centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 683

IMPLEMENTACIÓN DEL ENS EN CITRIX VIRTUAL APPS AND DESKTOPS SOBRE MICROSOFT WINDOWS SERVER 2016

FEBRERO 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

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

NIPO: 083-20-089-7

Fecha de Edición: febrero de 2020
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Febrero de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE CITRIX VIRTUAL APPS AND DESKTOPS EN EL ENS

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE CITRIX VIRTUAL APPS AND DESKTOPS

1. APLICACIÓN DE MEDIDAS EN CITRIX VIRTUAL APPS AND DESKTOPS

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de Citrix Virtual Apps and Desktops sobre servidores con Microsoft Windows Server 2016 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".

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

a) Aplicación de seguridad en el entorno de Citrix Virtual Apps and Desktops sobre Microsoft Windows Server 2016. Será, además, el mecanismo empleado para conducir la centralización y gestión de la seguridad.

b) Aplicación de seguridad en el entorno de Internet Information Services 10 sobre Microsoft Windows Server 2016 que pueda dar soporte a la organización y sobre el que se asientan muchos de los activos tecnológicos de dicha organización.

c) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestará la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows Server 2016 implementados siguiendo la guía CCN-STIC-570A – Implementación del ENS en Windows Server 2016.

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 aportan tanto Citrix para el producto Citrix Virtual Apps and Desktops como Microsoft para Internet Information Services 10, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema o al propio Directorio Activo, como la asignación de permisos para la segregación de roles y funciones.

Esta guía, por tanto, no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean nativas al sistema operativo o las funcionalidades que el propio rol pueda aportar. Por ejemplo, aunque es condición indispensable la implementación de un antivirus en los servidores, se establece que esta medida atiende a un criterio general de la organización y que, no siendo algo que pueda aportar el propio sistema operativo, se encontrará excluido del análisis e implementación.

Para un mejor entendimiento de las medidas, éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a 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 las diferentes categorías 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 a la categoría exigida. 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. 1. IDENTIFICACIÓN

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

Las limitaciones de acceso a los servicios se establecerán basándose en los métodos de identificación disponibles según el contenido al que se quiera acceder.

Debe tenerse en consideración que los requisitos para la identificación en un servidor serán gradualmente incrementados en cuanto a su robustez, según se eleve el nivel de seguridad en función de la categoría establecida por el ENS.

Dentro de las guías de paso a paso se sugerirán los mecanismos de identificación más adecuados a cada una de las categorías de seguridad contempladas por el ENS.

La identificación de cada usuario se traduce en la necesidad de crear cuentas con un identificador único e inequívoco para cada usuario y servicio.

Nunca deberán existir dos cuentas iguales, de forma que éstas no puedan confundirse o bien imputarse acciones a usuarios diferentes al que haya realizado la acción a auditar.

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.

Dichos procesos de segregación son factibles realizarlos a través de los propios mecanismos que proporciona Microsoft Windows Server 2016. Conforme a las necesidades planteadas en los dos primeros elementos, desarrollo de operaciones y la configuración, así como el mantenimiento del sistema de operación, el operador deberá tomar en consideración lo establecido en la última revisión de la guía “CCN-STIC-570A”. En dicho documento, además de otras cuestiones relativas a mejoras en la seguridad y procesos, se recogen los procedimientos que pueden ser llevados a cabo para la segregación de tareas, de tal forma que se pueden conceder determinados privilegios a usuarios concretos sin necesidad de facultarles de derechos completos.

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura y puesta en marcha de la guía “CCN-STIC-859 de recolección y consolidación de eventos” que aun habiendo sido emitida para Windows Server 2008 R2 es igualmente aplicable a sistemas Windows Server 2016. Aunque será mencionada a lo largo de la presente guía, con relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en Windows Server 2016 y sus servicios, a través del sistema de Suscripción de eventos con el que Microsoft ya dotó a Windows Server 2008.

Así mismo es importante la creación de grupos con el objetivo de establecer los permisos a través de dichos grupos, permitiendo una gestión global y sencilla sobre el acceso a los recursos que ofrece Citrix Virtual Apps and Desktops. De este modo se evita modificar los permisos individuales de cada usuario para conceder o no permisos sobre un mismo recurso.

A través de los mecanismos que proporciona Citrix Virtual Apps and Desktops es posible la definición de usuarios y grupos de directorio activo a los que se les permita la administración y/o realización de diversas tareas sobre la infraestructura.

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

Este proceso requiere consolidación de los derechos de acceso, de tal forma que:

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

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

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

Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

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

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

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

Se deberá tener en consideración debido a dicha norma que los permisos otorgados a los usuarios serán los mínimos requeridos no siendo necesario que estos posean permisos adicionales para la tarea que van a realizar. Por ejemplo, si un usuario tiene permiso para alterar el contenido de una carpeta no por ello implica que sea necesario que posea el permiso de “Control total”. Con la concesión de este permiso se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de modificar se debe considerar como la opción más óptima desde el punto de vista del ENS. Este mismo ejemplo es aplicable a Citrix Virtual Apps and Desktops ya que un usuario puede tener permisos sobre la entrega de un catálogo de máquinas, pero no sobre la gestión de los permisos de entrega de aplicaciones.

1.1.1.4. OP. ACC. 7. ACCESO REMOTO

La organización deberá mantener las consideraciones de seguridad, en cuanto al acceso remoto, cuando éstas se realicen fuera de las propias instalaciones de la organización y a través de redes de terceros.

Éstas deberán también garantizar la seguridad, tanto en el propio acceso en sí, como en el canal del acceso remoto.

Citrix Virtual Apps and Desktops faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible.

Para que el servidor web acepte las conexiones HTTPS se debe haber creado previamente un certificado de clave pública, dicho certificado debe estar firmado por una autoridad de certificación para que el navegador lo acepte.

1.1.1.5. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que Citrix Virtual Apps and Desktops debe configurarse previamente a su entrada en producción teniendo en cuenta las siguientes directrices:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

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

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

Adicionalmente se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición de la información manejada, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores. Debe valorarse la información remitida al fabricante en función de los acuerdos de soporte establecidos con el mismo y/o las normativas de seguridad internas referidas a la transmisión de datos a Internet.

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

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

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

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

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

1.1.1.7. OP. EXP. 5. GESTIÓN DE CAMBIOS

Para las categorías media y alta de seguridad se mantendrá un control continuo de los cambios realizados en el sistema, por lo que, todos los cambios anunciados por el proveedor o fabricante 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 nivel alto deberán ser aprobados explícitamente de forma previa a su implantación.

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

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

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

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

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

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

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

Citrix Virtual Apps and Desktops, implementa mecanismos para la auditoría de acceso a objetos y acciones realizadas dentro del propio servicio. El problema consiste en que de forma predeterminada los datos son almacenados localmente. Existen no obstante mecanismos nativos para la suscripción y recolección de evento. Ya comentado previamente, la guía CCN STIC-859 de recolección y consolidación de eventos con Windows 2008 R2 permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoria desde múltiples sistemas, permitiendo establecer así mecanismos de correlación.

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

Nuevamente, en las categorías altas se deberán implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:

a) Determinar el período de retención de los registros.

b) Asegurar fecha y hora del registro de la actividad.

c) Permitir el mantenimiento de los registros, sin que estos puedan ser alterados o eliminados por personal no autorizado, evitando la modificación accidental de los registros.

d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

Citrix Virtual Apps and Desktops, guardará los cambios administrativos durante un periodo de tiempo determinado en función del tipo de licenciamiento con el que cuente su organización, por ejemplo, para un licenciamiento Premium el tiempo de retención de registros y eventos administrativos asciende a un año.

Nuevamente, en la guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2, se articulan los mecanismos para garantizar la disponibilidad y retención de los registros, así como los procedimientos operativos para su salvaguarda.

1.2. MEDIDAS DE PROTECCIÓN

1.2.1. PROTECCIÓN DE LAS COMUNICACIONES

El conjunto de medidas orientadas a la protección de las comunicaciones tiene como objetivo proteger la información en tránsito, así como dotar a los mecanismos para la detección y bloqueo de intrusos en una red.

Aunque fundamentalmente tienen un alcance mayor en cuanto a la implementación de sistemas de electrónica de red y control perimetral, determinadas medidas pueden ser aplicables y gestionadas desde el propio servidor.

El Real Decreto 3/2010 de 8 de enero, de desarrollo del Esquema Nacional de Seguridad 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 por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

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

Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos.

Se establecerá una prevención activa de ataques garantizando, como mínimo, que estos sean detectados, y se procederá a activar los procedimientos previstos en el tratamiento de incidentes de los cuales se consideran ataques activos los siguientes supuestos:

a) La alteración de la información en el tránsito de la comunicación.

b) La inyección de información ilegitima en la comunicación con un fin fraudulento.

c) El secuestro de una sesión por una tercera parte.

En el caso de ser necesario asegurar la confidencialidad de las comunicaciones Web, es necesario hacer uso de la versión segura del protocolo, HTTPS. HTTPS utiliza SSL (Secure Socket Layer) o TLS (Transport Layer Security) para cifrar las comunicaciones entre el navegador Web y el servidor Web.

La gestión de sesiones en la aplicación Web debe realizarse empleando identificadores de sesión o tokens no predecibles, de suficiente longitud para que no puedan ser resueltos mediante técnicas de fuerza bruta, y que caduquen tras cierto tiempo.

Se deberán aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma de la aplicación Web: software de los dispositivos de red y firewalls, sistema operativo de los servidores (Web, aplicación, y base de datos), y software de la plataforma de desarrollo empleada (PHP, ASP, Java, etc).

Desde el punto de vista de la infraestructura Web, se debe disponer de un análisis detallado del usuario, grupo, permisos y derechos con los que ejecutarán cada uno de los componentes de la aplicación Web como, por ejemplo, los procesos del servidor Web o de aplicación. Este análisis permitirá aplicar todos los mecanismos de autorización necesarios.

Las cabeceras HTTP pueden ser manipuladas fácilmente por un atacante y no deben emplearse como método de validación o de envío de información. 60. Todos los mecanismos de interacción entre los distintos componentes del entorno Web (servidor Web, de aplicación y base de datos) deben realizarse de forma segura. Las comunicaciones entre estos elementos deberán estar cifradas, autentificadas y asegurarse su integridad.

Adicionalmente a los elementos de seguridad propios de un entorno Web, es necesario proteger todos los elementos de la infraestructura en la que reside la aplicación Web, tales como dispositivos de comunicaciones (routers, switches, etc) o la infraestructura de servidores de nombres (DNS).

1.2.2. PROTECCIÓN DE LOS SERVICIOS

1.2.2.1. MP. S. 2. PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.

a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:
   i. Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
   ii. Se prevendrán ataques de manipulación de URL.
   iii. Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies".
   iv. Se prevendrán ataques de inyección de código.
b) Se prevendrán intentos de escalado de privilegios.
c) Se prevendrán ataques de "cross site scripting".
d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "proxies" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "cachés".

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN CITRIX VIRTUAL APPS AND DESKTOPS

A continuación, se establece un cuadro resumen con las diferentes medidas a aplicar, así como los mecanismos que se implementarán para su aplicación. Dichas implementaciones podrán provenir de la revisión de otras guías de seguridad de la serie CCN-STIC-500, de la serie CCN-STIC-800 o bien la aplicación de políticas de seguridad a nivel de dominio o bien localmente.

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Identificación	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización. Aplicación de medidas asociadas a la guía CCN-STIC-570A.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
OP. EXP. 3	Gestión de la configuración	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
OP. EXP. 5	Gestión de cambios	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de guía CCN-STIC-683, 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.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación y de la integridad	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.
MP. S. 2	Protección de servicios y aplicaciones web	Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización.

ANEXO A.2. CATEGORÍA BÁSICA

ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD PARA CITRIX VIRTUAL APPS AND DESKTOPS EN SERVIDORES MIEMBROS DEL DOMINIO SOBRE MICROSOFT SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que asegurar Citrix Virtual Apps and Desktops sobre Microsoft Windows Server 2016 con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

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

1. PREPARACIÓN DEL DOMINIO

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que van a pertenecer cada uno de los roles de la infraestructura sobre los que implementará las configuraciones de seguridad. Los pasos descritos a continuación solo los debe realizar cuando vaya a realizar la primera implementación de seguridad en el dominio, ya que solo es necesario crear las unidades organizativas, modificar las plantillas de seguridad e incorporarlas en la directiva de grupo una única vez por dominio.

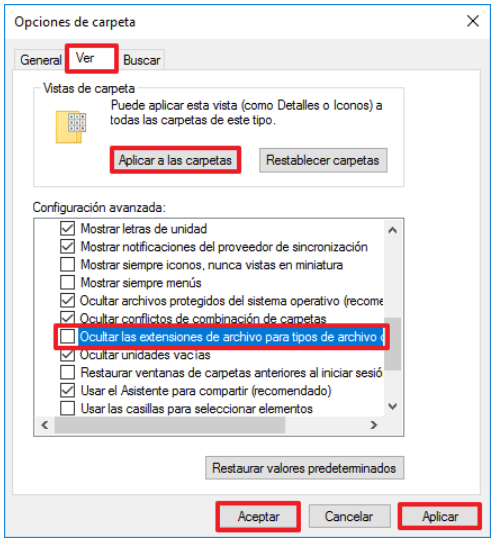
Se asume que ha realizado la implementación de las siguientes guías de seguridad sobre el servidor controlador de dominio donde se va a aplicar el siguiente paso a paso:

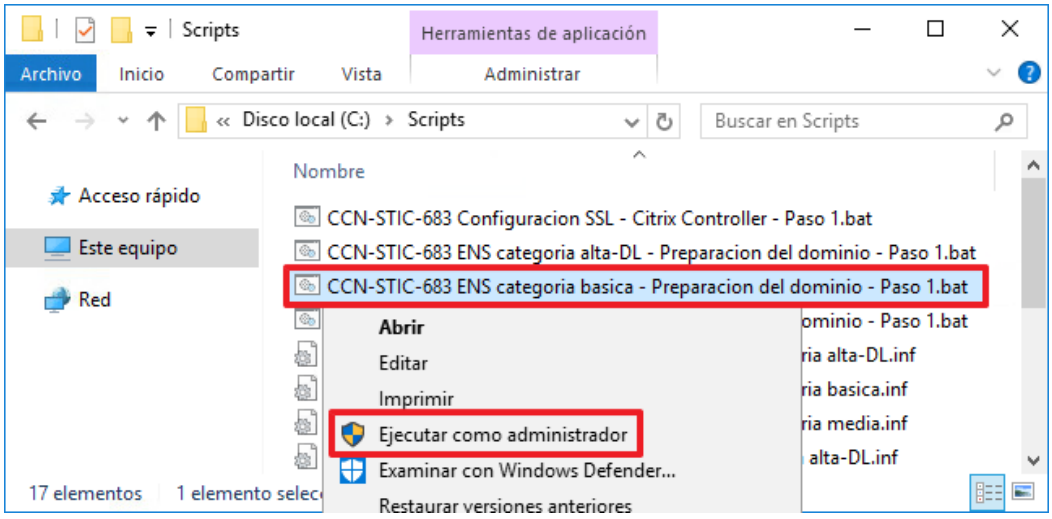
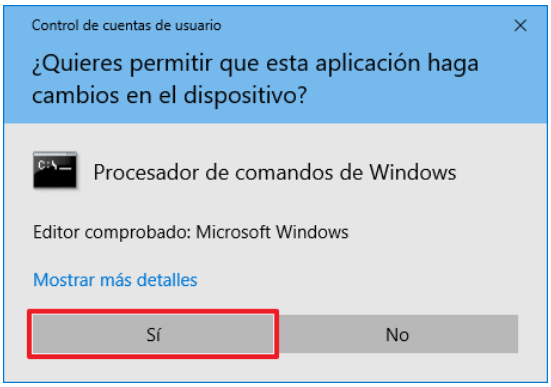
a) CCN-STIC-570A Anexo A Controlador de dominio – Categoría Básica.

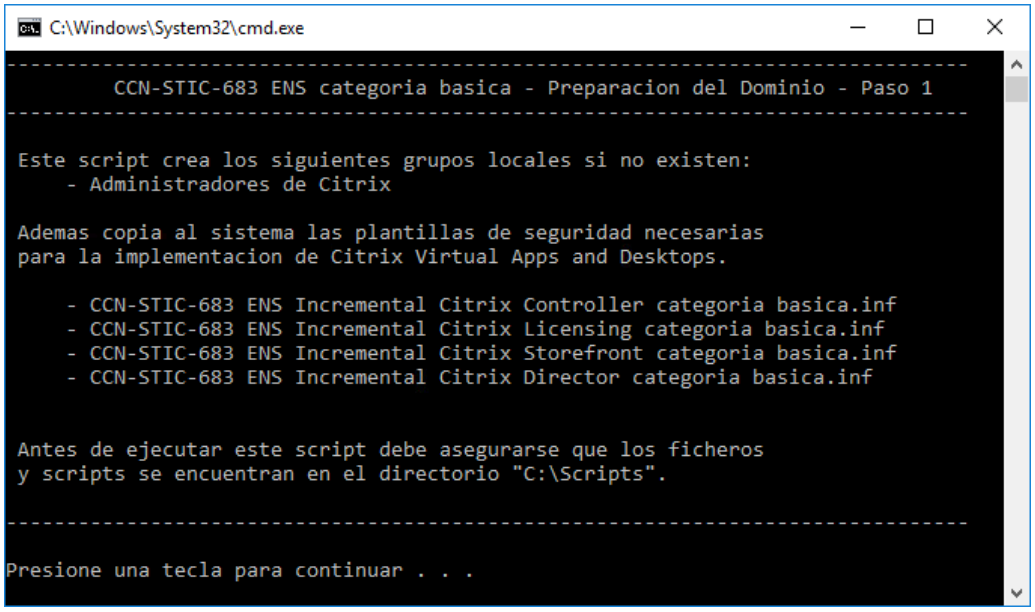
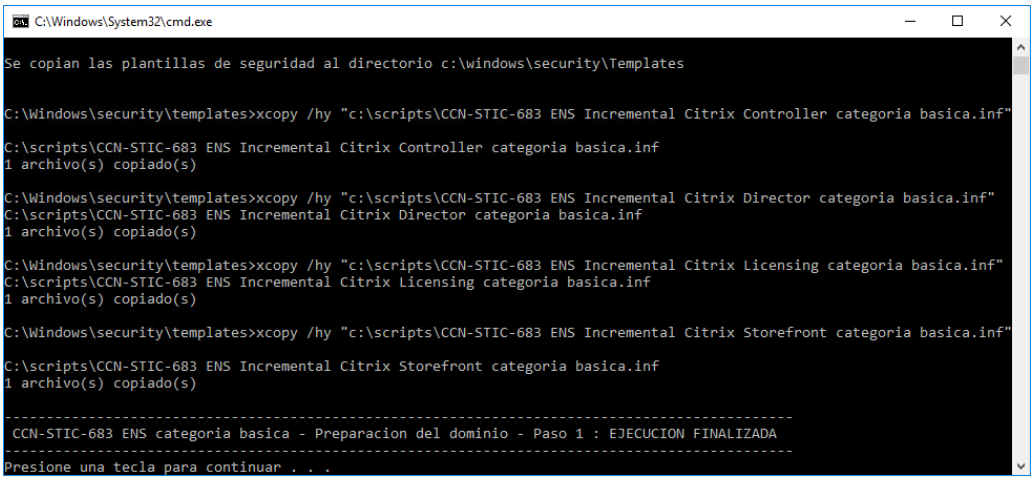
b) CCN-STIC-575 Anexo A Microsoft SQL server 2016 – Categoría Básica.

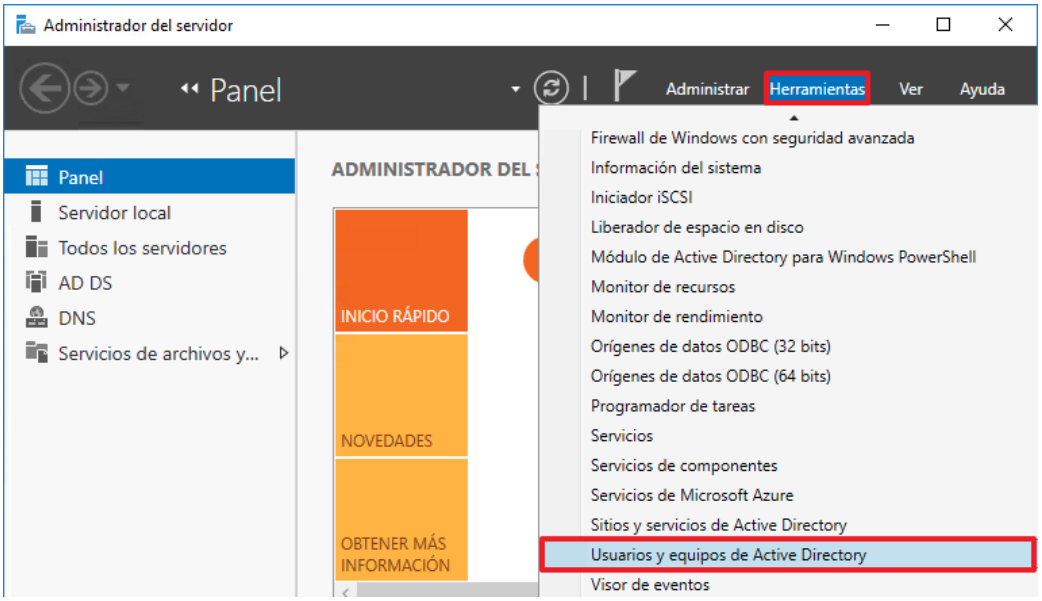
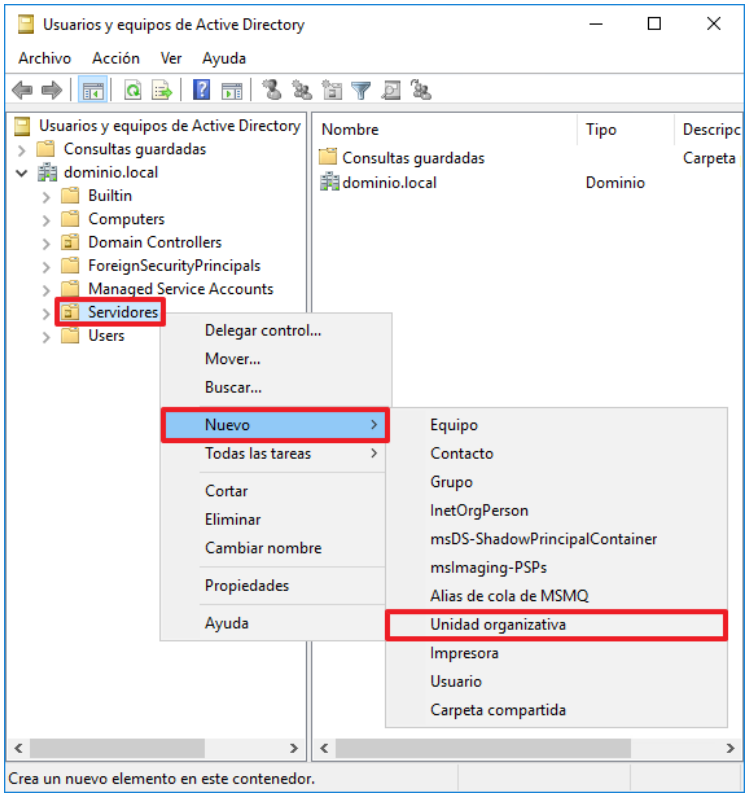
c) CCN-STIC-574 Anexo A Internet Information Services 10 – Categoría Básica.

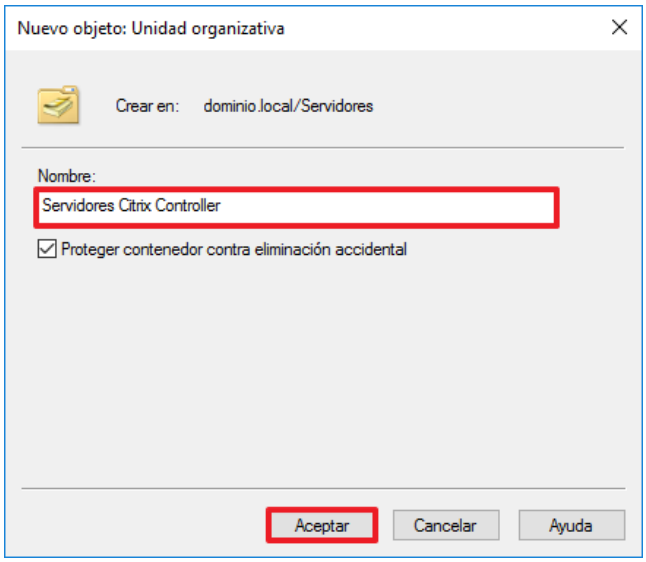
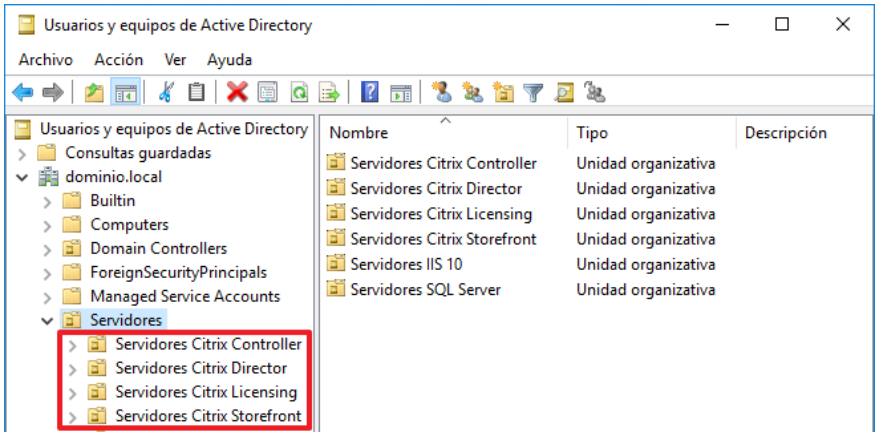
Nota: Las guías “CCN-STIC-575” y “CCN-STIC-574” deberán aplicarse en este servidor exclusivamente su apartado correspondiente al controlador de dominio.

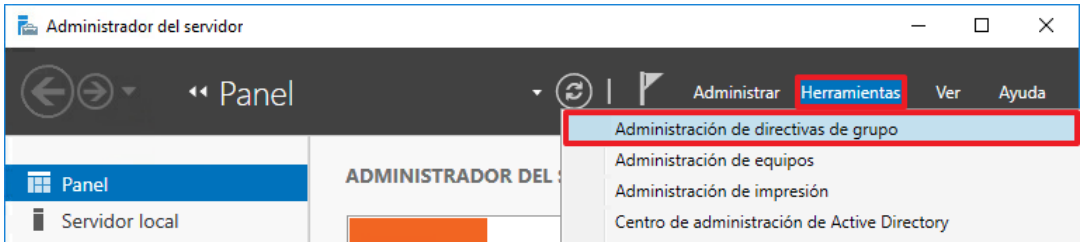
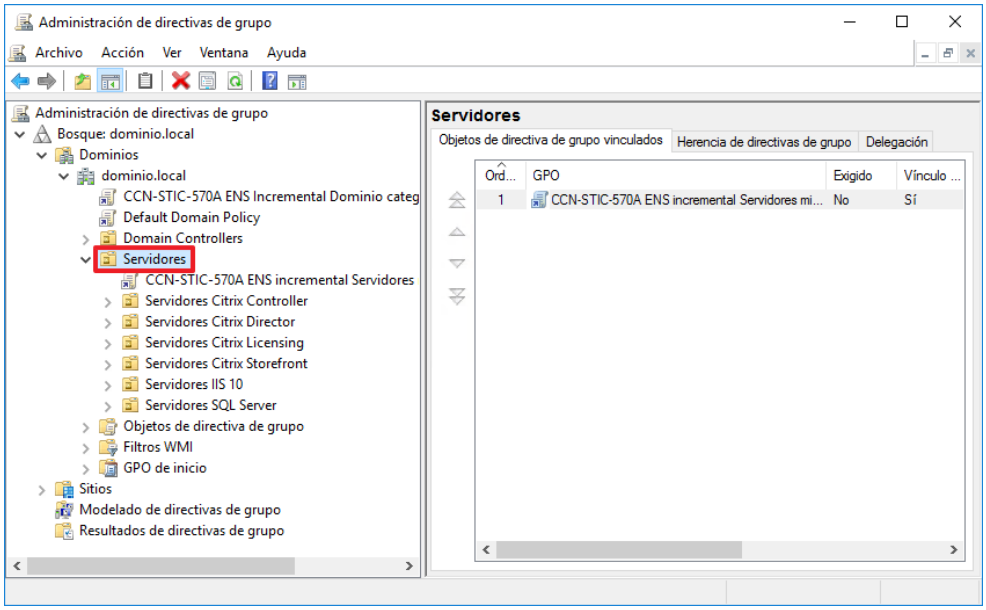
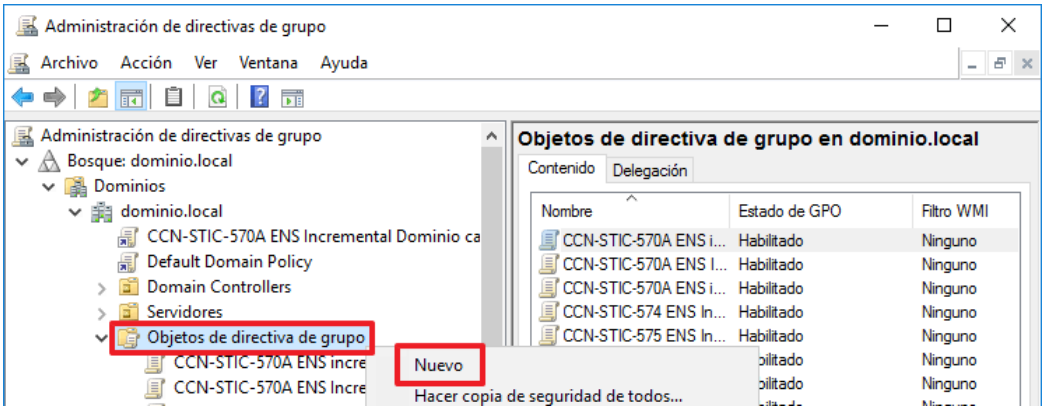
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los ficheros y directorios que acompañan a esta guía, al 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. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

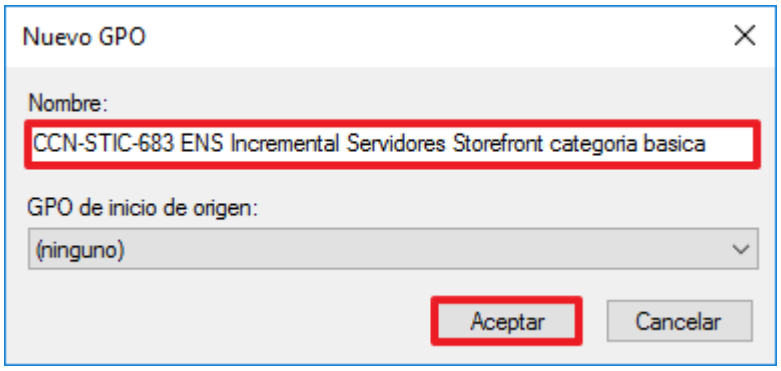
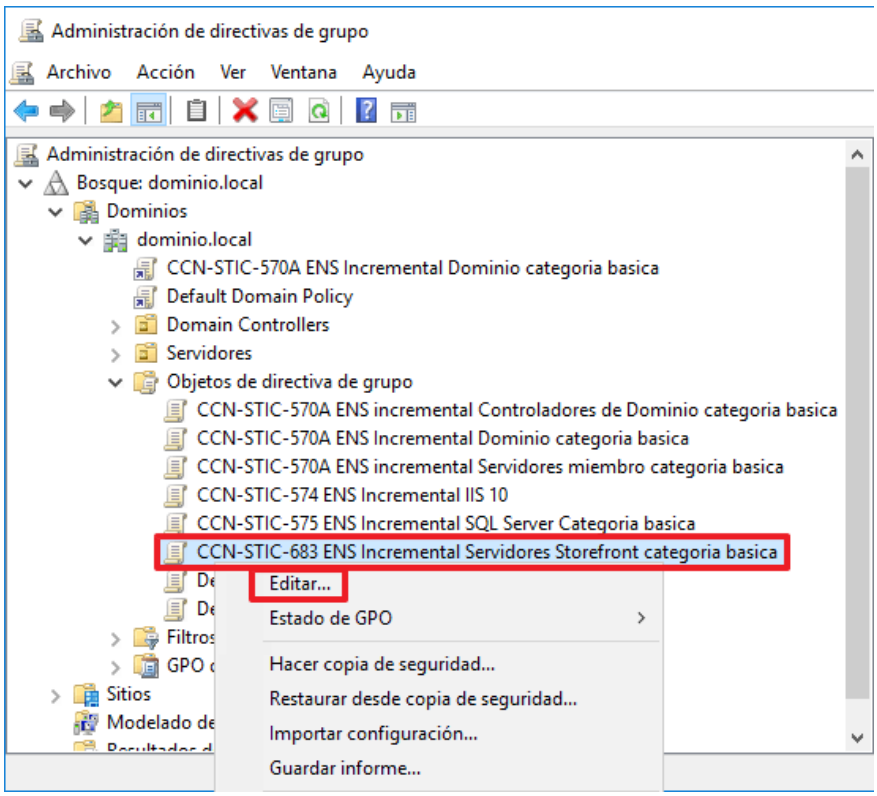
Paso	Descripción
5.	Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-683 ENS categoria basica - Preparacion del dominio - Paso 1.bat – CCN-STIC-683 ENS Incremental Citrix Controller categoria basica.inf – CCN-STIC-683 ENS Incremental Citrix Director categoria basica.inf – CCN-STIC-683 ENS Incremental Citrix Licensing categoria basica.inf – CCN-STIC-683 ENS Incremental Citrix Storefront categoria basica.inf
6.	Ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-683 ENS categoria basica - Preparacion del dominio – Paso 1.bat". Para ello, visualice la carpeta "C:\Scripts" en el Explorador de Windows, marque con el botón derecho el script y seleccione la opción **"Ejecutar como administrador"** del menú contextual, como se muestra en la siguiente figura.  **Nota:** Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
7.	El sistema solicitará elevación de privilegios, pulse "Si" para continuar. 

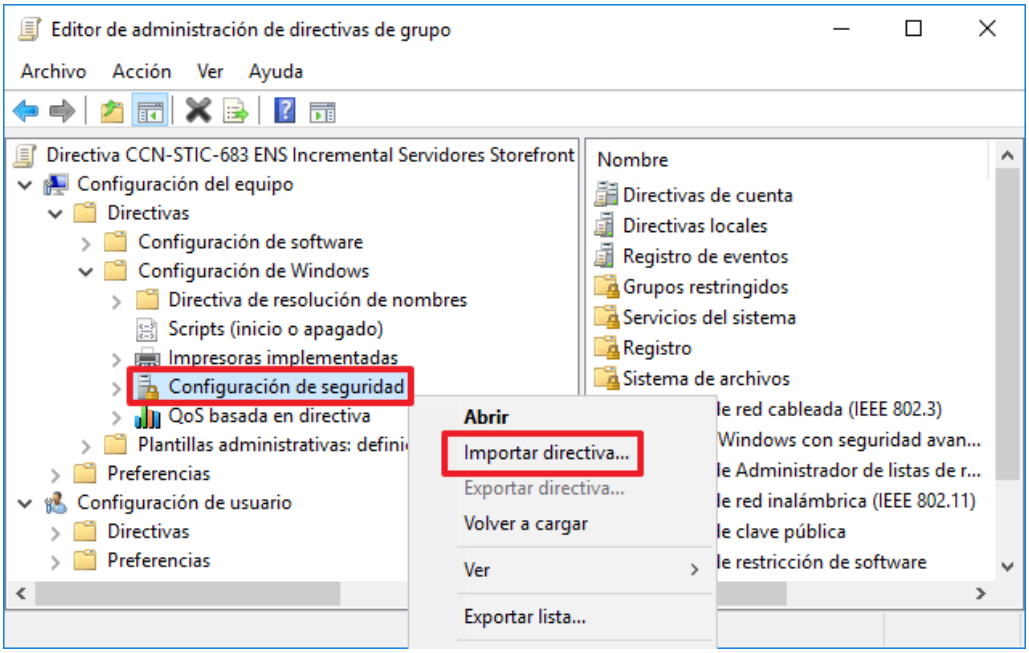
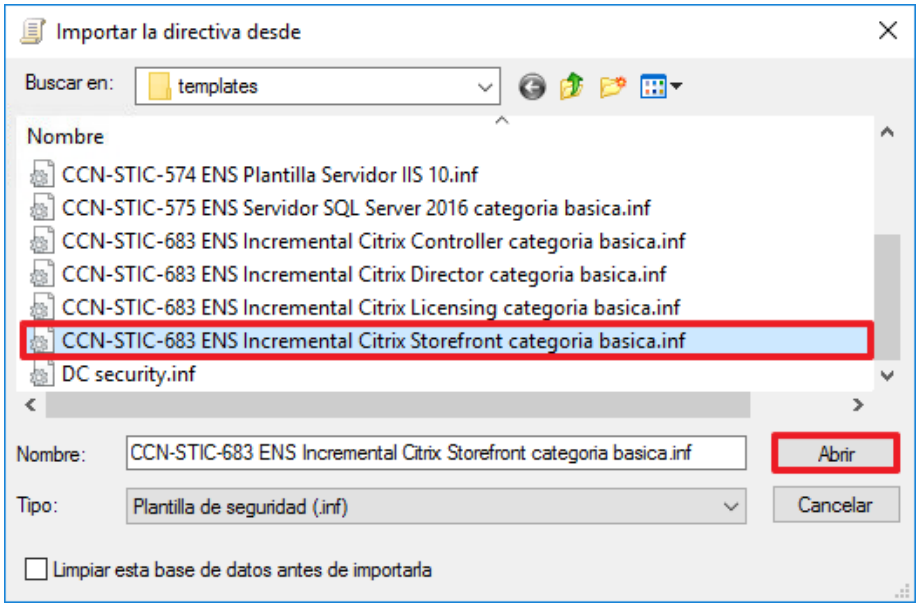
Paso	Descripción
8.	Se lanzará una ventana del intérprete de comandos “cmd.exe” como la mostrada en la siguiente figura. Este script copia todas las plantillas de seguridad a la ubicación “C:\Windows\security\templates” y crea el grupo de seguridad “Administradores de Citrix” en caso de que este no exista. 
9.	Pulse una tecla al finalizar la ejecución del script para cerrar la ventana. 

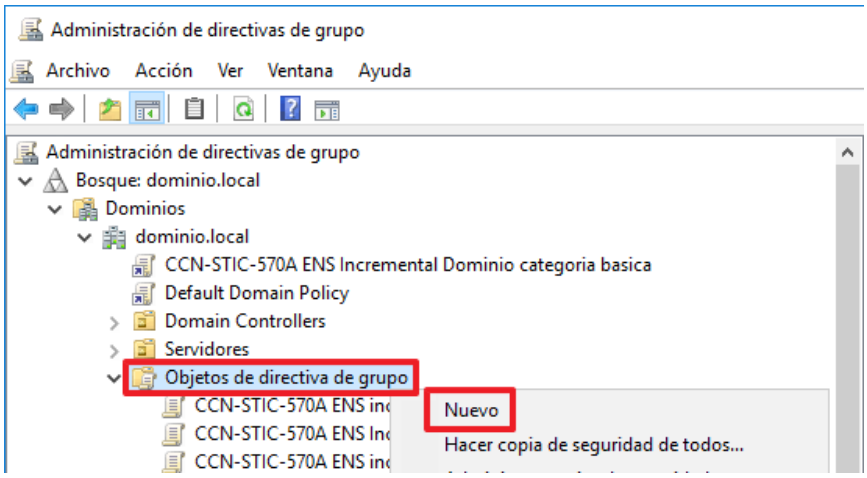
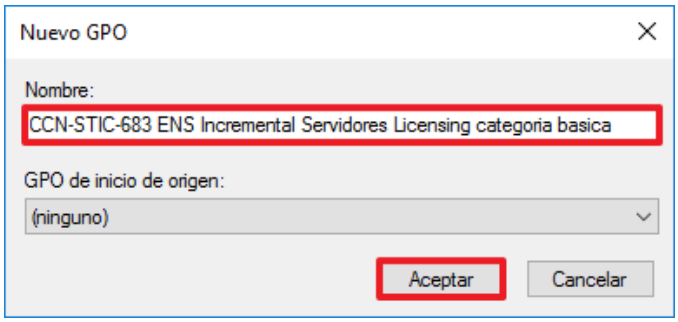
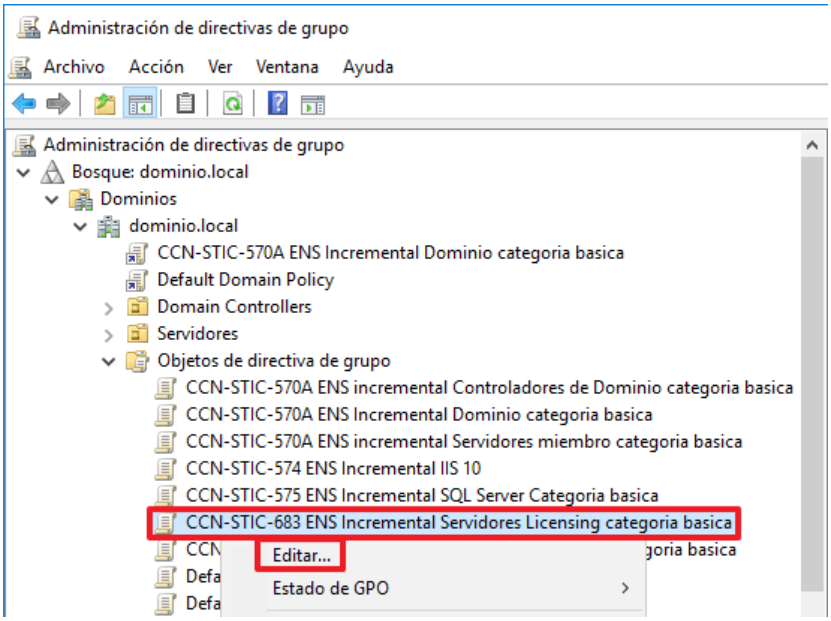
Paso	Descripción
10.	Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios. 
11.	A continuación, en la herramienta "Usuarios y equipos de Active Directory" expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio>" → Servidores"**, y marcándolo con el botón derecho del ratón, seleccione la opción **"Nuevo → Unidad organizativa"** del menú contextual que aparecerá, como se muestra en la siguiente figura. 

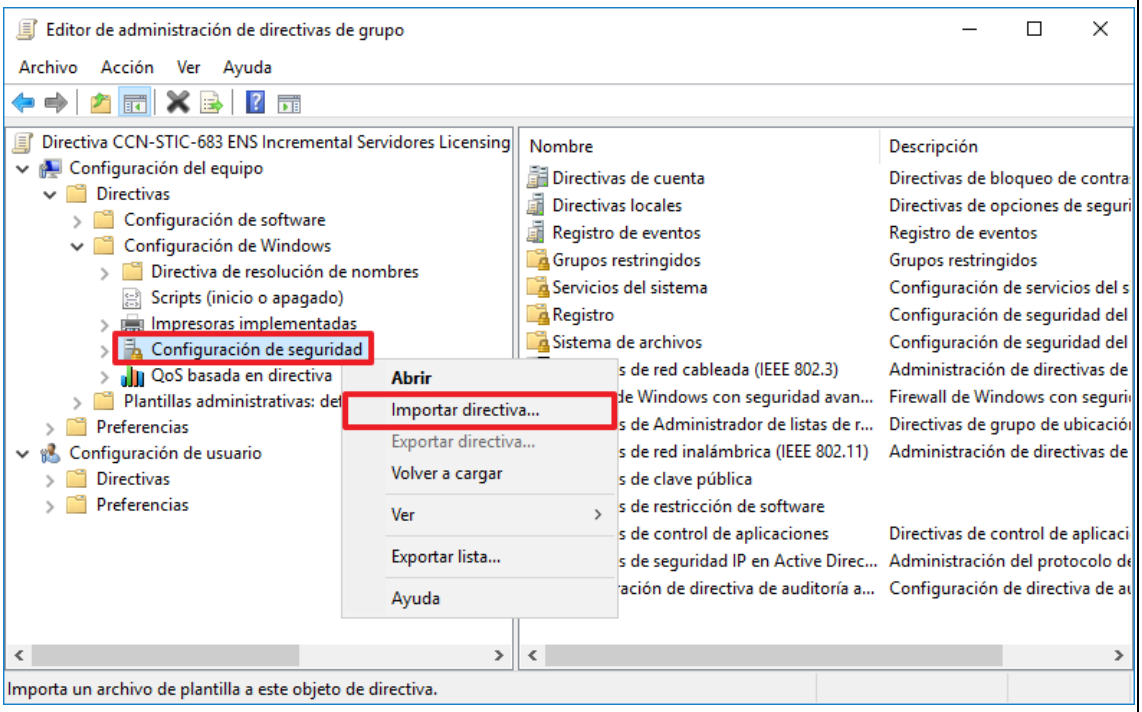
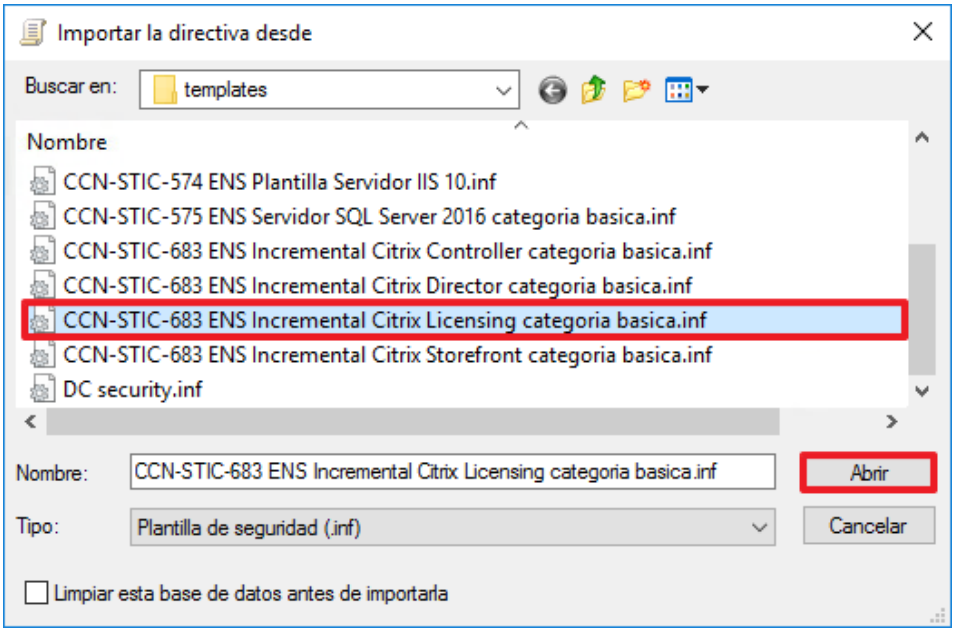
Paso	Descripción
12.	En la ventana resultante, introduzca como nombre de la nueva unidad organizativa “Servidores Citrix Controller” tal y como muestra en la imagen. No desmarque la opción “Proteger contenedores contra eliminación accidental”. Pulse “Aceptar” para crear el nuevo objeto. 
13.	Proceda a crear las siguientes unidades organizativas bajo la unidad organizativa “Servidores”. – Servidores Citrix Controller – Servidores Citrix Storefront – Servidores Citrix Licensing – Servidores Citrix Director
14.	Las nuevas unidades organizativas, aparecerán colgando de “Servidores”, como se muestra en la siguiente figura.  **Nota:** Las unidades organizativas “Servidores IIS 10” y “Servidores SQL Server” deberán haberse creado durante la aplicación de las guías de seguridad codificadas como “CCN-STIC-574” y “CCN-STIC-575”.

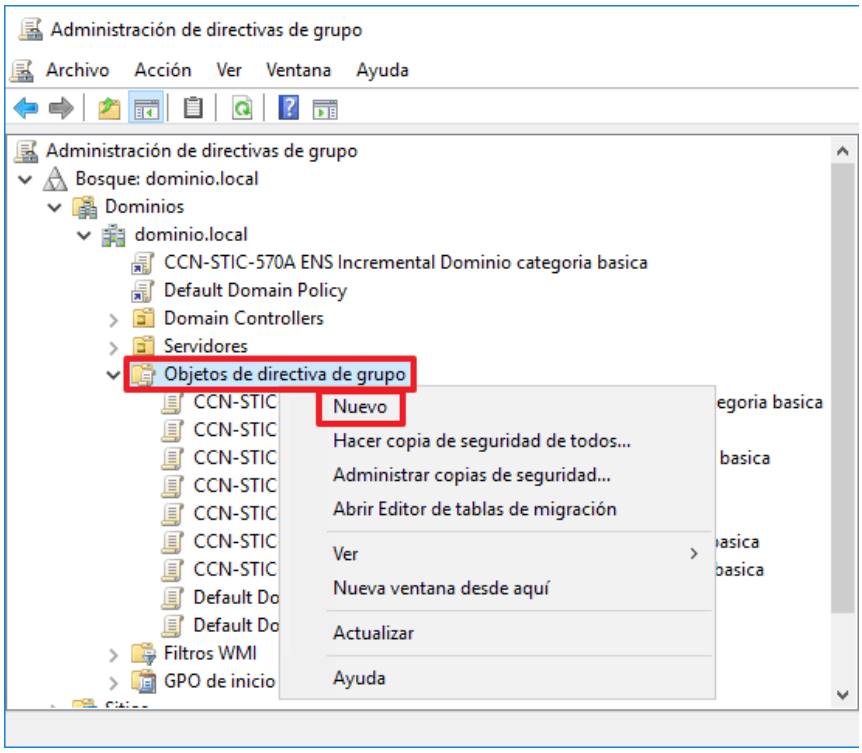
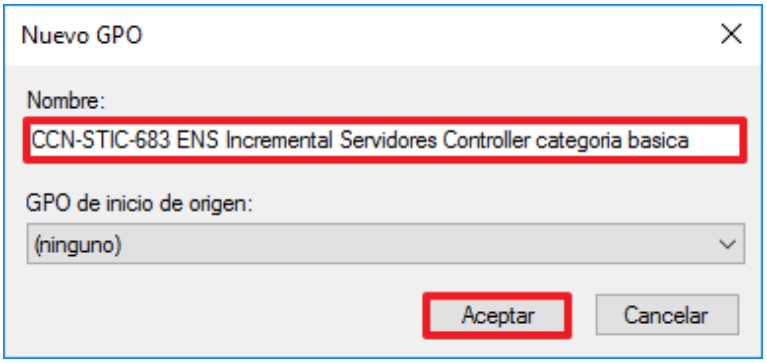
Paso	Descripción
15.	Utilice la herramienta "Administración de Directivas de grupo" (**Administrador del servidor → Herramientas → Administración de Directivas de grupo**). El sistema solicitará elevación de privilegios. 
16.	Expanda el contenedor **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores"**, como se muestra en la siguiente figura. 
17.	A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar la GPO correspondiente. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores del contenedor recién expandido "Servidores".
18.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 

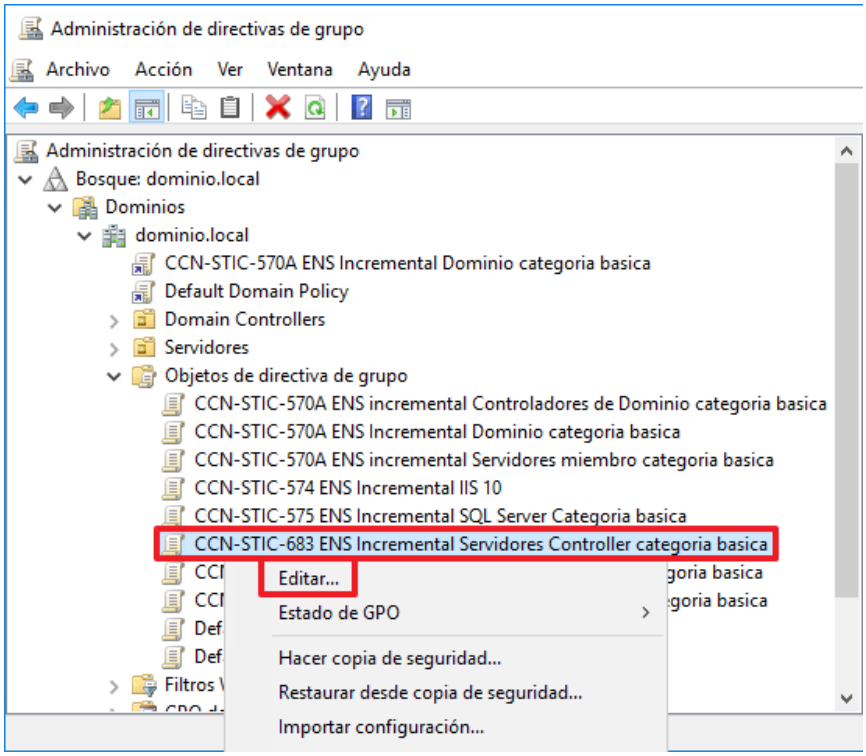
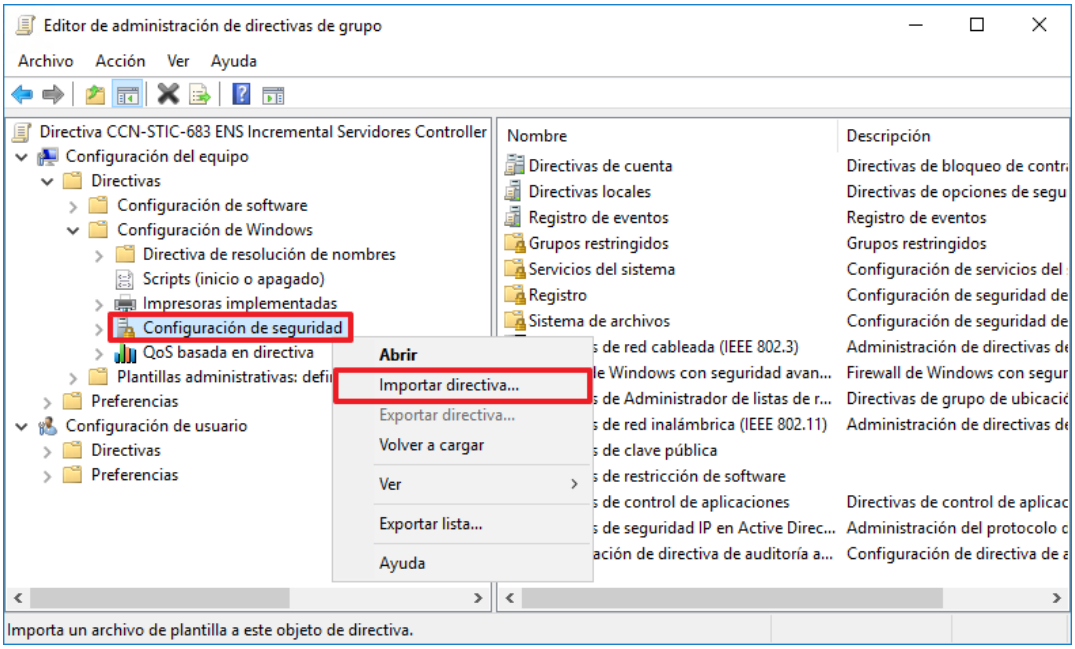
Paso	Descripción
19.	Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica" y pulse el botón “Aceptar”. 
20.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 

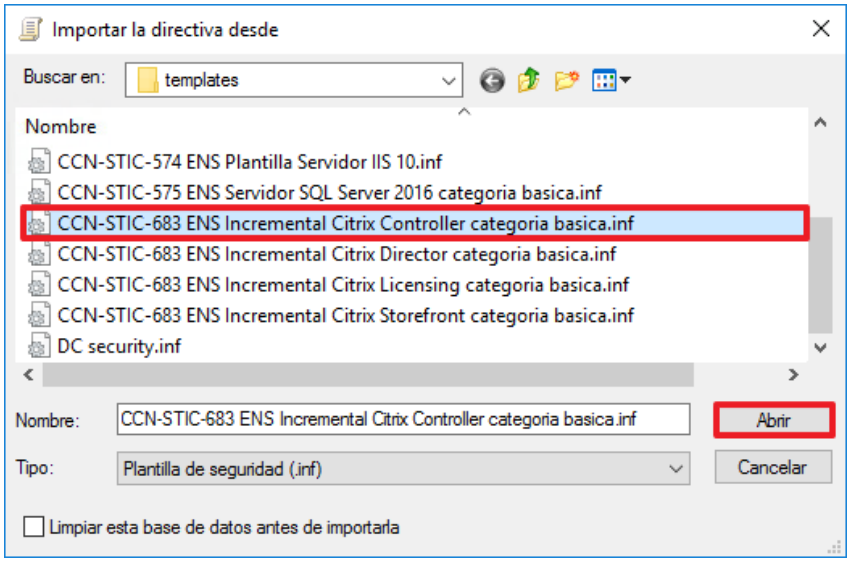
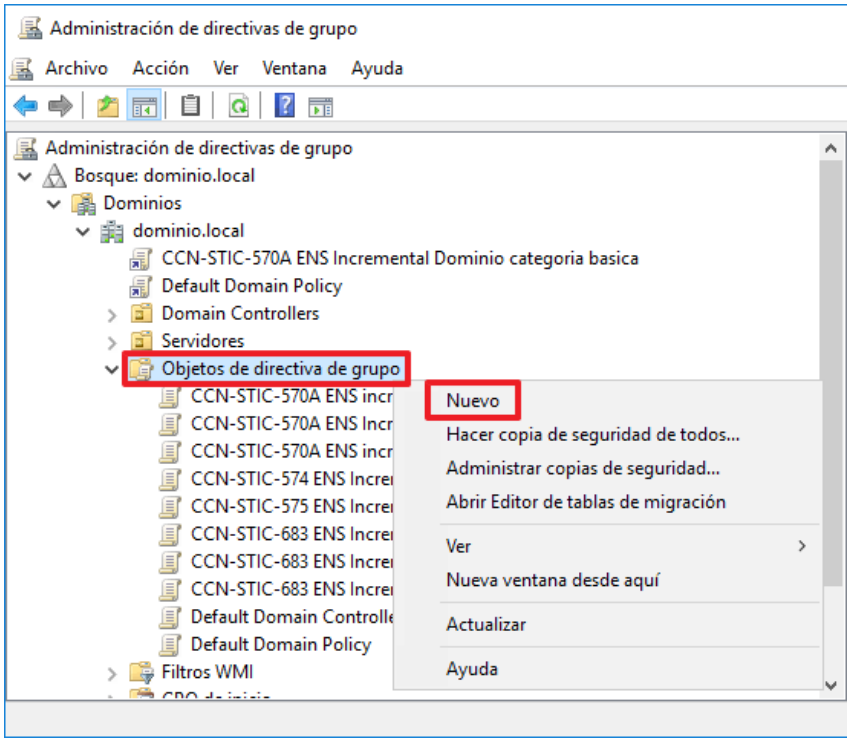
Paso	Descripción
21.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 
22.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Storefront categoria basica.inf" y pulse el botón "Abrir". 
23.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

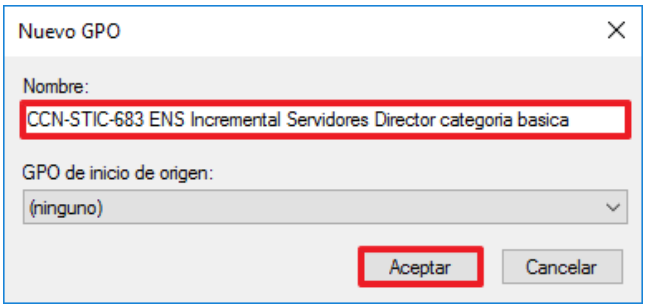
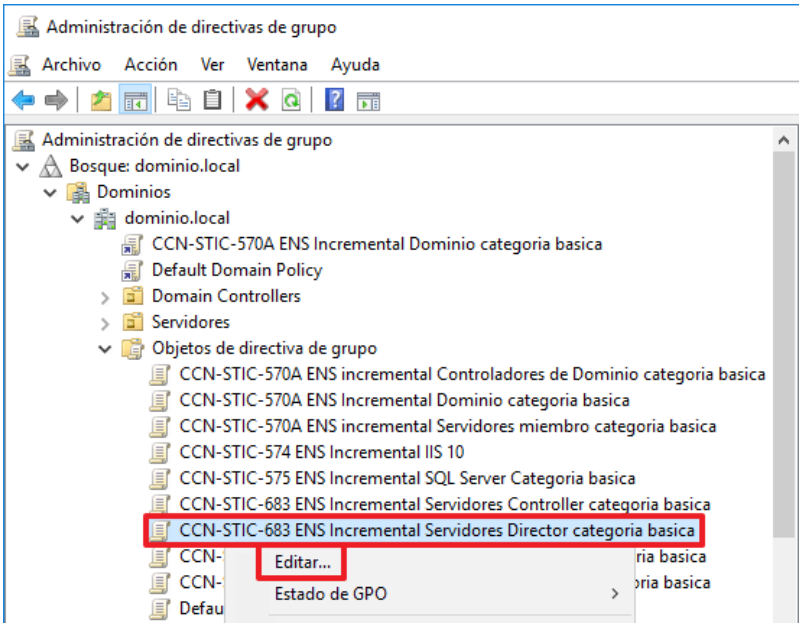
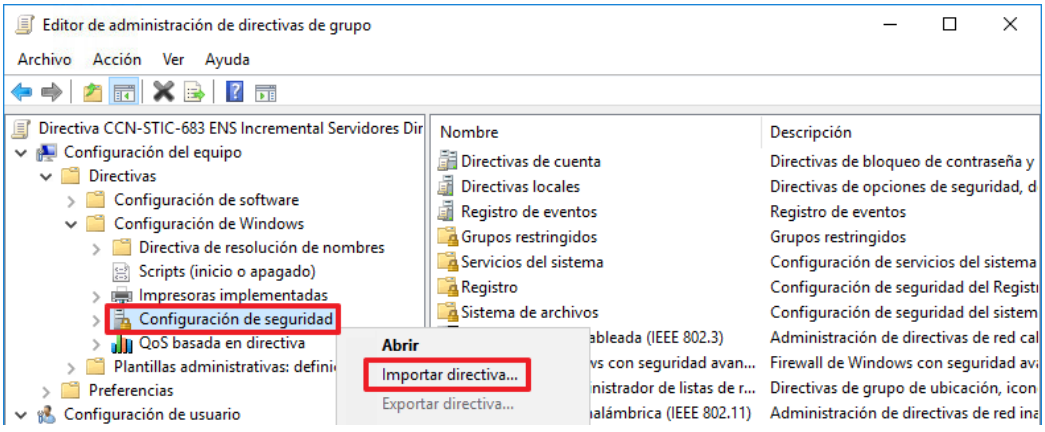
Paso	Descripción
24.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
25.	Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica" y pulse el botón “Aceptar”. 
26.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 

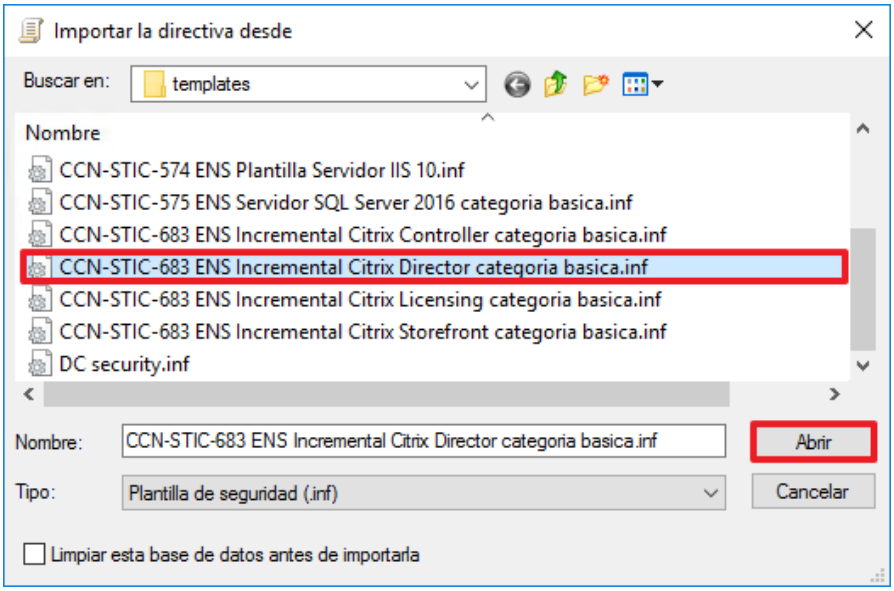
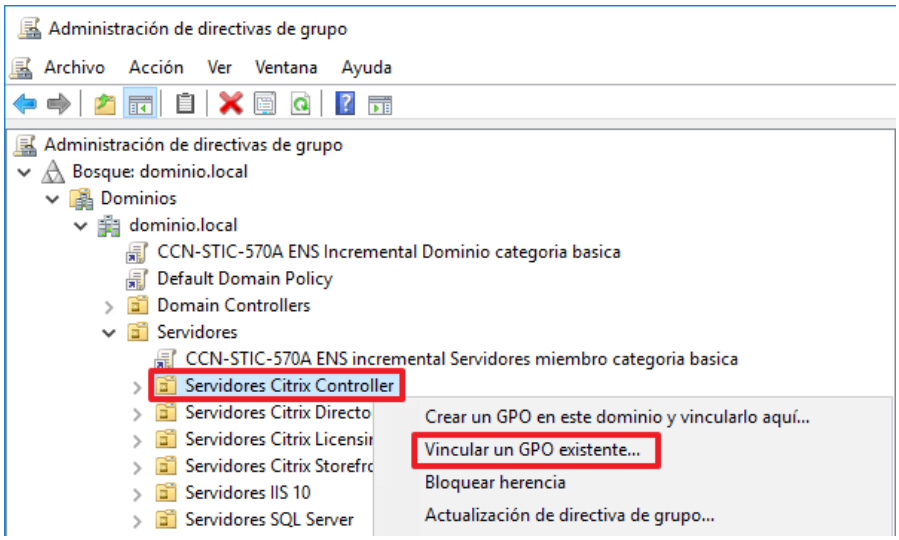
Paso	Descripción
27.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 
28.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Licensing categoria basica.inf" y pulse el botón "Abrir". 

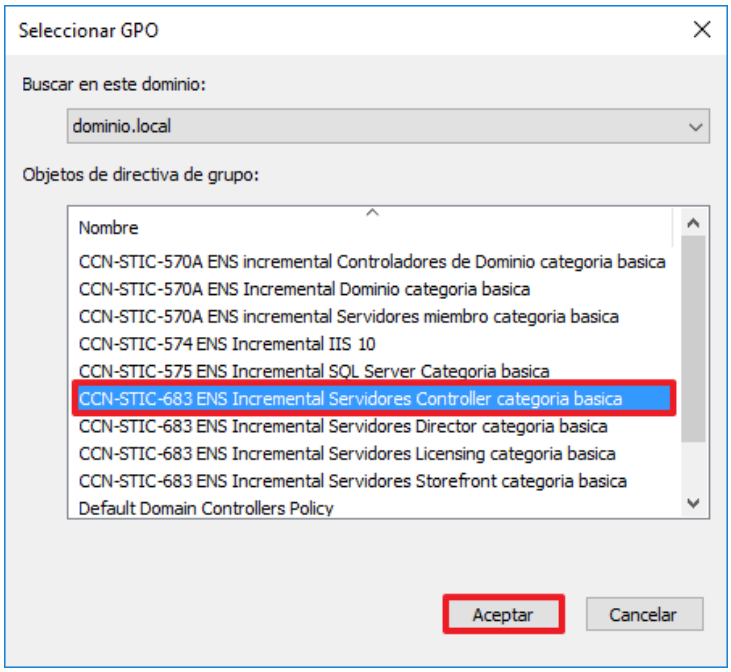
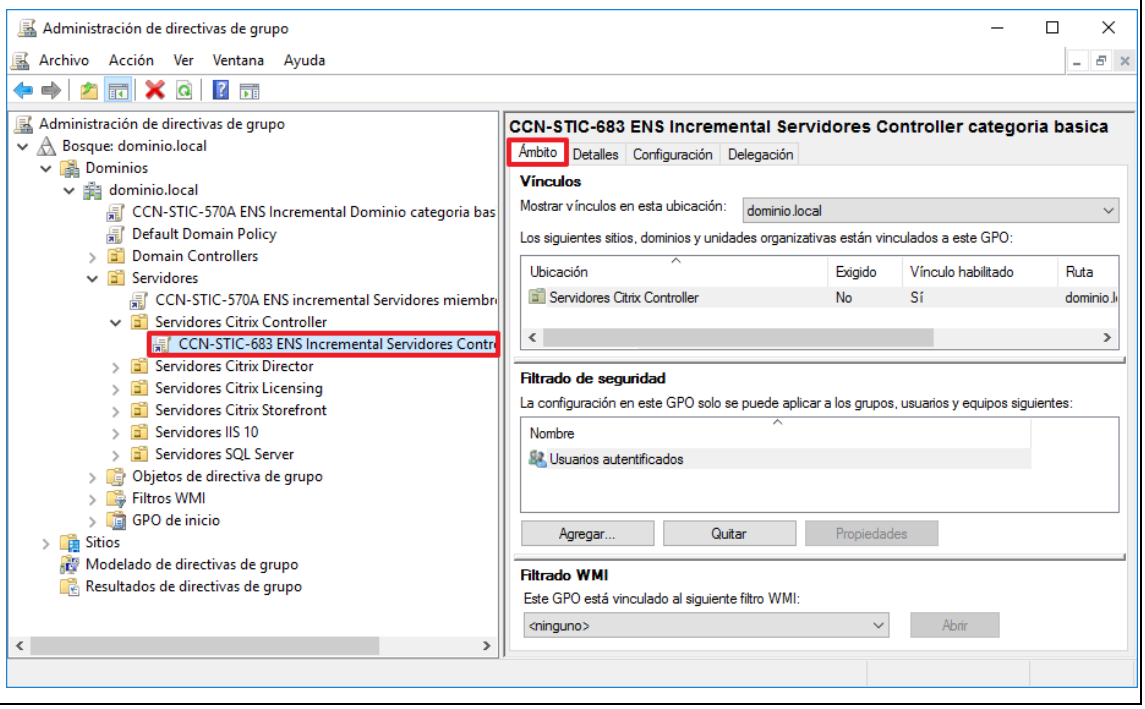
Paso	Descripción
29.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
30.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
31.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Controller categoria basica" y pulse el botón “Aceptar”. 

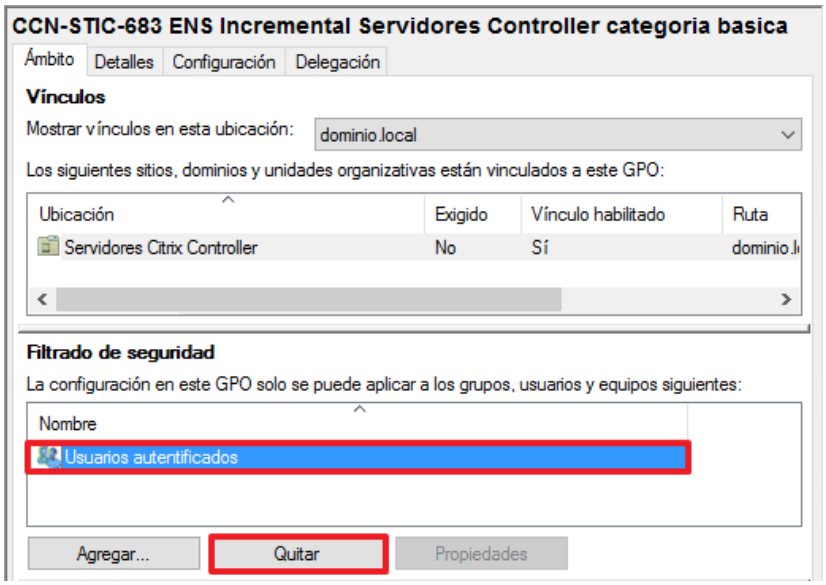
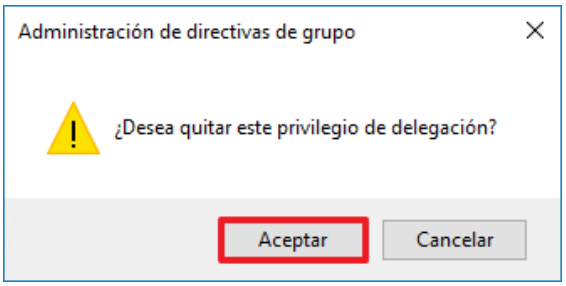
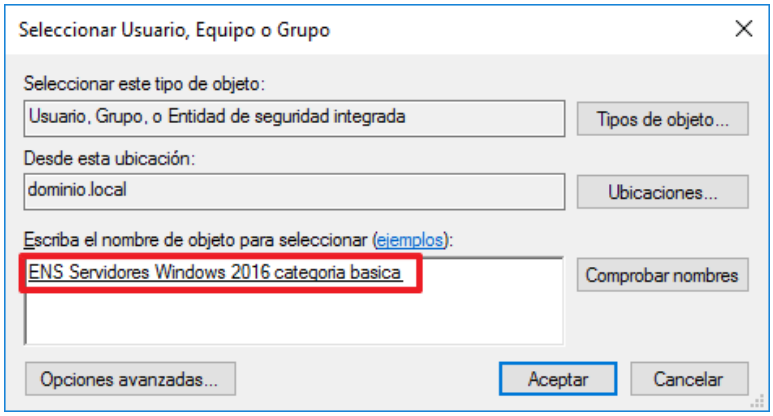
Paso	Descripción
32.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Controller categoria basica", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 
33.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 

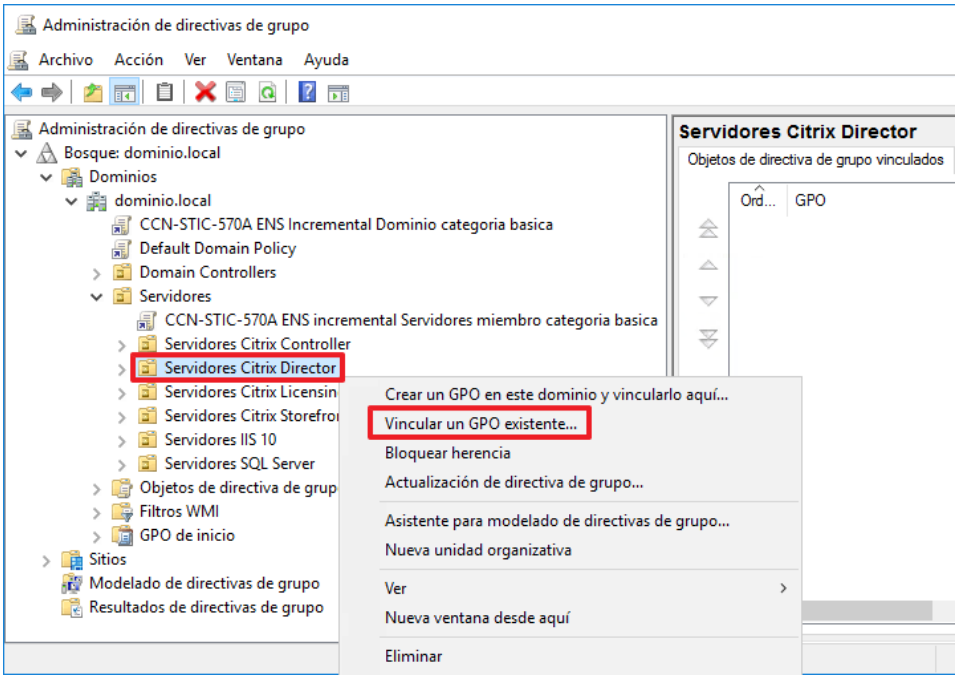
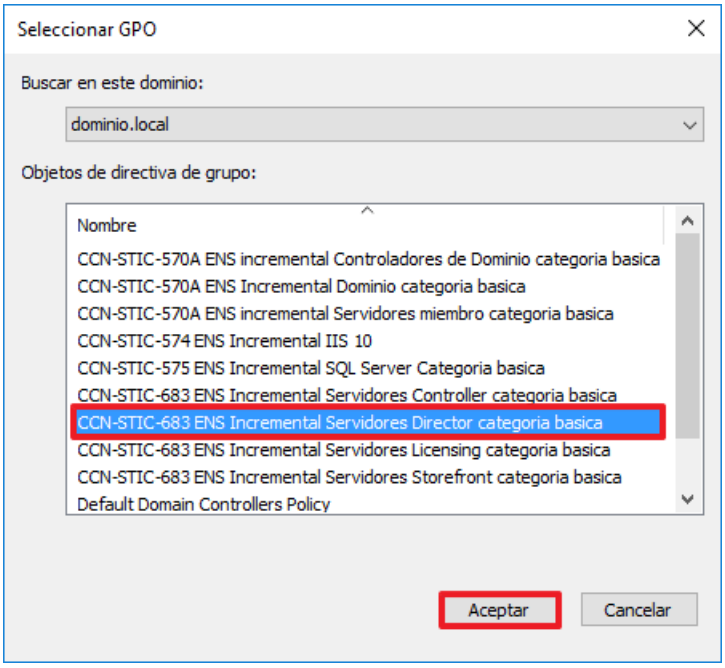
Paso	Descripción
34.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Controller categoria basica.inf" y pulse el botón "Abrir". 
35.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Controller categoria basica") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
36.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 

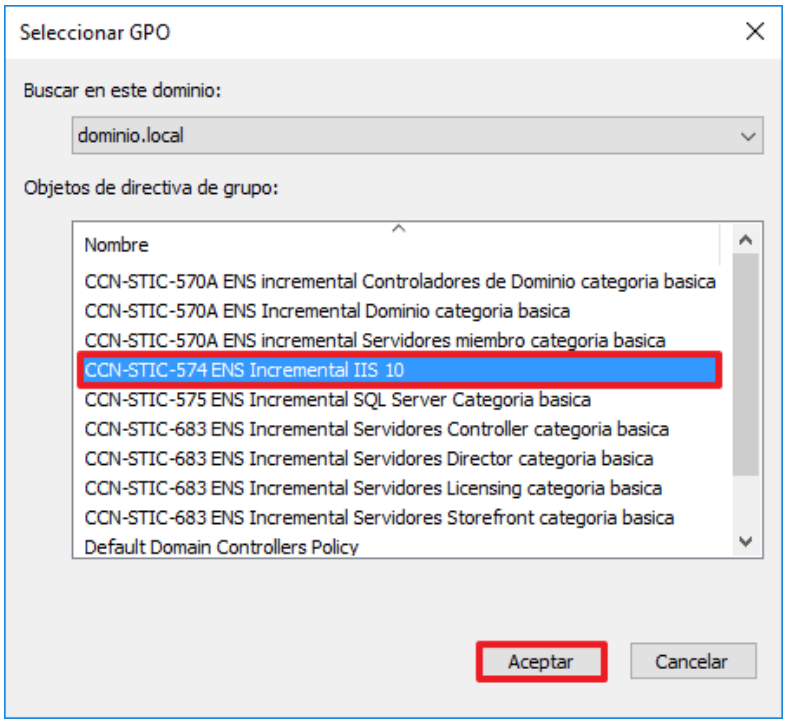
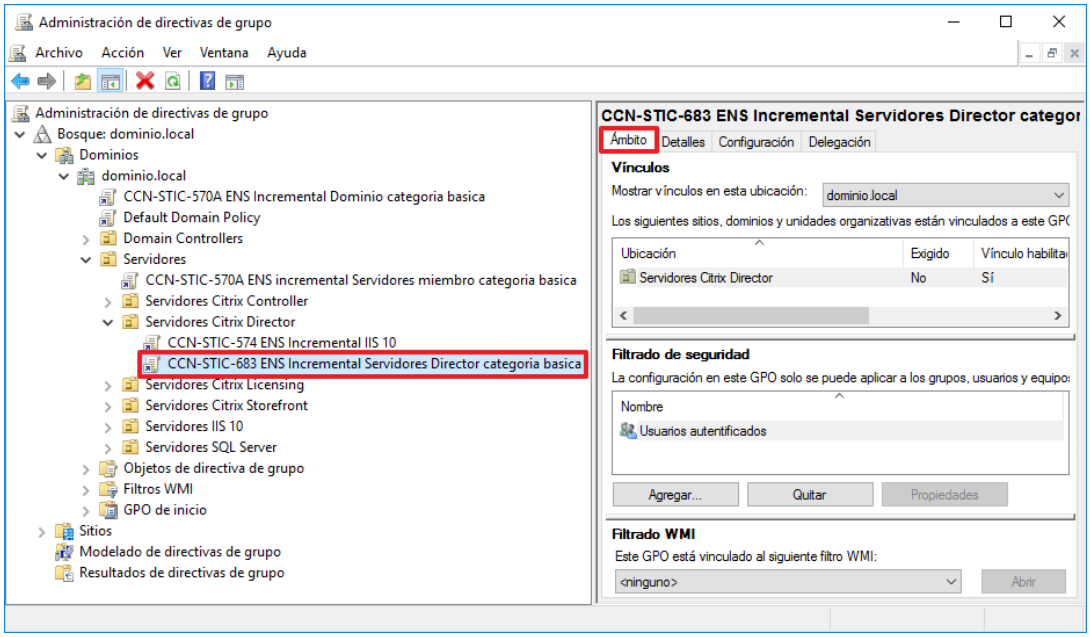
Paso	Descripción
37.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Director categoria basica" y pulse el botón “Aceptar”. 
38.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Director categoria basica", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 
39.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 

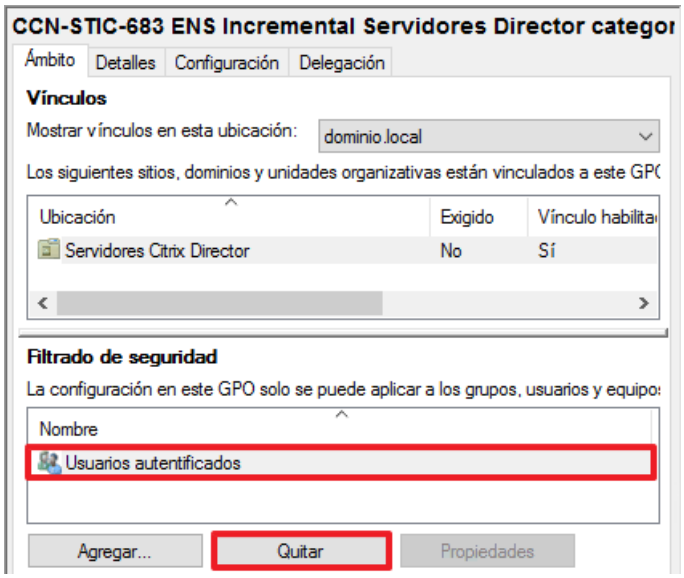
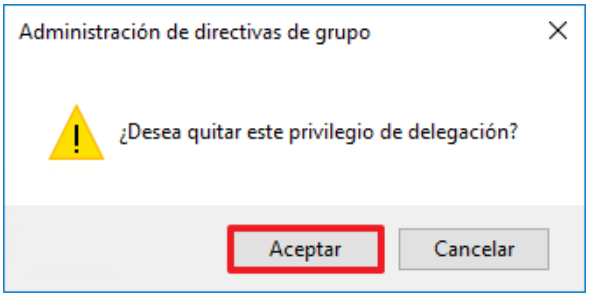
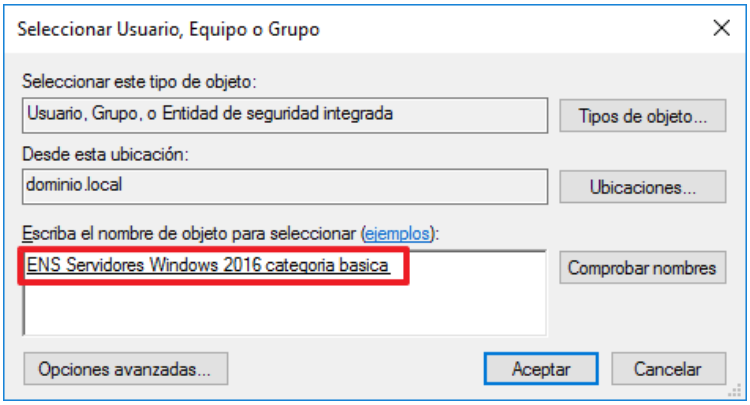
Paso	Descripción
40.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Director categoria basica.inf" y pulse el botón "Abrir". 
41.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Director categoria basica") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
42.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Controller”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 

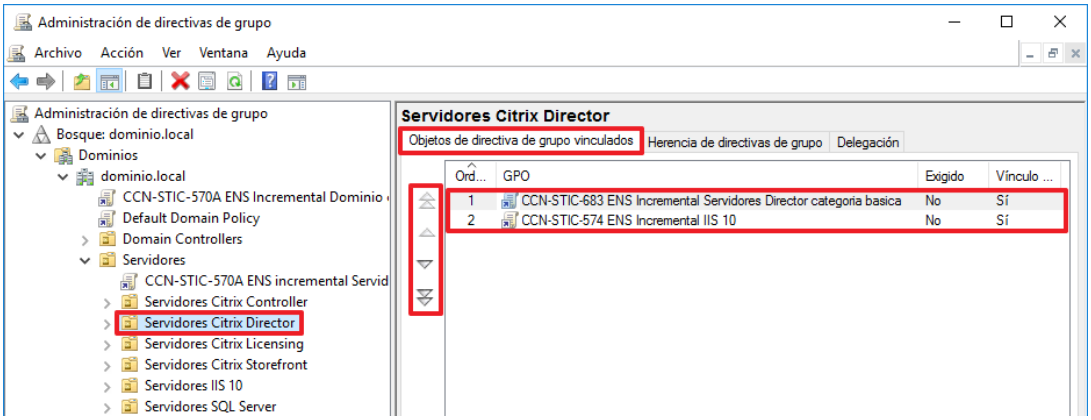
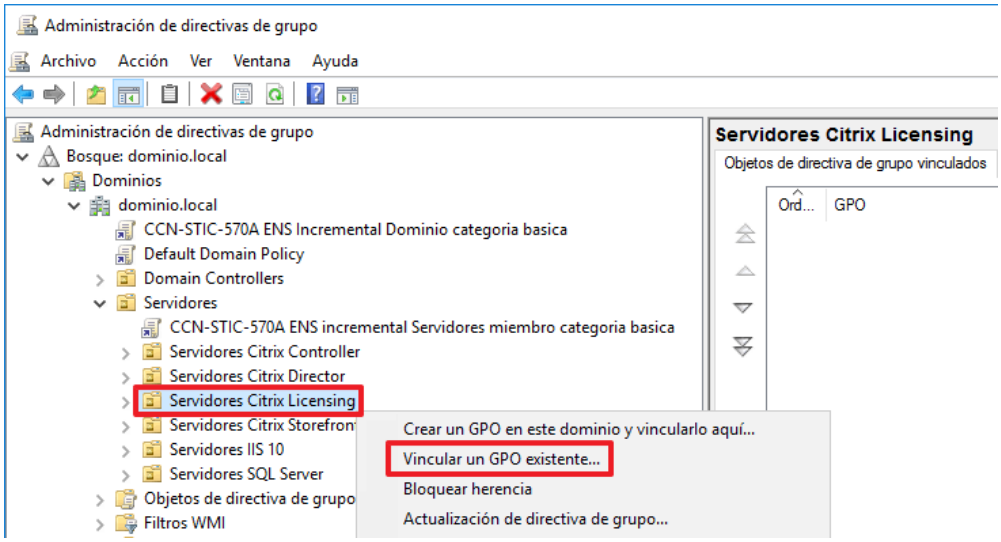
Paso	Descripción
43.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Controller categoria basica”. 
44.	Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

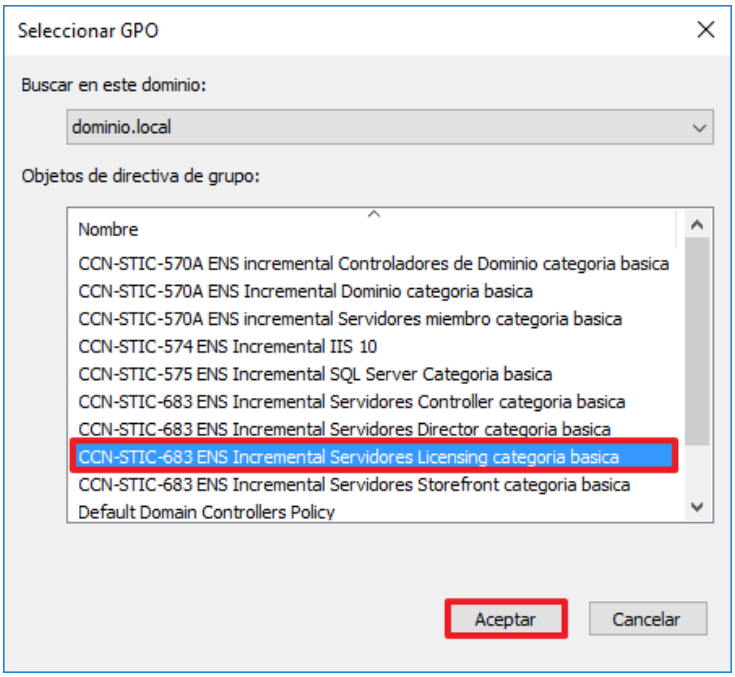
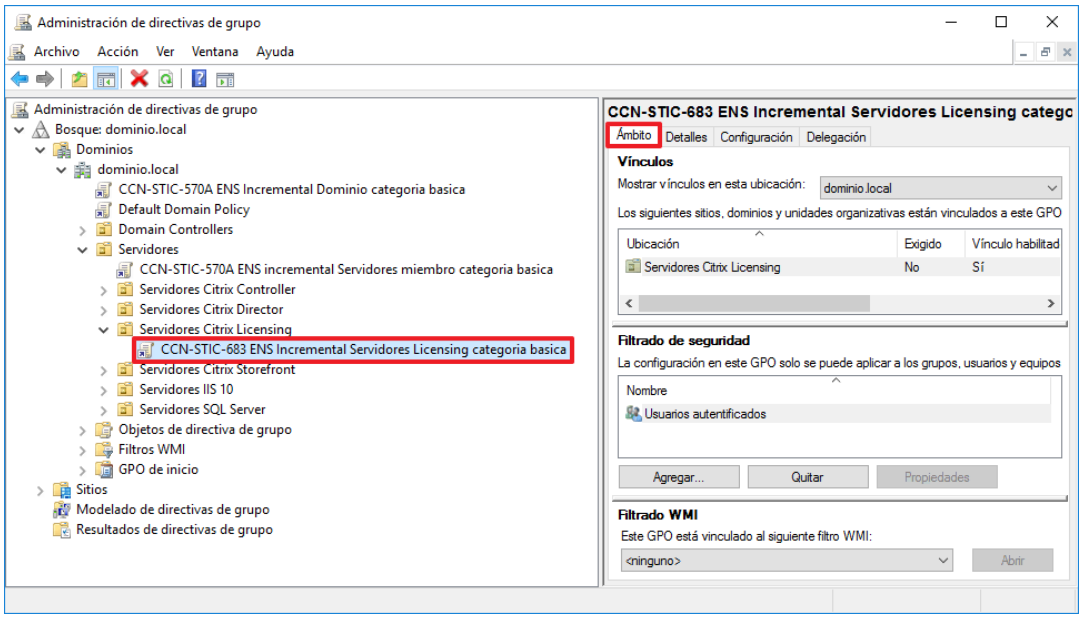
Paso	Descripción
45.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
46.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
47.	Una vez quitado, pulse el botón “Agregar…”.
48.	Introduzca como nombre “ENS servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

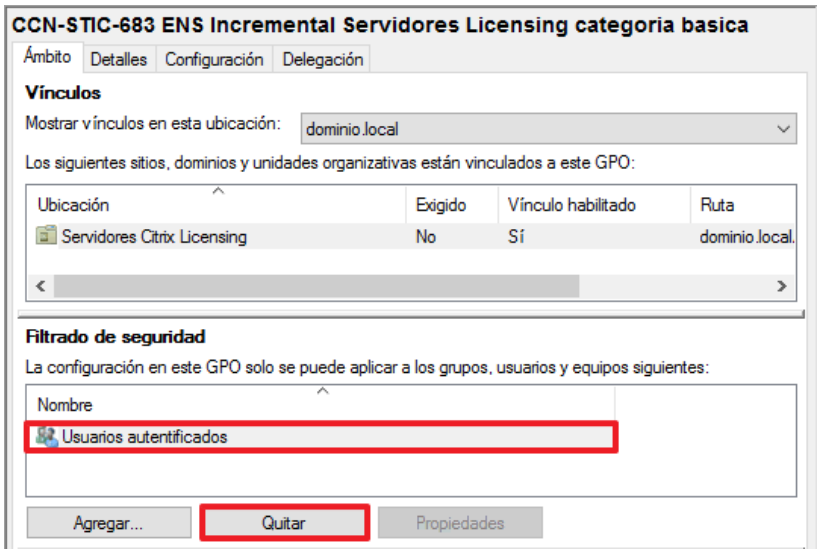
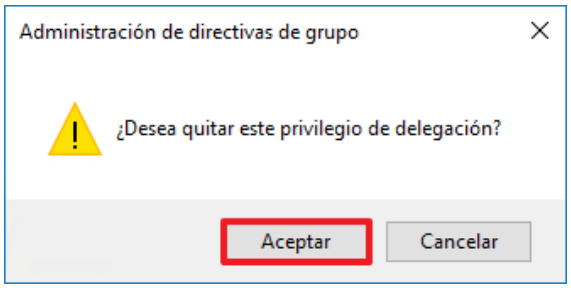
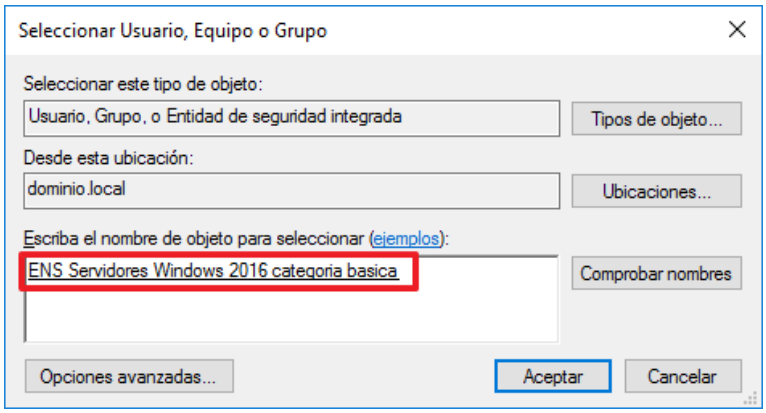
Paso	Descripción
49.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Director”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 
50.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Director categoria basica”. 

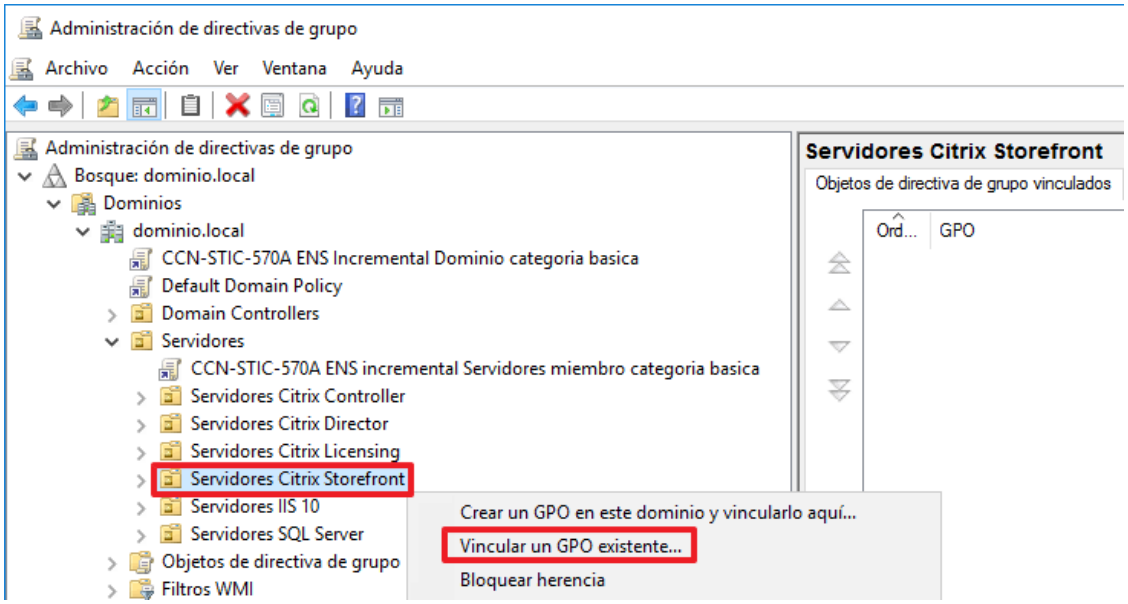
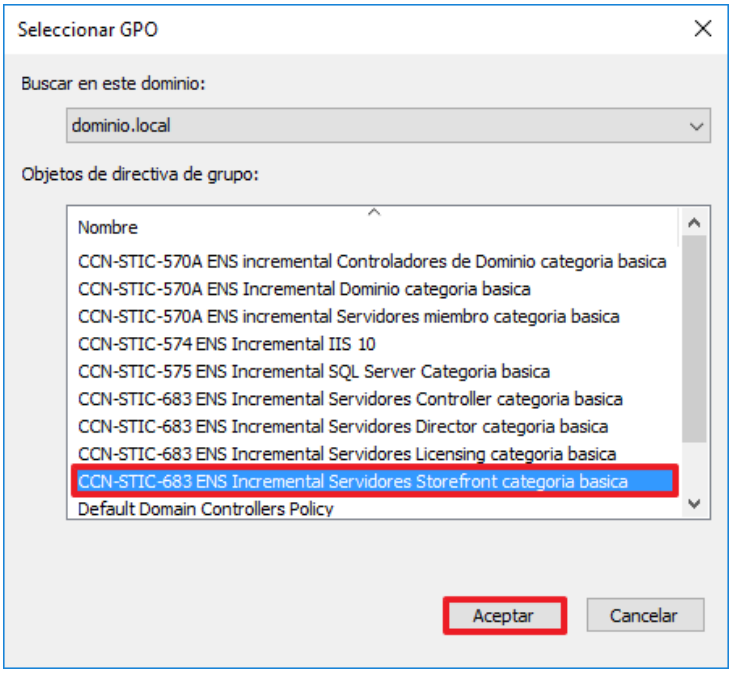
Paso	Descripción
51.	Repita el mismo proceso para vincular el GPO “CCN-STIC-574 ENS Incremental IIS 10”. 
52.	Seleccione la política de grupo “CCN-STIC-683 ENS Incremental Servidores Director categoria basica” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

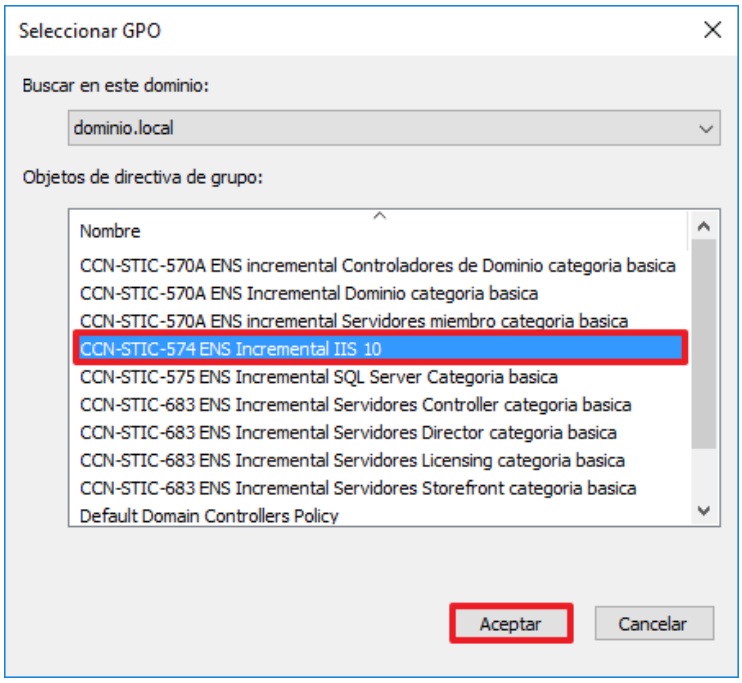
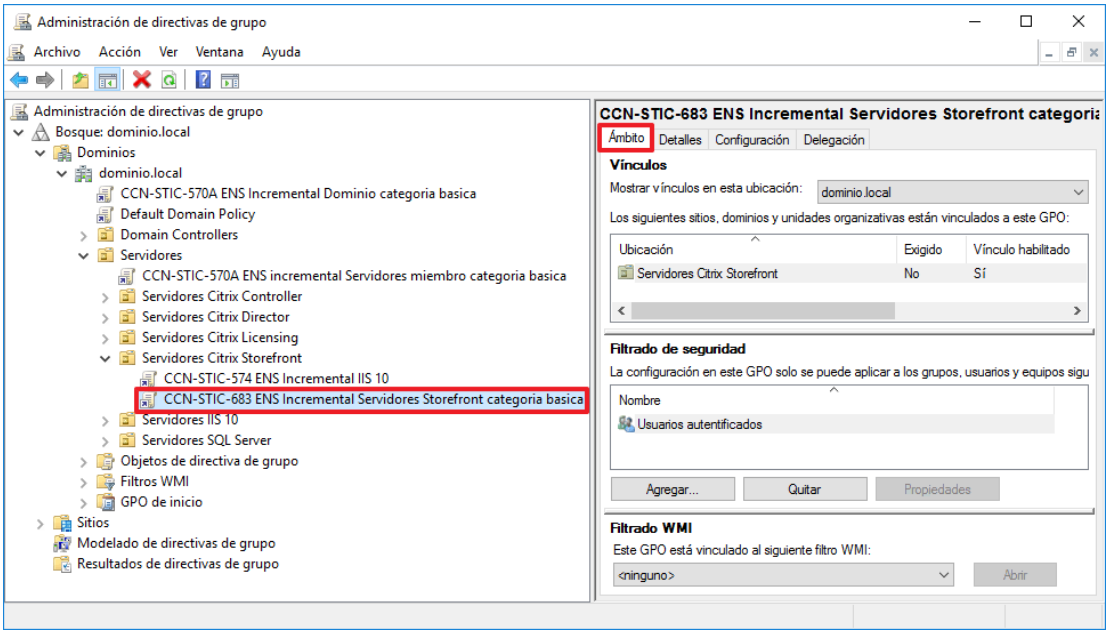
Paso	Descripción
53.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
54.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
55.	Una vez quitado, pulse el botón “Agregar…”.
56.	Introduzca como nombre “ENS servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

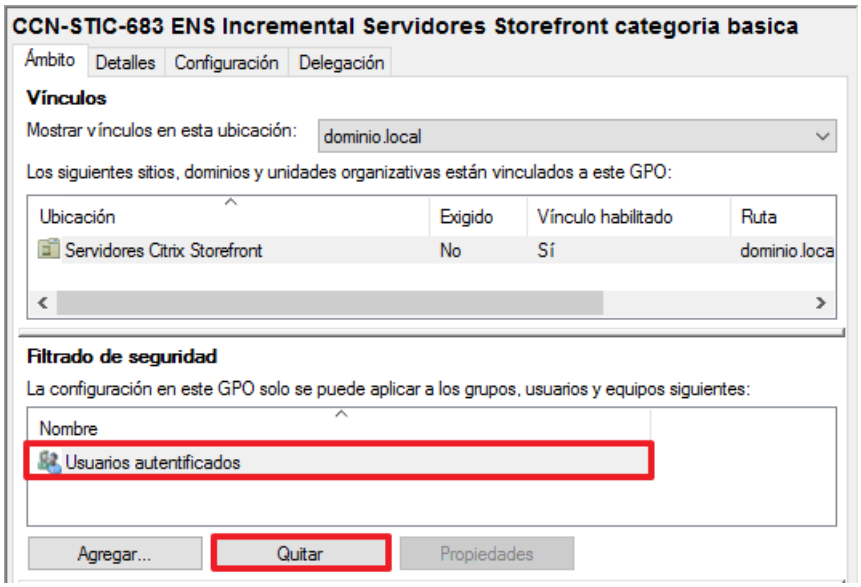
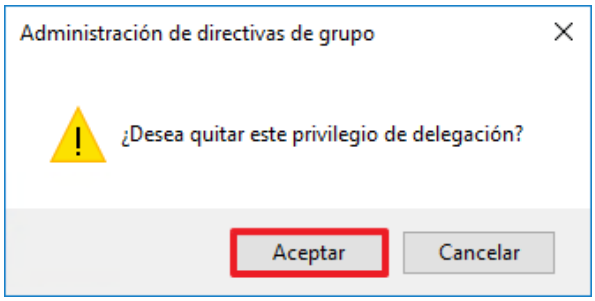
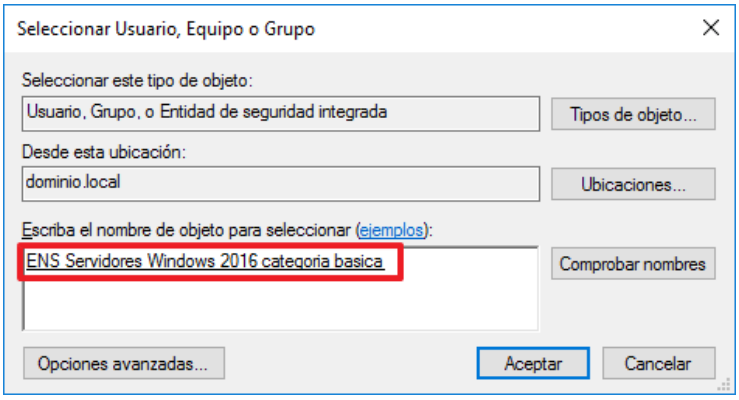
Paso	Descripción
57.	Seleccione el contenedor “Servidores Citrix Director” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura. – 1 - CCN-STIC-683 ENS Incremental Servidores Director categoria basica – 2 - CCN-STIC-574 ENS Incremental IIS 10 Si no lo es, modifique el orden de los vínculos para que sea igual al indicado. Para ello seleccione un vínculo y utilice las flechas hacia arriba y hacia abajo que hay en la parte izquierda de la pestaña. 
58.	Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá.
59.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Licensing”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 

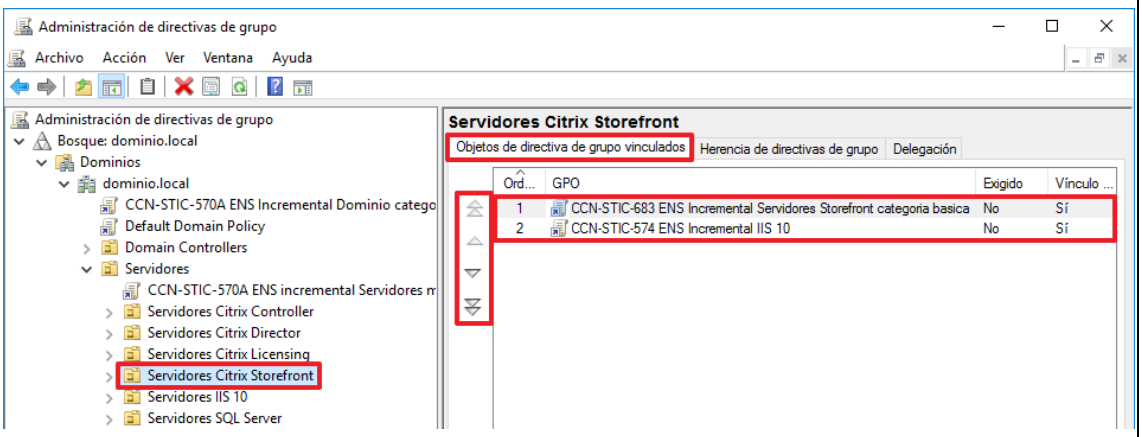
Paso	Descripción
60.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica”. 
61.	Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
62.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
63.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
64.	Una vez quitado, pulse el botón “Agregar…”.
65.	Introduzca como nombre “ENS servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

Paso	Descripción
66.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **"Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Storefront”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 
67.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica”. 

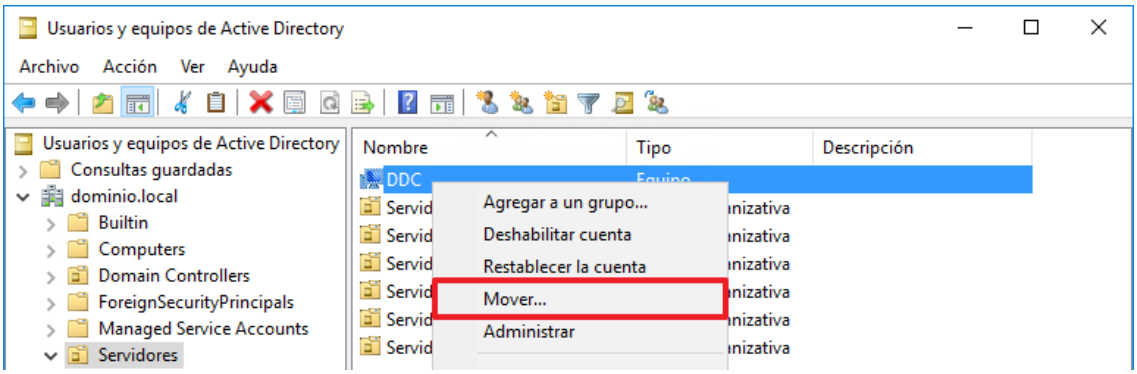
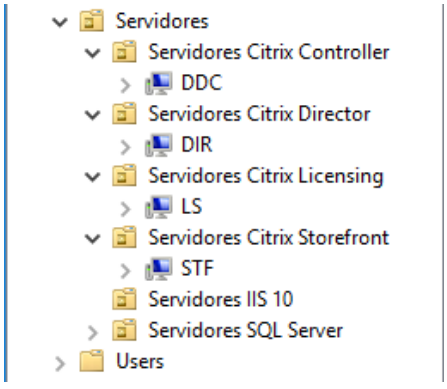
Paso	Descripción
68.	De manera análoga vincule la GPO denominada “CCN-STIC-574 ENS Incremental Servidores IIS 10”. 
69.	Seleccione la política de grupo “CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
70.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
71.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
72.	Una vez quitado, pulse el botón “Agregar…”.
73.	Introduzca como nombre “ENS servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

Paso	Descripción
74.	Seleccione el contenedor “Servidores Citrix Storefront” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura. – 1 - CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica – 2 - CCN-STIC-574 ENS Incremental IIS 10 Si no lo es, modifique el orden de los vínculos para que sea igual al indicado. Para ello seleccione un vínculo y utilice las flechas hacia arriba y hacia abajo que hay en la parte izquierda de la pestaña. 
75.	Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá.

