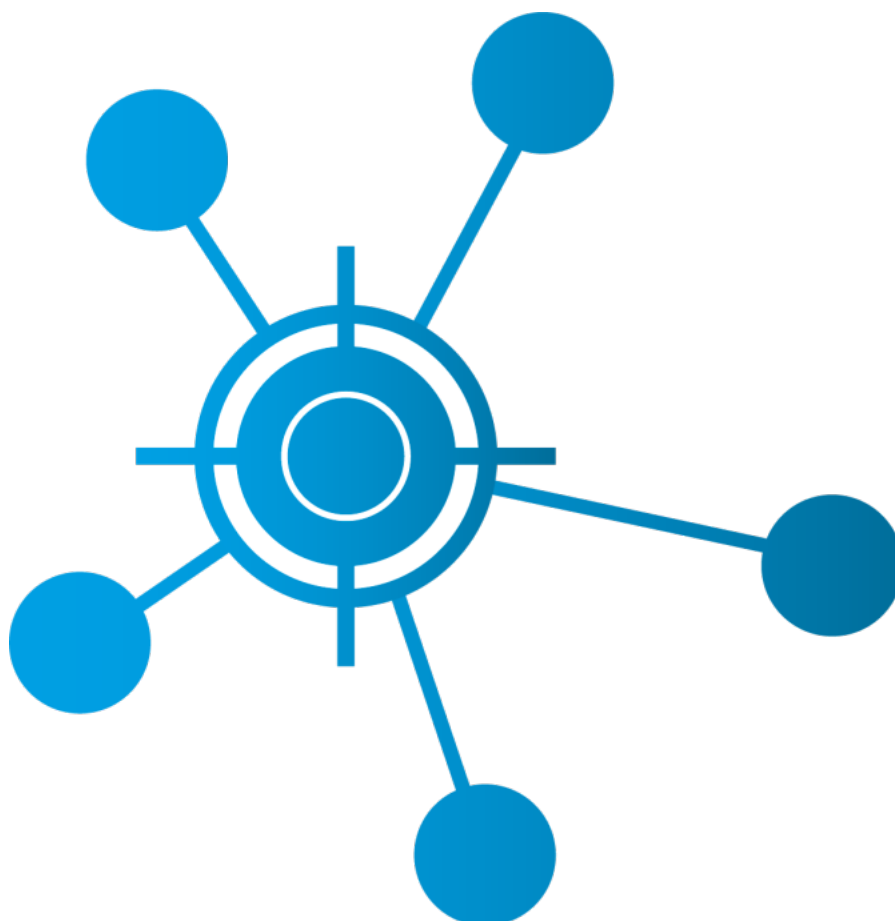


CCN-CERT IA-52/19

# Implementación Segura de Microsoft Windows/Office frente a la Campaña EMOTET



Octubre 2019

Edita:



© Centro Criptológico Nacional, 2019

Fecha de Edición: octubre de 2019

#### **LIMITACIÓN DE RESPONSABILIDAD**

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

#### **AVISO LEGAL**

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

## ÍNDICE

<b>1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL .....</b>	<b>4</b>
<b>2. INTRODUCCIÓN .....</b>	<b>4</b>
2.1 VECTOR DE ATAQUE .....	4
2.2 CONSECUENCIAS.....	5
<b>3. ALCANCE .....</b>	<b>5</b>
<b>4. PASO A PASO PARA IMPLEMENTACIÓN SEGURA EN UN ENTORNO DEFINIDO PARA CATEGORÍA ALTA.....</b>	<b>6</b>
4.1 CONTROLADOR DE DOMINIO.....	7
4.2 SERVIDOR MIEMBRO .....	9
4.3 CLIENTE MIEMBRO .....	12
4.4 MICROSOFT OFFICE 2016.....	15
4.5 TAREAS ADICIONALES .....	17
4.5.1 HABILITAR WINDOWS DEFENDER.....	17

## 1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

## 2. INTRODUCCIÓN

Cada vez más a menudo se muestra que las configuraciones predeterminadas con las que cuentan los sistemas operativos y aplicaciones no sirven para frenar acciones perniciosas que afectan a los sistemas de la información. Solo configuraciones de protección consolidadas y enfocadas a la mejora en la seguridad pueden ser capaz de frenar los vectores que actualmente emplean los atacantes y que en ocasiones pueden aprovechar funcionalidades propias de los productos.

Recientemente se ha identificado una campaña de acción por parte del código dañino EMOTET que está afectando de forma significativa a los sistemas de la información.

### 2.1 VECTOR DE ATAQUE

El código dañino EMOTET constituye una amenaza maliciosa con un vector de ataque bastante conocido y que presenta las siguientes características:

- a) El punto de entrada o infección se produce mediante la ejecución de código embebido desde un documento ofimático a través de aplicaciones tales como MS Word.
- b) Dicho script, inicializa un proceso de conexión contra servidores y sistemas de mando y control, existentes en Internet, que descargan un código dañino e inician la infección del sistema. Una vez producida la infección se lleva a cabo el cifrado sin consentimiento del sistema, realizándose además otras acciones no autorizadas.
- c) Para garantizar la fase de persistencia, el código dañino iniciará dos (2) potenciales acciones:
  - Alteración del sistema con elevación de privilegios.
  - Movimientos en la red mediante la dispersión, replicándose en otros sistemas.
- d) Otras acciones relacionadas con la explotación posterior, tomando en consideración la realización de movimientos laterales, exfiltración de datos o robo de información sensible.

## 2.2 CONSECUENCIAS

Una vez que la acción maliciosa se ha producido, el sistema de información se ve afectado por las siguientes consecuencias:

- a) El código dañino inicializa un proceso de secuestro del sistema mediante el cifrado del contenido en los sistemas de información afectados, servidores y puestos de trabajo.
- b) El código dañino puede robar y exfiltrar contenido sensible de la organización tales como documentos, información de índole bancaria, credenciales y otras que pueden afectar a la integridad del sistema o perjudicar la imagen de la organización afectada.
- c) Otras consecuencias tales como formar parte de una red de tipo “botnet” mediante la integración de los sistemas afectados en un sistema de mando y control para la manipulación y ejecución de acciones no autorizadas.

## 3. ALCANCE

El presente documento se ha elaborado para la correcta implementación de seguridad establecida en las guías publicadas por el ENS para sistemas Windows y proporcionar información específica para realizar una implementación del paquete ofimático Microsoft Office.

**Nota:** Las guías descritas en este apartado están definidas para los sistemas operativos MS Windows Server 2016, MS Windows 10 y el paquete ofimático MS Office 2016 (en sus versiones Standard y Professional Plus). No se contempla la implementación de las medidas de seguridad descritas en este documento sobre otros productos y su correcto funcionamiento, aunque pueden ser aplicadas con las pruebas oportunas.

Para poder realizar los pasos definidos durante los puntos posteriores deberá descargar los recursos de la página oficial del CCN mediante los siguientes enlaces:

## a) CCN-STIC-570A Controlador de dominio y servidor miembro.

- Anexo A (ENS): <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3182-ccn-stic-570a-ens-anexo-a/file.html>
- Scripts: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3185-ccn-stic-570a-ens-anexo-a-scripts.html>

## b) CCN-STIC-599A18 Cliente miembro de dominio.

- Anexo A (ENS): <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3097-ccn-stic-599a18-seguridad-en-windows-10-enterprise-ltsb-cliente-miembro-de-dominio-anexo-a.html>
- Scripts: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3100-ccn-stic-599a18-seguridad-en-windows-10-enterprise-ltsb-cliente-miembro-de-dominio-anexo-a-scripts.html>

## c) CCN-STIC-585 Microsoft Office 2016.

- Anexo A (ENS): <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3534-ccn-stic-585-ens-anexoa/file.html>
- Scripts: <https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3537-ccn-stic-585-ens-anexoa-scripts.html>

#### 4. PASO A PASO PARA IMPLEMENTACIÓN SEGURA EN UN ENTORNO DEFINIDO PARA CATEGORÍA ALTA

Tomando en consideración las medidas aplicables que recogen las guías de seguridad CCN-STIC para la categoría ALTA, se puede determinar que las acciones dañinas consecuencia de códigos como EMOTET pueden ser controladas, bien impidiendo su acción o bien limitando la misma.

Solo acciones conscientes del usuario y degradando la seguridad existente podrían suponer un riesgo general para la organización, habiendo aplicado las medidas de protección adecuadas.

Además, debe tenerse en consideración que en general la aplicación efectiva de los principios de mínima exposición, mínimo privilegio y mejora continua, sumados a la concienciación y educación en materia de ciberseguridad son elementos a tomar siempre en cuenta para limitar o impedir acciones dañinas a través de campañas tales como la originada por el código dañino EMOTET.

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

Antes de realizar la implementación descrita, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar la categoría de cada una de las

dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para los servicios e información manejada por la organización correspondieran, al menos, a la categoría ALTA para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente apartado.

Además, se debe tener en cuenta que la política global definirá, a través del análisis de cada una de sus dimensiones de seguridad, el nivel de la organización. No obstante, pudiera ser factible que algunos de los servidores proporcionaran servicios o manejaran información sujeta a categoría BÁSICA o MEDIA.

