centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 572

IMPLEMENTACIÓN DEL ENS EN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2016

NOVIEMBRE 2018

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

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
2018.11.29 15:30:46 +01'00'

NIPO: 083-19-034-0
Fecha de Edición: noviembre de 2018

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

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.

noviembre de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE SERVIDOR DE IMPRESIÓN EN EL ENS 6
ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2016 6
1. APLICACIÓN DE MEDIDAS EN UN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2016 6
1.1. MARCO OPERACIONAL 7
1.1.1. CONTROL DE ACCESO 7
1.1.2. EXPLOTACIÓN 8
1.2. MEDIDAS DE PROTECCIÓN 10
2. RESUMEN Y APLICACIÓN DE MEDIDAS EN SERVIDOR DE IMPRESIÓN 12
ANEXO A.2. CATEGORÍA BÁSICA 13
ANEXO A.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN 13
1. PREPARACIÓN DEL DOMINIO 13
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 25
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 25
2.2. GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN 30
2.3. GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN 35
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN PARA LA CATEGORÍA BÁSICA 38
ANEXO A.3. CATEGORÍA MEDIA 47
ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN 47
1. PREPARACIÓN DEL DOMINIO 48
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 59
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 59
2.2. GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN 64
2.3. GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN 69
2.4. GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN 72
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN PARA LA CATEGORÍA MEDIA 78
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA 86
ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN 86
1. PREPARACIÓN DEL DOMINIO 87
2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN 98
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN 98

2.2. GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN 103
2.3. GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN 108
2.4. GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN 112
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA 118

ANEXO A. CONFIGURACIÓN SEGURA DE SERVIDOR DE IMPRESIÓN EN EL ENS

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un puesto servidor que implemente el servicio de servidor de impresión bajo el sistema operativo Microsoft Windows Server 2016.

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2016

1. APLICACIÓN DE MEDIDAS EN UN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2016

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

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

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 el servidor de impresión, 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.

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 los niveles 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 la categoría básica mientras que en la categoría media y alta se requiere una mayor exigencia.

1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO

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

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

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

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

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia

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 de impresión en un dispositivo, 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 imprimir se debe considerar como la opción más óptima desde el punto de vista del ENS.

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

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

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

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de otra función.

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura y puesta en marcha de la guía “CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2”.

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

Estas medidas requieren consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para poder cumplir las obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

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 deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda imprimir contenido por un dispositivo de impresión no autorizado. Se establece por lo tanto a nivel de dispositivos de impresión el aplicar mecanismos de ACL para permitir la impresión de contenido a los usuarios que los requieran exclusivamente.

1.1.2. EXPLOTACIÓN

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

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

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Los dispositivos de impresión antes de su entrada en producción deberán configurarse de tal forma que:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplicará la regla de mínima funcionalidad.

c) Se deshabilitarán protocolos adicionales innecesarios para el correcto funcionamiento del dispositivo de impresión, tales como, SMTP, Telnet, etc.

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

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

Adicionalmente la guía configurará a través de objetos GPO o bien mostrará mecanismos de administración adicionales con objeto de reducir la superficie de exposición.

1.1.2.2. OP. EXP. 5. GESTIÓN DE CAMBIOS

En la categoría básica del ENS se recomienda mantener un control de los cambios realizados en el sistema, y en las categorías media y alta de seguridad se deberá mantener un control continuo de los cambios realizados en el sistema, por lo que, todos los cambios anunciados por el proveedor o fabricante de los controladores de los dispositivos de impresión, deberán serán analizados previamente para establecer su conveniencia en la incorporación al sistema o no.

Previamente a la puesta en producción de una modificación, se ha de comprobar su correcta funcionalidad en el sistema en un entorno que no esté en producción, este entorno debe ser un fiel reflejo del entorno de producción.

Todos los cambios realizados deben ser planificados con anterioridad para minimizar en la medida de lo posible el impacto sobre la prestación de los servicios afectados.

Se ha de tener en consideración mediante un análisis de riesgos si los cambios a realizar son de mayor o menor relevancia para la seguridad del sistema, por ello, aquellos cambios que impliquen una situación de riesgo de categoría alta deberán ser aprobados explícitamente de forma previa a su implantación.

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

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

a) Quién realiza la actividad, cuándo la realiza y sobre qué.

b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.

d) La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.

e) La categoría alta requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

El servidor de impresión implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que de forma predeterminada los datos son almacenados localmente. Existen no obstante mecanismos nativos para la suscripción y recolección de evento. 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 mecanismos de correlación.

1.2. MEDIDAS DE PROTECCIÓN

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

Solo estas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado son de aplicación sobre las funcionalidades del propio rol de servidor de impresión.

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

1.2.1.1. PROTECCIÓN DE LAS COMUNICACIONES

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

1.2.1.1.1. MP. COM. 2. PROTECCIÓN DE LA CONFIDENCIALIDAD

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

En aquellas organizaciones que les sea de aplicación cualquier categoría del ENS deberán tener en consideración la implementación en los dispositivos de impresión, de un sistema de seguridad de impresión mediante código o tarjeta identificativa, con el propósito de mantener la confidencialidad de los documentos impresos.

Se deberá asegurar el borrado de los documentos almacenados en el dispositivo de impresión, así como establecer mecanismos de cifrado en los datos almacenados, en caso de que el dispositivo de impresión lo permitiese. Para ello se deberá tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

1.2.1.2. PROTECCIÓN DE LA INFORMACIÓN

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

1.2.1.2.1. MP. INFO. 1. DATOS DE CARÁCTER PERSONAL

Se debe asegurar la integridad de la información con una categoría alta de confidencialidad durante su almacenamiento, transmisión o impresión.

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

Se deberá asegurar la implementación de seguridad en los dispositivos de impresión, mediante código o tarjeta identificativa, con el propósito de mantener la confidencialidad de los documentos impresos.

Se deberá asegurar el borrado de los documentos almacenados en el dispositivo de impresión, así como establecer mecanismos de cifrado en los datos almacenados, en caso de que el dispositivo de impresión lo permitiese. Para ello se deberá tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN SERVIDOR DE IMPRESIÓN

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

Control	Medida	Mecanismo de aplicación
OP. ACC.2	Requisitos de acceso	Revisión e implementación de guía CCN-STIC-572, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-572, adaptándolos a la organización.
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-572, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 8	Registro de la actividad de los usuarios	Revisión e implementación de guía CCN-STIC-572, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica. Revisión e implementación guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de impresión con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad.

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

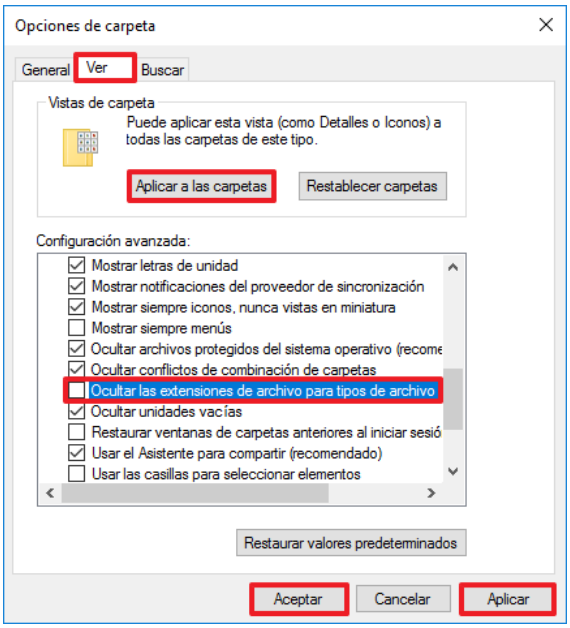
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

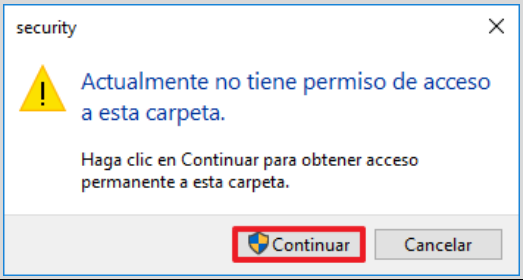
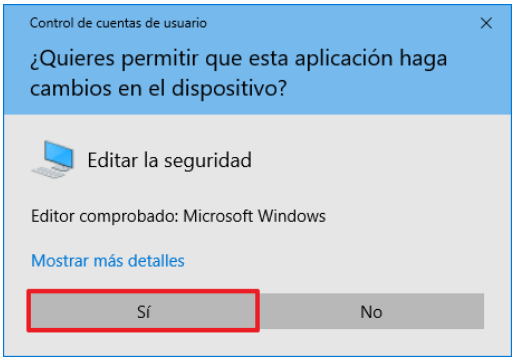
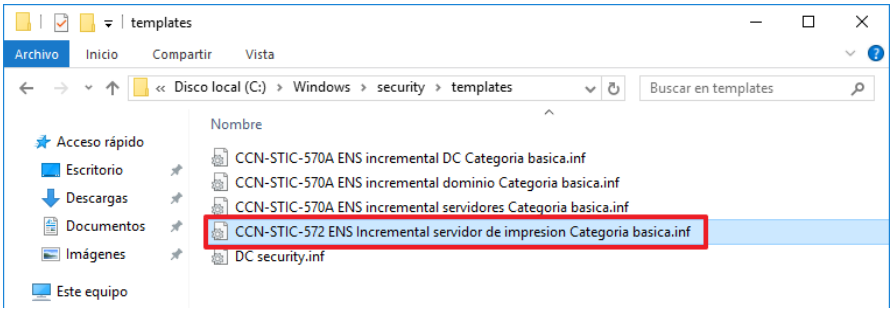
1. PREPARACIÓN DEL DOMINIO

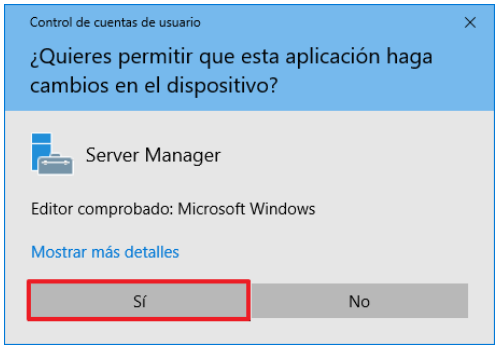
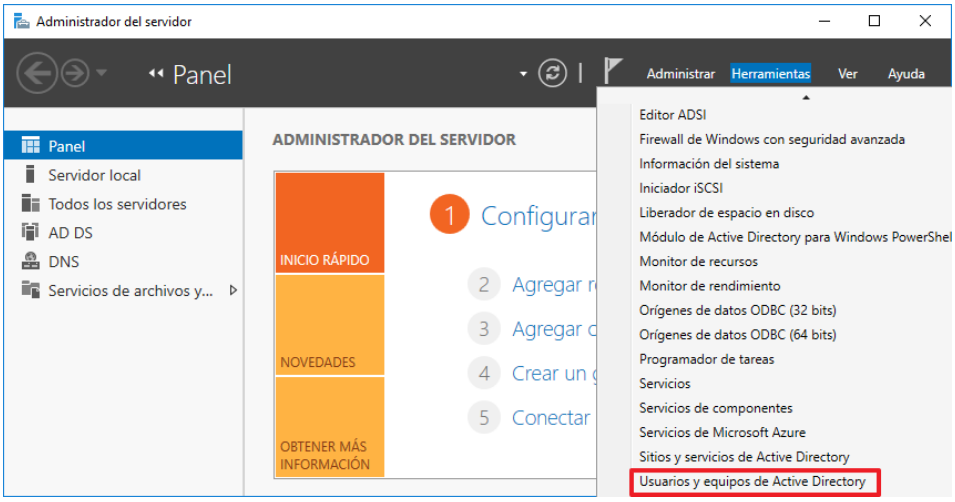
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de impresión miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de impresión y se realizan las configuraciones de políticas de grupo correspondientes.

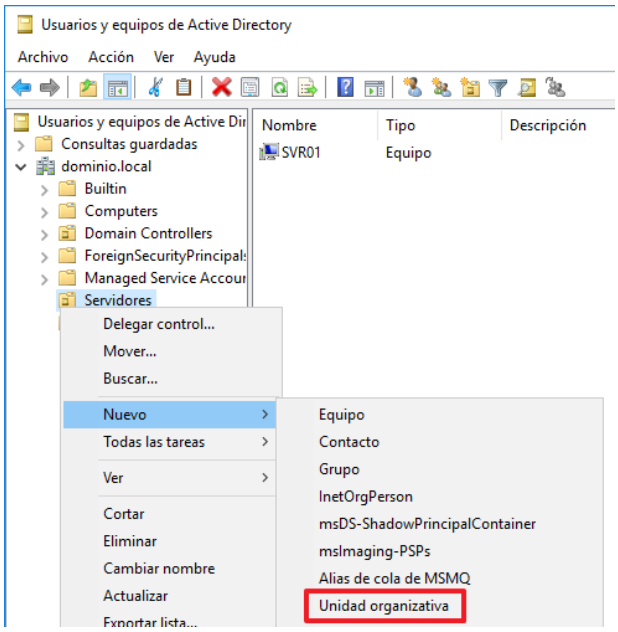
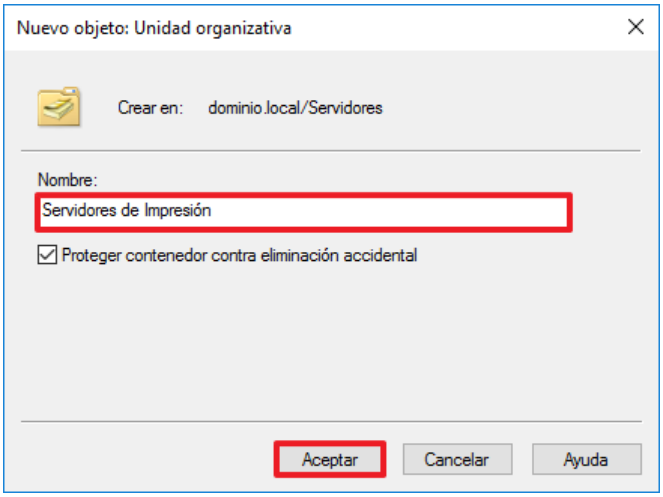
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de impresión que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

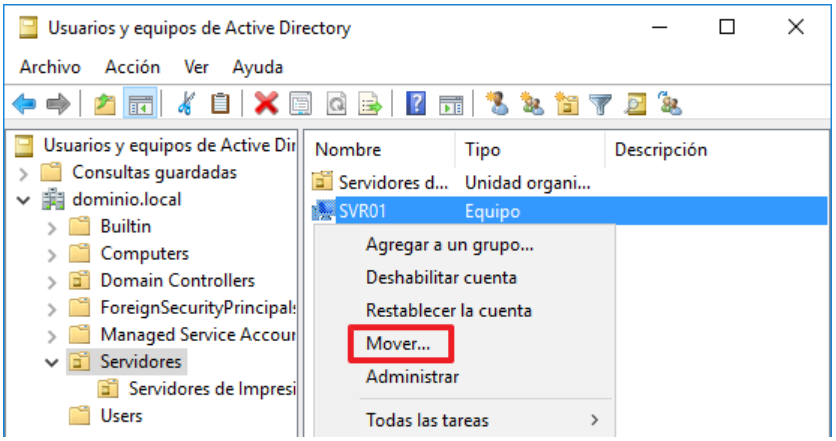
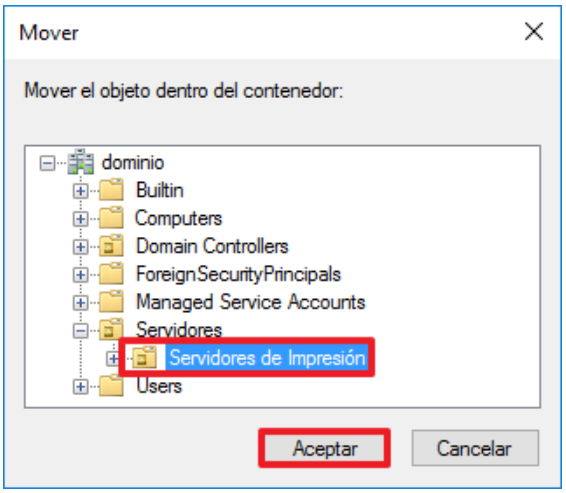
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

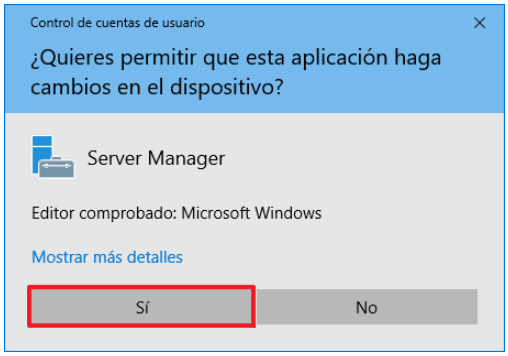
Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
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” muestra las extensiones de los archivos.
5.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. En la venta emergente, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la imagen.  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 “¿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".

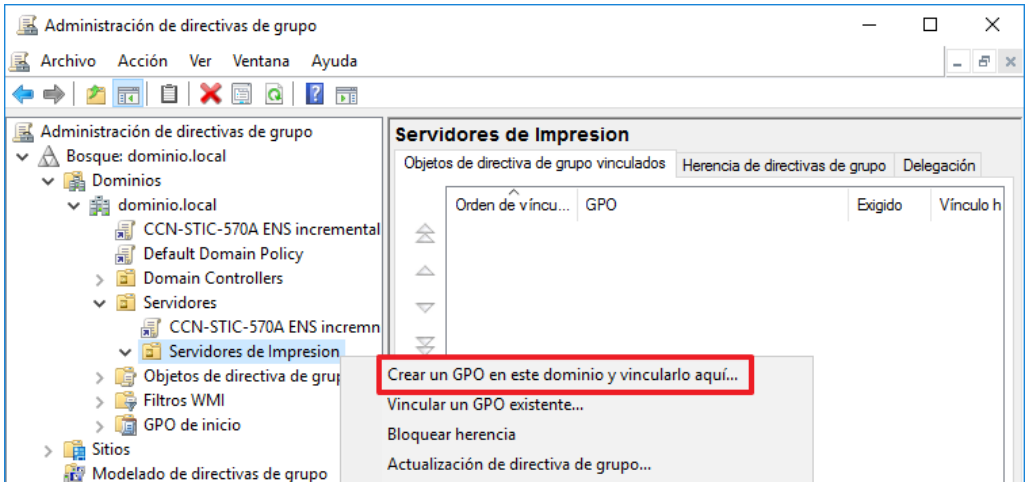
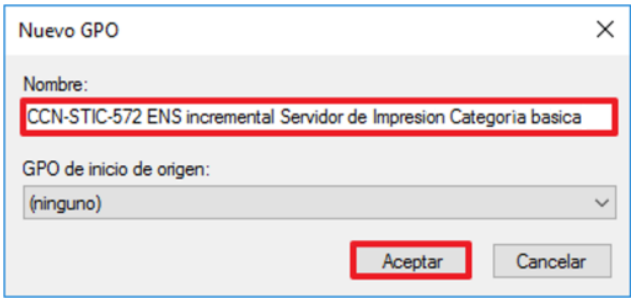
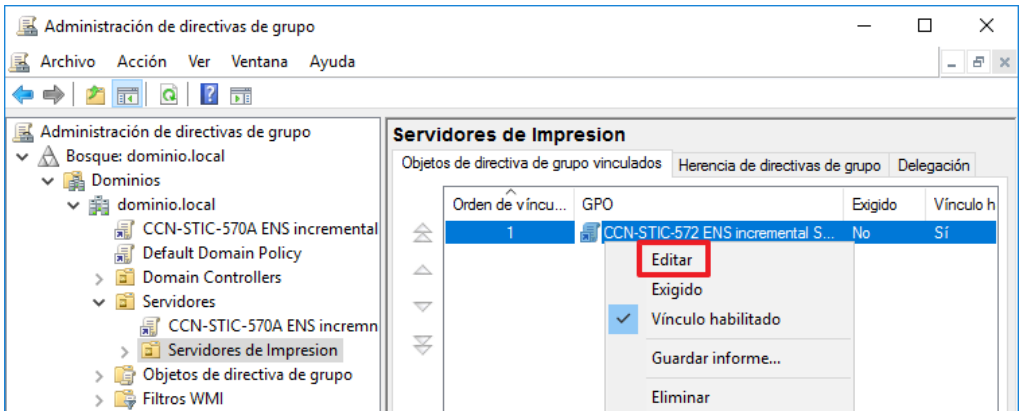
Paso	Descripción
6.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 
7.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
8.	Copie el fichero “CCN-STIC-572 ENS Incremental servidor de impresion Categoria basica.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 
9.	A continuación, deberá crear la unidad organizativa "Servidores de Impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

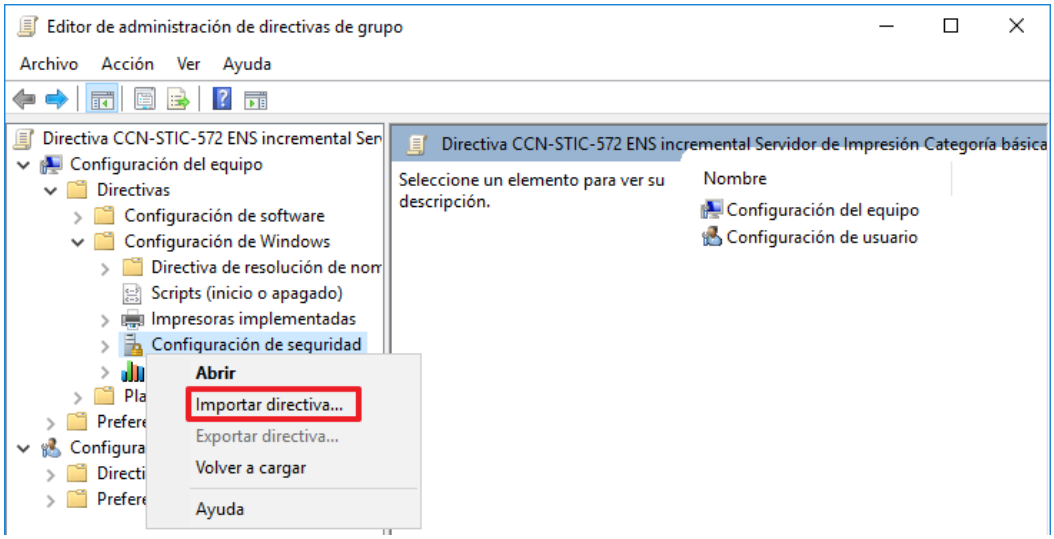
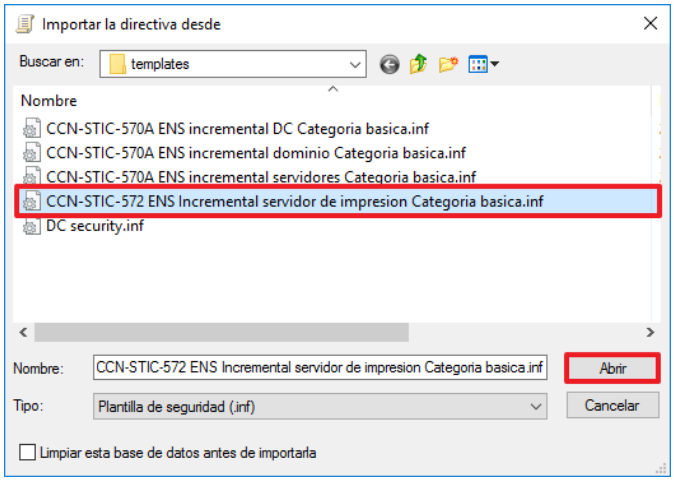
Paso	Descripción
10.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
11.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”**. 

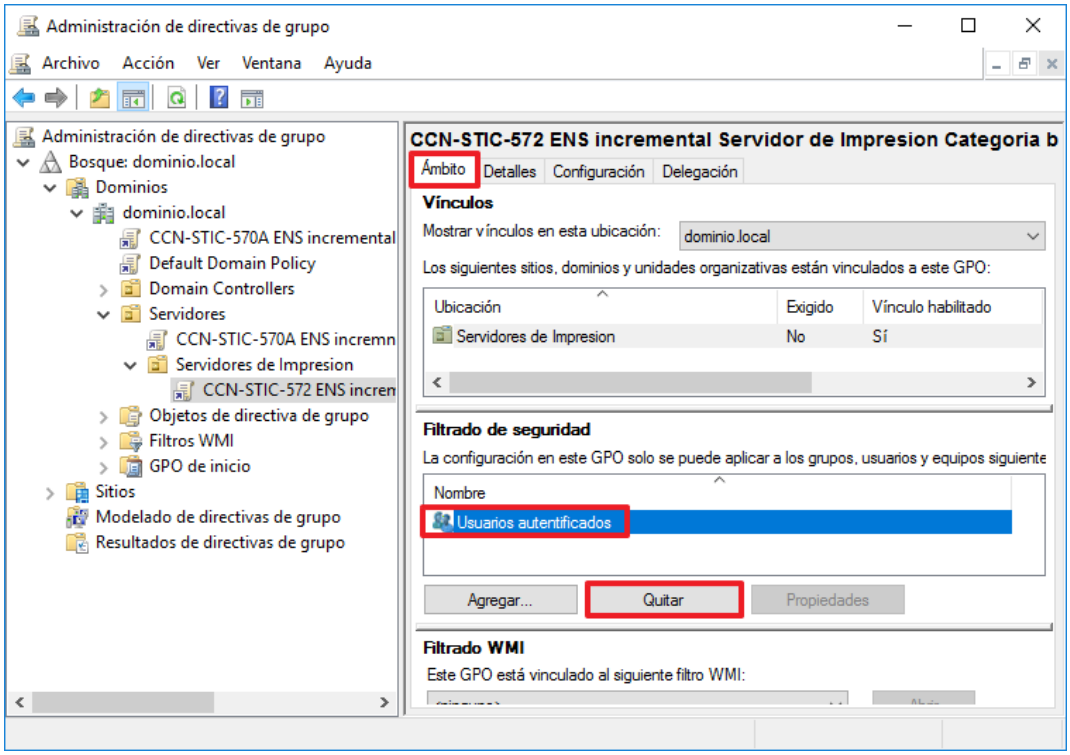
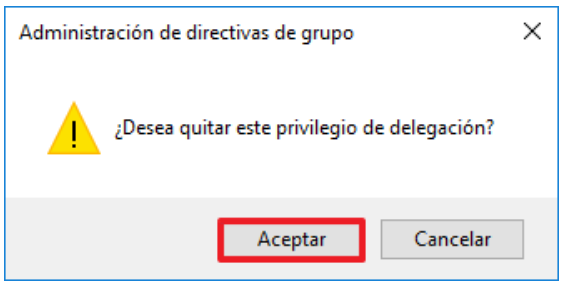
Paso	Descripción
12.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> → <<unidad organizativa>>"**, y desplegando el menú contextual con el botón derecho, seleccione la opción "Nuevo > Unidad organizativa".  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en **"dominio.local → Servidores"**.
13.	Introduzca el nombre "Servidores de impresión" tal y como se muestra en la imagen y pulse sobre "Aceptar". 

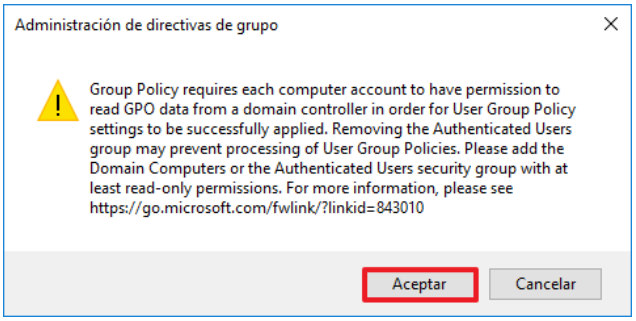
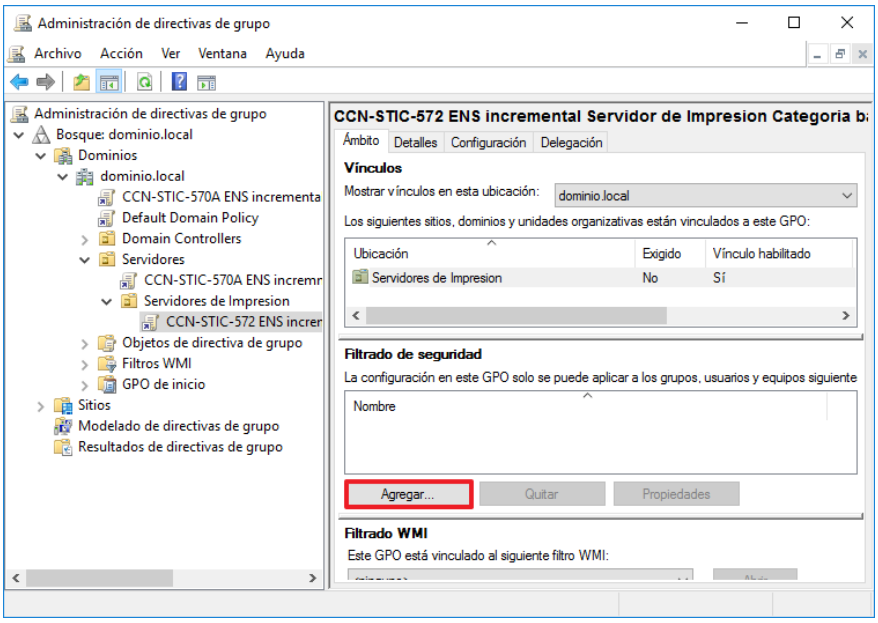
Paso	Descripción
14.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de impresión a la unidad organizativa “Servidores de impresión”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”. 
15.	A continuación, seleccione la unidad organizativa “Servidores de impresión” y pulse “Aceptar”. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	A continuación, deberá crear la GPO "CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

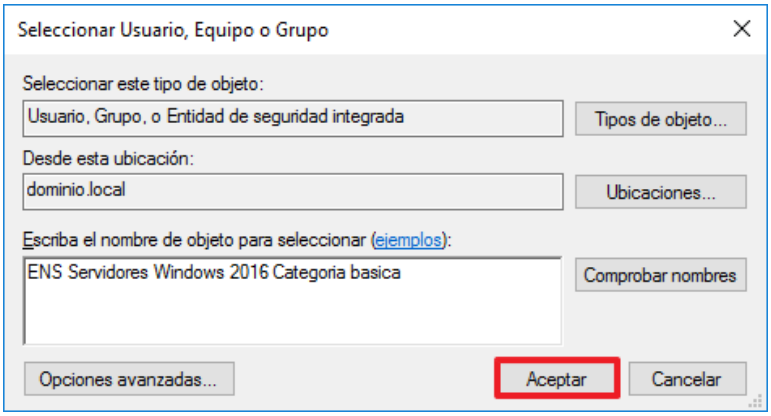
Paso	Descripción
18.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
19.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”.** 
20.	A continuación, despliegue el nodo **“Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de impresión”**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de impresión”.

Paso	Descripción
21.	Pulse con el botón derecho sobre la unidad organizativa “Servidores de impresión” y seleccione “Crear un GPO en este dominio y vincularlo aquí…”. 
22.	Escriba el nombre de la GPO “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica” y haga clic en el botón “Aceptar”. 
23.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
24.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.

Paso	Descripción
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva…”. 
26.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-572 ENS Incremental servidor de impresion categoria basica.inf” y pulse el botón “Abrir”. 
27.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

Paso	Descripción
28.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”. 

Paso	Descripción
30.	Pulse de nuevo “Aceptar” ante el mensaje de advertencia emergente. 
31.	A continuación, pulse el botón “Agregar…”. 

Paso	Descripción
32.	Introduzca como nombre “ENS Servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a las necesidades de su organización.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración.

Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría básica. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

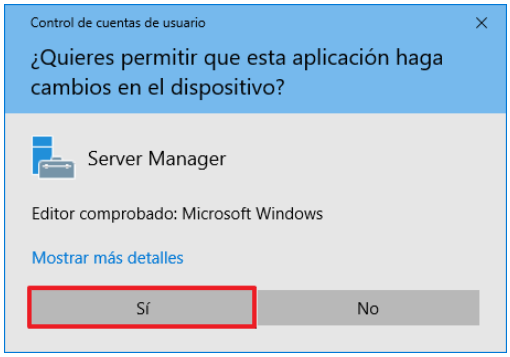
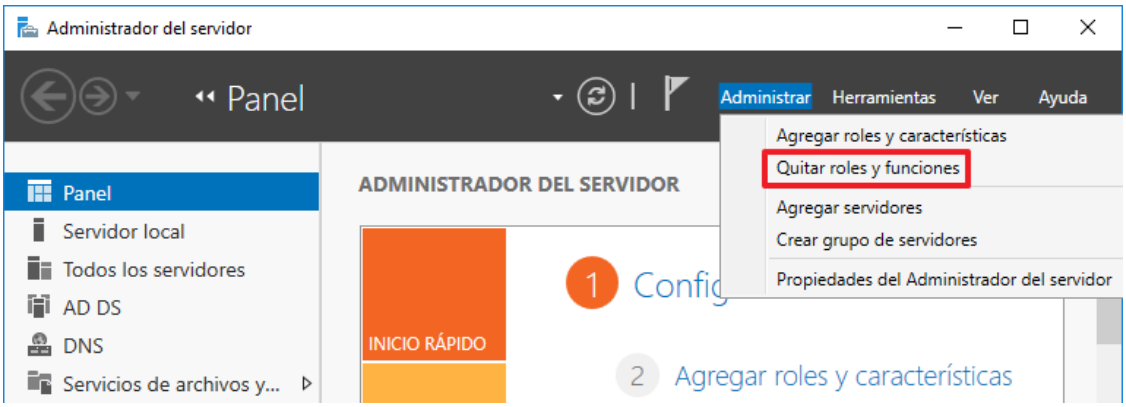
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

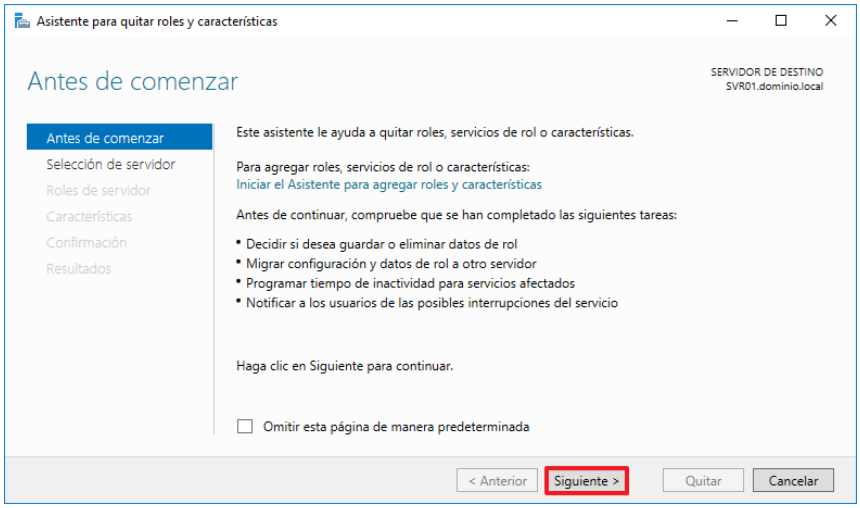
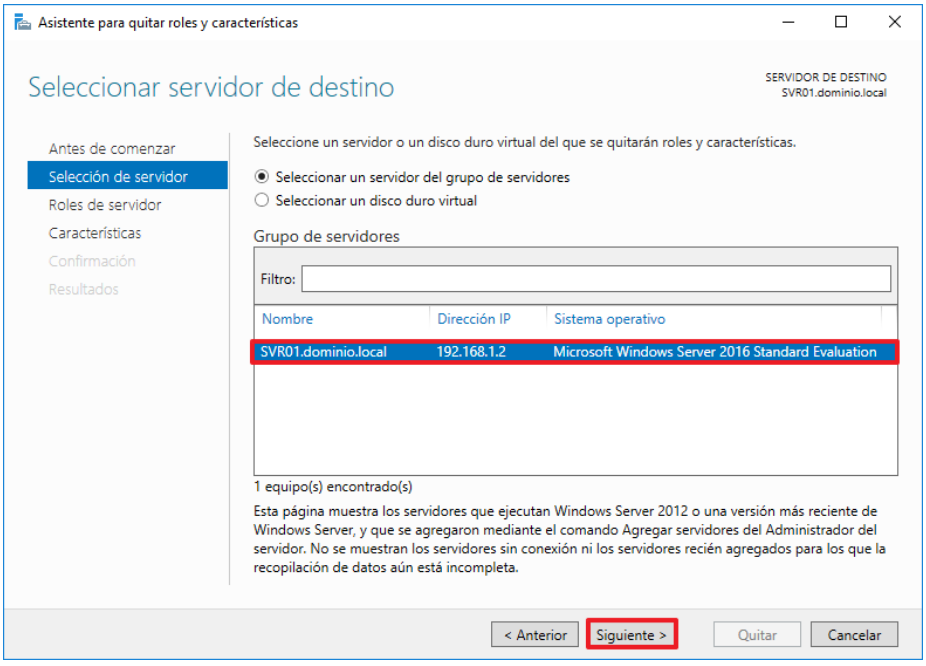
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

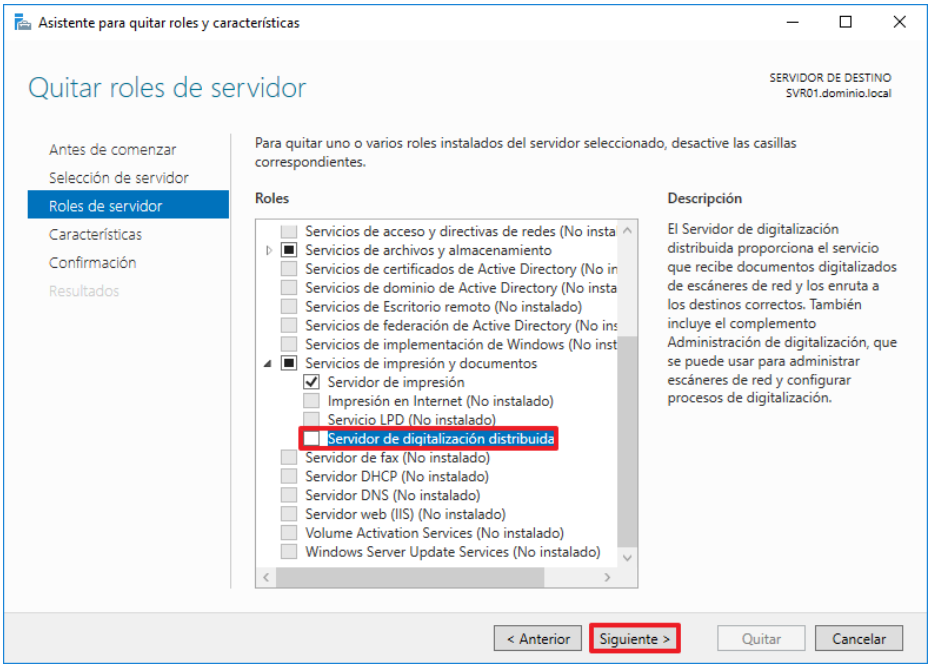
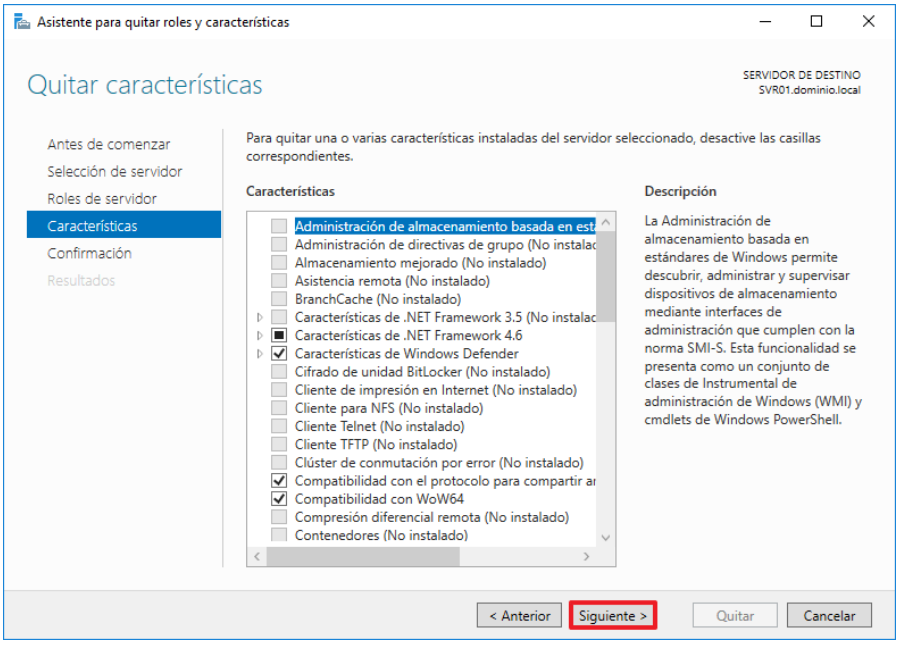
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

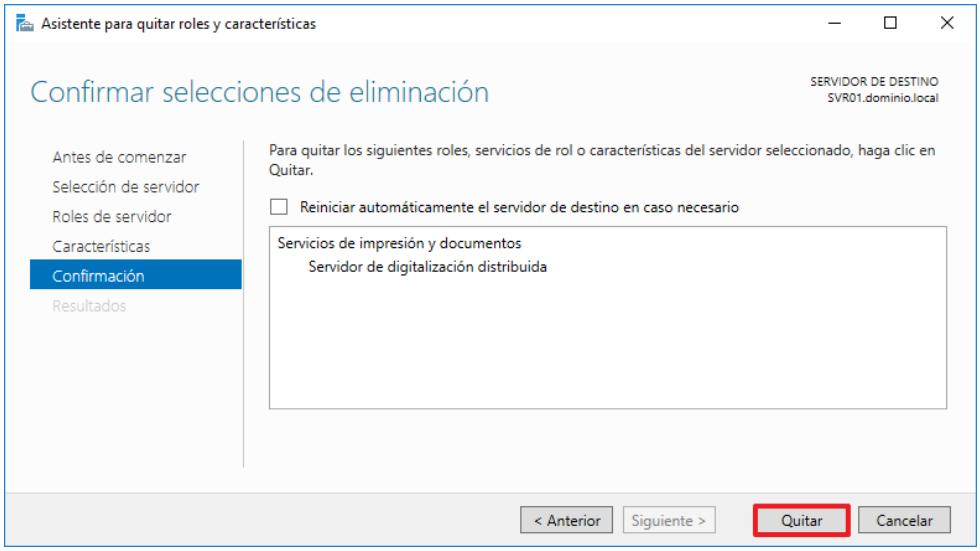
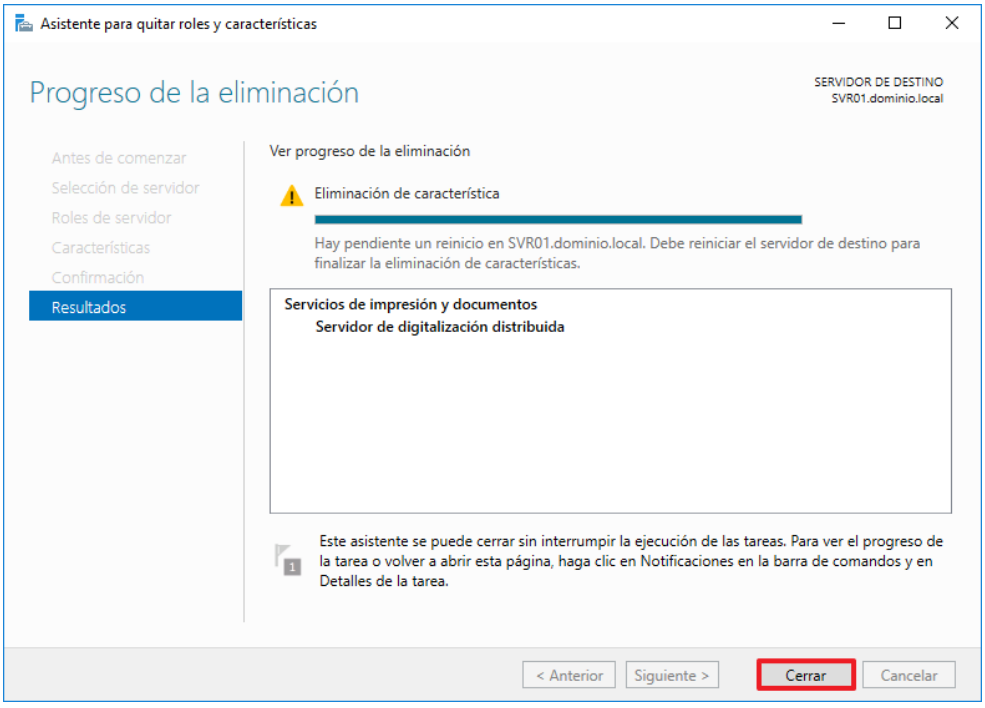
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de impresión.

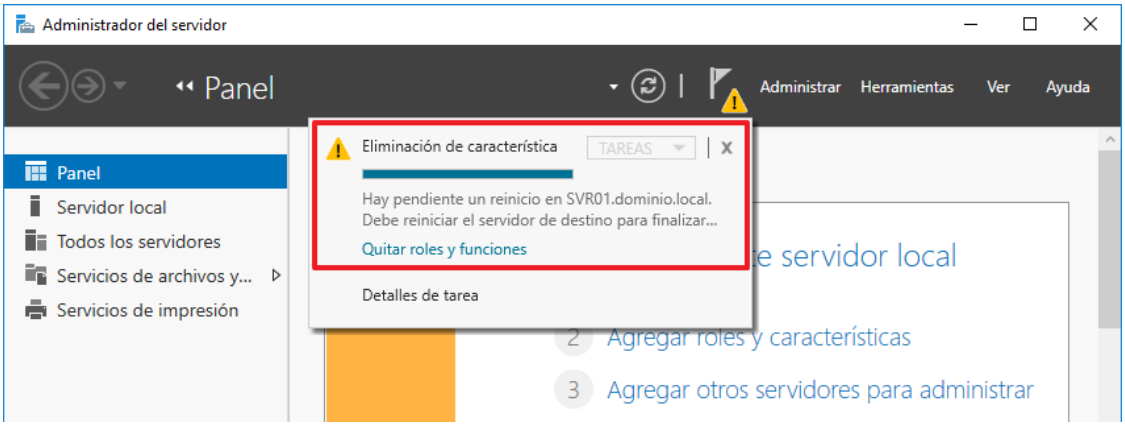
Paso	Descripción
33.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
34.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
35.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
36.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 

Paso	Descripción
37.	Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
38.	Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.

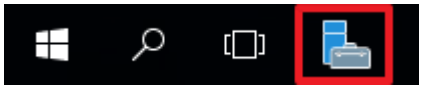
Paso	Descripción
39.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Servidor de digitalización distribuida”.
40.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 

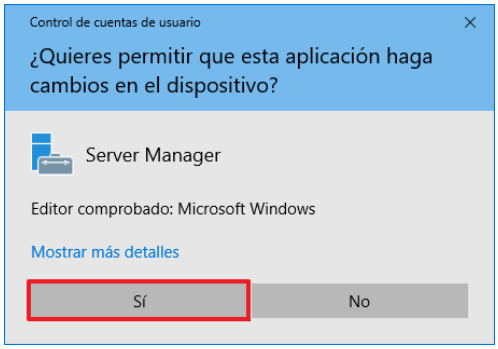
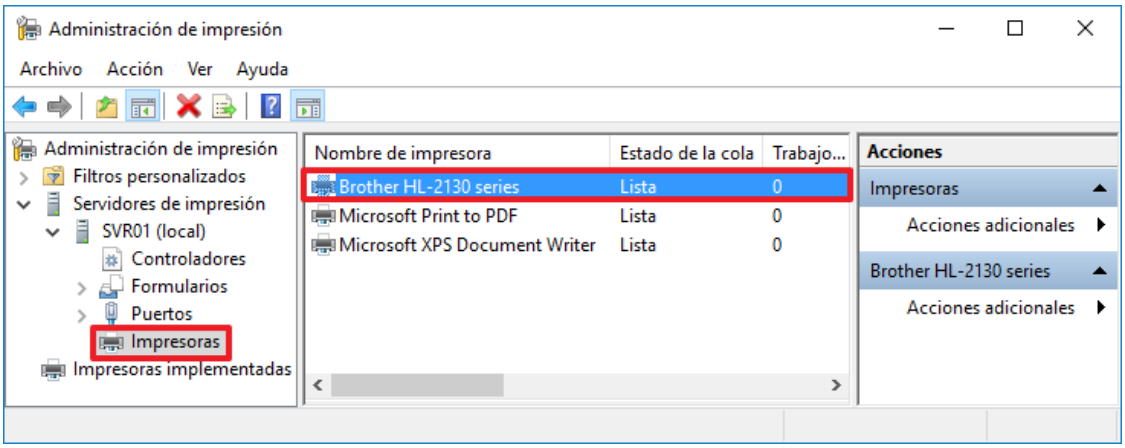
Paso	Descripción
41.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
42.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación. 

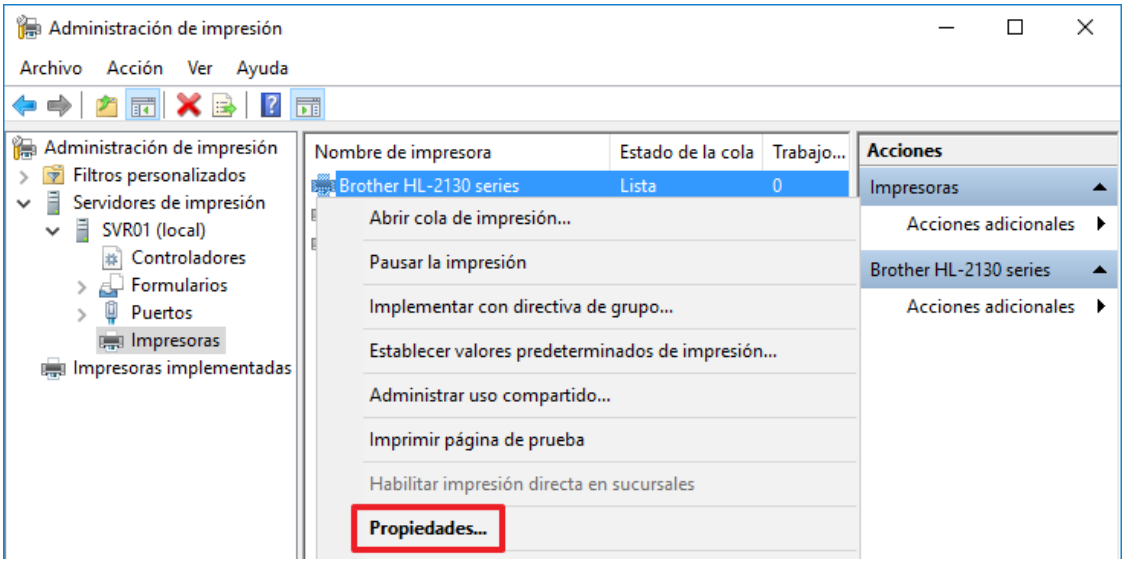
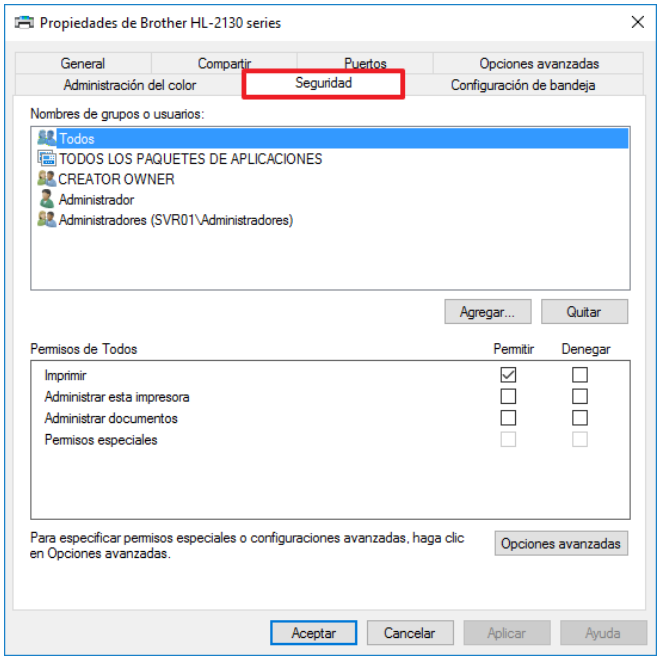
Paso	Descripción
43.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración. El "Administrador del servidor" mostrará una advertencia acerca de la necesidad de dicho reinicio. 

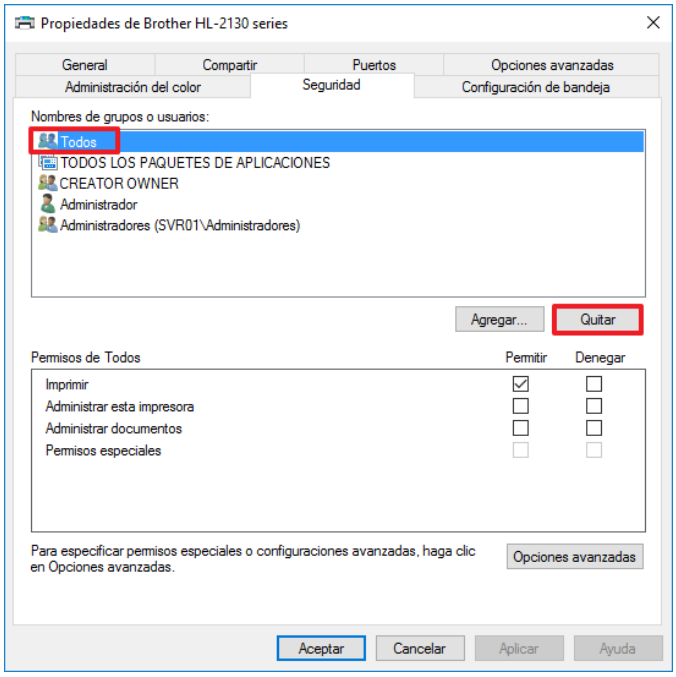
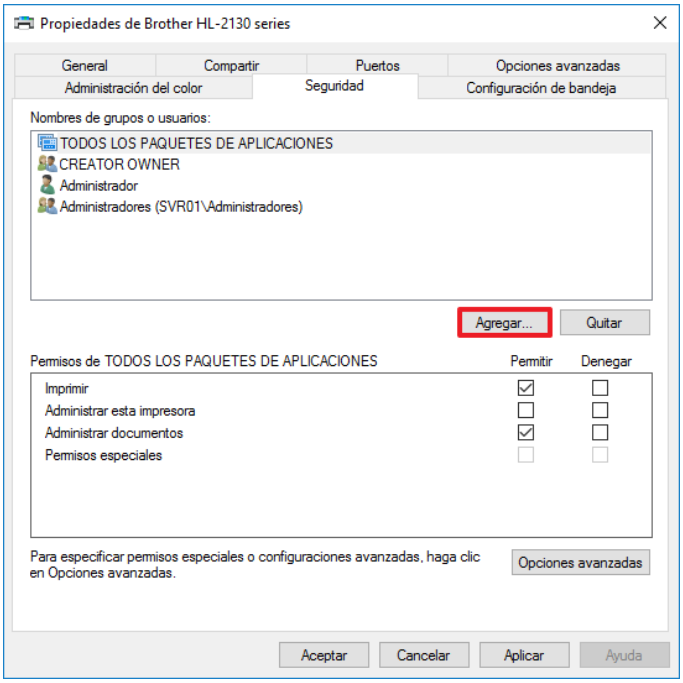
2.2. GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN

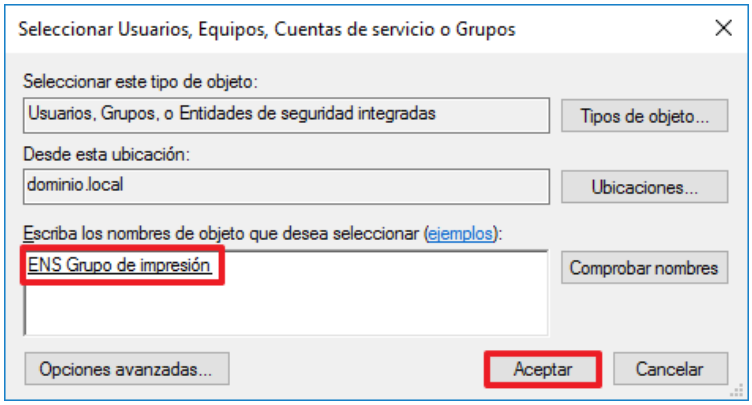
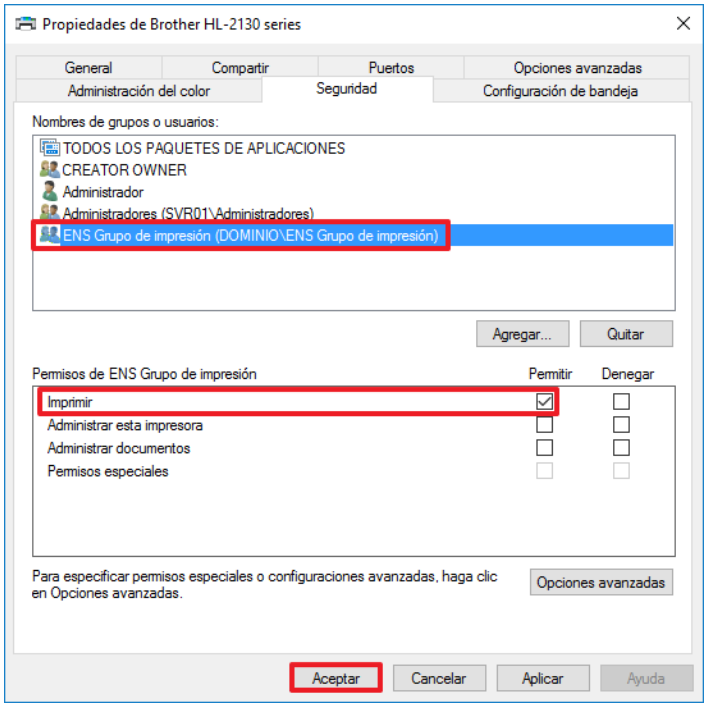
Es recomendable que, en el dispositivo de impresión solo se disponga de permiso de impresión, para el personal estrictamente necesario, además se recomienda hacer una gestión de los permisos de impresión empleando grupos de seguridad.

Paso	Descripción
44.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	A continuación, deberá iniciar la herramienta "Administración de impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
46.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
47.	Inicie la herramienta "Administración de impresión". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administración de impresión"**. 
48.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo **"Servidores de impresión → <<nombre del servidor>> → Impresora"**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión "Brother HL-2130 series", deberá adaptar los pasos a las necesidades su organización.

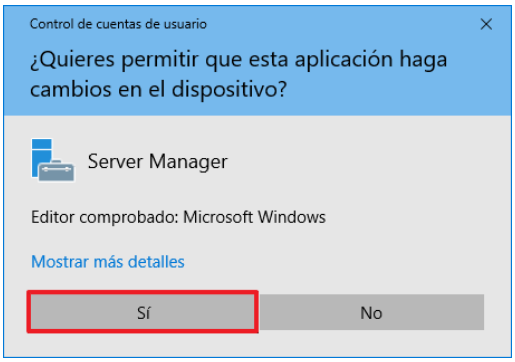
Paso	Descripción
49.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades…”.  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.
50.	A continuación, seleccione la pestaña “Seguridad”. 

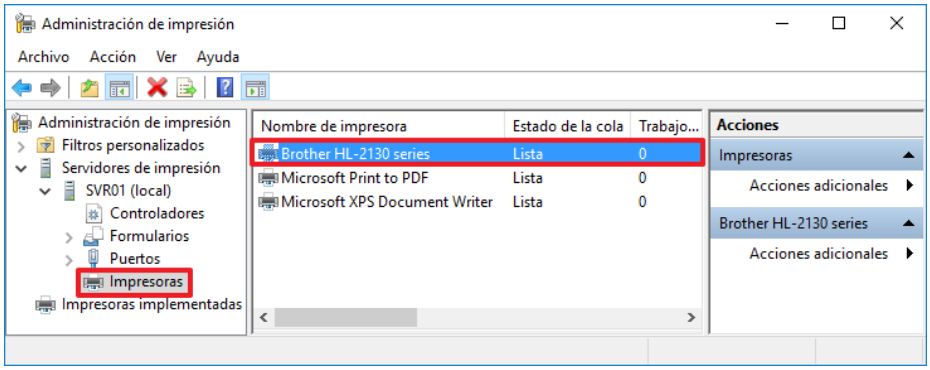
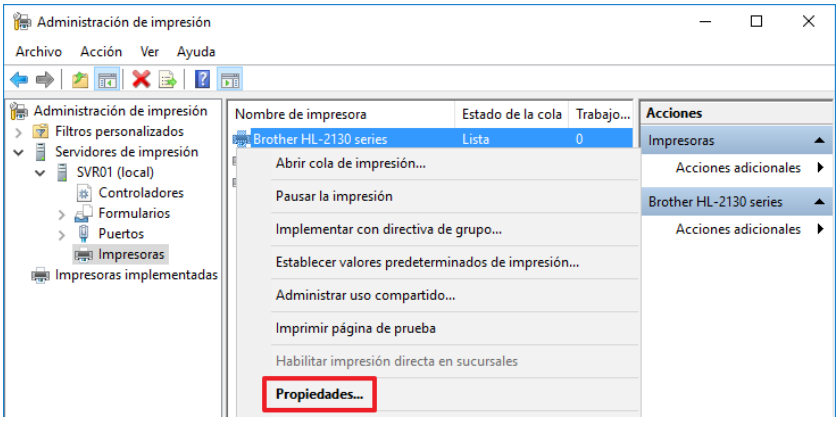
Paso	Descripción
51.	Seleccione el grupo de usuarios “Todos” y a continuación pulse en la opción “Quitar”.  **Nota:** Deberá adaptar este paso a los requisitos de su organización eliminando los usuarios o grupos de usuarios que no requieran de permisos sobre el dispositivo de impresión.
52.	A continuación, pulse sobre el botón “Agregar” para añadir el grupo de usuarios que tendrá permiso para poder imprimir por el dispositivo de impresión seleccionado. 

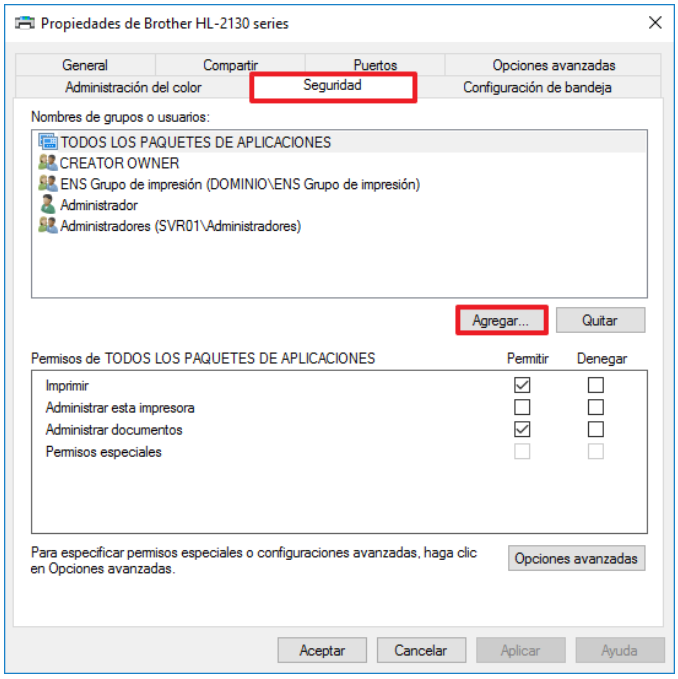
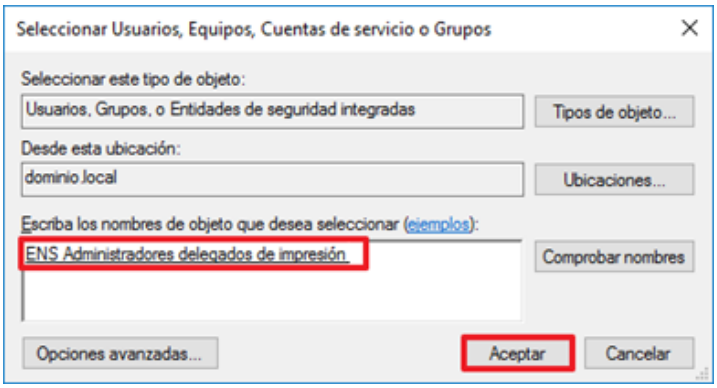
Paso	Descripción
53.	Localice el grupo que quiere añadir para que obtenga permisos para imprimir, y pulse sobre “Aceptar”.  **Nota:** En esta guía se selecciona el grupo de seguridad “ENS Grupo de impresión” al cual pertenecen los usuarios que van a obtener permiso para poder imprimir a través de los dispositivos de impresión seleccionados. Deberá adaptar este paso a los requisitos de su organización.
54.	Una vez añadido el grupo de seguridad, localice el grupo y seleccione en los permisos únicamente la opción de “Imprimir”. Pulse “Aceptar” para cerrar la ventana.  **Nota:** En este ejemplo se utiliza el grupo denominado “ENS Grupo de impresión”.
55.	Deberá repetir estos pasos para asignar permisos de impresión sobre todos los dispositivos de impresión sobre los que esté aplicando seguridad.

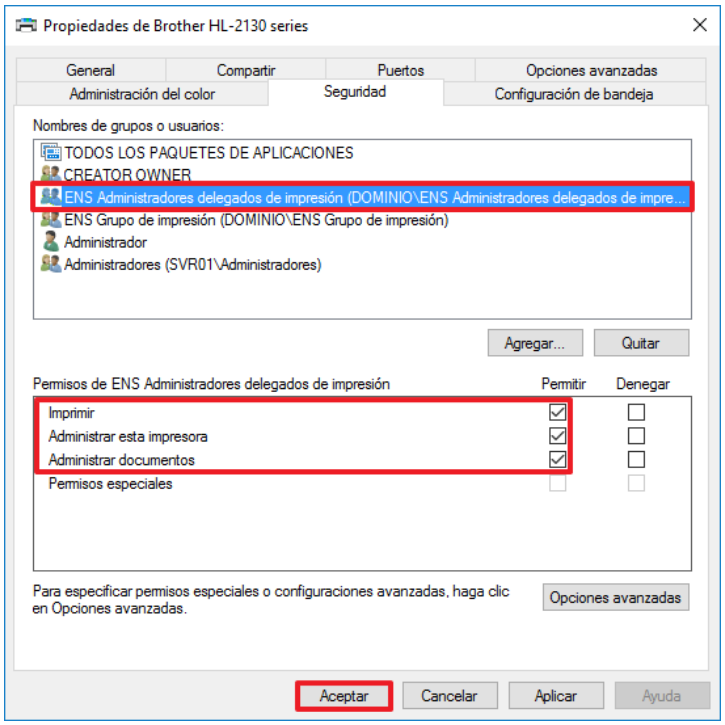
2.3. GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN

En este apartado se tendrá en consideración la gestión de permisos de administración sobre los dispositivos de impresión según lo establecido por el ENS, para con ello limitar y controlar el acceso a los dispositivos de impresión.

Paso	Descripción
56.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
57.	A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
58.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
59.	Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de impresión”**. 
60.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. Para ello despliegue el nodo **“Servidores de impresión → <<nombre del servidor>> → Impresora”**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.
61.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades…”.  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.

