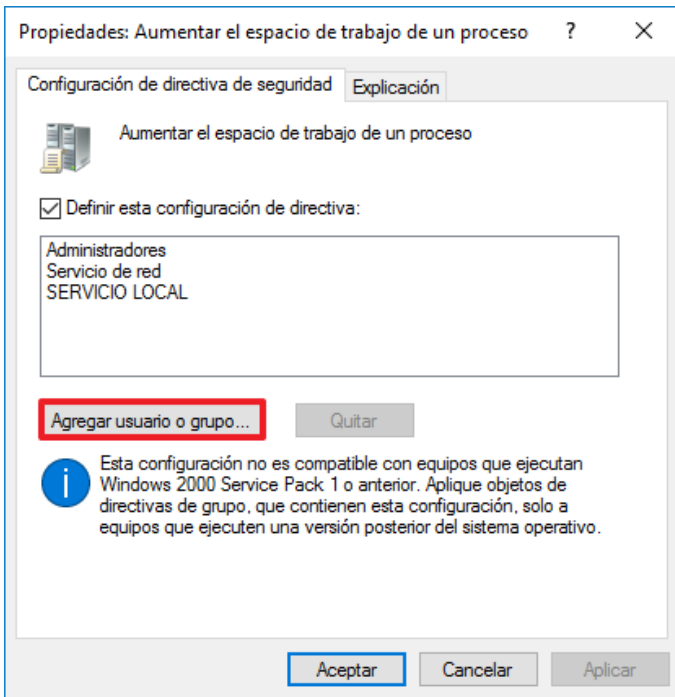
ANEXO D.2.3. SONIDO TRAS APLICACIÓN DE GUÍA CCN-STIC-599A19

A continuación, se indican los pasos a realizar para modificar la plantilla de seguridad a aplicar sobre equipos Windows 10, miembros del dominio, con el objetivo de habilitar el sonido del sistema. Para habilitar el sonido en los equipos, se deberá actualizar el objeto de directiva de grupo “CCN-STIC-599A19 Windows 10” siguiendo la configuración que se indica a continuación.

Nota: En caso de que solamente fuera necesario activar el sonido en algunos de los equipos, en lugar de modificar la directiva “CCN-STIC-599A19 Windows 10”, sería posible establecer una nueva directiva denominada, por ejemplo, “CCN-STIC-599A19 Windows 10 con sonido”. Crear así mismo una unidad organizativa específica llamada, por ejemplo, Clientes Windows 10 con sonido y, de una forma similar a los pasos efectuados en el anexo anterior, modificar la directiva vacía con los pasos siguientes y, vincular y mover equipos a la unidad organizativa que ha creado con esta finalidad.

Paso	Descripción
1.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar el sonido.
2.	Utilizando la herramienta "Administrador del servidor", Seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 
3.	En la consola “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo"
4.	Localice la directiva “CCN-STIC-599A19 Windows 10”, selecciónela con el botón derecho del ratón y pulse sobre “Editar...”. 

Paso	Descripción
5.	Edite los servicios de sistema mediante la siguiente ruta: "Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema" 
6.	Haga doble clic sobre el servicio "Audio de Windows", seleccione el modo de inicio "Automático" y pulse "Aceptar". 
7.	Repita el mismo proceso con el servicio "Compilador de extremo de audio de Windows". 

Paso	Descripción
8.	De nuevo en el “Editor de administración de directivas de grupo”, acceda al apartado “Asignación de derechos de usuario” mediante la siguiente ruta: "Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuarios"
9.	Haga doble clic sobre la directiva “Aumentar el espacio de trabajo de un proceso”. 
10.	En la ventana de “Propiedades: Aumentar el espacio de trabajo de un proceso” compruebe que al menos uno de estos dos elementos aparece en la lista y, de no ser así, añádalo mediante el botón “Agregar usuario o grupo...”: – Usuarios – SERVICIO LOCAL 

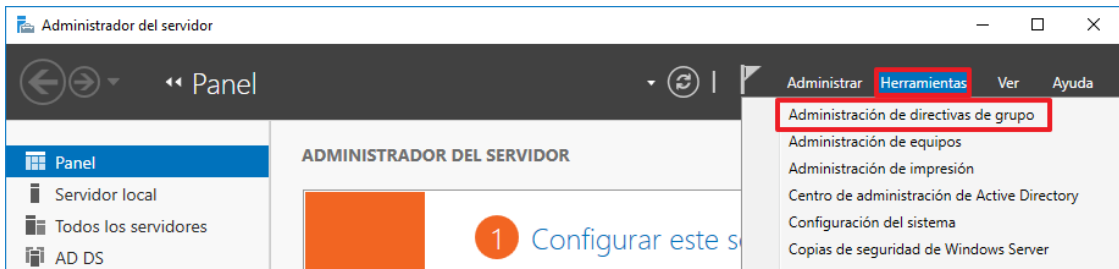
ANEXO D.2.4. CONFIGURACIÓN PARA USO DE NESSUS

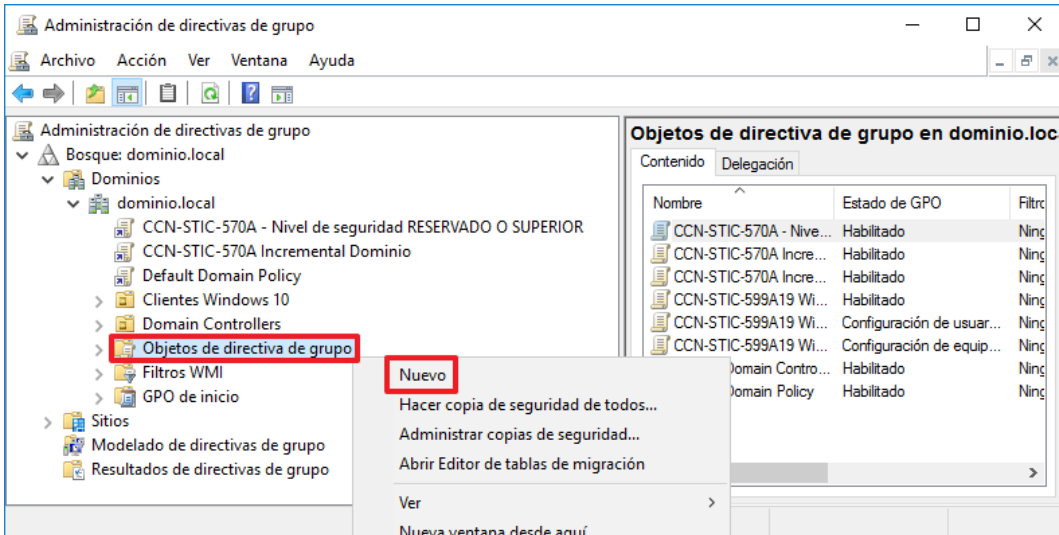
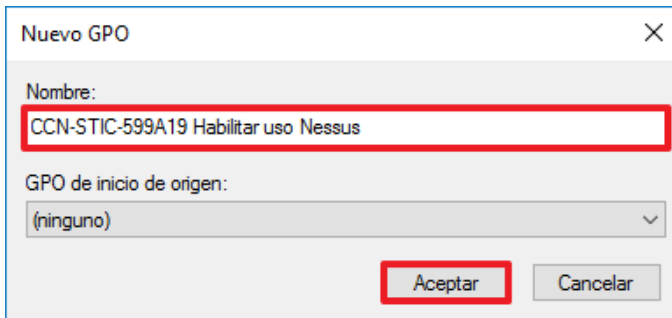
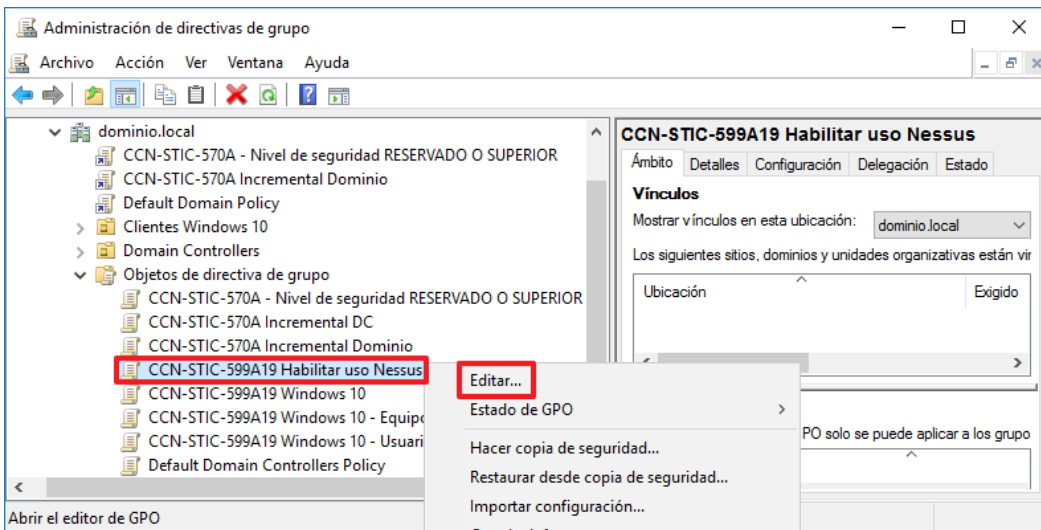
Este anexo ha sido diseñado con el objetivo de establecer la configuración necesaria para que se permita realizar un escáner de vulnerabilidades sobre los equipos Windows 10 haciendo uso de la aplicación Nessus (escáner de vulnerabilidades), localizada en una ubicación remota en la red.

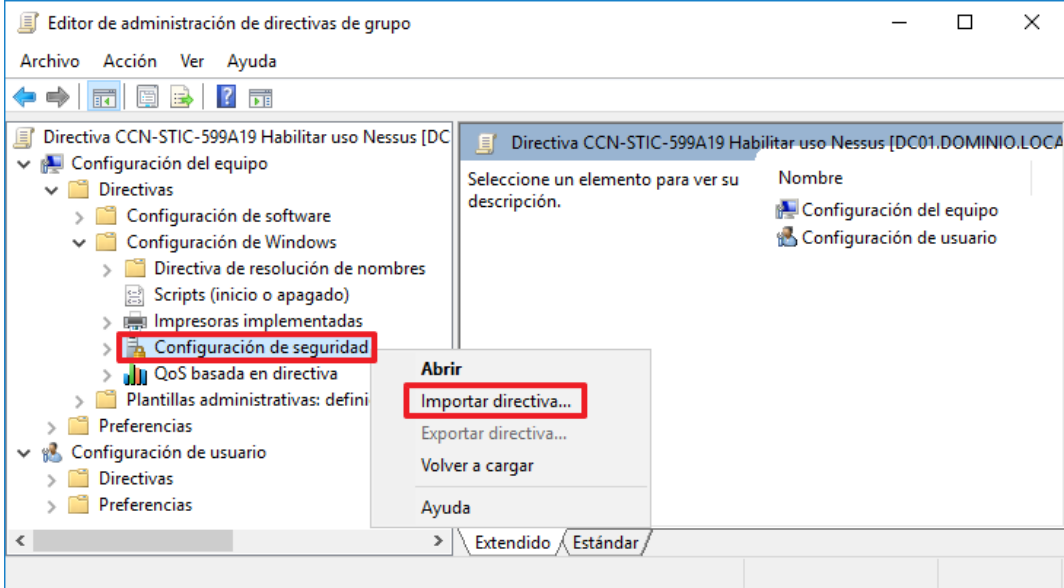
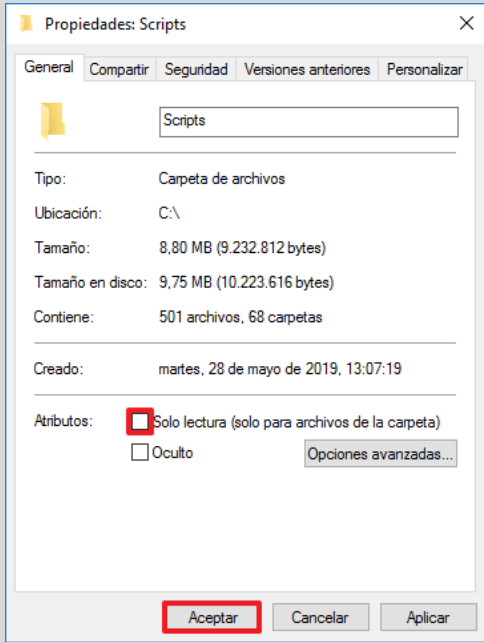
Es necesario resaltar que para permitir el uso de la herramienta Nessus, es necesario aplicar una configuración específica que habilita la comunicación NTLM, el uso compartido de archivos e impresoras en los adaptadores de red e iniciar el servicio “Servidor” durante la ejecución del escáner de vulnerabilidades.