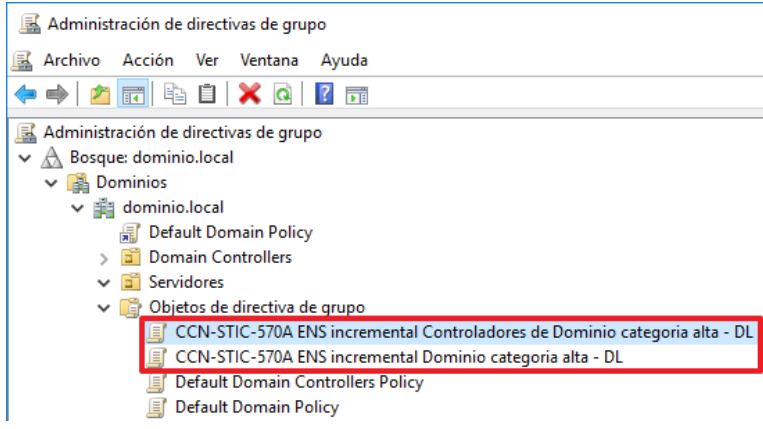
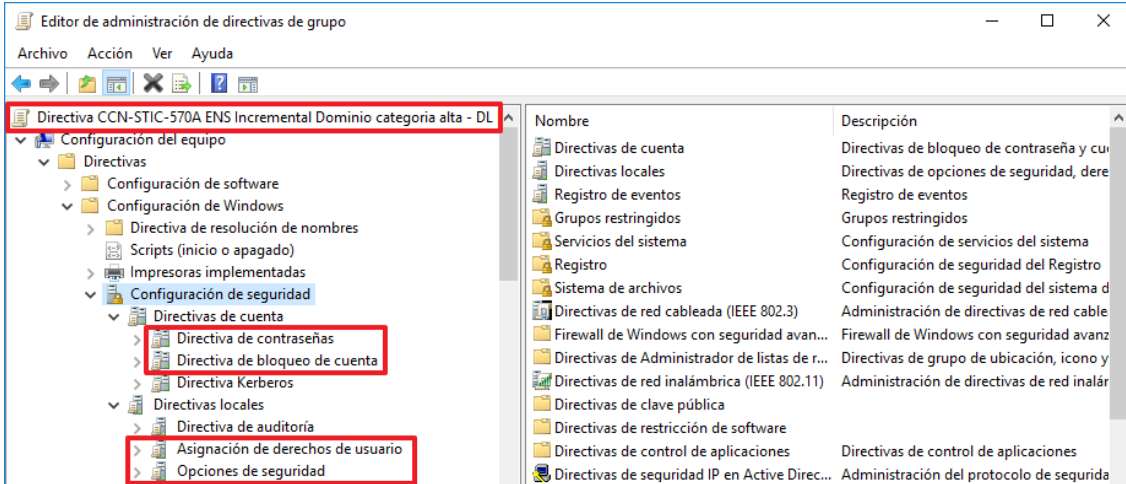
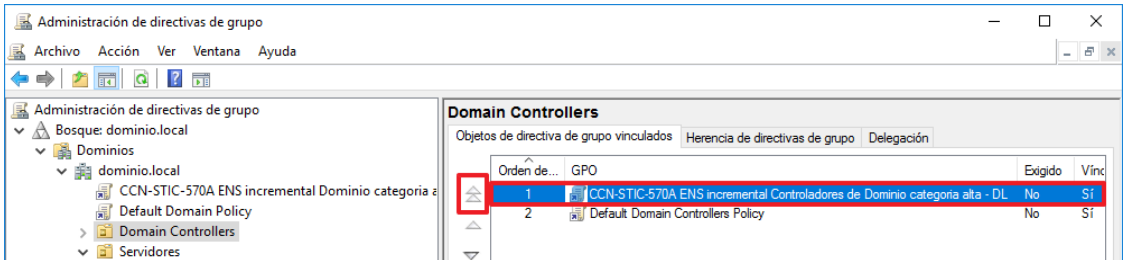
Por lo tanto, a estos servidores les podrían ser de aplicación las plantillas de seguridad determinadas para categoría BÁSICA o MEDIA. Sin embargo, la política de dominio y controladores de dominio, al ser de ámbito general, deberá especificar la correspondiente a la categoría ALTA siguiendo las pautas establecidas en los pasos posteriores.

Se debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en el presente documento, se deberá realizar pruebas en un entorno de preproducción con el objeto de familiarizarse con el escenario y realizar las pruebas de funcionalidad oportunas.

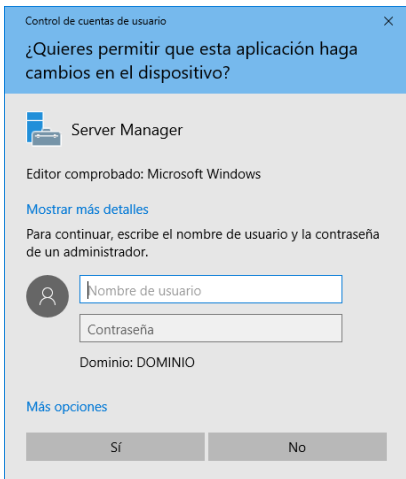
**Nota:** Siguiendo la advertencia definida en el párrafo anterior haga uso de grupos de control dentro del entorno de producción para validar la configuración implementada.

#### 4.1 CONTROLADOR DE DOMINIO

Paso	Descripción
1.	Para la correcta implementación de seguridad en el entorno, deberá aplicar seguridad en primer lugar, al dominio y a su controlador dominio (DC). Para ello, siga los pasos descritos en el punto “1. PREPARACIÓN DE DOMINIO” de la guía codificada como “CCN-STIC-570A” en su “ANEXO A.4.1. GUÍA PASO A PASO CONTROLADOR DE DOMINIO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA”.
2.	En dicho punto se describe la inclusión de los recursos y scripts asociados a la guía “CCN-STIC-570A”, la creación de los objetos GPO “CCN-STIC-570A ENS incremental Dominio categoría alta - DL” y “CCN-STIC-570A ENS incremental Controladores de Dominio categoría alta - DL”. A continuación, se realiza la importación de las directivas a los objetos GPO para su configuración.
3.	Después de aplicar dichos puntos deberá de obtener como resultado una configuración como la mostrada en la siguiente imagen, dos (2) objetos de políticas de grupo correctamente configurados.

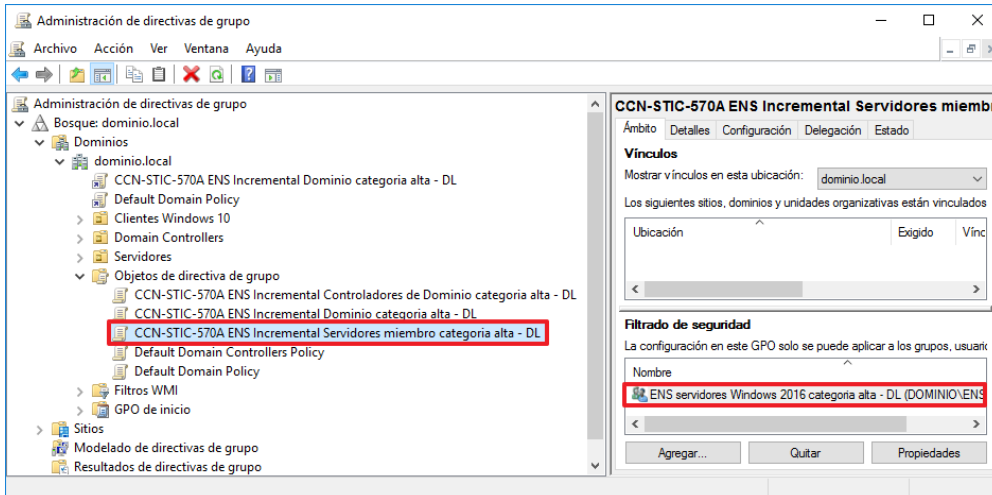
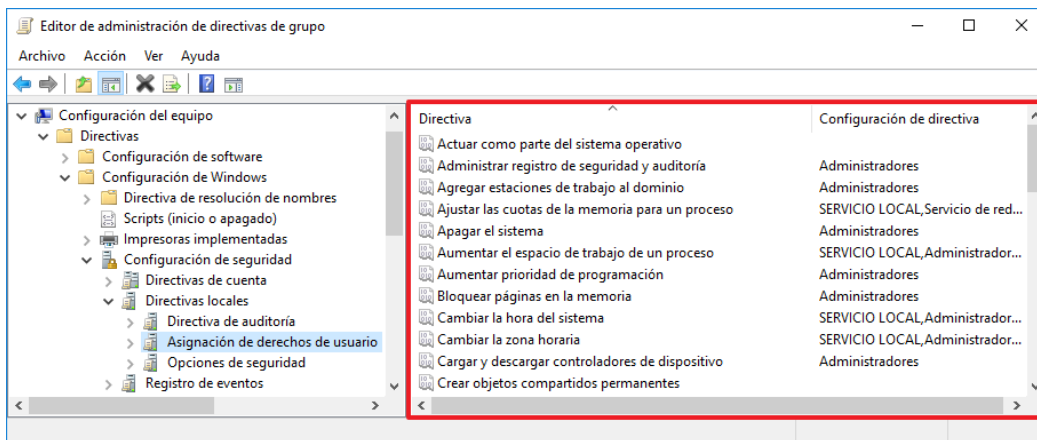
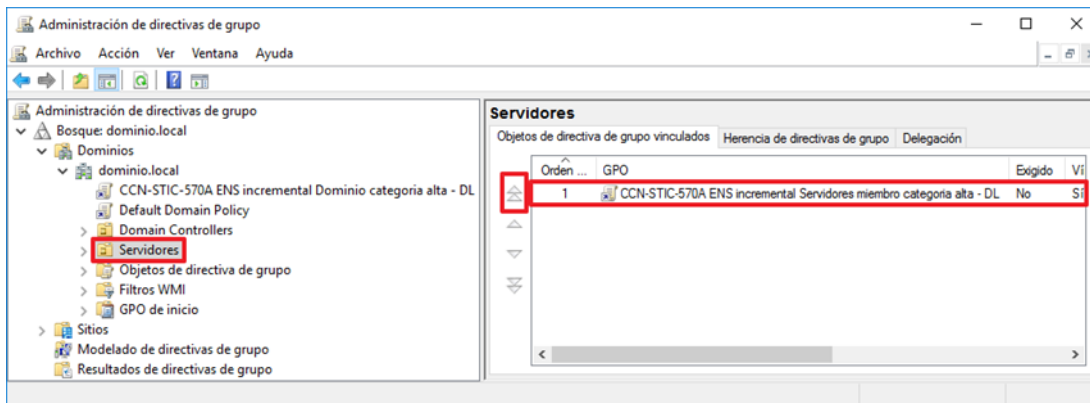
Paso	Descripción
	
4.	<p>A continuación, se procede a aplicar los pasos descritos en el punto “2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN” y sus subapartados. En dichos pasos se valoran y se establecen los valores para las contraseñas y bloqueo de cuentas, la asignación de derechos de usuario, el tiempo de bloqueo de sesión ante inactividad y se establece un mensaje disuasorio en el inicio de sesión. Dichas configuraciones se realizan en el objeto GPO “CCN-STIC-570A ENS incremental Dominio categoría alta - DL”.</p> 
5.	<p>En el siguiente punto, “3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD” se aplicarán los objetos GPO configurados previamente a las unidades organizativas correspondientes, además de establecer el orden de aplicación adecuado de estos.</p> 
6.	<p>Por último, se evalúa la configuración predeterminada de seguridad para el tipo de cifrado permitido de Kerberos en el punto “4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS”.</p>

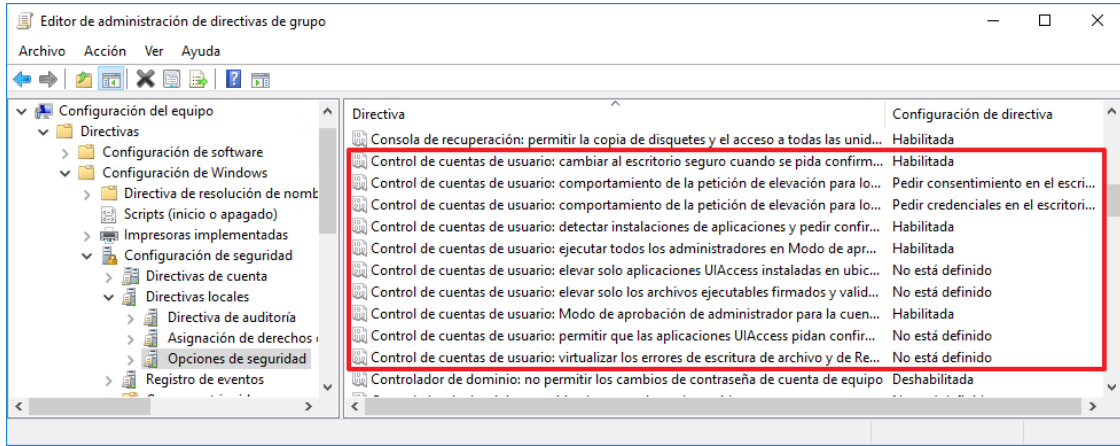
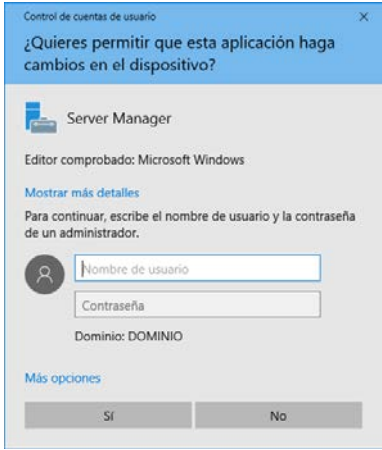