Paso	Descripción
62.	A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Agregar…”. 
63.	Localice el grupo que quiere añadir para que obtenga permisos para poder administrar el dispositivo de impresión seleccionado, y pulse sobre el “Aceptar”.  **Nota:** En esta guía se selecciona el grupo de seguridad “ENS Administradores delegados de impresión” al cual pertenecen los usuarios que van a obtener permisos administrativos sobre los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.

Paso	Descripción
64.	Una vez añadido el grupo de seguridad “Administradores delegados de impresión”, localice el grupo y seleccione los siguientes permisos. – Imprimir. – Administrar esta impresora. – Administrar documentos. Una vez establecidos los permisos, pulse “Aceptar” para confirmar los cambios y cerrar la ventana de propiedades del dispositivo de impresión. 

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN PARA LA CATEGORÍA BÁSICA

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de impresión sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación, primero se deberá iniciar sesión en un Controlador de Dominio con una cuenta de usuario que tenga privilegios de administración en el dominio. A continuación, se realizarán las comprobaciones comunes a todos los servidores de impresión que son miembros del dominio.

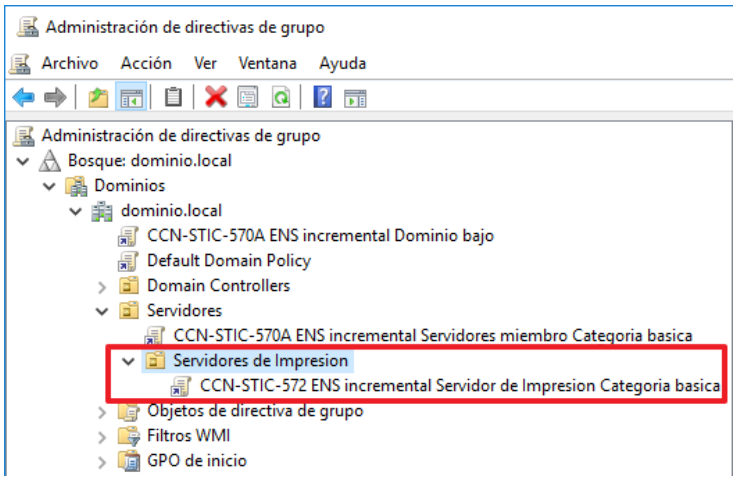
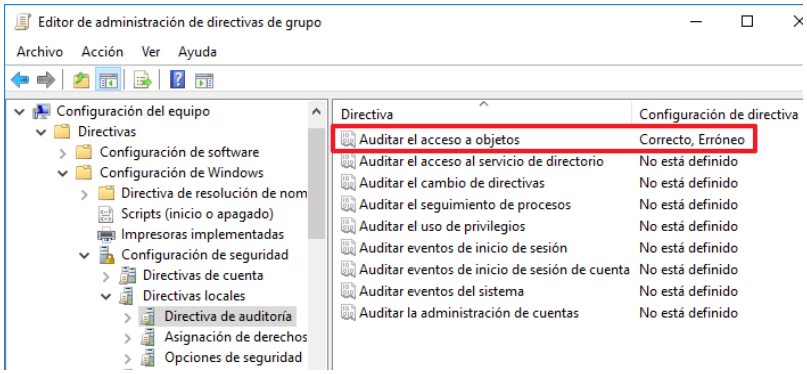
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de impresión, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios de administrador del dominio o administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

a) En el Controlador de Dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

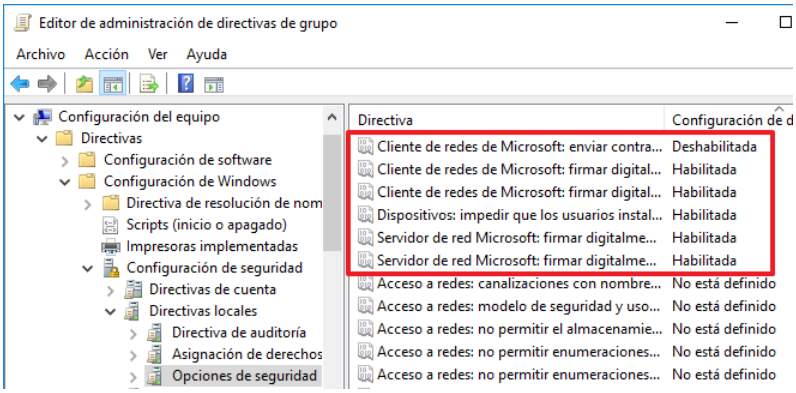
b) En el servidor de impresión:
   i. Administrador de Windows (explorer.exe).
   ii. PowerShell (powershell.exe).
   iii. Servicios (services.msc).
   iv. Editor de objetos de directiva de grupo (gpedit.msc).
   v. Administrador de impresión (printmanagement.msc).

Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado durante la presente guía. Deberá adaptar los pasos según la configuración de su organización.

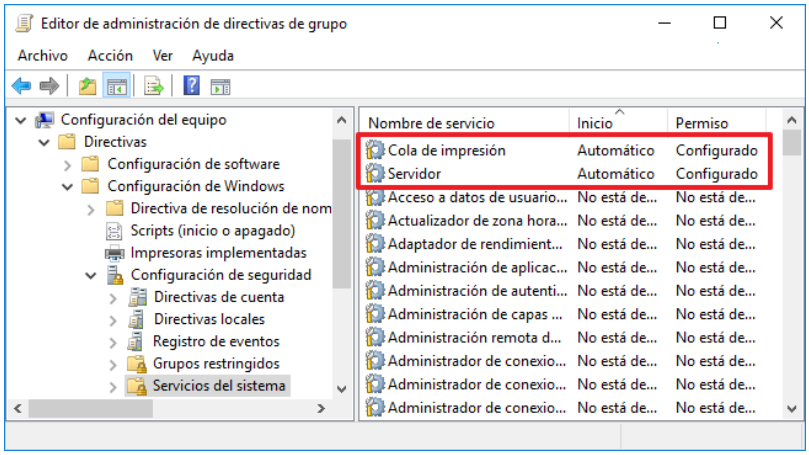
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que está creada la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica”.</td><td></td><td>Utilice el Administrador de directivas de grupo (“Inicio → Herramientas administrativas → Administración de directivas de grupo”) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de impresión” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica”.
 
</td></tr>
<tr><td>3. Verifique los valores de auditoría de la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica”.</td><td></td><td>Utilizando el editor de directiva de grupo, haga clic derecho sobre la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica” y seleccione la opción “Editar…”. Verifique que la directiva tiene los siguientes valores en las directivas de auditoría dentro de:
“Directiva CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”.
 

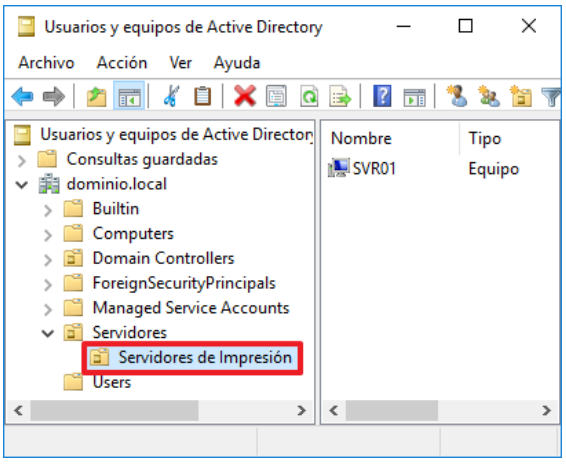
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
</table></td></tr>
</table>

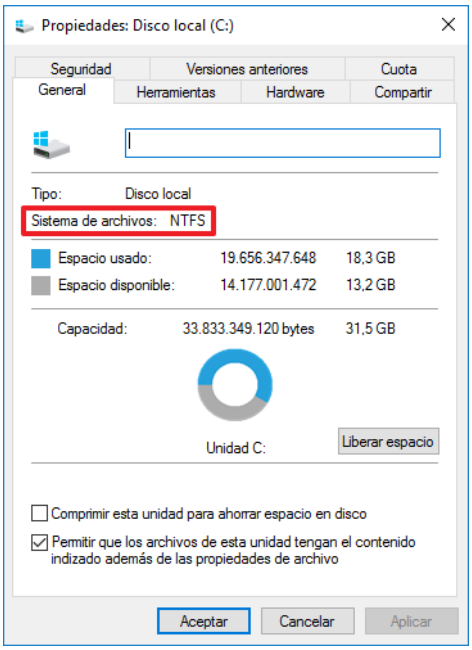
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>4. Verifique las opciones de seguridad de la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica”.</td><td></td><td>Utilizando el editor de directiva de grupo, verifique que la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica ” tiene los siguientes valores en las opciones de seguridad dentro de:
“Directiva CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cliente de redes Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Cliente de redes Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Cliente de redes Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
<tr><td>Dispositivos: Impedir que los usuarios instalen controladores de impresora</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red de Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

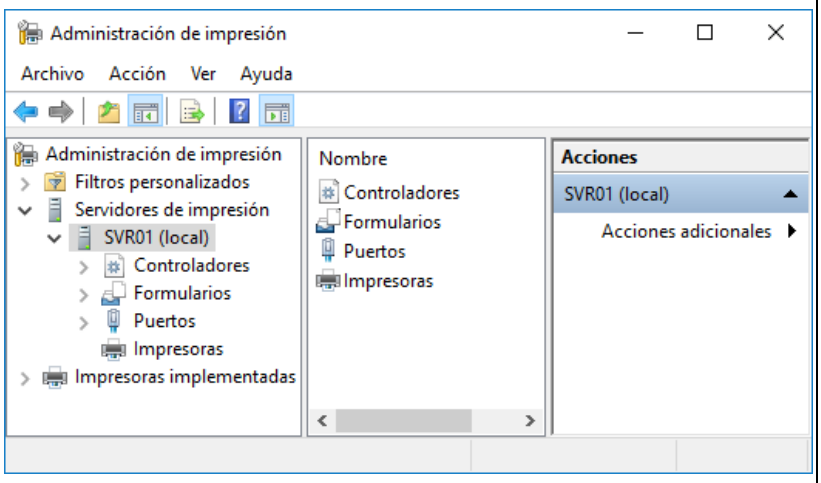
Servicio (Nombre largo)	Servicio (Nombre corto)	Inicio	Permisos	OK/NOK
Cola de impresión	Spooler	Automático		
Servidor	LanmanServer	Automático		

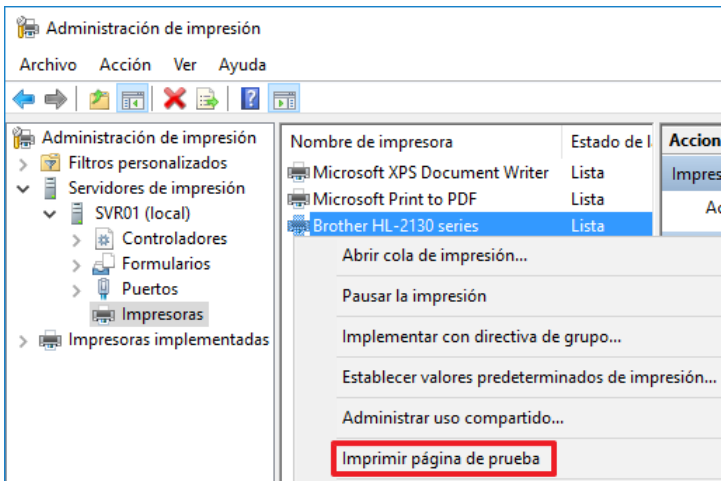
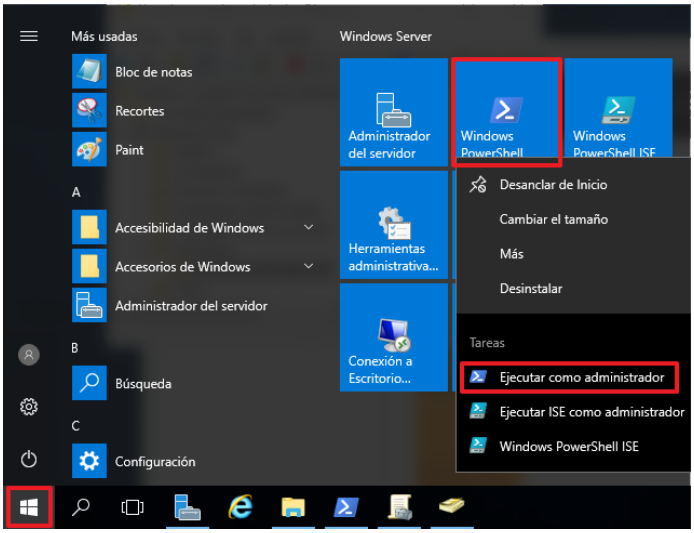
6. Verifique que el servidor de impresión está dentro de la unidad organizativa "Servidores de impresión".		Utilice la herramienta Usuarios y equipos de Active Directory (**"Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory"**) y seleccione la unidad organizativa "Servidores de impresión". Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de impresión que se están asegurando. 

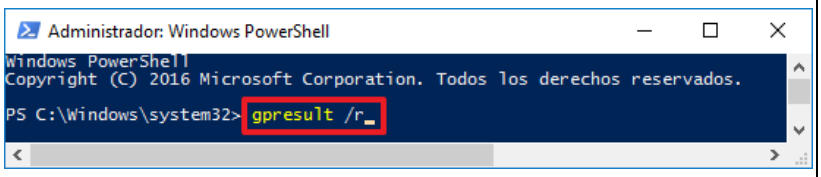
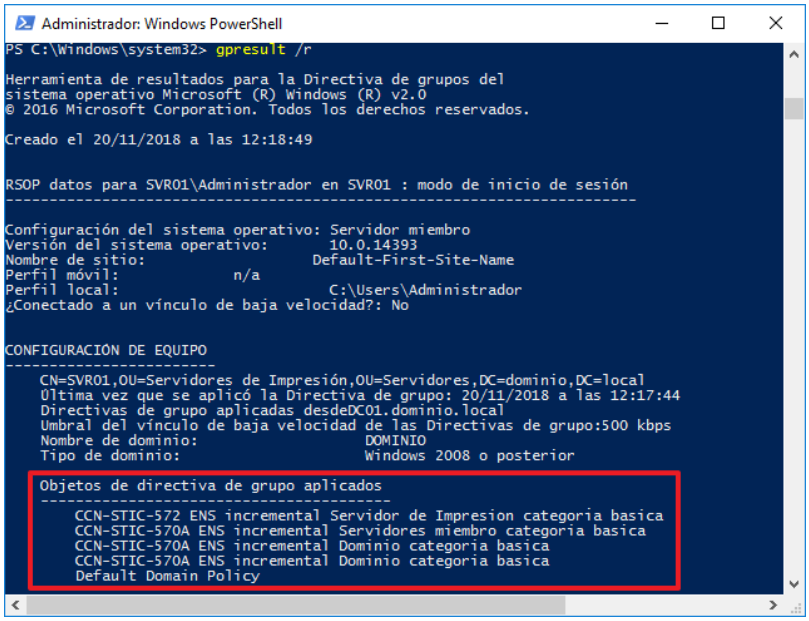
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Inicie sesión en el servidor de impresión.</td><td></td><td>Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.</td></tr>
<tr><td>8. Verifique que todos los volúmenes están formateados con NTFS.</td><td></td><td>Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL’s.
 
</td></tr>
<tr><td>9. Verifique que están instalados los componentes que se indican.</td><td></td><td>En el “Administrador del Servidor”, pulse sobre la opción “Servidor Local” del menú de la izquierda y diríjase a la parte final de la ventana principal, “Roles y características”, por medio del scroll lateral derecho.
<table>
<tr><th>Rol</th><th>OK/NOK</th></tr>
<tr><td>Servicios de impresión y documentos</td><td></td></tr>
<tr><td>Servidor de impresión</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique que los servicios del sistema relacionados con el servidor de impresión están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre **Inicio → Ejecutar**) y compruebe el tipo de inicio de los servicios.

Servicio (Nombre largo)	Servicio (Nombre corto)	Inicio	Permisos	OK/NOK
Cola de impresión	Spooler	Automático		
Servidor	LanmanServer	Automático		

11. Verifique que la instalación del servidor de impresión se ha realizado correctamente.		Utilizando la herramienta de administración de impresión (ejecutando **"printmanagement.msc"** desde, botón derecho sobre **Inicio → Ejecutar**), verifique que la consola se inicia y presenta el servidor local como un servidor de impresión.  **Nota:** En esta comprobación, el servidor se denomina "SVR01". En su organización debe comprobar que aparece el nombre del servidor de impresión que está implementando.

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.		Utilizando la herramienta de administración de impresión (ejecutando "printmanagement.msc" desde, botón derecho sobre **Inicio → Ejecutar**), verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión. Para ello, seleccione cada una de las impresoras que aparecen en el nodo "Impresoras" con el botón derecho del ratón y pulse sobre la opción "Imprimir página de prueba". 
13. Inicie la consola de PowerShell.		Ejecute la consola de PowerShell. Para ello pulse "Inicio",.seleccione "Powershell" con el botón derecho y pulse sobre "Ejecutar como administrador". 

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique que se estan aplicando las GPOs correspondientes.		Verifique que se estan aplicando las GPOs correspondientes ejecutando el comando “gpresult /r”. 
15. Verifique que se estan aplicando las GPOs correspondientes.		Verifique que se aplican las siguientes GPOs. – CCN-STIC-572 ENS incremental Servidor de Impresion categoria basica. – CCN-STIC-570A ENS incremental Servidores miembro categoria basica. – CCN-STIC-570A ENS incremental Dominio categoria basica. 

ANEXO A.3. CATEGORÍA MEDIA

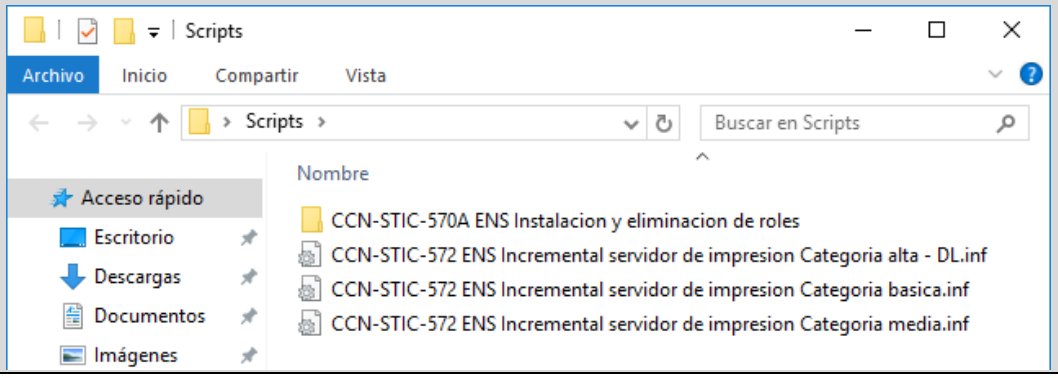
ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de impresión 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.

Nota: Si instala el Servidor de impresión por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016" encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta "Scripts" adjunta a la presente guía.

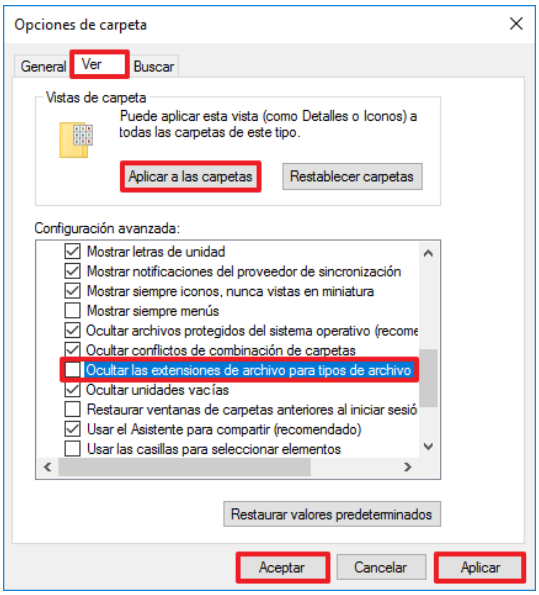
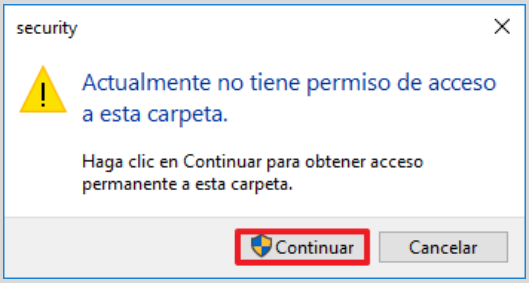


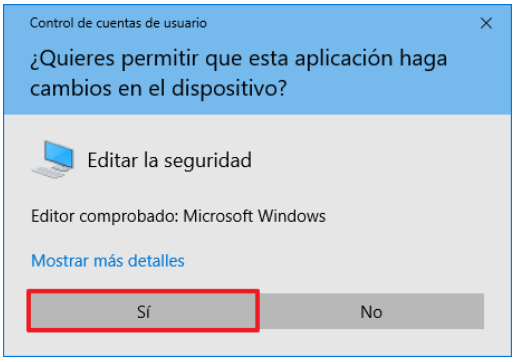
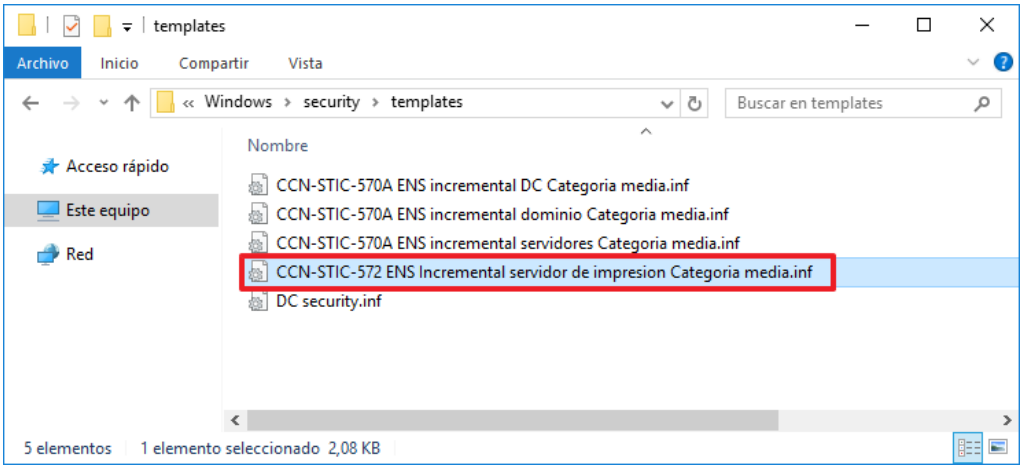
1. PREPARACIÓN DEL DOMINIO

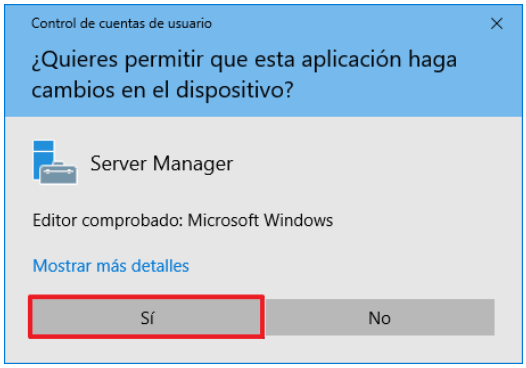
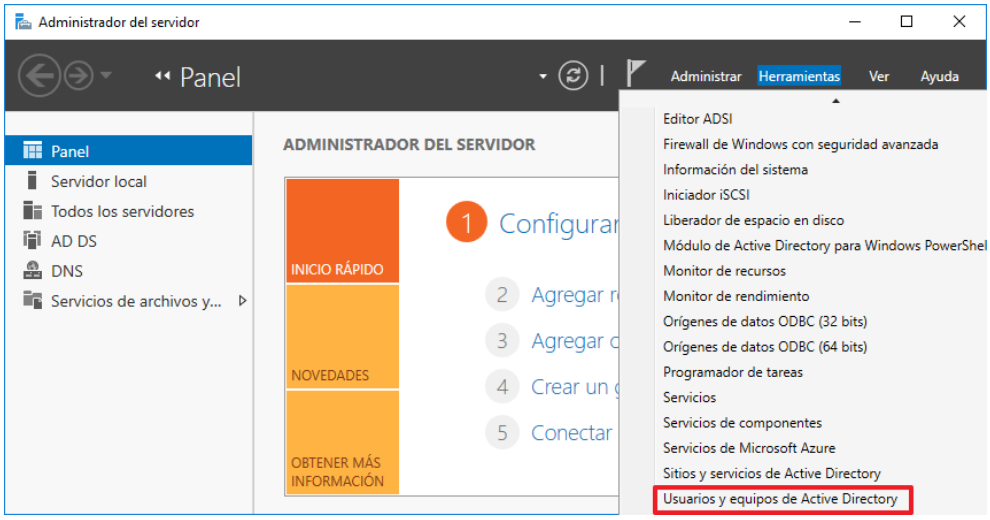
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de impresión miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de impresión y se realizan las configuraciones de políticas de grupo correspondientes.

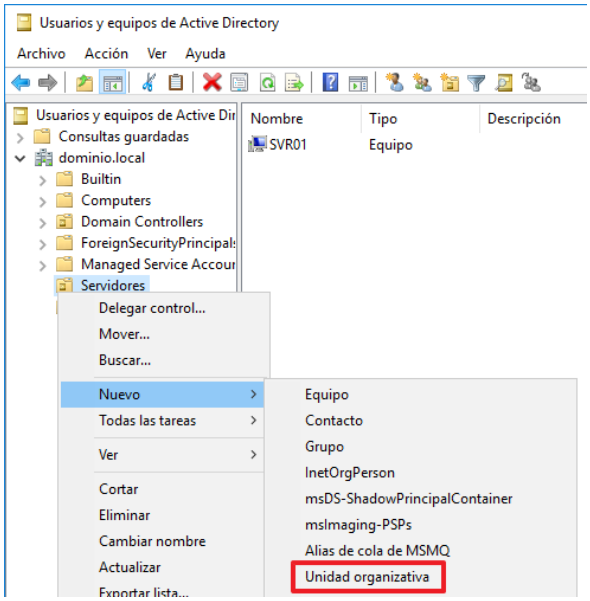
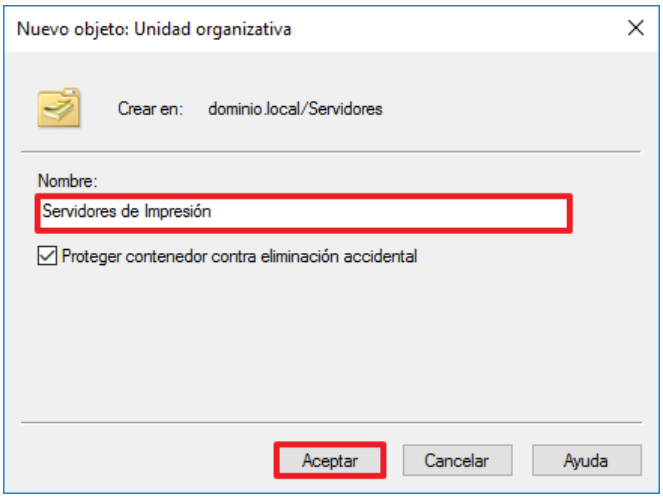
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de impresión que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

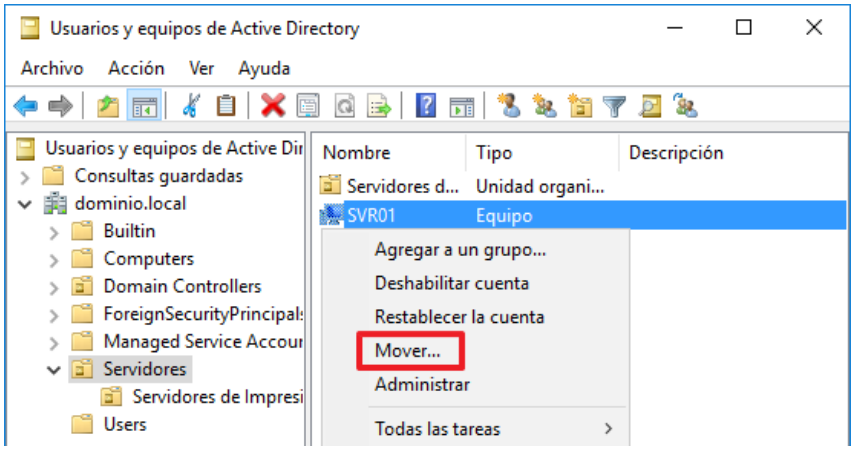
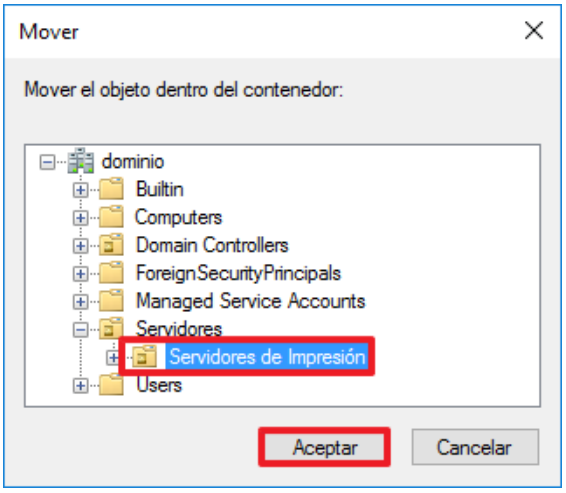
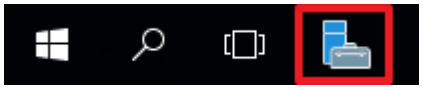
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
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" muestra las extensiones de los archivos.

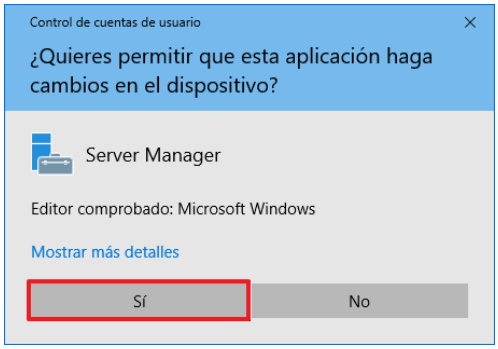
Paso	Descripción
5.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. En la venta emergente, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la imagen.  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 “¿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.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 

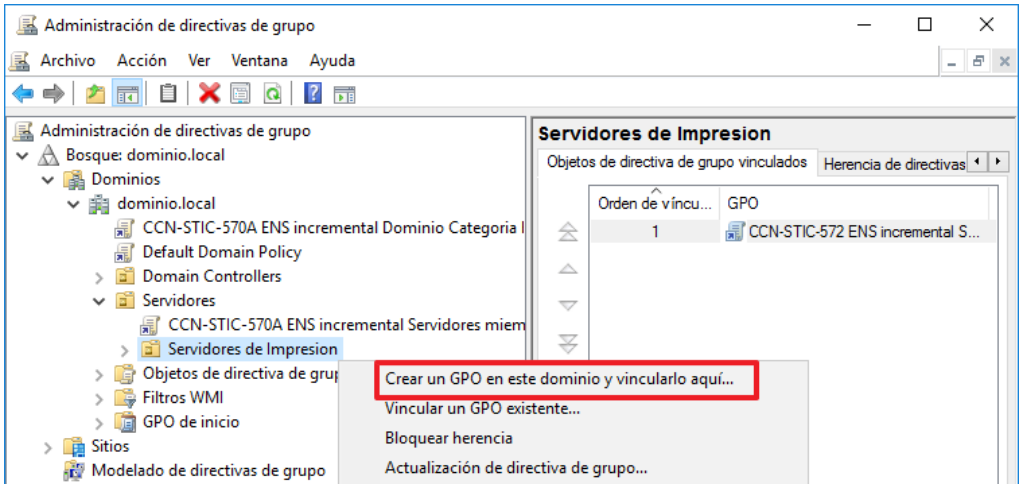
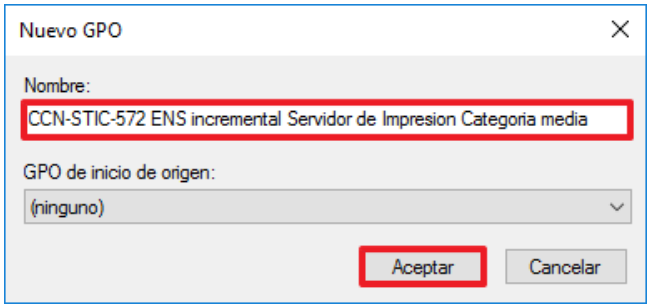
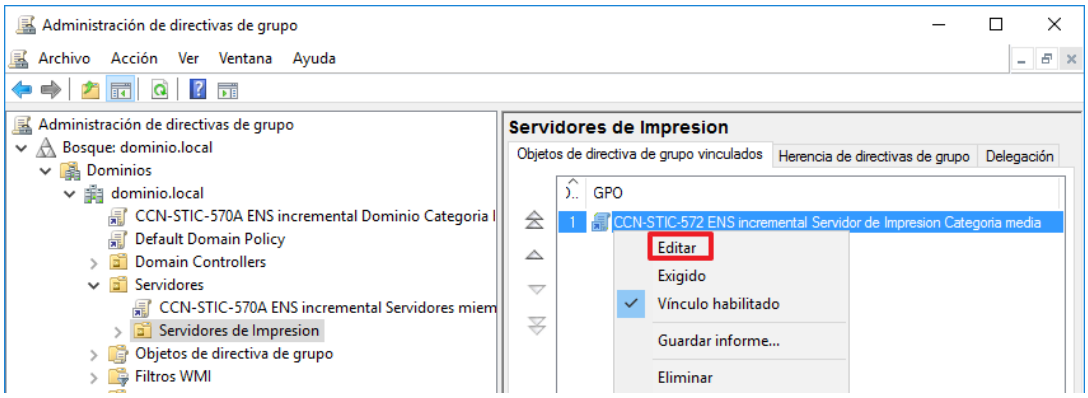
Paso	Descripción
7.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
8.	Copie el fichero “CCN-STIC-572 ENS Incremental servidor de impresion Categoria media.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 
9.	A continuación, deberá crear la unidad organizativa "Servidores de Impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

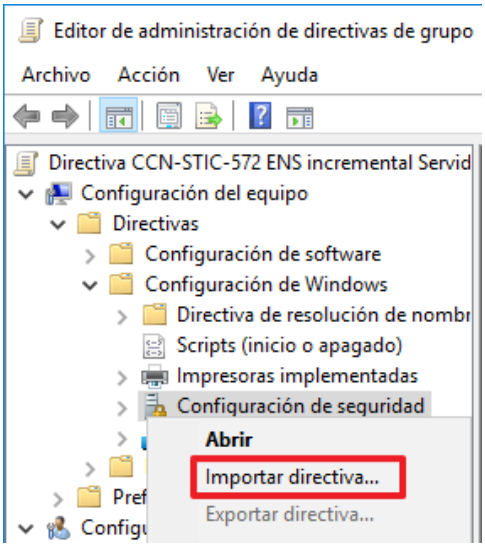
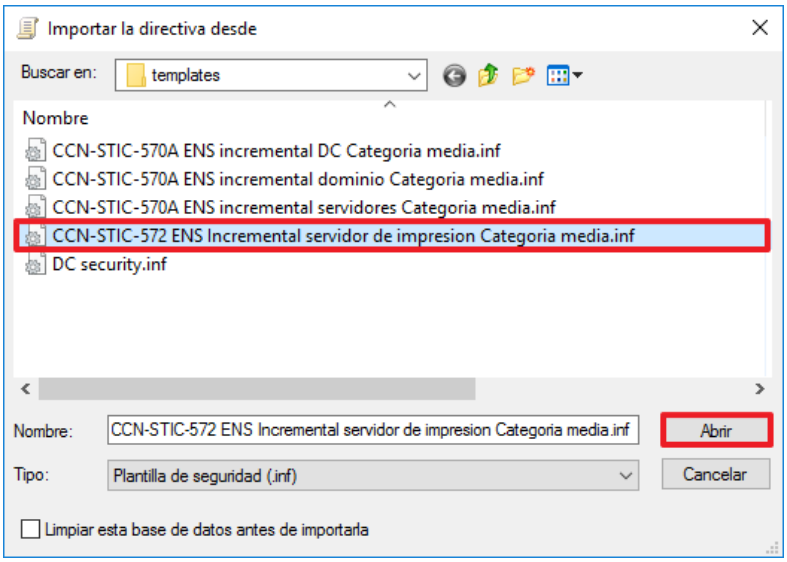
Paso	Descripción
10.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
11.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”**. 