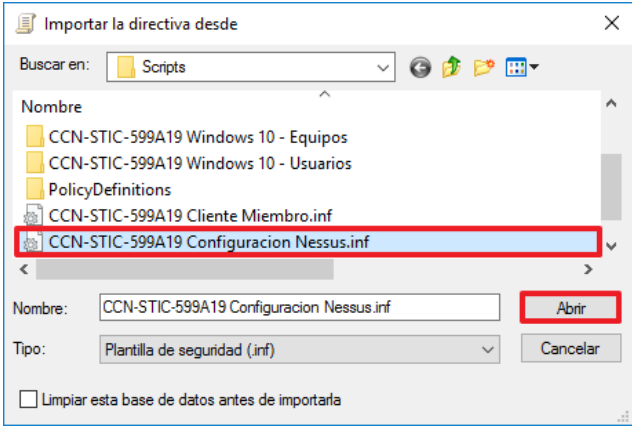
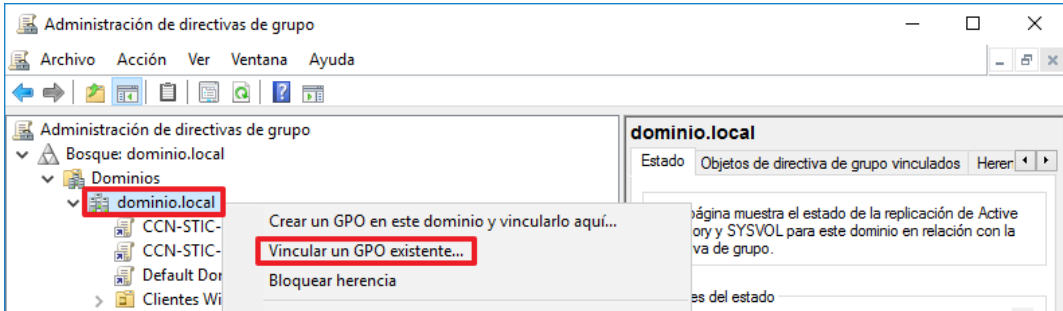
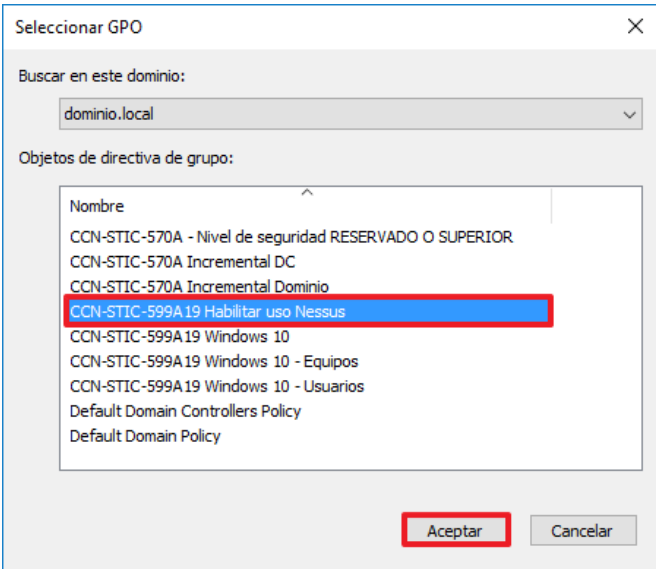
Nota: Dependiendo de la configuración de su equipo, es posible que la configuración que se lleva a cabo en los siguientes pasos ya se encuentre habilitada.

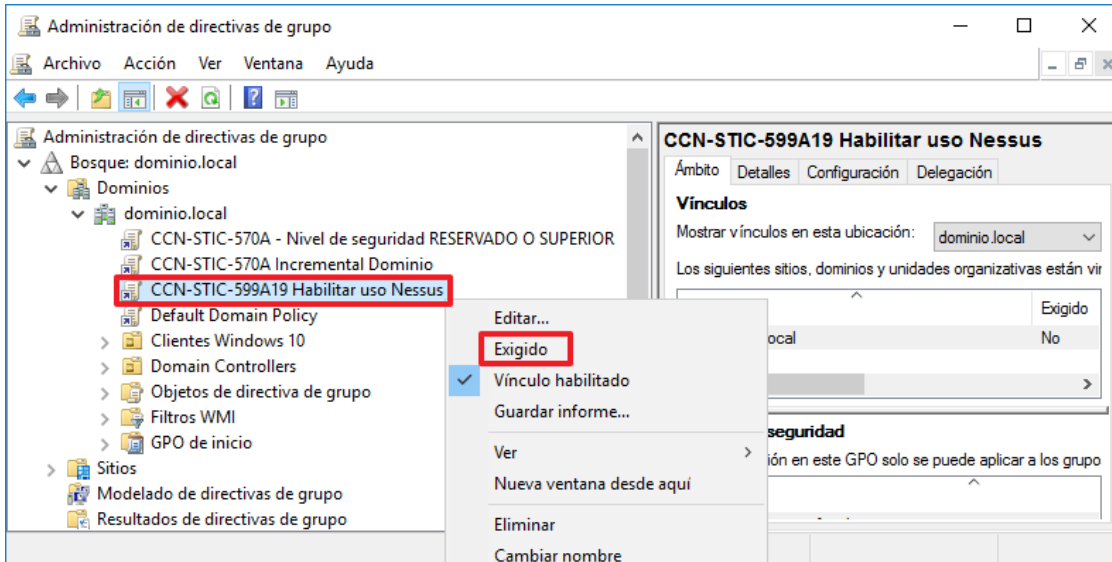
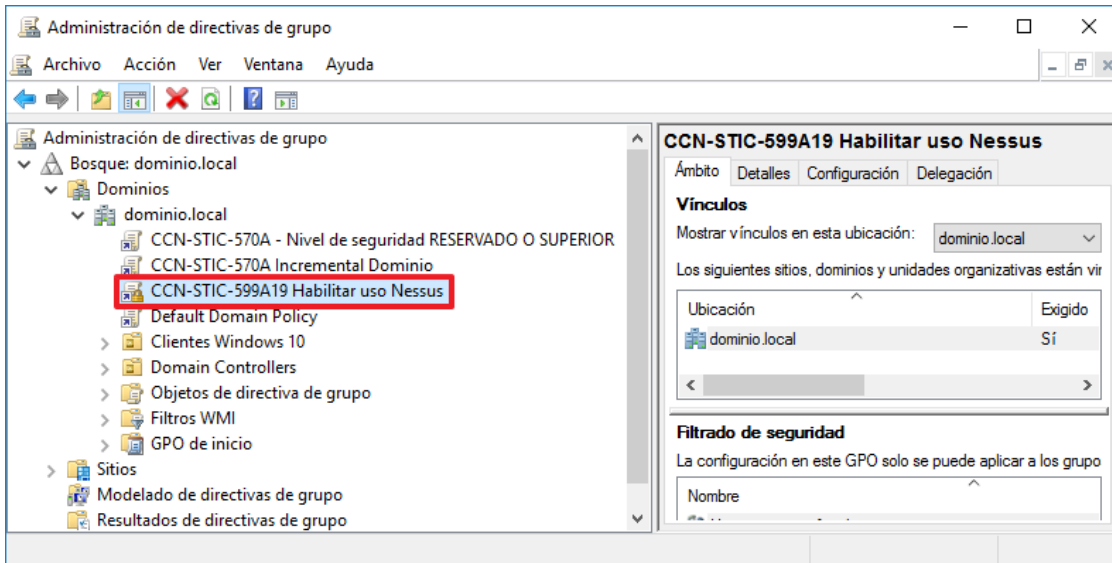
1. HABILITAR AUTENTICACIÓN PARA USO DE NESSUS

Paso	Descripción
1.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar la configuración para el uso de Nessus.
2.	Cree el directorio C:\Scripts.
3.	Copie los ficheros y directorios asociados a esta guía en el directorio “C:\Scripts” y asegúrese de que existen al menos los siguientes ficheros: – CCN-STIC-599A19 – Configuración Nessus.inf Nota: Los recursos asociados a esta guía se encuentran en el directorio “Scripts-599A19”.
4.	Utilizando la herramienta “Administrador del servidor”, seleccione en el menú superior “Herramientas” y pulse sobre “Administración de directivas de grupo”. 
5.	En la consola “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo"

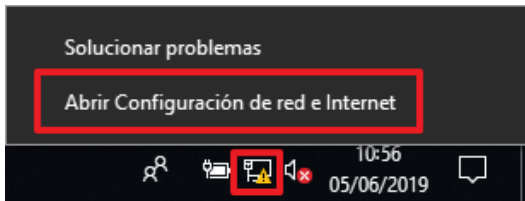
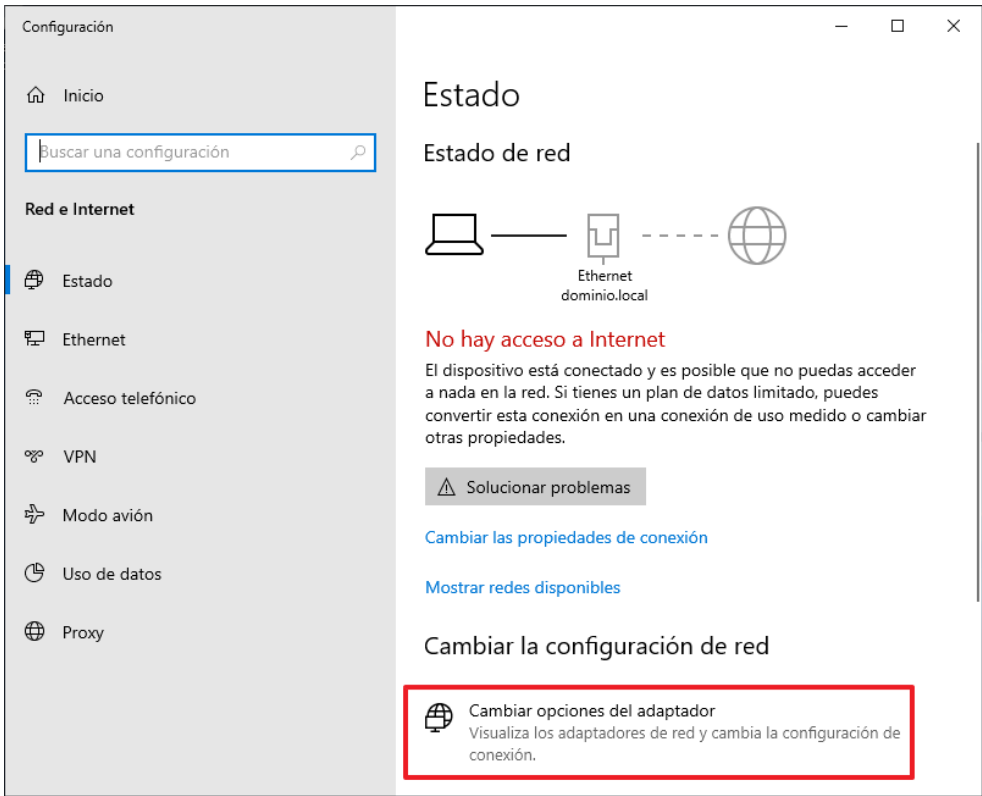
Paso	Descripción
6.	Pulse con el botón derecho sobre “Objetos de directiva de grupo” y seleccione la opción del menú contextual “Nuevo”. 
7.	Establezca el nombre para la GPO “CCN-STIC-599A19 Habilitar uso Nessus” y pulse “Aceptar” para continuar. 
8.	Haga clic derecho sobre la GPO recién creada y pulse sobre la opción del menú contextual “Editar...”. 

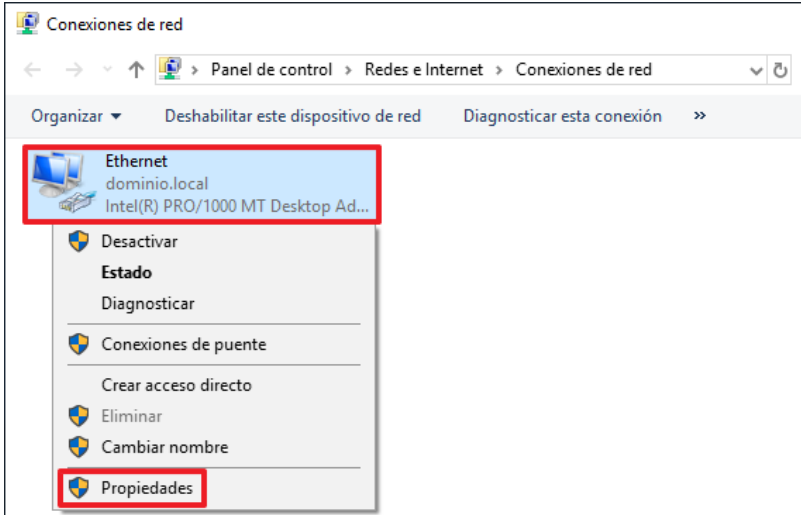
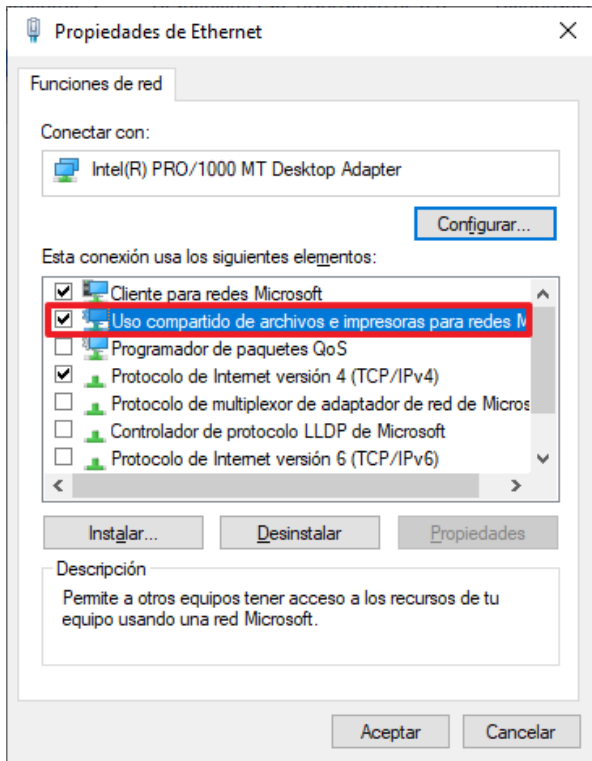
Paso	Descripción
9.	Despliegue la GPO hasta acceder al siguiente nodo: “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad” Haga clic derecho sobre “Configuración de seguridad” y seleccione la opción del menú contextual “Importar directiva...”.  Nota: Asegúrese de que los archivos alojados en “C:\Scripts” no se encuentran en modo solo lectura a la hora de realizar la importación de la copia de seguridad. Si realiza este proceso con los archivos en modo lectura, no se podrán modificar las directivas en un futuro. 