En este punto los GPOs se encuentran configurados correctamente en Active Directory y su configuración se aplicará automáticamente a los nuevos servidores que necesite añadir a la infraestructura. En pasos posteriores moverá cada uno de los objetos de equipo dentro de sus correspondientes unidades organizativas.

Paso	Descripción
76.	Si no lo ha hecho todavía, inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el servidor que va a asegurar, con una cuenta con derechos de administración en el dominio.
77.	Mueva las cuentas de equipo de cada uno de los roles que haya aprovisionado previamente para la implementación de la infraestructura de Citrix. En función del rol que haya aprovisionado previamente debe mover la cuenta de equipo a una unidad organizativa u otra. La siguiente tabla de referencia puede ayudarle con el proceso. **Nota:** Durante la aplicación de la guía “CCN-STIC-574” habrá situado los servidores correspondientes a los roles de Citrix Storefront y Citrix Director en la Unidad Organizativa “Servidores IIS 10” en este punto deberá mover dichos servidores a las nuevas Unidades Organizativas creadas para cada rol.

<table>
<tr><th>Paso</th><th colspan="3">Descripción</th></tr>
<tr><td></td><td>Rol</td><td>Unidad Organizativa</td><td>Cuenta de equipo</td></tr>
<tr><td></td><td>Citrix Controller</td><td>Servidores Citrix Controller</td><td>DDC</td></tr>
<tr><td></td><td>Citrix Storefront</td><td>Servidores Citrix Storefront</td><td>STF</td></tr>
<tr><td></td><td>Citrix Licensing</td><td>Servidores Citrix Licensing</td><td>LS</td></tr>
<tr><td></td><td>Citrix Director</td><td>Servidores Citrix Director</td><td>DIR</td></tr>
<tr><td>78.</td><td colspan="3">Para ello, abra la herramienta "Administrador del servidor" y despliegue el menú “Herramientas → Usuarios y equipos de Active Directory”. El sistema solicitará elevación de privilegios.
A continuación, en la herramienta “Usuarios y equipos de Active Directory” despliegue la ruta “<nombre de su dominio> → Servidores", y marcando con el botón derecho del ratón cada uno de los servidores, pulse la opción “Mover…”.
 
</td></tr>
<tr><td>79.</td><td colspan="3">De forma análoga, realice el paso anterior por cada uno de los servidores que desee añadir a la plataforma.</td></tr>
<tr><td>80.</td><td colspan="3">Finalmente, dentro de cada unidad organizativa debe apreciar cada uno de los servidores añadidos.
 
</td></tr>
<tr><td>81.</td><td colspan="3">Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor.</td></tr>
</table>

Con la anterior configuración cada uno de los servidores recogerá de forma automática las directivas de grupo configuradas para su rol.

Nota: En el caso de no aplicarse de forma automática la configuración de GPO aplicadas puede utilizar el comando **“gpupdate /force”** para forzar el proceso.

2. CERTIFICADOS

Citrix Virtual Apps and Desktops faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media y alta de seguridad del ENS el uso de certificados emitidos por entidades certificadoras de terceros, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está totalmente desaconsejado el uso de certificados autofirmados.

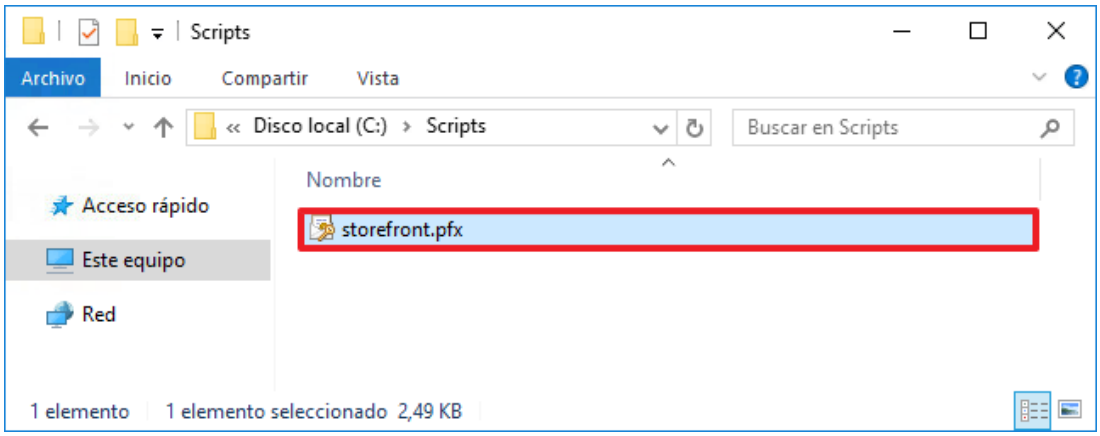
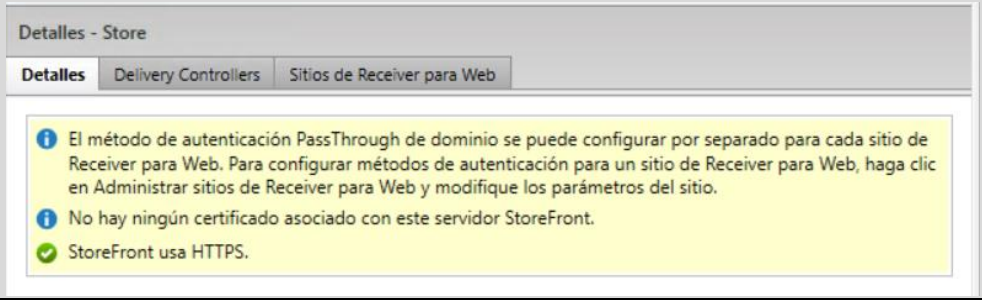
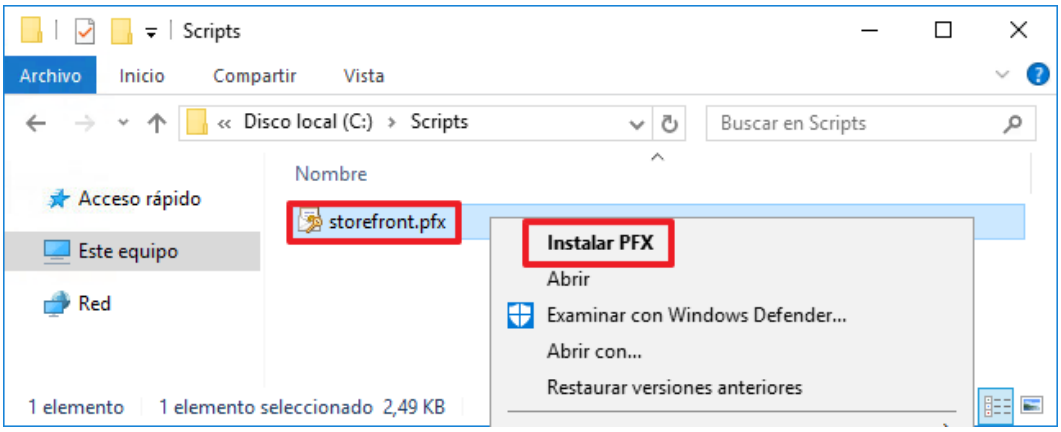
Para la categoría básica de seguridad del ENS se configuran certificados para los siguientes roles de la infraestructura:

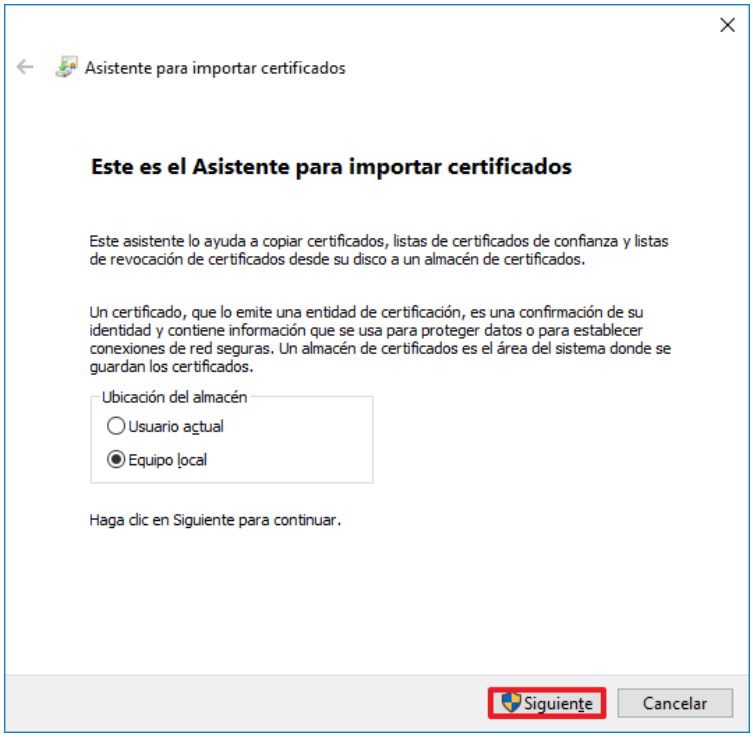
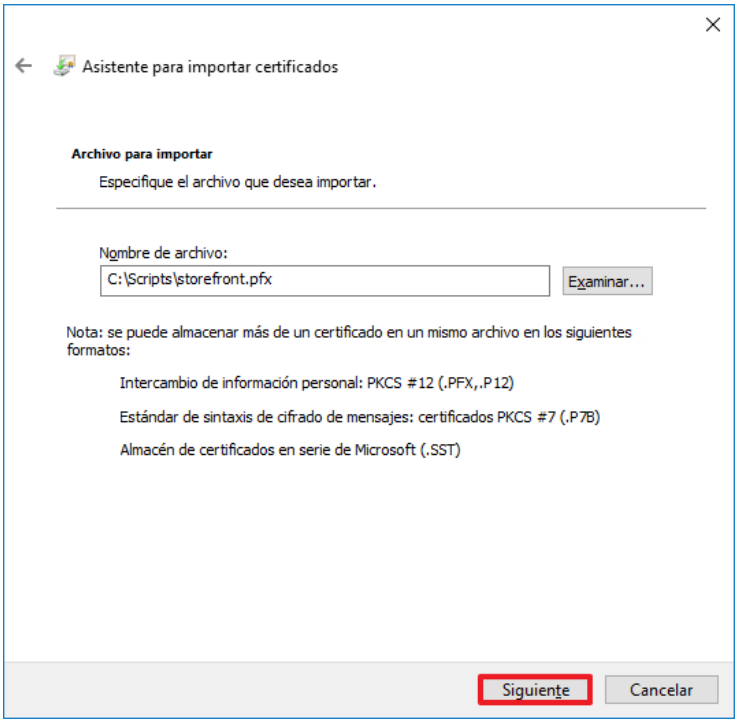
a) Servidor con el rol Citrix Storefront.

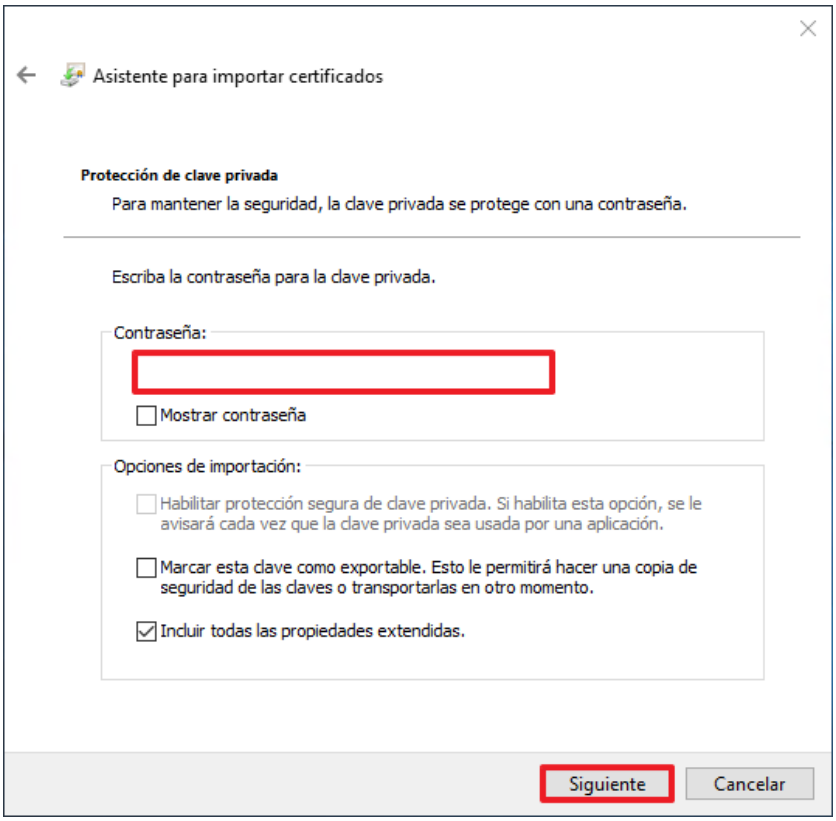
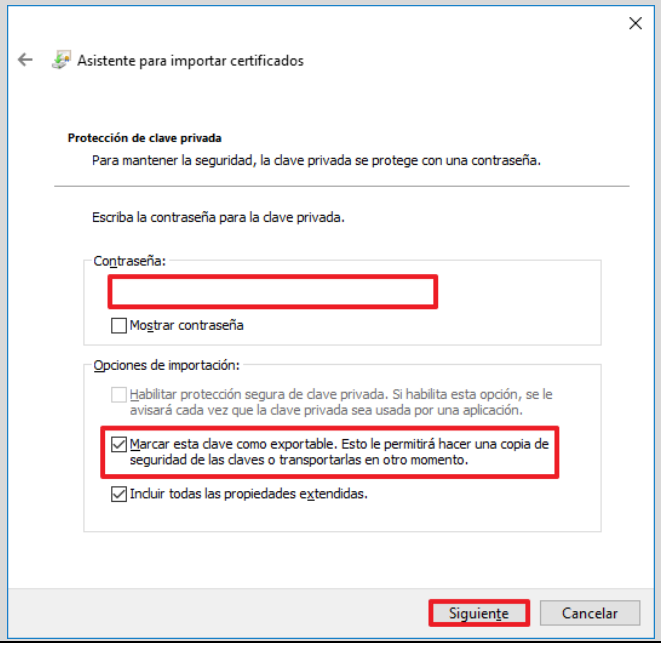
b) Servidores con el rol Citrix Director.

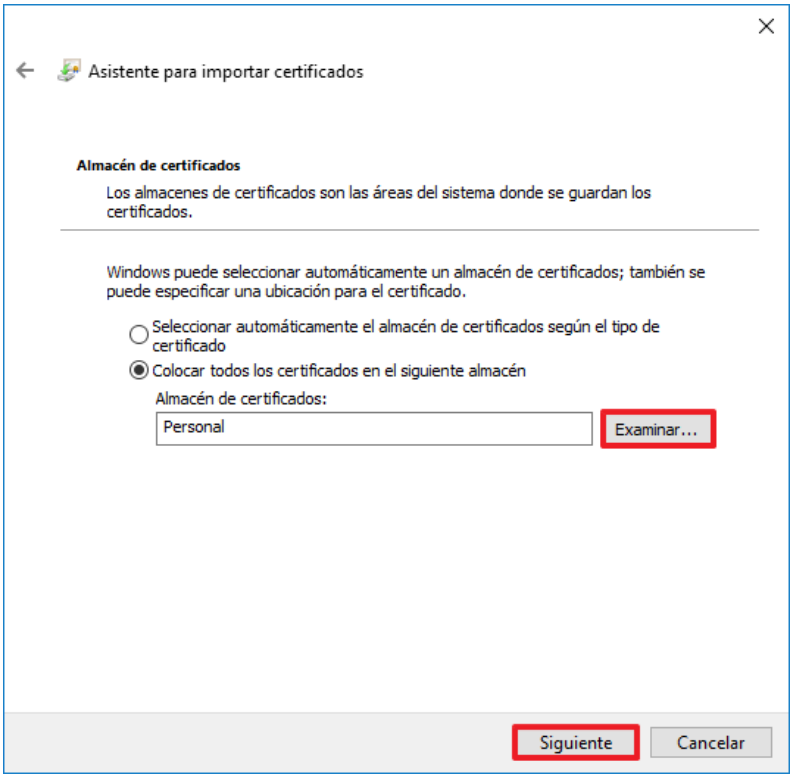
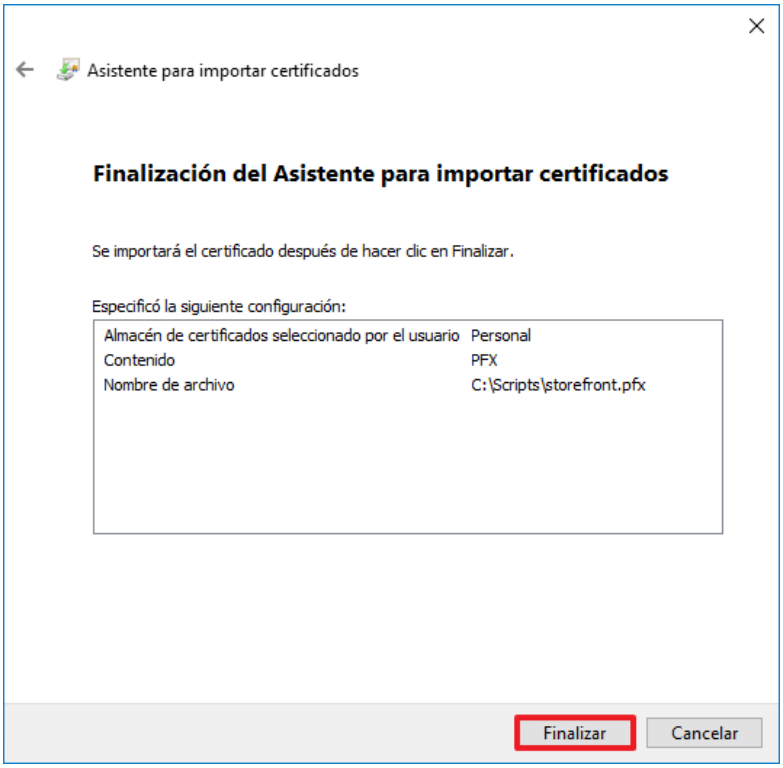
En primer lugar, se procederá a securizar las comunicaciones del servidor con el rol Citrix Storefront.

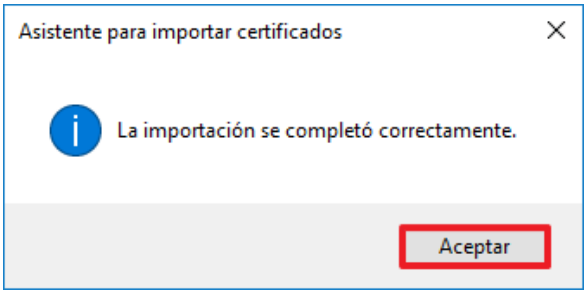
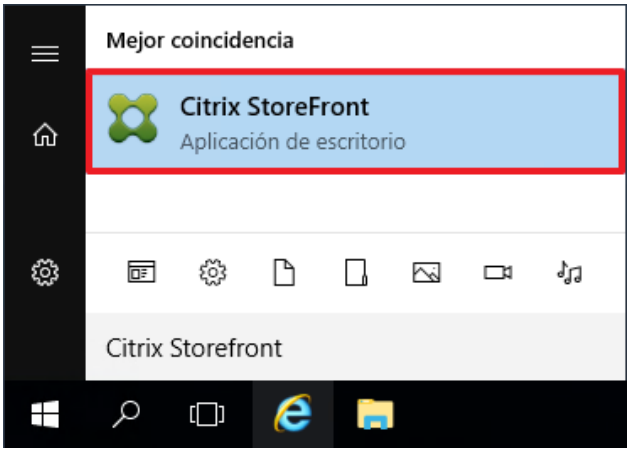
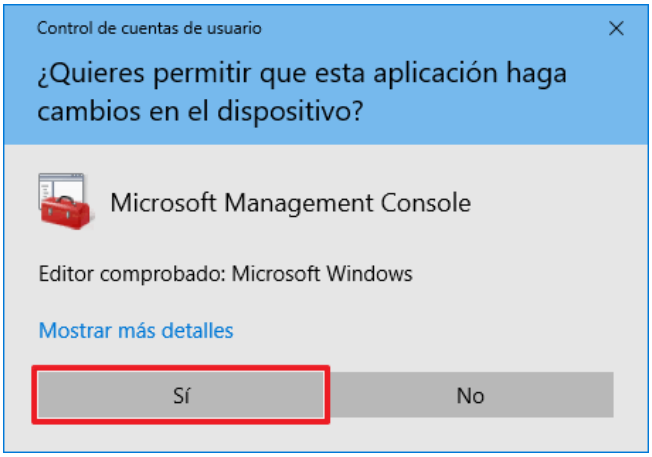
Paso	Descripción
82.	Inicie sesión en un servidor con el rol Citrix Storefront del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
83.	Cree el directorio “Scripts” en la unidad “C:\”.
84.	Será necesario la obtención de un certificado de equipo válido en el dominio ya que los equipos que se conecten al servidor validarán la presencia del certificado y su vigencia. Utilice un certificado cuyo nombre común coincida con la URL base que haya indicado en pasos anteriores. **Nota:** No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.

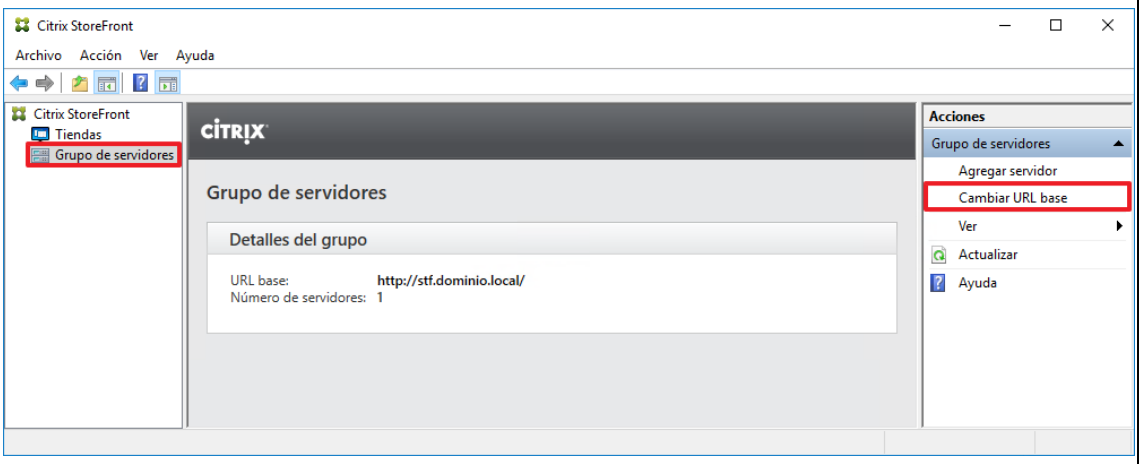
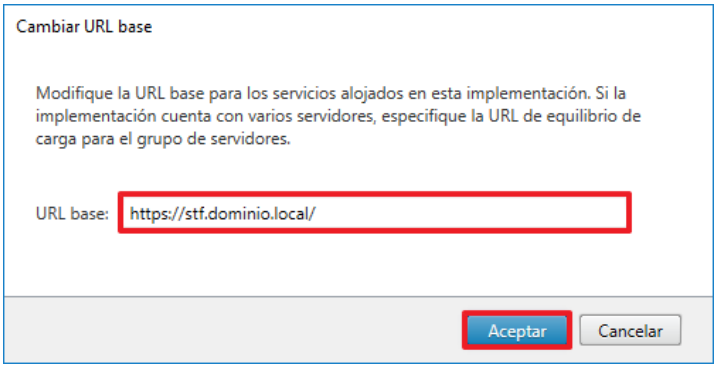
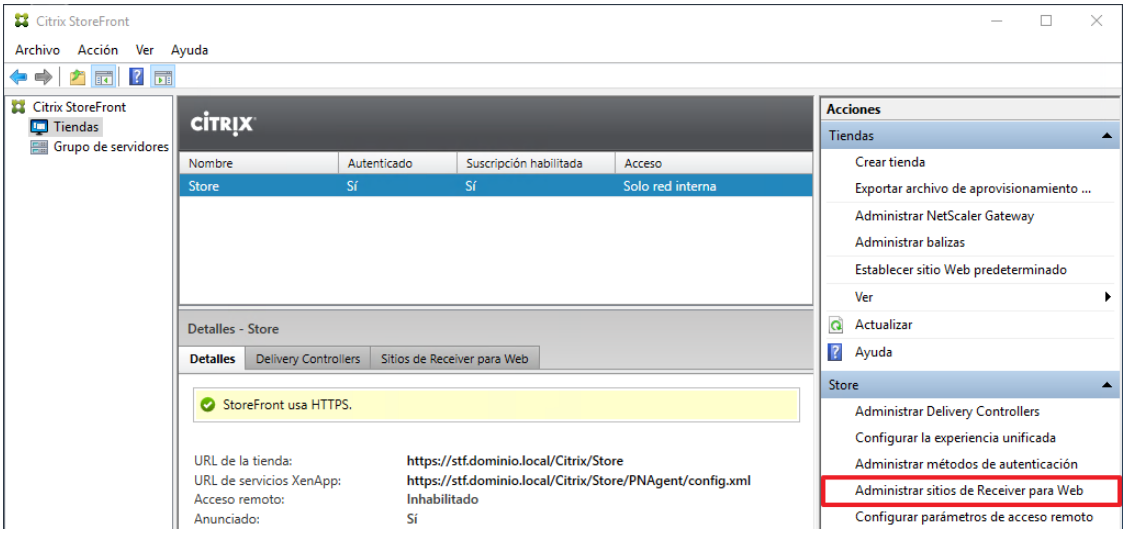
Paso	Descripción
85.	Copie el certificado en la unidad "C:\Scripts" y establezca un nombre de fichero identificativo. En esta guía se utilizará el fichero **"C:\Scripts\storefront.pfx"** a modo de ejemplo, no dude en ajustar el nombre de su archivo en los siguientes pasos. 
86.	Si no lo ha hecho todavía, proceda con los siguientes pasos para realizar la instalación del certificado sobre el almacén **"Personal"** de equipo. **Nota:** Durante la instalación puede ubicar el certificado en el almacén del equipo "Hospedaje de sitios web" pero encontrará advertencias en la consola de Storefront indicando que no hay ningún certificado asociado a este servidor Storefront. Para evitar problemas deberá ubicar el certificado en el almacén Personal del equipo tal y como se muestra en los siguientes pasos. 
87.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **"Instalar PFX"** tal y como se indica en la siguiente figura. 

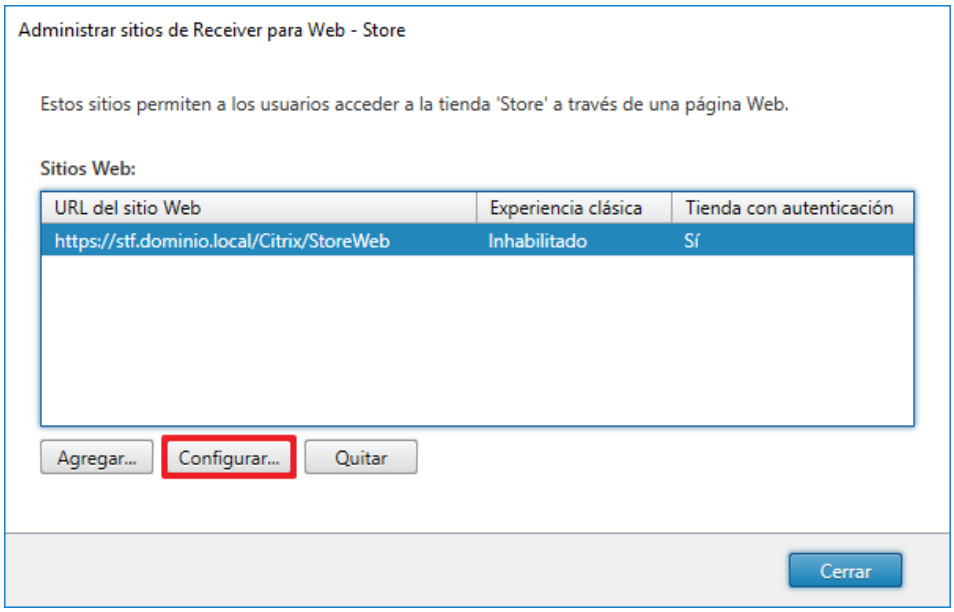
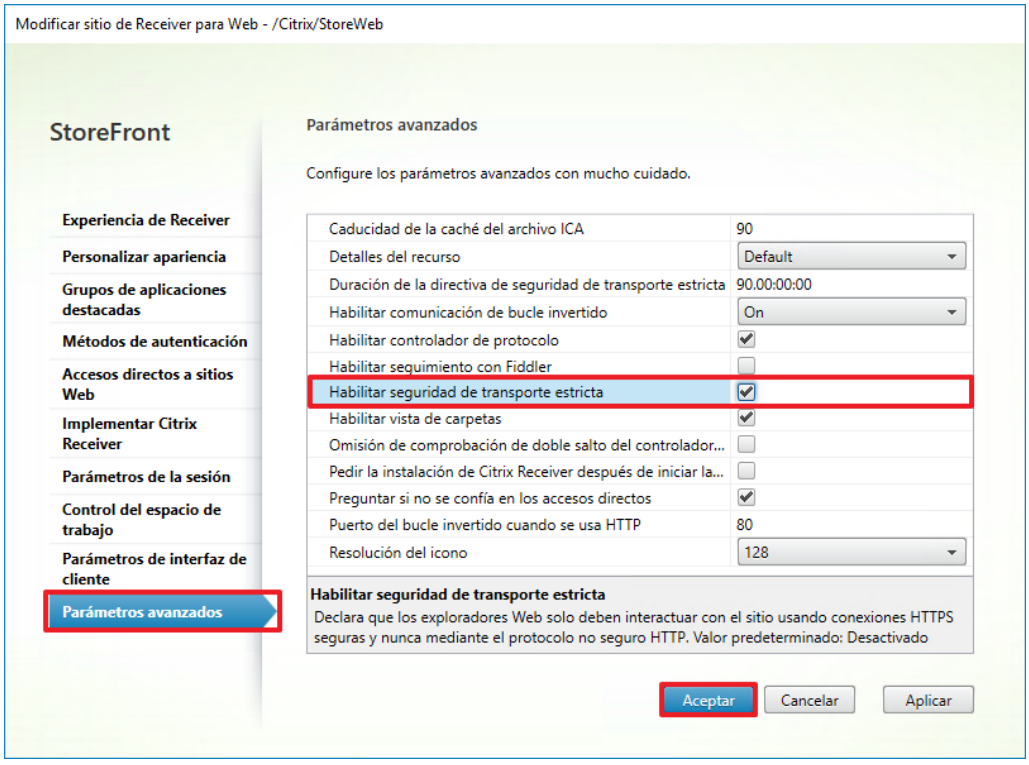
Paso	Descripción
88.	Se iniciará el asistente de importación de certificados. Pulse sobre “Equipo local” y a continuación pulse sobre “Siguiente”.  **Nota:** El sistema solicitará elevación de privilegios.
89.	Especifique el archivo a importar y continúe con el asistente pulsando sobre “Siguiente”. 

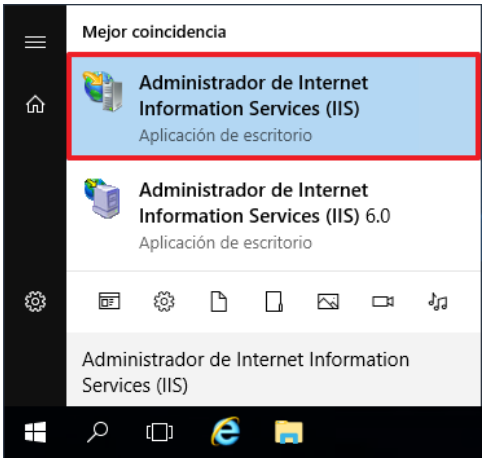
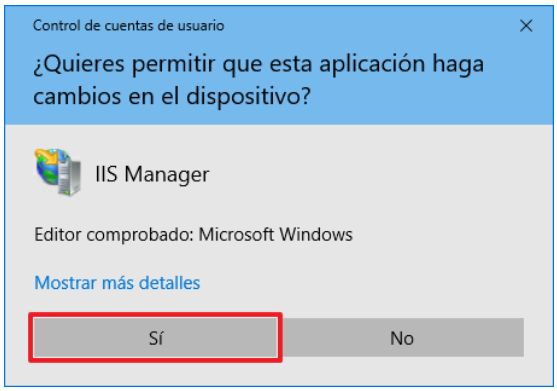
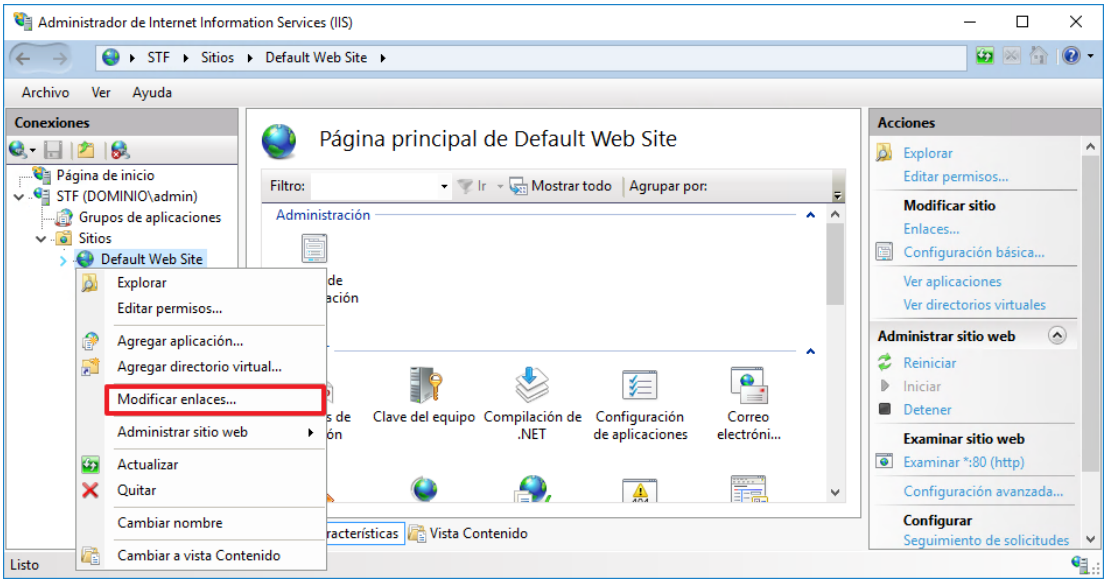
Paso	Descripción
90.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.  **Nota:** Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno. 

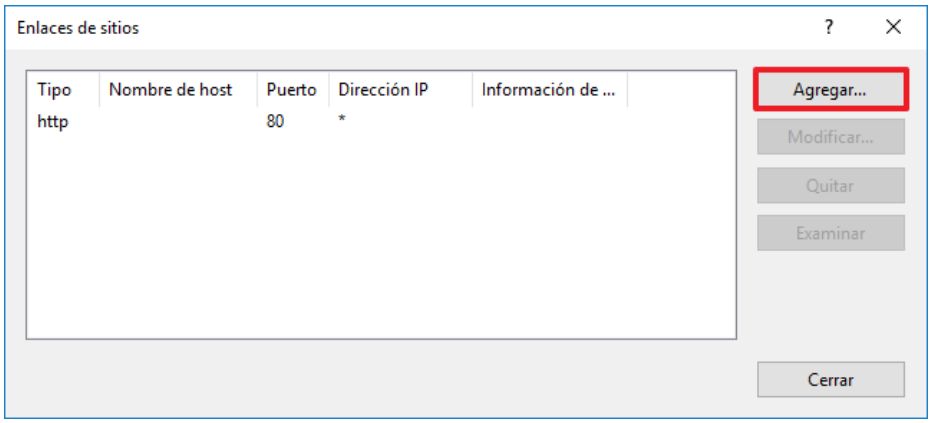
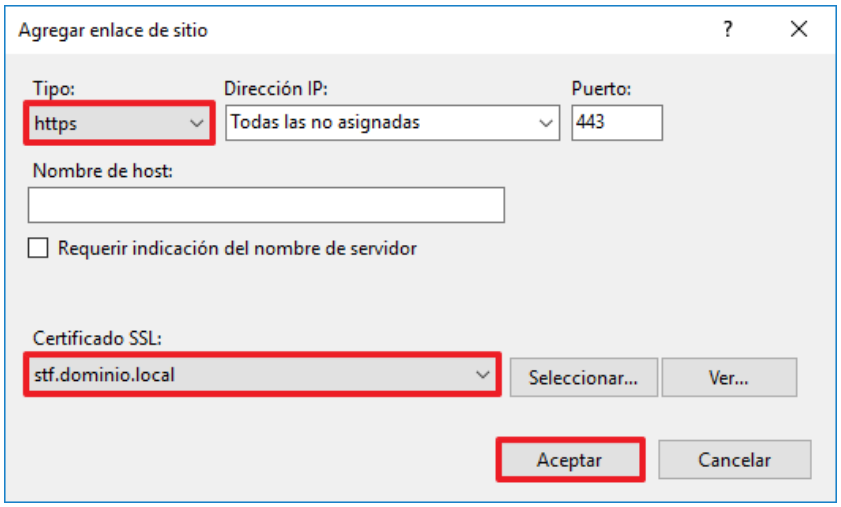
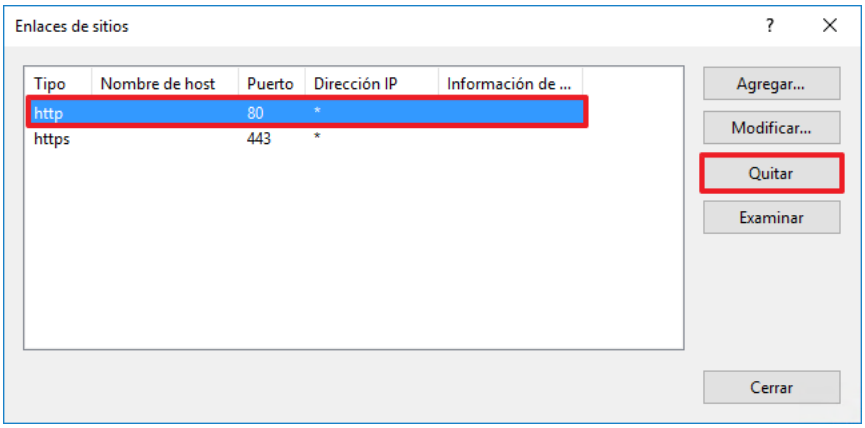
Paso	Descripción
91.	Localice el almacén personal del equipo pulsando sobre “Examinar” tal y como se muestra en la siguiente figura. Una vez establecido, pulse “Siguiente” para continuar. 
92.	El último punto del asistente muestra un resumen, pulse “Finalizar” para completar la importación del certificado sobre el equipo. 

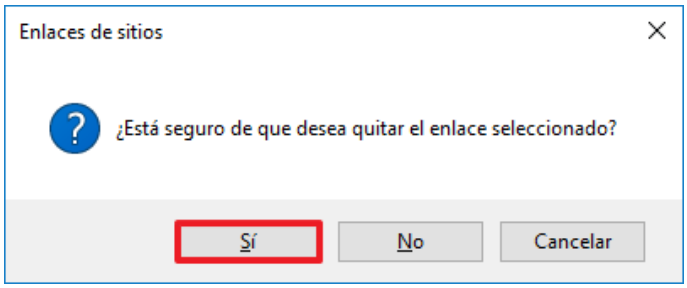
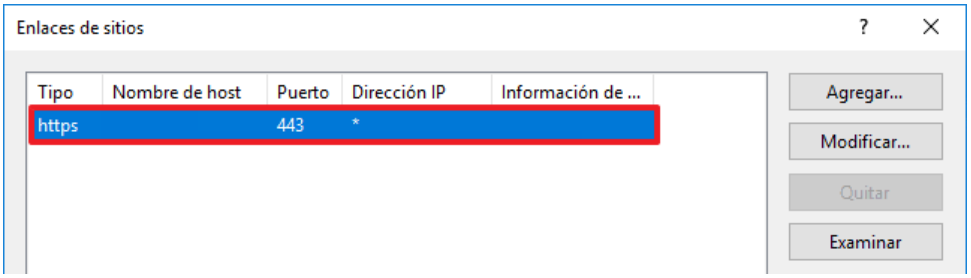
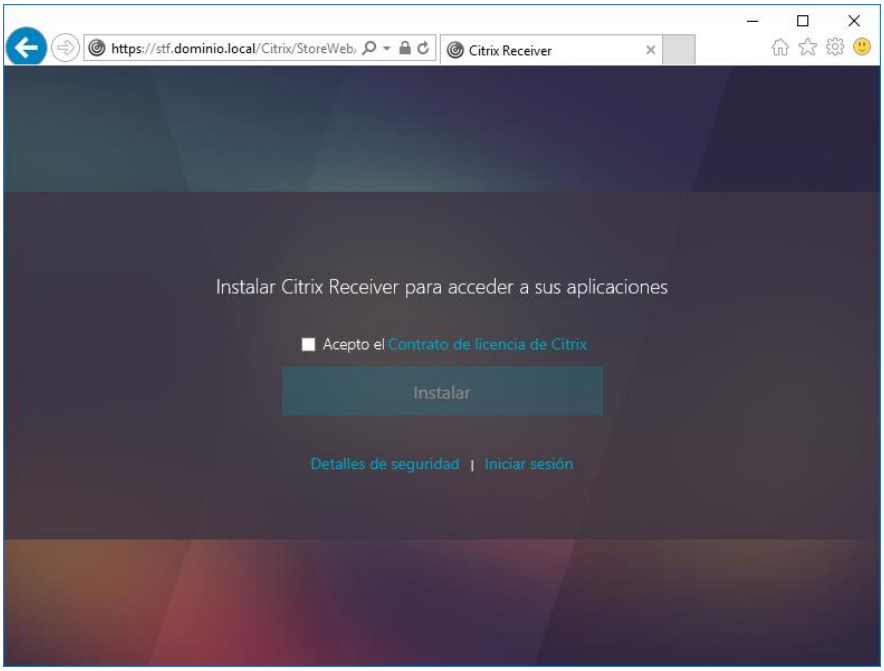
Paso	Descripción
93.	Espere unos segundos a que finalice el proceso, aparecerá un mensaje indicando que la importación se realizó correctamente. 
94.	A continuación, una vez importado el certificado, proceda a configurar la URL base del grupo de servidores. Abra la consola Citrix Storefront. 
95.	El sistema solicitará elevación de privilegios. Pulse “Si” para continuar. 

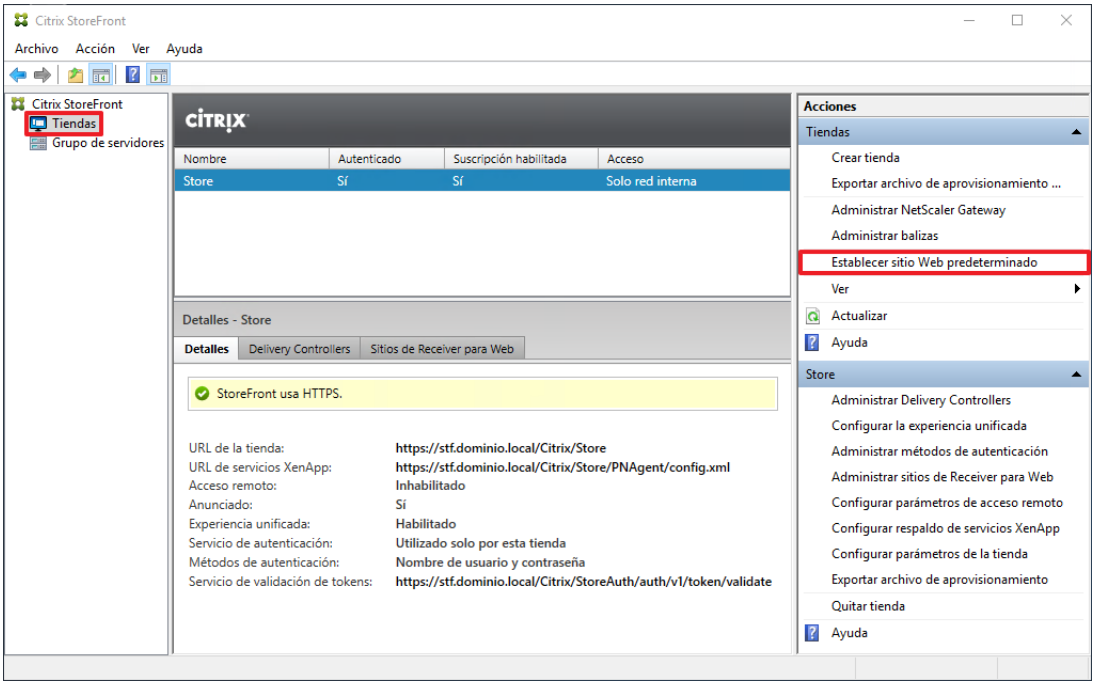
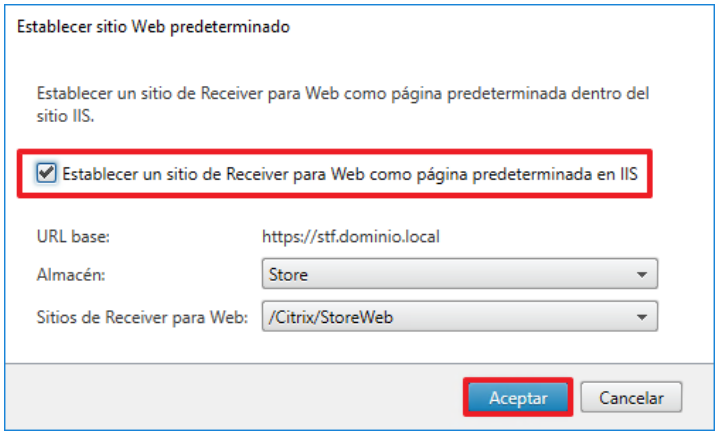
Paso	Descripción
96.	Dentro de la consola, diríjase al nodo de configuración **"Citrix Storefront → Grupo de servidores"** y pulse sobre **"Cambiar URL base"**. 
97.	Sobre la ventana emergente, establezca la URL, indicando el protocolo seguro HTTPS como se muestra en la siguiente figura. Pulse "Aceptar" para guardar los cambios. Acto seguido, verá reflejados los cambios. 
98.	A continuación, deberá configurar los parámetros de Receiver para Web, acceda al menú **"Tiendas → Store → Administrar sitios de Receiver para Web".** 

Paso	Descripción
99.	La ventana emergente le indicará los sitios creados. Pulse sobre **"Configurar…"**. 
100.	En el menú **"Modificar sitio de Receiver para Web"** diríjase al apartado **"Parámetros avanzados"** y marque la opción "Habilitar seguridad de transporte estricta".  **Nota:** La opción anterior deshabilita la posibilidad de conectarse a los sitios web de Citrix utilizando un protocolo no seguro como HTTP.

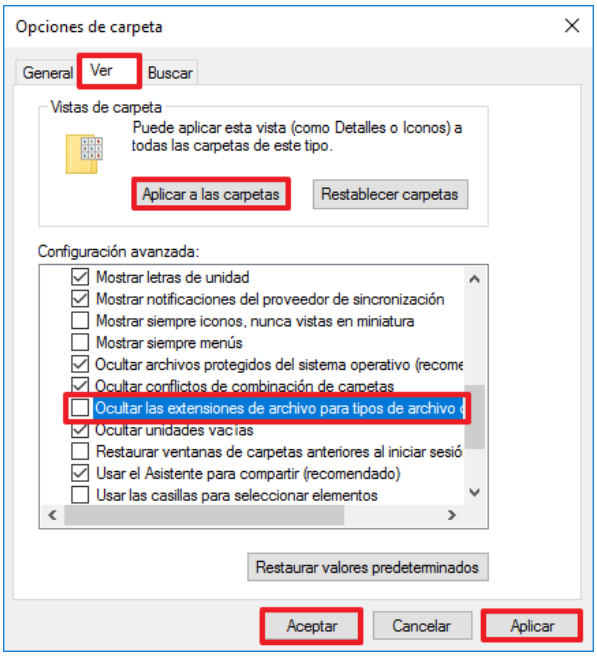
Paso	Descripción
101.	Continúe el proceso abriendo la consola **"Administrador de Internet Information Services (IIS)".** 
102.	El sistema solicitará elevación de privilegios, pulse "Sí" para continuar. 
103.	Abra el nodo de configuración **"<Su servidor>(Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"**. 

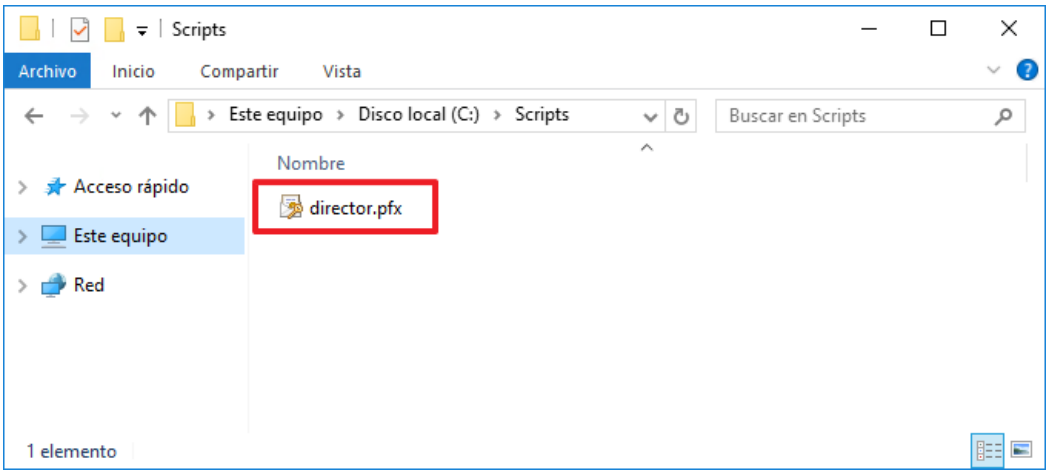
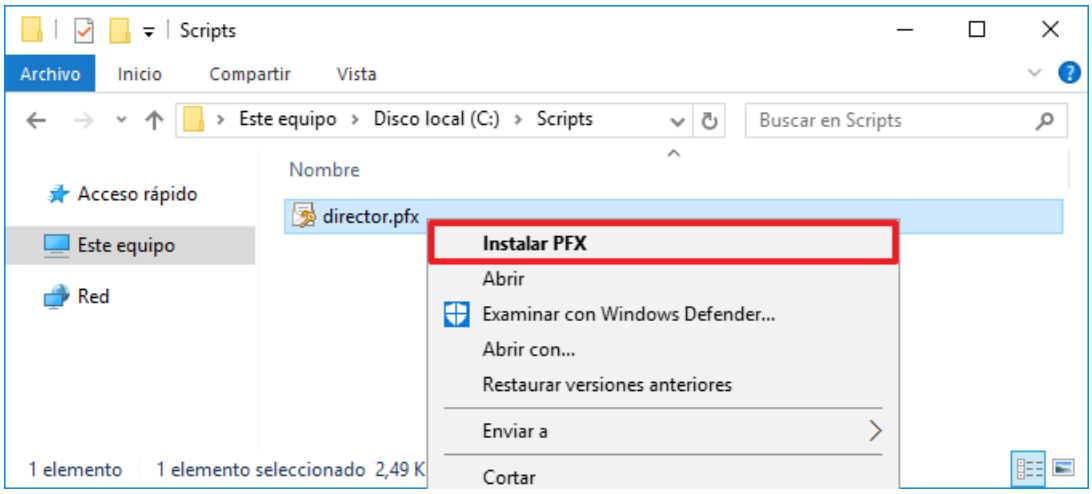
Paso	Descripción
104.	Sobre la ventana "Enlaces de sitios" pulse **"Agregar…"** para añadir un enlace nuevo. Por defecto, encontrará creado un enlace al puerto 80 que deberá eliminar más adelante para evitar conexiones no seguras al entorno. 
105.	Modifique en el formulario los parámetros necesarios y establezca su certificado SSL a utilizar, instalado en pasos anteriores. Pulse **"Aceptar"** para guardar los cambios". 
106.	Con ambos enlaces creados, seleccione el enlace de Tipo "http" y acto seguido pulse sobre **"Quitar"**. 

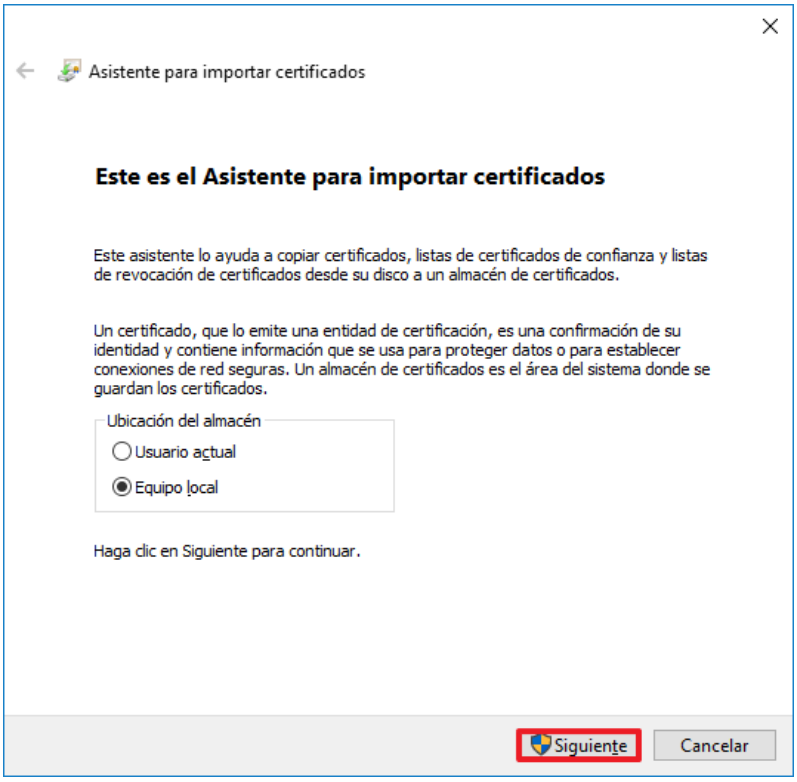
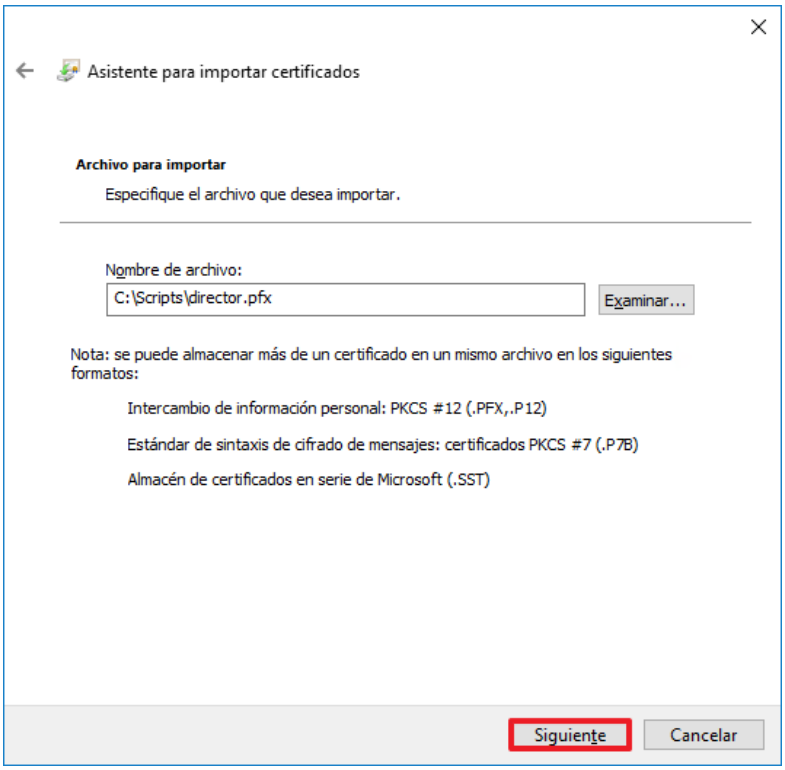
Paso	Descripción
107.	Sobre la ventana emergente, pulse “Si” para confirmar la eliminación del enlace seleccionado. 
108.	Al terminar, verifique que únicamente está configurado el enlace de tipo “https” recién creado con su certificado SSL. 
109.	Puede verificar que la configuración es correcta abriendo un Navegador y accediendo a la URL base de su entorno, en este caso, a modo de ejemplo se verifica el acceso a la dirección https://stf.dominio.local/Citrix/Storeweb.  **Nota:** Para realizar la prueba anterior, puede ser necesario que rebaje la seguridad de Internet Explorer habilitando JavaScript y las cookies en el navegador. No es necesario que realice ninguna acción sobre el propio servidor, únicamente verifique que tiene conectividad con la URL Base que ha definido y que el certificado utilizado es de confianza.

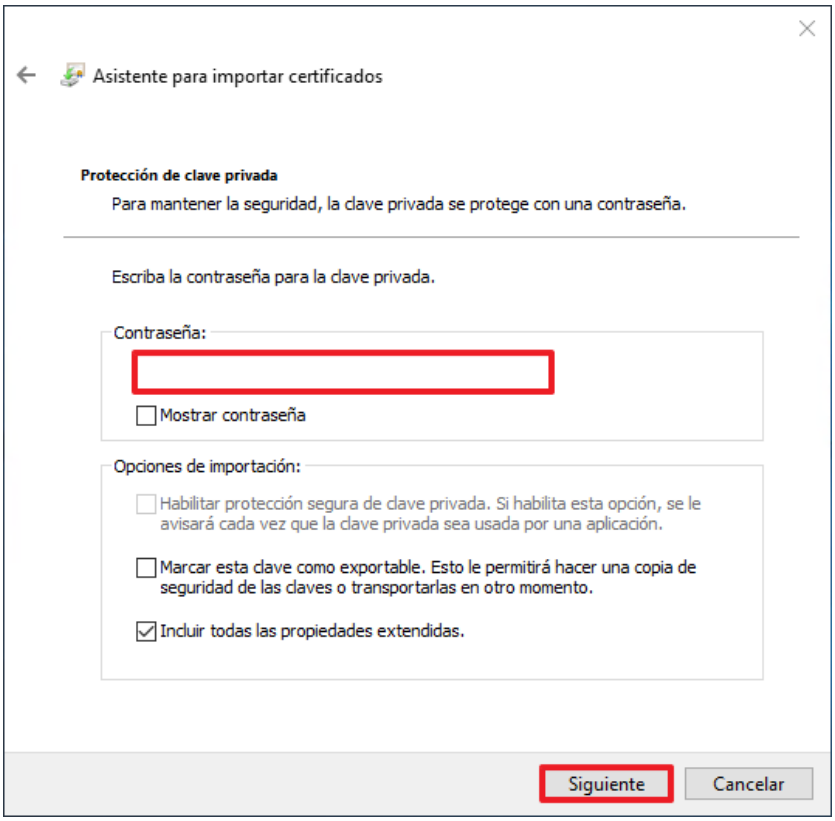
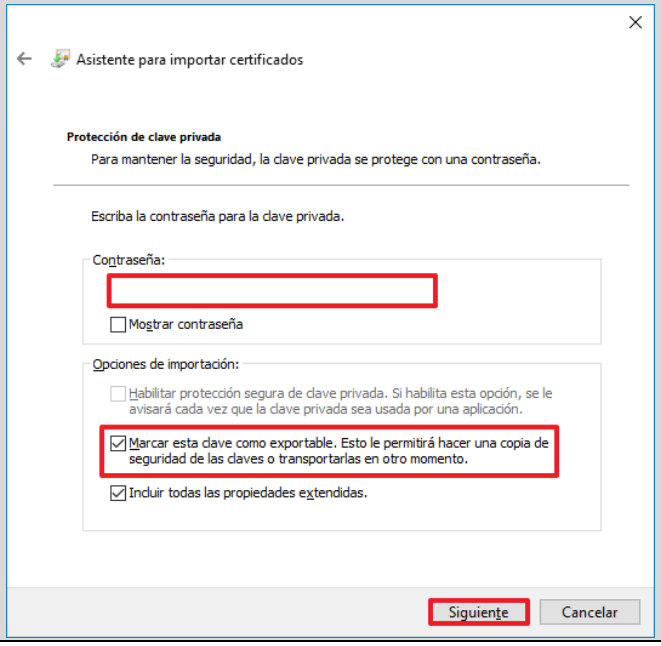
Paso	Descripción
110.	Dependiendo de su organización, y de las opciones seleccionadas durante la instalación del rol Citrix Storefront, es posible que no haya configurado su sitio web de Storefront como predeterminado en su servidor IIS. Si desea establecer su sitio de Receiver para web como página predeterminada de su servidor IIS acceda a **"Tiendas → Establecer sitio Web predeterminado"** dentro de la consola de "Citrix Storefront". 
111.	Marque la opción "Establecer un sitio de Receiver para Web como página predeterminada en IIS" y seleccione las opciones que se ajusten a las necesidades de su organización. Pulse "Aceptar" para guardar la configuración. 
112.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta "C:\Scripts" del servidor.

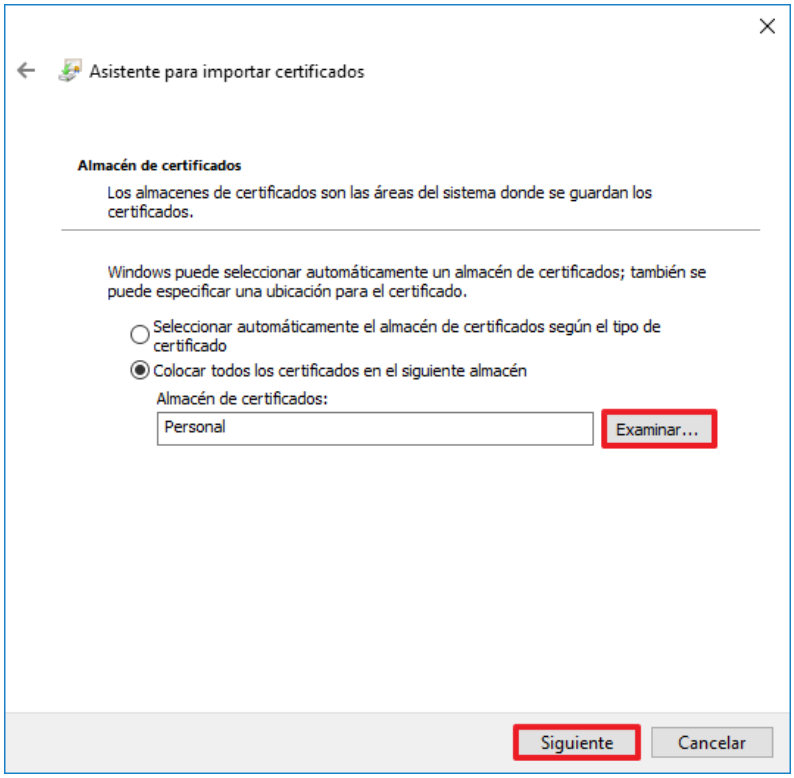
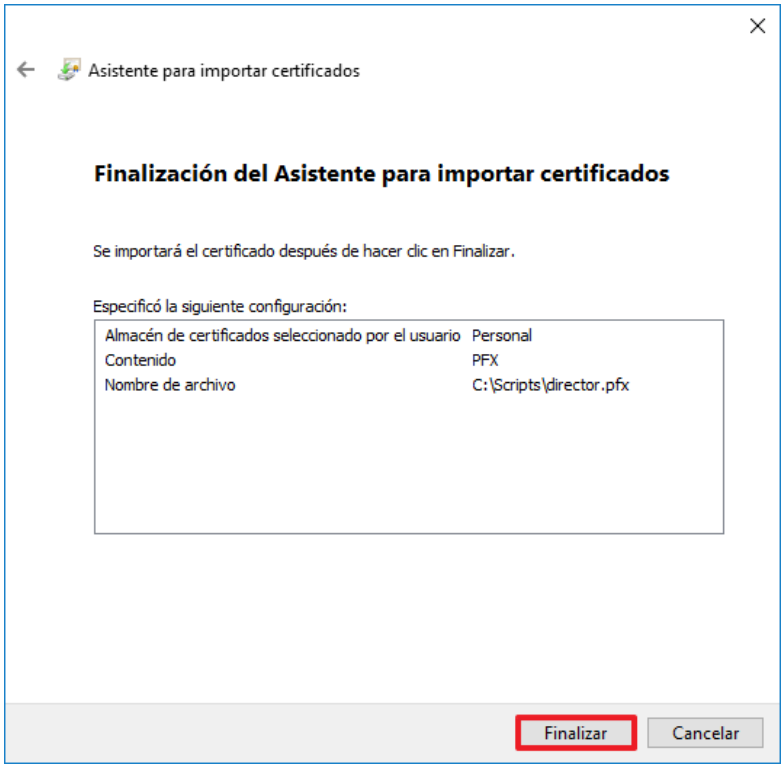
En este punto el servidor Citrix Storefront se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura. Una vez configurado el servidor con el rol Citrix Storefront deberá continuar con las configuraciones sobre el servidor con el rol Citrix Director.

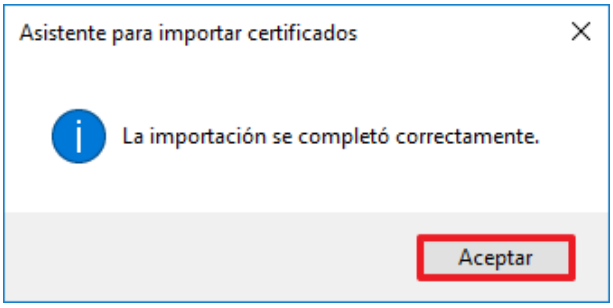
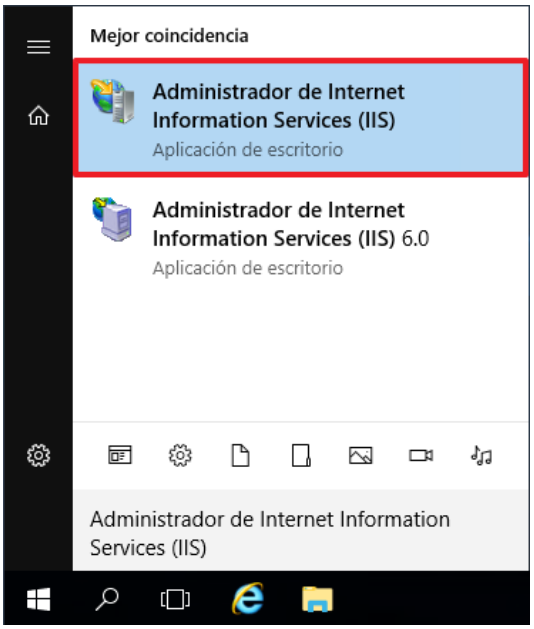
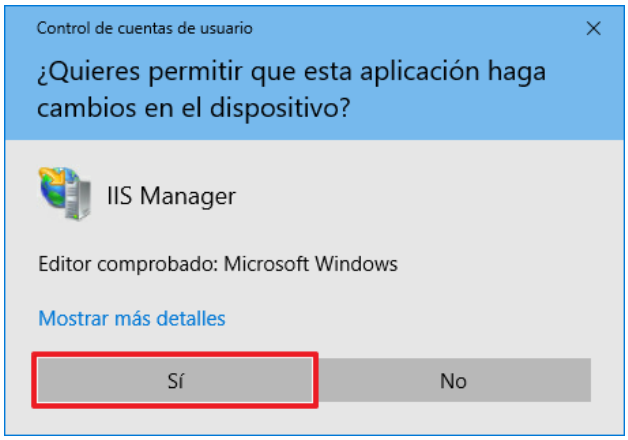
Paso	Descripción
113.	Inicie sesión en un servidor con el rol Citrix Director del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
114.	Cree el directorio “Scripts” en la unidad “C:\”.
115.	Configure el “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. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

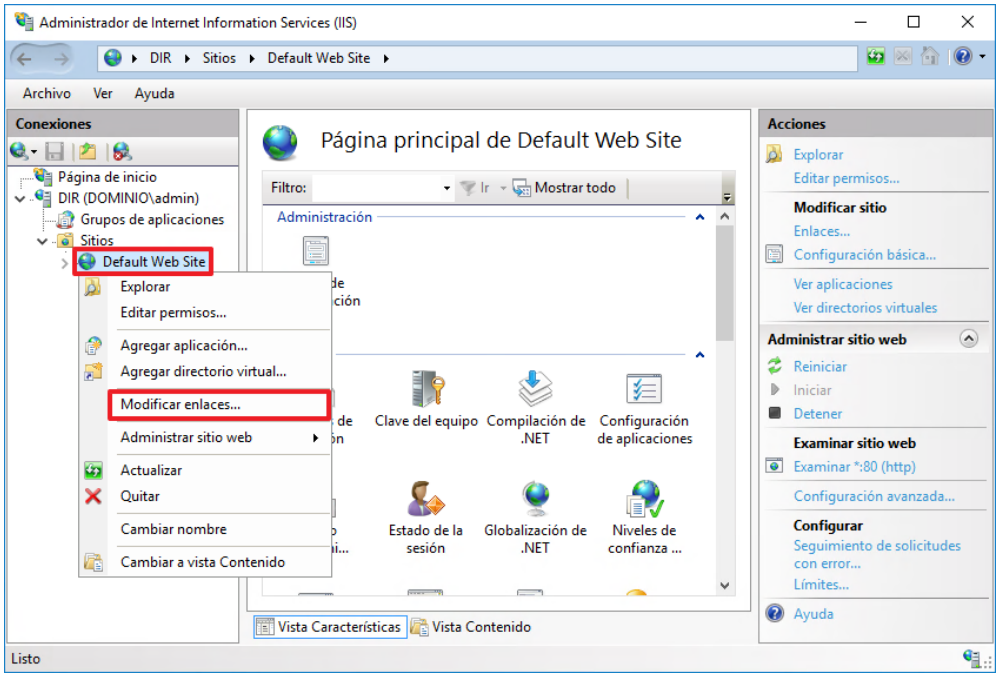
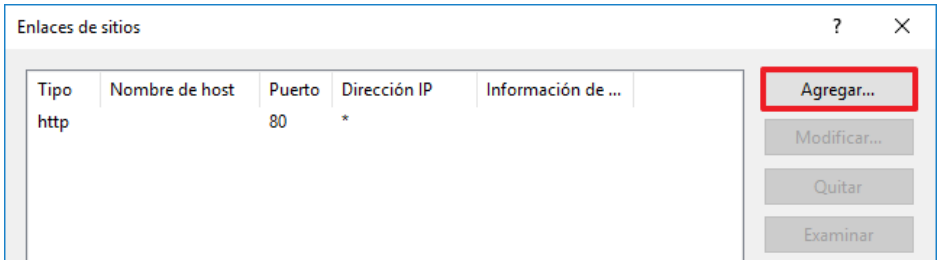
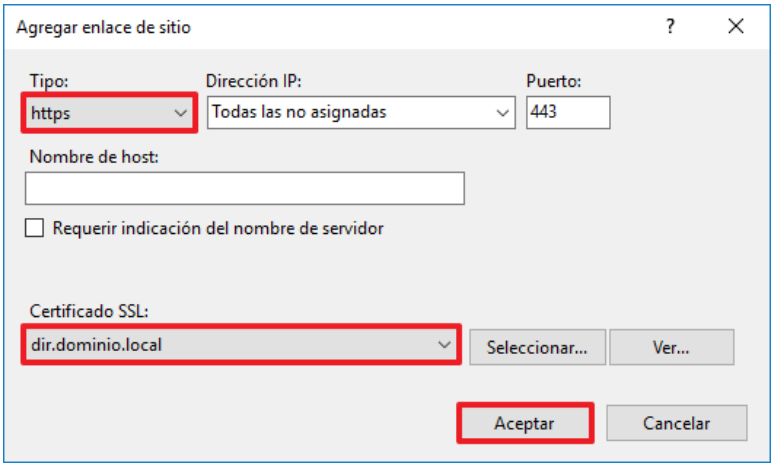
Paso	Descripción
116.	Para continuar, debe realizar la solicitud de un certificado válido en el dominio, cuyo Nombre común "CN" coincida con el FQDN del equipo sobre el que está implementando el rol Citrix Director. No debe utilizar un certificado de tipo wildcard ya que de utilizarlo encontrará problemas en los siguientes pasos de configuración. **Nota:** No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.
117.	Copie el certificado en la unidad "C:\Scripts" y establezca un nombre de fichero identificativo. En esta guía se utilizará el fichero **"C:\Scripts\director.pfx"** a modo de ejemplo, no dude en ajustar el nombre de su archivo en los siguientes pasos. 
118.	Si no lo ha hecho todavía, proceda con los siguientes pasos para realizar la instalación del certificado sobre el almacén **"Personal"** de equipo.
119.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **"Instalar PFX"** tal y como se indica en la siguiente figura. 

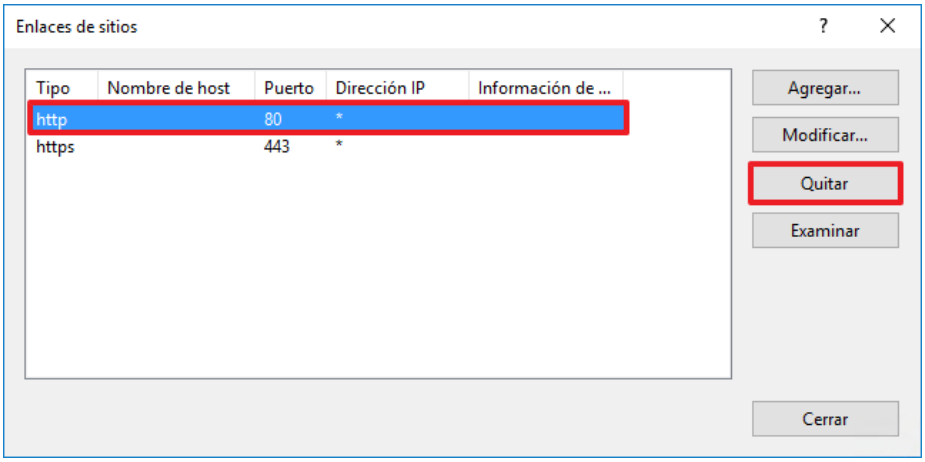
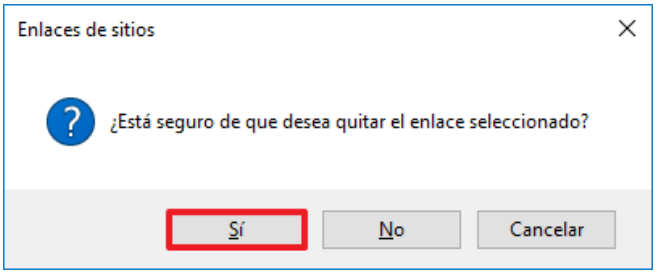
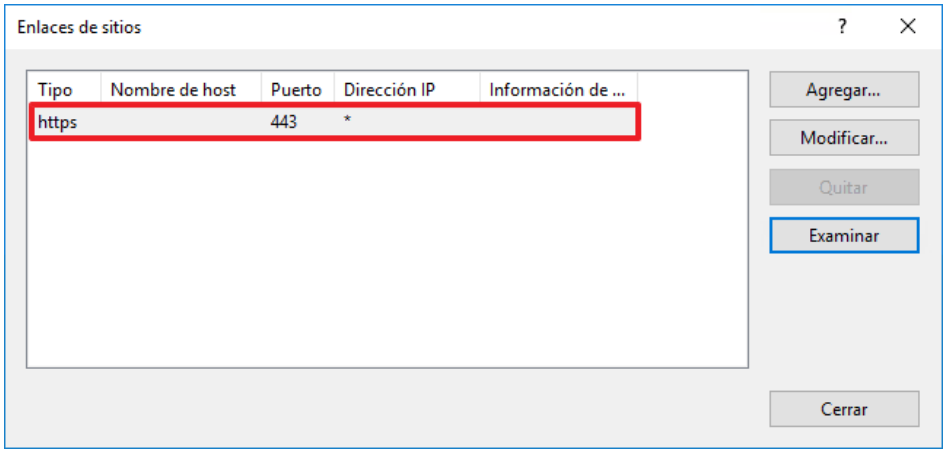
Paso	Descripción
120.	Se iniciará el asistente de importación de certificados. Pulse sobre “Equipo local” y a continuación pulse sobre “Siguiente”.  **Nota:** El sistema solicitará elevación de privilegios.
121.	Especifique el archivo a importar y continúe con el asistente pulsando sobre “Siguiente”. 

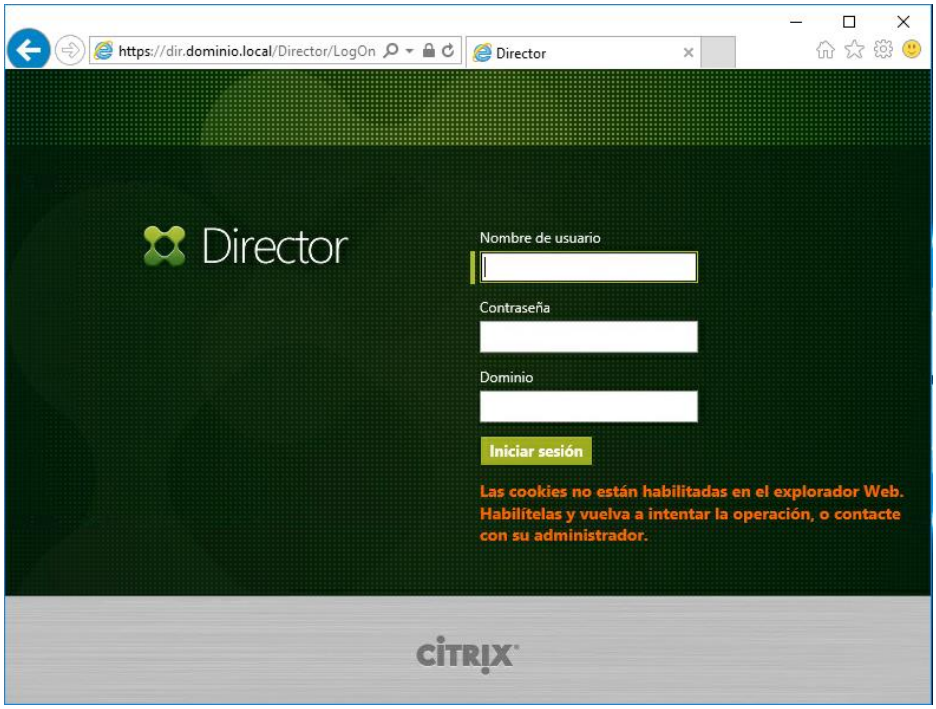
Paso	Descripción
122.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.  **Nota:** Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno. 

Paso	Descripción
123.	Localice el almacén “Personal” del equipo pulsando sobre “Examinar” tal y como se muestra en la siguiente figura. Una vez establecido, pulse “Siguiente” para continuar. 
124.	El último punto del asistente muestra un resumen, pulse “Finalizar” para completar la importación del certificado sobre el equipo. 

Paso	Descripción
125.	Espere unos segundos a que finalice el proceso, aparecerá un mensaje indicando que la importación se realizó correctamente. 
126.	Acto seguido, verá reflejados los cambios, continúe el proceso abriendo la consola **"Administrador de Internet Information Services (IIS)"**. 
127.	El sistema solicitará elevación de privilegios, pulse "Sí" para continuar. 

Paso	Descripción
128.	Abra el nodo de configuración **"<Su servidor> (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"**. 
129.	Sobre la ventana "Enlaces de sitios" pulse **"Agregar…"** para añadir un enlace nuevo. Por defecto, encontrará creado un enlace al puerto 80 que deberá eliminar más adelante para evitar conexiones no seguras al entorno. 
130.	Modifique en el formulario los parámetros necesarios y establezca su certificado SSL a utilizar, instalado en pasos anteriores. Pulse **"Aceptar"** para guardar los cambios". 

Paso	Descripción
131.	Con ambos enlaces creados, seleccione el enlace de Tipo “http” y acto seguido pulse sobre **“Quitar”**. 
132.	Sobre la ventana emergente, pulse “Si” para confirmar la eliminación del enlace seleccionado. 
133.	Al terminar, verifique que únicamente está configurado el enlace de Tipo “https” recién creado con su certificado SSL. 

Paso	Descripción
134.	Puede verificar que la configuración es correcta abriendo un navegador y accediendo a la URL base de su entorno, en este caso, a modo de ejemplo se verifica el acceso a la dirección https://dir.dominio.local/director.  **Nota:** Es posible que no tenga la herramienta "JavaScript" instalada en el equipo desde el que está accediendo al portal web. Será necesario realizar dicho proceso para el correcto funcionamiento del explorador. 
135.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta "C:\Scripts" del servidor.

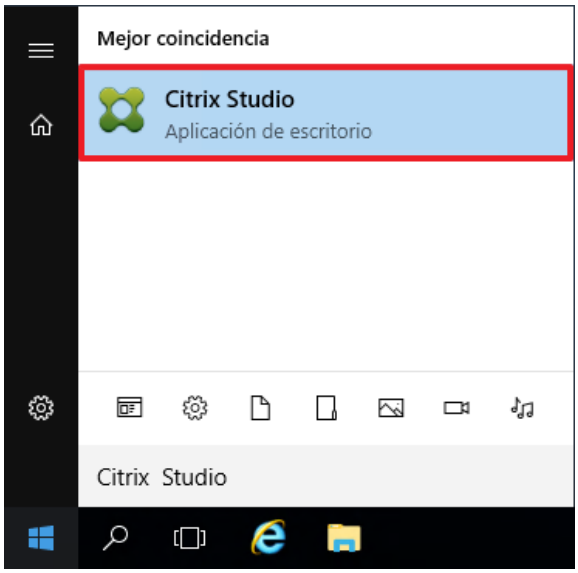
En este punto el servidor con el rol de Citrix Director se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura.

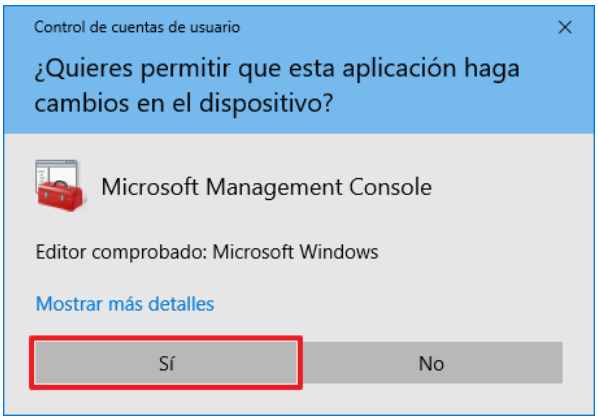
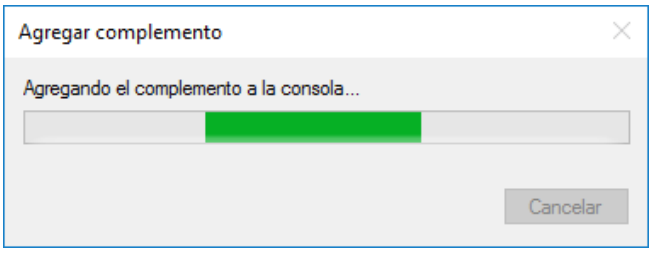
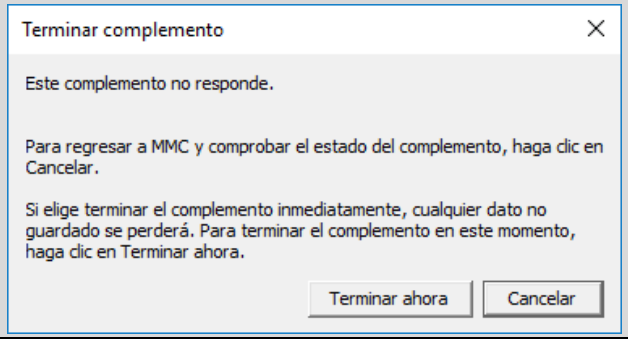
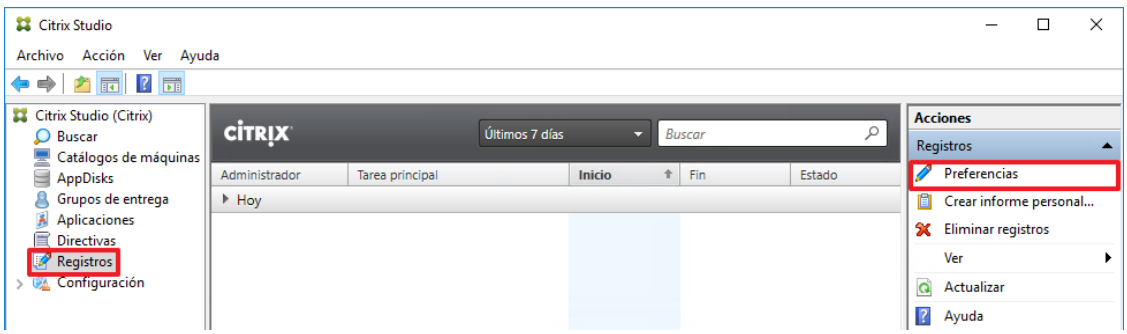
3. AUDITORÍA

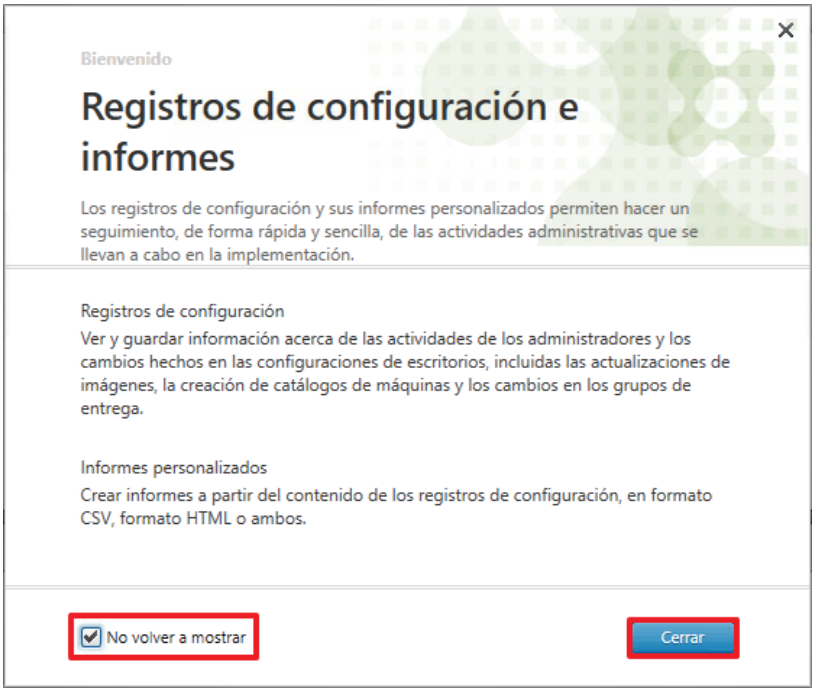
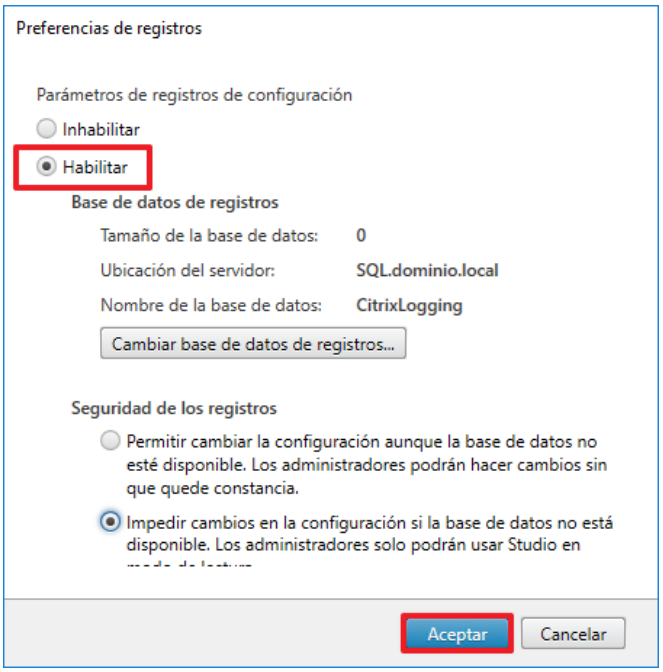
Con la aplicación del ENS para la categoría básica sobre Citrix Virtual Apps and Desktops quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

Para la categoría básica de seguridad del ENS deberá definir como "Habilitados" los registros sobre las modificaciones que se hagan en la infraestructura de Citrix Virtual Apps and Desktops.

Para ello, será necesario comprobar sobre el rol Citrix Controller que dicha configuración se encuentre configurada correctamente.

Paso	Descripción
136.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
137.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio. 

Paso	Descripción
138.	El sistema solicitará elevación de privilegios. Pulse “Si” para continuar. 
139.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse “Cancelar” para continuar. 
140.	A continuación, diríjase al nodo de configuración **“Citrix Studio → Registros → Acciones”** y pulse sobre “Preferencias”. 

Paso	Descripción
141.	Al navegar por primera vez por los diferentes nodos de la herramienta aparecerán distintos mensajes de bienvenida, marque la casilla “No volver a mostrar” y pulse “Cerrar” en cada uno de ellos. 
142.	Sobre la ventana emergente “Preferencias de registros” compruebe que la opción **“Habilitar”** se encuentra seleccionada como se indica en la siguiente figura. Pulse “Aceptar” para continuar. 

4. GESTIÓN DE DERECHOS DE ACCESO

Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda realizar tareas que no son requeridas para las funciones que desempeña.

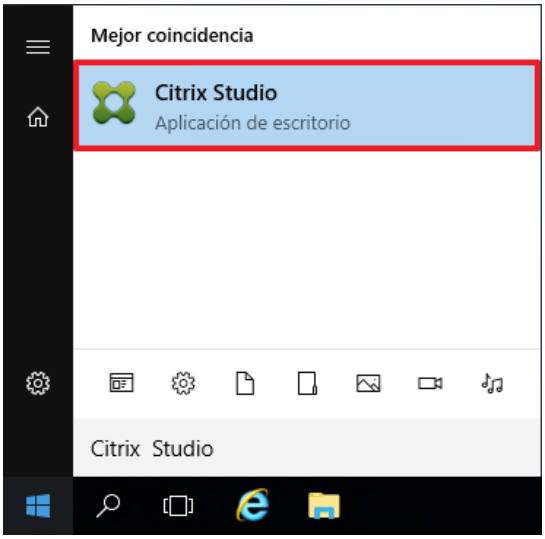
Para tal fin y de acuerdo con el Esquema Nacional de Seguridad se deberán definir, mediante grupos de seguridad, los usuarios que según su organización deban administrar la infraestructura y eliminar aquellos administradores genéricos que puedan existir.

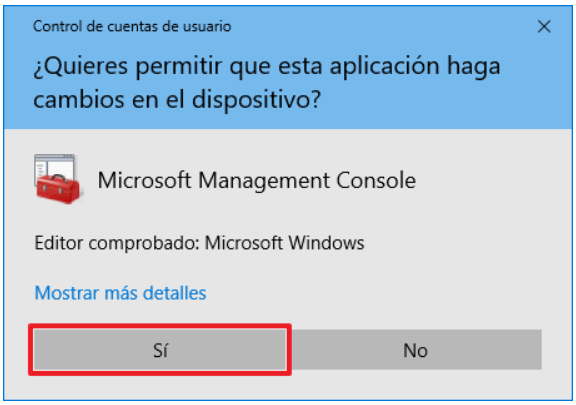
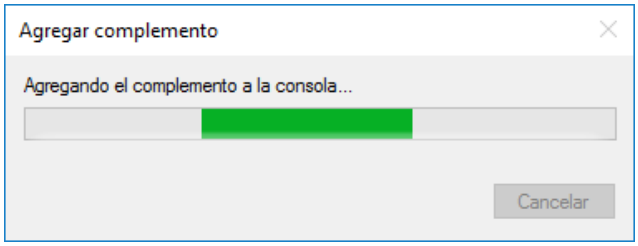
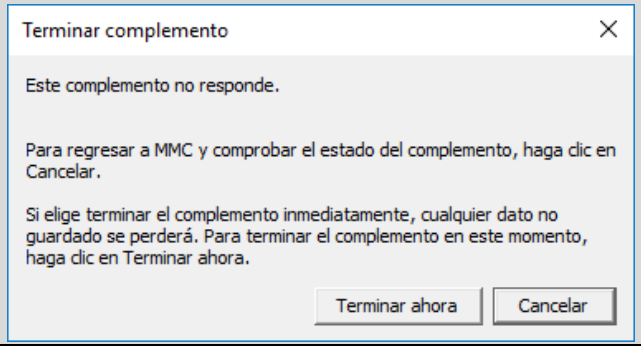
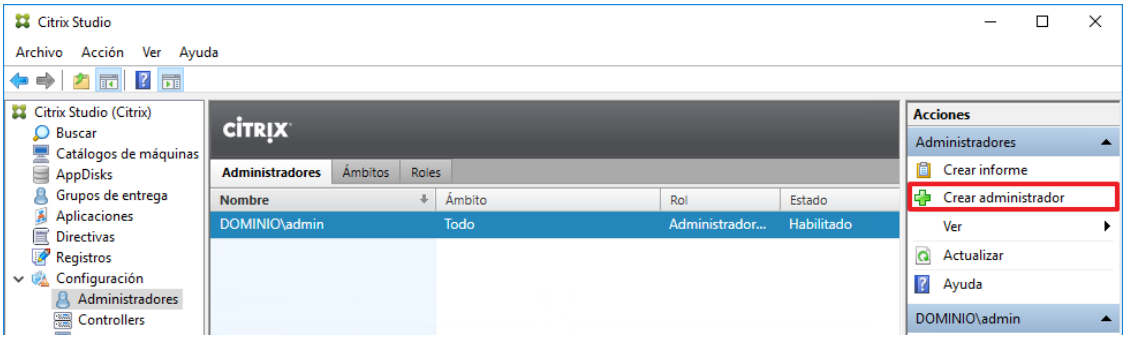
Esta configuración será de aplicación en los siguientes servidores de su infraestructura Citrix Virtual Apps and Desktops:

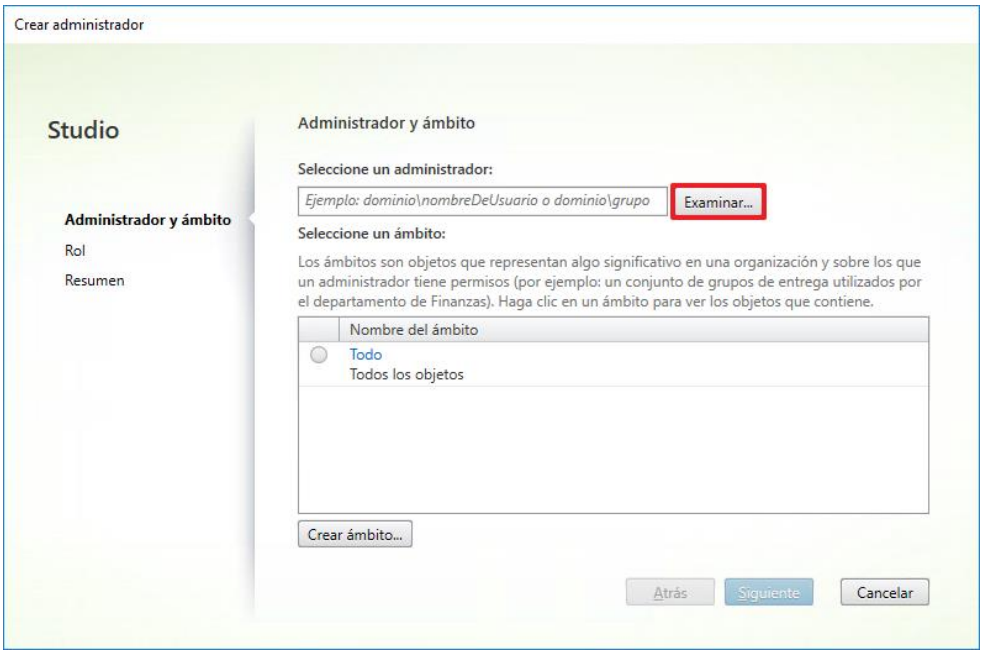
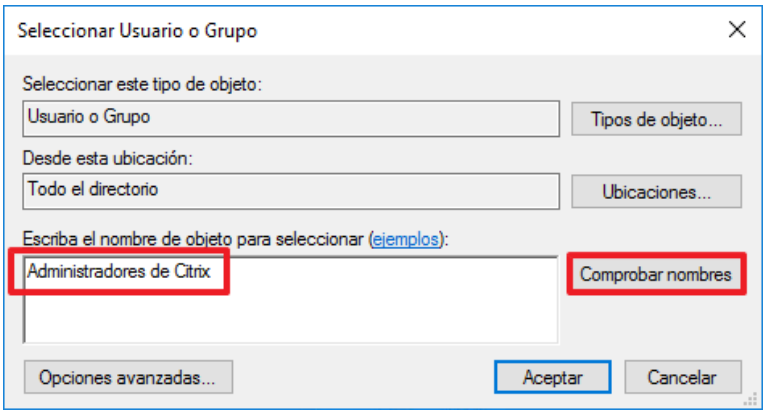
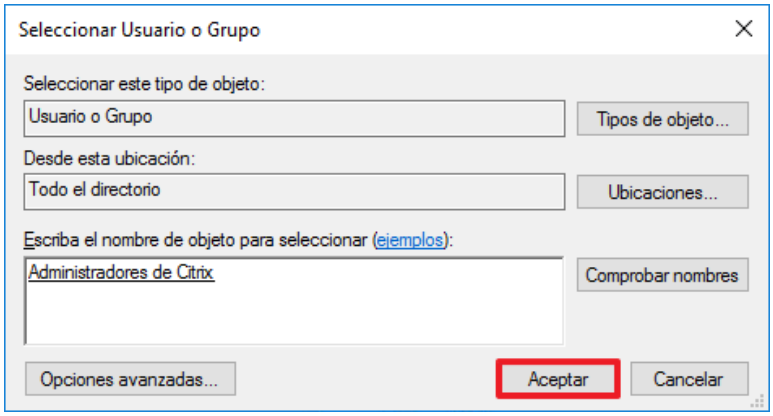
a) Servidor con el rol Citrix Controller

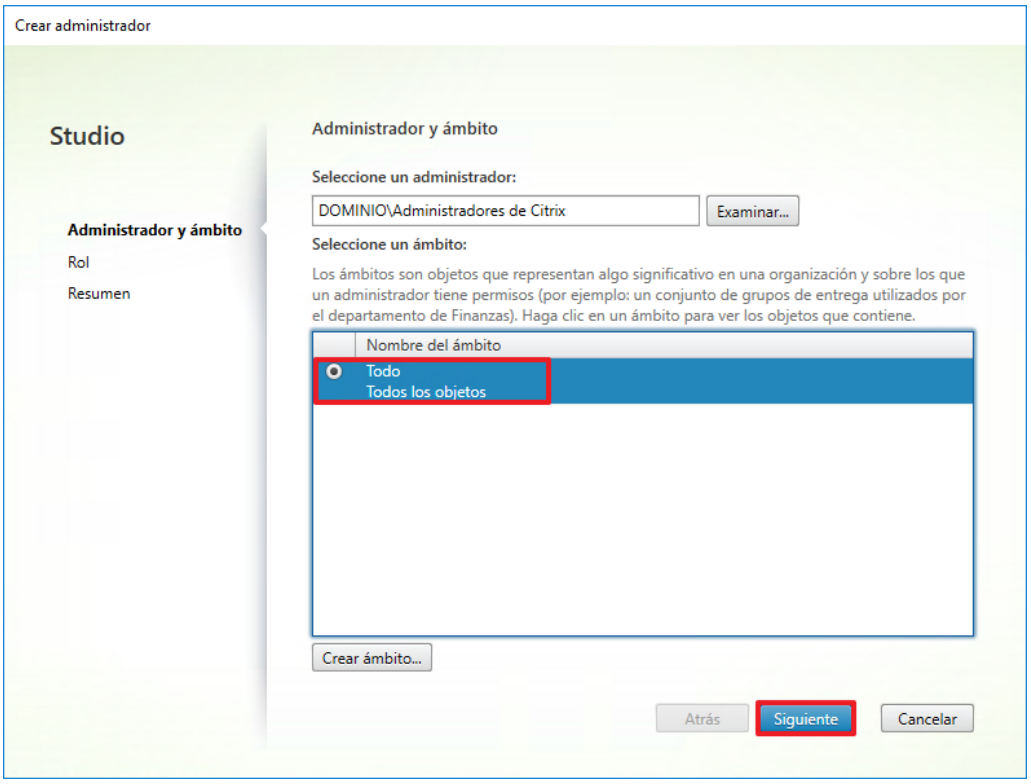
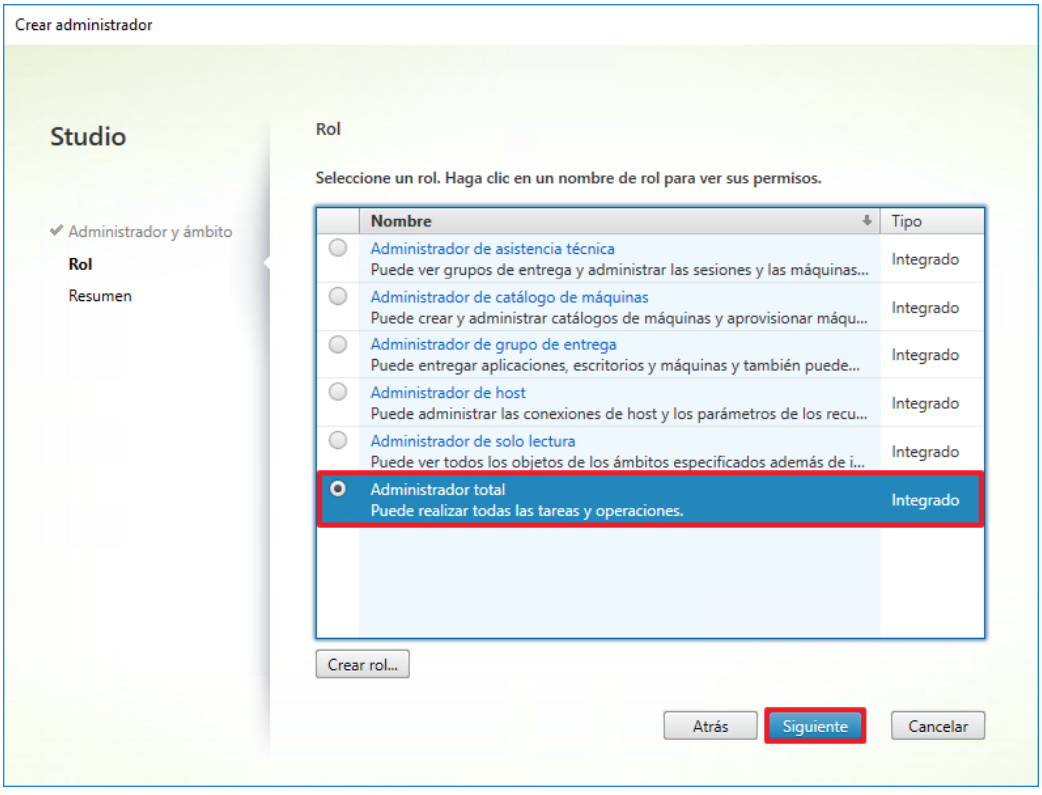
b) Servidor con el rol Citrix Licensing

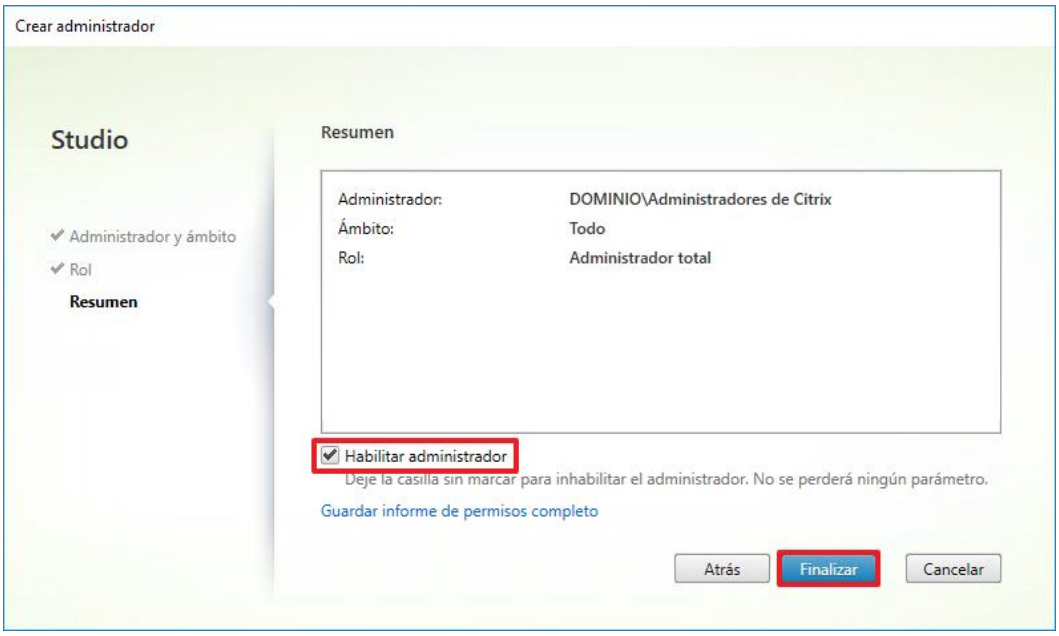
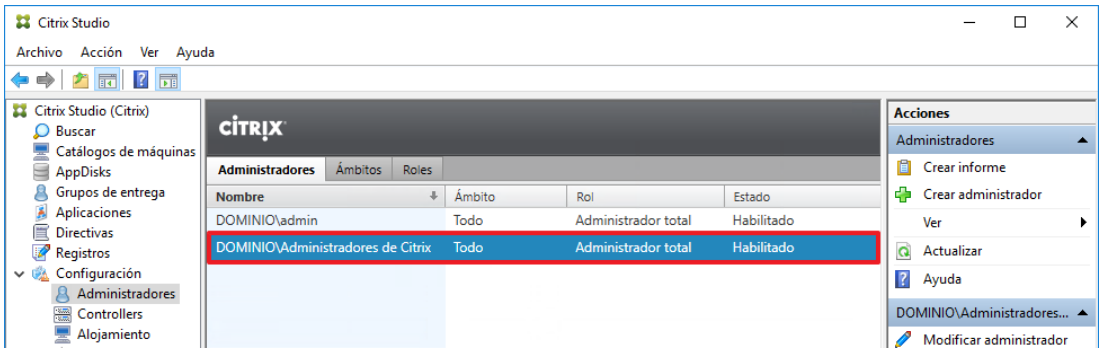
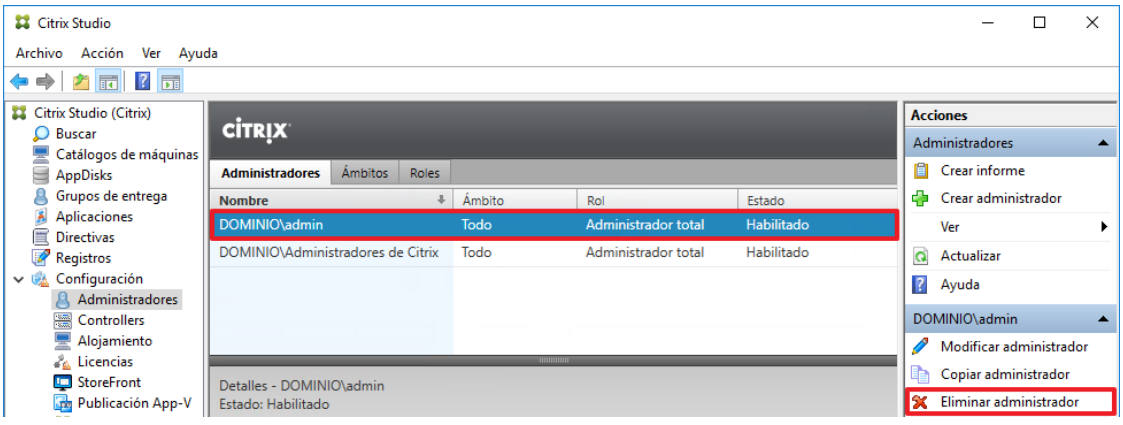
En primer lugar, se realizarán las configuraciones necesarias sobre el servidor con el rol Citrix Controller instalado.

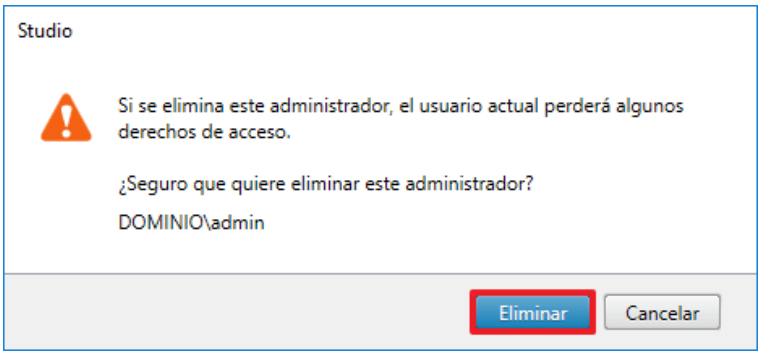
Paso	Descripción
143.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
144.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio. 

Paso	Descripción
145.	El sistema solicitará elevación de privilegios, pulse “Sí” para continuar. 
146.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse “Cancelar” para continuar. 
147.	Diríjase al menú de configuración **“Citrix Studio → Configuración → Administradores → Administradores”** y pulse sobre “Crear administrador”. 

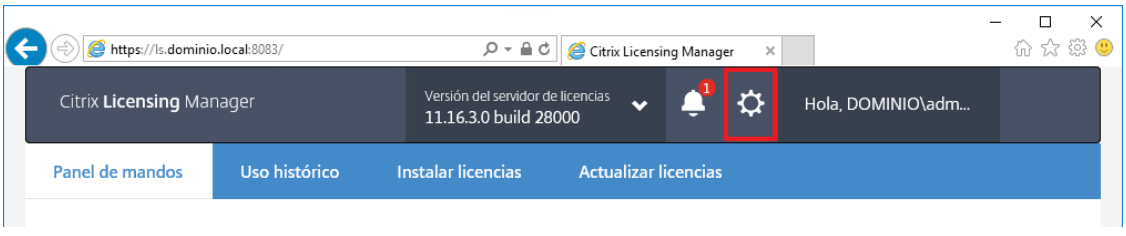
Paso	Descripción
148.	Sobre la ventana emergente, “Crear administrador” pulse sobre “Examinar”. 
149.	Introduzca el nombre del objeto “Administradores de Citrix” y pulse sobre “Comprobar nombres”. 
150.	Compruebe que el objeto “Administradores de Citrix” ha sido añadido correctamente. Pulse “Aceptar” para añadir el objeto y cerrar la ventana. 

