centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 585

IMPLEMENTACIÓN DEL ENS EN MICROSOFT OFFICE 2016 SOBRE MICROSOFT WINDOWS 10

FEBRERO 2019

MINISTERIO DE DEFENSA

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2019.02.15 12:41:57 +01'00'

NIPO: 083-19-119-2
Fecha de Edición: febrero de 2019

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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.

febrero de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE MICROSOFT OFFICE 2016 SOBRE MICROSOFT WINDOWS 10 EN EL ENS

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD EN MICROSOFT OFFICE 2016 SOBRE MICROSOFT WINDOWS 10

1. APLICACIÓN DE MEDIDAS EN MICROSOFT OFFICE 2016

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación del paquete de aplicaciones MS Office 2016 sobre equipos con Microsoft 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.

Nota: Tenga en cuenta que en el caso de una red clasificada que ha sido categorizada como Difusión Limitada se hará usó de la aplicación de medidas de seguridad descritas en el "ANEXO A.2.3 CATEGORÍA ALTA / DIFUSIÓN LIMITADA" o en el "ANEXO A.3.3 CATEGORÍA ALTA / DIFUSIÓN LIMITADA" según corresponda.

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

a) Aplicación de seguridad en el entorno de Microsoft Office 2016 sobre Microsoft Windows Server 2016 que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de dicha organización. Será, además, el mecanismo empleado para conducir la centralización y gestión de la seguridad.

b) Aplicación de seguridad en clientes miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows 10 implementados siguiendo la guía CCN-STIC-599A18 – Implementación del ENS en Windows 10.

c) Aplicación de seguridad en clientes independientes que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows 10 implementados siguiendo la guía CCN-STIC-599B18 – Implementación del ENS en Windows 10 Independiente.

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 las aplicaciones ofimáticas, 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 o al propio Directorio Activo, como la asignación de permisos para la segregación de roles y funciones.

Esta guía, por 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. Por ejemplo, aunque es condición indispensable la implementación de un antivirus en los servidores, se establece que esta medida atiende a un criterio general de la organización y que, no siendo algo que pueda aportar el propio sistema operativo, se encontrará excluido del análisis e implementación.

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 los diferentes niveles de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso cubre 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 usabilidad y la protección del sistema, de tal forma que la seguridad se irá incrementando en base al nivel exigido. Por lo tanto, se requiere una menor exigencia de seguridad para el nivel bajo mientras que en el nivel medio y alto se requiere una mayor exigencia.

1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde el nivel bajo y atenderán a la de necesidad proteger los recursos del sistema (ficheros, directorios y recursos compartidos) con algún mecanismo que impida su utilización, salvo a usuarios o perfiles de usuario que disfruten de los derechos de acceso suficientes.

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

Así mismo dicha persona responsable será la encargada de determinar aquellos recursos que serán compartidos y cuáles serán accesibles para los usuarios.

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 la 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 Microsoft Windows Server 2016, incluyendo los controles de acceso dinámicos.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/jj134043(v=ws.11)

https://docs.microsoft.com/es-es/windows-server/identity/solution-guides/dynamic-access-control--scenario-overview

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

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

Aplicable a partir del nivel medio. 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 Microsoft Windows Server 2016. Conforme a las necesidades planteadas en los dos primeros elementos, desarrollo de operaciones y la configuración, así como el mantenimiento del sistema de operación, el operador deberá tomar en consideración lo establecido en el Anexo B.7. de la última revisión la guía CCN-STIC-570A. En dicho Anexo, además de otras cuestiones relativas a mejoras en la seguridad y procesos, se recogen los procedimientos que pueden ser llevados a cabo para la segregación de tareas, de tal forma que se pueden conceder determinados privilegios a usuarios concretos sin necesidad de facultarles de derechos completos. Así, se muestran ejemplos para delegar las tareas de agregar equipos al dominio a determinados usuarios, sin que estos tengan la necesidad de ser administradores del dominio o bien atribuirles los permisos para poder gestionar las cuentas del Directorio Activo con la misma premisa de no ser administradores.

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" que aun habiendo sido emitida para Windows Server 2008 R2 es igualmente aplicable a sistemas Windows Server 2016. Aunque será mencionada a lo largo de la presente guía, en relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en Windows Server 2016 y sus servicios, a través del sistema de Suscripción de eventos con el que Microsoft ya dotó a Windows Server 2008.

Así mismo es importante la creación de grupos a la hora de conceder permisos sobre un recurso. Esto permitirá una gestión más global y sencilla sobre el acceso a los recursos evitando modificar los permisos individuales de cada usuario para conceder o no permisos sobre un mismo recurso.

Así mismo es interesante que los usuarios que pertenezcan a los grupos que usen las aplicaciones ofimáticas sean usuarios que no pertenezcan al grupo de administradores del dominio ni sean cuentas locales de administración.

Además, deben añadirse varias cuentas para administrar Office y sus recursos (mínimo dos) para evitar que toda la responsabilidad recaiga sobre una sola cuenta.

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

Altamente vinculado al punto "1.1.1.1 OP. ACC. 2. REQUISITOS DE ACCESO", este proceso requiere consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada recurso 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, Microsoft Windows Server 2016 se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

En la navegación a Internet, acceso a recursos o tratamientos ofimáticos por citar algunos ejemplos frecuentes, un usuario no requiere del privilegio de administrador para poder utilizarlos. 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.

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda visualizar contenido que no es requerido para las funciones que desempeña. Se establece por lo tanto a nivel de los recursos, el aplicar mecanismos de ACL para permitir la visualización de contenido o edición del mismo a los usuarios que los requieran exclusivamente.

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.

Se deberá tener en consideración debido a dicha norma que los permisos otorgados a los usuarios serán los mínimos requeridos no siendo necesario que estos posean permisos adicionales para la tarea que van a realizar. Por ejemplo, si un usuario tiene permiso para alterar el contenido de una carpeta no por ello implica que sea necesario que posea el permiso de "Control total". Con la concesión de este permiso se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de modificar se debe considerar como la opción más óptima desde el punto de vista del ENS.

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

Se considera que Microsoft Office debe configurarse previamente a su entrada en producción teniendo en cuenta las siguientes directrices:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

Se considera indispensable que el sistema no proporcione 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 niveles. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

Adicionalmente se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición de la información manejada, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

1.1.2.2. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN

Se deberá tener en consideración la configuración de los componentes del sistema que se gestione de forma que:

a) Se mantenga en todo momento la regla de funcionalidad mínima y seguridad por defecto.

b) El sistema debe adaptarse a las nuevas necesidades las cuales previamente han sido autorizadas y probadas en un entorno de test antes de la puesta en producción.

c) El sistema debe reaccionar ante vulnerabilidades reportadas e incidentes.

Se establecerán mecanismos para desinstalar productos de la suite ofimática, con el objetivo de prevenir código dañino y mantener la regla de mínima funcionalidad.

1.1.2.3. OP. EXP. 4. MANTENIMIENTO

Para mantener el equipamiento físico y lógico, se deberá 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 Office 2016. Debe tenerse en consideración que esta suite ofimática es un elemento en constante evolución que, ante la aparición de un riesgo de seguridad, deberá dotar de los mecanismos necesarios para paliar el problema. Para ello, Microsoft hace una constante difusión de actualizaciones de seguridad que se deberán evaluar e implementar sobre los servidores, con objeto de mantener las garantías de seguridad necesarias.

No es objeto de esta guía especificar los mecanismos a emplear para mantener actualizados los sistemas. Las plantillas de seguridad basarán las condiciones para que los sistemas puedan ser actualizados. Podrá encontrar más información relativa a la gestión e implementación de sistemas de actualizaciones en la siguiente dirección URL:

https://support.office.com/es-es/article/instalar-actualizaciones-de-office-2ab296f3-7f03-43a2-8e50-46de917611c5

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

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como «spyware», y en general, todo lo conocido como «malware».

Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

La presente guía especifica mediante configuración de plantillas administrativas la restricción de código malicioso en las aplicaciones ofimáticas, analizando las herramientas de automatización de dichos productos en documentos externos siempre que haya un software antivirus instalado. Si no fuese el caso impedirá la ejecución de los documentos.

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

Aplicable en los niveles altos 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) El nivel alto requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

Microsoft Office, implementa mecanismos para la auditoría de acceso a objetos. 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 de recolección y consolidación de eventos con Windows 2008 R2 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoria desde múltiples sistemas, permitiendo establecer así mecanismos de correlación.

Adicionalmente MS Office dispone de mecanismo que permiten emitir informes sobre todo aquello que se almacena, modifica o elimina pudiendo realizar seguimientos y acciones correspondientes.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN MICROSOFT OFFICE 2016

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, de la serie CCN-STIC-800 o bien la aplicación de políticas de seguridad a nivel de dominio o bien localmente.

Control	Medida	Mecanismo de aplicación
OP. ACC. 2	Requisitos de acceso	Revisión e implementación de guía CCN-STIC-585, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-585, adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-585, adaptándolos a la organización.
OP. EXP. 2	Configuración de seguridad	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. 3	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-585, adaptándolos a la organización.
OP. EXP. 4	Mantenimiento	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 6	Protección frente a código dañino	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-585, adaptándolos a la organización. Revisión e implementación de guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2

ANEXO A.2. IMPLEMENTACIÓN SEGURA DE MICROSOFT OFFICE 2016 EN UN CLIENTE WINDOWS 10 MIEMBRO DE UN DOMINIO

ANEXO A.2.1. CATEGORÍA BÁSICA

ANEXO A.2.1.1. GUÍA PASO A PASO DE IMPLEMENTACIÓN SEGURA

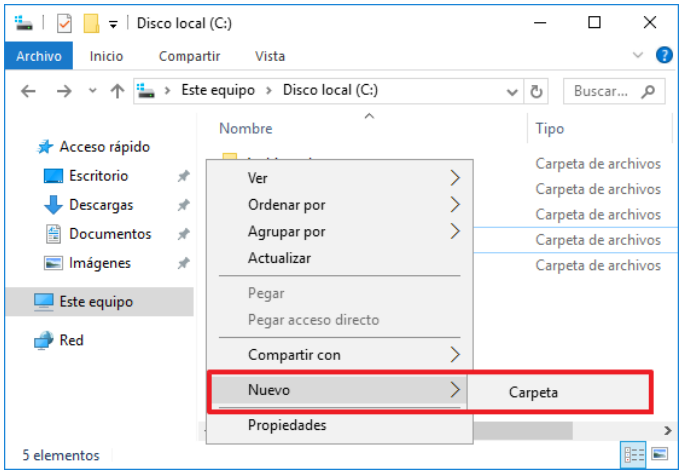
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen la suite de Microsoft Office 2016 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad.

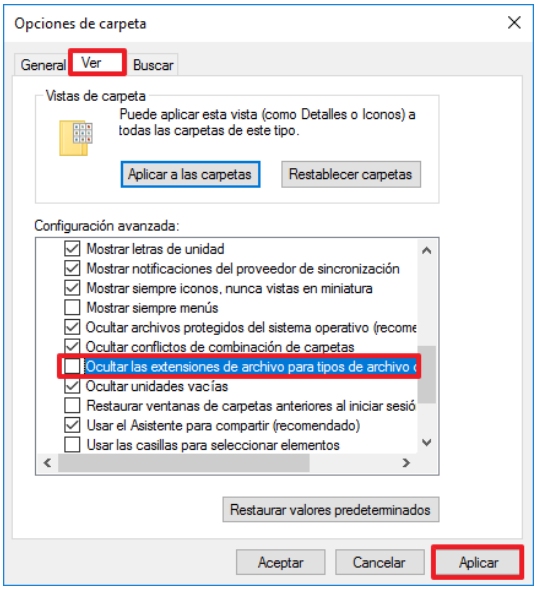
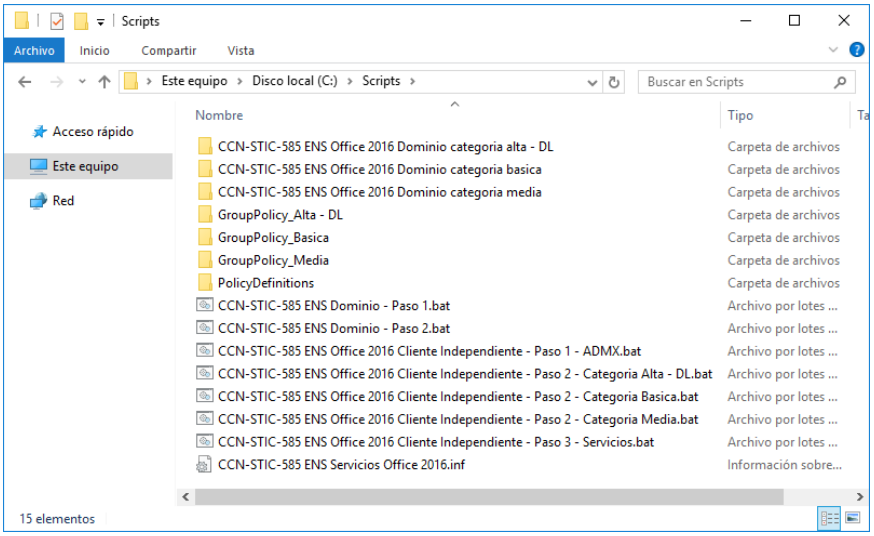
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

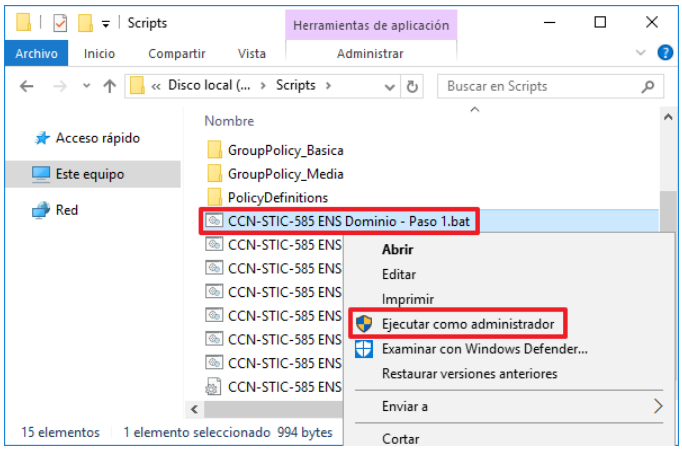
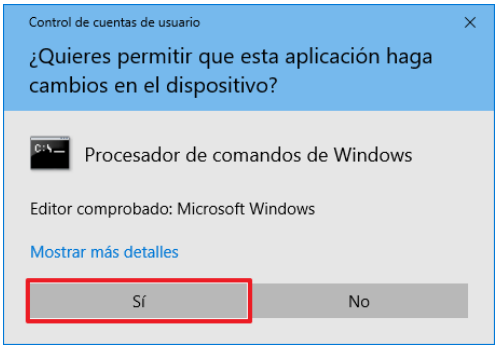
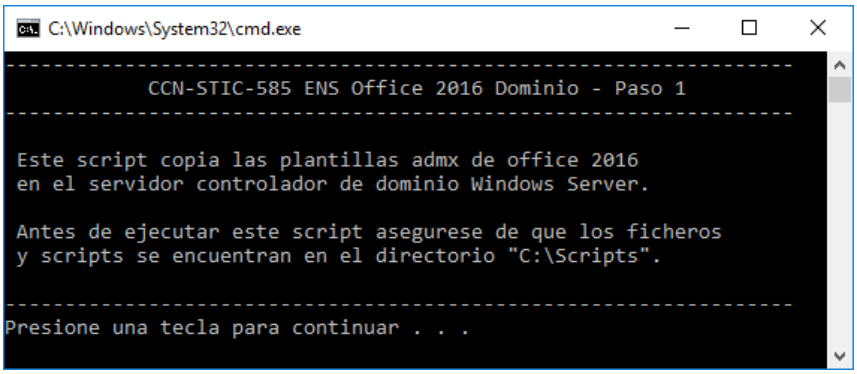
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

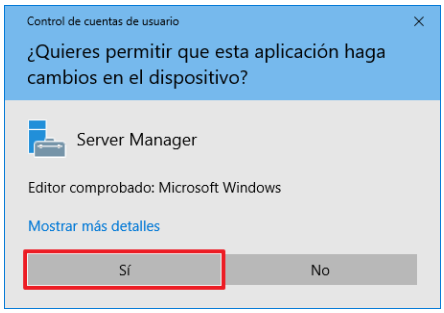
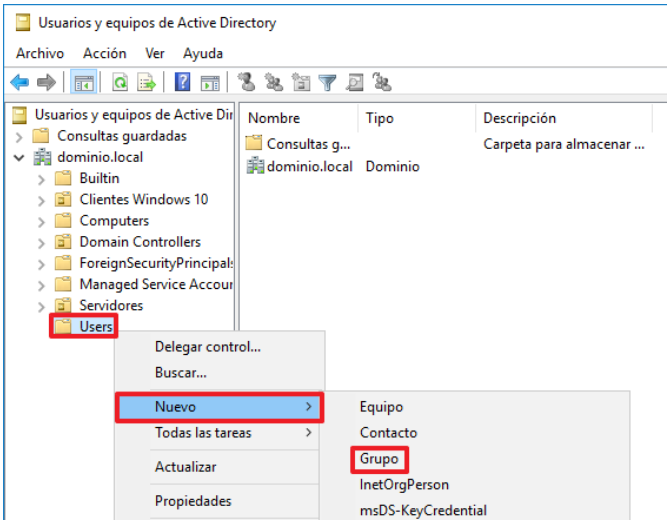
1. PREPARACIÓN DEL DIRECTORIO ACTIVO

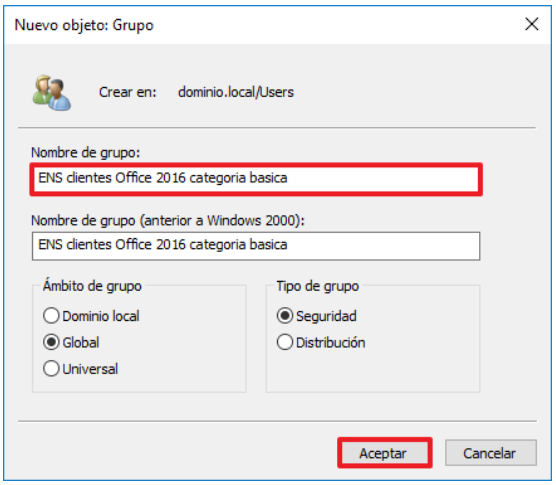
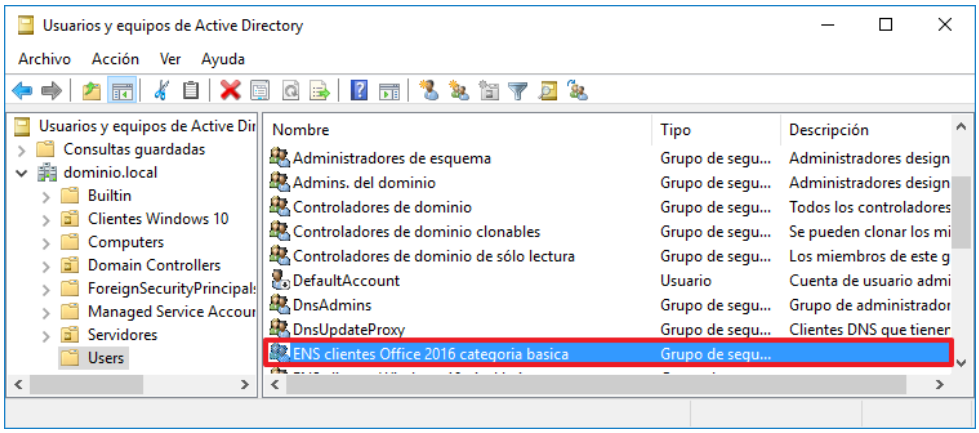
Los pasos que se describen a continuación se realizarán en un controlador de dominio, de la infraestructura a la que pertenecen los clientes en los que se va a securizar MS Office 2016.

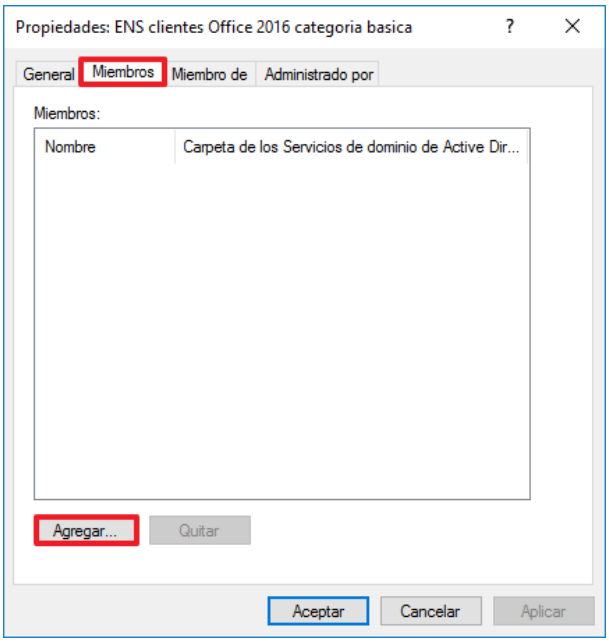
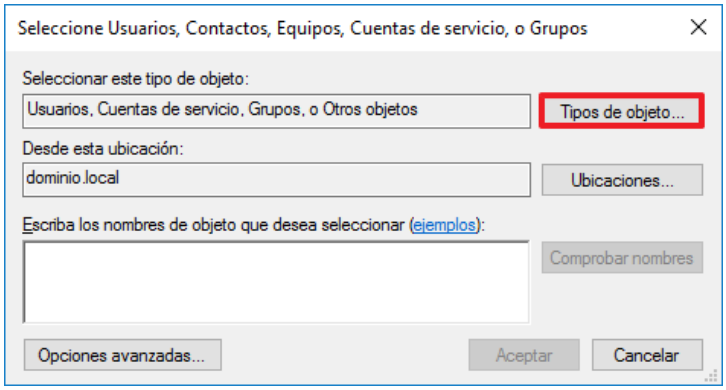
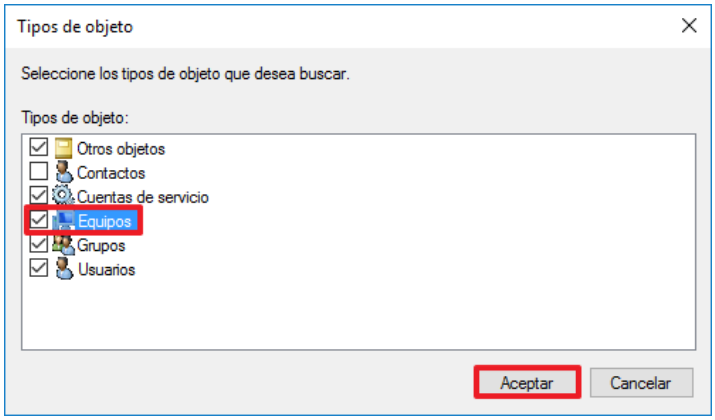
Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta que sea miembro del grupo “Admins. del domino” del dominio al que pertenecen los clientes donde se va a securizar MS Office 2016. **Nota:** En este ejemplo se utiliza un cliente Windows 10 con un controlador de dominio Windows Server 2016 con las guías CCN-STIC-570A y CCN-STIC-599A18 con categoría básica aplicadas. Este entorno puede variar con la estructura de su organización.
2.	Cree el directorio “Scripts” en la unidad “C:\”. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo → Carpeta”.** 
3.	Asigne el nombre “Scripts” al nuevo directorio.

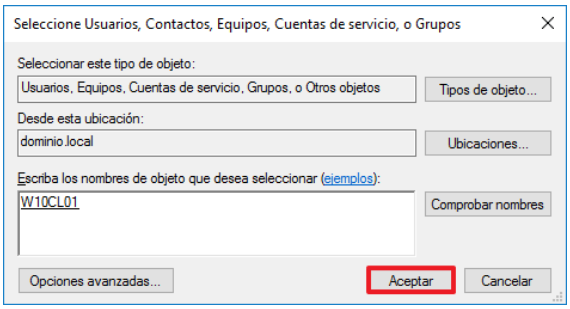
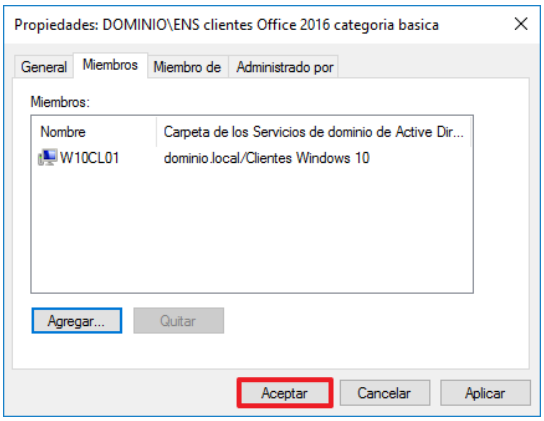
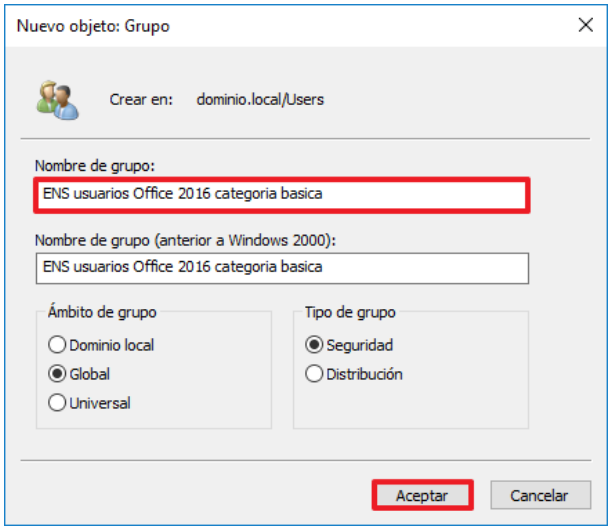
Paso	Descripción
4.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que Explorador de Windows sí muestra las extensiones de los archivos.
5.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".
6.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”. 

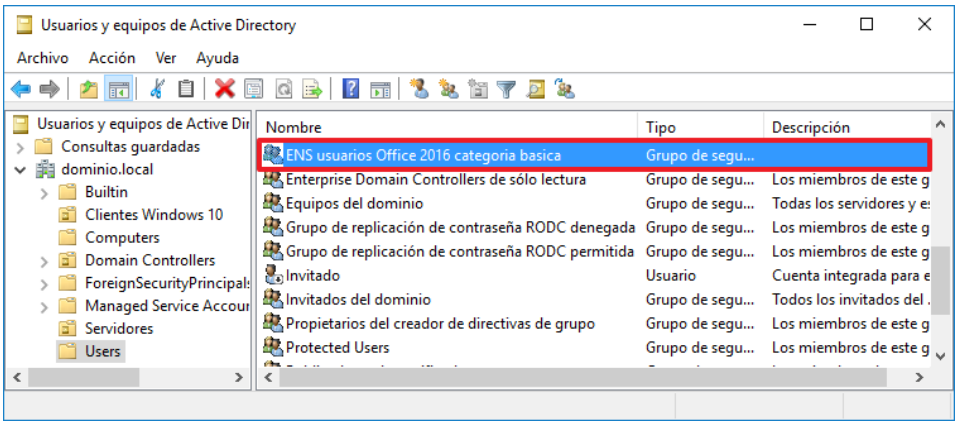
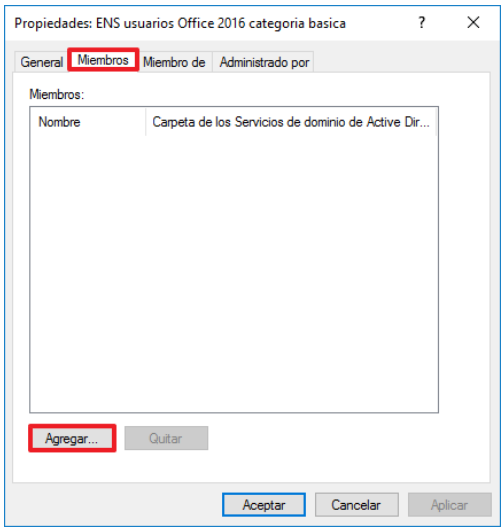
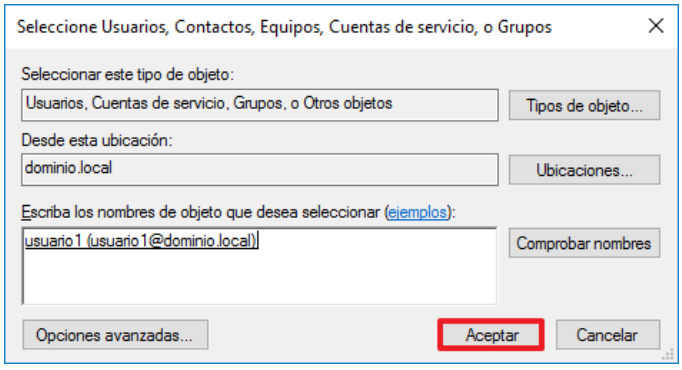
Paso	Descripción
7.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del servidor, de tal forma que se podrán realizar modificaciones, desde dicha máquina, de las políticas generadas. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script **"CCN-STIC-585 ENS Dominio - Paso1.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.
8.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Pulse "Sí" para continuar. 
9.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 

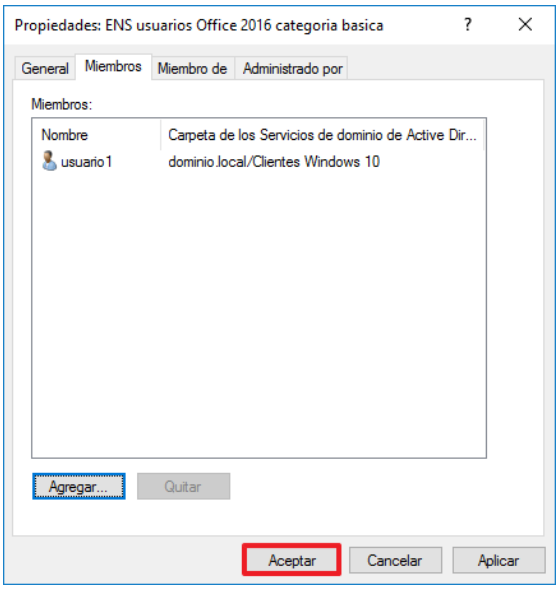
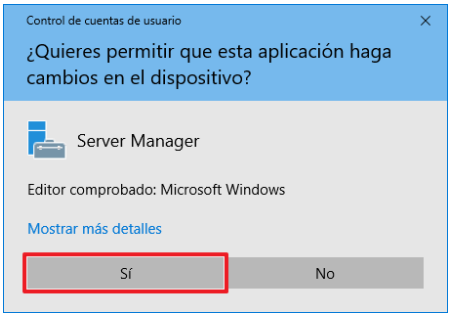
Paso	Descripción
10.	Inicie la herramienta "Usuarios y equipos de Active Directory", para ello ejecute la herramienta Administrador del servidor (**Inicio → Administrador del servidor**). Seleccione en el menú superior **"Herramientas → Usuarios y equipos de Active Directory"**. **Nota:** Los siguientes pasos describen el procedimiento para crear grupos de seguridad donde agregar los puestos de trabajo y usuarios 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 o los usuarios se encuentren en la ubicación predeterminada de "Computers" o "Users" 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.
11.	El control de cuentas de usuario le solicitará elevación de privilegios. Pulse "Sí" para continuar. 
12.	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"**. 

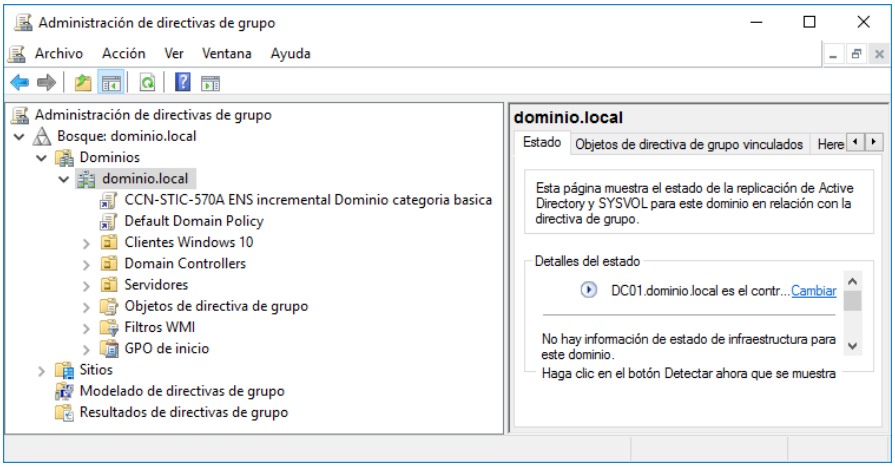
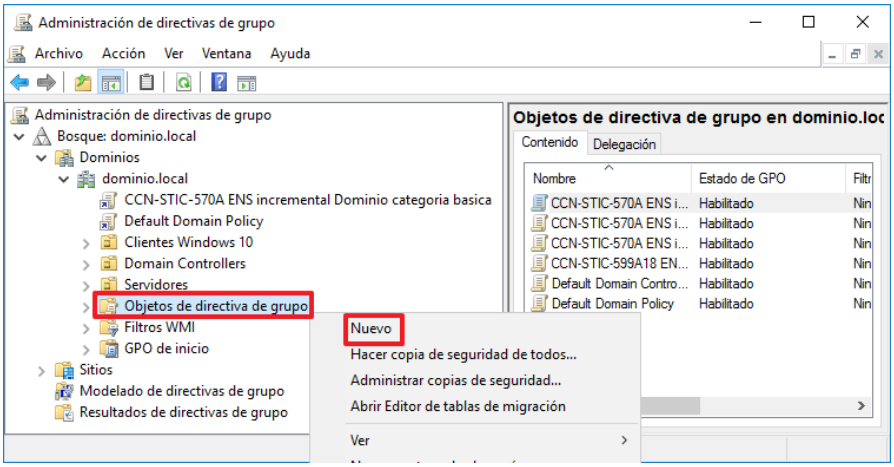
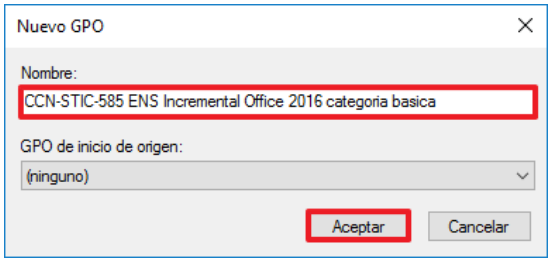
Paso	Descripción
13.	Introduzca como nombre “ENS clientes Office 2016 categoria basica”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes que vayan a usar Office 2016. 
14.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 

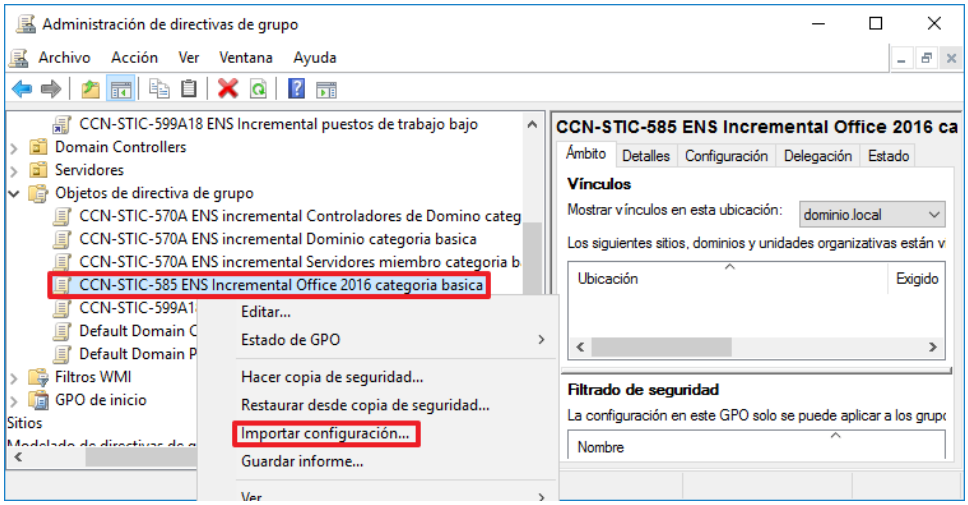
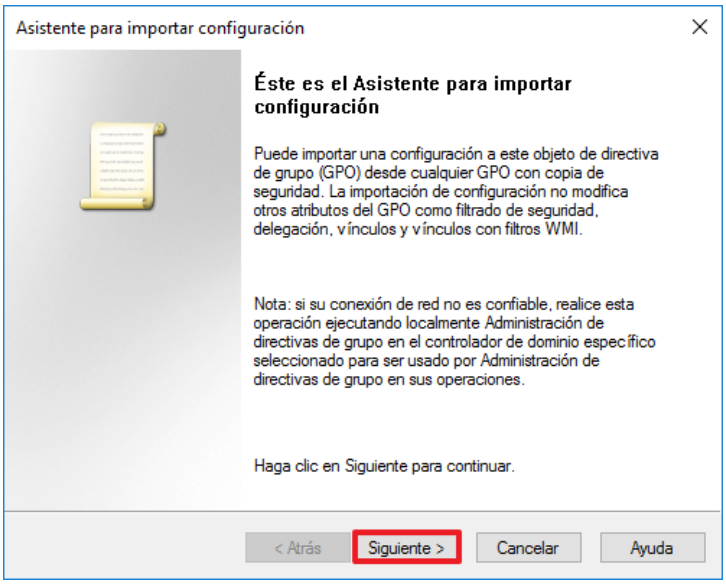
Paso	Descripción
15.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar…”. 
16.	Pulse sobre “Tipos de objeto…” 
17.	Marque la opción “Equipos” y pulse “Aceptar”. 

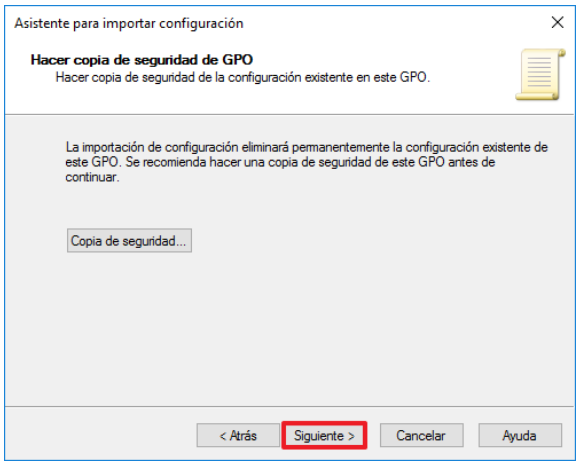
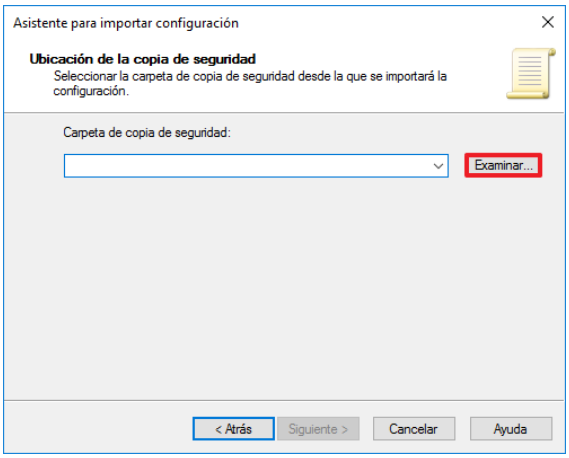
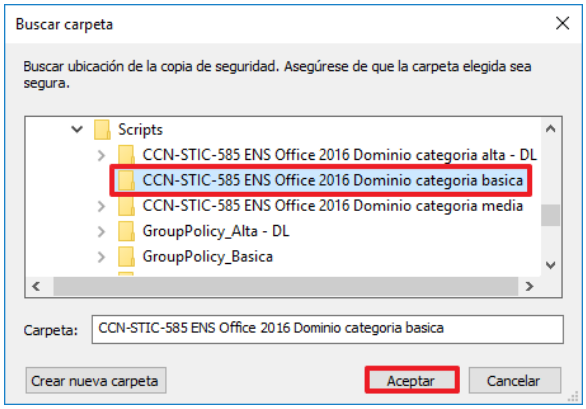
Paso	Descripción
18.	Introduzca el nombre de los equipos o utilice las opciones avanzadas para agregar todos aquellos equipos que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad básica que vayan a hacer uso de Office 2016 y pulse "Aceptar" para agregar la selección.  **Nota:** En este ejemplo se usa el equipo "W10CL01", deberá introducir los equipos acordes a su organización.
19.	Pulse nuevamente el botón "Aceptar" para guardar las propiedades del grupo y cerrar la ventana. 
20.	De manera análoga, cree un nuevo grupo con nombre "ENS usuarios Office 2016 categoria basica". Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre usuarios que vayan a usar Office 2016. 