Paso	Descripción
10.	Identifique el fichero “CCN-STIC-599A19 Configuración Nessus.inf” en el directorio “C:\Scripts” y pulse sobre el botón “Abrir”. 
11.	Con esto habrá quedado configurada la GPO para el uso de Nessus. Cierre el “Editor de administración de directivas de grupo”.
12.	A continuación sobre la raíz del dominio haga clic derecho y seleccione la opción del menú contextual “Vincular un GPO existente...”. 
13.	Seleccione la GPO denominada “CCN-STIC-599A19 Habilitar uso Nessus” y pulse “Aceptar”. 

Paso	Descripción
14.	Por último haga clic derecho sobre la GPO recién vinculada y seleccione la opción del menú contextual “Exigido”.  Nota: Deberá tener en consideración la posibilidad de que en su organización existan más GPOs configuradas con el valor “Exigido”. Ante esta casuística, la aplicación de la GPO varía teniendo preferencia la GPO de dominio sobre la de las Unidad Organizativas (UO). En caso de necesitar solo auditar ciertos equipos deberá crear un grupo al que se añadirán todos los equipos a auditar incluyendo de manera obligatoria a los servidores controladores de dominio. Tras esto deberá añadir dicho grupo en el filtrado de seguridad de la GPO de manera que únicamente a los equipos miembros del grupo les sea de aplicación dicha GPO.
15.	Asegúrese que la GPO esta en estado “exigida” para que se aplique siempre en primer lugar. 

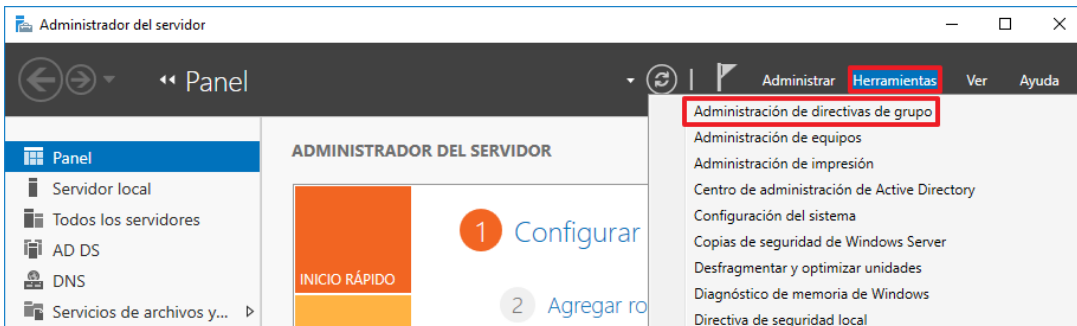
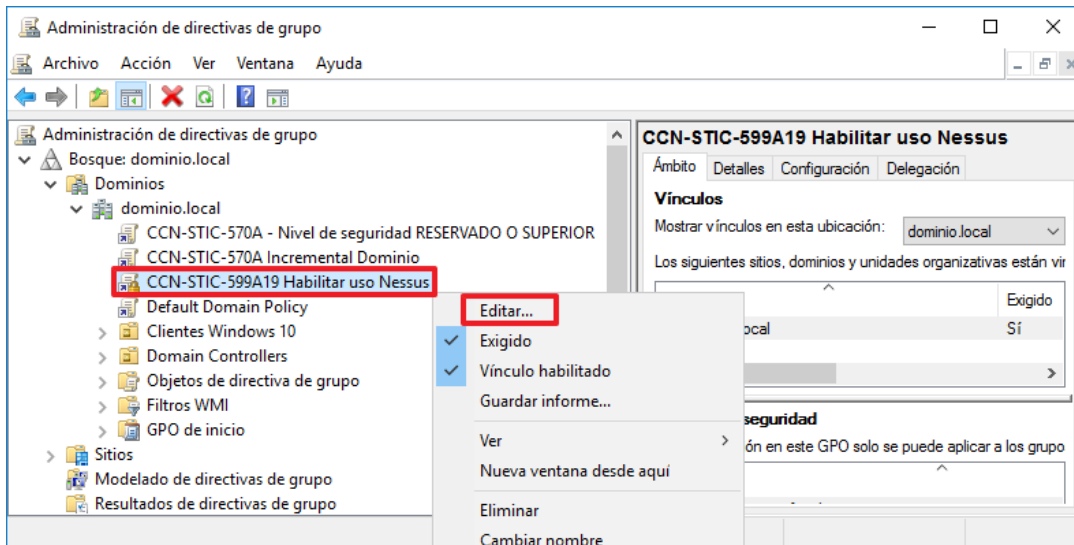
En este momento queda configurado el dominio para permitir el uso de Nessus. Los pasos realizados a continuación se deben hacer en cada equipo que se desea analizar con la herramienta Nessus.

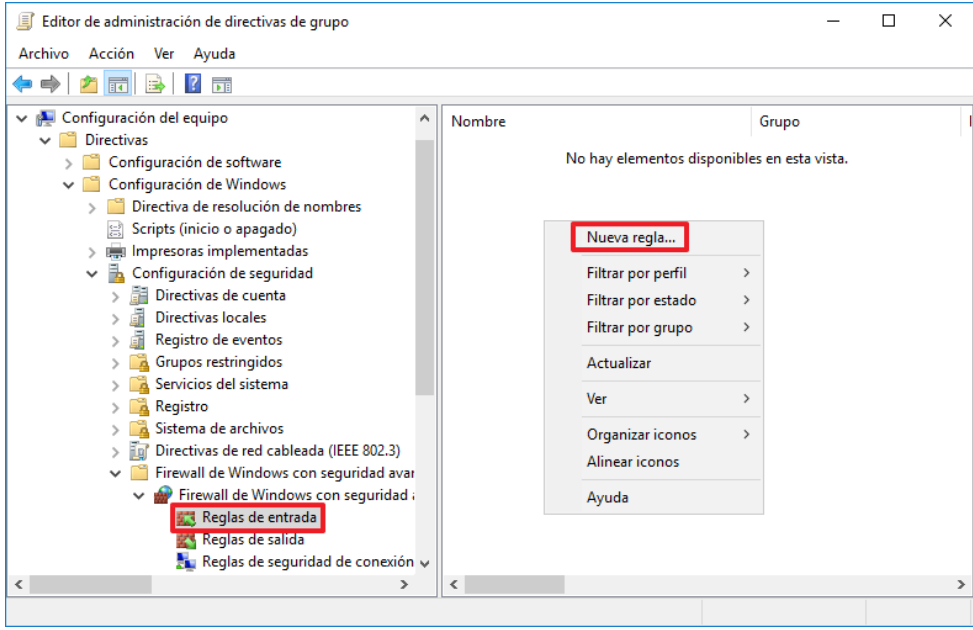
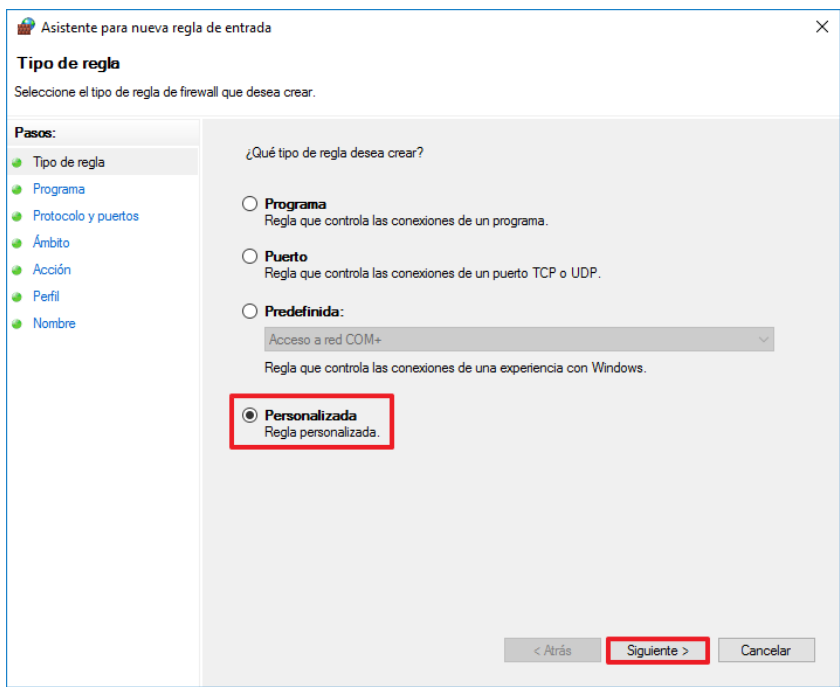
Paso	Descripción
16.	Inicie sesión en el equipo cliente sobre el que se desea permitir el análisis con la herramienta Nessus.
17.	Debe iniciar sesión con un usuario que posea permisos de administración del dominio.
18.	Seleccione el icono correspondiente a la red en la parte inferior derecha con el botón derecho del ratón y seleccione la opción “Abrir Configuración de red e Internet”. 
19.	En la ventana de configuración, seleccione la opción “Cambiar opciones del adaptador”. 

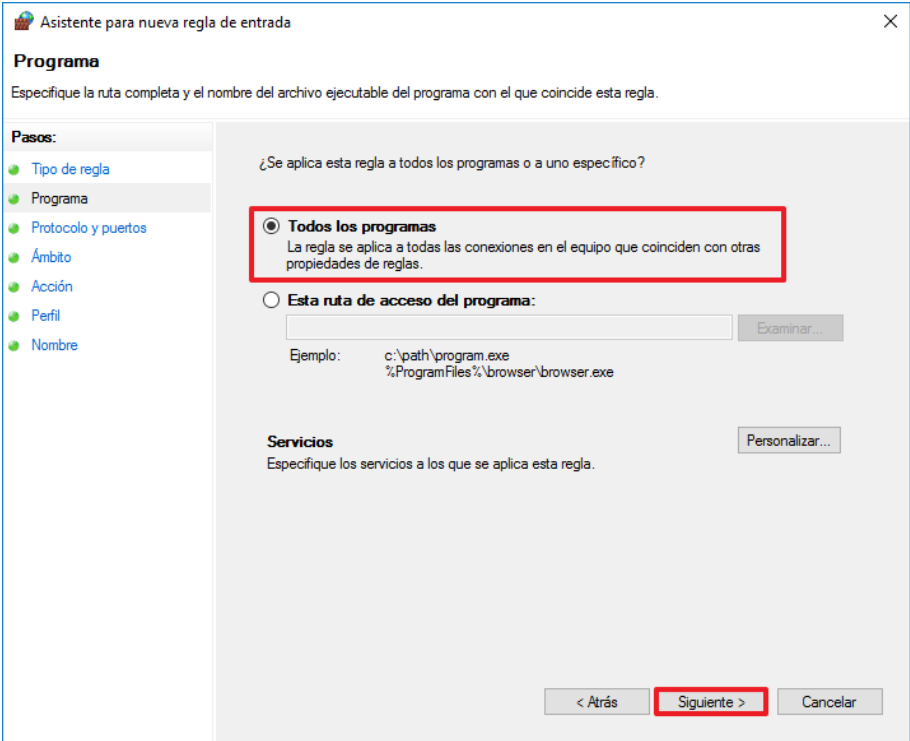
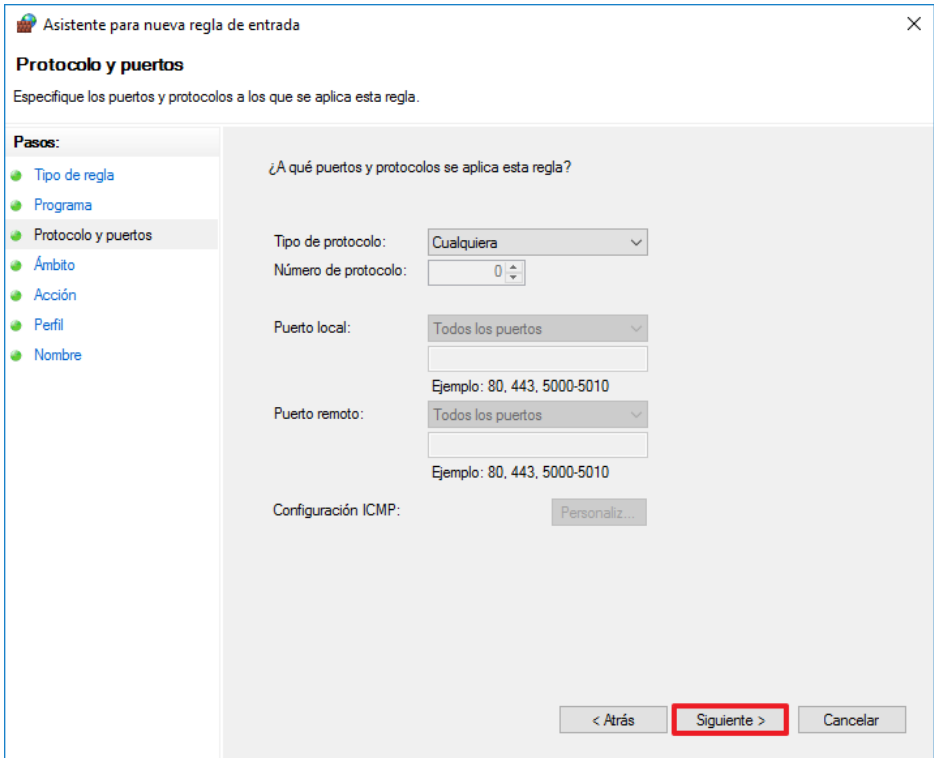
Paso	Descripción
20.	Seleccione con el botón derecho el adaptador de red correspondiente y seleccione la opción del menú contextual “Propiedades”. 
21.	El Control de cuentas de usuario le pedirá la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración del dominio.
22.	Asegurése que esta marcada la opción “Uso compartido de archivos e impresoras para redes Microsoft”. En caso contrario márquela y cierre todas las ventanas. 
23.	Elimine el directorio “C:\Scripts” del equipo controlador de dominio.
24.	Para finalizar reinicie el equipo o ejecute “gpupdate /force” en la línea de comandos para que se aplique la GPO configurada anteriormente.