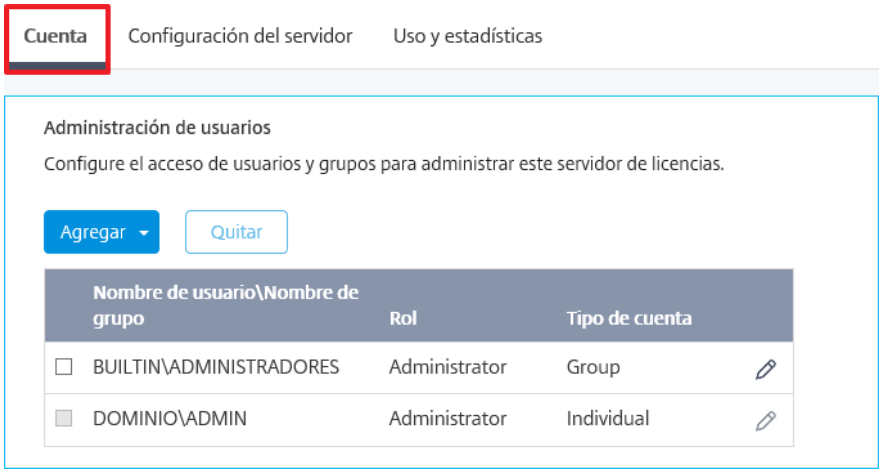
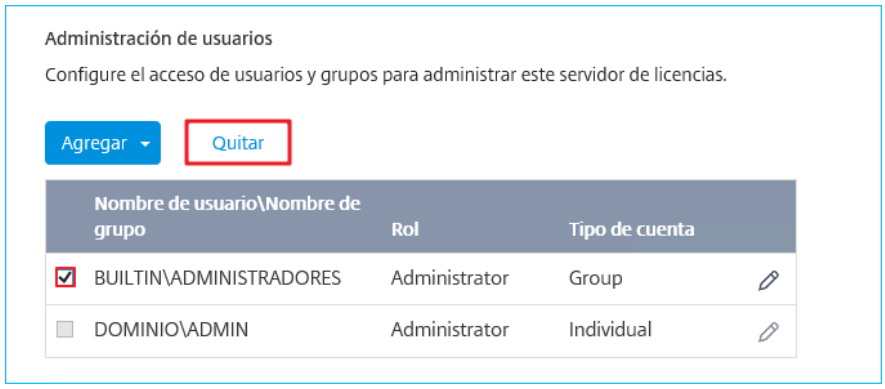
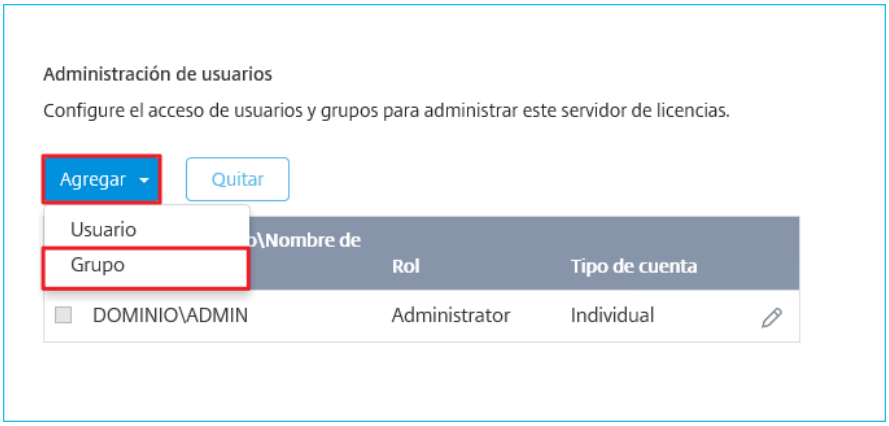
Paso	Descripción
151.	De vuelta en la ventana “Crear administrador”, seleccione el ámbito “Todo” y pulse “Siguiente”. 
152.	Marque el rol “Administrador total” y pulse sobre “Siguiente”. 

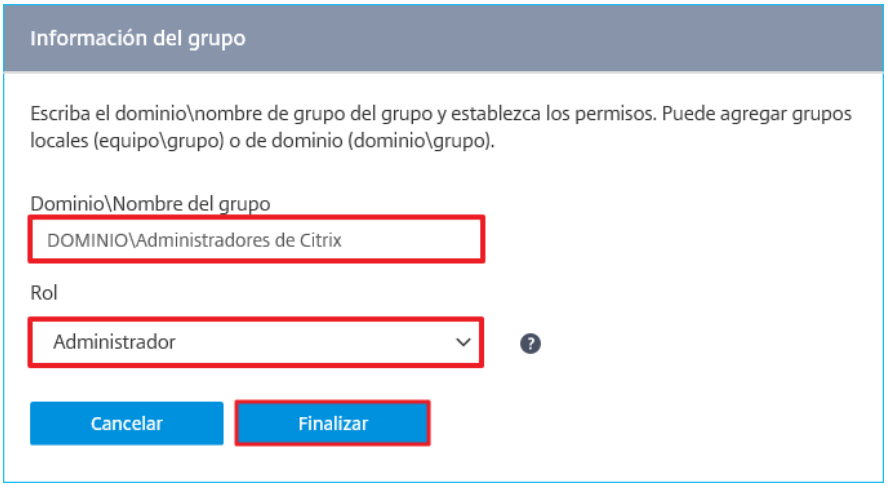
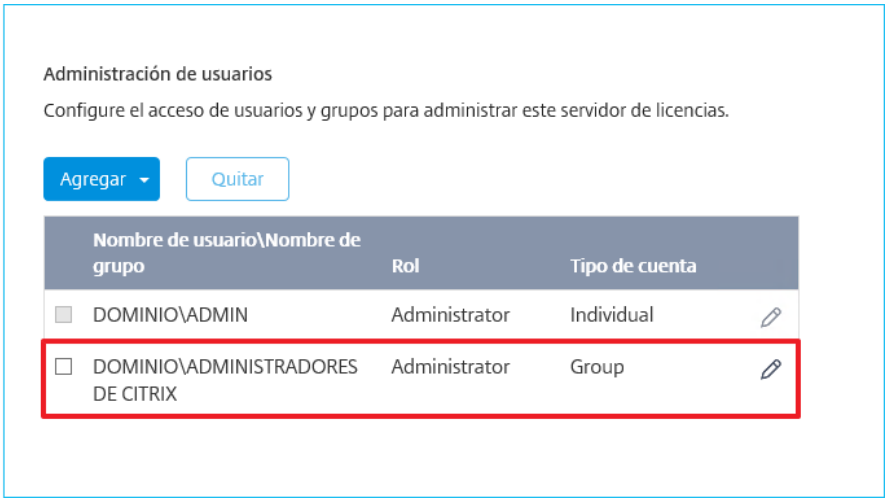
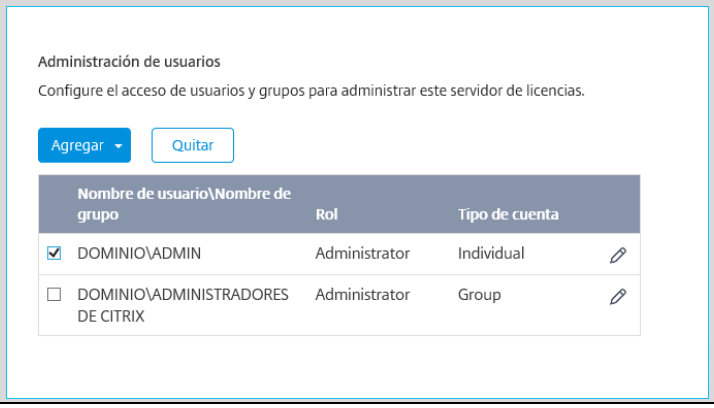
Paso	Descripción
153.	Verifique que la casilla **"Habilitar administrador"** está marcada y pulse sobre "Finalizar". 
154.	Acto seguido apreciará el grupo recientemente creado en la consola. 
155.	Para finalizar con el proceso debe eliminar cualquier usuario administrador que esté introducido a mano en el sistema. Marque el usuario y pulse sobre "Eliminar administrador". 

Paso	Descripción
156.	El sistema le indicará una advertencia indicando que el usuario actual perderá algunos derechos de acceso. Ignore la advertencia y pulse sobre “Eliminar”. 

A continuación, se procederá a realizar las configuraciones de seguridad necesarias en el servidor con el rol Citrix Licensing.

Paso	Descripción
157.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
158.	Acceda a la dirección URL del “Citrix Licensing Manager” https://ls.dominio.local:8083 adaptándolo a su entorno.
159.	Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre la rueda superior derecha. 

Paso	Descripción
160.	A continuación, acceda al nodo de configuración “Cuenta”, en los siguientes pasos definirá los administradores de licencias del servidor. Por defecto, el instalador del producto define los siguientes administradores. – BUILTIN\ADMINISTRADORES – DOMINIO\ADMIN  **Nota:** El usuario “DOMINIO\admin” se corresponde con el usuario utilizado para realizar el proceso de instalación del sistema y variará dependiendo de su entorno.
161.	Seleccione el grupo “BUILTIN\ADMINISTRADORES” y acto seguido pulse sobre el botón “Quitar”. 
162.	Despliegue el menú extraíble pulsando sobre el botón “Agregar” y pulse sobre “Grupo”. 

Paso	Descripción
163.	En la ventana emergente de configuración especifique el grupo creado anteriormente “DOMINIO\Administradores de Citrix” que deberá tener el rol “Administrador”. Pulse sobre “Finalizar” para añadir el nuevo grupo administrador. 
164.	Verifique que el grupo se ha agregado correctamente desde el apartado “Cuenta”.  **Nota:** Para eliminar el usuario con el que realizó la instalación deberá acceder al servidor con otro usuario diferente que pertenezca al grupo “DOMINIO\Administradores de Citrix” y proceder con su eliminación como en pasos anteriores. 

5. 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.

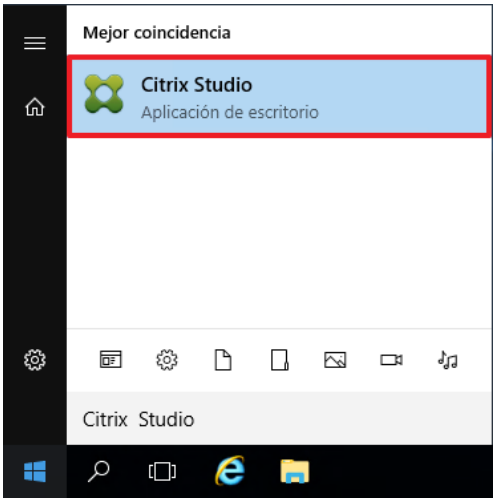
En el procedimiento que se describe a continuación, se desactiva el "Citrix Customer Experience Improvement Program" para evitar el envío de información al fabricante.

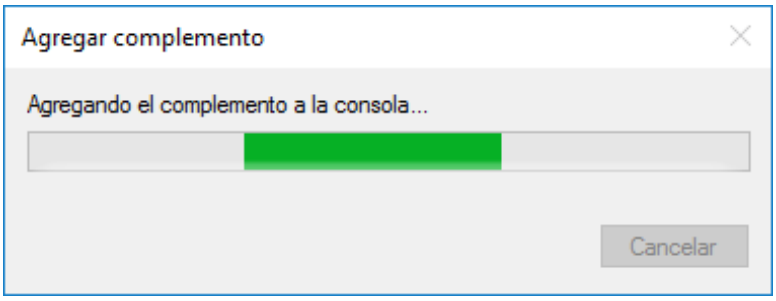
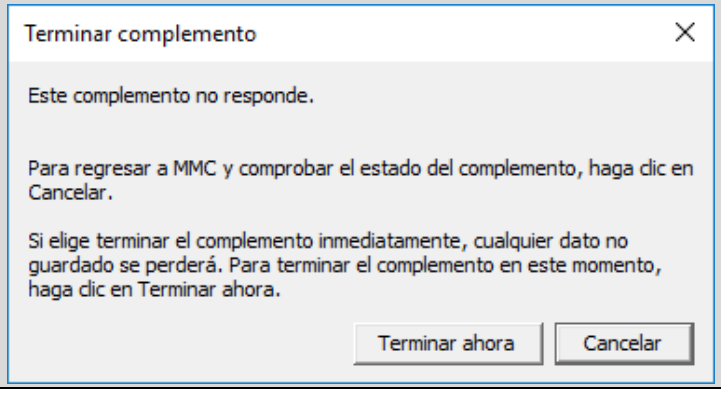
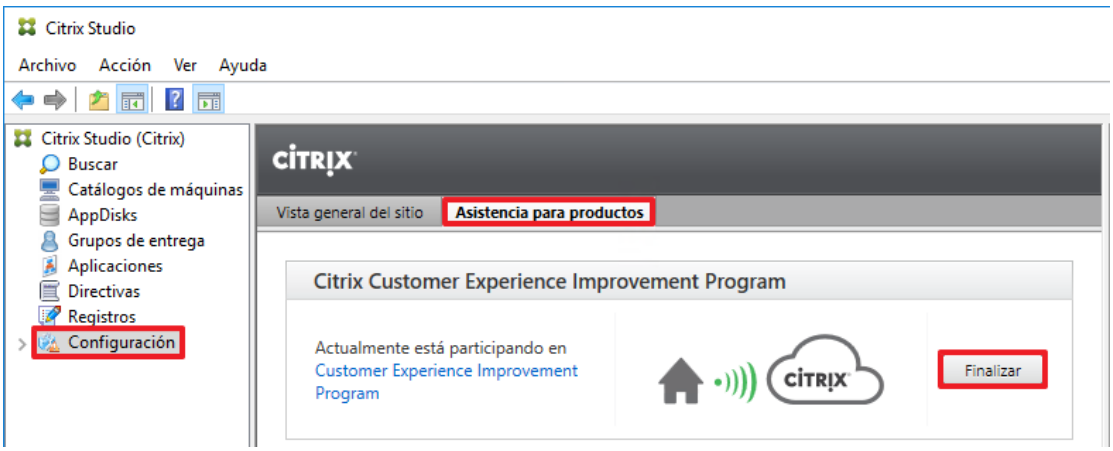
Esta configuración será de aplicación en los siguientes servidores de su infraestructura Citrix Virtual Apps and Desktops:

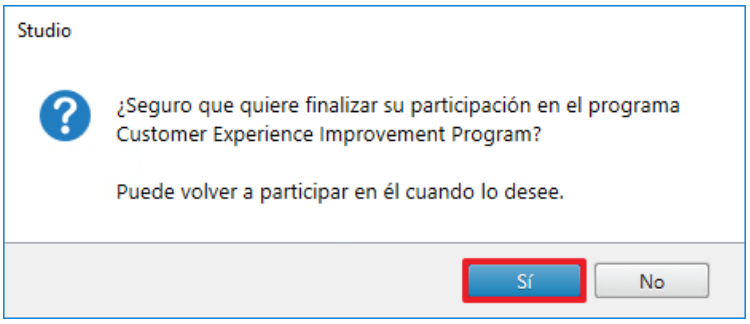
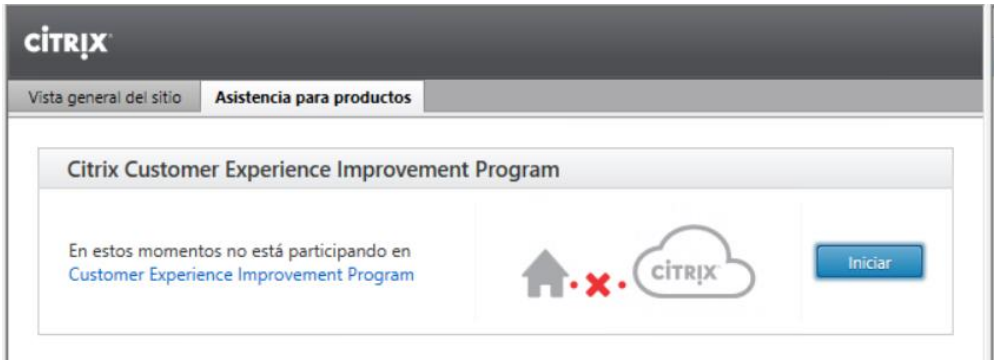
a) Servidor con el rol Citrix Controller

b) Servidor con el rol Citrix Licensing

En primer lugar, se realizarán las configuraciones necesarias sobre el servidor con el rol Citrix Controller instalado.

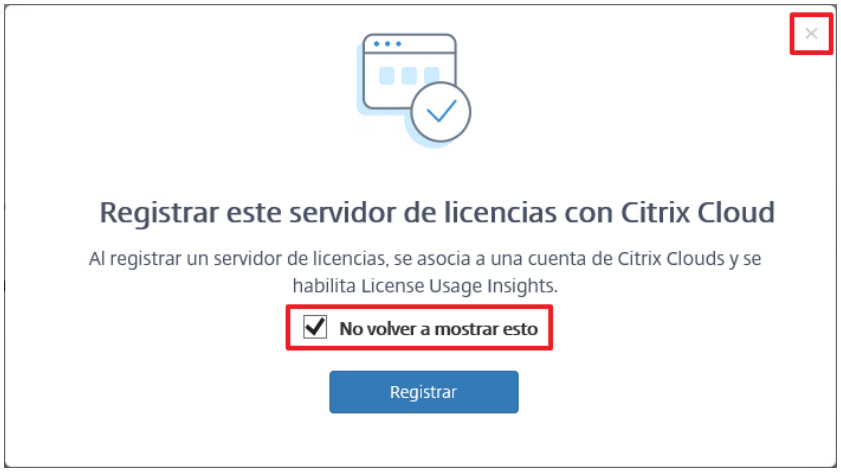
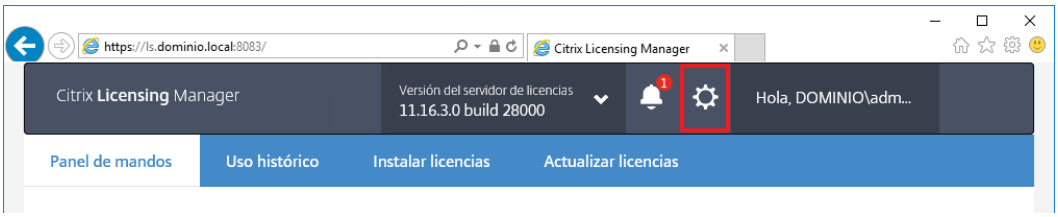
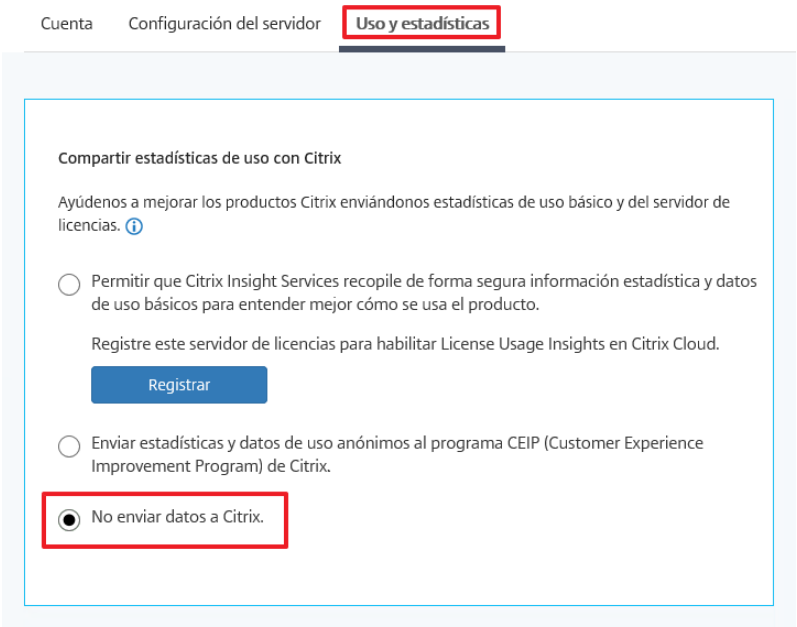
Paso	Descripción
165.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
166.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios.

Paso	Descripción
167.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
168.	Sobre la consola "Citrix Studio" diríjase al nodo **"Citrix Studio → Configuración → Asistencia para productos"**. Por defecto, los productos de Citrix participan automáticamente en el "Customer Experience Improvement Program" por lo que envían información a Citrix para la solución de errores en el producto. Pulse sobre "Finalizar" para detener el envío de información. 

Paso	Descripción
169.	En la ventana emergente que aparecerá pulse sobre “Si” para finalizar la participación en el programa. 
170.	Tras unos instantes puede apreciar como la consola indica que no está participando en el programa de mejora de la experiencia del usuario. 

A continuación, se procederá a realizar las configuraciones de seguridad necesarias en el servidor con el rol Citrix Licensing.

Paso	Descripción
171.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
172.	Acceda a la dirección URL del “Citrix Licensing Manager” https://ls.dominio.local:8083 adaptándolo a su entorno.

Paso	Descripción
173.	Es posible que le aparezca una ventana donde se le ofrece registrar el servidor de licencias con Citrix Cloud. Marque la casilla “No volver a mostrar esto” si no lo realizó anteriormente, y cierre la ventana pulsando el aspa de la parte superior derecha de la ventana. 
174.u	Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre la rueda superior derecha. 
175.	Acceda al apartado “Uso y estadísticas” y pulse sobre “No enviar datos a Citrix” para evitar compartir estadísticas de uso con el fabricante. 

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA CITRIX VIRTUAL APPS AND DESKTOPS SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

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

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

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.2.1.IMPLEMENTACIÓN DE SEGURIDAD PARA CITRIX VIRTUAL APPS AND DESKTOPS EN SERVIDORES MIEMBROS DEL DOMINIO SOBRE MICROSOFT SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS"

1. CONTROLADOR DE DOMINIO

Los siguientes pasos determinan el procedimiento para verificar la configuración del dominio en el que se despliega el sistema de virtualización.

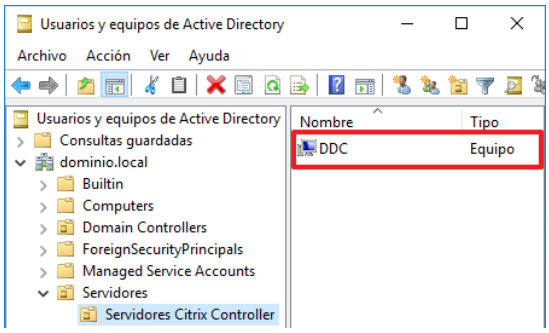
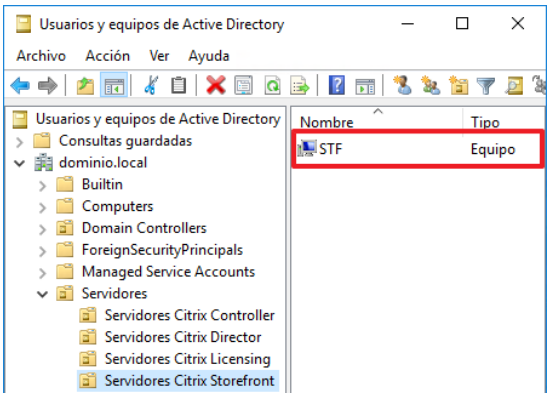
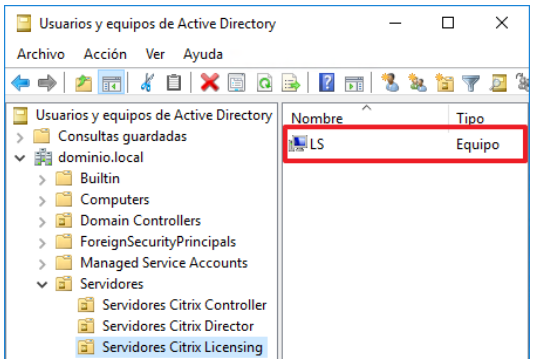
Las consolas y herramientas que se utilizarán son las siguientes:

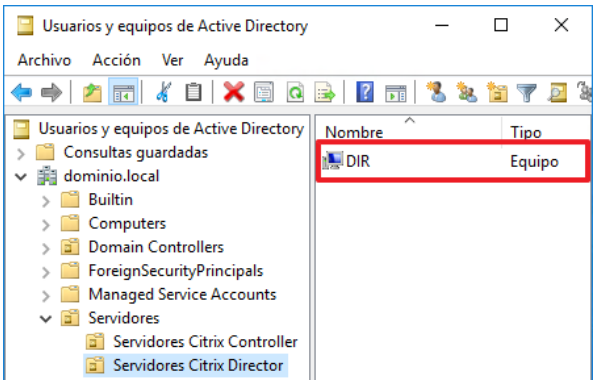
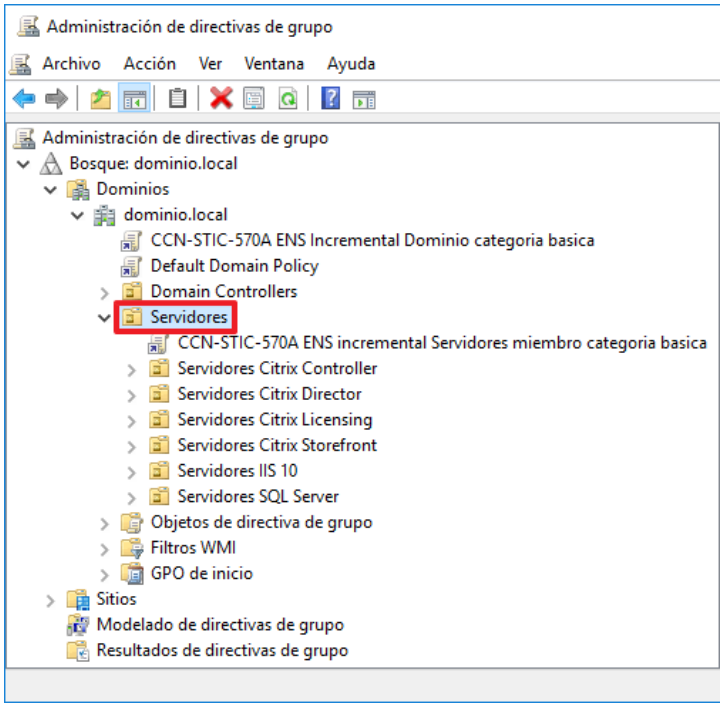
a) En el controlador de dominio:

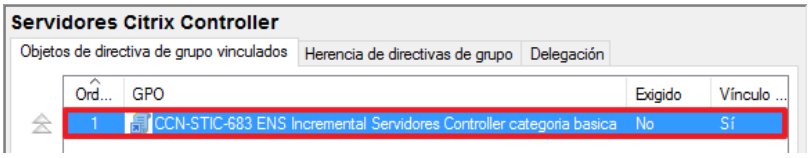
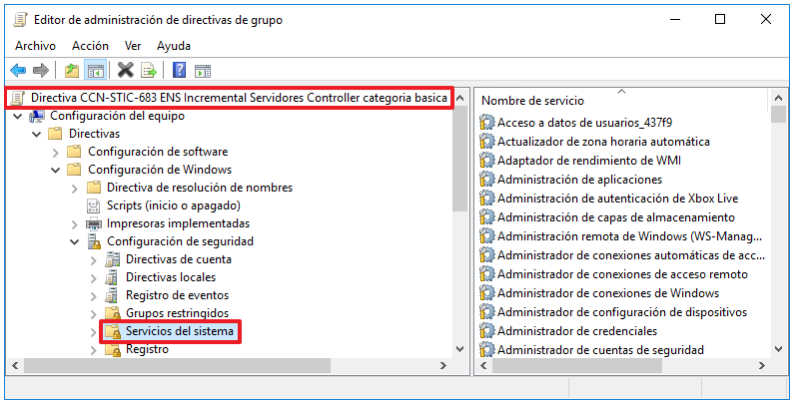
i. Usuarios y equipos de Active Directory (dsa.msc).

ii. Administrador de directivas de grupo (gpmc.msc).

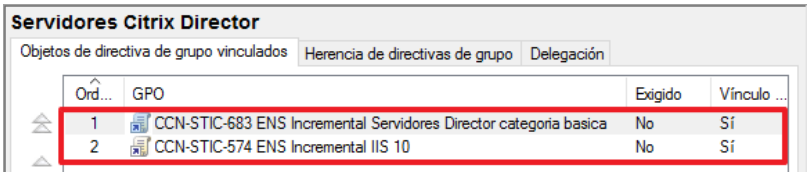
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un servidor controlador de dominio.		En un servidor controlador de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que están creadas las unidades organizativas de Citrix y que alojan sus respectivos servidores.		Ejecute la herramienta "Usuarios y equipos de Active Directory" desde: "**Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**". El sistema le solicitará elevación de privilegios para acceder a la consola de administración.

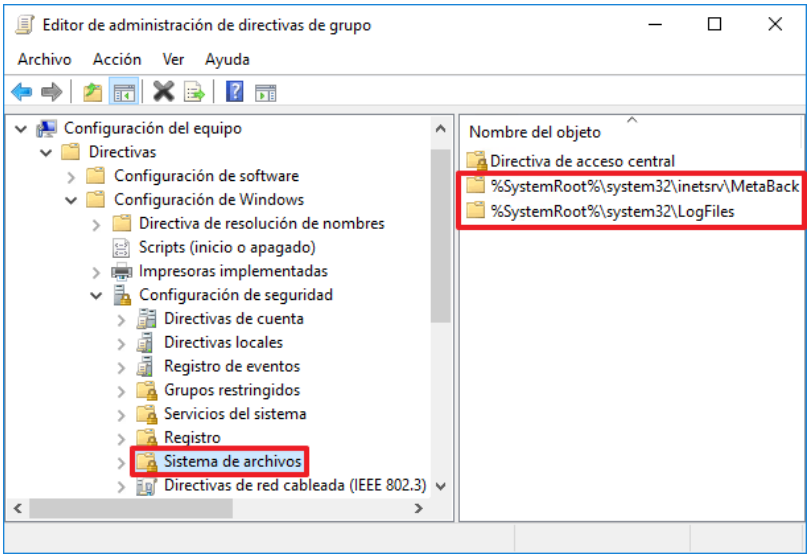
Comprobación	OK/NOK	Cómo hacerlo
3. La unidad organizativa "Servidores Citrix Controller" debe albergar todos los servidores con el rol Citrix Controller de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Controller" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "DDC", en su caso debe figurar el nombre de su equipo.
4. La unidad organizativa "Servidores Citrix Storefront" debe albergar todos los servidores con el rol Citrix Storefront de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Storefront" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "STF", en su caso debe figurar el nombre de su equipo.
5. La unidad organizativa "Servidores Citrix Licensing" debe albergar todos los servidores con el rol Citrix Licensing de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Licensing" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "LS", en su caso debe figurar el nombre de su equipo.

Comprobación	OK/NOK	Cómo hacerlo
6. La unidad organizativa "Servidores Citrix Director" debe albergar todos los servidores con el rol Citrix Director de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Director" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "DIR", en su caso debe figurar el nombre de su equipo.
7. Verifique que están creadas las directivas de configuración de Citrix.		Ejecute la herramienta "Administración de directivas de grupo" desde: **"Menú inicio → Herramientas administrativas → Administración de directivas de grupo"**. El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio. Seleccione la unidad organizativa "Servidores", situada en **"Bosque → Dominios → [Su dominio] → Servidores"**. 

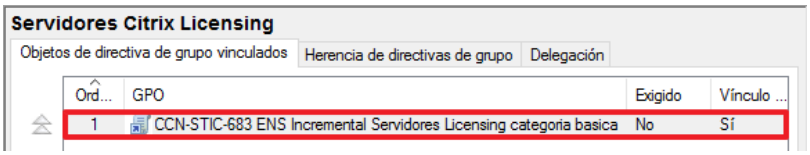
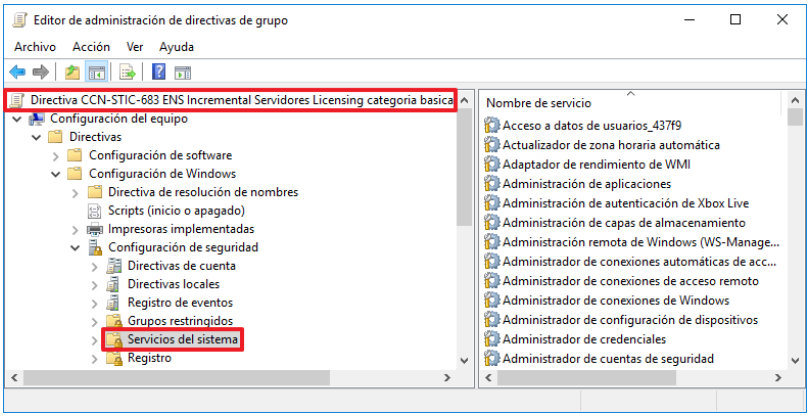
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique las políticas aplicadas a "Servidores Citrix Controller".		Seleccione la unidad organizativa "Servidores Citrix Controller", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Controller"** y revise que, como mínimo, tiene aplicada la siguiente directiva y tiene el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Controller categoria basica 
9. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Controller categoria basica".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Controller categoria basica" tiene los siguientes valores de servicios de sistema. "**Directiva CCN-STIC-683 ENS Incremental Servidores Controller categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema**".  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Asignador de extremos de RPC	RpcEptMapper	Automático	
Citrix AD Identity Service	CitrixADIdentityService	Automático	
Citrix Analytics	CitrixAnalytics	Automático	
Citrix App Library	CitrixAppLibrary	Automático	
Citrix Broker Service	CitrixBrokerService	Automático	
Citrix Config Synchronizer Service	CitrixConfigSyncService	Automático	
Citrix Configuration Service	CitrixConfigurationService	Automático	
Citrix Configuration Logging Service	CitrixConfigurationLogging	Automático	

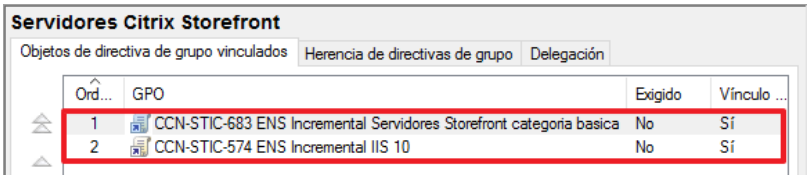
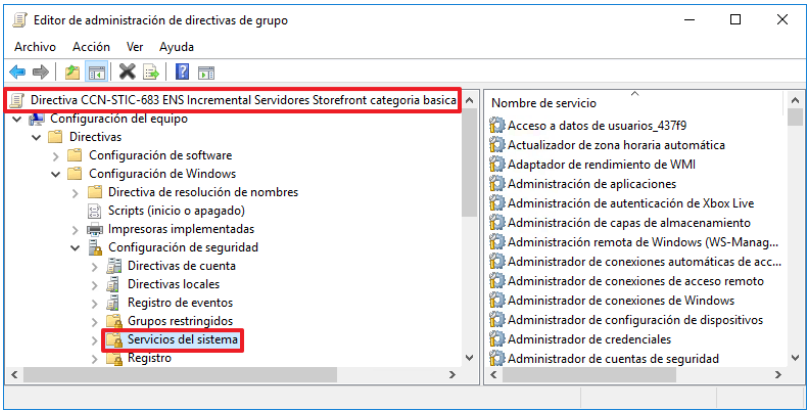
<table>
<tr><th colspan="2">Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td colspan="3">Servicio (nombre largo)</td><td>Servicio (nombre corto)</td><td>Inicio</td><td>OK/NOK</td></tr>
<tr><td colspan="3">Citrix Smart Tools Agent Service</td><td>CitrixConnector</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="3">Citrix Delegated Administration Service</td><td>CitrixDelegatedAdmin</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Enviroment Test Service</td><td>CitrixEnvTest</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix High Availability Service</td><td>CitrixHighAvailabilityService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Host Service</td><td>CitrixHostService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Machine Creation Service</td><td>CitrixMachineCreationService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Monitor Service</td><td>CitrixMonitor</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Orchestration Service</td><td>CitrixOrchestration</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Storefront Privileged Administration Service</td><td>CitrixPrivilegedService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Storefront Service</td><td>CitrixStorefront</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Telemetry Service</td><td>CitrixTelemetryService</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="3">Citrix Trust Service</td><td>CitrixTrust</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Estación de trabajo</td><td>LanmanWorkstation</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Iniciador de procesos de servidor DCOM</td><td>DcomLaunch</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Llamada a procedimiento remoto (RPC)</td><td>RpcSs</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Servicio Interfaz de almacenamiento en red</td><td>nsi</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Remote Broker Provider</td><td>XaXdCloudProxy</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Smart Tools Monitor Service</td><td>Monitor Agent</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">10. Verifique las políticas aplicadas a “Servidores Citrix Director”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Servidores Citrix Director”, situada en “Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Director” y revise que, como mínimo, la unidad organizativa “Servidores Citrix Director” tiene aplicadas las siguientes directivas en el orden adecuado y tienen el vínculo habilitado.
– CCN-STIC-683 ENS Incremental Servidores Director categoria basica
– CCN-STIC-574 ENS Incremental Servidores IIS 10
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique los valores de los permisos del sistema de archivos de la directiva "CCN-STIC-683 ENS Incremental Servidores Director categoria basica".		Utilizando el "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Director categoria basica" tiene los siguientes valores de permisos de sistema de archivos. **"Directiva CCN-STIC-683 ENS Incremental Servidores Director categoria basica→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos"**.  **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\inetsrv\MetaBack	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	
%SystemRoot%\system32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique las políticas aplicadas a Servidores Citrix Licensing.		Seleccione la unidad organizativa "Servidores Citrix Licensing", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Licensing"** y revise que, como mínimo, la unidad organizativa "Servidores Citrix Licensing" tiene aplicada la siguiente directiva y tiene el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica 
13. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica" tiene los siguientes valores de servicios de sistema. "**Directiva CCN-STIC-683 ENS Incremental Servidores Licensing categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema**".  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Licensing	Citrix Licensing	Automático	
Citrix Web Services for Licensing	CitrixWebServicesforLicensing	Automático	
Citrix Licensing Support Service	CtxLSPortSvc	Automático	
Citrix Licensing WMI	Citrix_GTLicensingProv	Manual	

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique las políticas aplicadas a "Servidores Citrix Storefront".		Seleccione la unidad organizativa "Servidores Citrix Storefront", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Storefront"** y revise que, como mínimo, la unidad organizativa "Servidores Citrix Storefront" tiene aplicadas las siguientes directivas en el orden adecuado y tienen el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica – CCN-STIC-574 ENS Incremental IIS 10 
15. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica" tiene los siguientes valores de servicios de sistema. "**Directiva CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema**".  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	
Citrix Peer Resolution Service	Citrix Peer Resolution Service	Automático	
Citrix Configuration Replication	CitrixConfigurationReplication	Automático	
Citrix Credential Wallet	CitrixCredentialWallet	Automático	
Citrix Default Domain Service	CitrixDefaultDomainService	Automático	
Citrix Service Monitor	CitrixServiceMonitor	Automático	

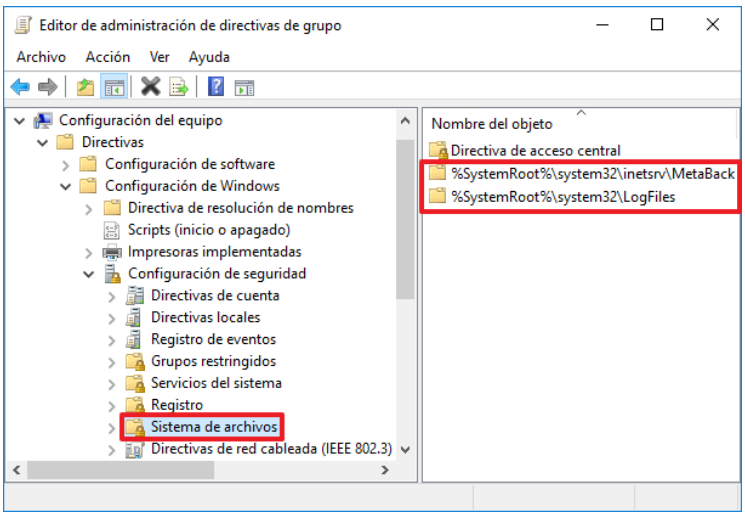
Comprobación	OK/NOK	Cómo hacerlo

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Subscriptions Store	CitrixSubscriptionsStore	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Automático	
Servidor	LanmanServer	Automático	
Citrix Cluster Service	CitrixClusterService	Deshabilitado	

16. Verifique los valores de los permisos del sistema de archivos de la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica".

Utilizando el "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica" tiene los siguientes valores de permisos de sistema de archivos.

"Directiva CCN-STIC-683 ENS Incremental Servidores Storefront categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos".



Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...".
Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\inetsrv\MetaBack	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	
%SystemRoot%\system32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	

2. CITRIX CONTROLLER

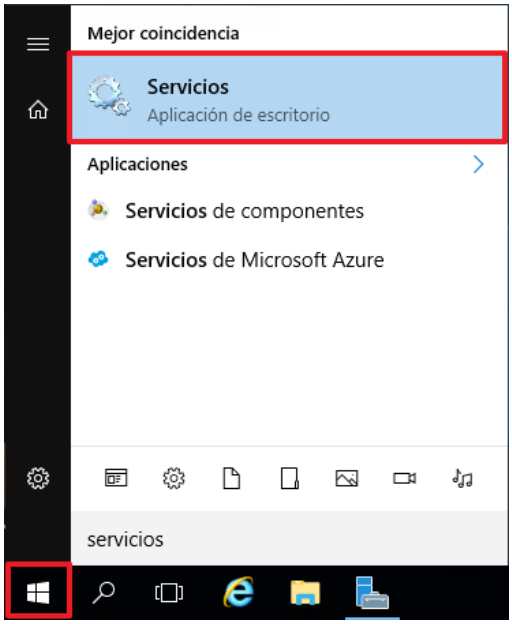
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Controller, y las configuraciones propias implementadas sobre este servidor.

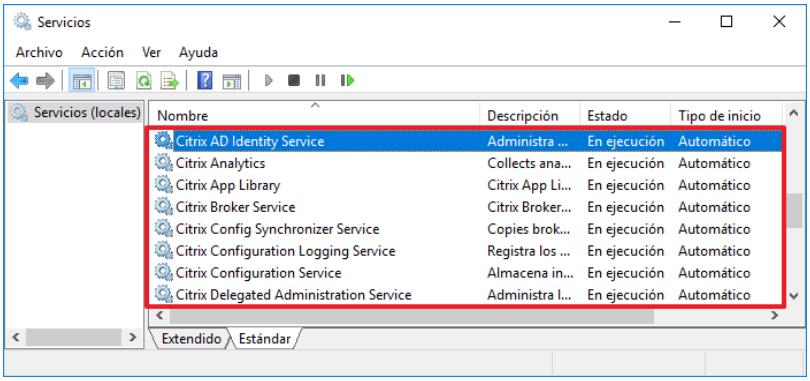
Las consolas y herramientas que se utilizarán son las siguientes:

a) En el servidor miembro Citrix Controller:

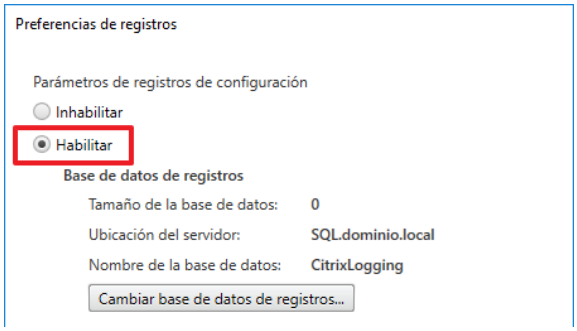
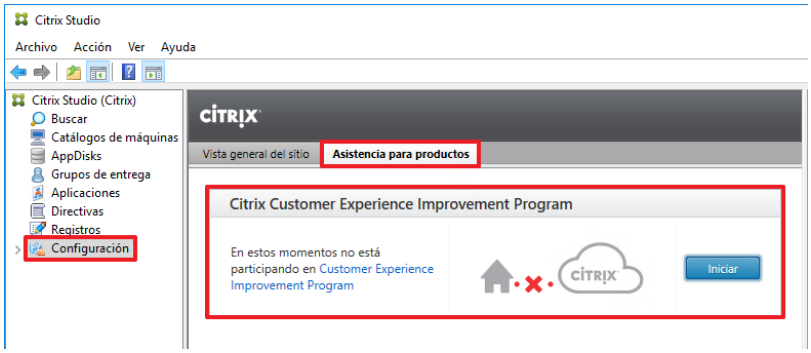
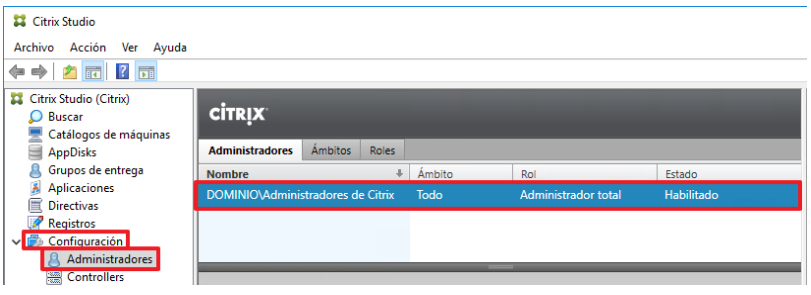
i. Servicios (services.msc).

ii. Consola de Citrix Studio.

Comprobación	OK/NOK	Cómo hacerlo
17. Inicie sesión en un servidor con el rol Citrix Controller.		En un servidor con el rol Citrix Controller, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
18. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios. 

Comprobación	OK/NOK	Cómo hacerlo
19. Sobre cada uno de los servidores con el rol Citrix Controller revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Asignador de extremos de RPC	RpcEptMapper	Automático	
Citrix AD Identity Service	CitrixADIdentityService	Automático	
Citrix Analytics	CitrixAnalytics	Automático	
Citrix App Library	CitrixAppLibrary	Automático	
Citrix Broker Service	CitrixBrokerService	Automático	
Citrix Config Synchronizer Service	CitrixConfigSyncService	Automático	
Citrix Configuration Service	CitrixConfigurationService	Automático	
Citrix Configuration Logging Service	CitrixConfigurationLogging	Automático	
Citrix Smart Tools Agent Service	CitrixConnector	Deshabilitado	
Citrix Delegated Administration Service	CitrixDelegatedAdmin	Automático	
Citrix Enviroment Test Service	CitrixEnvTest	Automático	
Citrix High Availability Service	CitrixHighAvailabilityService	Automático	
Citrix Host Service	CitrixHostService	Automático	
Citrix Machine Creation Service	CitrixMachineCreationService	Automático	
Citrix Monitor Service	CitrixMonitor	Automático	
Citrix Orchestration Service	CitrixOrchestration	Automático	
Citrix Storefront Privileged Administration Service	CitrixPrivilegedService	Automático	
Citrix Storefront Service	CitrixStorefront	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Citrix Trust Service	CitrixTrust	Automático	
Estación de trabajo	LanmanWorkstation	Automático	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**OK/NOK**
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	
Servicio Interfaz de almacenamiento en red		nsi	Automático	
Citrix Remote Broker Provider		XaXdCloudProxy	Automático	
Citrix Smart Tools Monitor Service		Monitor Agent	Deshabilitado	
20. Bajo la consola Citrix Studio revise la configuración de registro.		Acceda a la consola "Citrix Studio" y bajo el apartado **"Registros → Preferencias"** verifique que en "Parámetros de registros de configuración" se encuentra marcada la opción **"Habilitar"**. 		
21. Compruebe la no participación en Citrix CEIP.		Sobre la consola "Citrix Studio" diríjase al nodo **"Citrix Studio → Configuración → Asistencia para productos"**. Compruebe que el "Citrix Customer Experience Improvement Program" se encuentra detenido. 		
22. Revisión permisos administrativos		Dirjase al menú de configuración **"Citrix Studio → Configuración → Administradores"** y compruebe que se han restringido los permisos administrativos a los necesarios en función de su organización. 		

3. CITRIX STOREFRONT

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Storefront, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

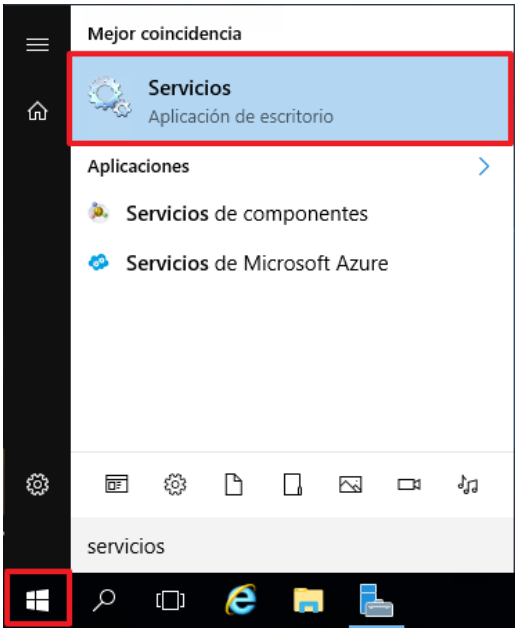
a) En el servidor miembro Citrix Storefront:

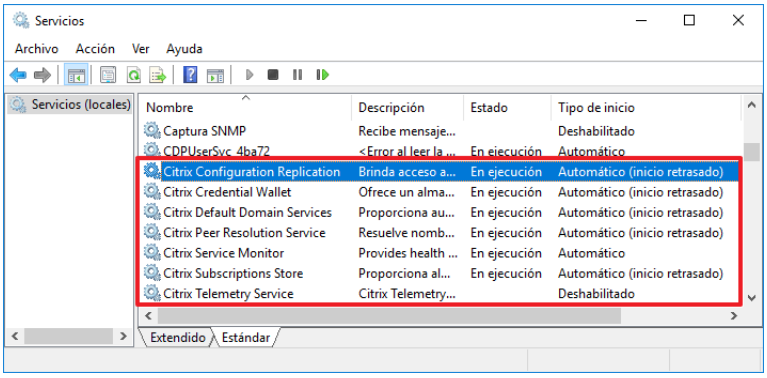
i. Servicios (services.msc).

ii. Consola de administración de Microsoft (mmc.exe).

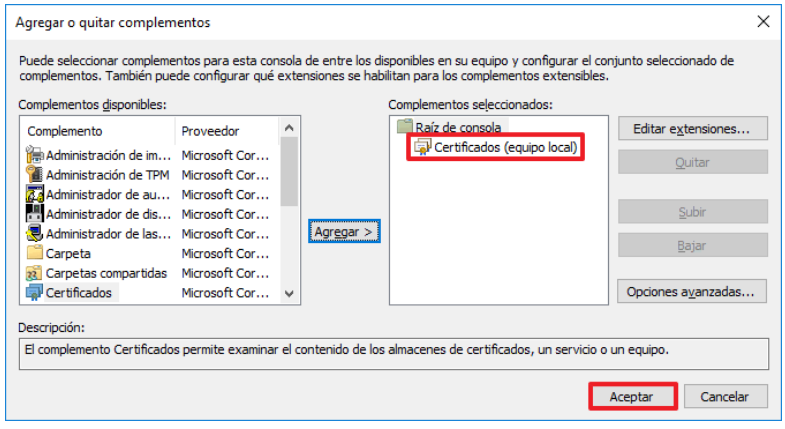
iii. Administrador de Internet Information Service (IIS).

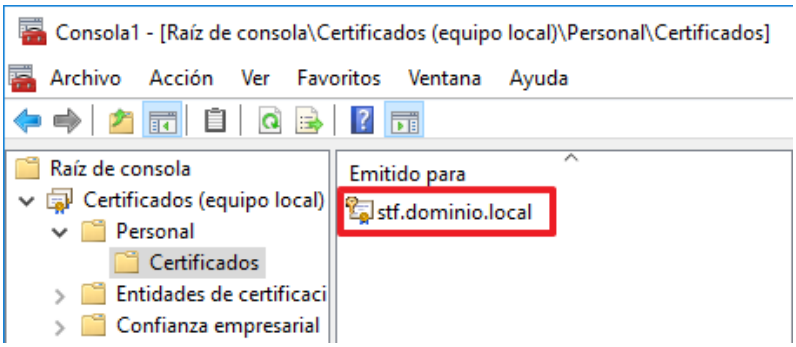
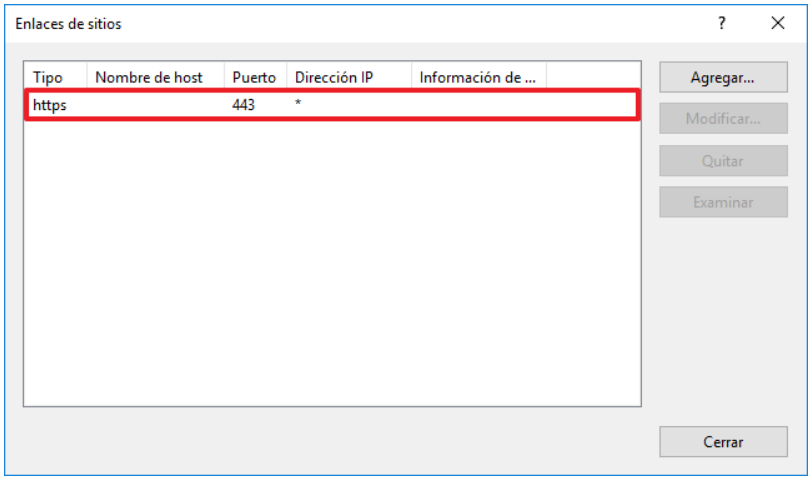
iv. Consola de Citrix Storefront.

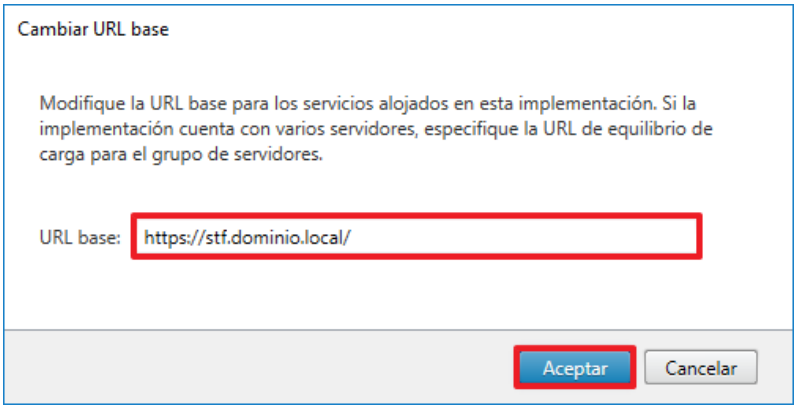
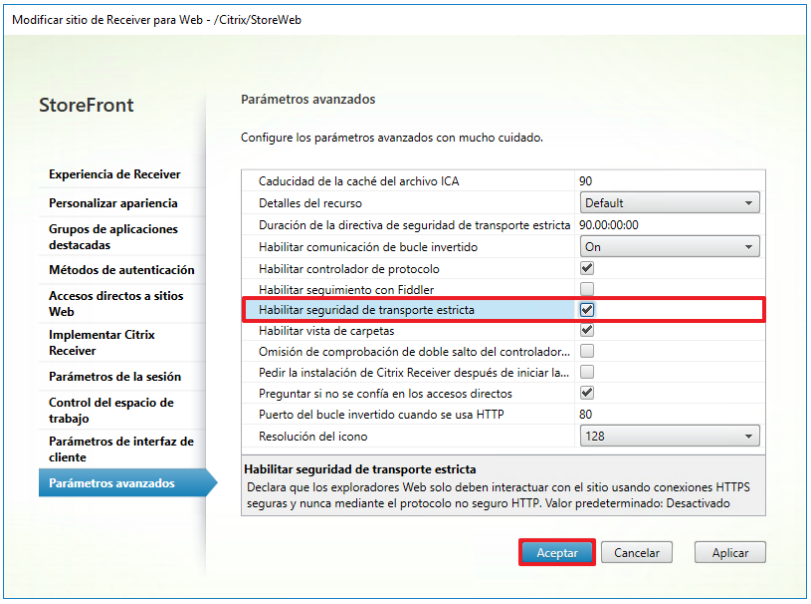
Comprobación	OK/NOK	Cómo hacerlo
23. Inicie sesión en un servidor con el rol Citrix Storefront.		En un servidor con el rol Citrix Storefront, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
24. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios. 

Comprobación	OK/NOK	Cómo hacerlo
25. Sobre cada uno de los servidores con el rol Citrix Storefront revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	
Citrix Peer Resolution Service	Citrix Peer Resolution Service	Automático	
Citrix Configuration Replication	CitrixConfigurationReplication	Automático	
Citrix Credential Wallet	CitrixCredentialWallet	Automático	
Citrix Default Domain Service	CitrixDefaultDomainService	Automático	
Citrix Service Monitor	CitrixServiceMonitor	Automático	
Citrix Subscriptions Store	CitrixSubscriptionsStore	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Automático	
Servidor	LanmanServer	Automático	
Citrix Cluster Service	CitrixClusterService	Deshabilitado	

26. Verifique la instalación del certificado local para cada uno de los servidores Citrix Storefront.		Acceda a la consola “mmc.exe” desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado “Ctrl + M”. 

Comprobación	OK/NOK	Cómo hacerlo
27. Verifique la instalación del certificado local para cada uno de los servidores Citrix Storefront.		Despliegue el nodo **"Personal → Certificados"**. Deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo "Emitido para" variará dependiendo del nombre de su servidor.
28. Ejecute la consola de administración de IIS.		Ejecute la herramienta "Administrador de Internet Information Services (IIS)" desde: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)".** El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.
29. Enlaces de sitios configurado para HTTPS.		Abra el nodo de configuración **"Su servidor (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"** Compruebe que únicamente se encuentra configurado el tipo "https" con el puerto 443. 

Comprobación	OK/NOK	Cómo hacerlo
30. URL base del sitio configurada para HTTPS.		Ejecute la consola Citrix Storefront. Desde la pestaña **"Grupo de servidores"**, acceda a la opción "Cambiar URL base", compruebe que la URL de la tienda incluye el protocolo seguro HTTPS como se muestra en la siguiente figura. 
31. Seguridad de transporte estricta habilitada.		Continúe con las comprobaciones accediendo a la consola "Citrix Storefront" y diríjase al menú de configuración **"Tiendas → Store → Administrar sitios de Receiver para Web"**, en la configuración de su sitio web, dentro del apartado de parámetros avanzados compruebe que se encuentra marcada la opción: – Habilitar seguridad de transporte estricta 

4. CITRIX LICENSING

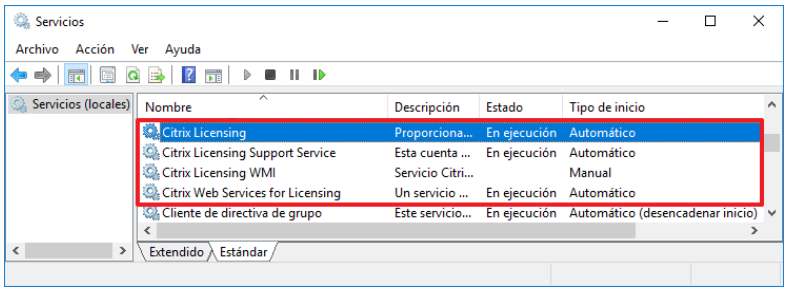
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Licensing, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

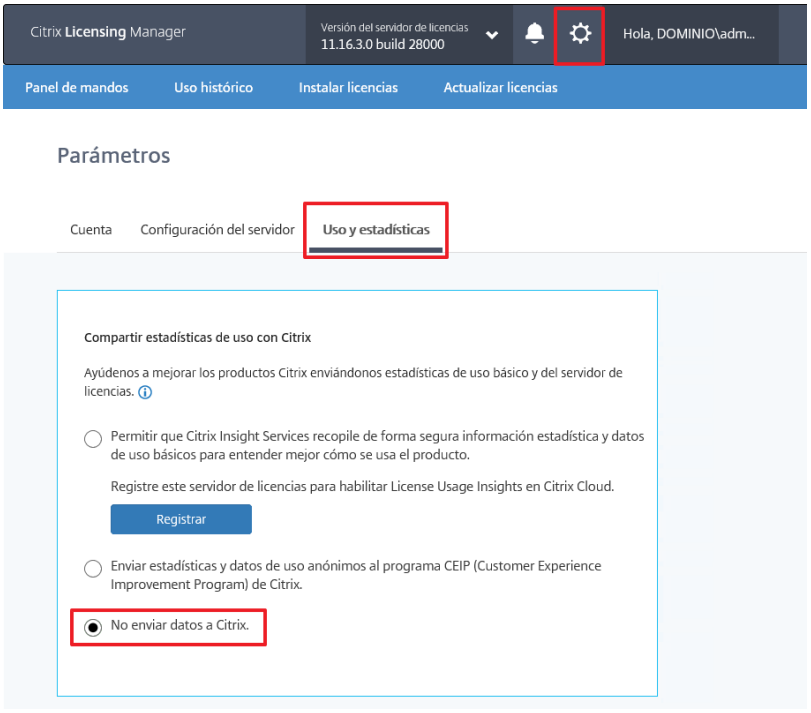
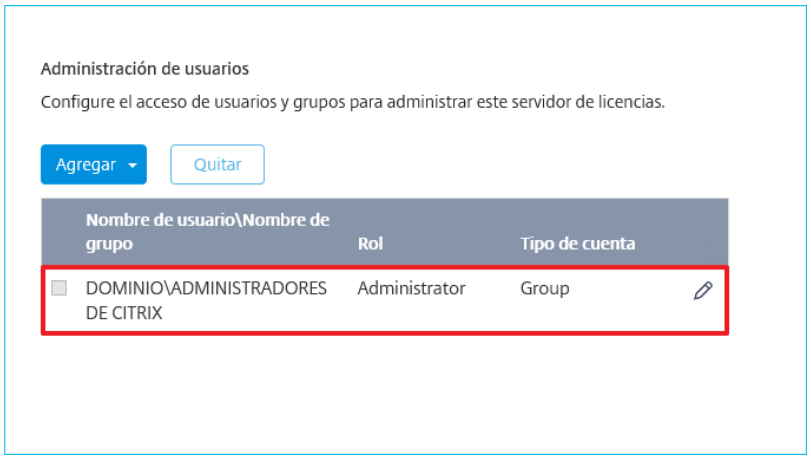
a) En el servidor miembro Citrix Licensing:

i. Servicios (services.msc).

ii. Consola de Citrix Licensing.

Comprobación	OK/NOK	Cómo hacerlo
32. Inicie sesión en un servidor con el rol Citrix Licensing.		En un servidor con el rol Citrix Licensing, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
33. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios.
34. Sobre cada uno de los servidores con el rol Citrix Licensing revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Licensing	Citrix Licensing	Automático	
Citrix Web Services for Licensing	CitrixWebServicesforLicensing	Automático	
Citrix Licensing Support Service	CtxLSPortSvc	Automático	
Citrix Licensing WMI	Citrix_GTLicensingProv	Manual	

Comprobación	OK/NOK	Cómo hacerlo
35. Restringir envío de información a Citrix.		Acceda a la dirección URL https://ls.dominio.local:8083 adaptándolo a su entorno. Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre el botón de configuración en la parte superior derecha. Acceda al apartado "Uso y estadísticas". Compruebe que está marcada la opción "No enviar datos a Citrix". 
36. Restricción permisos Citrix Licensing.		A continuación, acceda al nodo de configuración "Cuenta". Verifique que se han restringido los permisos administrativos a los necesarios en función de su organización. 

5. CITRIX DIRECTOR

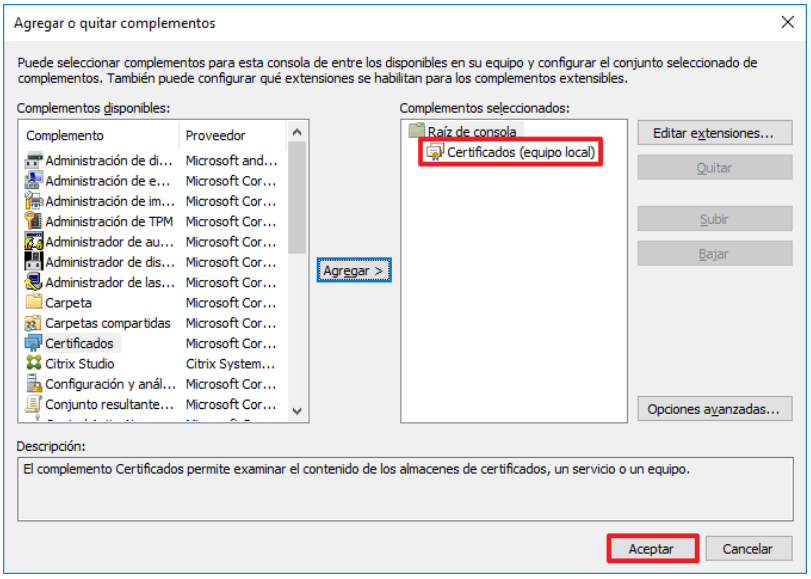
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Director, y las configuraciones propias implementadas sobre este servidor.

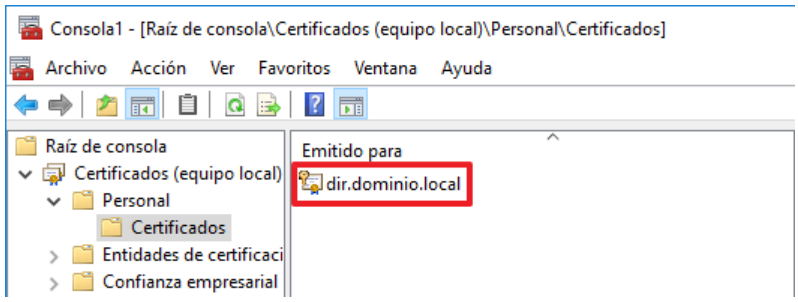
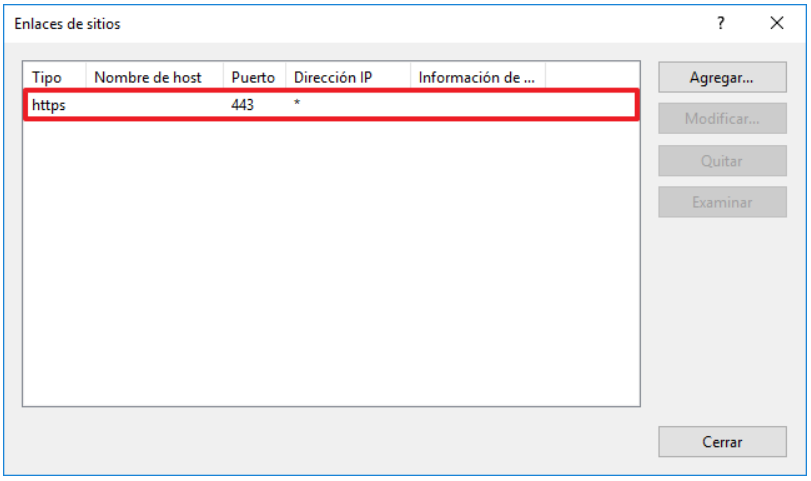
Las consolas y herramientas que se utilizarán son las siguientes:

a) En el servidor miembro Citrix Director:

i. Consola de administración de Microsoft (mmc.exe).

ii. Administrador de Internet Information Service (IIS).

Comprobación	OK/NOK	Cómo hacerlo
37. Inicie sesión en un servidor con el rol Citrix Director.		En un servidor con el rol Citrix Director, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
38. Verifique la instalación del certificado local para cada uno de los servidores Citrix Director.		Acceda a la consola "mmc.exe" desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado "Ctrl + M". 

Comprobación	OK/NOK	Cómo hacerlo
39. Verifique la instalación del certificado local para cada uno de los servidores Citrix Director.		Despliegue el nodo **"Personal → Certificados"**. Deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo "Emitido para" variará dependiendo del nombre de su servidor.
40. Ejecute la consola de administración de IIS.		Ejecute la herramienta "Administrador de Internet Information Services (IIS)" desde: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)".** El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.
41. Enlaces de sitios configurado para HTTPS.		Abra el nodo de configuración **"Su servidor (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"** Compruebe que únicamente se encuentra configurado el tipo "https" con el puerto 443. 

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD PARA CITRIX VIRTUAL APPS AND DESKTOPS EN SERVIDORES MIEMBROS DEL DOMINIO SOBRE MICROSOFT SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que securizar Citrix Virtual Apps and Desktops sobre Microsoft Windows Server 2016 con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, deberá realizar las implementaciones según se referencian en el presente anexo.

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

1. PREPARACIÓN DEL DOMINIO

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que van a pertenecer cada uno de los roles de la infraestructura sobre los que implementará las configuraciones de seguridad. Los pasos descritos a continuación solo los debe realizar cuando vaya a realizar la primera implementación de seguridad en el dominio, ya que solo es necesario crear las unidades organizativas, modificar las plantillas de seguridad e incorporarlas en la directiva de grupo una única vez por dominio.

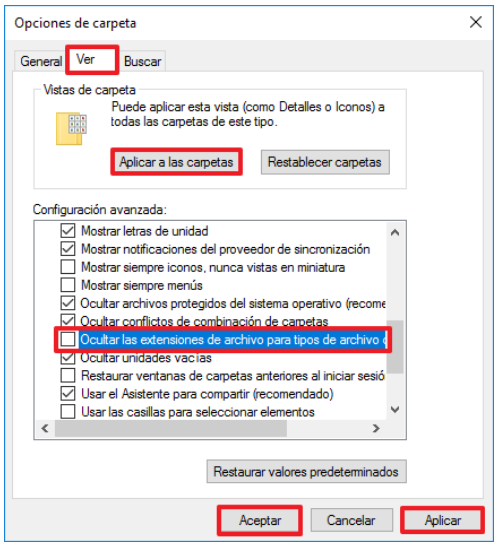
Se asume que ha realizado la implementación de las siguientes guías de seguridad sobre el servidor controlador de dominio donde se va a aplicar el siguiente paso a paso:

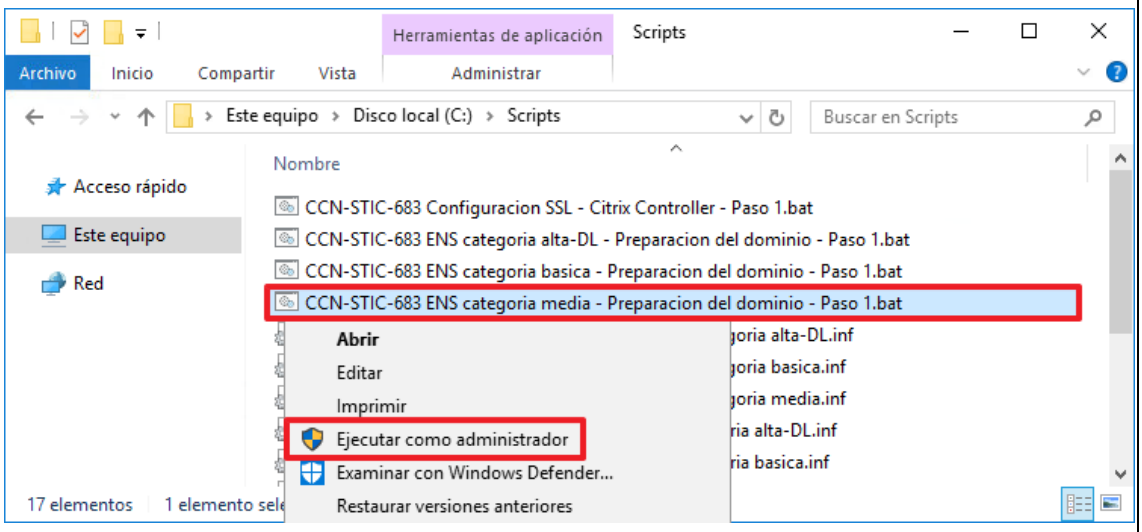
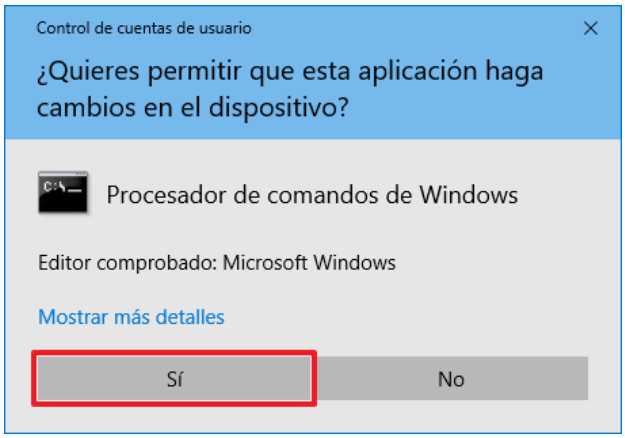
a) CCN-STIC-570A Anexo A Controlador de dominio – Categoría Media.

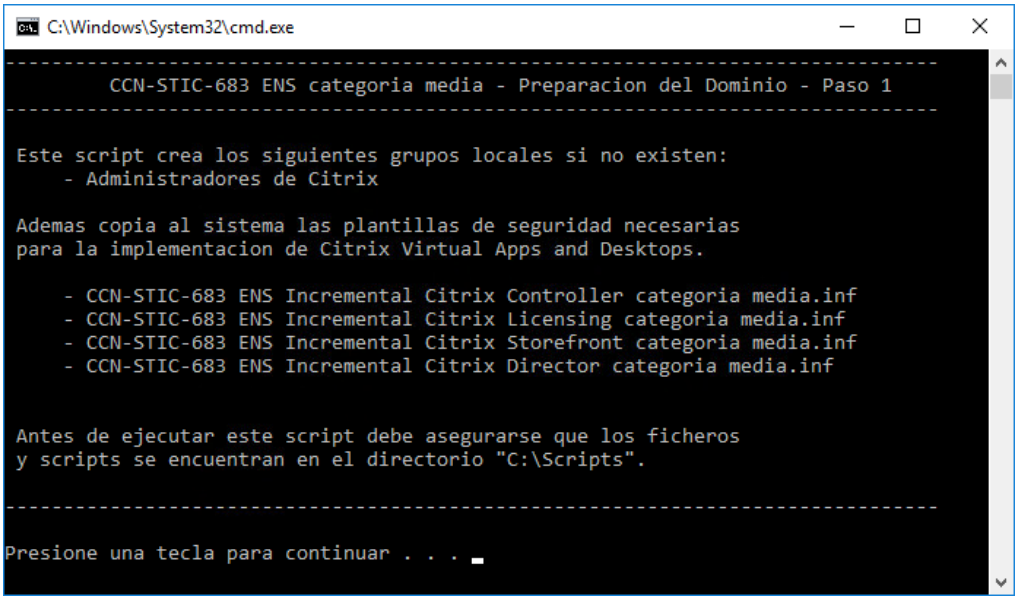
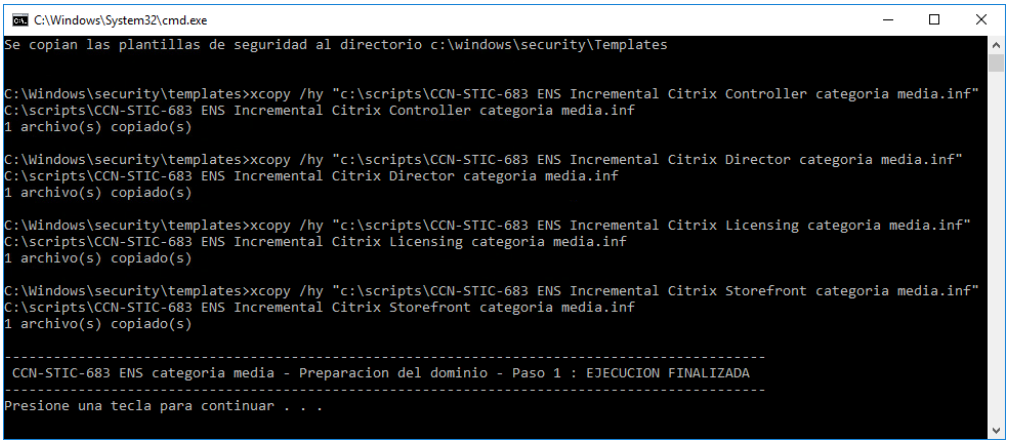
b) CCN-STIC-575 Anexo A Microsoft SQL server 2016 – Categoría Media.

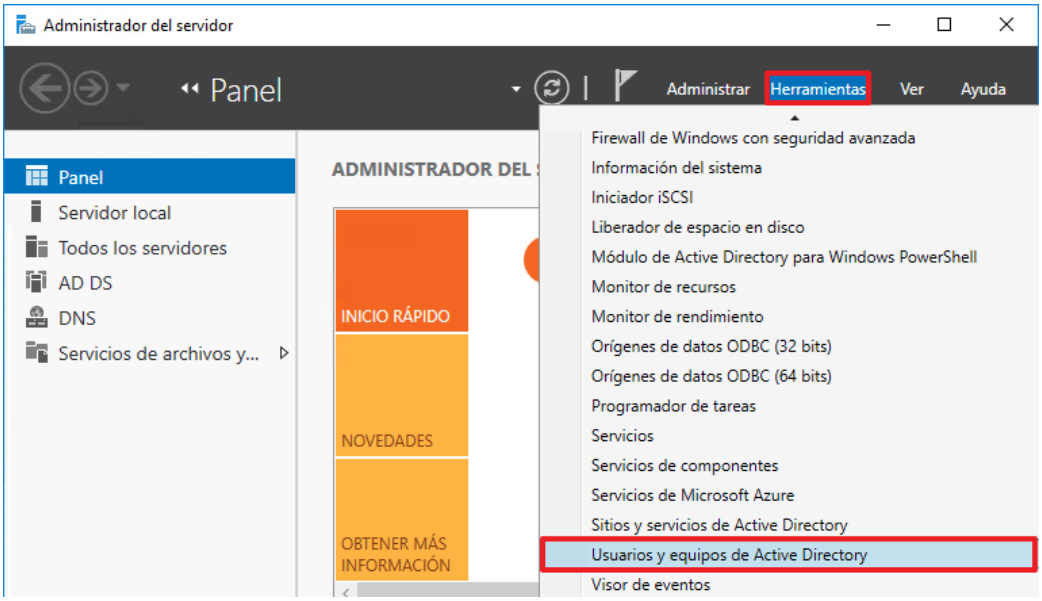
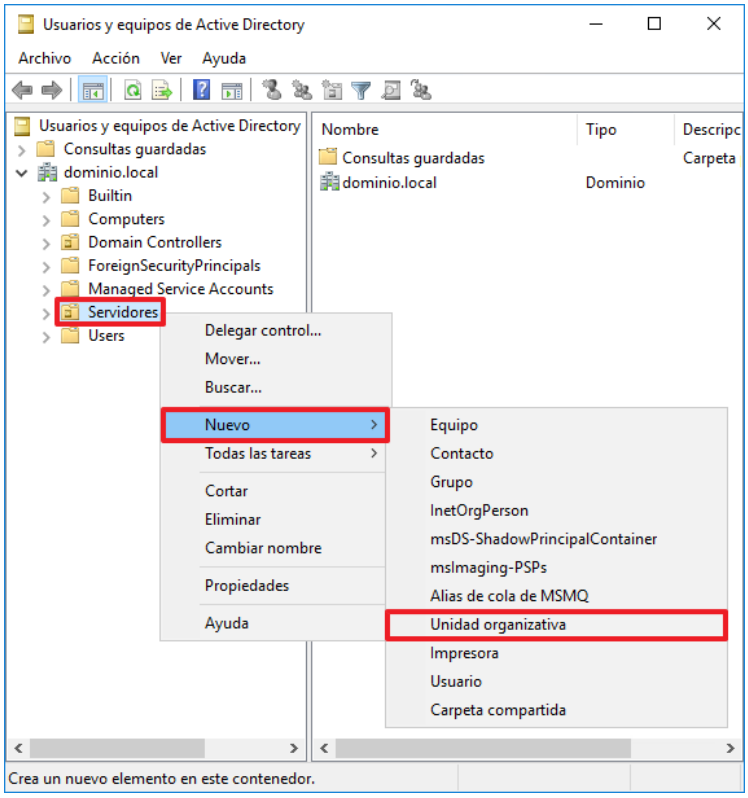
c) CCN-STIC-574 Anexo A Internet Information Services 10 – Categoría Media.

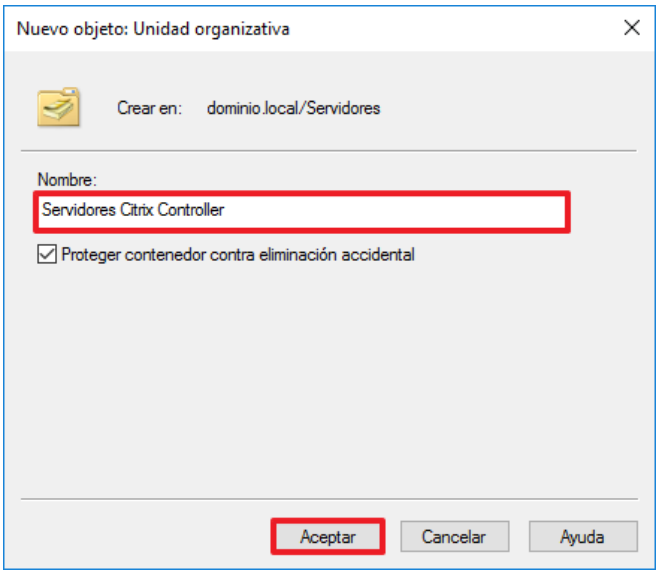
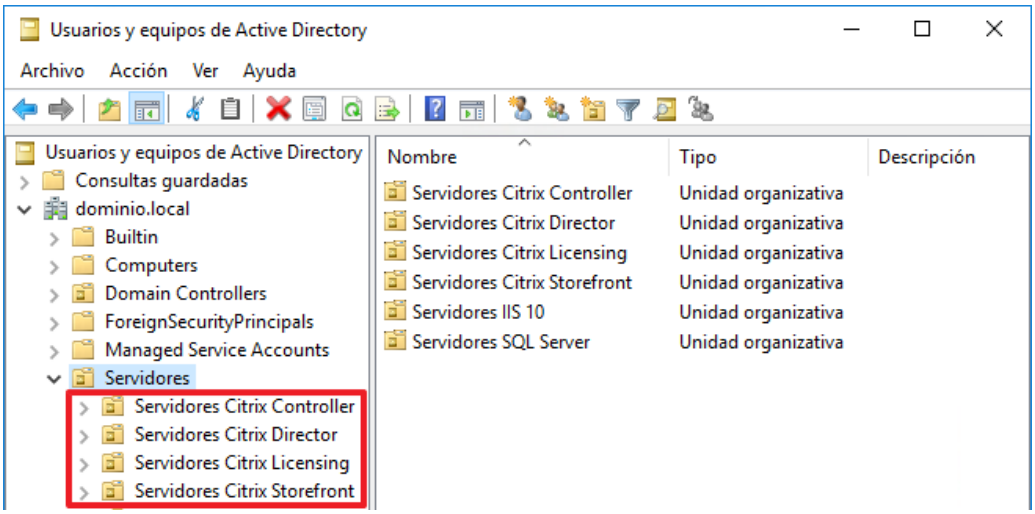
Nota: Las guías “CCN-STIC-575” y “CCN-STIC-574” deberán aplicarse en este servidor exclusivamente su apartado correspondiente al controlador de dominio.

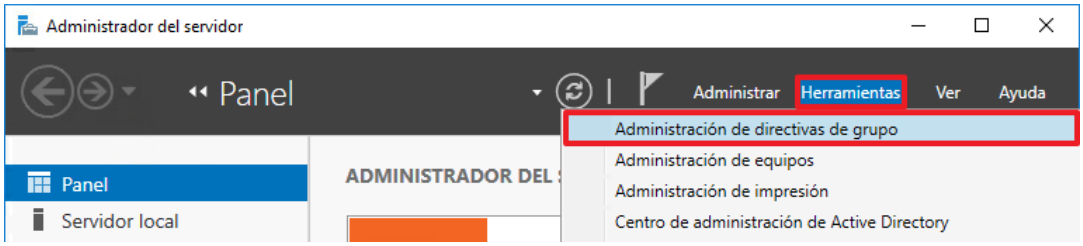
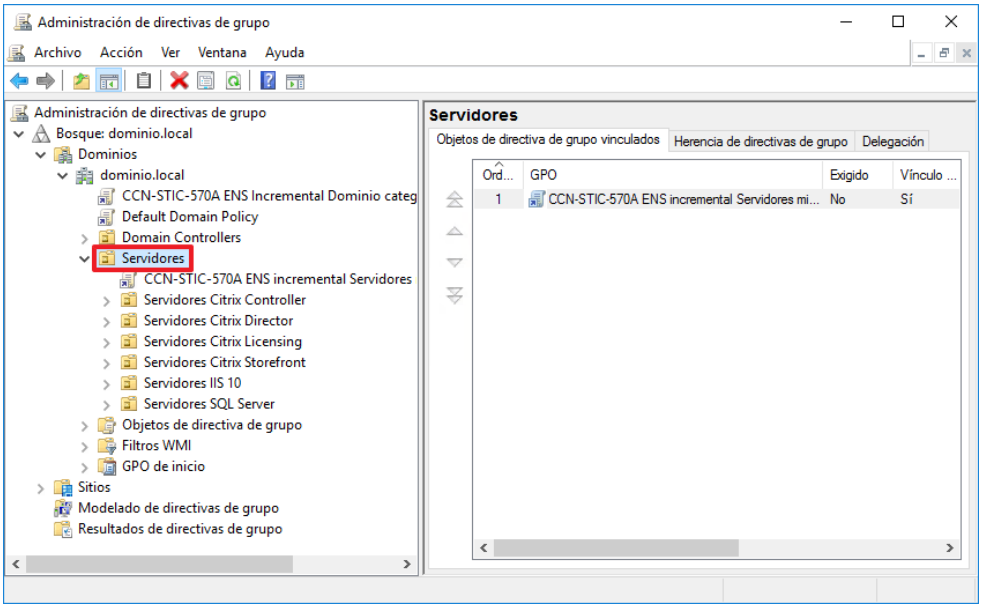
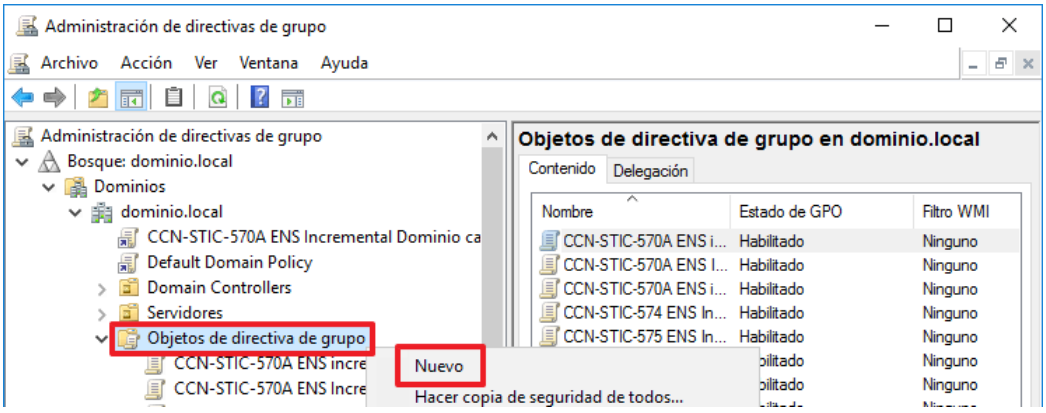
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los ficheros y directorios que acompañan a esta guía, al 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. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

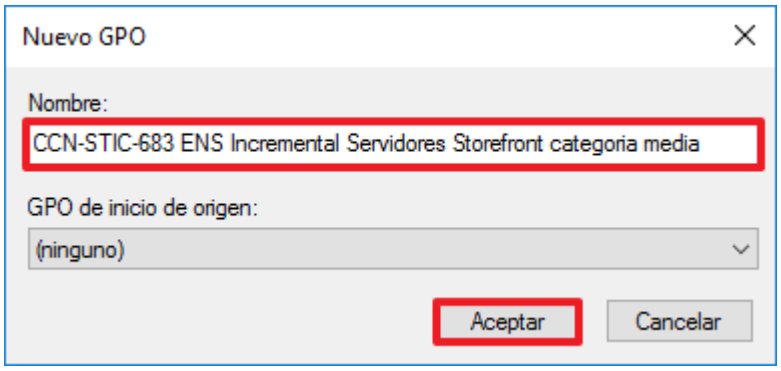
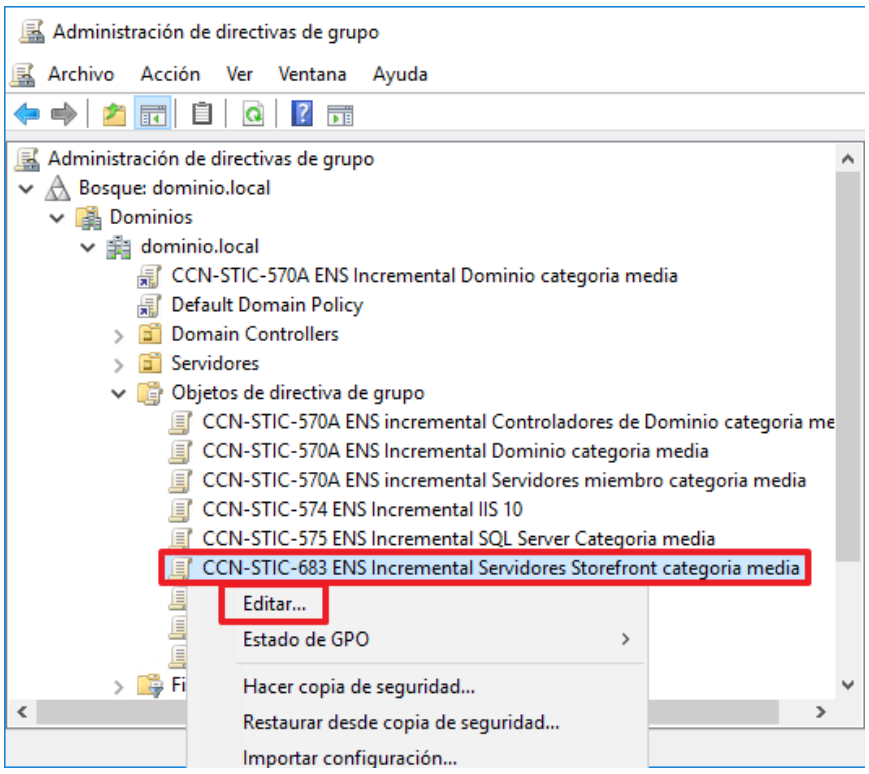
Paso	Descripción
5.	Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-683 ENS categoria media - Preparacion del dominio - Paso 1.bat – CCN-STIC-683 ENS Incremental Citrix Controller categoria media.inf – CCN-STIC-683 ENS Incremental Citrix Director categoria media.inf – CCN-STIC-683 ENS Incremental Citrix Licensing categoria media.inf – CCN-STIC-683 ENS Incremental Citrix Storefront categoria media.inf
6.	Ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-683 ENS categoria media - Preparacion del dominio – Paso 1.bat". Para ello, visualice la carpeta "C:\Scripts" en el Explorador de Windows, marque con el botón derecho el script y seleccione la opción **"Ejecutar como administrador"** del menú contextual, como se muestra en la siguiente figura.  **Nota:** Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
7.	El sistema solicitará elevación de privilegios, pulse "Si" para continuar. 

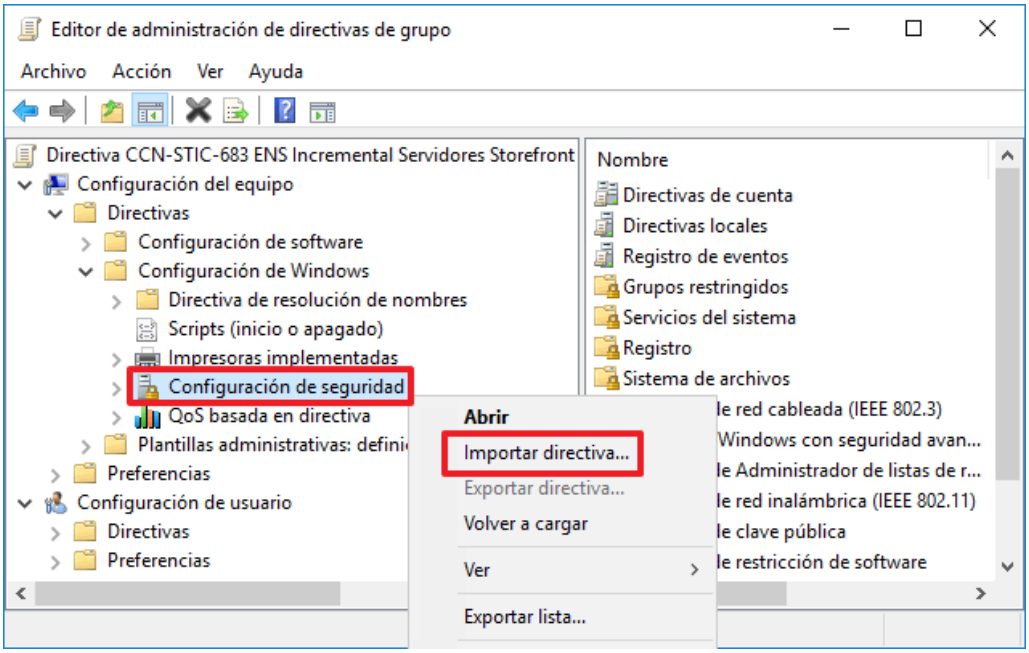
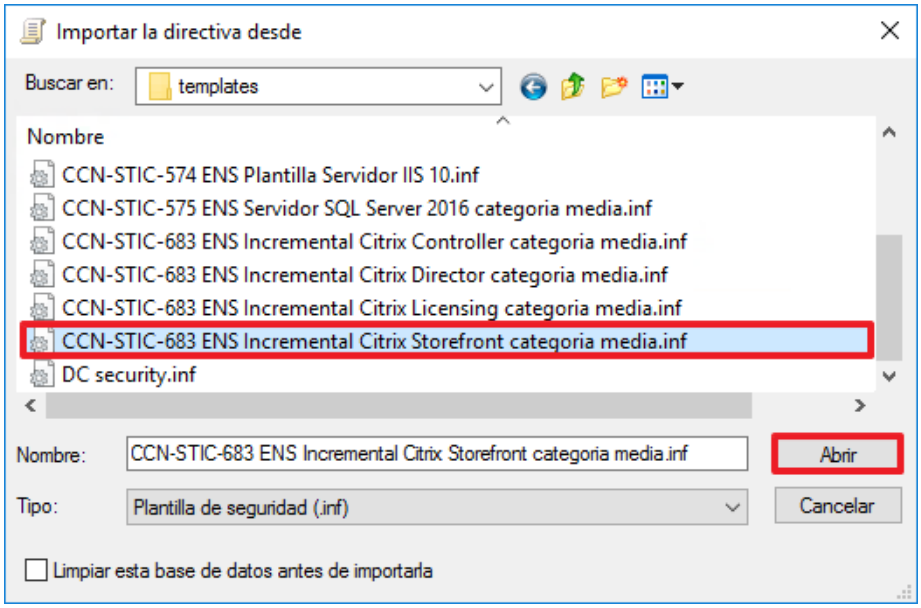
Paso	Descripción
8.	Se lanzará una ventana del intérprete de comandos “cmd.exe” como la mostrada en la siguiente figura. Este script copia todas las plantillas de seguridad a la ubicación “C:\Windows\security\templates” y crea el grupo de seguridad “Administradores de Citrix” en caso de que este no exista. 
9.	Pulse una tecla al finalizar la ejecución del script para cerrar la ventana. 

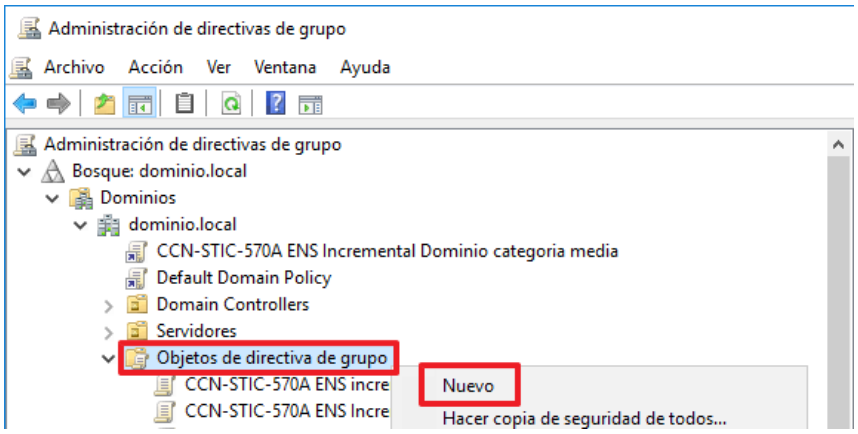
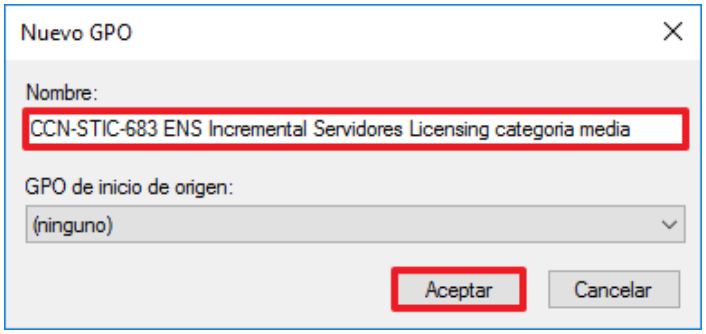
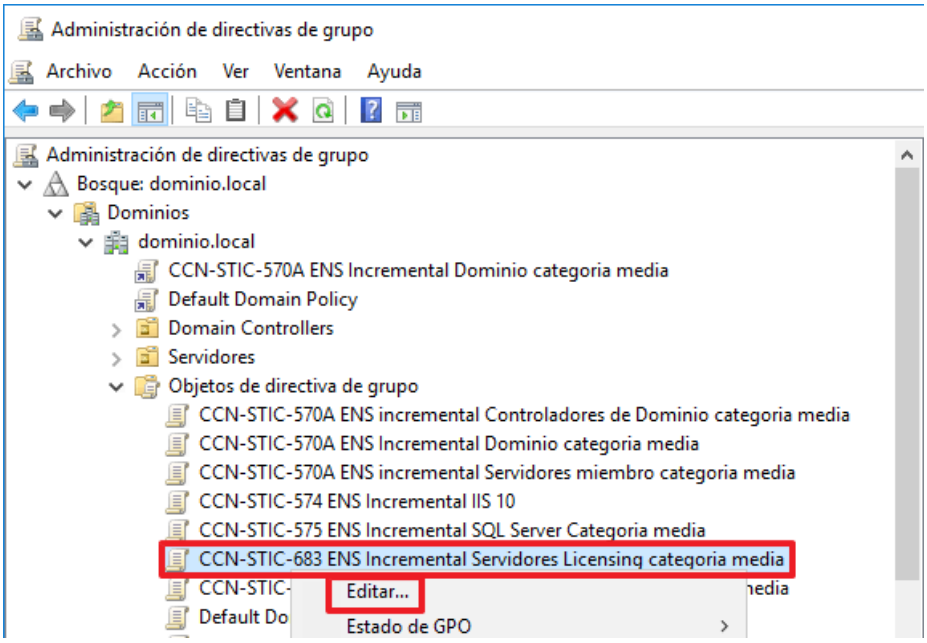
Paso	Descripción
10.	Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios. 
11.	A continuación, en la herramienta "Usuarios y equipos de Active Directory" expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio>" → Servidores"**, y marcándolo con el botón derecho del ratón, seleccione la opción **"Nuevo → Unidad organizativa"** del menú contextual que aparecerá, como se muestra en la siguiente figura. 

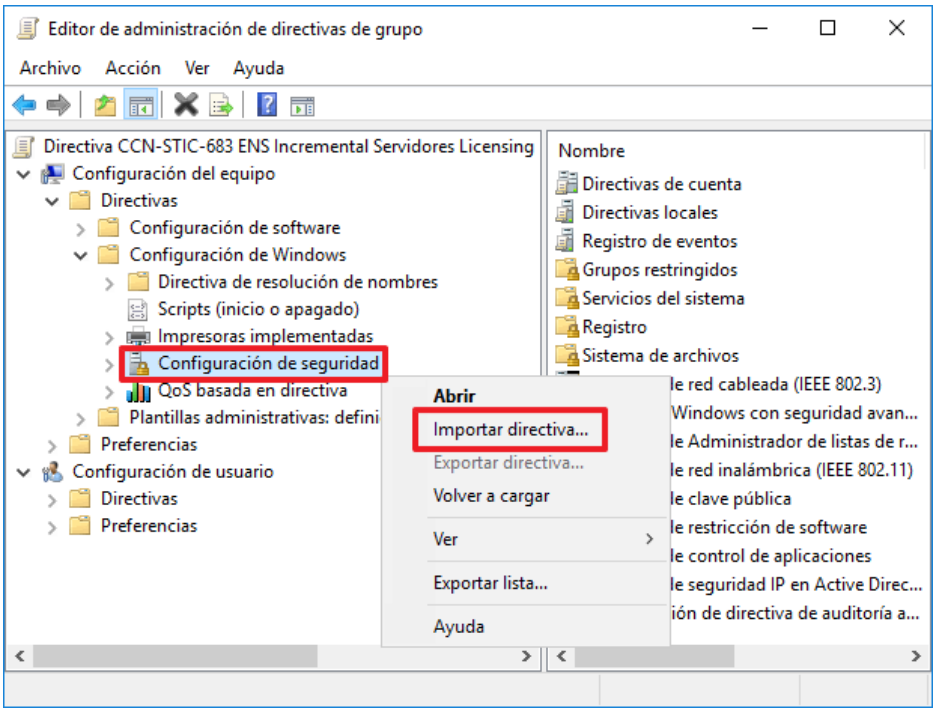
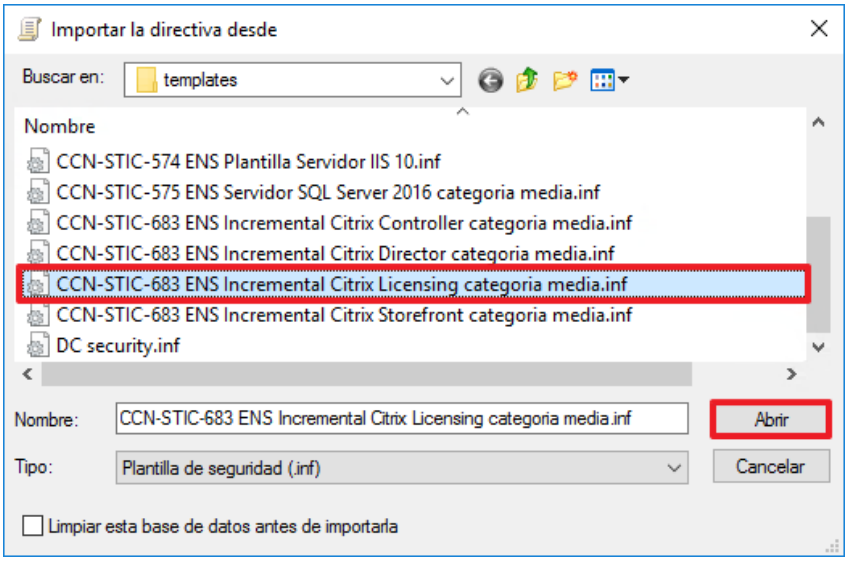
Paso	Descripción
12.	En la ventana resultante, introduzca como nombre de la nueva unidad organizativa “Servidores Citrix Controller” tal y como muestra en la imagen. No desmarque la opción “Proteger contenedores contra eliminación accidental”. Pulse “Aceptar” para crear el nuevo objeto. 
13.	Proceda a crear las siguientes unidades organizativas bajo la unidad organizativa “Servidores”. – Servidores Citrix Controller – Servidores Citrix Storefront – Servidores Citrix Licensing – Servidores Citrix Director
14.	Las nuevas unidades organizativas, aparecerán colgando de “Servidores”, como se muestra en la siguiente figura.  **Nota:** Las unidades organizativas “Servidores IIS 10” y “Servidores SQL Server” deberán haberse creado durante la aplicación de las guías de seguridad codificadas como “CCN-STIC-574” y CCN-STIC-575”.