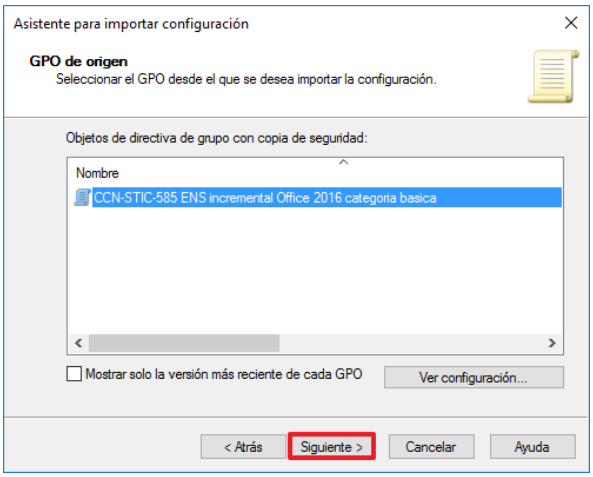
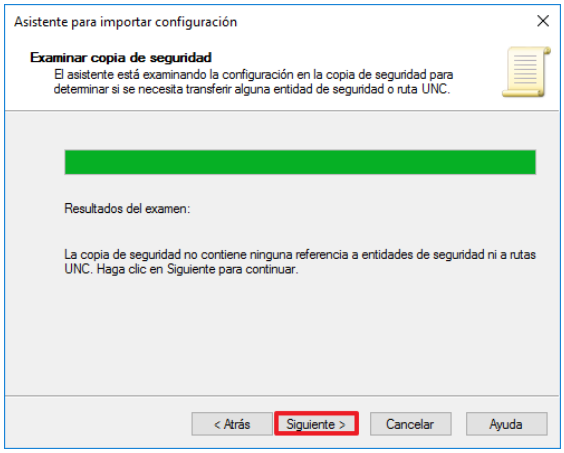
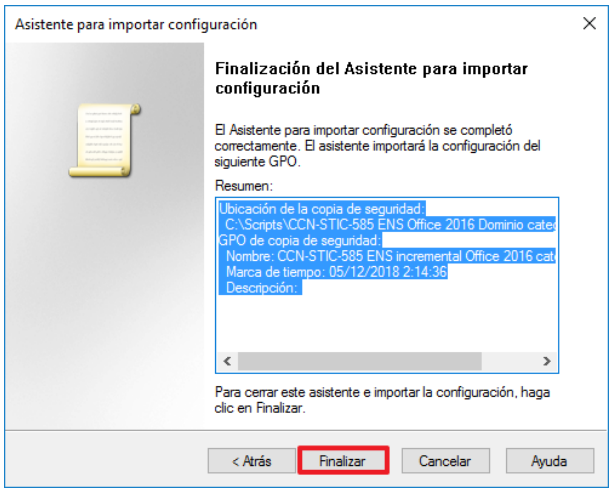
Paso	Descripción
21.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
22.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar…”. 
23.	Introduzca el nombre de los usuarios o utilice las opciones avanzadas para agregar todos aquellos usuarios que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad básica que vayan a hacer uso de Office 2016 y pulse “Aceptar” para agregar la selección.  **Nota:** En este ejemplo se usa el usuario “usuario1”, deberá introducir los usuarios acordes a su organización. Recuerde que dichos usuarios deberán situarse en la unidad organizativa donde se vaya a implementar la seguridad.

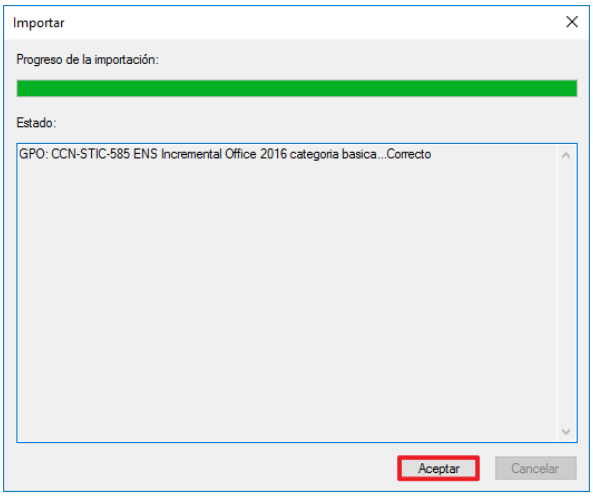
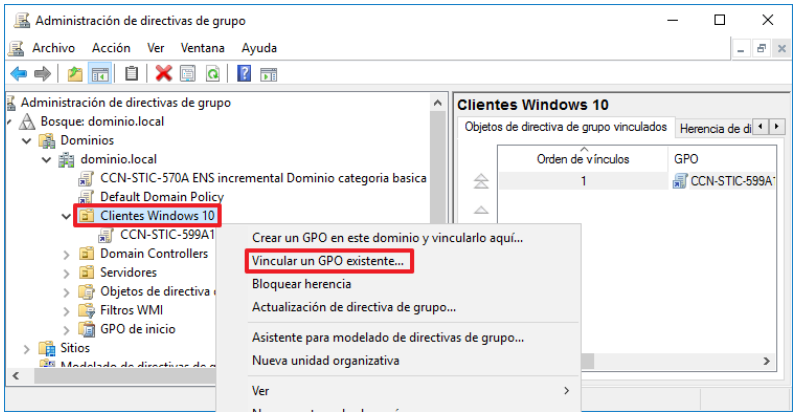
Paso	Descripción
24.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
25.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
26.	Inicie la herramienta de administración de directivas de grupo, para ello ejecute la herramienta Administrador del servidor (**Inicio → Administrador del servidor**). Seleccione en el menú superior **"Herramientas → Administrador de directivas de grupo”**.
27.	El control de cuentas de usuario le solicitará elevación de privilegios. Pulse “Sí” para continuar. 

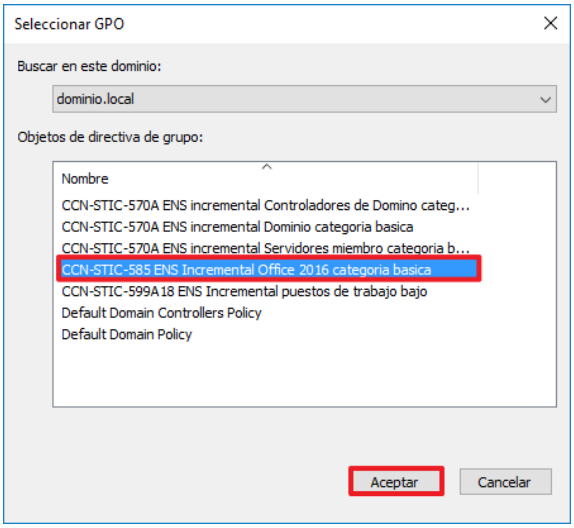
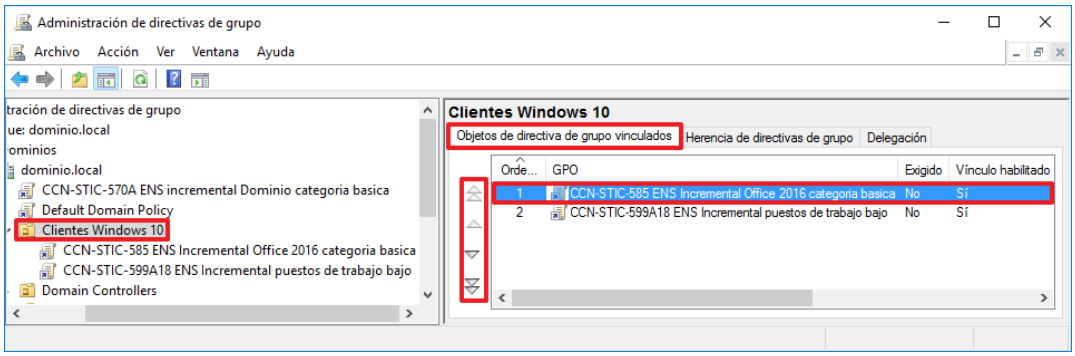
Paso	Descripción
28.	Expanda el contenedor **"Administración de directivas de grupo Bosque:<nombre de su bosque> Dominios *[nombre de su dominio]*"**, como se muestra en la siguiente imagen.  A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPO correspondientes. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores del recién expandido (*[nombre de su dominio]*). **Nota:** En este ejemplo se utiliza como nombre de dominio "dominio.local".
29.	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. 
30.	Asigne el siguiente nombre a la nueva política, GPO, que se está creando: "CCN-STIC-585 ENS Incremental Office 2016 categoria basica" y pulse "Aceptar". 

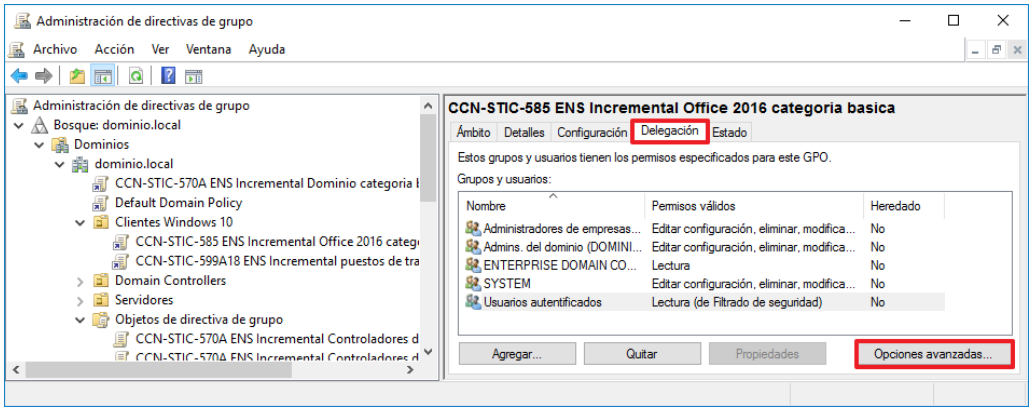
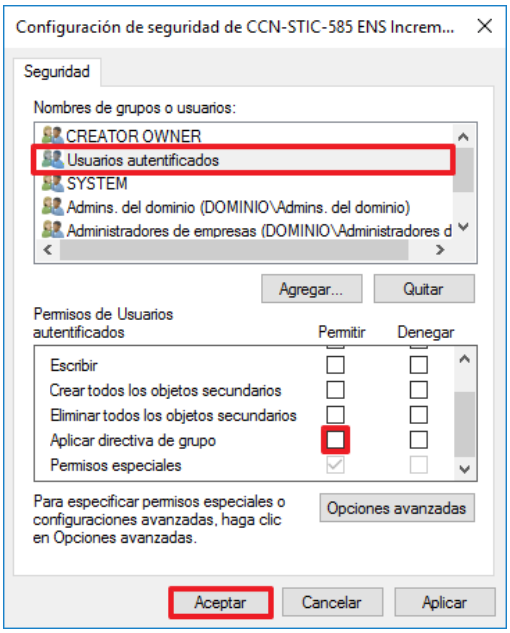
Paso	Descripción
31.	Seleccione el objeto de directiva de grupo, GPO, recién creado y marcando con el botón derecho en ella, elija la opción “Importar configuración” del menú contextual que aparecerá. 
32.	Se iniciará el asistente para la importación de configuración, pulse el botón “Siguiente >”. 

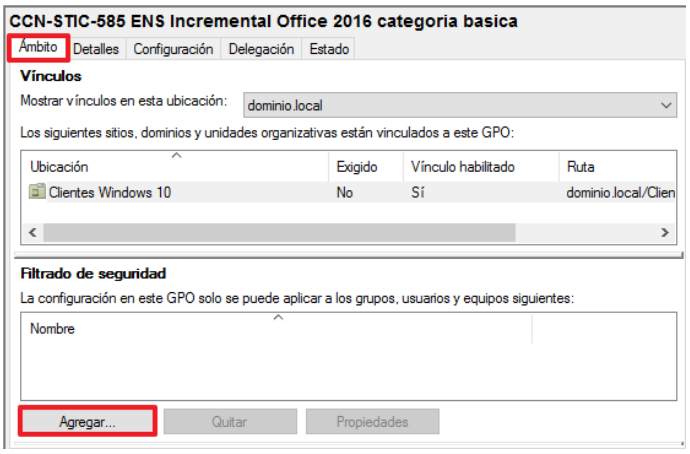
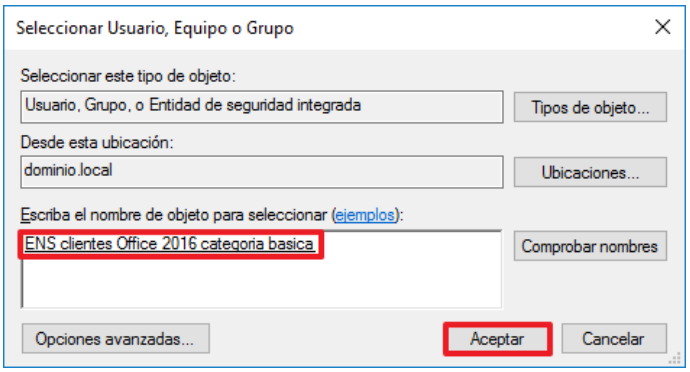
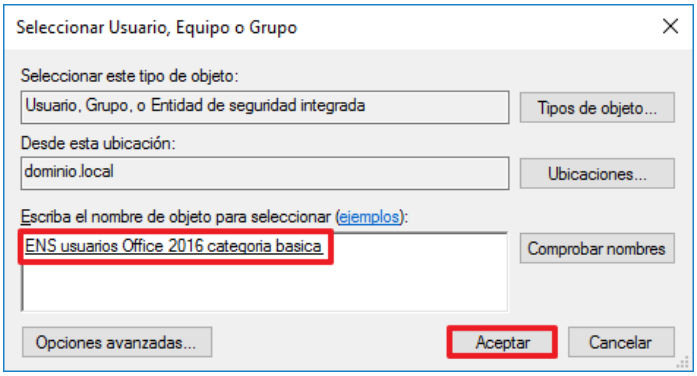
Paso	Descripción
33.	El asistente para la importación de la configuración ofrecerá la opción de realizar una copia de seguridad de la configuración actual de la GPO. Como la política se encuentra vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón “Siguiente >” 
34.	A continuación, deberá seleccionar la carpeta de copia de seguridad desde la que se importará la configuración. Seleccione el botón “Examinar…”. 
35.	Busque y seleccione la carpeta “**C:\Scripts\CCN-STIC-585 ENS Office 2016 Dominio categoria basica**”. Pulse el botón “Aceptar” y volverá a la ventana del asistente. Pulse el botón “Siguiente >”. 

Paso	Descripción
36.	Deberá indicarse el objeto GPO desde el que desea importar la configuración. Pulse “Siguiente >”. 
37.	El asistente procederá a realizar una verificación de la configuración de la copia de seguridad. Pulse el botón “Siguiente >”. 
38.	El asistente para importar la configuración mostrará, entonces, una ventana resumen con los datos de la importación que se va a realizar. Pulse el botón “Finalizar”. 

Paso	Descripción
39.	El asistente procederá a realizar la importación. Pulse “Aceptar”. Con ello habrá quedado importada la configuración de la nueva política generada, estando lista para ser asignada a la unidad organizativa de usuarios creada en pasos anteriores, cuestión que se realizará a continuación. 
40.	Expanda y seleccione el contenedor de usuarios en la unidad organizativa donde tenga alojada la configuración de los clientes, **“Menú inicio → Herramientas administrativas → Administración de directivas de grupo → Bosque: *[nombre de su bosque]* → Dominios → *[nombre de su dominio]* → Clientes Windows 10”**, y márquelo con el botón derecho del ratón, seleccione la opción “Vincular un GPO existente…”  **Nota:** En este caso, el nombre del bosque y del dominio es “dominio.local” y las unidades organizativas fueron creadas durante el proceso de instalación de equipos Windows 10 dentro de un dominio, según la guía CCN-STIC-599A18. Si todos los equipos y usuarios a los que va a aplicar esta configuración no se encuentran en esta unidad organizativa deberá vincular la GPO a nivel de dominio.

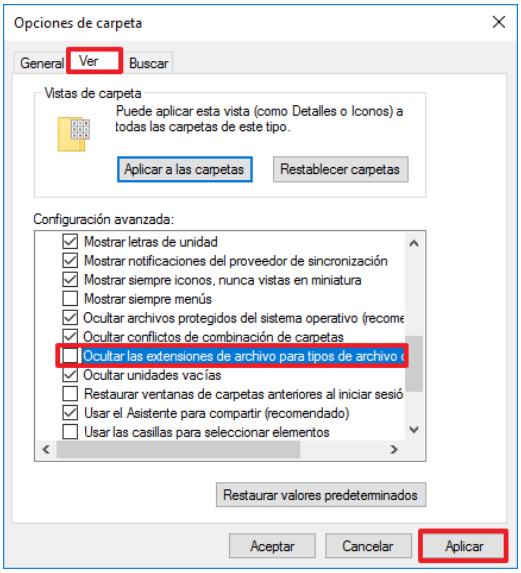
Paso	Descripción
41.	En la ventana que aparece, seleccione el GPO “CCN-STIC-585 ENS Incremental Office 2016 categoria basica” y pulse el botón “Aceptar”. 
42.	El objeto de directiva de grupo, GPO, habrá quedado vinculado a la unidad organizativa “Clientes Windows 10”.
43.	Ahora, se determinará el orden de los vínculos. Deberá quedar, la nueva directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”, en la primera posición para asegurar un resultado adecuado en la aplicación. Para ello, se deben utilizar las flechas de posicionamiento de la ficha “Objetos de directiva de grupo vinculados” de la unidad organizativa “Clientes Windows 10”. 

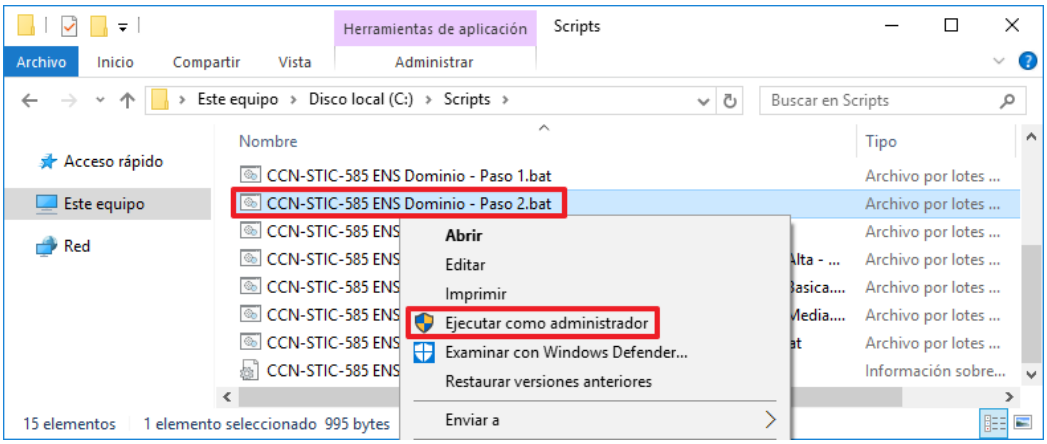
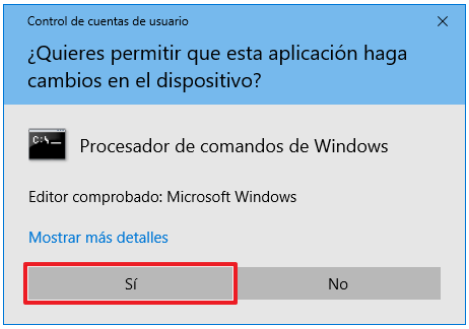
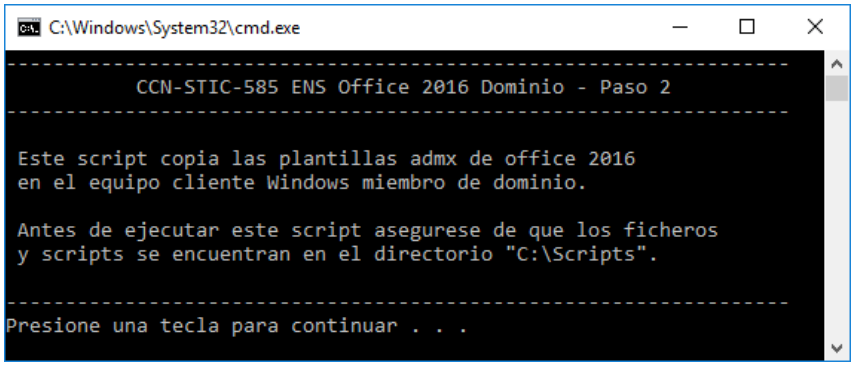
Paso	Descripción
44.	Seleccione la nueva GPO configurada. Vaya a las opciones de Delegación que se encuentran en el panel derecho. Seleccione “Usuarios autentificados” y pulse sobre el botón “Opciones avanzadas”.  **Nota:** En el caso de que todos los equipos cliente vayan a tener instalado Office 2016 puede mantener el grupo del sistema “Usuarios autentificados” sin modificar y saltar al paso 49
45.	Seleccione “Usuarios autentificados” y en la parte inferior “Permisos de Usuarios autentificados” quite el check “Permitir” en “Aplicar directiva de grupo” y pulse el botón “Aceptar”. 

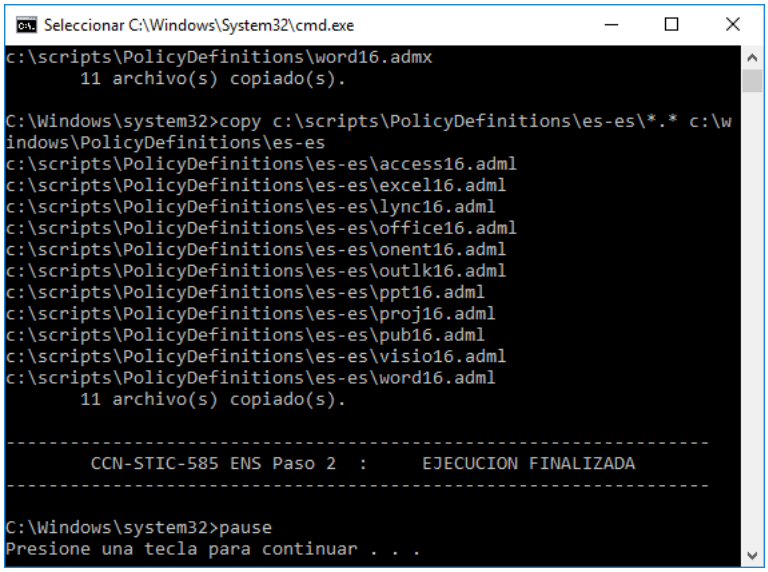
Paso	Descripción
46.	Vaya a la pestaña “Ámbito” y pulse sobre el botón “Agregar…”. 
47.	Introduzca como nombre “ENS clientes Office 2016 categoria basica”. A continuación, pulse el botón “Aceptar”. 
48.	De manera análoga, introduzca el grupo “ENS usuarios Office 2016 categoria basica” y pulse “Aceptar”. Estos grupos corresponden con los generados en pasos previos. 
49.	El objeto de directiva de grupo, GPO, habrá quedado configurada correctamente. **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
50.	Elimine la carpeta “C:\Scripts” del servidor.

2. PREPARACIÓN DEL CLIENTE PARA LA SECURIZACIÓN DE MS OFFICE 2016 EN UN EQUIPO DEL DOMINIO

Los siguientes pasos describen el proceso de securización de Microsoft Office 2016 en un cliente Windows 10 miembro de un dominio.

Paso	Descripción
51.	En el puesto de trabajo, equipo cliente miembro de dominio con Windows 10, preparado siguiendo las recomendaciones de la guía CCN-STIC-599A18, se procederá a iniciar sesión con una cuenta con los suficientes privilegios para ejecutar scripts. **Nota:** En este ejemplo se utiliza un cliente Windows 10 con un controlador de dominio Windows Server 2016 con las guías CCN-STIC-570A y CCN-STIC-599A18 con categoría básica aplicadas. Este entorno puede variar con la estructura de su organización.
52.	Cree el directorio “Scripts” en la unidad “C:\”.
53.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio **“C:\Scripts”**.
54.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.
55.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".

Paso	Descripción
56.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del cliente. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script **"CCN-STIC-585 ENS Dominio – Paso2.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.
57.	El control de cuentas de usuario le solicitará elevación de privilegios. Pulse "Sí" para continuar. 
58.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 

Paso	Descripción
59.	Se producirá la copia de un total de 22 ficheros. 
60.	Pulse cualquier tecla para continuar y finalizar la ejecución del *script*.
61.	Reinicie el equipo cliente.
62.	En este punto habrá quedado securizado MS Office 2016 en el equipo cliente.

ANEXO A.2.1.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016

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

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

a) En el controlador de dominio:
   i. Administración de directivas de grupo.
   ii. Editor de administración de directivas de grupo.

b) En el equipo cliente:
   i. Explorador de Windows.
   ii. PowerShell.
   iii. Símbolo del sistema.
   iv. Consola de servicios.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio con un administrador del dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. Este controlador de dominio deberá contener las plantillas de directivas de MS Office 2016.
2. Verifique que está creada la directiva		Utilizando la herramienta Administración de directivas de grupo (“**Inicio → Herramientas administrativas → Administración de directivas de grupo**”). Despliegue hasta llegar a la política **“CCN-STIC-585 ENS**

Comprobación	OK/NOK	Cómo hacerlo
de equipo (CCN-STIC-585 ENS Incremental Office 2016 categoria basica)		**Incremental Office 2016 categoria basica"** en la ruta "**Bosque:** ***[nombre de su bosque]*** → **Dominios** → ***[nombre de su dominio]*** → **Clientes Windows 10**". Pulsando el botón derecho sobre el objeto de política, deberá seleccionarse la opción "Editar". Se abrirá la herramienta "Editor de objetos de directiva de grupo" que permitirá verificar los valores de la directiva. **Nota:** En este ejemplo la directiva a comprobar está en la unidad organizativa "Clientes Windows 10". En el entorno de su organización puede variar.
3. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria basica"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de servicios de sistema dentro de: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"** **Nota:** Dependiendo de los servicios que estén instalados en el controlador de dominio utilizado para la verificación, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales.

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

4. Verifique los valores seguridad del sistema de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria basica"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración del equipo → Directivas → Plantillas administrativas → Microsoft Office 2016 (Equipo) → Configuración de seguridad"**

Directiva	Valor	OK/NOK
Deshabilitar el almacenamiento en caché de contraseñas	Habilitada	
Deshabilitar reparación de paquetes	Habilitada	

5. Verifique los valores de seguridad aplicados de Microsoft Excel 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria basica"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad"**

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="2"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Examinar macros cifradas en libros de formato Open XML de Excel</td><td>Habilitada (Examinar macros cifradas (predeterminado))</td><td></td></tr>
<tr><td rowspan="4">6. Verifique los valores del Centro de confianza de MS Excel 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Bloquear la ejecución de macros en archivos de Office procedentes de Internet</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">7. Verifique los valores de Ayuda de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Ayuda”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Búsqueda federada para obtener ayuda</td><td>Deshabilitada</td><td></td></tr>
</table>

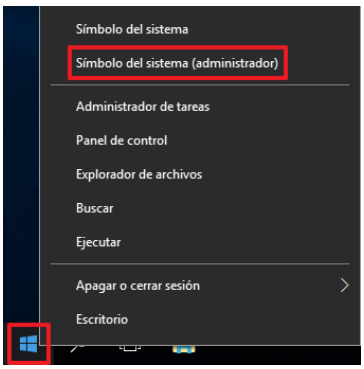
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="5">8. Verifique los valores de Configuración de seguridad de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Establecer longitud mínima de contraseña</td><td>Habilitada (8)</td><td></td></tr>
<tr><td colspan="2">Establecer nivel de reglas de contraseña</td><td>Habilitada (Comprobación de longitud local)</td><td></td></tr>
<tr><td colspan="2">Seguridad de automatización</td><td>Habilitada (Deshabilitar macros de forma predeterminada)</td><td></td></tr>
<tr><td rowspan="3">9. Verifique los valores de la primera vista de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Panel de telemetría”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Activar la recopilación de datos de telemetría</td><td>Deshabilitada</td><td></td></tr>
</table>

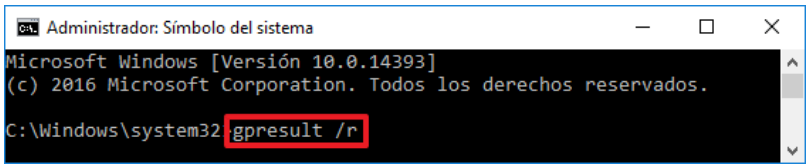
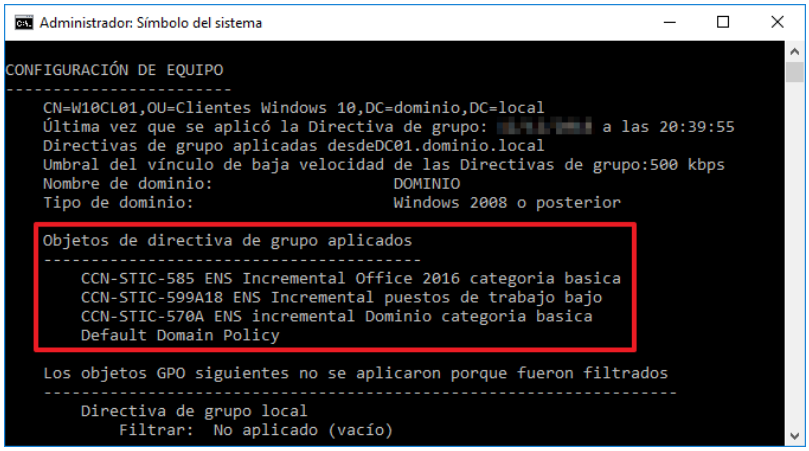
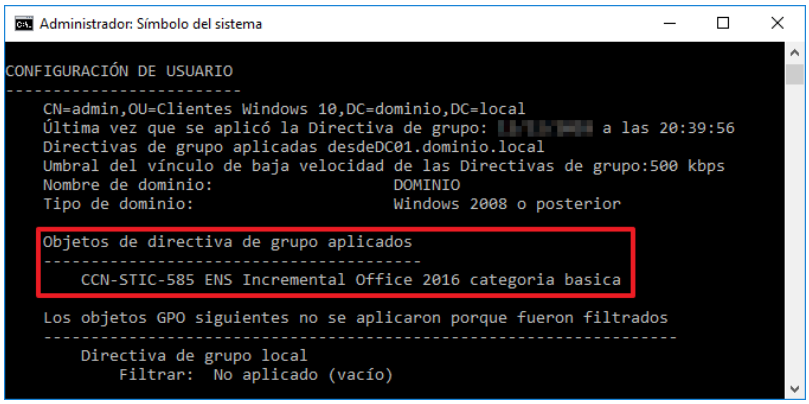
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="6">10. Verifique los valores centro de confianza de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Privacidad → Centro de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el Asistente para participar la primera vez que se ejecute</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Enviar comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Enviar información personal</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar programa de mejora de experiencia del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir la inclusión de capturas de pantalla con los comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="4">11. Verifique varios valores de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Varios”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Mostrar inicio de sesión OneDrive</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar las ubicaciones de archivos al abrir o guardar archivos</td><td>Habilitada (Ocultar OneDrive Personal, SharePoint Online y OneDrive para la Empresa)</td><td></td></tr>
</table>

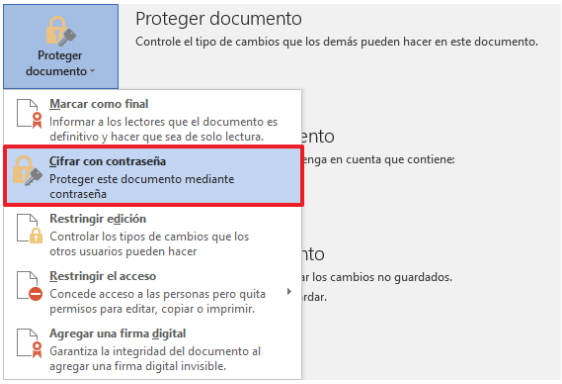
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3">12. Verifique los valores de seguridad de los cuadros de diálogo de estado de la firma de aplicación Microsoft Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro → Autoarchivar”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar Archivo/Archivar</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">13. Verifique los valores de seguridad de Microsoft PowerPoint 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Varios → Configuración PST”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que los usuarios agreguen archivos PST a perfiles de Outlook y/o evitar el uso de archivos PST para compartirlos de manera exclusiva</td><td>Habilitada (se pueden agregar archivos PST)</td><td></td></tr>
<tr><td colspan="2">Impedir a los usuarios agregar nuevo contenido a archivos PST existentes</td><td>Habilitada</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique que están configurados los servicios de MS Office 2016		Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador. Ejecute la herramienta "Windows PowerShell" con privilegios de administrador. Para ello vaya a la siguiente ruta: **"Menú inicio → Todos los programas → Accesorios → Windows PowerShell"** Seleccione mediante botón derecho en Windows PowerShell la opción **"Ejecutar como administrador"**. En la shell abierta ejecute **services.msc**. Compruebe que los siguientes servicios se encuentran configurados en modo manual: – Office Source Engine – Servicio de caché de fuentes de Windows – Servicio Hacer clic y ejecutar de Microsoft Office **Nota:** Dependiendo de la versión de Office instalada puede aparecer el servicio "OSE" o "OSE64" y puede no aparecer el servicio "ClickToRunSvc".

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

15. Inicie sesión con un usuario al que le apliquen las directivas de Office.		Inicie sesión con un usuario cuya cuenta se encuentre dentro del grupo de seguridad "ENS usuarios Office 2016 categoria basica" y permisos de administrador.
16. Ejecute una consola de comandos		Ejecute con permisos de administrador una consola de comandos. Para ello pulse con botón derecho sobre el botón de inicio y seleccione "Símbolo del sistema (administrador)".  **Nota:** El sistema le solicitará elevación de privilegios.

Comprobación	OK/NOK	Cómo hacerlo
17. Compruebe que se aplican las GPO de seguridad en el cliente.		Introduzca “gpresult /r” y pulse “Enter” para verificar que se están aplicando las políticas de grupo.  Confirme que aparece en los apartados de equipo y usuario la GPO “CCN-STIC-585 ENS Incremental Office 2016 categoria basica”.  
18. Compruebe que las aplicaciones de MS Office 2016 funcionan correctamente		Pruebe a abrir alguna de las aplicaciones de MS Office 2016, como, por ejemplo, MS Word, MS Excel o MS PowerPoint. Compruebe que puede crear un nuevo documento y guardarlo.

Comprobación	OK/NOK	Cómo hacerlo
19. Compruebe que puede proteger un documento con contraseña y que esta es robusta.		Proteja un documento con contraseña. Para ello acceda al menú "**Archivo → Información → Proteger documento → Cifrar con contraseña**".  Compruebe que no puede introducir una contraseña inferior a 8 caracteres.
20. Compruebe los metadatos de los archivos.		Abra cualquiera de las aplicaciones de la *suite* Office, por ejemplo Word, seleccione comenzar un documento en blanco y vaya al menú "**Archivo → Información → Propiedades**" y compruebe que los datos corresponden a los del usuario que inició la sesión. 

ANEXO A.2.2. CATEGORÍA MEDIA

ANEXO A.2.2.1. GUÍA PASO A PASO DE IMPLEMENTACIÓN SEGURA

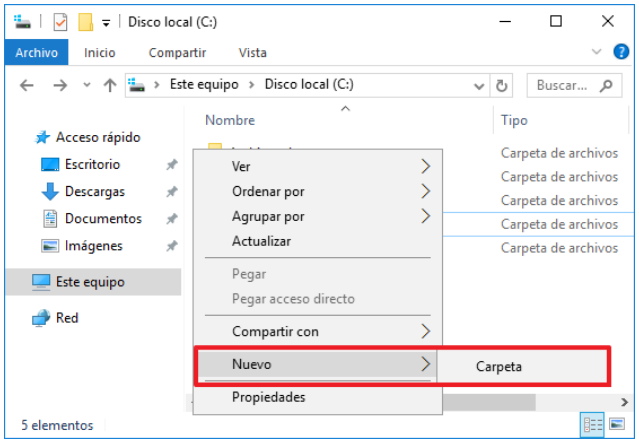
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen la suite de Microsoft Office 2016 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

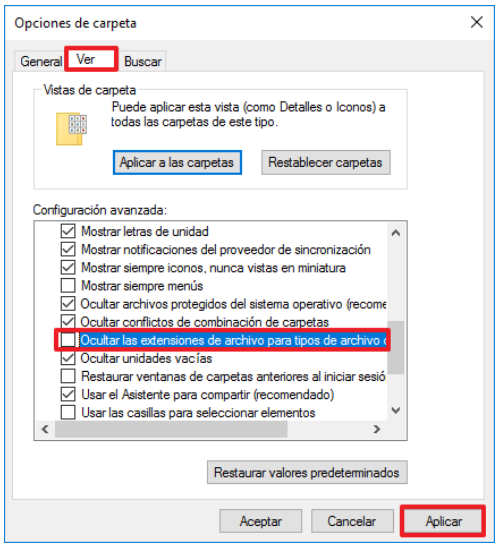
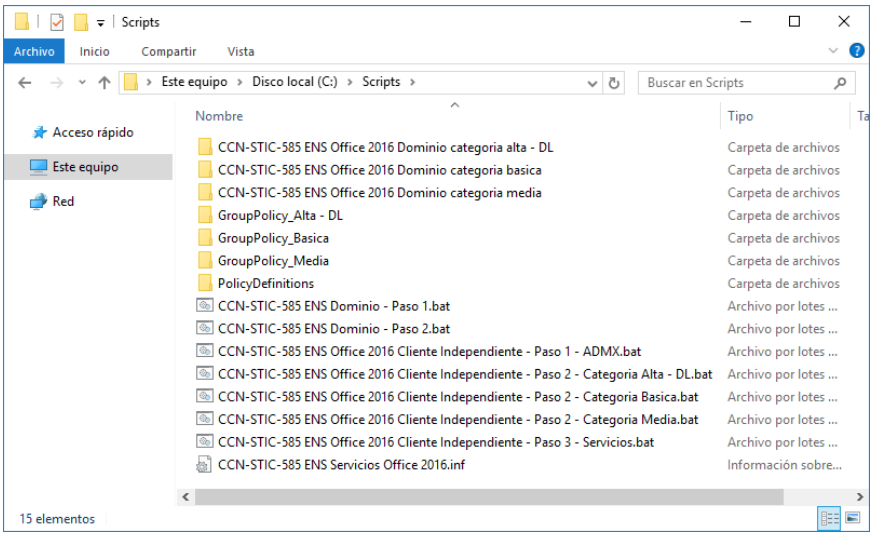
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

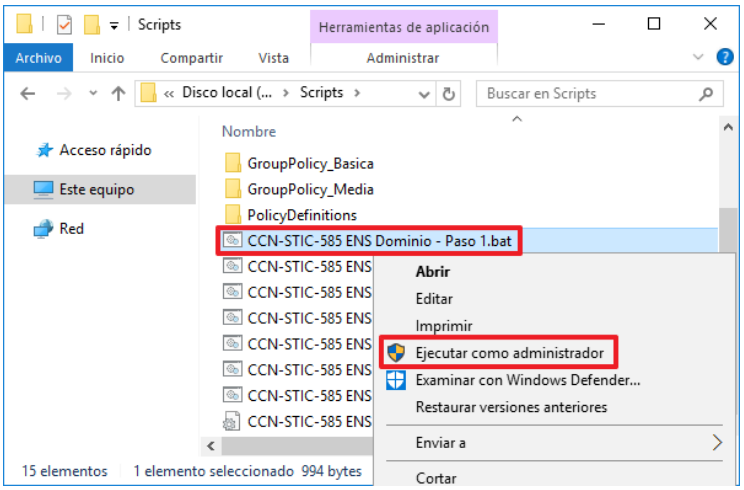
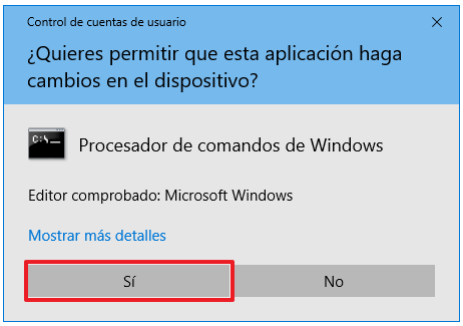
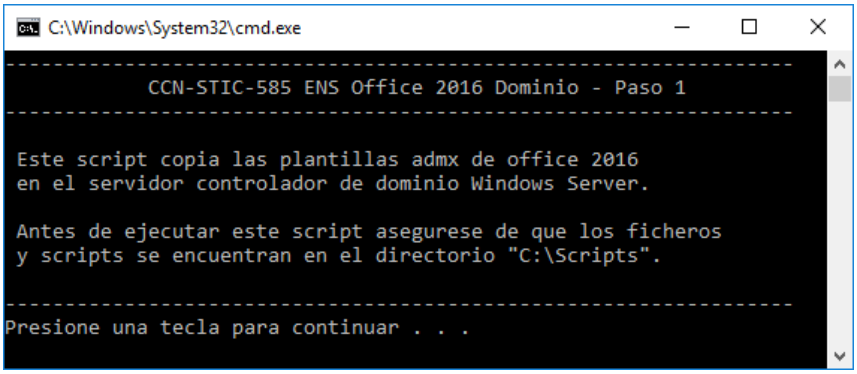
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

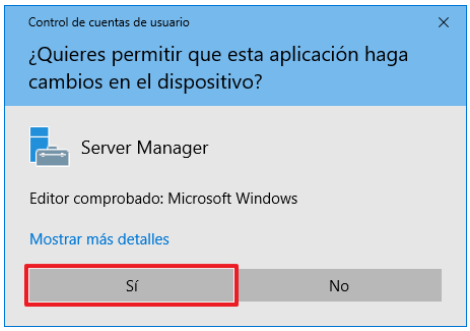
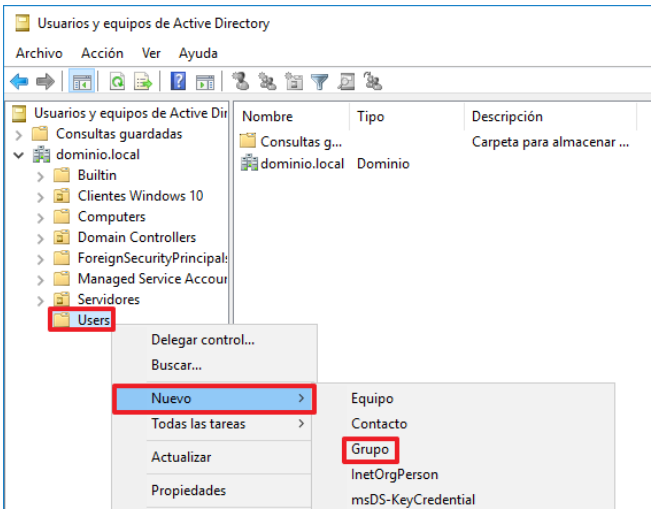
1. PREPARACIÓN DEL DIRECTORIO ACTIVO

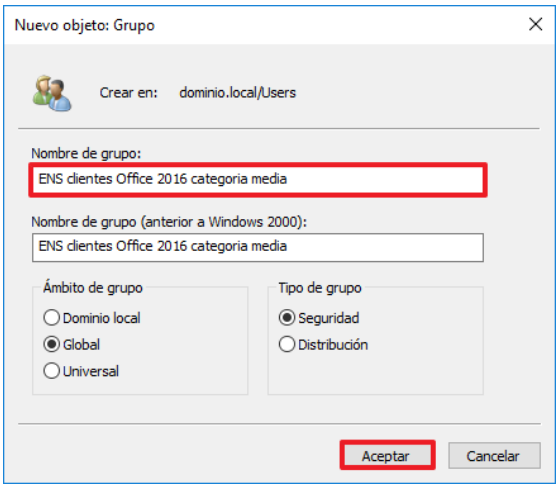
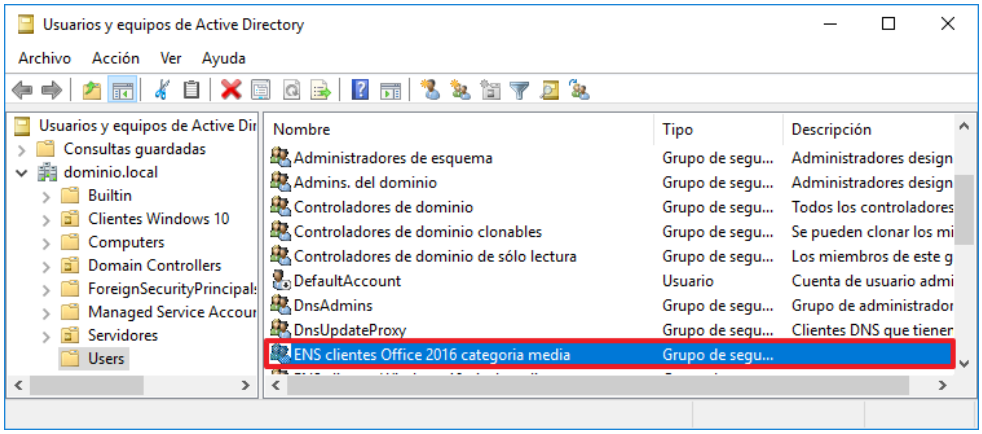
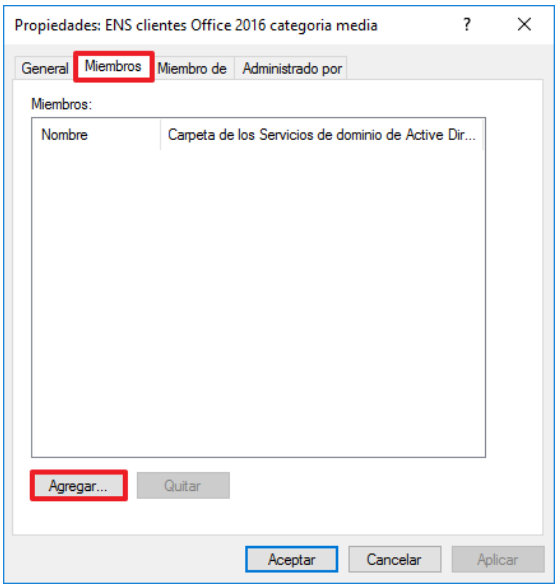
Los pasos que se describen a continuación se realizarán en un controlador de dominio, de la infraestructura a la que pertenecen los clientes en los que se va a securizar MS Office 2016.