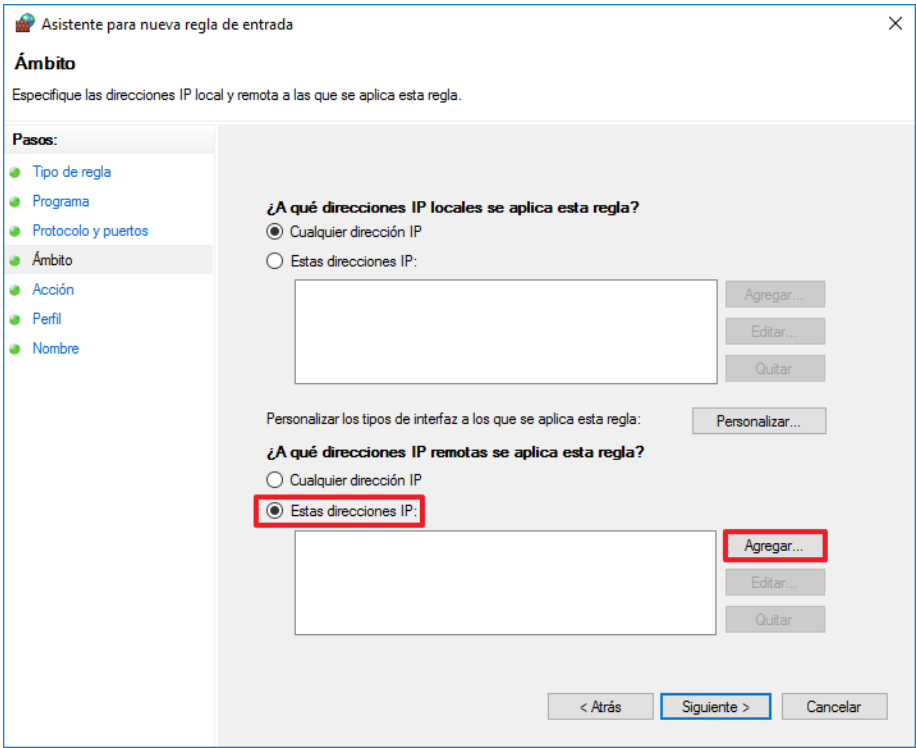
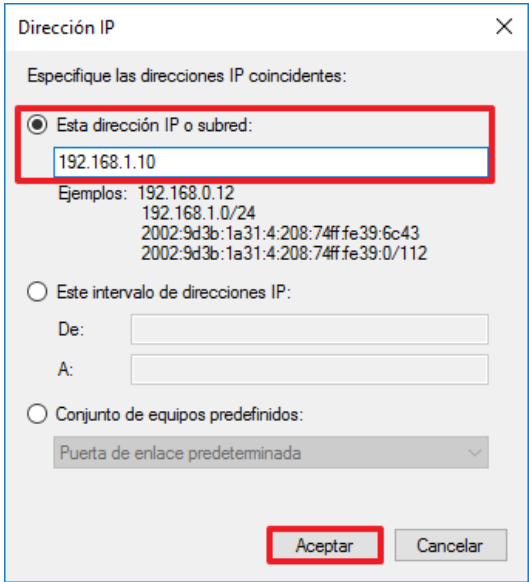
2. PERMITIR COMUNICACIÓN EN EL FIREWALL

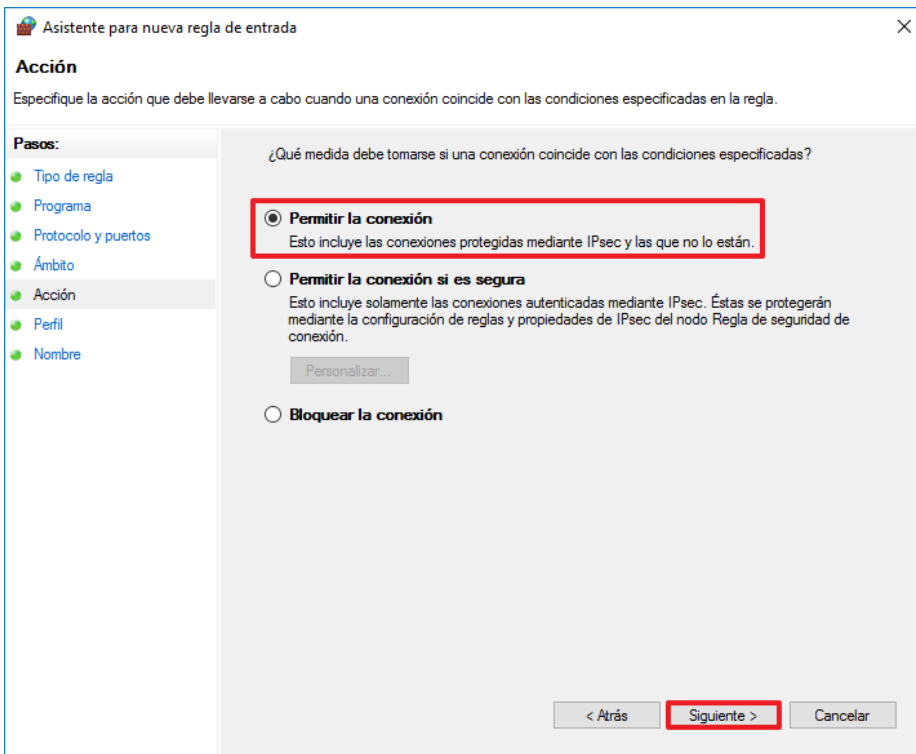
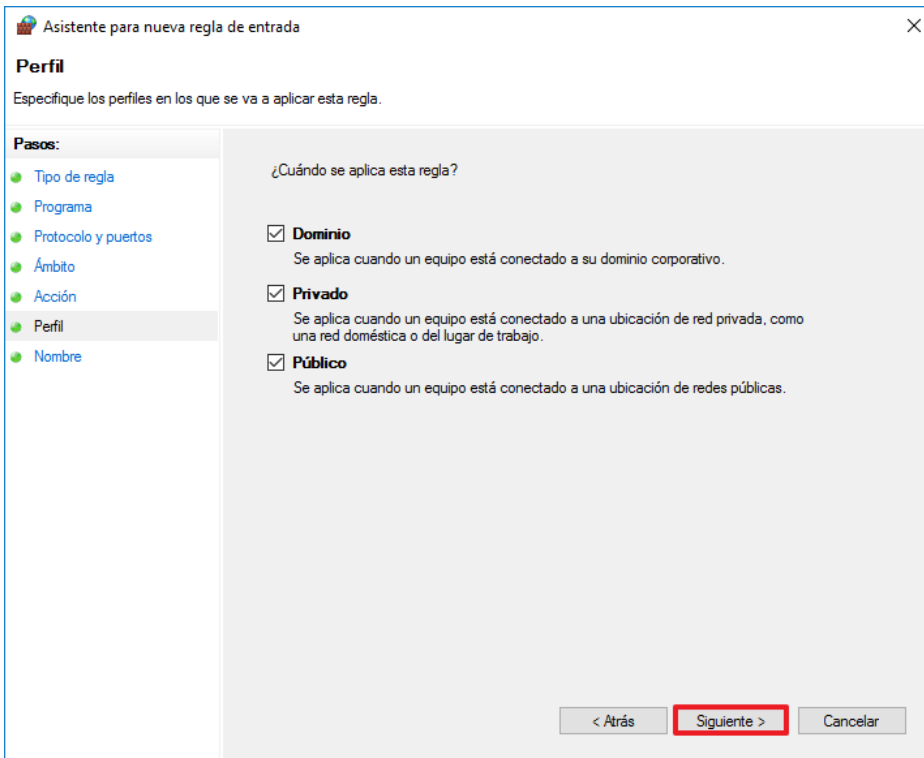
El siguiente procedimiento establece los pasos necesarios para permitir una comunicación total a través del firewall entre el equipo donde se encuentra instalada la aplicación Nessus, y el equipo que se analiza.

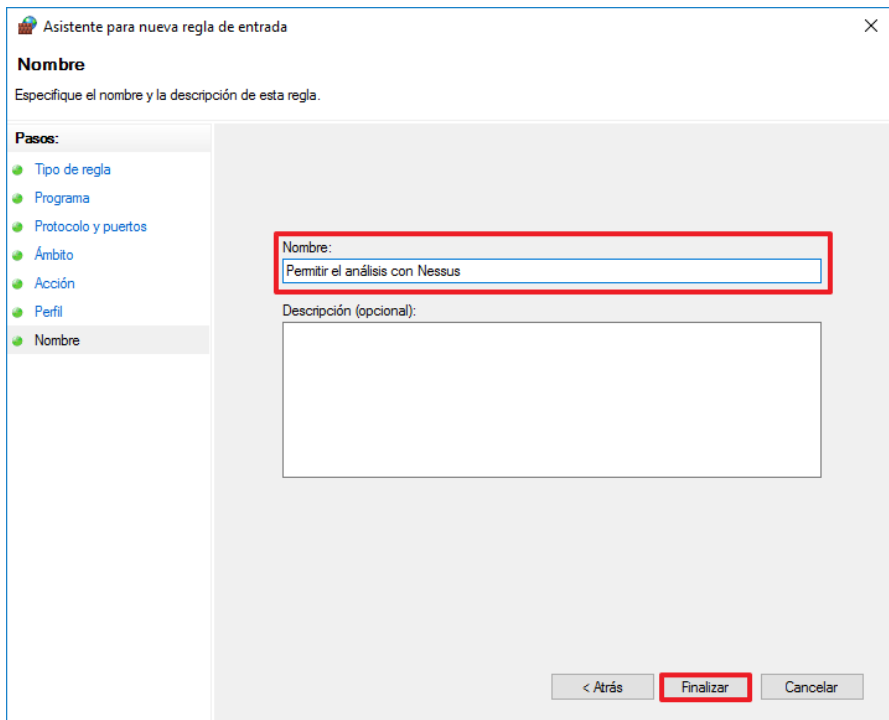
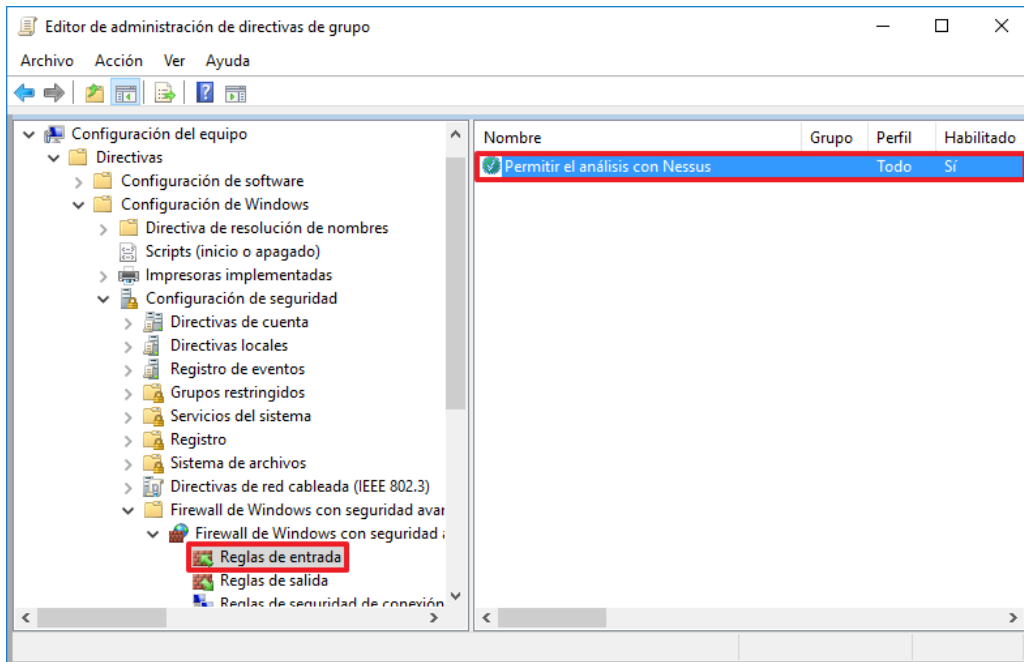
Paso	Descripción
25.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar la configuración para el uso de Nessus.
26.	Utilizando la herramienta "Administrador del servidor", Seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 
27.	En la consola "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta: "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> → Objetos de directiva de grupo"
28.	Sobre la GPO configurada en pasos anteriores, "CCN-STIC-599A19 Habilitar uso Nessus", pulse con el botón derecho y seleccione la opción del menú contextual "Editar". 