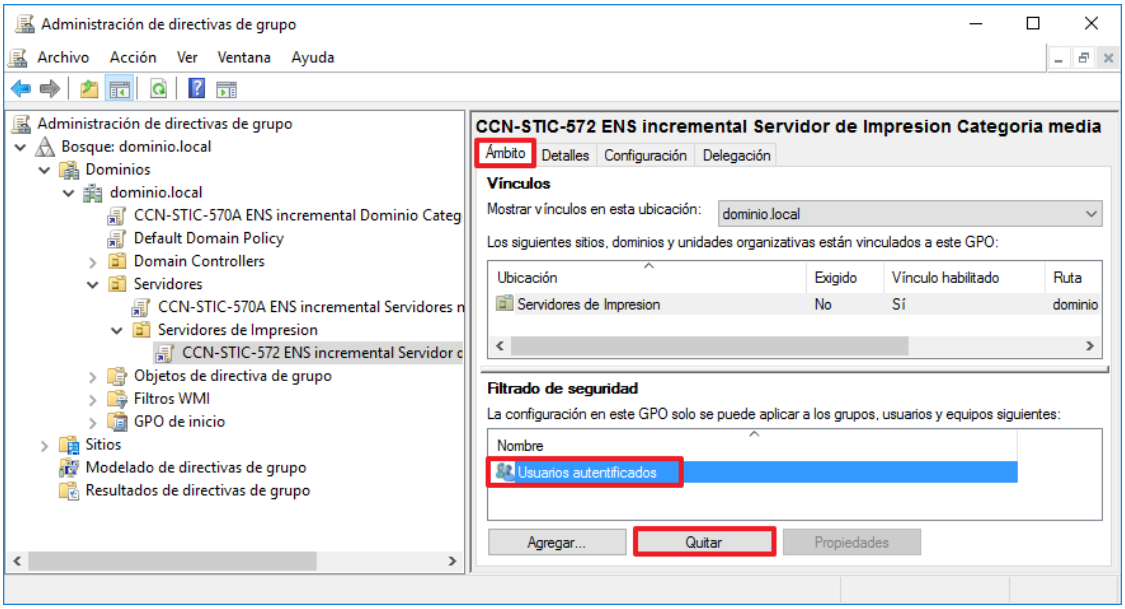
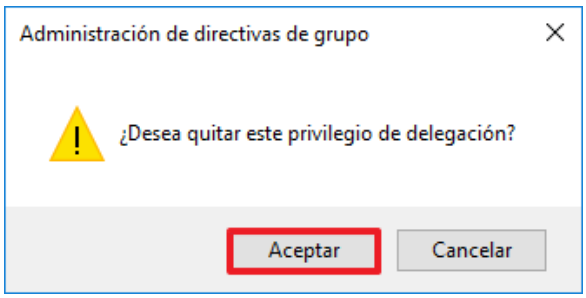
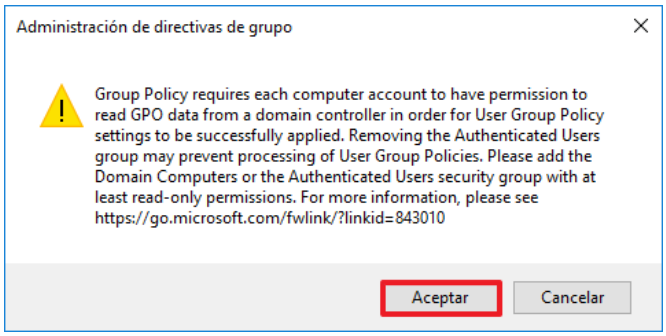
Paso	Descripción
12.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> → <<unidad organizativa>>"**, y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nuevo → Unidad organizativa"**.  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en **"dominio.local → Servidores"**.
13.	Introduzca el nombre "Servidores de impresión" tal y como se muestra en la imagen y pulse sobre "Aceptar". 

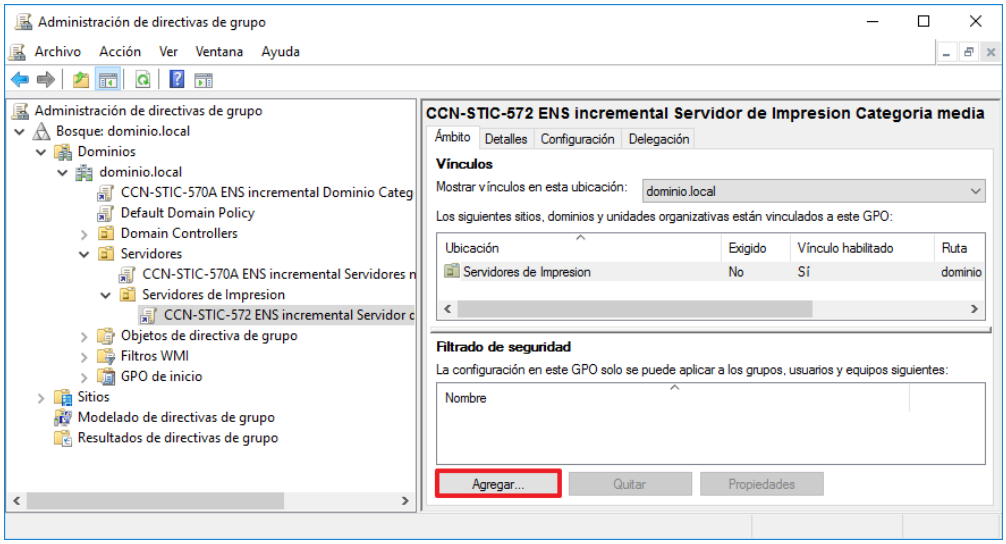
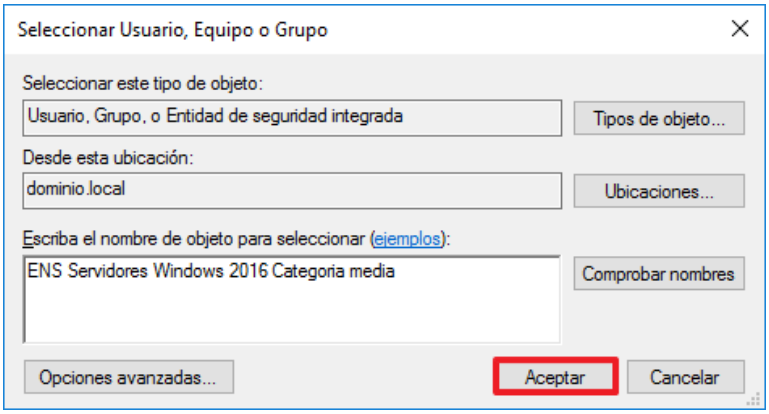
Paso	Descripción
14.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de impresión a la unidad organizativa “Servidores de impresión”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”. 
15.	A continuación, seleccione la unidad organizativa “Servidores de impresión” y pulse “Aceptar”. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	A continuación, deberá crear la GPO "CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
18.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
19.	Inicie la herramienta "Administración de Directivas de Grupo". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administración de directivas de grupo"**. 
20.	A continuación, despliegue el nodo **"Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de impresión"**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es "Servidores de impresión".

Paso	Descripción
21.	Pulse con el botón derecho sobre la unidad organizativa “Servidores de impresión” y seleccione “Crear un GPO en este dominio y vincularlo aquí…”. 
22.	Escriba el nombre de la GPO “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media” y haga clic en el botón “Aceptar”. 
23.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
24.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.

Paso	Descripción
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva…”. 
26.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-572 ENS Incremental servidor de impresion Categoria media.inf” y pulse el botón “Abrir”. 
27.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

Paso	Descripción
28.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”. 
30.	Pulse de nuevo “Aceptar” ante el mensaje de advertencia emergente. 

Paso	Descripción
31.	A continuación, pulse el botón “Agregar…”. 
32.	Introduzca como nombre “ENS Servidores Windows 2016 Categoria media”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a las necesidades de su organización.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración.

Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría media. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

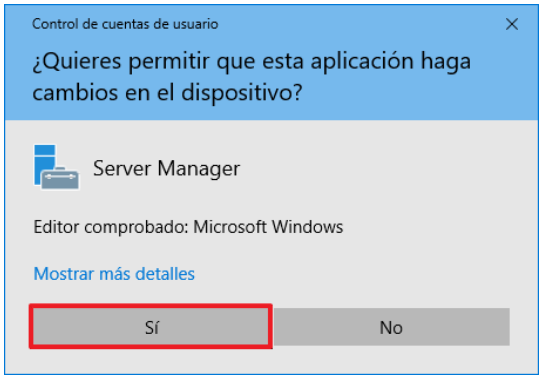
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

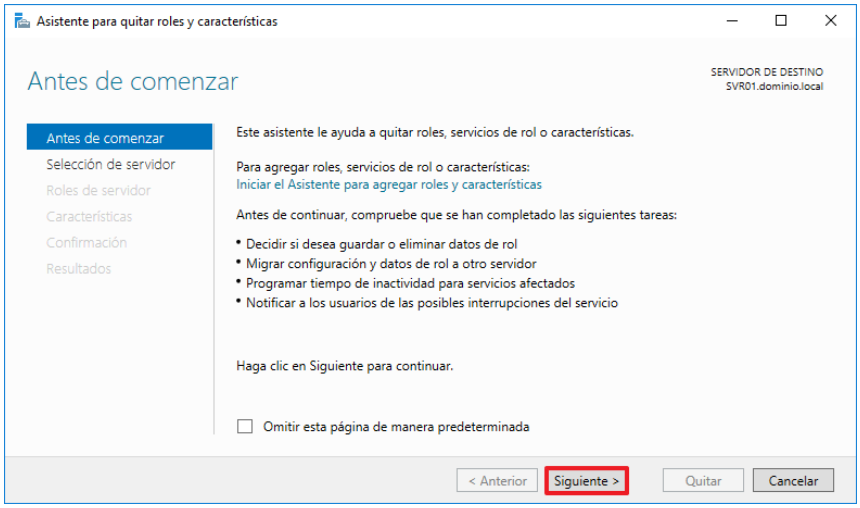
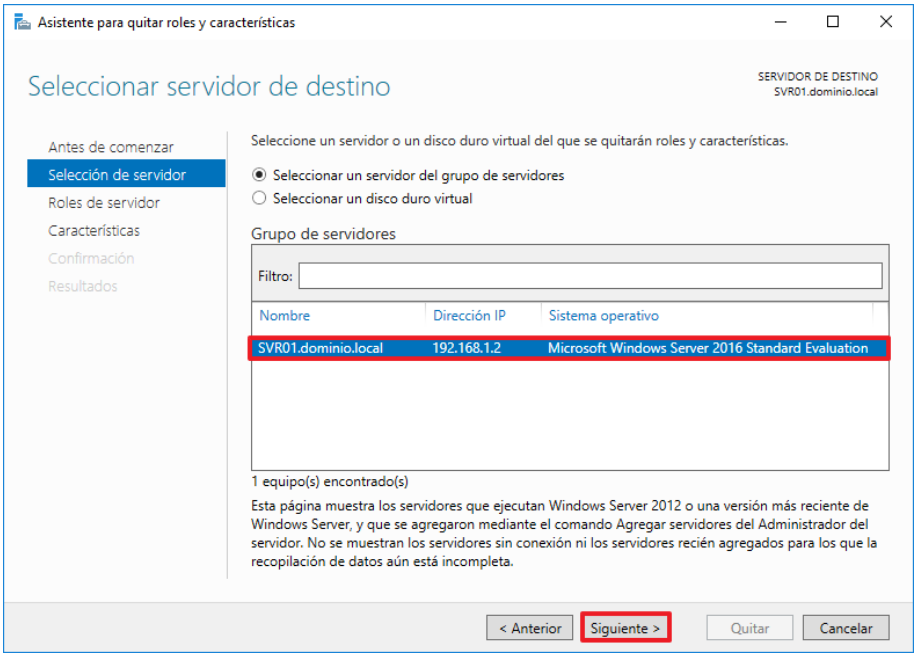
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

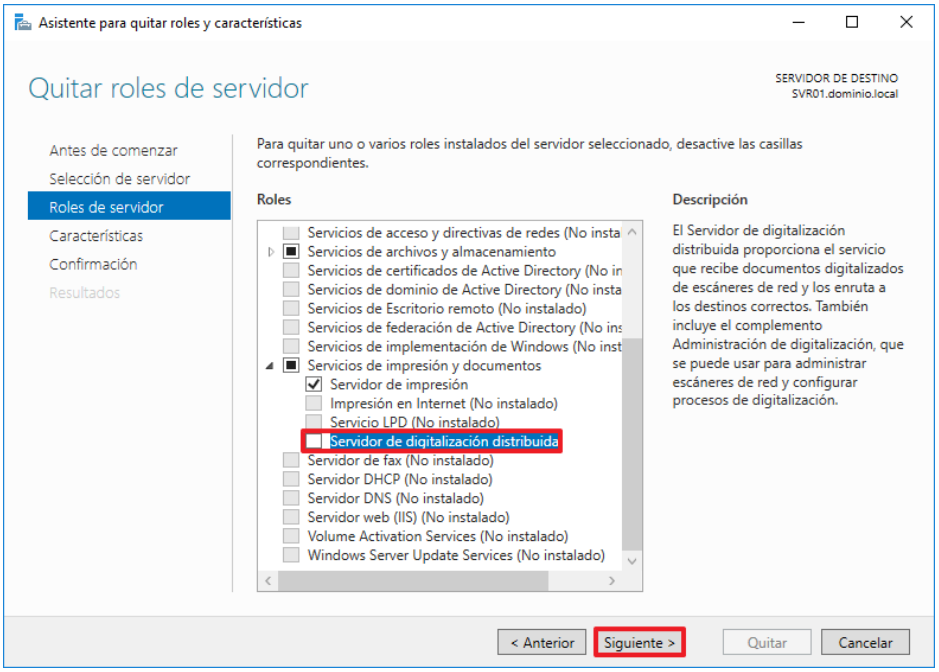
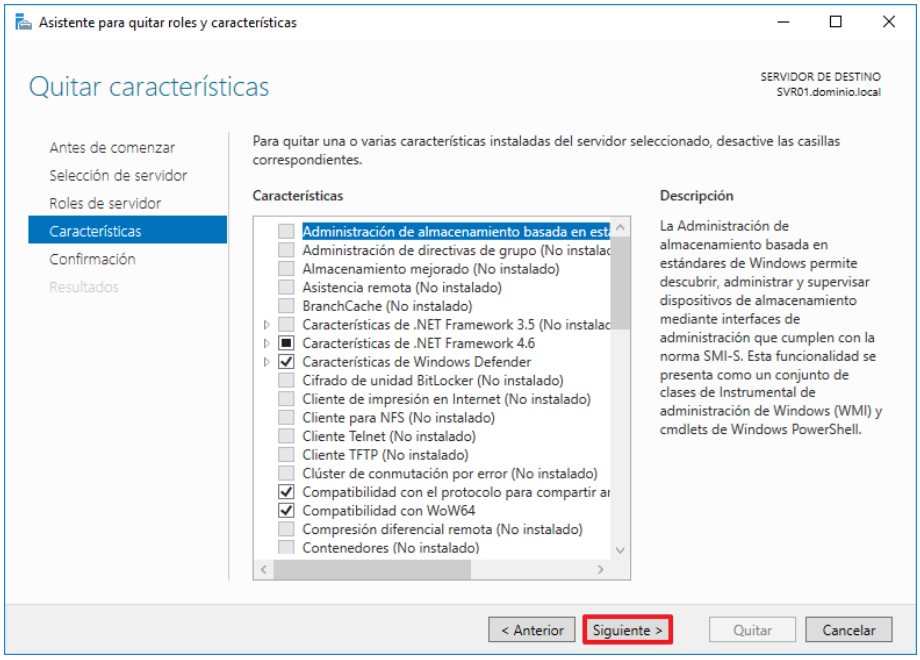
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

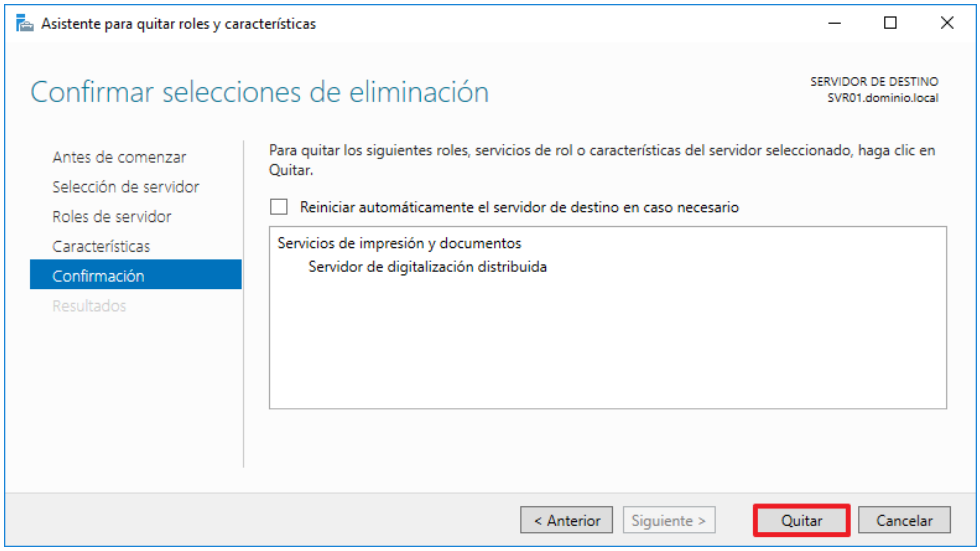
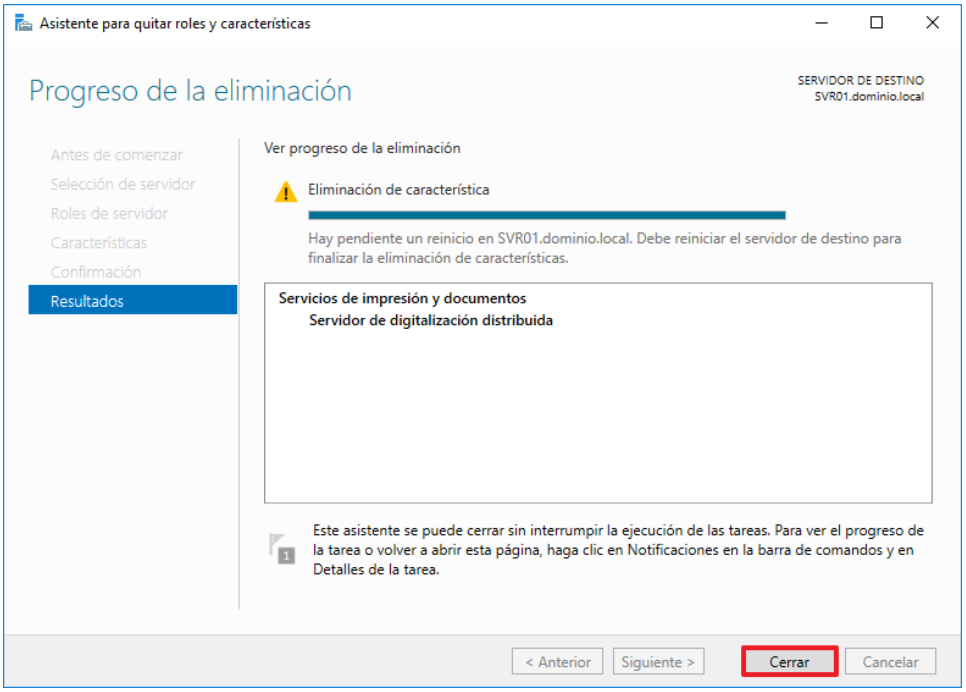
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de impresión.

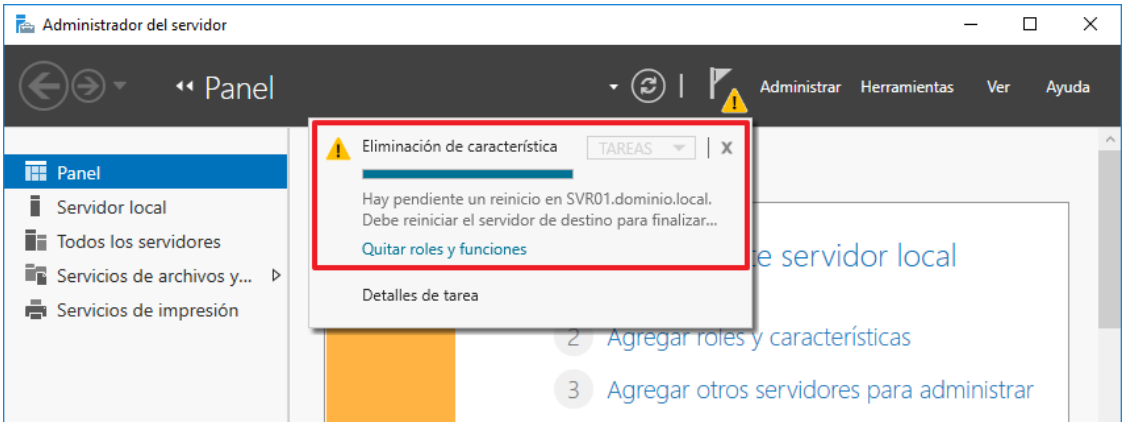
Paso	Descripción
33.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
34.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
35.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
36.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 

Paso	Descripción
37.	Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
38.	Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.

Paso	Descripción
39.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Servidor de digitalización distribuida”.
40.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 

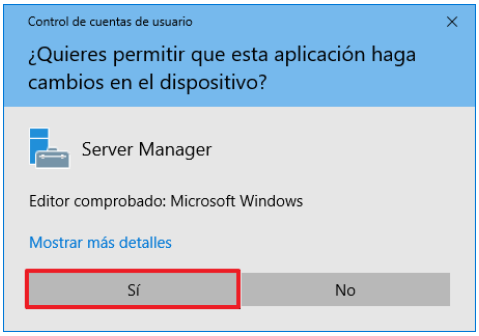
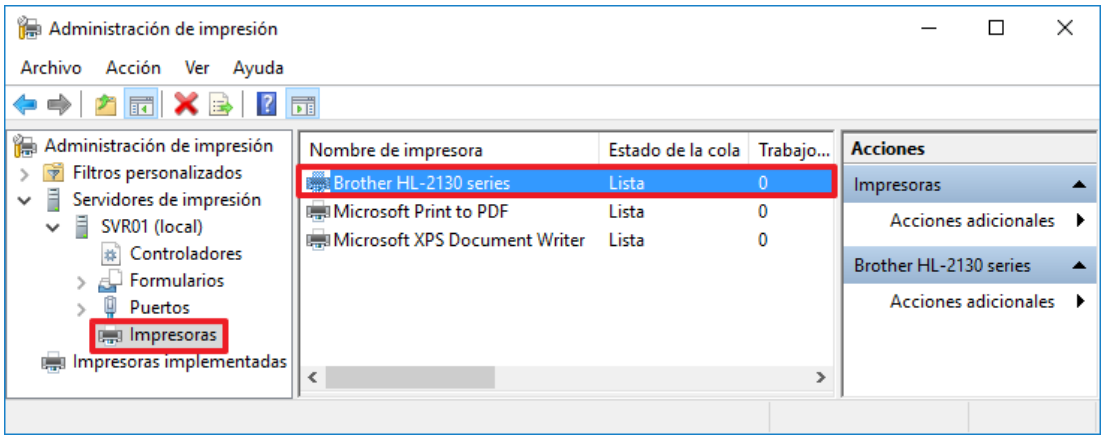
Paso	Descripción
41.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
42.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación. 

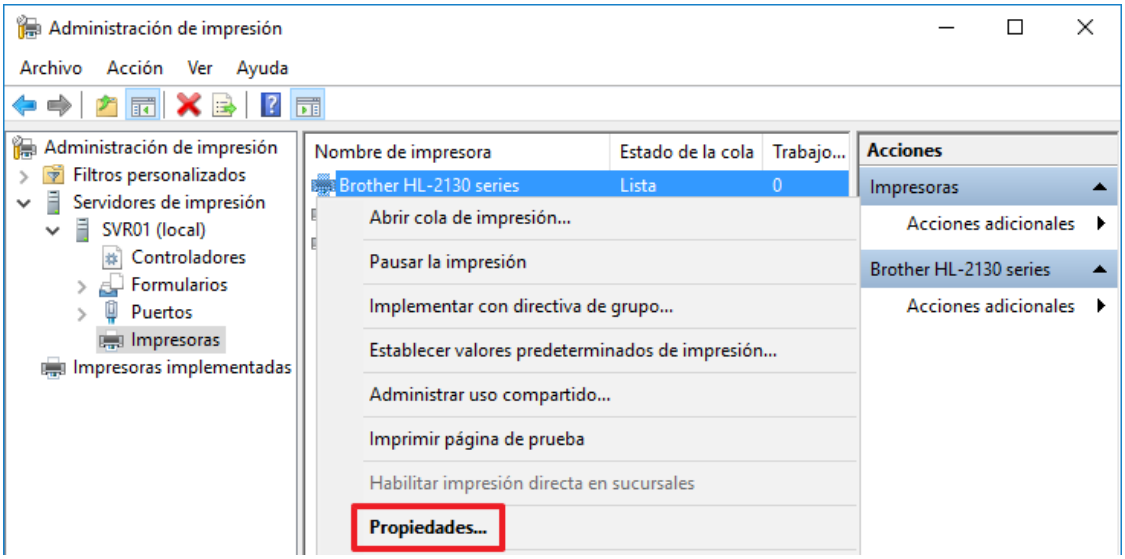
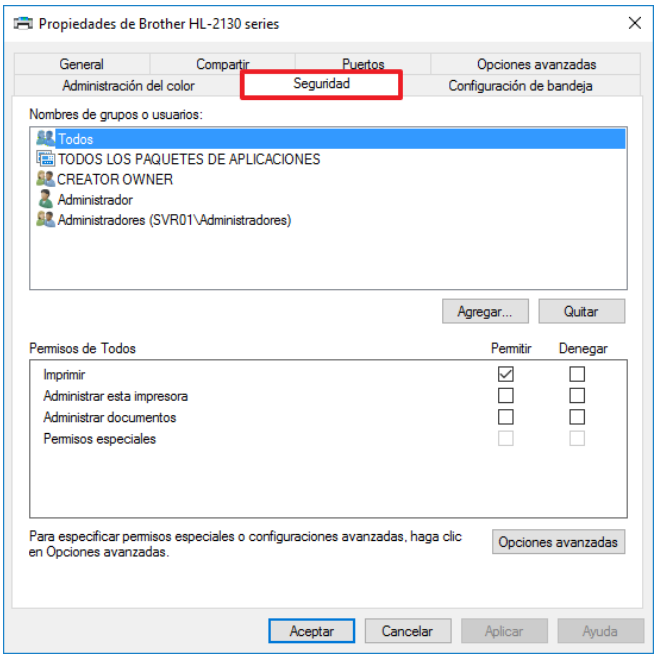
Paso	Descripción
43.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración. El "Administrador del servidor" mostrará una advertencia acerca de la necesidad de dicho reinicio. 

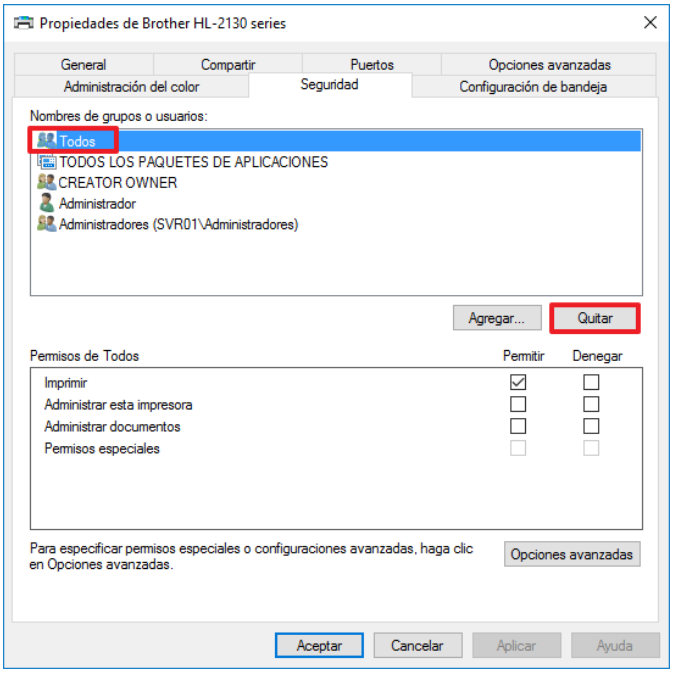
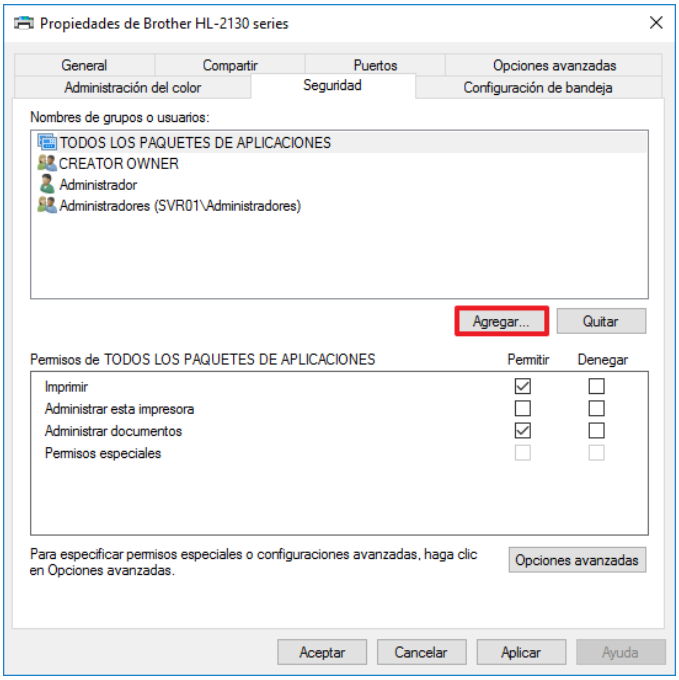
2.2. GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN

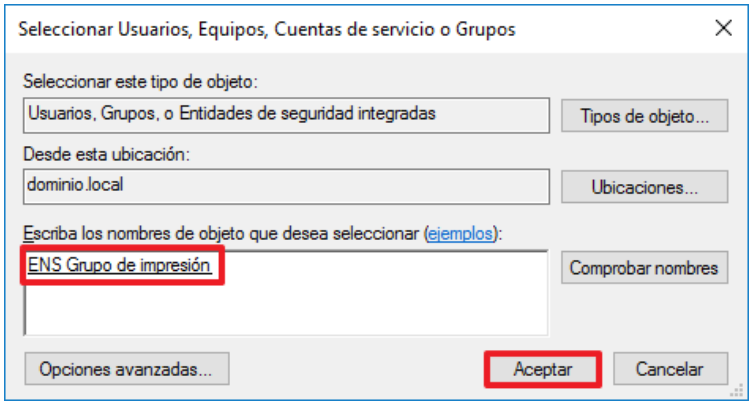
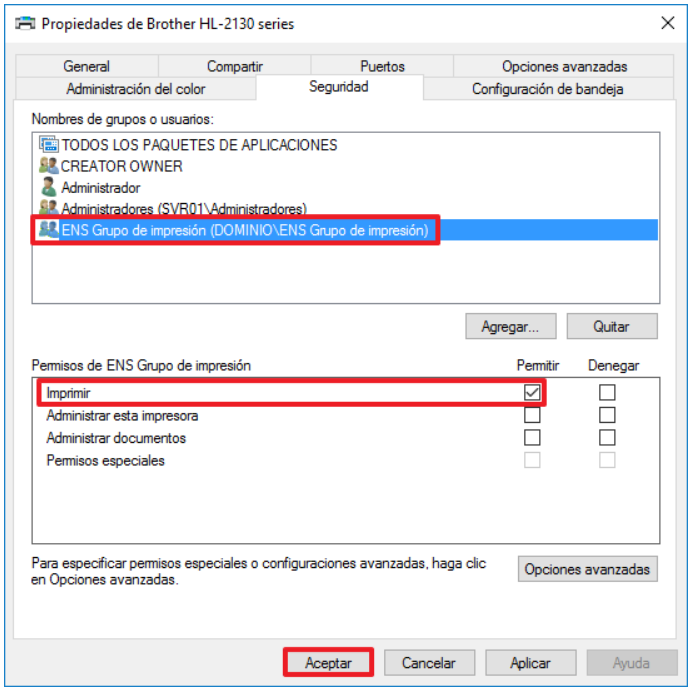
Es recomendable que, en el dispositivo de impresión solo se disponga de permiso de impresión, para el personal estrictamente necesario, además se recomienda hacer una gestión de los permisos de impresión empleando grupos de seguridad.