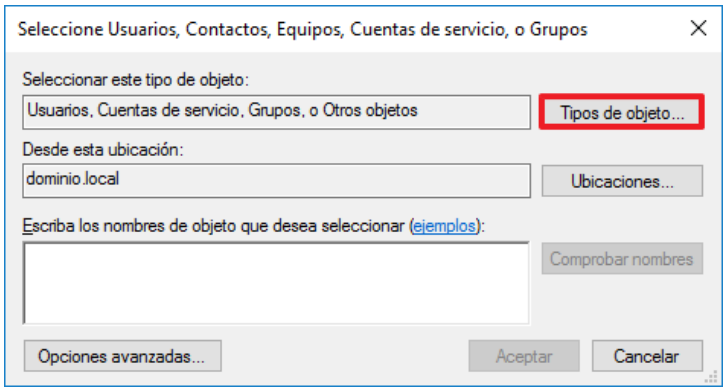
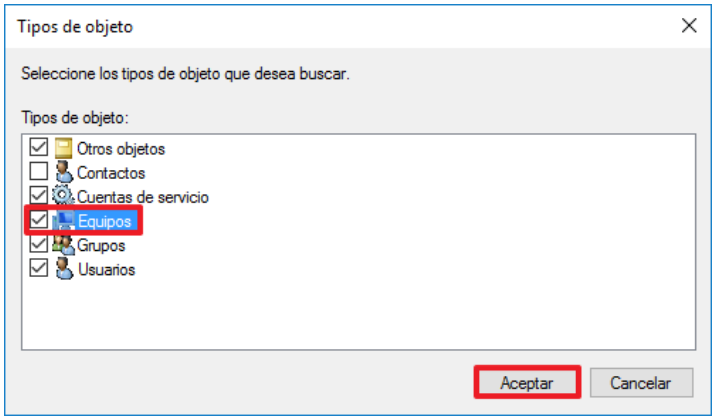
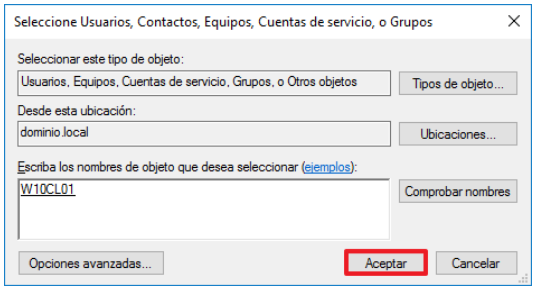
Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta que sea miembro del grupo “Admins. del domino” del dominio al que pertenecen los clientes donde se va a securizar MS Office 2016. **Nota:** En este ejemplo se utiliza un cliente Windows 10 con un controlador de dominio Windows Server 2016 con las guías CCN-STIC-570A y CCN-STIC-599A18 con categoría media aplicadas. Este entorno puede variar con la estructura de su organización.
2.	Cree el directorio “Scripts” en la unidad “C:\”. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo → Carpeta”.** 
3.	Asigne el nombre “Scripts” al nuevo directorio.
4.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.

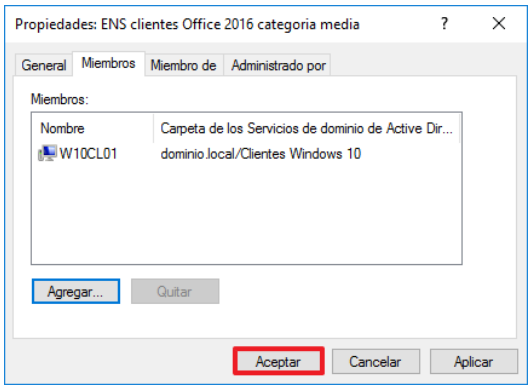
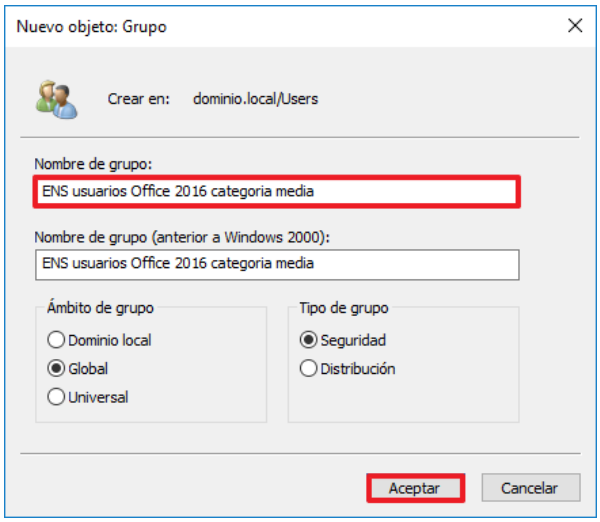
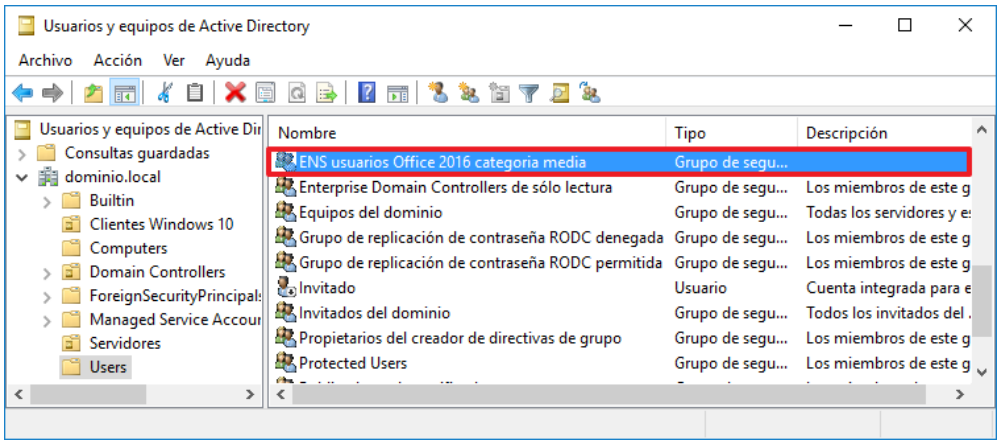
Paso	Descripción
5.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".
6.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”. 

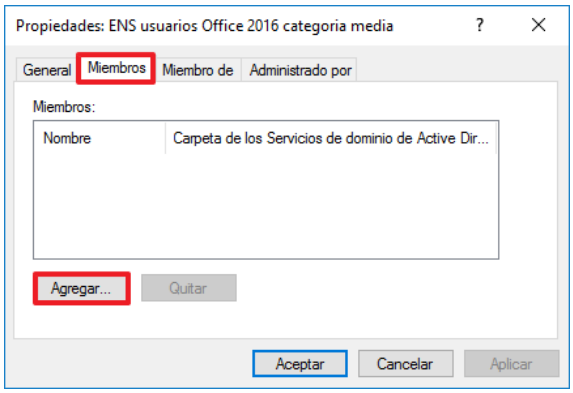
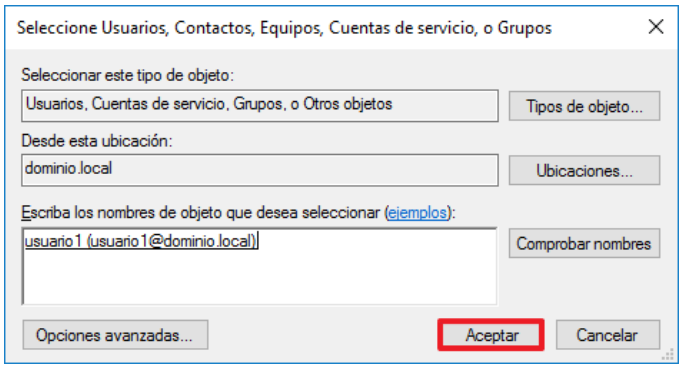
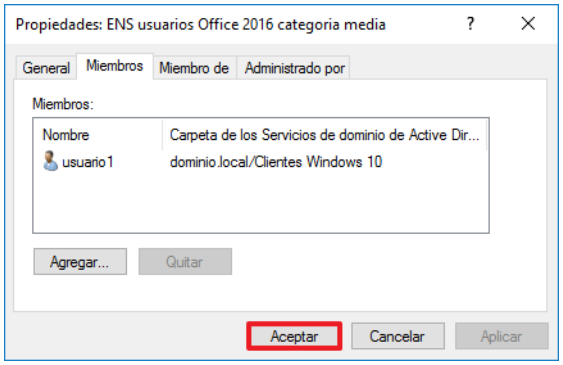
Paso	Descripción
7.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del servidor, de tal forma que se podrán realizar modificaciones, desde dicha máquina, de las políticas generadas. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script **"CCN-STIC-585 ENS Dominio - Paso1.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.
8.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Pulse "Sí" para continuar. 
9.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 

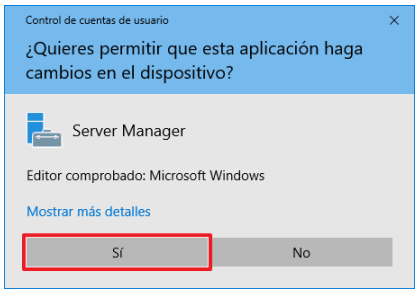
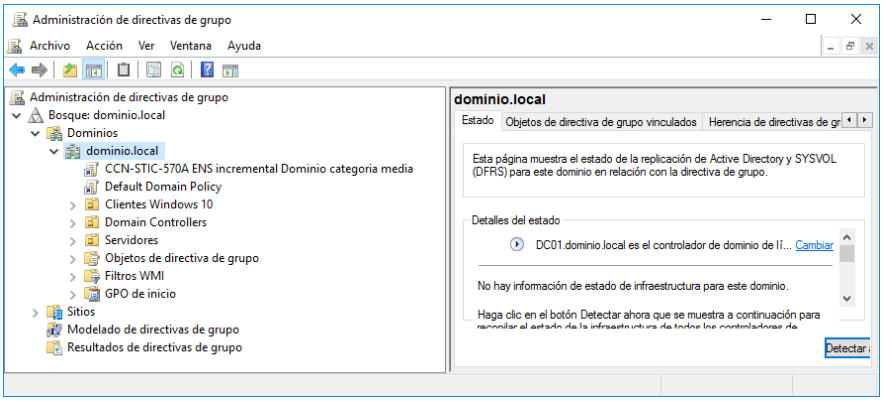
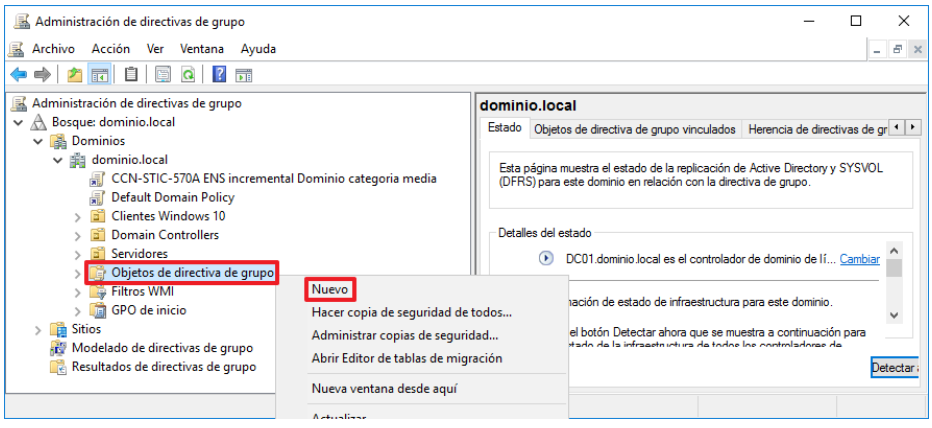
Paso	Descripción
10.	Inicie la herramienta "Usuarios y equipos de Active Directory", para ello ejecute la herramienta Administrador del servidor (**Inicio → Administrador del servidor**). Seleccione en el menú superior **"Herramientas → Usuarios y equipos de Active Directory"**. **Nota:** Los siguientes pasos describen el procedimiento para crear grupos de seguridad donde agregar los puestos de trabajo y usuarios 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 o los usuarios se encuentren en la ubicación predeterminada de "Computers" o "Users" 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.
11.	El control de cuentas de usuario le solicitará elevación de privilegios. Pulse "Sí" para continuar. 
12.	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"**. 

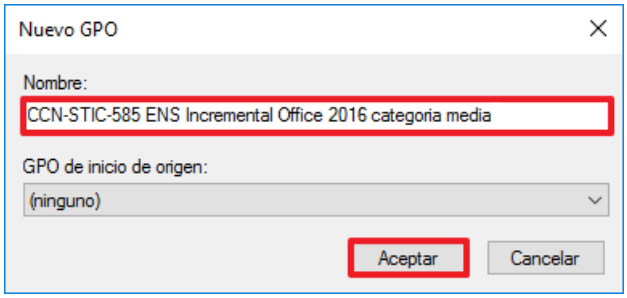
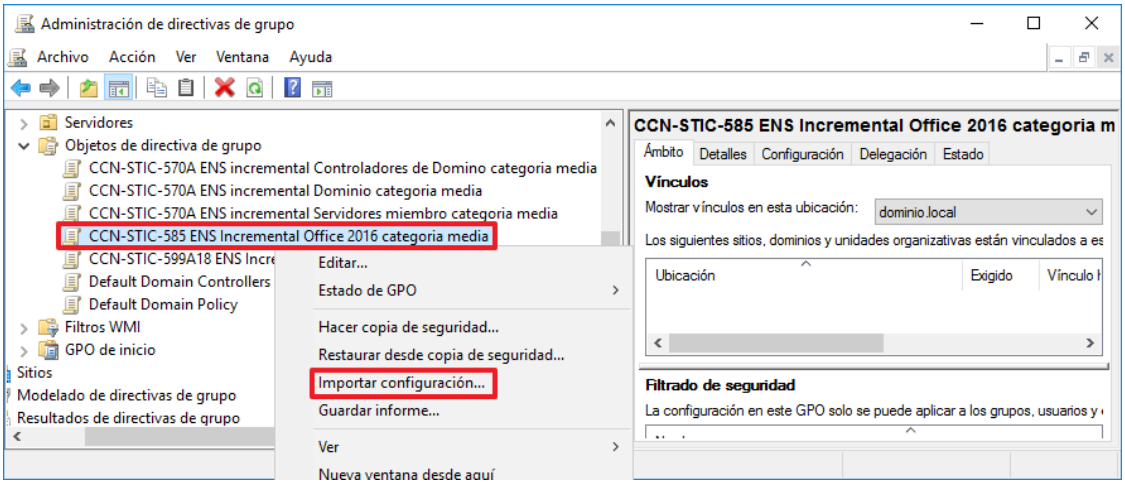
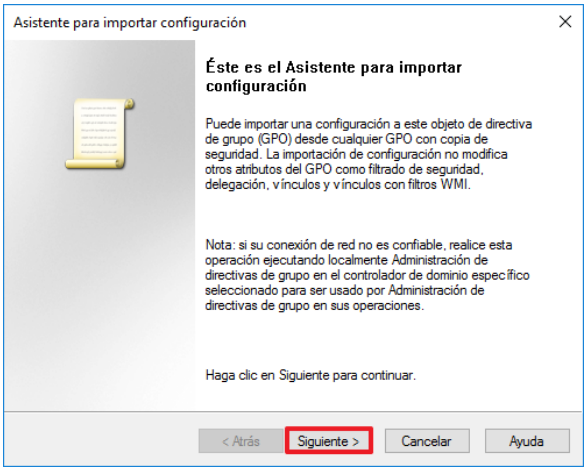
Paso	Descripción
13.	Introduzca como nombre “ENS clientes Office 2016 categoria media”. No modifique el resto de opciones y pulse el botón “Aceptar”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre clientes que vayan a usar Office 2016. 
14.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
15.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar…”. 

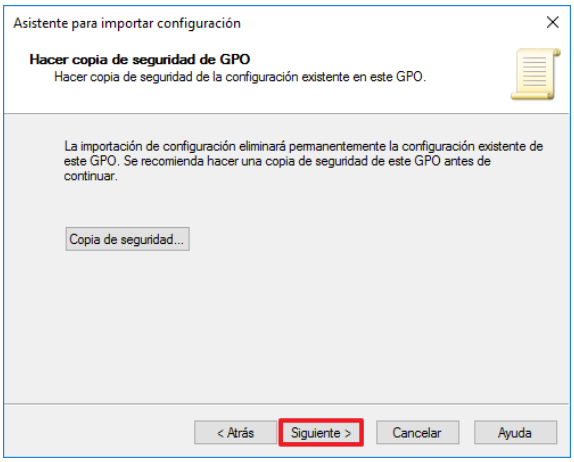
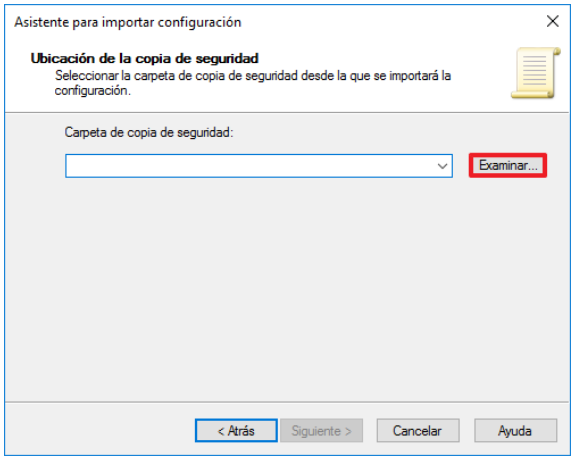
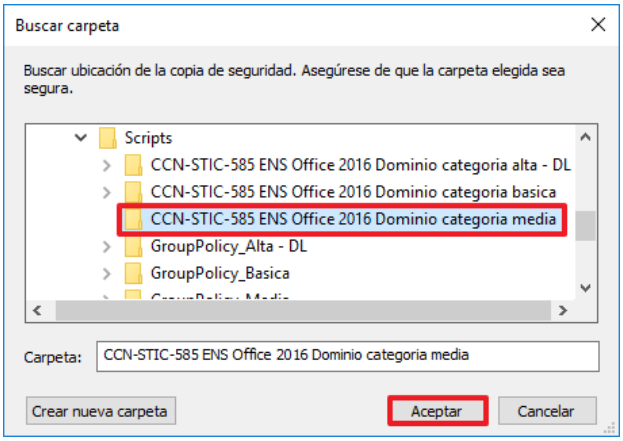
Paso	Descripción
16.	Pulse sobre “Tipos de objeto…” 
17.	Marque la opción “Equipos” y pulse “Aceptar”. 
18.	Introduzca el nombre de los equipos o utilice las opciones avanzadas para agregar todos aquellos equipos que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad media que vayan a hacer uso de Office 2016 y pulse “Aceptar” para agregar la selección.  **Nota:** En este ejemplo se usa el equipo “W10CL01”, deberá introducir los equipos acordes a su organización.

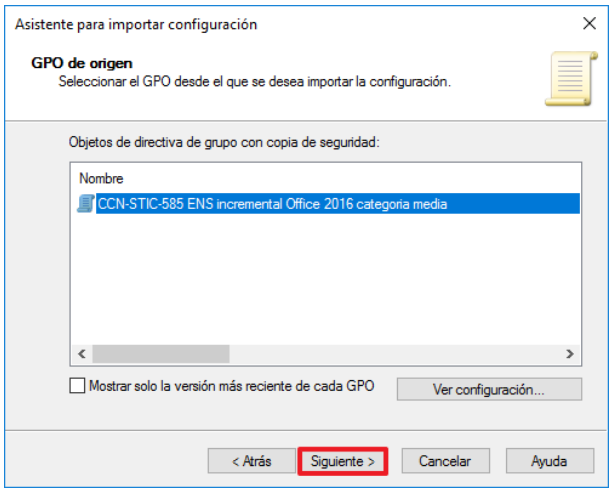
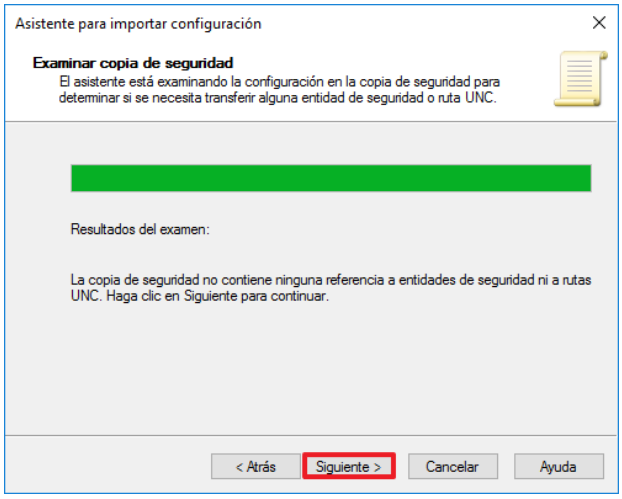
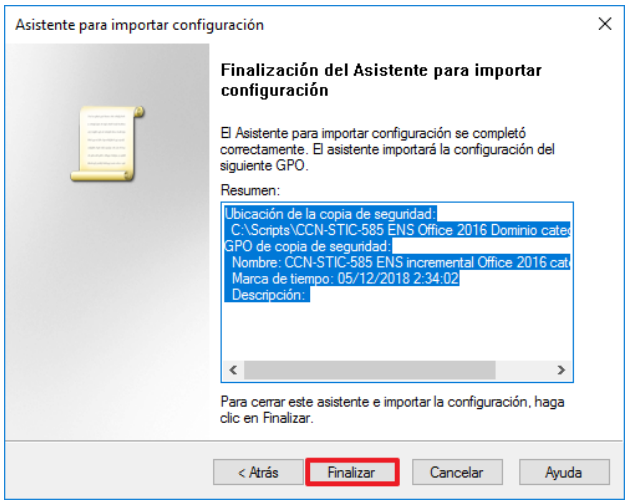
Paso	Descripción
19.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
20.	De manera análoga, cree un nuevo grupo con nombre “ENS usuarios Office 2016 categoria media”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre usuarios que vayan a usar Office 2016. 
21.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 

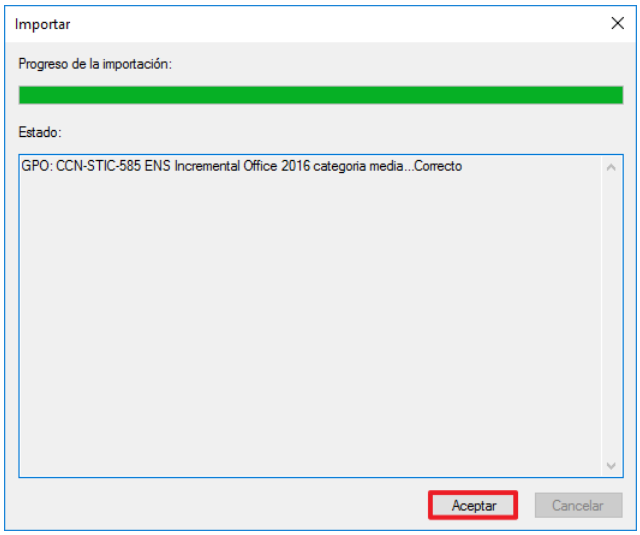
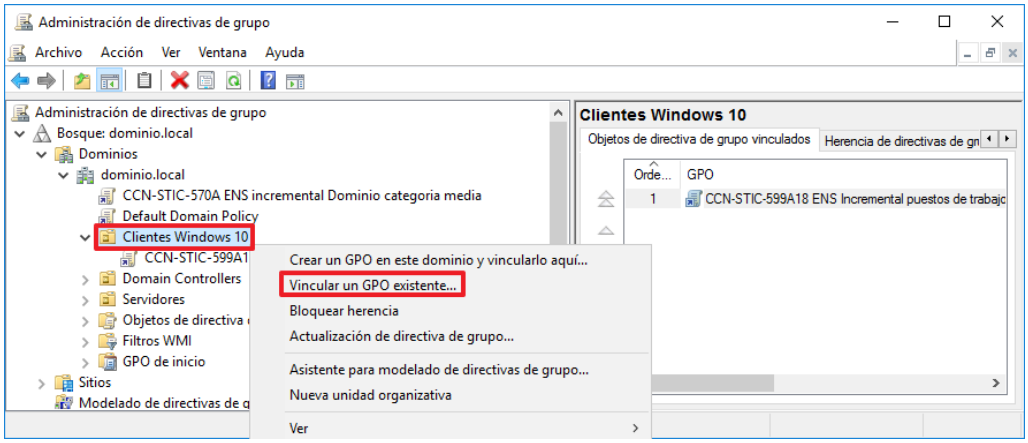
Paso	Descripción
22.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar…”. 
23.	Introduzca el nombre de los usuarios o utilice las opciones avanzadas para agregar todos aquellos usuarios que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad media que vayan a hacer uso de Office 2016 y pulse “Aceptar” para agregar la selección.  **Nota:** En este ejemplo se usa el usuario “usuario1”, deberá introducir los usuarios acordes a su organización. Recuerde que dichos usuarios deberán situarse en la unidad organizativa donde se vaya a implementar la seguridad.
24.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 
25.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
26.	Inicie la herramienta de administración de directivas de grupo, para ello ejecute la herramienta Administrador del servidor (**Inicio → Administrador del servidor**). Seleccione en el menú superior **"Herramientas → “Administrador de directivas de grupo”**.

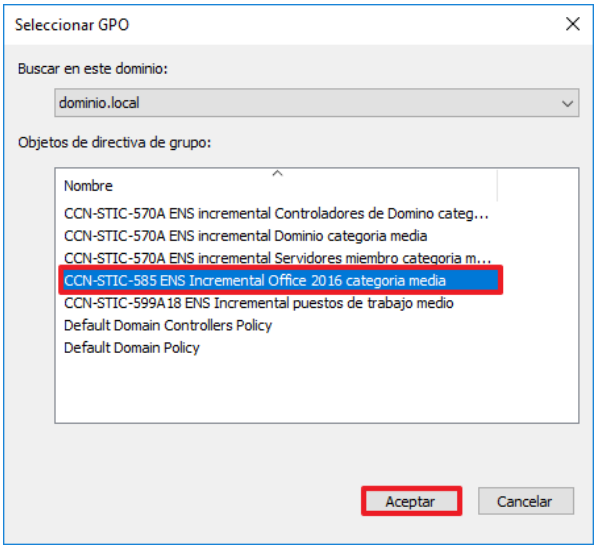
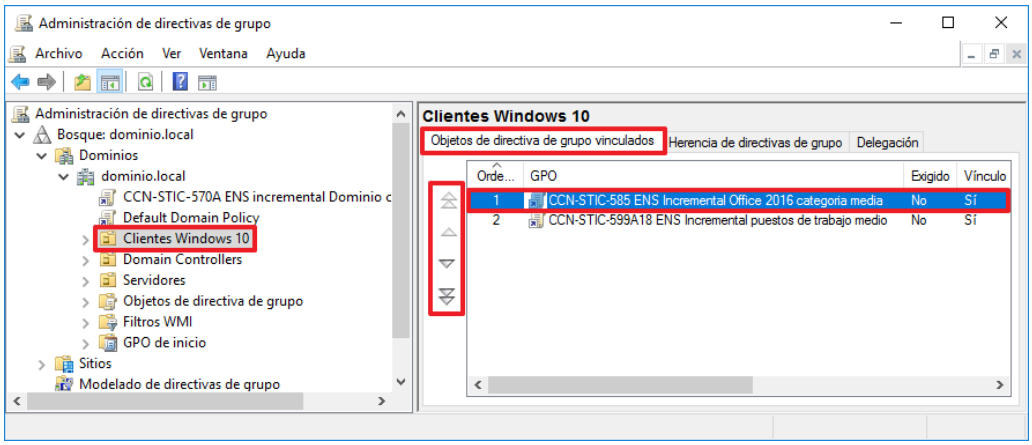
Paso	Descripción
27.	El control de cuentas de usuario le solicitará elevación de privilegios. Pulse “Sí” para continuar. 
28.	Expanda el contenedor **“Administración de directivas de grupo → Bosque:<nombre de su bosque> → Dominios → *[nombre de su dominio]*”**, como se muestra en la siguiente imagen.  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 del recién expandido (*[nombre de su dominio]*). **Nota:** En este ejemplo se utiliza como nombre de dominio “dominio.local”.
29.	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. 

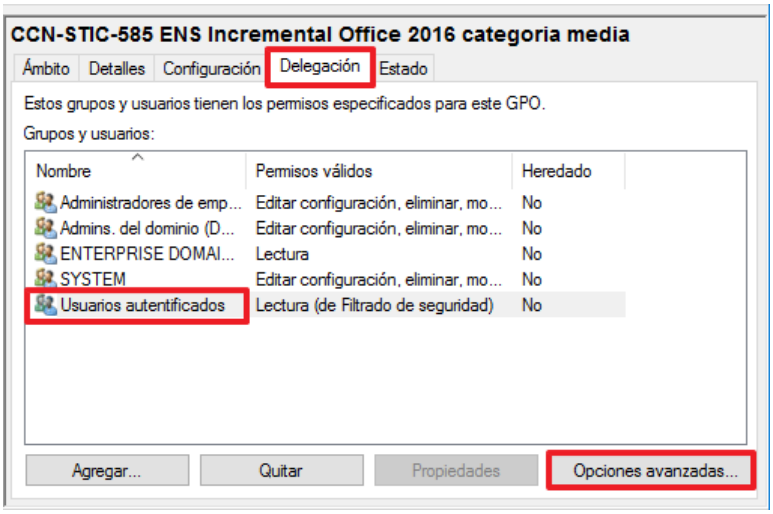
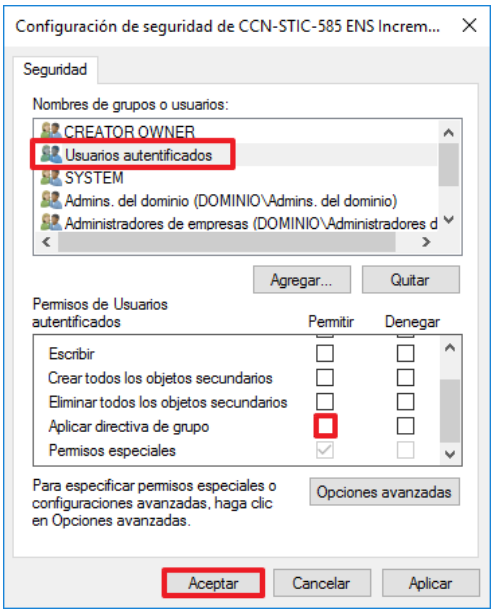
Paso	Descripción
30.	Asigne el siguiente nombre a la nueva política, GPO, que se está creando: "CCN-STIC-585 ENS Incremental Office 2016 categoria media" y pulse "Aceptar". 
31.	Seleccione el objeto de directiva de grupo, GPO, recién creado y marcando con el botón derecho en ella, elija la opción "Importar configuración" del menú contextual que aparecerá. 
32.	Se iniciará el asistente para la importación de configuración, pulse el botón "Siguiente >". 

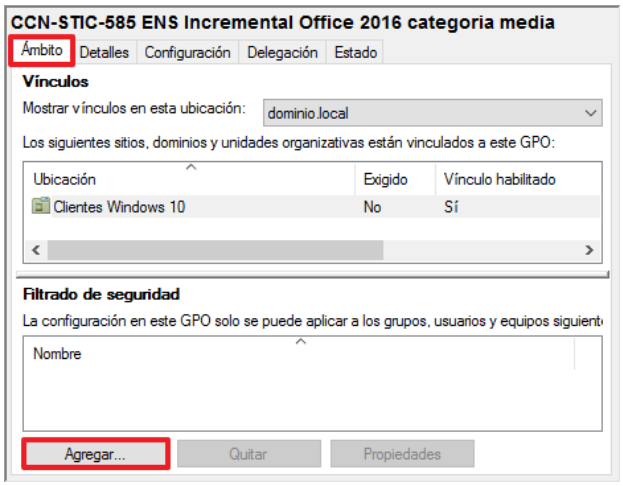
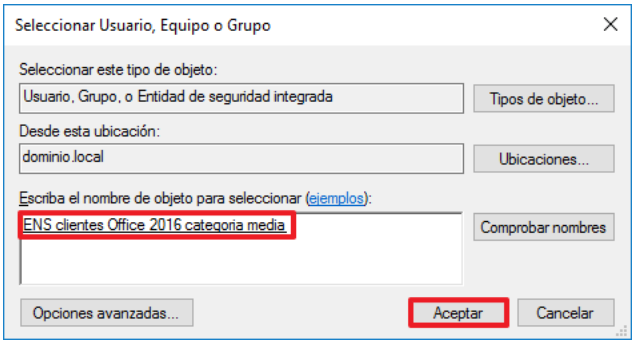
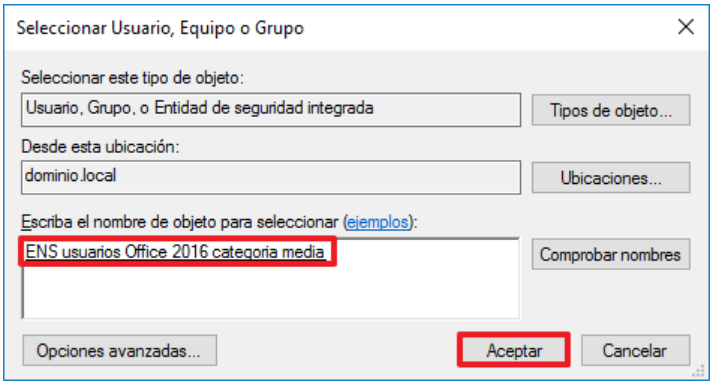
Paso	Descripción
33.	El asistente para la importación de la configuración ofrecerá la opción de realizar una copia de seguridad de la configuración actual de la GPO. Como la política se encuentra vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón “Siguiente >” 
34.	A continuación, deberá seleccionar la carpeta de copia de seguridad desde la que se importará la configuración. Seleccione el botón “Examinar…”. 
35.	Busque y seleccione la carpeta “**C:\Scripts\CCN-STIC-585 ENS Office 2016 Dominio categoria media”**. Pulse el botón “Aceptar” y volverá a la ventana del asistente. Pulse el botón “Siguiente >”. 

Paso	Descripción
36.	Deberá indicarse el objeto GPO desde el que desea importar la configuración. Pulse “Siguiente >”. 
37.	El asistente procederá a realizar una verificación de la configuración de la copia de seguridad. Pulse el botón “Siguiente >”. 
38.	El asistente para importar la configuración mostrará, entonces, una ventana resumen con los datos de la importación que se va a realizar. Pulse el botón “Finalizar”. 

Paso	Descripción
39.	El asistente procederá a realizar la importación. Pulse “Aceptar”. Con ello habrá quedado importada la configuración de la nueva política generada, estando lista para ser asignada a la unidad organizativa de usuarios creada en pasos anteriores, cuestión que se realizará a continuación. 
40.	Expanda y seleccione el contenedor de usuarios en la unidad organizativa donde tenga alojada la configuración de los clientes, **“Menú inicio → Herramientas administrativas → Administración de directivas de grupo → Bosque: *[nombre de su bosque]* → Dominios → *[nombre de su dominio]* → Clientes Windows 10”**, y márquelo con el botón derecho del ratón, seleccione la opción “Vincular un GPO existente…”  **Nota:** En este caso, el nombre del bosque y del dominio es “dominio.local” y las unidades organizativas fueron creadas durante el proceso de instalación de equipos Windows 10 dentro de un dominio, según la guía CCN-STIC-599A18. Si todos los equipos y usuarios a los que va a aplicar esta configuración no se encuentran en esta unidad organizativa deberá vincular la GPO a nivel de dominio.