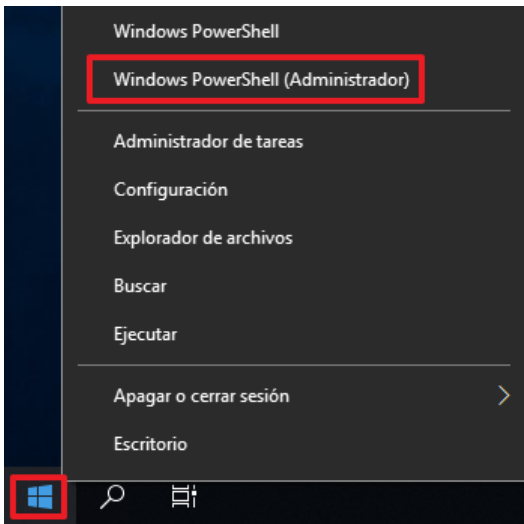
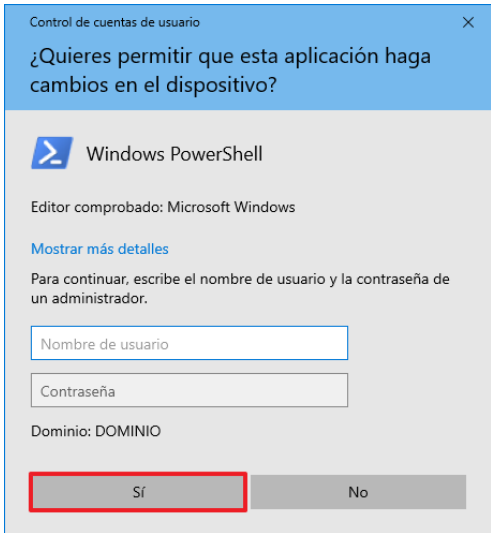
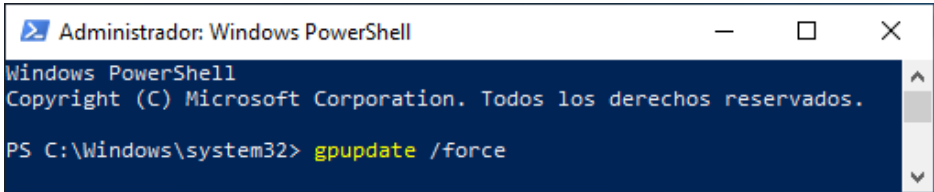
Paso	Descripción
29.	Despliegue la GPO hasta acceder al siguiente nodo: “Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Firewall de Windows con Seguridad Avanzada → Firewall de Windows con Seguridad Avanzada → Reglas de entrada” Haga clic derecho sobre un espacio en blanco y seleccione la opción del menú contextual “Nueva regla...”. 
30.	En el apartado “Tipo de regla” seleccione tipo de regla “Personalizada” y pulse “Siguiente >”. 

Paso	Descripción
31.	En el apartado “Programa” seleccione la opción “Todos los programas” y pulse “Siguiente >”. 
32.	En el apartado “Protocolo y puertos” seleccione la opción “Cualquiera” y pulse “Siguiente >” para continuar. 

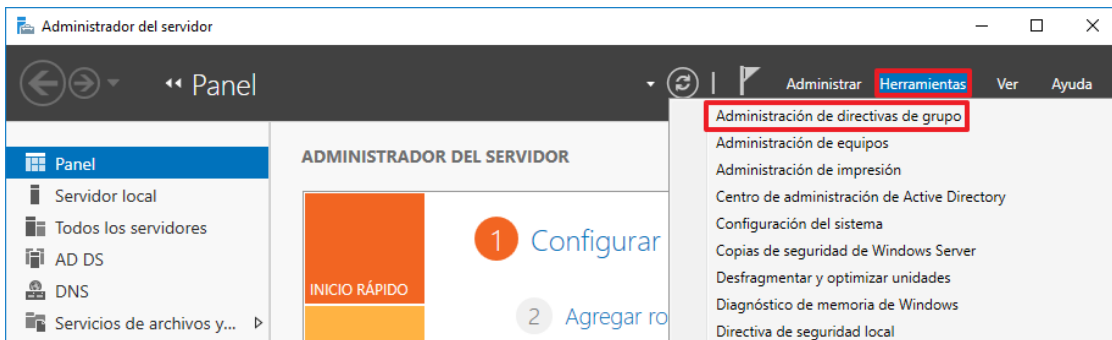
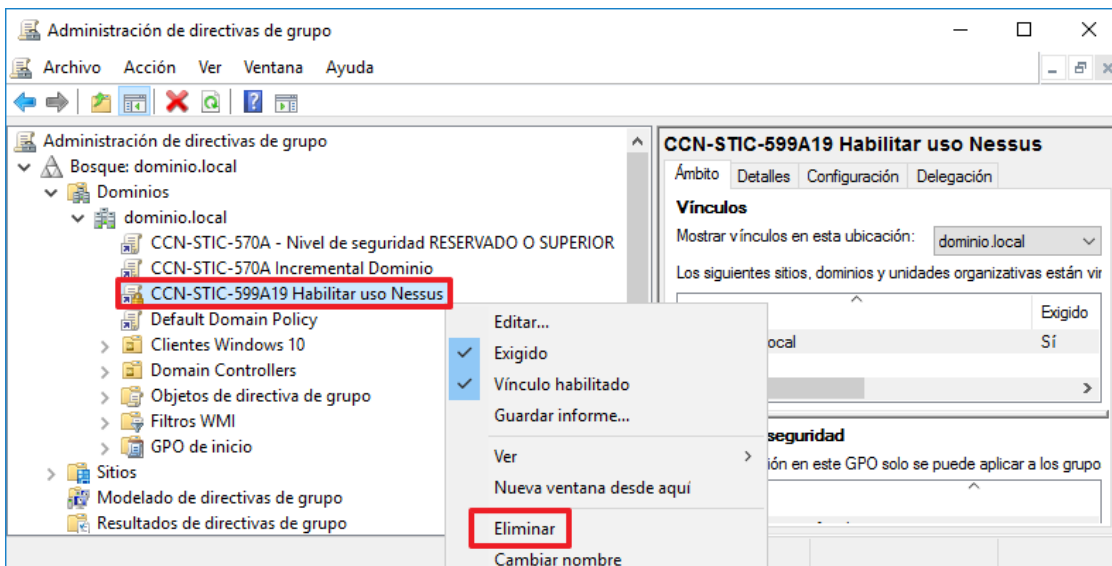
Paso	Descripción
33.	En la ventana “Ámbito”, seleccione en el apartado de IP remotas la opción “Estas direcciones IP:” y a continuación pulse sobre “Agregar...”. 
34.	Seleccione la opción “Esta dirección IP o subred:” y establezca la dirección IP desde donde se va a ejecutar la herramienta Nessus. Pulse “Aceptar” para continuar.  Nota: En este ejemplo, la herramienta Nessus se ejecuta desde la dirección IP “192.168.1.10”.
35.	Pulse “Siguiente >” una vez haya configurado las IP necesarias.

Paso	Descripción
36.	En el apartado “Acción” marque la opción “Permitir la conexión” y pulse “Siguiente >”. 
37.	Pulse “Siguiente >” en el apartado “Perfil”.  Nota: Dependiendo de la configuración de red podrá adaptar este paso y seleccionar el tipo de perfil. Aún así no será necesario realizar ninguna configuración.

Paso	Descripción								
38.	Por último, establezca un nombre para la regla y pulse sobre el botón “Finalizar”. 								
39.	Verifique que ha sido creada la regla de entrada.  <table><tr><th>Nombre</th><th>Grupo</th><th>Perfil</th><th>Habilitado</th></tr><tr><td>Permitir el análisis con Nessus</td><td></td><td>Todo</td><td>Sí</td></tr></table>	Nombre	Grupo	Perfil	Habilitado	Permitir el análisis con Nessus		Todo	Sí
Nombre	Grupo	Perfil	Habilitado						
Permitir el análisis con Nessus		Todo	Sí						

Paso	Descripción
40.	Por último deberá forzar la aplicación de políticas en todos los equipos a analizar al igual que en los equipos controladores de dominio. Para ello ejecute una consola de Powershell con permisos de administrador de dominio pulsando con botón derecho en “Inicio → Windows PowerShell (Administrador)”. 
41.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca la credenciales de un usuario con permisos de administrador de dominio y pulse “Si” para continuar. 
42.	Ejecute el comando “gpupdate /force” y espere a que finalice. 

3. ELIMINACIÓN DE LA CONFIGURACIÓN PARA EL USO DE NESSUS

Paso	Descripción
43.	Inicie sesión en un controlador de dominio del dominio al que pertenecen los equipos Windows 10 sobre los que desea habilitar la configuración para el uso de Nessus.
44.	Utilizando la herramienta "Administrador del servidor", seleccione en el menú superior "Herramientas" y pulse sobre "Administración de directivas de grupo". 
45.	En la consola "Administración de directivas de grupo", expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio> Elimine la GPO para permitir el análisis con Nessus haciendo clic derecho sobre ella y seleccionando la opción del menú contextual "Eliminar". 

ANEXO D.2.5. 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”.

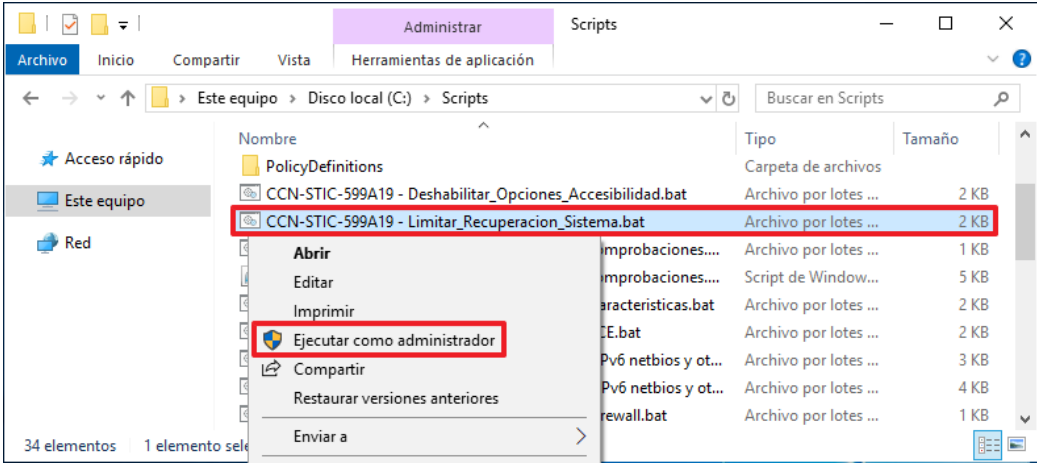
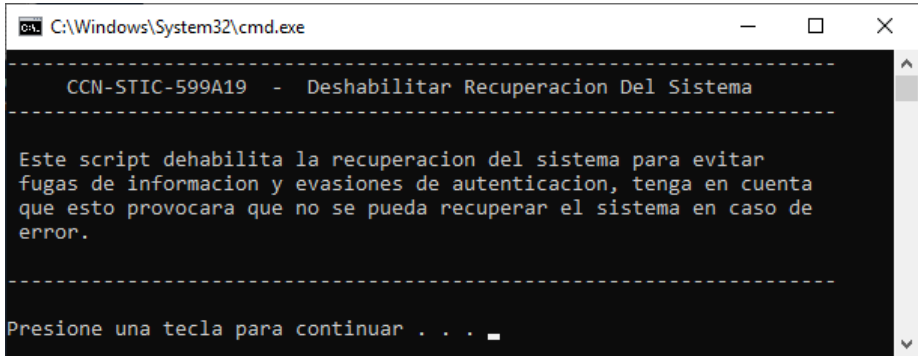
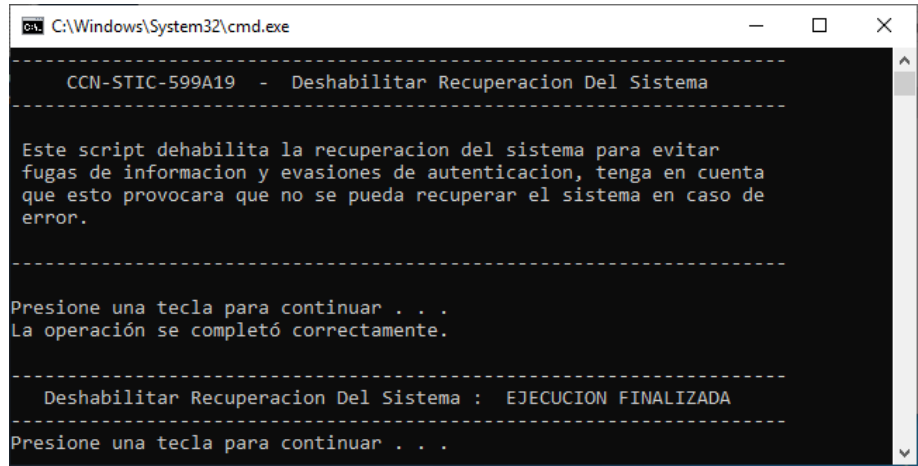
Las medidas a aplicar podrán ser:

- 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.