Paso	Descripción
44.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	A continuación, deberá iniciar la herramienta "Administración de impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
46.	El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. 
47.	Inicie la herramienta "Administración de impresión". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione **"Herramientas → Administración de impresión"**. 
48.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo **"Servidores de impresión → <<nombre del servidor>> → Impresora"**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión "Brother HL-2130 series", deberá adaptar los pasos a las necesidades su organización.

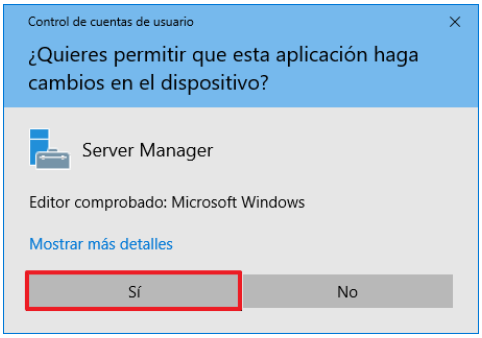
Paso	Descripción
49.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades…”.  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.
50.	A continuación, seleccione la pestaña “Seguridad”. 

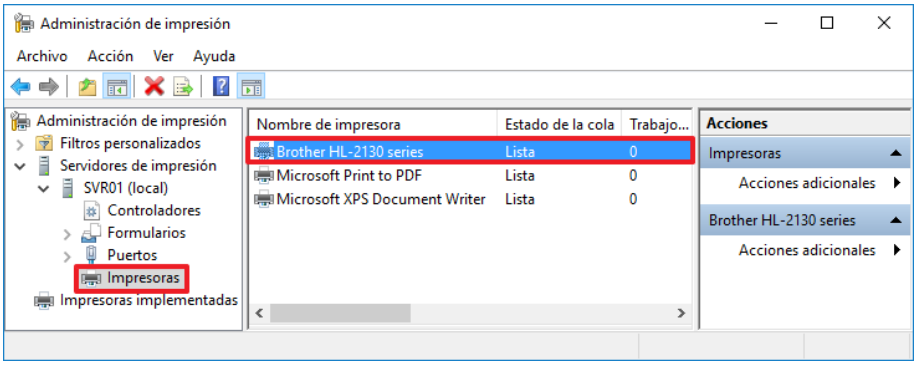
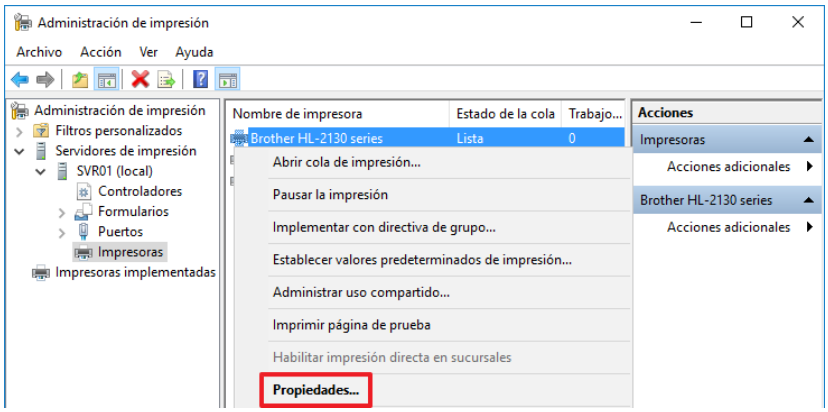
Paso	Descripción
51.	Seleccione el grupo de usuarios “Todos” y a continuación pulse en la opción “Quitar”.  **Nota:** Deberá adaptar este paso a los requisitos de su organización eliminando los usuarios o grupos de usuarios que no requieran de permisos sobre el dispositivo de impresión.
52.	A continuación, pulse sobre el botón “Agregar” para añadir el grupo de usuarios que tendrá permiso para poder imprimir por el dispositivo de impresión seleccionado. 

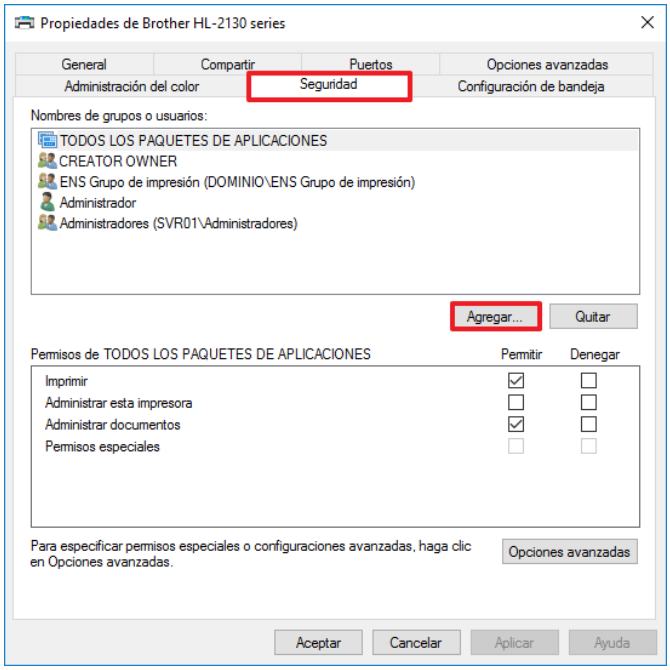
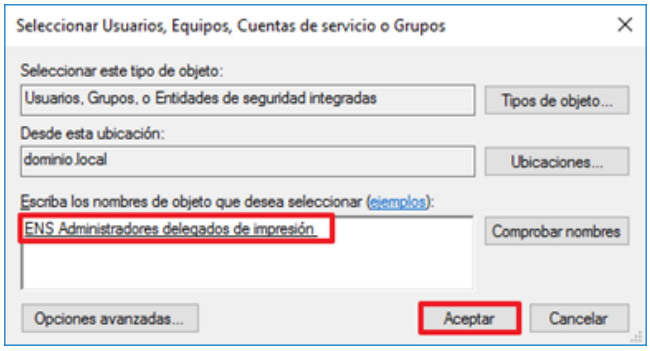
Paso	Descripción
53.	Localice el grupo que quiere añadir para que obtenga permisos para imprimir, y pulse sobre “Aceptar”.  **Nota:** En esta guía se selecciona el grupo de seguridad “ENS Grupo de impresión” al cual pertenecen los usuarios que van a obtener permiso para poder imprimir a través de los dispositivos de impresión seleccionados. Deberá adaptar este paso a los requisitos de su organización.
54.	Una vez añadido el grupo de seguridad, localice el grupo y seleccione en los permisos únicamente la opción de “Imprimir”. Pulse “Aceptar” para cerrar la ventana.  **Nota:** En este ejemplo se utiliza el grupo denominado “ENS Grupo de impresión”.
55.	Deberá repetir estos pasos para asignar permisos de impresión sobre todos los dispositivos de impresión sobre los que esté aplicando seguridad.

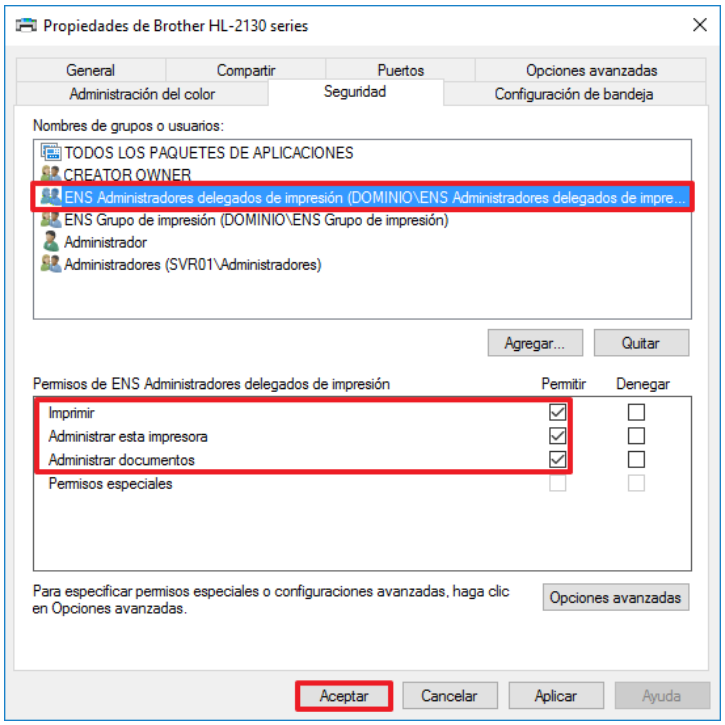
2.3. GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN

En este apartado se tendrá en consideración la gestión de permisos de administración sobre los dispositivos de impresión según lo establecido por el ENS, para con ello limitar y controlar el acceso a los dispositivos de impresión.

Paso	Descripción
56.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
57.	A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
58.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
59.	Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de impresión”**. 
60.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. Para ello despliegue el nodo **“Servidores de impresión → <<nombre del servidor>> → Impresora”**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.
61.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades…”.  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.

Paso	Descripción
62.	A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Agregar…”. 
63.	Localice el grupo que quiere añadir para que obtenga permisos para poder administrar el dispositivo de impresión seleccionado, y pulse sobre el “Aceptar”.  **Nota:** En esta guía se selecciona el grupo de seguridad “ENS Administradores delegados de impresión” al cual pertenecen los usuarios que van a obtener permisos administrativos sobre los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.

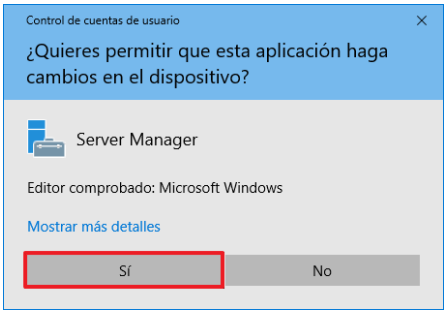
Paso	Descripción
64.	Una vez añadido el grupo de seguridad “Administradores delegados de impresión”, localice el grupo y seleccione los siguientes permisos. – Imprimir. – Administrar esta impresora. – Administrar documentos. Una vez establecidos los permisos, pulse “Aceptar” para confirmar los cambios y cerrar la ventana de propiedades del dispositivo de impresión. 

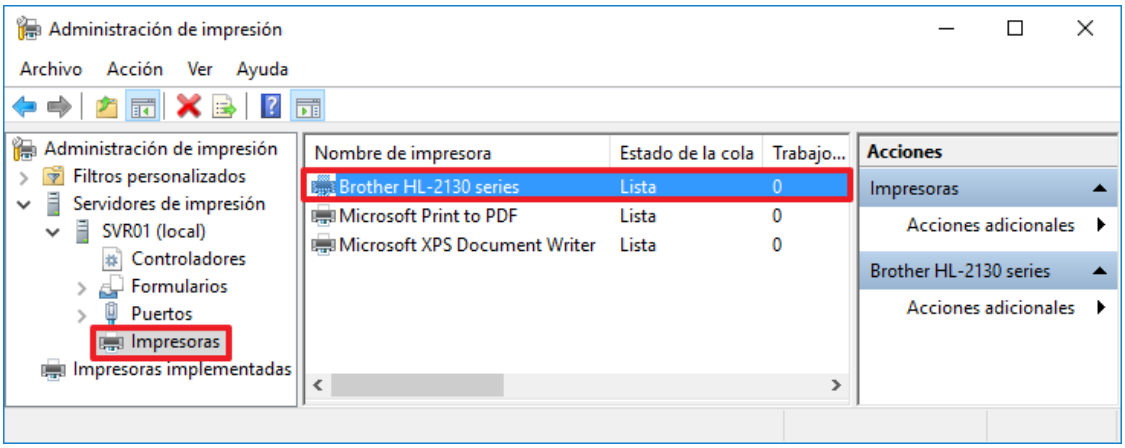
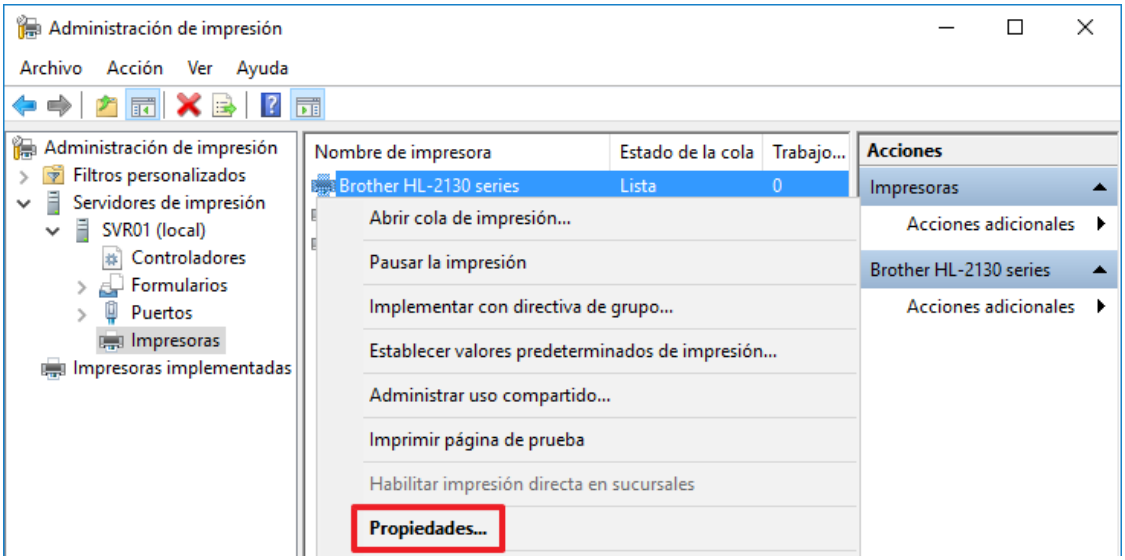
2.4. GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN

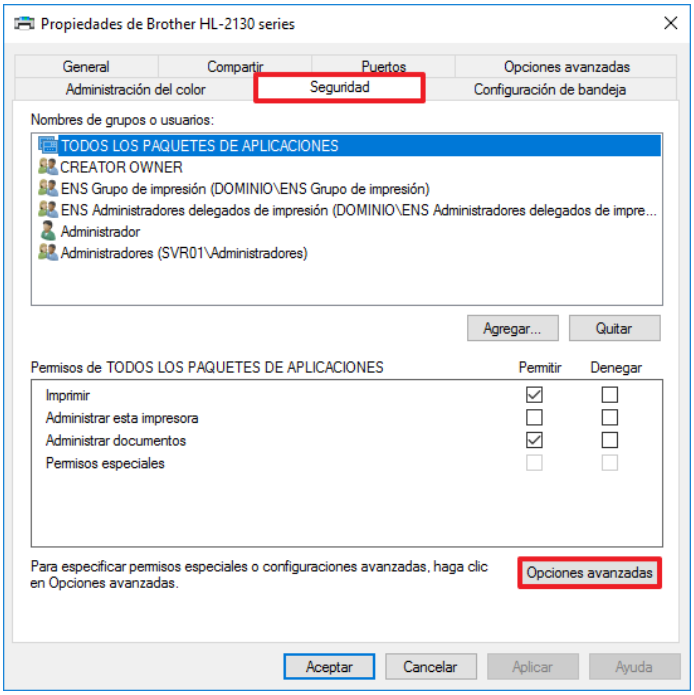
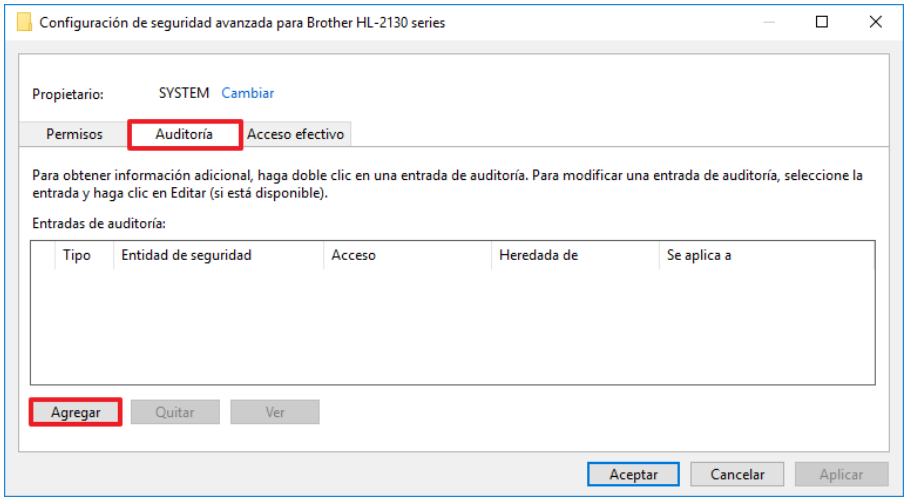
En este apartado se tendrá en consideración la habilitación de la auditoria en los dispositivos de impresión tal y como se especifica para las categorias media y alta que establece el ENS.

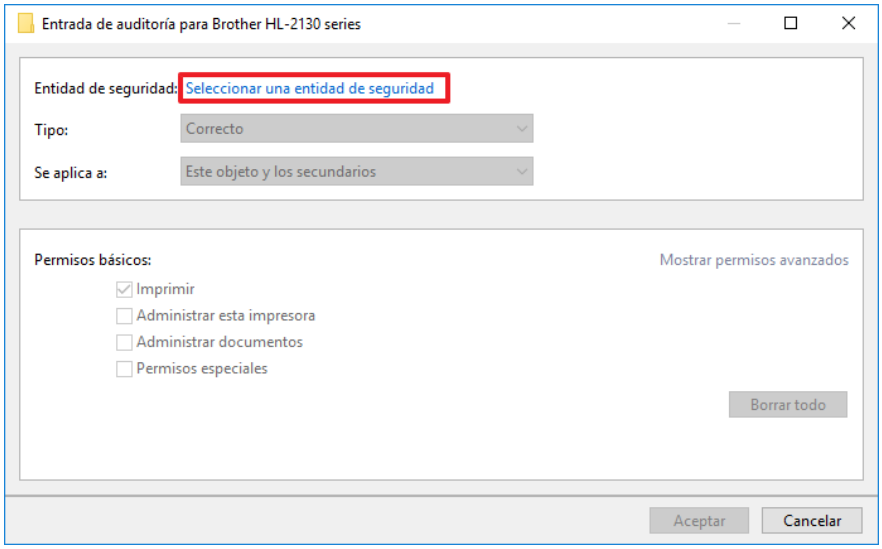
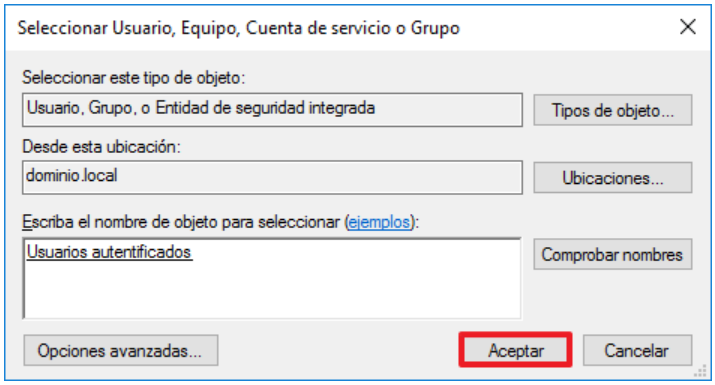
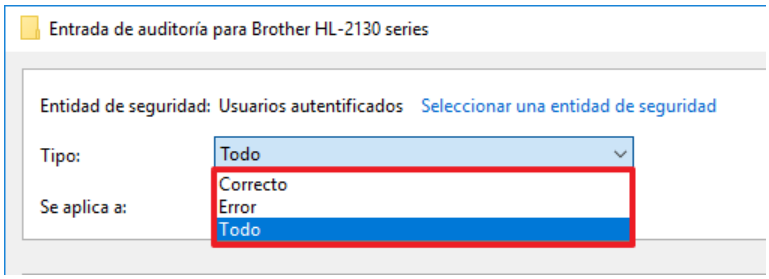
A continuación, se muestra el procedimiento para habilitar la auditoría en un dispositivo de impresión, instalado previamente, para un grupo de usuarios específicos.

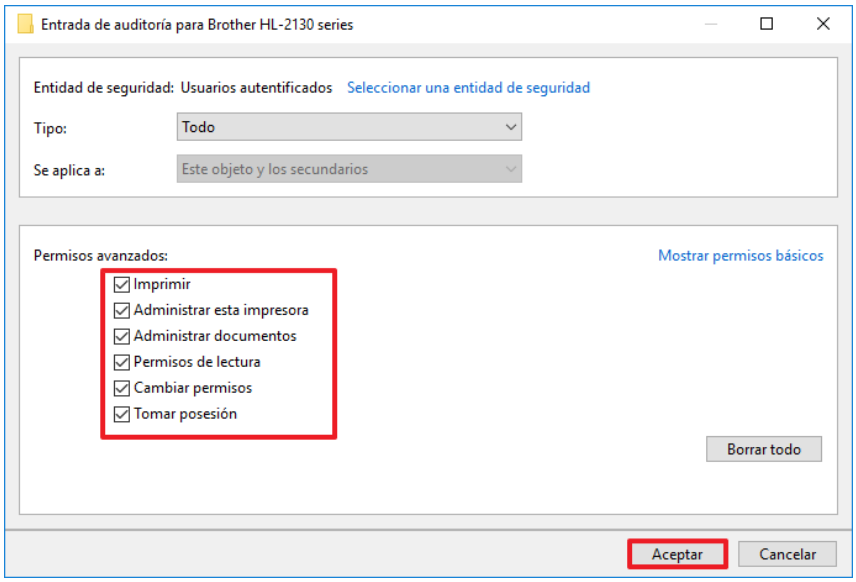
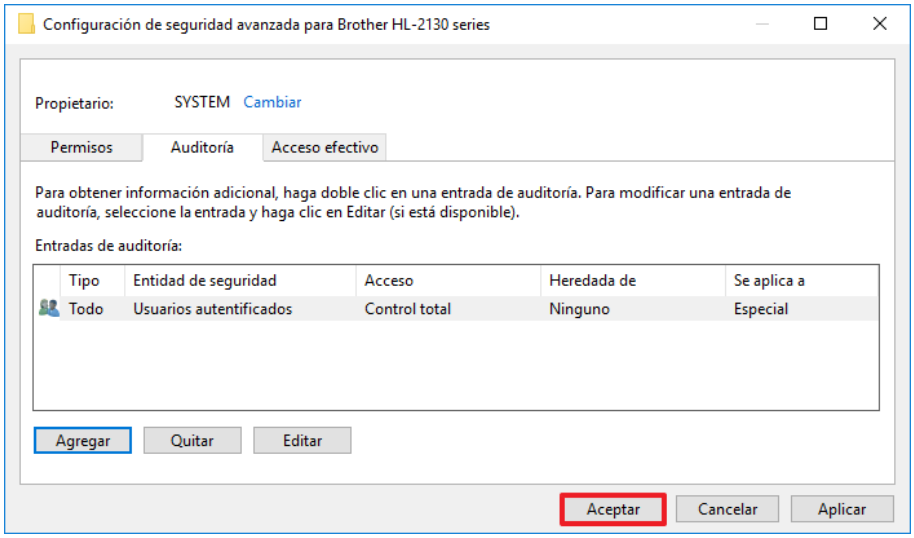
Nota: Para realizar este procedimiento se utiliza el dispositivo de impresión denominado “Brother HL-230 series”, utilizado para la creación de esta guía.

Paso	Descripción
65.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
66.	A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
67.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
68.	Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de impresión”**. 

Paso	Descripción
69.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo **"Servidores de impresión → <<nombre del servidor>> → Impresora"**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión "Brother HL-2130 series", deberá adaptar los pasos a las necesidades su organización.
70.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción "Propiedades…".  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado "Brother HL-2130 series".

Paso	Descripción
71.	A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Opciones avanzadas”. 
72.	Sitúese en la pestaña “Auditoría” y a continuación pulse sobre “Agregar”. 

Paso	Descripción
73.	Pulse sobre “Seleccionar una entidad de seguridad”. 
74.	Añada los grupos sobre los que desee realizar la auditoría y pulse “Aceptar”.  **Nota:** En este ejemplo se utiliza el grupo “Usuarios autentificados”.
75.	En la ventana desplegable “Tipo”, seleccione “Todo”, para que se visualicen tanto los eventos erróneos como los eventos correctos. 

Paso	Descripción
76.	En la parte derecha de la ventana, pulse sobre “Mostrar permisos avanzados” y seleccione todas las casillas de eventos auditables, tal y como se muestra en la imagen. Pulse sobre el botón “Aceptar”. 
77.	Pulse de nuevo sobre el botón “Aceptar” para cerrar la configuración de seguridad avanzada de la impresora. 
78.	Finalmente pulse “Aceptar” para cerrar la ventana de “Propiedades” de la impresora.
79.	Repita estos mismos pasos para cada uno de los dispositivos de impresión que deben ser auditados en su organización.

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN PARA LA CATEGORÍA MEDIA

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de impresión sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación, primero se deberá iniciar sesión en un Controlador de Dominio con una cuenta de usuario que tenga privilegios de administración en el dominio. A continuación, se realizarán las comprobaciones comunes a todos los servidores de impresión que son miembros del dominio.

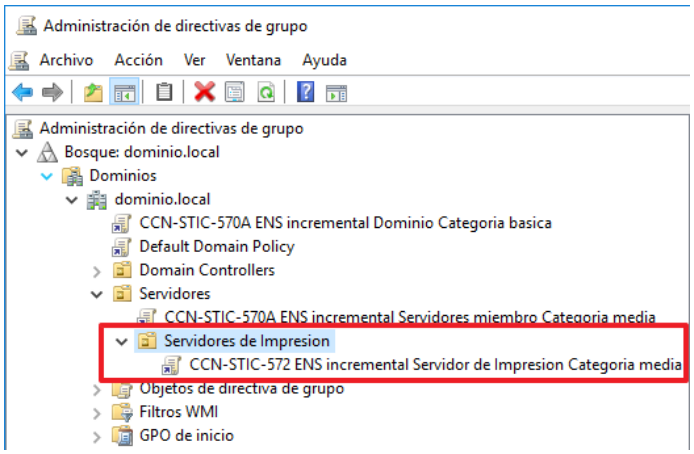
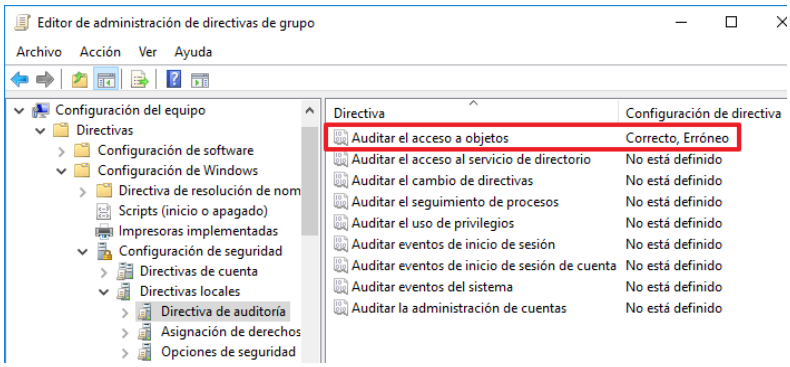
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de impresión, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios de administrador del dominio o administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

a) En el Controlador de Dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

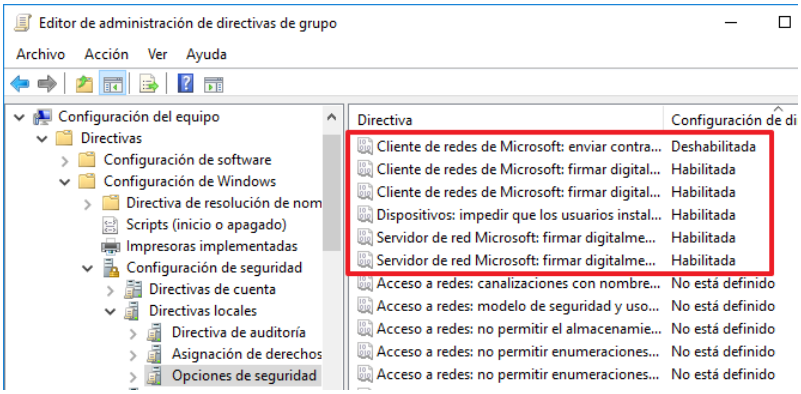
b) En el servidor de impresión:
   i. Administrador de Windows (explorer.exe).
   ii. PowerShell (powershell.exe).
   iii. Servicios (services.msc).
   iv. Editor de objetos de directiva de grupo (gpedit.msc).
   v. Administrador de impresión (printmanagement.msc).

Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado durante la presente guía. Deberá adaptar los pasos según la configuración de su organización.

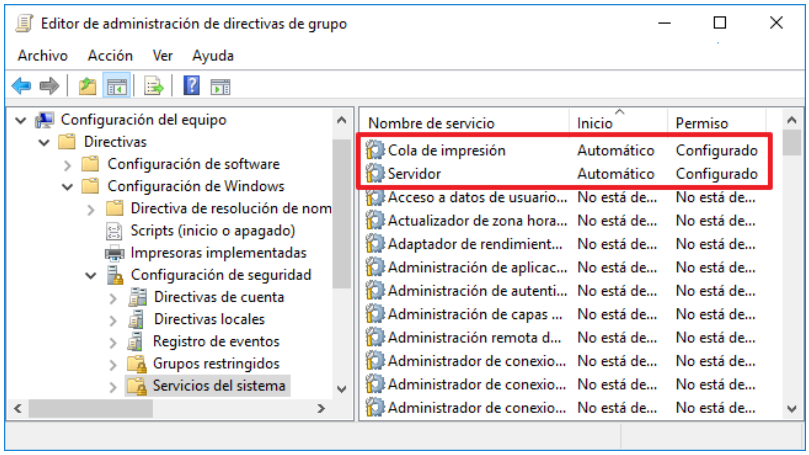
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que está creada la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media”.</td><td></td><td>Utilice el Administrador de directivas de grupo (“Inicio → Herramientas administrativas → Administración de directivas de grupo”) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de impresión” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media”.
 
</td></tr>
<tr><td>3. Verifique los valores de auditoría de la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media”.</td><td></td><td>Utilizando el editor de directiva de grupo, haga clic derecho sobre la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media” y seleccione la opción “Editar…”. Verifique que la directiva tiene los siguientes valores en las directivas de auditoría dentro de:
“Directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”.
 