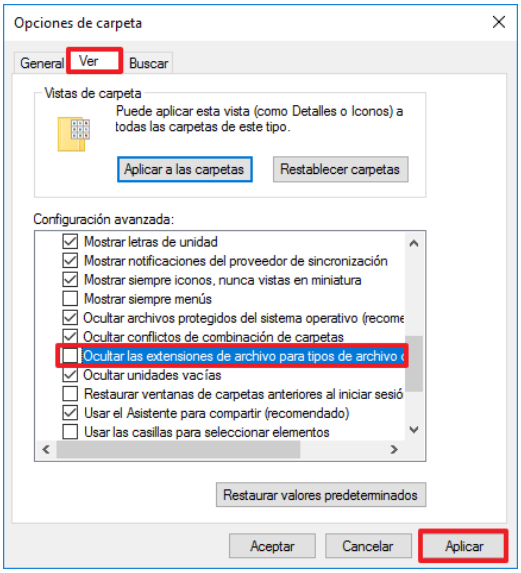
Paso	Descripción
41.	En la ventana que aparece, seleccione el GPO “CCN-STIC-585 ENS Incremental Office 2016 categoria media” y pulse el botón “Aceptar”. 
42.	El objeto de directiva de grupo, GPO, habrá quedado vinculado a la unidad organizativa “Clientes Windows 10”.
43.	Ahora, se determinará el orden de los vínculos. Deberá quedar, la nueva directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”, en la primera posición para asegurar un resultado adecuado en la aplicación. Para ello, se deben utilizar las flechas de posicionamiento de la ficha “Objetos de directiva de grupo vinculados” de la unidad organizativa “Clientes Windows 10”. 

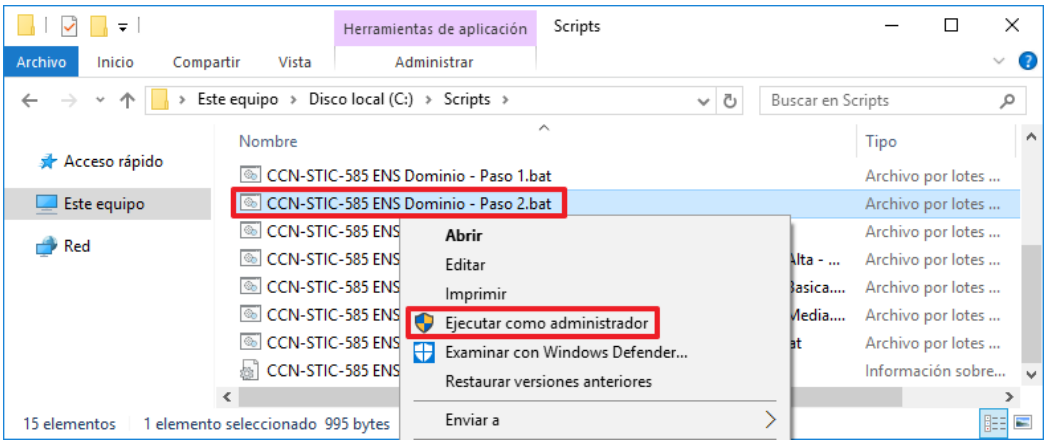
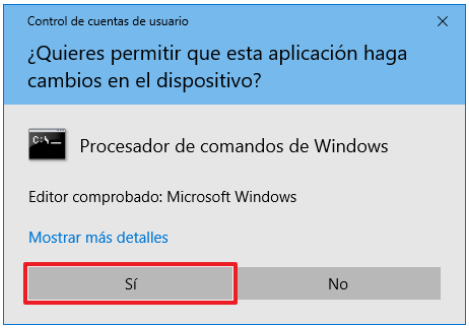
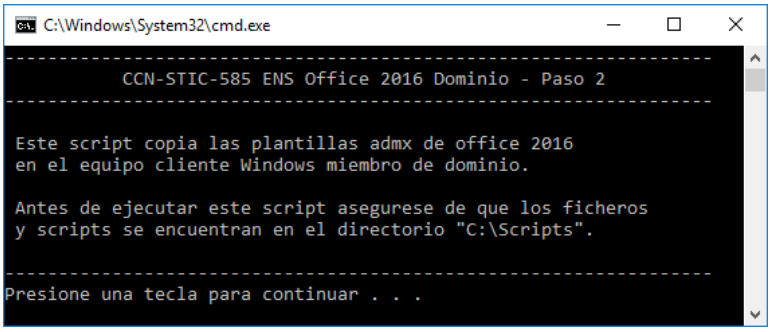
Paso	Descripción
44.	Seleccione la nueva GPO configurada. Vaya a las opciones de delegación que se encuentran en el panel derecho y seleccione “Usuarios autentificados” y pulse sobre el botón “Opciones avanzadas…”.  **Nota:** En el caso de que todos los equipos y usuarios cliente vayan a tener instalado Office 2016 puede mantener el grupo del sistema “Usuarios autentificados” sin cambios y saltar al paso 49.
45.	Seleccione “Usuarios autentificados” y sitúese en la ventana inferior de “Permisos de Usuarios autentificados”, quite el check permitir correspondiente a “Aplicar directiva de grupo”. 

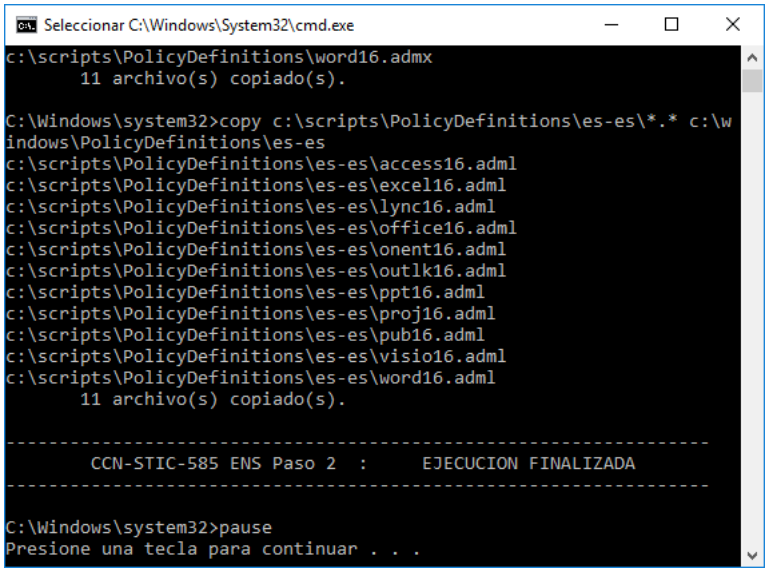
Paso	Descripción
46.	Vaya a la pestaña “Ámbito” y pulse sobre el botón “Agregar…”. 
47.	Introduzca como nombre “ENS clientes Office 2016 categoria media”. A continuación, pulse el botón “Aceptar”. 
48.	De manera análoga, introduzca el grupo “ENS usuarios Office 2016 categoria media” y pulse “Aceptar”. Estos grupos corresponden con los generados en pasos previos. 
49.	El objeto de directiva de grupo, GPO, habrá quedado configurada correctamente. **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
50.	Elimine la carpeta **“C:\Scripts”** del servidor.

2. PREPARACIÓN DEL CLIENTE PARA LA SECURIZACIÓN DE MS OFFICE 2016 EN UN EQUIPO DEL DOMINIO

Los siguientes pasos describen el proceso de securización de Microsoft Office 2016 en un cliente Windows 10 miembro de un dominio.

Paso	Descripción
51.	En el puesto de trabajo, equipo cliente miembro de dominio con Windows 10, preparado siguiendo las recomendaciones de la guía CCN-STIC-599A18, se procederá a iniciar sesión con una cuenta con los suficientes privilegios para ejecutar scripts. **Nota:** En este ejemplo se utiliza un cliente Windows 10 con un controlador de dominio Windows Server 2016 con las guías CCN-STIC-570A y CCN-STIC-599A18 con categoría media aplicadas. Este entorno puede variar con la estructura de su organización.
52.	Cree el directorio “Scripts” en la unidad “C:\”.
53.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio **“C:\Scripts”**.
54.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.
55.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".

Paso	Descripción
56.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del cliente. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script **"CCN-STIC-585 ENS Dominio – Paso2.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.
57.	El control de cuentas de usuario le solicitará elevación de privilegios. Pulse "Sí" para continuar. 
58.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 

Paso	Descripción
59.	Se producirá la copia de un total de 22 ficheros: 
60.	Pulse cualquier tecla para continuar y finalizar la ejecución del *script*.
61.	Reinicie el equipo cliente.
62.	En este punto habrá quedado securizado MS Office 2016 en el equipo cliente.

ANEXO A.2.2.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016

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

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

a) En el controlador de dominio:
   i. Administración de directivas de grupo.
   ii. Editor de administración de directivas de grupo.

b) En el equipo cliente:
   i. Explorador de Windows.
   ii. PowerShell.
   iii. Símbolo del sistema.
   iv. Consola de servicios.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio con un administrador del dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. Este controlador de dominio deberá contener las plantillas de directivas de MS Office 2016.
2. Verifique que está creada la directiva		Utilizando la herramienta Administración de directivas de grupo (“**Inicio → Herramientas administrativas → Administración de directivas de grupo**”). Despliegue hasta llegar a la política **“CCN-STIC-585 ENS**

Comprobación	OK/NOK	Cómo hacerlo
de equipo (CCN-STIC-585 ENS Incremental Office 2016 categoria media)		**Incremental Office 2016 categoria media"** en la ruta "**Bosque: *[nombre de su bosque]* → Dominios → *[nombre de su dominio]* → Clientes Windows 10**". Pulsando el botón derecho sobre el objeto de política, deberá seleccionarse la opción "Editar". Se abrirá la herramienta "Editor de objetos de directiva de grupo" que permitirá verificar los valores de la directiva. **Nota:** En este ejemplo la directiva a comprobar está en la unidad organizativa "Clientes Windows 10". En el entorno de su organización puede variar.

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique los valores de los servicios del sistema de la directiva ”CCN-STIC-585 ENS Incremental Office 2016 categoria media”		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de servicios de sistema dentro de: **“Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”** **Nota:** Dependiendo de los servicios que estén instalados en el controlador de dominio utilizado para la verificación, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales.

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

4. Verifique los valores seguridad del sistema de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **“Configuración del equipo → Directivas → Plantillas administrativas → Microsoft Office 2016 (Equipo) → Configuración de seguridad”**

Directiva	Valor	OK/NOK
Deshabilitar el almacenamiento en caché de contraseñas	Habilitada	
Deshabilitar reparación de paquetes	Habilitada	

5. Verifique los valores de seguridad aplicados de Microsoft Excel 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad”**

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	**Valor**	**OK/NOK**
		Examinar macros cifradas en libros de formato Open XML de Excel	Habilitada (Examinar macros cifradas (predeterminado))	
6. Verifique los valores del Centro de confianza de MS Excel 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria media"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza"**		
		Directiva	**Valor**	**OK/NOK**
		Bloquear la ejecución de macros en archivos de Office procedentes de Internet	Habilitada	
7. Verifique los valores de la Vista protegida de MS Excel 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria media"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza → Vista protegida"**		
		Directiva	**Valor**	**OK/NOK**
		Abrir archivos de UNC de intranet local en Vista protegida	Deshabilitada	
		Desactivar Vista protegida para los datos adjuntos abiertos en Outlook	Deshabilitada	
		Establecer el comportamiento del documento en caso de error en la validación de documento	Habilitado (Bloquear archivos, No permitir edición)	
		No abrir archivos de la zona de Internet en Vista protegida	Deshabilitado	
		No abrir archivos de ubicaciones inseguras en Vista protegida	Deshabilitado	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="2">8. Verifique los valores de Varios de MS Excel 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Varios”</td></tr>
<tr><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>No almacenar archivos de red en la memoria caché local</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">9. Verifique los valores de Ayuda de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Ayuda”</td></tr>
<tr><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Búsqueda federada para obtener ayuda</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">10. Verifique los valores de Configuración de seguridad de MS Office 2016 de la directiva “CCN-STIC-585 Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad”</td></tr>
<tr><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Establecer longitud mínima de contraseña</td><td>Habilitada (10)</td><td></td></tr>
<tr><td>Establecer nivel de reglas de contraseña</td><td>Habilitada (Comprobación de longitud local)</td><td></td></tr>
<tr><td>Seguridad de automatización</td><td>Habilitada (Deshabilitar macros de forma predeterminada)</td><td></td></tr>
</table></td></tr>
<tr><td rowspan="2">11. Verifique los valores de Catálogos de confianza de MS Office 2016 de la directiva “CCN-STIC-585 Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad → Centro de confianza → Catálogos de confianza”</td></tr>
<tr><td colspan="4"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Bloquear complementos web</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

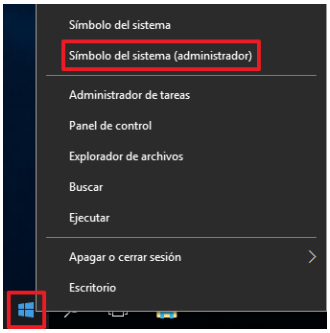
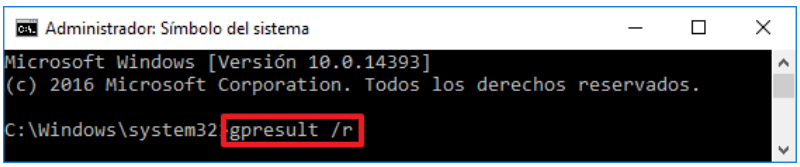
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="2">Bloquear Tienda Office</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">12. Verifique los valores de Contenido en línea de MS Office 2016 de la directiva “CCN-STIC-585 Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Herramientas | Opciones | General | Opciones de servicios… → Contenido en línea”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Opciones de contenido en línea</td><td>Habilitada (No permitir que Office se conecte a Internet)</td><td></td></tr>
<tr><td colspan="2">Opciones de nivel de servicio</td><td>Habilitada (Solo servicios de Microsoft)</td><td></td></tr>
<tr><td rowspan="3">13. Verifique los valores del Panel de telemetría de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Panel de telemetría”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Activar la recopilación de datos de telemetría</td><td>Deshabilitada</td><td></td></tr>
</table>

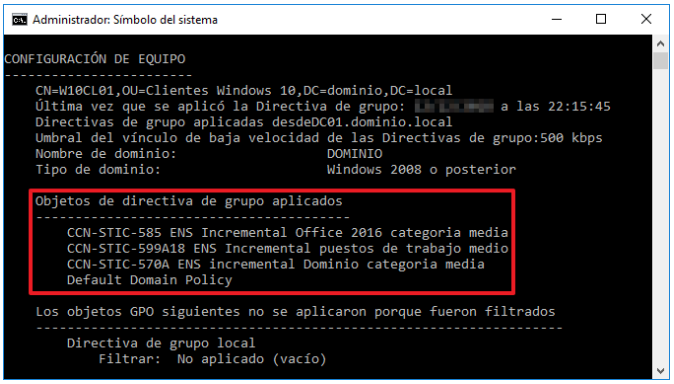
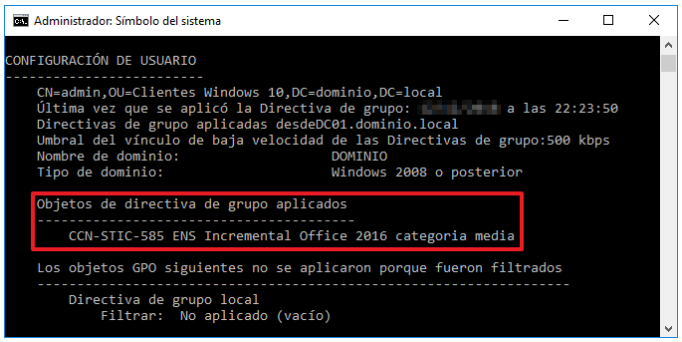
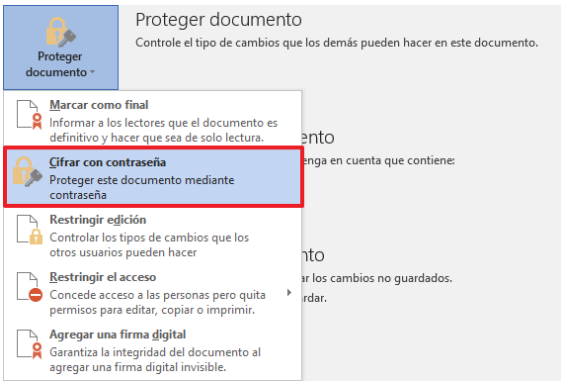
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="6">14. Verifique los valores del Centro de confianza de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Privacidad → Centro de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el Asistente para participar la primera vez que se ejecute</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Enviar comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Enviar información personal</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar programa de mejora de experiencia del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir la inclusión de capturas de pantalla con los comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="5">15. Verifique los valores de varios de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Varios”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Mostrar características de LinkedIn en aplicaciones de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Mostrar inicio de sesión OneDrive</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar las ubicaciones de archivos al abrir o guardar archivos</td><td>Habilitada (Ocultar OneDrive Personal, SharePoint Online y OneDrive para la Empresa)</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3">16. Verifique las opciones de Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Ocultar el botón de Tienda Office</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">17. Verifique los valores de autoarchivar de Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro → Autoarchivar”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar Archivo/Archivar</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">18. Verifique los valores de seguridad de criptografía de Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Seguridad → Criptografía”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Advertencia de firma</td><td>Habilitada (Advertir siempre sobre las firmas no válidas)</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4">19. Verifique los valores de seguridad de Microsoft PowerPoint 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Varios → Configuración PST”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que los usuarios agreguen archivos PST a perfiles de Outlook y/o evitar el uso de archivos PST para compartirlos de manera exclusiva</td><td>Habilitada (se pueden agregar archivos PST)</td><td></td></tr>
<tr><td colspan="2">Impedir a los usuarios agregar nuevo contenido a archivos PST existentes</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="7">20. Verifique los valores de la Vista protegida de MS PowerPoint 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft PowerPoint 2016 → Opciones de PowerPoint → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Abrir archivos de UNC de intranet local en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de la zona de Internet en Vista protegida</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de ubicaciones inseguras en Vista protegida</td><td>Deshabilitado</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>21. Verifique los valores de la Vista protegida de MS Word 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria media”</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Word 2016 → Opciones de Word → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Abrir archivos de UNC de intranet local en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Desactivar Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
<tr><td>No abrir archivos de la zona de Internet en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td>No abrir archivos de ubicaciones inseguras en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
</table>
</td></tr>
<tr><td>22. Verifique que están configurados los servicios de MS Office 2016</td><td></td><td>Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador.
Ejecute la herramienta “Windows PowerShell” con privilegios de administrador. Para ello vaya a la siguiente ruta:
“Menú inicio → Todos los programas → Accesorios → Windows PowerShell”
Seleccione mediante botón derecho en Windows PowerShell la opción “Ejecutar como administrador”.
En la shell abierta ejecute services.msc.
Compruebe que los siguientes servicios se encuentran configurados en modo manual:
– Office Source Engine
– Servicio de caché de fuentes de Windows
– Servicio Hacer clic y ejecutar de Microsoft Office
Nota: Dependiendo de la versión de Office instalada puede aparecer el servicio “OSE” o “OSE64” y puede no aparecer el servicio “ClickToRunSvc”.</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Servicio (nombre corto)</th><th>Servicio (nombre largo)</th><th>Inicio</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>ClickToRunSvc</td><td>Servicio Hacer clic y ejecutar de Microsoft Office</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>FontCache</td><td>Servicio de caché de fuentes de Windows</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>OSE</td><td>Office Source Engine</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>OSE64</td><td>Office 64 Source Engine</td><td>Manual</td><td>Configurado</td><td></td></tr>
</table>
</td></tr>
<tr><td>23. Inicie sesión con un usuario al que le apliquen las directivas de Office.</td><td></td><td>Inicie sesión con un usuario cuya cuenta se encuentre dentro del grupo de seguridad “ENS usuarios Office 2016 categoria media” y permisos de administrador.</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
24. Ejecute una consola de comandos.		Ejecute con permisos de administrador una consola de comandos. Para ello pulse con botón derecho sobre el botón de inicio y seleccione "Símbolo del sistema (administrador)"  **Nota:** El sistema le solicitará elevación de privilegios.
25. Compruebe que se aplican las GPO de seguridad en el cliente.		Introduzca "gpresult /r" y pulse "Enter" para verificar que se están aplicando las políticas de grupo. 

Comprobación	OK/NOK	Cómo hacerlo
		Confirme que aparece en los apartados de equipo y usuario la GPO "CCN-STIC-585 ENS Incremental Office 2016 categoria media".  
26. Compruebe que las aplicaciones de MS Office 2016 funcionan correctamente		Pruebe a abrir alguna de las aplicaciones de MS Office 2016, como, por ejemplo, MS Word, MS Excel o MS PowerPoint. Compruebe que puede crear un nuevo documento y guardarlo.
27. Compruebe que puede proteger un documento con contraseña y que esta es robusta.		Proteja un documento con contraseña. Para ello acceda al menú "**Archivo → Información → Proteger documento → Cifrar con contraseña**".  Compruebe que no puede introducir una contraseña inferior a 10 caracteres.

Comprobación	OK/NOK	Cómo hacerlo
28. Compruebe los metadatos de los archivos.		Abra cualquiera de las aplicaciones de la *suite* Office, por ejemplo Word, seleccione comenzar un documento en blanco y vaya al menú "**Archivo → Información → Propiedades**" y compruebe que los datos corresponden a los del usuario que inició la sesión. 
29. Compruebe las opciones de contenido en línea.		Verifique que, a la hora de editar un documento en Word, por ejemplo, dentro de la pestaña insertar están desmarcadas las opciones de contenido en línea. 

ANEXO A.2.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.2.3.1. GUÍA PASO A PASO DE IMPLEMENTACIÓN SEGURA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee la suite de Microsoft Office 2016 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.

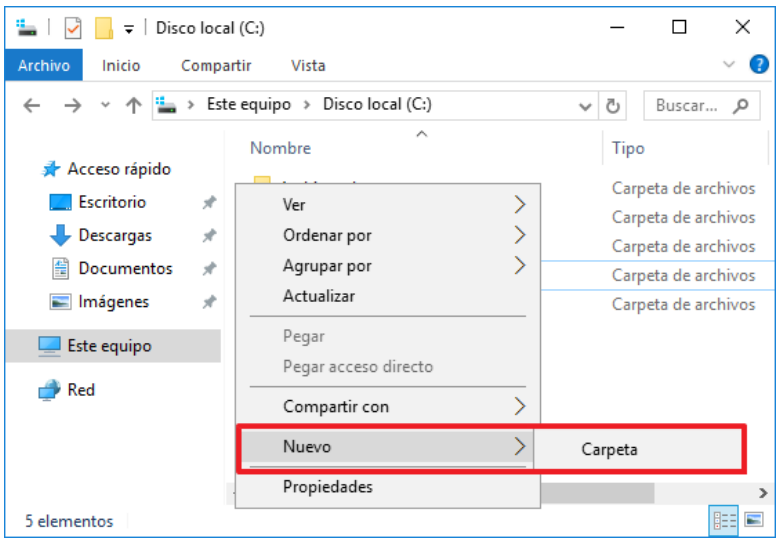
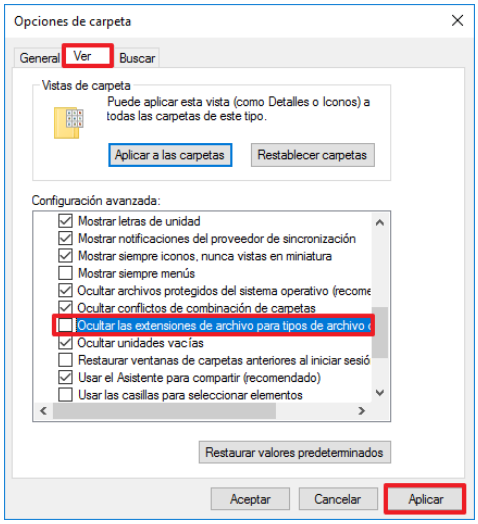
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho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

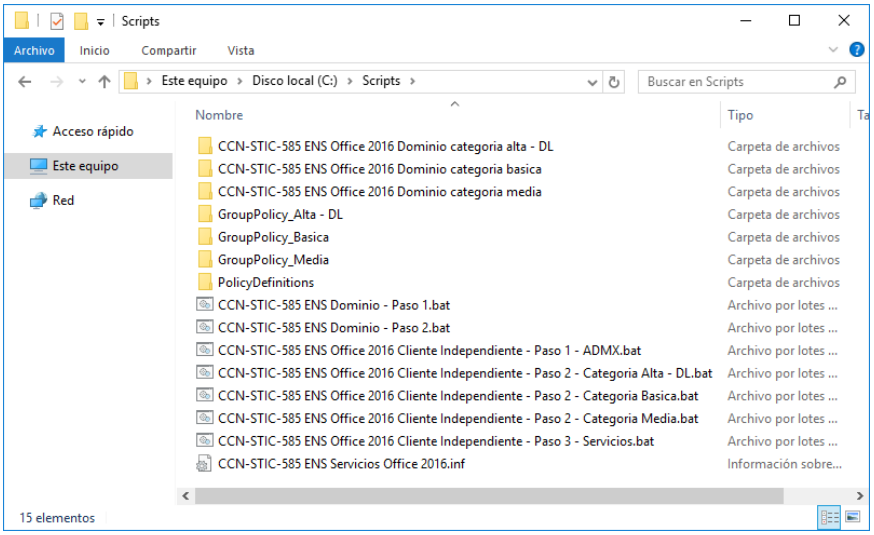
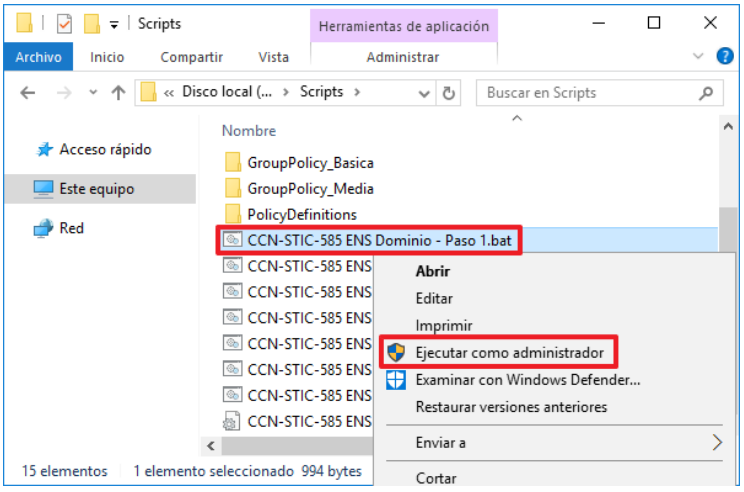
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

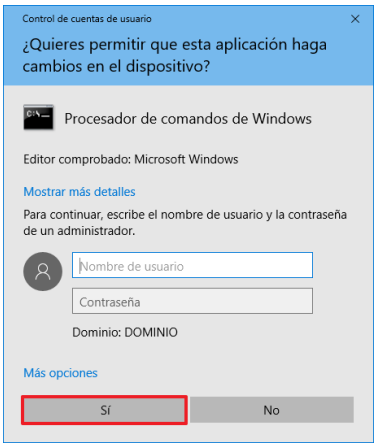
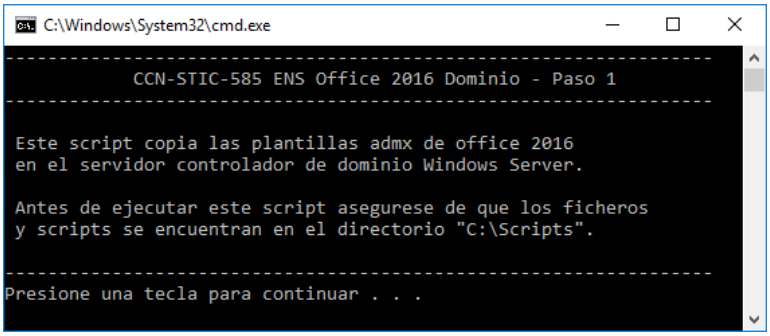
1. PREPARACIÓN DEL DIRECTORIO ACTIVO

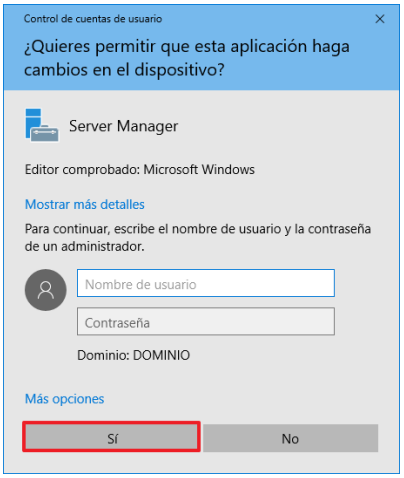
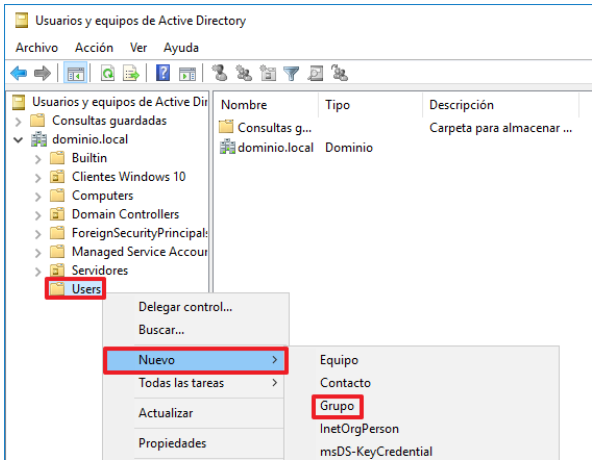
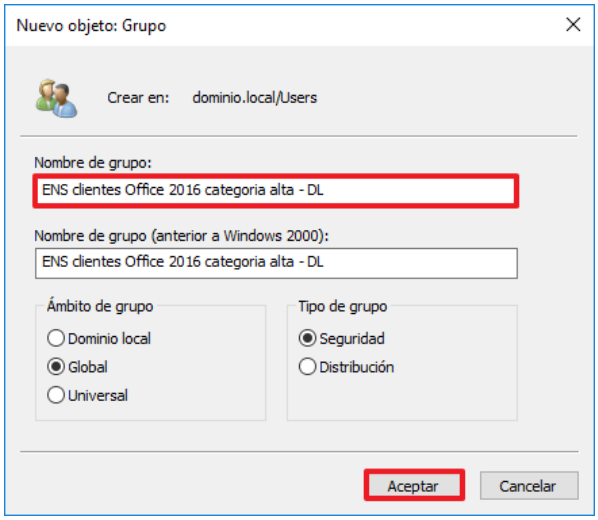
Los pasos que se describen a continuación se realizarán en un controlador de dominio, de la infraestructura a la que pertenecen los clientes en los que se va a securizar MS Office 2016.

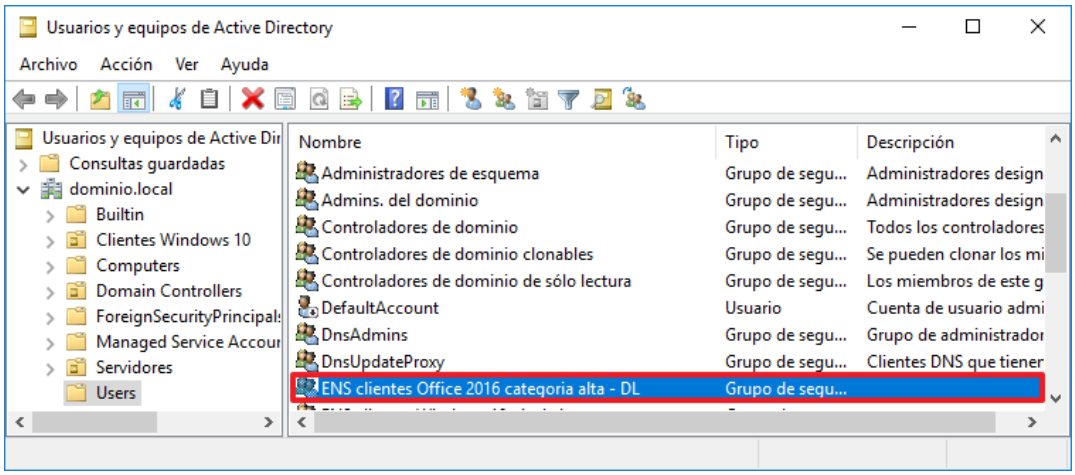
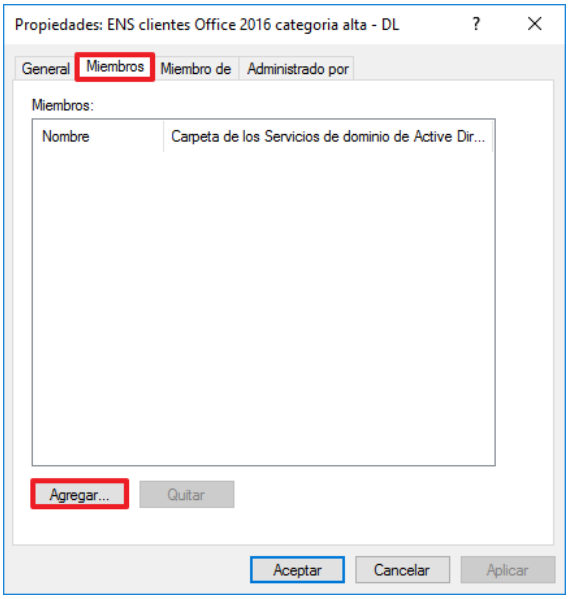
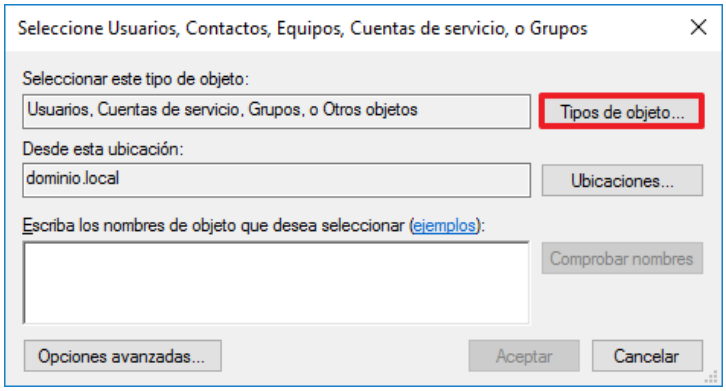
Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta que sea miembro del grupo “Admins. del domino” del dominio al que pertenecen los clientes donde se va a securizar MS Office 2016. **Nota:** En este ejemplo se utiliza un cliente Windows 10 con un controlador de dominio Windows Server 2016 con las guías CCN-STIC-570A y CCN-STIC-599A18 con categoría alta /Difusión Limitada aplicadas. Este entorno puede variar con la estructura de su organización.

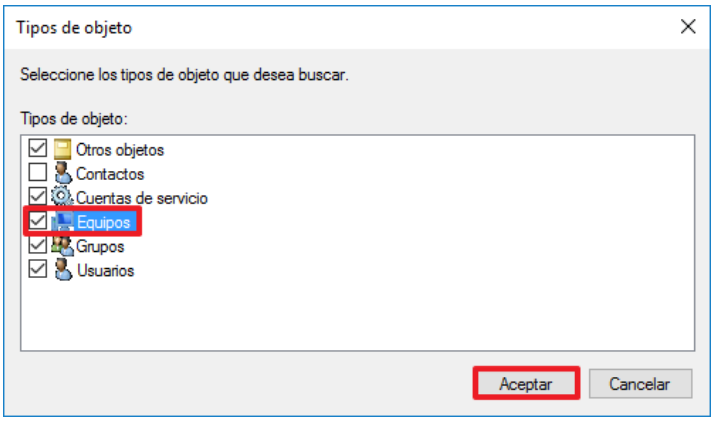
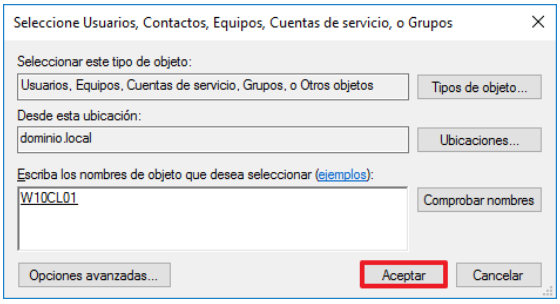
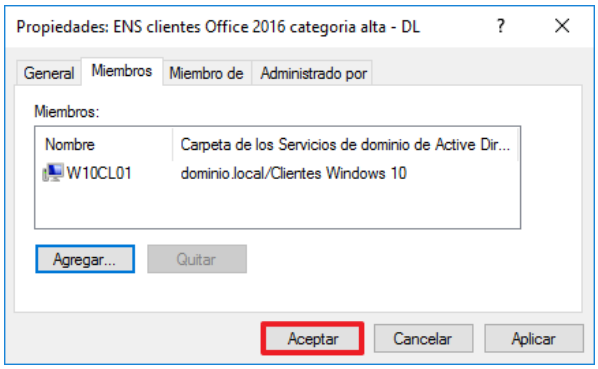
Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo → Carpeta”.** 
3.	Asigne el nombre “Scripts” al nuevo directorio.
4.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.
5.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones". De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".

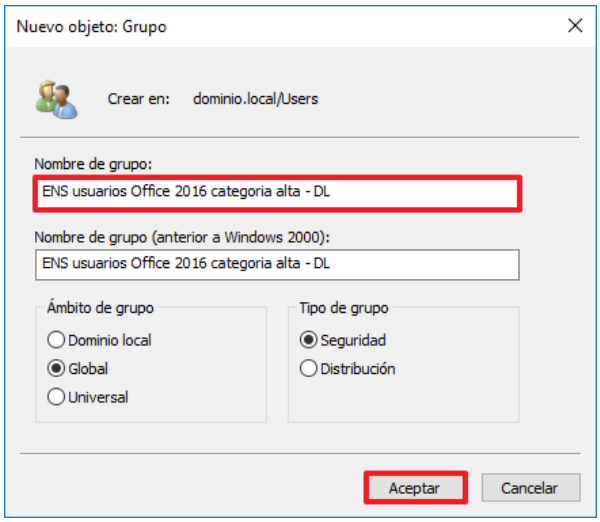
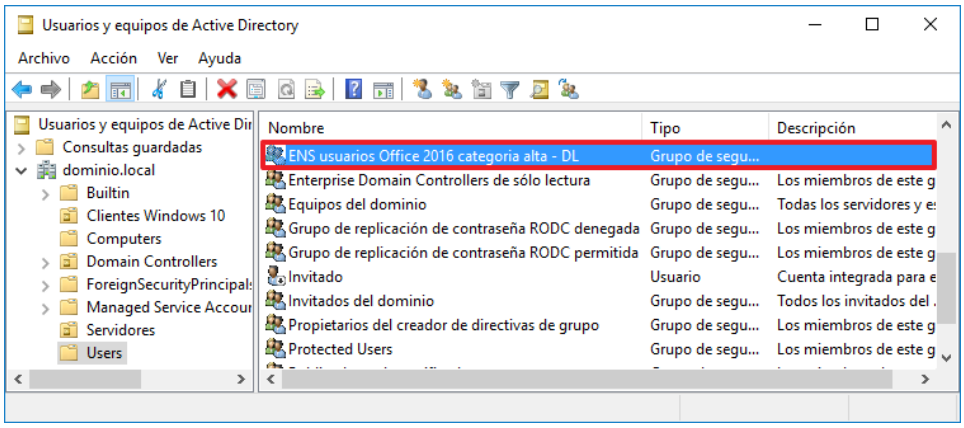
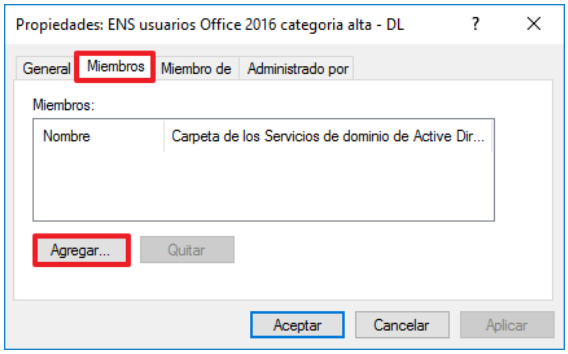
Paso	Descripción
6.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”. 
7.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del servidor, de tal forma que se podrán realizar modificaciones, desde dicha máquina, de las políticas generadas. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script **“CCN-STIC-585 ENS Dominio - Paso1.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.