Paso	Descripción
7.	Para confirmar que se han aplicado correctamente las configuraciones establecidas, deberá seguir el “ANEXO A.4.2. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO CONTROLADOR DE DOMINIO PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA”.
8.	<p>Un indicativo rápido para determinar si se están aplicando las medidas de seguridad es que a la hora de ejecutar cualquier elemento que necesite privilegios de administrador, se deberá solicitar el usuario y la contraseña para poder continuar.</p>  <p><b>Nota:</b> La solicitud de credenciales durante la ejecución de un elemento como administrador no es un indicativo final que determine que todas las configuraciones se encuentren correctamente aplicadas. Para ello deberá seguir las indicaciones del paso anterior.</p>
9.	<p>Cabe destacar que durante la aplicación de la guía no se define un software específico contra código dañino. Para ello, deberá instalar en sus equipos la solución antivirus que más se adapte a las necesidades de su organización.</p> <p>Si desea habilitar la solución por defecto proporcionada por Microsoft Windows (Windows Defender) deberá seguir los pasos indicados en el “APARTADO 4.5. TAREAS ADICIONALES” en el punto “4.5.1 HABILITAR WINDOWS DEFENDER” del presente documento.</p>

## 4.2 SERVIDOR MIEMBRO

Paso	Descripción
1.	En el caso de que su organización disponga de servidores miembro deberá aplicar los pasos definidos en el punto “1. PREPARACIÓN DE DOMINIO” del “ANEXO A.4.3. GUÍA PASO A PASO SERVIDOR MIEMBRO QUE LE SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA”.
2.	En dicho punto se describe la creación del grupo de seguridad del ENS para servidores miembro, la inclusión de los servidores a los que se les va a aplicar la configuración del ENS para la categoría ALTA en dicho grupo, la creación de los objetos GPO “CCN-STIC-570A ENS incremental Servidores miembro categoría ALTA - DL”, la importación de las directivas a dicho objeto GPO para su correcta configuración y se establece el filtrado de seguridad para que se aplique únicamente al grupo de seguridad de servidores mencionado.

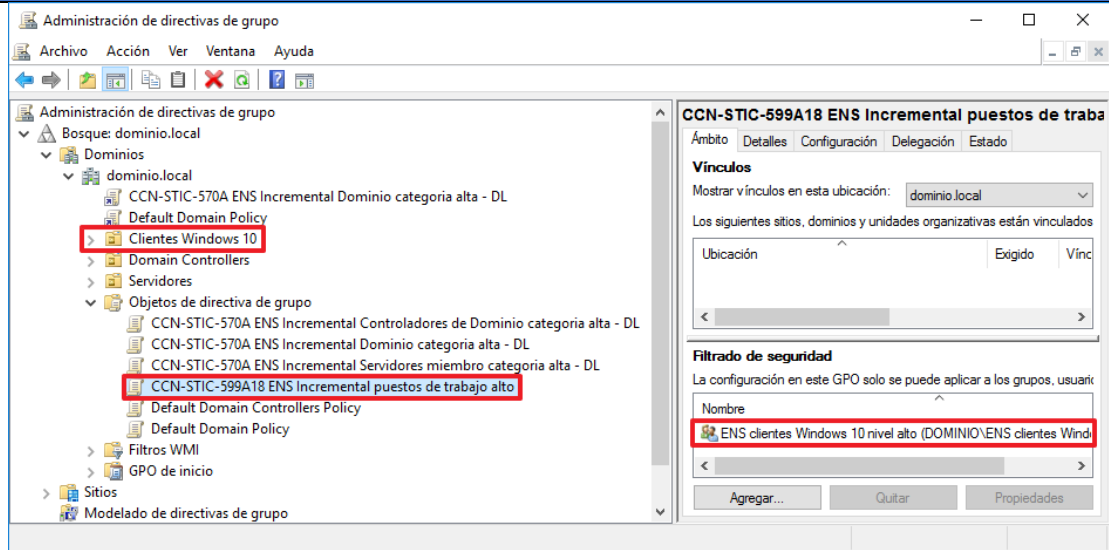
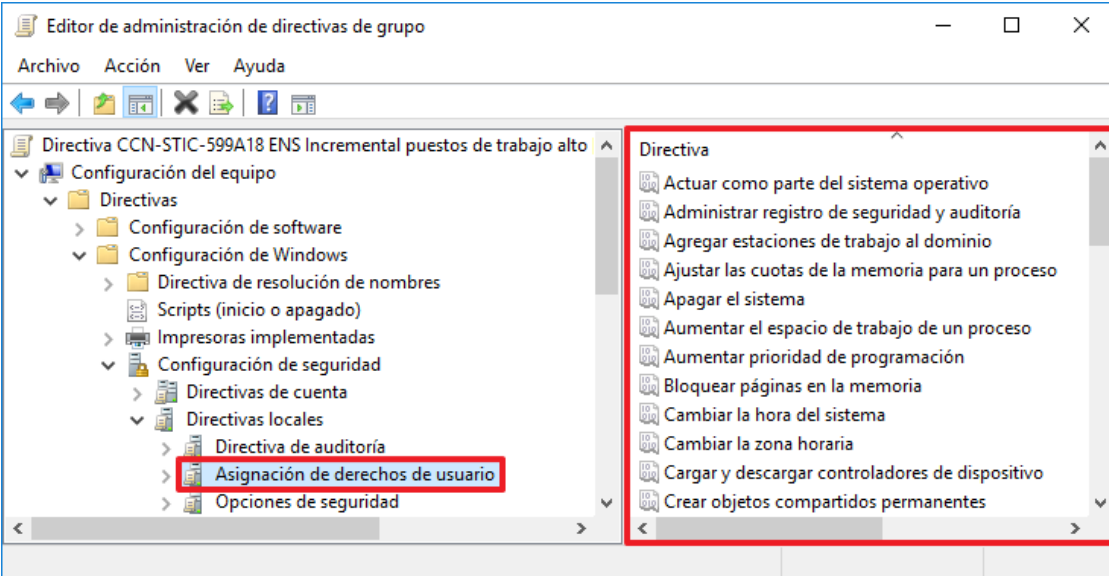
Paso	Descripción
	
3.	<p>En el siguiente punto a implementar “2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN” se advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Deberá modificar las directivas, incluyendo los usuarios o grupos de usuarios a los que desea conceder derechos adicionales en caso de ser necesario.</p> 
4.	<p>El punto “3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD”, establece la aplicación de las políticas de seguridad (GPO) en las unidades organizativas correspondientes en su orden adecuado una vez que se han tenido en consideración las condiciones definidas en pasos previos.</p> 

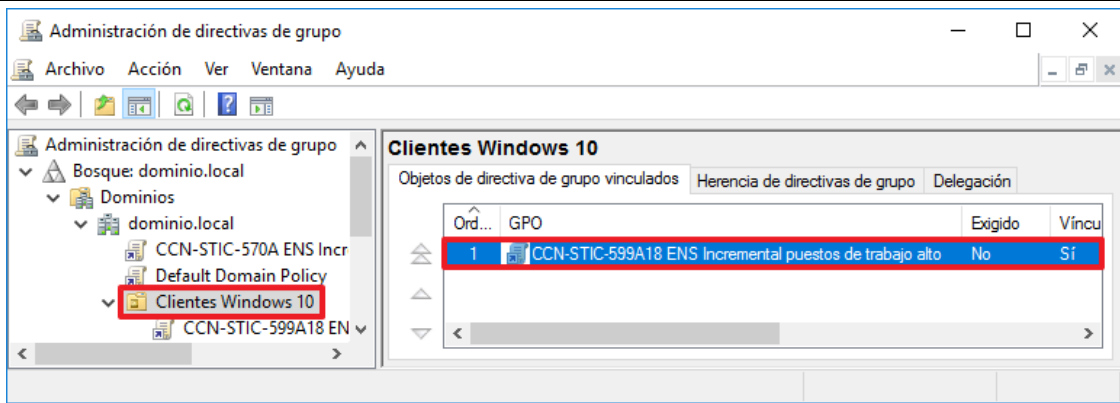
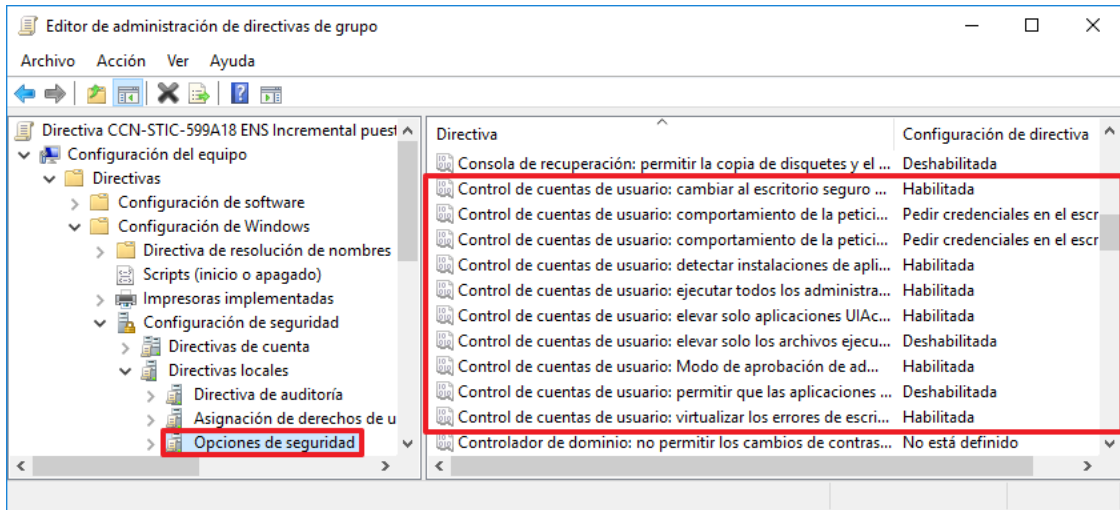
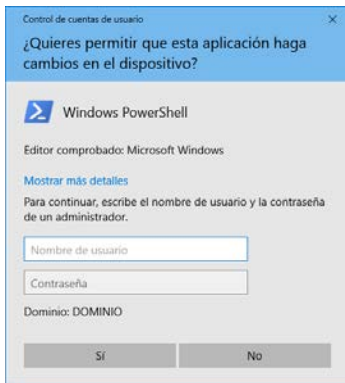
Paso	Descripción
	<p><b>Nota:</b> En la guía de seguridad no se define la unidad organizativa donde se alojarán los servidores, deberá aplicar estos pasos sobre la unidad organizativa que más se adecúen a las necesidades de su organización.</p>
5.	<p>Por último, se evalúan las configuraciones mínimas establecidas para la categoría ALTA del ENS en relación al control de cuentas de usuario en el punto “4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD EN LOS EQUIPOS”.</p> 
6.	<p>Para confirmar que se han aplicado correctamente las configuraciones establecidas, deberá seguir el “ANEXO A.4.4. LISTA DE COMPROBACIÓN DE WINDOWS SERVER 2016 COMO SERVIDOR MIEMBRO DE DOMINIO PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA”.</p>
7.	<p>Un indicativo rápido para determinar si se están aplicando las medidas de seguridad es que a la hora de ejecutar cualquier elemento que necesite privilegios de administrador, se deberá solicitar el usuario y la contraseña para poder continuar.</p>  <p><b>Nota:</b> La solicitud de credenciales durante la ejecución de un elemento como administrador no es un indicativo final que determine que todas las configuraciones se encuentren correctamente aplicadas. Para ello deberá seguir las indicaciones del paso anterior.</p>
8.	<p>De forma predeterminada el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local y queda activo durante la implementación de la guía CCN-STIC. No obstante, existe la posibilidad de realizar un control centralizado a través de la aplicación de objetos de políticas de grupo (GPO). Para ello debe seguir los pasos indicados en el “ANEXO A.5.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA”. La configuración que se establece en dichos pasos</p>