1. DESHABILITAR LA FUNCIONALIDAD DE RESTAURACIÓN

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

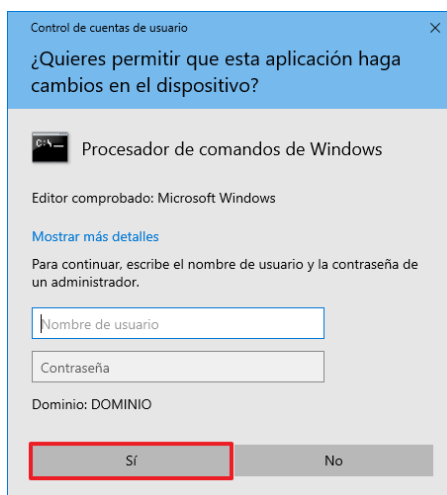
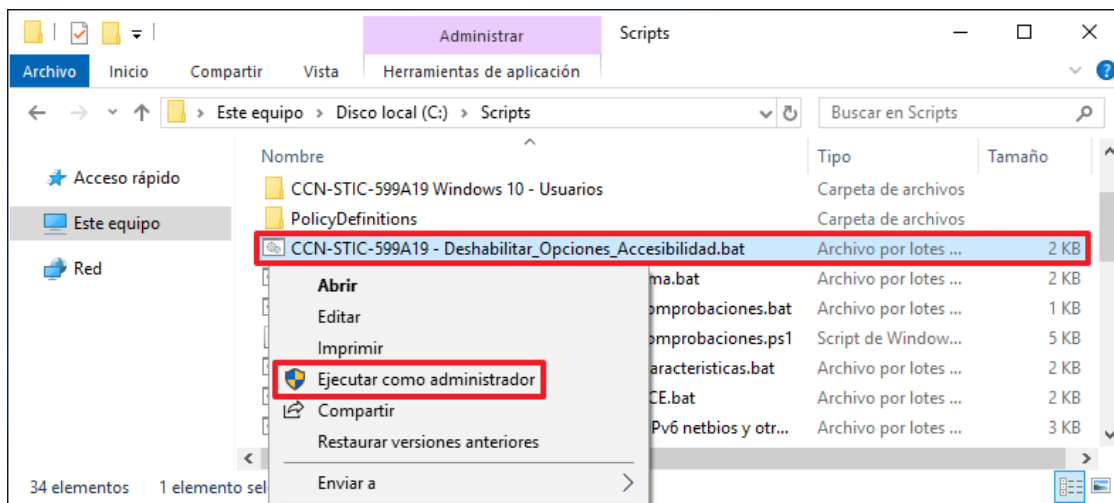
Paso	Descripción
1.	Inicie sesión en el equipo cliente Windows 10 con una cuenta con permisos de administrador del dominio.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.

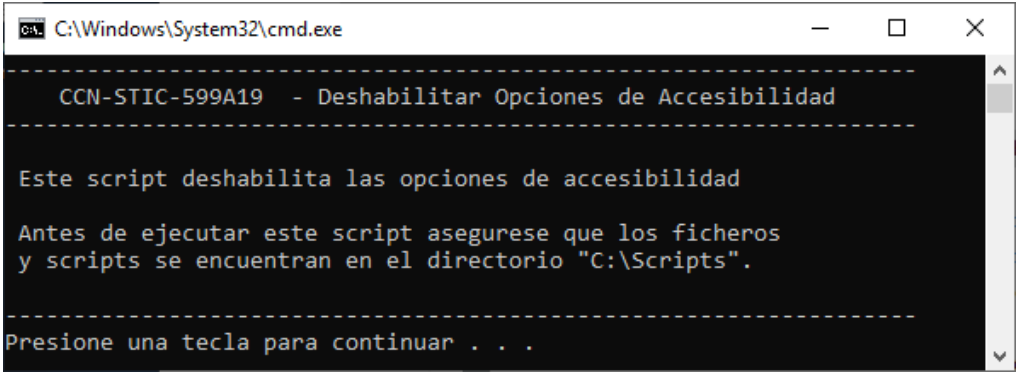
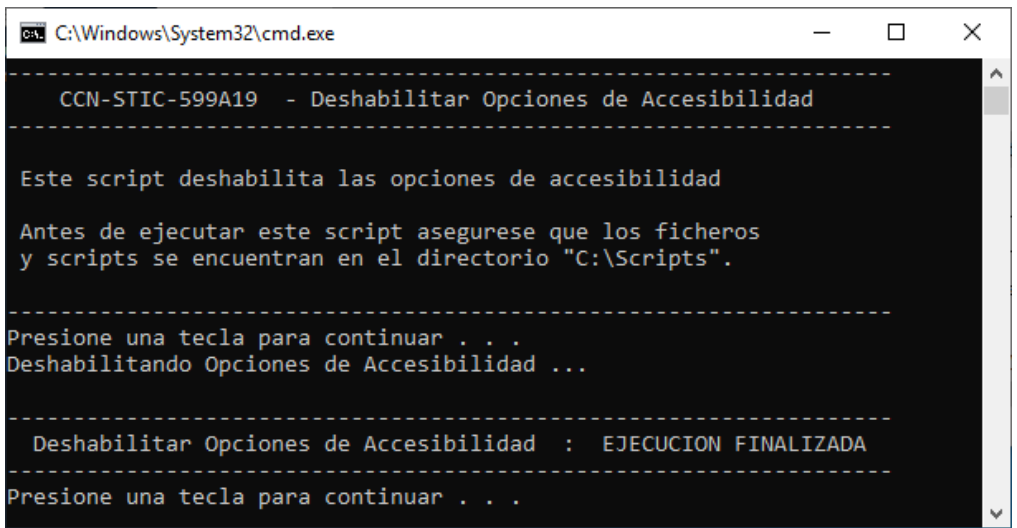
Paso	Descripción
3.	Localice el archivo “CCN-STIC-599A19 – Limitar_Recuperacion_Sistema.bat” haga clic derecho sobre este y seleccione la opción “Ejecutar como administrador”. 
4.	El control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario perteneciente 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.

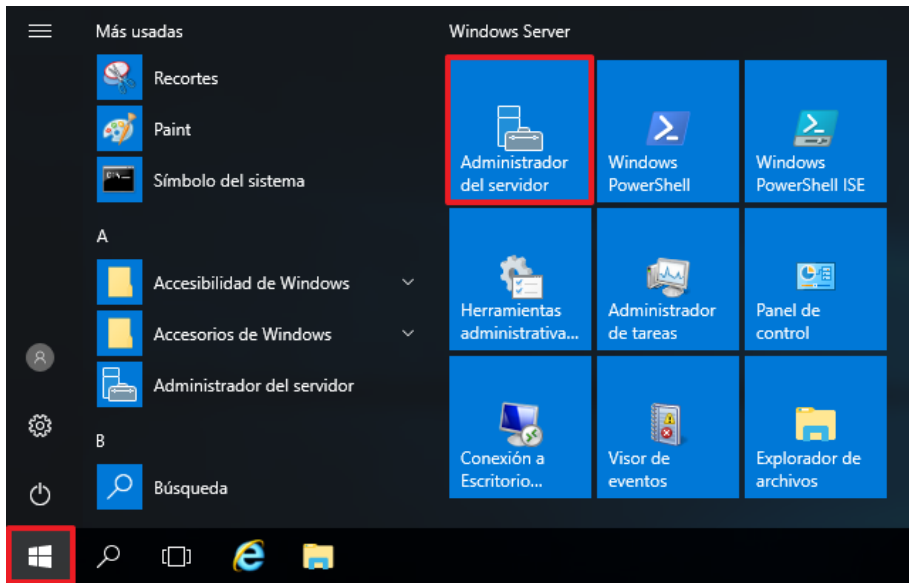
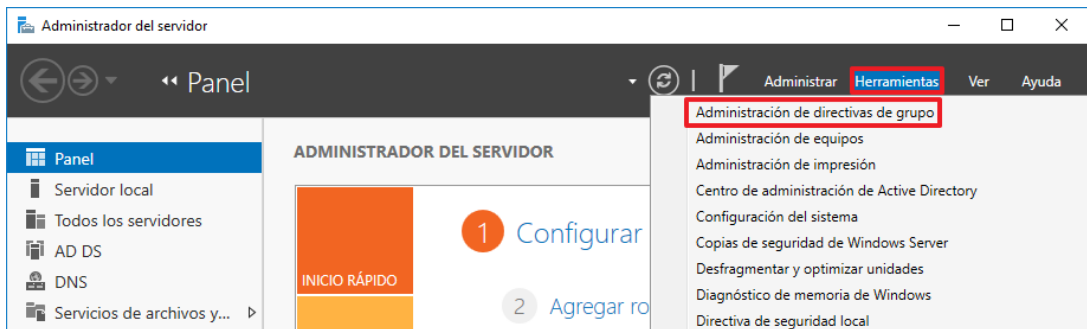
Paso	Descripción
1.	Inicie sesión en el equipo cliente Windows 10 con una cuenta con permisos de administrador del dominio.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts” y sitúese en dicho directorio.
3.	Localice el archivo “CCN-STIC-599A19 – Deshabilitar_Opciones_Accesibilidad.bat” 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”.

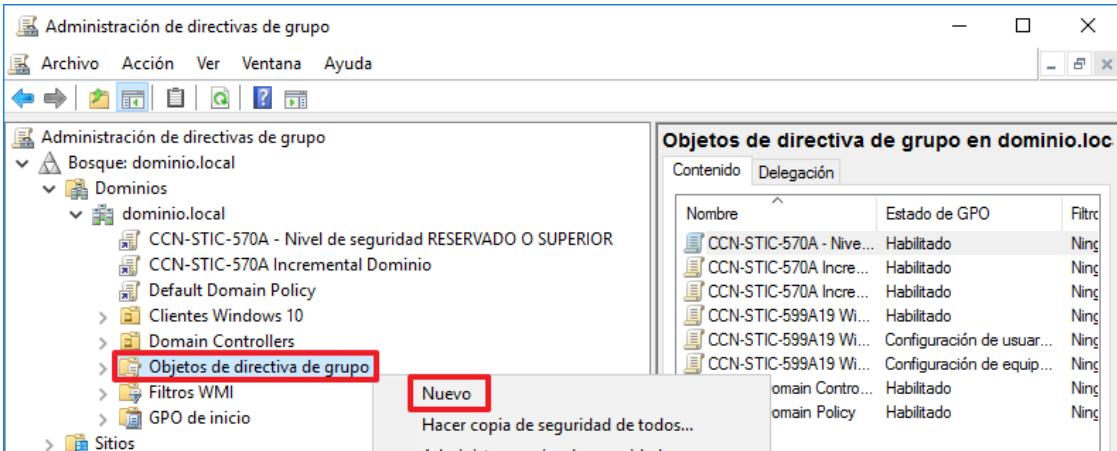
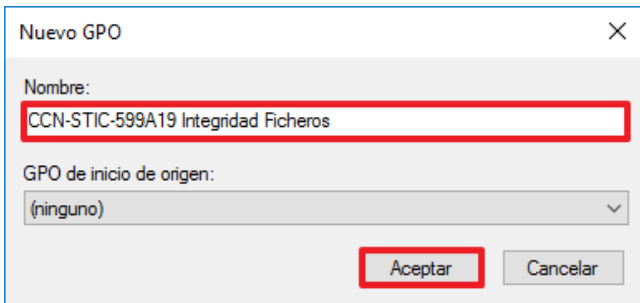
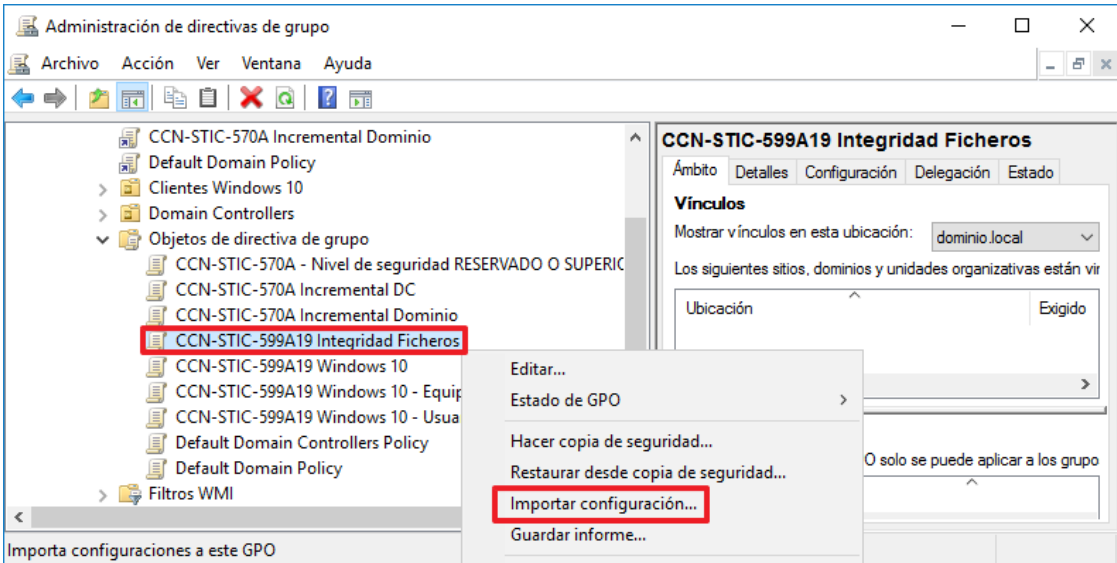