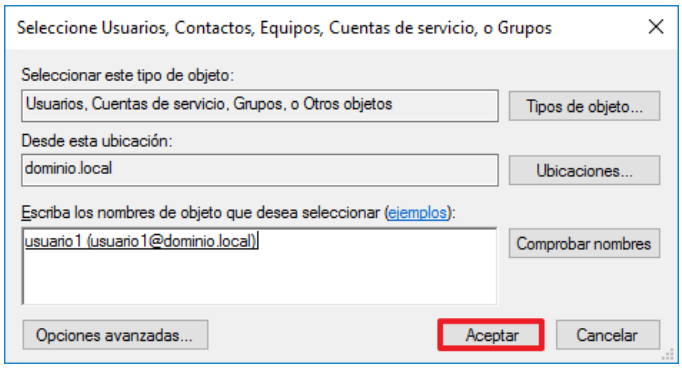
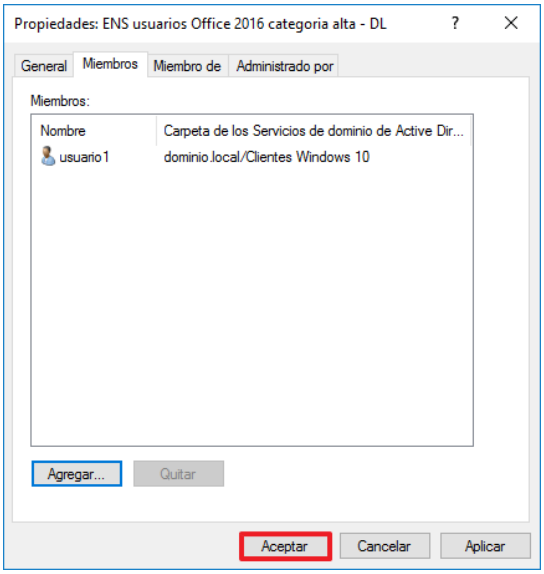
Paso	Descripción
8.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador. 
9.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 
10.	Inicie la herramienta “Usuarios y equipos de Active Directory”, para ello ejecute la herramienta Administrador del servidor (**Inicio → Administrador del servidor**). Seleccione en el menú superior **"Herramientas → Usuarios y equipos de Active Directory”**. **Nota:** Los siguientes pasos describen el procedimiento para crear grupos de seguridad donde agregar los puestos de trabajo y usuarios que le sean de aplicación la categoría alta de seguridad según los criterios definidos del ENS o Difusión Limitada. En el caso de que sus puestos de trabajo o los usuarios se encuentren en la ubicación predeterminada de “Computers” o “Users” 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.

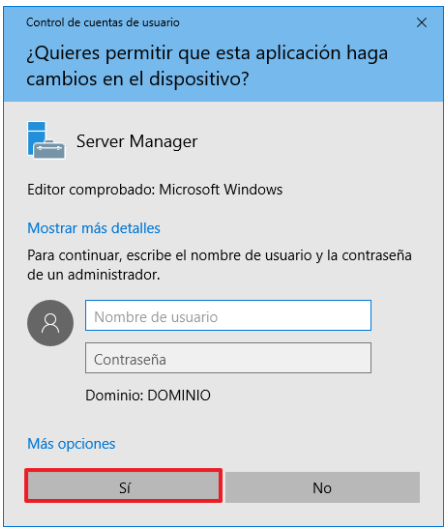
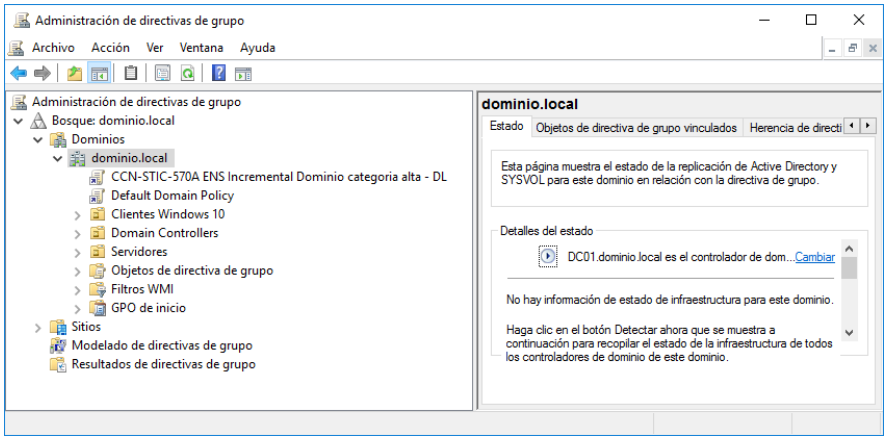
Paso	Descripción
11.	El control de cuentas de usuario le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador. 
12.	Despliegue a continuación el dominio y vaya a la carpeta “Users”. Pulse con el botón derecho del ratón sobre dicha carpeta y seleccione la opción **“Nuevo → Grupo”**. 
13.	Introduzca como nombre “ENS clientes Office 2016 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 que vayan a usar Office 2016. 

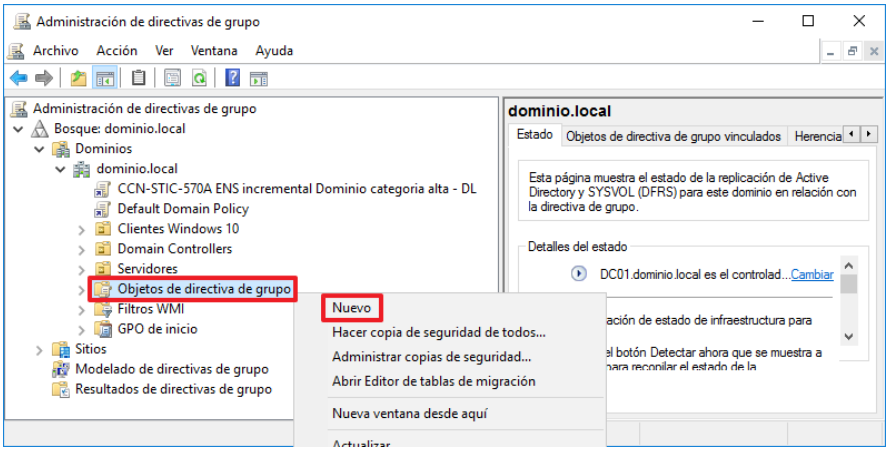
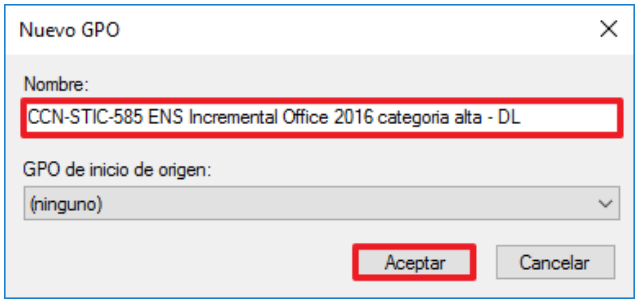
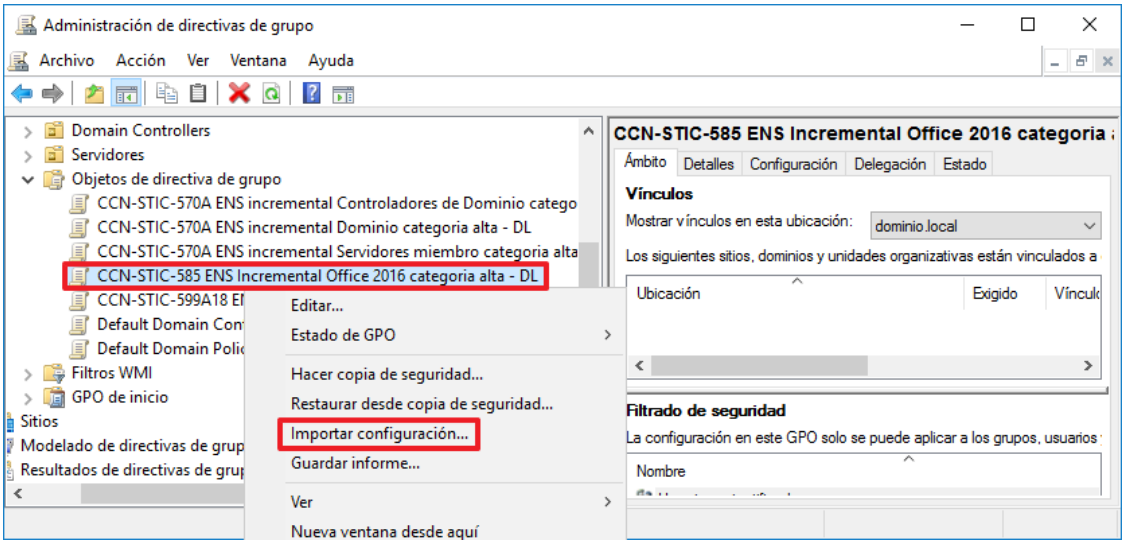
Paso	Descripción
14.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
15.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar…”. 
16.	Pulse sobre “Tipos de objeto…” 

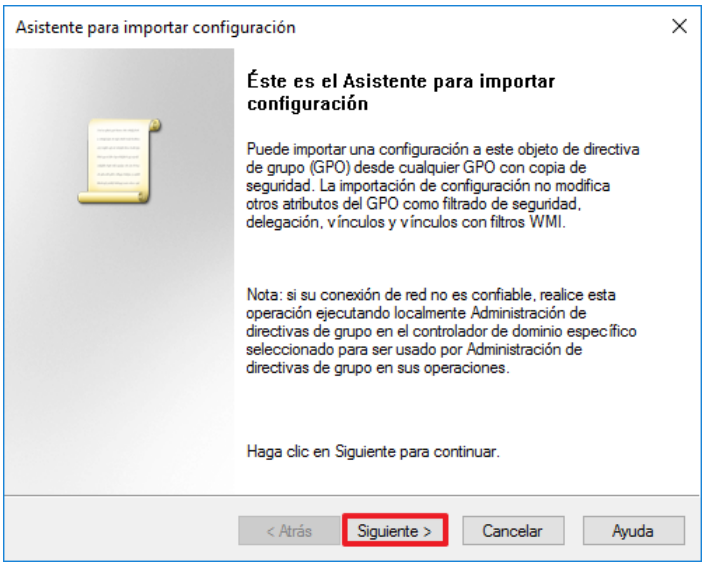
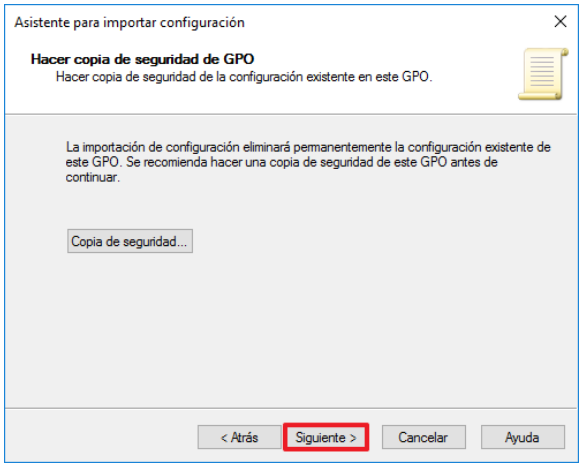
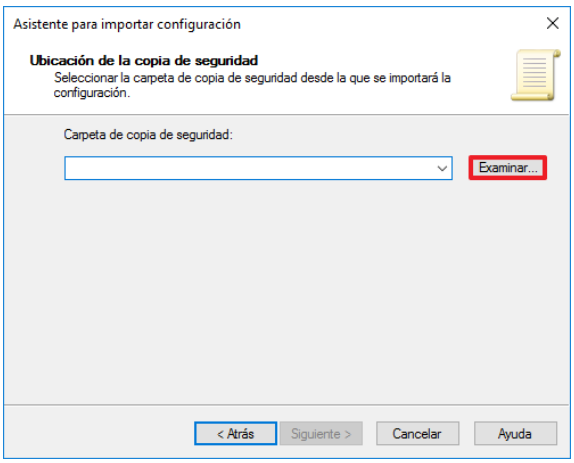
Paso	Descripción
17.	Marque la opción “Equipos” y pulse “Aceptar”. 
18.	Introduzca el nombre de los equipos o utilice las opciones avanzadas para agregar todos aquellos equipos que se encuentren afectados por el cumplimiento del ENS en su categoría de seguridad alta o Redes Clasificadas en su categoría Difusión Limitada que vayan a hacer uso de Office 2016 y pulse “Aceptar” para agregar la selección.  **Nota:** En este ejemplo se usa el equipo “W10CL01”, deberá introducir los equipos acordes a su organización.
19.	Pulse nuevamente el botón “Aceptar” para guardar las propiedades del grupo y cerrar la ventana. 

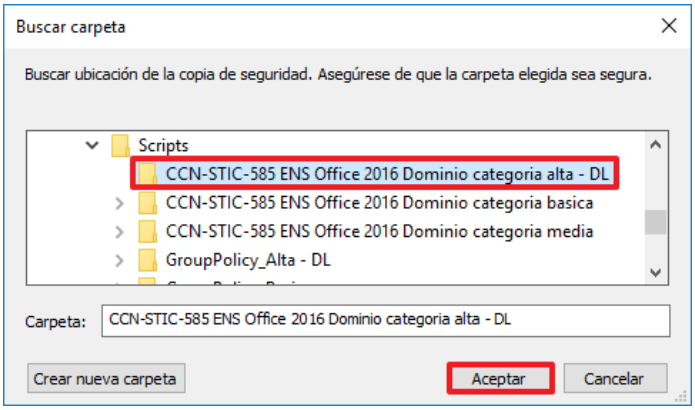
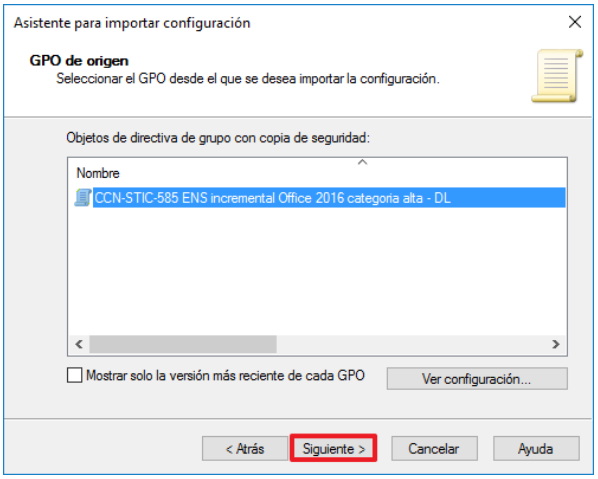
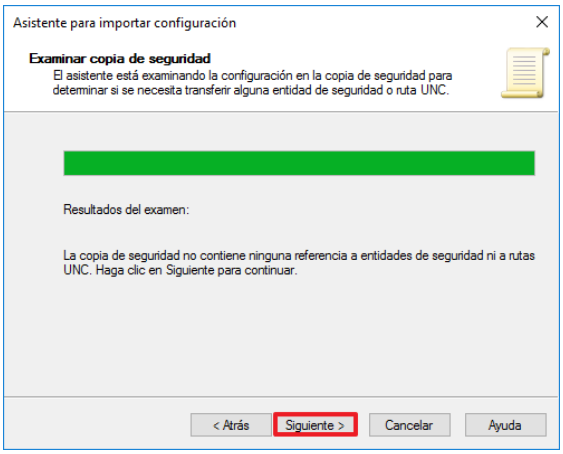
Paso	Descripción
20.	De manera análoga, cree un nuevo grupo con nombre “ENS usuarios Office 2016 categoria alta - DL”. Este grupo se utilizará posteriormente para aplicar las GPO de seguridad sobre usuarios que vayan a usar Office 2016. 
21.	Abra las propiedades del nuevo grupo creado haciendo doble clic sobre el mismo. 
22.	Vaya a la pestaña “Miembros” y pulse el botón “Agregar…”. 

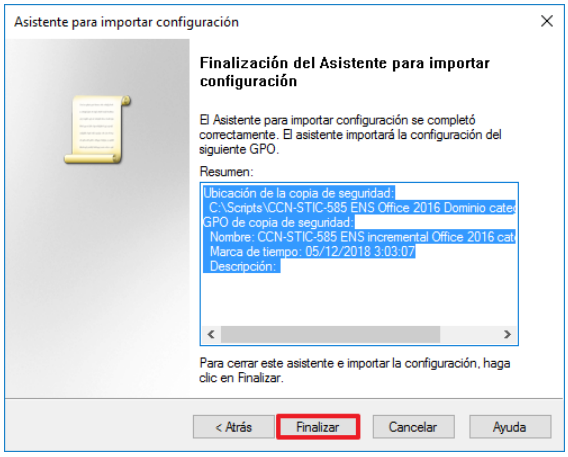
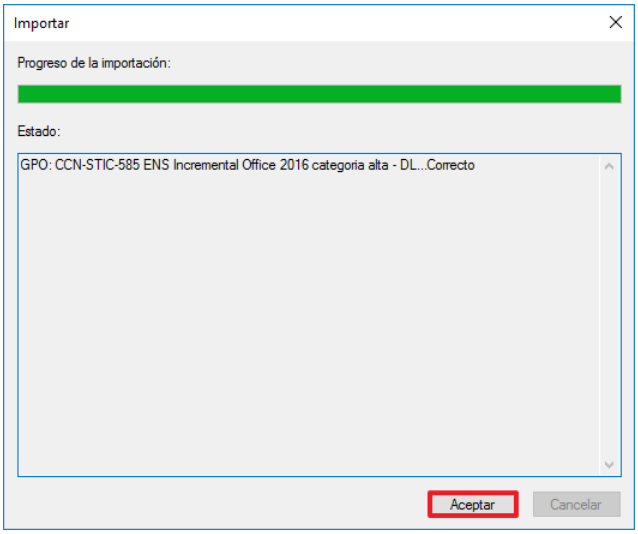
Paso	Descripción
23.	Introduzca el nombre de los usuarios o utilice las opciones avanzadas para agregar todos aquellos usuarios que se encuentren afectados por el cumplimiento en su categoría de seguridad alta del ENS o Difusión Limitada que vayan a hacer uso de Office 2016 y pulse "Aceptar" para agregar la selección.  **Nota:** En este ejemplo se usa el usuario "usuario1", deberá introducir los usuarios acordes a su organización. Recuerde que dichos usuarios deberán estar situados en la unidad organizativa donde se vaya a implementar la seguridad.
24.	Pulse nuevamente el botón "Aceptar" para guardar las propiedades del grupo y cerrar la ventana. 
25.	Cierre la herramienta "Usuarios y equipos de Active Directory".
26.	Inicie la herramienta de administración de directivas de grupo, para ello ejecute la herramienta Administrador del servidor (**Inicio → Administrador del servidor**). Seleccione en el menú superior **"Herramientas → "Administrador de directivas de grupo"**.

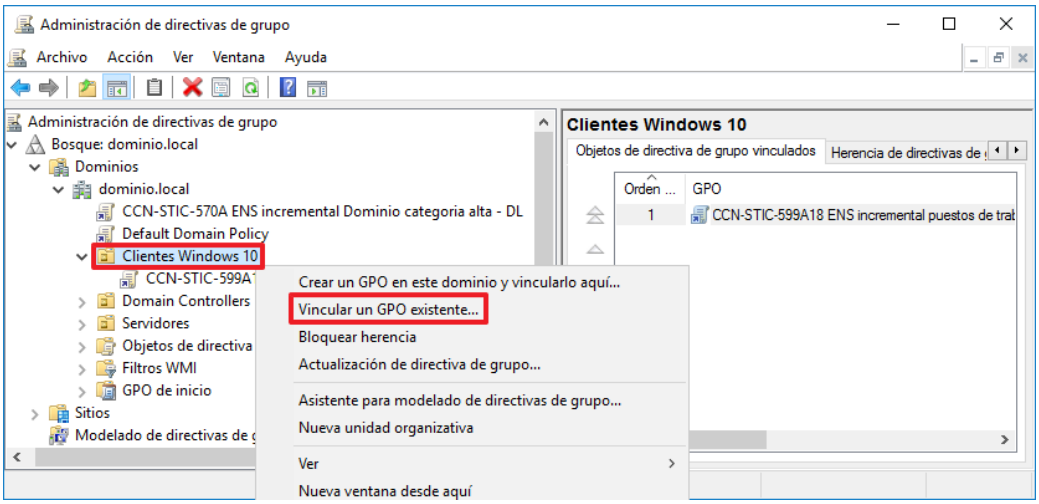
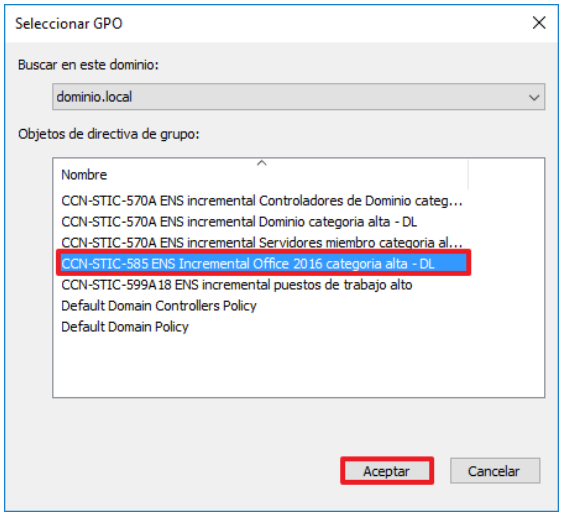
Paso	Descripción
27.	El control de cuentas de usuario le solicitará elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador. 
28.	Expanda el contenedor **"Administración de directivas de grupo → Bosque:<nombre de su bosque> → Dominios → *[nombre de su dominio]*"**, como se muestra en la siguiente imagen.  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 del recién expandido (*[nombre de su dominio]*). **Nota:** En este ejemplo se utiliza como nombre de dominio "dominio.local".

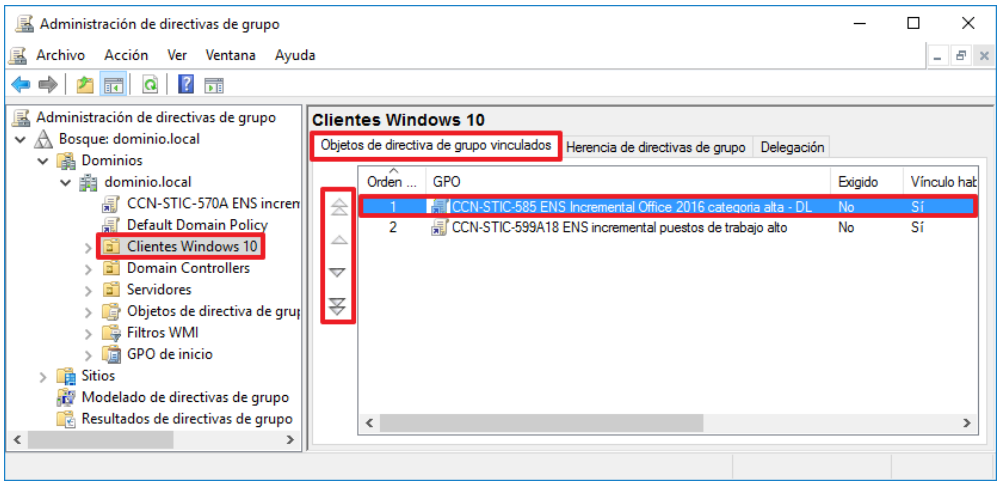
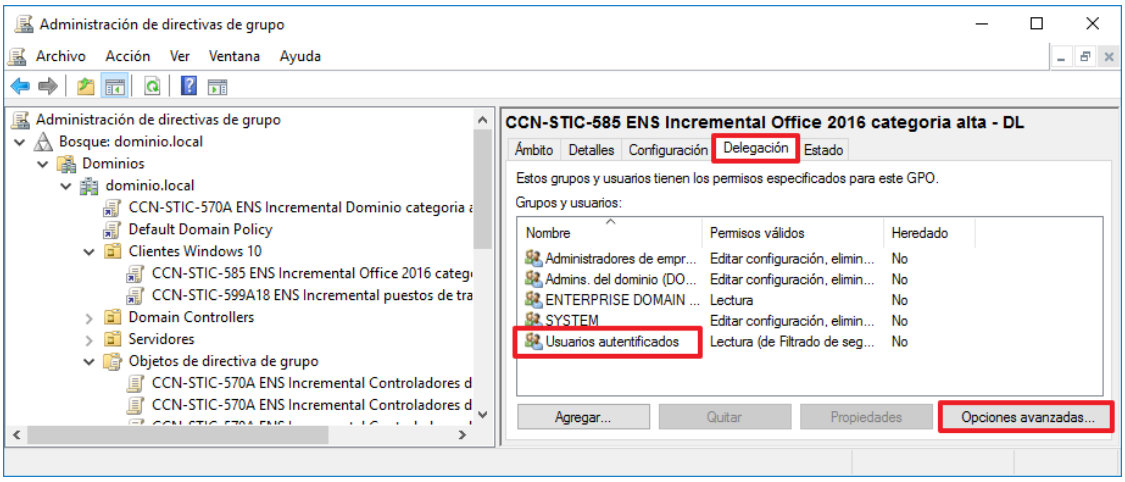
Paso	Descripción
29.	Expanda y seleccione el contenedor **"Objetos de directiva de grupo"**, y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
30.	Asigne el siguiente nombre a la nueva política, GPO, que se está creando: "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL" y pulse "Aceptar". 
31.	Seleccione el objeto de directiva de grupo, GPO, recién creado y marcando con el botón derecho en ella, elija la opción "Importar configuración" del menú contextual que aparecerá. 

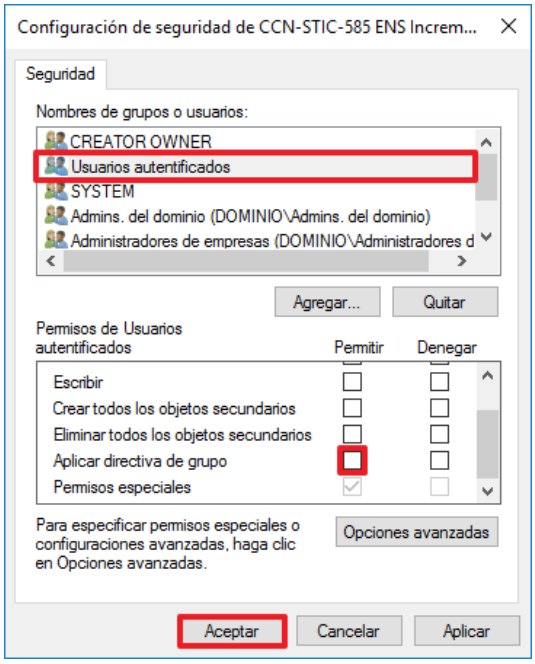
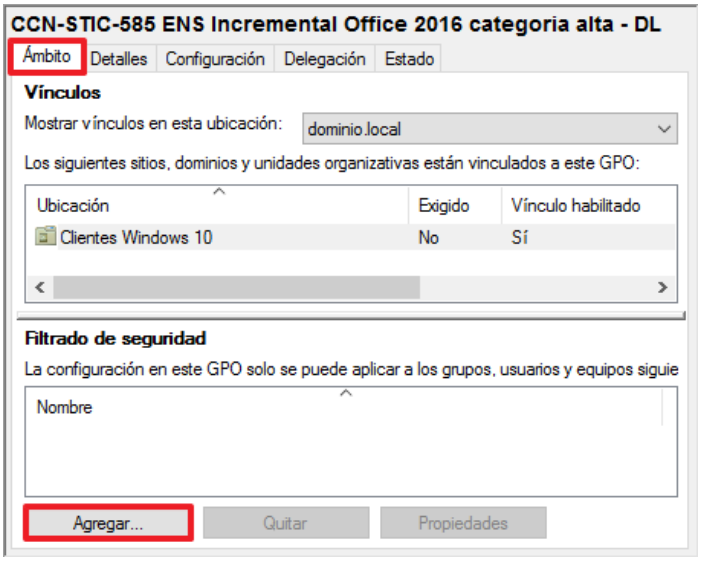
Paso	Descripción
32.	Se iniciará el asistente para la importación de configuración, pulse el botón “Siguiente >”. 
33.	El asistente para la importación de la configuración ofrecerá la opción de realizar una copia de seguridad de la configuración actual de la GPO. Como la política se encuentra vacía, no será necesario realizar ninguna copia de seguridad. Pulse el botón “Siguiente >” 
34.	A continuación, deberá seleccionar la carpeta de copia de seguridad desde la que se importará la configuración. Seleccione el botón “Examinar…”. 

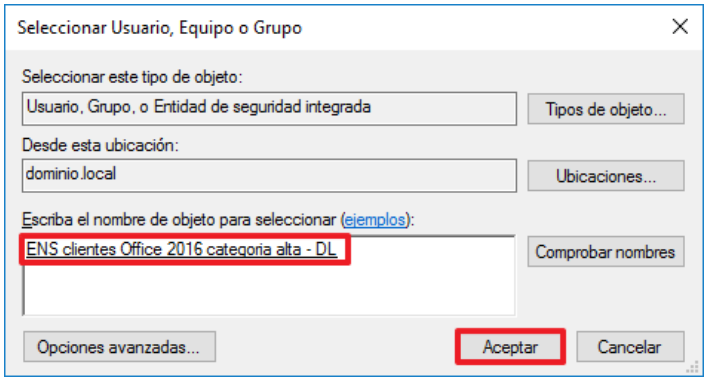
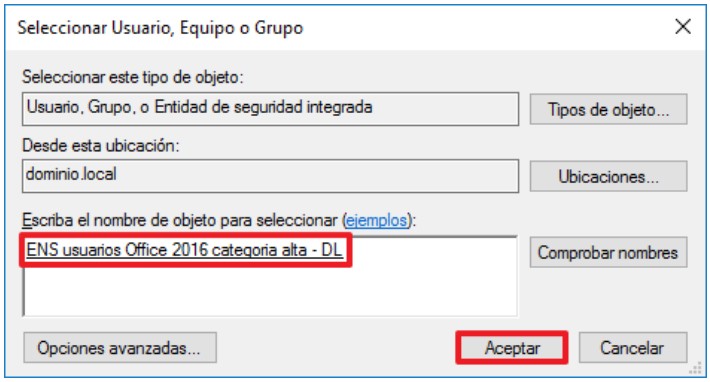
Paso	Descripción
35.	Busque y seleccione la carpeta “**C:\Scripts\CCN-STIC-585 ENS Office 2016 Dominio categoria alta - DL”**. Pulse el botón “Aceptar” y volverá a la ventana del asistente. Pulse el botón “Siguiente >”. 
36.	Deberá indicarse el objeto GPO desde el que desea importar la configuración. Pulse “Siguiente >”. 
37.	El asistente procederá a realizar una verificación de la configuración de la copia de seguridad. Pulse el botón “Siguiente >”. 

Paso	Descripción
38.	El asistente para importar la configuración mostrará, entonces, una ventana resumen con los datos de la importación que se va a realizar. Pulse el botón “Finalizar”. 
39.	El asistente procederá a realizar la importación. Pulse “Aceptar”. Con ello habrá quedado importada la configuración de la nueva política generada, estando lista para ser asignada a la unidad organizativa de usuarios creada en pasos anteriores, cuestión que se realizará a continuación. 

Paso	Descripción
40.	Expanda y seleccione el contenedor de usuarios en la unidad organizativa donde tenga alojada la configuración de los clientes, **"Menú inicio → Herramientas administrativas → Administración de directivas de grupo → Bosque: *[nombre de su bosque]* → Dominios → *[nombre de su dominio]* → Clientes Windows 10"**, y márquelo con el botón derecho del ratón, seleccione la opción "Vincular un GPO existente…"  **Nota:** En este caso, el nombre del bosque y del dominio es "dominio.local" y las unidades organizativas fueron creadas durante el proceso de instalación de equipos Windows 10 dentro de un dominio, según la guía CCN-STIC-599A18. Si todos los equipos y usuarios a los que va a aplicar esta configuración no se encuentran en esta unidad organizativa deberá vincular la GPO a nivel de dominio.
41.	En la ventana que aparece, seleccione el GPO "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL" y pulse el botón "Aceptar". 
42.	El objeto de directiva de grupo, GPO, habrá quedado vinculado a la unidad organizativa "Clientes Windows 10".

Paso	Descripción
43.	Ahora, se determinará el orden de los vínculos. Deberá quedar, la nueva directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”, en la primera posición para asegurar un resultado adecuado en la aplicación. Para ello, se deben utilizar las flechas de posicionamiento de la ficha “Objetos de directiva de grupo vinculados” de la unidad organizativa “Clientes Windows 10”. 
44.	Seleccione la nueva GPO configurada. Vaya a las opciones de Delegación que se encuentran en el panel derecho. Seleccione “Usuarios autentificados” y pulse sobre el botón “Opciones avanzadas”.  **Nota:** En el caso de que todos los equipos cliente vayan a tener instalado Office 2016 puede mantener el grupo del sistema “Usuarios autentificados” y saltar al paso 49.

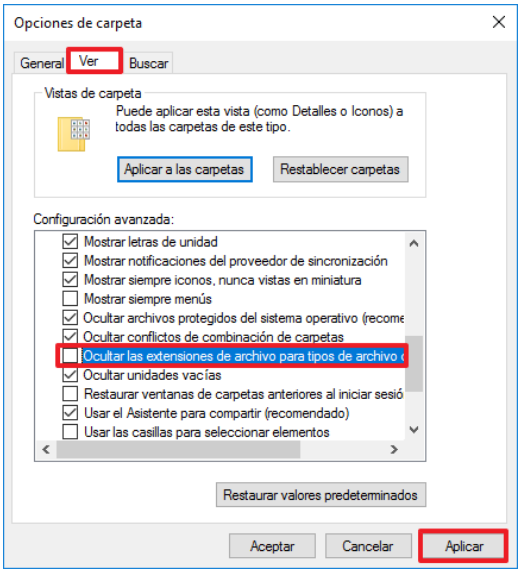
Paso	Descripción
45.	Seleccione “Usuarios autentificados” y en la parte inferior “Permisos de Usuarios autentificados” quite el check “Permitir” en “Aplicar directiva de grupo” y pulse el botón “Aceptar”. 
46.	Vaya a la pestaña “Ámbito” y pulse sobre el botón “Agregar…”. 

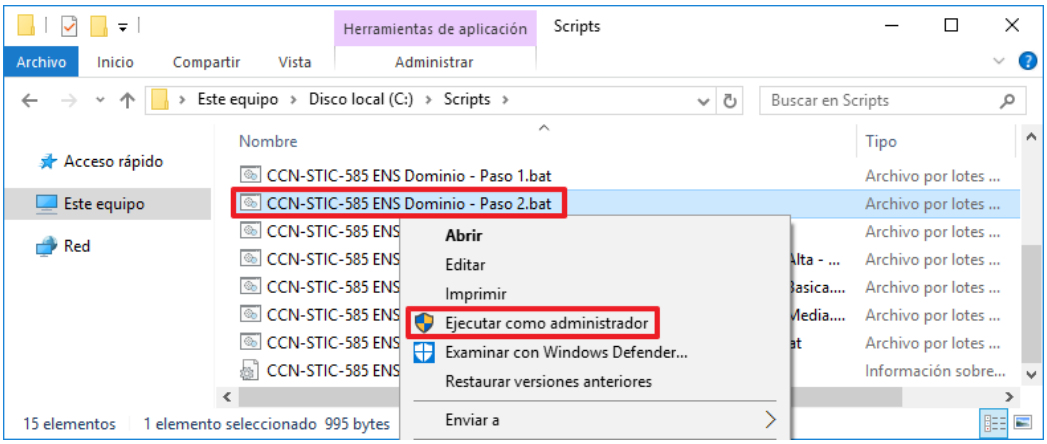
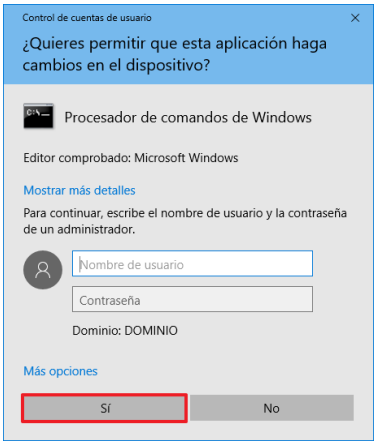
Paso	Descripción
47.	Introduzca como nombre “ENS clientes Office 2016 categoria alta - DL”. A continuación, pulse el botón “Aceptar”. 
48.	De manera análoga, introduzca el grupo “ENS usuarios Office 2016 categoria alta - DL” y pulse “Aceptar”. Estos grupos corresponden con los generados en pasos previos. 
49.	El objeto de directiva de grupo, GPO, habrá quedado configurada correctamente. **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
50.	Elimine la carpeta **“C:\Scripts”** del servidor.

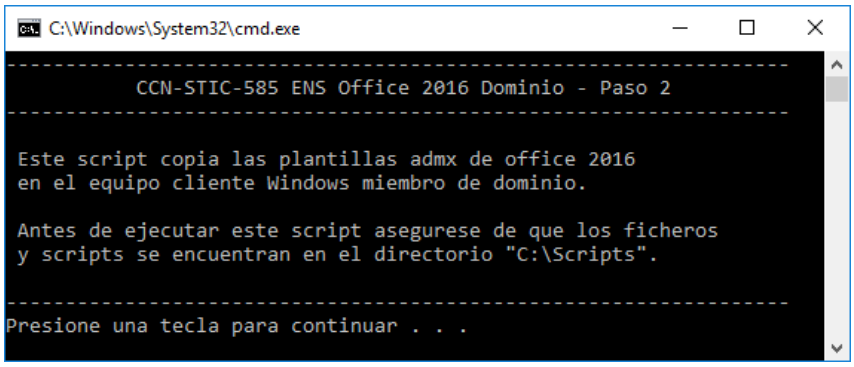
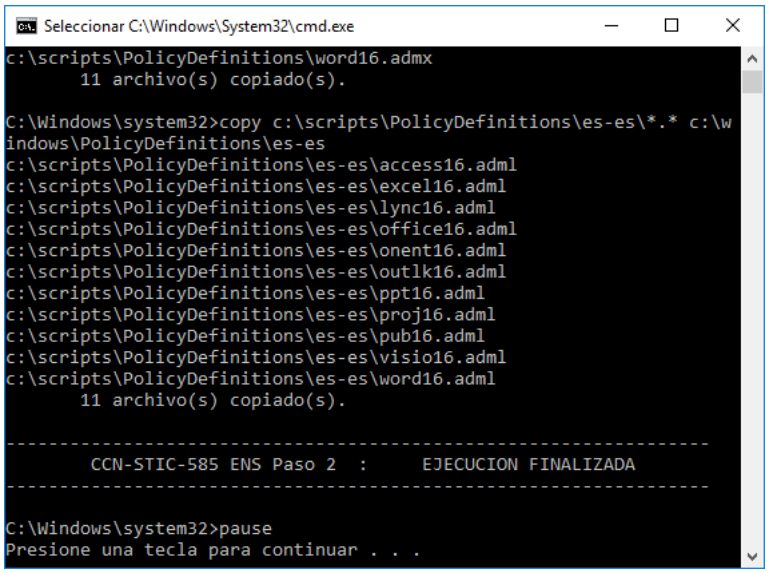
2. PREPARACIÓN DEL CLIENTE PARA LA SECURIZACIÓN DE MS OFFICE 2016 EN UN EQUIPO DEL DOMINIO

Los siguientes pasos describen el proceso de securización de Microsoft Office 2016 en un cliente Windows 10 miembro de un dominio.

Paso	Descripción
51.	En el puesto de trabajo, equipo cliente miembro de dominio con Windows 10, preparado siguiendo las recomendaciones de la guía CCN-STIC-599A18, se procederá a iniciar sesión con una cuenta con los suficientes privilegios para ejecutar scripts. **Nota:** En este ejemplo se utiliza un cliente Windows 10 con un controlador de dominio Windows Server 2016 con las guías CCN-STIC-570A y CCN-STIC-599A18 con categoría alta / Difusión Limitada aplicadas. Este entorno puede variar con la estructura de su organización.
52.	Cree el directorio “Scripts” en la unidad “C:\”.

Paso	Descripción
53.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio **"C:\Scripts"**.
54.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.
55.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú "Vista" y dentro de dicho menú, "Opciones". De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".

Paso	Descripción
56.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del cliente. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script **"CCN-STIC-585 ENS Dominio – Paso2.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.
57.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador. 

Paso	Descripción
58.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 
59.	Se producirá la copia de un total de 22 ficheros: 
60.	Pulse cualquier tecla para continuar y finalizar la ejecución del *script*.
61.	Reinicie el equipo cliente.
62.	En este punto habrá quedado securizado MS Office 2016 en el equipo cliente.

ANEXO A.2.3.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016

Este anexo se ha diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad de la presente guía para la categoría alta / Difusión Limitada.