Paso	Descripción
	<p>permite la gestión del Firewall de Windows a través de dominio y se realiza la explicación de cómo definir reglas de entrada.</p> 
9.	<p>Cabe destacar que durante la aplicación de la guía no se define un software específico contra código dañino. Para ello deberá instalar en sus equipos la solución antivirus que más se adapte a las necesidades de su organización.</p> <p>Si desea habilitar la solución por defecto proporcionada por Microsoft Windows (Windows Defender) deberá seguir los pasos indicados en el “APARTADO 4.5. TAREAS ADICIONALES” en el punto “4.5.1 HABILITAR WINDOWS DEFENDER” del presente documento.</p>

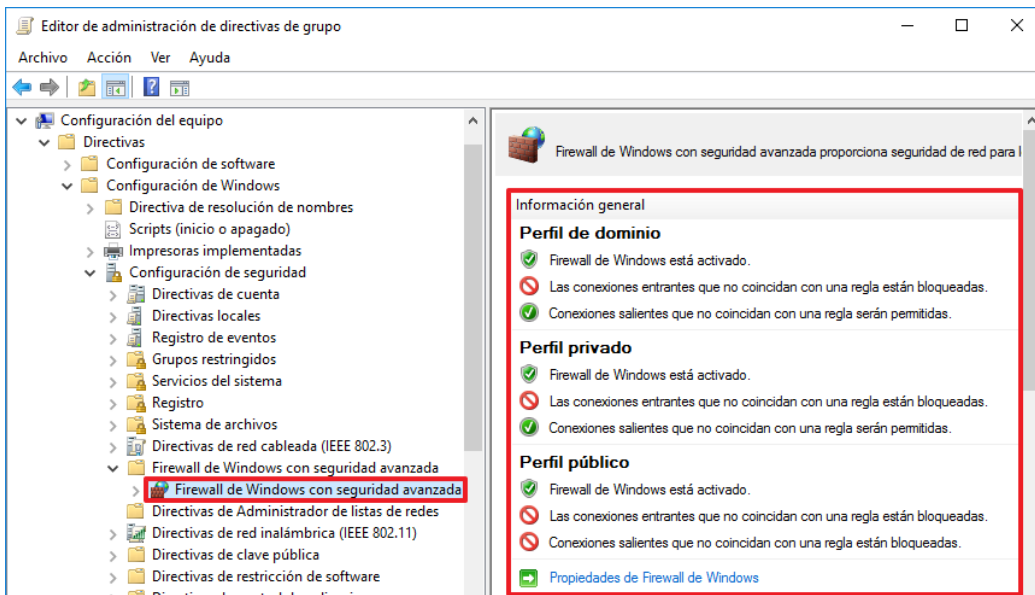
### 4.3 CLIENTE MIEMBRO

Paso	Descripción
1.	<p>En el presente punto deberá aplicar seguridad en los equipos cliente. Para ello, siga los pasos descritos en el punto “1. PREPARACIÓN DE DOMINIO” de la guía codificada como “CCN-STIC-599A18” en su “ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE CLIENTES MICROSOFT WINDOWS 10 QUE LES SEAN DE APLICACIÓN EL NIVEL ALTO DEL ENS”.</p>
2.	<p>En dicho punto se describen los siguientes aspectos:</p> <ul style="list-style-type: none"> <li>• Inclusión de los recursos y scripts asociados a la guía “CCN-STIC-599A18”.</li> <li>• Importación de los ficheros ADMX necesarios en el controlador de dominio.</li> <li>• Creación de la unidad organizativa y grupos de seguridad necesarios, así como la vinculación de usuarios y equipos a dichos grupos.</li> <li>• Creación del objeto GPO “CCN-STIC-599A18 ENS Incremental puestos de trabajo alto”.</li> <li>• Importación de directivas a dichos objetos GPO para su correcta configuración.</li> <li>• Se establece el filtrado de seguridad de la GPO para que aplique únicamente al grupo de seguridad de equipos cliente creado anteriormente.</li> </ul> <p>Cuando finalice deberá obtener una configuración similar a la siguiente.</p>

Paso	Descripción
	
3.	<p>A continuación, se evalúa la posibilidad de modificar las directivas en relación a la asignación de derechos de usuario en el punto “2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN PARA LOS PUESTOS DE TRABAJO EN EL NIVEL ALTO” dependiendo de las necesidades de su organización.</p> 
4.	<p>El punto “3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD” establece la aplicación de las políticas de seguridad en las unidades organizativas correspondientes en su orden adecuado, una vez que se han tenido en consideración las condiciones definidas en pasos previos.</p>

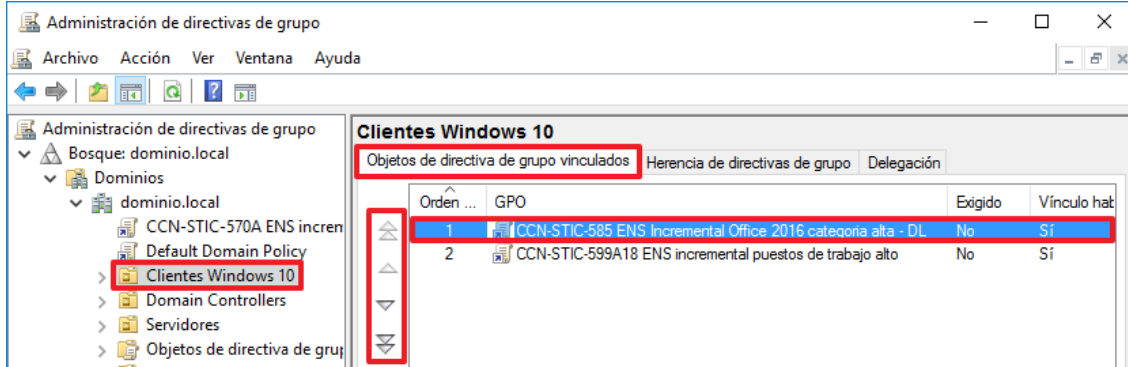
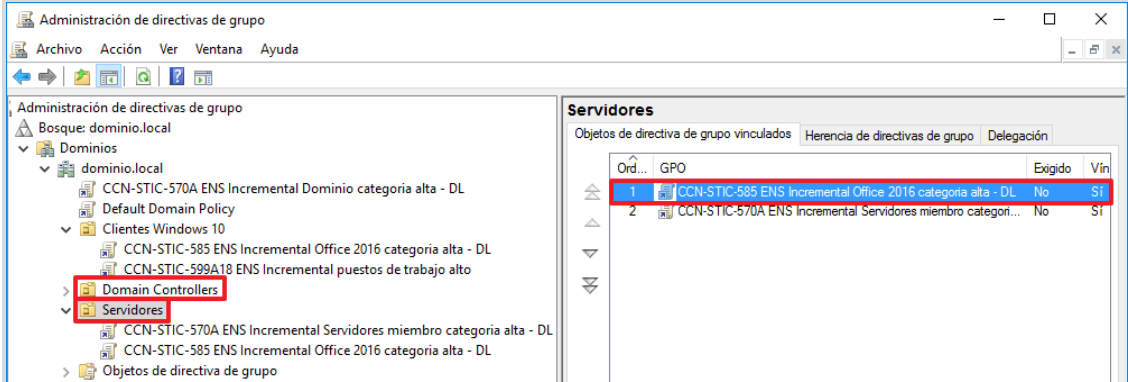
Paso	Descripción
	
5.	<p>Por último, se evalúan las configuraciones predeterminadas establecidas para la categoría ALTA del ENS en relación al control de cuentas de usuario en el punto “4. RESOLUCIÓN DE INCIDENCIAS TRAS LA APLICACIÓN DE LAS CONFIGURACIONES DE SEGURIDAD”.</p> 
6.	<p>Para confirmar que se han aplicado correctamente las configuraciones establecidas, deberá seguir el “ANEXO A.4.2. LISTA DE COMPROBACIÓN DE CLIENTE MICROSOFT WINDOWS 10 PARA EL NIVEL ALTO”.</p>
7.	<p>Un indicativo rápido para determinar si se están aplicando las medidas de seguridad es que a la hora de ejecutar cualquier elemento que necesite privilegios de administrador, se deberá solicitar el usuario y la contraseña para poder continuar.</p> 



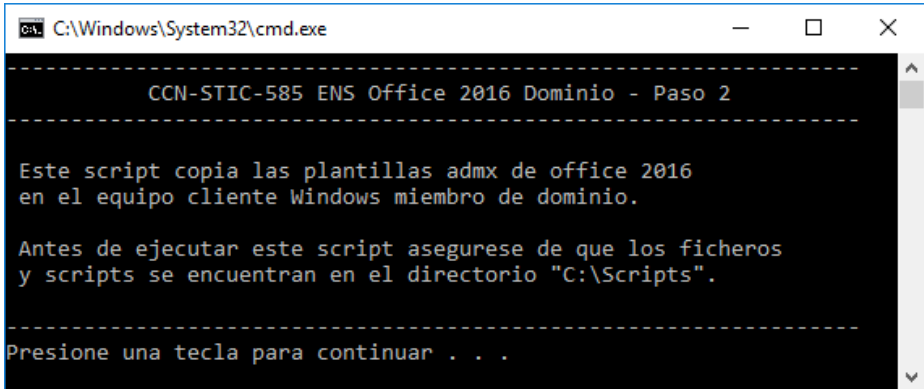
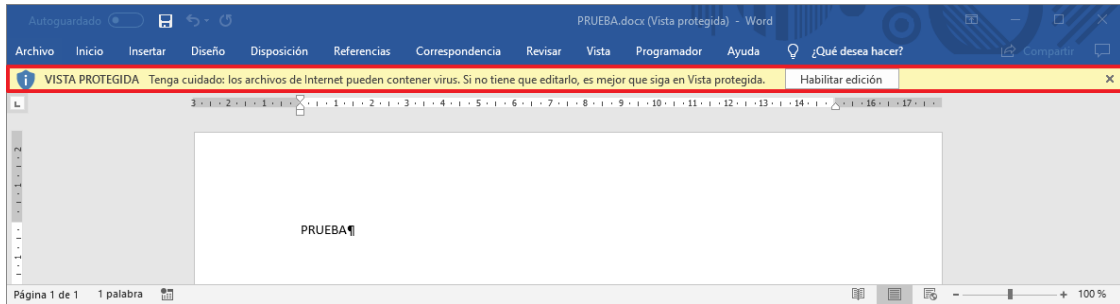
Paso	Descripción
	<p><b>Nota:</b> La solicitud de credenciales durante la ejecución de un elemento como administrador no es un indicativo final que determine que todas las configuraciones se encuentren correctamente aplicadas. Para ello deberá seguir las indicaciones del paso anterior.</p>
8.	De forma predeterminada el control de la configuración del cortafuegos con seguridad avanzada se establece a nivel local y queda activo durante la implementación de la guía CCN-STIC.
9.	<p>No obstante, existe la posibilidad de realizar un control centralizado a través de la aplicación de objetos de políticas de grupo. Para ello debe seguir los pasos indicados en el “ANEXO A.5.1. IMPLEMENTACIÓN DE CORTAFUEGOS CON SEGURIDAD AVANZADA”. La configuración que se establece en dichos pasos permite la gestión del Firewall de Windows a través de dominio y se realiza la explicación de cómo crear reglas de entrada.</p> 
10.	<p>Cabe destacar que durante la aplicación de la guía no se define un software específico contra código dañino. Para ello deberá instalar en sus equipos la solución antivirus que más se adapte a las necesidades de su organización.</p> <p>Si desea habilitar la solución por defecto proporcionada por Microsoft Windows (Windows Defender) deberá seguir los pasos indicados en el “APARTADO 4.5. TAREAS ADICIONALES” en el punto “4.5.1 HABILITAR WINDOWS DEFENDER” del presente documento.</p>