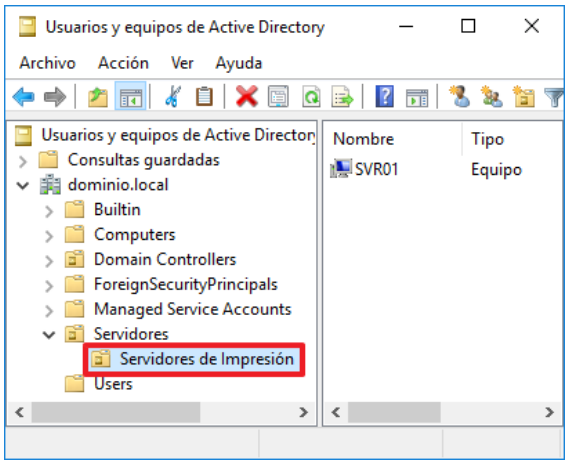
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
</table></td></tr>
</table>

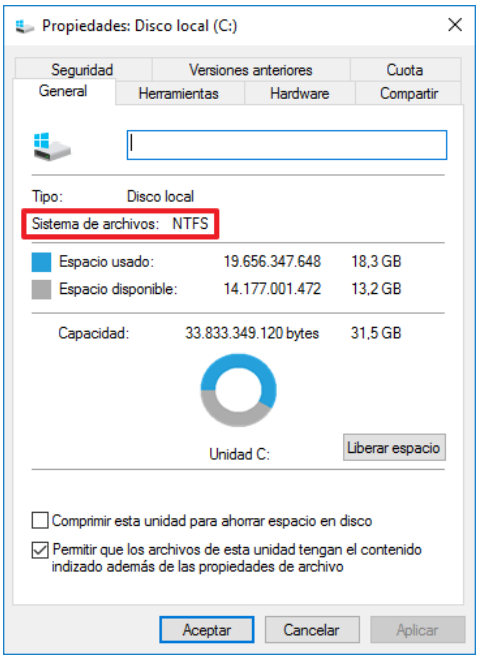
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>4. Verifique las opciones de seguridad de la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media”.</td><td></td><td>Utilizando el editor de directiva de grupo, verifique que la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media” tiene los siguientes valores en las opciones de seguridad dentro de:
“Directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cliente de redes Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Cliente de redes Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Cliente de redes Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
<tr><td>Dispositivos: Impedir que los usuarios instalen controladores de impresora</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red de Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

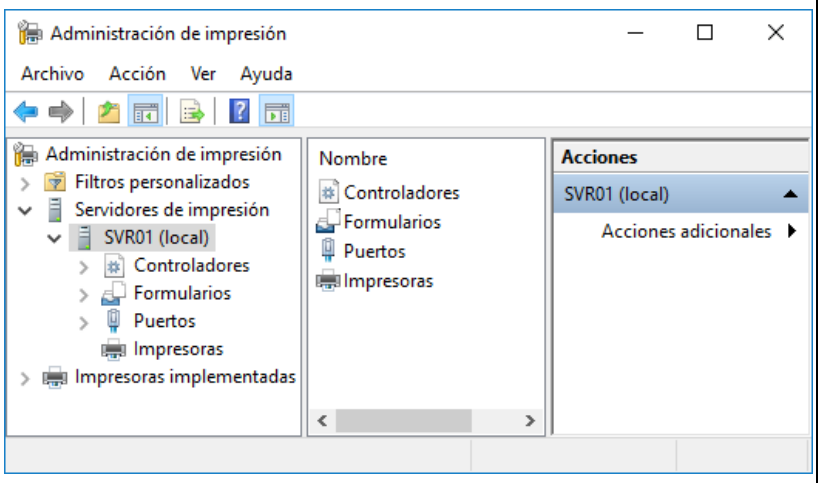
Servicio (Nombre largo)	Servicio (Nombre corto)	Inicio	Permisos	OK/NOK
Cola de impresión	Spooler	Automático		
Servidor	LanmanServer	Automático		

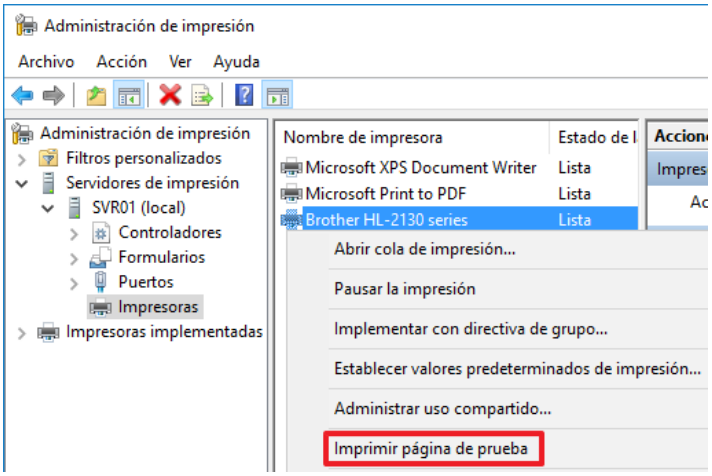
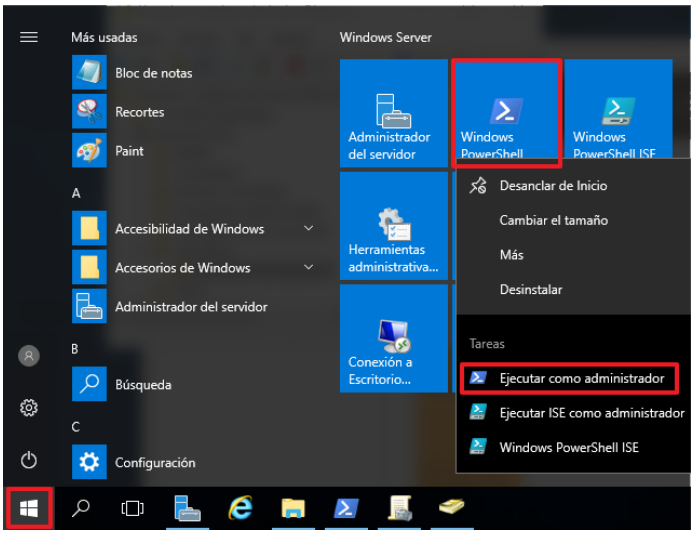
6. Verifique que el servidor de impresión está dentro de la unidad organizativa "Servidores de impresión".		Utilice la herramienta Usuarios y equipos de Active Directory (**"Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory"**) y seleccione la unidad organizativa "Servidores de impresión". Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de impresión que se están asegurando. 

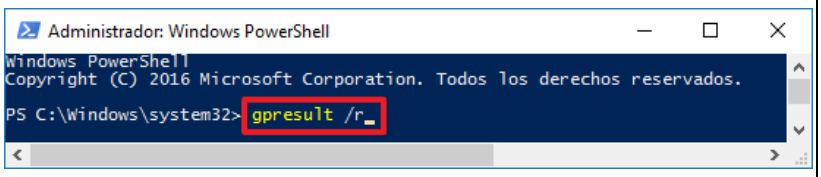
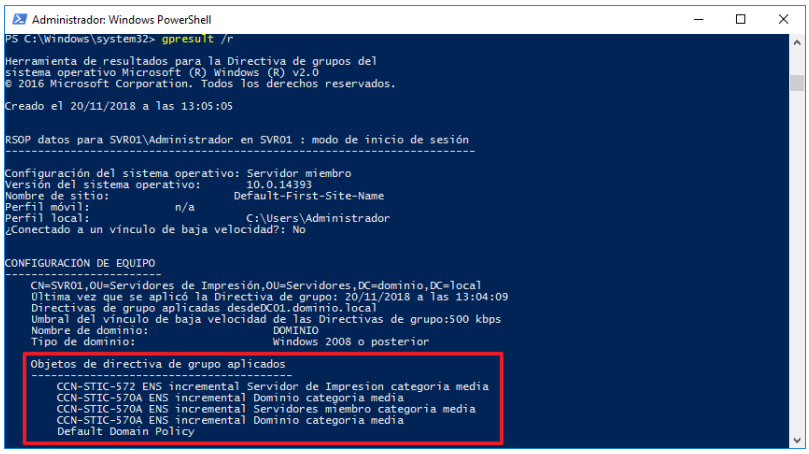
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Inicie sesión en el servidor de impresión.</td><td></td><td>Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.</td></tr>
<tr><td>8. Verifique que todos los volúmenes están formateados con NTFS.</td><td></td><td>Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL’s.
 
</td></tr>
<tr><td rowspan="3">9. Verifique que están instalados los componentes que se indican.</td><td></td><td>En el “Administrador del Servidor”, pulse sobre la opción “Servidor Local” del menú de la izquierda y diríjase a la parte final de la ventana principal, “Roles y características”, por medio del scroll lateral derecho.</td></tr>
<tr><td colspan="2"><table>
<tr><th>Rol</th><th>OK/NOK</th></tr>
<tr><td>Servicios de impresión y documentos</td><td></td></tr>
<tr><td>Servidor de impresión</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique que los servicios del sistema relacionados con el servidor de impresión están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre **Inicio → Ejecutar**) y compruebe el tipo de inicio de los servicios.

Servicio (Nombre largo)	Servicio (Nombre corto)	Inicio	Permisos	OK/NOK
Cola de impresión	Spooler	Automático		
Servidor	LanmanServer	Automático		

11. Verifique que la instalación del servidor de impresión se ha realizado correctamente.		Utilizando la herramienta de administración de impresión (ejecutando "printmanagement.msc" desde, botón derecho sobre **Inicio → Ejecutar**), verifique que la consola se inicia y presenta el servidor local como un servidor de impresión.  **Nota:** En esta comprobación, el servidor se denomina "SVR01". En su organización debe comprobar que aparece el nombre del servidor de impresión que está implementando.

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.		Utilizando la herramienta de administración de impresión (ejecutando "printmanagement.msc" desde, botón derecho sobre **Inicio → Ejecutar**), verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión. Para ello, seleccione cada una de las impresoras que aparecen en el nodo "Impresoras" con el botón derecho del ratón y pulse sobre la opción "Imprimir página de prueba". 
13. Inicie la consola de PowerShell.		Ejecute la consola de PowerShell. Para ello pulse "Inicio",.seleccione "Powershell" con el botón derecho y pulse sobre "Ejecutar como administrador". 

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique que se estan aplicando las GPOs correspondientes.		Verifique que se estan aplicando las GPOs correspondientes ejecutando el comando “gpresult /r”. 
15. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se aplican las siguientes GPOs. – CCN-STIC-572 ENS incremental Servidor de Impresion Categoria media. – CCN-STIC-570A ENS incremental Servidores miembro Categoria media. – CCN-STIC-570A ENS incremental Dominio Categoria media. 

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN

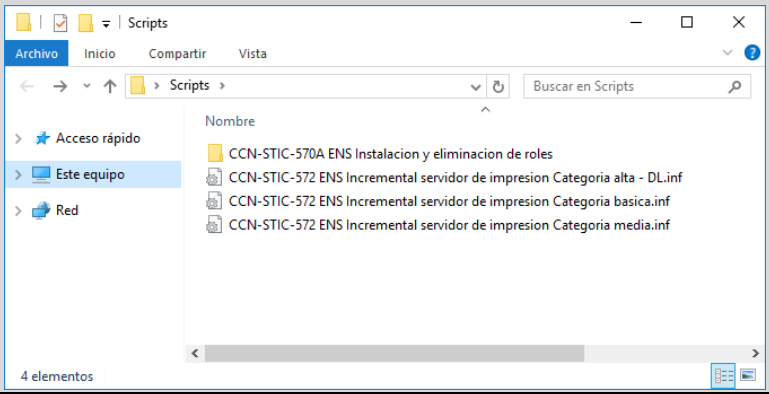
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de impresión con una categorización de seguridad alta según los criterios del Esquema Nacional de Seguridad. Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad cumpla con los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

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 los servicios e información manejada por la organización correspondieran, al menos, a la categoría alta o difusión limitada para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

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 a las peculiaridades del sistema operativo utilizado en el caso de una red de este tipo.

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.

Nota: Si instala el Servidor de impresión por primera vez con la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016 aplicada debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.
En la guía mencionada anteriormente se describe el procedimiento para implementar el objeto GPO que permite la instalación de roles y características. En caso de no disponer de los datos adjuntos a la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016" encontrará una copia de seguridad para poder importar la GPO necesaria en la carpeta "Scripts" adjunta a la presente guía.

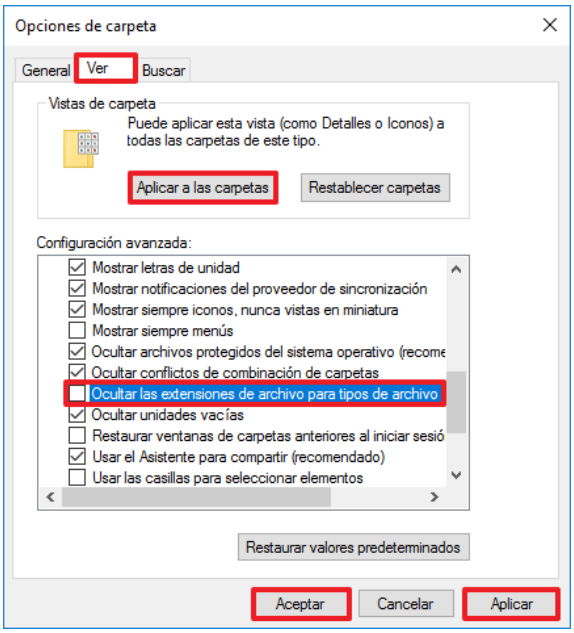
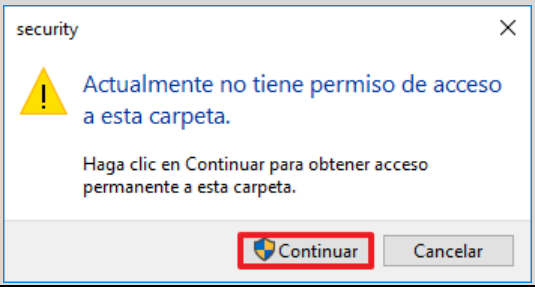


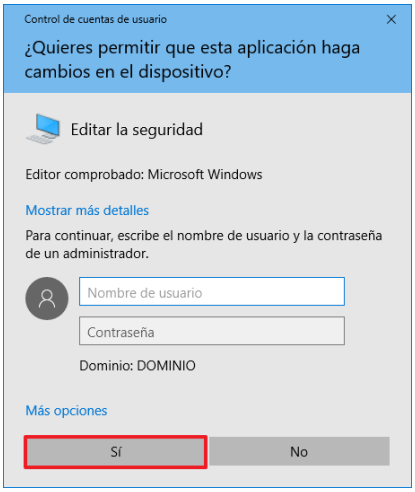
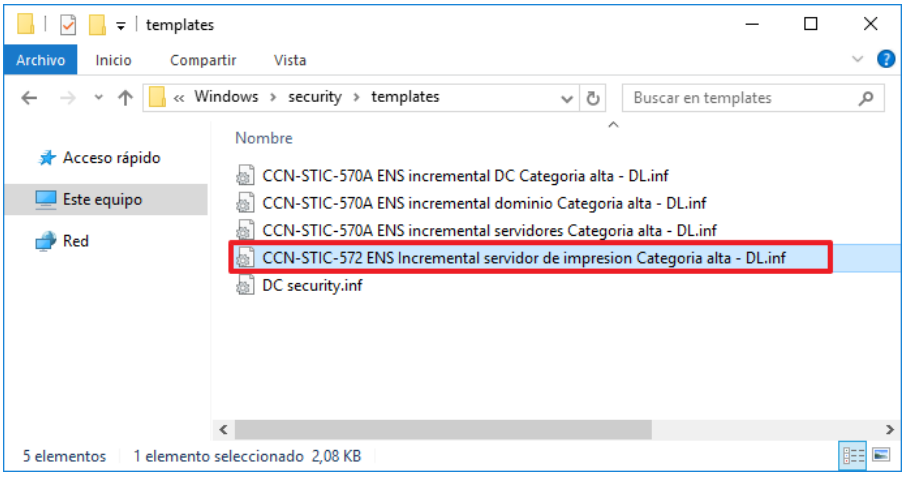
1. PREPARACIÓN DEL DOMINIO

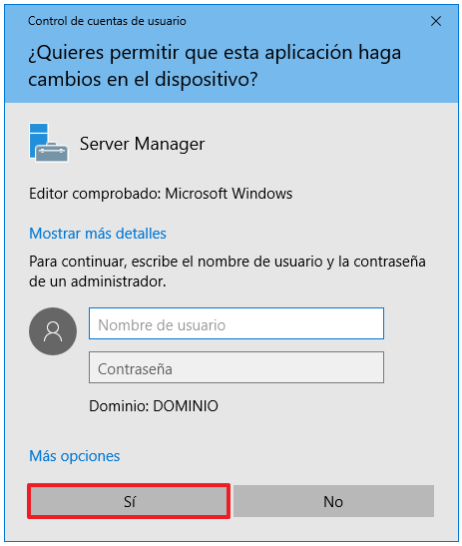
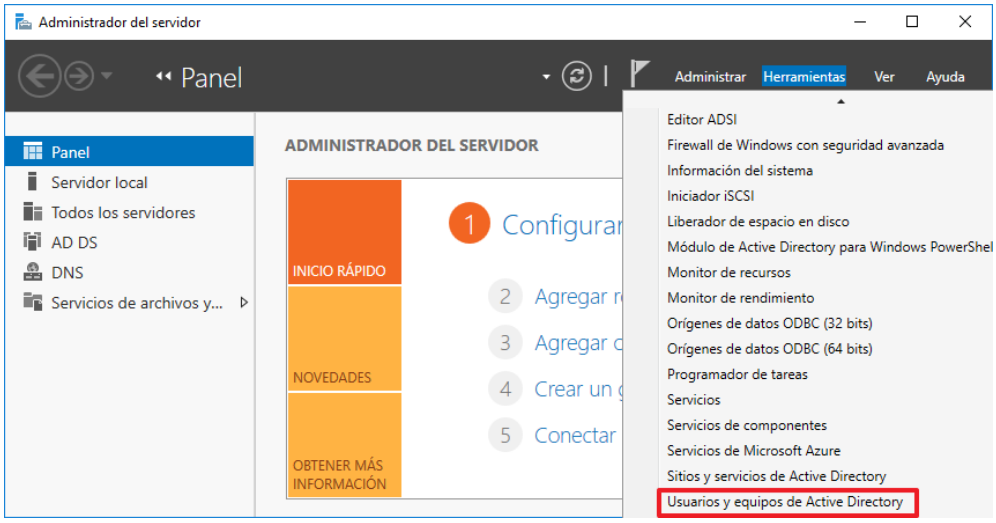
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de impresión miembro del dominio. Durante este procedimiento se crea la unidad organizativa que contiene los servidores de impresión y se realizan las configuraciones de políticas de grupo correspondientes.

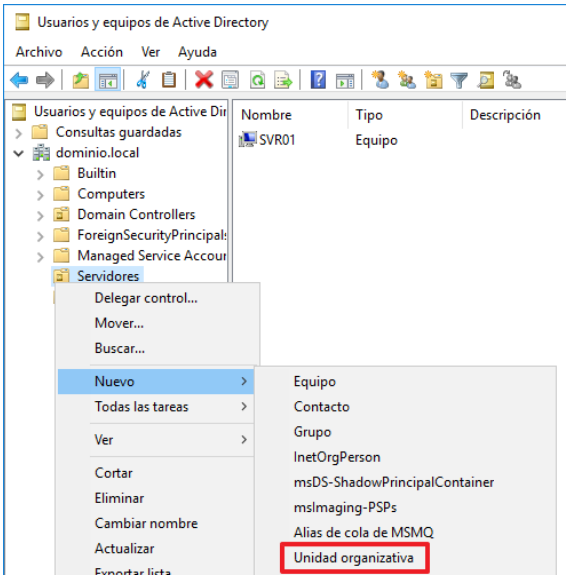
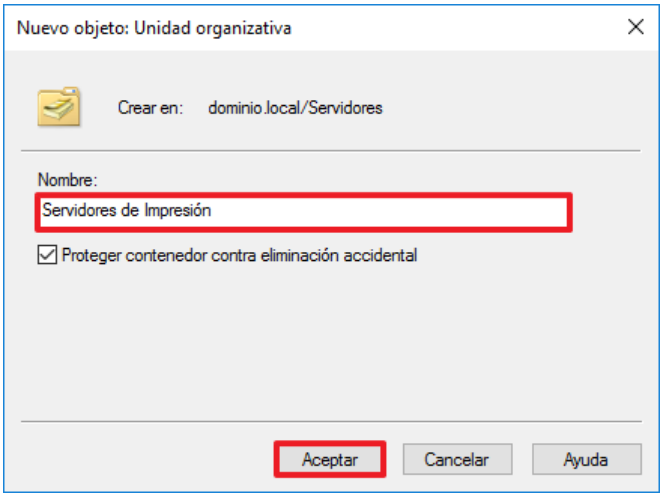
Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de impresión que está asegurando, se les ha aplicado la configuración descrita en la guía "CCN-STIC-570A Implementación del ENS en Microsoft Windows Server 2016". Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

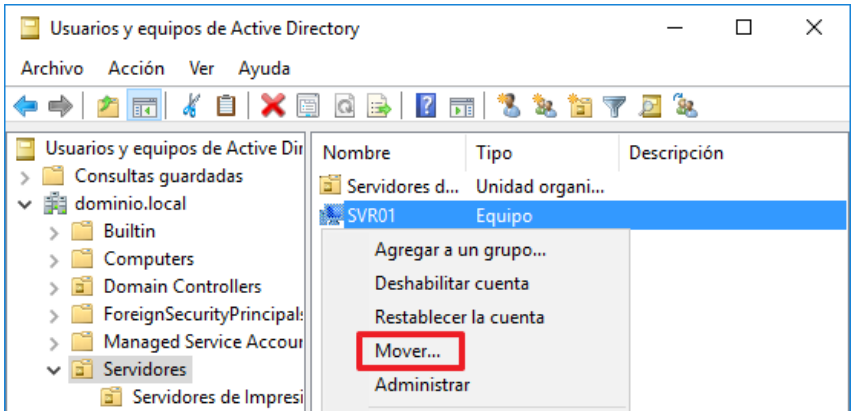
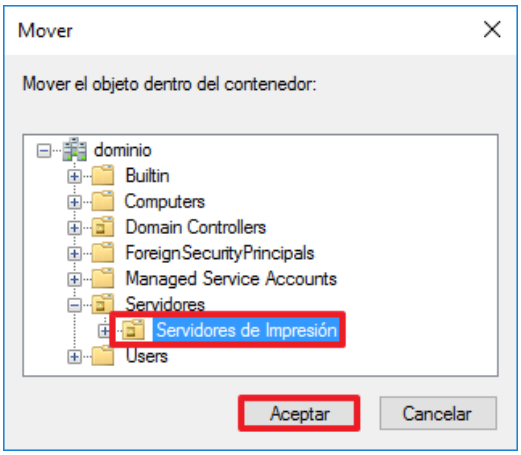
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio "Scripts" en la unidad "C:\". **Nota:** Los scripts asumen que su ubicación en el sistema será bajo "C:\Scripts". Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
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" muestra las extensiones de los archivos.

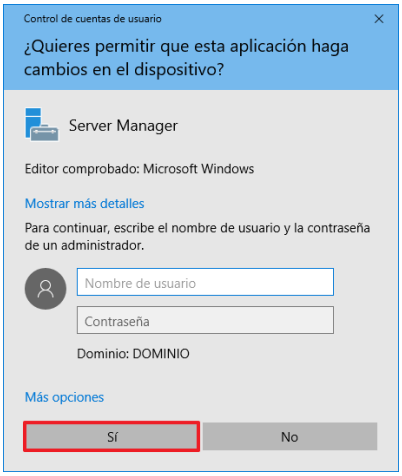
Paso	Descripción
5.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. En la venta emergente, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la imagen.  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 “¿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.	Adicionalmente acceda al directorio “C:\Windows\Security\Templates”. **Nota:** Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente. 

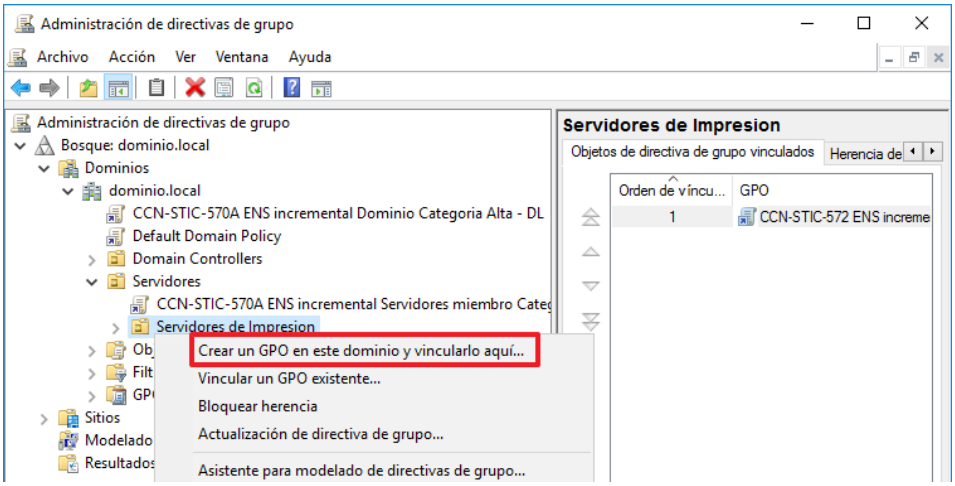
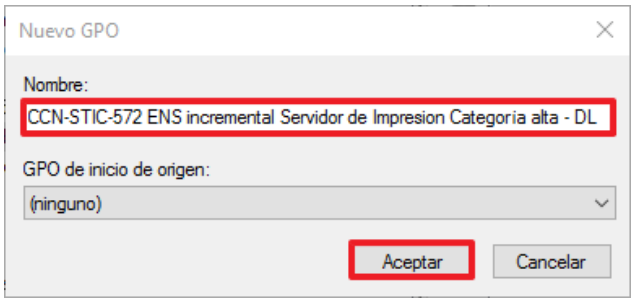
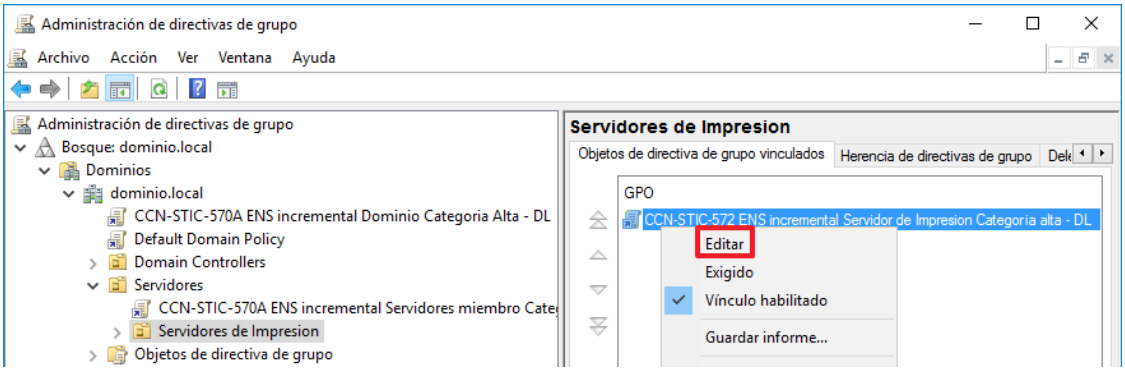
Paso	Descripción
7.	El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar. 
8.	Copie el fichero “CCN-STIC-572 ENS Incremental servidor de impresion Categoria alta – DL.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\Security\Templates”. 
9.	A continuación, deberá crear la unidad organizativa "Servidores de Impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

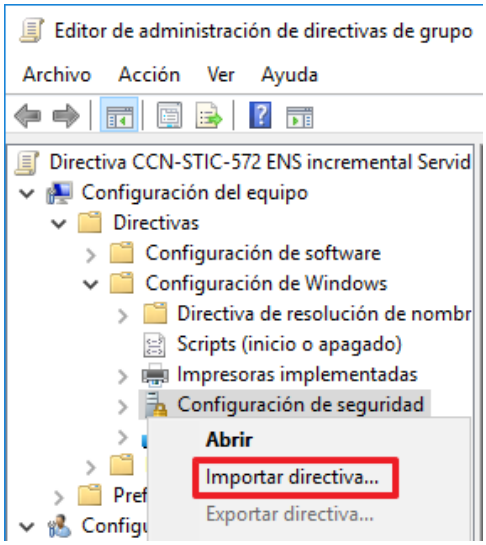
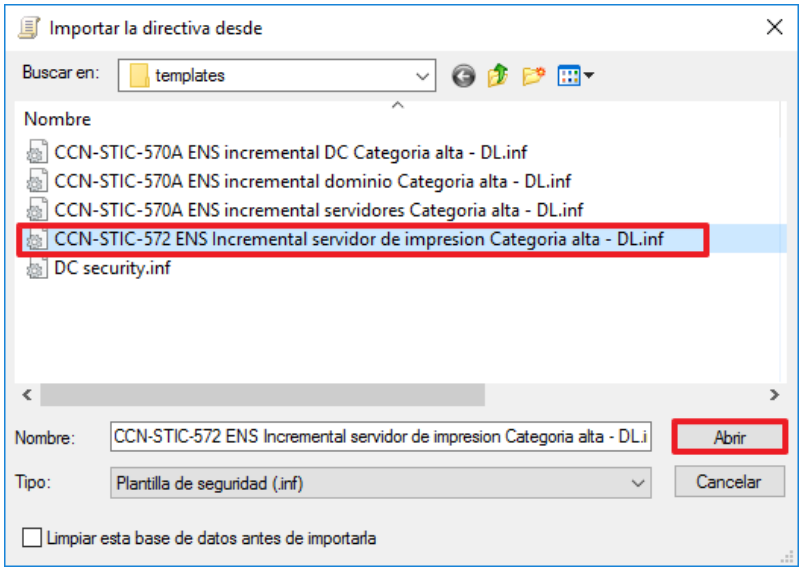
Paso	Descripción
10.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
11.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Usuarios y equipos de Active Directory”** 

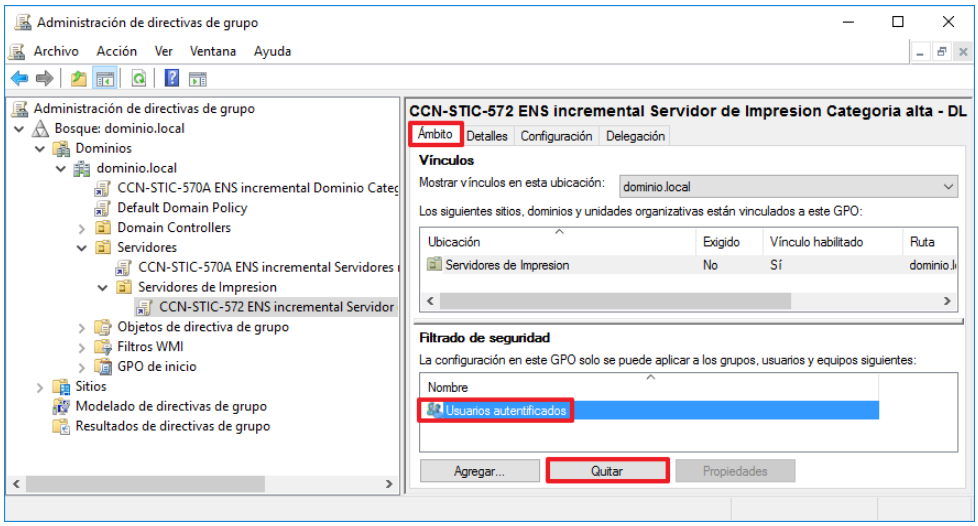
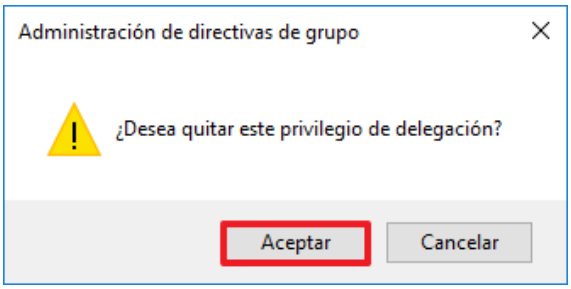
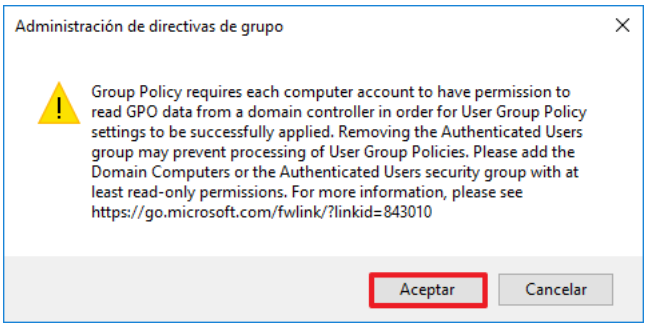
Paso	Descripción
12.	En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. Para ello, seleccione el nodo **"<<dominio>> → <<unidad organizativa>>"**, y desplegando el menú contextual con el botón derecho, seleccione la opción **"Nuevo → Unidad organizativa"**.  **Nota:** En este ejemplo, la unidad organizativa de servidores se encuentra en **"dominio.local → Servidores"**.
13.	Introduzca el nombre "Servidores de impresión" tal y como se muestra en la imagen y pulse sobre "Aceptar". 

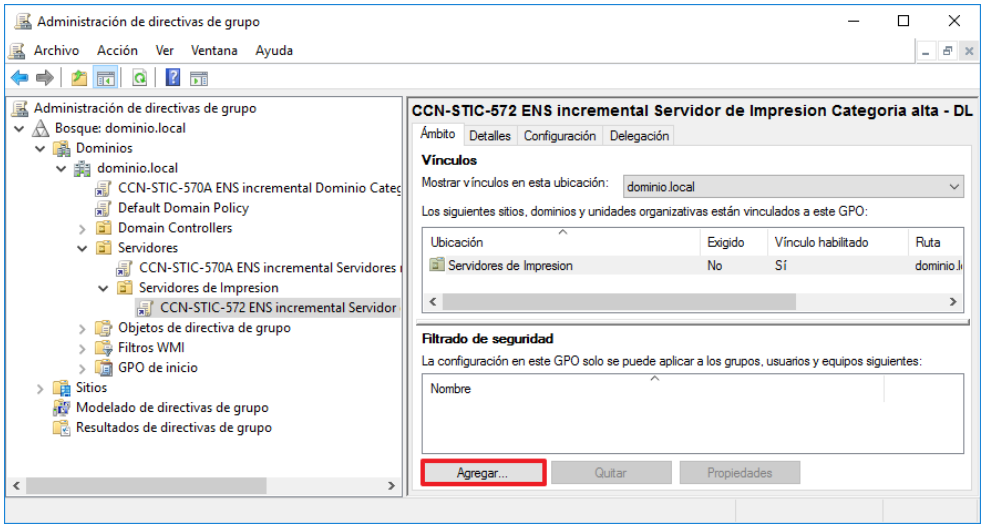
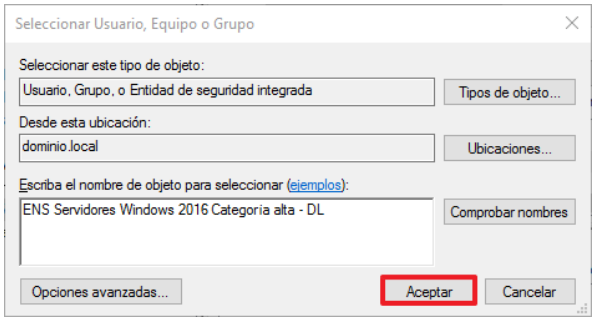
Paso	Descripción
14.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores de impresión a la unidad organizativa “Servidores de impresión”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”. 
15.	A continuación, seleccione la unidad organizativa “Servidores de impresión” y pulse “Aceptar”. 
16.	Cierre la herramienta “Usuarios y equipos de Active Directory”.
17.	A continuación, deberá crear la GPO "CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
18.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
19.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de directivas de grupo”.** 
20.	A continuación, despliegue el nodo **“Bosque: <<nombre de bosque>> → Dominios → <<nombre de dominio>> → Servidores → Servidores de impresión”**. **Nota:** En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de impresión”.