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

a) En el controlador de dominio:
   i. Administración de directivas de grupo.
   ii. Editor de administración de directivas de grupo.

b) En el equipo cliente:
   i. Explorador de Windows.
   ii. PowerShell.
   iii. Símbolo del sistema.
   iv. Consola de servicios.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un controlador de dominio con un administrador del dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. Este controlador de dominio deberá contener las plantillas de directivas de MS Office 2016.
2. Verifique que está creada la directiva de equipo (CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL)		Utilizando la herramienta Administración de directivas de grupo ("**Inicio → Herramientas administrativas → Administración de directivas de grupo**"). Despliegue hasta llegar a la política **"CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"** en la ruta "**Bosque: *[nombre de su bosque]* → Dominios → *[nombre de su dominio]* → Clientes Windows 10**". Pulsando el botón derecho sobre el objeto de política, deberá seleccionarse la opción "Editar". Se abrirá la herramienta "Editor de objetos de directiva de grupo" que permitirá verificar los valores de la directiva. **Nota:** En este ejemplo la directiva a comprobar está en la unidad organizativa "Clientes Windows 10". En el entorno de su organización puede variar.

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de servicios de sistema dentro de: **"Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"** **Nota:** Dependiendo de los servicios que estén instalados en el controlador de dominio utilizado para la verificación, es posible que aparezcan los nombres cortos de los servicios o que aparezcan servicios adicionales.

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

4. Verifique los valores seguridad del sistema de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración del equipo → Directivas → Plantillas administrativas → Microsoft Office 2016 (Equipo) → Configuración de seguridad"**

Directiva	Valor	OK/NOK
Deshabilitar el almacenamiento en caché de contraseñas	Habilitada	
Deshabilitar reparación de paquetes	Habilitada	

5. Verifique los valores del centro de confianza de Microsoft Access 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Access 2016 → Configuración de la aplicación → Seguridad → Centro de confianza"**

Directiva	Valor	OK/NOK
Desactivar documentos confiables	Habilitada	

6. Verifique los valores de criptografía aplicados de Microsoft Access 2016 de la directiva "CCN-STIC-585 ENS Incremental Office		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Access 2016 → Configuración de la aplicación → Seguridad → Criptografía"**

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="5">2016 categoria alta - DL”</td><td></td><td colspan="3"></td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Especificar algoritmo hash CNG</td><td>Habilitada (SHA512)</td><td></td></tr>
<tr><td colspan="2">Especificar compatibilidad de cifrado</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Especificar longitud de contraseña CNG con sal</td><td>Habilitada (32)</td><td></td></tr>
<tr><td rowspan="3">7. Verifique los valores de seguridad aplicados de Microsoft Excel 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Examinar macros cifradas en libros de formato Open XML de Excel</td><td>Habilitada (Examinar macros cifradas (predeterminado))</td><td></td></tr>
<tr><td>8. Verifique los valores del Centro de confianza de MS Excel 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza”</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
		Directiva	**Valor**	**OK/NOK**
		Bloquear la ejecución de macros en archivos de Office procedentes de Internet	Habilitada	
9. Verifique los valores de la Vista protegida de MS Excel 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza → Vista protegida"**		
		Directiva	**Valor**	**OK/NOK**
		Abrir archivos de UNC de intranet local en Vista protegida	Deshabilitada	
		Desactivar Vista protegida para los datos adjuntos abiertos en Outlook	Deshabilitada	
		Establecer el comportamiento del documento en caso de error en la validación de documento	Habilitado (Bloquear archivos, No permitir edición)	
		No abrir archivos de la zona de Internet en Vista protegida	Deshabilitado	
		No abrir archivos de ubicaciones inseguras en Vista protegida	Deshabilitado	
10. Verifique los valores de criptografía aplicados de Microsoft Excel 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Criptografía"**		
		Directiva	**Valor**	**OK/NOK**
		Especificar algoritmo hash CNG	Habilitada (SHA512)	
		Especificar compatibilidad de cifrado	Habilitada (Guardar todos arch. con form. próx. generac.)	
		Especificar longitud de contraseña CNG con sal	Habilitada (32)	
		Usar nueva clave cuando cambie la contraseña	Habilitada	
11. Verifique los valores de Varios de MS Excel 2016 de la directiva "CCN-STIC-585 ENS Incremental		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Excel 2016 → Varios"**		

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="2">Office 2016 categoria alta - DL”</td><td></td><td colspan="3"></td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td rowspan="3">12. Verifique los valores de Ayuda de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td colspan="2">No almacenar archivos de red en la memoria caché local</td><td>Habilitada</td><td></td></tr>
<tr><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Ayuda”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td rowspan="4">13. Verifique los valores de Configuración de seguridad de MS Office 2016 de la directiva “CCN-STIC-585 Incremental Office 2016 categoria alta - DL”</td><td colspan="2">Búsqueda federada para obtener ayuda</td><td>Deshabilitada</td><td></td></tr>
<tr><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Establecer longitud mínima de contraseña</td><td>Habilitada (12)</td><td></td></tr>
<tr><td colspan="2">Establecer nivel de reglas de contraseña</td><td>Habilitada (Comprobación de longitud local)</td><td></td></tr>
<tr><td colspan="2">Seguridad de automatización</td><td>Habilitada (Deshabilitar macros de forma predeterminada)</td><td></td></tr>
<tr><td rowspan="4">14. Verifique los valores de Catálogos de confianza de MS Office 2016 de la directiva “CCN-STIC-585 Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad → Centro de confianza → Catálogos de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Bloquear complementos web</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Bloquear Tienda Office</td><td>Habilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4">15. Verifique los valores de Contenido en línea de MS Office 2016 de la directiva “CCN-STIC-585 Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Herramientas | Opciones | General | Opciones de servicios… → Contenido en línea”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Opciones de contenido en línea</td><td>Habilitada (No permitir que Office se conecte a Internet)</td><td></td></tr>
<tr><td colspan="2">Opciones de nivel de servicio</td><td>Habilitada (Solo servicios de Microsoft)</td><td></td></tr>
<tr><td rowspan="3">16. Verifique los valores del Panel de telemetría de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Panel de telemetría”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Activar la recopilación de datos de telemetría</td><td>Deshabilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="6">17. Verifique los valores del Centro de confianza de MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Privacidad → Centro de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el Asistente para participar la primera vez que se ejecute</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Enviar comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Enviar información personal</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar programa de mejora de experiencia del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir la inclusión de capturas de pantalla con los comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="6">18. Verifique valores de Varios en MS Office 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Office 2016 → Varios”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Abrir vínculos de archivos de Office en Office Online</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">Mostrar características de LinkedIn en aplicaciones de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Mostrar inicio de sesión OneDrive</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar las ubicaciones de archivos al abrir o guardar archivos</td><td>Habilitada (Ocultar OneDrive Personal, SharePoint Online y OneDrive para la Empresa)</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3">19. Verifique los valores de criptografía aplicados de Microsoft Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Seguridad → Criptografía”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Advertencia de firma</td><td>Habilitada (Advertir siempre sobre firmas no válidas)</td><td></td></tr>
<tr><td rowspan="3">20. Verifique las opciones de Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Ocultar el botón de Tienda Office</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">21. Verifique los valores de seguridad de autoarchivar de Microsoft Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro → Autoarchivar”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar Archivo/Archivar</td><td>Habilitada</td><td></td></tr>
</table>

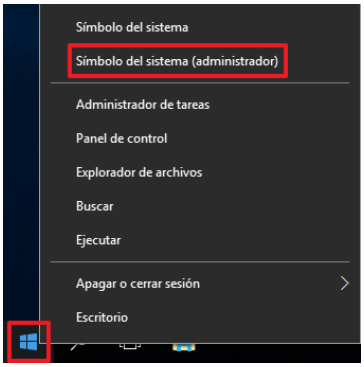
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3">22. Verifique los valores de seguridad de criptografía de Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Seguridad → Criptografía”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Advertencia de firma</td><td>Habilitada (Advertir siempre sobre las firmas no válidas)</td><td></td></tr>
<tr><td rowspan="4">23. Verifique los valores de configuración PST de Microsoft Outlook 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Outlook 2016 → Varios → Configuración PST”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que los usuarios agreguen archivos PST a perfiles de Outlook y/o evitar el uso de archivos PST para compartirlos de manera exclusiva</td><td>Habilitada (se pueden agregar archivos PST)</td><td></td></tr>
<tr><td colspan="2">Impedir a los usuarios agregar nuevo contenido a archivos PST existentes</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="2">24. Verifique los valores de la Vista protegida de MS PowerPoint 2016 de la directiva “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Directivas → Plantillas administrativas → Microsoft PowerPoint 2016 → Opciones de PowerPoint → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">Abrir archivos de UNC de intranet local en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td></td><td colspan="2">Desactivar Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td></td><td colspan="2">Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
</table>

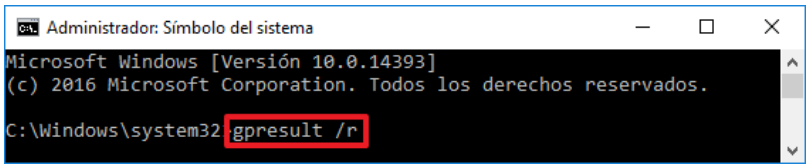
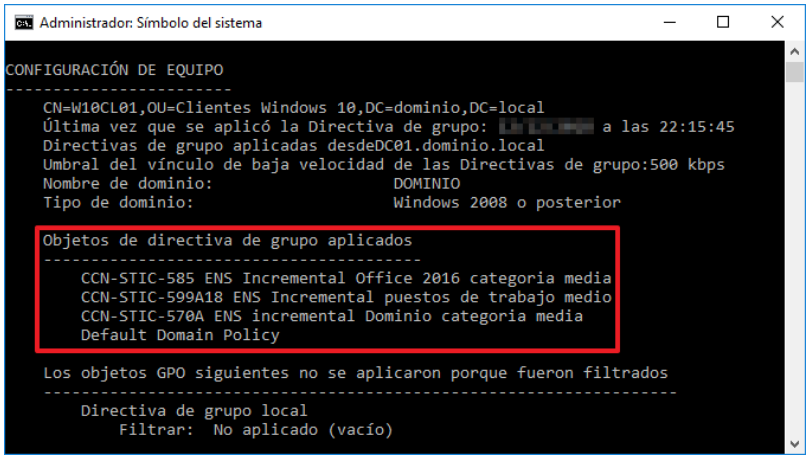
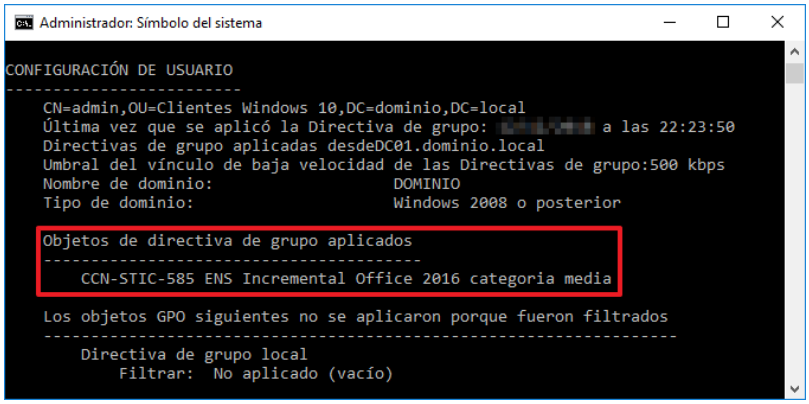
Comprobación	OK/NOK	Cómo hacerlo		
	No abrir archivos de la zona de Internet en Vista protegida		Deshabilitado	
	No abrir archivos de ubicaciones inseguras en Vista protegida		Deshabilitado	
25. Verifique los valores de criptografía aplicados de PowerPoint 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft PowerPoint 2016 → Opciones de PowerPoint → Seguridad → Criptografía"**		
	Directiva		**Valor**	**OK/NOK**
	Especifica la longitud de salt CNG		Habilitada (32)	
	Especificar algoritmo hash CNG		Habilitada (SHA512)	
	Especificar compatibilidad de cifrado		Habilitada (Todos los archivos se guardan con última generación)	
	Usar una clave nueva al cambiar la contraseña		Habilitada	
26. Verifique los valores de criptografía aplicados de Microsoft Project 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Project 2016 → Opciones de proyecto → Seguridad → Criptografía"**		
	Directiva		**Valor**	**OK/NOK**
	Especificar algoritmo hash CNG		Habilitada (SHA512)	
	Especificar longitud de contraseña CNG con salt		Habilitada (32)	
27. Verifique los valores de la Vista protegida de MS Word 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Word 2016 → Opciones de Word → Seguridad → Centro de confianza → Vista protegida"**		
	Directiva		**Valor**	**OK/NOK**

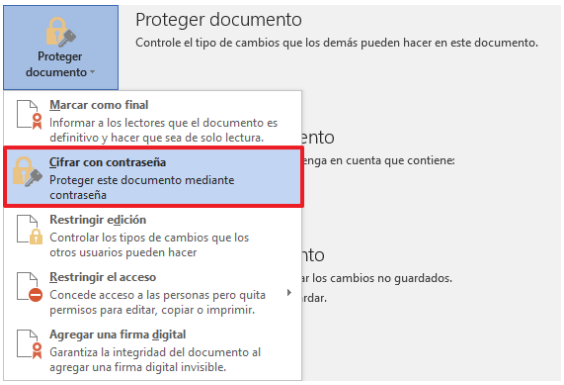
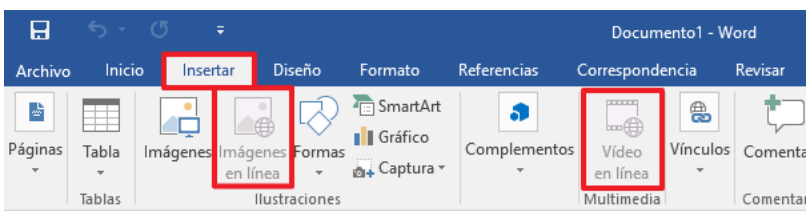
Comprobación	OK/NOK	Cómo hacerlo		
	Abrir archivos de UNC de intranet local en Vista protegida		Deshabilitada	
	Desactivar Vista protegida para los datos adjuntos abiertos desde Outlook		Deshabilitada	
	Establecer el comportamiento del documento si se producen errores durante la validación del archivo		Habilitado (Bloquear archivos, No permitir edición)	
	No abrir archivos de la zona de Internet en Vista protegida		Deshabilitada	
	No abrir archivos de ubicaciones inseguras en Vista protegida		Deshabilitada	
28. Verifique los valores de criptografía aplicados de Microsoft Word 2016 de la directiva "CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL"		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Directivas → Plantillas administrativas → Microsoft Word 2016 → Opciones de Word → Seguridad → Criptografía"**		
	Directiva		**Valor**	**OK/NOK**
	Especificar algoritmo hash CNG		Habilitada (SHA512)	
	Especificar compatibilidad de cifrado		Habilitada (Guardar todos arch. Con form. próx. generac.)	
	Especificar longitud de contraseña CNG con salt		Habilitada (32)	
	Usar nueva clave cuando cambie la contraseña		Habilitado	

Comprobación	OK/NOK	Cómo hacerlo
29. Verifique que están configurados los servicios de MS Office 2016		Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador. Ejecute la herramienta "Windows PowerShell" con privilegios de administrador. Para ello vaya a la siguiente ruta: **"Menú inicio → Todos los programas → Accesorios → Windows PowerShell"** Seleccione mediante botón derecho en Windows PowerShell la opción **"Ejecutar como administrador"**. En la shell abierta ejecute **services.msc**. Compruebe que los siguientes servicios se encuentran configurados en modo manual: – Office Source Engine – Servicio de caché de fuentes de Windows – Servicio Hacer clic y ejecutar de Microsoft Office **Nota:** Dependiendo de la versión de Office instalada puede aparecer el servicio "OSE" o "OSE64" y puede no aparecer el servicio "ClickToRunSvc".

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

30. Inicie sesión con un usuario al que le apliquen las directivas de Office.		Inicie sesión con un usuario cuya cuenta se encuentre dentro del grupo de seguridad "ENS usuarios Office 2016 categoria alta - DL " y permisos de administrador.
31. Ejecute una consola de comandos.		Ejecute con permisos de administrador una consola de comandos. Para ello pulse con botón derecho sobre el botón de inicio y seleccione "Símbolo del sistema (administrador)"  **Nota:** El sistema le solicitará elevación de privilegios.

Comprobación	OK/NOK	Cómo hacerlo
32. Compruebe que se aplican las GPO de seguridad en el cliente.		Introduzca “gpresult /r” y pulse “Enter” para verificar que se están aplicando las políticas de grupo.  Confirme que aparece en los apartados de equipo y usuario la GPO “CCN-STIC-585 ENS Incremental Office 2016 categoria alta - DL”.  
33. Compruebe que las aplicaciones de MS Office 2016 funcionan correctamente		Pruebe a abrir alguna de las aplicaciones de MS Office 2016, como, por ejemplo, MS Word, MS Excel o MS PowerPoint. Compruebe que puede crear un nuevo documento y guardarlo.

Comprobación	OK/NOK	Cómo hacerlo
34. Compruebe que puede proteger un documento con contraseña y que esta es robusta.		Proteja un documento con contraseña. Para ello acceda al menú **"Archivo → Información → Proteger documento → Cifrar con contraseña"**.  Compruebe que no puede introducir una contraseña inferior a 12 caracteres.
35. Compruebe los metadatos de los archivos.		Abra cualquiera de las aplicaciones de la *suite* Office, por ejemplo Word, seleccione comenzar un documento en blanco y vaya al menú "**Archivo → Información → Propiedades**" y compruebe que los datos corresponden a los del usuario que inició la sesión. 
36. Compruebe las opciones de contenido en línea.		Verifique que, a la hora de editar un documento en Word, por ejemplo, dentro de la pestaña insertar están desmarcadas las opciones de contenido en línea. 

ANEXO A.3. IMPLEMENTACIÓN SEGURA DE MICROSOFT OFFICE 2016 EN UN CLIENTE WINDOWS 10 INDEPENDIENTE

ANEXO A.3.1. CATEGORÍA BÁSICA

ANEXO A.3.1.1. GUÍA PASO A PASO DE IMPLEMENTACIÓN SEGURA

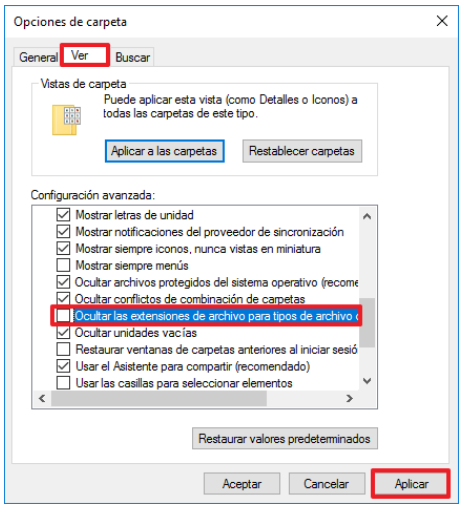
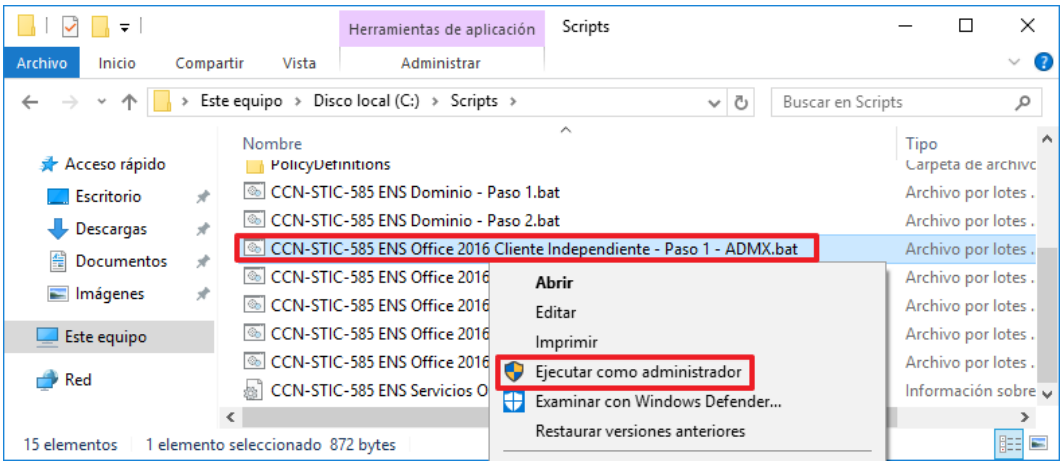
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee la suite de Microsoft Office 2016 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad.

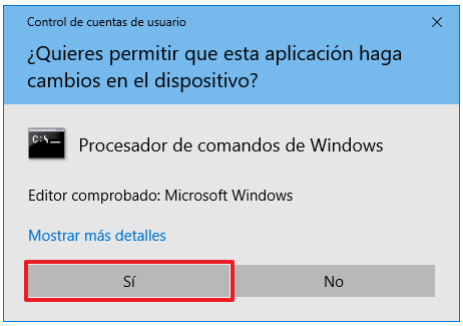
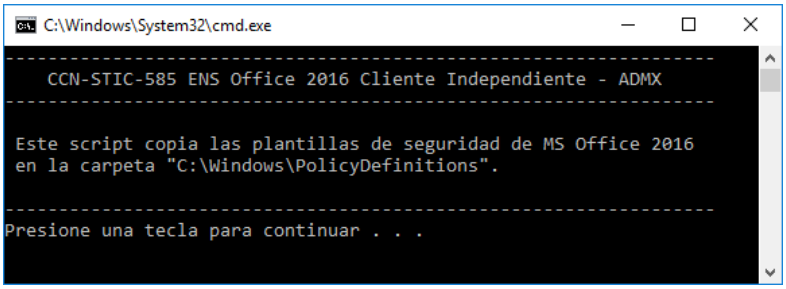
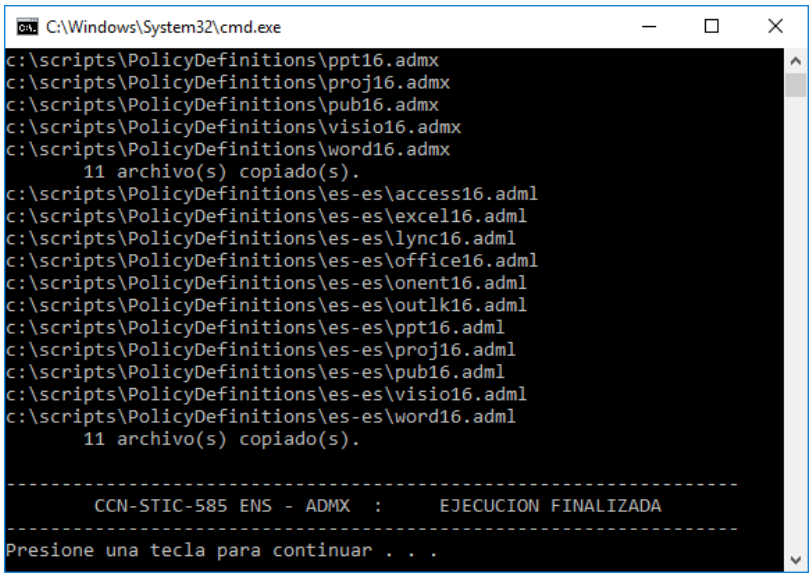
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

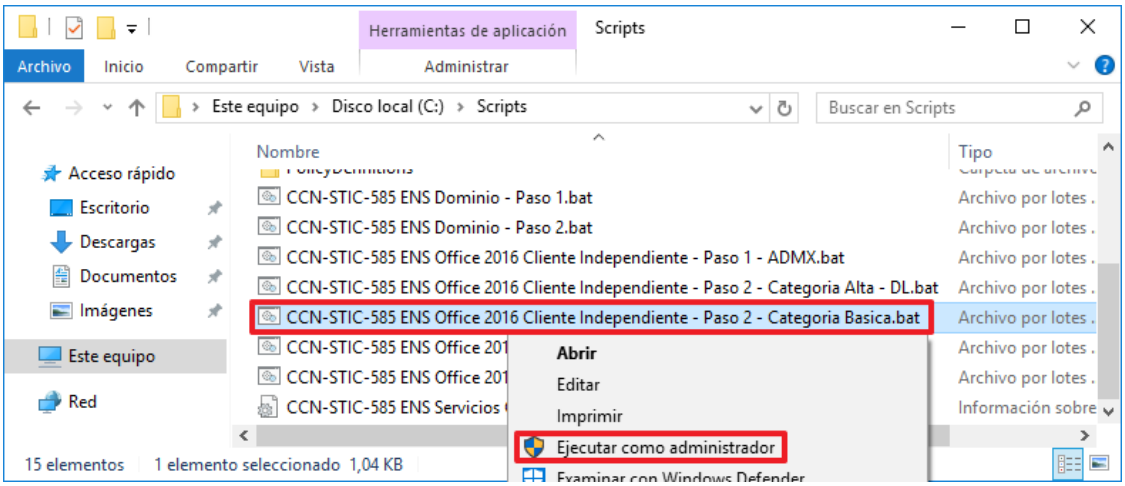
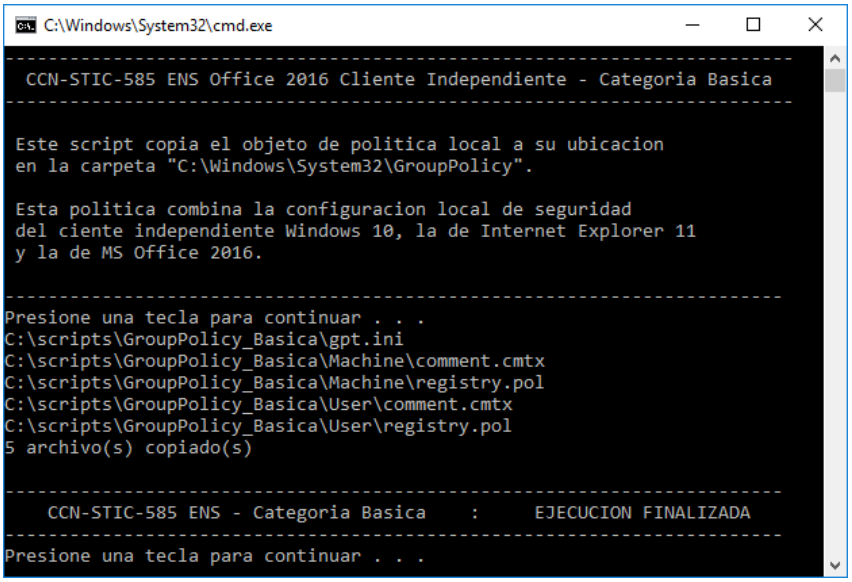
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

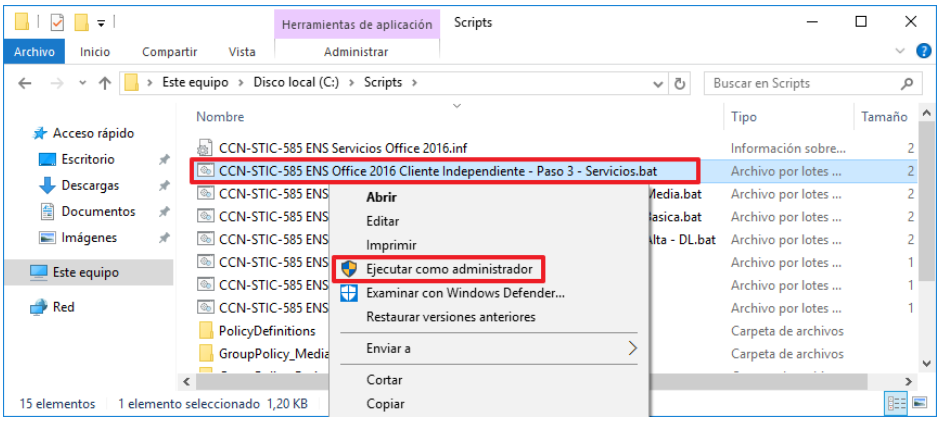
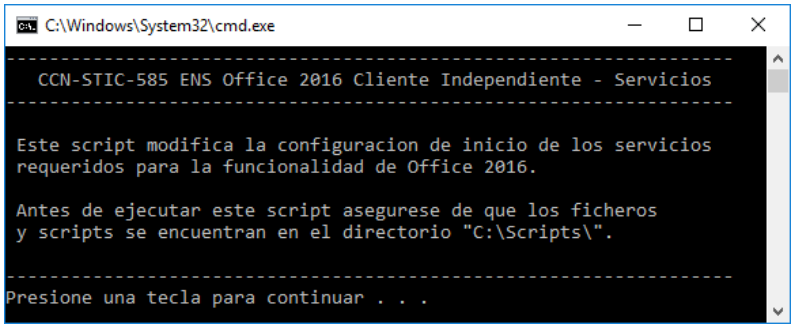
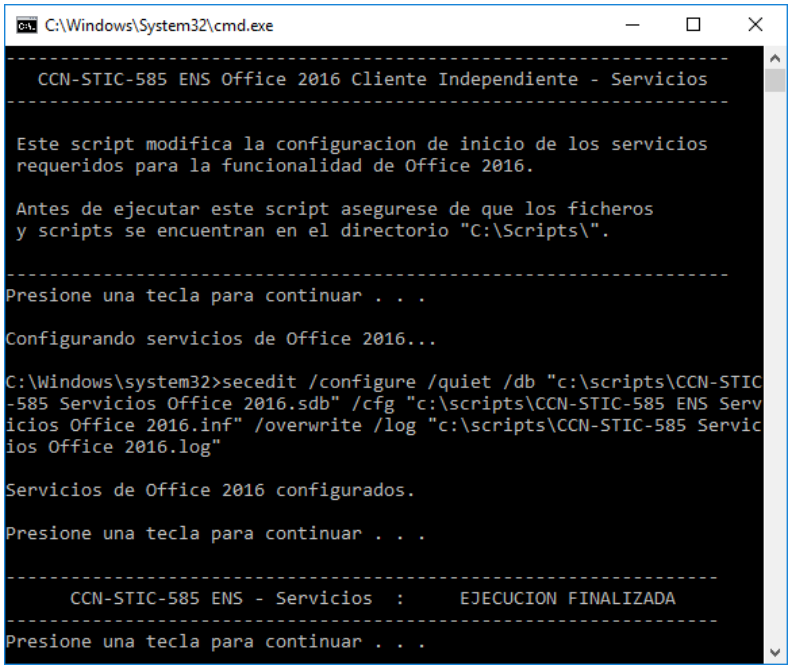
Partiendo de la premisa de que el equipo cuenta con las condiciones de seguridad necesarias para la ejecución de los diferentes productos de la solución ofimática MS Office 2016, se debe proceder a preparar el equipo aplicando las configuraciones de seguridad adecuadas a través de su política local. Previamente a esta configuración paso a paso deberán haberse tenido en cuenta y aplicarse todos los procedimientos descritos en la guía CCN-STIC-599B18 para entornos del ENS en su categoría básica, en clientes independientes.

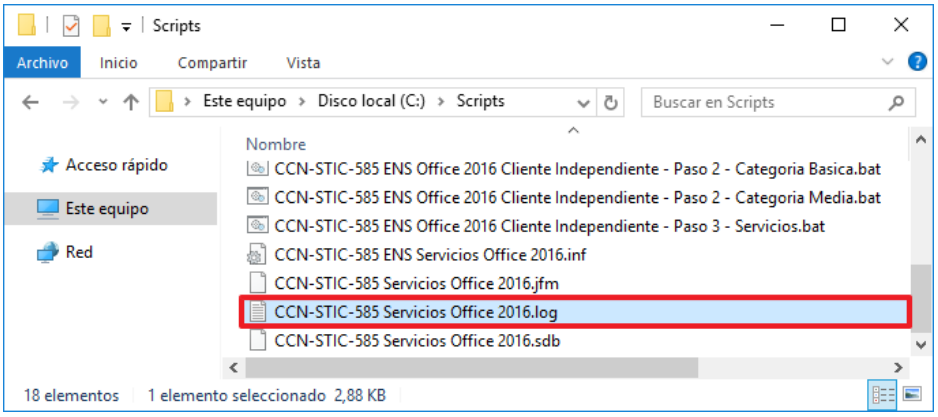
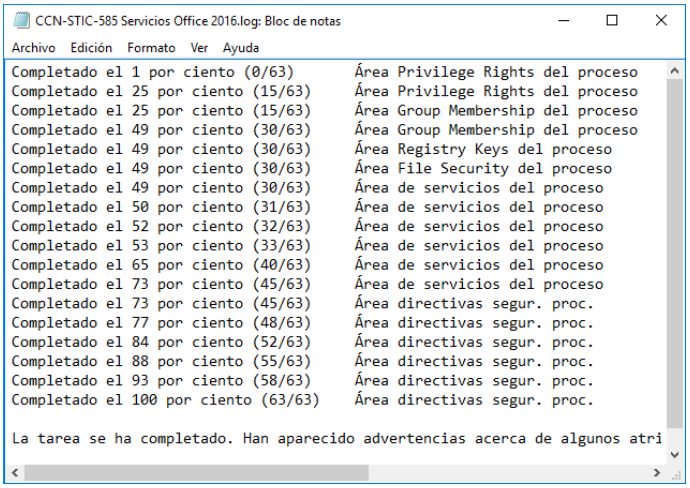
Paso	Descripción
1.	Inicie sesión en el equipo con un usuario local con privilegios de administrador.
2.	Cree el directorio “Scripts” en la unidad “C:\”. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo → Carpeta”.**
3.	Asigne el nombre “Scripts” al nuevo directorio.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema puede solicitar una elevación de privilegios.
5.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.

Paso	Descripción
6.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones". De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".
7.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del cliente, de tal forma que se podrán realizar modificaciones de las políticas generadas. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script “**CCN-STIC-585 ENS Office 2016 Cliente Independiente - Paso1 - 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, 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.

Paso	Descripción
8.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Pulse “Sí” para continuar. 
9.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 
10.	Se producirá la copia de un total de 22 ficheros de plantilla de Office. 
11.	Pulse una tecla para continuar y finalizar la ejecución del *script*.
12.	A continuación, se procederá a realizar la copia de la nueva política de seguridad local que une las directivas del cliente independiente (Windows 10) definidas en la guía CCN-STIC-599B18 y las correspondientes a la presente guía.

Paso	Descripción
13.	Ejecute como administrador el script “CCN-STIC-585 ENS Office 2016 Cliente Independiente - Paso 2 – Categoria Basica.bat”. El sistema le solicitará elevación de privilegios.  **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
14.	Se realizará la copia de 5 ficheros.  **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
15.	Pulse una tecla para finalizar la ejecución del *script*.
16.	El último paso consiste en la configuración de los servicios que se implementarán en la instalación de MS Office 2016.

Paso	Descripción
17.	Ejecute con botón derecho la opción “Ejecutar como administrador” el script “CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat”. El sistema le solicitará elevación de privilegios. 
18.	Ante la solicitud en la descripción deberá pulsar una tecla cualquiera: 
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 

Paso	Descripción
20.	El paso anterior crea un fichero histórico para poderlo revisar en caso de error, **"CCN-STIC-585 Servicios Office 2016.log"**. 
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados tal y como se muestra en la siguiente imagen.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script "CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat". Si llegado a este punto aún no ha instalado el paquete MS Office 2016, deberá volver a ejecutar el script "CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat" después de la instalación.
22.	Para finalizar, reinicie el equipo.

ANEXO A.3.1.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016

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

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

a) Explorador de Windows.

b) PowerShell.

c) Editor de políticas de grupo locales.

d) Consola de servicios.

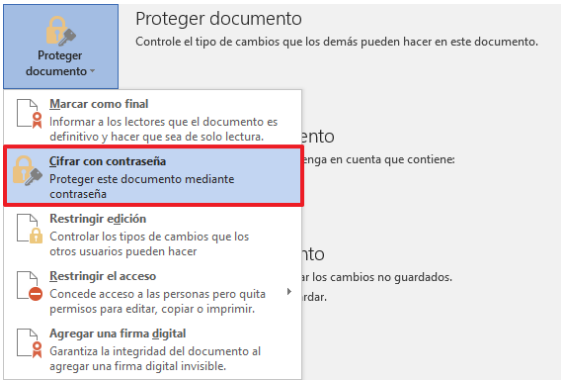
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el puesto de trabajo y ejecute el editor de Políticas de Grupo.		Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador. Ejecute la herramienta Windows PowerShell con privilegios de administrador. Para ello vaya a la siguiente ruta: **"Menú inicio → Todos los programas → Accesorios → Windows PowerShell"** Seleccione mediante botón derecho en Windows PowerShell la opción "Ejecutar como administrador". En la *shell* abierta ejecute "**gpedit.msc**". **Nota:** El sistema le solicitará elevación de privilegios.
2. Verifique los valores de seguridad de MS Office 2016 para el equipo.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración del equipo → Plantillas administrativas → Microsoft Office 2016 (Equipo) → Configuración de seguridad"**
	Directiva	**Valor** / **OK/NOK**
	Deshabilitar el almacenamiento en caché de contraseñas	Habilitada
	Deshabilitar reparación de paquetes	Habilitada
3. Verifique los valores de seguridad aplicados de MS Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad"**
	Directiva	**Valor** / **OK/NOK**
	Examinar macros cifradas en libros de formato Open XML de Excel	Habilitada (Examinar macros cifradas (predeterminado))
4. Verifique los valores del Centro de confianza de MS Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza"**
	Directiva	**Valor** / **OK/NOK**
	Bloquear la ejecución de macros en archivos de Office procedentes de Internet	Habilitada

Comprobación	OK/NOK	Cómo hacerlo		
5. Verifique los valores de Ayuda de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Ayuda"**		
		Directiva	**Valor**	**OK/NOK**
		Búsqueda federada para obtener ayuda	Deshabilitada	
6. Verifique los valores de Configuración de seguridad de MS Office 2016 usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad"**		
		Directiva	**Valor**	**OK/NOK**
		Establecer longitud mínima de contraseña	Habilitada (8)	
		Establecer nivel de reglas de contraseña	Habilitada (Comprobación de longitud local)	
		Seguridad de automatización	Habilitada (Deshabilitar macros de forma predeterminada)	
7. Verifique los valores del panel de telemetría de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Panel de telemetría"**		
		Directiva	**Valor**	**OK/NOK**
		Activar la recopilación de datos de telemetría	Deshabilitada	
8. Verifique los valores centro de confianza de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Privacidad → Centro de confianza"**		
		Directiva	**Valor**	**OK/NOK**
		Deshabilitar el Asistente para participar la primera vez que se ejecute	Habilitada	
		Enviar comentarios de Office	Deshabilitada	
		Enviar información personal	Deshabilitada	
		Directiva	**Valor**	**OK/NOK**
		Habilitar programa de mejora de experiencia del cliente	Deshabilitada	
		Permitir la inclusión de capturas de pantalla con los comentarios de Office	Deshabilitada	
9. Verifique los valores de Varios de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Varios"**		
		Directiva	**Valor**	**OK/NOK**
		Mostrar inicio de sesión OneDrive	Deshabilitada	

Comprobación	OK/NOK	Cómo hacerlo		
	Ocultar las ubicaciones de archivos al abrir o guardar archivos		Habilitada (Ocultar OneDrive Personal, SharePoint Online y OneDrive para la Empresa)	
10. Verifique los valores de Autoarchivar de Microsoft Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro → Autoarchivar"**		
	Directiva		**Valor**	**OK/NOK**
	Deshabilitar Archivo/Archivar		Habilitada	
11. Verifique los valores de configuración PST de Microsoft Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Varios → Configuración PST"**		
	Directiva		**Valor**	**OK/NOK**
	Evitar que los usuarios agreguen archivos PST a perfiles de Outlook y/o evitar el uso de archivos PST para compartirlos de manera exclusiva		Habilitada (se pueden agregar archivos PST)	
	Impedir a los usuarios agregar nuevo contenido a archivos PST existentes		Habilitada	

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique que están configurados los servicios de MS Office 2016		Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador. Ejecute la herramienta "Windows PowerShell" con privilegios de administrador. Para ello vaya a la siguiente ruta: **"Menú inicio → Todos los programas → Accesorios → Windows PowerShell"** Seleccione mediante botón derecho en Windows PowerShell la opción **"Ejecutar como administrador"**. En la shell abierta ejecute **services.msc**. Compruebe que los siguientes servicios se encuentran configurados en modo manual: – Office Source Engine – Servicio de caché de fuentes de Windows – Servicio Hacer clic y ejecutar de Microsoft Office **Nota:** Dependiendo de la versión de Office instalada puede aparecer el servicio "OSE" o "OSE64" y puede no aparecer el servicio "ClickToRunSvc".