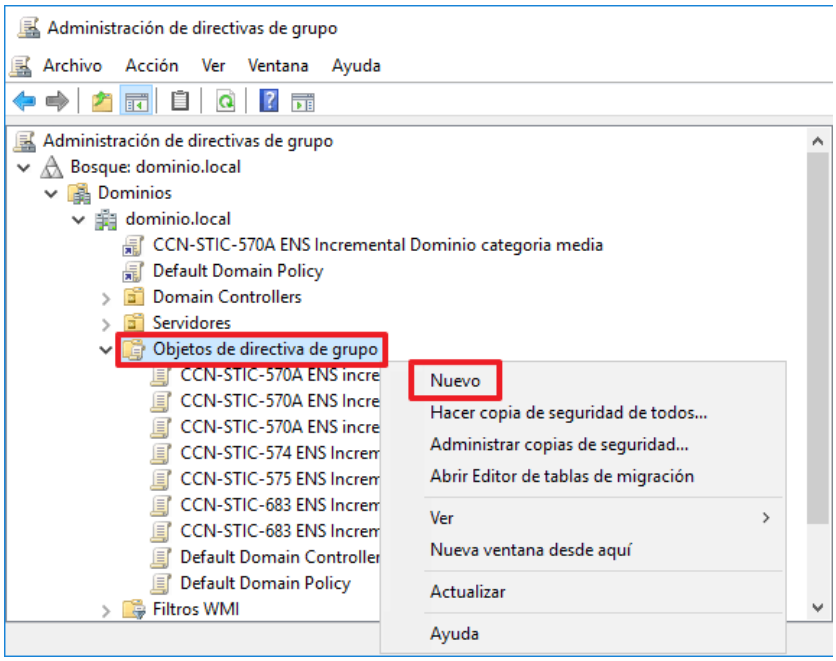
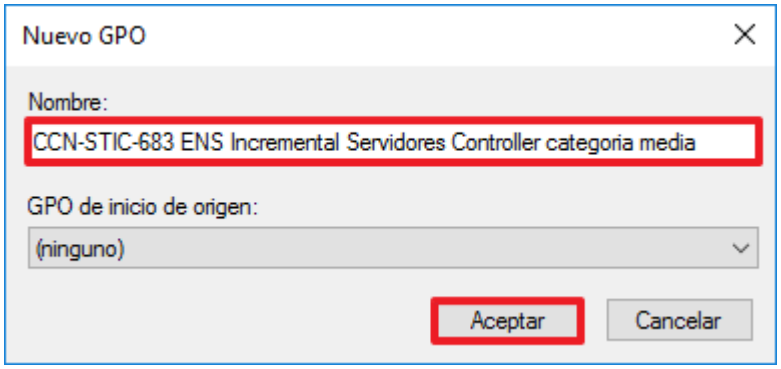
Paso	Descripción
15.	Utilice la herramienta "Administración de Directivas de grupo" (**Administrador del servidor → Herramientas → Administración de Directivas de grupo**). El sistema solicitará elevación de privilegios. 
16.	Expanda el contenedor **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores"**, como se muestra en la siguiente figura. 
17.	A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar la GPO correspondiente. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores del contenedor recién expandido "Servidores".
18.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 

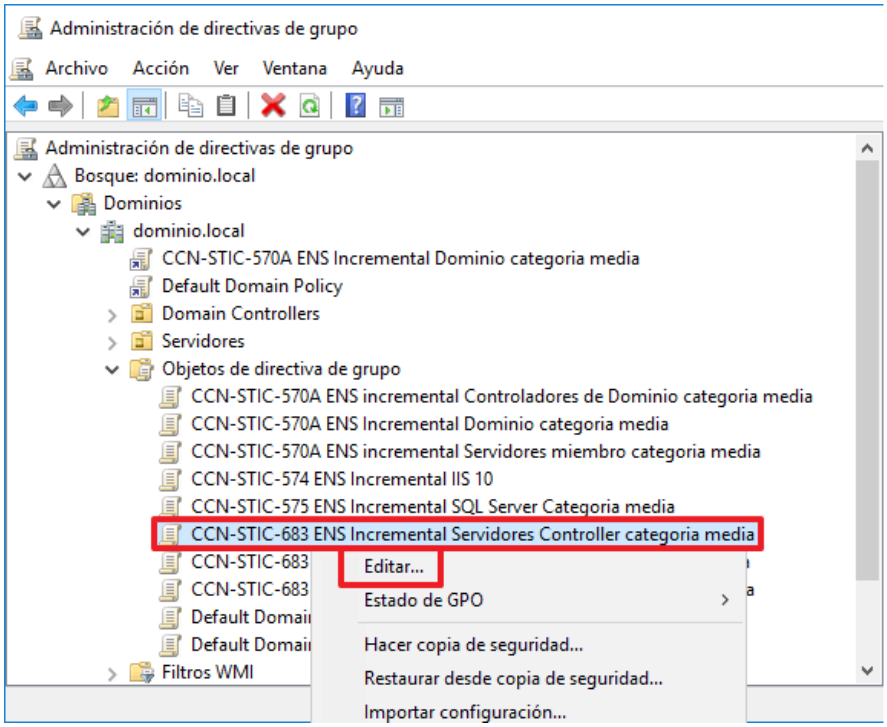
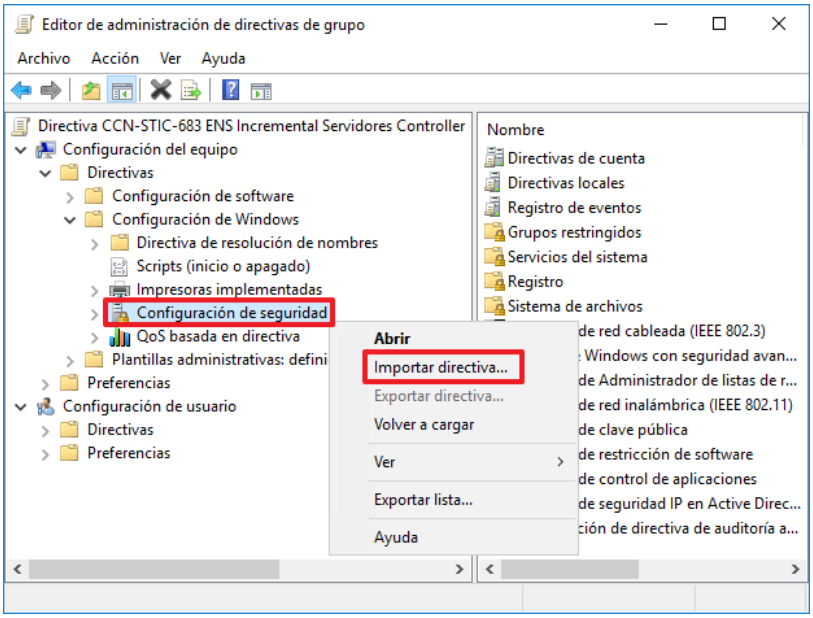
Paso	Descripción
19.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Storefront categoria media" y pulse el botón “Aceptar”. 
20.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Storefront categoria media", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 

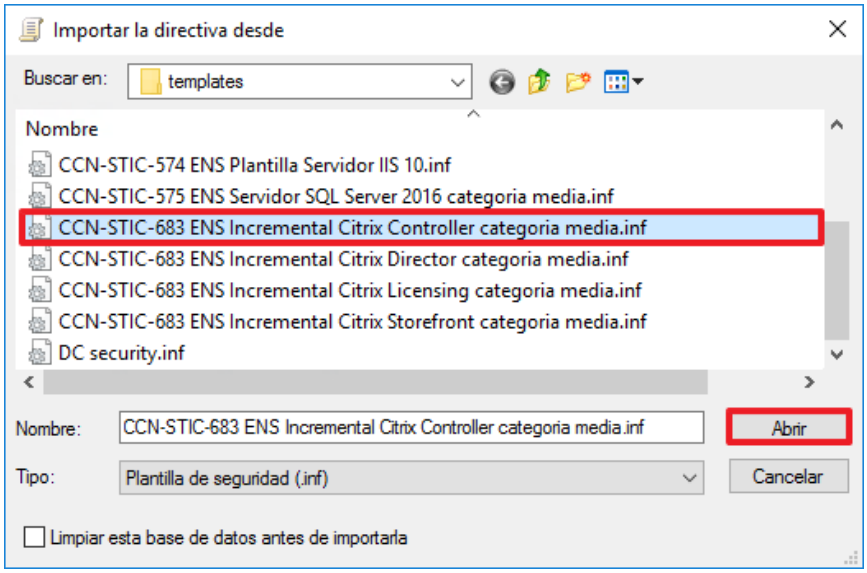
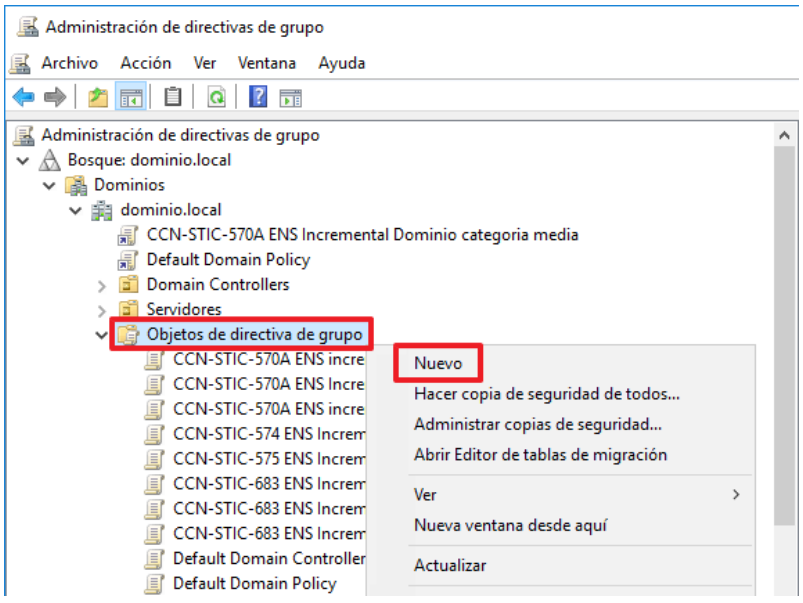
Paso	Descripción
21.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 
22.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Storefront categoria media.inf" y pulse el botón "Abrir". 
23.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Storefront categoria media") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

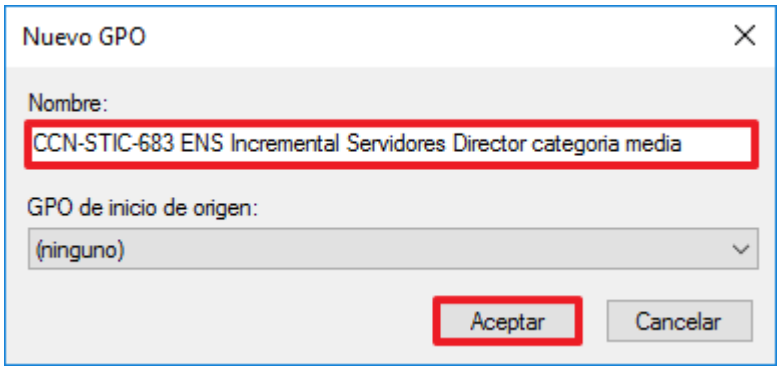
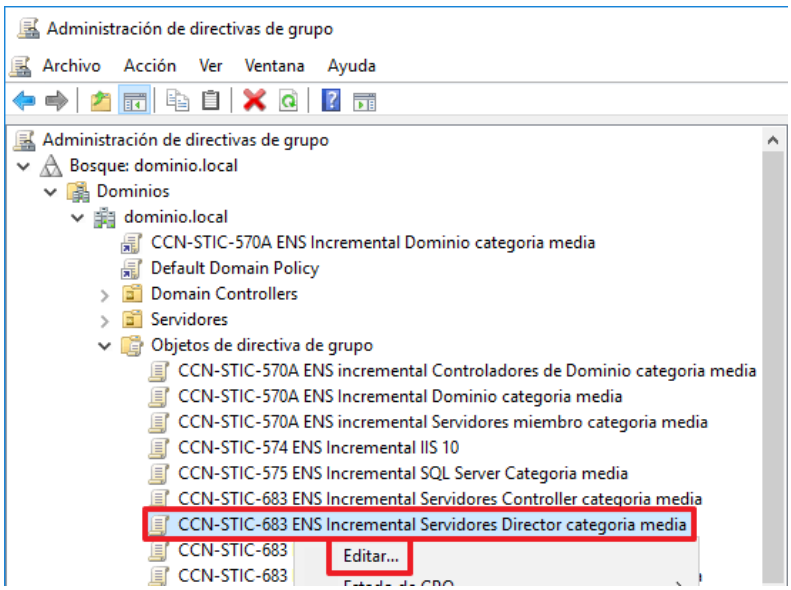
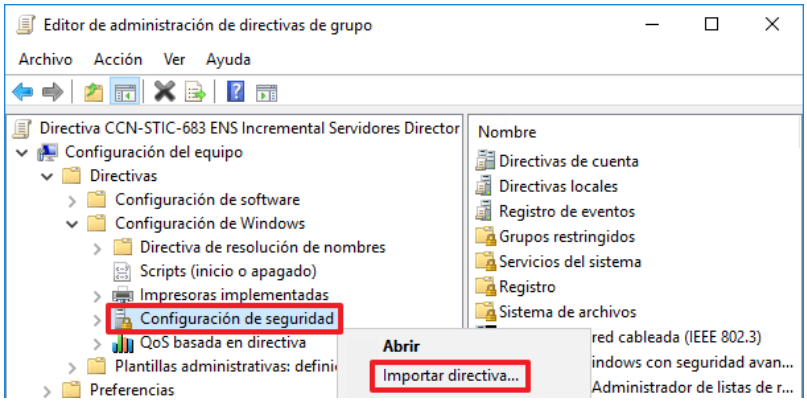
Paso	Descripción
24.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
25.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Licensing categoria media" y pulse el botón “Aceptar”. 
26.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Licensing categoria media", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 

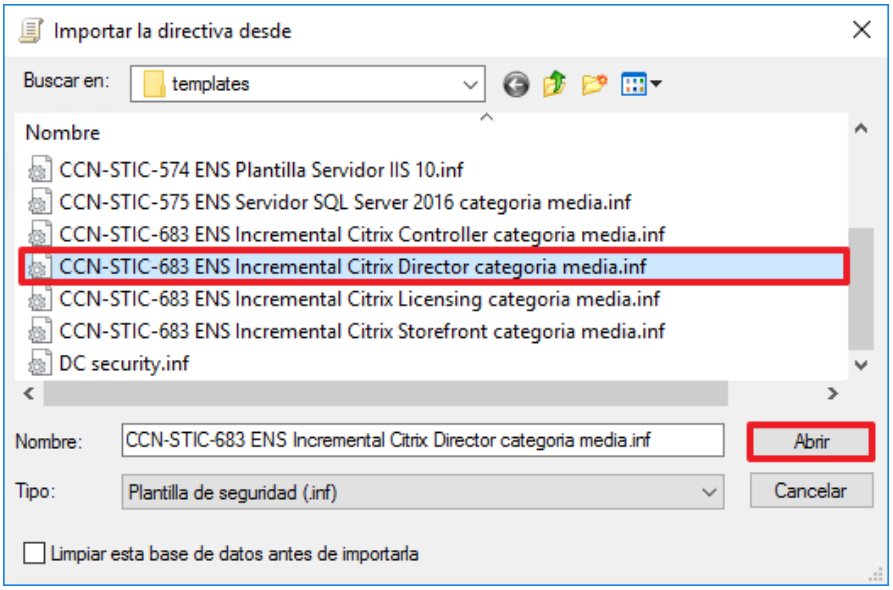
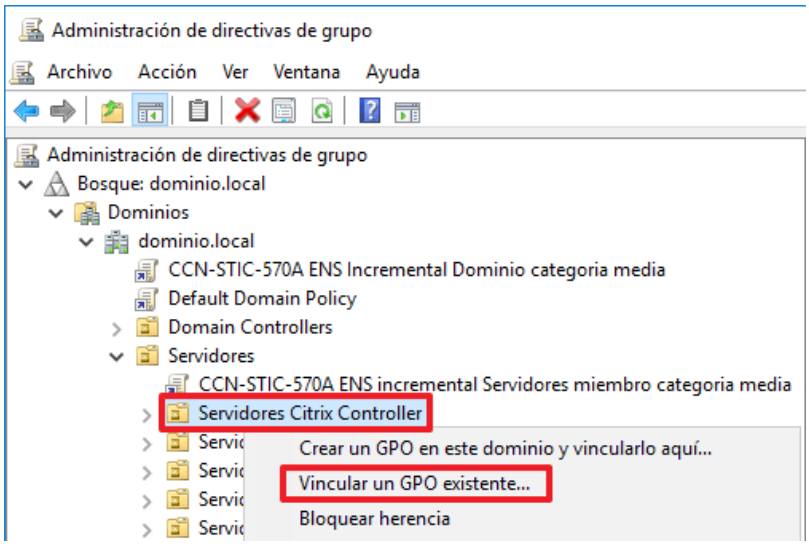
Paso	Descripción
27.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 
28.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Licensing categoria media.inf" y pulse el botón "Abrir". 

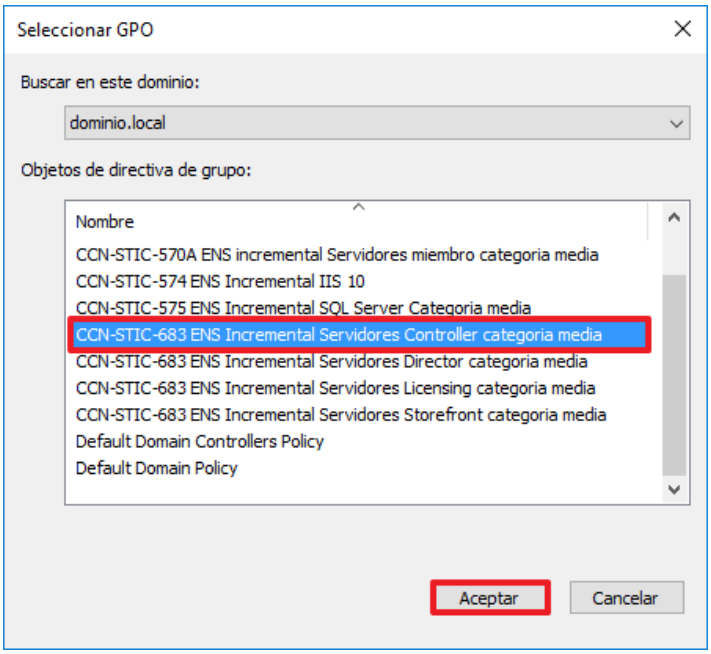
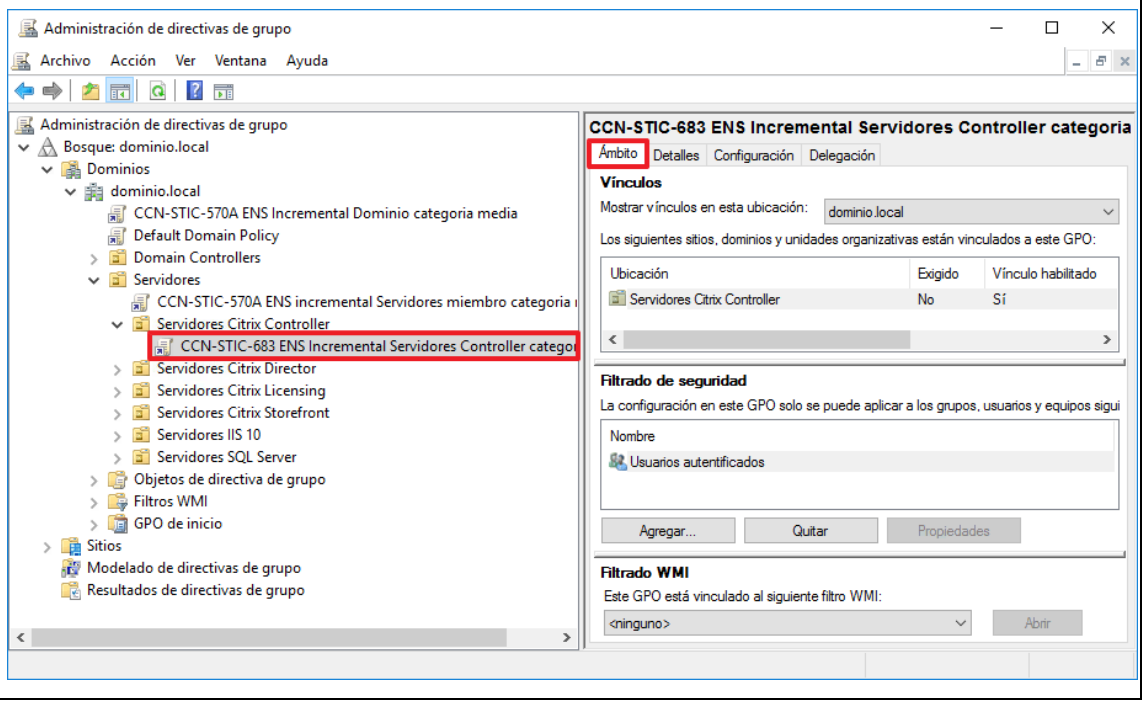
Paso	Descripción
29.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Licensing categoria media") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
30.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
31.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Controller categoria media" y pulse el botón “Aceptar”. 

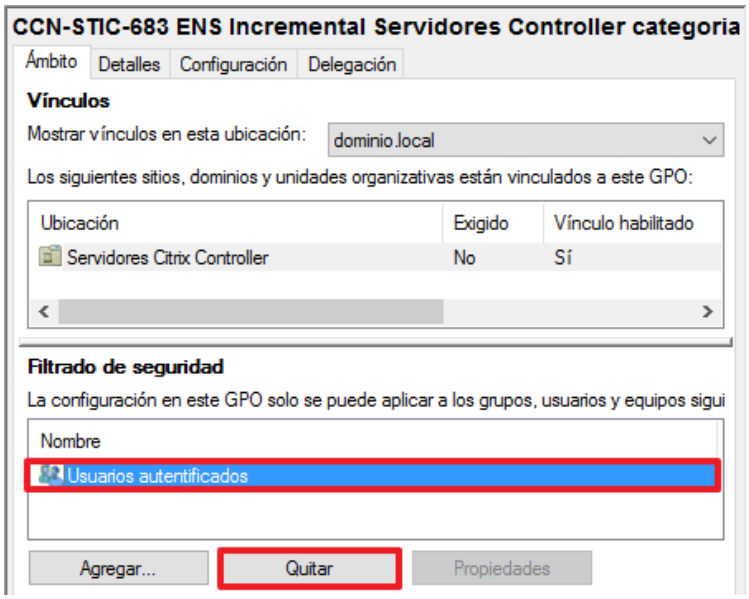
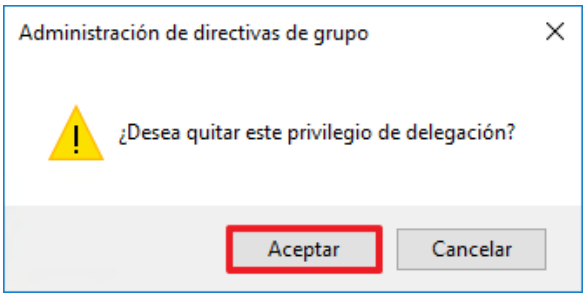
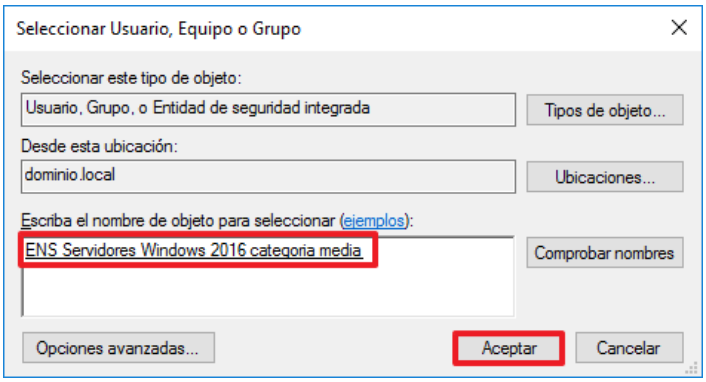
Paso	Descripción
32.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Controller categoria media", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 
33.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 

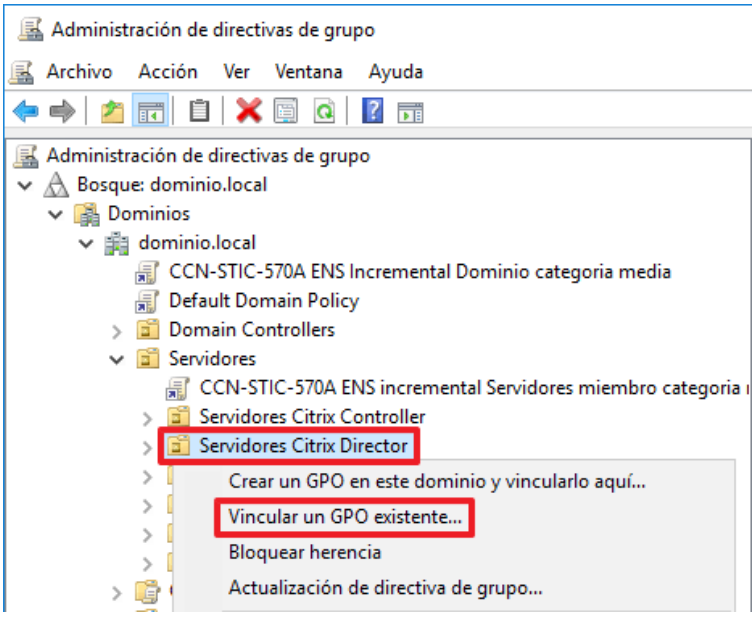
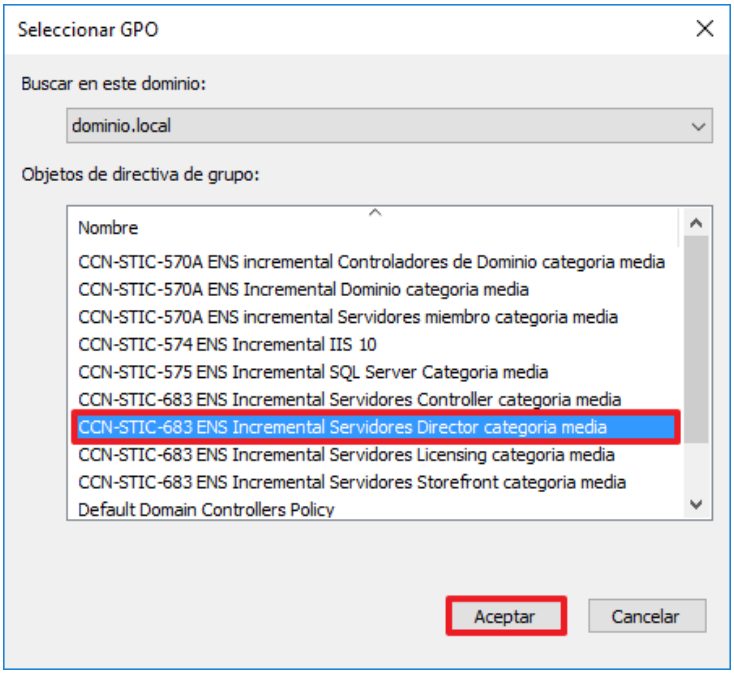
Paso	Descripción
34.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Controller categoria media.inf" y pulse el botón "Abrir". 
35.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Controller categoria media") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
36.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 

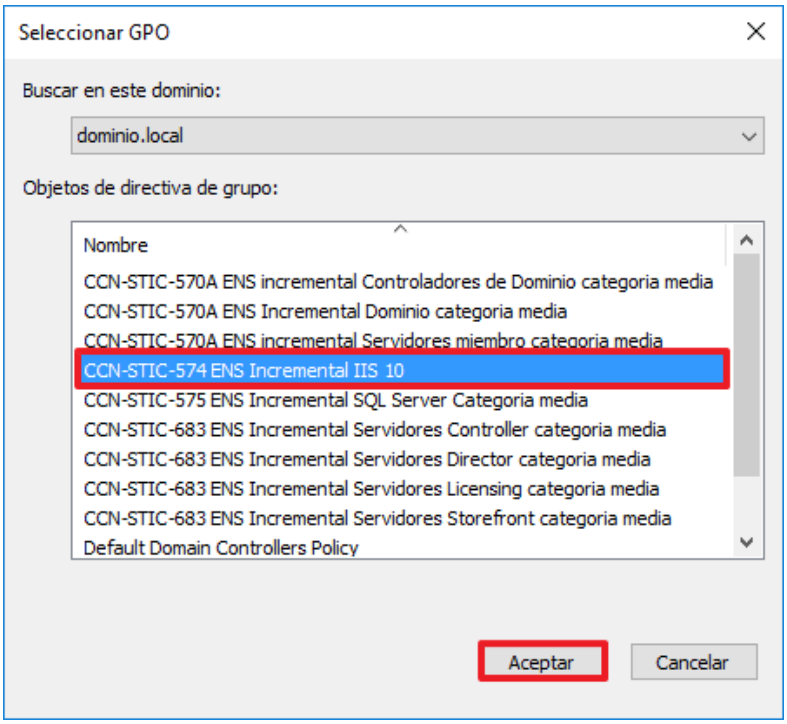
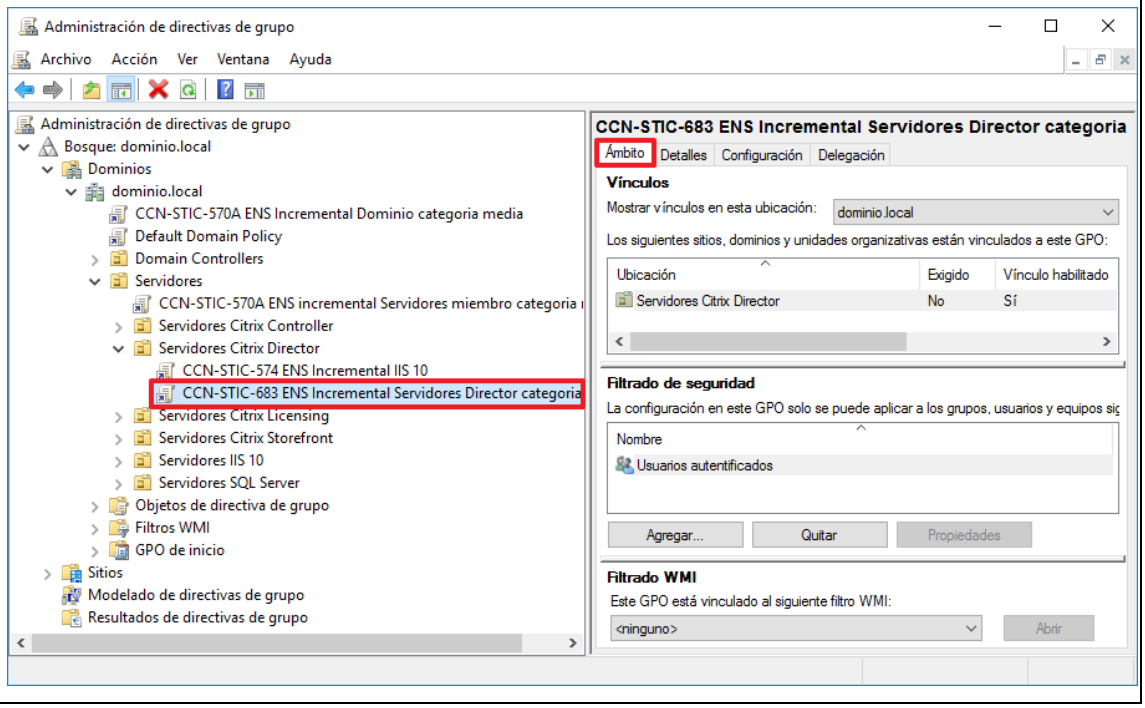
Paso	Descripción
37.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Director categoria media" y pulse el botón “Aceptar”. 
38.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Director categoria media", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 
39.	Despliegue el objeto de directiva de grupo y sitúese en la ruta **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 

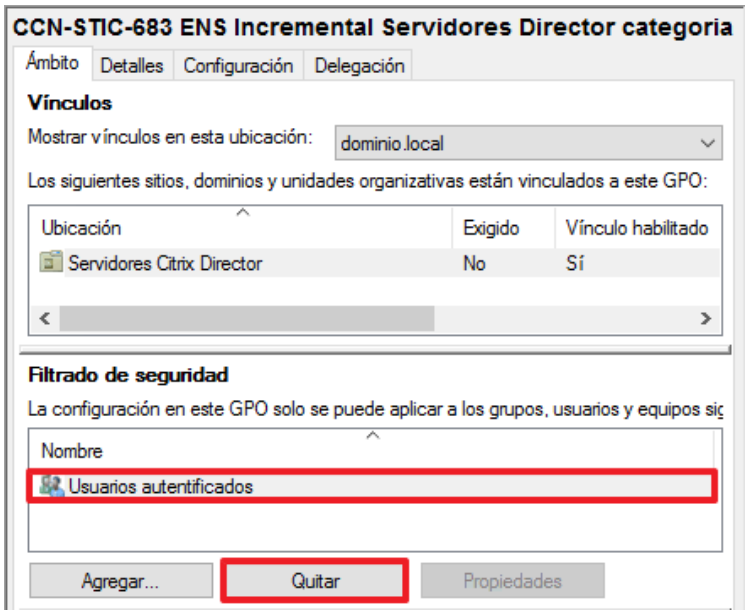
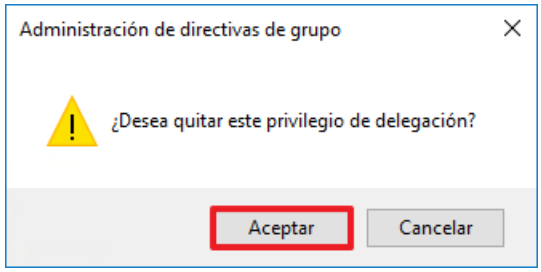
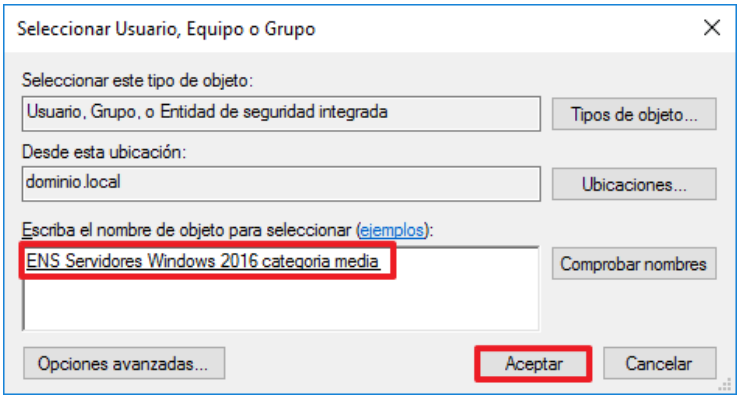
Paso	Descripción
40.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Director categoria media.inf" y pulse el botón "Abrir". 
41.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Director categoria media") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
42.	En la ventana "Administración de directivas de grupo", expanda y seleccione el contenedor **"Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Controller"**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 

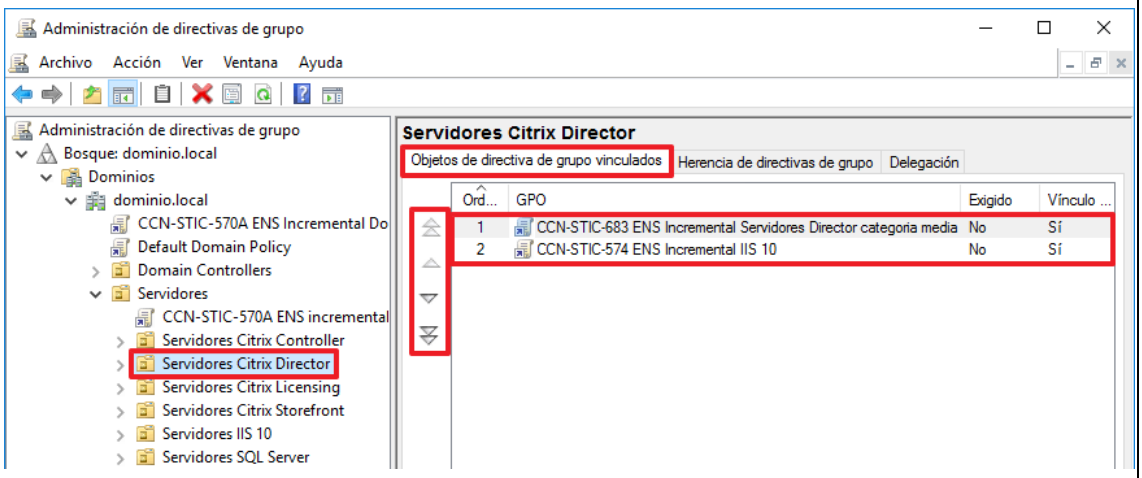
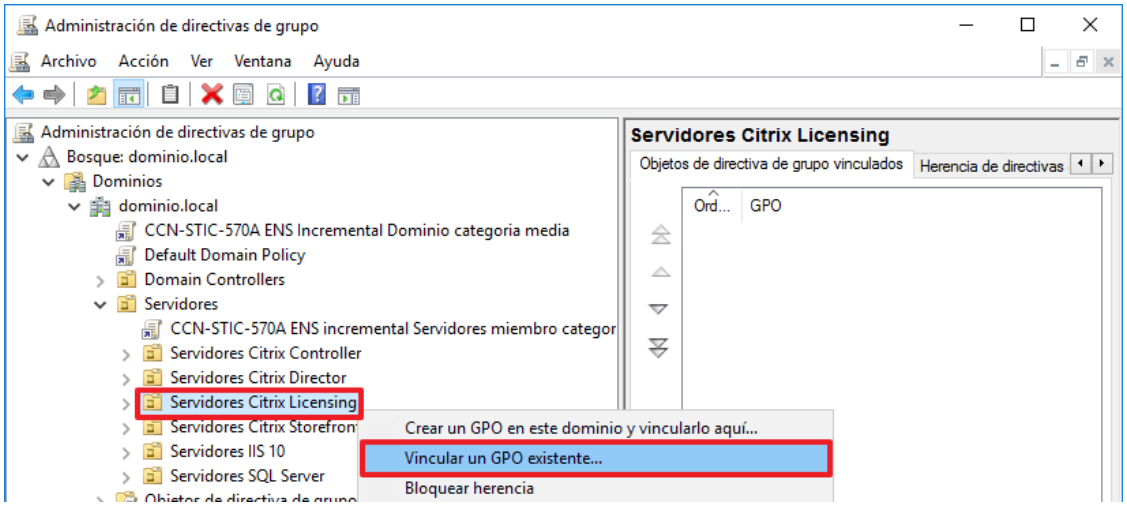
Paso	Descripción
43.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Controller categoria media” y pulse “Aceptar”. 
44.	Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

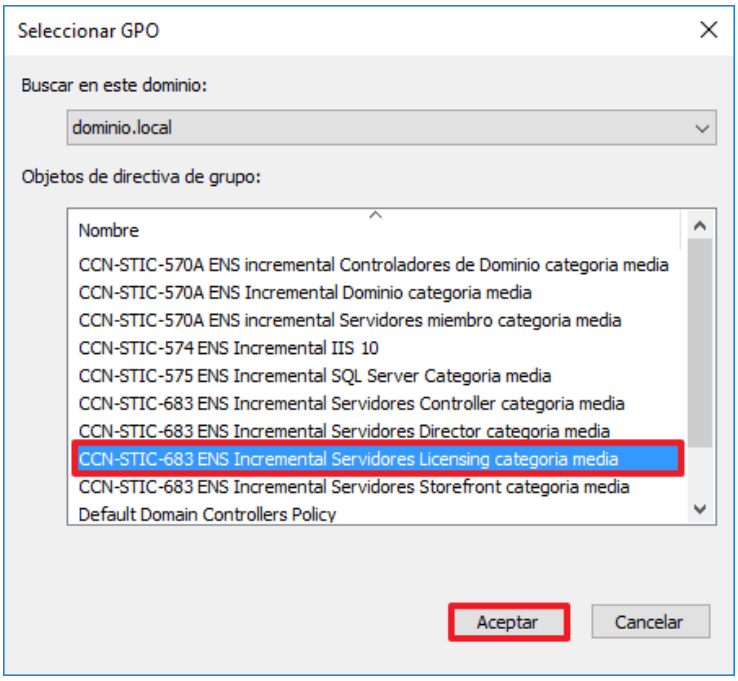
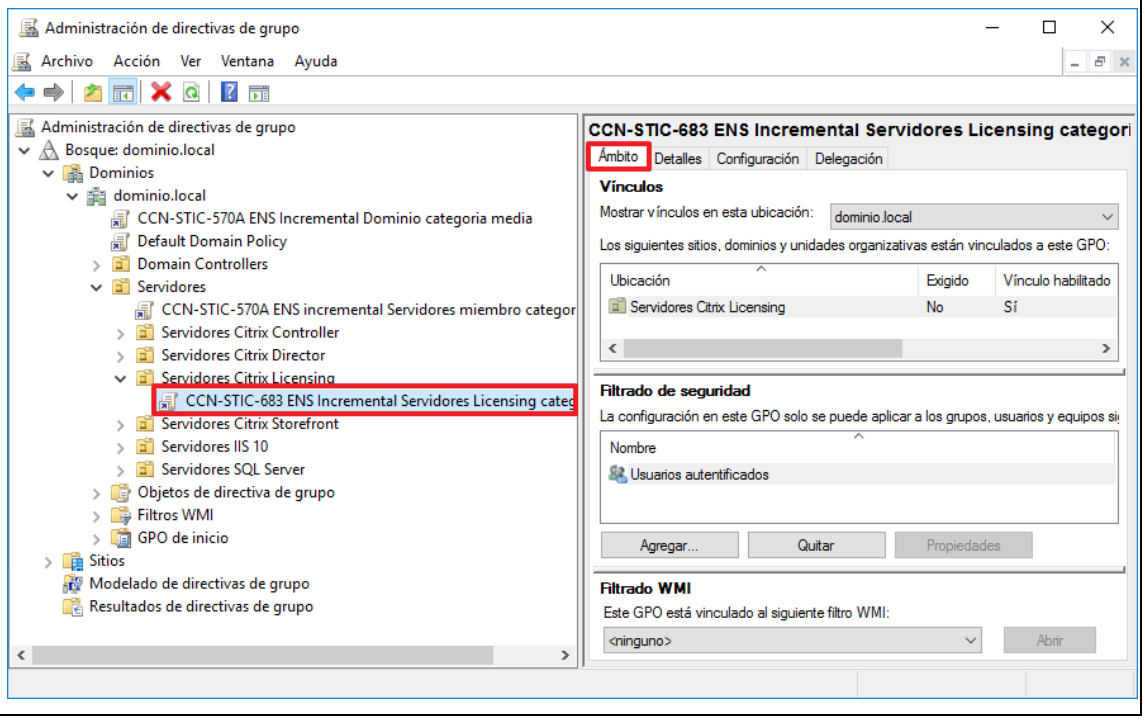
Paso	Descripción
45.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
46.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
47.	Una vez quitado, pulse el botón “Agregar…”.
48.	Introduzca como nombre “ENS servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

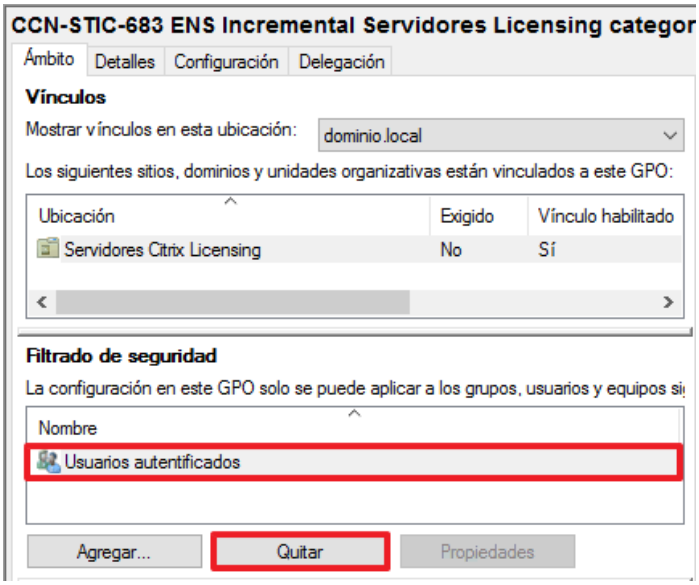
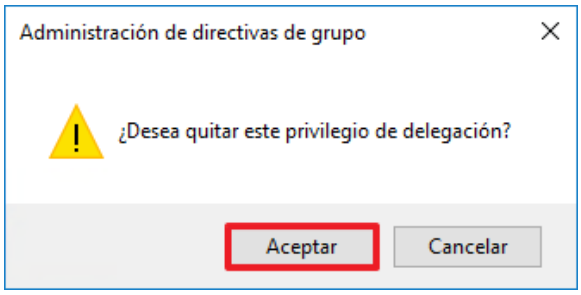
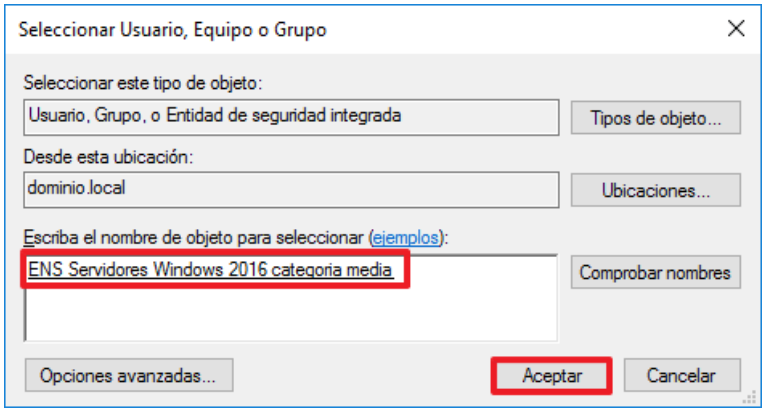
Paso	Descripción
49.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Director”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 
50.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Director categoria media”. 

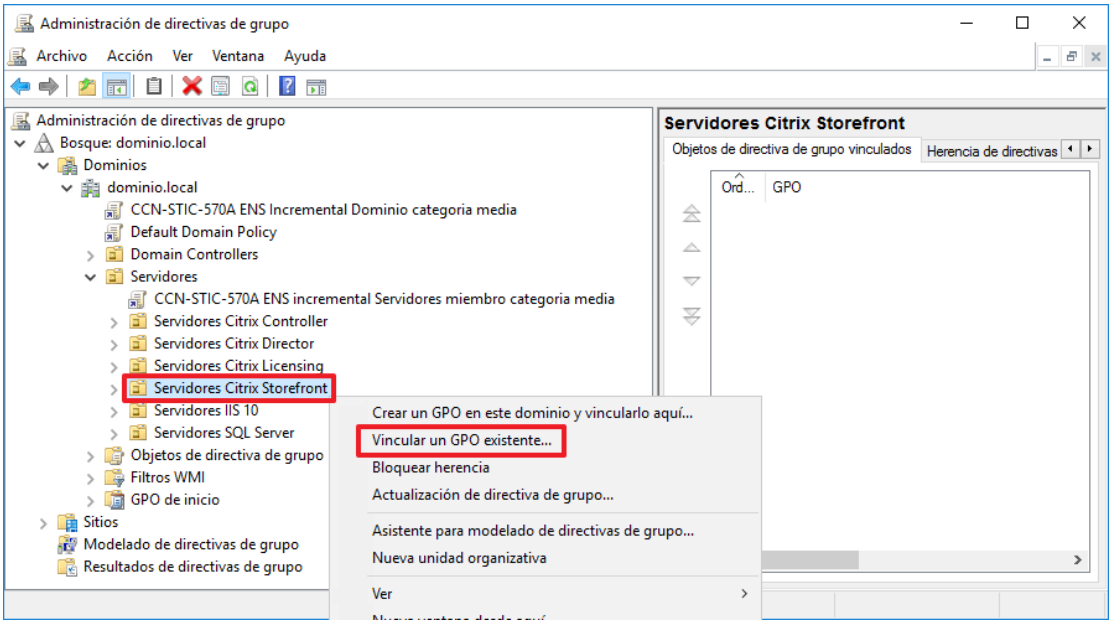
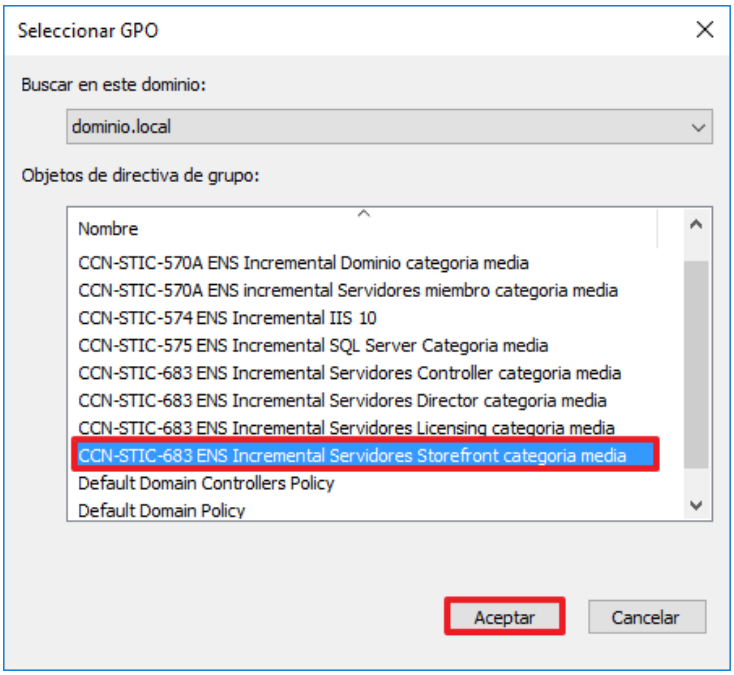
Paso	Descripción
51.	Repita el mismo proceso para vincular el GPO “CCN-STIC-574 ENS Incremental IIS 10”. 
52.	Seleccione la política de grupo “CCN-STIC-683 ENS Incremental Servidores Director categoria media” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

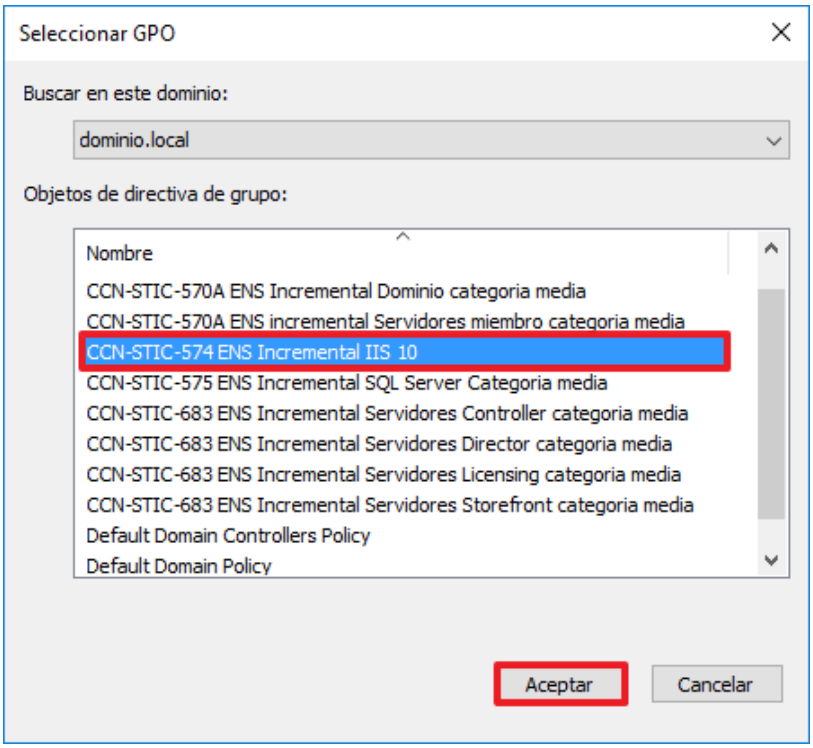
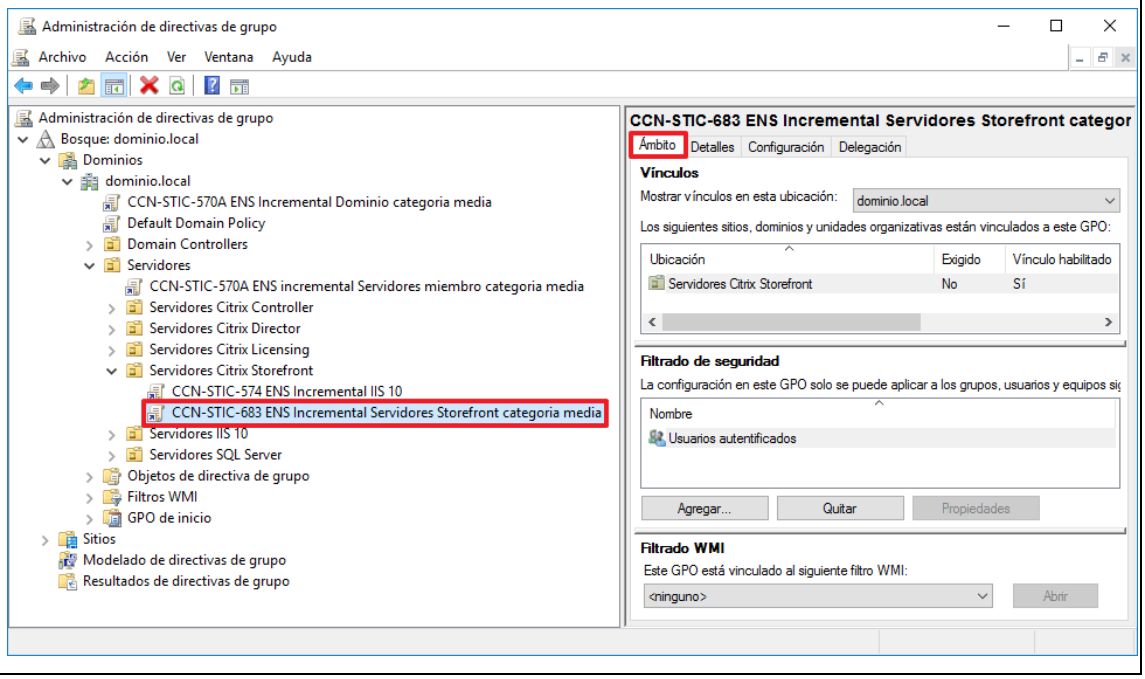
Paso	Descripción
53.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
54.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
55.	Una vez quitado, pulse el botón “Agregar…”.
56.	Introduzca como nombre “ENS servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

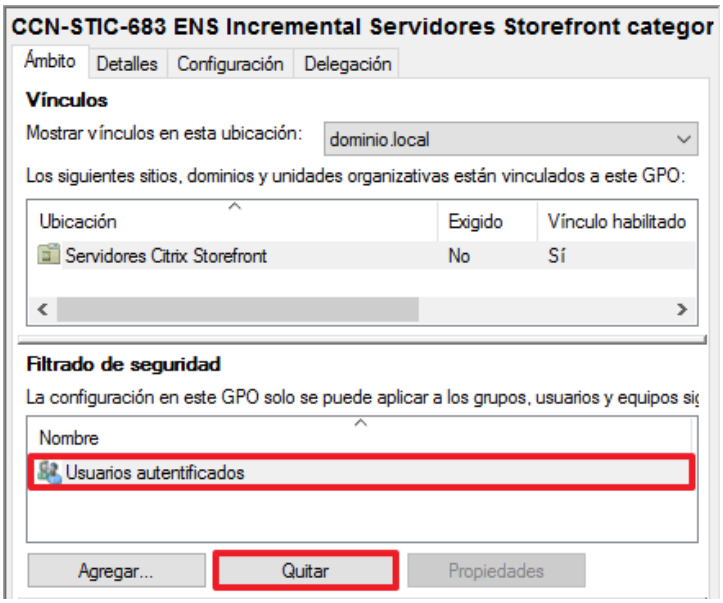
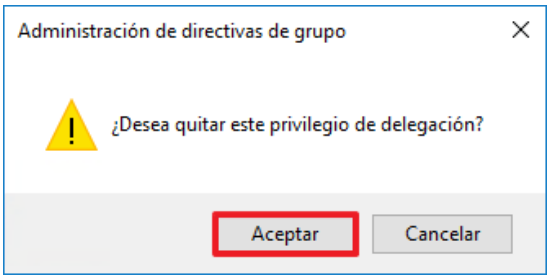
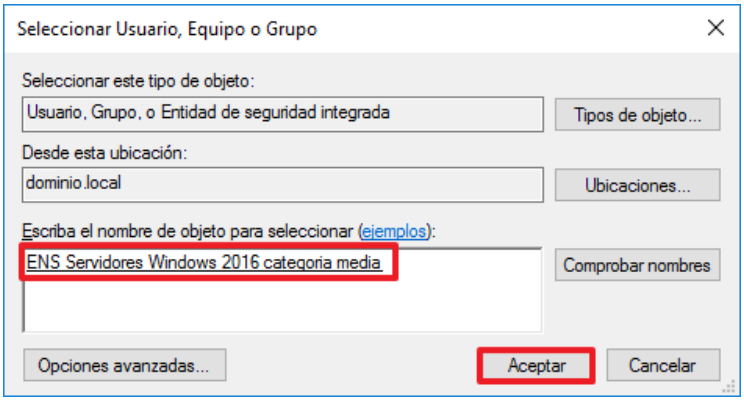
Paso	Descripción
57.	Seleccione el contenedor “Servidores Citrix Director” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura. – 1 - CCN-STIC-683 ENS Incremental Servidores Director categoria media – 2 - CCN-STIC-574 ENS Incremental IIS 10 Si no lo es, modifique el orden de los vínculos para que sea igual al indicado. Para ello seleccione un vínculo y utilice las flechas hacia arriba y hacia abajo que hay en la parte izquierda de la pestaña. 
58.	Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá.
59.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Licensing”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 

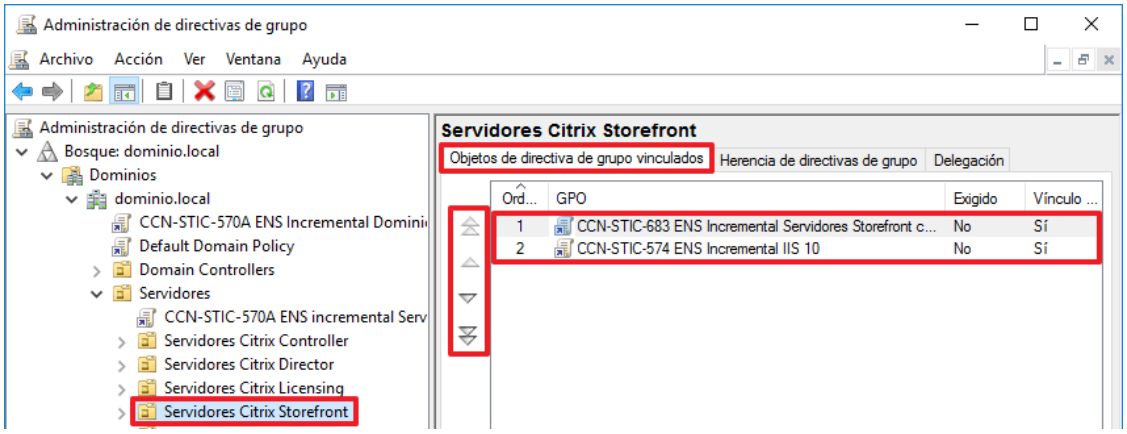
Paso	Descripción
60.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Licensing categoria media”. 
61.	Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
62.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
63.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
64.	Una vez quitado, pulse el botón “Agregar…”.
65.	Introduzca como nombre “ENS servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

Paso	Descripción
66.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **"Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Storefront”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 
67.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Storefront categoria media” y pulse “Aceptar”. 

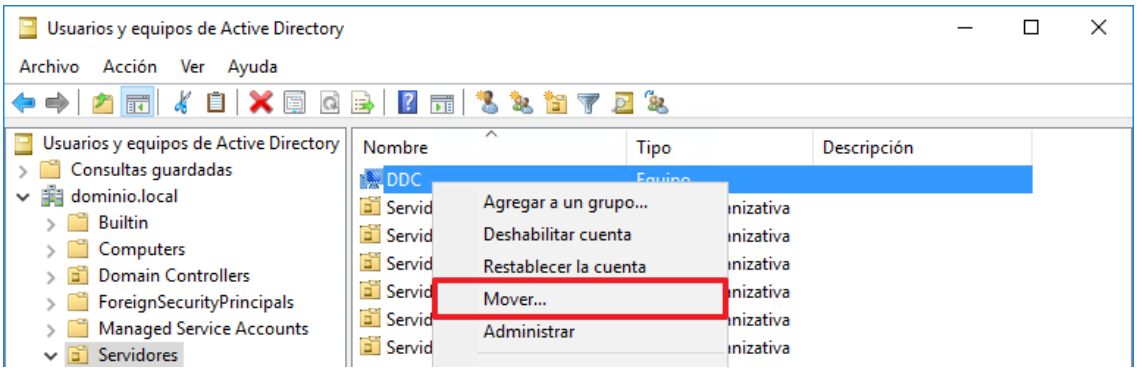
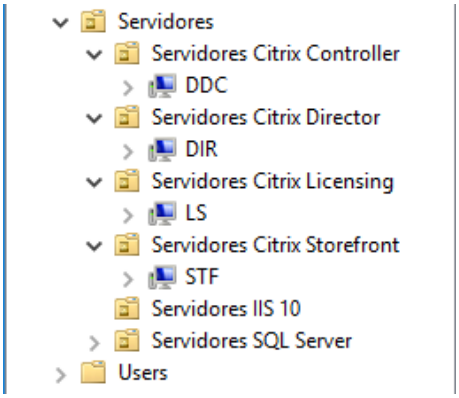
Paso	Descripción
68.	De manera análoga vincule la GPO denominada “CCN-STIC-574 ENS Incremental Servidores IIS 10”. 
69.	Seleccione la política de grupo “CCN-STIC-683 ENS Incremental Servidores Storefront categoria media” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
70.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
71.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
72.	Una vez quitado, pulse el botón “Agregar…”.
73.	Introduzca como nombre “ENS servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

Paso	Descripción
74.	Seleccione el contenedor “Servidores Citrix Storefront” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura. – 1 - CCN-STIC-683 ENS Incremental Servidores Storefront categoria media – 2 - CCN-STIC-574 ENS Incremental IIS 10 Si no lo es, modifique el orden de los vínculos para que sea igual al indicado. Para ello seleccione un vínculo y utilice las flechas hacia arriba y hacia abajo que hay en la parte izquierda de la pestaña. 
75.	Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá.

En este punto los GPOs se encuentran configurados correctamente en Active Directory y su configuración se aplicará automáticamente a los nuevos servidores que necesite añadir a la infraestructura. En pasos posteriores moverá cada uno de los objetos de equipo dentro de sus correspondientes unidades organizativas.

Paso	Descripción
76.	Si no lo ha hecho todavía, inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el servidor que va a asegurar, con una cuenta con derechos de administración en el dominio.
77.	Mueva las cuentas de equipo de cada uno de los roles que haya aprovisionado previamente para la implementación de la infraestructura de Citrix. En función del rol que haya aprovisionado previamente debe mover la cuenta de equipo a una unidad organizativa u otra. La siguiente tabla de referencia puede ayudarle con el proceso. **Nota:** Durante la aplicación de la guía “CCN-STIC-574” habrá situado los servidores correspondientes a los roles de Citrix Storefront y Citrix Director en la Unidad Organizativa “Servidores IIS 10” en este punto deberá mover dichos servidores a las nuevas Unidades Organizativas creadas para cada rol.

<table>
<tr><th>Paso</th><th colspan="3">Descripción</th></tr>
<tr><td></td><td>Rol</td><td>Unidad Organizativa</td><td>Cuenta de equipo</td></tr>
<tr><td></td><td>Citrix Controller</td><td>Servidores Citrix Controller</td><td>DDC</td></tr>
<tr><td></td><td>Citrix Storefront</td><td>Servidores Citrix Storefront</td><td>STF</td></tr>
<tr><td></td><td>Citrix Licensing</td><td>Servidores Citrix Licensing</td><td>LS</td></tr>
<tr><td></td><td>Citrix Director</td><td>Servidores Citrix Director</td><td>DIR</td></tr>
<tr><td>78.</td><td colspan="3">Para ello, abra la herramienta "Administrador del servidor" y despliegue el menú “Herramientas → Usuarios y equipos de Active Directory”. El sistema solicitará elevación de privilegios.
A continuación, en la herramienta “Usuarios y equipos de Active Directory” despliegue la ruta “<nombre de su dominio> → Servidores", y marcando con el botón derecho del ratón cada uno de los servidores, pulse la opción “Mover…”.
 
</td></tr>
<tr><td>79.</td><td colspan="3">De forma análoga, realice el paso anterior por cada uno de los servidores que desee añadir a la plataforma.</td></tr>
<tr><td>80.</td><td colspan="3">Finalmente, dentro de cada unidad organizativa debe apreciar cada uno de los servidores añadidos.
 
</td></tr>
<tr><td>81.</td><td colspan="3">Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor.</td></tr>
</table>

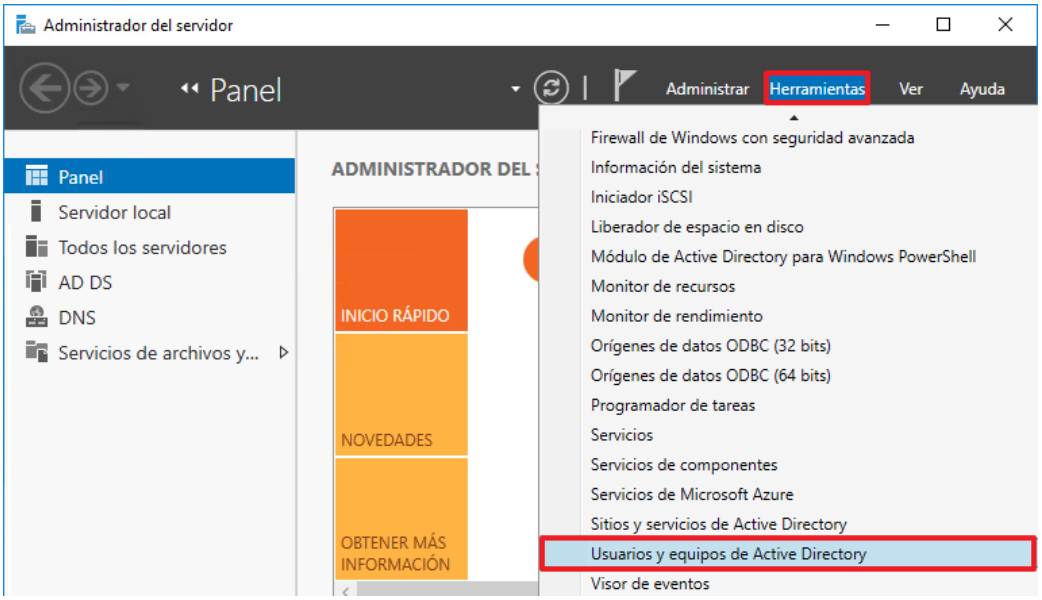
Con la anterior configuración cada uno de los servidores recogerá de forma automática las directivas de grupo configuradas para su rol.

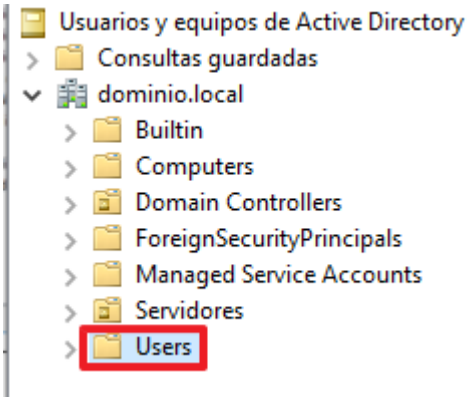
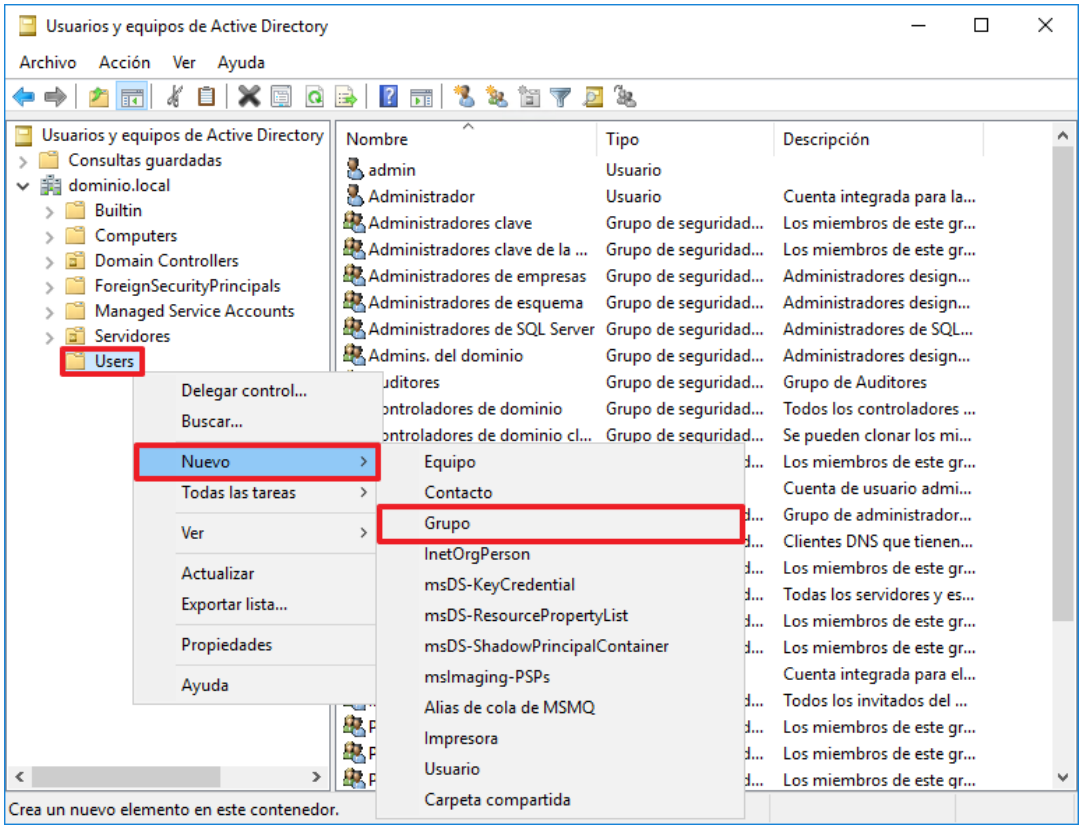
Nota: En el caso de no aplicarse de forma automática la configuración de GPO aplicadas puede utilizar el comando **“gpupdate /force”** para forzar el proceso.

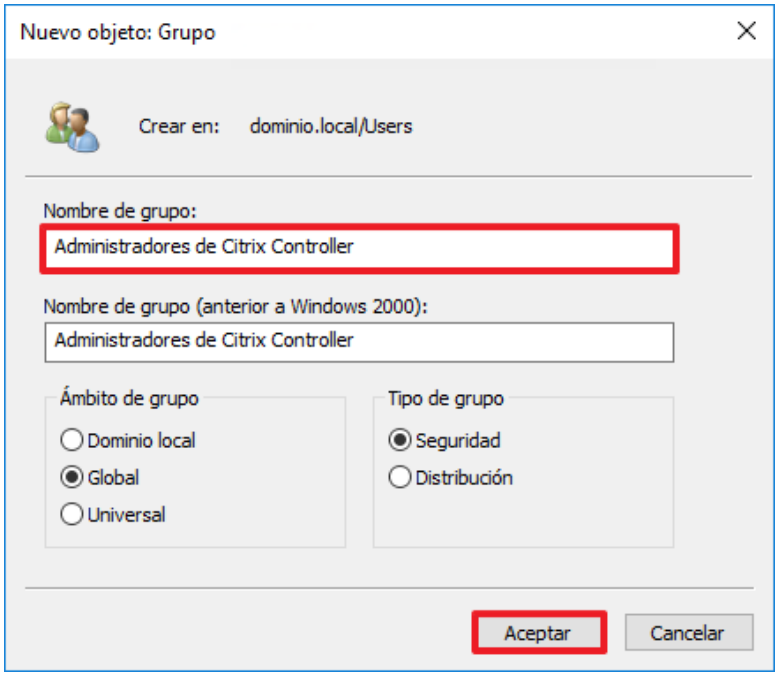
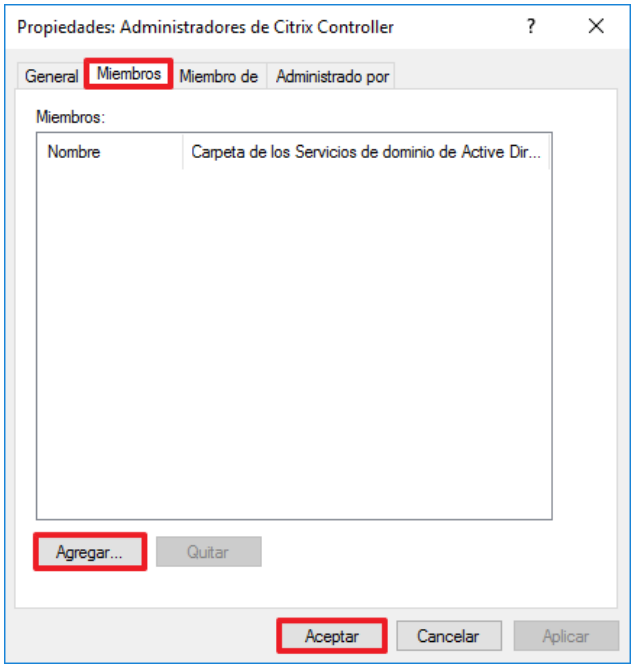
2. SEGREGACIÓN DE ROLES

Con la aplicación del ENS para la categoría media sobre una infraestructura de Citrix Virtual Apps and Desktops será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar la propia infraestructura.

En los siguientes pasos se procederá a crear, a modo de ejemplo, un grupo de usuarios cuya función será la de administrar uno de los roles de la infraestructura.

Paso	Descripción
82.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
83.	Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios. 

Paso	Descripción
84.	Expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"**, como se muestra en la siguiente figura. 
85.	Pulsando con el botón derecho sobre "Users" diríjase al apartado de configuración **"Nuevo → Grupo"**. 

Paso	Descripción
86.	Sobre la ventana emergente para la creación del nuevo grupo introduzca "Administradores de Citrix Controller" y pulse sobre "Aceptar" como se indica en la siguiente imagen. 
87.	A continuación, deberá agregar los usuarios que realizarán la administración de los servidores Citrix Controller al grupo "Administradores de Citrix Controller". Para ello diríjase a las propiedades del grupo recién creado y en el apartado "Miembros" añada cada usuario pulsando sobre el botón "Agregar...". Una vez introducidos todos los usuarios pulse "Aceptar". 

3. CERTIFICADOS

Citrix Virtual Apps and Desktops faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media y alta de seguridad del ENS el uso de certificados emitidos por entidades certificadoras de terceros, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está totalmente desaconsejado el uso de certificados autofirmados.

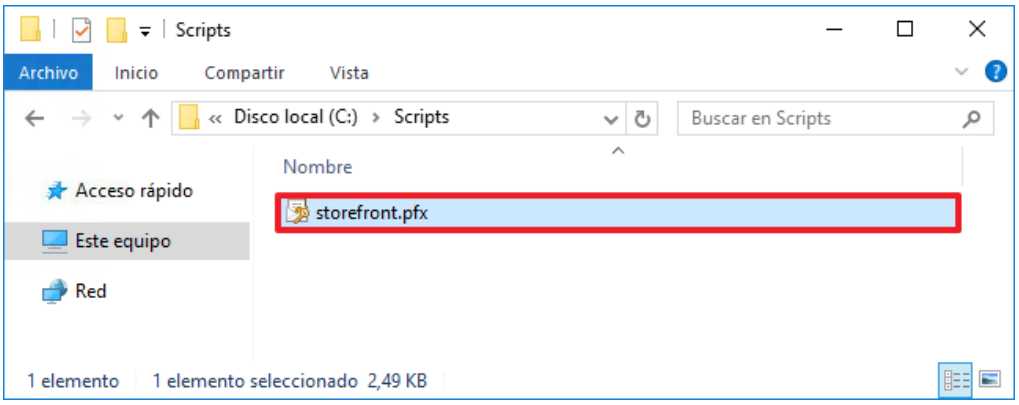
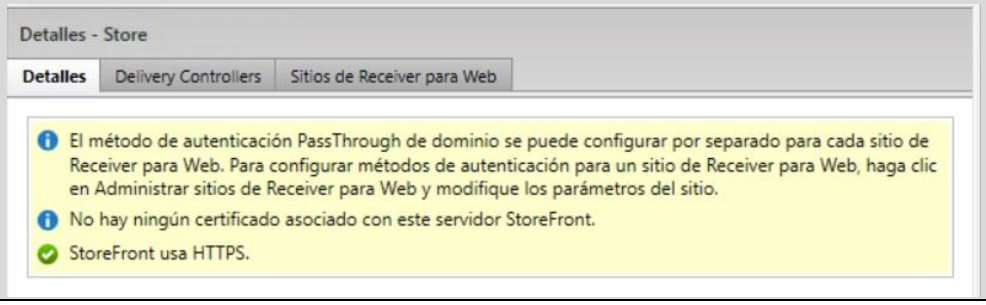
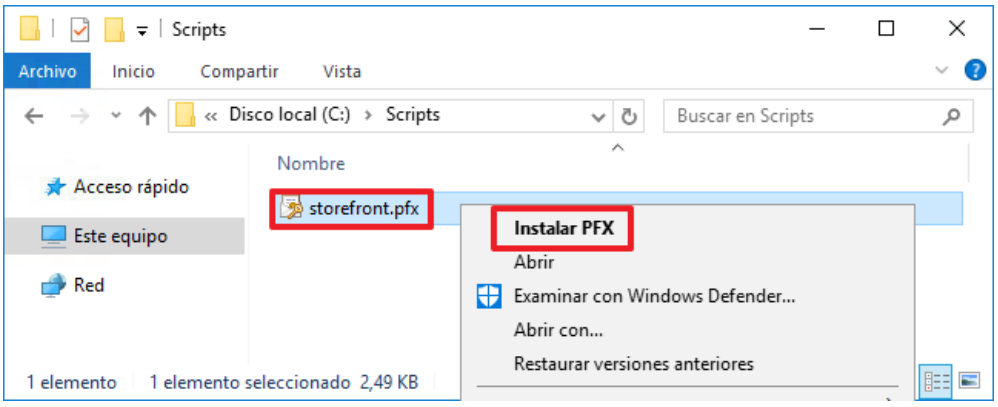
Para la categoría media de seguridad del ENS se configuran certificados para los siguientes roles de la infraestructura:

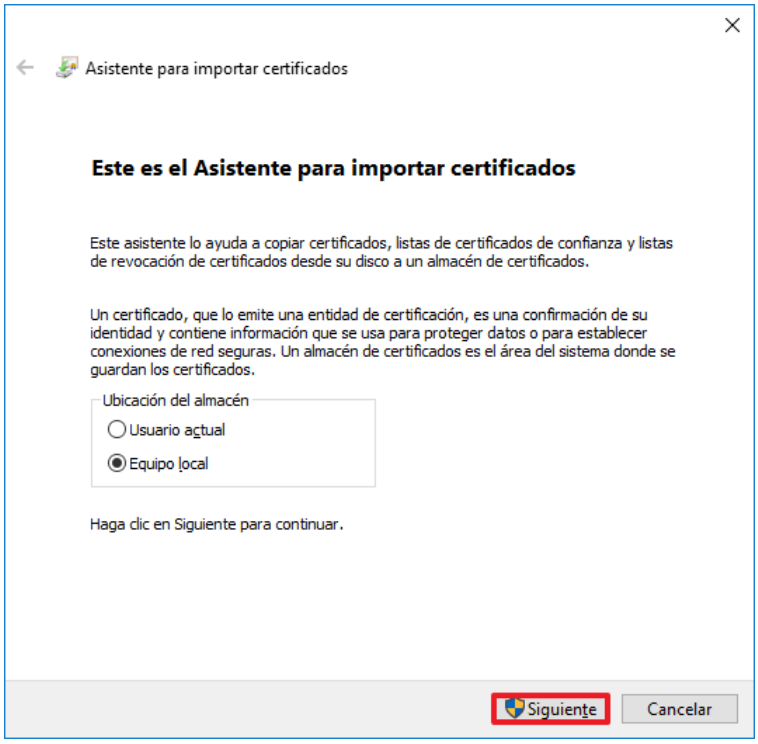
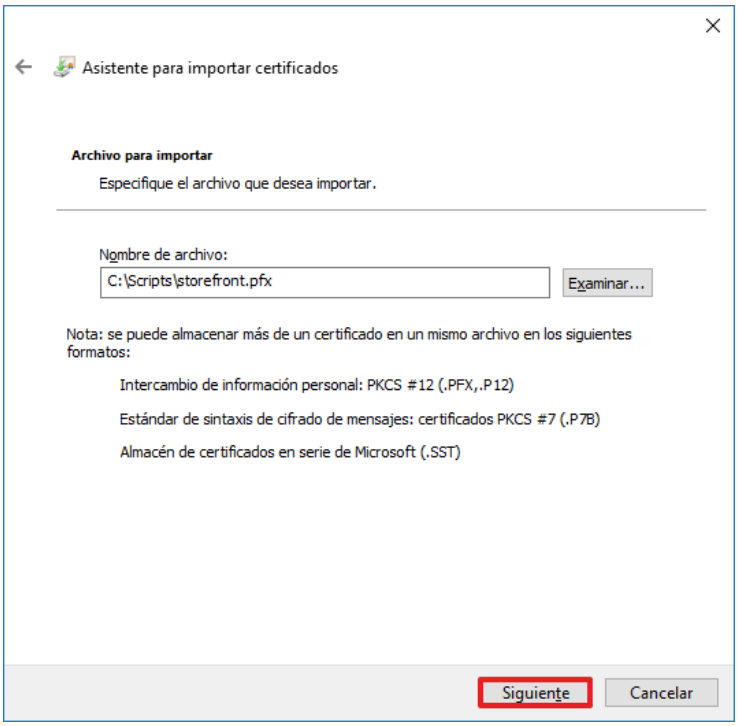
a) Servidor con el rol Citrix Storefront.

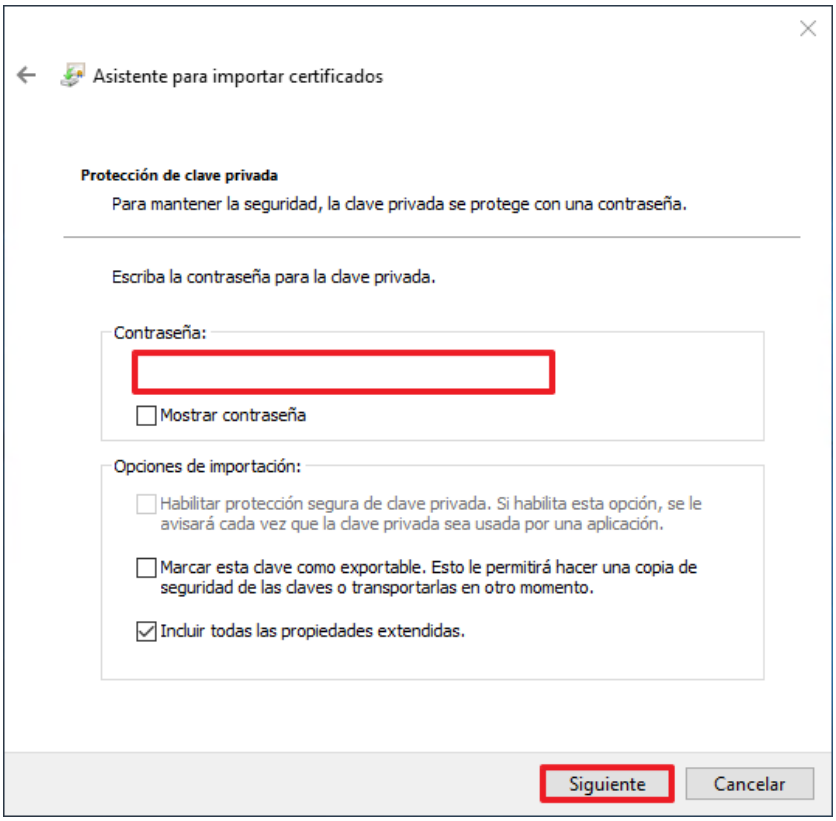
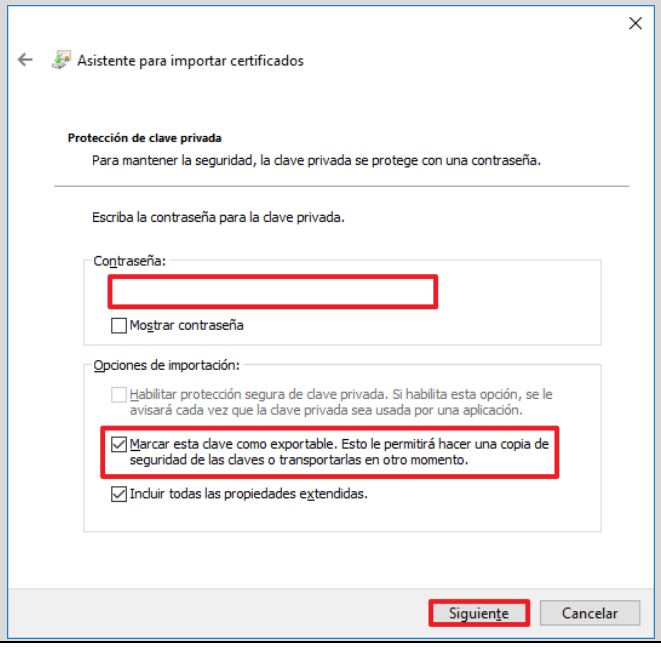
b) Servidores con el rol Citrix Director.

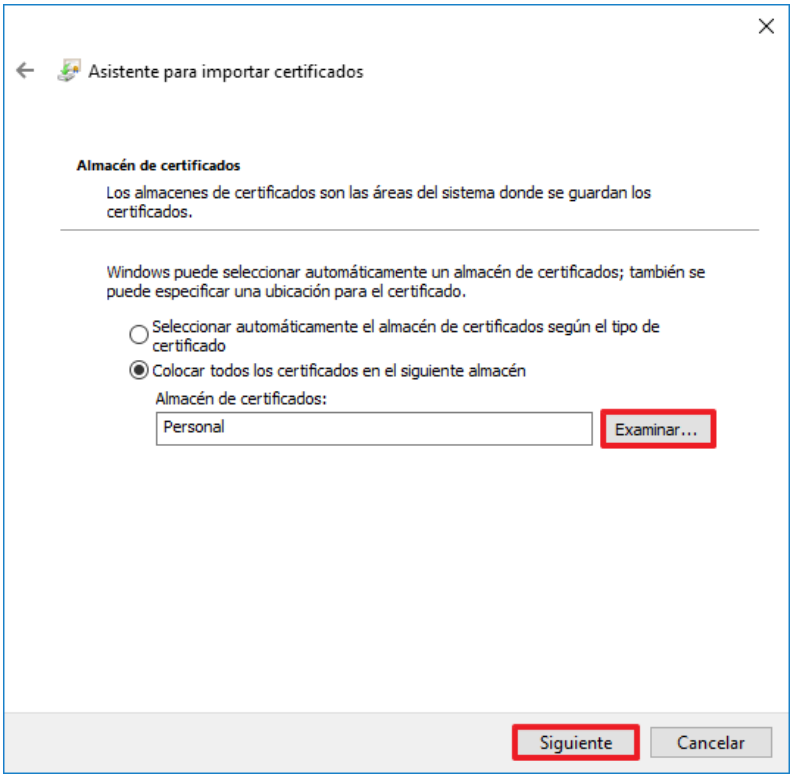
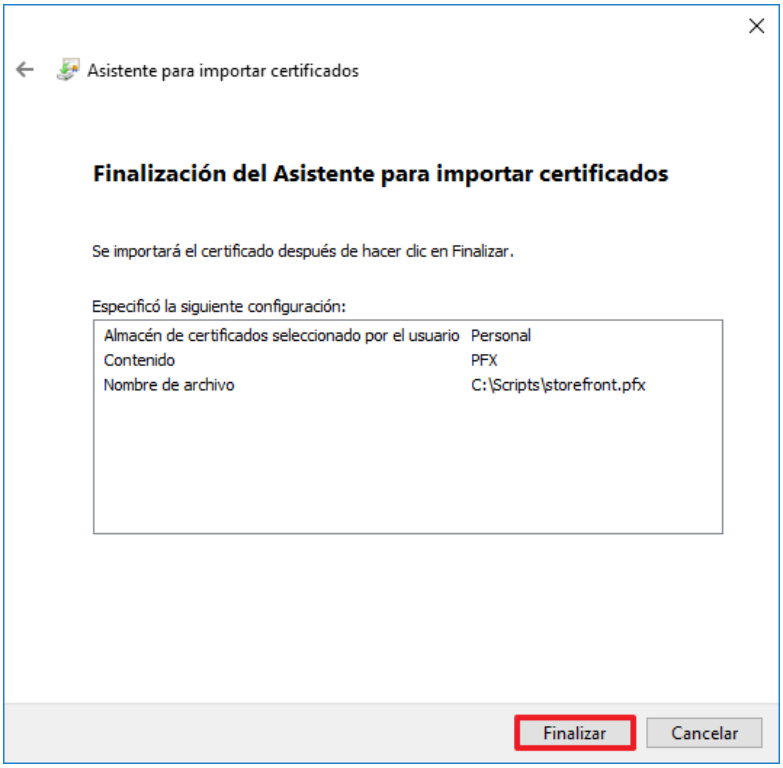
En primer lugar, se procederá a securizar las comunicaciones del servidor con el rol Citrix Storefront.

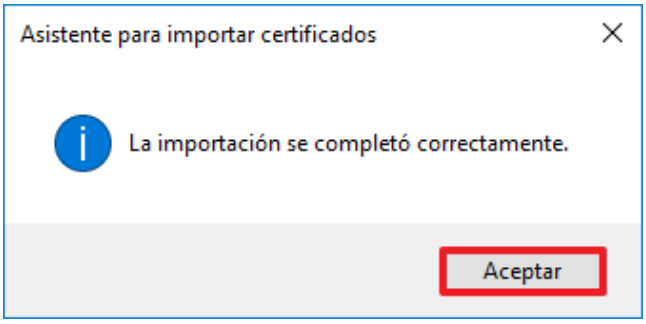
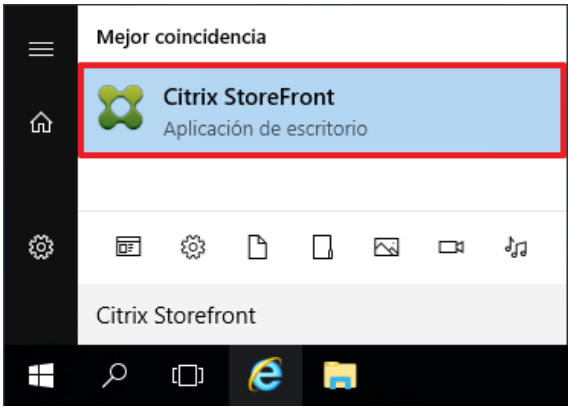
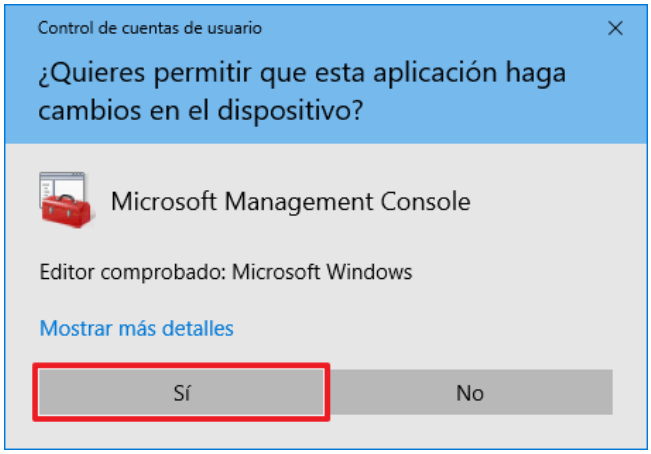
Paso	Descripción
88.	Inicie sesión en un servidor con el rol Citrix Storefront del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
89.	Cree el directorio “Scripts” en la unidad “C:\”.
90.	Será necesario la obtención de un certificado de equipo válido en el dominio ya que los equipos que se conecten al servidor validarán la presencia del certificado y su vigencia. Utilice un certificado cuyo nombre común coincida con la URL base que haya indicado en pasos anteriores. **Nota:** No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.

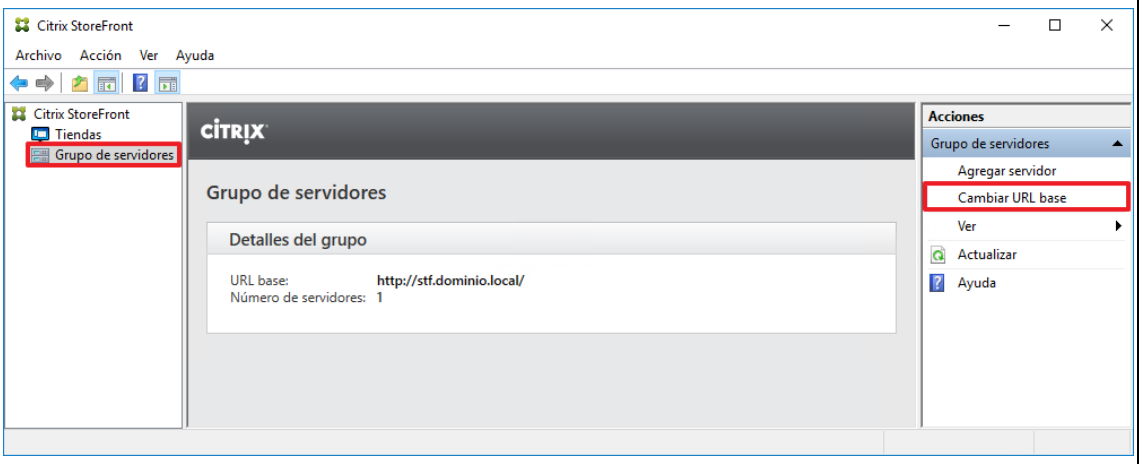
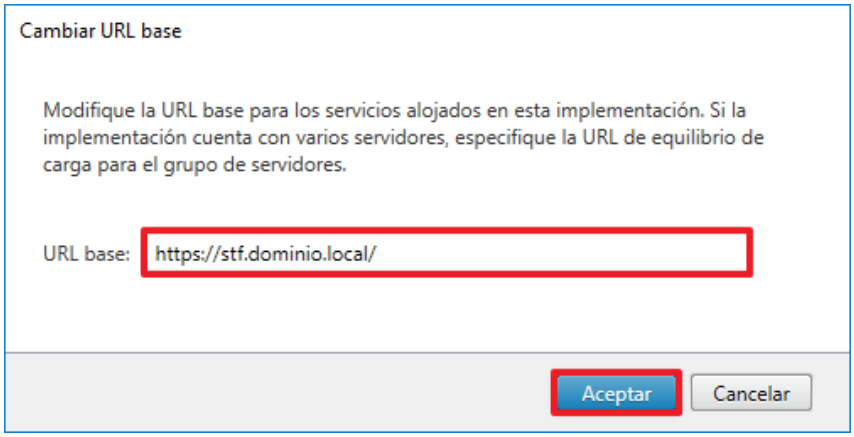
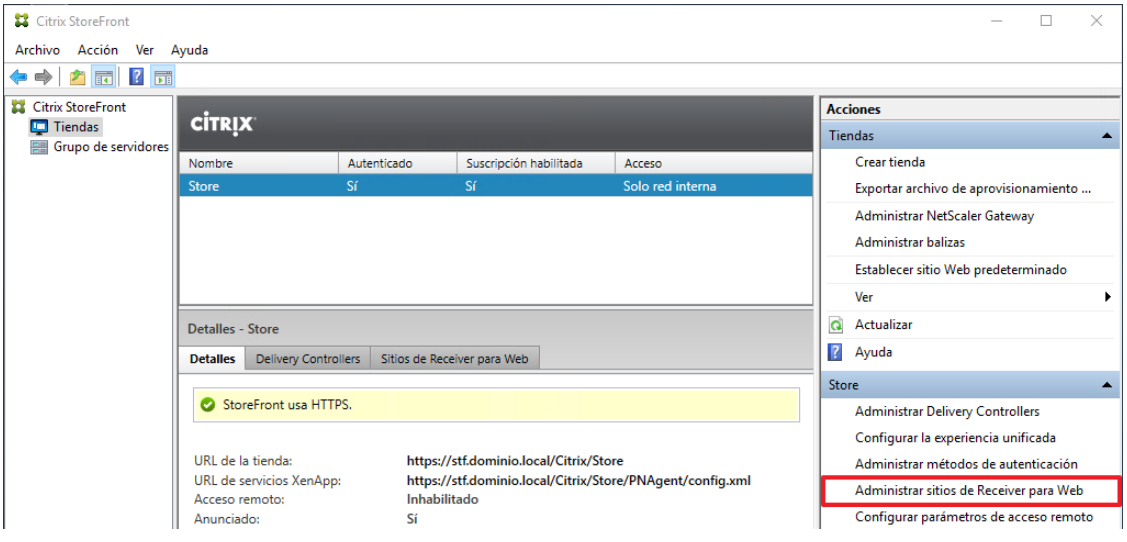
Paso	Descripción
91.	Copie el certificado en la unidad "C:\Scripts" y establezca un nombre de fichero identificativo. En esta guía se utilizará el fichero **"C:\Scripts\storefront.pfx"** a modo de ejemplo, no dude en ajustar el nombre de su archivo en los siguientes pasos. 
92.	Si no lo ha hecho todavía, proceda con los siguientes pasos para realizar la instalación del certificado sobre el almacén **"Personal"** de equipo. **Nota:** Durante la instalación puede ubicar el certificado en el almacén del equipo "Hospedaje de sitios web" pero encontrará advertencias en la consola de Storefront indicando que no hay ningún certificado asociado a este servidor Storefront. Para evitar problemas deberá ubicar el certificado en el almacén Personal del equipo tal y como se muestra en los siguientes pasos. 
93.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **"Instalar PFX"** tal y como se indica en la siguiente figura. 

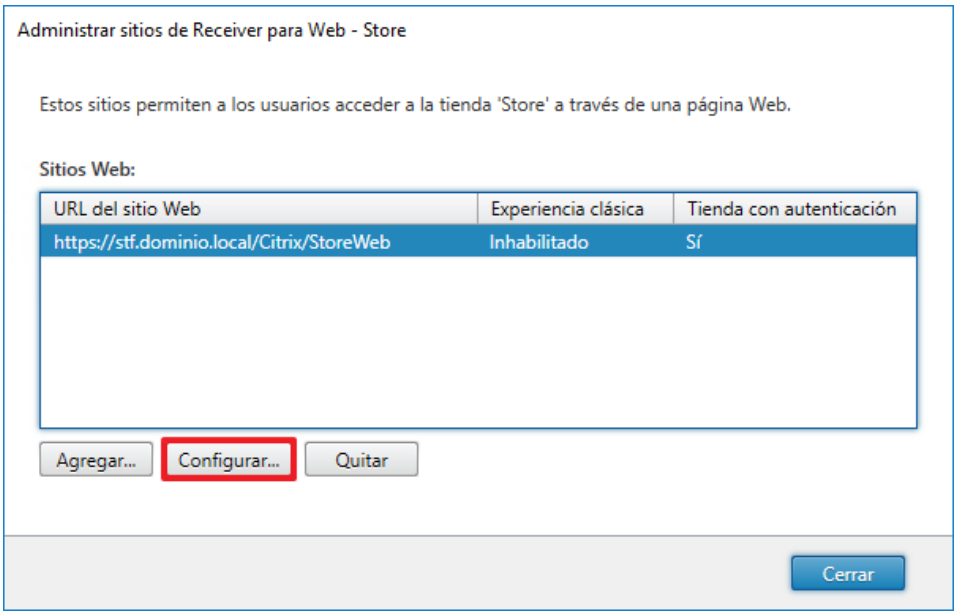
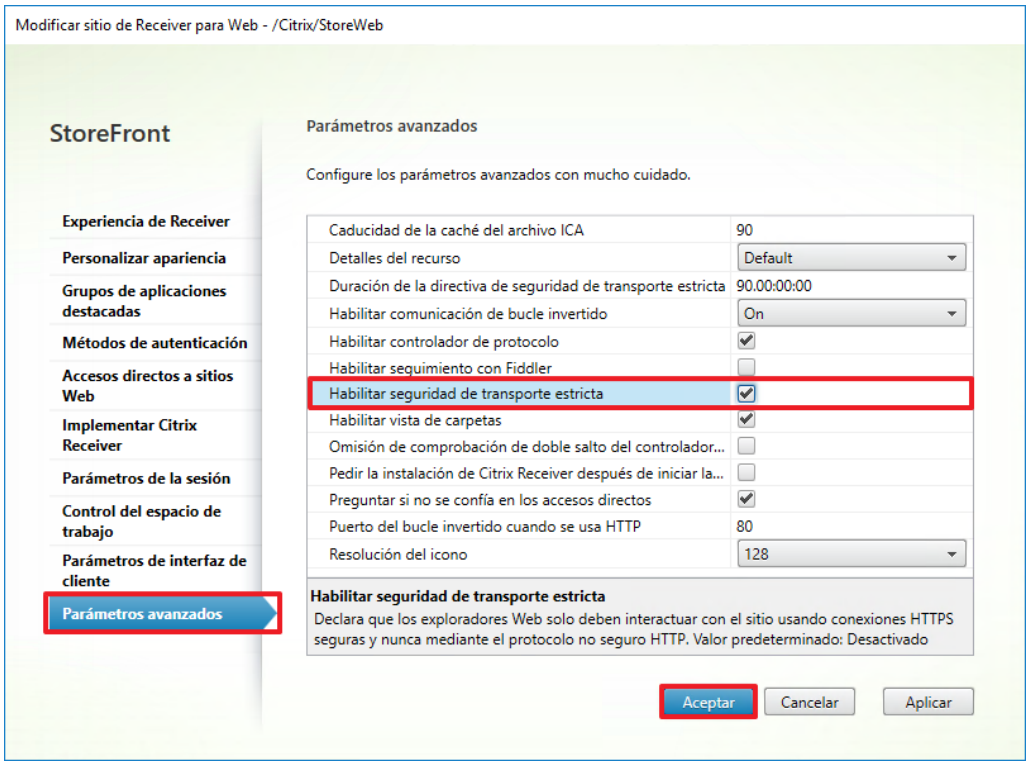
Paso	Descripción
94.	Se iniciará el asistente de importación de certificados. Pulse sobre “Equipo local” y a continuación pulse sobre “Siguiente”.  **Nota:** El sistema solicitará elevación de privilegios.
95.	Especifique el archivo a importar y continúe con el asistente pulsando sobre “Siguiente”. 

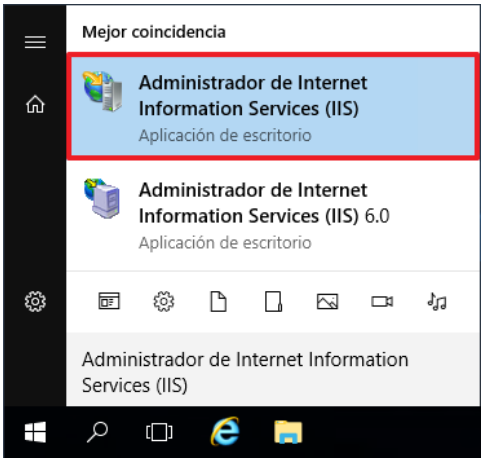
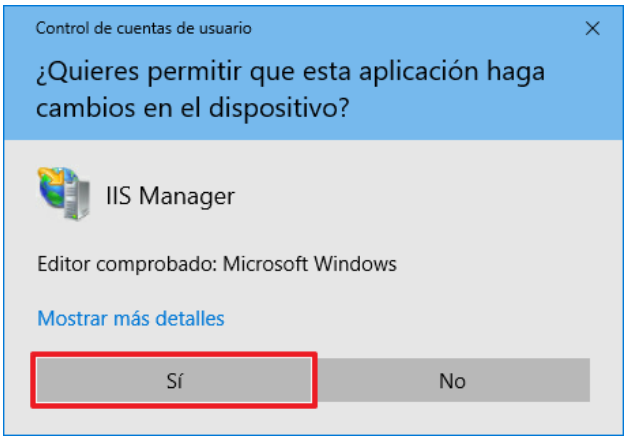
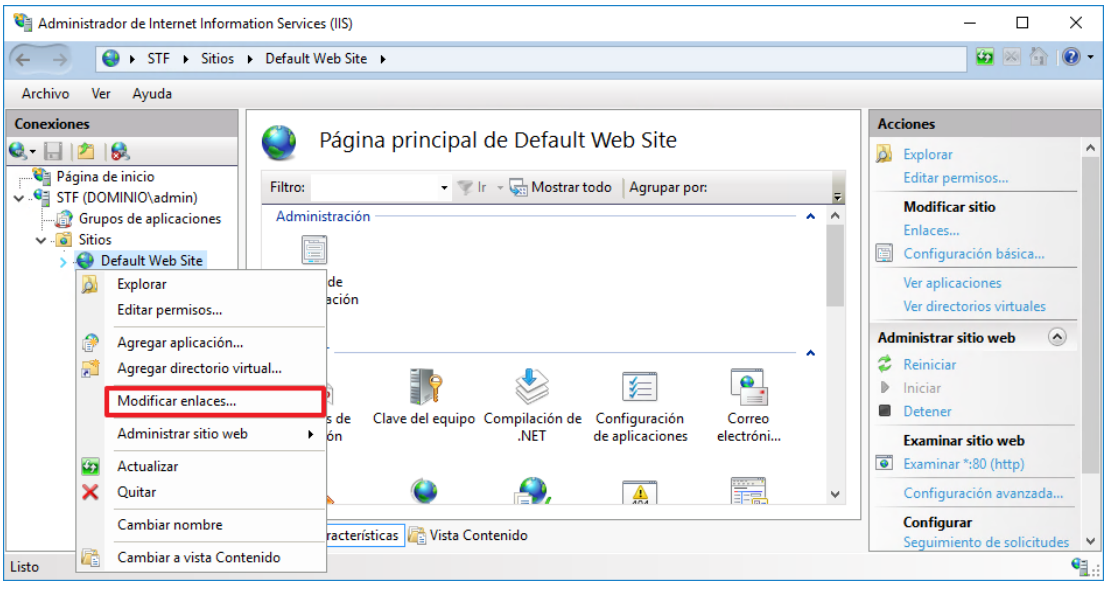
Paso	Descripción
96.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.  **Nota:** Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno. 

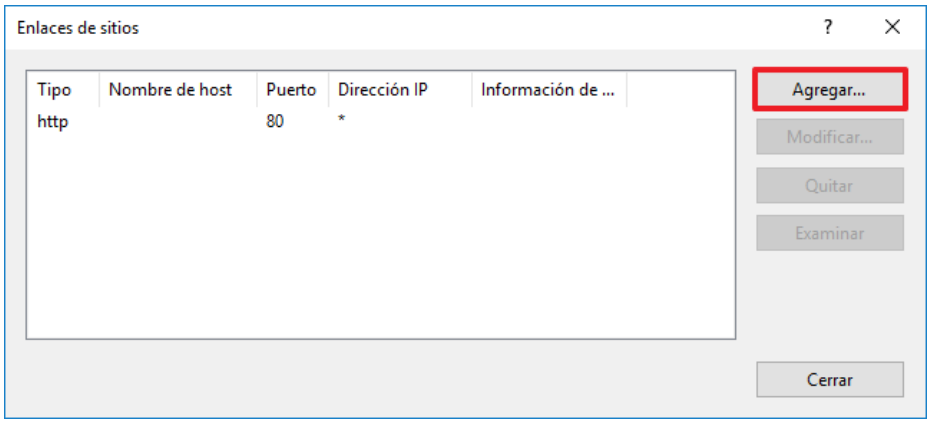
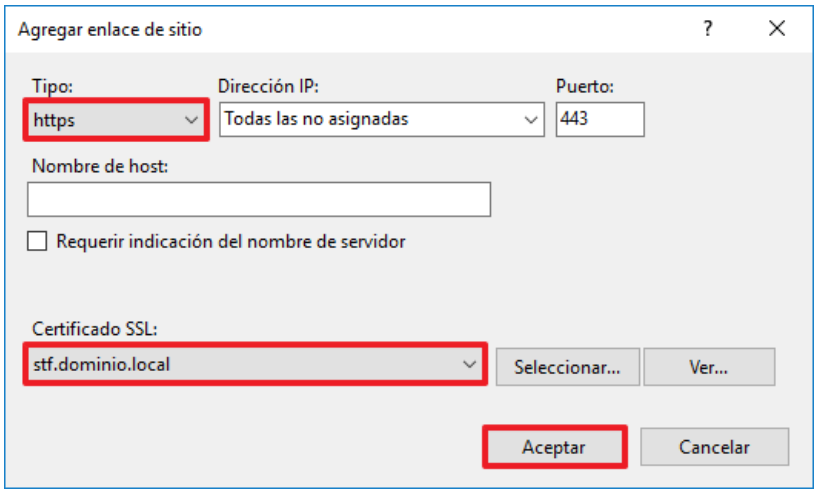
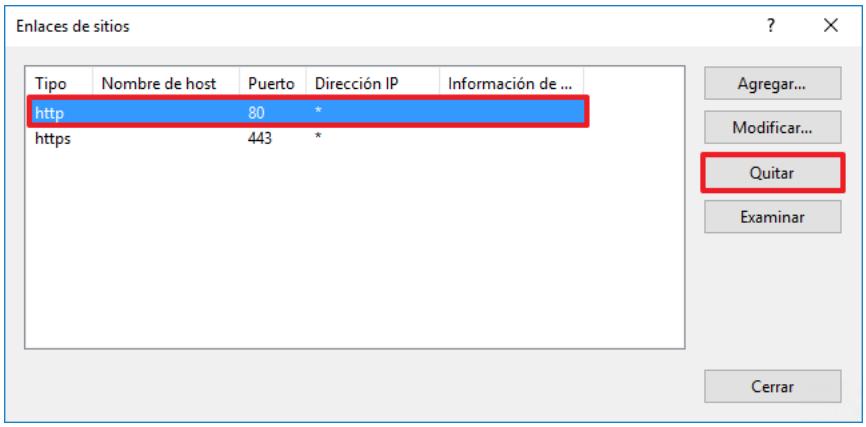
Paso	Descripción
97.	Localice el almacén personal del equipo pulsando sobre “Examinar” tal y como se muestra en la siguiente figura. Una vez establecido, pulse “Siguiente” para continuar. 
98.	El último punto del asistente muestra un resumen, pulse “Finalizar” para completar la importación del certificado sobre el equipo. 

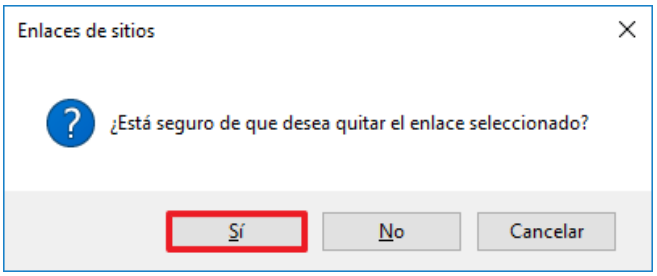
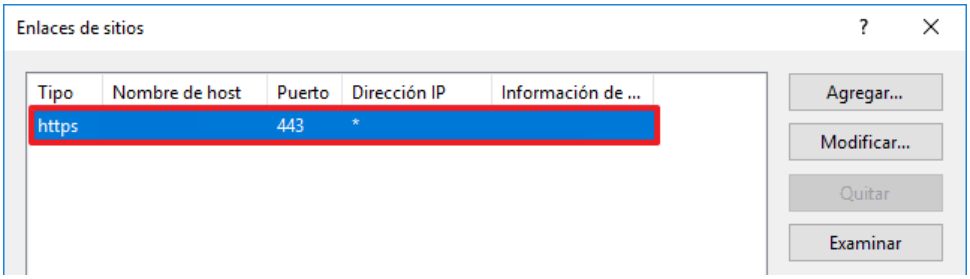
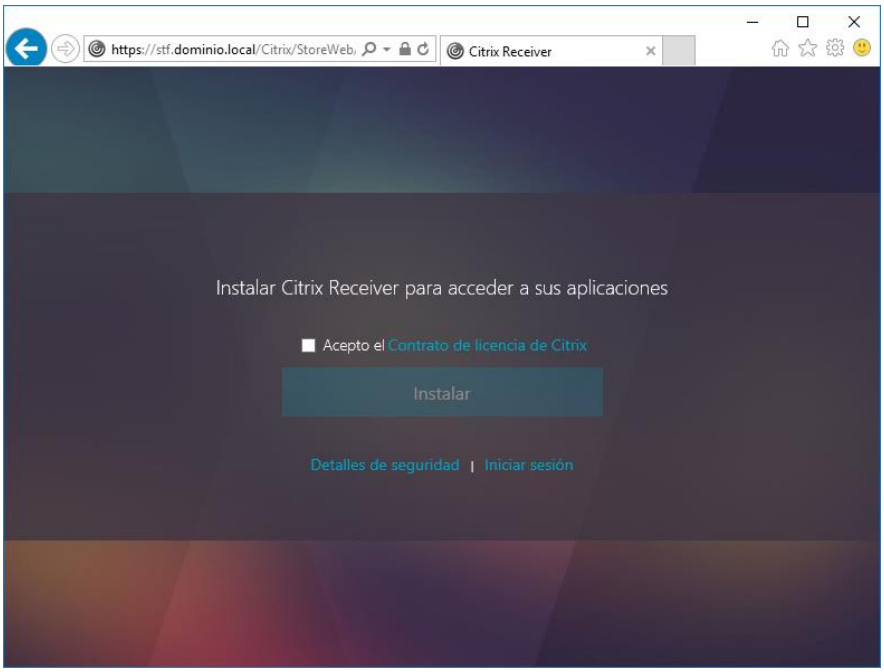
Paso	Descripción
99.	Espere unos segundos a que finalice el proceso, aparecerá un mensaje indicando que la importación se realizó correctamente. 
100.	A continuación, una vez importado el certificado, proceda a configurar la URL base del grupo de servidores. Abra la consola Citrix Storefront. 
101.	El sistema solicitará elevación de privilegios. Pulse “Si” para continuar. 

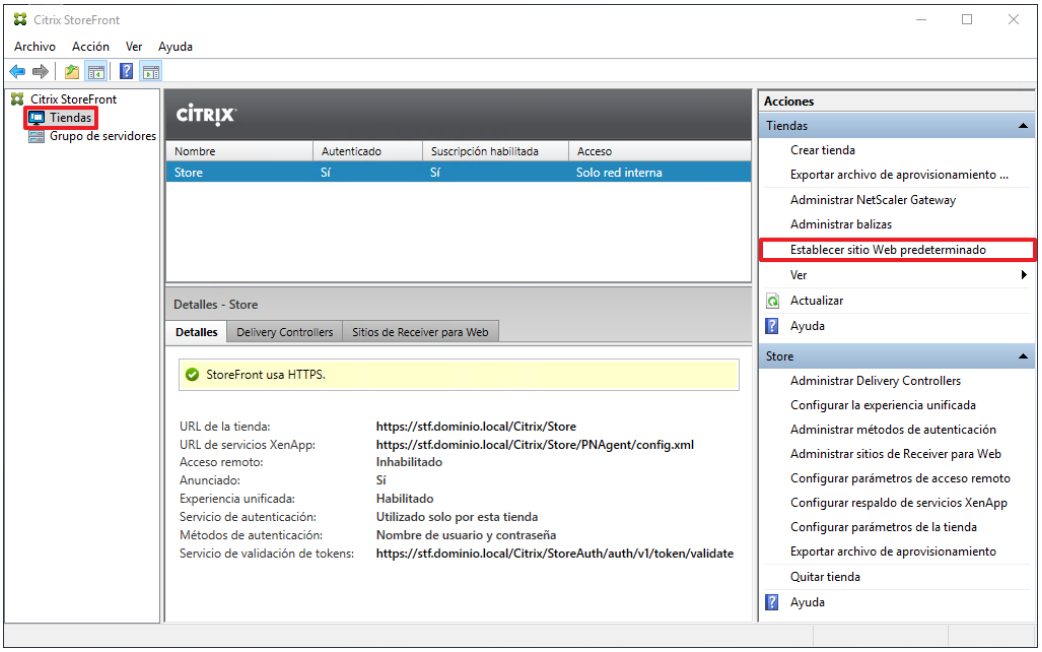
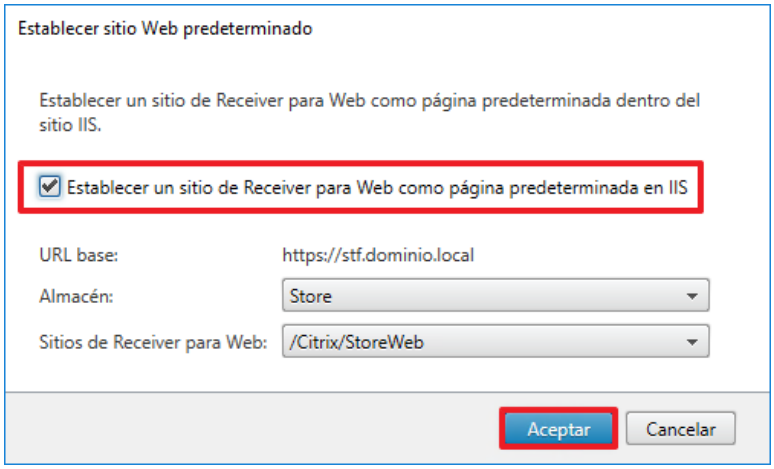
Paso	Descripción
102.	Dentro de la consola, diríjase al nodo de configuración **"Citrix Storefront → Grupo de servidores"** y pulse sobre **"Cambiar URL base"**. 
103.	Sobre la ventana emergente, establezca la URL, indicando el protocolo seguro HTTPS como se muestra en la siguiente figura. Pulse "Aceptar" para guardar los cambios. Acto seguido, verá reflejados los cambios. 
104.	A continuación, deberá configurar los parámetros de "Receiver para Web", acceda al menú **"Tiendas → Store → Administrar sitios de Receiver para Web".** 

Paso	Descripción
105.	La ventana emergente le indicará los sitios creados. Pulse sobre **"Configurar…"**. 
106.	En el menú **"Modificar sitio de Receiver para Web"** diríjase al apartado **"Parámetros avanzados"** y marque la opción "Habilitar seguridad de transporte estricta".  **Nota:** La opción anterior deshabilita la posibilidad de conectarse a los sitios web de Citrix utilizando un protocolo no seguro como HTTP.