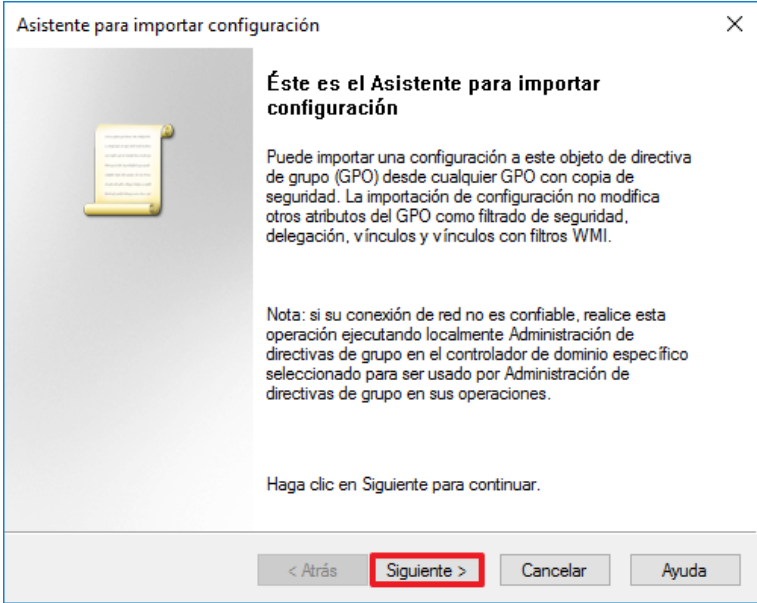
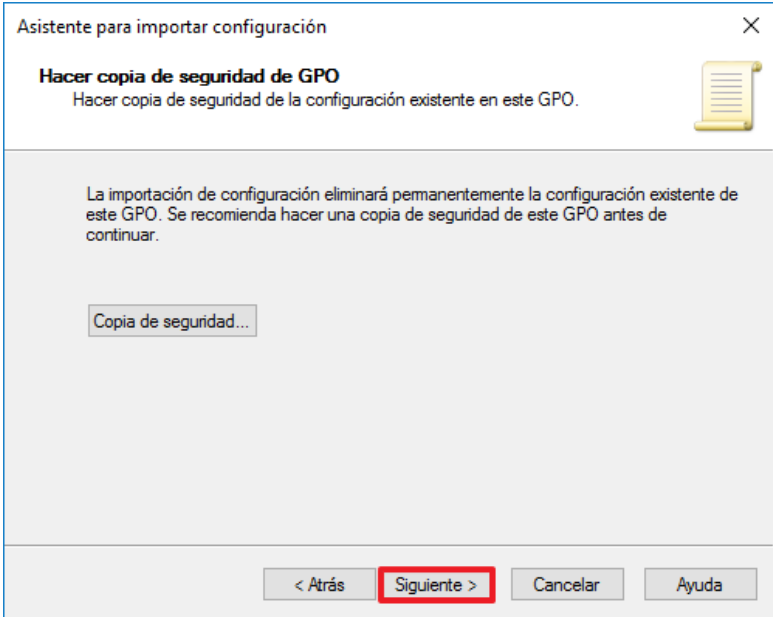
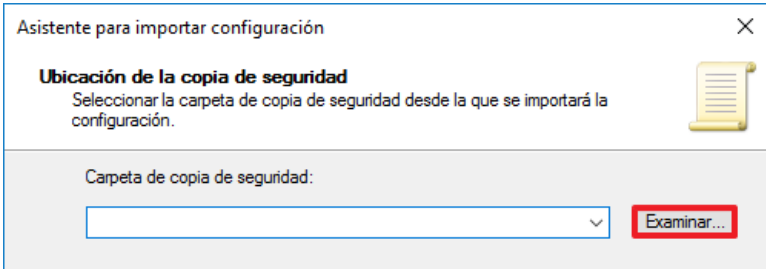
Paso	Descripción
5.	Una vez abierta la consola de comandos, pulse una tecla para continuar el proceso. Este script deshabilita las opciones de accesibilidad de Windows. 
6.	De nuevo pulse una tecla para finalizar la ejecución del script y cerrar la ventana de comando 
7.	Por último, deberá reiniciar 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”.

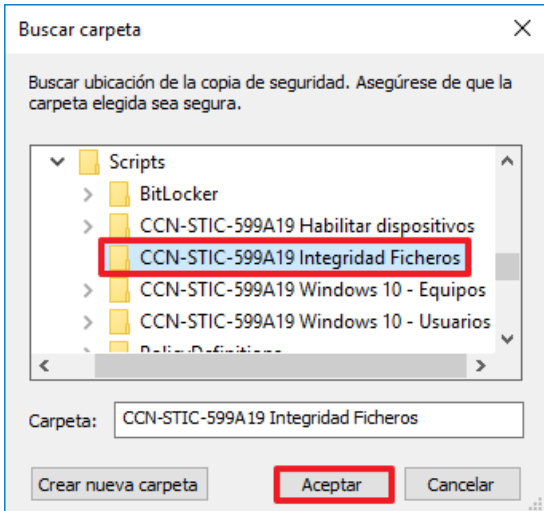
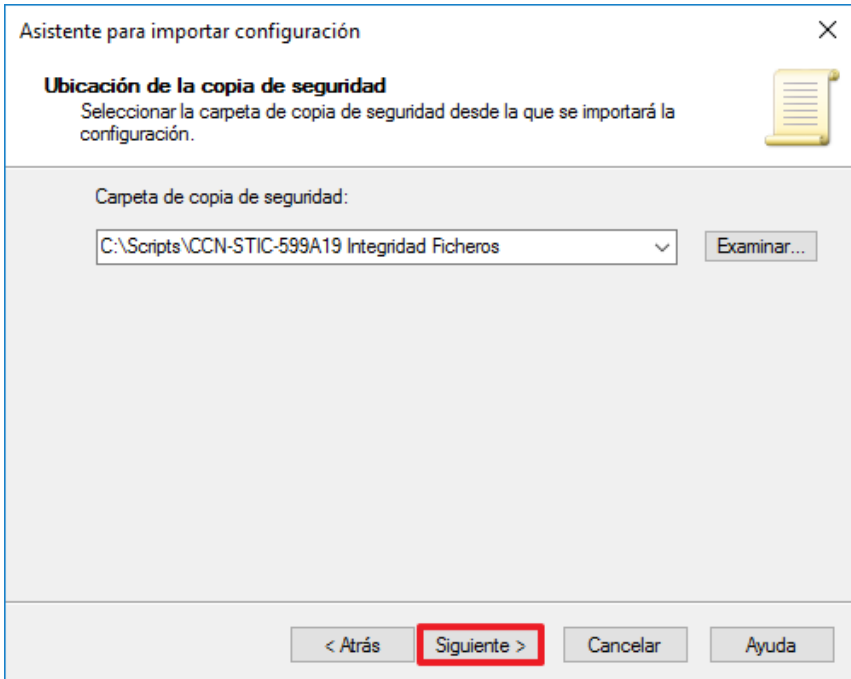
3. RESTAURAR LA INTEGRIDAD DE LOS FICHEROS

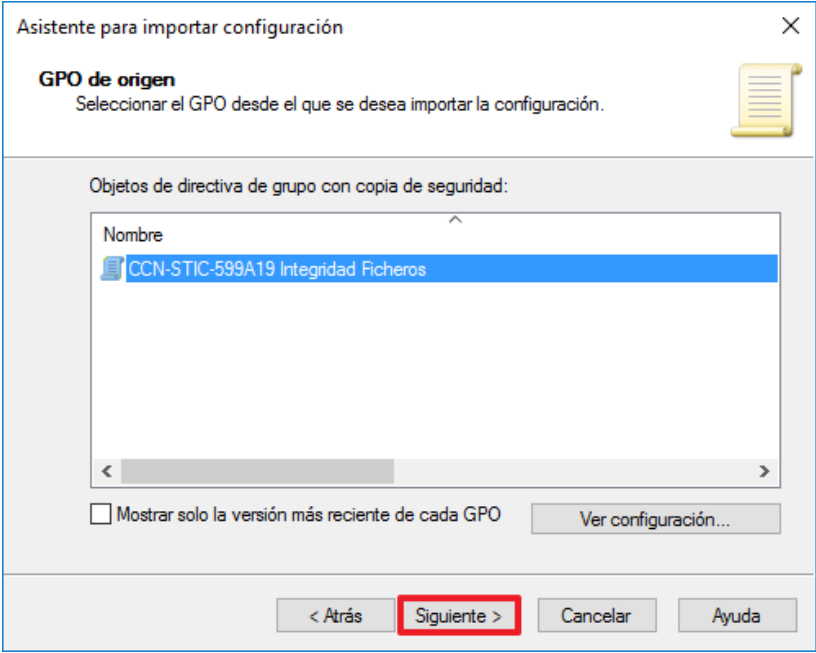
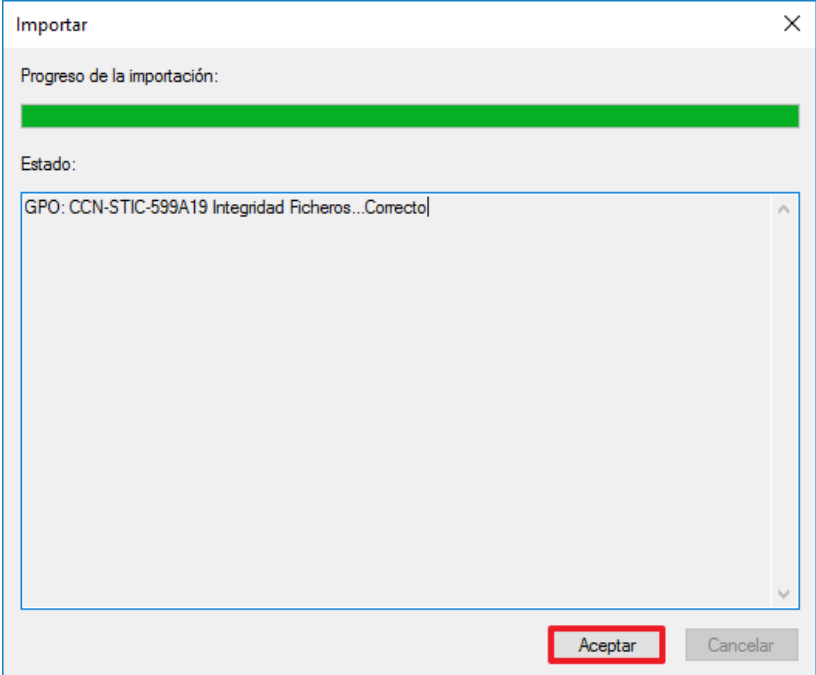
A continuación, se indican los pasos a realizar para crear una tarea programada en la cual se analizará la integridad de los ficheros cada vez que el equipo se inicie.