Paso	Descripción
21.	Pulse con el botón derecho sobre la unidad organizativa “Servidores de impresión” y seleccione “Crear un GPO en este dominio y vincularlo aquí…”. 
22.	Escriba el nombre de la GPO “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL” y haga clic en el botón “Aceptar”. 
23.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 
24.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**.

Paso	Descripción
25.	Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva…”. 
26.	Seleccione de la ruta “C:\Windows\Security\Templates” el fichero “CCN-STIC-572 ENS Incremental servidor de impresion Categoria alta - DL.inf” y pulse el botón “Abrir”. 
27.	Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

Paso	Descripción
28.	Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
29.	Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”. 
30.	Pulse de nuevo “Aceptar” ante el mensaje de advertencia emergente. 

Paso	Descripción
31.	A continuación, pulse el botón “Agregar…”. 
32.	Introduzca como nombre “ENS Servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-570A Implementación del ENS en Windows Server 2016. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a las necesidades de su organización.

2. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

El presente punto advierte al operador que realice la implementación de la guía sobre una serie de condiciones y consideraciones a tener en cuenta antes de la aplicación de la nueva configuración. Debe tenerse en consideración que cada organización puede presentar configuraciones previas y, por lo tanto, deben valorarse con respecto a la aplicación de la presente configuración.

Las plantillas de seguridad que se han configurado tienen en consideración los puntos tratados en el Esquema Nacional de Seguridad para la categoría alta. No obstante, determinadas configuraciones podrían ser contrarias a las implementadas actualmente por la organización y debe tomarse en consideración su adaptación paulatina como, por ejemplo, lo concerniente a la política de credenciales.

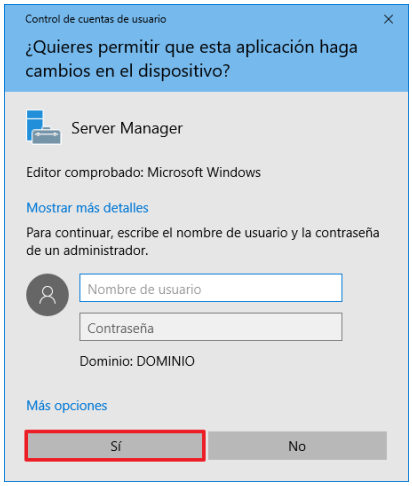
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

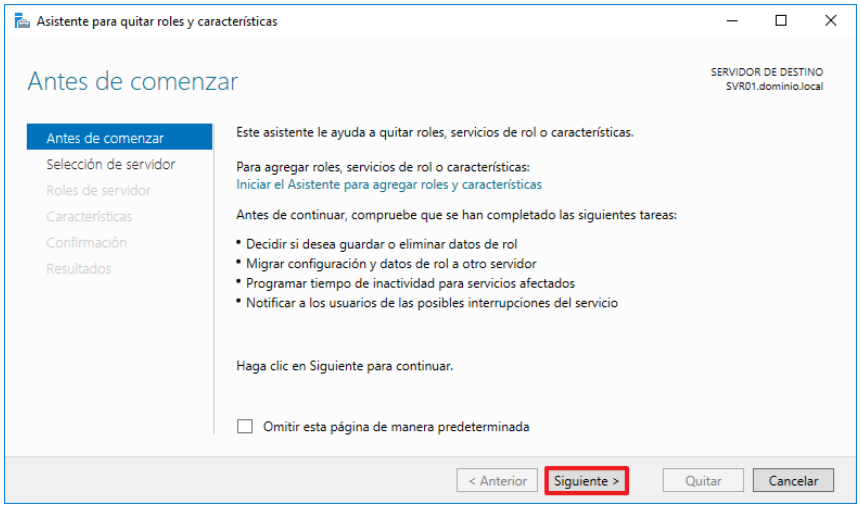
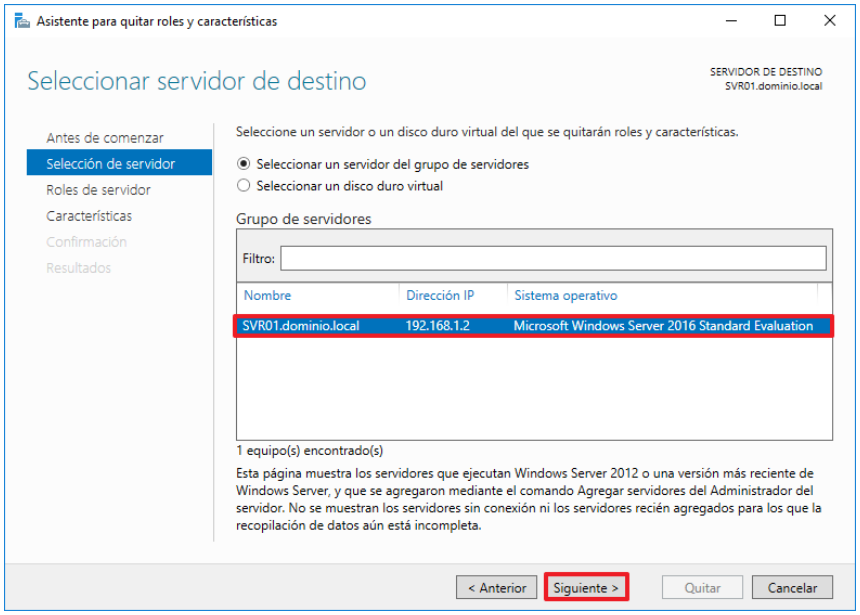
2.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

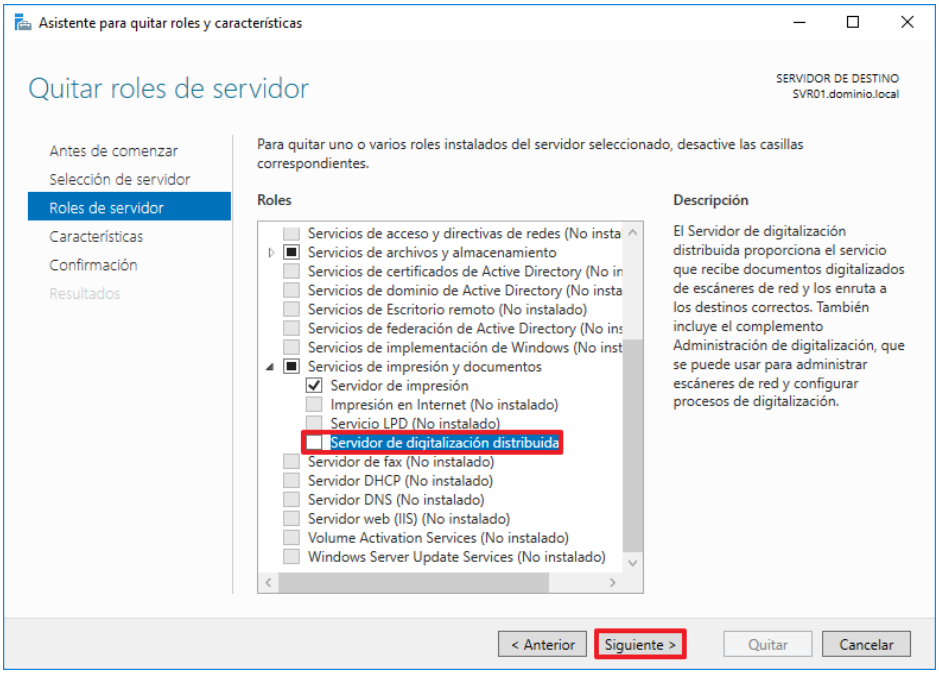
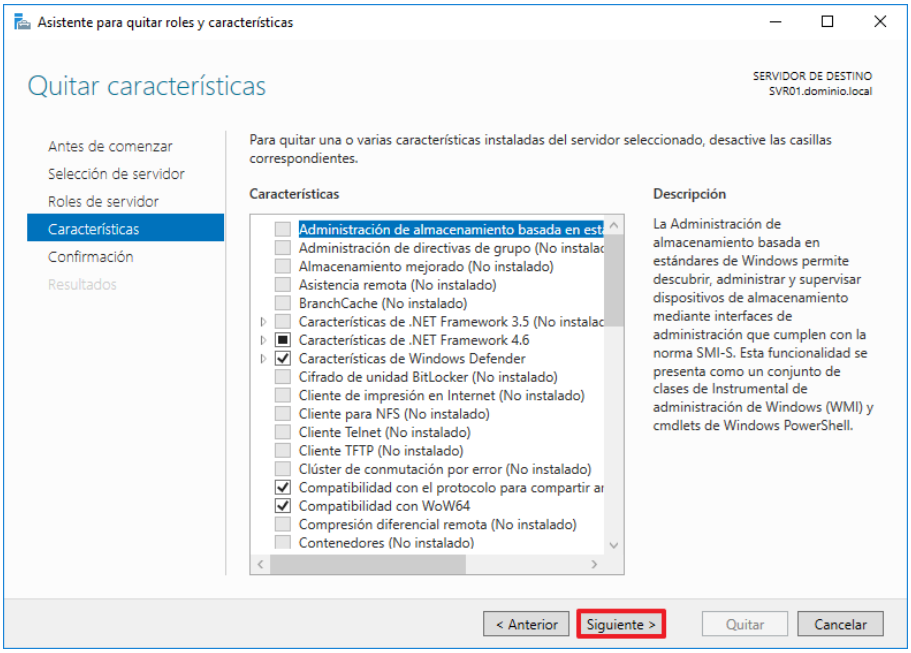
Uno de los aspectos que marca el ENS, desde su requisito de categoría básica en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

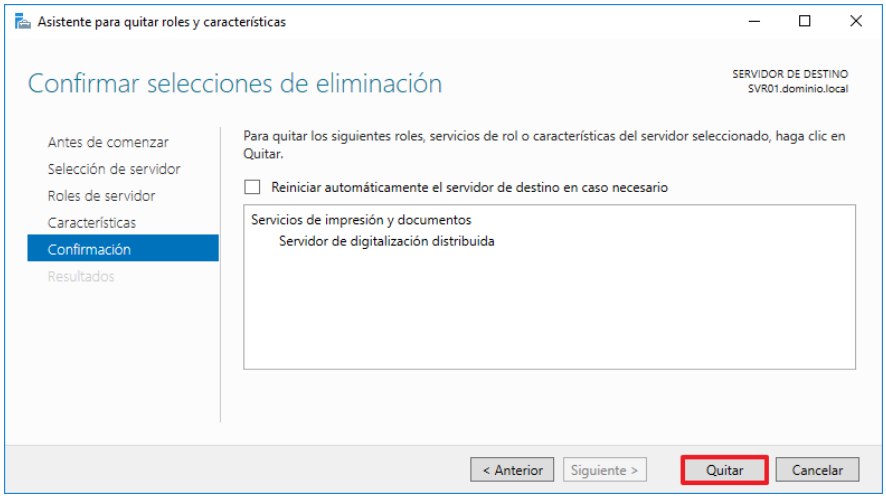
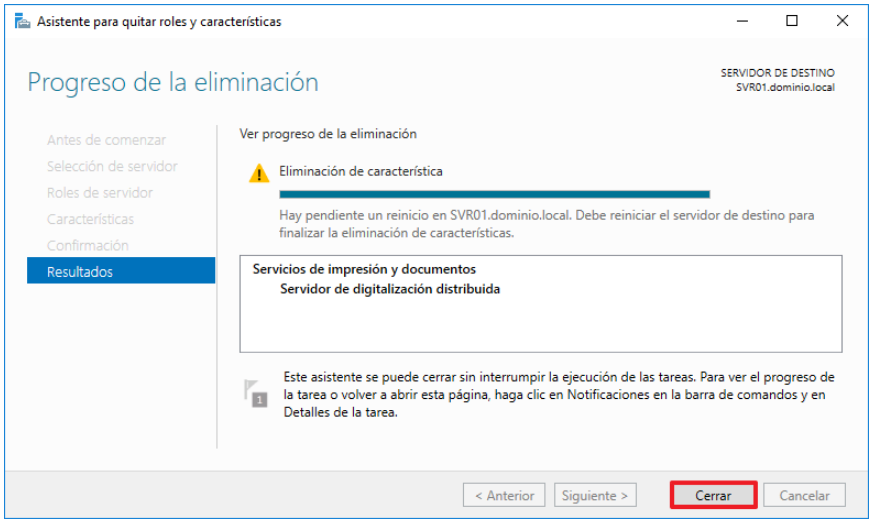
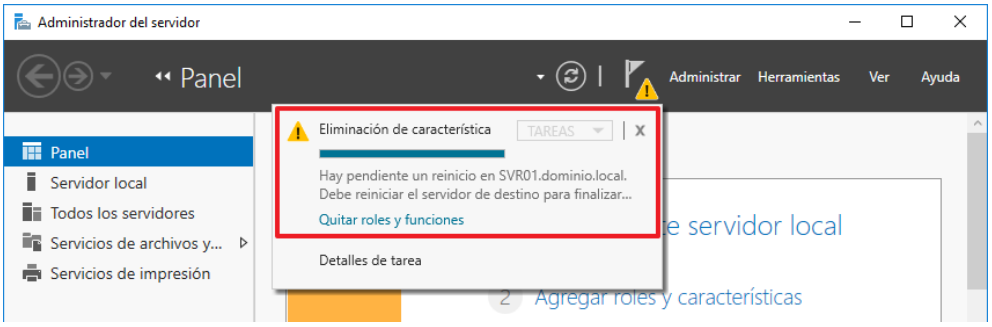
En el procedimiento que se describe a continuación, a modo de ejemplo, desinstala un rol que actualmente no está siendo utilizado por el Servidor de impresión.

Paso	Descripción
33.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.

Paso	Descripción
34.	Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas. 
35.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
36.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”. 

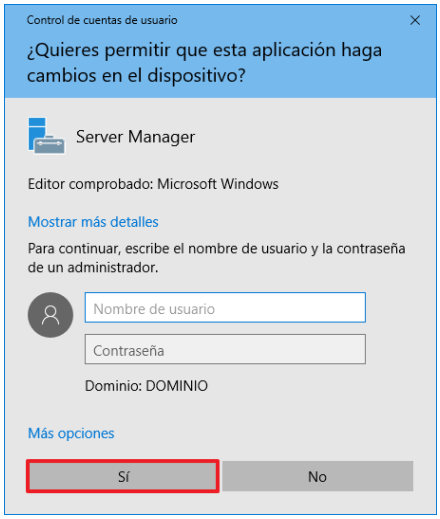
Paso	Descripción
37.	Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar. 
38.	Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.  **Nota:** En este ejemplo se utiliza el servidor con el nombre “SVR01”.

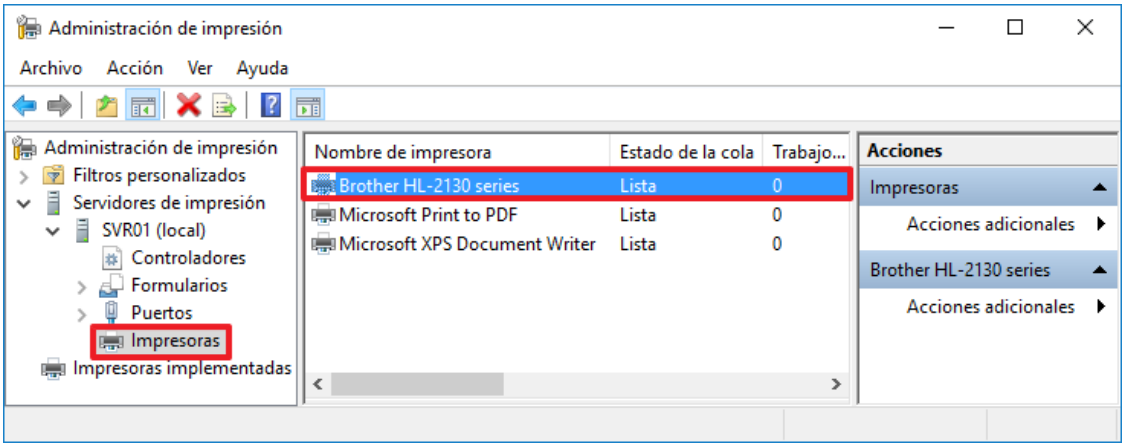
Paso	Descripción
39.	En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.  **Nota:** En este ejemplo se desinstala el rol “Servidor de digitalización distribuida”.
40.	En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. 

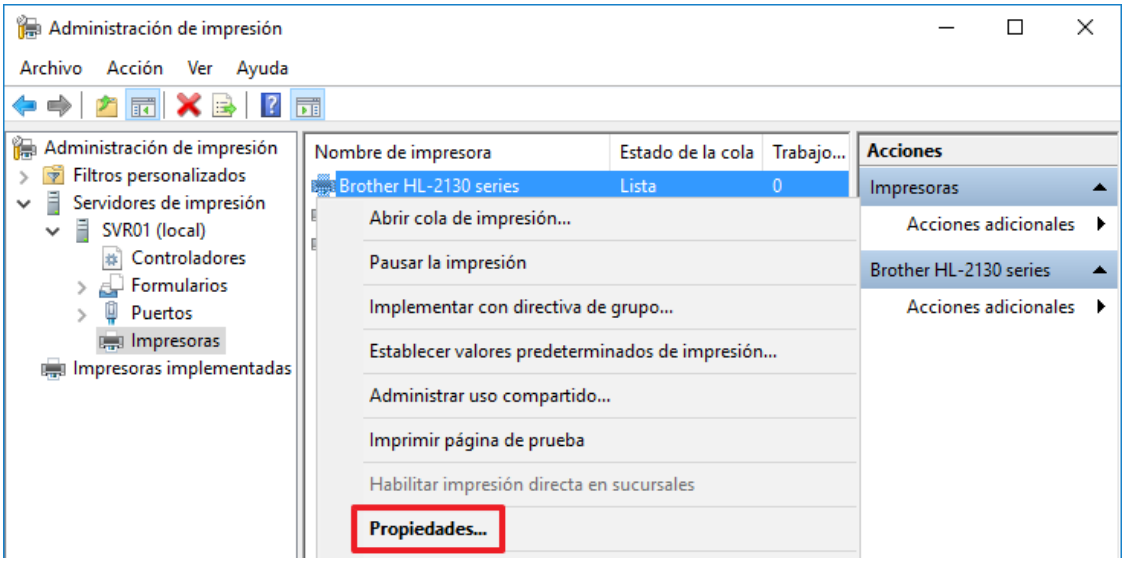
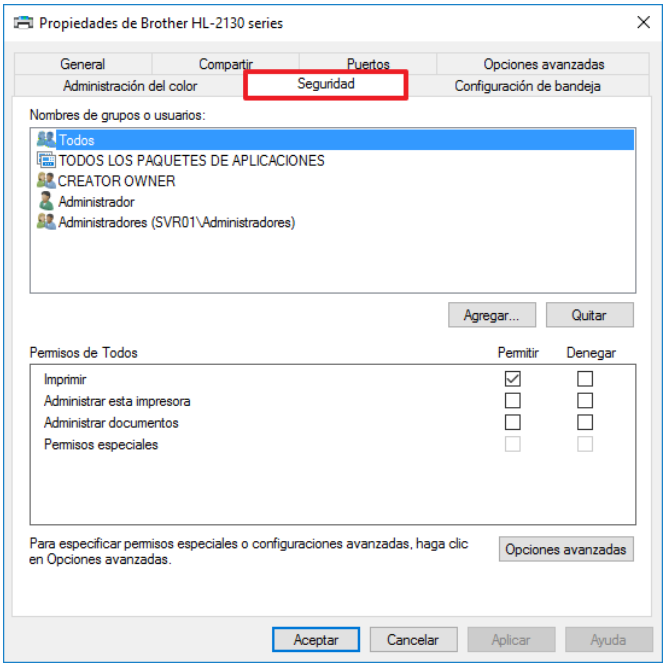
Paso	Descripción
41.	En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. 
42.	El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación. 
43.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración. El “Administrador del servidor” mostrará una advertencia acerca de la necesidad de dicho reinicio. 

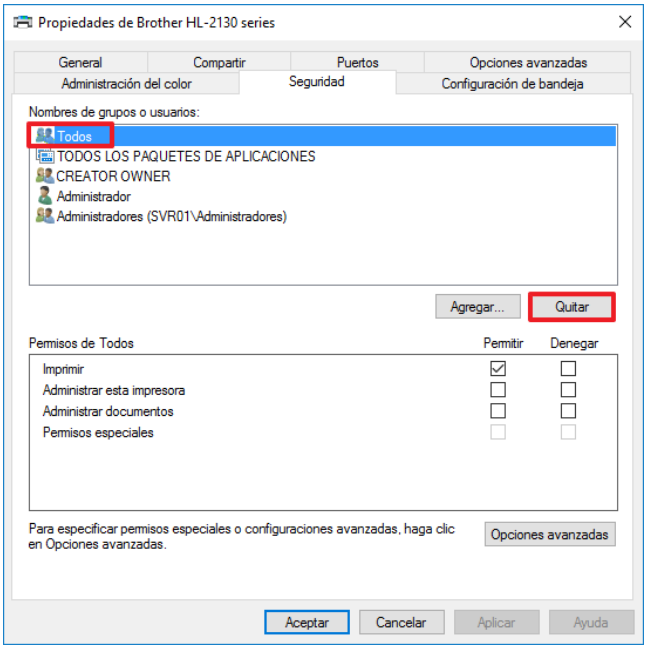
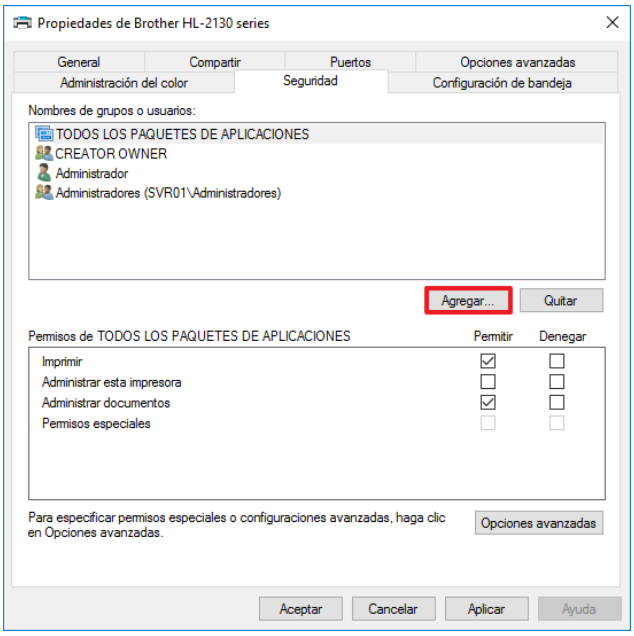
2.2. GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN

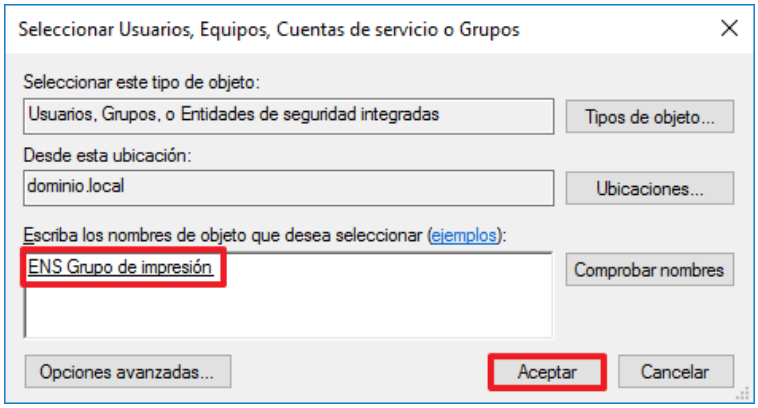
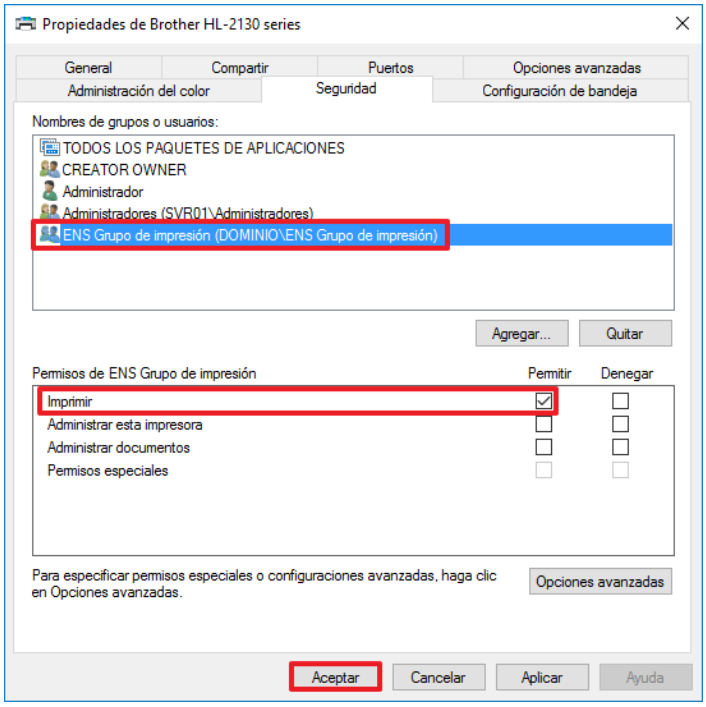
Es recomendable que, en el dispositivo de impresión solo se disponga de permiso de impresión, para el personal estrictamente necesario, además se recomienda hacer una gestión de los permisos de impresión empleando grupos de seguridad.

Paso	Descripción
44.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
45.	A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
46.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
47.	Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de impresión”**. 
48.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo **“Servidores de impresión → <<nombre del servidor>> → Impresora”**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

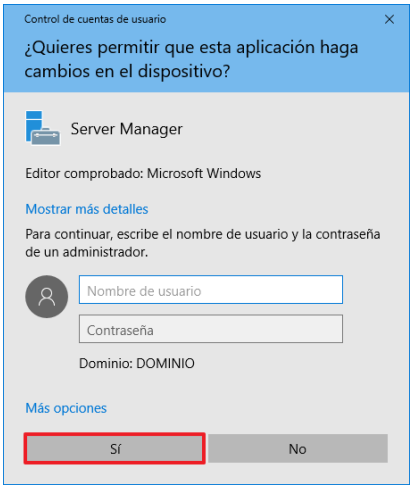
Paso	Descripción
49.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades…”.  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.
50.	A continuación, seleccione la pestaña “Seguridad”. 

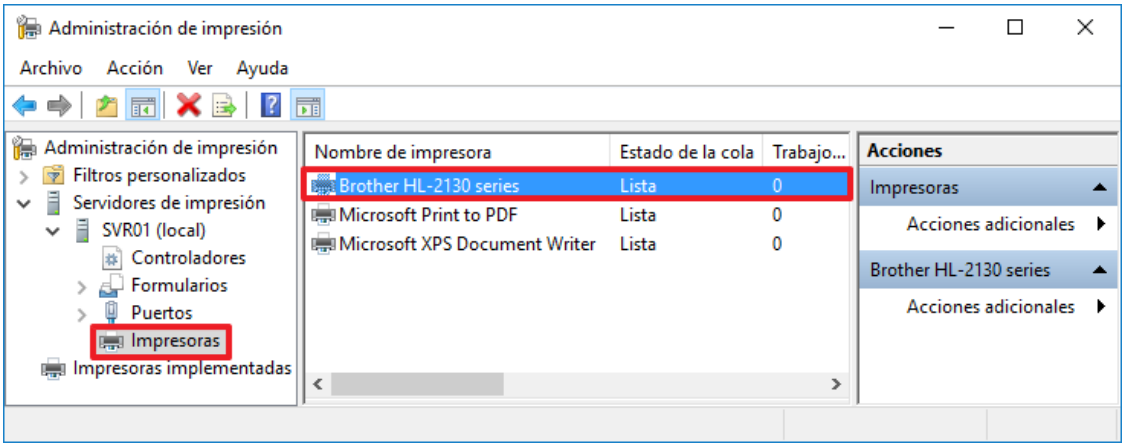
Paso	Descripción
51.	Seleccione el grupo de usuarios “Todos” y a continuación pulse en la opción “Quitar”.  **Nota:** Deberá adaptar este paso a los requisitos de su organización eliminando los usuarios o grupos de usuarios que no requieran de permisos sobre el dispositivo de impresión.
52.	A continuación, pulse sobre el botón “Agregar” para añadir el grupo de usuarios que tendrá permiso para poder imprimir por el dispositivo de impresión seleccionado. 

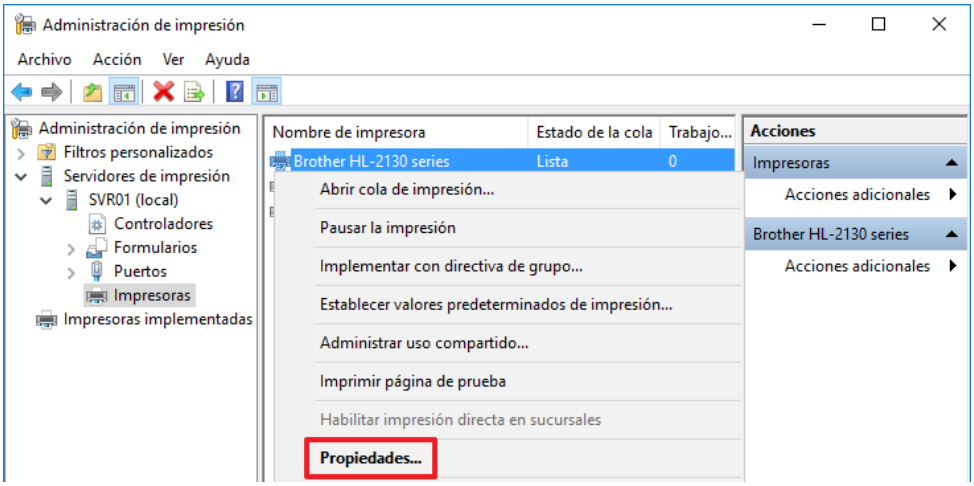
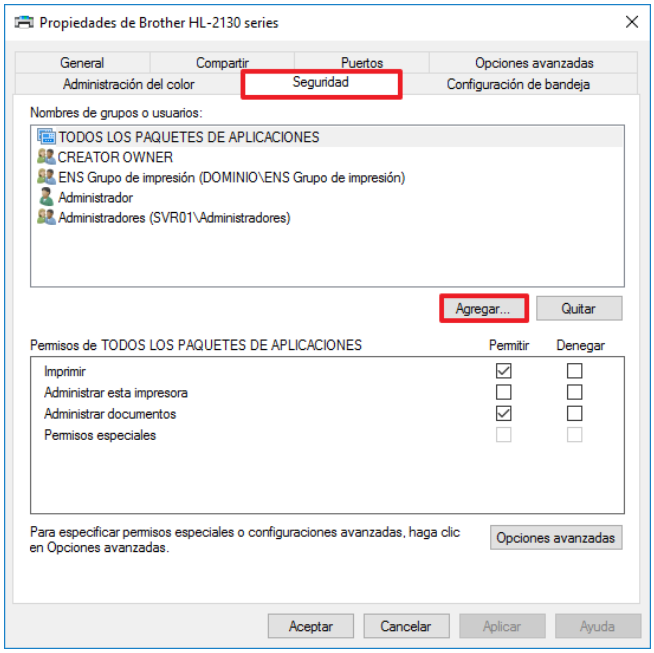
Paso	Descripción
53.	Localice el grupo que quiere añadir para que obtenga permisos para imprimir, y pulse sobre “Aceptar”.  **Nota:** En esta guía se selecciona el grupo de seguridad “ENS Grupo de impresión” al cual pertenecen los usuarios que van a obtener permiso para poder imprimir a través de los dispositivos de impresión seleccionados. Deberá adaptar este paso a los requisitos de su organización.
54.	Una vez añadido el grupo de seguridad, localice el grupo y seleccione en los permisos únicamente la opción de “Imprimir”. Pulse “Aceptar” para cerrar la ventana.  **Nota:** En este ejemplo se utiliza el grupo denominado “ENS Grupo de impresión”.
55.	Deberá repetir estos pasos para asignar permisos de impresión sobre todos los dispositivos de impresión sobre los que esté aplicando seguridad.

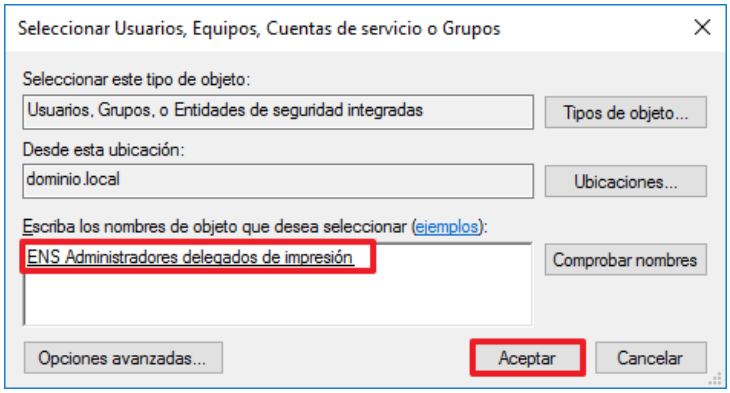
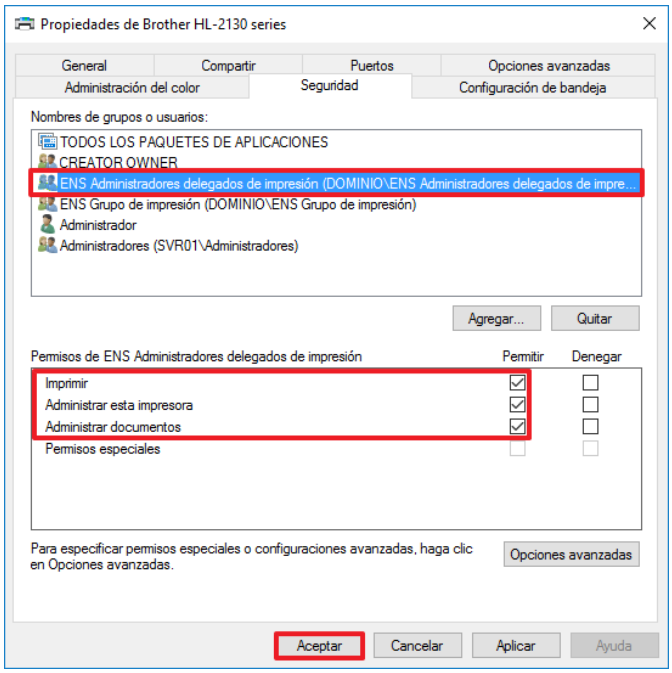
2.3. GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN

En este apartado se tendrá en consideración la gestión de permisos de administración sobre los dispositivos de impresión según lo establecido por el ENS, para con ello limitar y controlar el acceso a los dispositivos de impresión.