#### 4.4 MICROSOFT OFFICE 2016

Paso	Descripción
1.	Para aplicar los estándares de seguridad del ENS en su categoría ALTA para el producto MS Office, deberá aplicar los pasos definidos en el punto “1. PREPARACIÓN DEL DIRECTORIO ACTIVO” del “ANEXO A.2.3. CATEGORÍA ALTA / DIFUSIÓN LIMITADA”.
2.	<p>En dicho punto se describen los siguientes aspectos:</p> <ul style="list-style-type: none"> <li>Introducción de los recursos y scripts asociados a la guía “CCN-STIC-585”.</li> <li>Importación de los ficheros ADMX necesarios en el controlador de dominio.</li> <li>Creación de los grupos de seguridad necesarios, así como la vinculación de usuarios y equipos a dichos grupos.</li> </ul>

Paso	Descripción
	<ul style="list-style-type: none"> <li>Creación del objeto GPO "CCN-STIC-585 ENS Incremental Office 2016 categoría alta - DL".</li> <li>Importación de directivas a dicho objeto GPO para su correcta configuración.</li> <li>Vinculación del objeto GPO en las unidades organizativas correspondientes en su orden adecuado.</li> <li>Se establece el filtrado de seguridad de la GPO para que aplique únicamente al grupo de seguridad de equipos creado anteriormente.</li> </ul> <p>Cuando finalice deberá obtener una configuración similar a la siguiente.</p>  <p><b>Nota:</b> En el caso de que por motivos de necesidad de negocio de su organización tenga que hacer uso del paquete ofimático MS Office en servidores, deberá vincular el objeto GPO "CCN-STIC-585 ENS Incremental Office 2016 categoría ALTA - DL" en las unidades organizativas donde se ubiquen dichos equipos. <b>NO ES RECOMENDABLE LA INCLUSIÓN DE UN PAQUETE OFIMÁTICO EN LOS SERVIDORES DE UNA ORGANIZACIÓN, ASÍ COMO LA NAVEGACIÓN A INTERNET DESDE LOS MISMOS.</b></p> 
3.	<p>En el punto "2. PREPARACIÓN DEL CLIENTE PARA LA SECURIZACIÓN DE MS OFFICE 2016 EN UN EQUIPO DEL DOMINIO" se describe el proceso de securización de Microsoft Office 2016 en un cliente Windows 10 miembro de un dominio.</p> <p>Los pasos definidos en dicho punto implican la importación de los ficheros ADMX necesarios en el equipo y el reinicio del mismo para la correcta aplicación de las medidas de seguridad establecidas por políticas de dominio.</p>



Paso	Descripción
	
4.	Para confirmar que se han aplicado correctamente las configuraciones establecidas, deberá seguir el “ANEXO A.2.3.2. LISTA DE COMPROBACIÓN DE SEGURIDAD DE MS OFFICE 2016”.
5.	<p>En este punto habrá quedado securizado MS Office 2016 en el equipo cliente. A parte de la lista de comprobación podrá verificar el correcto funcionamiento de la seguridad aplicada si se envía un documento “.docx” de Microsoft Word desde una cuenta de correo procedente de fuera del dominio de su organización. Dicho documento al intentar ser abierto lo hará en el modo “VISTA PROTEGIDA”, evitando toda ejecución de código que se pudiera generar desde el mismo.</p> 

## 4.5 TAREAS ADICIONALES

### 4.5.1 HABILITAR WINDOWS DEFENDER

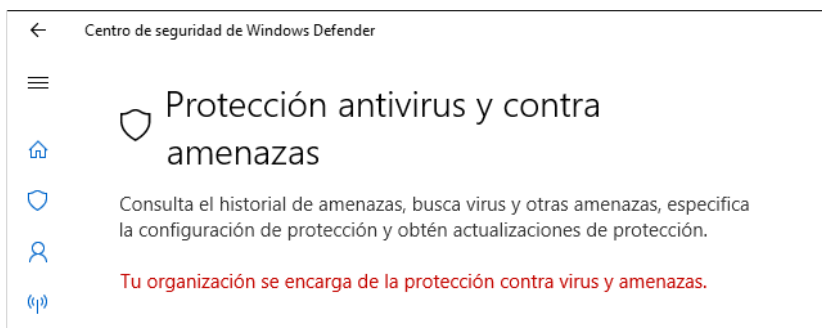
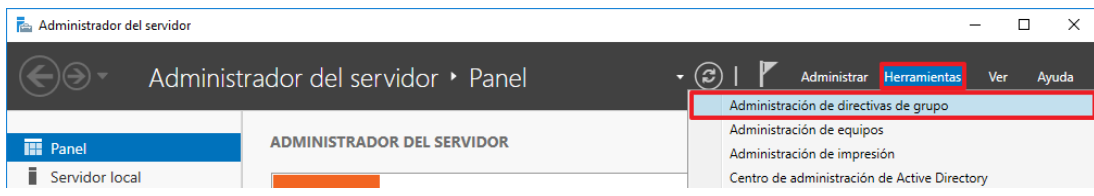
Según lo definido en la medida de seguridad “OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO”, y tal como reflejan las guías CCN-STIC, la organización para puestos de trabajo deberá implementar una solución antimalware que proteja contra código dañino. Se considerarán como tal los virus, gusanos, troyanos, programas espías y en general cualquier tipo de aplicación considerada como código dañino.

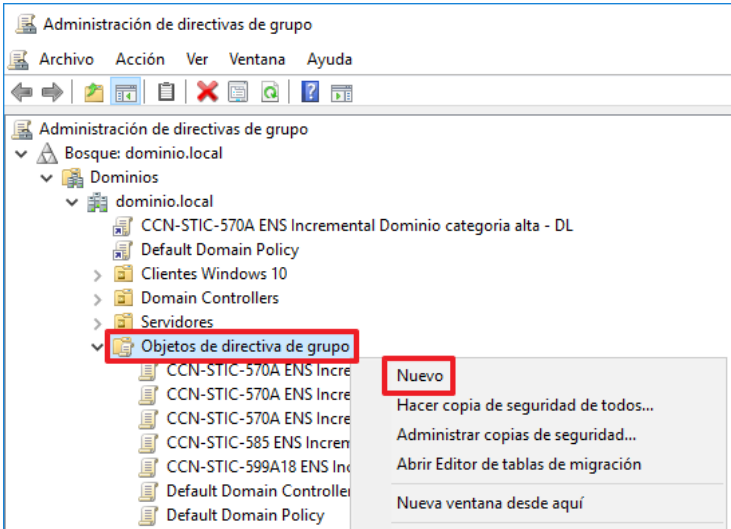
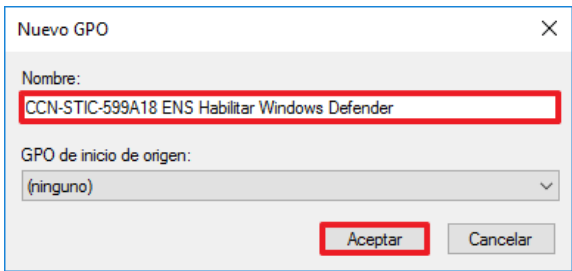
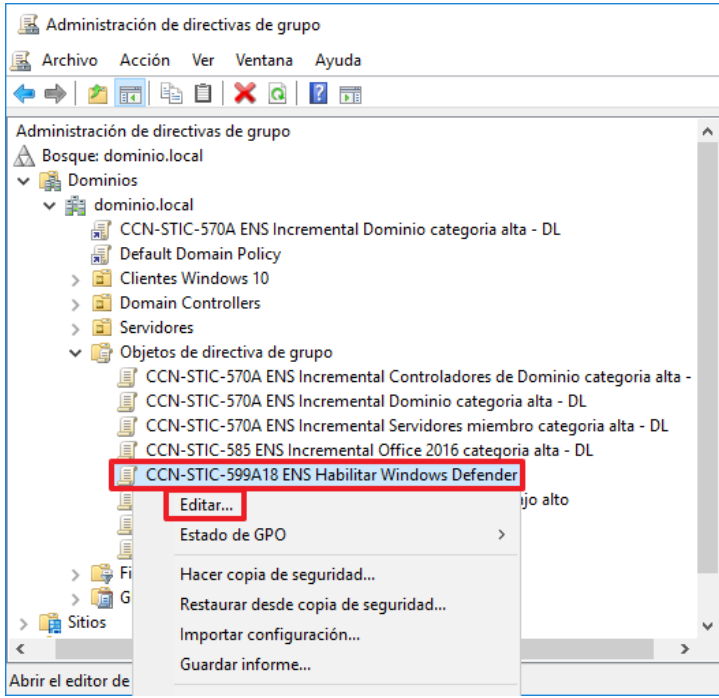
Debe tomarse en consideración que, aunque Windows 10 tenga implementada de forma predeterminada la solución Windows Defender, ésta no cubre todo el espectro de protección frente a código dañino. Por ejemplo, sin una solución de administración centralizada como la aportada por MS System Center 2012 Endpoint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