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

13. Compruebe que las aplicaciones de MS Office 2016 funcionan correctamente		Pruebe a abrir alguna de las aplicaciones de MS Office 2016, como, por ejemplo, MS Word, MS Excel o MS PowerPoint. Compruebe que puede crear un nuevo documento y guardarlo.
14. Compruebe que puede proteger un documento con contraseña y que esta es robusta.		Proteja un documento con contraseña. Para ello acceda al menú "**Archivo → Información → Proteger documento → Cifrar con contraseña**".  Compruebe que no puede introducir una contraseña inferior a 8 caracteres.
15. Compruebe los metadatos de los archivos.		Abra cualquiera de las aplicaciones de la *suite* Office, por ejemplo Word, seleccione comenzar un documento en blanco y vaya al menú "**Archivo → Información → Propiedades**" y compruebe que los datos corresponden a los del usuario que inició la sesión.

Comprobación	OK/NOK	Cómo hacerlo
		

ANEXO A.3.2. CATEGORÍA MEDIA

ANEXO A.3.2.1. GUÍA PASO A PASO DE IMPLEMENTACIÓN SEGURA

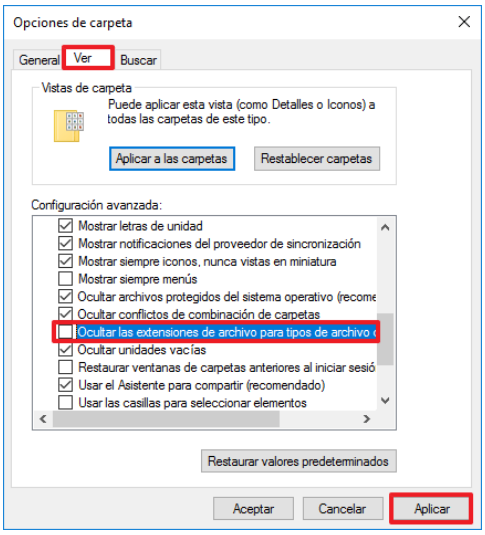
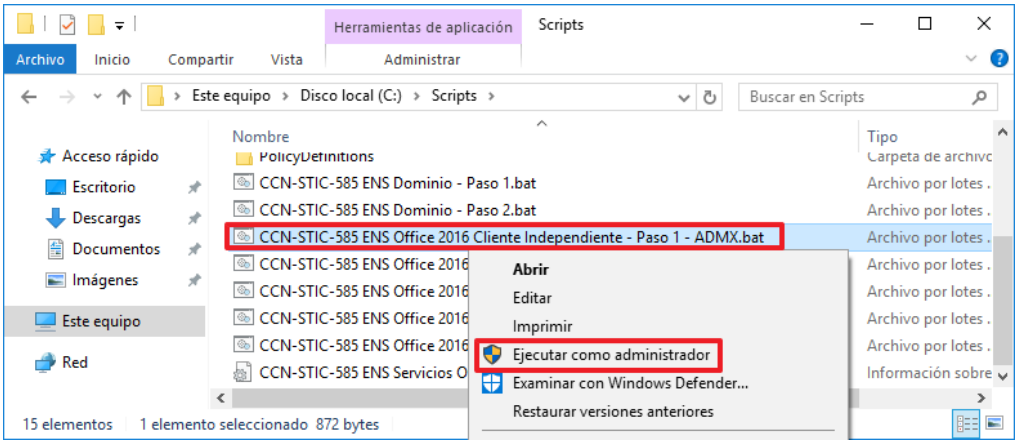
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee la suite de Microsoft Office 2016 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

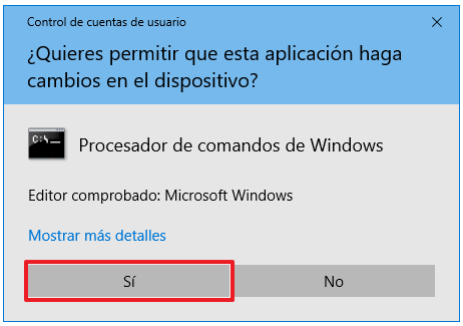
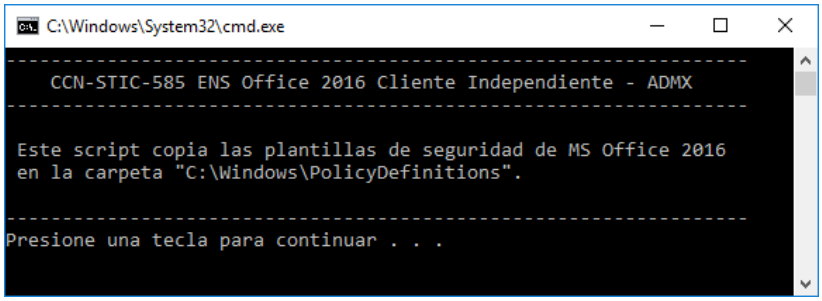
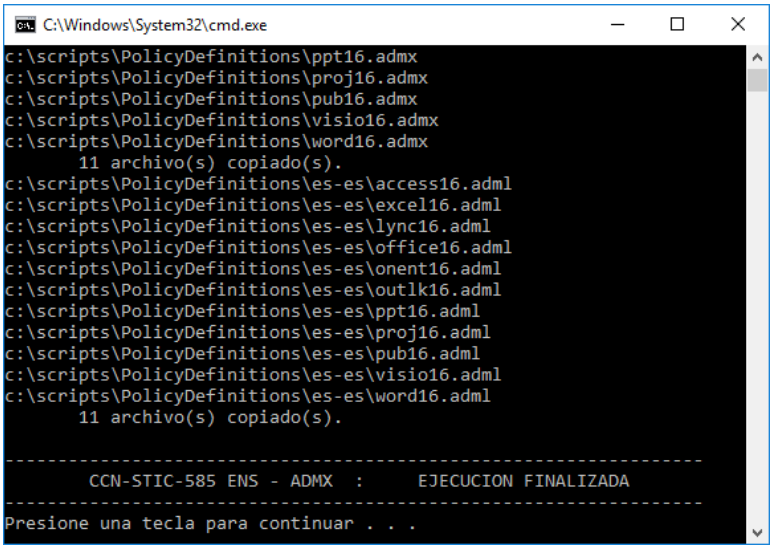
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

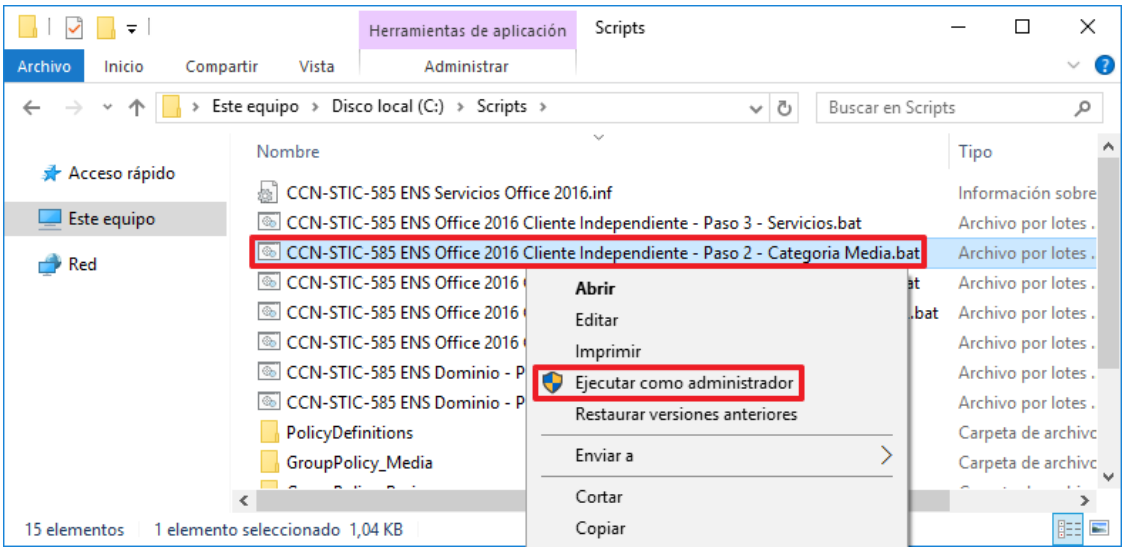
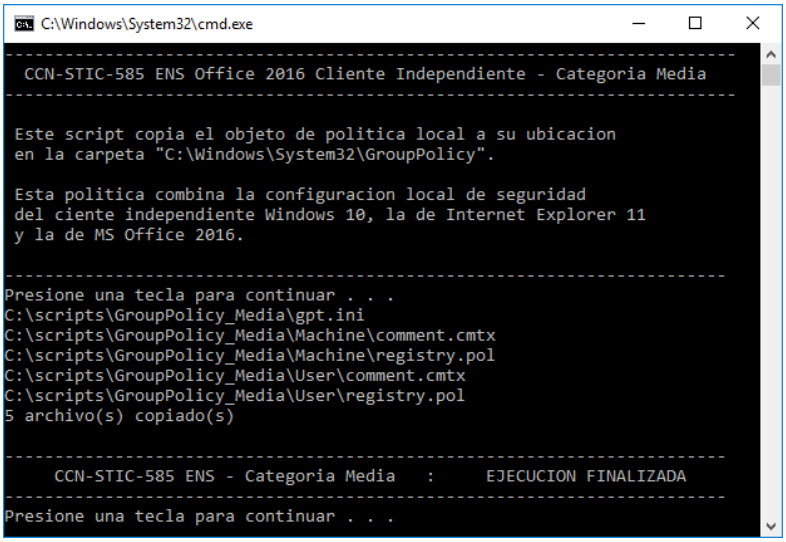
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

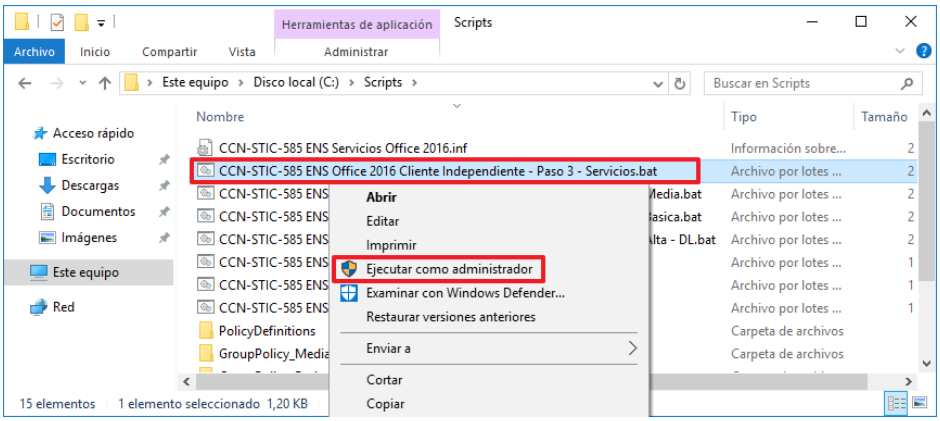
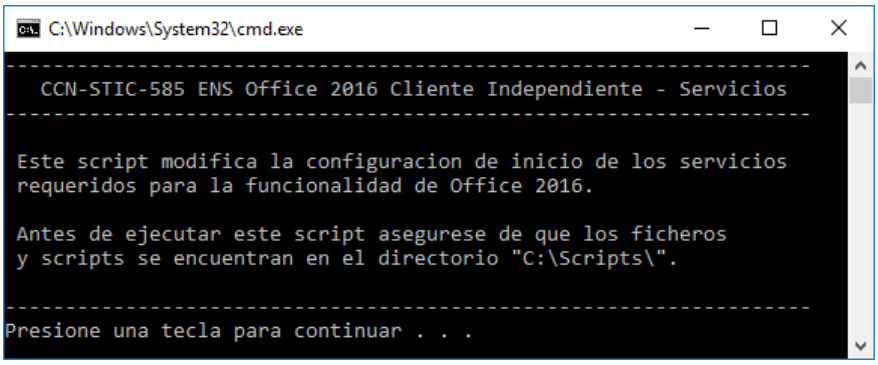
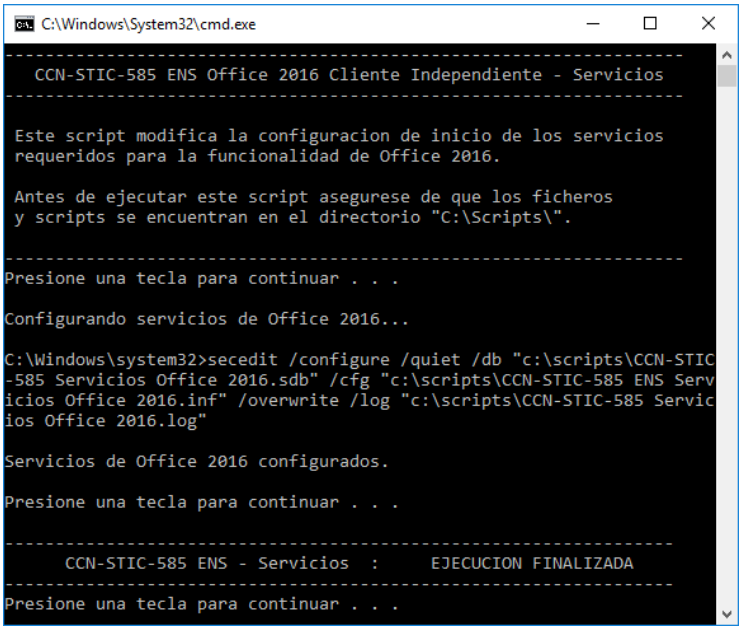
Partiendo de la premisa de que el equipo cuenta con las condiciones de seguridad necesarias para la ejecución de los diferentes productos de la solución ofimática MS Office 2016, se debe proceder a preparar el equipo aplicando las configuraciones de seguridad adecuadas a través de su política local. Previamente a esta configuración paso a paso deberán haberse tenido en cuenta y aplicarse todos los procedimientos descritos en la guía CCN-STIC-599B18 para entornos del ENS en su categoría media, en clientes independientes.

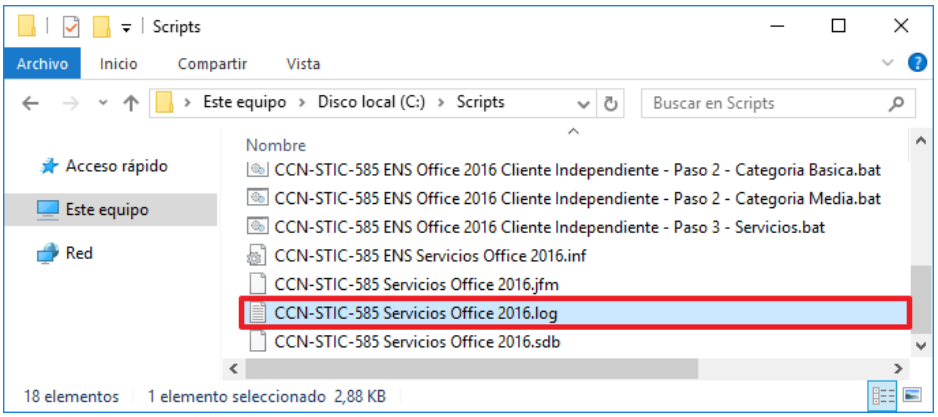
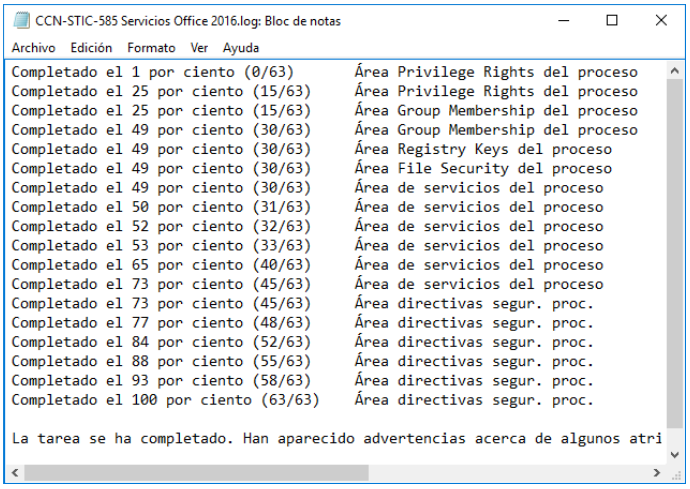
Paso	Descripción
1.	Inicie sesión en el equipo con un usuario local con privilegios de administrador.
2.	Cree el directorio “Scripts” en la unidad “C:\”. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo → Carpeta”.**
3.	Asigne el nombre “Scripts” al nuevo directorio.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema puede solicitar una elevación de privilegios.
5.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.

Paso	Descripción
6.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".
7.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del cliente, de tal forma que se podrán realizar modificaciones de las políticas generadas. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script “**CCN-STIC-585 ENS Office 2016 Cliente Independiente - Paso1 - 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, 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.

Paso	Descripción
8.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Pulse “Sí” para continuar. 
9.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 
10.	Se producirá la copia de un total de 22 ficheros de plantilla de Office. 
11.	Pulse una tecla para continuar y finalizar la ejecución del *script*.
12.	A continuación, se procederá a realizar la copia de la nueva política de seguridad local que une las directivas del cliente independiente (Windows 10) definidas en la guía CCN-STIC-599B18 y las correspondientes a la presente guía.

Paso	Descripción
13.	Ejecute como administrador el script “CCN-STIC-585 ENS Office 2016 Cliente Independiente - Paso 2 – Categoria Media.bat”. El sistema le solicitará elevación de privilegios.  **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
14.	Se realizará la copia de 5 ficheros.  **Nota:** Debe tener en cuenta que **la nueva política reemplaza a la anterior**. Si ha realizado modificaciones de la política manualmente sobre las definidas en la guía CCN-STIC-599B18 Seguridad en Windows 10 (cliente independiente), deberá anotar las modificaciones que hubiera efectuado y realizarlas manualmente tras la aplicación de esta nueva directiva.
15.	Pulse una tecla para finalizar la ejecución del *script*.
16.	El último paso consiste en la configuración de los servicios que se implementarán en la instalación de MS Office 2016.

Paso	Descripción
17.	Ejecute con botón derecho la opción “Ejecutar como administrador” el script “CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat”. El sistema le solicitará elevación de privilegios. 
18.	Ante la solicitud en la descripción deberá pulsar una tecla cualquiera: 
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 

Paso	Descripción
20.	El paso anterior crea un fichero histórico para poderlo revisar en caso de error, **"CCN-STIC-585 Servicios Office 2016.log"**. 
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados tal y como se muestra en la siguiente imagen.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script "CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat". Si llegado a este punto aún no ha instalado el paquete MS Office 2016, deberá volver a ejecutar el script "CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat" después de la instalación.
22.	Para finalizar, reinicie el equipo.

ANEXO A.3.2.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016

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

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

a) Explorador de Windows.

b) PowerShell.

c) Editor de políticas de grupo locales.

d) Consola de servicios.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>1. Inicie sesión en el puesto de trabajo y ejecute el editor de Políticas de Grupo.</td><td></td><td>Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador.
Ejecute la herramienta Windows PowerShell con privilegios de administrador. Para ello vaya a la siguiente ruta:
“Menú inicio → Todos los programas → Accesorios → Windows PowerShell”
Seleccione mediante botón derecho en Windows PowerShell la opción “Ejecutar como administrador”.
En la shell abierta ejecute “gpedit.msc”.
Nota: El sistema le solicitará elevación de privilegios.</td></tr>
<tr><td rowspan="3">2. Verifique los valores de seguridad de MS Office 2016 para el equipo.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración del equipo → Plantillas administrativas → Microsoft Office 2016 (Equipo) → Configuración de seguridad”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Deshabilitar el almacenamiento en caché de contraseñas</td><td>Habilitada</td><td></td></tr>
<tr><td>Deshabilitar reparación de paquetes</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
<tr><td rowspan="3">3. Verifique los valores de seguridad aplicados de MS Excel 2016 de usuario.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Examinar macros cifradas en libros de formato Open XML de Excel</td><td>Habilitada (Examinar macros cifradas (predeterminado))</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
<tr><td rowspan="3">4. Verifique los valores del Centro de confianza de MS Excel 2016 de usuario.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza”</td></tr>
<tr><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Bloquear la ejecución de macros en archivos de Office procedentes de Internet</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
5. Verifique los valores de la Vista protegida de MS Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza → Vista protegida"**		
		Directiva	**Valor**	**OK/NOK**
		Abrir archivos de UNC de intranet local en Vista protegida	Deshabilitada	
		Desactivar Vista protegida para los datos adjuntos abiertos en Outlook	Deshabilitada	
		Establecer el comportamiento del documento en caso de error en la validación de documento	Habilitado (Bloquear archivos, No permitir edición)	
		No abrir archivos de la zona de Internet en Vista protegida	Deshabilitado	
		No abrir archivos de ubicaciones inseguras en Vista protegida	Deshabilitado	
6. Verifique los valores de Varios de MS Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Varios"**		
		Directiva	**Valor**	**OK/NOK**
		No almacenar archivos de red en la memoria caché local	Habilitada	
7. Verifique los valores de Ayuda de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Ayuda"**		
		Directiva	**Valor**	**OK/NOK**
		Búsqueda federada para obtener ayuda	Deshabilitada	
8. Verifique los valores de Configuración de seguridad de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad"**		
		Directiva	**Valor**	**OK/NOK**
		Establecer longitud mínima de contraseña	Habilitada (10)	
		Directiva	**Valor**	**OK/NOK**
		Establecer nivel de reglas de contraseña	Habilitada (Comprobación de longitud local)	
		Seguridad de automatización	Habilitada (Deshabilitar macros de forma predeterminada)	
9. Verifique los valores de Catálogos de confianza de MS		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad → Centro de confianza → Catálogos de confianza"**		

Comprobación	OK/NOK	Cómo hacerlo		
Office 2016 de usuario.				
		Directiva	**Valor**	**OK/NOK**
		Bloquear complementos web	Habilitada	
		Bloquear Tienda Office	Habilitada	
10. Verifique los valores de Contenido en línea de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Herramientas | Opciones | General | Opciones de servicios… → Contenido en línea"**		
		Directiva	**Valor**	**OK/NOK**
		Opciones de contenido en línea	Habilitada (No permitir que Office se conecte a Internet)	
		Opciones de nivel de servicio	Habilitada (Solo servicios de Microsoft)	
11. Verifique los valores del Panel de telemetría de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Panel de telemetría"**		
		Directiva	**Valor**	**OK/NOK**
		Activar la recopilación de datos de telemetría	Deshabilitada	
12. Verifique los valores del Centro de confianza de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Privacidad → Centro de confianza"**		
		Directiva	**Valor**	**OK/NOK**
		Deshabilitar el Asistente para participar la primera vez que se ejecute	Habilitada	
		Enviar comentarios de Office	Deshabilitada	
		Enviar información personal	Deshabilitada	
		Directiva	**Valor**	**OK/NOK**
		Habilitar programa de mejora de experiencia del cliente	Deshabilitada	
		Permitir la inclusión de capturas de pantalla con los comentarios de Office	Deshabilitada	
13. Verifique los valores de varios de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Varios"**		
		Directiva	**Valor**	**OK/NOK**
		Mostrar características de LinkedIn en aplicaciones de Office	Deshabilitada	
		Mostrar inicio de sesión OneDrive	Deshabilitada	
		Ocultar las ubicaciones de archivos al abrir o guardar archivos	Habilitada (Ocultar OneDrive Personal,	

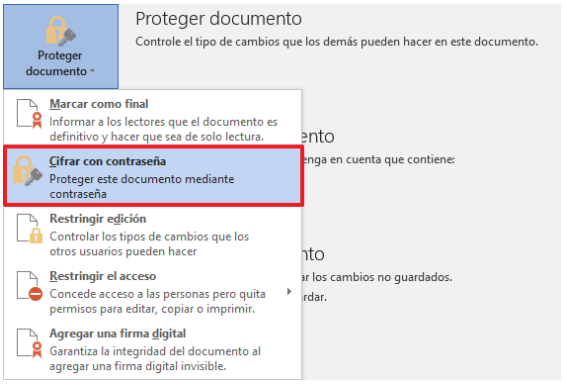
Comprobación	OK/NOK	Cómo hacerlo		
			SharePoint Online y OneDrive para la Empresa)	
14. Verifique las opciones de Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro"**		
		Directiva	**Valor**	**OK/NOK**
		Ocultar el botón de Tienda Office	Habilitada	
15. Verifique los valores de autoarchivar de Microsoft Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro → Autoarchivar"**		
		Directiva	**Valor**	**OK/NOK**
		Deshabilitar Archivo/Archivar	Habilitada	
16. Verifique los valores de seguridad de criptografía de Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Seguridad → Criptografía"**		
		Directiva	**Valor**	**OK/NOK**
		Advertencia de firma	Habilitada (Advertir siempre sobre las firmas no válidas)	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4">17. Verifique los valores de configuración pst de Outlook 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Varios → Configuración PST”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que los usuarios agreguen archivos PST a perfiles de Outlook y/o evitar el uso de archivos PST para compartirlos de manera exclusiva</td><td>Habilitada (se pueden agregar archivos PST)</td><td></td></tr>
<tr><td colspan="2">Impedir a los usuarios agregar nuevo contenido a archivos PST existentes</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="7">18. Verifique los valores de la Vista protegida de MS PowerPoint 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft PowerPoint 2016 → Opciones de PowerPoint → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Abrir archivos de UNC de intranet local en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de la zona de Internet en Vista protegida</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de ubicaciones inseguras en Vista protegida</td><td>Deshabilitado</td><td></td></tr>
<tr><td rowspan="5">19. Verifique los valores de la Vista protegida de MS Word 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Word 2016 → Opciones de Word → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Abrir archivos de UNC de intranet local en la Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
<tr><td rowspan="3"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">No abrir archivos de la zona de Internet en la Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de ubicaciones inseguras en la Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td>20. Verifique que están configurados los</td><td></td><td colspan="3">Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador.</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
servicios de MS Office 2016		Ejecute la herramienta "Windows PowerShell" con privilegios de administrador. Para ello vaya a la siguiente ruta: **"Menú inicio → Todos los programas → Accesorios → Windows PowerShell"** Seleccione mediante botón derecho en Windows PowerShell la opción **"Ejecutar como administrador"**. En la shell abierta ejecute **services.msc**. Compruebe que los siguientes servicios se encuentran configurados en modo manual: – Office Source Engine – Servicio de caché de fuentes de Windows – Servicio Hacer clic y ejecutar de Microsoft Office **Nota:** Dependiendo de la versión de Office instalada puede aparecer el servicio "OSE" o "OSE64" y puede no aparecer el servicio "ClickToRunSvc". El sistema solicitará elevación de privilegios.

Servicio (nombre corto)	Servicio (nombre largo)	Inicio	Permiso	OK/NOK
ClickToRunSvc	Servicio Hacer clic y ejecutar de Microsoft Office	Manual	Configurado	
FontCache	Servicio de caché de fuentes de Windows	Manual	Configurado	
OSE	Office Source Engine	Manual	Configurado	
OSE64	Office 64 Source Engine	Manual	Configurado	

21. Compruebe que las aplicaciones de MS Office 2016 funcionan correctamente		Pruebe a abrir alguna de las aplicaciones de MS Office 2016, como, por ejemplo, MS Word, MS Excel o MS PowerPoint. Compruebe que puede crear un nuevo documento y guardarlo.

Comprobación	OK/NOK	Cómo hacerlo
22. Compruebe que puede proteger un documento con contraseña y que esta es robusta.		Proteja un documento con contraseña. Para ello acceda al menú "**Archivo → Información → Proteger documento → Cifrar con contraseña**".  Compruebe que no puede introducir una contraseña inferior a 10 caracteres.
23. Compruebe los metadatos de los archivos.		Abra cualquiera de las aplicaciones de la *suite* Office, por ejemplo Word, seleccione comenzar un documento en blanco y vaya al menú "**Archivo → Información → Propiedades**" y compruebe que los datos corresponden a los del usuario que inició la sesión. 
24. Compruebe las opciones de contenido en línea.		Verifique que, a la hora de editar un documento en Word, por ejemplo, dentro de la pestaña insertar están desmarcadas las opciones de contenido en línea. 

ANEXO A.3.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.3.3.1. GUÍA PASO A PASO DE IMPLEMENTACIÓN SEGURA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee la suite Microsoft Office 2016 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.

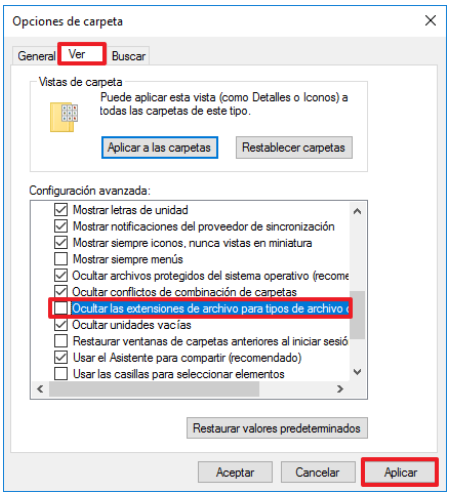
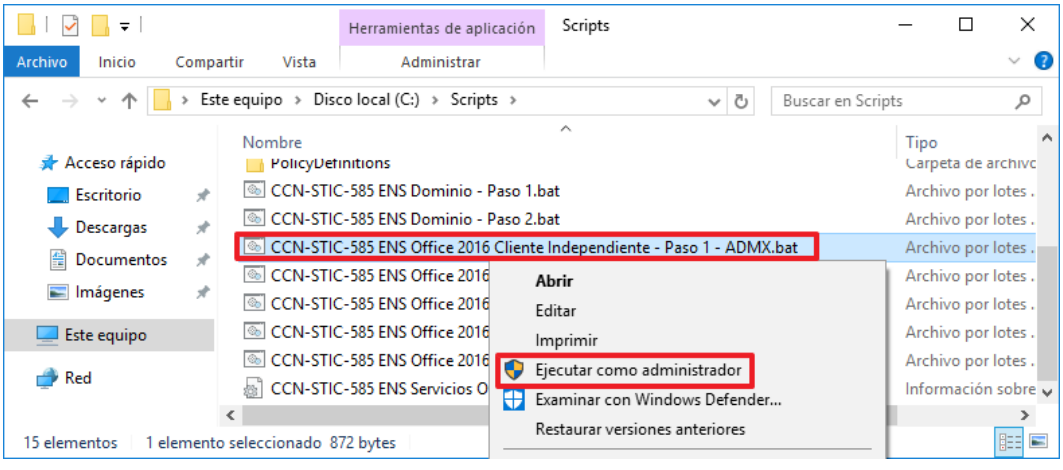
Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

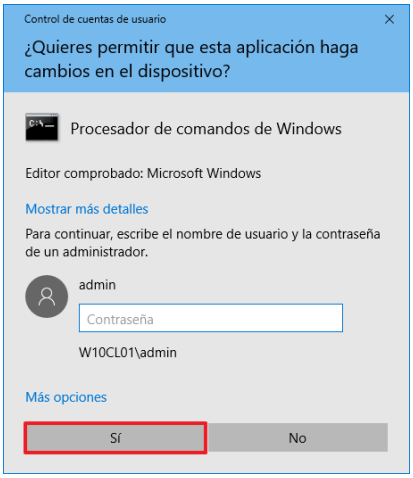
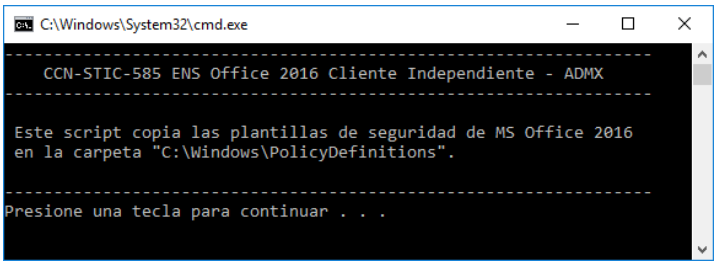
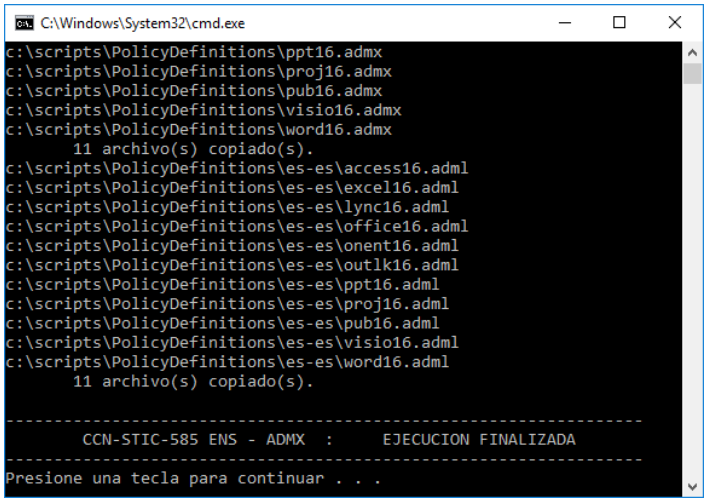
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho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

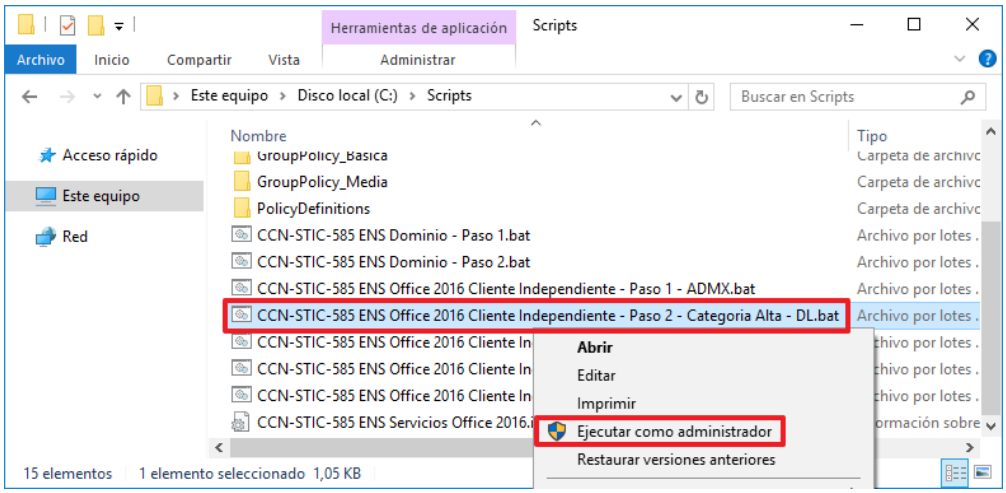
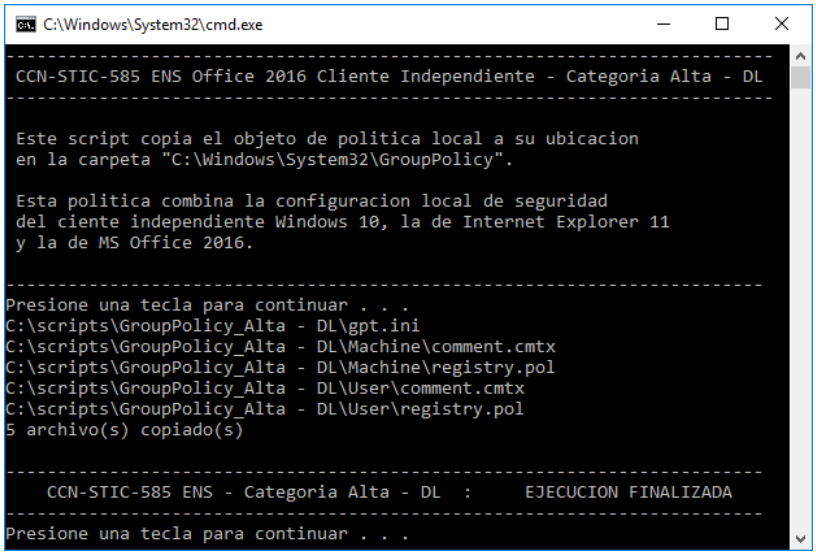
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

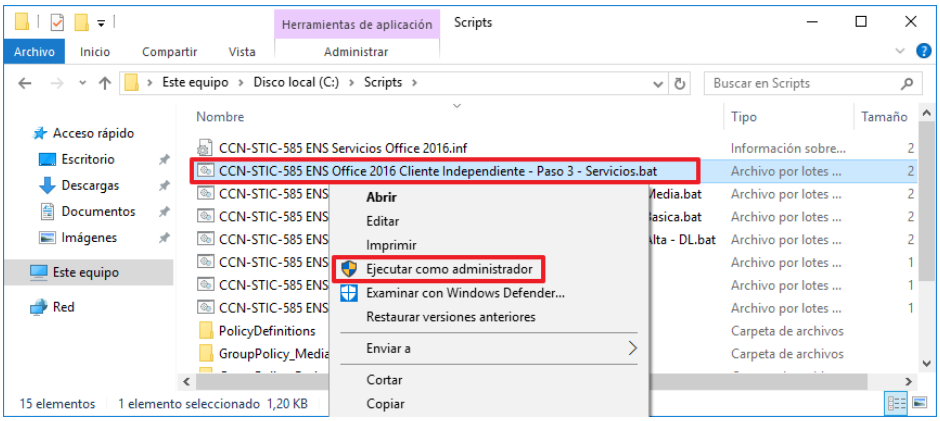
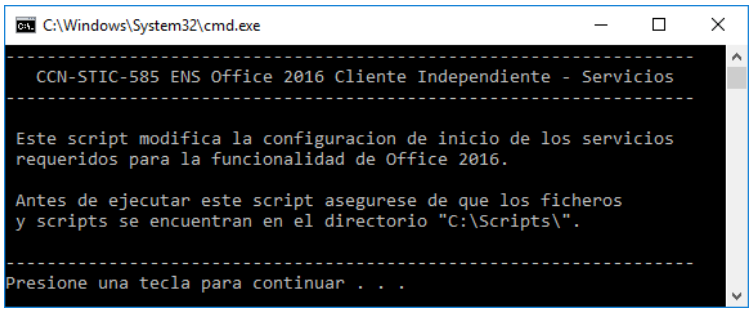
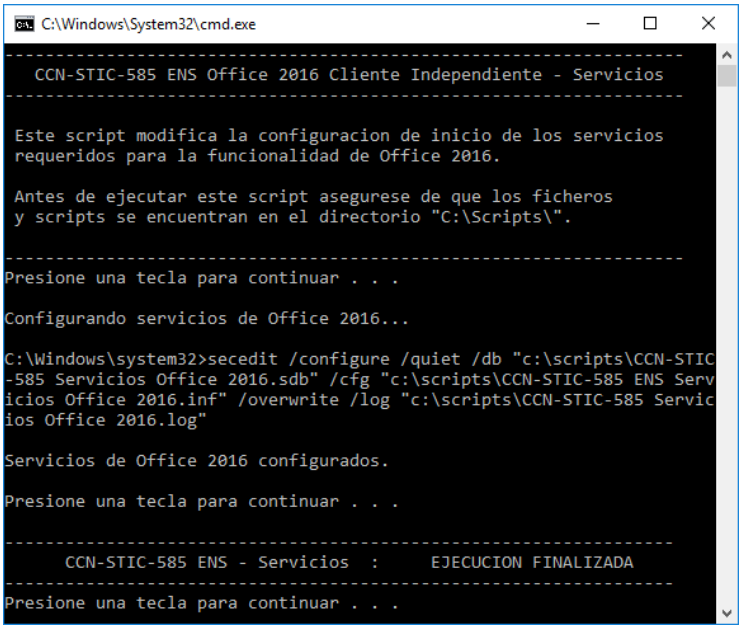
Partiendo de la premisa de que el equipo cuenta con las condiciones de seguridad necesarias para la ejecución de los diferentes productos de la solución ofimática MS Office 2016, se debe proceder a preparar el equipo aplicando las configuraciones de seguridad adecuadas a través de su política local. Previamente a esta configuración paso a paso deberán haberse tenido en cuenta y aplicarse todos los procedimientos descritos en la guía CCN-STIC-599B18 para la categoría alta del ENS o Difusión Limitada, en clientes independientes.