Paso	Descripción
56.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
57.	A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 
58.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 

Paso	Descripción
59.	Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de impresión”**. 
60.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. Para ello despliegue el nodo **“Servidores de impresión → <<nombre del servidor>> → Impresora”**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

Paso	Descripción
61.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades…”.  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.
62.	A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Agregar…”. 

Paso	Descripción
63.	Localice el grupo que quiere añadir para que obtenga permisos para poder administrar el dispositivo de impresión seleccionado, y pulse sobre el “Aceptar”.  **Nota:** En esta guía se selecciona el grupo de seguridad “ENS Administradores delegados de impresión” al cual pertenecen los usuarios que van a obtener permisos administrativos sobre los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.
64.	Una vez añadido el grupo de seguridad “Administradores delegados de impresión”, localice el grupo y seleccione los siguientes permisos. – Imprimir. – Administrar esta impresora. – Administrar documentos. Una vez establecidos los permisos, pulse “Aceptar” para confirmar los cambios y cerrar la ventana de propiedades del dispositivo de impresión. 

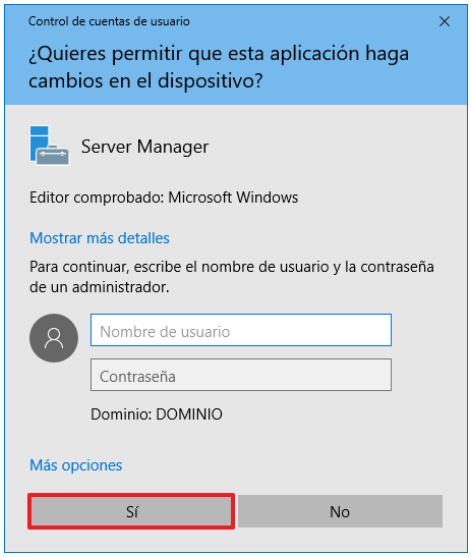
2.4. GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN

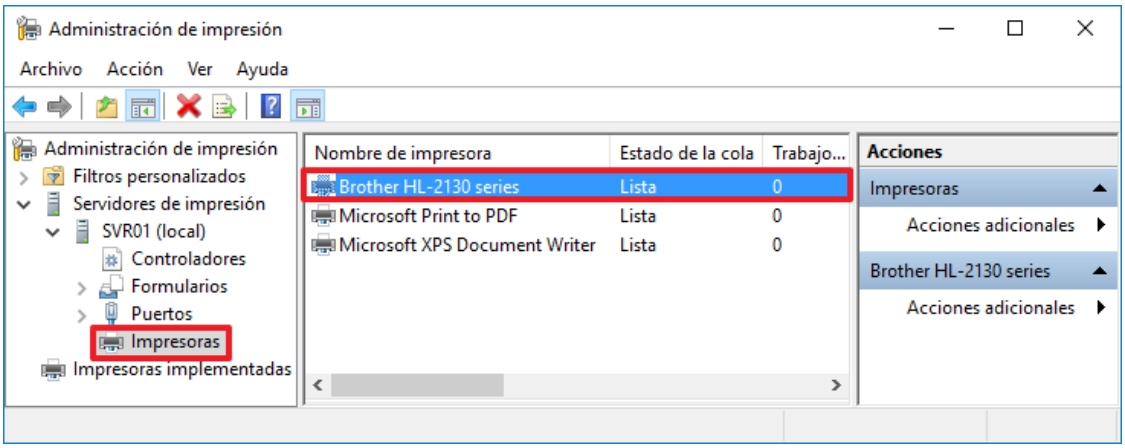
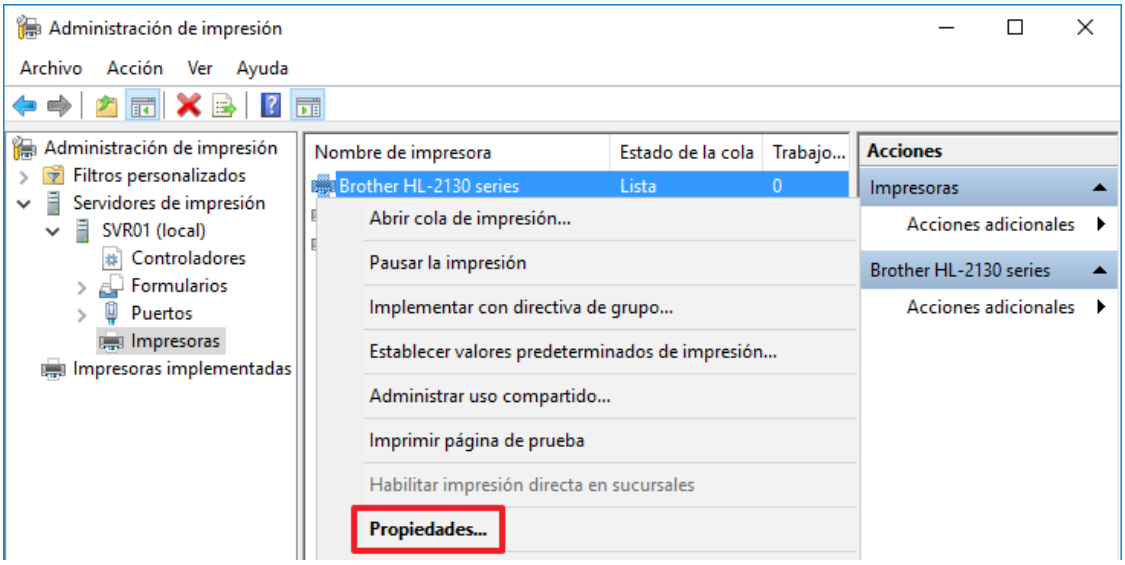
En este apartado se tendrá en consideración la habilitación de la auditoria en los dispositivos de impresión tal y como se especifica para las categorías media y alta que establece el ENS.

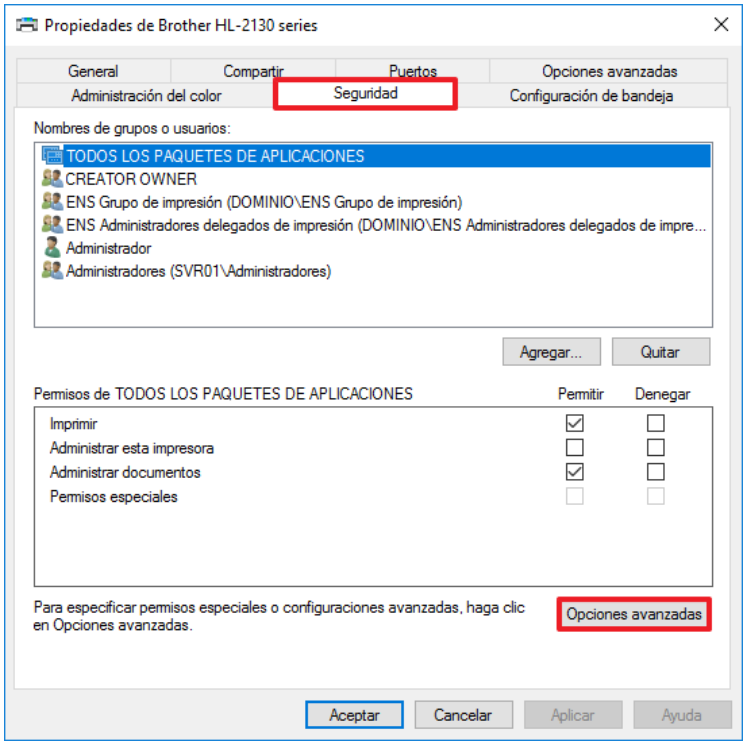
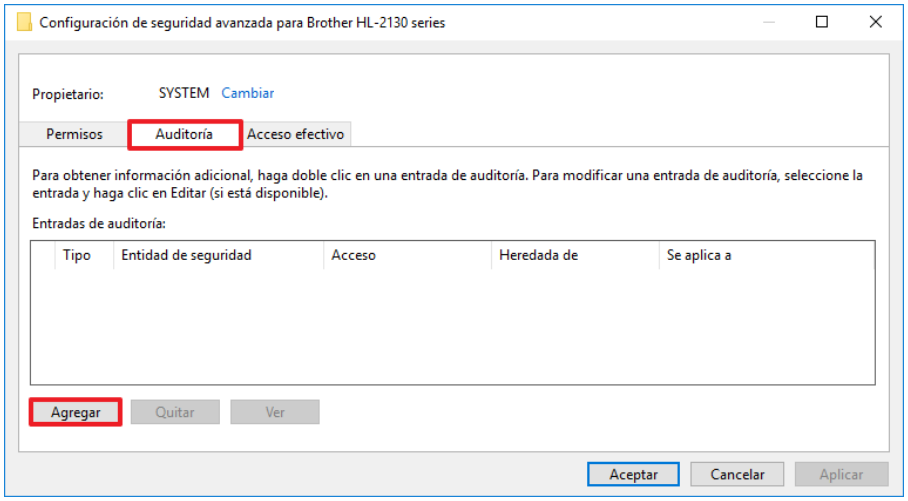
A continuación, se muestra el procedimiento para habilitar la auditoría en un dispositivo de impresión, instalado previamente, para un grupo de usuarios específicos.

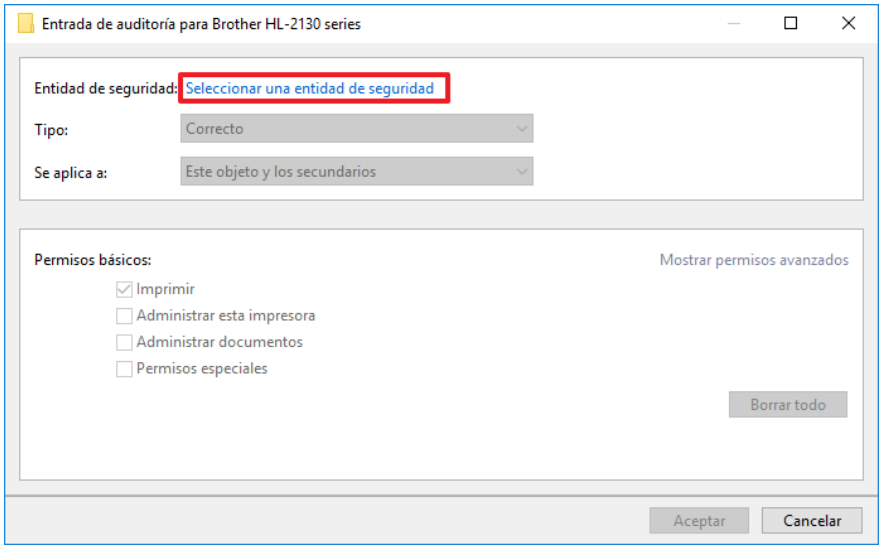
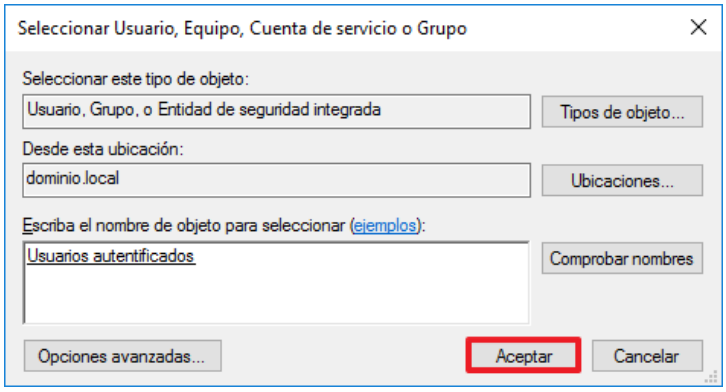
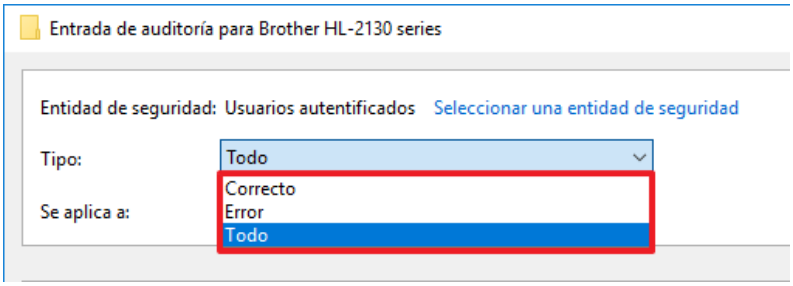
Nota: Para realizar este procedimiento se utiliza el dispositivo de impresión denominado “Brother HL-230 series”, utilizado para la creación de esta guía.

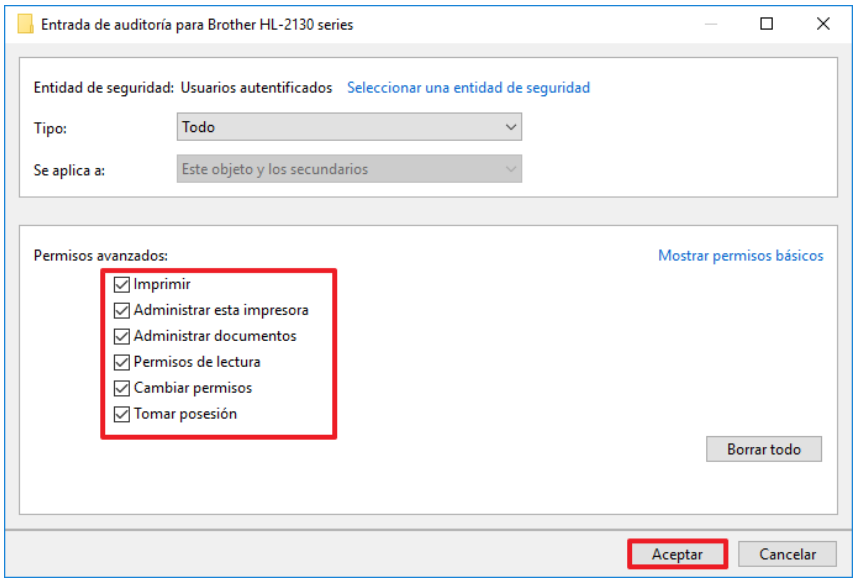
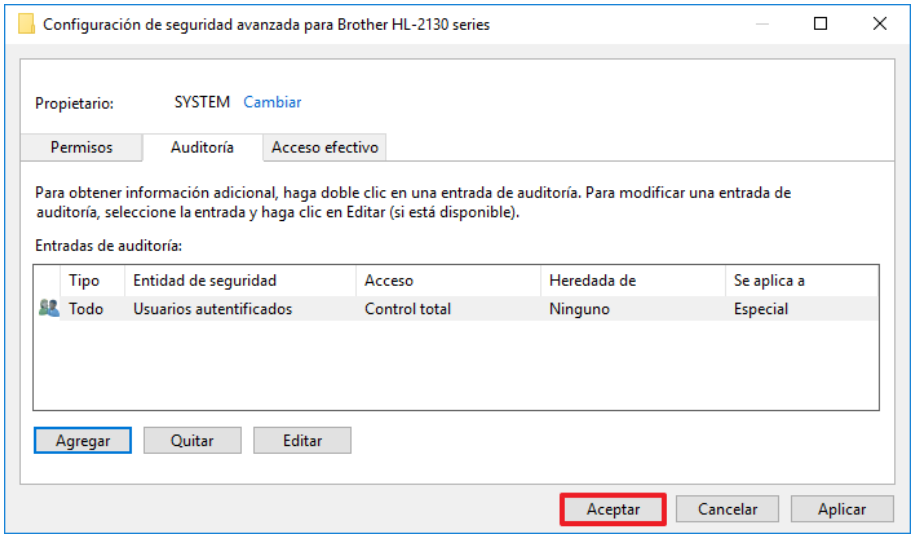
Paso	Descripción
65.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS.  **Nota:** Inicie sesión con una cuenta que sea administrador del dominio.
66.	A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. 

Paso	Descripción
67.	El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar. 
68.	Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione **“Herramientas → Administración de impresión”**. 

Paso	Descripción
69.	Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo **"Servidores de impresión → <<nombre del servidor>> → Impresora"**.  **Nota:** En este ejemplo se selecciona el dispositivo de impresión "Brother HL-2130 series", deberá adaptar los pasos a las necesidades su organización.
70.	Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción "Propiedades…".  **Nota:** En este ejemplo se utiliza el dispositivo de impresión denominado "Brother HL-2130 series".

Paso	Descripción
71.	A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Opciones avanzadas”. 
72.	Sitúese en la pestaña “Auditoría” y a continuación pulse sobre “Agregar”. 

Paso	Descripción
73.	Pulse sobre “Seleccionar una entidad de seguridad”. 
74.	Añada los grupos sobre los que desee realizar la auditoría y pulse “Aceptar”.  **Nota:** En este ejemplo se utiliza el grupo “Usuarios autentificados”.
75.	En la ventana desplegable “Tipo”, seleccione “Todo”, para que se visualicen tanto los eventos erróneos como los eventos correctos. 

Paso	Descripción
76.	En la parte derecha de la ventana, pulse sobre “Mostrar permisos avanzados” y seleccione todas las casillas de eventos auditables, tal y como se muestra en la imagen. Pulse sobre el botón “Aceptar”. 
77.	Pulse de nuevo sobre el botón “Aceptar” para cerrar la configuración de seguridad avanzada de la impresora. 
78.	Finalmente pulse “Aceptar” para cerrar la ventana de “Propiedades” de la impresora.
79.	Repita estos mismos pasos para cada uno de los dispositivos de impresión que deben ser auditados en su organización.

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN SEGURA DE SERVIDORES DE IMPRESIÓN PARA LA CATEGORÍA ALTA / DIFUSIÓN LIMITADA

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de impresión sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría alta del ENS.

Para realizar esta lista de comprobación, primero se deberá iniciar sesión en un Controlador de Dominio con una cuenta de usuario que tenga privilegios de administración en el dominio. A continuación, se realizarán las comprobaciones comunes a todos los servidores de impresión que son miembros del dominio.

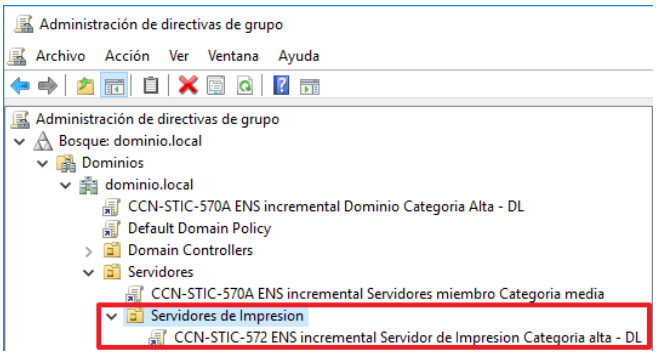
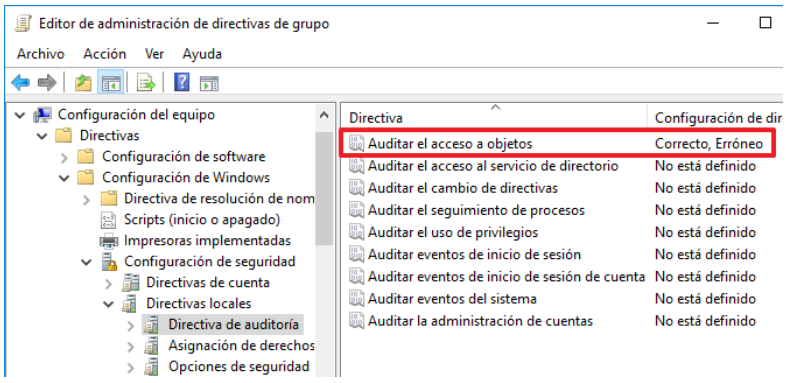
Posteriormente, se deberán realizar las comprobaciones en el propio servidor de impresión, para lo que será necesario ejecutar diferentes consolas de administración y herramientas del sistema, las cuales estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario con privilegios de administrador del dominio o administrador local del servidor. Las consolas y herramientas que se utilizarán son las siguientes:

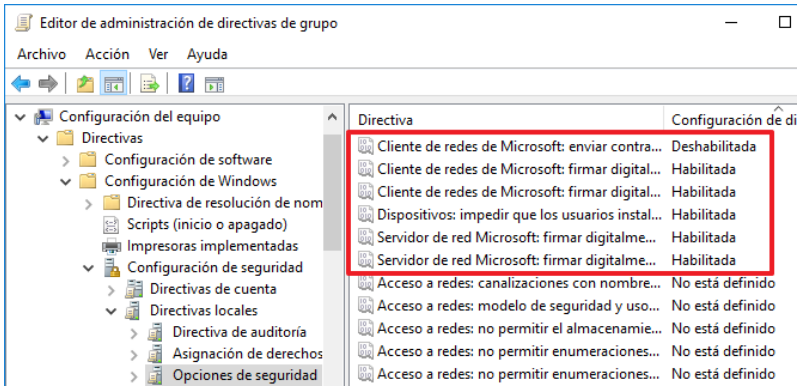
a) En el Controlador de Dominio:
   i. Usuarios y equipos de Active Directory (dsa.msc).
   ii. Administrador de directivas de grupo (gpmc.msc).
   iii. Editor de objetos de directiva de grupo (gpedit.msc).

b) En el servidor de impresión:
   i. Administrador de Windows (explorer.exe).
   ii. PowerShell (powershell.exe).
   iii. Servicios (services.msc).
   iv. Editor de objetos de directiva de grupo (gpedit.msc).
   v. Administrador de impresión (printmanagement.msc).

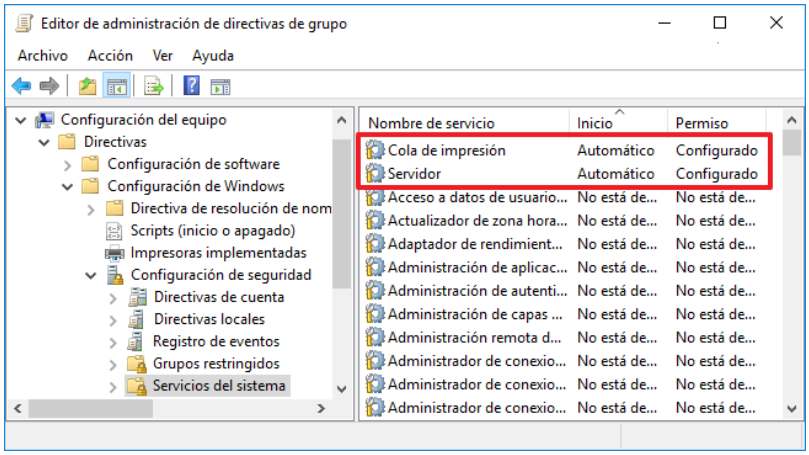
Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado durante la presente guía. Deberá adaptar los pasos según la configuración de su organización.

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

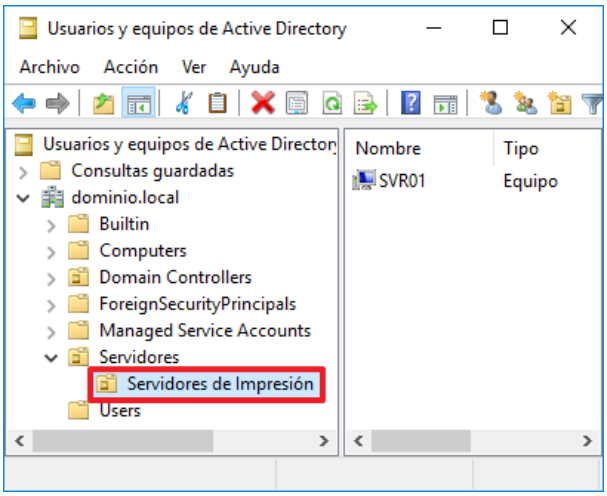
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>2. Verifique que está creada la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL”.</td><td></td><td>Utilice el Administrador de directivas de grupo (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de impresión” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL”.
 
</td></tr>
<tr><td rowspan="3">3. Verifique los valores de auditoría de la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL”.</td><td></td><td>Utilizando el editor de directiva de grupo, haga clic derecho sobre la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL” y seleccione la opción “Editar…”. Verifique que la directiva tiene los siguientes valores en las directivas de auditoría dentro de:
“Directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Directiva de auditoría”.
 
</td></tr>
<tr><td colspan="2">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr>
</table>
</td></tr>
</table>

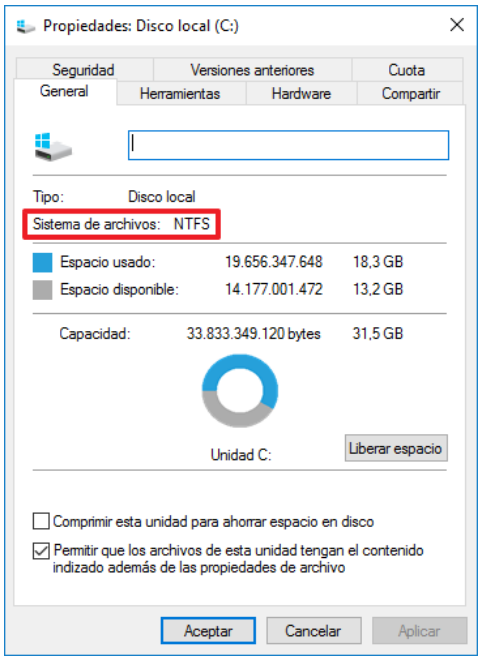
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>4. Verifique las opciones de seguridad de la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL”.</td><td></td><td>Utilizando el editor de directiva de grupo, verifique que la directiva “CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL” tiene los siguientes valores en las opciones de seguridad dentro de:
“Directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cliente de redes Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros</td><td>Deshabilitada</td><td></td></tr>
<tr><td>Cliente de redes Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Cliente de redes Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
<tr><td>Dispositivos: Impedir que los usuarios instalen controladores de impresora</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red de Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)</td><td>Habilitada</td><td></td></tr>
<tr><td>Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)</td><td>Habilitada</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL" tiene los siguientes valores de servicios de sistema dentro de: **"Directiva CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**. 

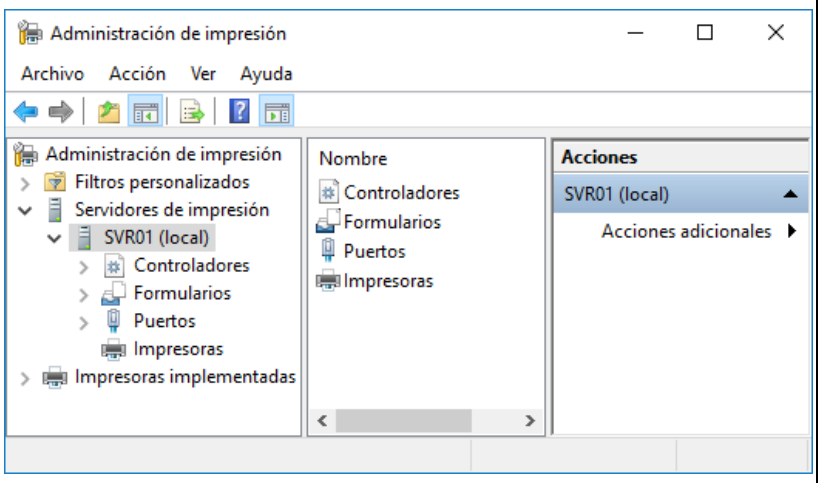
Servicio (Nombre largo)	Servicio (Nombre corto)	Inicio	Permisos	OK/NOK
Cola de impresión	Spooler	Automático		
Servidor	LanmanServer	Automático		

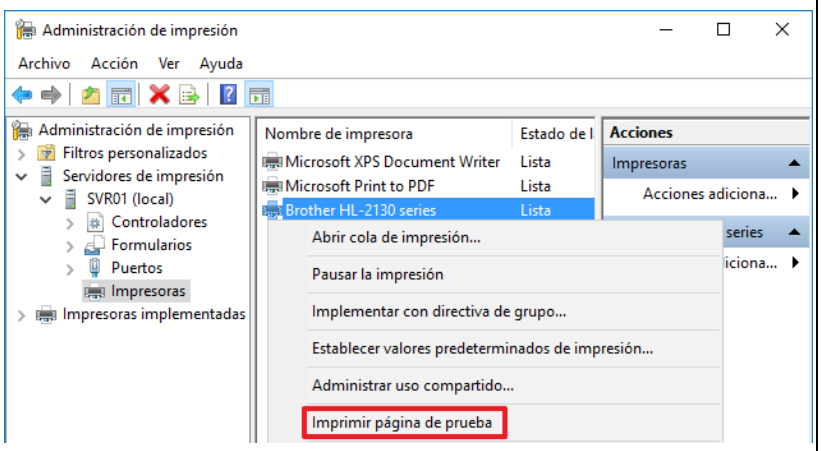
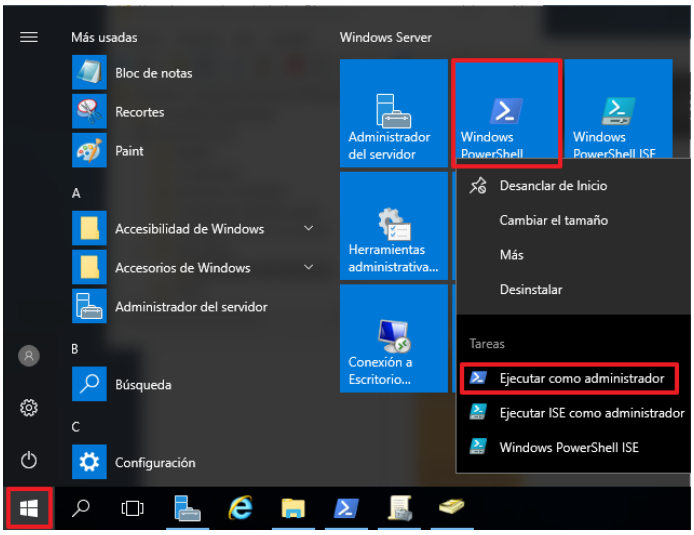
6. Verifique que el servidor de impresión está dentro de la unidad organizativa "Servidores de impresión".		Utilice la herramienta Usuarios y equipos de Active Directory (**Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**) y seleccione la unidad organizativa "Servidores de impresión". Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de impresión que se están asegurando. 

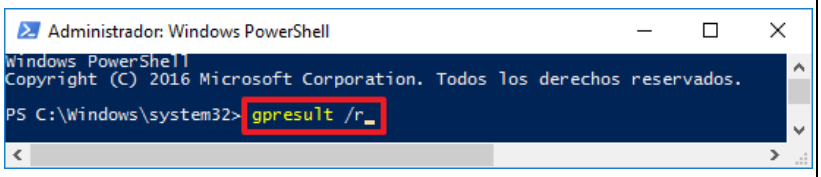
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>7. Inicie sesión en el servidor de impresión.</td><td></td><td>Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.</td></tr>
<tr><td>8. Verifique que todos los volúmenes están formateados con NTFS.</td><td></td><td>Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL’s.
 
</td></tr>
<tr><td rowspan="3">9. Verifique que están instalados los componentes que se indican.</td><td></td><td>En el “Administrador del Servidor”, pulse sobre la opción “Servidor Local” del menú de la izquierda y diríjase a la parte final de la ventana principal, “Roles y características”, por medio del scroll lateral derecho.</td></tr>
<tr><td colspan="2"><table>
<tr><th>Rol</th><th>OK/NOK</th></tr>
<tr><td>Servicios de impresión y documentos</td><td></td></tr>
<tr><td>Servidor de impresión</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique que los servicios del sistema relacionados con el servidor de impresión están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre **Inicio → Ejecutar**) y compruebe el tipo de inicio de los servicios.

Servicio (Nombre largo)	Servicio (Nombre corto)	Inicio	Permisos	OK/NOK
Cola de impresión	Spooler	Automático		
Servidor	LanmanServer	Automático		

11. Verifique que la instalación del servidor de impresión se ha realizado correctamente.		Utilizando la herramienta de administración de impresión (ejecutando "printmanagement.msc" desde, botón derecho sobre **Inicio → Ejecutar**), verifique que la consola se inicia y presenta el servidor local como un servidor de impresión.  **Nota:** En esta comprobación, el servidor se denomina "SVR01". En su organización debe comprobar que aparece el nombre del servidor de impresión que está implementando.

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.		Utilizando la herramienta de administración de impresión (ejecutando "printmanagement.msc" desde, botón derecho sobre **Inicio → Ejecutar**), verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión. Para ello, seleccione cada una de las impresoras que aparecen en el nodo "Impresoras" con el botón derecho del ratón y pulse sobre la opción "Imprimir página de prueba". 
13. Inicie la consola de PowerShell.		Ejecute la consola de PowerShell. Para ello pulse "Inicio",.seleccione "Powershell" con el botón derecho y pulse sobre "Ejecutar como administrador". 

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se están aplicando las GPOs correspondientes ejecutando el comando “gpresult /r”. 
15. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se aplican las siguientes GPOs. – CCN-STIC-572 ENS incremental Servidor de Impresion Categoria alta - DL. – CCN-STIC-570A ENS incremental Servidores miembro Categoria alta - DL. – CCN-STIC-570A ENS incremental Dominio Categoria alta - DL.