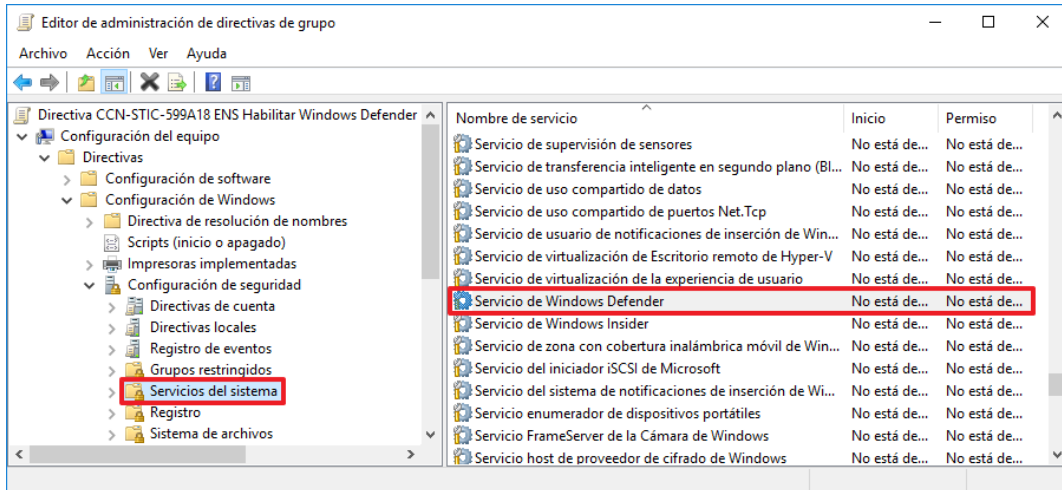
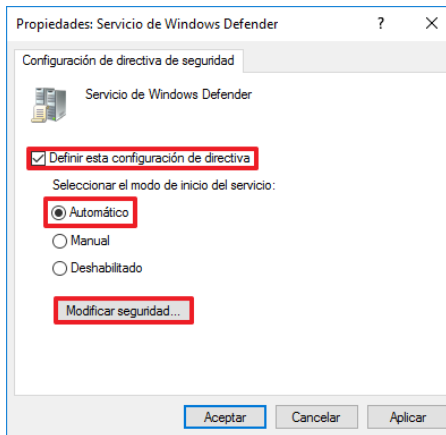
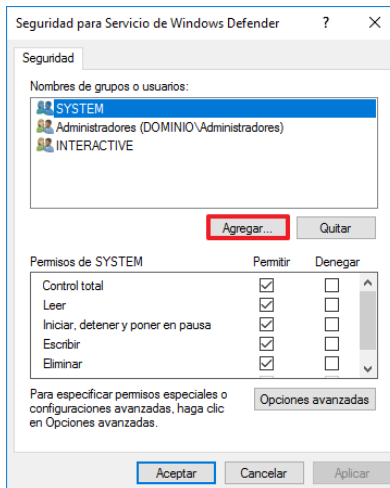
Adicionalmente este producto en sí mismo no ofrece un mecanismo de protección con administración centralizada, objetivo fundamental de toda organización no solo para centralizar los procesos de despliegue y configuración de políticas de protección, sino de la centralización de los estados y reportes de detección y eliminación de código dañino.

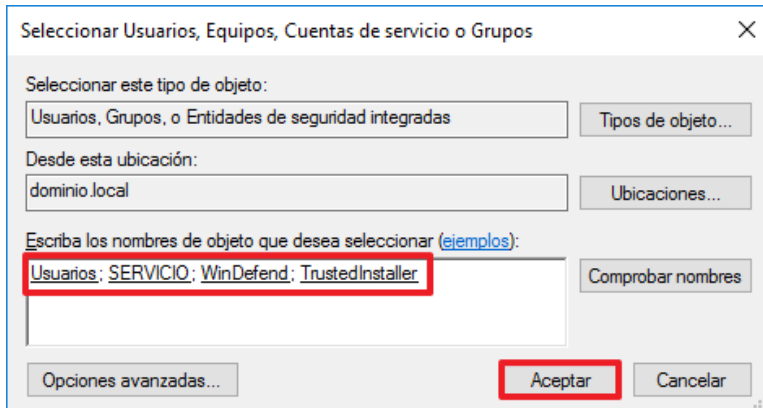
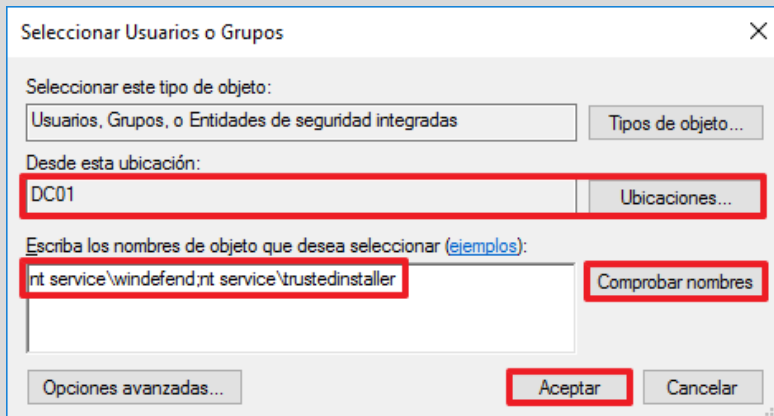
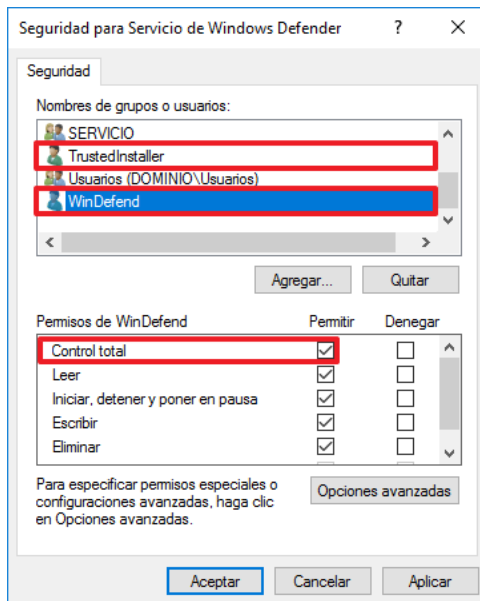
Las organizaciones deberán por lo tanto proveer de otra solución frente a código dañino que ofrezca un alcance completo en la detección y eliminación de código dañino, así como atender a las recomendaciones del fabricante para su mantenimiento.

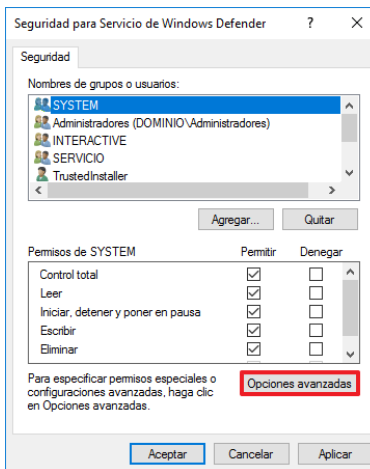
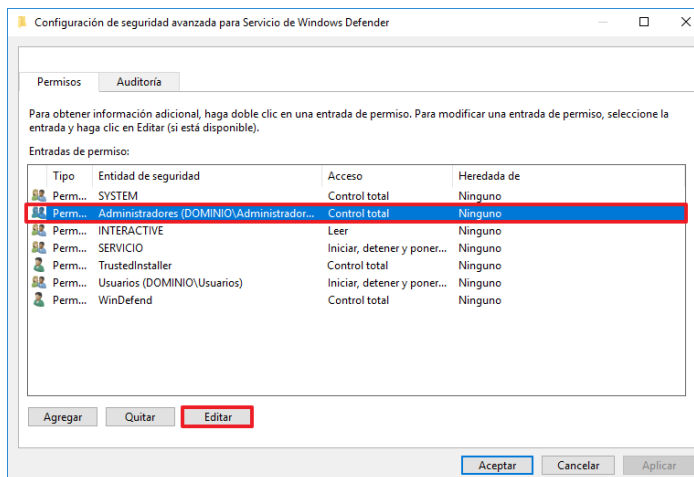
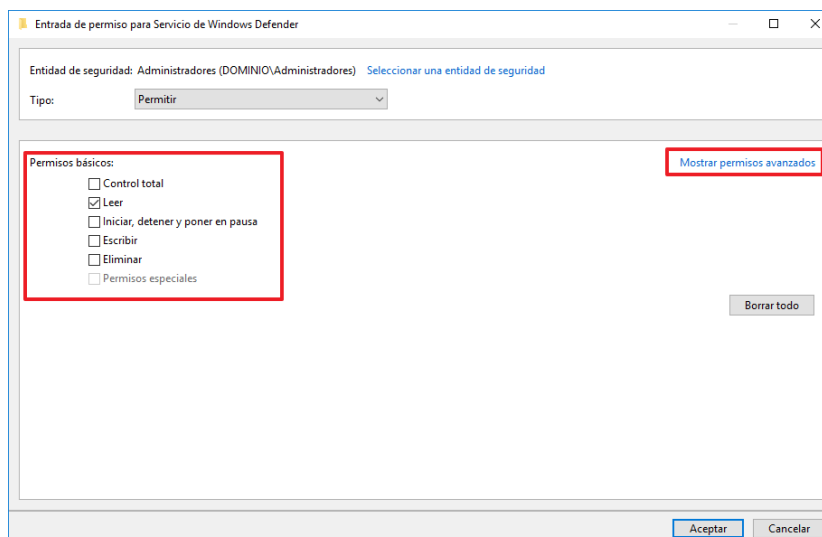
En el caso de no disponer de otra solución contra código dañino, se podrá habilitar el producto ofrecido por defecto por el fabricante siguiendo el siguiente paso a paso.