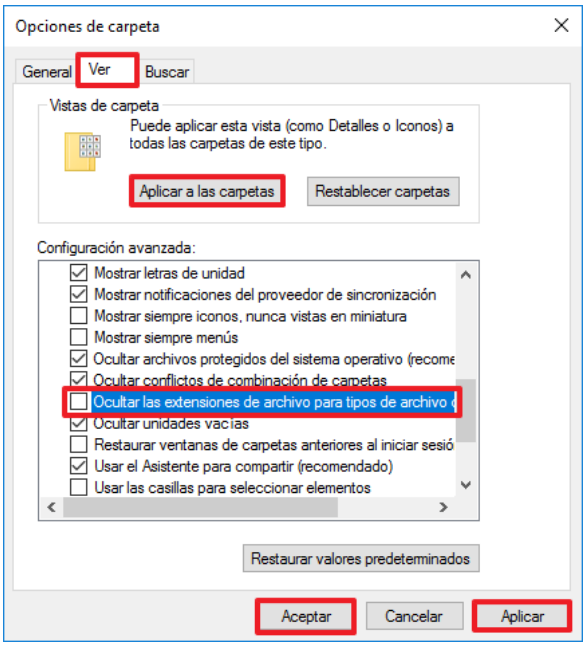
Paso	Descripción
107.	Continúe el proceso abriendo la consola **"Administrador de Internet Information Services (IIS)".** 
108.	El sistema solicitará elevación de privilegios, pulse "Sí" para continuar. 
109.	Abra el nodo de configuración "**<Su servidor>(Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"**. 

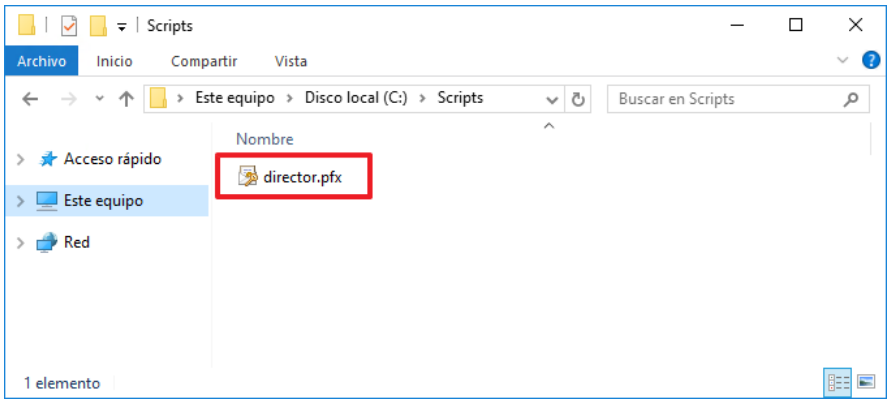
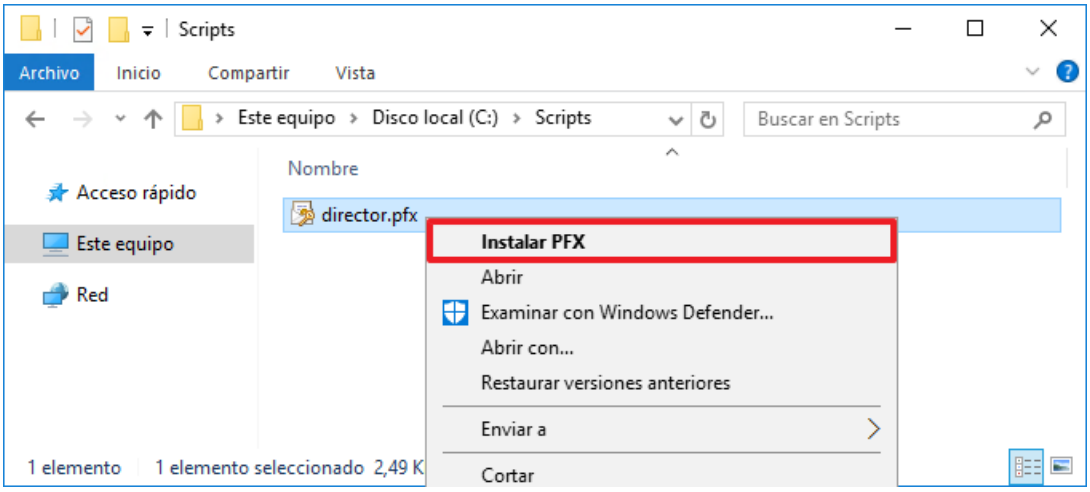
Paso	Descripción
110.	Sobre la ventana "Enlaces de sitios" pulse **"Agregar…"** para añadir un enlace nuevo. Por defecto, encontrará creado un enlace al puerto 80 que deberá eliminar más adelante para evitar conexiones no seguras al entorno. 
111.	Modifique en el formulario los parámetros necesarios y establezca su certificado SSL a utilizar, instalado en pasos anteriores. Pulse **"Aceptar"** para guardar los cambios". 
112.	Con ambos enlaces creados, seleccione el enlace de Tipo "http" y acto seguido pulse sobre **"Quitar"**. 

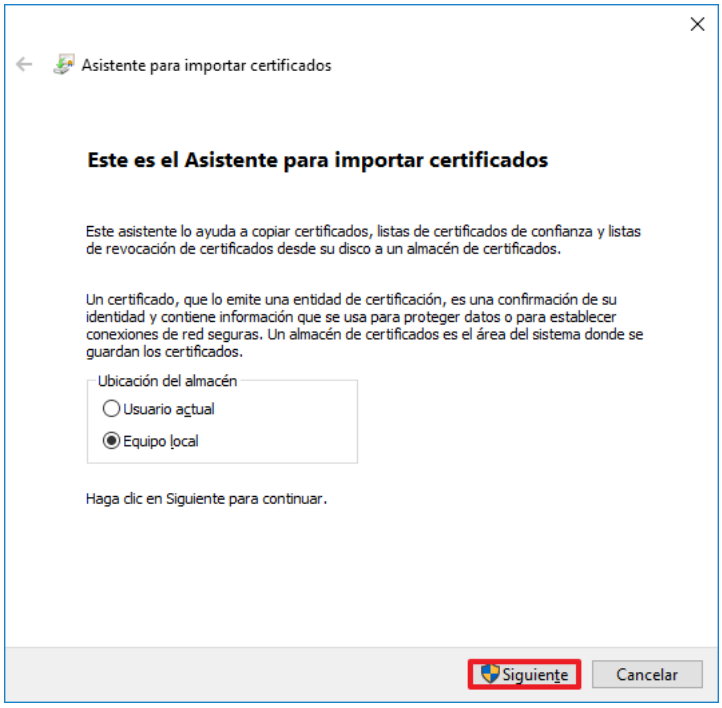
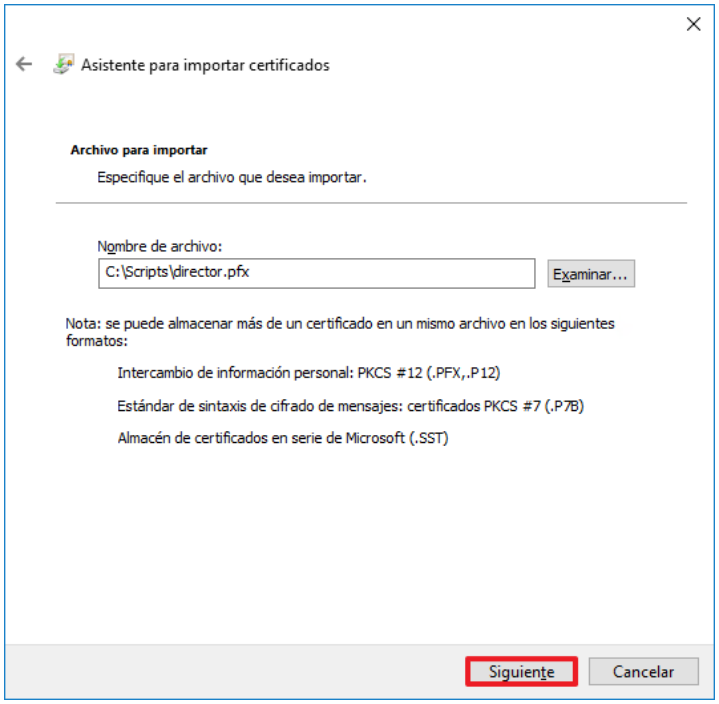
Paso	Descripción
113.	Sobre la ventana emergente, pulse “Sí” para confirmar la eliminación del enlace seleccionado. 
114.	Al terminar, verifique que únicamente está configurado el enlace de tipo “https” recién creado con su certificado SSL. 
115.	Puede verificar que la configuración es correcta abriendo un navegador y accediendo a la URL base de su entorno, en este caso, a modo de ejemplo se verifica el acceso a la dirección https://stf.dominio.local/Citrix/Storeweb.  **Nota:** Para realizar la prueba anterior, puede ser necesario que rebaje la seguridad de Internet Explorer habilitando JavaScript y las cookies en el navegador. No es necesario que realice ninguna acción sobre el propio servidor, únicamente verifique que tiene conectividad con la URL Base que ha definido y que el certificado utilizado es de confianza.

Paso	Descripción
116.	Dependiendo de su organización, y de las opciones seleccionadas durante la instalación del rol Citrix Storefront, es posible que no haya configurado su sitio web de Storefront como predeterminado en su servidor IIS. Si desea establecer su sitio de Receiver para web como página predeterminada de su servidor IIS acceda a **"Tiendas → Establecer sitio Web predeterminado"** dentro de la consola de "Citrix Storefront". 
117.	Marque la opción "Establecer un sitio de Receiver para Web como página predeterminada en IIS" y seleccione las opciones que se ajusten a las necesidades de su organización. Pulse "Aceptar" para guardar la configuración. 
118.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta "C:\Scripts" del servidor.

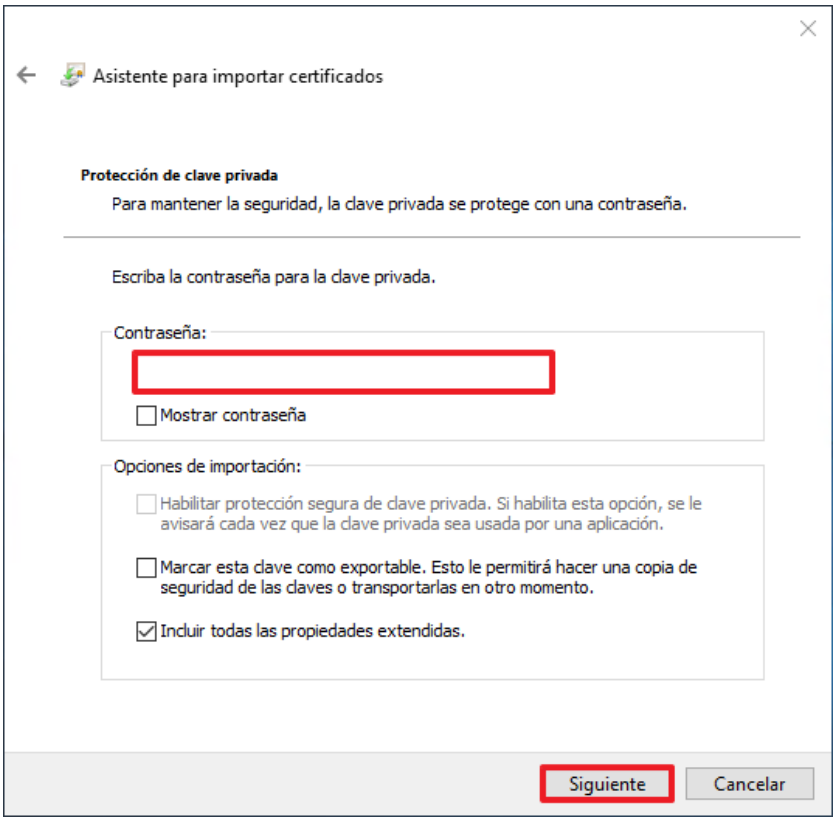
En este punto el servidor Citrix Storefront se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura. Una vez configurado el servidor con el rol Citrix Storefront deberá continuar con las configuraciones sobre el servidor con el rol Citrix Director.

Paso	Descripción
119.	Inicie sesión en un servidor con el rol Citrix Director del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
120.	Cree el directorio “Scripts” en la unidad “C:\”.
121.	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. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

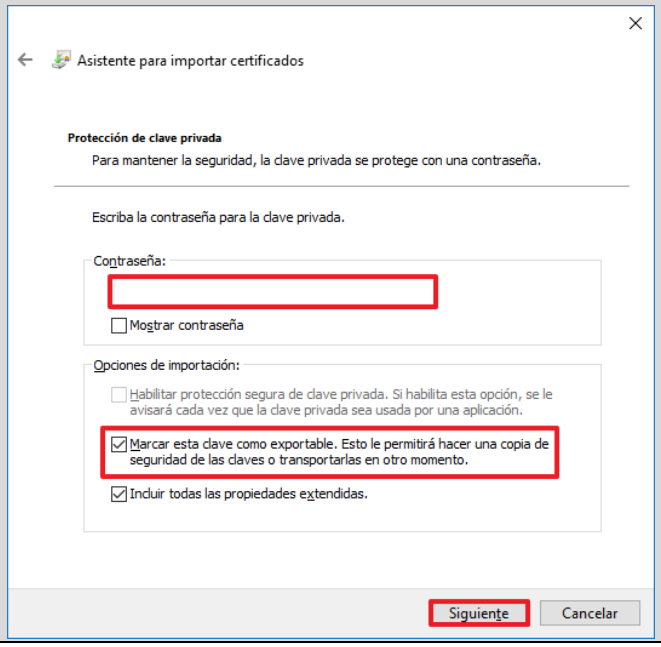
Paso	Descripción
122.	Para continuar, debe realizar la solicitud de un certificado válido en el dominio, cuyo Nombre común "CN" coincida con el FQDN del equipo sobre el que está implementando el rol Citrix Director. No debe utilizar un certificado de tipo "wildcard" ya que de utilizarlo encontrará problemas en los siguientes pasos de configuración. **Nota:** No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.
123.	Copie el certificado en la unidad "C:\Scripts" y establezca un nombre de fichero identificativo. En esta guía se utilizará el fichero **"C:\Scripts\director.pfx"** a modo de ejemplo, no dude en ajustar el nombre de su archivo en los siguientes pasos. 
124.	Si no lo ha hecho todavía, proceda con los siguientes pasos para realizar la instalación del certificado sobre el almacén **"Personal"** de equipo.
125.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **"Instalar PFX"** tal y como se indica en la siguiente figura. 

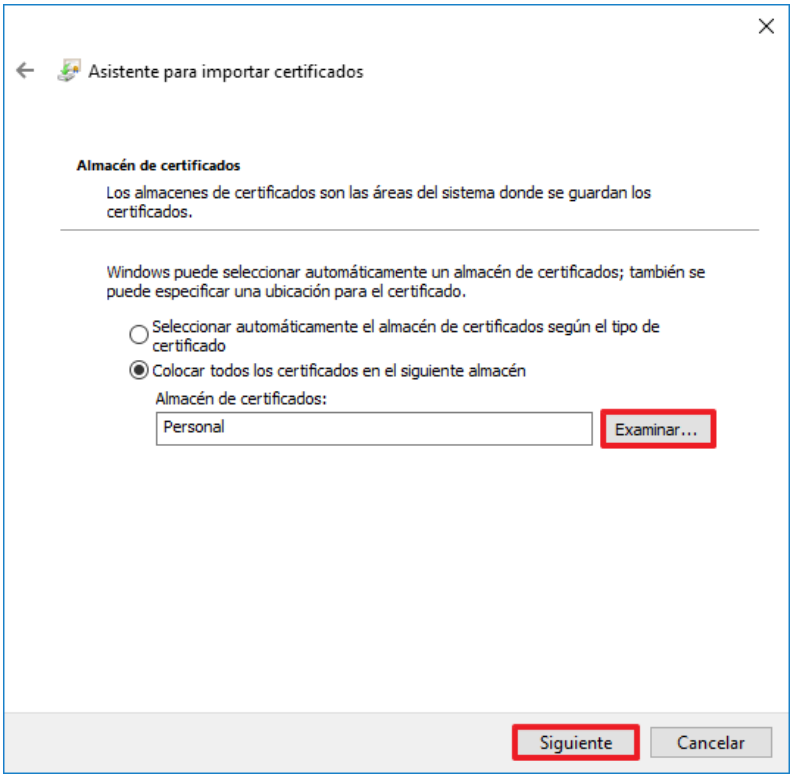
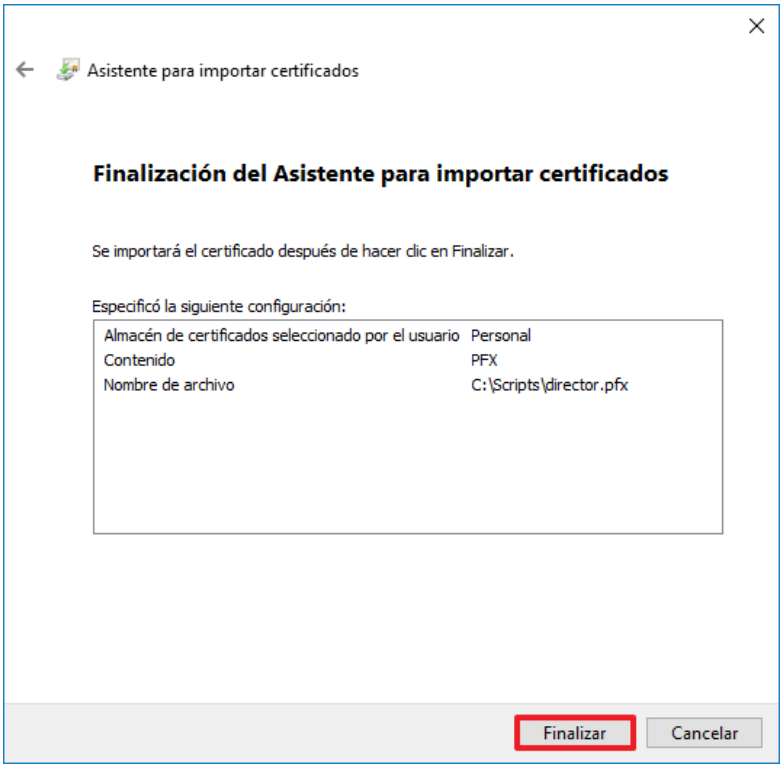
Paso	Descripción
126.	Se iniciará el asistente de importación de certificados. Pulse sobre “Equipo local” y a continuación pulse sobre “Siguiente”.  **Nota:** El sistema solicitará elevación de privilegios.
127.	Especifique el archivo a importar y continúe con el asistente pulsando sobre “Siguiente”. 

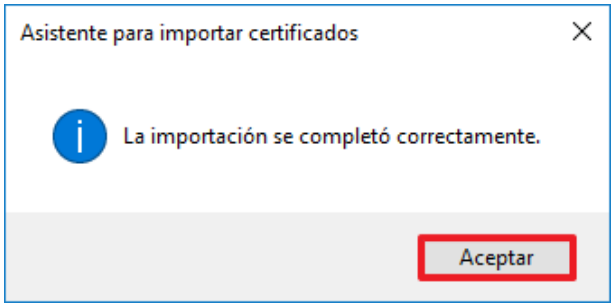
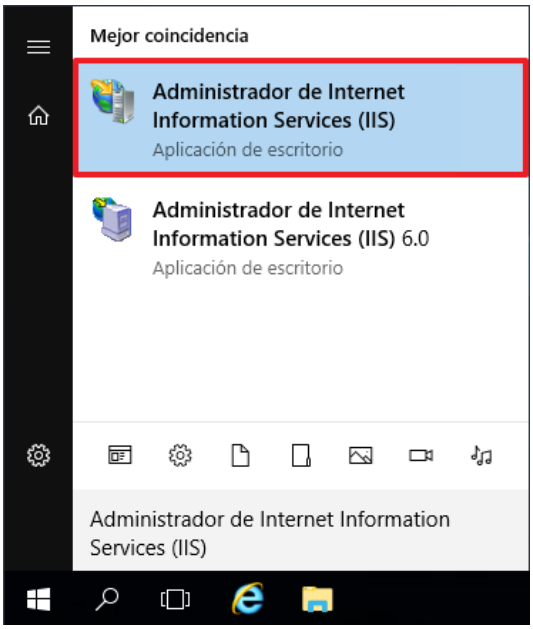
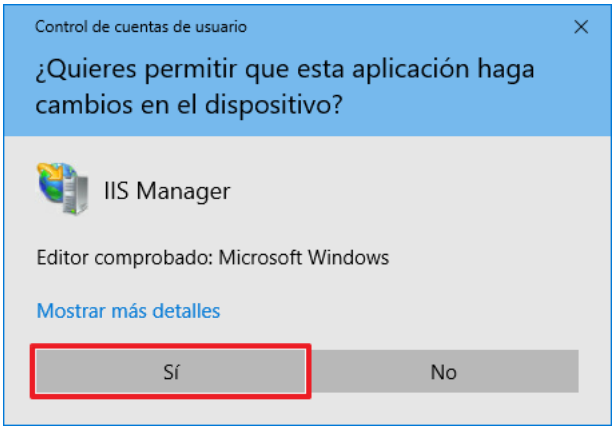
Paso	Descripción
128.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.

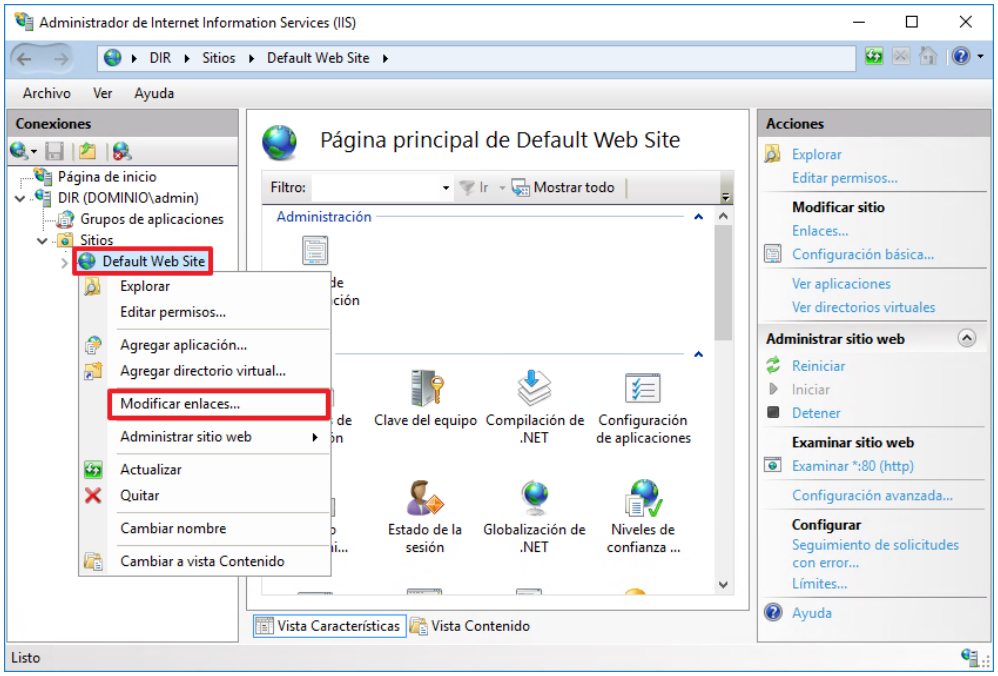
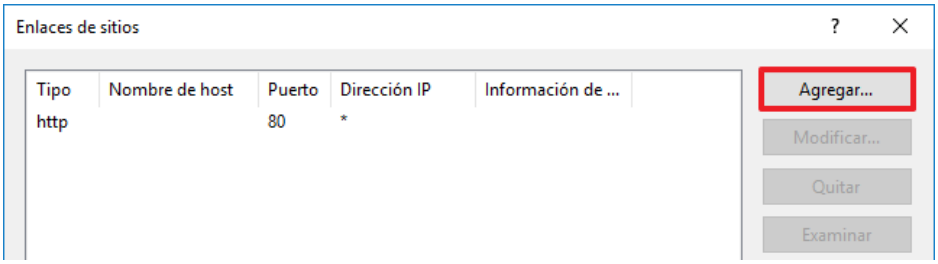
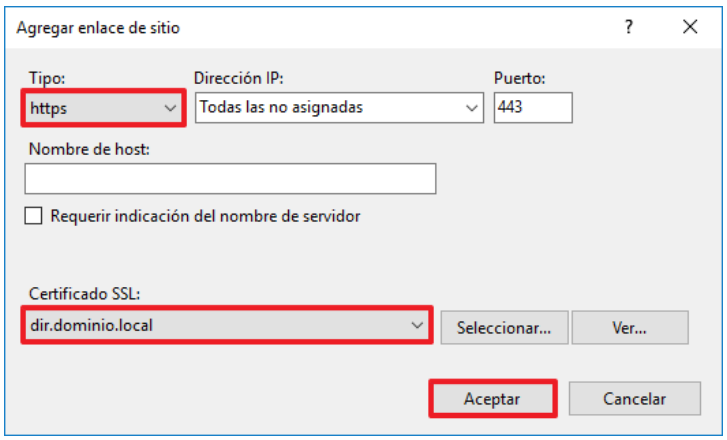


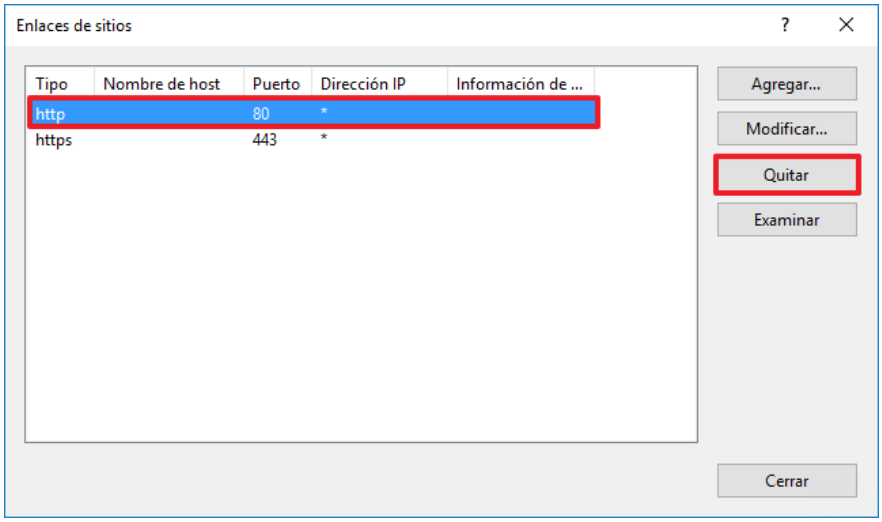
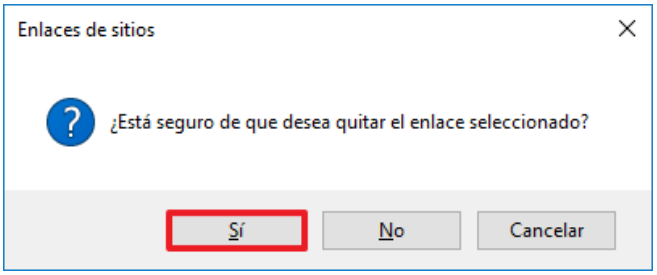
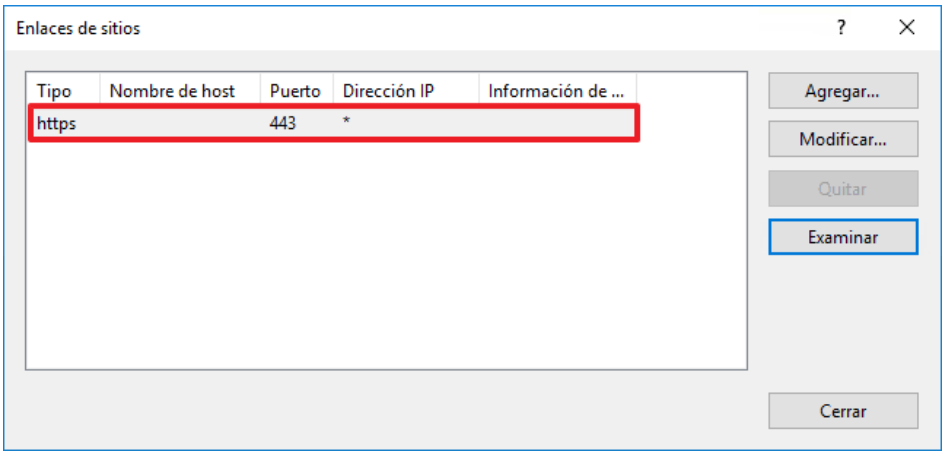
Nota: Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno.

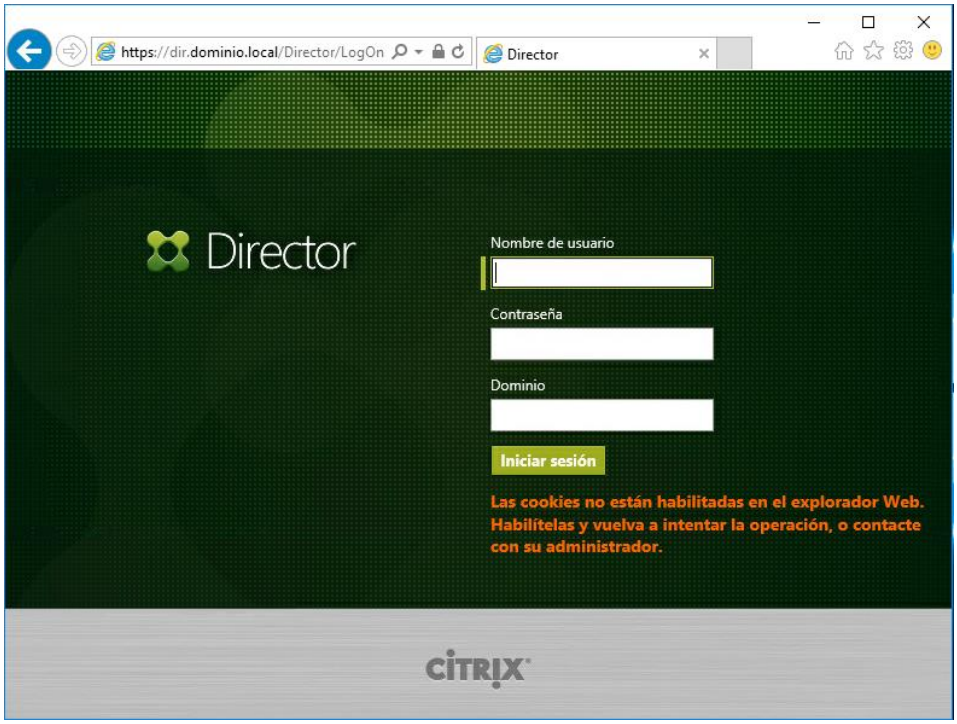


Paso	Descripción
129.	Localice el almacén “Personal” del equipo pulsando sobre “Examinar” tal y como se muestra en la siguiente figura. Una vez establecido, pulse “Siguiente” para continuar. 
130.	El último punto del asistente muestra un resumen, pulse “Finalizar” para completar la importación del certificado sobre el equipo. 

Paso	Descripción
131.	Espere unos segundos a que finalice el proceso, aparecerá un mensaje indicando que la importación se realizó correctamente. 
132.	Acto seguido, verá reflejados los cambios, continúe el proceso abriendo la consola **"Administrador de Internet Information Services (IIS)"**. 
133.	El sistema solicitará elevación de privilegios, pulse "Sí" para continuar. 

Paso	Descripción
134.	Abra el nodo de configuración **"<Su servidor> (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"**. 
135.	Sobre la ventana "Enlaces de sitios" pulse **"Agregar…"** para añadir un enlace nuevo. Por defecto, encontrará creado un enlace al puerto 80 que deberá eliminar más adelante para evitar conexiones no seguras al entorno. 
136.	Modifique en el formulario los parámetros necesarios y establezca su certificado SSL a utilizar, instalado en pasos anteriores. Pulse **"Aceptar"** para guardar los cambios". 

Paso	Descripción
137.	Con ambos enlaces creados, seleccione el enlace de Tipo “http” y acto seguido pulse sobre **“Quitar”**. 
138.	Sobre la ventana emergente, pulse “Si” para confirmar la eliminación del enlace seleccionado. 
139.	Al terminar, verifique que únicamente está configurado el enlace de Tipo “https” recién creado con su certificado SSL. 

Paso	Descripción
140.	Puede verificar que la configuración es correcta abriendo un navegador y accediendo a la URL base de su entorno, en este caso, a modo de ejemplo se verifica el acceso a la dirección https://dir.dominio.local/director.  **Nota:** Es posible que no tenga la herramienta "JavaScript" instalada en el equipo desde el que está accediendo al portal web. Será necesario realizar dicho proceso para el correcto funcionamiento del explorador. 
141.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta "C:\Scripts" del servidor.

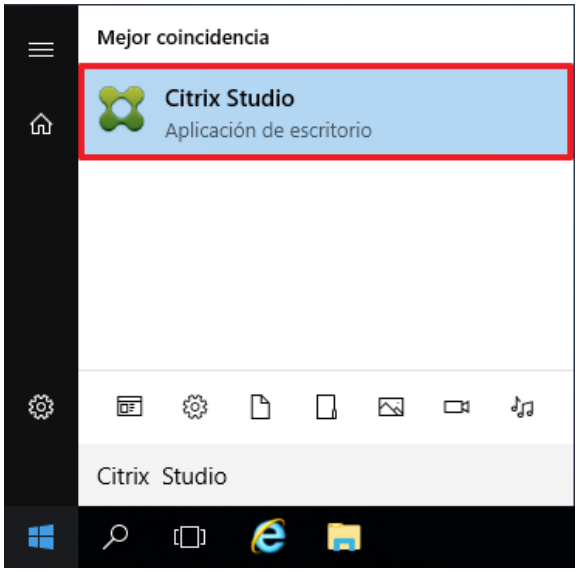
En este punto el servidor con el rol de Citrix Director se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura.

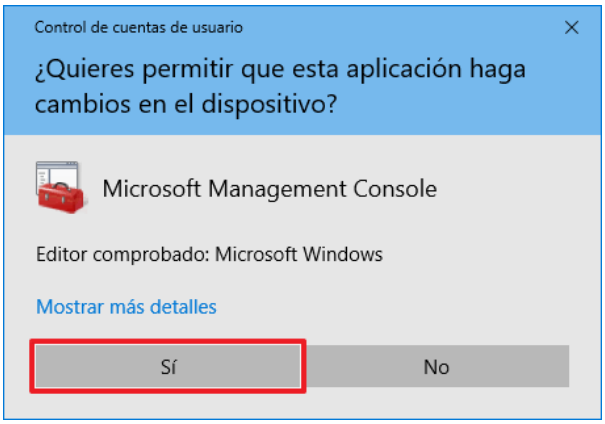
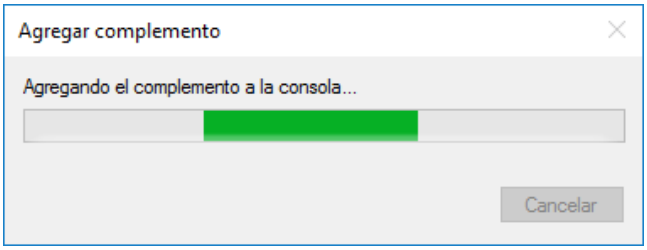
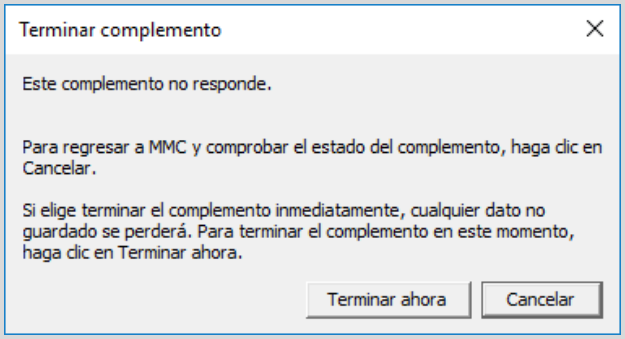
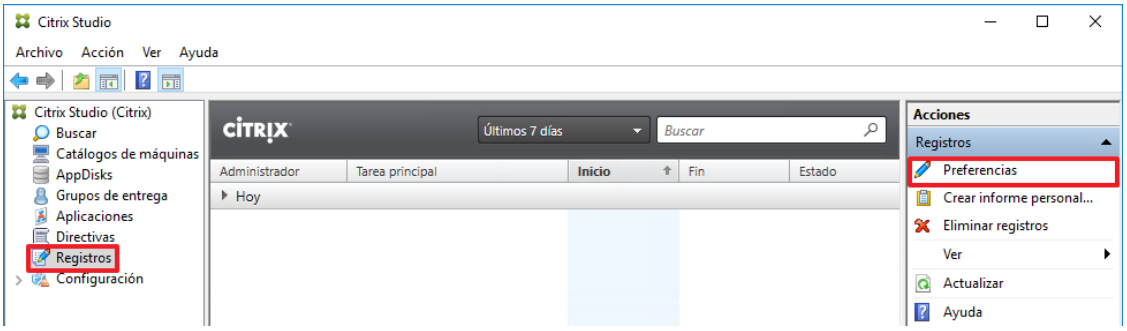
4. AUDITORÍA

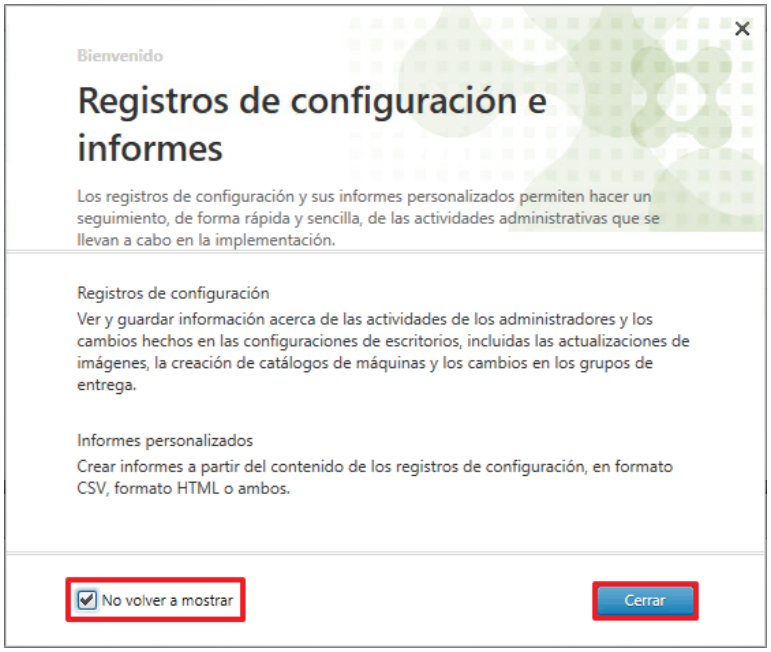
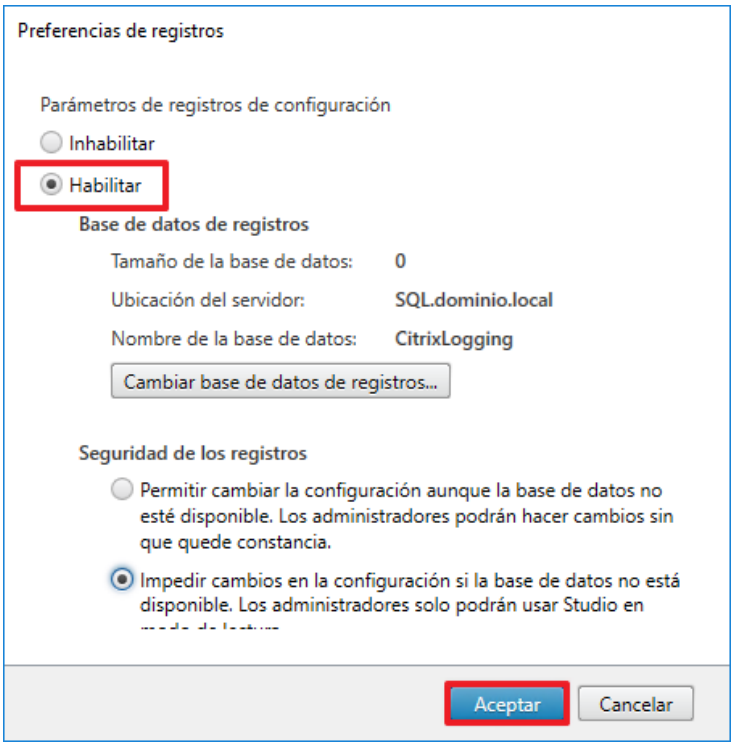
Con la aplicación del ENS para la categoría media sobre Citrix Virtual Apps and Desktops quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

Para la categoría media de seguridad del ENS deberá definir como "Habilitados" los registros sobre las modificaciones que se hagan en la infraestructura de Citrix Virtual Apps and Desktops.

Para ello, será necesario comprobar sobre el rol Citrix Controller que dicha configuración se encuentre configurada correctamente.

Paso	Descripción
142.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
143.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio. 

Paso	Descripción
144.	El sistema solicitará elevación de privilegios, pulse “Sí” para continuar. 
145.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse “Cancelar” para continuar. 
146.	A continuación, diríjase al nodo de configuración **“Citrix Studio → Registros → Acciones”** y pulse sobre “Preferencias”. 

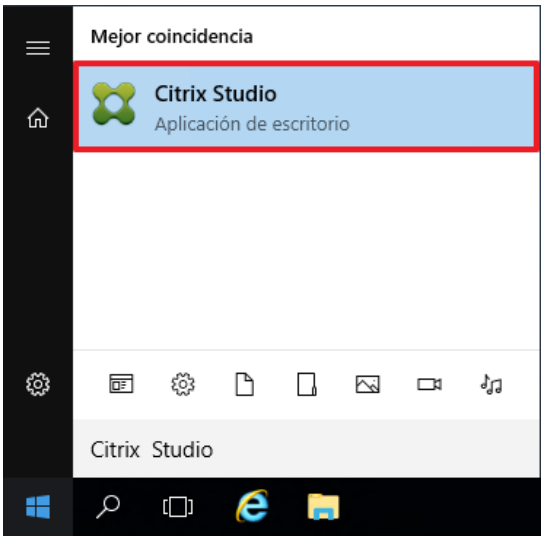
Paso	Descripción
147.	Al navegar por primera vez por los diferentes nodos de la herramienta aparecerán distintos mensajes de bienvenida, marque la casilla “No volver a mostrar” y pulse “Cerrar” en cada uno de ellos. 
148.	Sobre la ventana emergente “Preferencias de registros” compruebe que la opción **“Habilitar”** se encuentra seleccionada como se indica en la siguiente figura. Pulse “Aceptar” para continuar. 

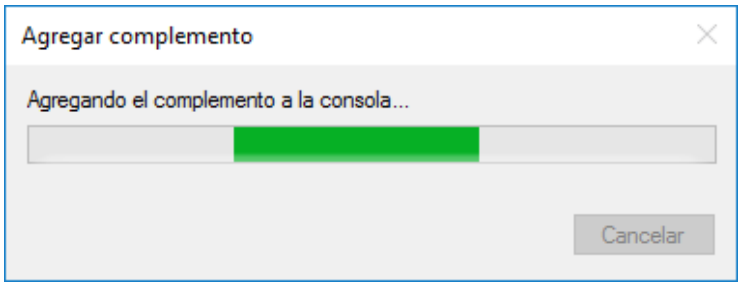
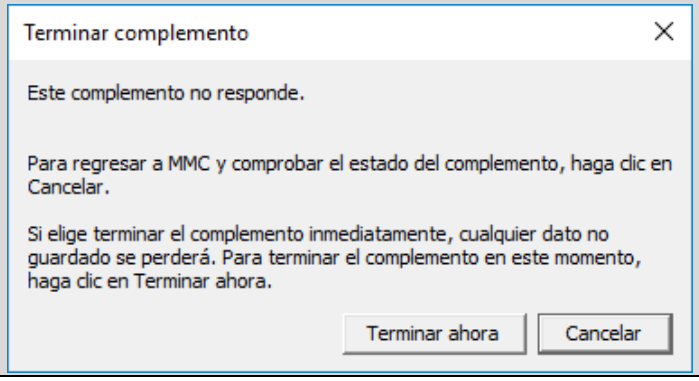
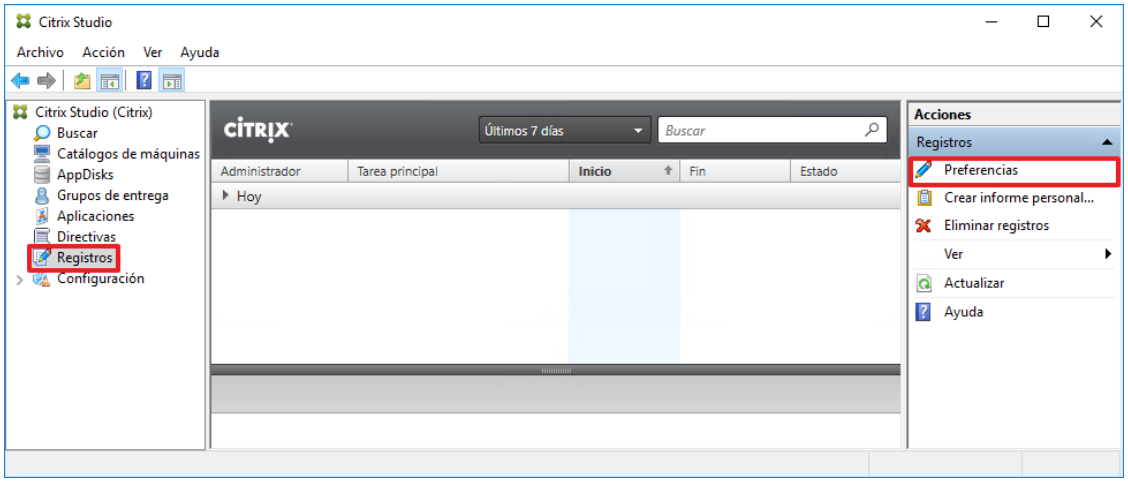
5. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

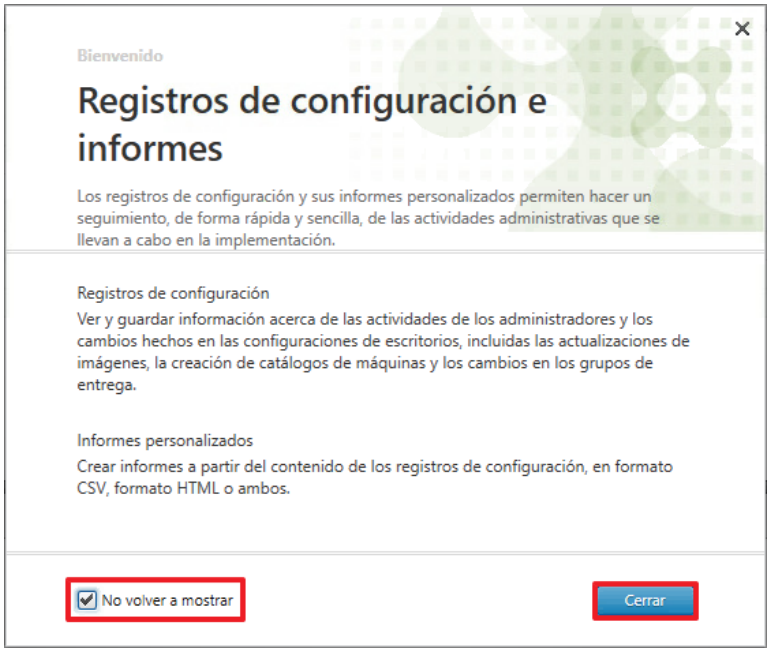
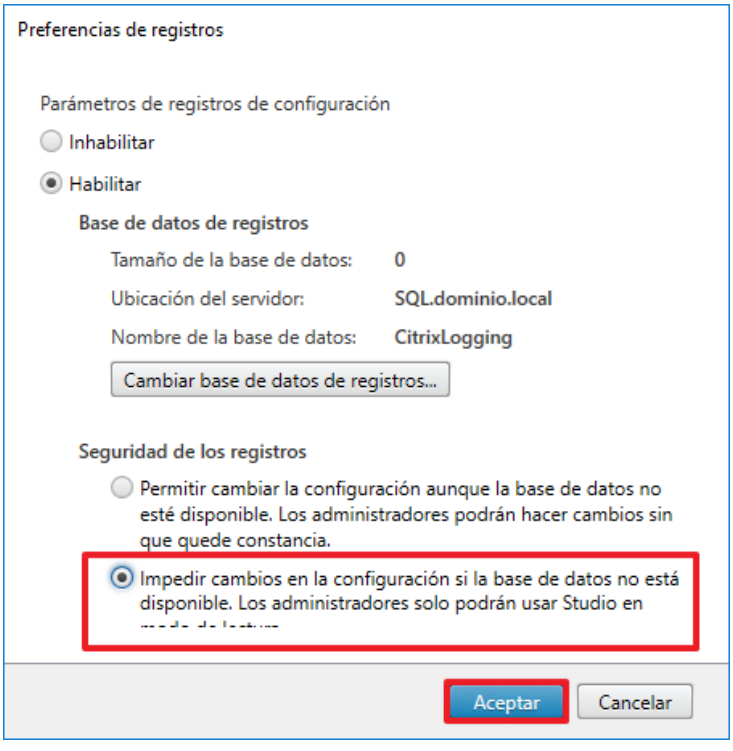
Aplicable en las categorías media y alta de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones que se realizan sobre los servidores de la infraestructura de Citrix Virtual Apps and Desktops.

Para este fin, se deberá impedir cualquier modificación de las configuraciones en caso de que la base de datos en la que se recogen los registros de dichas modificaciones no esté disponible.

Esta configuración se deberá llevar a cabo en la herramienta Citrix Studio instalada en el servidor con el rol Citrix Controller de su infraestructura.

Paso	Descripción
149.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
150.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios

Paso	Descripción
151.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
152.	A continuación, diríjase al nodo de configuración **"Citrix Studio → Registros → Acciones"** y pulse sobre "Preferencias". 

Paso	Descripción
153.	Al navegar por primera vez por los diferentes nodos de la herramienta aparecerán distintos mensajes de bienvenida, marque la casilla “No volver a mostrar” y pulse “Cerrar” en cada uno de ellos. 
154.	Sobre la ventana emergente “Preferencias de registros” marque la opción **“Impedir cambios en la configuración si la base de datos no está disponible. Los administradores solo podrán utilizar Studio en modo de lectura”** como se indica en la siguiente figura. Pulse “Aceptar” para continuar. 

6. GESTIÓN DE DERECHOS DE ACCESO

Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda realizar tareas que no son requeridas para las funciones que desempeña.

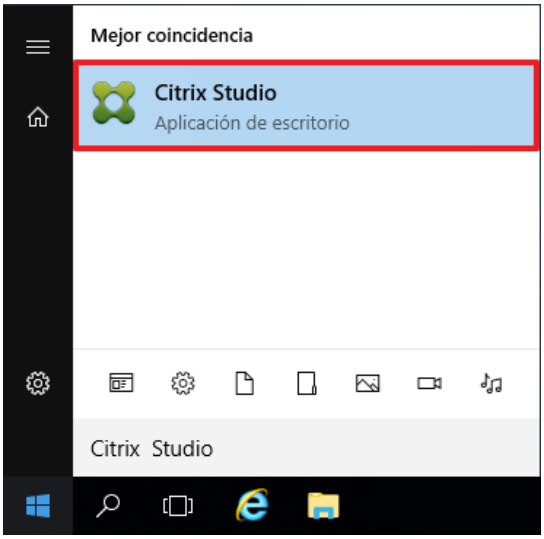
Para tal fin y de acuerdo con el Esquema Nacional de Seguridad se deberán definir, mediante grupos de seguridad, los usuarios que según su organización deban administrar la infraestructura y eliminar aquellos administradores genéricos que puedan existir.

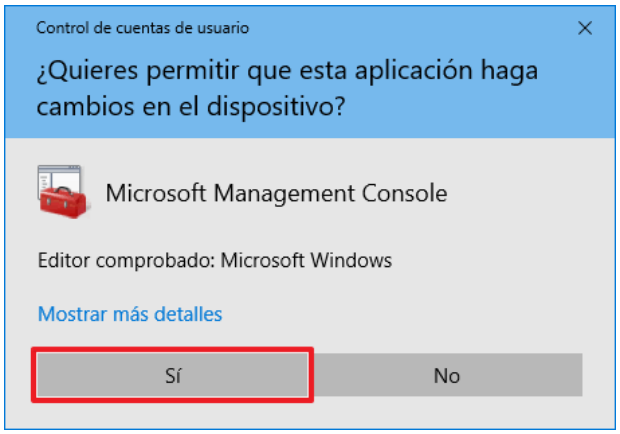
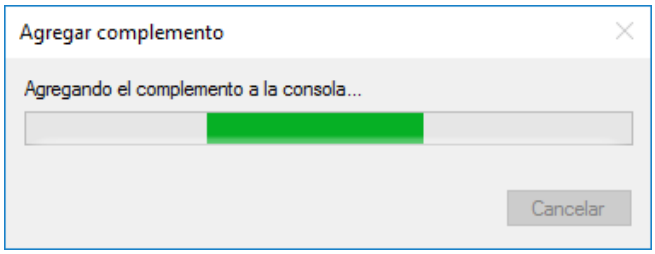
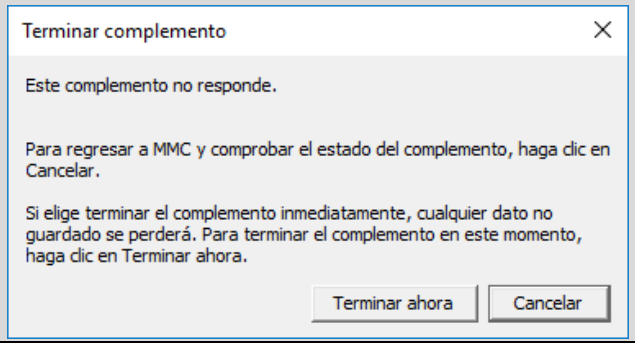
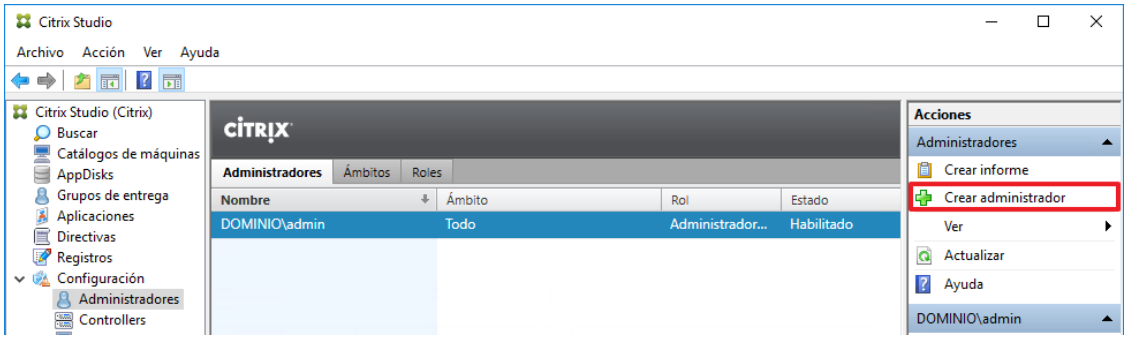
Esta configuración será de aplicación en los siguientes servidores de su infraestructura Citrix Virtual Apps and Desktops:

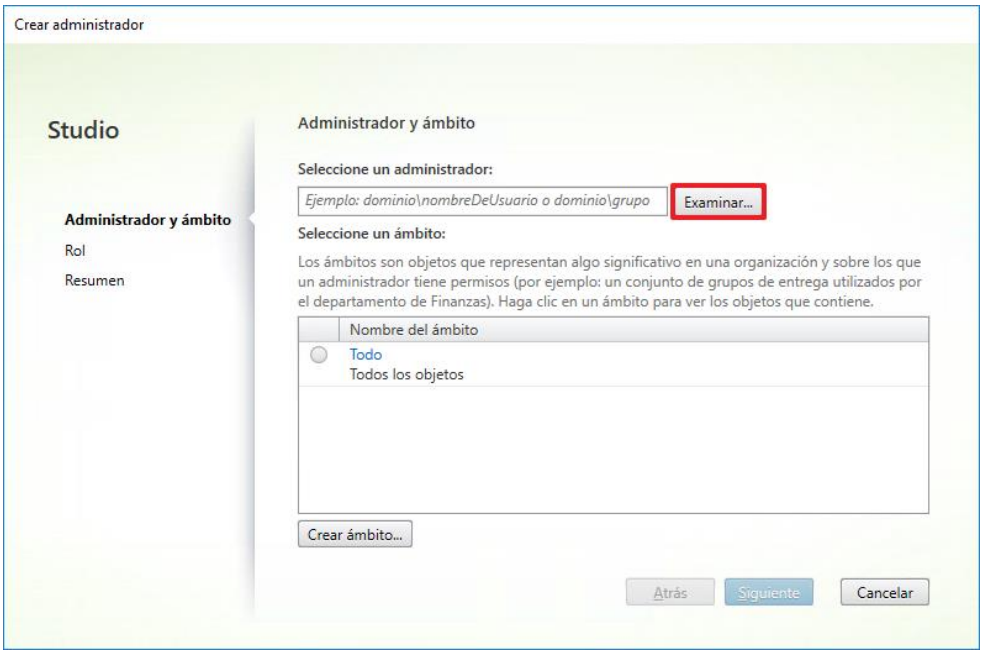
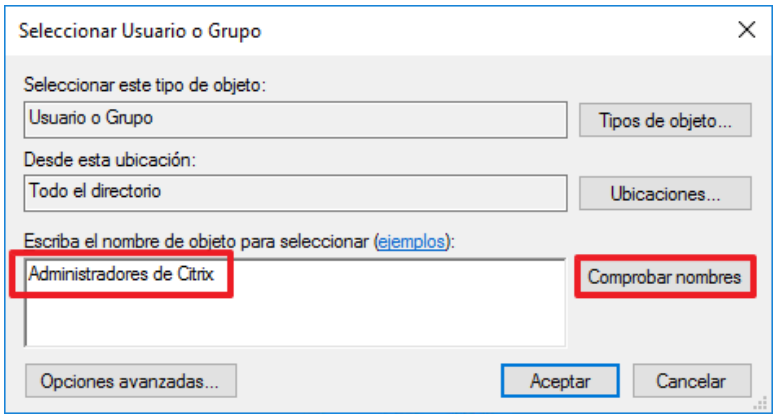
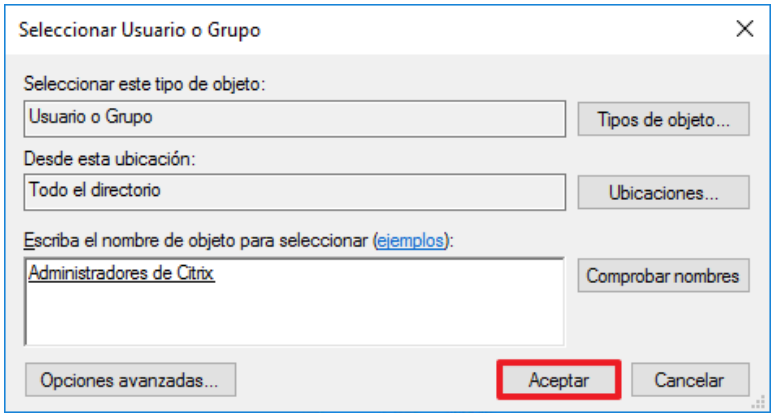
a) Servidor con el rol Citrix Controller

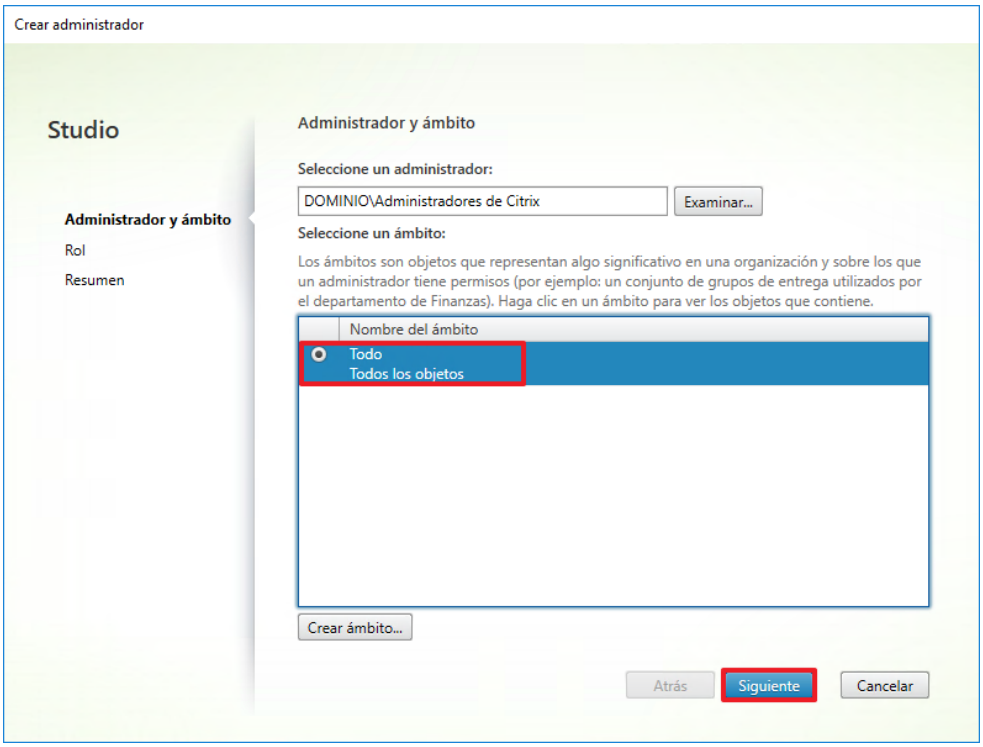
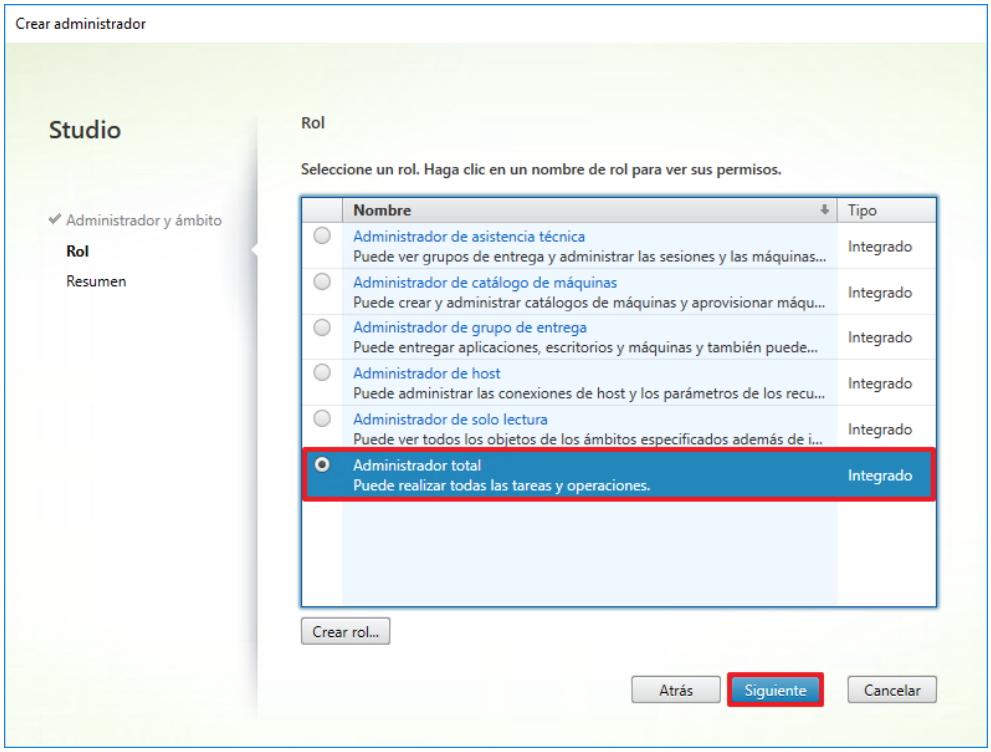
b) Servidor con el rol Citrix Licensing

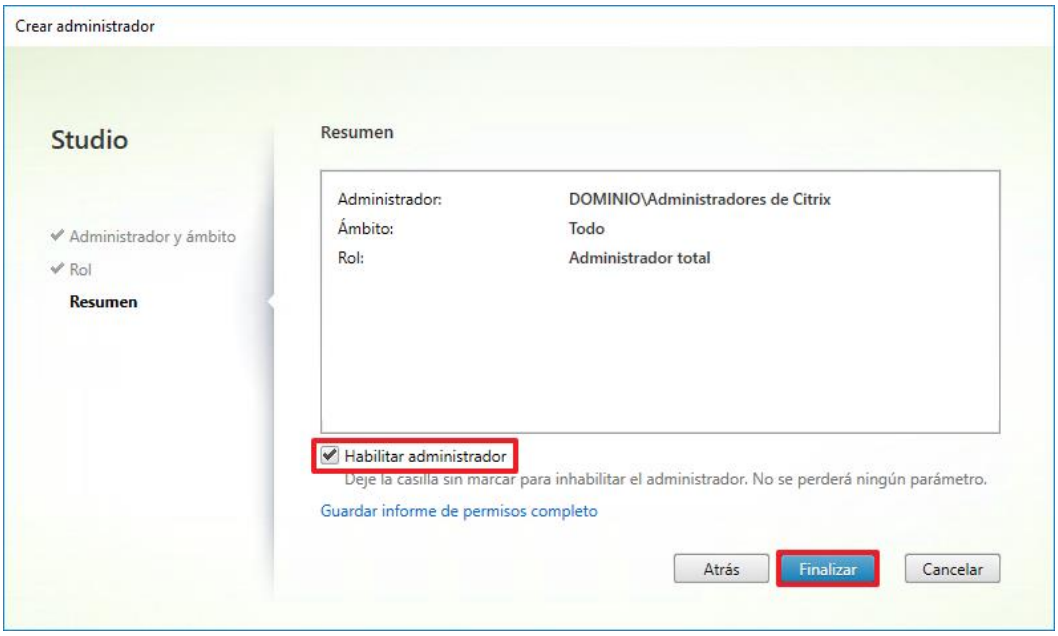
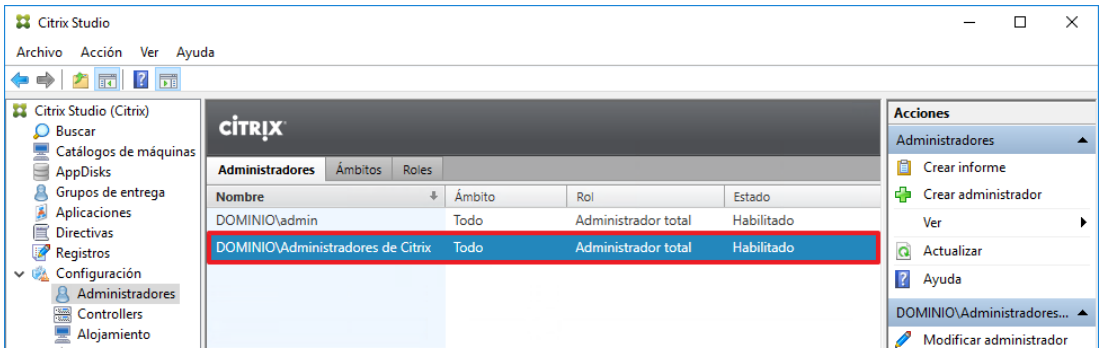
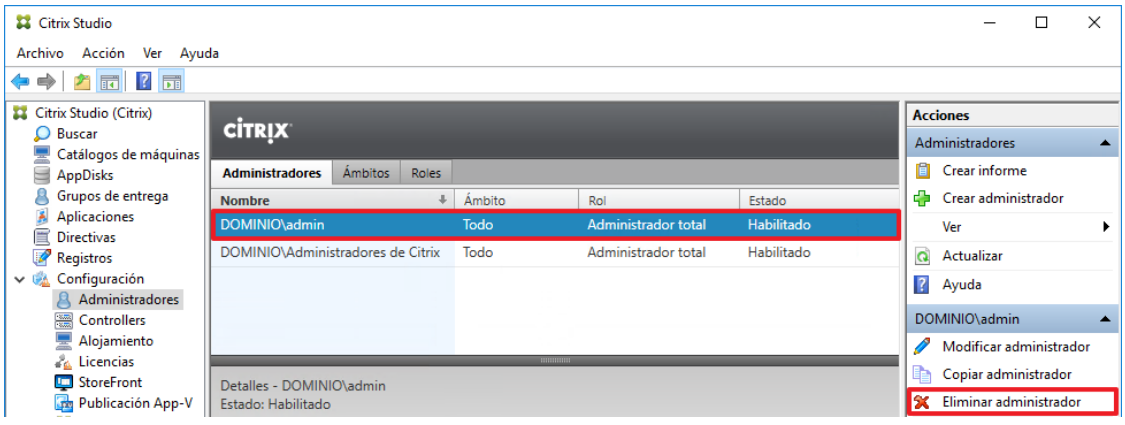
En primer lugar, se realizarán las configuraciones necesarias sobre el servidor con el rol Citrix Controller instalado.

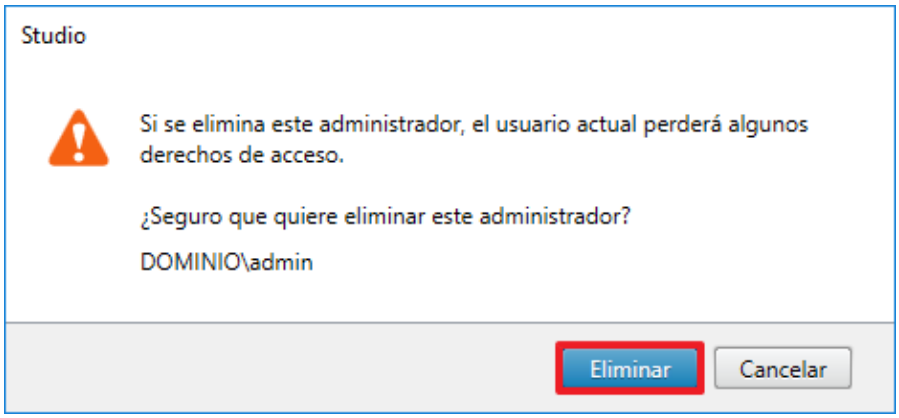
Paso	Descripción
155.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
156.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio. 

Paso	Descripción
157.	El sistema solicitará elevación de privilegios, pulse “Sí” para continuar. 
158.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse “Cancelar” para continuar. 
159.	Diríjase al menú de configuración **“Citrix Studio → Configuración → Administradores → Administradores”** y pulse sobre “Crear administrador”. 

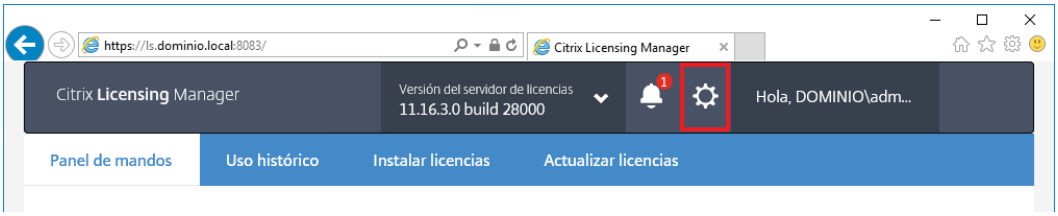
Paso	Descripción
160.	Sobre la ventana emergente, “Crear administrador” pulse sobre “Examinar”. 
161.	Introduzca el nombre del objeto “Administradores de Citrix” y pulse sobre “Comprobar nombres”. 
162.	Compruebe que el objeto “Administradores de Citrix” ha sido añadido correctamente. Pulse “Aceptar” para añadir el objeto y cerrar la ventana. 

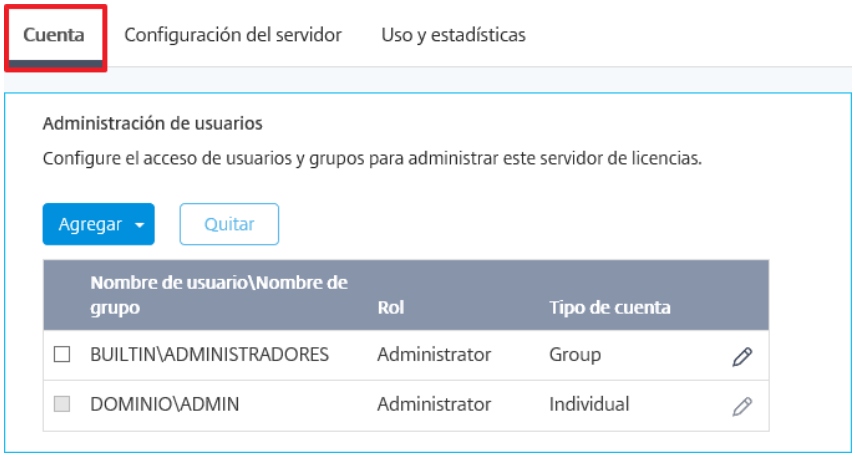
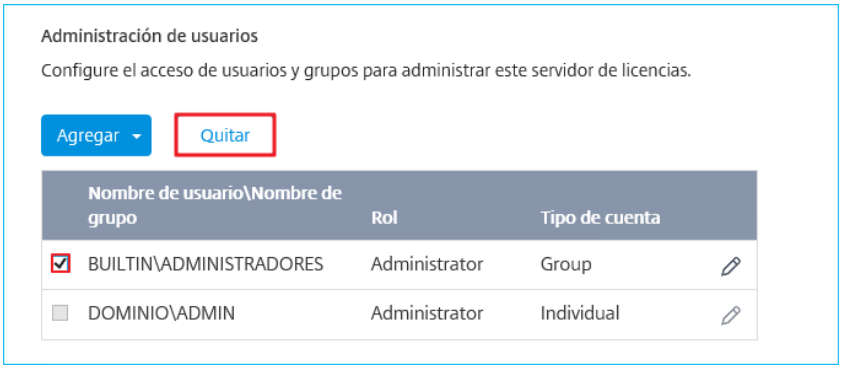
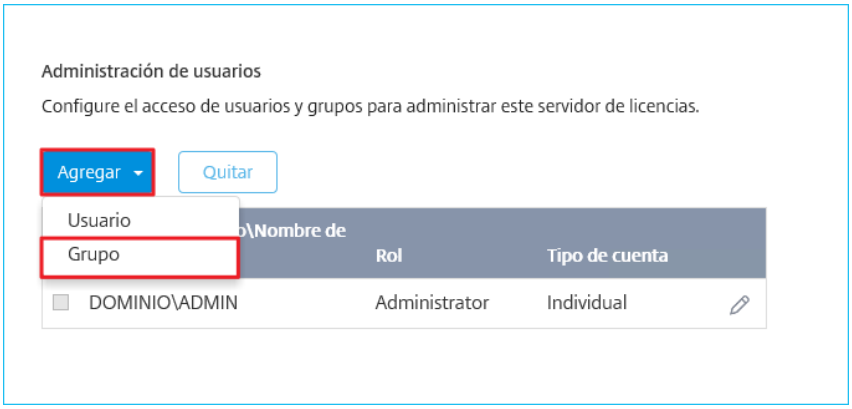
Paso	Descripción
163.	De vuelta en la ventana “Crear administrador”, seleccione el ámbito “Todo” y pulse “Siguiente”. 
164.	Marque el rol “Administrador total” y pulse sobre “Siguiente”.  **Nota:** Para una adecuada gestión de derechos de acceso a la administración de Citrix Studio, deberá crear previamente los grupos correspondientes en el dominio, asociados a los roles de administración que más se adecuen a su organización.

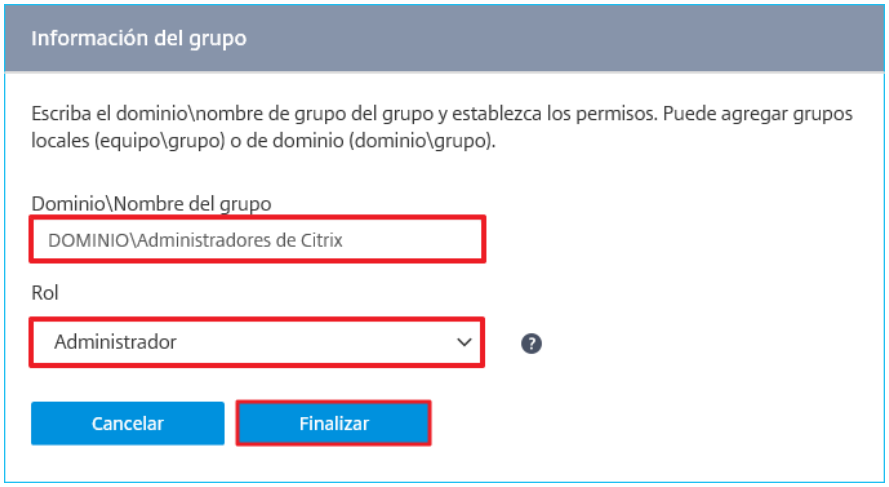
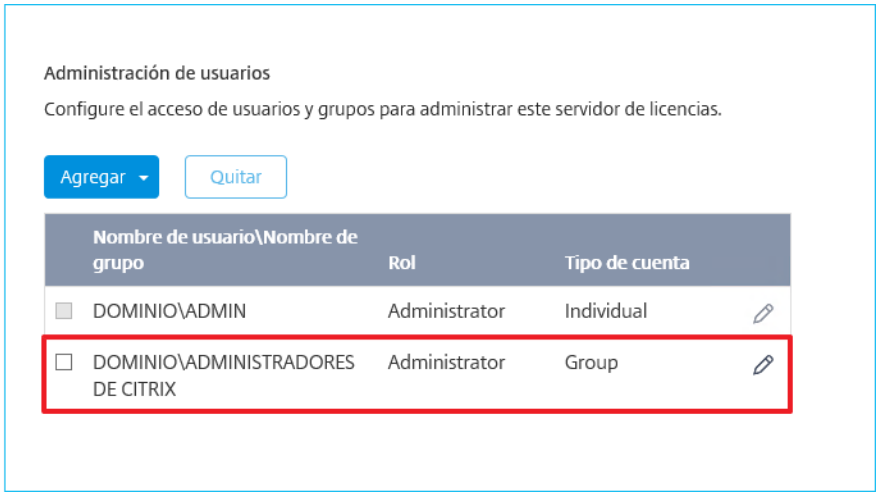
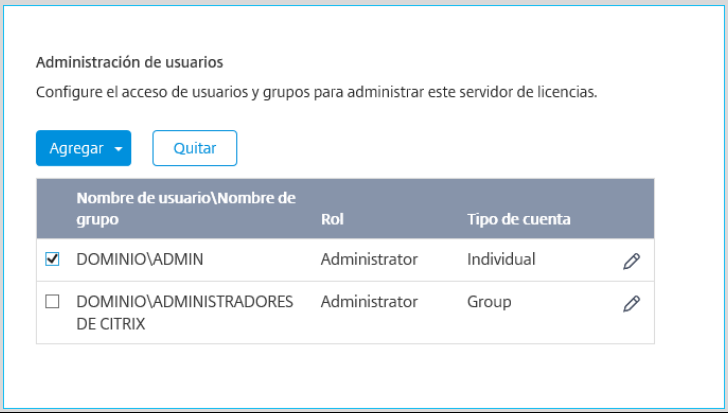
Paso	Descripción
165.	Verifique que la casilla **"Habilitar administrador"** está marcada y pulse sobre "Finalizar". 
166.	Acto seguido apreciará el grupo recientemente creado en la consola. 
167.	Para finalizar con el proceso debe eliminar cualquier usuario administrador que esté introducido a mano en el sistema. Marque el usuario y pulse sobre "Eliminar administrador". 

Paso	Descripción
168.	El sistema le indicará una advertencia indicando que el usuario actual perderá algunos derechos de acceso. Ignore la advertencia y pulse sobre “Eliminar”. 

A continuación, se procederá a realizar las configuraciones de seguridad necesarias en el servidor con el rol Citrix Licensing.

Paso	Descripción
169.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
170.	Acceda a la dirección URL del “Citrix Licensing Manager” https://ls.dominio.local:8083 adaptándolo a su entorno.
171.	Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre la rueda superior derecha. 

Paso	Descripción
172.	A continuación, acceda al nodo de configuración “Cuenta”, en los siguientes pasos definirá los administradores de licencias del servidor. Por defecto, el instalador del producto define los siguientes administradores. – BUILTIN\ADMINISTRADORES – DOMINIO\ADMIN  **Nota:** El usuario “DOMINIO\admin” se corresponde con el usuario utilizado para realizar el proceso de instalación del sistema y variará dependiendo de su entorno.
173.	Seleccione el grupo “BUILTIN\ADMINISTRADORES” y acto seguido pulse sobre el botón “Quitar”. 
174.	Despliegue el menú extraíble pulsando sobre el botón “Agregar” y pulse sobre “Grupo”. 

Paso	Descripción
175.	En la ventana emergente de configuración especifique el grupo creado anteriormente “DOMINIO\Administradores de Citrix” que deberá tener el rol “Administrador”. Pulse sobre “Finalizar” para añadir el nuevo grupo administrador. 
176.	Verifique que el grupo se ha agregado correctamente desde el apartado “Cuenta”.  **Nota:** Para eliminar el usuario con el que realizó la instalación deberá acceder al servidor con otro usuario diferente que pertenezca al grupo “DOMINIO\Administradores de Citrix” y proceder con su eliminación como en pasos anteriores. 

7. 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.

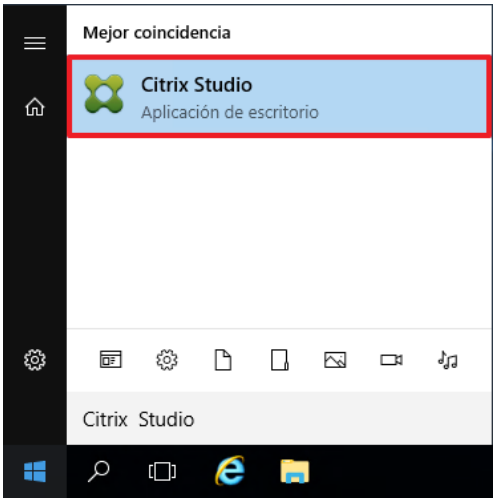
En el procedimiento que se describe a continuación, se desactiva el "Citrix Customer Experience Improvement Program" para evitar el envío de información al fabricante.

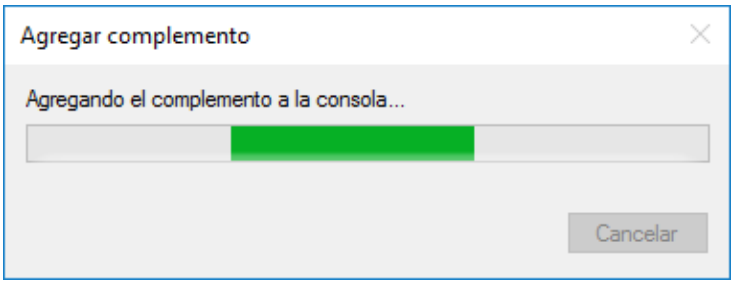
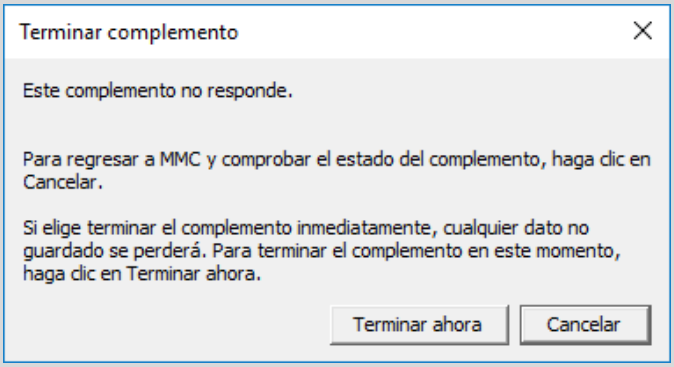
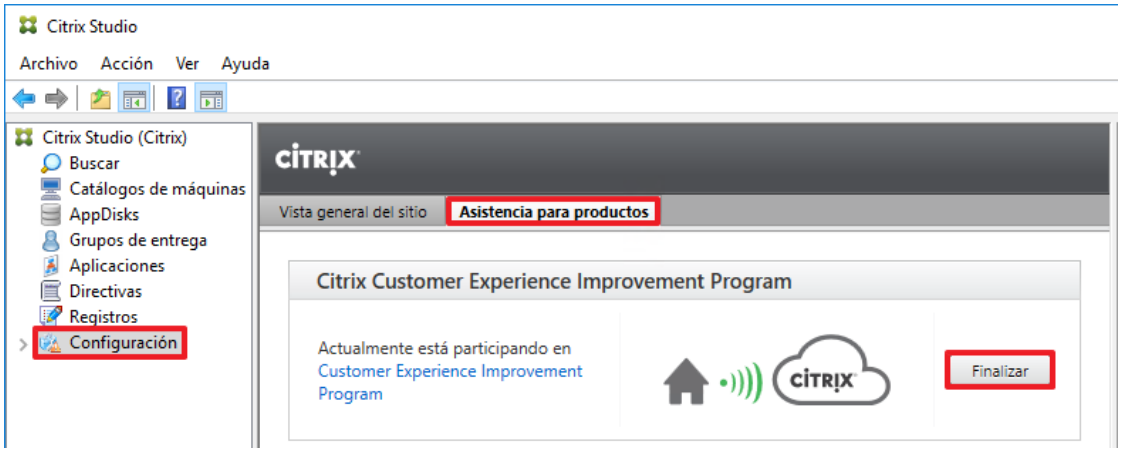
Esta configuración será de aplicación en los siguientes servidores de su infraestructura Citrix Virtual Apps and Desktops:

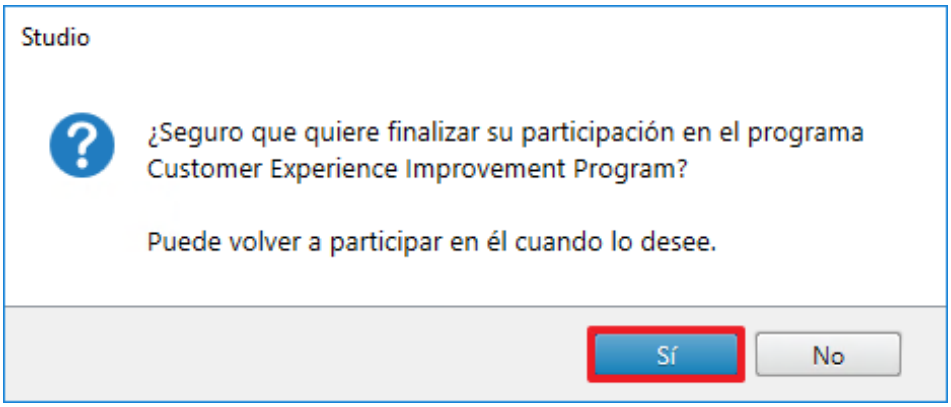
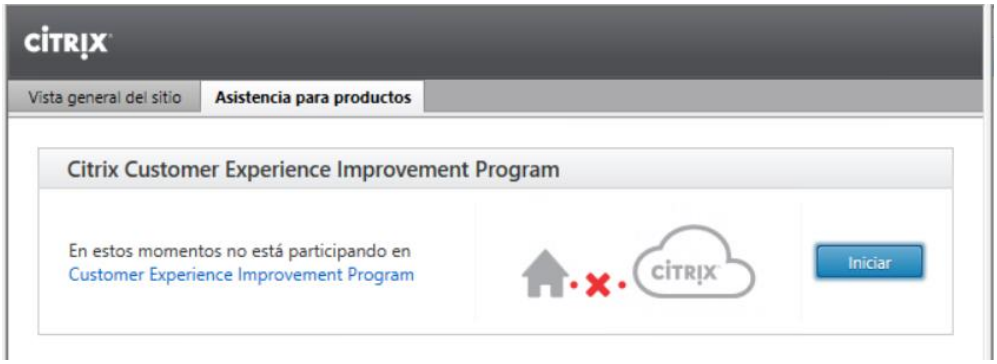
a) Servidor con el rol Citrix Controller

b) Servidor con el rol Citrix Licensing

En primer lugar, se realizarán las configuraciones necesarias sobre el servidor con el rol Citrix Controller instalado.

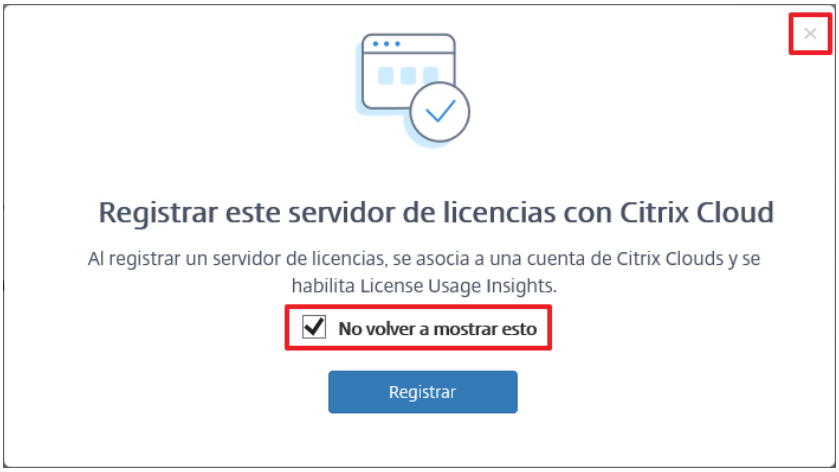
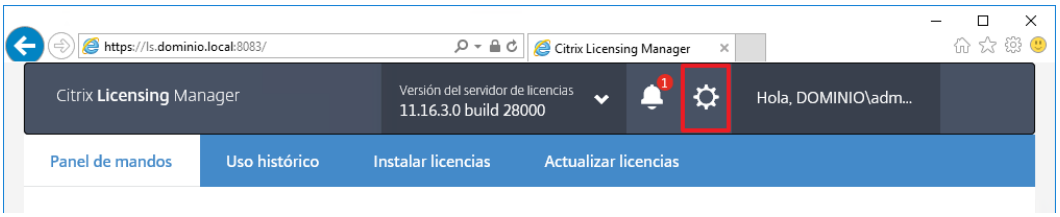
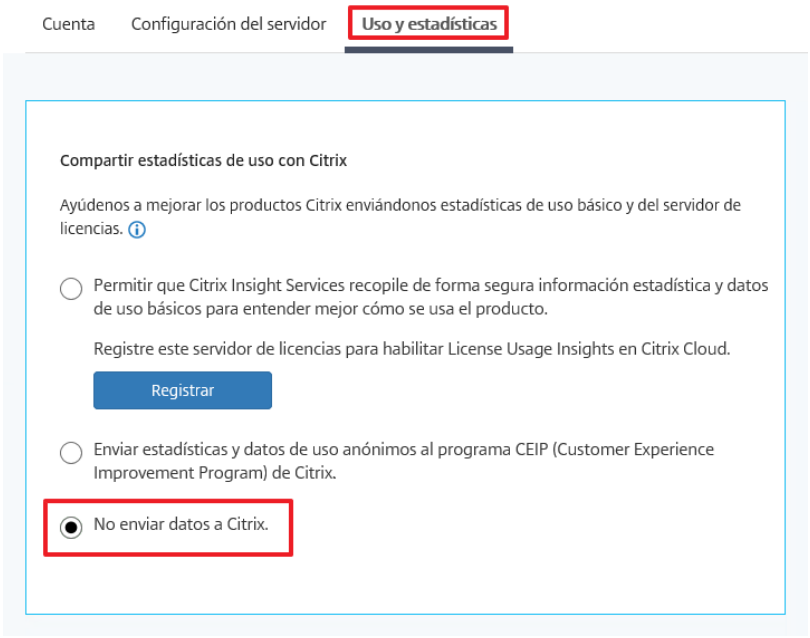
Paso	Descripción
177.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
178.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios.

Paso	Descripción
179.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
180.	Sobre la consola "Citrix Studio" diríjase al nodo **"Citrix Studio → Configuración → Asistencia para productos"**. Por defecto, los productos de Citrix participan automáticamente en el "Customer Experience Improvement Program" por lo que envían información a Citrix para la solución de errores en el producto. Pulse sobre "Finalizar" para detener el envío de información. 

Paso	Descripción
181.	En la ventana emergente que aparecerá pulse sobre “Si” para finalizar la participación en el programa. 
182.	Tras unos instantes puede apreciar como la consola indica que no está participando en el programa de mejora de la experiencia del usuario. 

A continuación, se procederá a realizar las configuraciones de seguridad necesarias en el servidor con el rol Citrix Licensing.

Paso	Descripción
183.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
184.	Acceda a la dirección URL del “Citrix Licensing Manager” https://ls.dominio.local:8083 adaptándolo a su entorno.

Paso	Descripción
185.	Es posible que le aparezca una ventana donde se le ofrece registrar el servidor de licencias con Citrix Cloud. Marque la casilla “No volver a mostrar esto” si no lo realizó anteriormente, y cierre la ventana pulsando el aspa de la parte superior derecha de la ventana. 
186.u	Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre la rueda superior derecha. 
187.	Acceda al apartado “Uso y estadísticas” y pulse sobre “No enviar datos a Citrix” para evitar compartir estadísticas de uso con el fabricante. 

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA CITRIX VIRTUAL APPS AND DESKTOPS SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

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

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

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.3.1.IMPLEMENTACIÓN DE SEGURIDAD PARA CITRIX VIRTUAL APPS AND DESKTOPS EN SERVIDORES MIEMBROS DEL DOMINIO SOBRE MICROSOFT SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

1. CONTROLADOR DE DOMINIO

Los siguientes pasos determinan el procedimiento para verificar la configuración del dominio en el que se despliega el sistema de virtualización.

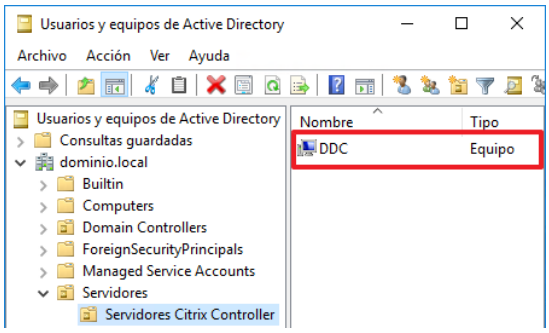
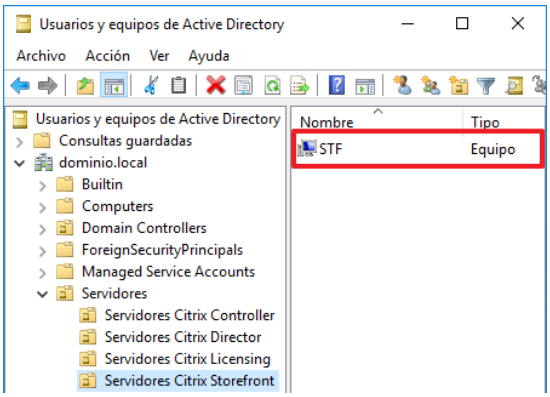
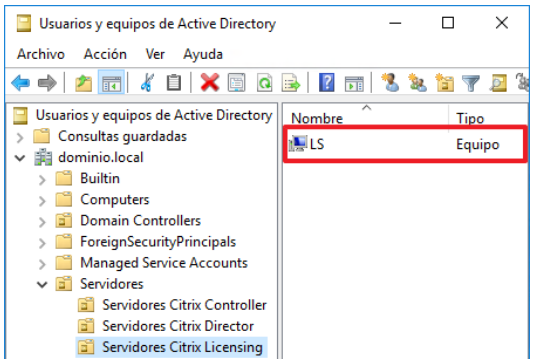
Las consolas y herramientas que se utilizarán son las siguientes:

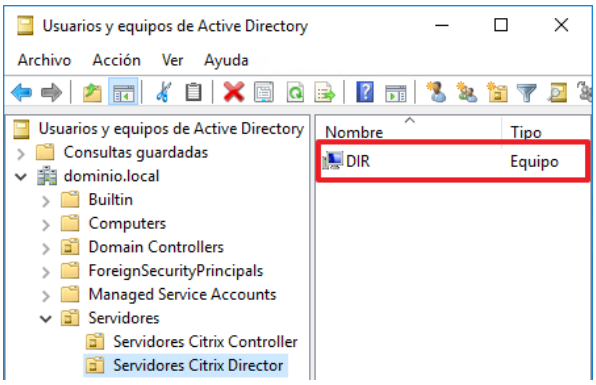
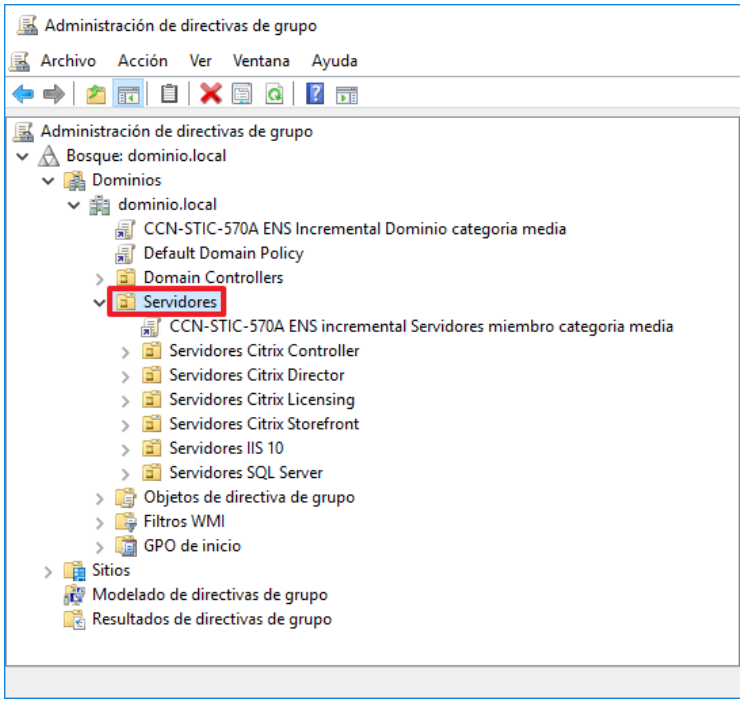
a) En el controlador de dominio:

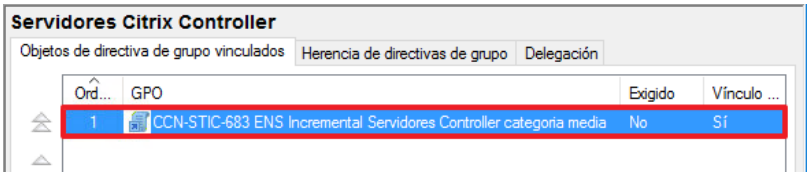
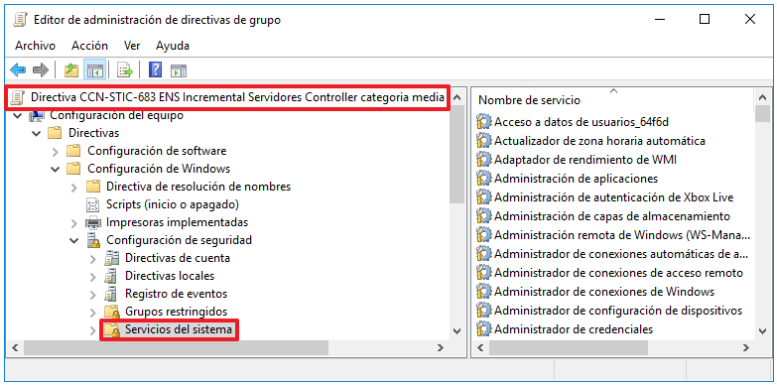
i. Usuarios y equipos de Active Directory (dsa.msc).

ii. Administrador de directivas de grupo (gpmc.msc).

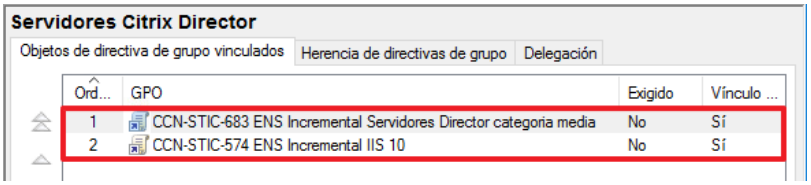
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un servidor controlador de dominio.		En un servidor controlador de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que están creadas las unidades organizativas de Citrix y que alojan sus respectivos servidores.		Ejecute la herramienta "Usuarios y equipos de Active Directory" desde: "**Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**". El sistema le solicitará elevación de privilegios para acceder a la consola de administración.

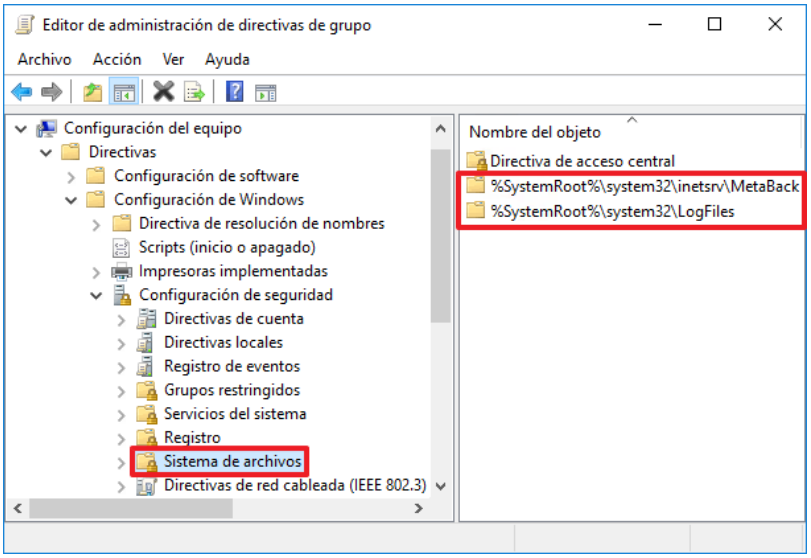
Comprobación	OK/NOK	Cómo hacerlo
3. La unidad organizativa "Servidores Citrix Controller" debe albergar todos los servidores con el rol Citrix Controller de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Controller" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "DDC", en su caso debe figurar el nombre de su equipo.
4. La unidad organizativa "Servidores Citrix Storefront" debe albergar todos los servidores con el rol Citrix Storefront de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Storefront" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "STF", en su caso debe figurar el nombre de su equipo.
5. La unidad organizativa "Servidores Citrix Licensing" debe albergar todos los servidores con el rol Citrix Licensing de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Licensing" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "LS", en su caso debe figurar el nombre de su equipo.

Comprobación	OK/NOK	Cómo hacerlo
6. La unidad organizativa "Servidores Citrix Director" debe albergar todos los servidores con el rol Citrix Director de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Director" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "DIR", en su caso debe figurar el nombre de su equipo.
7. Verifique que están creadas las directivas de configuración de Citrix.		Ejecute la herramienta "Administración de directivas de grupo" desde: **"Menú inicio → Herramientas administrativas → Administración de directivas de grupo"**. El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio. Seleccione la unidad organizativa "Servidores", situada en **"Bosque → Dominios → [Su dominio] → Servidores"**. 

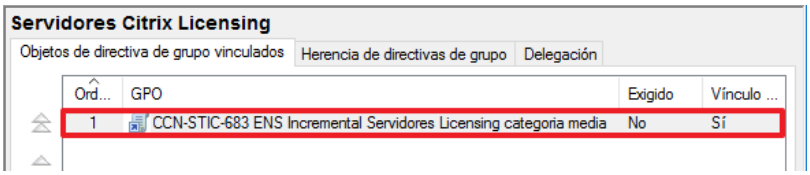
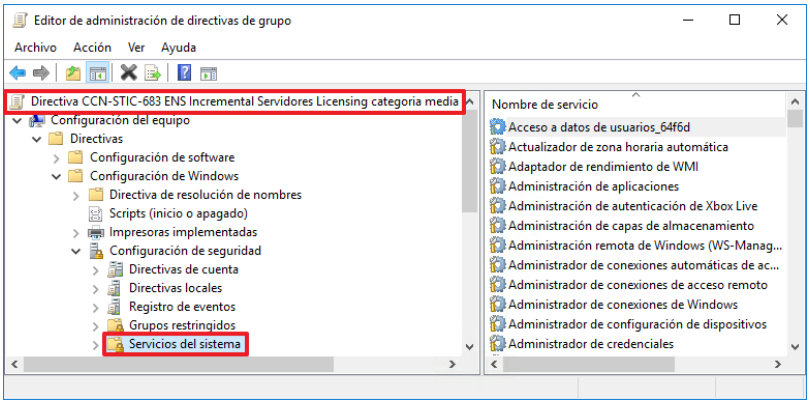
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique las políticas aplicadas a "Servidores Citrix Controller".		Seleccione la unidad organizativa "Servidores Citrix Controller", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Controller"** y revise que, como mínimo, tiene aplicada la siguiente directiva y tiene el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Controller categoria media 
9. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Controller categoria media".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Controller categoria media" tiene los siguientes valores de servicios de sistema. "**Directiva CCN-STIC-683 ENS Incremental Servidores Controller categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema**".  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Asignador de extremos de RPC	RpcEptMapper	Automático	
Citrix AD Identity Service	CitrixADIdentityService	Automático	
Citrix Analytics	CitrixAnalytics	Automático	
Citrix App Library	CitrixAppLibrary	Automático	
Citrix Broker Service	CitrixBrokerService	Automático	
Citrix Config Synchronizer Service	CitrixConfigSyncService	Automático	
Citrix Configuration Service	CitrixConfigurationService	Automático	
Citrix Configuration Logging Service	CitrixConfigurationLogging	Automático	

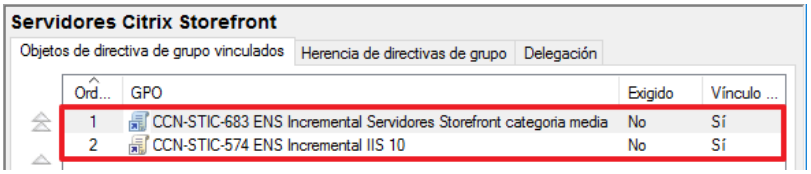
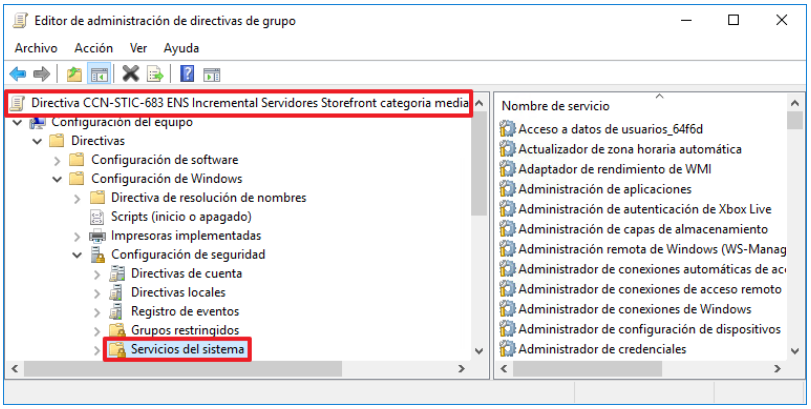
<table>
<tr><th colspan="2">Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td colspan="3">Servicio (nombre largo)</td><td>Servicio (nombre corto)</td><td>Inicio</td><td>OK/NOK</td></tr>
<tr><td colspan="3">Citrix Smart Tools Agent Service</td><td>CitrixConnector</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="3">Citrix Delegated Administration Service</td><td>CitrixDelegatedAdmin</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Enviroment Test Service</td><td>CitrixEnvTest</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix High Availability Service</td><td>CitrixHighAvailabilityService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Host Service</td><td>CitrixHostService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Machine Creation Service</td><td>CitrixMachineCreationService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Monitor Service</td><td>CitrixMonitor</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Orchestration Service</td><td>CitrixOrchestration</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Storefront Privileged Administration Service</td><td>CitrixPrivilegedService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Storefront Service</td><td>CitrixStorefront</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Telemetry Service</td><td>CitrixTelemetryService</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="3">Citrix Trust Service</td><td>CitrixTrust</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Estación de trabajo</td><td>LanmanWorkstation</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Iniciador de procesos de servidor DCOM</td><td>DcomLaunch</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Llamada a procedimiento remoto (RPC)</td><td>RpcSs</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Servicio Interfaz de almacenamiento en red</td><td>nsi</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Remote Broker Provider</td><td>XaXdCloudProxy</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Smart Tools Monitor Service</td><td>Monitor Agent</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">10. Verifique las políticas aplicadas a “Servidores Citrix Director”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Servidores Citrix Director”, situada en “Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Director” y revise que, como mínimo, la unidad organizativa “Servidores Citrix Director” tiene aplicadas las siguientes directivas en el orden adecuado y tienen el vínculo habilitado.
– CCN-STIC-683 ENS Incremental Servidores Director categoria media
– CCN-STIC-574 ENS Incremental Servidores IIS 10
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique los valores de los permisos del sistema de archivos de la directiva "CCN-STIC-683 ENS Incremental Servidores Director categoria media".		Utilizando el "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Director categoria media" tiene los siguientes valores de permisos de sistema de archivos. **"Directiva CCN-STIC-683 ENS Incremental Servidores Director categoria media→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos"**.  **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\inetsrv\MetaBack	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	
%SystemRoot%\system32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique las políticas aplicadas a "Servidores Citrix Licensing".		Seleccione la unidad organizativa "Servidores Citrix Licensing", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Licensing"** y revise que, como mínimo, la unidad organizativa "Servidores Citrix Licensing" tiene aplicada la siguiente directiva y tiene el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Licensing categoria media 
13. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Licensing categoria media".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Licensing categoria media" tiene los siguientes valores de servicios de sistema. "**Directiva CCN-STIC-683 ENS Incremental Servidores Licensing categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema**".  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Licensing	Citrix Licensing	Automático	
Citrix Web Services for Licensing	CitrixWebServicesforLicensing	Automático	
Citrix Licensing Support Service	CtxLSPortSvc	Automático	
Citrix Licensing WMI	Citrix_GTLicensingProv	Manual	

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique las políticas aplicadas a "Servidores Citrix Storefront".		Seleccione la unidad organizativa "Servidores Citrix Storefront", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Storefront"** y revise que, como mínimo, la unidad organizativa "Servidores Citrix Storefront" tiene aplicadas las siguientes directivas en el orden adecuado y tienen el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Storefront categoria media – CCN-STIC-574 ENS Incremental IIS 10 
15. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria media".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria media" tiene los siguientes valores de servicios de sistema. "**Directiva CCN-STIC-683 ENS Incremental Servidores Storefront categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema**".  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	
Citrix Peer Resolution Service	Citrix Peer Resolution Service	Automático	
Citrix Configuration Replication	CitrixConfigurationReplication	Automático	
Citrix Credential Wallet	CitrixCredentialWallet	Automático	
Citrix Default Domain Service	CitrixDefaultDomainService	Automático	
Citrix Service Monitor	CitrixServiceMonitor	Automático	

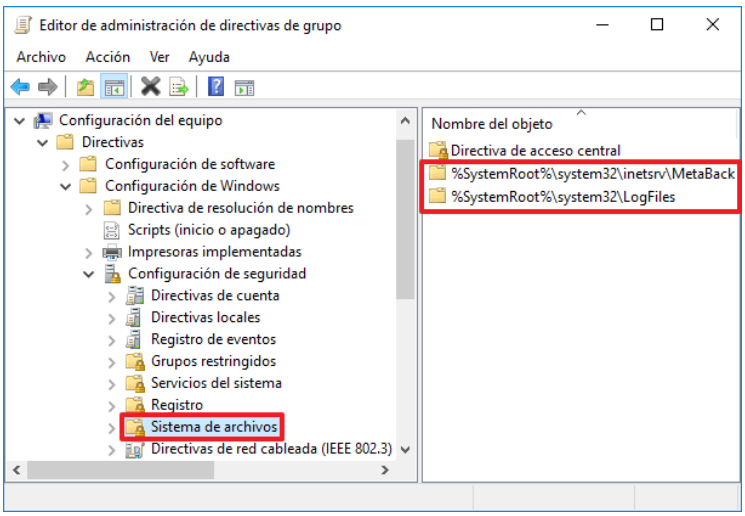
Comprobación	OK/NOK	Cómo hacerlo

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Subscriptions Store	CitrixSubscriptionsStore	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Automático	
Servidor	LanmanServer	Automático	
Citrix Cluster Service	CitrixClusterService	Deshabilitado	

16. Verifique los valores de los permisos del sistema de archivos de la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria media".