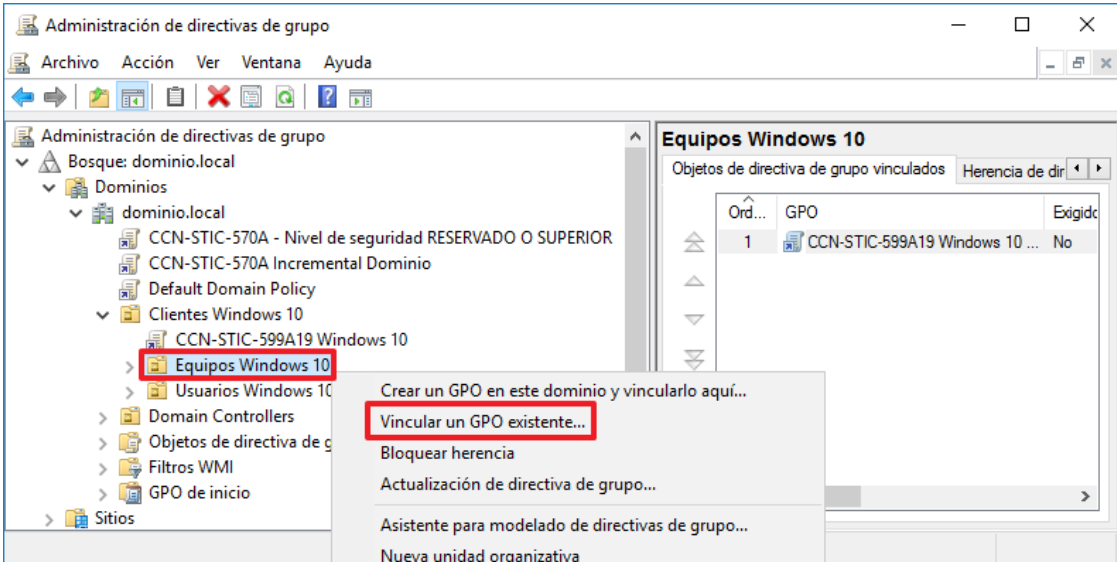
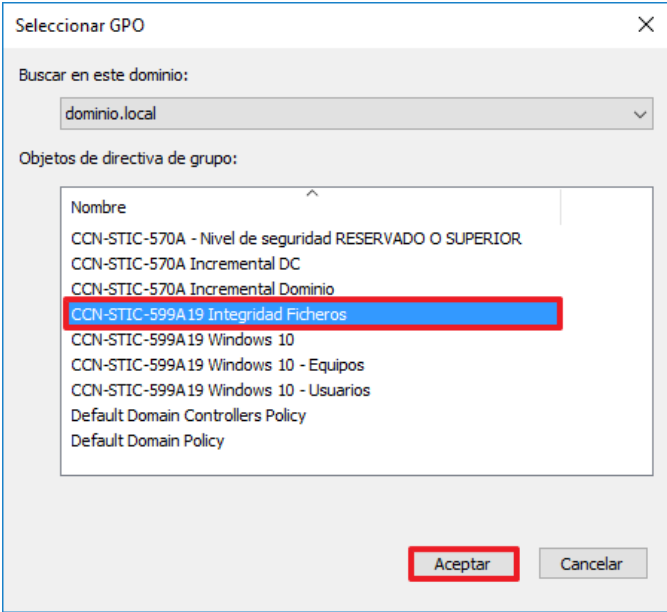
Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio al que pertenecen los equipos cliente que van a asegurar, con una cuenta con derechos de administración en el dominio.
2.	Copie los ficheros que acompañan a esta guía en el directorio “C:\Scripts”.
3.	Inicie el “Administrador del servidor” desde el icono correspondiente en el menú de inicio.  Nota: El sistema le solicitará elevación de privilegios.
4.	Pulse sobre “Herramientas” en el menú superior y localice, en el menú contextual desplegado “Administración de directivas de grupo”. 
5.	En la consola de “Administración de directivas de grupo”, expanda el contenedor con el nombre del dominio mediante la siguiente ruta. "Bosque:<Nombre de su bosque> → Dominios → <Nombre de su dominio>"

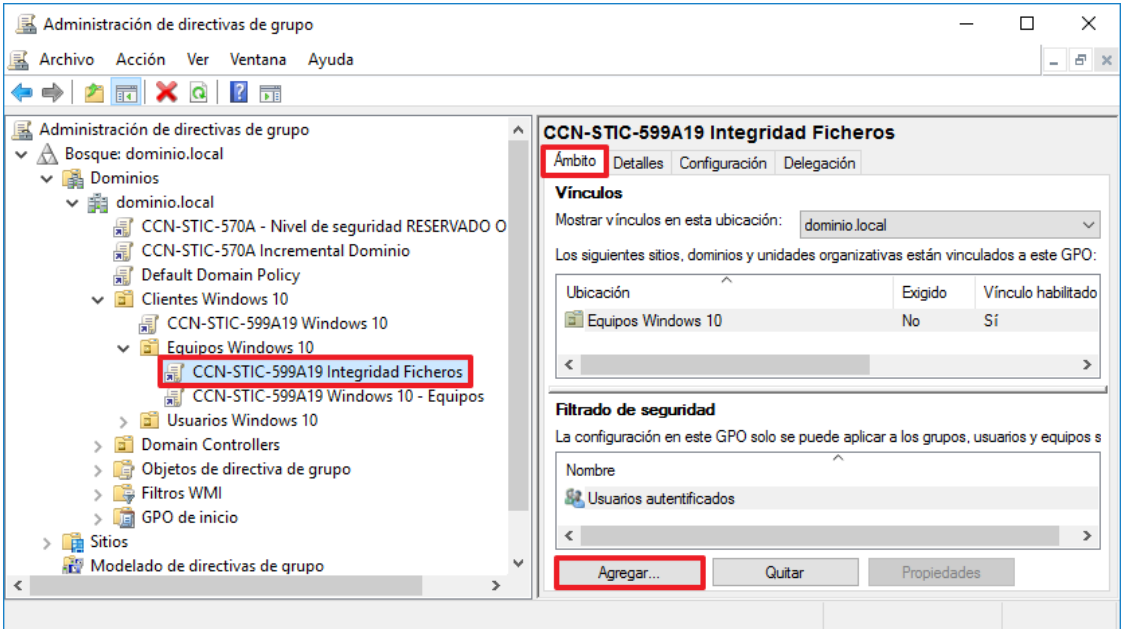
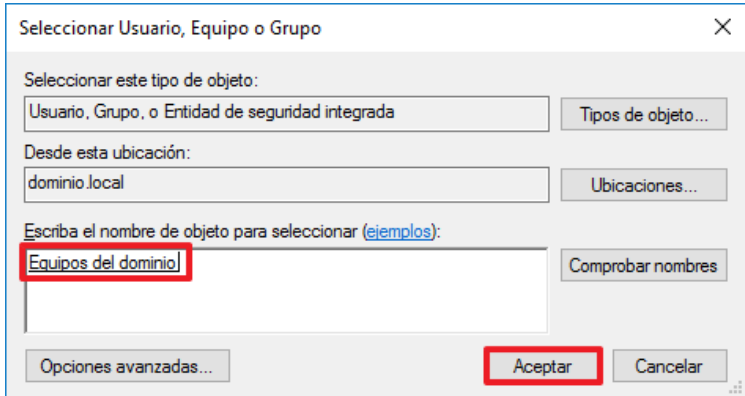
Paso	Descripción
6.	Expanda y seleccione el contenedor "Objetos de directiva de grupo" y, marcando con el botón derecho sobre él, elija la opción "Nuevo" del menú contextual que aparecerá. 
7.	Asigne el siguiente nombre "CCN-STIC-599A19 Integridad Ficheros" a la nueva GPO y pulse "Aceptar". 
8.	Seleccione la GPO recién creada, "CCN-STIC-599A19 Integridad Ficheros " con el botón derecho y pulse sobre la opción "Importar configuración..." en el menú contextual que aparecerá. 

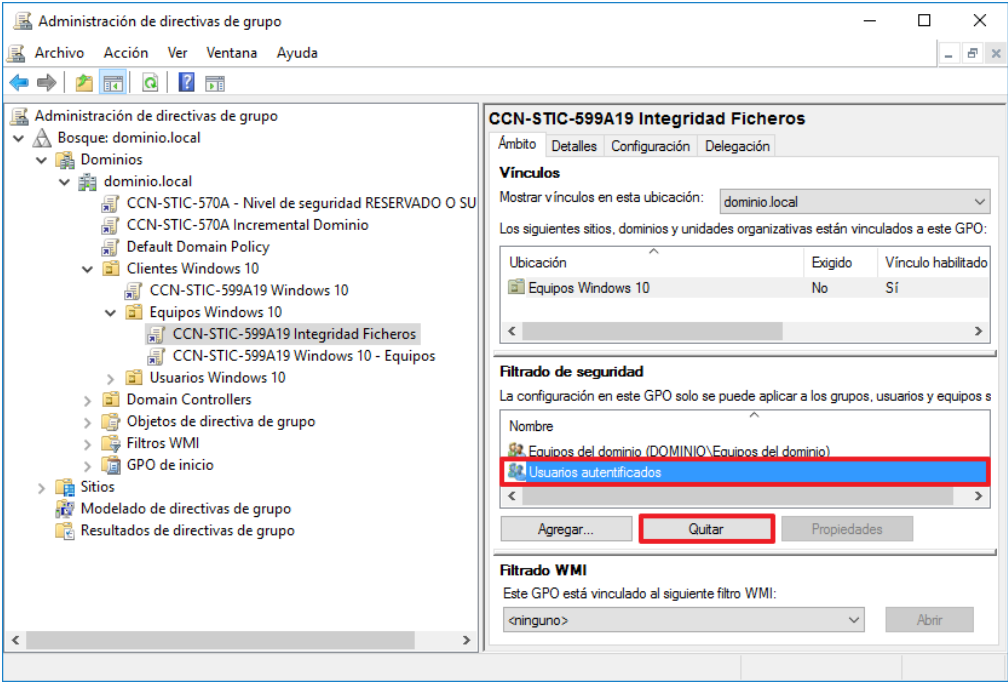
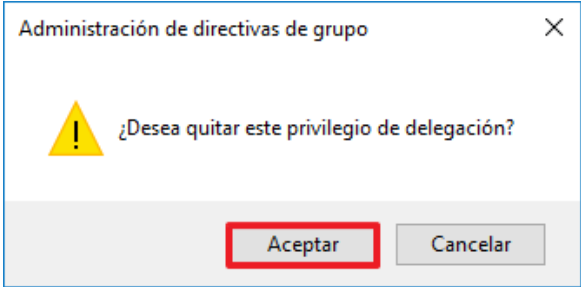
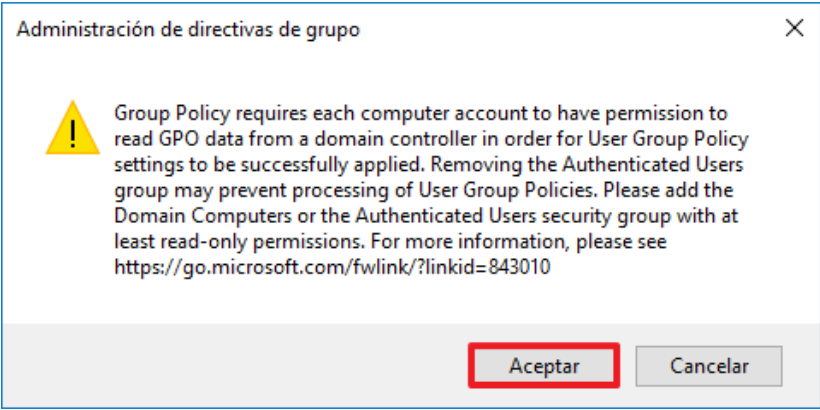
Paso	Descripción
9.	En el “Asistente para importar configuración” pulse “Siguiente >”. 
10.	Como la GPO está vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón "Siguiente >" en la ventana “Hacer copia de seguridad de GPO”. 
11.	En “Ubicación de la copia de seguridad” pulse sobre el botón “Examinar...”. 

Paso	Descripción
12.	Localice la carpeta “CCN-STIC-599A19 Integridad Ficheros” en el directorio “C:\Scripts” y pulse “Aceptar”. 
13.	Pulse “Siguiente >” para continuar. 

Paso	Descripción
14.	En “GPO de origen” pulse “Siguiente >”. 
15.	En “Examinar copia de seguridad” pulse “Siguiente >”.
16.	Pulse “Finalizar” para realizar la importación.
17.	Compruebe que el resultado de la importación es correcto y pulse “Aceptar” para cerrar la ventana. 

Paso	Descripción
18.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” navegue hasta la unidad organizativa “Equipos Windows 10” a través de la siguiente ruta: “Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10 → Equipos Windows 10” Pulsando con el botón derecho sobre la unidad organizativa seleccione la opción “Vincular un GPO existente...”. 
19.	Seleccione “CCN-STIC-599A19 Integridad Ficheros” de la lista y pulse “Aceptar”. 

Paso	Descripción
20.	Utilizando de nuevo la herramienta “Administración de directivas de grupo” seleccione la unidad organizativa “Equipos Windows 10” y a continuación la GPO que acaba de vincular. En el panel de la derecha seleccione la pestaña “Ámbito” y en el apartado “Filtrado de seguridad” seleccione “Agregar...”. 
21.	En la ventana emergente introduzca el nombre “Equipos del dominio” y pulse en sobre “Aceptar”. 

Paso	Descripción
22.	A continuación, en el apartado “Filtrado de seguridad” seleccione el grupo “Usuarios autenticados” y pulse sobre “Quitar”. 
23.	Pulse “Aceptar” ante la advertencia emergente “¿Desea quitar este privilegio de delegación?”. 
24.	Pulse “Aceptar” ante la ventana emergente. 
25.	Elimine el directorio “C:\Scripts”.