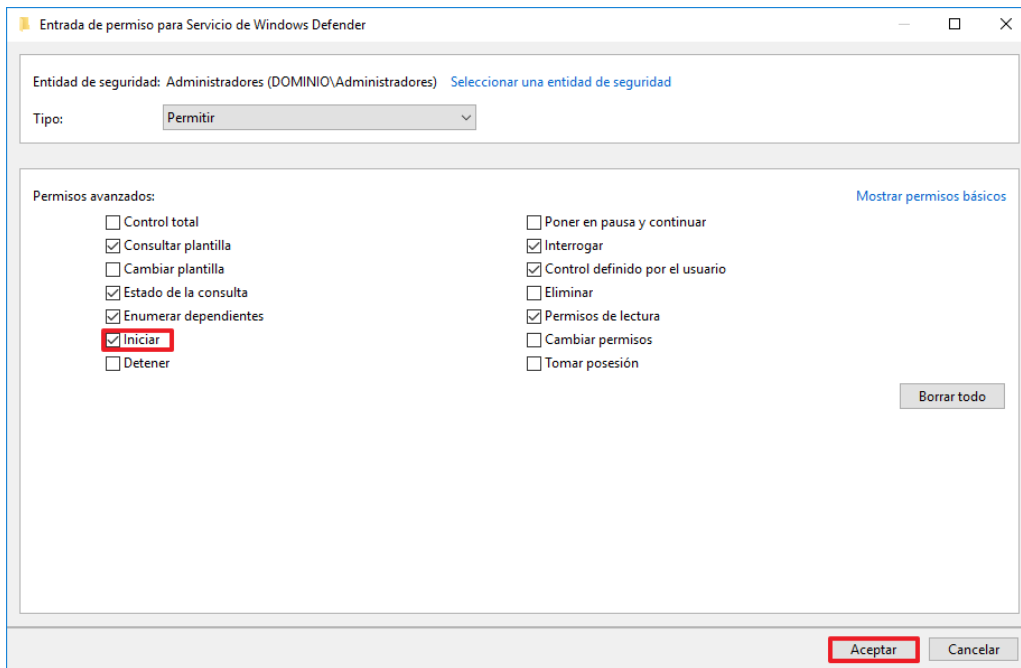
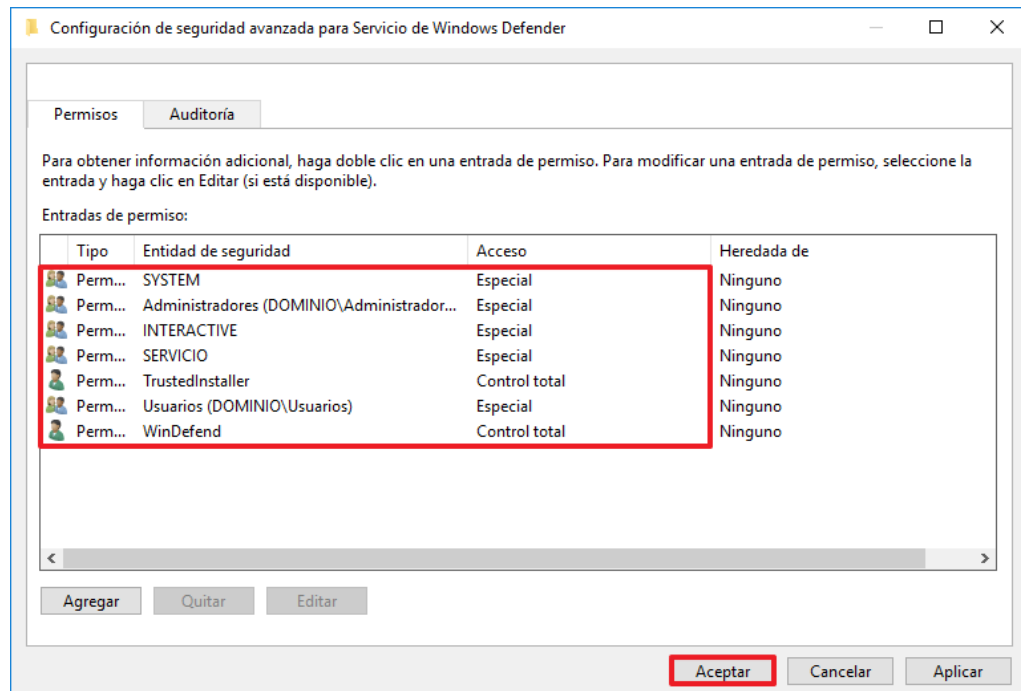
Paso	Descripción
1.	<p>Como se ha indicado anteriormente, Windows Defender se encuentra deshabilitado en los sistemas a los que se les ha implementado las configuraciones de seguridad del ENS para su categoría ALTA con el fin de poder implementar otra solución de forma centralizada y cumpla todos los requisitos descritos anteriormente.</p> 
2.	<p>Para implementar la solución "Windows Defender" inicie sesión en el controlador de dominio de su sistema con un usuario con privilegios de administrador.</p>
3.	<p>Inicie la herramienta "Administración de Directivas de Grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione:</p> <p><b>"Herramientas → Administración de directivas de grupo"</b></p> 
4.	<p>Despliegue el nodo "Objetos de directiva de grupo", haga clic derecho sobre él y seleccione la opción "Nuevo" del menú contextual.</p>

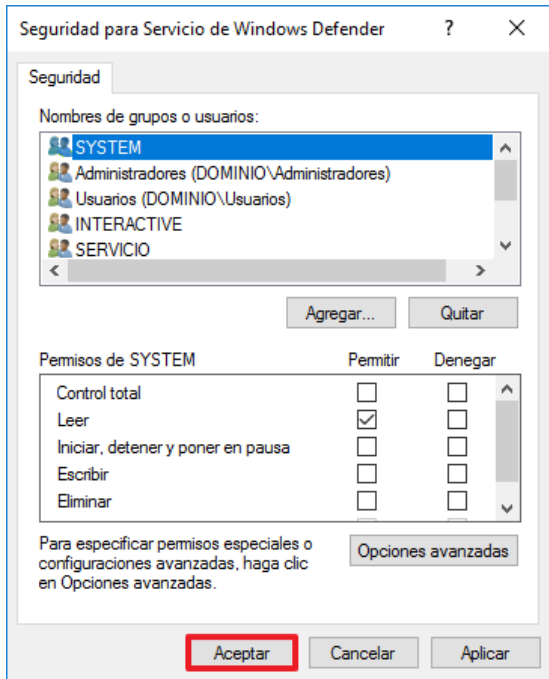
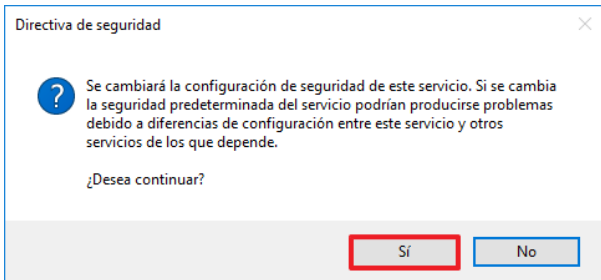
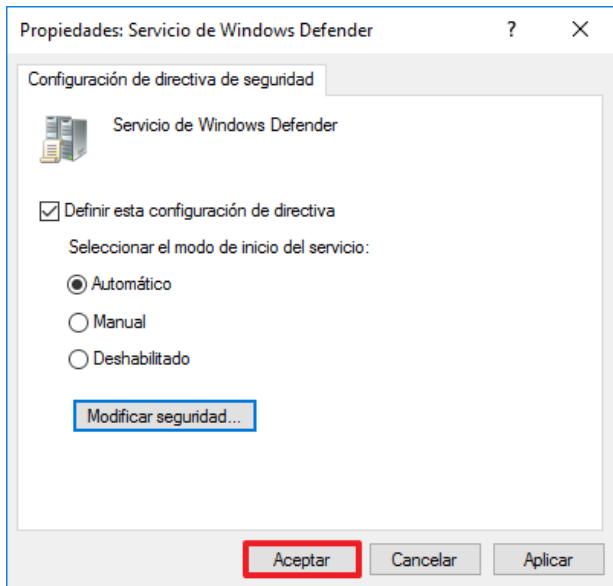
Paso	Descripción
	
5.	<p>Establezca el nombre “CCN-STIC-599A18 ENS Habilitar Windows Defender” al objeto GPO que se va a crear.</p> 
6.	<p>Haga clic derecho sobre la política de grupo recién creada y seleccione la opción “Editar...” del menú contextual.</p> 

Paso	Descripción
7.	<p>Despliegue el nodo “CCN-STIC-599A18 ENS Habilitar Windows Defender → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema” y haga doble clic sobre el servicio “Servicio de Windows Defender”.</p> 
8.	<p>Establezca la opción “Definir esta configuración de directiva”, marque el modo de inicio “Automático” y pulse “Modificar seguridad...”.</p> 
9.	<p>Seleccione la opción “Agregar”.</p> 

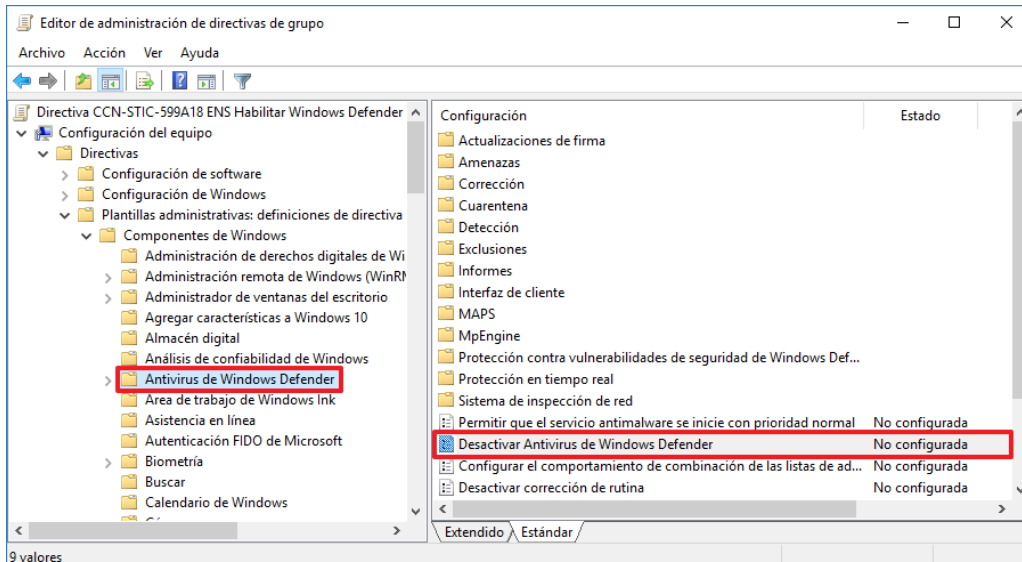
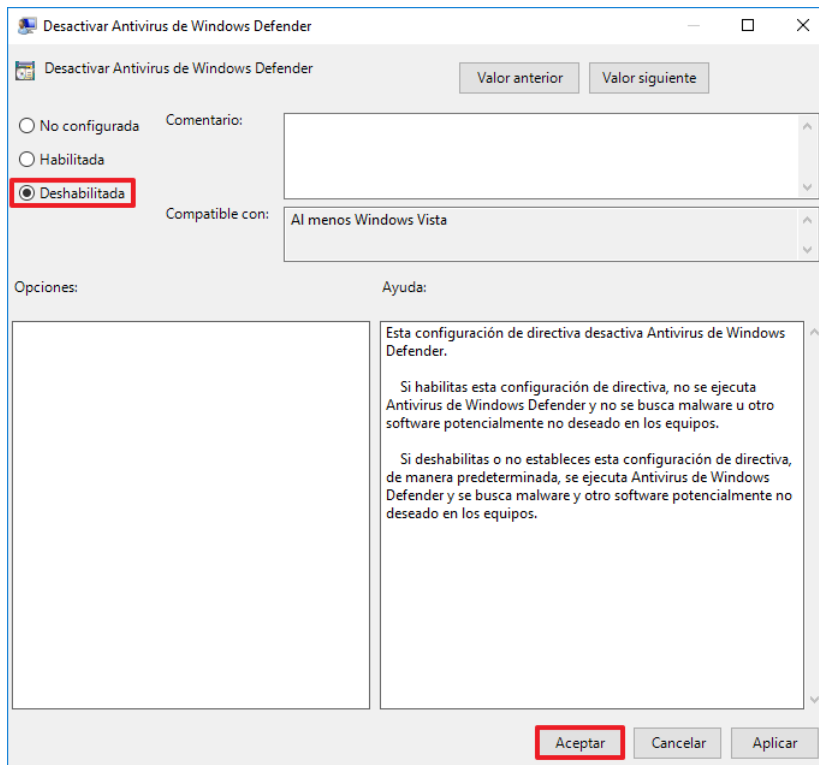
Paso	Descripción
10.	<p>Añada los objetos “Usuarios”, “SERVICIO”, “WinDefend”, “TrustedInstaller” y pulse “Aceptar”.</p>  <p><b>Nota:</b> Para agregar las entidades de seguridad “WinDefend” y “TrustedInstaller” deberá escribir “nt service\windefend; nt service\trustedinstaller” habiendo establecido la ubicación en el equipo local.</p> 
11.	<p>Establezca en “Control total” los permisos de “TrustedInstaller” y “WinDefend”.</p> 