Utilizando el "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria media" tiene los siguientes valores de permisos de sistema de archivos.

"Directiva CCN-STIC-683 ENS Incremental Servidores Storefront categoria media→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos".



Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...".
Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\inetsrv\MetaBack	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	
%SystemRoot%\system32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	

2. CITRIX CONTROLLER

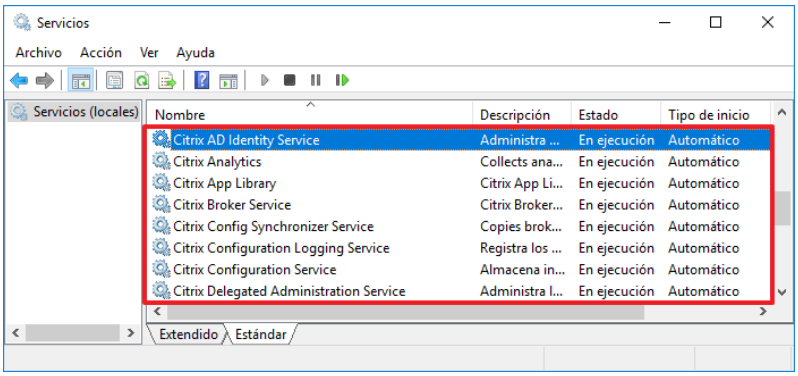
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Controller, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

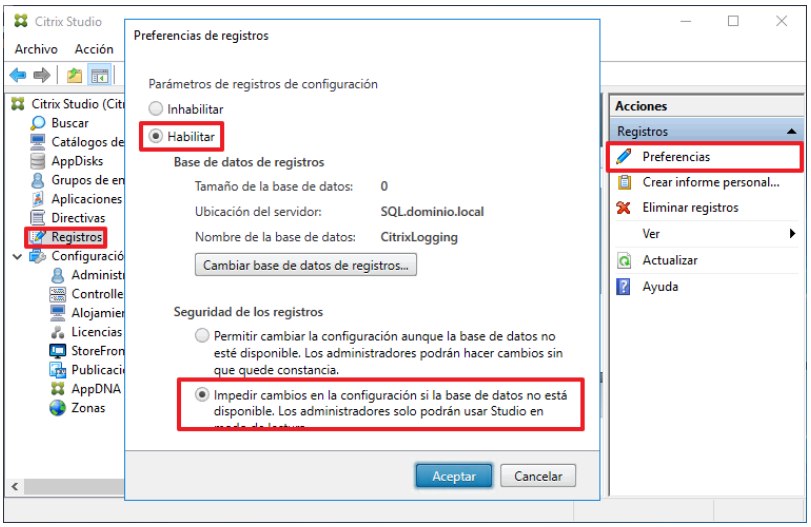
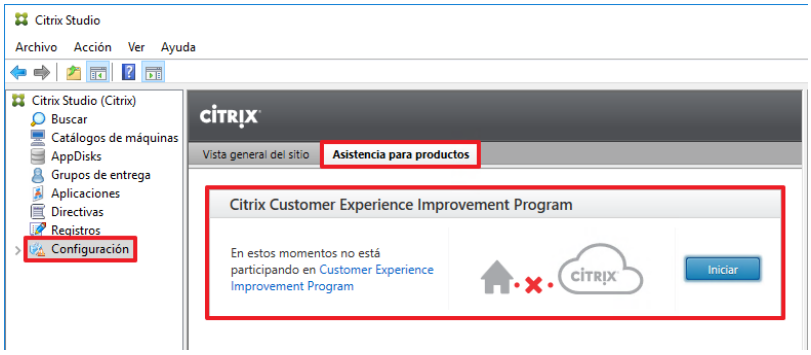
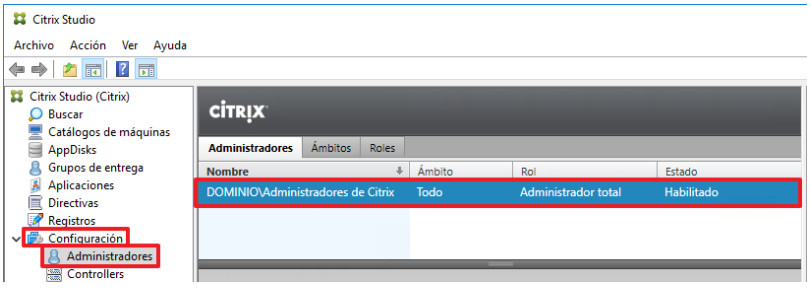
a) En el servidor miembro Citrix Controller:

i. Servicios (services.msc).

ii. Consola de Citrix Studio.

Comprobación	OK/NOK	Cómo hacerlo
17. Inicie sesión en un servidor con el rol Citrix Controller.		En un servidor con el rol Citrix Controller, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
18. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios.
19. Sobre cada uno de los servidores con el rol Citrix Controller revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Comprobación	OK/NOK	Cómo hacerlo		
Servicio (nombre largo)		**Servicio (nombre corto)**	**Inicio**	**OK/NOK**
Asignador de extremos de RPC		RpcEptMapper	Automático	
Citrix AD Identity Service		CitrixADIdentityService	Automático	
Citrix Analytics		CitrixAnalytics	Automático	
Citrix App Library		CitrixAppLibrary	Automático	
Citrix Broker Service		CitrixBrokerService	Automático	
Citrix Config Synchronizer Service		CitrixConfigSyncService	Automático	
Citrix Configuration Service		CitrixConfigurationService	Automático	
Citrix Configuration Logging Service		CitrixConfigurationLogging	Automático	
Citrix Smart Tools Agent Service		CitrixConnector	Deshabilitado	
Citrix Delegated Administration Service		CitrixDelegatedAdmin	Automático	
Citrix Enviroment Test Service		CitrixEnvTest	Automático	
Citrix High Availability Service		CitrixHighAvailabilityService	Automático	
Citrix Host Service		CitrixHostService	Automático	
Citrix Machine Creation Service		CitrixMachineCreationService	Automático	
Citrix Monitor Service		CitrixMonitor	Automático	
Citrix Orchestration Service		CitrixOrchestration	Automático	
Citrix Storefront Privileged Administration Service		CitrixPrivilegedService	Automático	
Citrix Storefront Service		CitrixStorefront	Automático	
Citrix Telemetry Service		CitrixTelemetryService	Deshabilitado	
Citrix Trust Service		CitrixTrust	Automático	
Estación de trabajo		LanmanWorkstation	Automático	
Iniciador de procesos de servidor DCOM		DcomLaunch	Automático	
Llamada a procedimiento remoto (RPC)		RpcSs	Automático	
Servicio Interfaz de almacenamiento en red		nsi	Automático	
Citrix Remote Broker Provider		XaXdCloudProxy	Automático	
Citrix Smart Tools Monitor Service		Monitor Agent	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo
20. Bajo la consola Citrix Studio revise la configuración de registro.		Acceda a la consola "Citrix Studio" y bajo el apartado **"Registros → Preferencias"** verifique que en "Parámetros de registros de configuración" se encuentra marcada la opción **"Habilitar"** y tiene aplicada la configuración **"Impedir cambios en la configuración si la base de datos no está disponible. Los administradores solo podrán utilizar Studio en modo de lectura"**. 
21. Compruebe la no participación en Citrix CEIP.		Sobre la consola "Citrix Studio" diríjase al nodo **"Citrix Studio → Configuración → Asistencia para productos"**. Compruebe que el "Citrix Customer Experience Improvement Program" se encuentra detenido. 
22. Revisión permisos administrativos		Dirjase al menú de configuración **"Citrix Studio → Configuración → Administradores"** y compruebe que se han restringido los permisos administrativos a los necesarios en función de su organización. 

3. CITRIX STOREFRONT

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Storefront, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

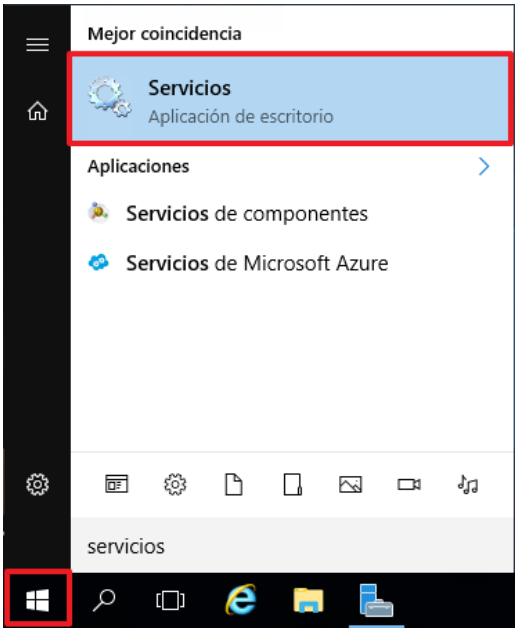
a) En el servidor miembro Citrix Storefront:

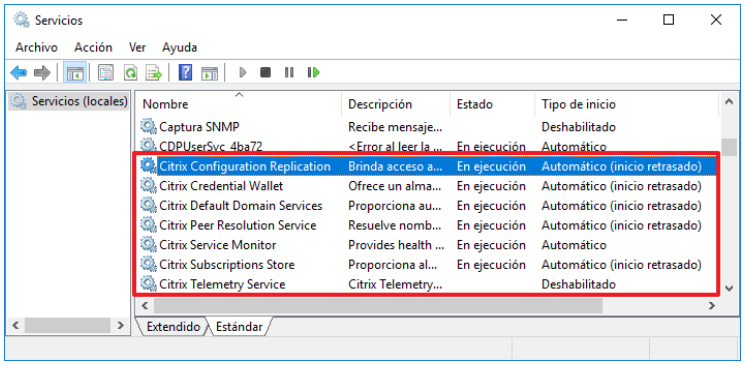
i. Servicios (services.msc).

ii. Consola de administración de Microsoft (mmc.exe).

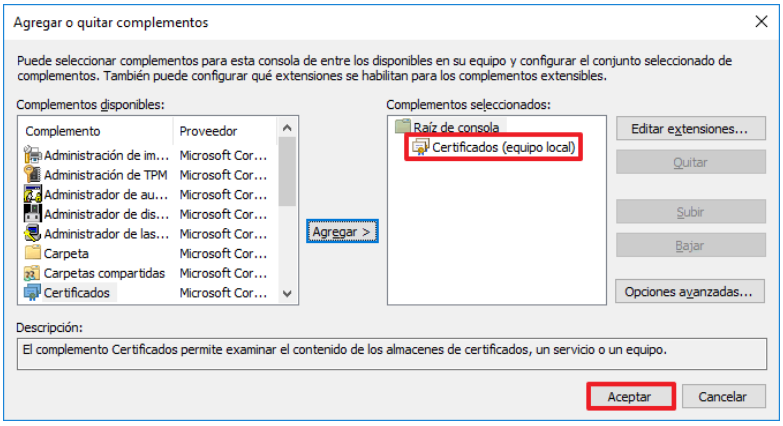
iii. Administrador de Internet Information Service (IIS).

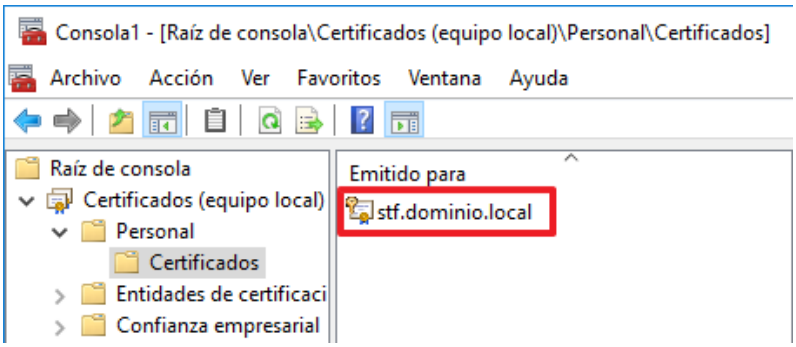
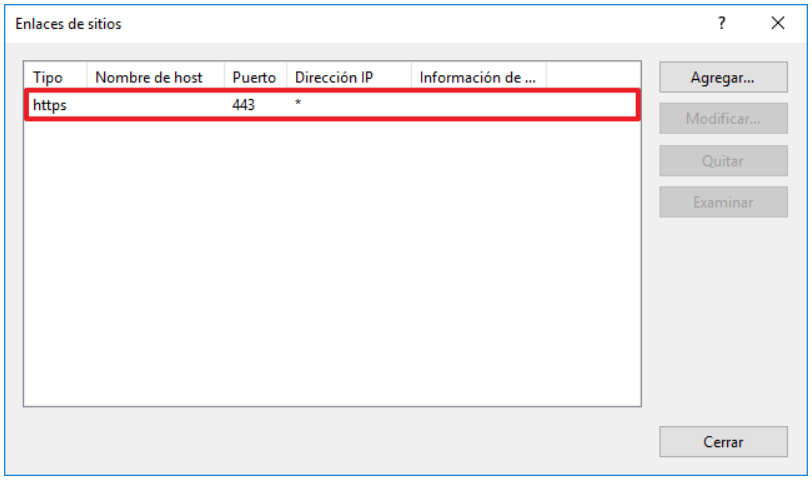
iv. Consola de Citrix Storefront.

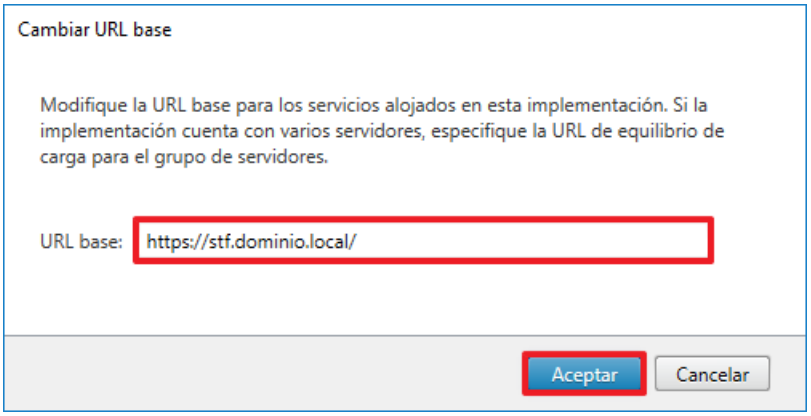
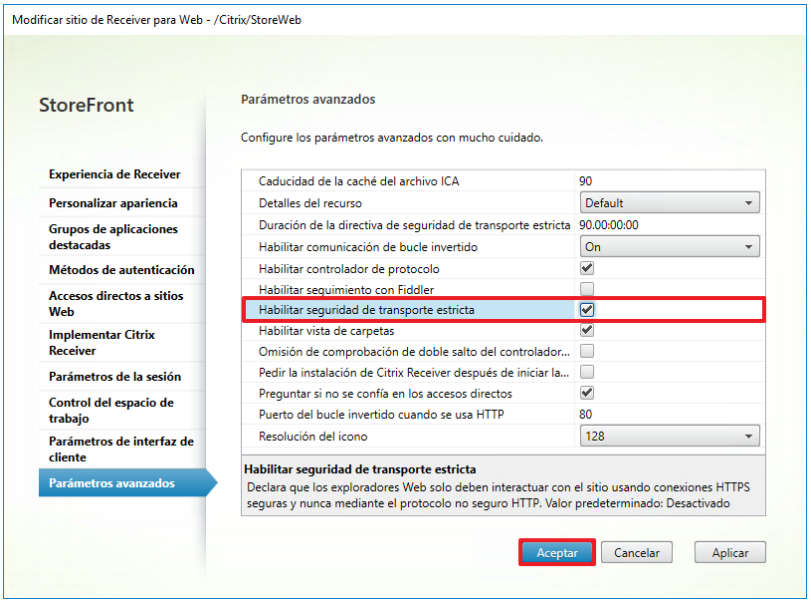
Comprobación	OK/NOK	Cómo hacerlo
23. Inicie sesión en un servidor con el rol Citrix Storefront.		En un servidor con el rol Citrix Storefront, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
24. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios. 

Comprobación	OK/NOK	Cómo hacerlo
25. Sobre cada uno de los servidores con el rol Citrix Storefront revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	
Citrix Peer Resolution Service	Citrix Peer Resolution Service	Automático	
Citrix Configuration Replication	CitrixConfigurationReplication	Automático	
Citrix Credential Wallet	CitrixCredentialWallet	Automático	
Citrix Default Domain Service	CitrixDefaultDomainService	Automático	
Citrix Service Monitor	CitrixServiceMonitor	Automático	
Citrix Subscriptions Store	CitrixSubscriptionsStore	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Automático	
Servidor	LanmanServer	Automático	
Citrix Cluster Service	CitrixClusterService	Deshabilitado	

26. Verifique la instalación del certificado local para cada uno de los servidores Citrix Storefront.		Acceda a la consola “mmc.exe” desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado “Ctrl + M”. 

Comprobación	OK/NOK	Cómo hacerlo
27. Verifique la instalación del certificado local para cada uno de los servidores Citrix Storefront.		Despliegue el nodo **"Personal → Certificados"**. Deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo "Emitido para" variará dependiendo del nombre de su servidor.
28. Ejecute la consola de administración de IIS.		Ejecute la herramienta "Administrador de Internet Information Services (IIS)" desde: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)".** El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.
29. Enlaces de sitios configurado para HTTPS.		Abra el nodo de configuración **"Su servidor (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"** Compruebe que únicamente se encuentra configurado el tipo "https" con el puerto 443. 

Comprobación	OK/NOK	Cómo hacerlo
30. URL base del sitio configurada para HTTPS.		Ejecute la consola Citrix Storefront. Desde la pestaña **"Grupo de servidores"**, acceda a la opción "Cambiar URL base", compruebe que la URL de la tienda incluye el protocolo seguro HTTPS como se muestra en la siguiente figura. 
31. Seguridad de transporte estricta habilitada.		Continúe con las comprobaciones accediendo a la consola "Citrix Storefront" y diríjase al menú de configuración **"Tiendas → Store → Administrar sitios de Receiver para Web"**, en la configuración de su sitio web, dentro del apartado de parámetros avanzados compruebe que se encuentra marcada la opción "Habilitar seguridad de transporte estricta". 

4. CITRIX LICENSING

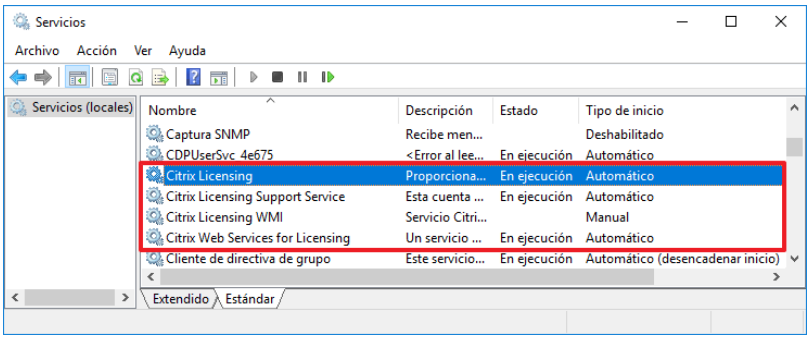
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Licensing, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

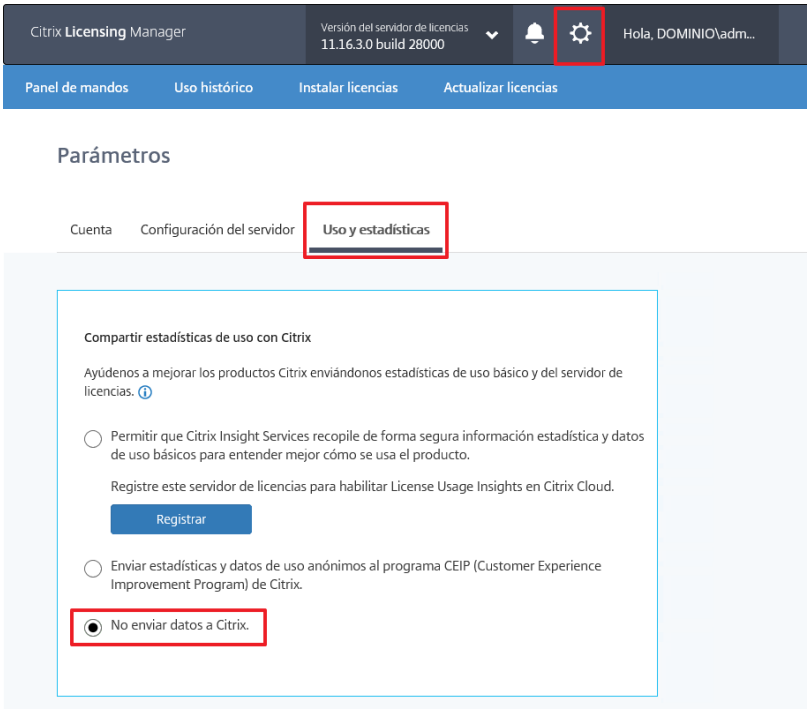
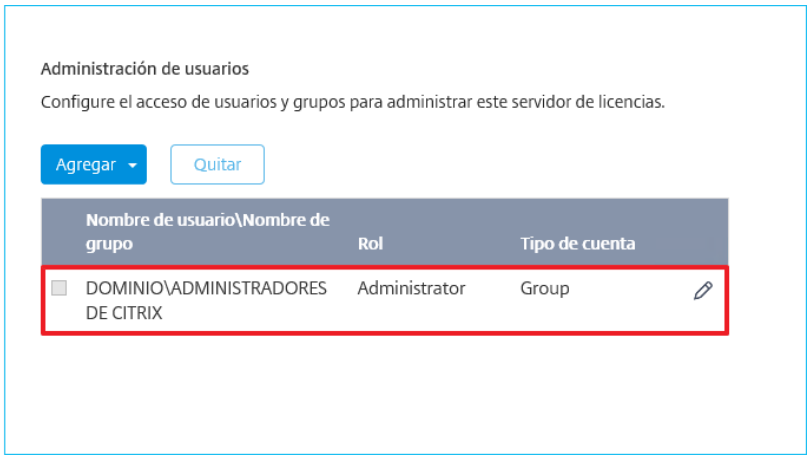
a) En el servidor miembro Citrix Licensing:

i. Servicios (services.msc).

ii. Consola de Citrix Licensing.

Comprobación	OK/NOK	Cómo hacerlo
32. Inicie sesión en un servidor con el rol Citrix Licensing		En un servidor con el rol Citrix Licensing, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
33. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios.
34. Sobre cada uno de los servidores con el rol Citrix Licensing revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Licensing	Citrix Licensing	Automático	
Citrix Web Services for Licensing	CitrixWebServicesforLicensing	Automático	
Citrix Licensing Support Service	CtxLSPortSvc	Automático	
Citrix Licensing WMI	Citrix_GTLicensingProv	Manual	

Comprobación	OK/NOK	Cómo hacerlo
35. Restringir envío de información a Citrix.		Acceda a la dirección URL https://ls.dominio.local:8083 adaptándolo a su entorno. Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre el botón de configuración en la parte superior derecha. Acceda al apartado "Uso y estadísticas". Compruebe que está marcada la opción "No enviar datos a Citrix". 
36. Restricción permisos Citrix Licensing.		A continuación, acceda al nodo de configuración "Cuenta". Verifique que se han restringido los permisos administrativos a los necesarios en función de su organización. 

5. CITRIX DIRECTOR

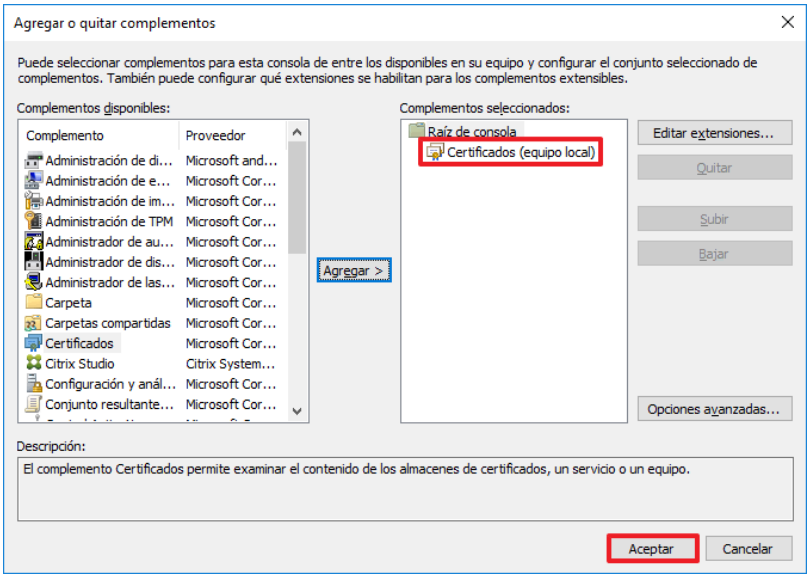
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Director, y las configuraciones propias implementadas sobre este servidor.

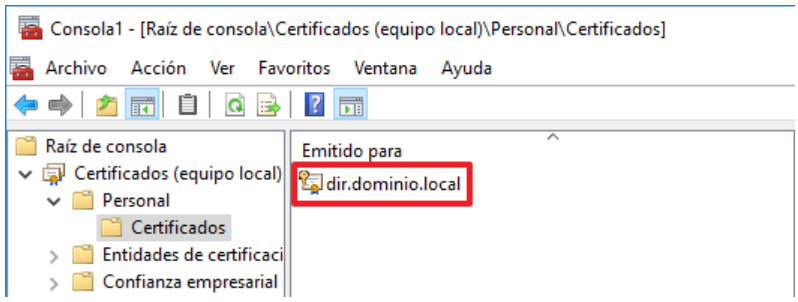
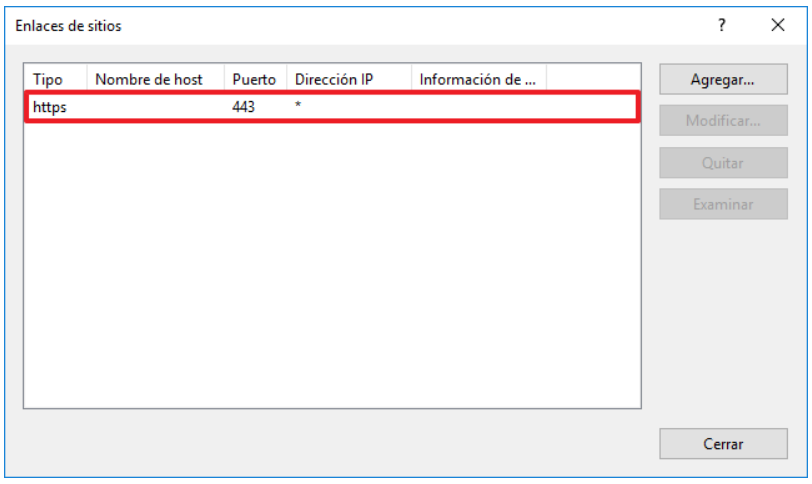
Las consolas y herramientas que se utilizarán son las siguientes:

a) En el servidor miembro Citrix Director:

i. Consola de administración de Microsoft (mmc.exe).

ii. Administrador de Internet Information Service (IIS).

Comprobación	OK/NOK	Cómo hacerlo
37. Inicie sesión en un servidor con el rol Citrix Director.		En un servidor con el rol Citrix Director, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
38. Verifique la instalación del certificado local para cada uno de los servidores Citrix Director.		Acceda a la consola "mmc.exe" desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado "Ctrl + M". 

Comprobación	OK/NOK	Cómo hacerlo
39. Verifique la instalación del certificado local para cada uno de los servidores Citrix Director.		Despliegue el nodo **"Personal → Certificados"**. Deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo "Emitido para" variará dependiendo del nombre de su servidor.
40. Ejecute la consola de administración de IIS.		Ejecute la herramienta "Administrador de Internet Information Services (IIS)" desde: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)".** El sistema le solicitará elevación de privilegios para acceder a la consola de administración.
41. Enlaces de sitios configurado para HTTPS.		Abra el nodo de configuración **"Su servidor (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"** Compruebe que únicamente se encuentra configurado el tipo "https" con el puerto 443. 

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD PARA CITRIX VIRTUAL APPS AND DESKTOPS EN SERVIDORES MIEMBROS DEL DOMINIO SOBRE MICROSOFT SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se tenga que asegurar Citrix Virtual Apps and Desktops 10 sobre Microsoft Windows Server 2016 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 para alguno de ellos, deberá realizar las implementaciones según se referencian en el presente anexo.

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

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

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

1. PREPARACIÓN DEL DOMINIO

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio al que van a pertenecer cada uno de los roles de la infraestructura sobre los que implementará las configuraciones de seguridad. Los pasos descritos a continuación solo los debe realizar cuando vaya a realizar la primera implementación de seguridad en el dominio, ya que solo es necesario crear las unidades organizativas, modificar las plantillas de seguridad e incorporarlas en la directiva de grupo una única vez por dominio.

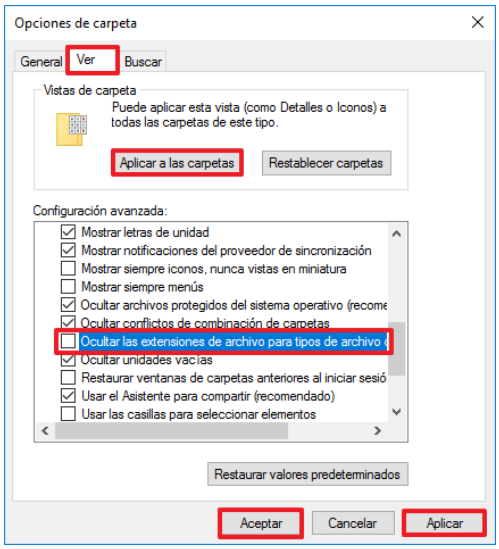
Se asume que ha realizado la implementación de las siguientes guías de seguridad sobre el servidor controlador de dominio donde se va a aplicar el siguiente paso a paso:

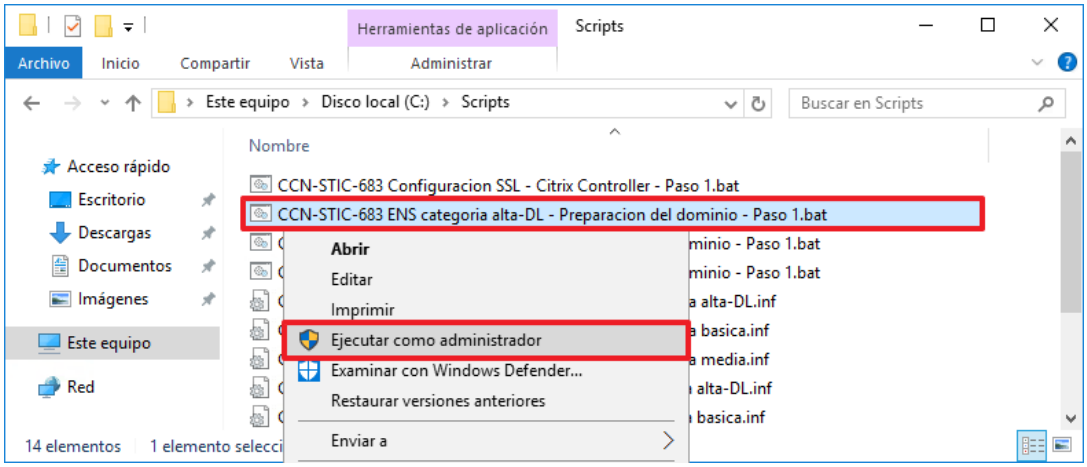
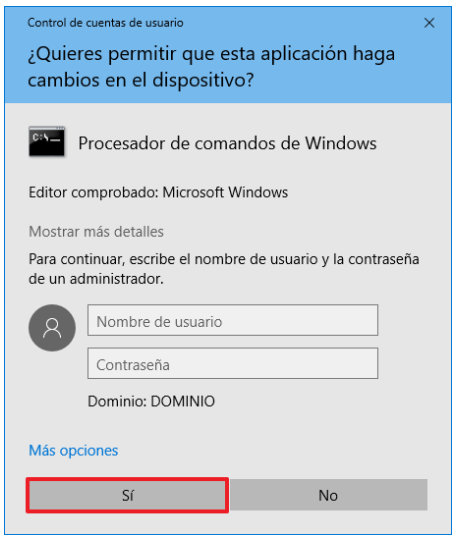
a) CCN-STIC-570A Anexo A Controlador de dominio - Categoría Alta / Difusión Limitada.

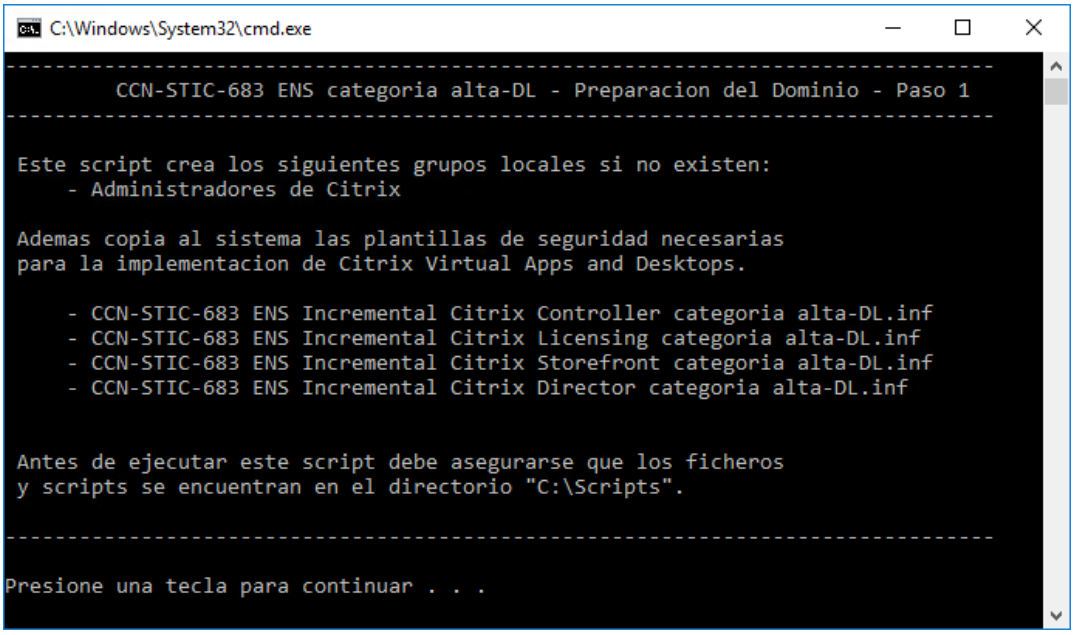
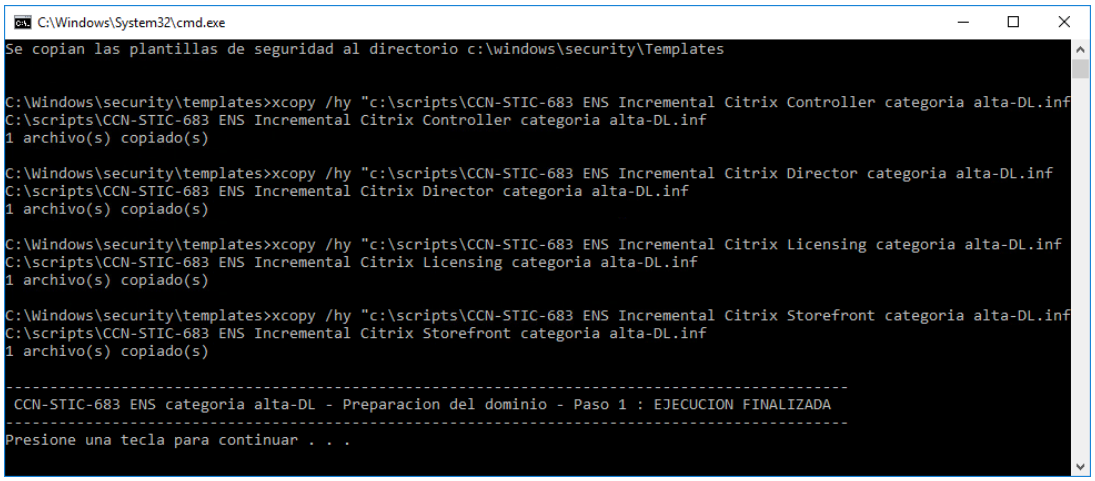
b) CCN-STIC-575 Anexo A Microsoft SQL server 2016 - Categoría Alta / Difusión Limitada.

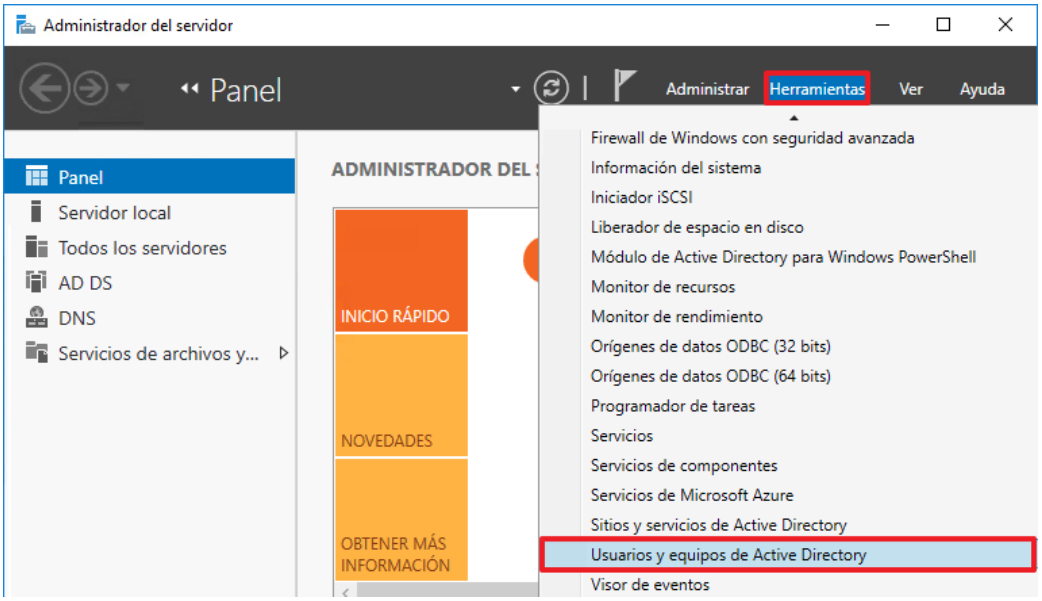
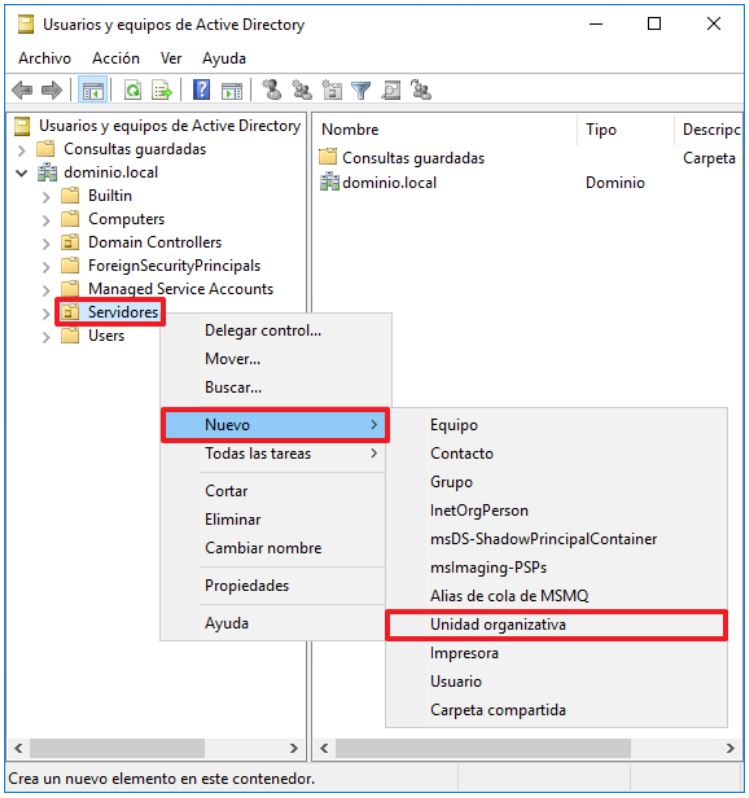
c) CCN-STIC-574 Anexo A Internet Information Services 10 - Categoría Alta / Difusión Limitada.

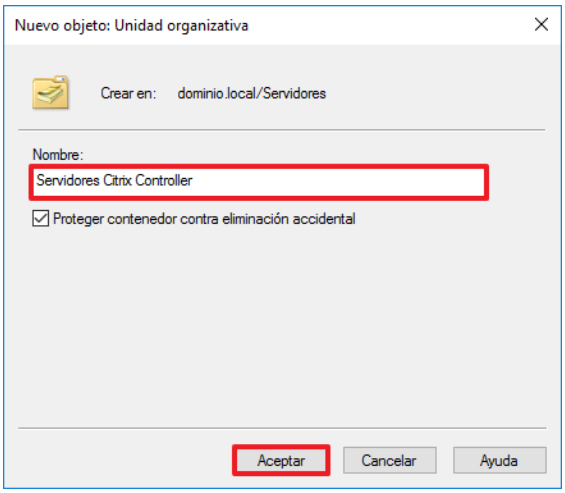
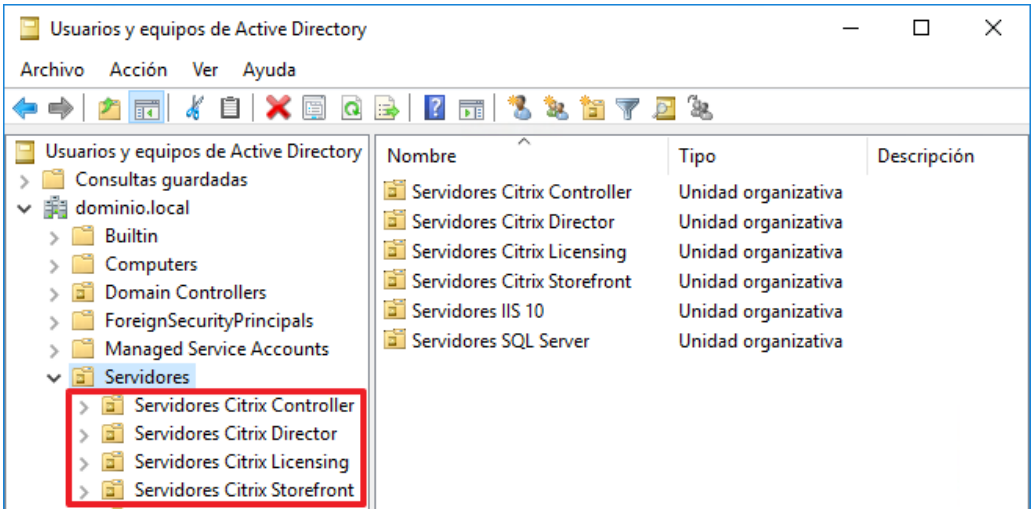
Nota: Las guías “CCN-STIC-575” y “CCN-STIC-574” deberán aplicarse en este servidor exclusivamente su apartado correspondiente al controlador de dominio.

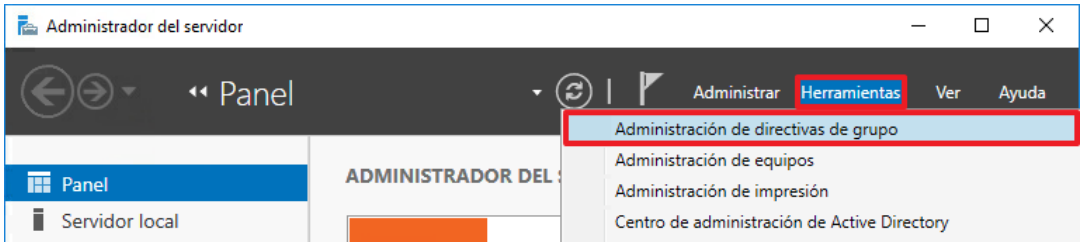
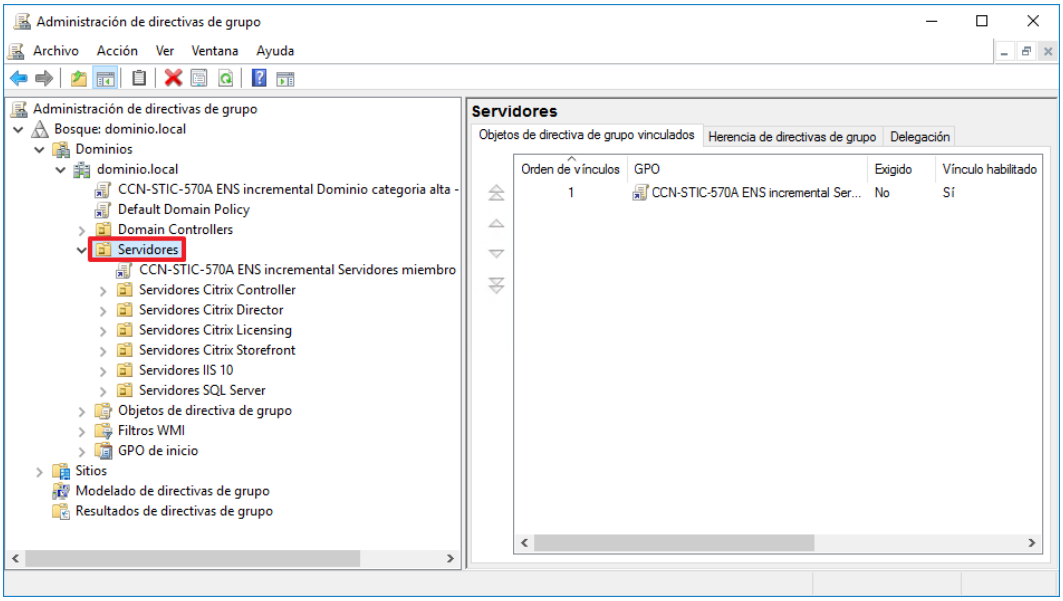
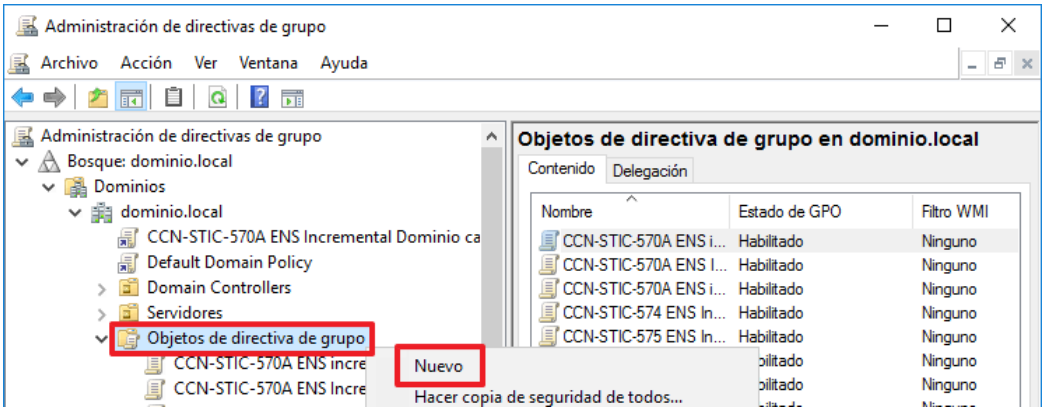
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los ficheros y directorios que acompañan a esta guía, al 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. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

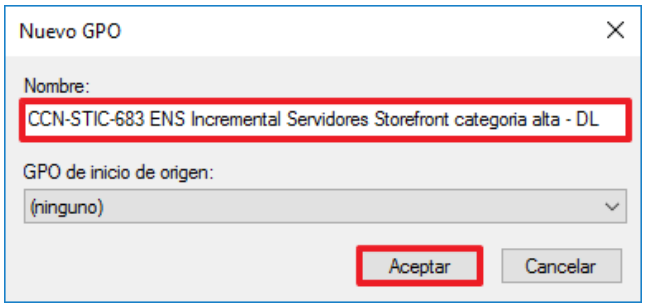
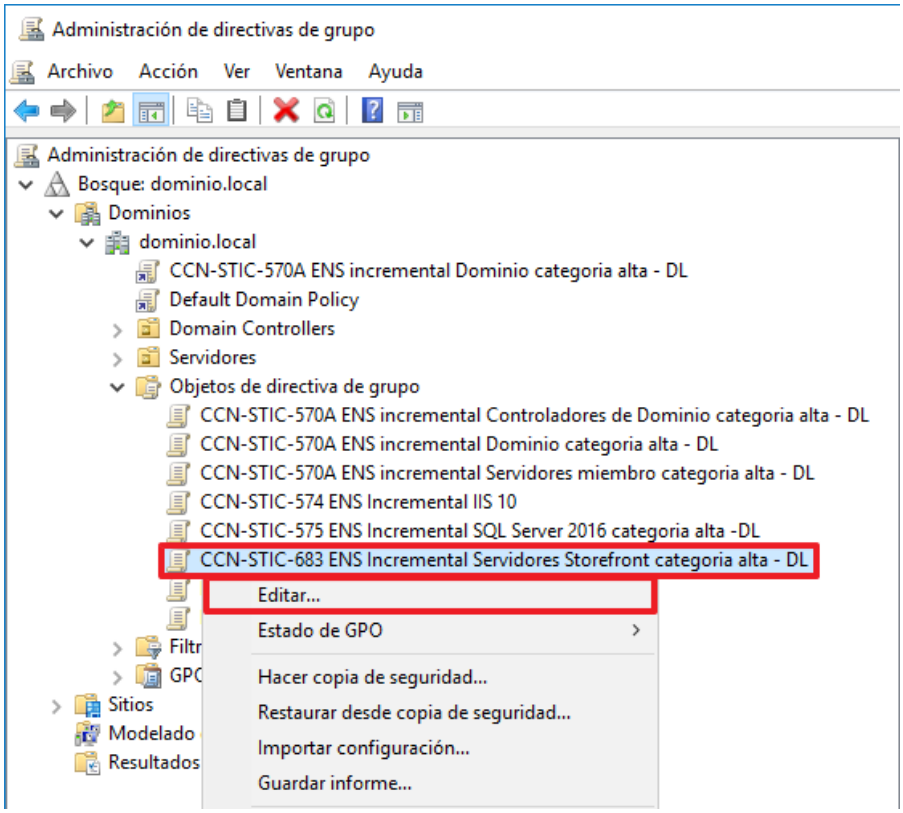
Paso	Descripción
5.	Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-683 ENS categoria alta-DL - Preparacion del dominio - Paso 1.bat – CCN-STIC-683 ENS Incremental Citrix Controller categoria alta-DL.inf – CCN-STIC-683 ENS Incremental Citrix Director categoria alta-DL.inf – CCN-STIC-683 ENS Incremental Citrix Licensing categoria alta-DL.inf – CCN-STIC-683 ENS Incremental Citrix Storefront categoria alta-DL.inf
6.	Ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-683 ENS categoria alta-DL - Preparacion del dominio – Paso 1.bat". Para ello, visualice la carpeta "C:\Scripts" en el Explorador de Windows, marque con el botón derecho el script y seleccione la opción **"Ejecutar como administrador"** del menú contextual, como se muestra en la siguiente figura.  **Nota:** Aunque la sesión se haya iniciado con un usuario administrador, es imprescindible utilizar la opción "Ejecutar como administrador" para que el script se ejecute efectivamente con privilegios de administrador.
7.	El control de cuentas de usuario solicitará elevación de privilegios, introduzca las credenciales de un usuario con permisos de administrador. 

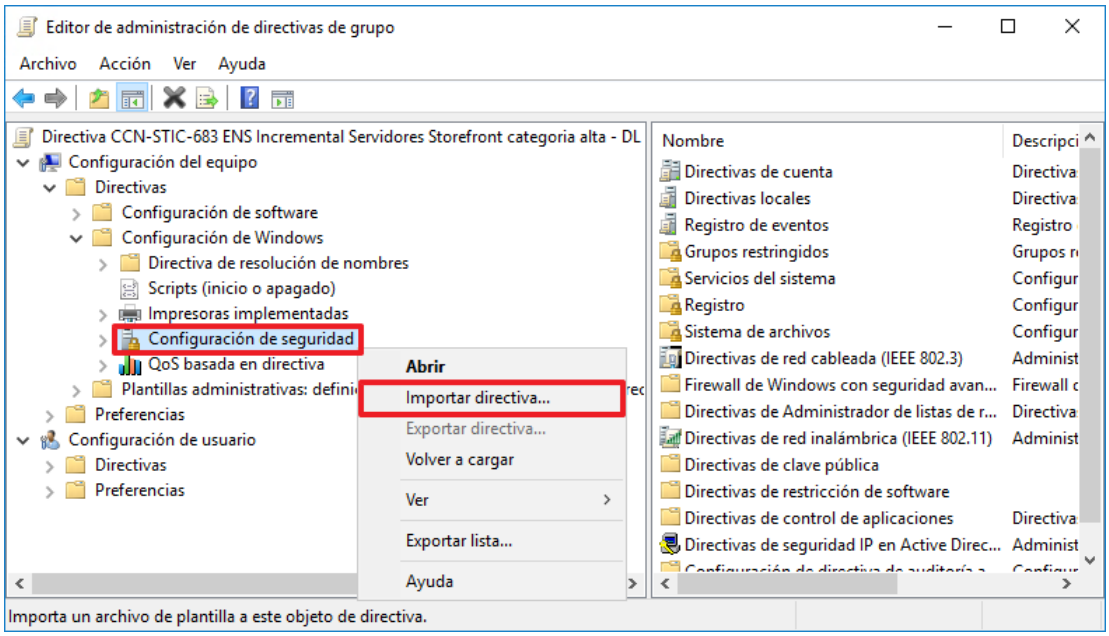
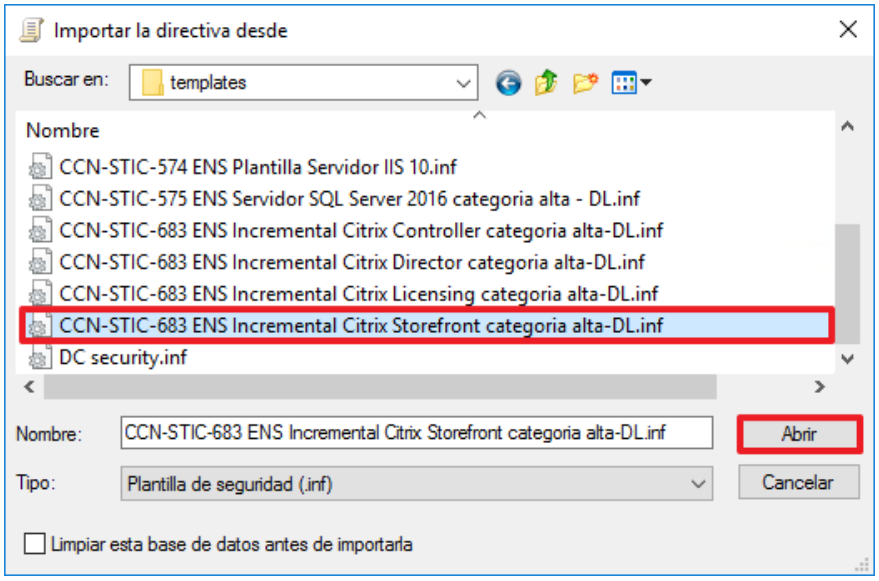
Paso	Descripción
8.	Se lanzará una ventana del intérprete de comandos “cmd.exe” como la mostrada en la siguiente figura. Este script copia todas las plantillas de seguridad a la ubicación “C:\Windows\security\templates” y crea el grupo de seguridad “Administradores de Citrix” en caso de que este no exista. 
9.	Pulse una tecla al finalizar la ejecución del script para cerrar la ventana. 

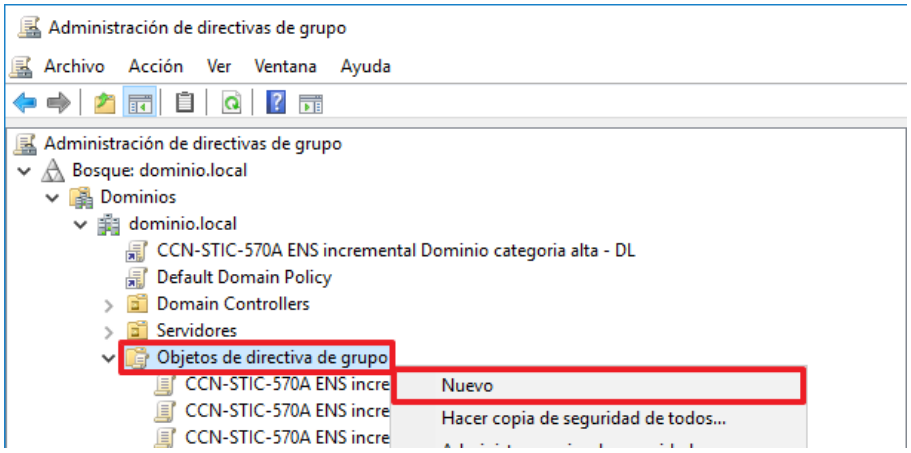
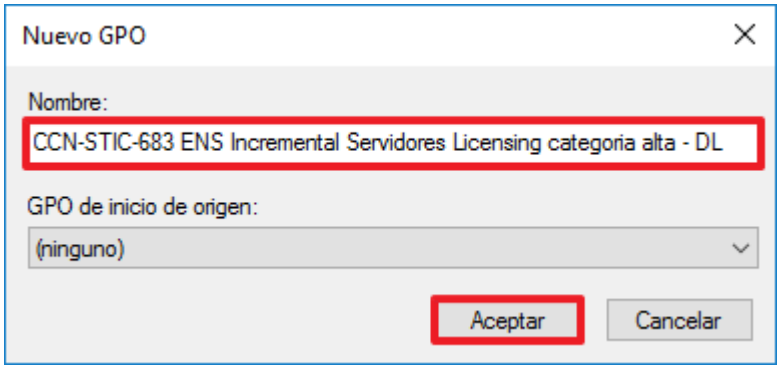
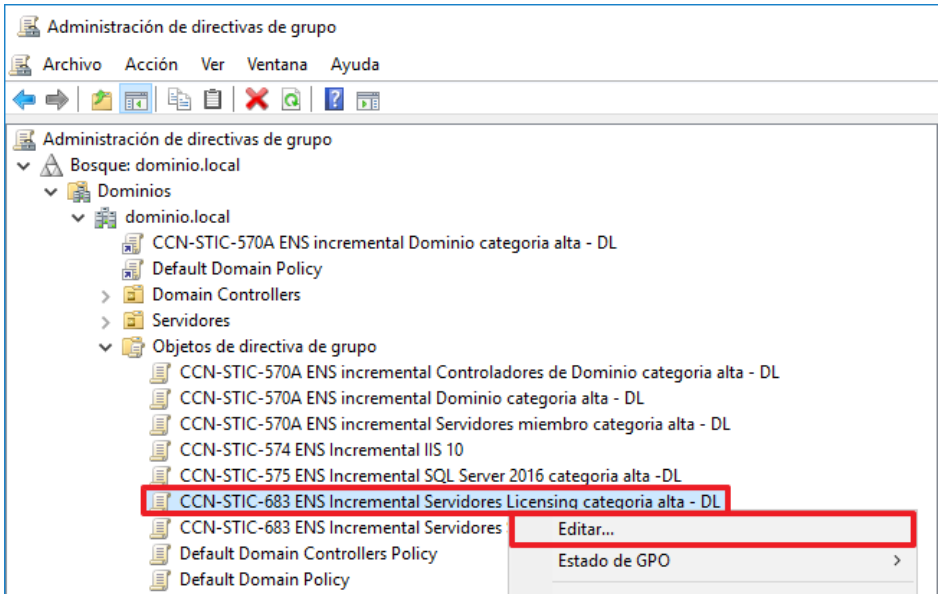
Paso	Descripción
10.	Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios. 
11.	A continuación, en la herramienta "Usuarios y equipos de Active Directory" expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio>" → Servidores"**, y marcándolo con el botón derecho del ratón, seleccione la opción **"Nuevo → Unidad organizativa"** del menú contextual que aparecerá, como se muestra en la siguiente figura. 

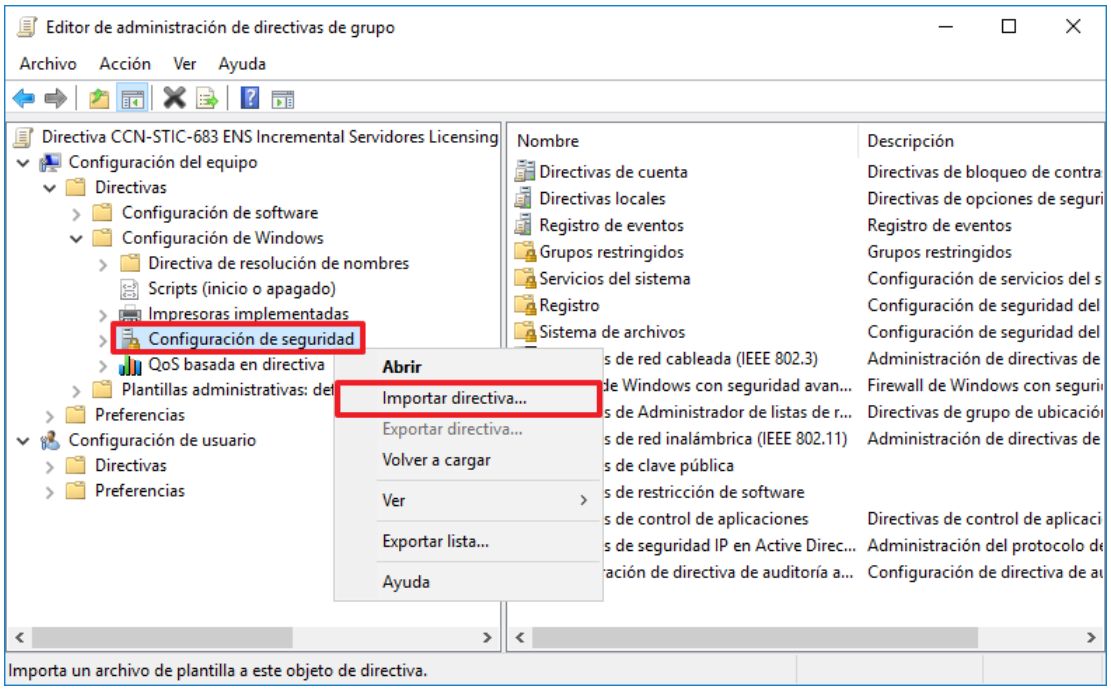
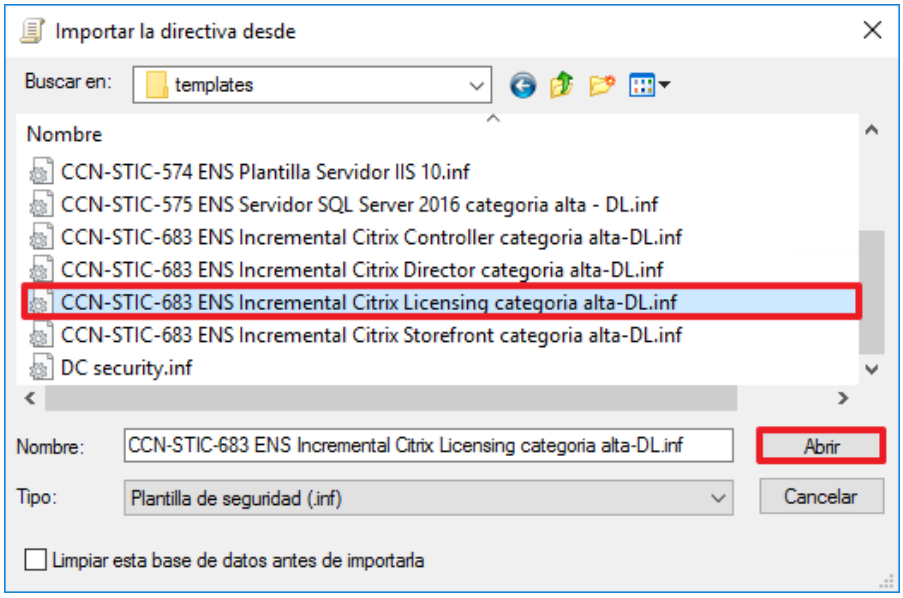
Paso	Descripción
12.	En la ventana resultante, introduzca como nombre de la nueva unidad organizativa “Servidores Citrix Controller” tal y como muestra en la imagen. No desmarque la opción “Proteger contenedores contra eliminación accidental”. Pulse “Aceptar” para crear el nuevo objeto. 
13.	Proceda a crear las siguientes unidades organizativas bajo la unidad organizativa “Servidores”. – Servidores Citrix Controller – Servidores Citrix Storefront – Servidores Citrix Licensing – Servidores Citrix Director
14.	Las nuevas unidades organizativas, aparecerán colgando de “Servidores”, como se muestra en la siguiente figura.  **Nota:** Las unidades organizativas “Servidores IIS 10” y “Servidores SQL Server” deberán haberse creado durante la aplicación de las guías de seguridad codificadas como “CCN-STIC-574” y CCN-STIC-575”.

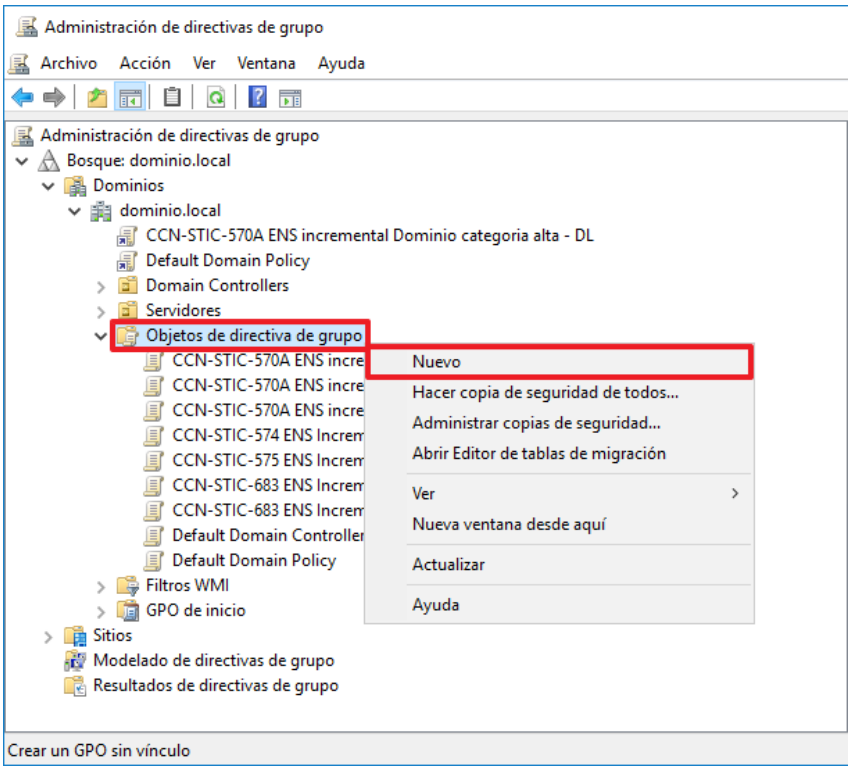
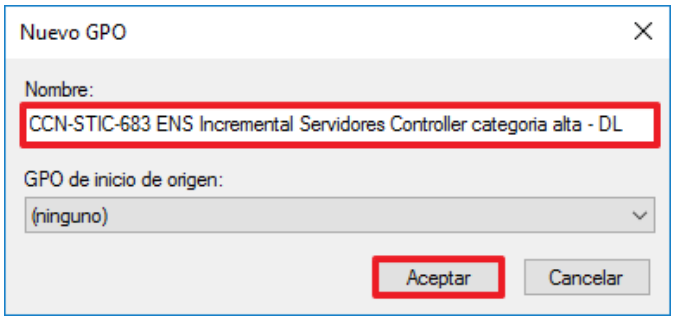
Paso	Descripción
15.	Utilice la herramienta "Administración de Directivas de grupo" (**Administrador del servidor → Herramientas → Administración de Directivas de grupo**). El sistema solicitará elevación de privilegios. 
16.	Expanda el contenedor **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores"**, como se muestra en la siguiente figura. 
17.	A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar la GPO correspondiente. Hasta que se indique lo contrario, los contenedores a los que se hará referencia serán subcontenedores del contenedor recién expandido "Servidores".
18.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 

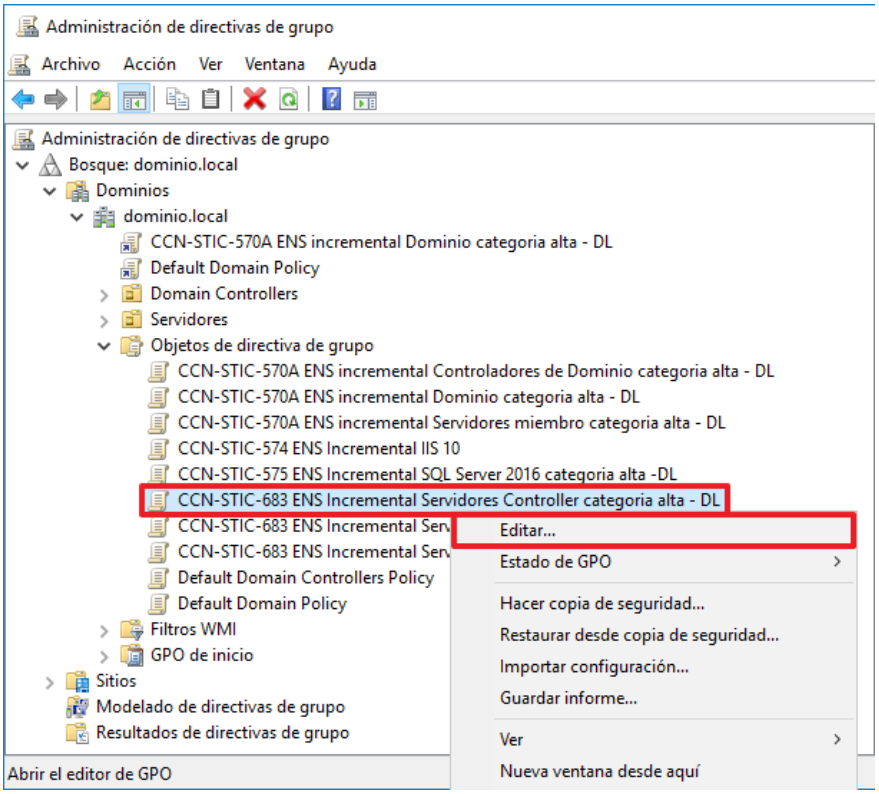
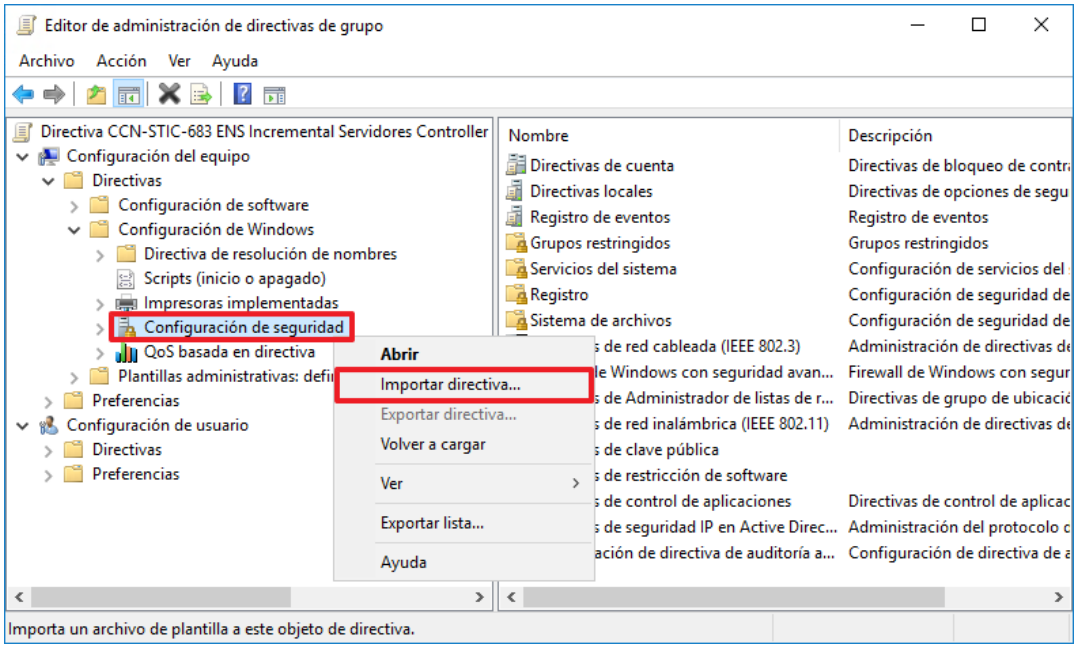
Paso	Descripción
19.	Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL" y pulse el botón “Aceptar”. 
20.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 

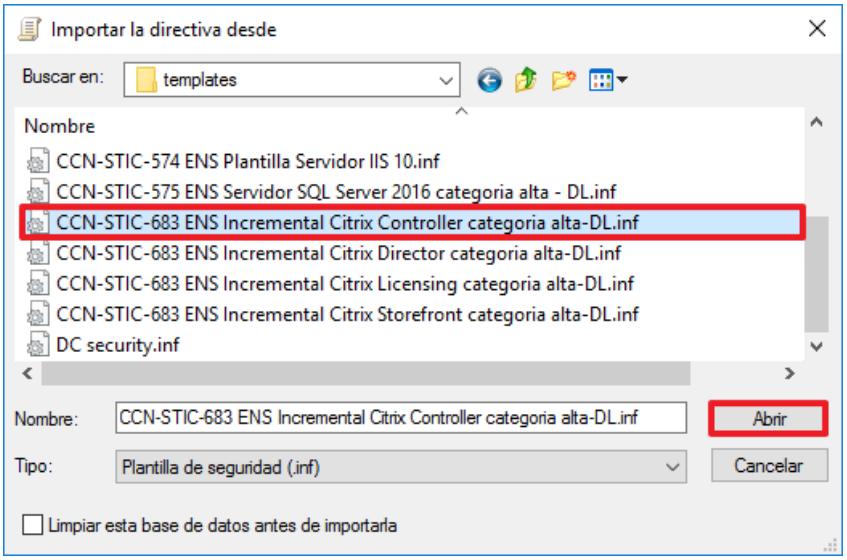
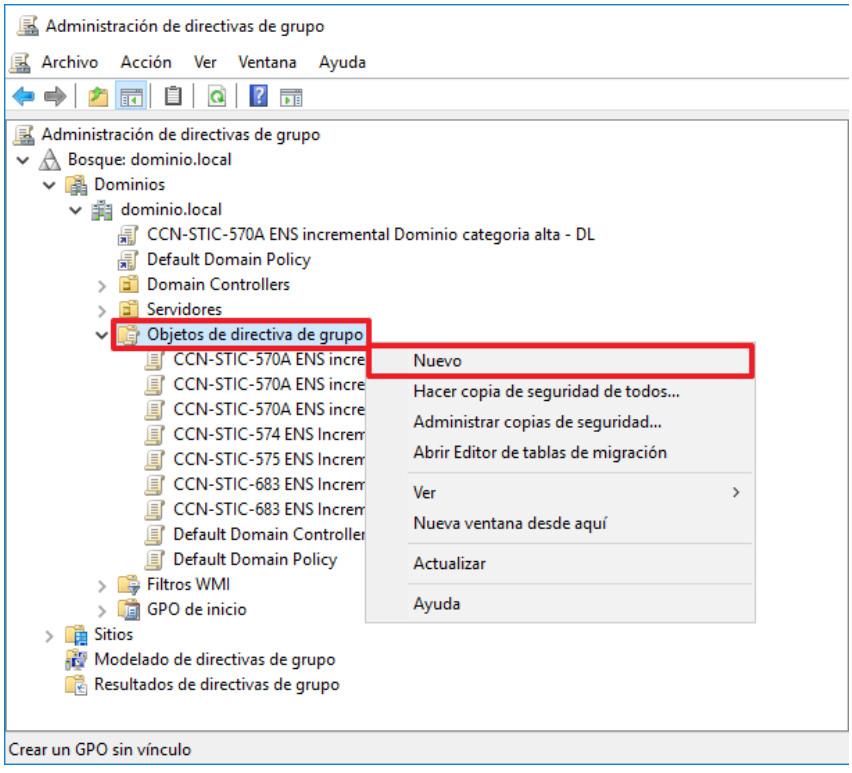
Paso	Descripción
21.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 
22.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Storefront categoria alta-DL.inf" y pulse el botón "Abrir". 
23.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

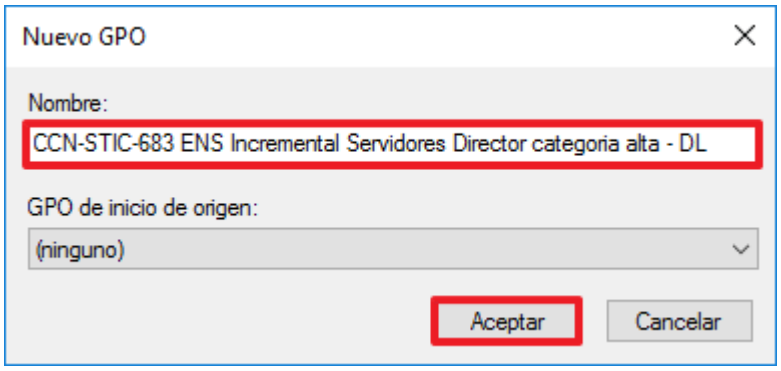
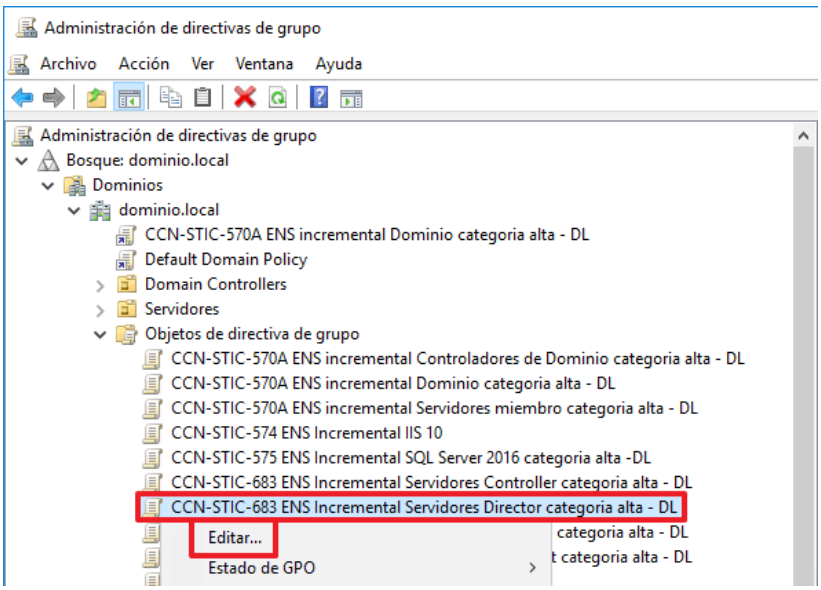
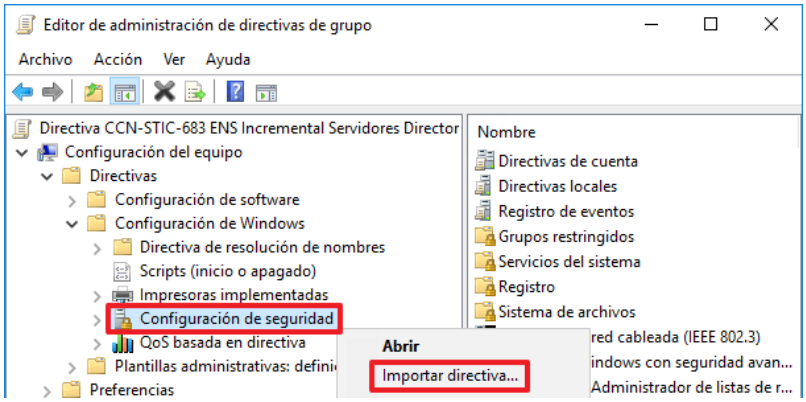
Paso	Descripción
24.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
25.	Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL" y pulse el botón “Aceptar”. 
26.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá. 

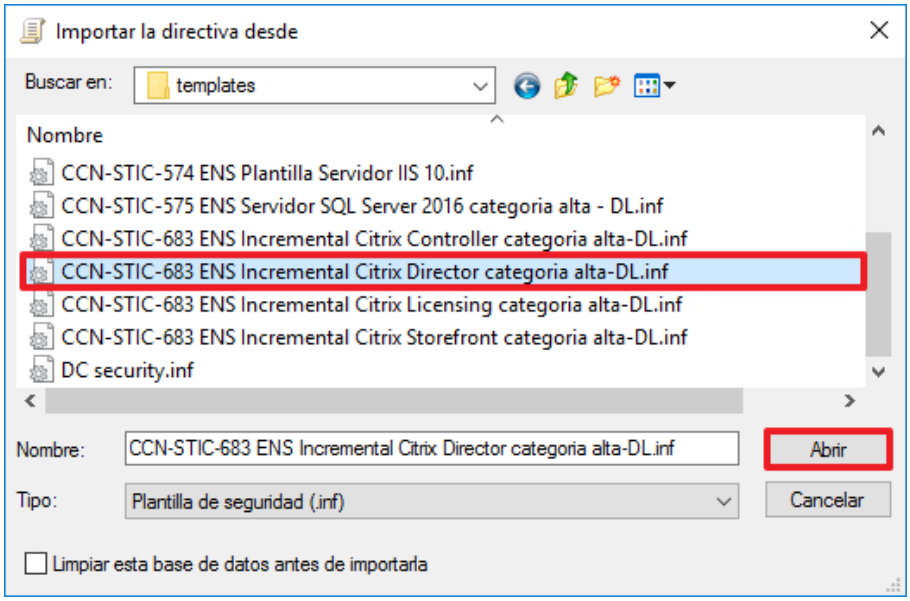
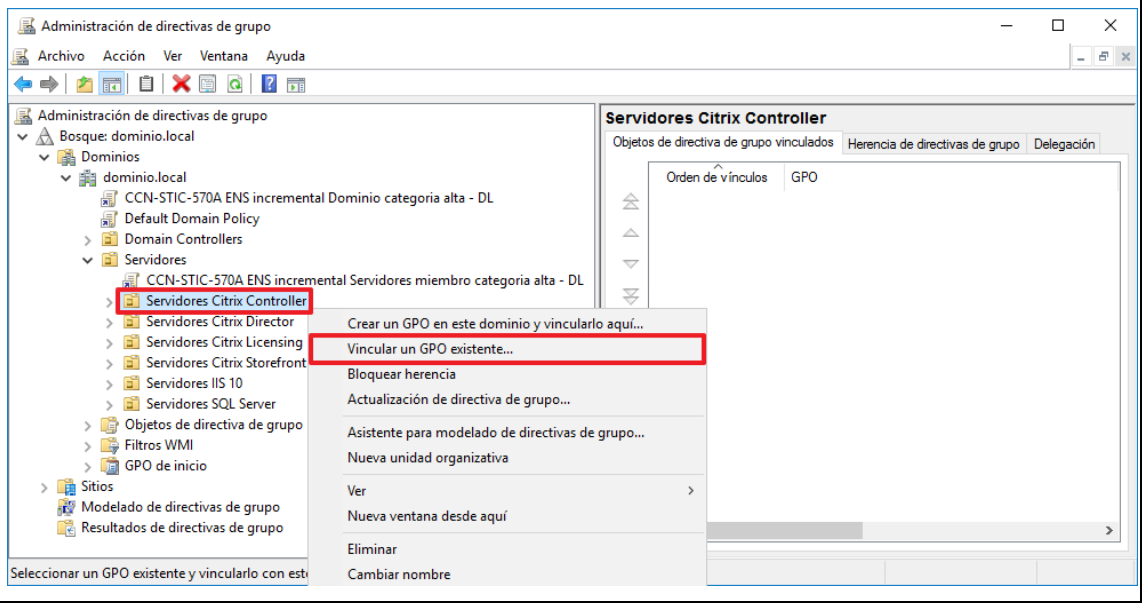
Paso	Descripción
27.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 
28.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Licensing categoria alta-DL.inf" y pulse el botón "Abrir". 

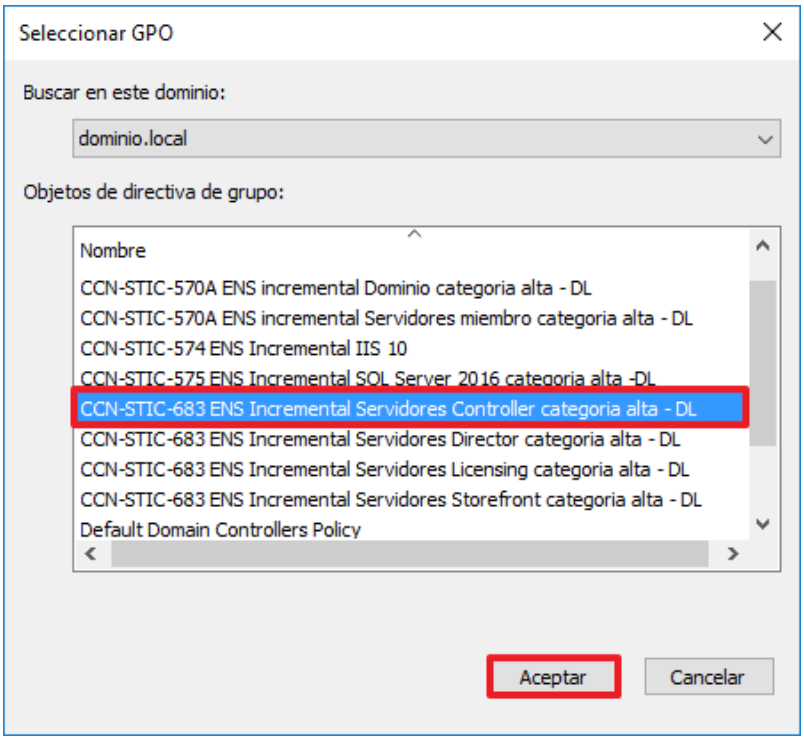
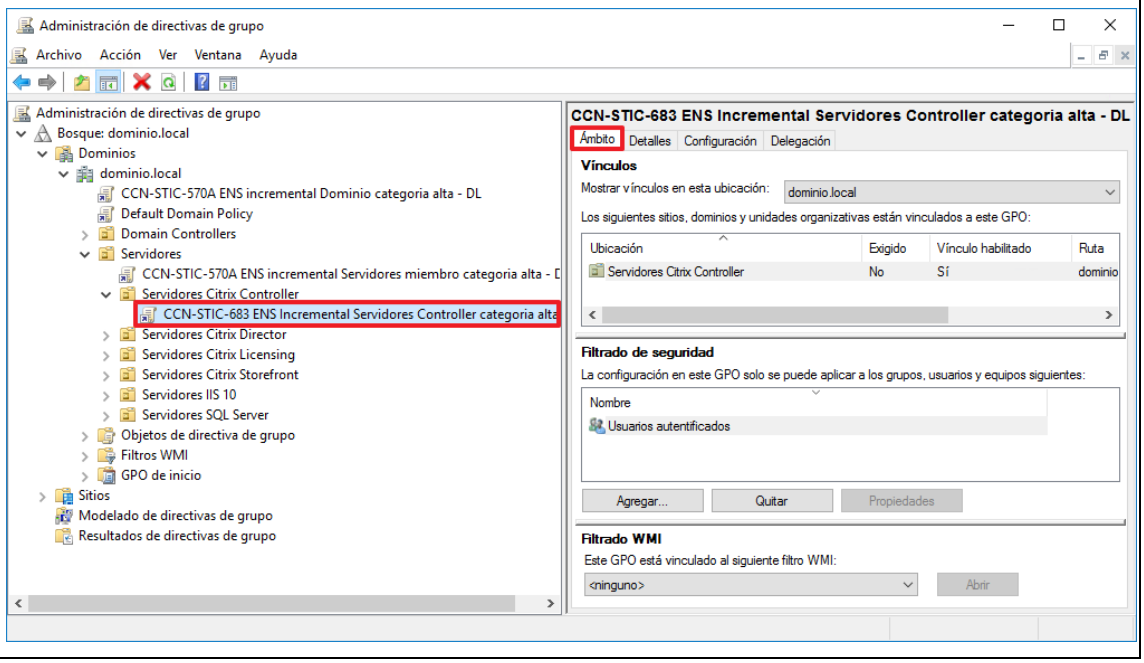
Paso	Descripción
29.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
30.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 
31.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL" y pulse el botón “Aceptar”. 

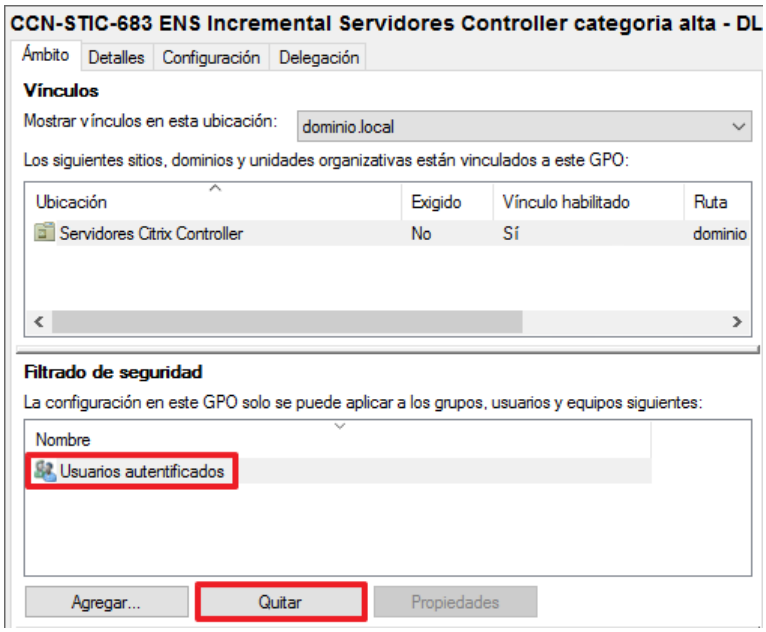
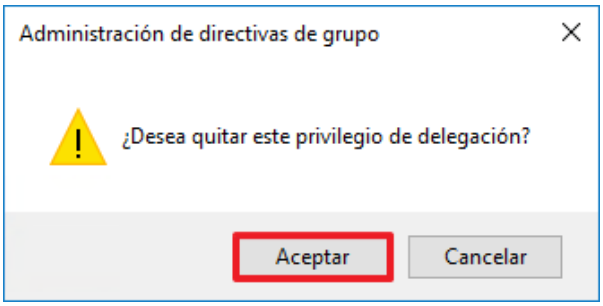
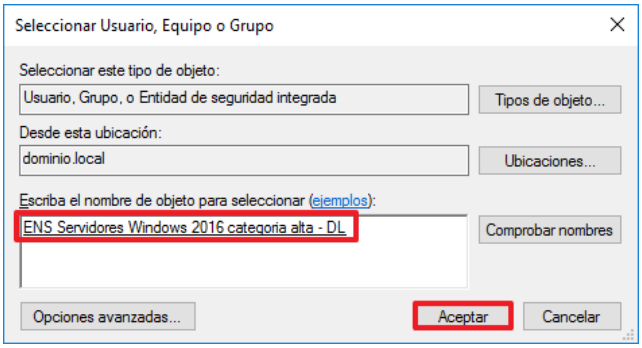
Paso	Descripción
32.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 
33.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 

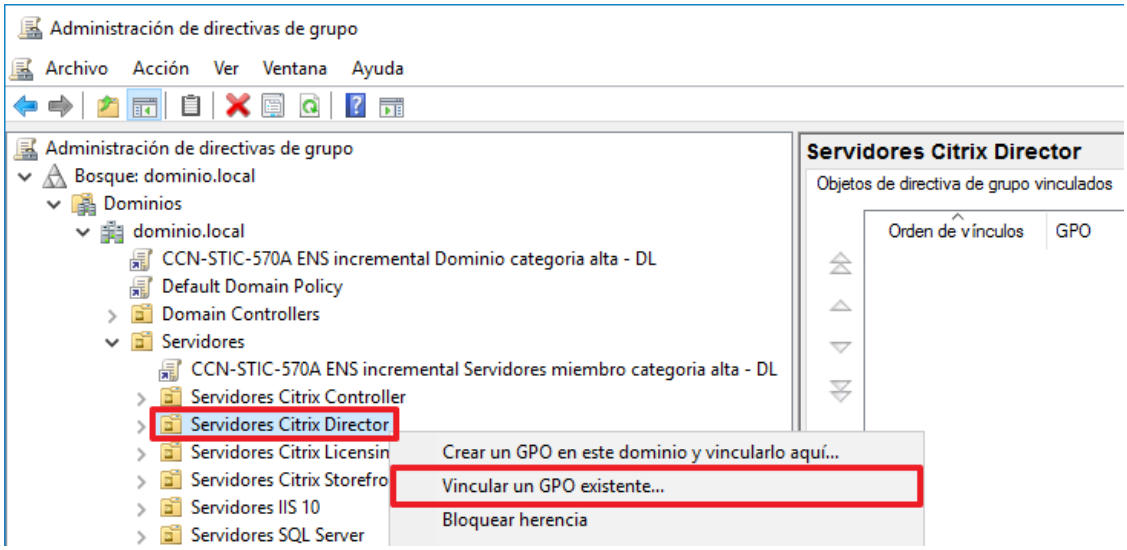
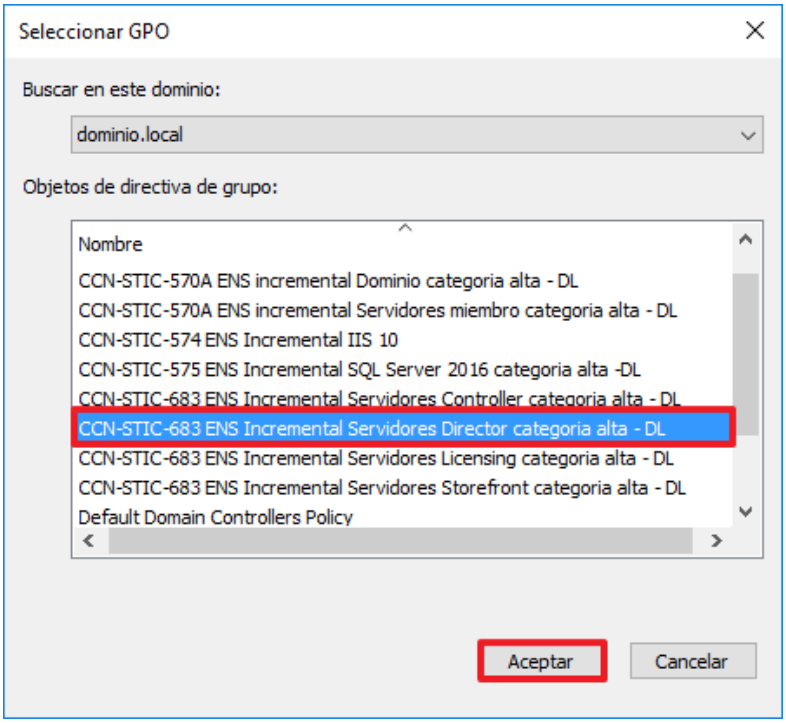
Paso	Descripción
34.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Controller categoria alta-DL.inf" y pulse el botón "Abrir". 
35.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
36.	Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá. 

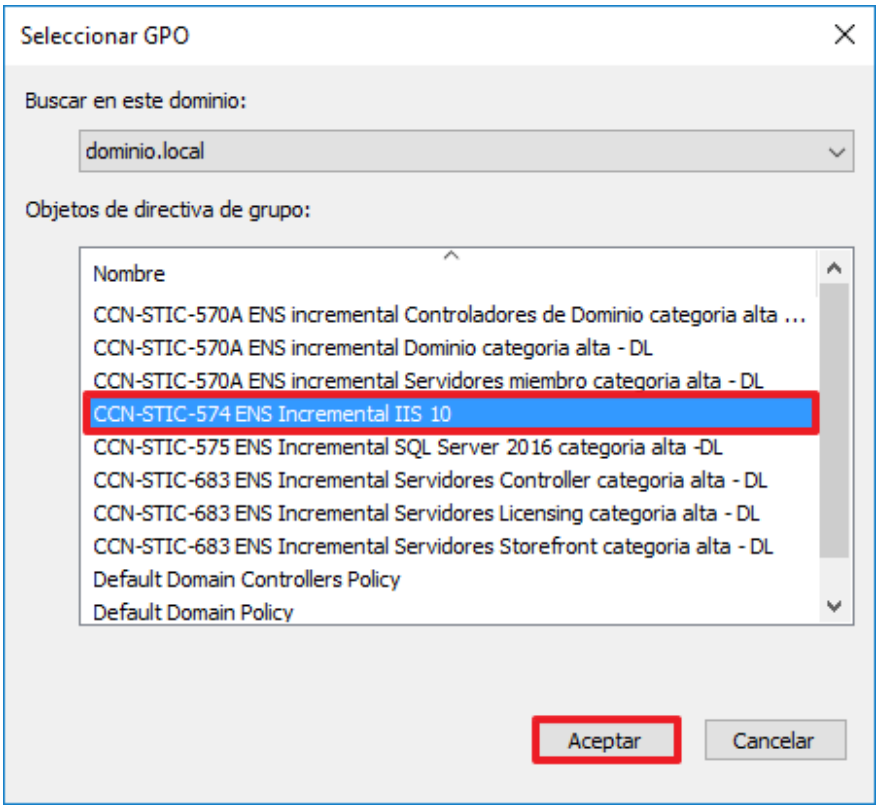
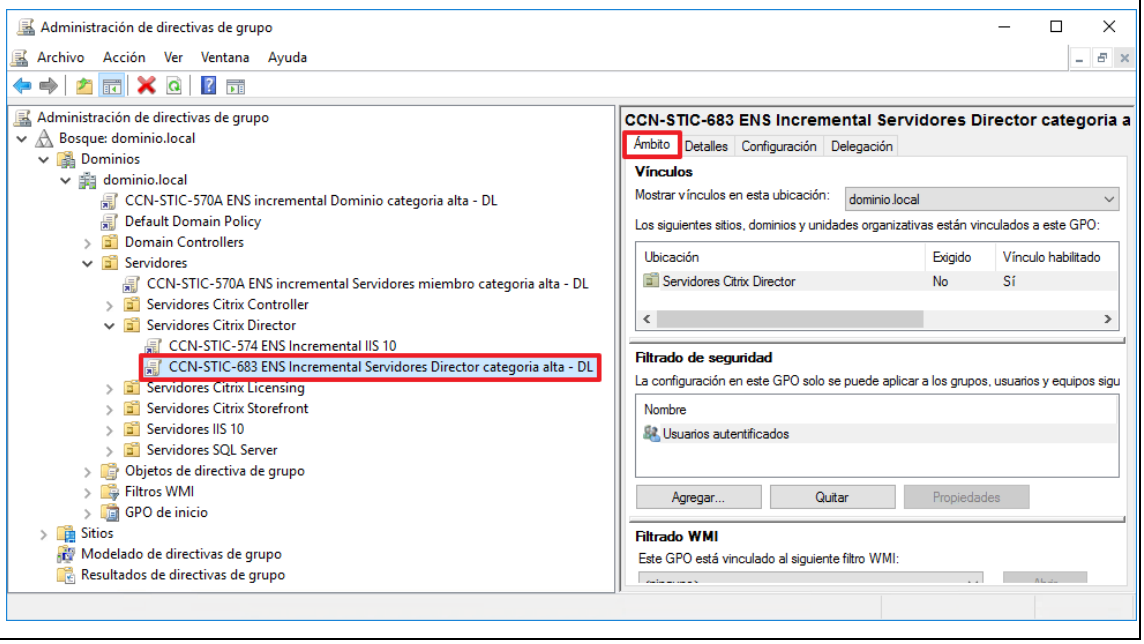
Paso	Descripción
37.	Asigne el siguiente nombre al nuevo GPO "CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL" y pulse el botón “Aceptar”. 
38.	Seleccione el GPO recién creado, "CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá. 
39.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta. **“Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad”**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá. 

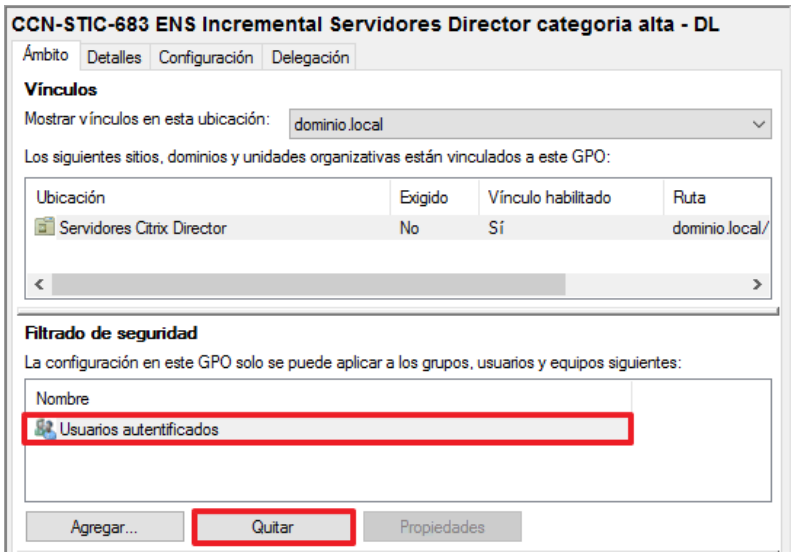
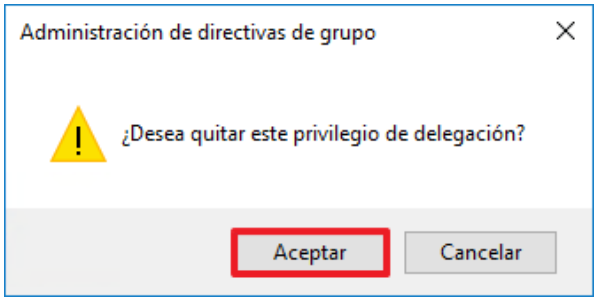
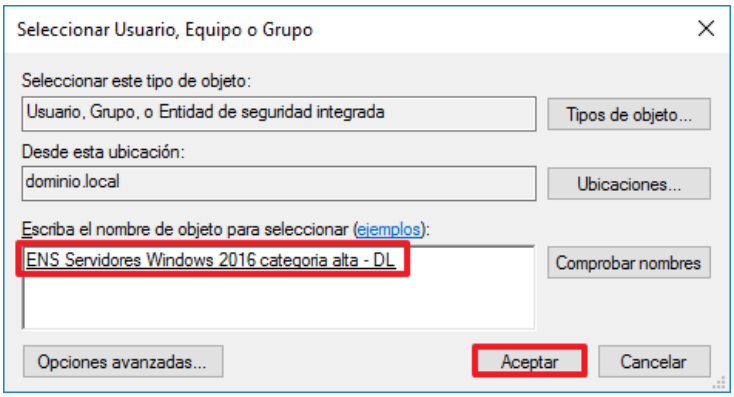
Paso	Descripción
40.	En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-683 ENS Incremental Citrix Director categoria alta-DL.inf" y pulse el botón "Abrir". 
41.	Con ello este GPO ("CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
42.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Controller”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 

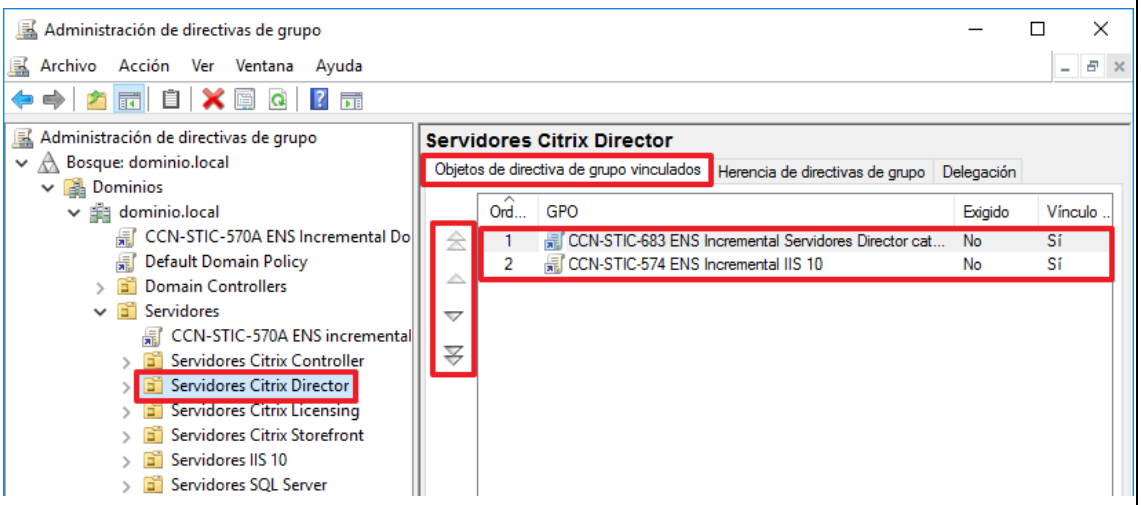
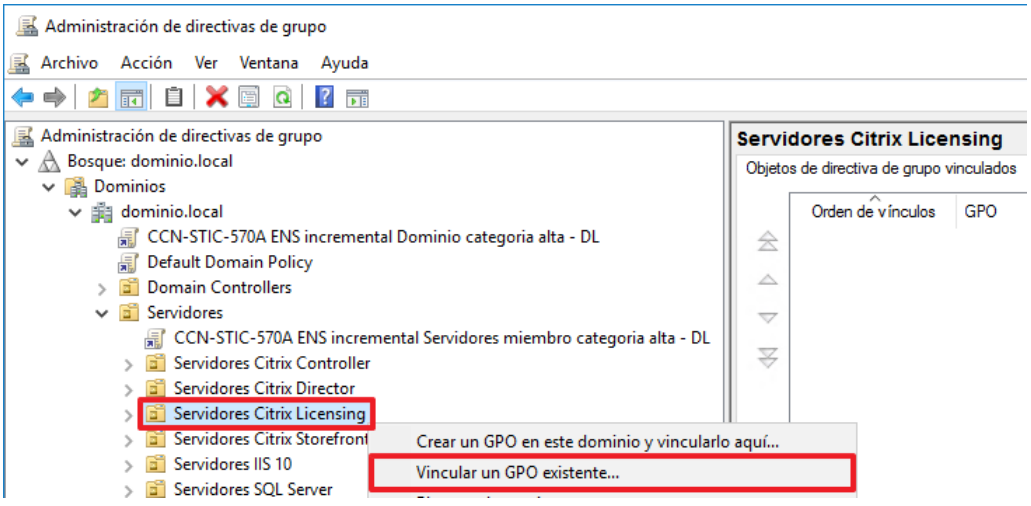
Paso	Descripción
43.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL”. 
44.	Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

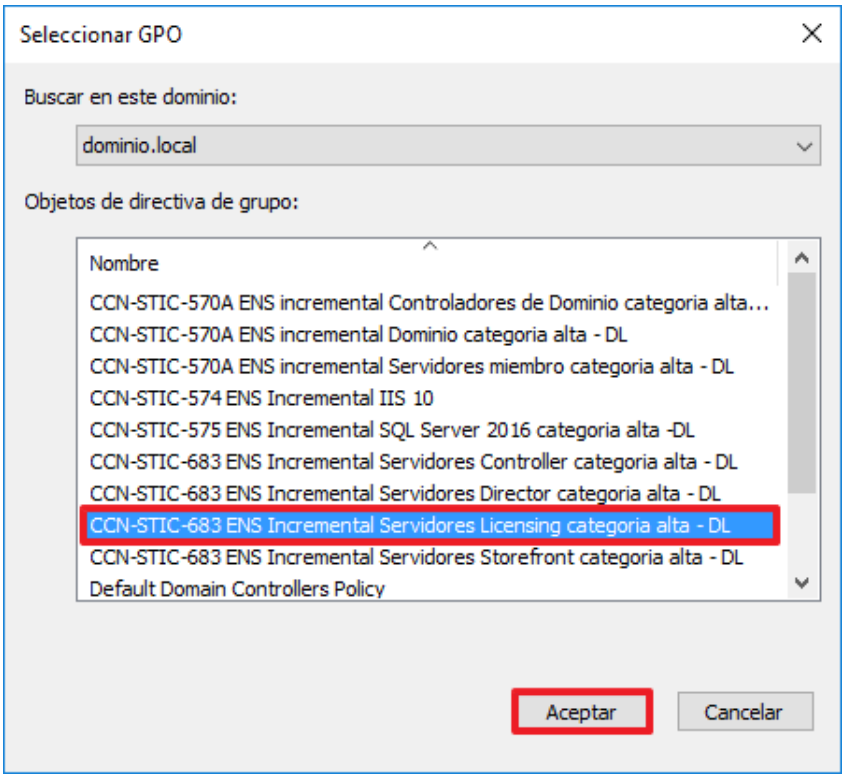
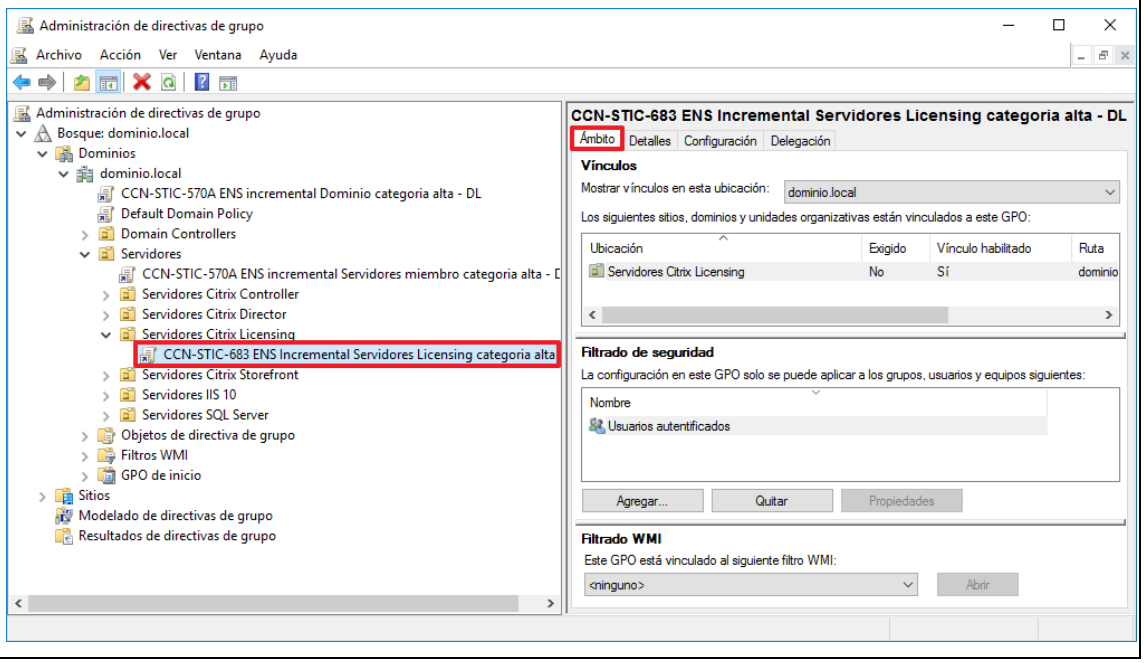
Paso	Descripción
45.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
46.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
47.	Una vez quitado, pulse el botón “Agregar…”.
48.	Introduzca como nombre “ENS servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

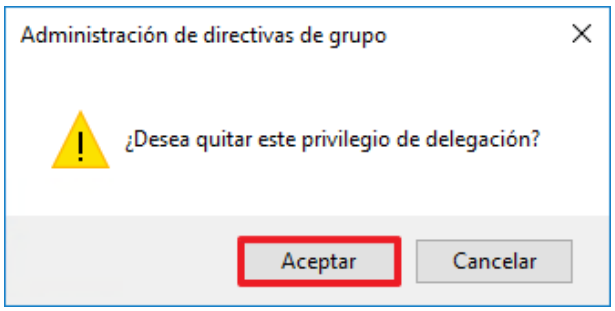
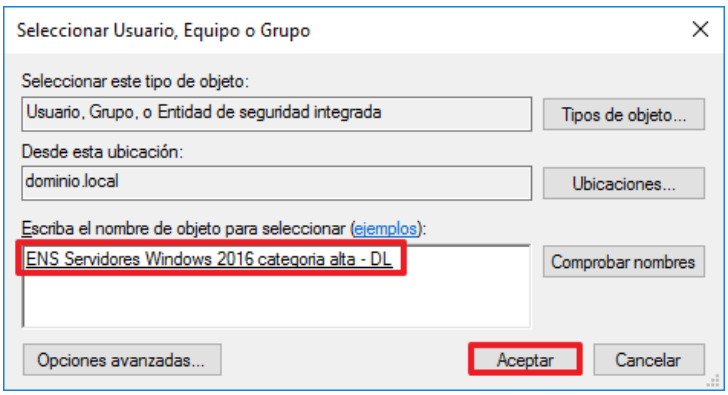
Paso	Descripción
49.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Director”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 
50.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL”. 