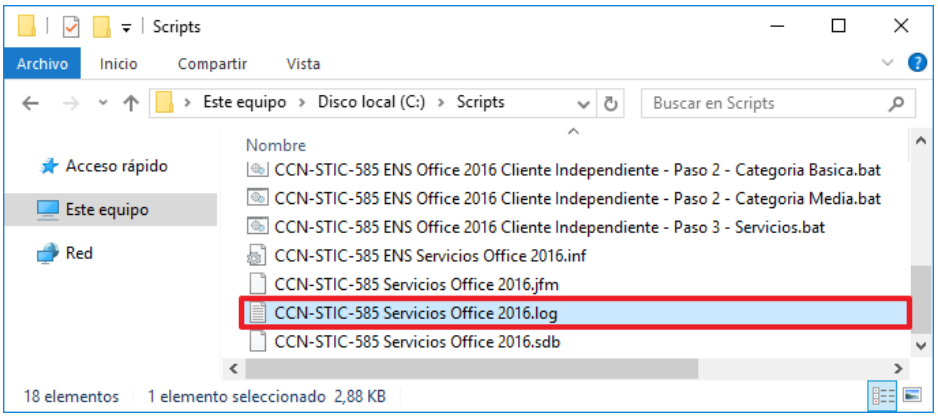
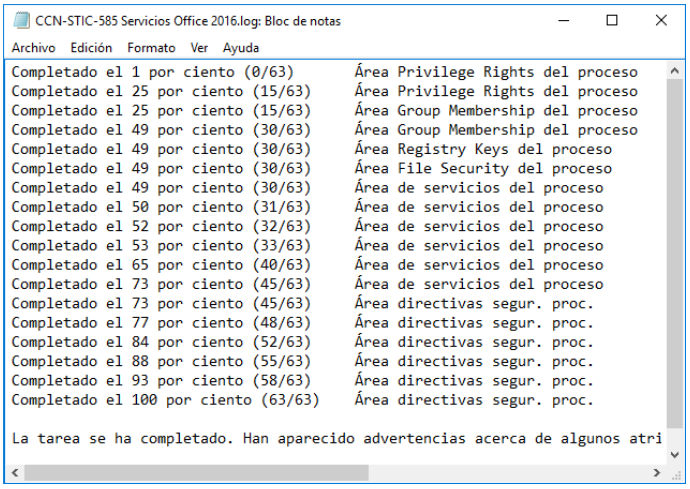
Paso	Descripción
1.	Inicie sesión en el equipo con un usuario local con privilegios de administrador.
2.	Cree el directorio “Scripts” en la unidad “C:\”. Pulse con el botón derecho del ratón sobre un espacio en blanco y seleccione **“Nuevo → Carpeta”.**
3.	Asigne el nombre “Scripts” al nuevo directorio.
4.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
5.	Configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, el 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.

Paso	Descripción
6.	Para configurar el Explorador de Windows y mostrar las extensiones de todos los archivos, abra una ventana de Explorador de Windows, seleccione el menú “Vista” y dentro de dicho menú, "Opciones". De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), 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".
7.	Deberán copiarse las plantillas .admx y .adml de MS Office 2016 en el repositorio local del cliente, de tal forma que se podrán realizar modificaciones de las políticas generadas. Ejecute con permisos de administrador (opción "Ejecutar como administrador") el script “**CCN-STIC-585 ENS Office 2016 Cliente Independiente - Paso1 - 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, 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.

Paso	Descripción
8.	El control de cuentas de usuario le solicitará de nuevo elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador y pulse "Sí" para continuar. 
9.	Se lanzará un intérprete de comandos como el mostrado en la siguiente imagen. Será preciso que presione cualquier tecla varias veces durante la ejecución del script, siguiendo las instrucciones que éste muestre en pantalla. 
10.	Se producirá la copia de un total de 22 ficheros de plantilla de Office. 
11.	Pulse una tecla para continuar y finalizar la ejecución del *script*.
12.	A continuación, se procederá a realizar la copia de la nueva política de seguridad local que une las directivas del cliente independiente (Windows 10) definidas en la guía CCN-STIC-599B18 y las correspondientes a la presente guía.

Paso	Descripción
13.	Ejecute como administrador el script “CCN-STIC-585 ENS Office 2016 Cliente Independiente - Paso 2 – Categoria Alta - DL.bat”. El sistema le solicitará elevación de privilegios.  **Nota:** Recuerde que las políticas han sido diseñadas para entornos de seguridad. Deberá modificar las políticas para amoldarlas a su organización.
14.	Se realizará la copia de 5 ficheros.  **Nota:** Debe tener en cuenta que **la nueva política reemplaza a la anterior**. Si ha realizado modificaciones de la política manualmente sobre las definidas en la guía CCN-STIC-599B18 Seguridad en Windows 10 (cliente independiente), deberá anotar las modificaciones que hubiera efectuado y realizarlas manualmente tras la aplicación de esta nueva directiva.
15.	Pulse una tecla para finalizar la ejecución del *script*.
16.	El último paso consiste en la configuración de los servicios que se implementarán en la instalación de MS Office 2016.

Paso	Descripción
17.	Ejecute con botón derecho la opción “Ejecutar como administrador” el script “CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat”. El sistema le solicitará elevación de privilegios. 
18.	Ante la solicitud en la descripción deberá pulsar una tecla cualquiera: 
19.	Una vez completado el proceso, pulse una tecla para continuar. Pulse de nuevo una tecla para finalizar la ejecución del script. 

Paso	Descripción
20.	El paso anterior crea un fichero histórico para poderlo revisar en caso de error, **"CCN-STIC-585 Servicios Office 2016.log"**. 
21.	Abra este registro para comprobar si la configuración de los servicios ha sido o no correcta. Un proceso de ejecución normal mostrará los resultados tal y como se muestra en la siguiente imagen.  **Nota:** En caso de identificar errores resuelva los mismos y vuelva a ejecutar el script "CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat". Si llegado a este punto aún no ha instalado el paquete MS Office 2016, deberá volver a ejecutar el script "CCN-STIC-585 ENS Office 2016 Cliente Independiente – Paso3 - Servicios.bat" después de la instalación.
22.	Para finalizar, reinicie el equipo.

ANEXO A.3.3.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016

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

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

a) Explorador de Windows.

b) PowerShell.

c) Editor de políticas de grupo locales.

d) Consola de servicios.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>1. Inicie sesión en el puesto de trabajo y ejecute el editor de Políticas de Grupo.</td><td></td><td>Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador.
Ejecute la herramienta Windows PowerShell con privilegios de administrador. Para ello vaya a la siguiente ruta:
“Menú inicio → Todos los programas → Accesorios → Windows PowerShell”
Seleccione mediante botón derecho en Windows PowerShell la opción “Ejecutar como administrador”.
En la shell abierta ejecute “gpedit.msc”.
Nota: El sistema le solicitará elevación de privilegios.</td></tr>
<tr><td rowspan="3">2. Verifique los valores de seguridad de MS Office 2016 para el equipo.</td><td></td><td colspan="2">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración del equipo → Plantillas administrativas → Microsoft Office 2016 (Equipo) → Configuración de seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el almacenamiento en caché de contraseñas</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Deshabilitar reparación de paquetes</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">3. Verifique los valores del centro de confianza de Microsoft Access 2016 de usuario.</td><td></td><td colspan="2">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Access 2016 → Configuración de la aplicación → Seguridad → Centro de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Desactivar documentos confiables</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">4. Verifique los valores de criptografía aplicados de Microsoft Access 2016 de usuario.</td><td></td><td colspan="2">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Access 2016 → Configuración de la aplicación → Seguridad → Criptografía”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Especificar algoritmo hash CNG</td><td>Habilitada (SHA512)</td><td></td></tr>
<tr><td colspan="2">Especificar compatibilidad de cifrado</td><td>Habilitada</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
	Especificar longitud de contraseña CNG con sal		Habilitada (32)	
5. Verifique los valores de seguridad aplicados de Microsoft Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad"**		
	Directiva		**Valor**	**OK/NOK**
	Examinar macros cifradas en libros de formato Open XML de Excel		Habilitada (Examinar macros cifradas (predeterminado))	
6. Verifique los valores del Centro de confianza de MS Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza"**		
	Directiva		**Valor**	**OK/NOK**
	Bloquear la ejecución de macros en archivos de Office procedentes de Internet		Habilitada	
7. Verifique los valores de la Vista protegida de MS Excel 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Centro de confianza → Vista protegida"**		
	Directiva		**Valor**	**OK/NOK**
	Abrir archivos de UNC de intranet local en Vista protegida		Deshabilitada	
	Desactivar Vista protegida para los datos adjuntos abiertos en Outlook		Deshabilitada	
	Establecer el comportamiento del documento en caso de error en la validación de documento		Habilitado (Bloquear archivos, No permitir edición)	
	No abrir archivos de la zona de Internet en Vista protegida		Deshabilitado	
	No abrir archivos de ubicaciones inseguras en Vista protegida		Deshabilitado	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="6">8. Verifique los valores de criptografía aplicados de Microsoft Excel 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Opciones de Excel → Seguridad → Criptografía”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Especificar algoritmo hash CNG</td><td>Habilitada (SHA512)</td><td></td></tr>
<tr><td colspan="2">Especificar compatibilidad de cifrado</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Especificar longitud de contraseña CNG con sal</td><td>Habilitada (32)</td><td></td></tr>
<tr><td colspan="2">Usar nueva clave cuando cambie la contraseña</td><td>Habilitado</td><td></td></tr>
<tr><td rowspan="3">9. Verifique los valores de Varios de MS Excel 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Excel 2016 → Varios”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">No almacenar archivos de red en la memoria caché local</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="3">10. Verifique los valores de Ayuda de MS Office 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Ayuda”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Búsqueda federada para obtener ayuda</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="5">11. Verifique los valores de Configuración de seguridad de MS Office 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Establecer longitud mínima de contraseña</td><td>Habilitada (12)</td><td></td></tr>
<tr><td colspan="2">Establecer nivel de reglas de contraseña</td><td>Habilitada (Comprobaciones de longitud local)</td><td></td></tr>
<tr><td colspan="2">Seguridad de automatización</td><td>Habilitada (Deshabilitar macros de forma predeterminada)</td><td></td></tr>
</table>

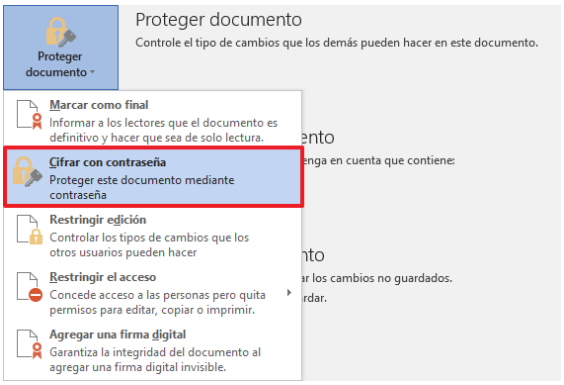
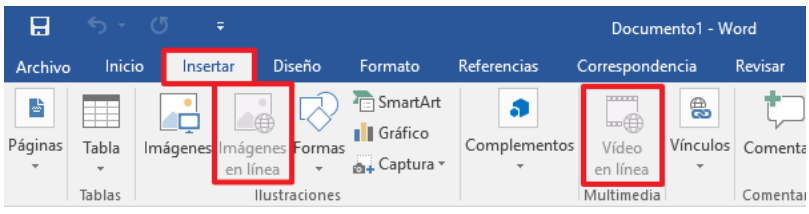
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4">12. Verifique los valores de Catálogos de confianza de MS Office 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Configuración de seguridad → Centro de confianza → Catálogos de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Bloquear complementos web</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Bloquear Tienda Office</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="4">13. Verifique los valores de Contenido en línea de MS Office 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Herramientas | Opciones | General | Opciones de servicios… → Contenido en línea”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Opciones de contenido en línea</td><td>Habilitada (No permitir que Office se conecte a Internet)</td><td></td></tr>
<tr><td colspan="2">Opciones de nivel de servicio</td><td>Habilitada (Sólo servicios de Microsoft)</td><td></td></tr>
<tr><td rowspan="4">14. Verifique los valores del Panel de telemetría de MS Office 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Panel de telemetría”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Activar la recopilación de datos de telemetría</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="6">15. Verifique los valores del Centro de confianza de MS Office 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:
“Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Privacidad → Centro de confianza”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Deshabilitar el Asistente para participar la primera vez que se ejecute</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Enviar comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Enviar información personal</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar programa de mejora de experiencia del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir la inclusión de capturas de pantalla con los comentarios de Office</td><td>Deshabilitada</td><td></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo		
16. Verifique los valores de varios de MS Office 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Office 2016 → Varios"**		
		Directiva	**Valor**	**OK/NOK**
		Abrir vínculos de archivos de Office en Office Online	Deshabilitado	
		Mostrar características de LinkedIn en aplicaciones de Office	Deshabilitada	
		Mostrar inicio de sesión OneDrive	Deshabilitada	
		Ocultar las ubicaciones de archivos al abrir o guardar archivos	Habilitada (Ocultar OneDrive Personal, SharePoint Online y OneDrive para la Empresa)	
17. Verifique los valores de criptografía aplicados de Microsoft Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Seguridad → Criptografía"**		
		Directiva	**Valor**	**OK/NOK**
		Advertencia de firma	Habilitada (Advertir siempre sobre las firmas no válidas)	
18. Verifique las opciones de Otro en Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro"**		
		Directiva	**Valor**	**OK/NOK**
		Ocultar el botón de Tienda Office	Habilitada	
19. Verifique los valores de seguridad de autoarchivar de Microsoft Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Opciones de Outlook → Otro → Autoarchivar"**		
		Directiva	**Valor**	**OK/NOK**
		Deshabilitar Archivo/Archivar	Habilitada	
20. Verifique los valores de seguridad de criptografía de Outlook 2016 de usuario.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores: **"Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Seguridad → Criptografía"**		
		Directiva	**Valor**	**OK/NOK**
		Advertencia de firma	Habilitada (Advertir siempre sobre las firmas no válidas)	
21. Verifique los valores de		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores:		

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4">configuración PST de Microsoft Outlook 2016 de usuario.</td><td></td><td colspan="3">“Configuración de usuario → Plantillas administrativas → Microsoft Outlook 2016 → Varios → Configuración PST”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Evitar que los usuarios agreguen archivos PST a perfiles de Outlook y/o evitar el uso de archivos PST para compartirlos de manera exclusiva</td><td>Habilitada (se pueden agregar archivos PST)</td><td></td></tr>
<tr><td colspan="2">Impedir a los usuarios agregar nuevo contenido a archivos PST existentes</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="7">22. Verifique los valores de la Vista protegida de MS PowerPoint 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft PowerPoint 2016 → Opciones de PowerPoint → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Abrir archivos de UNC de intranet local en Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de la zona de Internet en Vista protegida</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de ubicaciones inseguras en Vista protegida</td><td>Deshabilitado</td><td></td></tr>
<tr><td>23. Verifique los valores de criptografía aplicados de Microsoft PowerPoint 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft PowerPoint 2016 → Opciones de PowerPoint → Seguridad → Criptografía”</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="5"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Especificar algoritmo hash CNG</td><td>Habilitada (SHA512)</td><td></td></tr>
<tr><td colspan="2">Especificar compatibilidad de cifrado</td><td>Habilitada (Todos los archivos se guardan con última generación)</td><td></td></tr>
<tr><td colspan="2">Especificar longitud de contraseña CNG con salt</td><td>Habilitada (32)</td><td></td></tr>
<tr><td colspan="2">Usar nueva clave cuando cambie la contraseña</td><td>Habilitado</td><td></td></tr>
<tr><td rowspan="4">24. Verifique los valores de criptografía aplicados de Microsoft Project 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Project 2016 → Opciones de proyecto → Seguridad → Criptografía”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Especificar algoritmo hash CNG</td><td>Habilitada (SHA512)</td><td></td></tr>
<tr><td colspan="2">Especificar longitud de contraseña CNG con sal</td><td>Habilitada (32)</td><td></td></tr>
<tr><td rowspan="6">25. Verifique los valores de la Vista protegida de MS Word 2016 de usuario.</td><td></td><td colspan="3">Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Word 2016 → Opciones de Word → Seguridad → Centro de confianza → Vista protegida”</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Abrir archivos de UNC de intranet local en la Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Desactivar la Vista protegida para los datos adjuntos abiertos desde Outlook</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Establecer el comportamiento del documento si se producen errores durante la validación del archivo</td><td>Habilitado (Bloquear archivos, No permitir edición)</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de la zona de Internet en la Vista protegida</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">No abrir archivos de ubicaciones inseguras en la Vista protegida</td><td>Deshabilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>26. Verifique los valores de criptografía aplicados de Microsoft Word 2016 de usuario.</td><td></td><td>Utilizando el editor de objetos de directiva de grupo, verifique que la directiva tiene los siguientes valores de:
“Configuración de usuario → Plantillas administrativas → Microsoft Word 2016 → Seguridad → Criptografía”</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Especificar algoritmo hash CNG</td><td>Habilitada (SHA512)</td><td></td></tr>
<tr><td>Especificar compatibilidad de cifrado</td><td>Habilitada (Guardar todos arch. Con form. próx. generac.)</td><td></td></tr>
<tr><td>Especificar longitud de contraseña CNG con salt</td><td>Habilitada (32)</td><td></td></tr>
<tr><td>Usar nueva clave cuando cambie la contraseña</td><td>Habilitado</td><td></td></tr>
</table>
</td></tr>
<tr><td>27. Verifique que están configurados los servicios de MS Office 2016</td><td></td><td>Inicie sesión en el equipo Windows cliente con un usuario con privilegios de administrador.
Ejecute la herramienta “Windows PowerShell” con privilegios de administrador. Para ello vaya a la siguiente ruta:
“Menú inicio → Todos los programas → Accesorios → Windows PowerShell”
Seleccione mediante botón derecho en Windows PowerShell la opción “Ejecutar como administrador”.
En la shell abierta ejecute services.msc.
Compruebe que los siguientes servicios se encuentran configurados en modo manual:
– Office Source Engine
– Servicio de caché de fuentes de Windows
– Servicio Hacer clic y ejecutar de Microsoft Office
Nota: Dependiendo de la versión de Office instalada puede aparecer el servicio “OSE” o “OSE64” y puede no aparecer el servicio “ClickToRunSvc”.
El sistema le solicitará elevación de privilegios.</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Servicio (nombre corto)</th><th>Servicio (nombre largo)</th><th>Inicio</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>ClickToRunSvc</td><td>Servicio Hacer clic y ejecutar de Microsoft Office</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>FontCache</td><td>Servicio de caché de fuentes de Windows</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>OSE</td><td>Office Source Engine</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>OSE64</td><td>Office 64 Source Engine</td><td>Manual</td><td>Configurado</td><td></td></tr>
</table>
</td></tr>
<tr><td>28. Compruebe que las aplicaciones de MS Office 2016 funcionan correctamente</td><td></td><td>Pruebe a abrir alguna de las aplicaciones de MS Office 2016, como, por ejemplo, MS Word, MS Excel o MS PowerPoint.
Compruebe que puede crear un nuevo documento y guardarlo.</td></tr>
<tr><td>29. Compruebe que puede proteger un documento con contraseña y que esta es robusta.</td><td></td><td>Proteja un documento con contraseña. Para ello acceda al menú “Archivo → Información → Proteger documento → Cifrar con contraseña”.</td></tr>
</table>

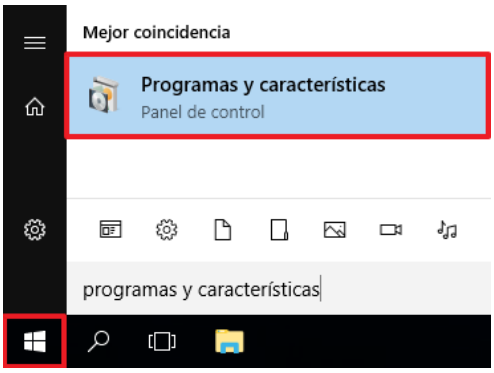
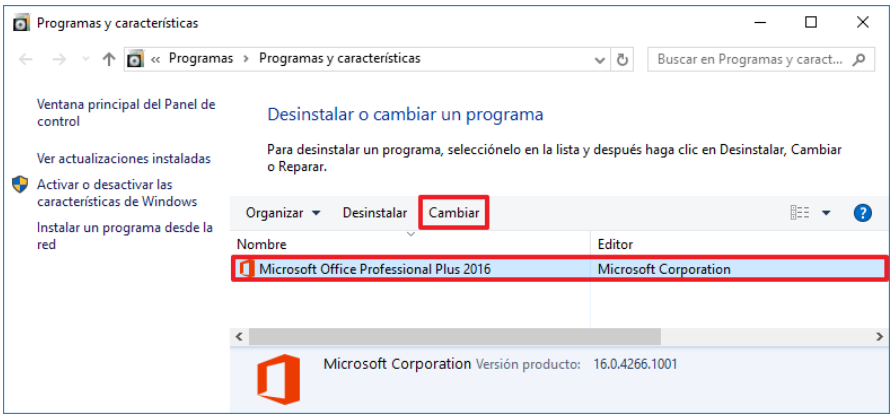
Comprobación	OK/NOK	Cómo hacerlo
		 Compruebe que no puede introducir una contraseña inferior a 12 caracteres.
30. Compruebe los metadatos de los archivos.		Abra cualquiera de las aplicaciones de la *suite* Office, por ejemplo Word, seleccione comenzar un documento en blanco y vaya al menú "**Archivo → Información → Propiedades**" y compruebe que los datos corresponden a los del usuario que inició la sesión. 
31. Compruebe las opciones de contenido en línea.		Verifique que, a la hora de editar un documento en Word, por ejemplo, dentro de la pestaña insertar están desmarcadas las opciones de contenido en línea. 

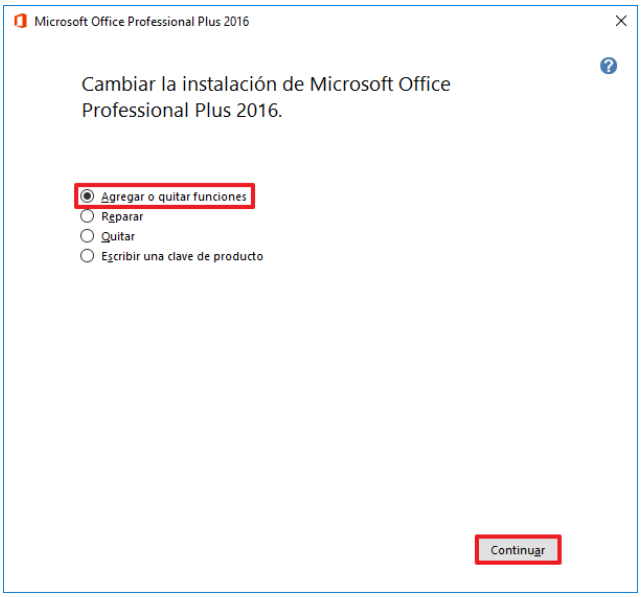
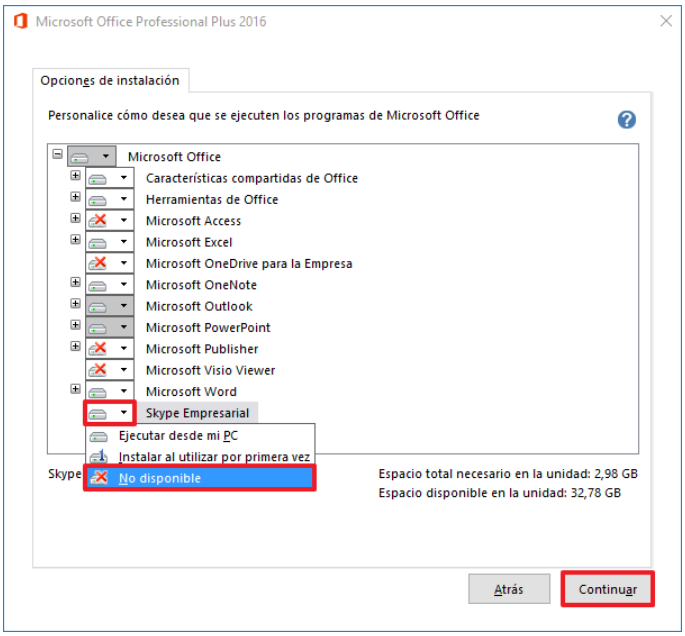
ANEXO A.4. TAREAS ADICIONALES

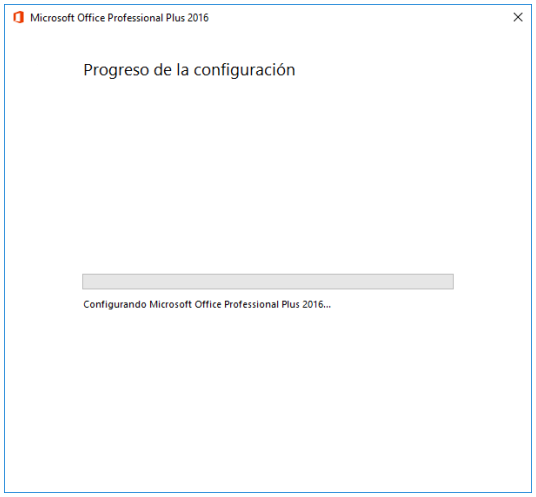
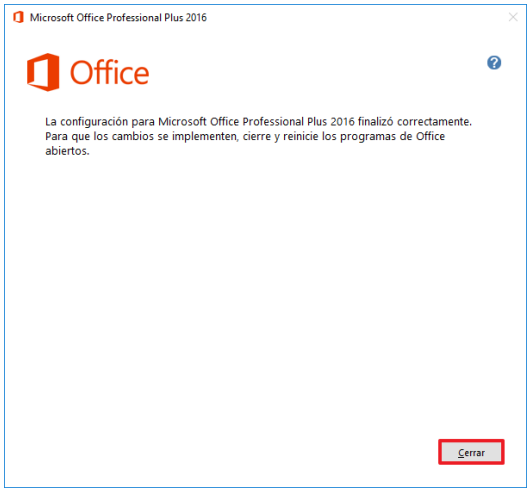
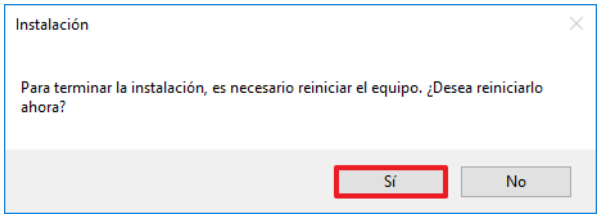
ANEXO A.4.1. DESINSTALACIÓN DE APLICACIONES DE LA SUITE

El presente Anexo ha sido diseñado para ayudar a los operadores de sistemas a desinstalar aplicaciones de la suite de Office 2016, para atender al principio de mínima exposición que faculta a un sistema a reducir los riesgos minimizando los puntos de entrada al mismo.

Tenga en cuenta que este procedimiento solo podrá aplicarlo si la versión de Office 2016 instalada es de volumen, que permite seleccionar las aplicaciones para instalar o desinstalar de forma individual.

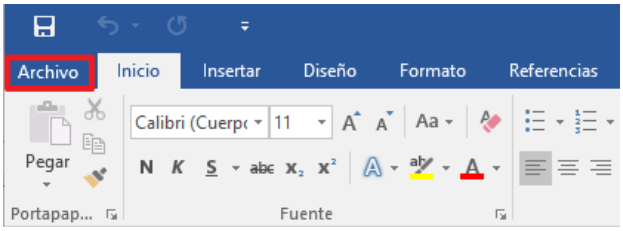
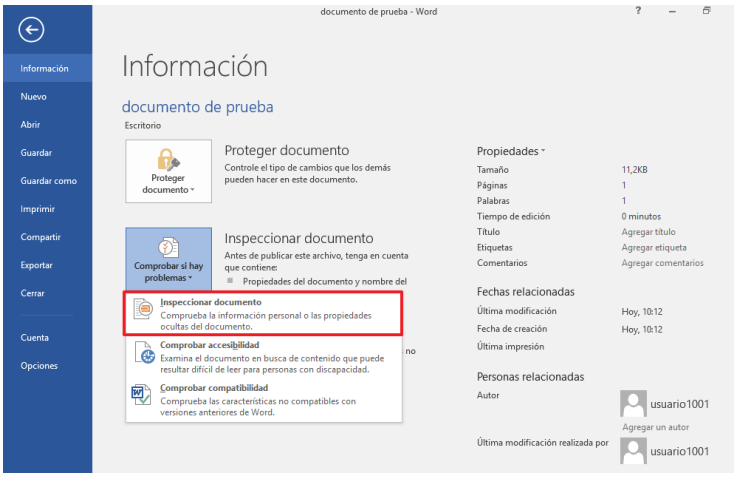
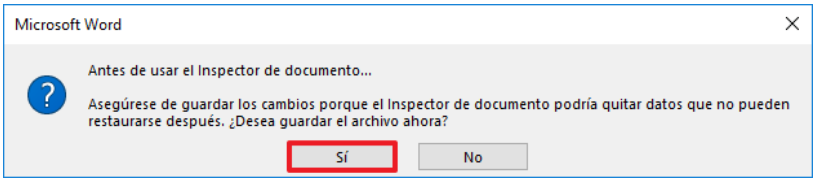
Paso	Descripción
1.	Inicie sesión en el equipo cliente donde se van a desinstalar las aplicaciones innecesarias.
2.	Pulse sobre botón de inicio y busque “Programas y características”. 
3.	Seleccione la aplicación de Office 2016 y pulse sobre “Cambiar”. El sistema le solicitará elevación de privilegios. 

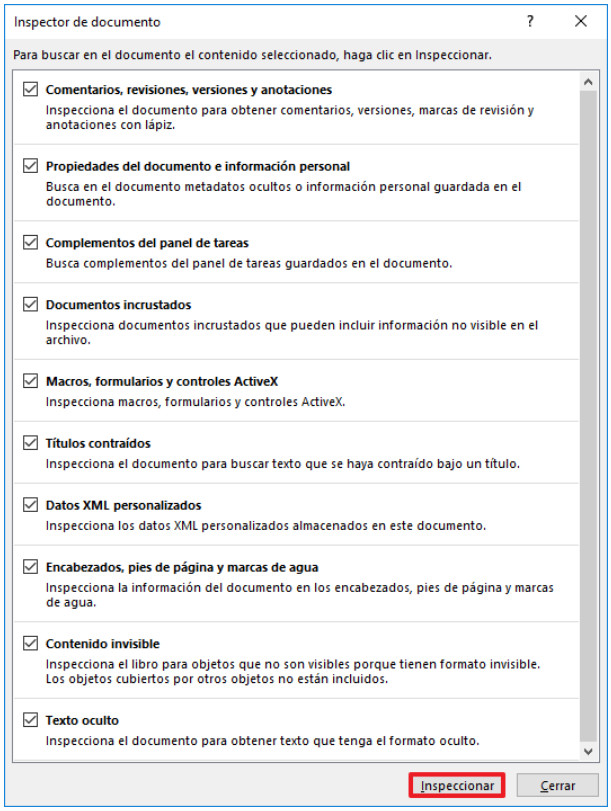
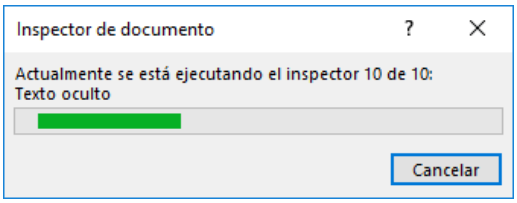
Paso	Descripción
4.	Se abrirá el asistente de Office 2016. Mantenga la opción de “Agregar o quitar funciones” y pulse “Continuar”. 
5.	Seleccione la opción “No disponible” para cada una de las aplicaciones que se vayan a desinstalar y pulse “Continuar”.  **Nota:** En este ejemplo se desinstala Skype Empresarial. Ejecute este paso acorde a los requerimientos de su organización.

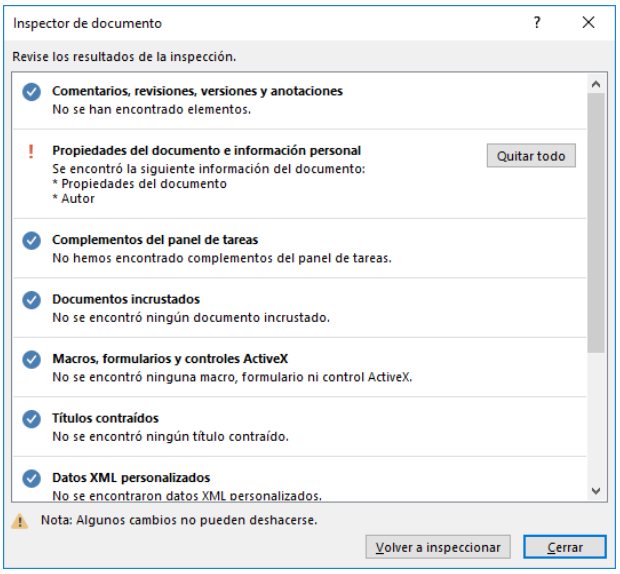
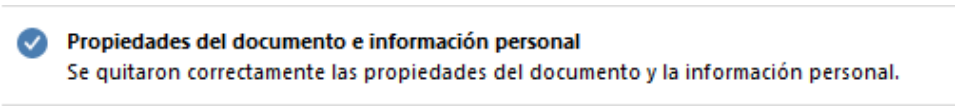
Paso	Descripción
6.	Espere a que finalice el proceso. 
7.	Una vez acabado pulse “Cerrar”. 
8.	En el caso de necesitar un reinicio de la máquina le aparecerá la siguiente ventana emergente. Pulse “Sí” para continuar. 
9.	Una vez reiniciado el equipo, compruebe que las aplicaciones ya no se encuentran disponibles en el sistema.

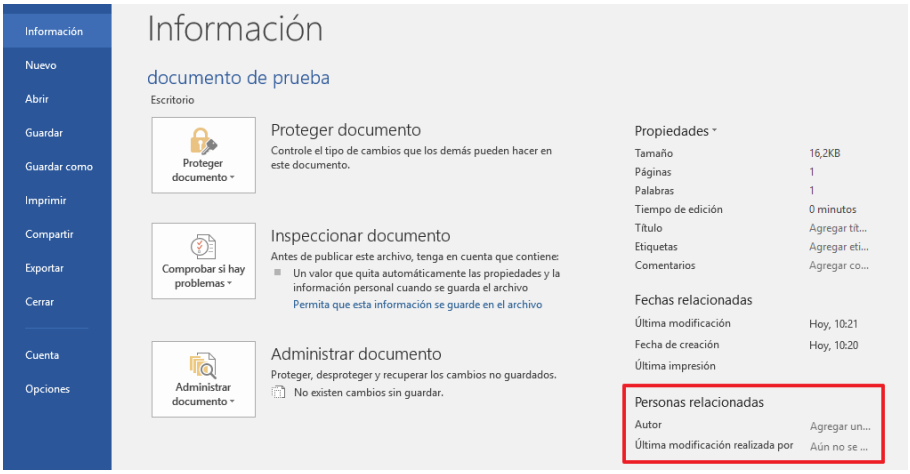
ANEXO A.4.2. LIMPIEZA DE METADATOS DE DOCUMENTOS

Los documentos portan información adicional al contenido, oculta o visible, que puede suponer una filtración de información significativa. Para ello, MS Office 2016 incorpora, a través de sus herramientas, mecanismos para la limpieza de metadatos de los documentos. Se muestra a continuación, como ejemplo, cómo realizar la eliminación de metadatos en un documento creado con la aplicación MS Word 2016.

Paso	Descripción
1.	Antes de cerrar un documento deberá prepararlo para su exposición limpia de metadatos. Para ello acceda al menú "Archivo" de MS Word 2016. 
2.	Haga uso de la función "**Información → Comprobar si hay problemas → Inspeccionar documento**".  **Nota:** En la imagen superior se aprecian los valores de algunos de los metadatos, tales como el nombre del autor , el último editor, fechas, horas, etc.
3.	Si aparece la opción de que el archivo contiene cambios que no se guardaron, pulse el botón "Sí". 

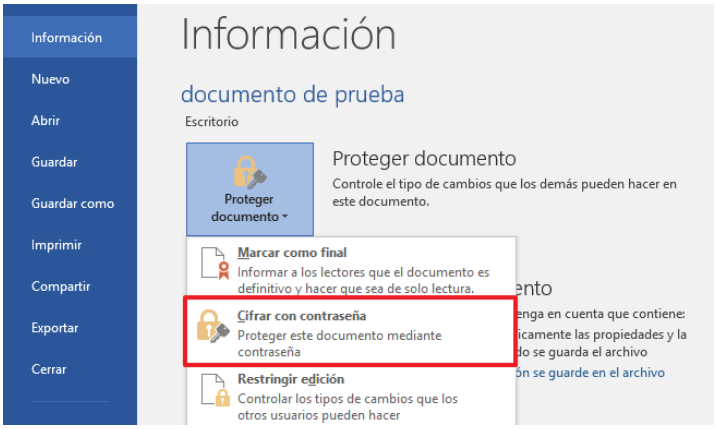
Paso	Descripción
4.	Deje marcado todo el contenido y pulse el botón “Inspeccionar”:  Todavía no se está realizando la limpieza por lo que esta acción no supone ningún riesgo de borrado accidental de información.
5.	Se iniciará la inspección del documento y se identificarán todos aquellos elementos que se encuentran en el fichero y son susceptibles de mostrar información relevante, durante este proceso se abre una ventana de progreso durante unos segundos. 

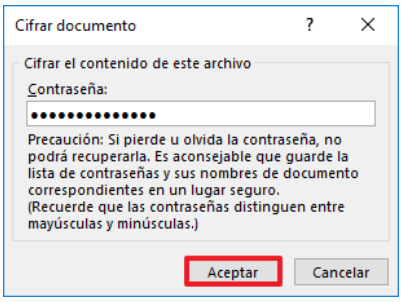
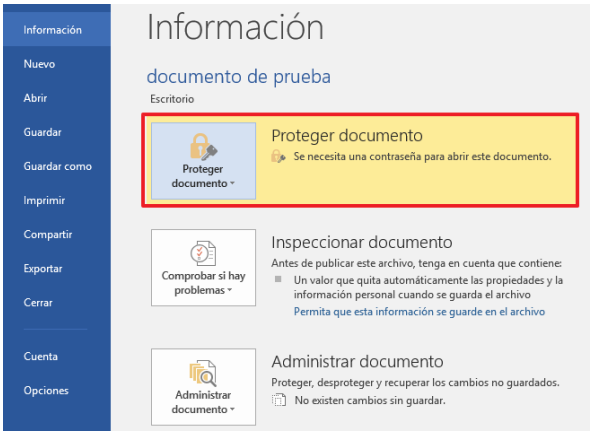
Paso	Descripción
6.	Finalizada la inspección, se mostrará un resumen de aquellos apartados con información que ha encontrado y ofrecerá la posibilidad de quitar los datos, sean visibles o no. 
7.	Quite, al menos, del documento la información correspondiente a: – Propiedades del documento e información personal. – Contenido invisible. – Texto oculto. Revise el resto de elementos para evaluar si debe ser eliminado también, por ofrecer información relevante del usuario, los sistemas informáticos o detalles de la propia organización. Para eliminar un contenido seleccione el botón correspondiente “Quitar todo”. En el ejemplo “Quitar todo” de las “Propiedades del documento e información personal”. **Nota:** Tenga en cuenta que ciertos cambios realizados desde esta ventana no son reversibles, como se avisa, y debería recuperar una versión anterior para recuperarlos.
8.	Una vez quitado el contenido, se mostrará un mensaje con el resultado de la acción.  Podría volver a revisar el documento en busca de datos que no hubieran podido ser eliminados por cualquier circunstancia. En este caso se cierra la ventana pulsando sobre “Cerrar”.

Paso	Descripción
9.	Cuando haya eliminado todos los datos relevantes, guarde el documento y compruebe que se han eliminado. En este ejemplo, se vuelve a la ventana de información del documento donde se puede observar que no figura el dato del autor ni otros similares. 

ANEXO A.4.3. PROTECCIÓN DE FICHERO CON CONTRASEÑA

Si desea evitar que el fichero pueda ser abierto por cualquiera que pueda tener acceso al mismo, pero sí que lo abran determinadas personas, puede protegerlo por medio de una contraseña. Esta protección, además de impedir su apertura, cifra su contenido para garantizar la seguridad frente a un ataque de tipo offline, donde el atacante consigue acceder al contenido del archivo sin conocer la contraseña ya que, aunque consiguiera el acceso, encontraría contenido ilegible. La política de seguridad aplicada establece la necesidad de introducir una contraseña de al menos 8 caracteres para la categoría básica, 10 para la media y 12 para la categoría alta / Difusión Limitada. Se muestra como ejemplo la protección de un documento con contraseña con la aplicación MS Word 2016.

Paso	Descripción
1.	Para proteger un fichero con contraseña acceda al menú “Archivo” de MS Word 2016 y haga uso de la función “**Información → Proteger documento → Cifrar con contraseña**”. 

Paso	Descripción
2.	Introduzca la contraseña deseada, teniendo en cuenta las restricciones definidas para tipo de credenciales, pulse “Aceptar”, entonces deberá volver a repetir la contraseña para garantizar que la ha introducido correctamente. Después pulse nuevamente en “Aceptar”.  **Nota:** Si utiliza una contraseña que no cumpla con los requerimientos mínimos, por ejemplo una longitud inferior a la establecida por las políticas que aplican las diferentes categorías, le será requerido el cambio hasta que se atenga a ellos.
3.	A partir de ese momento será necesario utilizar la contraseña para abrir el documento, como así lo indica el panel de información del documento.  **Nota:** Este cifrado es independiente y distinto del que se puede generar con el propio sistema de archivos del sistema operativo Windows 10 pero, a diferencia de este, el cifrado de Office permite abrir el documento en cualquier ordenador a cualquier persona que conozca la contraseña.
4.	Puede guardar los cambios y cerrar el fichero.
5.	Cuando vaya a abrir el documento, la aplicación correspondiente, en este ejemplo Microsoft Word, le solicitará la contraseña de acceso. Introdúzcala y presione “Aceptar”.