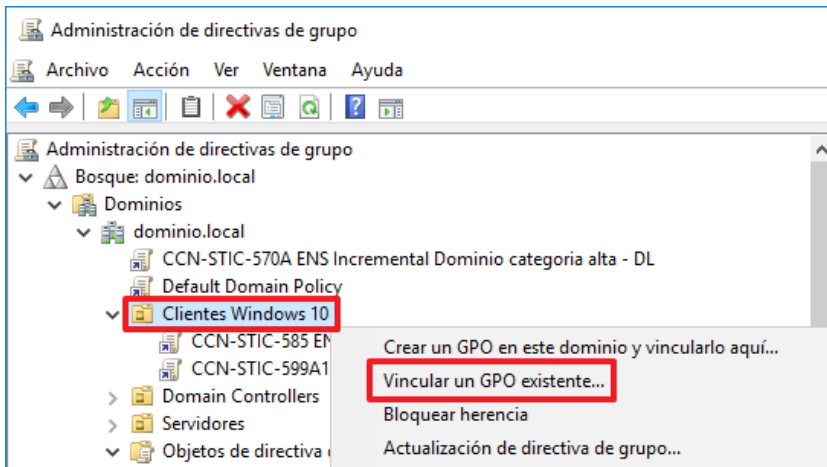
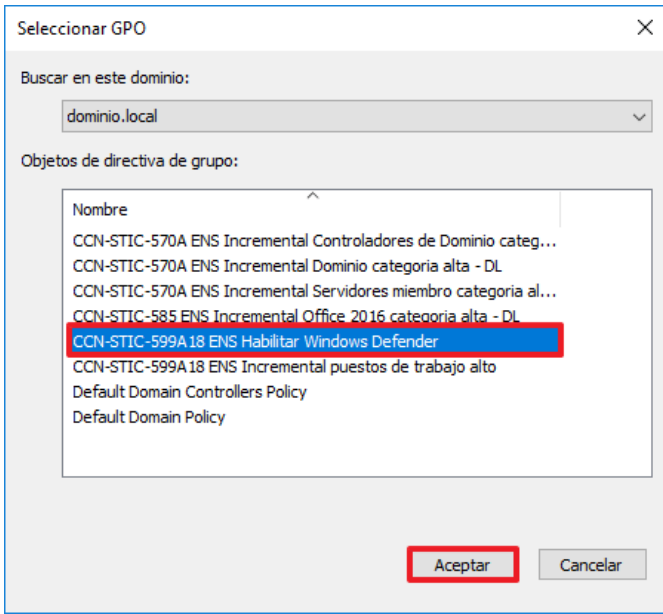
Paso	Descripción
12.	<p>Pulse en “Opciones avanzadas”.</p> 
13.	<p>Seleccione el grupo “Administradores” y pulse “Editar”.</p> 
14.	<p>Desmarque los permisos básicos hasta mantener únicamente el permiso de lectura y seleccione la opción “Mostrar permisos avanzados”.</p> 

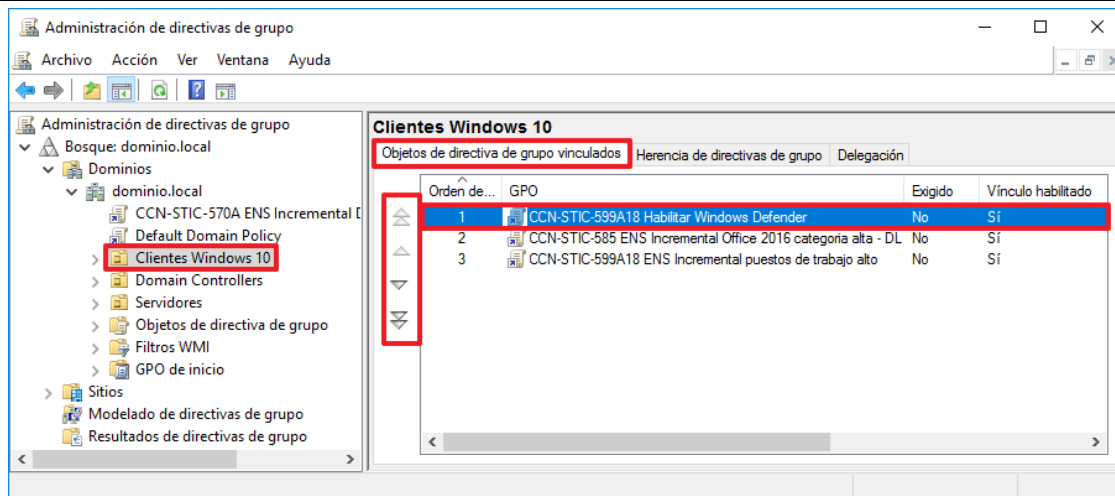
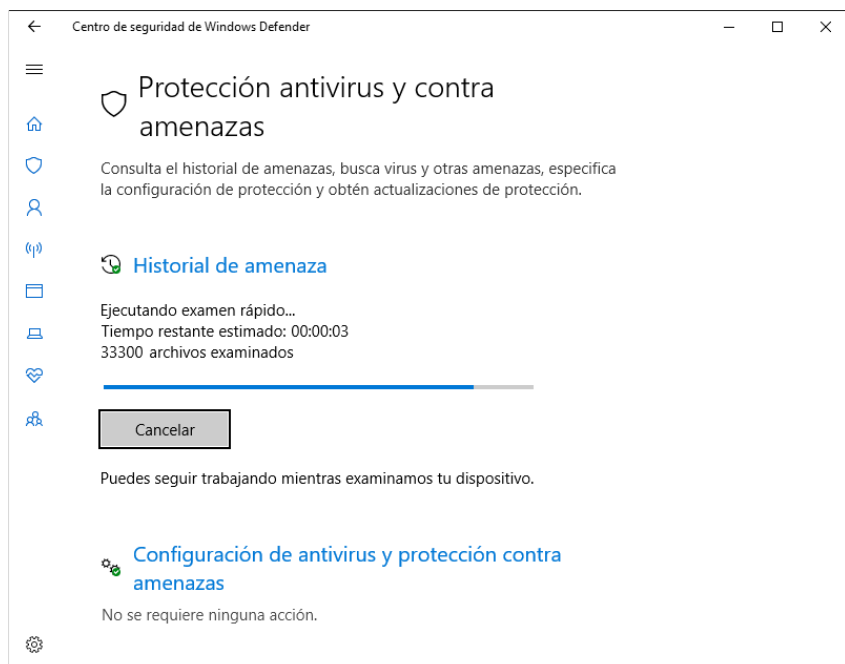
Paso	Descripción
15.	<p>Adicionalmente a los permisos establecidos, añada el permiso avanzado de “Iniciar” y pulse “Aceptar”.</p> 
16.	<p>Repita los pasos para las entidades de seguridad “Usuarios”, “SERVICIO”, “SYSTEM” e “INTERACTIVE” y pulse “Aceptar”.</p> 
17.	<p>Pulse nuevamente sobre “Aceptar”.</p>

Paso	Descripción
	
18.	<p>Ante la ventana emergente, pulse “Sí” para continuar.</p> 
19.	<p>Pulse “Aceptar” para finalizar la configuración de los servicios.</p> 



Paso	Descripción
20.	<p>Despliegue el nodo “CCN-STIC-599A18 ENS Habilitar Windows Defender → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Antivirus de Windows Defender” y modifique la directiva “Desactivar Antivirus de Windows Defender” haciendo doble clic sobre ella.</p> 
21.	<p>Establezca el valor en “Deshabilitada” y pulse “Aceptar”.</p> 
22.	Cierre el “Editor de administración de directivas de grupo”.
23.	<p>Seleccione con botón derecho la unidad organizativa donde se encuentren los equipos a los que se les va a habilitar “Windows Defender” y seleccione la opción “Vincular un GPO existente...” dentro de la</p>

Paso	Descripción
	<p>herramienta “Administración de directivas de grupo”.</p>  <p><b>Nota:</b> En este ejemplo se establece la configuración en la unidad organizativa “Clientes Windows 10”. Si desea habilitar Windows Defender en los servidores deberá realizar estos pasos en las unidades organizativas donde se alojen dichas máquinas.</p>
24.	<p>Seleccione el objeto GPO “CCN-STIC 599A18 ENS Habilitar Windows Defender” y pulse “Aceptar” para continuar.</p> 
25.	<p>Una vez agregado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 599A18 ENS Habilitar Windows Defender”.</p>
26.	<p>Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC-599A18 Habilitar Windows Defender” en primer lugar dentro del orden de vínculo.</p>

Paso	Descripción																
	 <p>Administración de directivas de grupo</p> <p>Objetos de directiva de grupo vinculados</p> <table><thead><tr><th>Orden de...</th><th>GPO</th><th>Exigido</th><th>Vínculo habilitado</th></tr></thead><tbody><tr><td>1</td><td>CCN-STIC-599A18 Habilitar Windows Defender</td><td>No</td><td>Si</td></tr><tr><td>2</td><td>CCN-STIC-585 ENS Incremental Office 2016 categoría alta - DL</td><td>No</td><td>Si</td></tr><tr><td>3</td><td>CCN-STIC-599A18 ENS Incremental puestos de trabajo alto</td><td>No</td><td>Si</td></tr></tbody></table>	Orden de...	GPO	Exigido	Vínculo habilitado	1	CCN-STIC-599A18 Habilitar Windows Defender	No	Si	2	CCN-STIC-585 ENS Incremental Office 2016 categoría alta - DL	No	Si	3	CCN-STIC-599A18 ENS Incremental puestos de trabajo alto	No	Si
Orden de...	GPO	Exigido	Vínculo habilitado														
1	CCN-STIC-599A18 Habilitar Windows Defender	No	Si														
2	CCN-STIC-585 ENS Incremental Office 2016 categoría alta - DL	No	Si														
3	CCN-STIC-599A18 ENS Incremental puestos de trabajo alto	No	Si														
27.	En este momento habrá quedado correctamente configurado el objeto GPO que implementa las necesidades a través de dominio para habilitar la solución antivirus Windows Defender. Reinicie los equipos a los que se les va a aplicar dichas configuraciones.																
28.	Una vez iniciados los equipos, podrá comprobar que la herramienta “Centro de seguridad de Windows Defender” ubicada en “Configuración de Windows → Actualización y seguridad → Seguridad de Windows → Protección contra virus y amenazas” funciona correctamente y es capaz de examinar el equipo en busca de amenazas.																
	 <p>Centro de seguridad de Windows Defender</p> <p>Protección antivirus y contra amenazas</p> <p>Consulta el historial de amenazas, busca virus y otras amenazas, especifica la configuración de protección y obtén actualizaciones de protección.</p> <p>Historial de amenaza</p> <p>Ejecutando examen rápido... Tiempo restante estimado: 00:00:03 33300 archivos examinados</p> <p>Cancelar</p> <p>Puedes seguir trabajando mientras examinamos tu dispositivo.</p> <p>Configuración de antivirus y protección contra amenazas</p> <p>No se requiere ninguna acción.</p>																