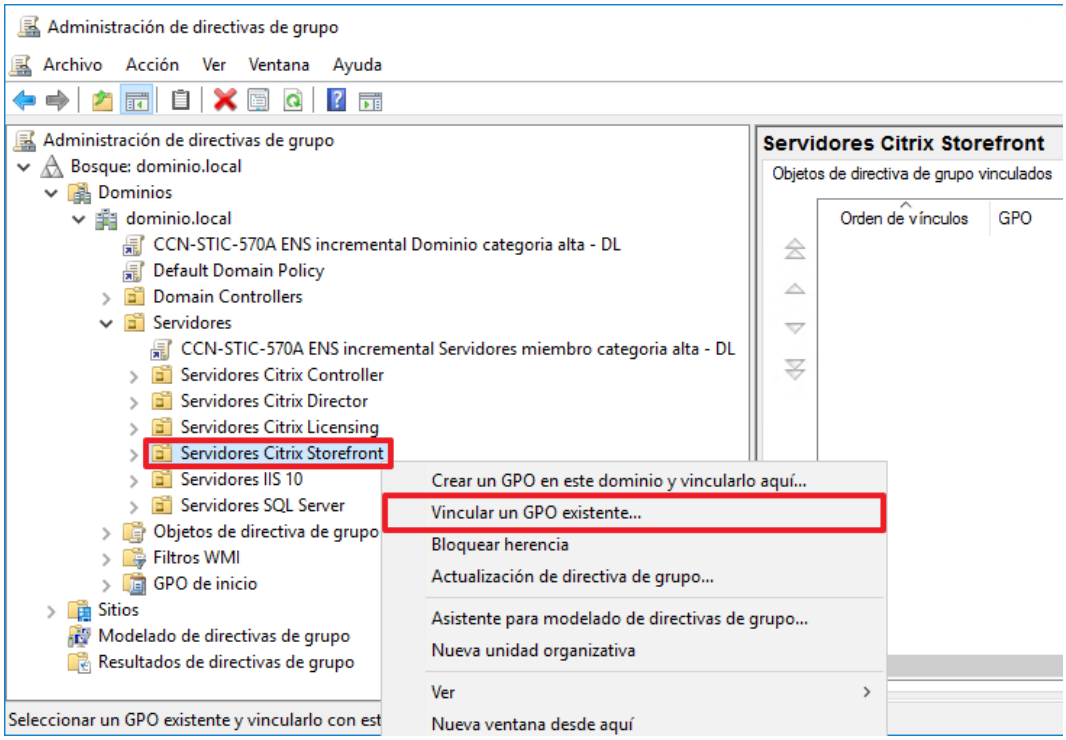
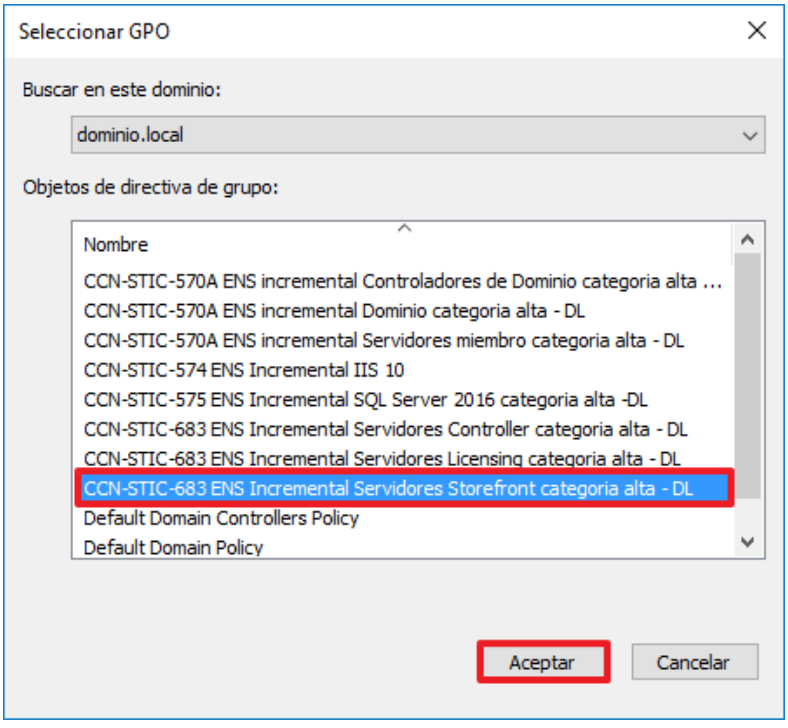
Paso	Descripción
51.	Repita el mismo proceso para vincular el GPO “CCN-STIC-574 ENS Incremental IIS 10”. 
52.	Seleccione la política de grupo “CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

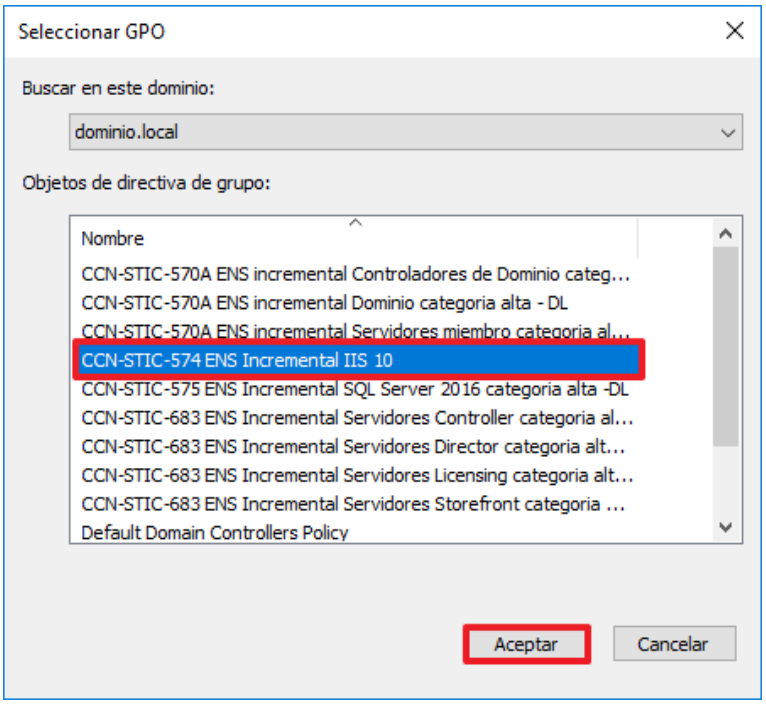
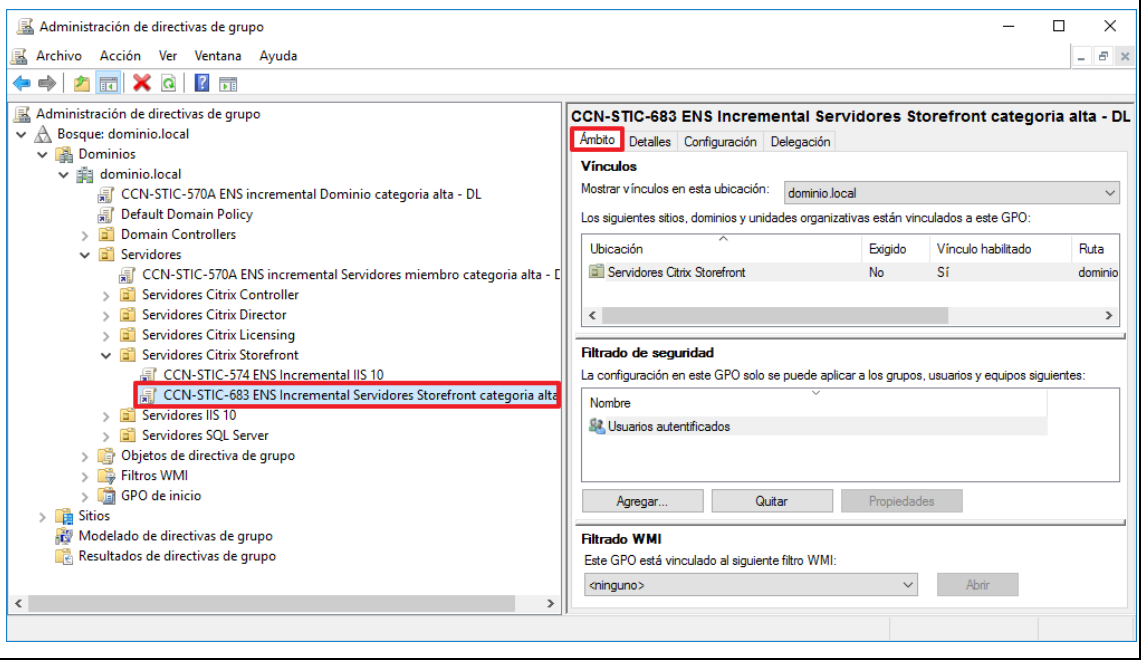
Paso	Descripción
53.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
54.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
55.	Una vez quitado, pulse el botón “Agregar…”.
56.	Introduzca como nombre “ENS servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

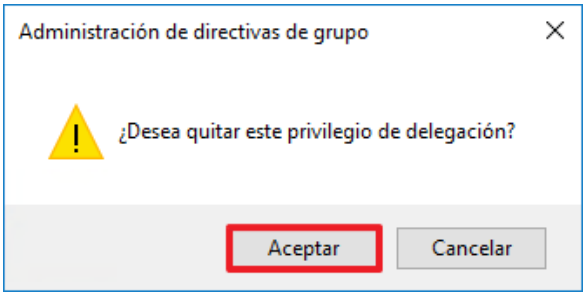
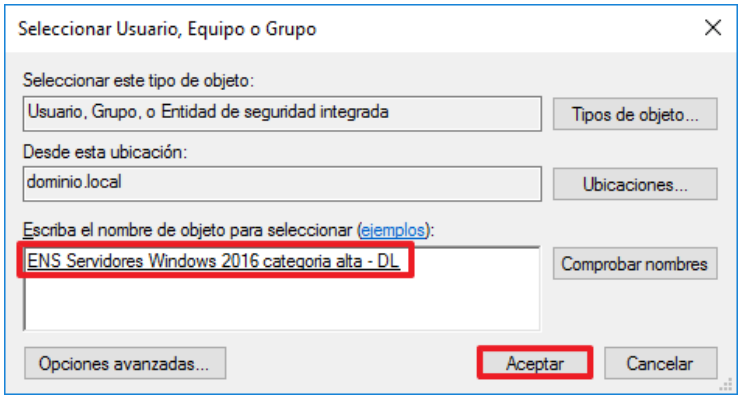
Paso	Descripción
57.	Seleccione el contenedor “Servidores Citrix Director” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura. – 1 - CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL – 2 - CCN-STIC-574 ENS Incremental IIS 10 Si no lo es, modifique el orden de los vínculos para que sea igual al indicado. Para ello seleccione un vínculo y utilice las flechas hacia arriba y hacia abajo que hay en la parte izquierda de la pestaña. 
58.	Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá.
59.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Licensing”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 

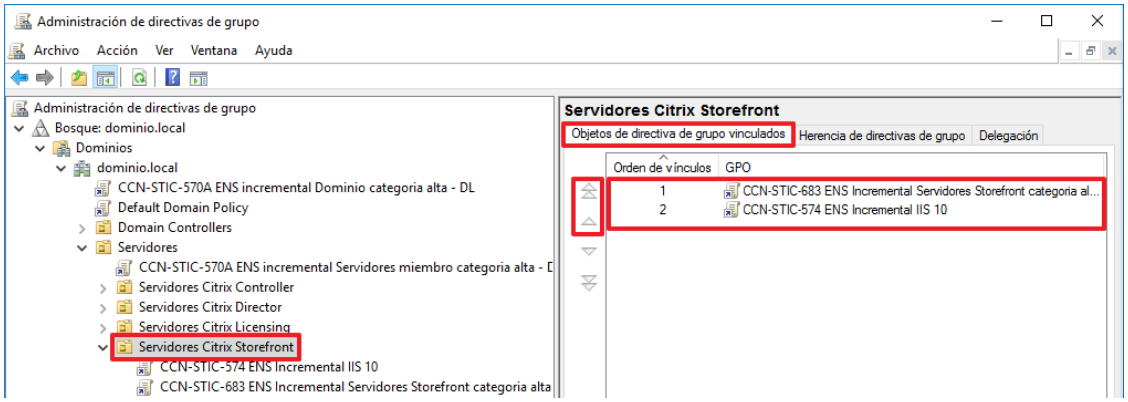
Paso	Descripción
60.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL”. 
61.	Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
62.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
63.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
64.	Una vez quitado, pulse el botón “Agregar…”.
65.	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”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

Paso	Descripción
66.	En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **"Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Storefront”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá. 
67.	En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL”. 

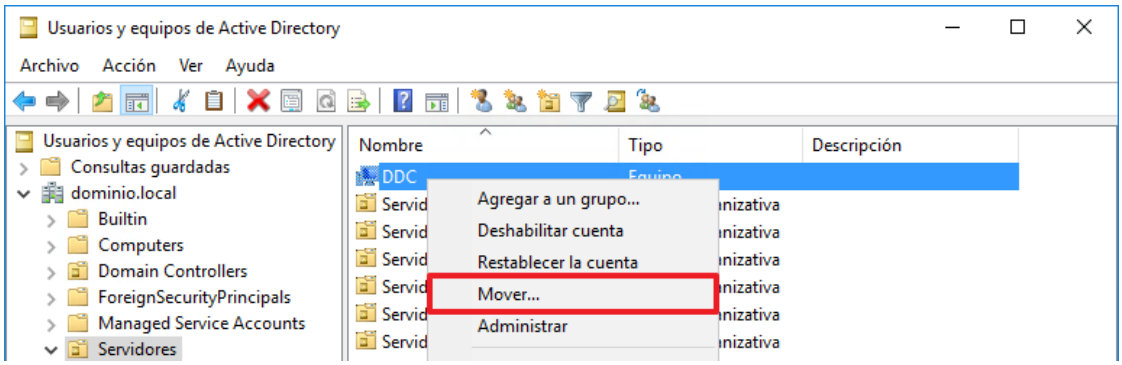
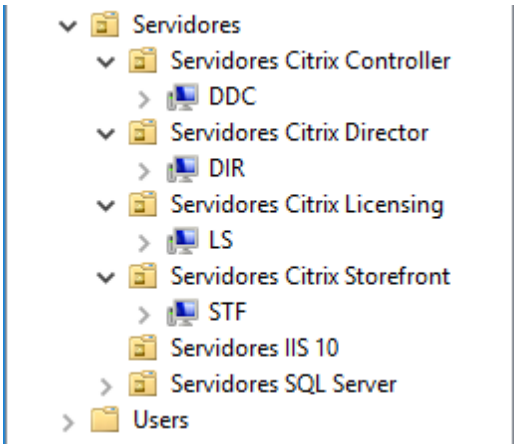
Paso	Descripción
68.	De manera análoga vincule la GPO denominada “CCN-STIC-574 ENS Incremental Servidores IIS 10”. 
69.	Seleccione la política de grupo “CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. 

Paso	Descripción
70.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
71.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
72.	Una vez quitado, pulse el botón “Agregar…”.
73.	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”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización.

Paso	Descripción
74.	Seleccione el contenedor “Servidores Citrix Storefront” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura. – 1 - CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL – 2 - CCN-STIC-574 ENS Incremental IIS 10 Si no lo es, modifique el orden de los vínculos para que sea igual al indicado. Para ello seleccione un vínculo y utilice las flechas hacia arriba y hacia abajo que hay en la parte izquierda de la pestaña. 
75.	Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá.

En este punto los GPOs se encuentran configurados correctamente en Active Directory y su configuración se aplicará automáticamente a los nuevos servidores que necesite añadir a la infraestructura. En pasos posteriores moverá cada uno de los objetos de equipo dentro de sus correspondientes unidades organizativas.

Paso	Descripción
76.	Si no lo ha hecho todavía, inicie sesión en un servidor controlador de dominio del dominio al que va a pertenecer el servidor que va a asegurar, con una cuenta con derechos de administración en el dominio.
77.	Mueva las cuentas de equipo de cada uno de los roles que haya aprovisionado previamente para la implementación de la infraestructura de Citrix. En función del rol que haya aprovisionado previamente debe mover la cuenta de equipo a una unidad organizativa u otra. La siguiente tabla de referencia puede ayudarle con el proceso. **Nota:** Durante la aplicación de la guía “CCN-STIC-574” habrá situado los servidores correspondientes a los roles de Citrix Storefront y Citrix Director en la Unidad Organizativa “Servidores IIS 10” en este punto deberá mover dichos servidores a las nuevas Unidades Organizativas creadas para cada rol.

<table>
<tr><th>Paso</th><th colspan="3">Descripción</th></tr>
<tr><td></td><td>Rol</td><td>Unidad Organizativa</td><td>Cuenta de equipo</td></tr>
<tr><td></td><td>Citrix Controller</td><td>Servidores Citrix Controller</td><td>DDC</td></tr>
<tr><td></td><td>Citrix Storefront</td><td>Servidores Citrix Storefront</td><td>STF</td></tr>
<tr><td></td><td>Citrix Licensing</td><td>Servidores Citrix Licensing</td><td>LS</td></tr>
<tr><td></td><td>Citrix Director</td><td>Servidores Citrix Director</td><td>DIR</td></tr>
<tr><td>78.</td><td colspan="3">Para ello, abra la herramienta "Administrador del servidor" y despliegue el menú “Herramientas → Usuarios y equipos de Active Directory”. El sistema solicitará elevación de privilegios.
A continuación, en la herramienta “Usuarios y equipos de Active Directory” despliegue la ruta “<nombre de su dominio> → Servidores", y marcando con el botón derecho del ratón cada uno de los servidores, pulse la opción “Mover…”.
 
</td></tr>
<tr><td>79.</td><td colspan="3">De forma análoga, realice el paso anterior por cada uno de los servidores que desee añadir a la plataforma.</td></tr>
<tr><td>80.</td><td colspan="3">Finalmente, dentro de cada unidad organizativa debe apreciar cada uno de los servidores añadidos.
 
</td></tr>
<tr><td>81.</td><td colspan="3">Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor.</td></tr>
</table>

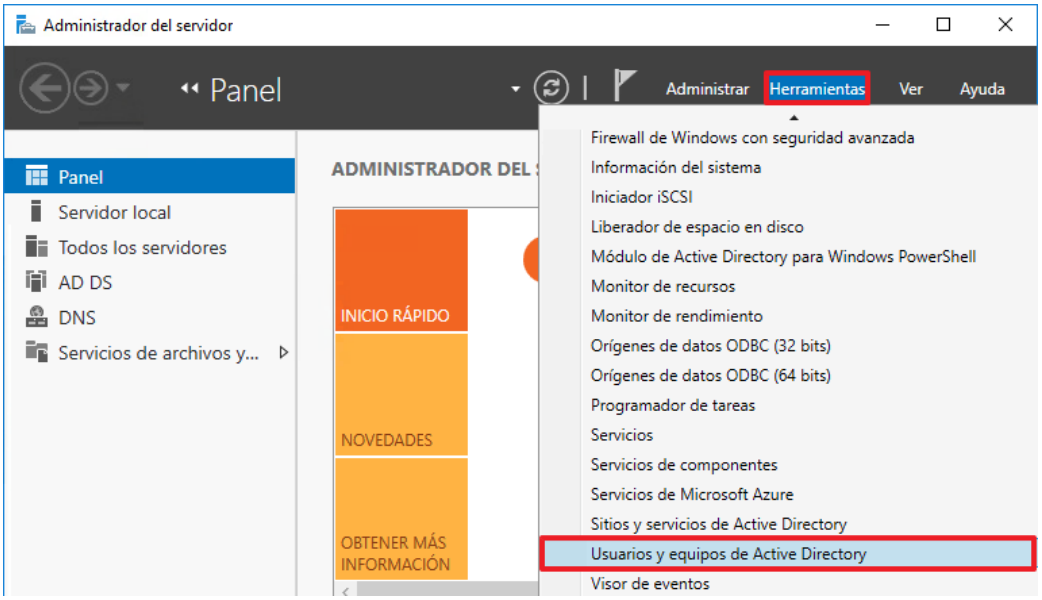
Con la anterior configuración cada uno de los servidores recogerá de forma automática las directivas de grupo configuradas para su rol.

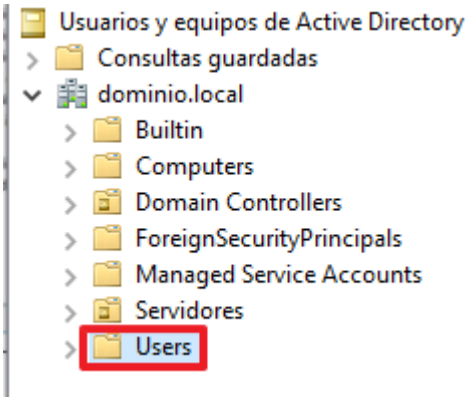
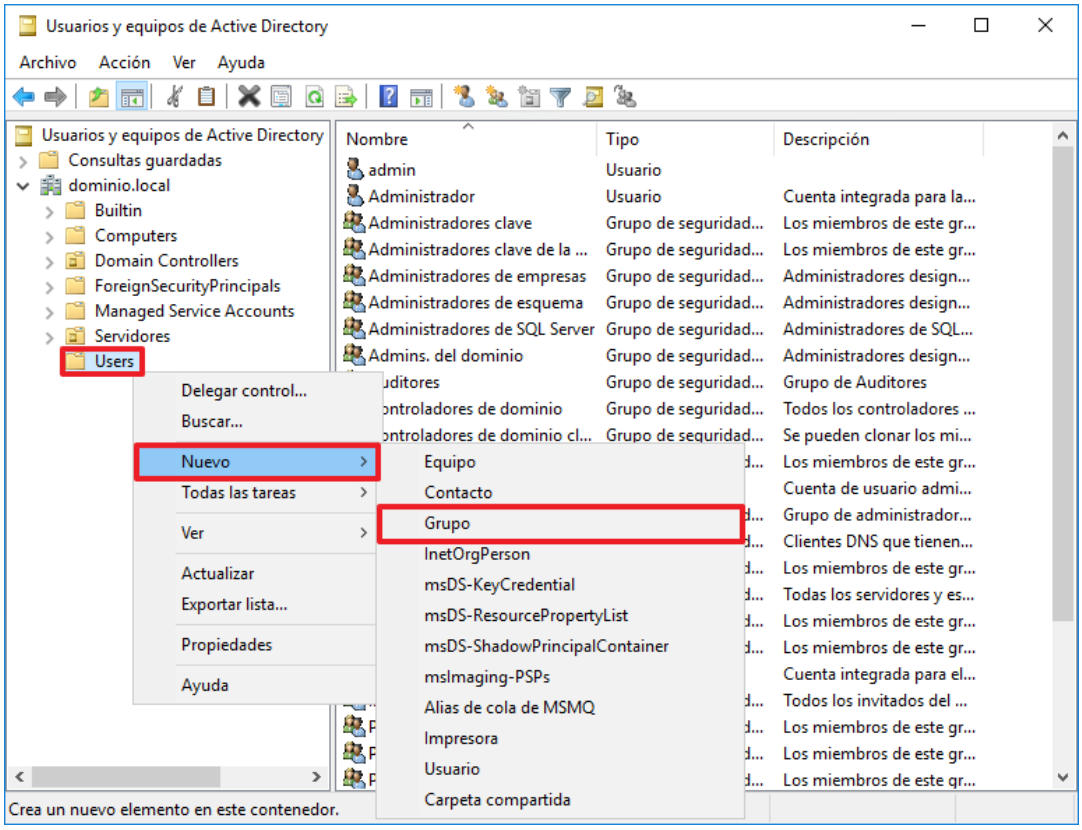
Nota: En el caso de no aplicarse de forma automática la configuración de GPO aplicadas puede utilizar el comando **“gpupdate /force”** para forzar el proceso.

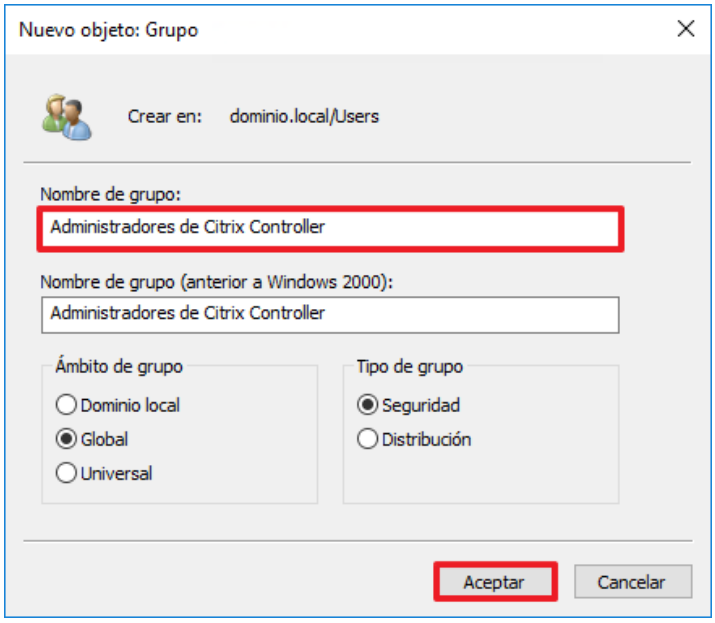
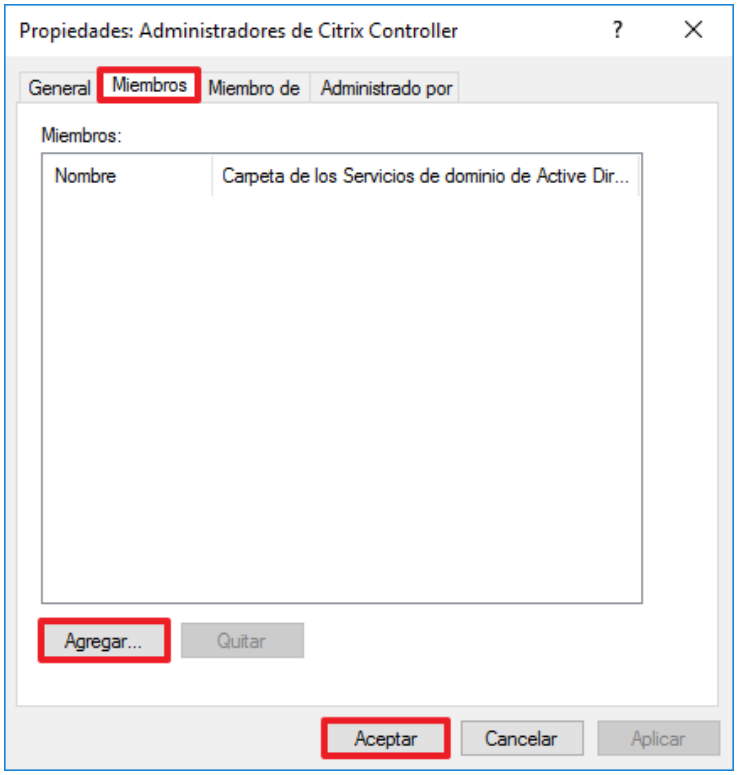
2. SEGREGACIÓN DE ROLES

Con la aplicación del ENS para la categoría alta – DL sobre una infraestructura de Citrix Virtual Apps and Desktops será necesario crear grupos de usuarios para conceder o denegar permisos sobre un recurso, así como administrar la propia infraestructura.

En los siguientes pasos se procederá a crear, a modo de ejemplo, un grupo de usuarios cuya función será la de administrar uno de los roles de la infraestructura.

Paso	Descripción
82.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
83.	Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios. 

Paso	Descripción
84.	Expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"**, como se muestra en la siguiente figura. 
85.	Pulsando con el botón derecho sobre "Users" diríjase al apartado de configuración **"Nuevo → Grupo"**. 

Paso	Descripción
86.	Sobre la ventana emergente para la creación del nuevo grupo introduzca "Administradores de Citrix Controller" y pulse sobre "Aceptar" como se indica en la siguiente imagen. 
87.	A continuación, deberá agregar los usuarios que realizarán la administración de los servidores Citrix Controller al grupo "Administradores de Citrix Controller". Para ello diríjase a las propiedades del grupo recién creado y en el apartado "Miembros" añada cada usuario pulsando sobre el botón "Agregar...". Una vez introducidos todos los usuarios pulse "Aceptar". 

3. CERTIFICADOS

Citrix Virtual Apps and Desktops faculta el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación usando HTTPS que utiliza un cifrado basado en SSL/TLS para crear un canal cifrado para el tráfico de información sensible. Para lugares públicos es un requisito indispensable en la categoría media y alta de seguridad del ENS el uso de certificados emitidos por entidades certificadoras de terceros, para el caso de sitios internos se recomienda el uso de certificados emitidos por una entidad certificadora interna, está totalmente desaconsejado el uso de certificados autofirmados.

Para la categoría más alta de seguridad del ENS se configuran certificados para cada uno de los roles de la infraestructura, a saber:

a) Servidor con el rol Citrix Controller.

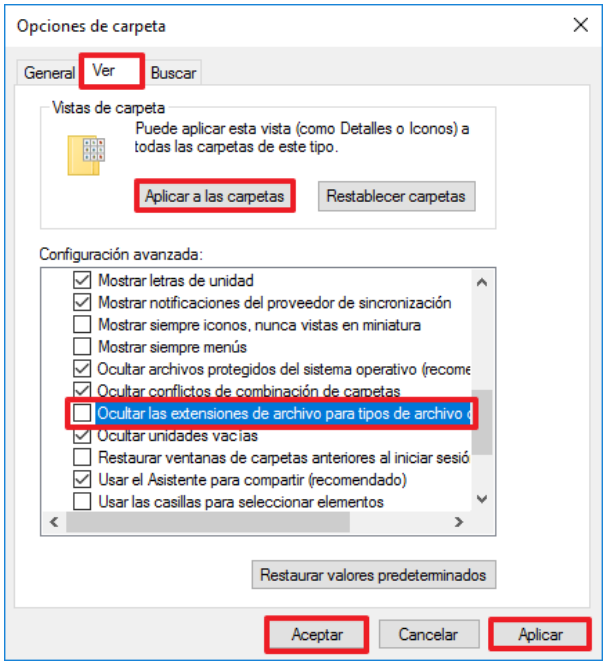
b) Servidor con el rol Citrix Storefront.

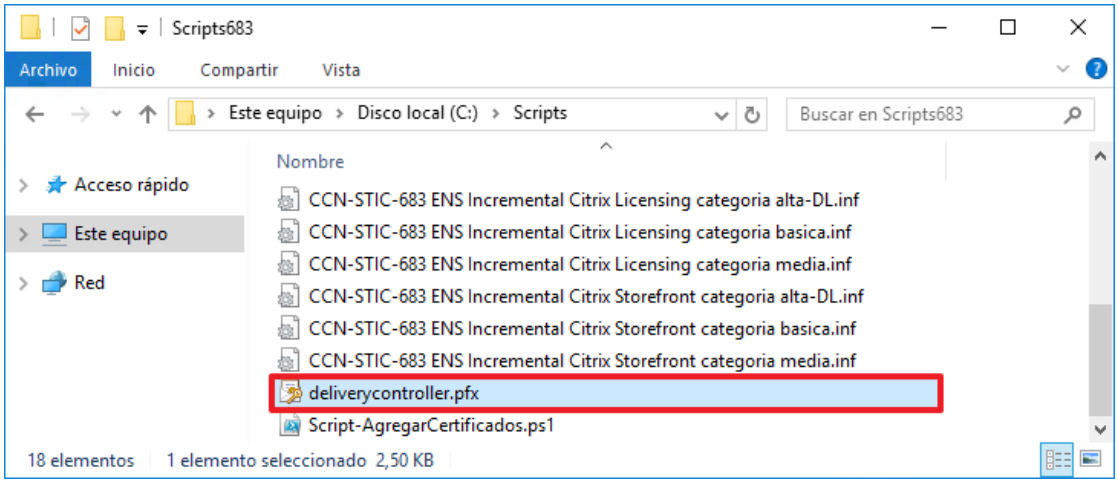
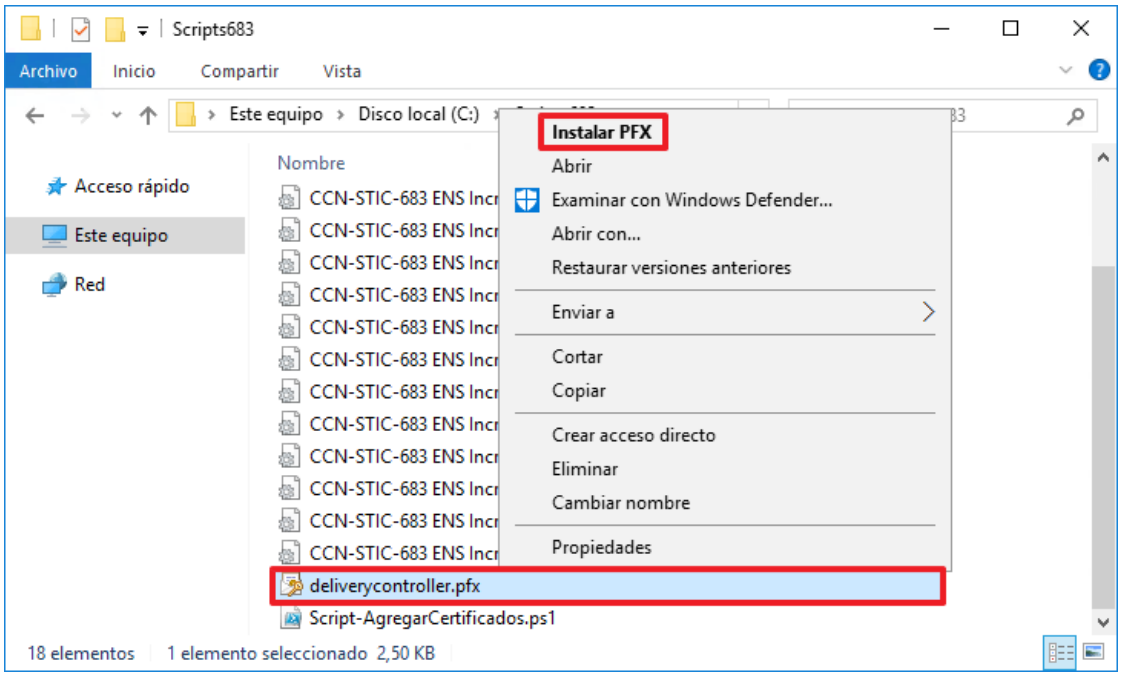
c) Servidor con el rol Citrix Licensing.

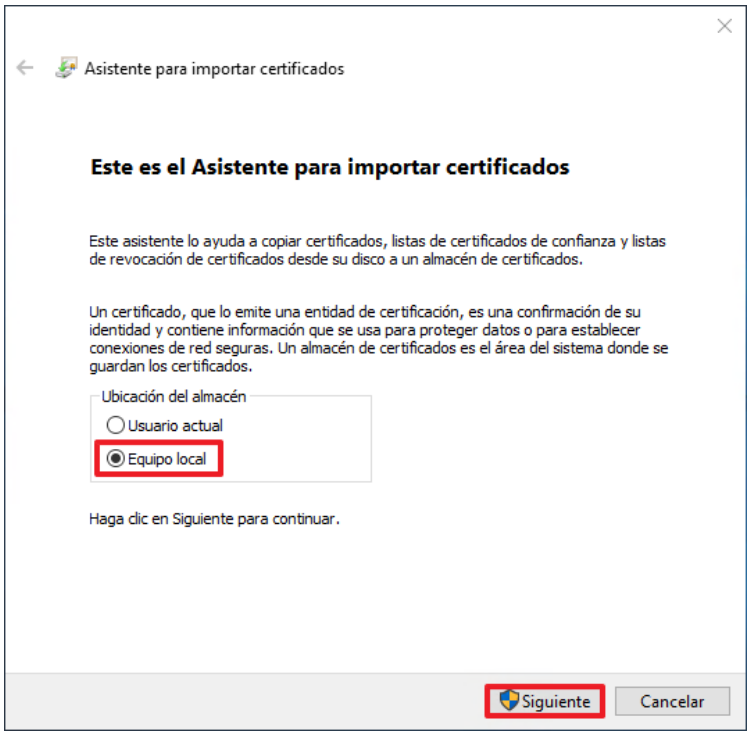
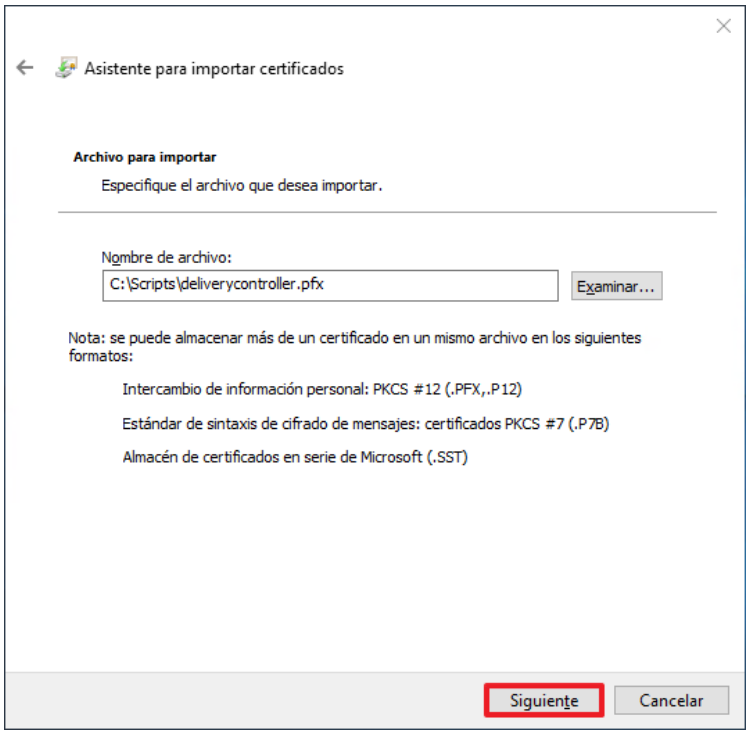
d) Servidores con el rol Citrix Director.

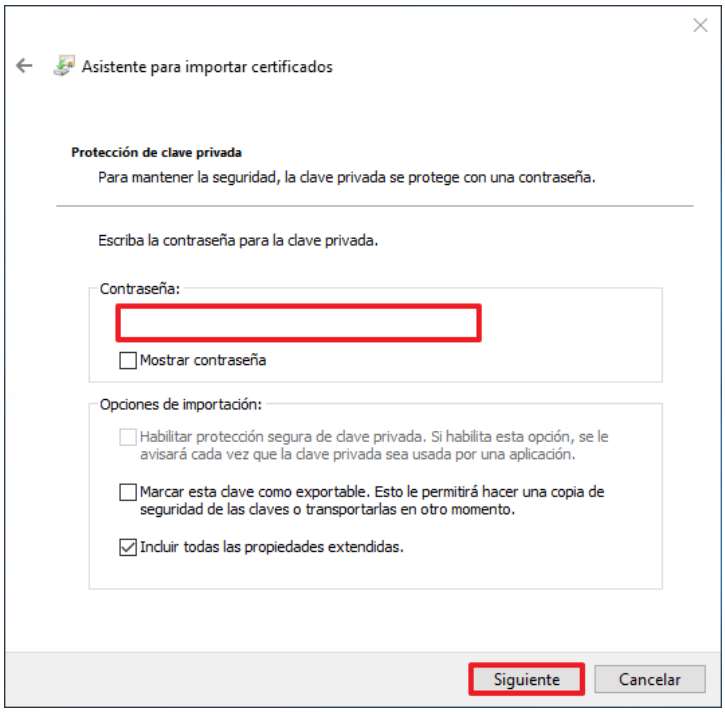
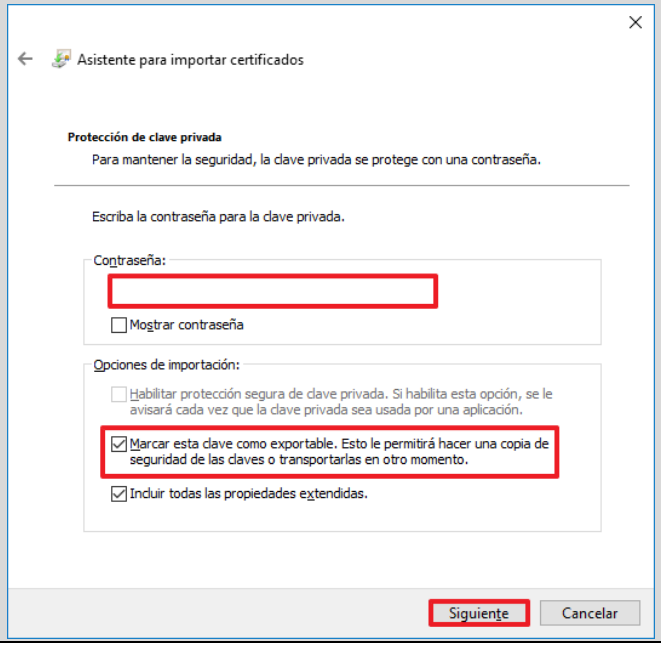
En primer lugar, se procederá a securizar las comunicaciones del servidor con el rol Citrix Controller.

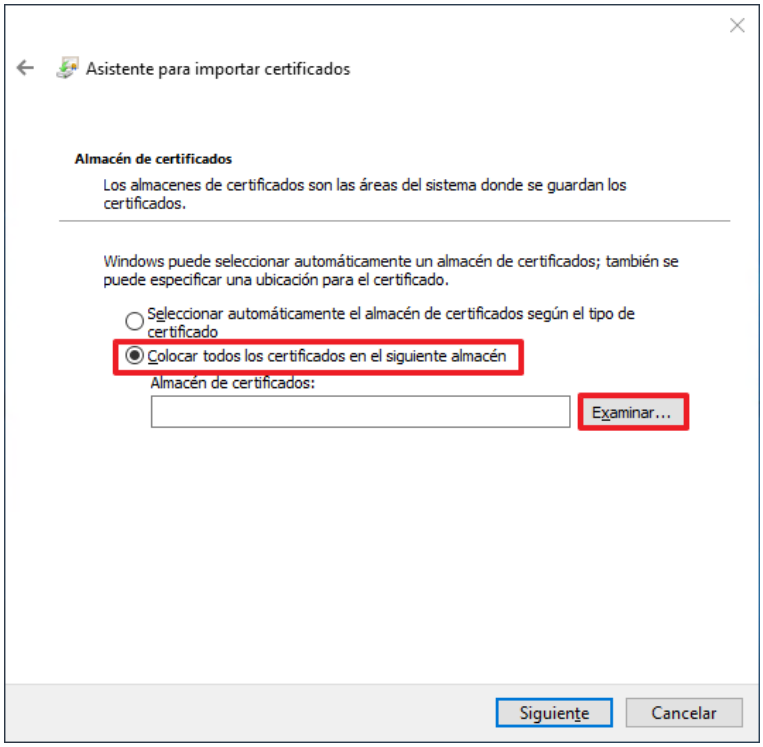
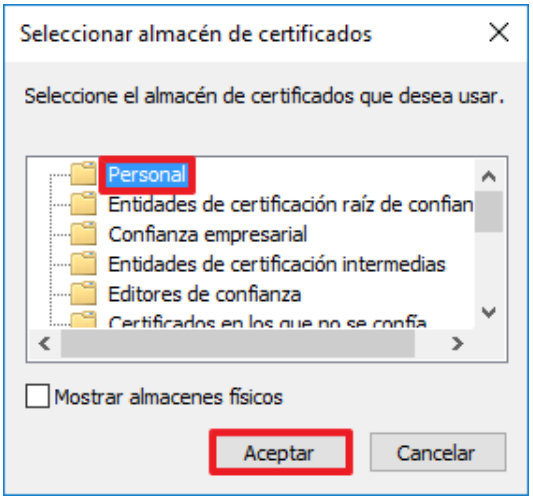
Paso	Descripción
88.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
89.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\Scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
90.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts".

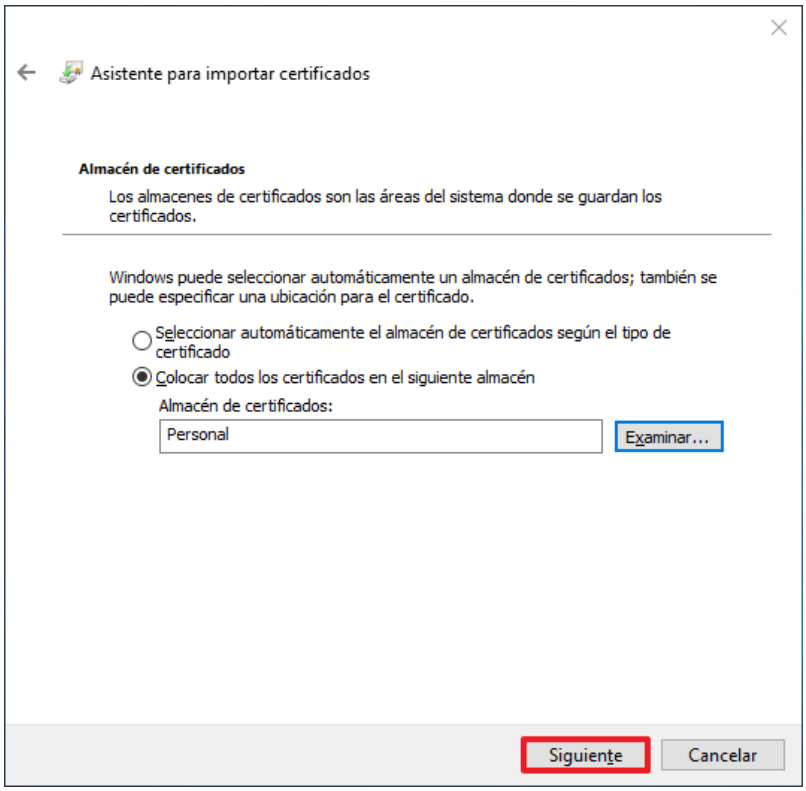
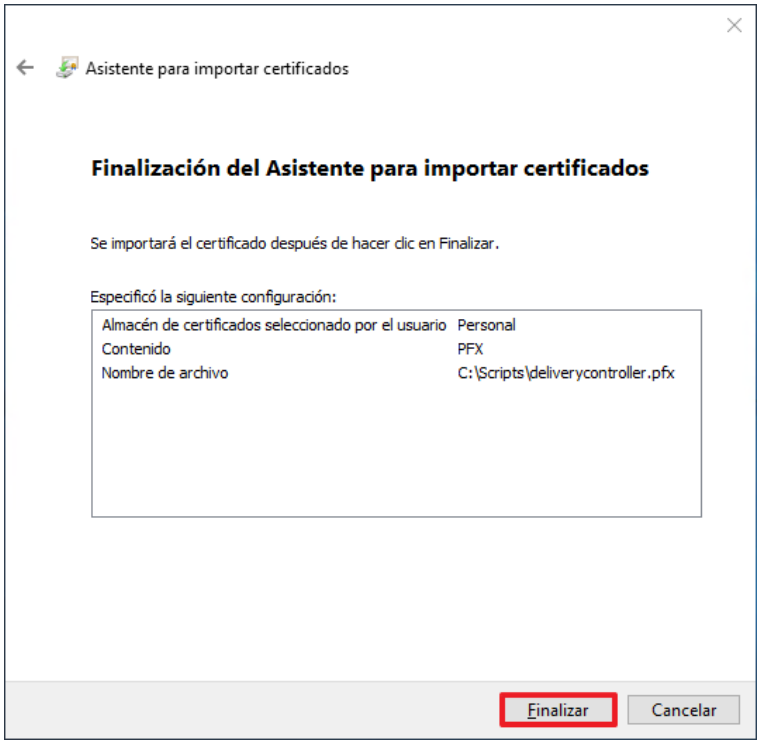
Paso	Descripción
91.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
92.	Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio. – CCN-STIC-683 Configuración SSL – Citrix Controller – Paso1.bat – Script-AgregarCertificados.ps1
93.	Para continuar, debe realizar la solicitud de un certificado válido en el dominio, cuyo Nombre común “CN” coincida con el FQDN del equipo sobre el que está implementando el rol Citrix Controller. No debe utilizar un certificado de tipo wildcard ya que de utilizarlo encontrará problemas en los siguientes pasos de configuración. No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.

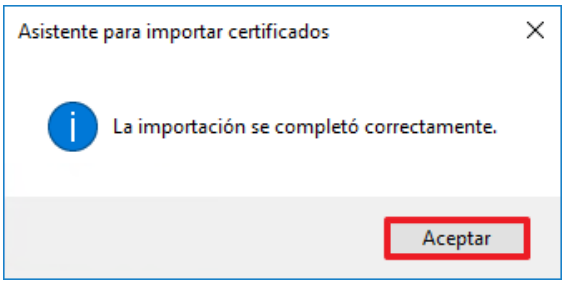
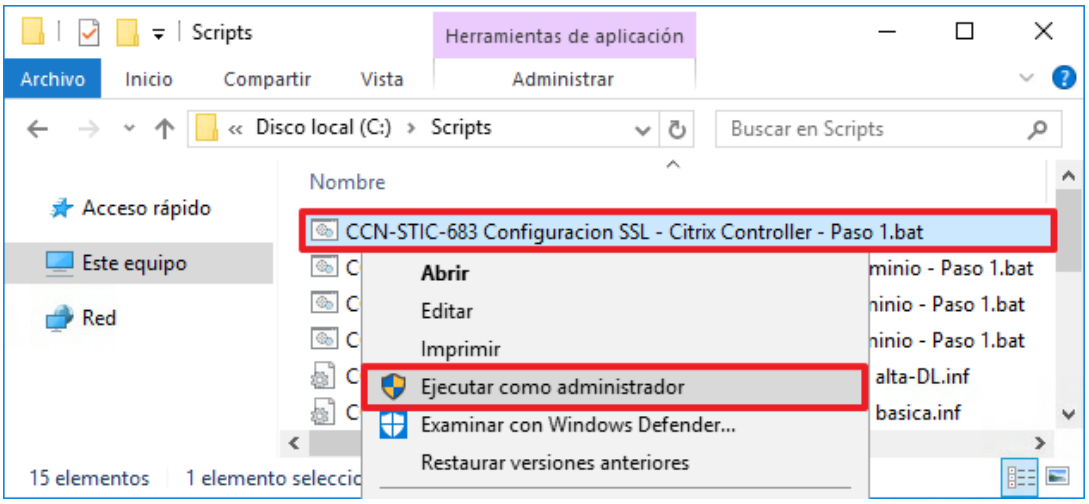
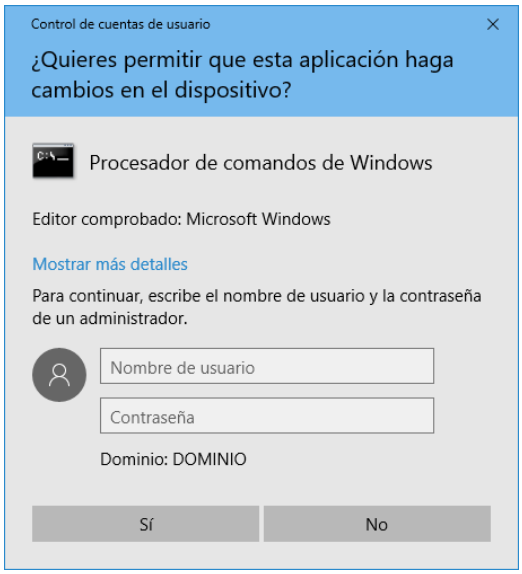
Paso	Descripción
94.	Una vez obtenido el certificado, ubíquelo en la unidad “C:\Scripts”, a modo de ejemplo en los siguientes pasos se utiliza el certificado “deliverycontroller.pfx” cuyo CN coincide con el FQDN de la maquina utilizada. 
95.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **“Instalar PFX”** tal y como se indica en la siguiente figura. 

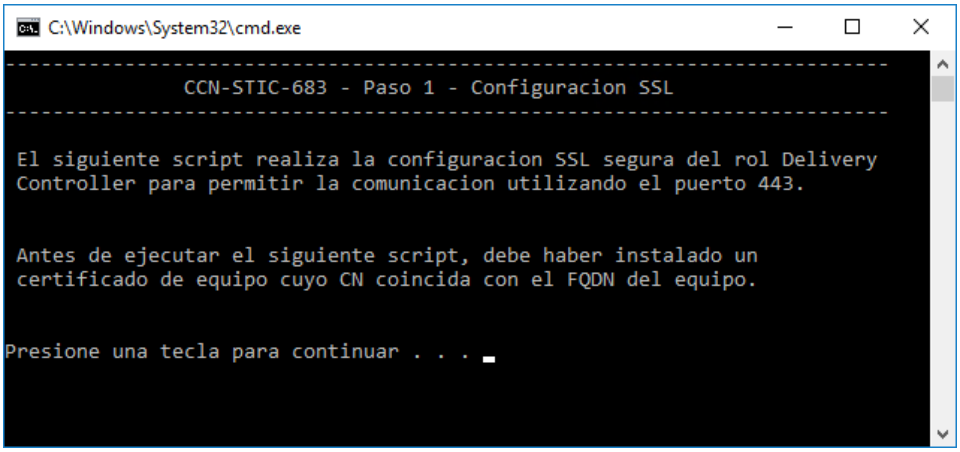
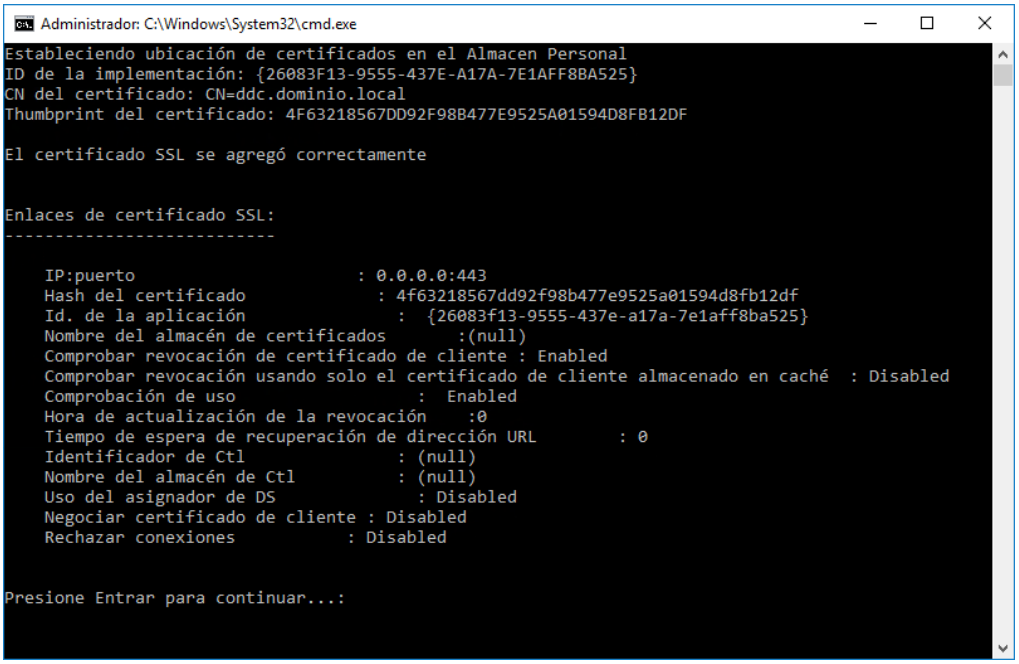
Paso	Descripción
96.	Sobre la ventana emergente "Asistente para importar certificados" seleccione **"Equipo local"** y pulse **"Siguiente"** para continuar.  **Nota:** El sistema solicitará elevación de privilegios.
97.	En la siguiente figura encontrará la ruta del certificado que desea instalar. Pulse "Siguiente" para continuar. 

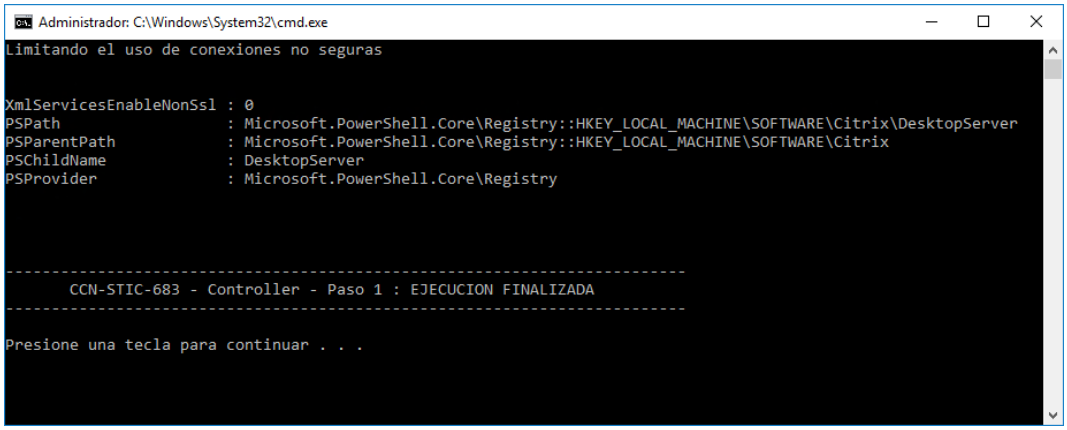
Paso	Descripción
98.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.  **Nota:** Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno. 

Paso	Descripción
99.	Seleccione la opción **"Colocar todos los certificados en el siguiente almacén"** y pulse sobre "Examinar" para indicar el almacén de certificados que albergará el certificado instalado. 
100.	Sobre la ventana emergente "Seleccionar almacén de certificados" especifique el almacén "Personal" y pulse sobre "Aceptar". 

Paso	Descripción
101.	Verifique que las opciones introducidas coinciden con la siguiente figura. Pulse “Siguiente” para continuar con el proceso. 
102.	Por último, pulse sobre “Finalizar” para terminar con el proceso de importación de certificados. 

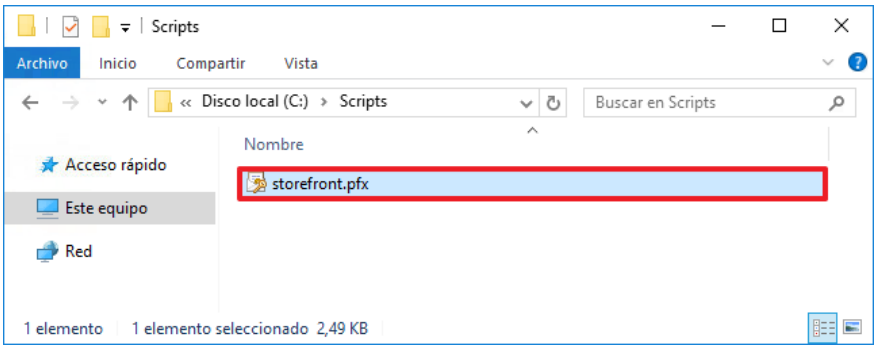
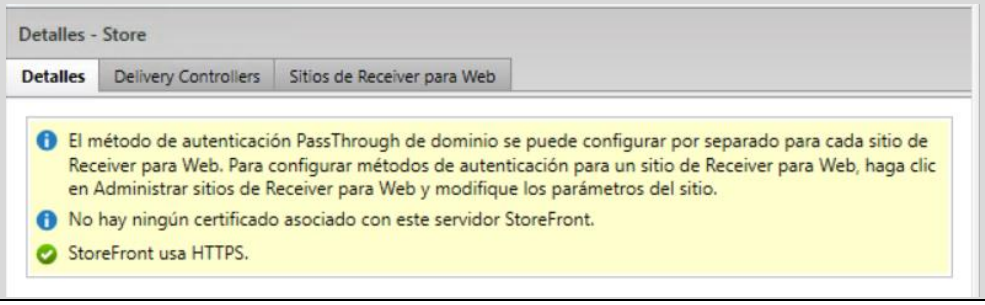
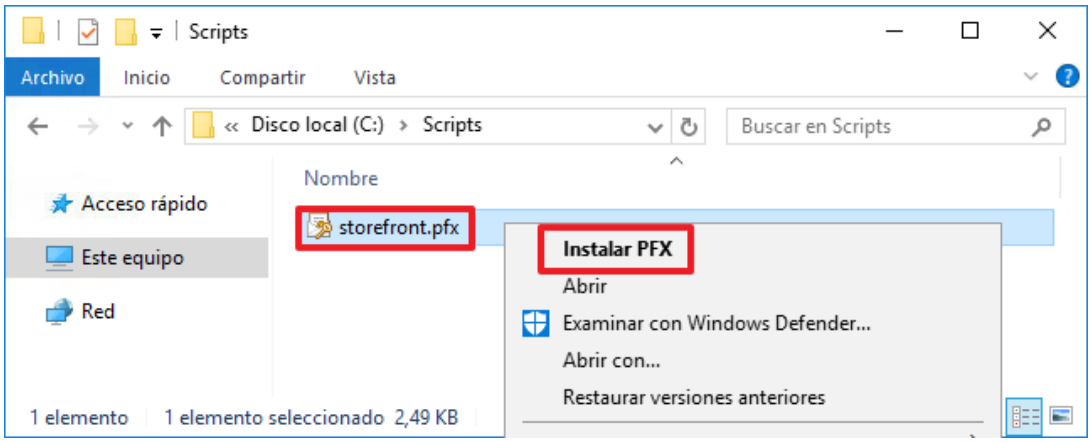
Paso	Descripción
103.	Si el proceso de importación ha funcionado correctamente aparecerá el siguiente mensaje informativo. Pulse “Aceptar” para continuar. 
104.	Diríjase a la carpeta “C:\Script” y pulsando con el botón derecho ejecute con permisos de administrador el script “CCN-STIC-683 Configuración SSL – Citrix Controller – Paso 1.bat. 
105.	Control de cuentas de usuario le indicará que escriba el usuario y la contraseña de un administrador para continuar. 

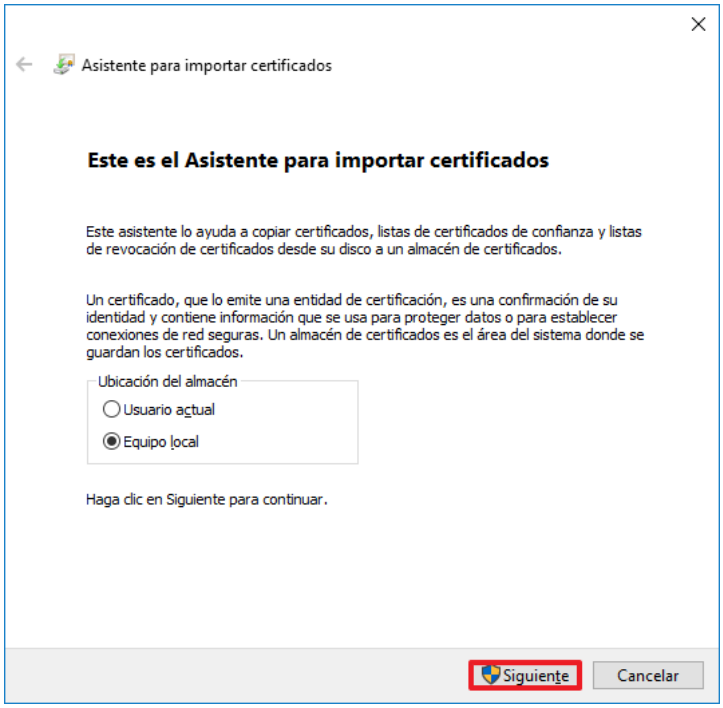
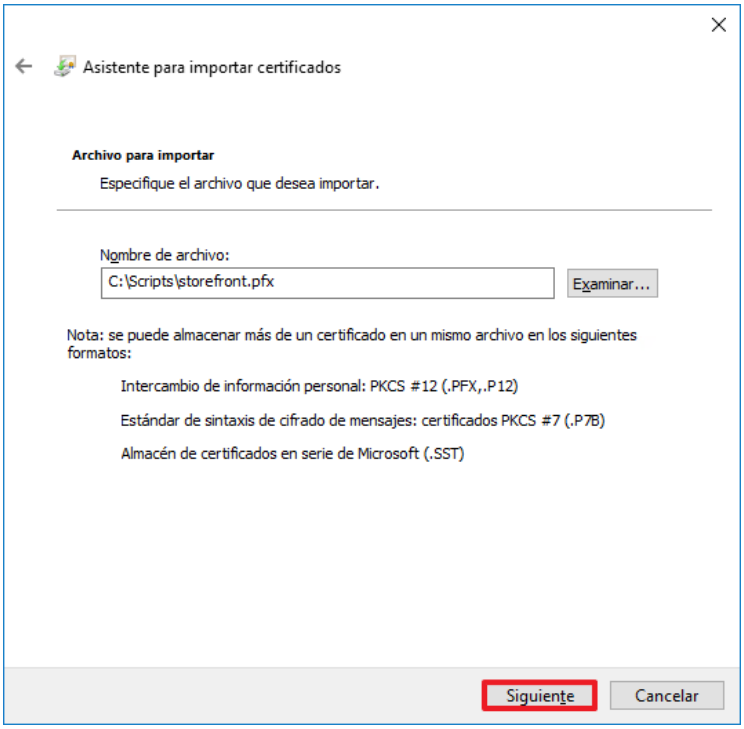
Paso	Descripción
106.	Se abrirá un terminal CMD con una descripción del script. Pulse cualquier tecla para continuar. Es importante que haya realizado los pasos anteriores para evitar cualquier error en su ejecución. 
107.	El primer paso del script es localizar dentro del almacén personal del equipo el certificado recientemente instalado, una vez localizado, mostrará por pantalla la información del certificado y de la implementación de Citrix. Si la configuración es correcta aparecerá un mensaje similar al que puede apreciar en la siguiente figura indicando que el certificado SSL se agregó correctamente. Presione “Entrar” para continuar con la ejecución. 

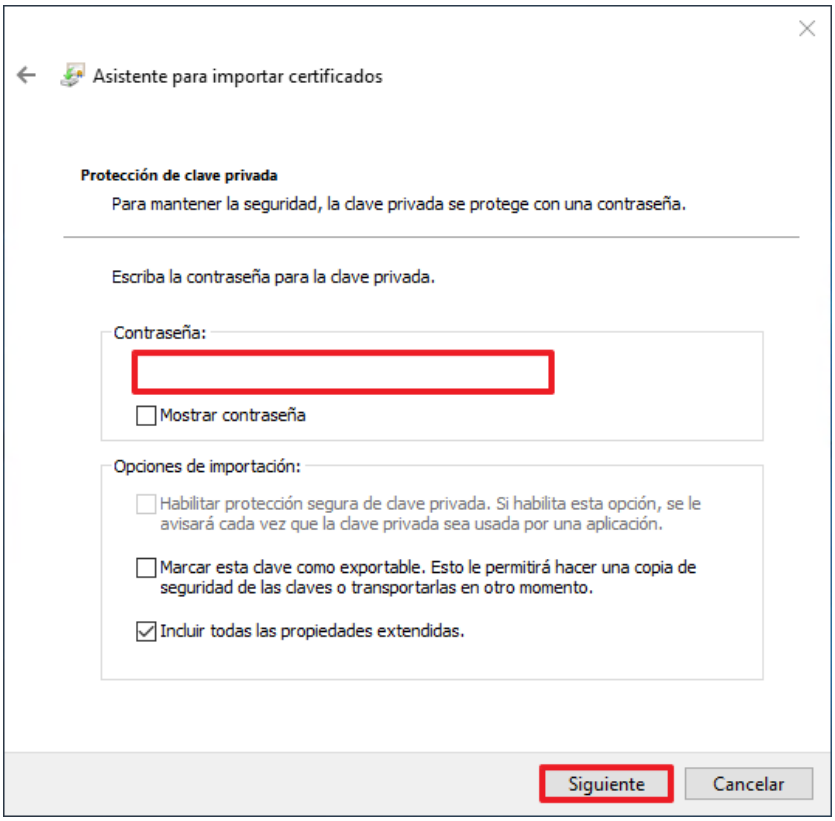
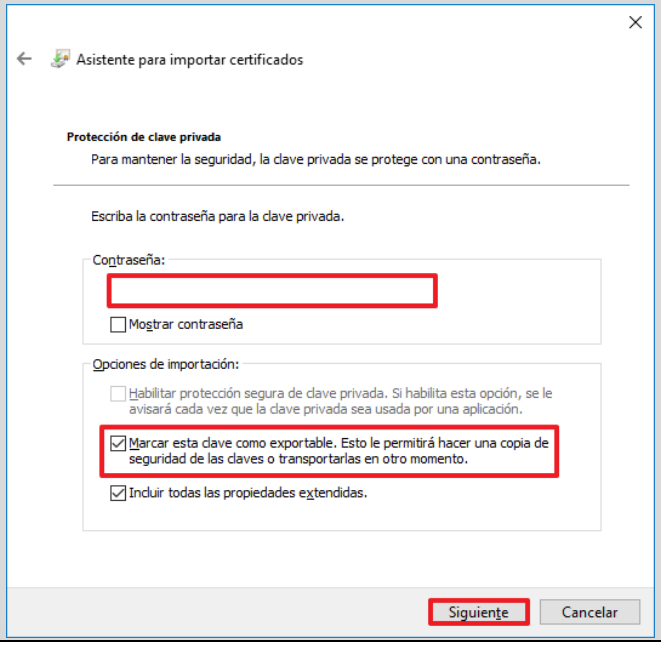
Paso	Descripción
108.	La segunda parte de la ejecución del script genera una clave de registro que limita la conexión al servidor utilizando conexiones no seguras por el protocolo HTTP. Presione cualquier tecla para terminar con la ejecución del script. 
109.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor.

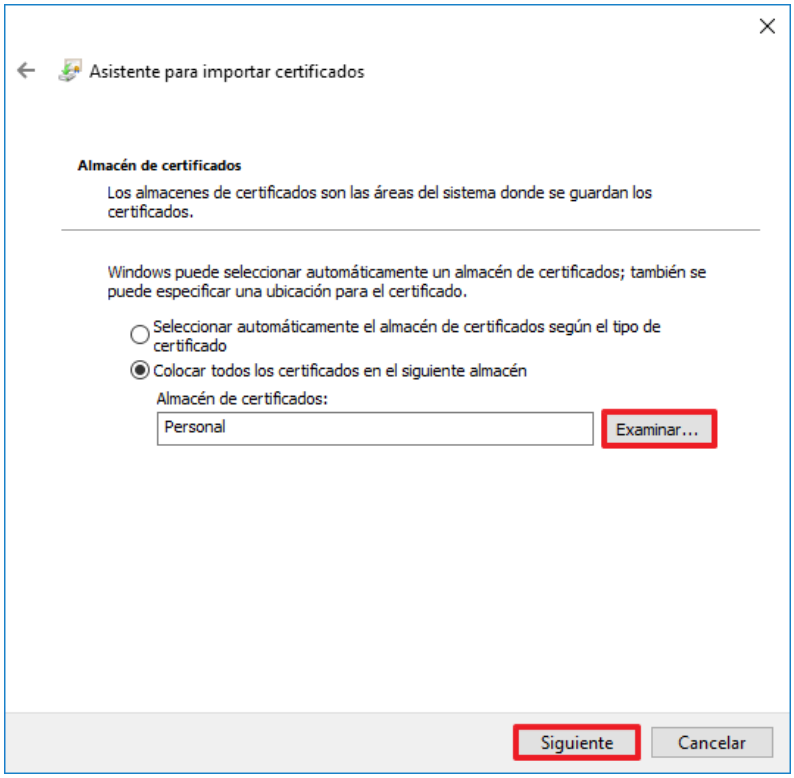
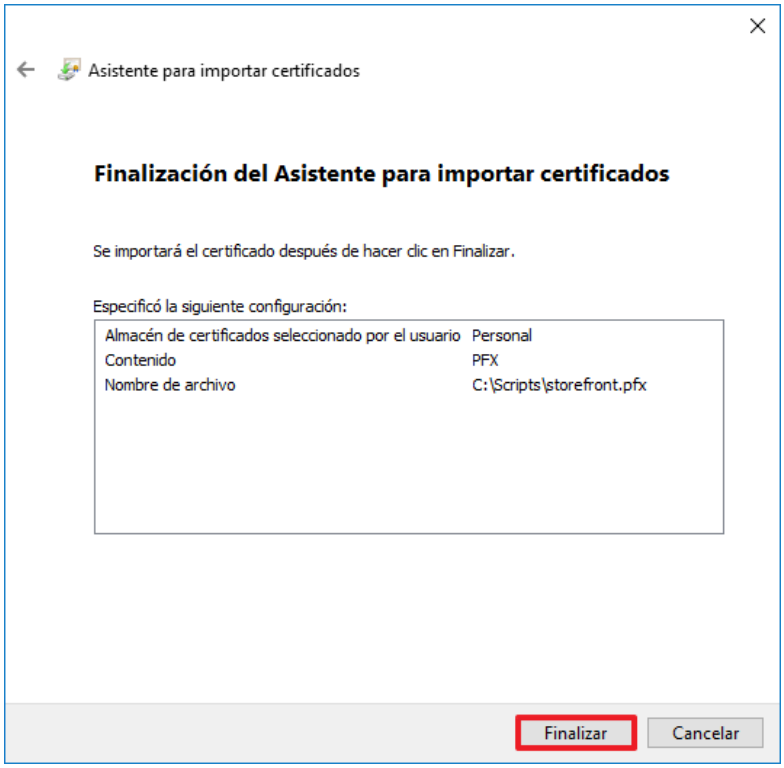
En este punto el servidor Citrix Controller se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura. Una vez configurado el servidor con el rol Citrix Controller deberá continuar con las configuraciones sobre el servidor con el rol Citrix Storefront.

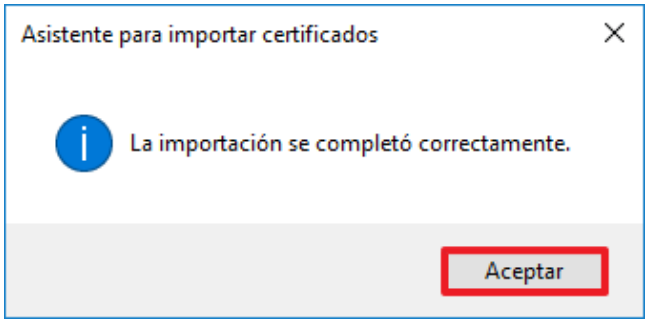
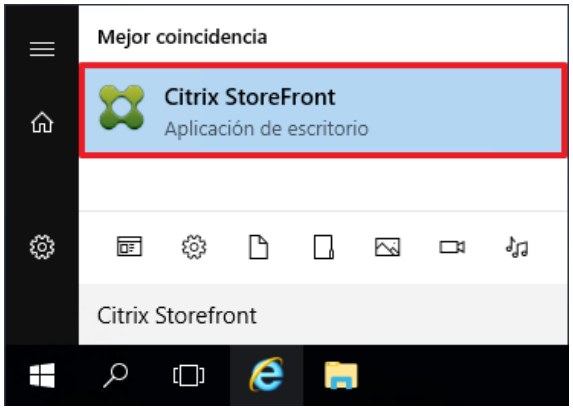
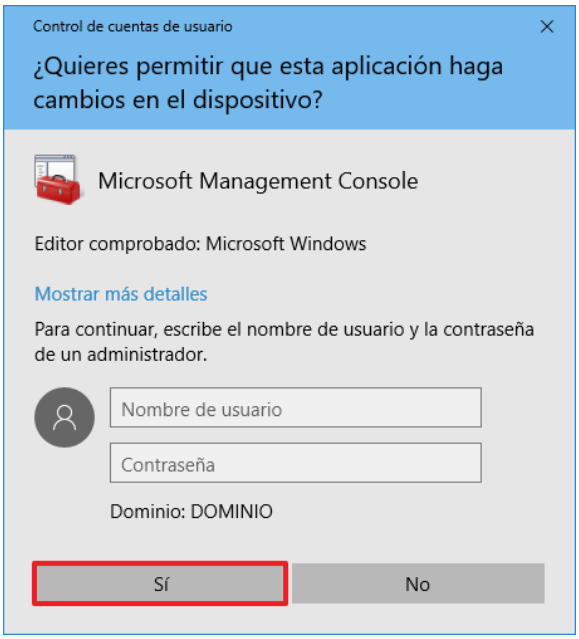
Paso	Descripción
110.	Inicie sesión en un servidor con el rol Citrix Storefront del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
111.	Cree el directorio “Scripts” en la unidad “C:\”.
112.	Será necesario la obtención de un certificado de equipo válido en el dominio ya que los equipos que se conecten al servidor validarán la presencia del certificado y su vigencia. Utilice un certificado cuyo nombre común coincida con la URL base que haya indicado en pasos anteriores. **Nota:** No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.

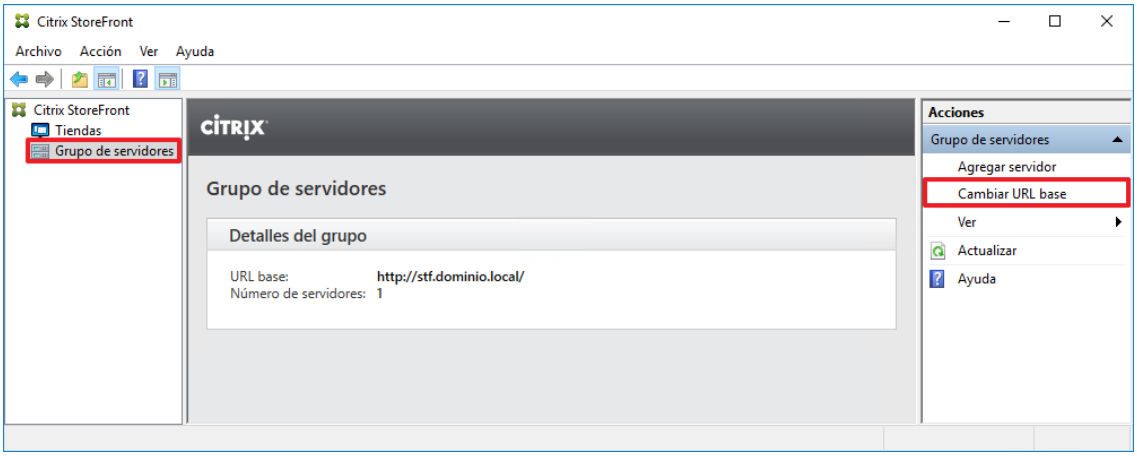
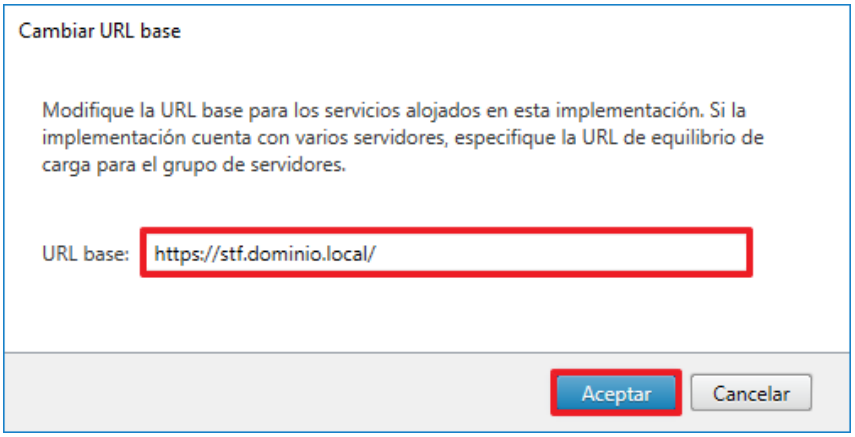
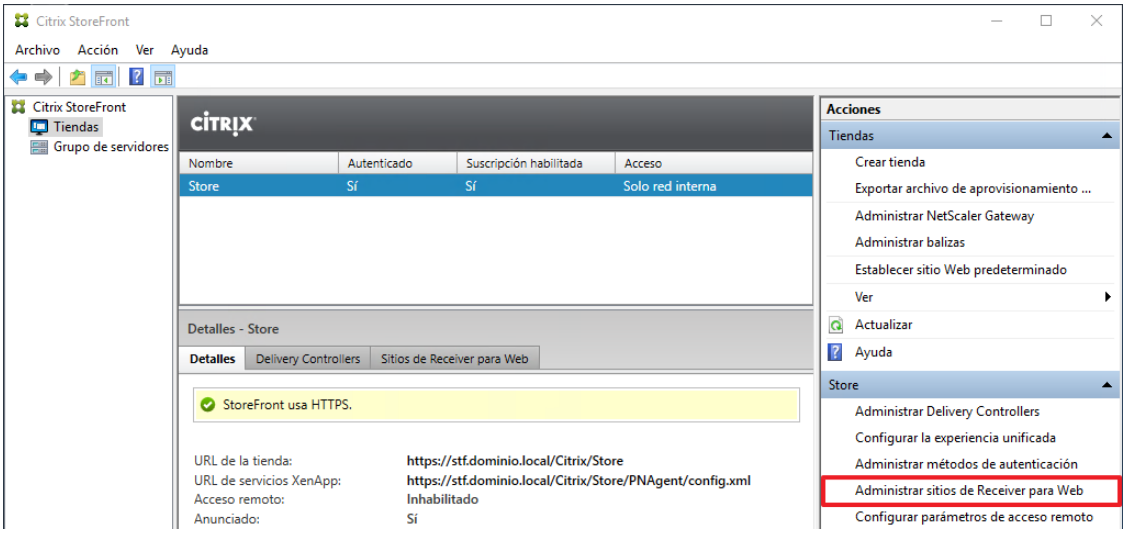
Paso	Descripción
113.	Copie el certificado en la unidad "C:\Scripts" y establezca un nombre de fichero identificativo. En esta guía se utilizará el fichero **"C:\Scripts\storefront.pfx"** a modo de ejemplo, no dude en ajustar el nombre de su archivo en los siguientes pasos. 
114.	Si no lo ha hecho todavía, proceda con los siguientes pasos para realizar la instalación del certificado sobre el almacén **"Personal"** de equipo. **Nota:** Durante la instalación puede ubicar el certificado en el almacén del equipo "Hospedaje de sitios web" pero encontrará advertencias en la consola de Storefront indicando que no hay ningún certificado asociado a este servidor Storefront. Para evitar problemas deberá ubicar el certificado en el almacén Personal del equipo tal y como se muestra en los siguientes pasos. 
115.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **"Instalar PFX"** tal y como se indica en la siguiente figura. 

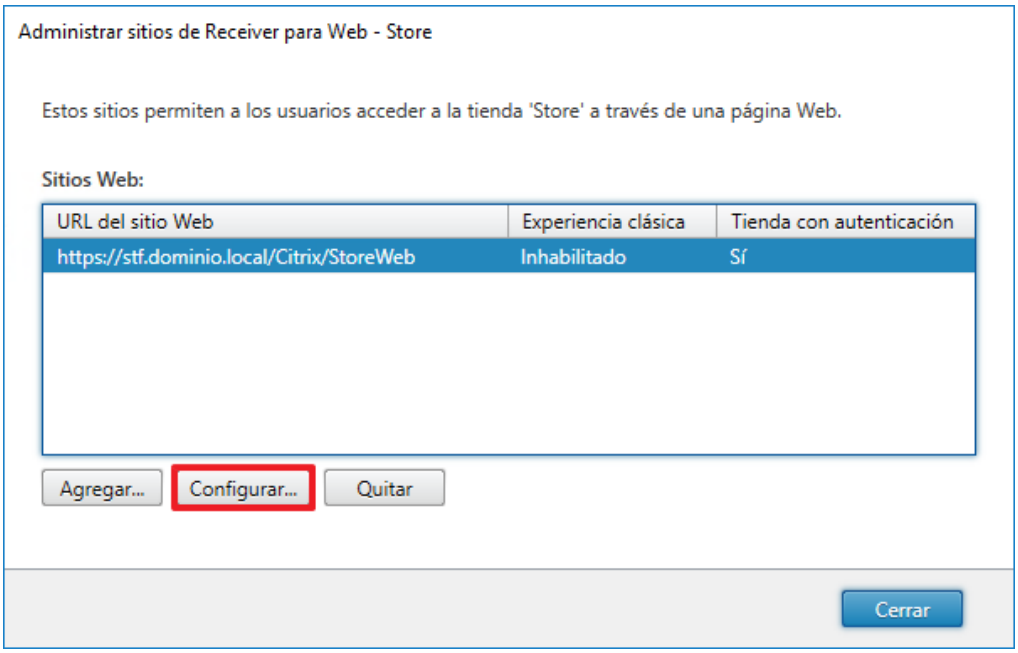
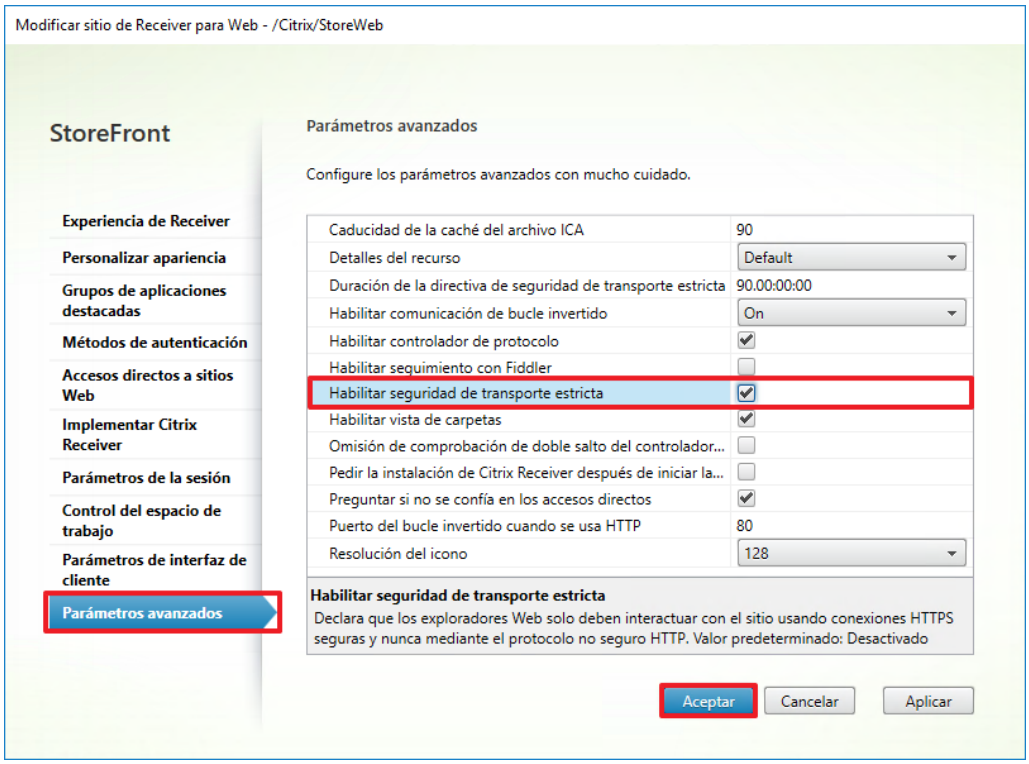
Paso	Descripción
116.	Se iniciará el asistente de importación de certificados. Pulse sobre “Equipo local” y a continuación pulse sobre “Siguiente”.  **Nota:** El sistema solicitará elevación de privilegios.
117.	Especifique el archivo a importar y continúe con el asistente pulsando sobre “Siguiente”. 

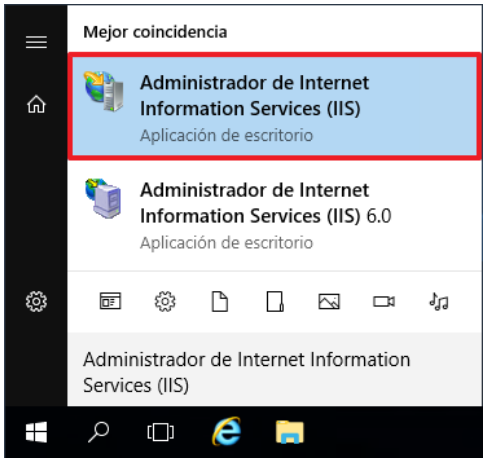
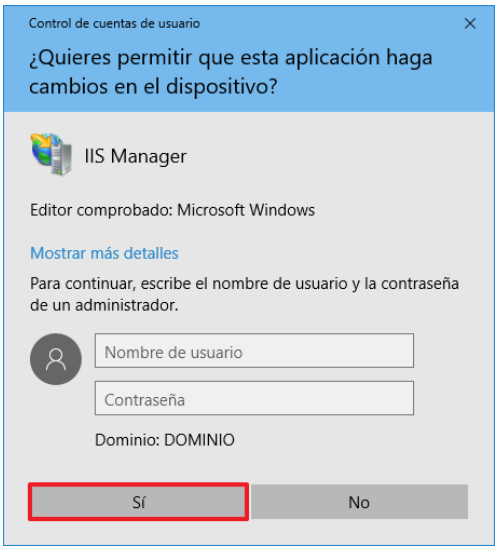
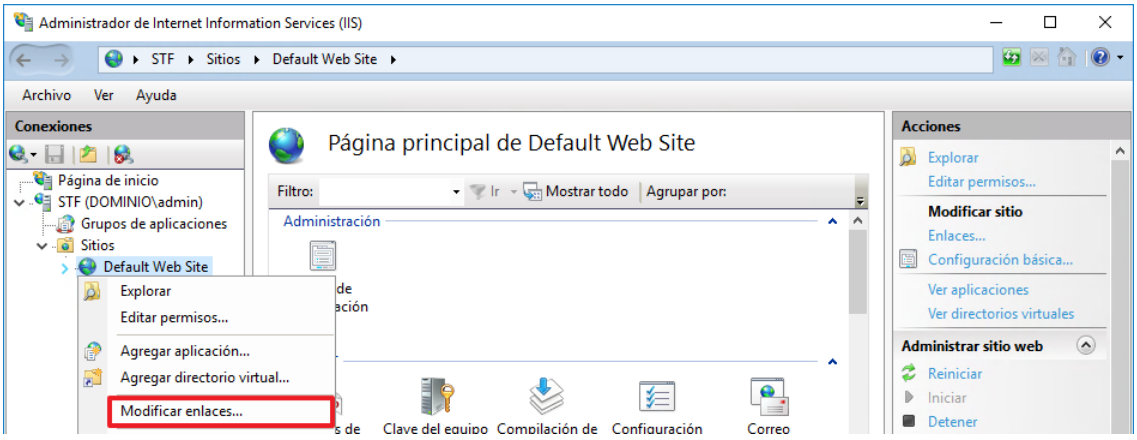
Paso	Descripción
118.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.  **Nota:** Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno. 

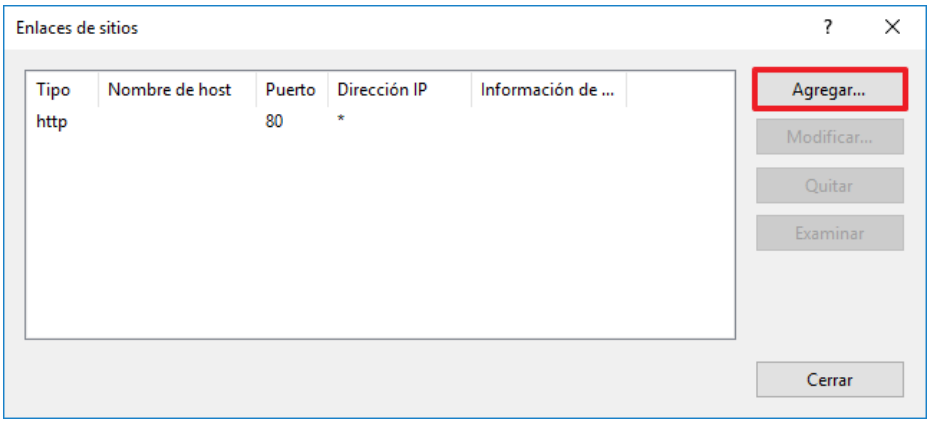
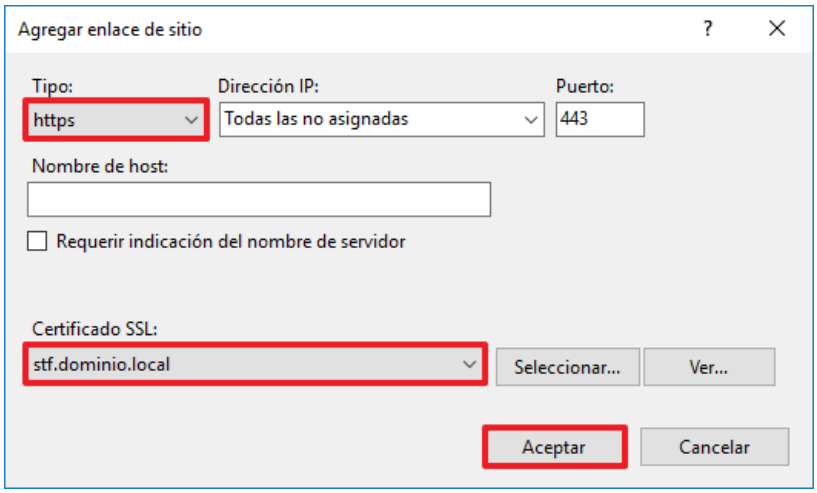
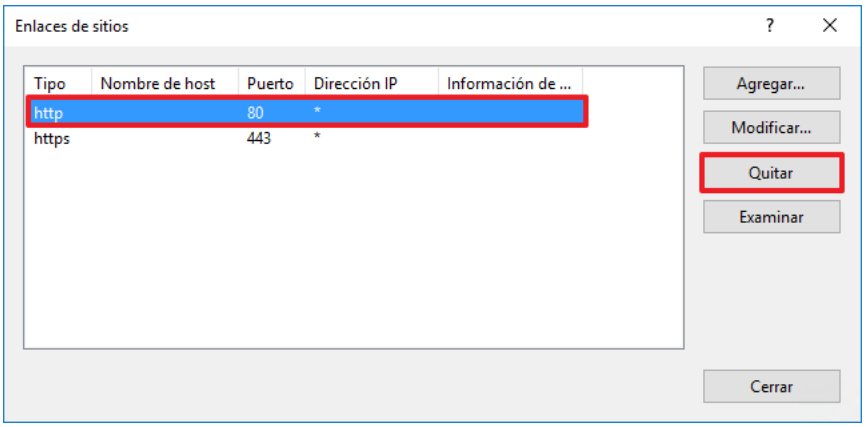
Paso	Descripción
119.	Localice el almacén personal del equipo pulsando sobre “Examinar” tal y como se muestra en la siguiente figura. Una vez establecido, pulse “Siguiente” para continuar. 
120.	El último punto del asistente muestra un resumen, pulse “Finalizar” para completar la importación del certificado sobre el equipo. 

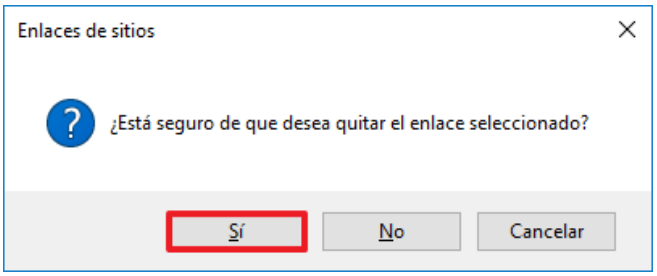
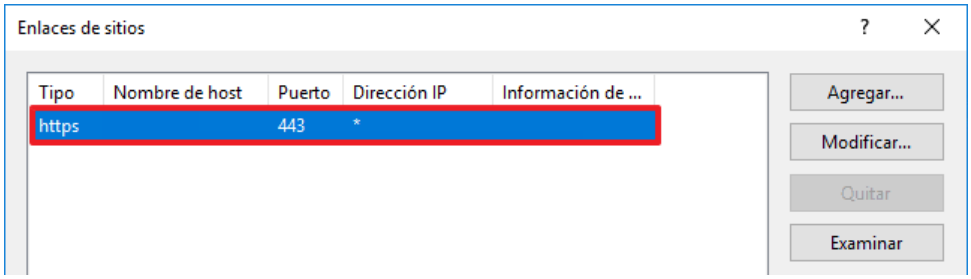
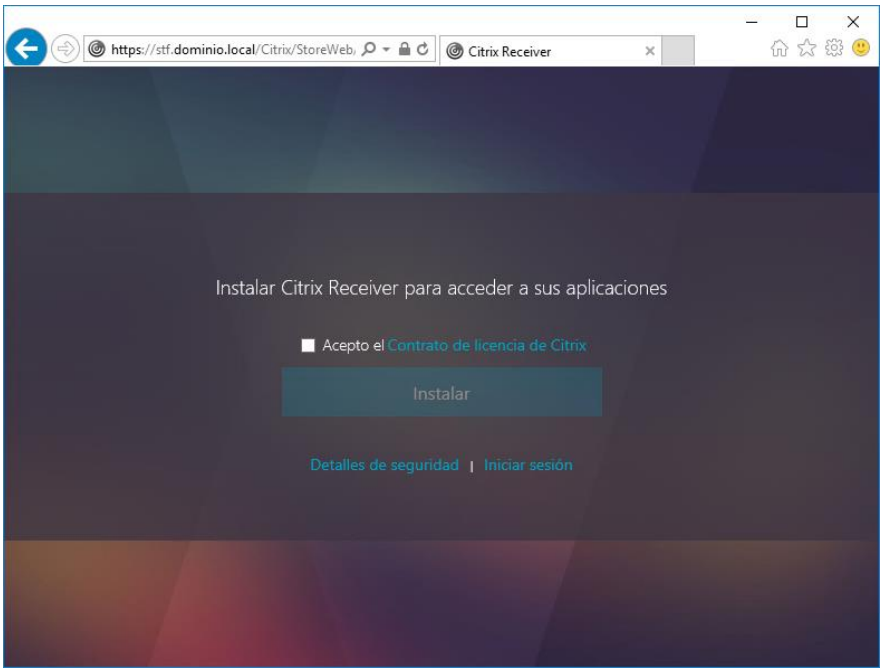
Paso	Descripción
121.	Espere unos segundos a que finalice el proceso, aparecerá un mensaje indicando que la importación se realizó correctamente. 
122.	A continuación, una vez importado el certificado, proceda a configurar la URL base del grupo de servidores. Abra la consola Citrix Storefront. 
123.	Control de cuentas de usuario le solicitará las credenciales de un usuario administrador para continuar. 

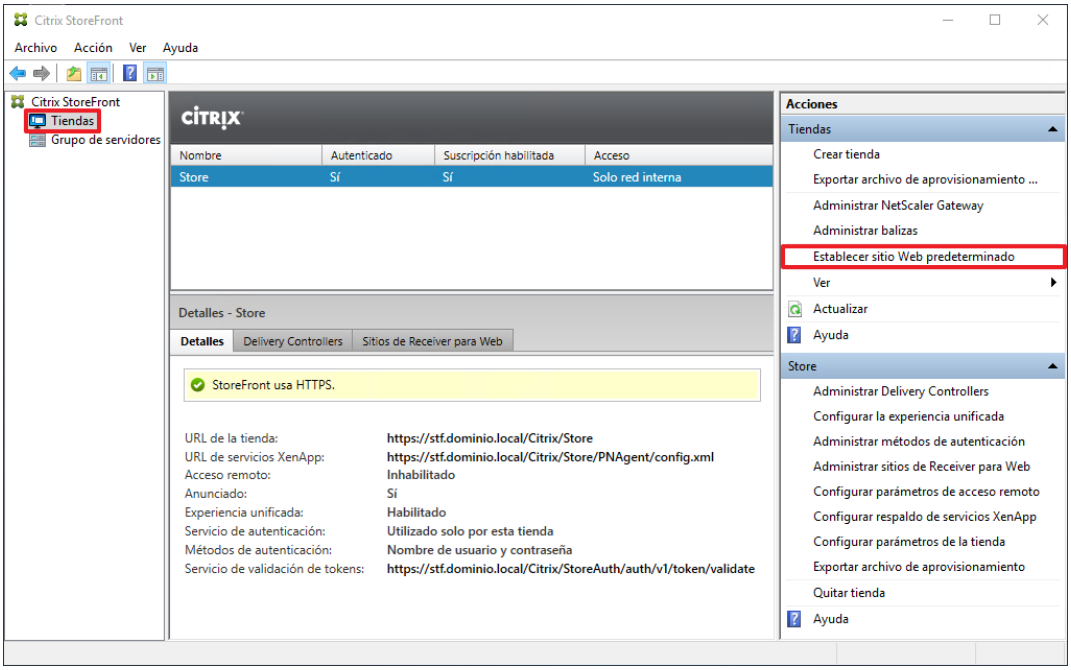
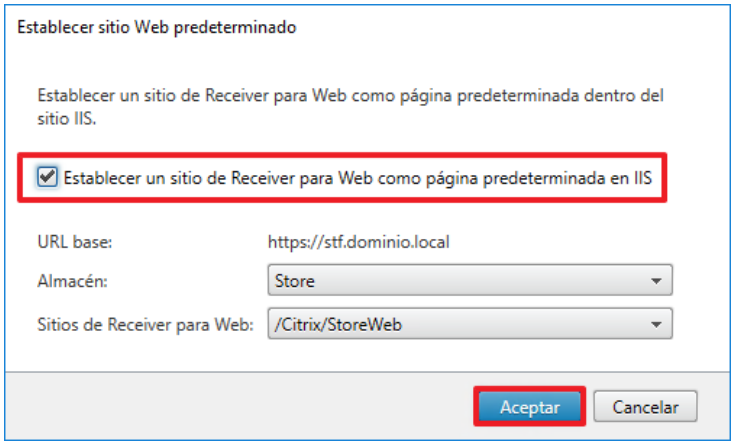
Paso	Descripción
124.	Dentro de la consola, diríjase al nodo de configuración **"Citrix Storefront → Grupo de servidores"** y pulse sobre **"Cambiar URL base".** 
125.	Sobre la ventana emergente, establezca la URL, indicando el protocolo seguro HTTPS como se muestra en la siguiente figura. Pulse "Aceptar" para guardar los cambios. Acto seguido, verá reflejados los cambios. 
126.	A continuación, deberá configurar los parámetros de Receiver para Web, acceda al menú **"Tiendas → Store → Administrar sitios de Receiver para Web".** 

Paso	Descripción
127.	La ventana emergente le indicará los sitios creados. Pulse sobre **"Configurar…"**. 
128.	En el menú **"Modificar sitio de Receiver para Web"** diríjase al apartado **"Parámetros avanzados"** y marque la opción "Habilitar seguridad de transporte estricta".  **Nota:** La opción anterior deshabilita la posibilidad de conectarse a los sitios web de Citrix utilizando un protocolo no seguro como HTTP.

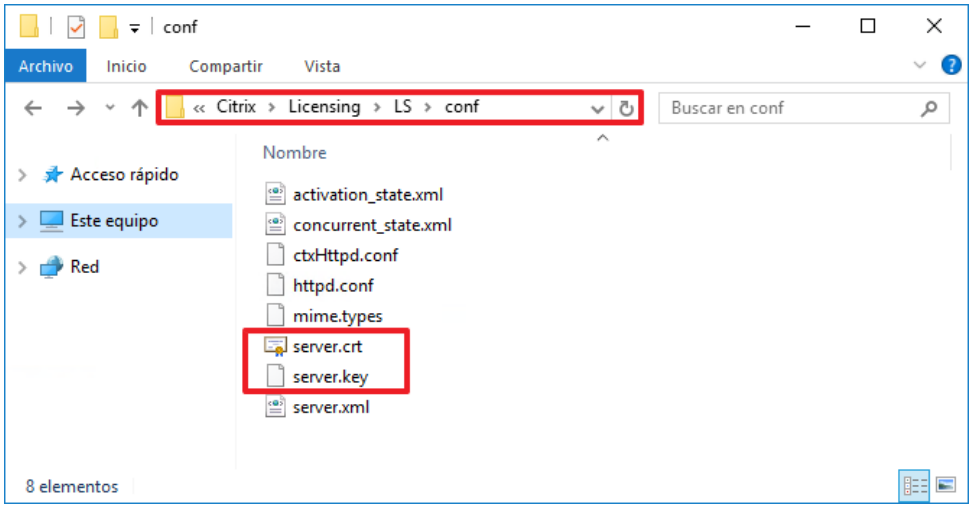
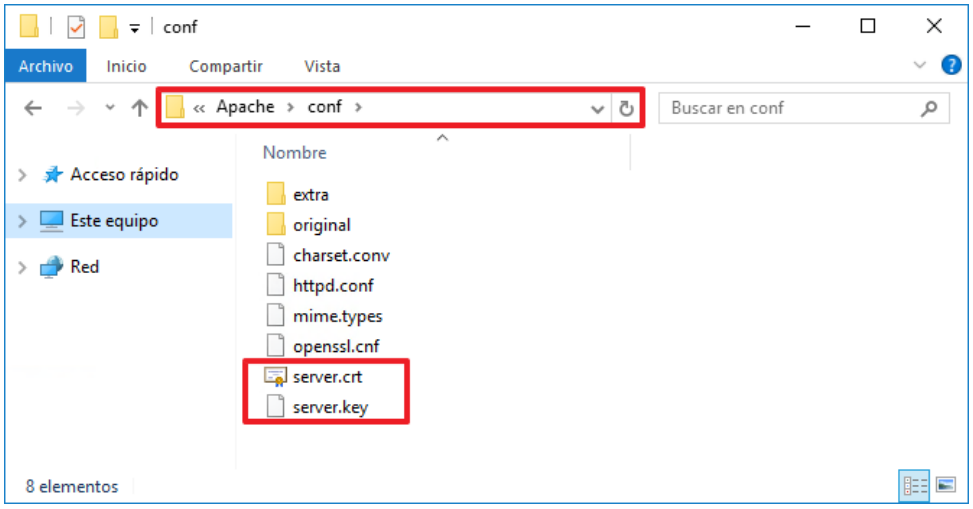
Paso	Descripción
129.	Continúe el proceso abriendo la consola **"Administrador de Internet Information Services (IIS)".** 
130.	El sistema solicitará elevación de privilegios. 
131.	Abra el nodo de configuración "**<Su servidor>(Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"**. 

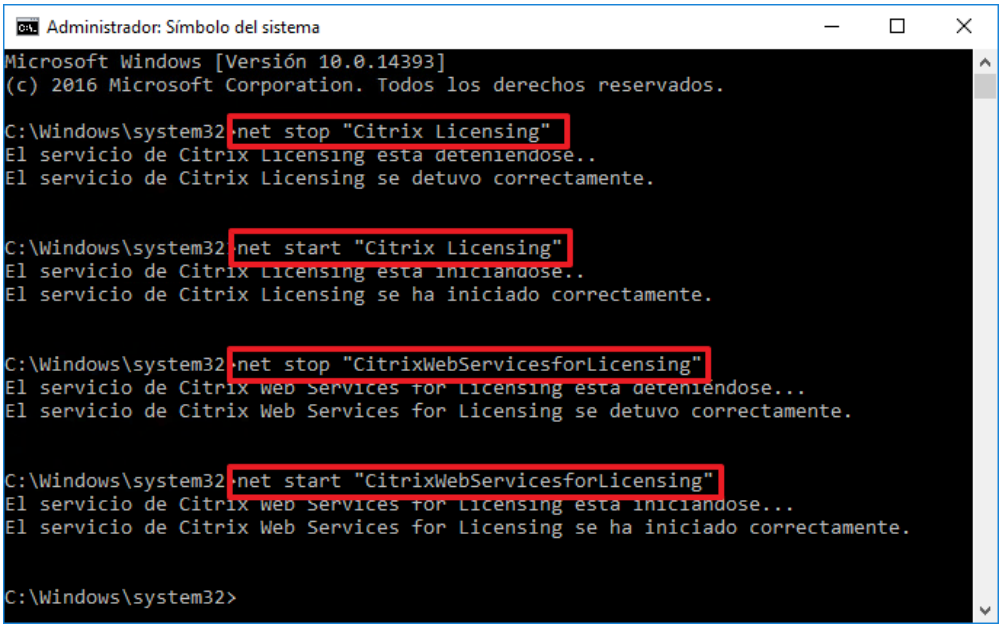
Paso	Descripción
132.	Sobre la ventana “Enlaces de sitios” pulse **“Agregar…”** para añadir un enlace nuevo. Por defecto, encontrará creado un enlace al puerto 80 que deberá eliminar más adelante para evitar conexiones no seguras al entorno. 
133.	Modifique en el formulario los parámetros necesarios y establezca su certificado SSL a utilizar, instalado en pasos anteriores. Pulse **“Aceptar”** para guardar los cambios”. 
134.	Con ambos enlaces creados, seleccione el enlace de Tipo “http” y acto seguido pulse sobre **“Quitar”**. 

Paso	Descripción
135.	Sobre la ventana emergente, pulse “Si” para confirmar la eliminación del enlace seleccionado. 
136.	Al terminar, verifique que únicamente está configurado el enlace de tipo “https” recién creado con su certificado SSL. 
137.	Puede verificar que la configuración es correcta abriendo un Navegador y accediendo a la URL base de su entorno, en este caso, a modo de ejemplo se verifica el acceso a la dirección https://stf.dominio.local/Citrix/Storeweb.  **Nota:** Para realizar la prueba anterior, puede ser necesario que rebaje la seguridad de Internet Explorer habilitando JavaScript y las cookies en el navegador. No es necesario que realice ninguna acción sobre el propio servidor, únicamente verifique que tiene conectividad con la URL Base que ha definido y que el certificado utilizado es de confianza.

Paso	Descripción
138.	Dependiendo de su organización, y de las opciones seleccionadas durante la instalación del rol Citrix Storefront, es posible que no haya configurado su sitio web de Storefront como predeterminado en su servidor IIS. Si desea establecer su sitio de Receiver para web como página predeterminada de su servidor IIS acceda a **"Tiendas → Establecer sitio Web predeterminado"** dentro de la consola de "Citrix Storefront". 
139.	Marque la opción "Establecer un sitio de Receiver para Web como página predeterminada en IIS" y seleccione las opciones que se ajusten a las necesidades de su organización. Pulse "Aceptar" para guardar la configuración. 
140.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta "C:\Scripts" del servidor.

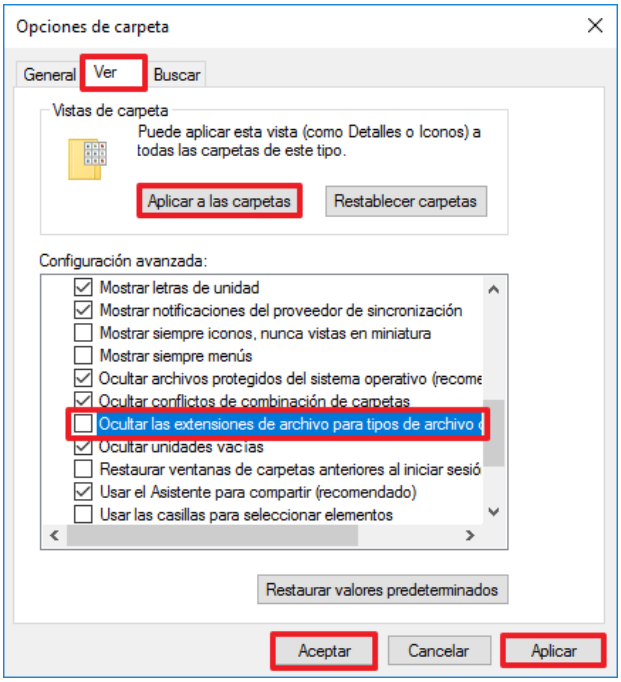
En este punto el servidor Citrix Storefront se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura. Una vez configurado el servidor con el rol Citrix Storefront deberá continuar con las configuraciones sobre el servidor con el rol Citrix Licensing.

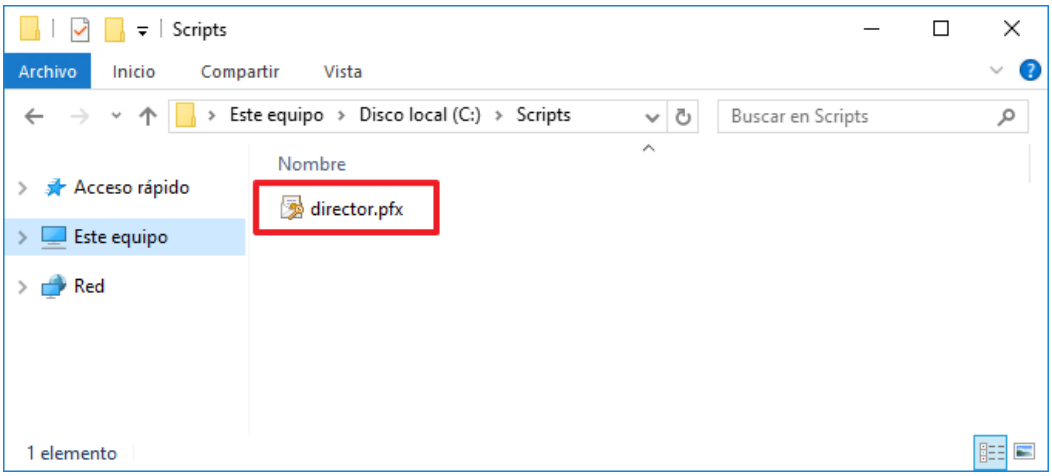
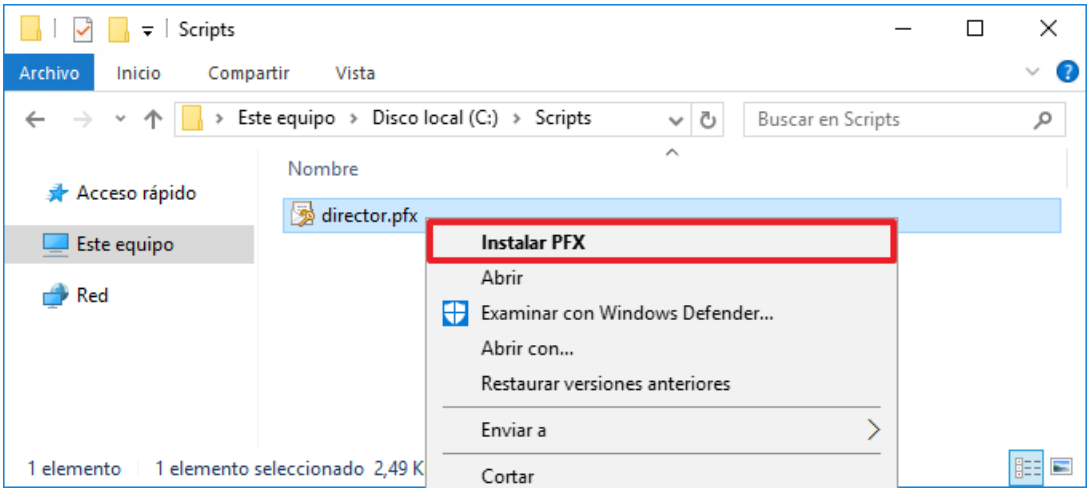
Paso	Descripción
141.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS. **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
142.	Copie los archivos de certificados "server.crt" y "server.key" que deberá haber generado previamente a las siguientes rutas. – C:\Pogram Files (x86)\Citrix\Licensing\WebServicesForLicensing\Apache\conf – C:\Pogram Files (x86)\Citrix\Licensing\LS\conf   **Nota:** En esta guía la instalación del rol Citrix Licensing se ha efectuado sobre la unidad "C:\". Deberá copiar los archivos de certificados adaptando este paso a la ruta de instalación del rol Citrix Licensing en su organización. No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar. El sistema solicitará elevación de privilegios.

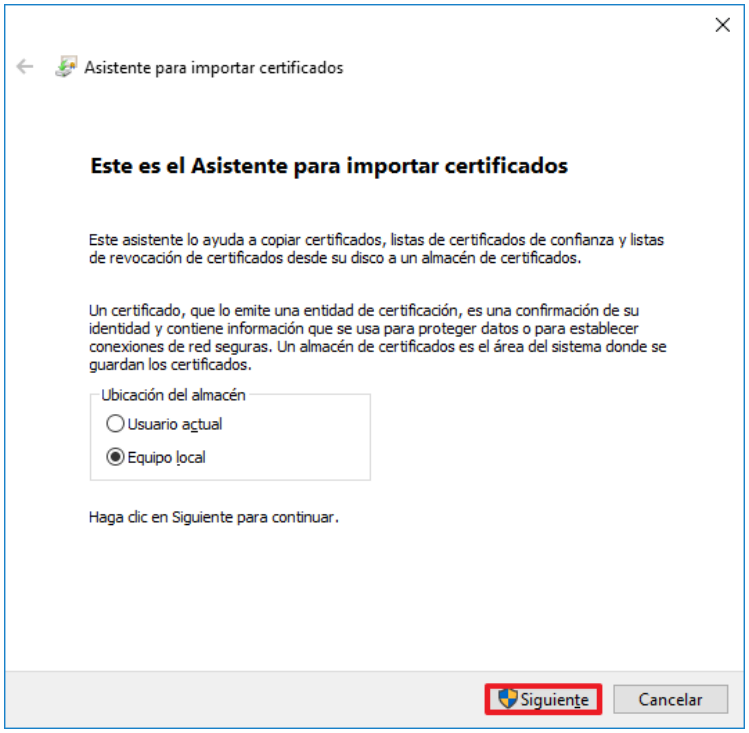
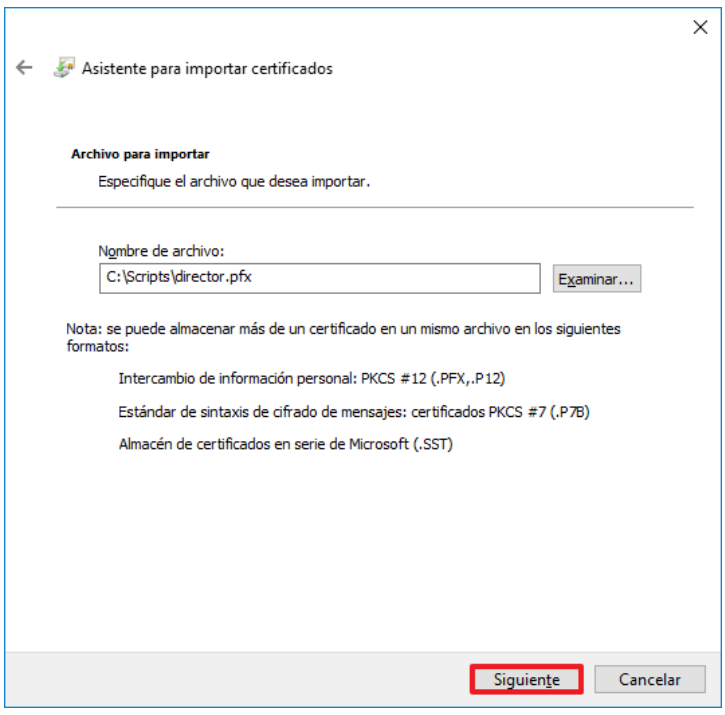
Paso	Descripción
143.	Abra un terminal “cmd.exe” con privilegios de administrador, y ejecute los siguientes comandos para reiniciar los servicios “Citrix Licensing” y “CitrixWebServicesforLicensing”. – net stop "Citrix Licensing" – net start "Citrix Licensing" – net stop "CitrixWebServicesforLicensing" – net start "CitrixWebServicesforLicensing" 

En este punto el servidor Citrix Licensing se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura. Una vez configurado el servidor con el rol Citrix Licensing deberá continuar con las configuraciones sobre el servidor con el rol Citrix Director.

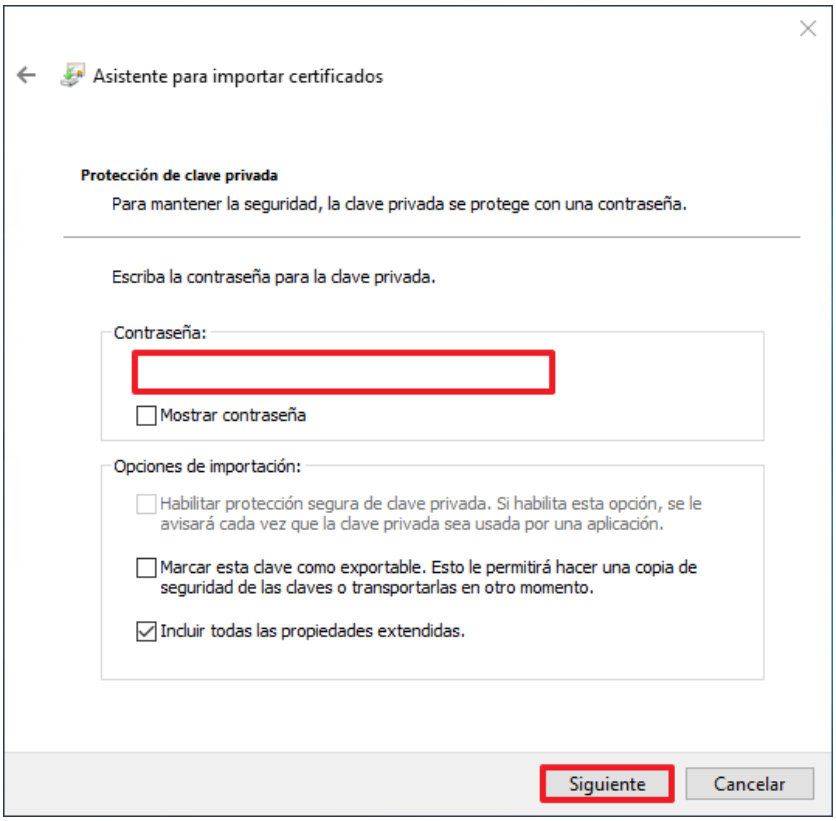
Paso	Descripción
144.	Inicie sesión en un servidor con el rol Citrix Director del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
145.	Cree el directorio “Scripts” en la unidad “C:\”.

Paso	Descripción
146.	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. Para configurar “Explorador de Windows” y poder mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
147.	Para continuar, debe realizar la solicitud de un certificado válido en el dominio, cuyo Nombre común “CN” coincida con el FQDN del equipo sobre el que está implementando el rol Citrix Director. No debe utilizar un certificado de tipo wildcard ya que de utilizarlo encontrará problemas en los siguientes pasos de configuración. **Nota:** No es el objetivo de esta guía mostrarle el proceso de obtención de un certificado ya que dependiendo de su organización los pasos pueden variar.

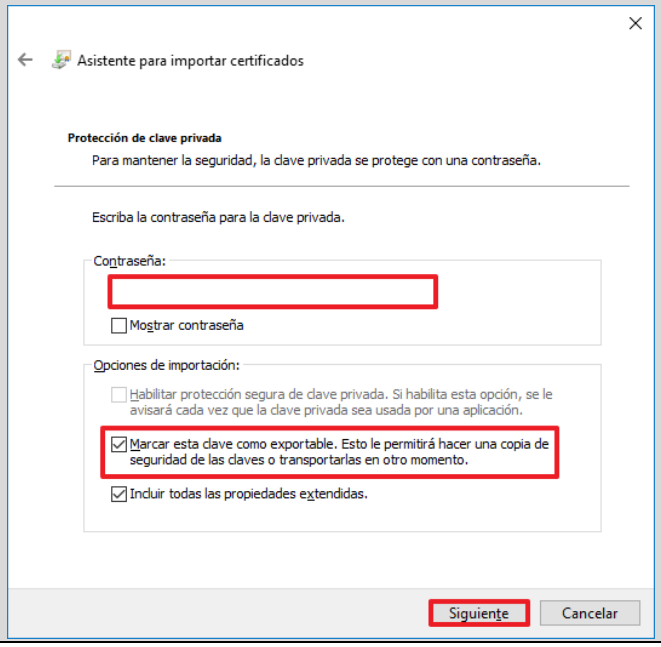
Paso	Descripción
148.	Copie el certificado en la unidad "C:\Scripts" y establezca un nombre de fichero identificativo. En esta guía se utilizará el fichero **"C:\Scripts\director.pfx"** a modo de ejemplo, no dude en ajustar el nombre de su archivo en los siguientes pasos. 
149.	Si no lo ha hecho todavía, proceda con los siguientes pasos para realizar la instalación del certificado sobre el almacén **"Personal"** de equipo.
150.	Pulsando con el botón derecho sobre el certificado, pulse sobre la opción **"Instalar PFX"** tal y como se indica en la siguiente figura. 

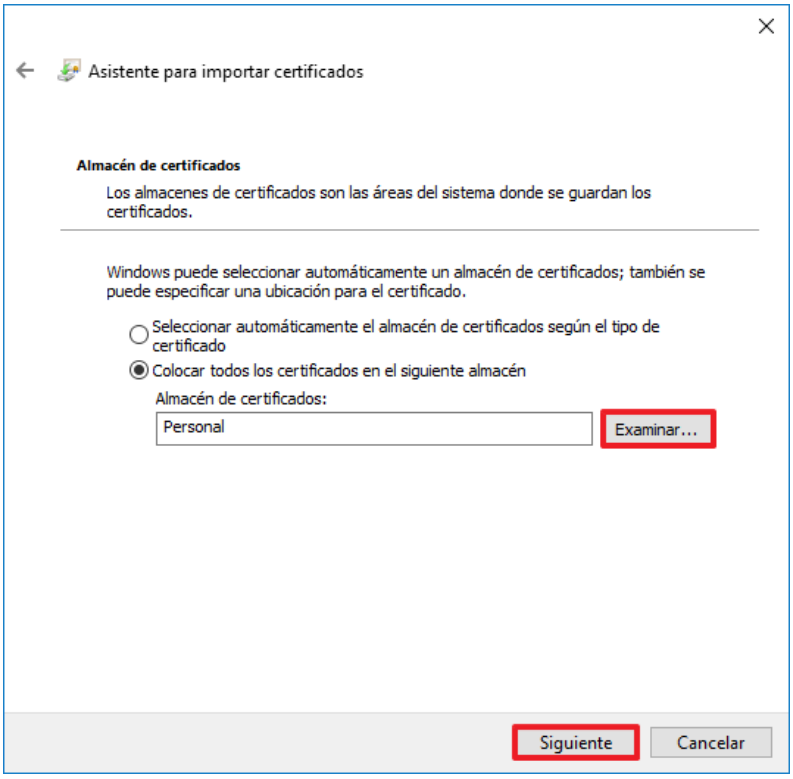
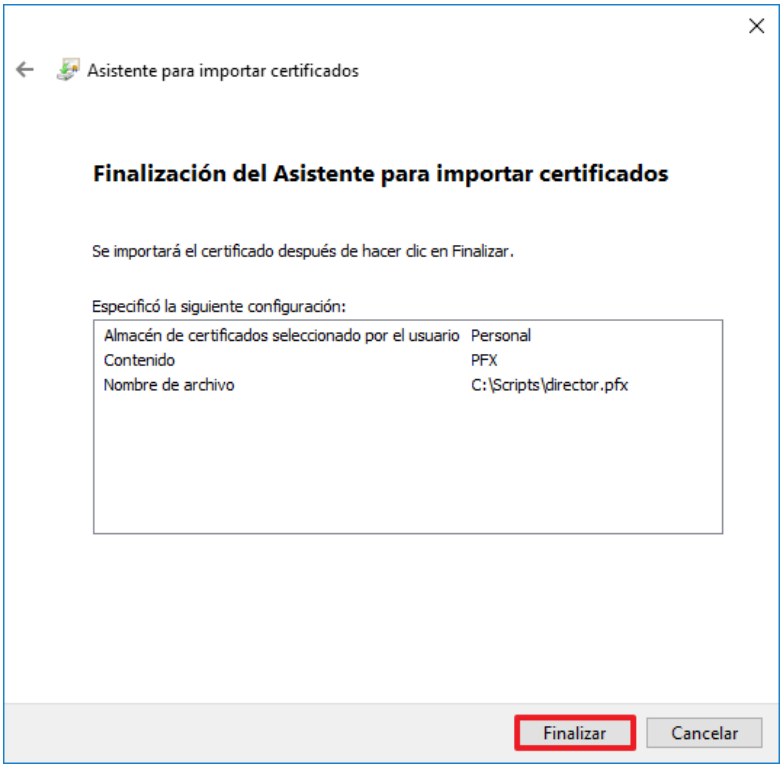
Paso	Descripción
151.	Se iniciará el asistente de importación de certificados. Pulse sobre “Equipo local” y a continuación pulse sobre “Siguiente”.  **Nota:** El sistema solicitará elevación de privilegios.
152.	Especifique el archivo a importar y continúe con el asistente pulsando sobre “Siguiente”. 

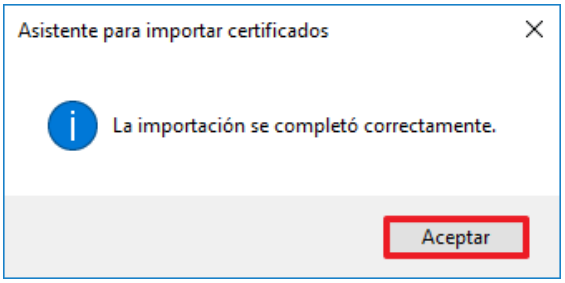
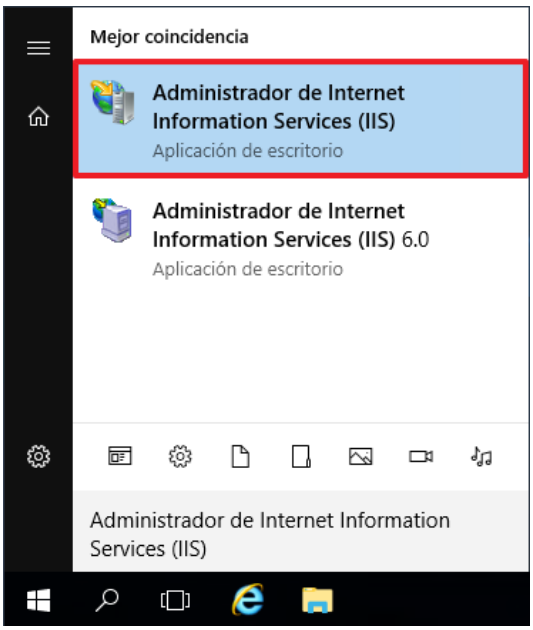
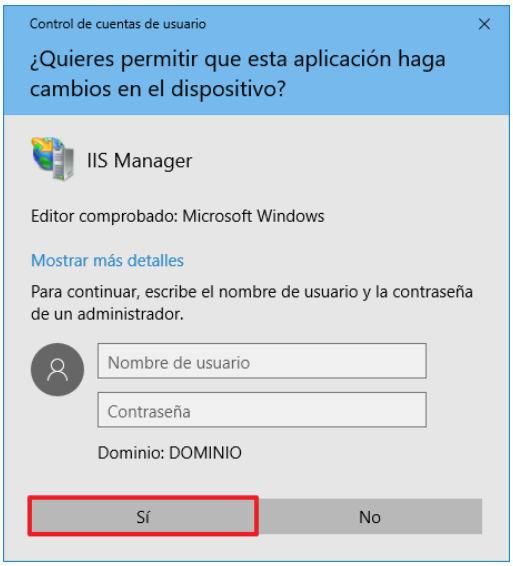
Paso	Descripción
153.	Establezca la contraseña de importación para la clave privada. Pulse “Siguiente” para continuar.

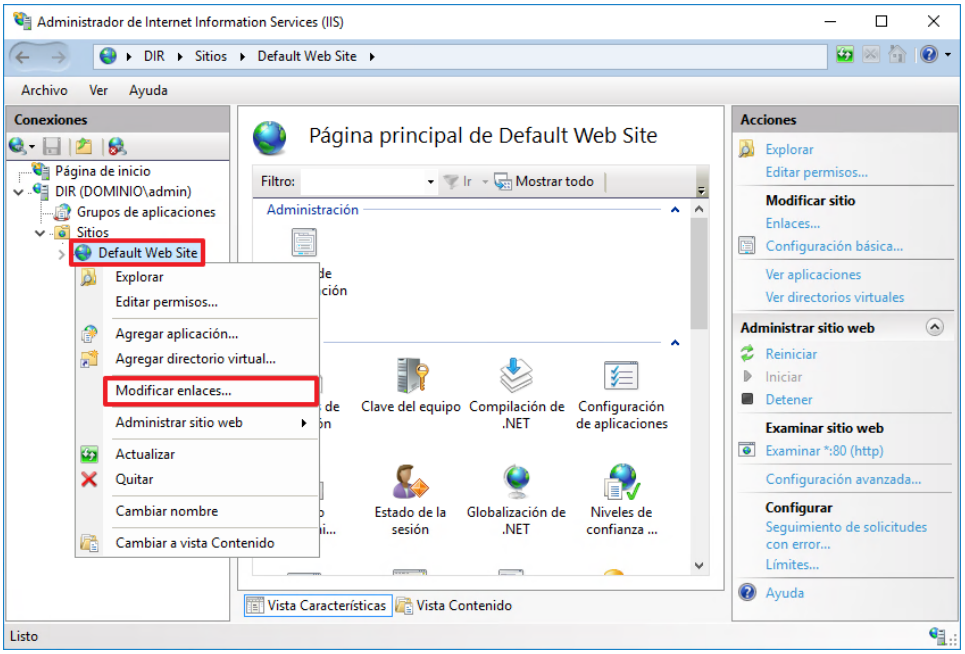
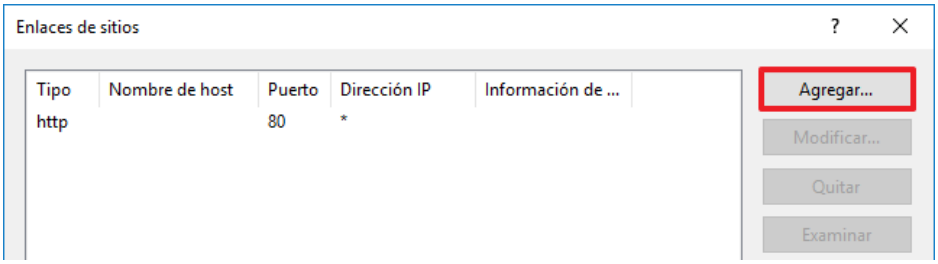
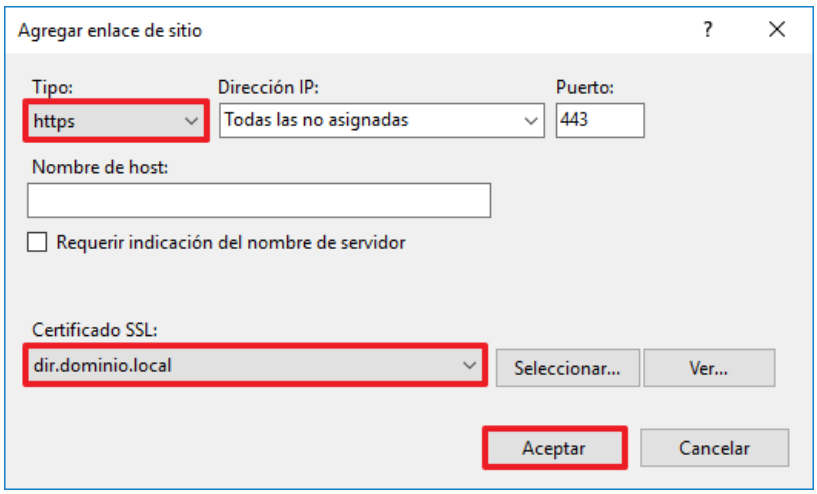


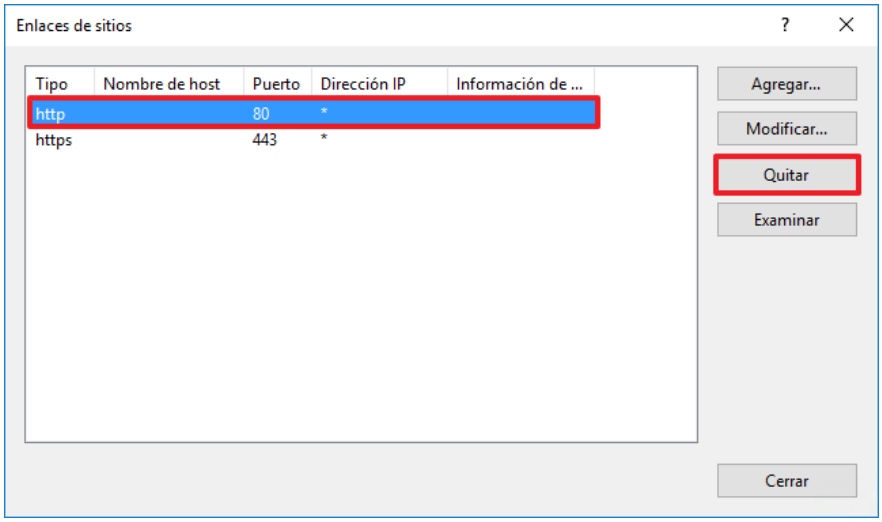
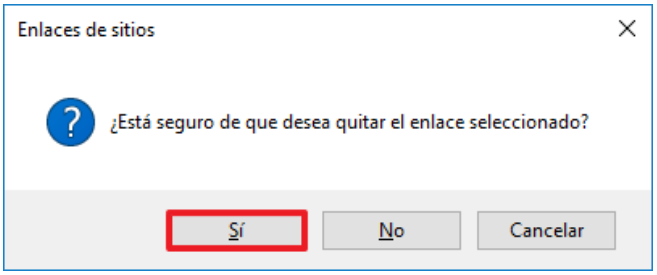
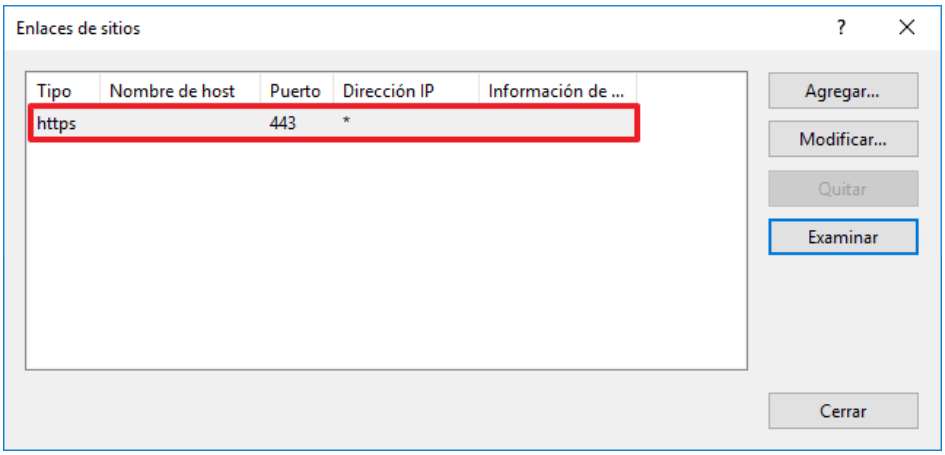
Nota: Opcionalmente puede marcar la casilla “Marcar esta clave como exportable” para permitirle en un futuro exportar la clave privada del certificado. Esta opción puede serle de utilidad para crear copias de seguridad de los certificados e instalar los mismos en diferentes equipos de su entorno.

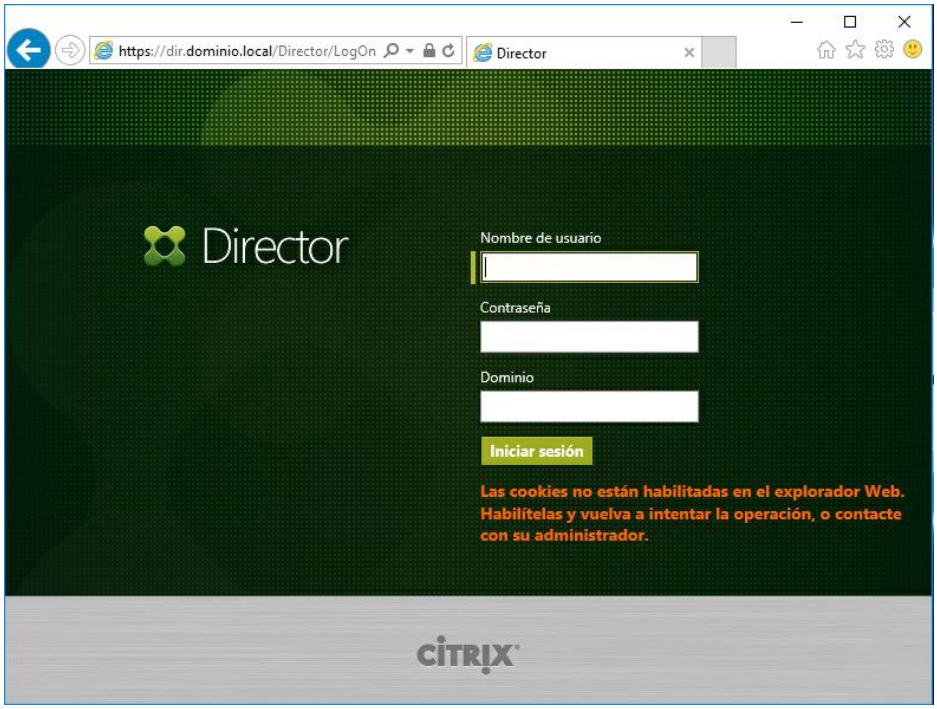


Paso	Descripción
154.	Localice el almacén “Personal” del equipo pulsando sobre “Examinar” tal y como se muestra en la siguiente figura. Una vez establecido, pulse “Siguiente” para continuar. 
155.	El último punto del asistente muestra un resumen, pulse “Finalizar” para completar la importación del certificado sobre el equipo. 

Paso	Descripción
156.	Espere unos segundos a que finalice el proceso, aparecerá un mensaje indicando que la importación se realizó correctamente. 
157.	Acto seguido, verá reflejados los cambios, continúe el proceso abriendo la consola **"Administrador de Internet Information Services (IIS)"**. 
158.	El sistema solicitará elevación de privilegios. 

Paso	Descripción
159.	Abra el nodo de configuración **"<Su servidor> (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"**. 
160.	Sobre la ventana "Enlaces de sitios" pulse **"Agregar…"** para añadir un enlace nuevo. Por defecto, encontrará creado un enlace al puerto 80 que deberá eliminar más adelante para evitar conexiones no seguras al entorno. 
161.	Modifique en el formulario los parámetros necesarios y establezca su certificado SSL a utilizar, instalado en pasos anteriores. Pulse **"Aceptar"** para guardar los cambios". 

Paso	Descripción
162.	Con ambos enlaces creados, seleccione el enlace de Tipo “http” y acto seguido pulse sobre **“Quitar”**. 
163.	Sobre la ventana emergente, pulse “Si” para confirmar la eliminación del enlace seleccionado. 
164.	Al terminar, verifique que únicamente está configurado el enlace de Tipo “https” recién creado con su certificado SSL. 

Paso	Descripción
165.	Puede verificar que la configuración es correcta abriendo un navegador y accediendo a la URL base de su entorno, en este caso, a modo de ejemplo se verifica el acceso a la dirección https://dir.dominio.local/director.  **Nota:** Es posible que no tenga la herramienta "JavaScript" instalada en el equipo desde el que está accediendo al portal web. Será necesario realizar dicho proceso para el correcto funcionamiento del explorador. 
166.	Ya puede cerrar todas las consolas abiertas y eliminar la carpeta "C:\Scripts" del servidor.

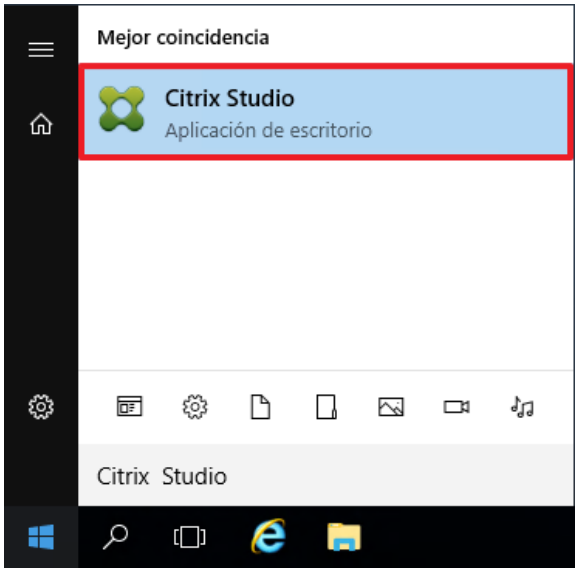
En este punto el servidor con el rol de Citrix Director se encuentra configurado y con las directivas de seguridad que aseguran sus comunicaciones con el resto de servicios de la infraestructura.

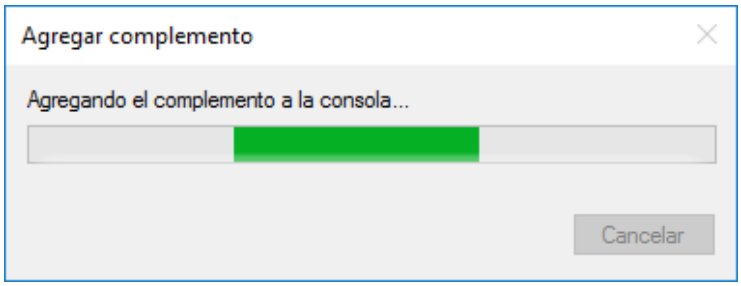
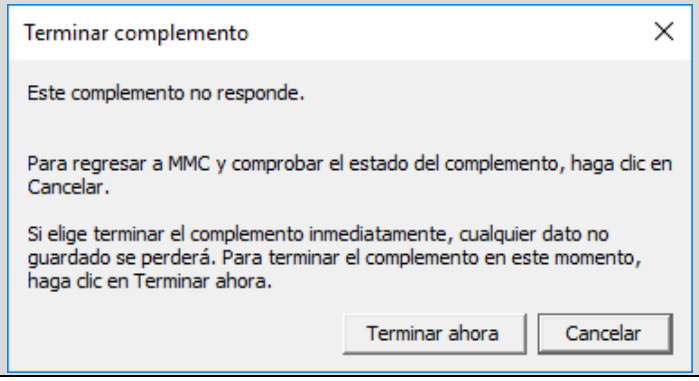
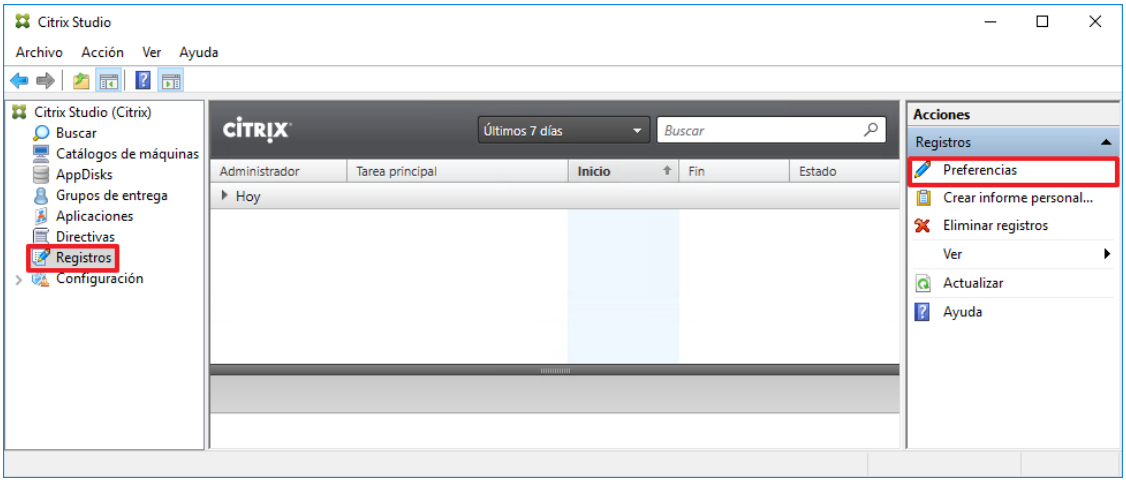
4. AUDITORÍA

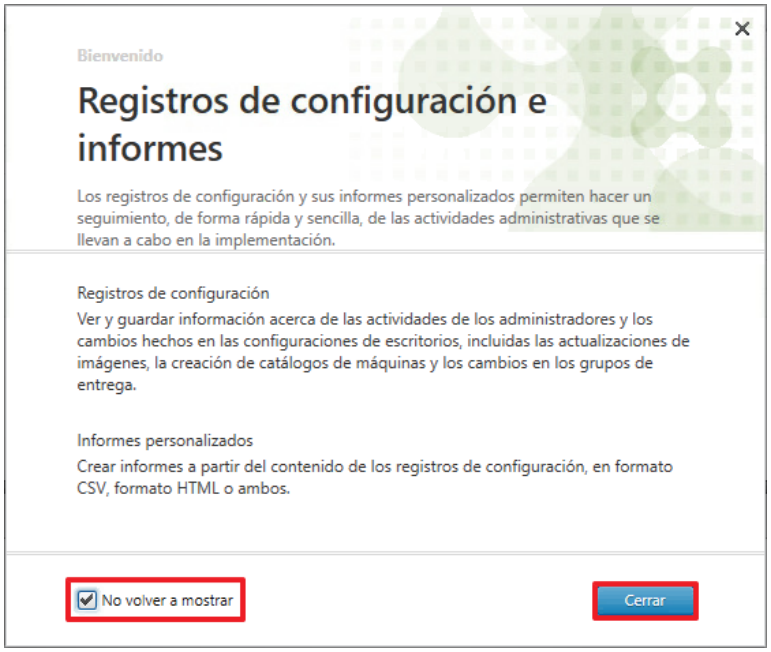
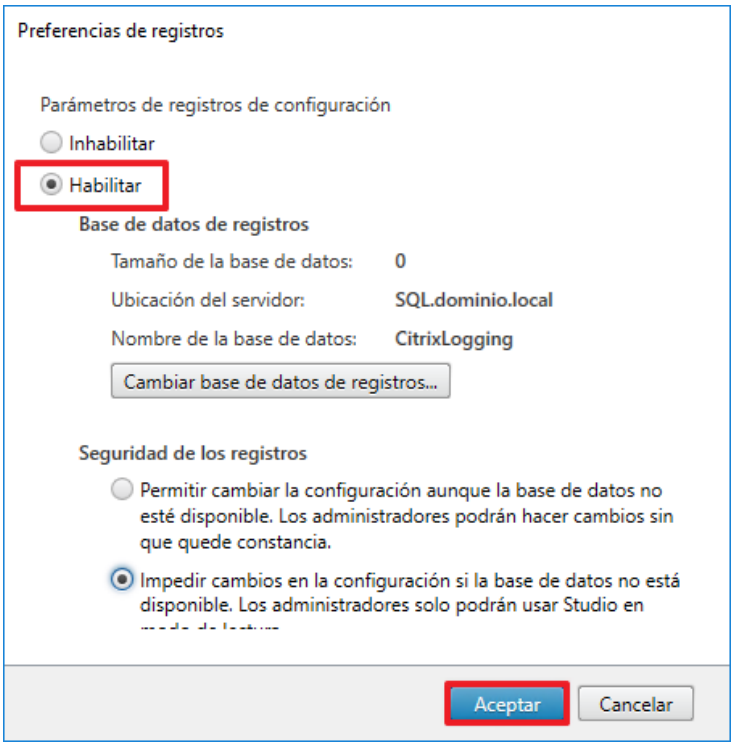
Con la aplicación del ENS para la categoría alta o Difusión Limitada sobre Citrix Virtual Apps and Desktops quedará registrado el uso del sistema para poder detectar y reaccionar a cualquier fallo accidental o deliberado, quedando registrado en el sistema quien realiza la actividad, cuando y sobre qué información con el fin de detectar anomalías o intentos frustrados de acceso a información no autorizada.

Para la categoría más alta de seguridad del ENS deberá definir como "Habilitados" los registros sobre las modificaciones que se hagan en la infraestructura de Citrix Virtual Apps and Desktops.

Para ello, será necesario comprobar sobre el rol Citrix Controller que dicha configuración se encuentre configurada correctamente.

Paso	Descripción
167.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
168.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios.

Paso	Descripción
169.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
170.	A continuación, diríjase al nodo de configuración **"Citrix Studio → Registros → Acciones"** y pulse sobre "Preferencias". 

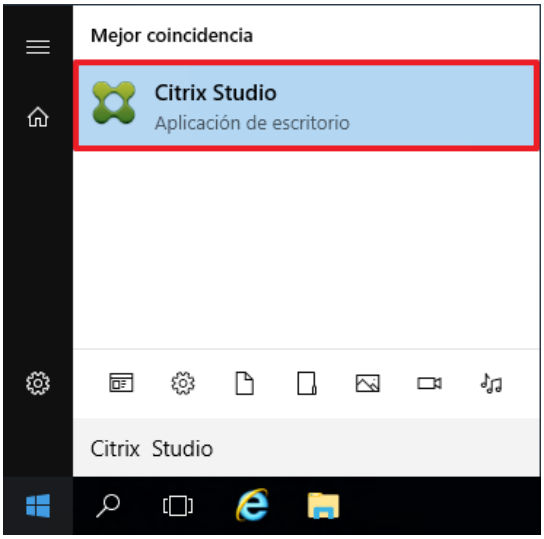
Paso	Descripción
171.	Al navegar por primera vez por los diferentes nodos de la herramienta aparecerán distintos mensajes de bienvenida, marque la casilla “No volver a mostrar” y pulse “Cerrar” en cada uno de ellos. 
172.	Sobre la ventana emergente “Preferencias de registros” compruebe que la opción **“Habilitar”** se encuentra seleccionada como se indica en la siguiente figura. Pulse “Aceptar” para continuar. 

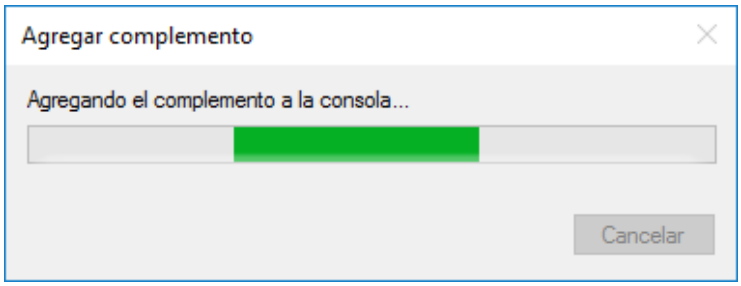
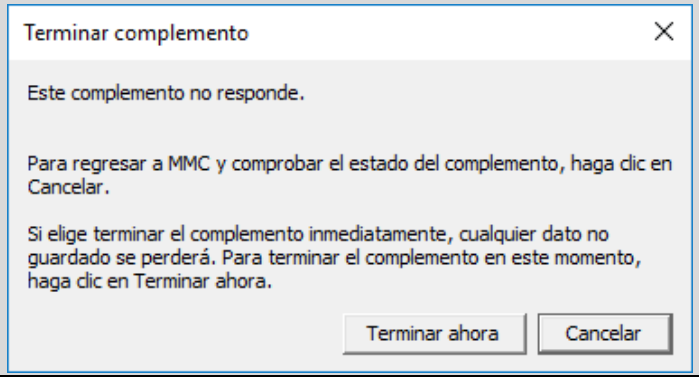
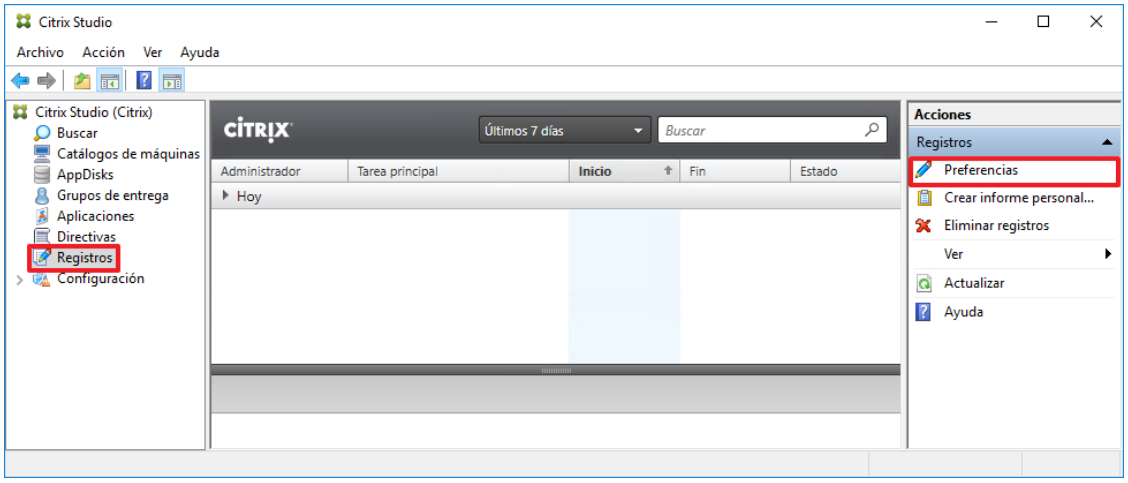
5. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

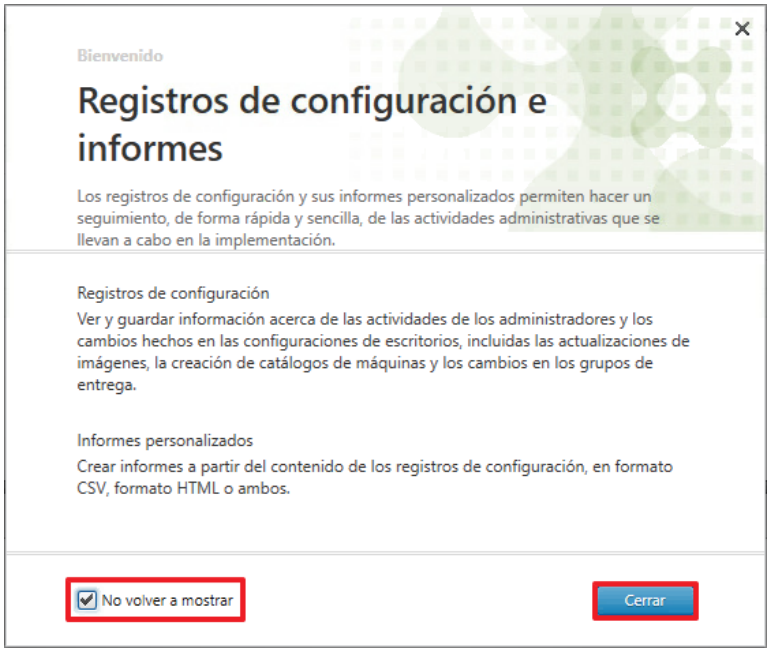
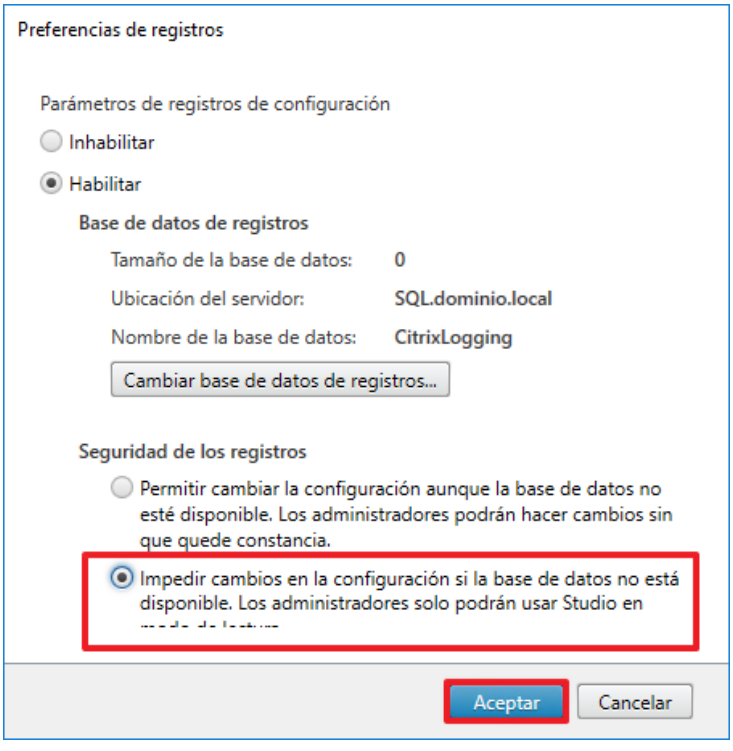
Aplicable en las categorías media y alta de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones que se realizan sobre los servidores de la infraestructura de Citrix Virtual Apps and Desktops.

Para este fin, se deberá impedir cualquier modificación de las configuraciones en caso de que la base de datos en la que se recogen los registros de dichas modificaciones no esté disponible.

Esta configuración se deberá llevar a cabo en la herramienta Citrix Studio instalada en el servidor con el rol Citrix Controller de su infraestructura.

Paso	Descripción
173.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
174.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios

Paso	Descripción
175.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
176.	A continuación, diríjase al nodo de configuración **"Citrix Studio → Registros → Acciones"** y pulse sobre "Preferencias". 

Paso	Descripción
177.	Al navegar por primera vez por los diferentes nodos de la herramienta aparecerán distintos mensajes de bienvenida, marque la casilla “No volver a mostrar” y pulse “Cerrar” en cada uno de ellos. 
178.	Sobre la ventana emergente “Preferencias de registros” marque la opción **“Impedir cambios en la configuración si la base de datos no está disponible. Los administradores solo podrán utilizar Studio en modo de lectura”** como se indica en la siguiente figura. Pulse “Aceptar” para continuar. 

6. GESTIÓN DE DERECHOS DE ACCESO

Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda realizar tareas que no son requeridas para las funciones que desempeña.

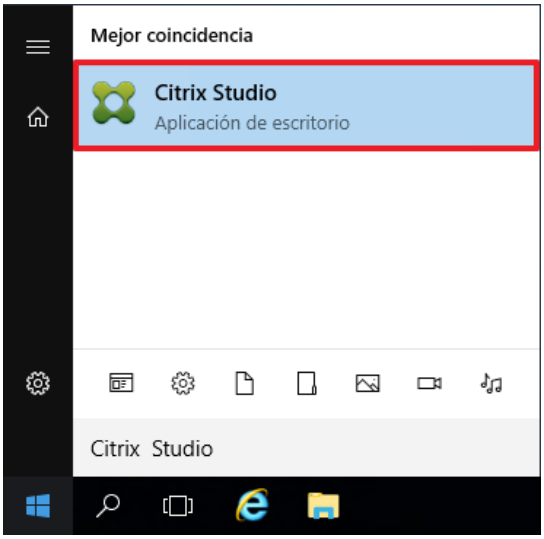
Para tal fin y de acuerdo con el Esquema Nacional de Seguridad se deberán definir, mediante grupos de seguridad, los usuarios que según su organización deban administrar la infraestructura y eliminar aquellos administradores genéricos que puedan existir.

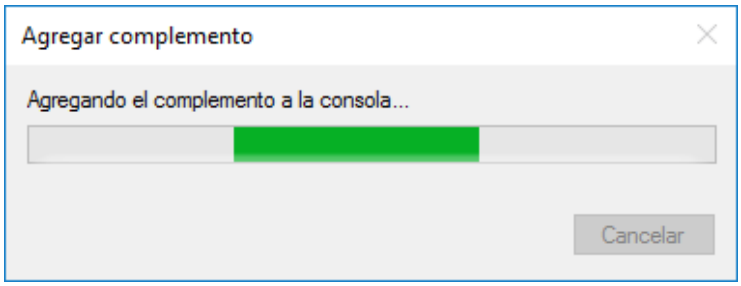
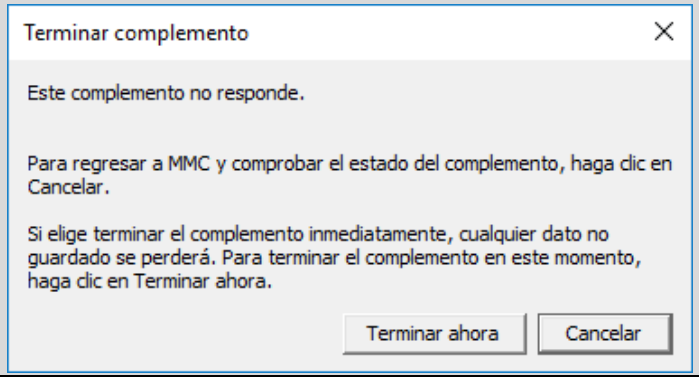
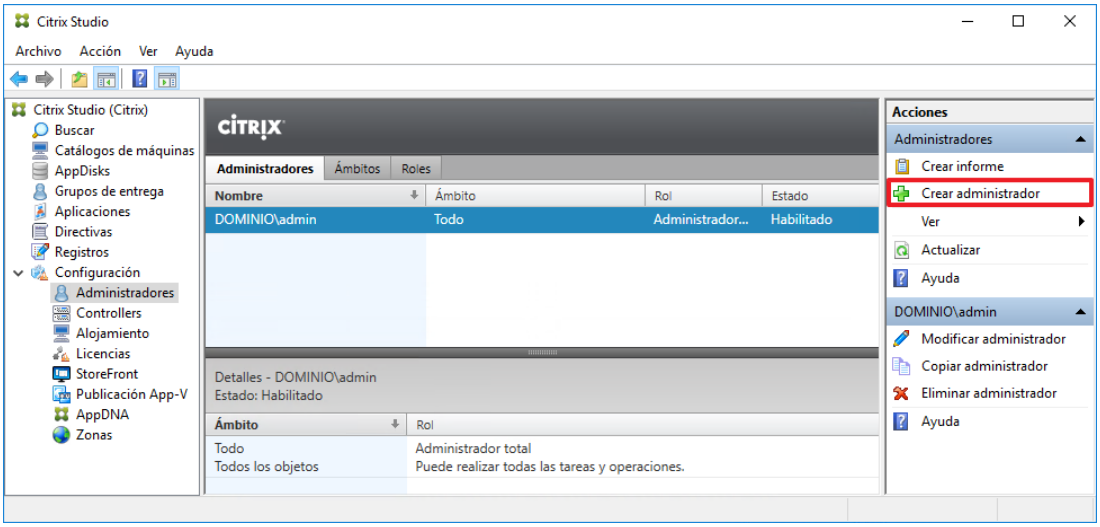
Esta configuración será de aplicación en los siguientes servidores de su infraestructura Citrix Virtual Apps and Desktops:

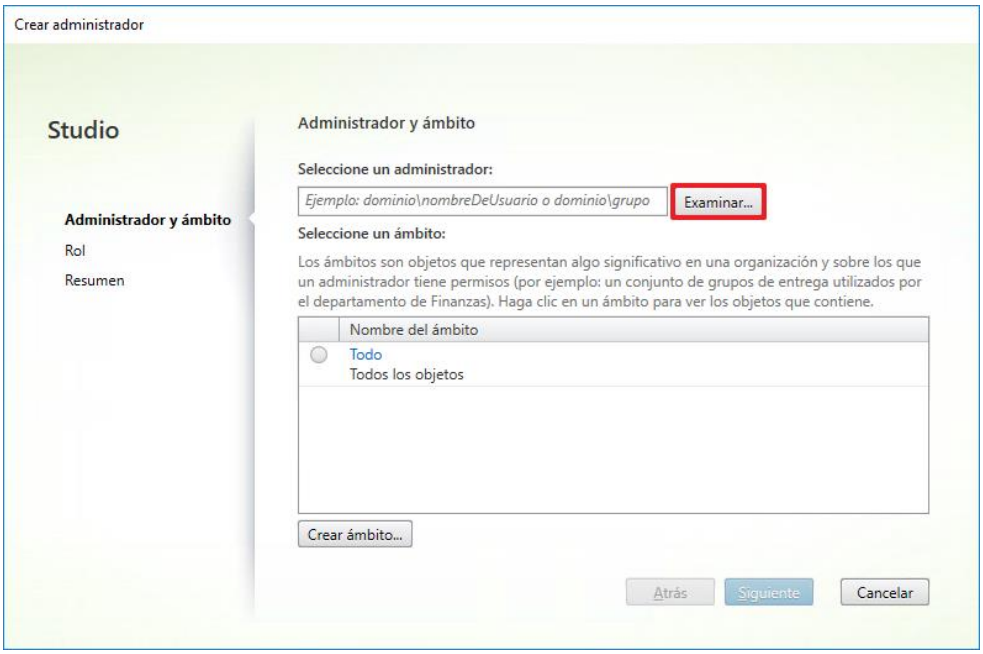
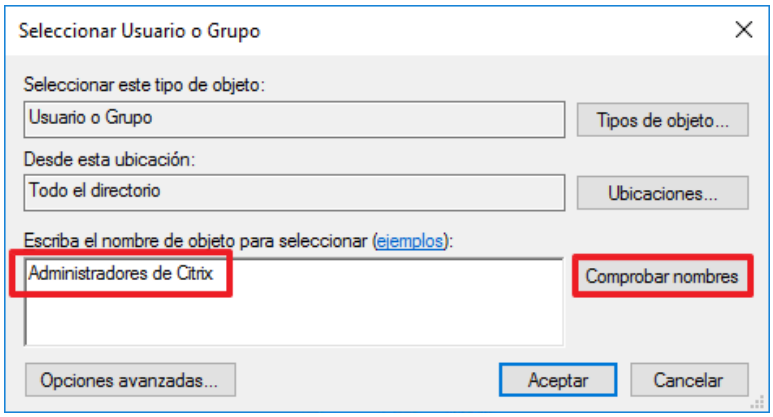
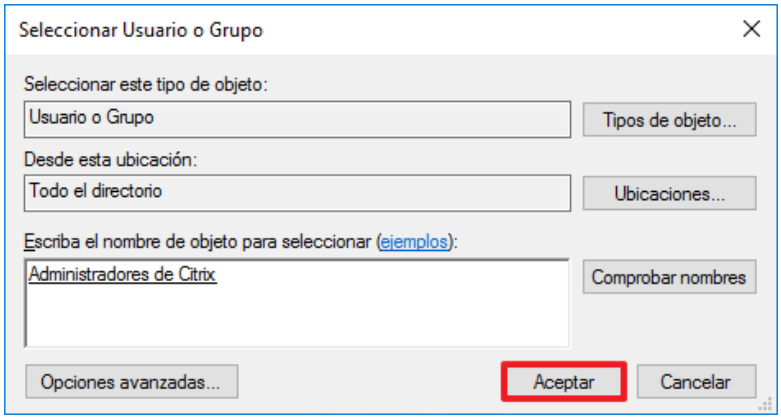
a) Servidor con el rol Citrix Controller

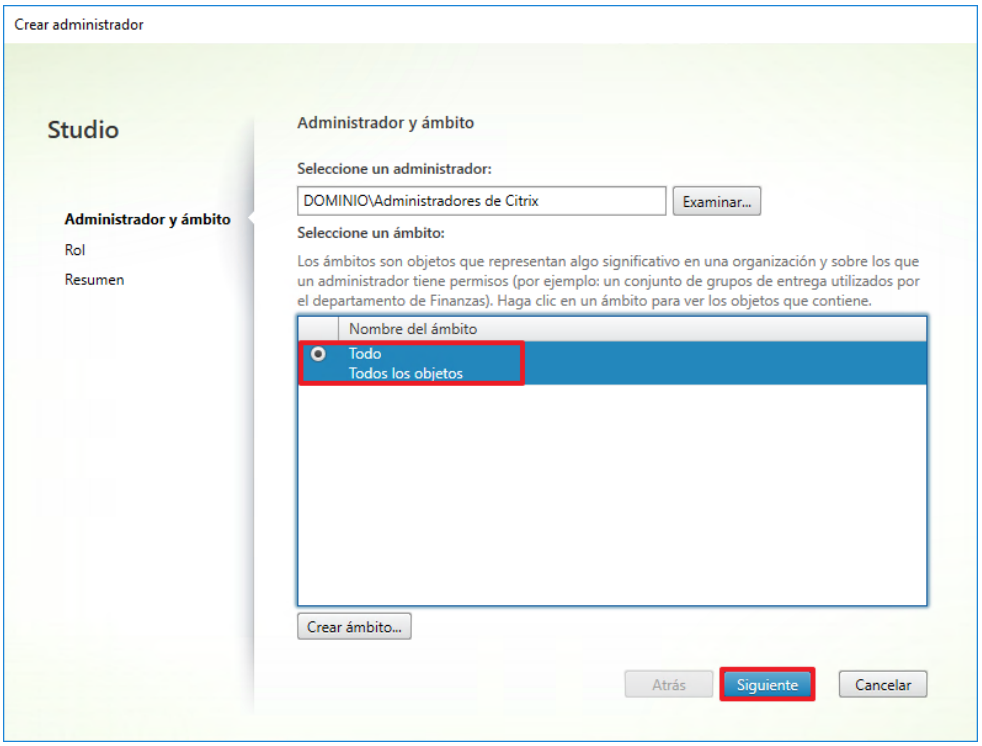
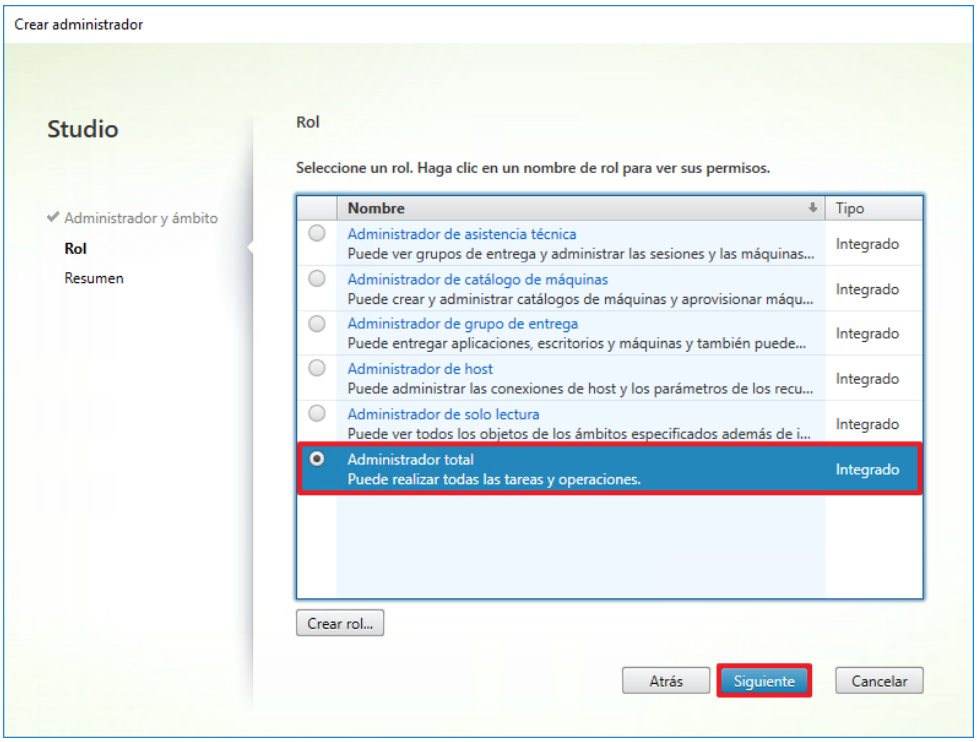
b) Servidor con el rol Citrix Licensing

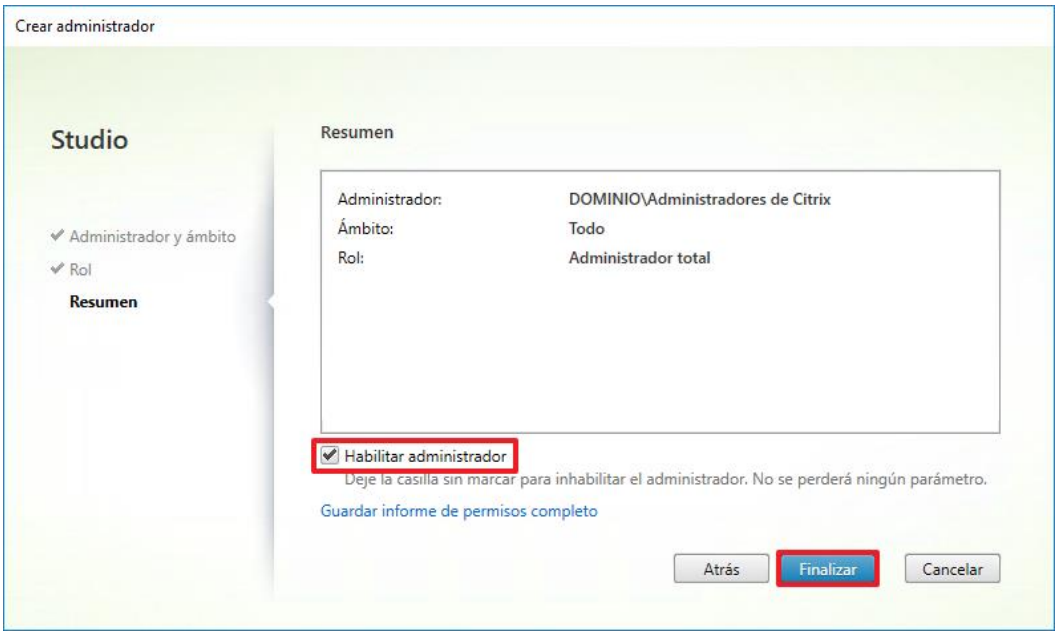
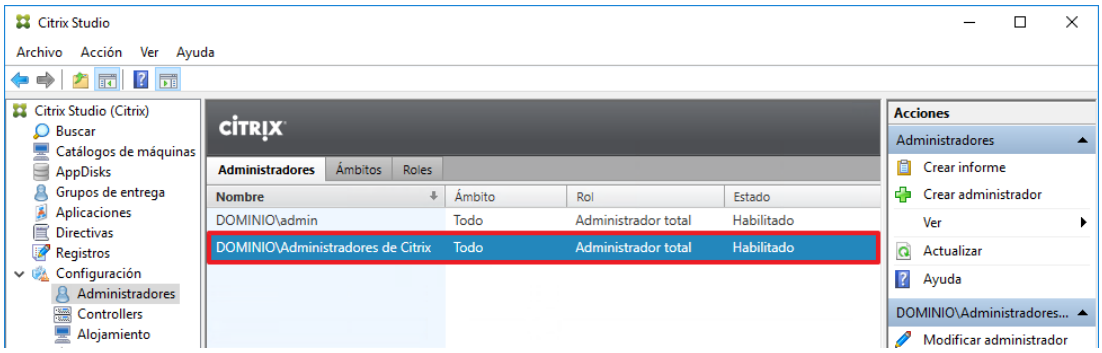
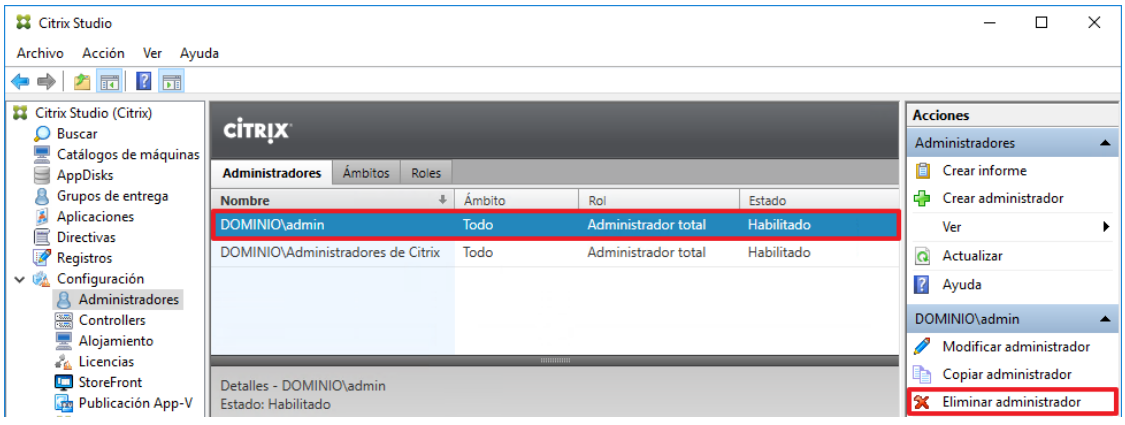
En primer lugar, se realizarán las configuraciones necesarias sobre el servidor con el rol Citrix Controller instalado.

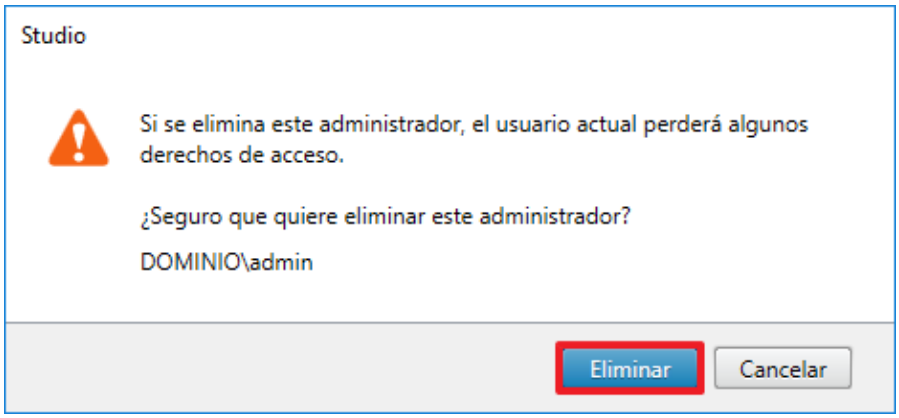
Paso	Descripción
179.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
180.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios.

Paso	Descripción
181.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
182.	Diríjase al menú de configuración **"Citrix Studio → Configuración → Administradores → Administradores"** y pulse sobre "Crear administrador". 

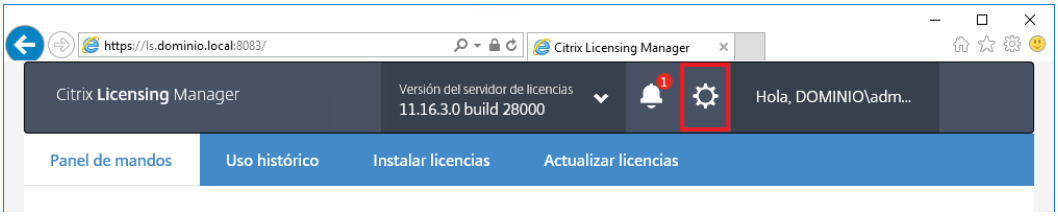
Paso	Descripción
183.	Sobre la ventana emergente, “Crear administrador” pulse sobre “Examinar”. 
184.	Introduzca el nombre del objeto “Administradores de Citrix” y pulse sobre “Comprobar nombres”. 
185.	Compruebe que el objeto “Administradores de Citrix” ha sido añadido correctamente. Pulse “Aceptar” para añadir el objeto y cerrar la ventana. 

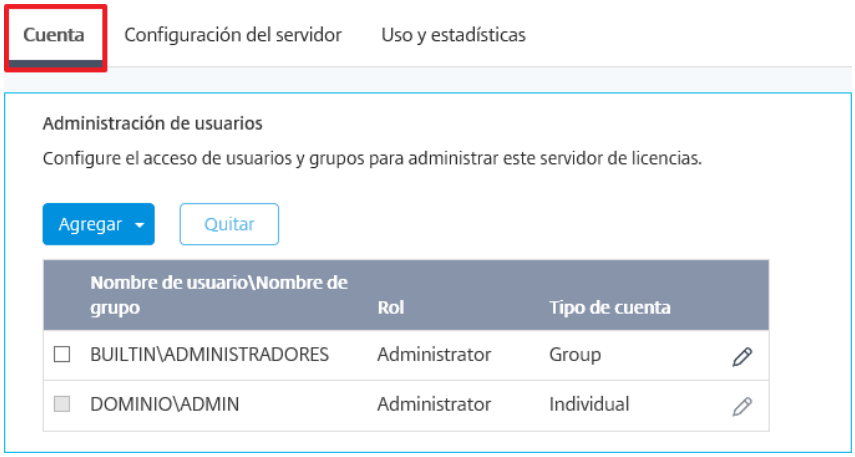
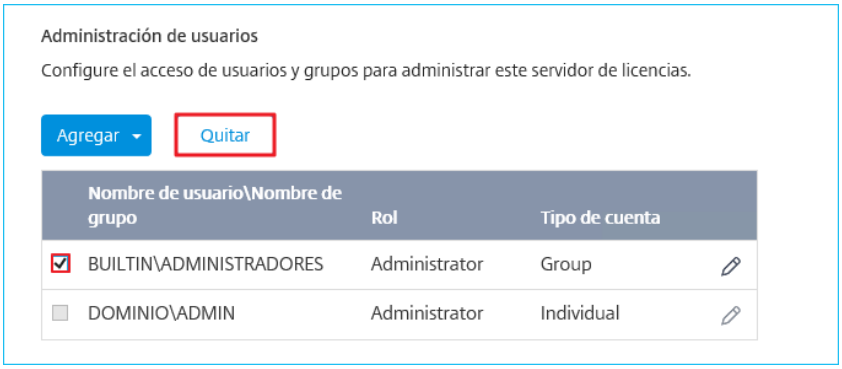
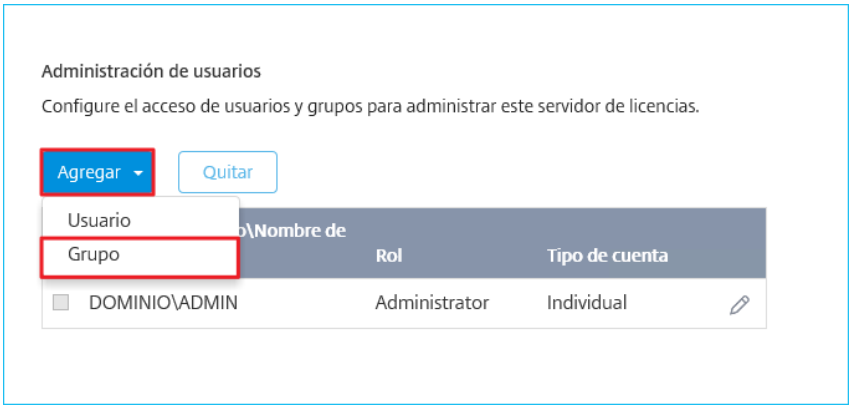
Paso	Descripción
186.	De vuelta en la ventana “Crear administrador”, seleccione el ámbito “Todo” y pulse “Siguiente”. 
187.	Marque el rol “Administrador total” y pulse sobre “Siguiente”.  **Nota:** Para una adecuada gestión de derechos de acceso a la administración de Citrix Studio, deberá crear previamente los grupos correspondientes en el dominio, asociados a los roles de administración que más se adecuen a su organización.

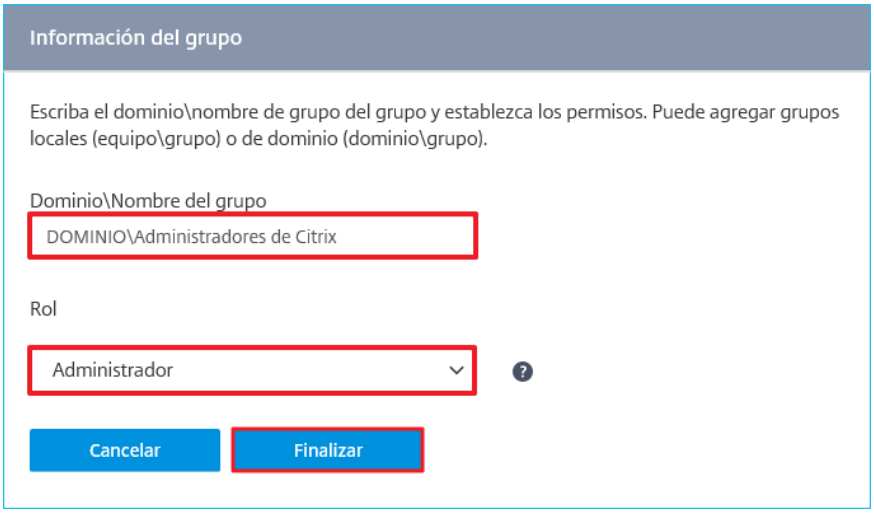
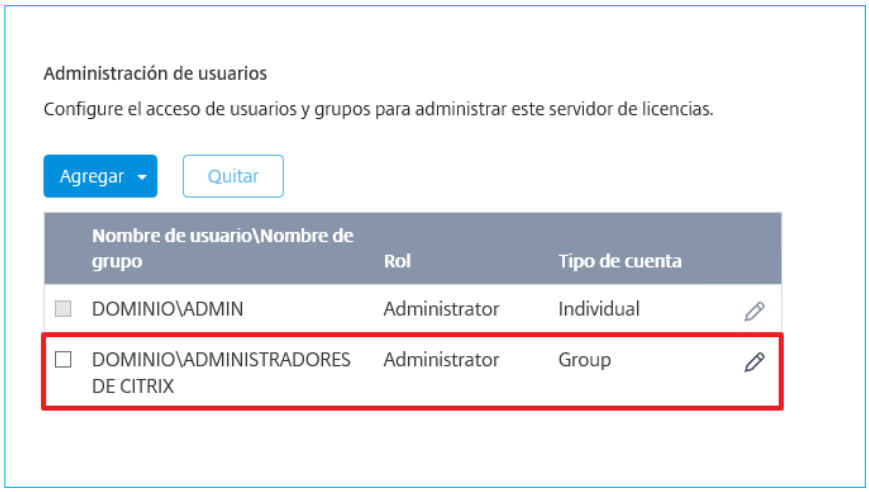
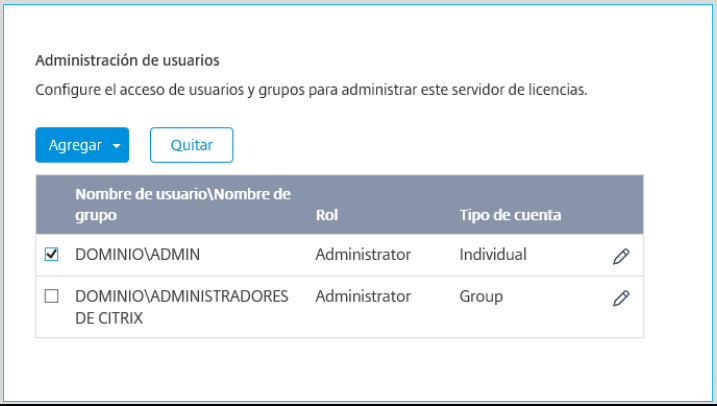
Paso	Descripción
188.	Verifique que la casilla **"Habilitar administrador"** está marcada y pulse sobre "Finalizar". 
189.	Acto seguido apreciará el grupo recientemente creado en la consola. 
190.	Para finalizar con el proceso debe eliminar cualquier usuario administrador que esté introducido a mano en el sistema. Marque el usuario y pulse sobre "Eliminar administrador". 

Paso	Descripción
191.	El sistema le indicará una advertencia indicando que el usuario actual perderá algunos derechos de acceso. Ignore la advertencia y pulse sobre “Eliminar”. 

A continuación, se procederá a realizar las configuraciones de seguridad necesarias en el servidor con el rol Citrix Licensing.

Paso	Descripción
192.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
193.	Acceda a la dirección URL del “Citrix Licensing Manager” https://ls.dominio.local:8083 adaptándolo a su entorno.
194.	Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre la rueda superior derecha. 

Paso	Descripción
195.	A continuación, acceda al nodo de configuración “Cuenta”, en los siguientes pasos definirá los administradores de licencias del servidor. Por defecto, el instalador del producto define los siguientes administradores. – BUILTIN\ADMINISTRADORES – DOMINIO\ADMIN  **Nota:** El usuario “DOMINIO\admin” se corresponde con el usuario utilizado para realizar el proceso de instalación del sistema y variará dependiendo de su entorno.
196.	Seleccione el grupo “BUILTIN\ADMINISTRADORES” y acto seguido pulse sobre el botón “Quitar”. 
197.	Despliegue el menú extraíble pulsando sobre el botón “Agregar” y pulse sobre “Grupo”. 

Paso	Descripción
198.	En la ventana emergente de configuración especifique el grupo creado anteriormente “DOMINIO\Administradores de Citrix” que deberá tener el rol “Administrador”. Pulse sobre “Finalizar” para añadir el nuevo grupo administrador. 
199.	Verifique que el grupo se ha agregado correctamente desde el apartado “Cuenta”.  **Nota:** Para eliminar el usuario con el que realizó la instalación deberá acceder al servidor con otro usuario diferente que pertenezca al grupo “DOMINIO\Administradores de Citrix” y proceder con su eliminación como en pasos anteriores. 

7. 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.

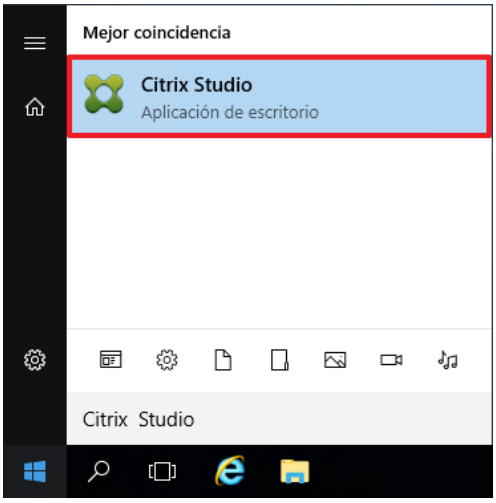
En el procedimiento que se describe a continuación, se desactiva el "Citrix Customer Experience Improvement Program" para evitar el envío de información al fabricante.

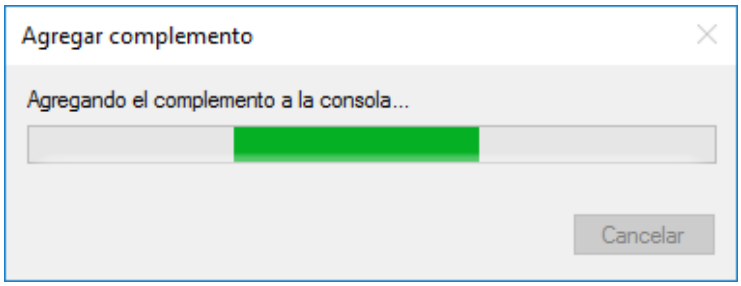
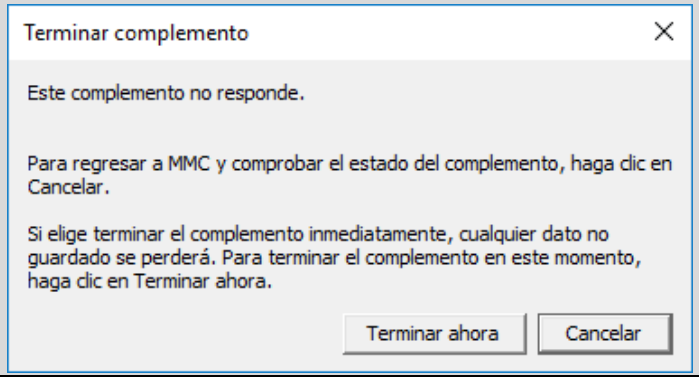
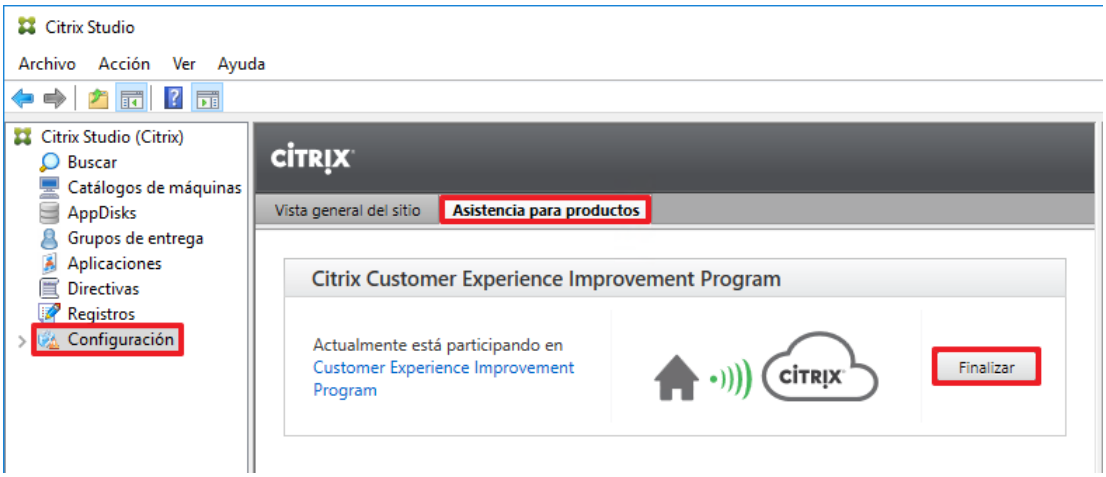
Esta configuración será de aplicación en los siguientes servidores de su infraestructura Citrix Virtual Apps and Desktops:

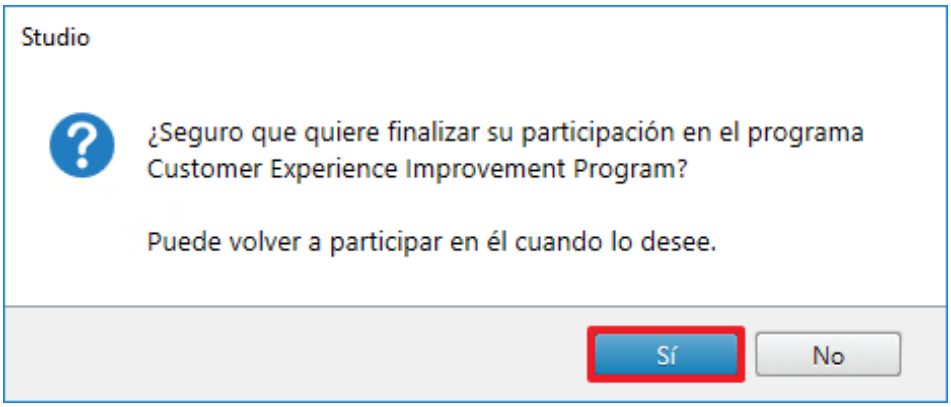
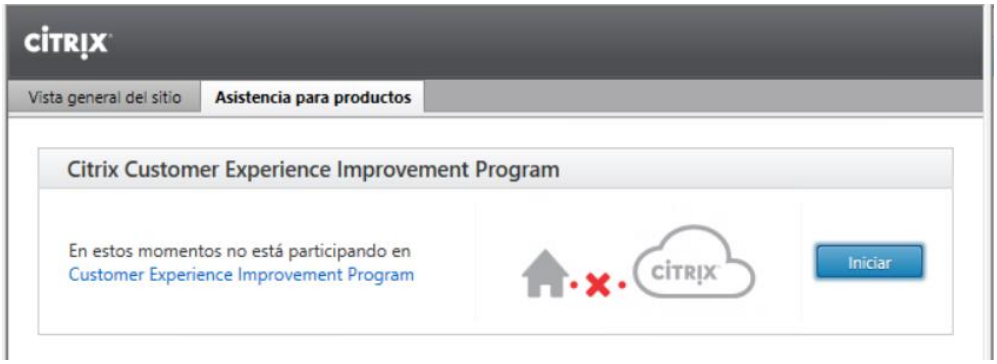
a) Servidor con el rol Citrix Controller

b) Servidor con el rol Citrix Licensing

En primer lugar, se realizarán las configuraciones necesarias sobre el servidor con el rol Citrix Controller instalado.

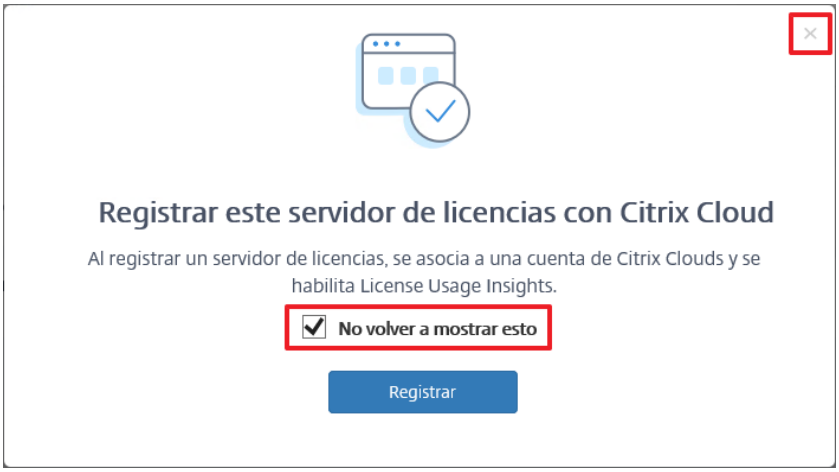
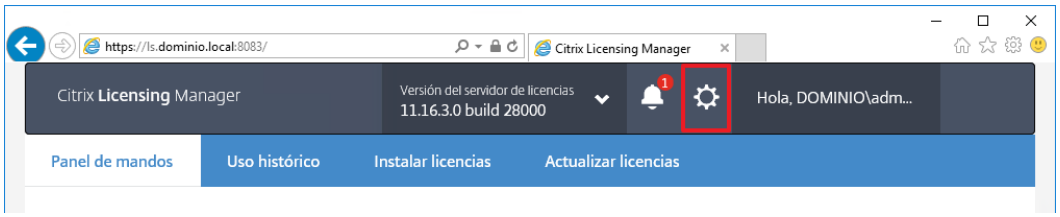
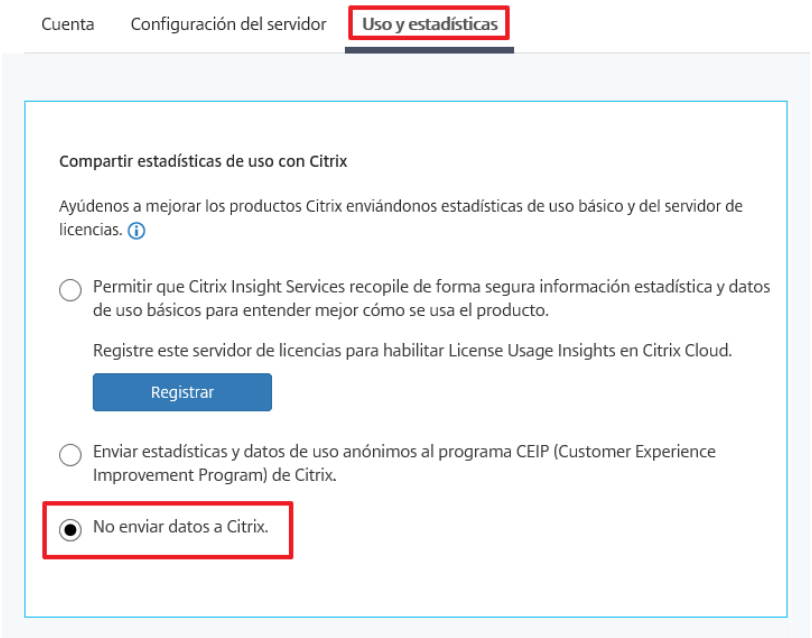
Paso	Descripción
200.	Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
201.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.  **Nota:** El sistema solicitará elevación de privilegios.

Paso	Descripción
202.	Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.  **Nota:** Ignore cualquier advertencia que le indique que el complemento no responde, debido a que el entorno no cuenta con salida a internet, la propia consola no puede validar la revocación de los certificados y muestra dichos errores. Pulse "Cancelar" para continuar. 
203.	Sobre la consola "Citrix Studio" diríjase al nodo **"Citrix Studio → Configuración → Asistencia para productos"**. Por defecto, los productos de Citrix participan automáticamente en el "Customer Experience Improvement Program" por lo que envían información a Citrix para la solución de errores en el producto. Pulse sobre "Finalizar" para detener el envío de información. 

Paso	Descripción
204.	En la ventana emergente que aparecerá pulse sobre “Si” para finalizar la participación en el programa. 
205.	Tras unos instantes puede apreciar como la consola indica que no está participando en el programa de mejora de la experiencia del usuario. 

A continuación, se procederá a realizar las configuraciones de seguridad necesarias en el servidor con el rol Citrix Licensing.

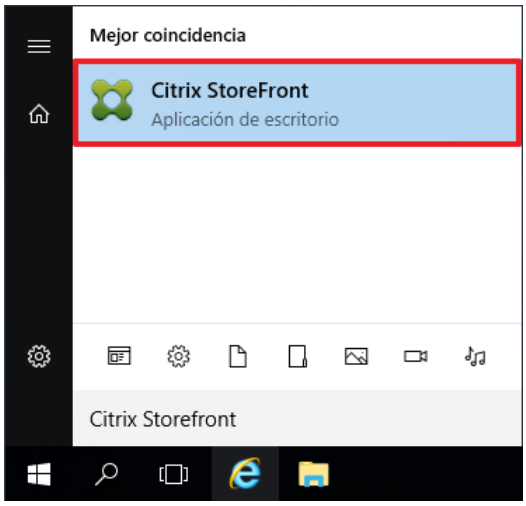
Paso	Descripción
206.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
207.	Acceda a la dirección URL del “Citrix Licensing Manager” https://ls.dominio.local:8083 adaptándolo a su entorno.

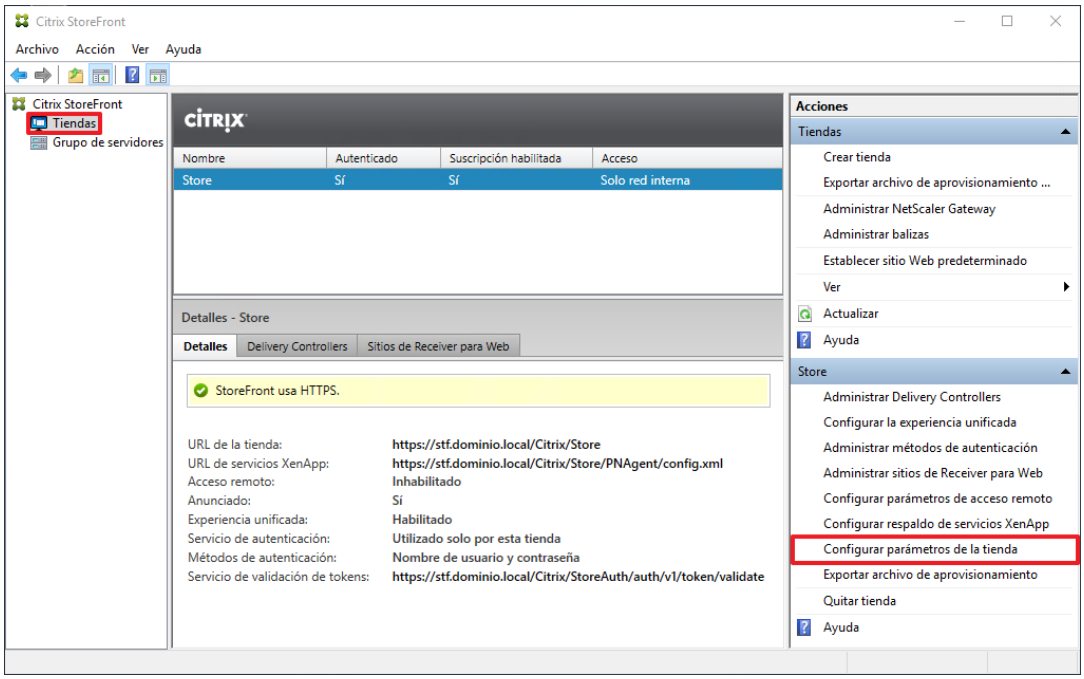
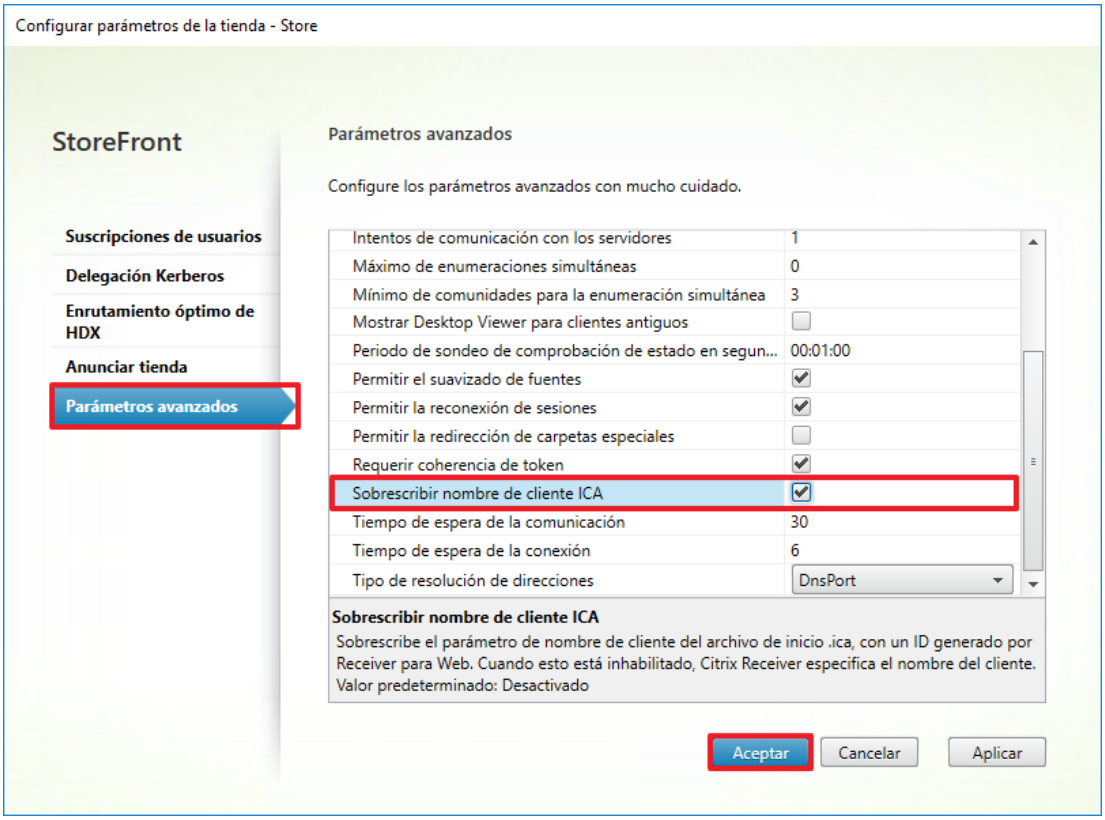
Paso	Descripción
208.	Es posible que le aparezca una ventana donde se le ofrece registrar el servidor de licencias con Citrix Cloud. Marque la casilla “No volver a mostrar esto” si no lo realizó anteriormente, y cierre la ventana pulsando el aspa de la parte superior derecha de la ventana. 
209.u	Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre la rueda superior derecha. 
210.	Acceda al apartado “Uso y estadísticas” y pulse sobre “No enviar datos a Citrix” para evitar compartir estadísticas de uso con el fabricante. 

8. CLIENTE ICA

Con la aplicación del ENS para la categoría alta o Difusión Limitada sobre Citrix Virtual Apps and Desktops, se limita la información que el propio producto genera, sobrescribiendo los archivos .ICA generados por la aplicación con un ID aleatorio.

Para ello deberá llevar a cabo adecuaciones sobre el servidor con el rol Citrix Storefront.

Paso	Descripción
211.	Inicie sesión en un servidor con el rol Citrix Storefront del dominio donde se va a aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
212.	Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Storefront.  **Nota:** El sistema solicitará elevación de privilegios.

Paso	Descripción
213.	Dentro de la consola, diríjase al menú de configuración **"Tiendas → Store → Configurar parámetros de la tienda"**. 
214.	Habilite la opción "Sobrescribir nombre de cliente ICA" en el apartado "Parámetros avanzados" y pulse "Aceptar" para aplicar los cambios. 

ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA CITRIX VIRTUAL APPS AND DESKTOPS SOBRE MICROSOFT WINDOWS SERVER 2016 EN ENTORNO DE DOMINIO

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores Citrix Virtual Apps and Desktops sobre Microsoft Windows Server 2016 con implementación de seguridad de categoría alta del ENS / Difusión Limitada.

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

Posteriormente, se deberán realizar las comprobaciones en los propios servidores donde está implementado cada uno de los roles de Citrix.

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar la sección de la guía "ANEXO A.4.1 IMPLEMENTACIÓN DE SEGURIDAD PARA CITRIX VIRTUAL APPS AND DESKTOPS EN SERVIDORES MIEMBROS DEL DOMINIO SOBRE MICROSOFT SERVER 2016 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA".

1. CONTROLADOR DE DOMINIO

Los siguientes pasos determinan el procedimiento para verificar la configuración del dominio en el que se despliega el sistema de virtualización.

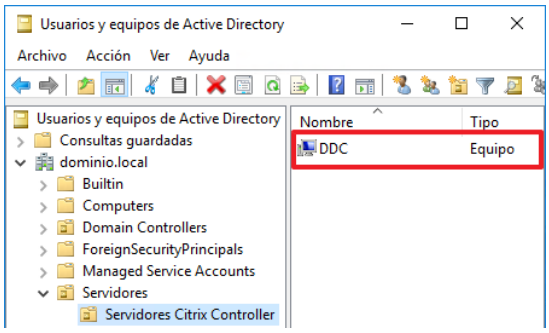
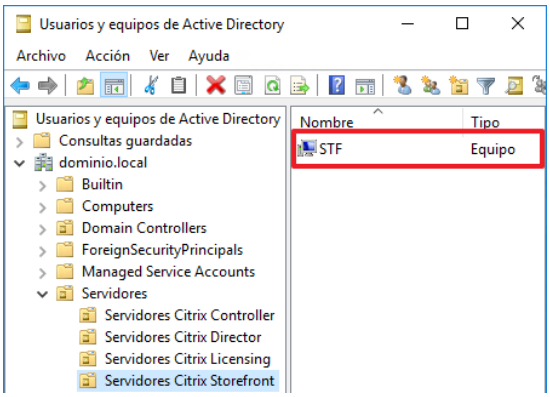
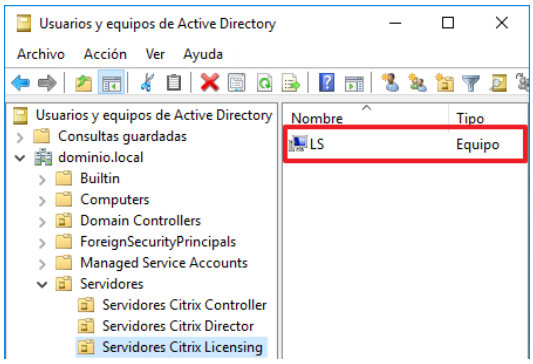
Las consolas y herramientas que se utilizarán son las siguientes:

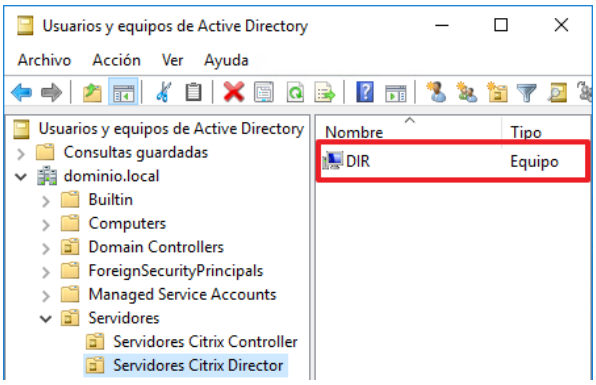
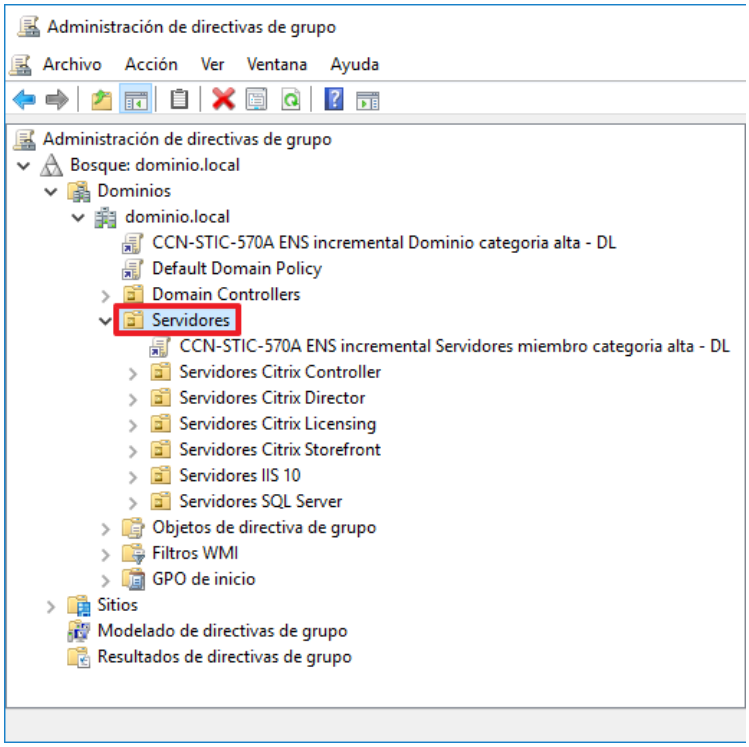
a) En el controlador de dominio:

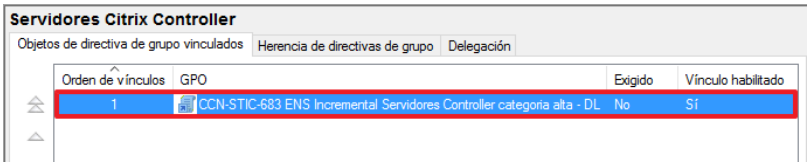
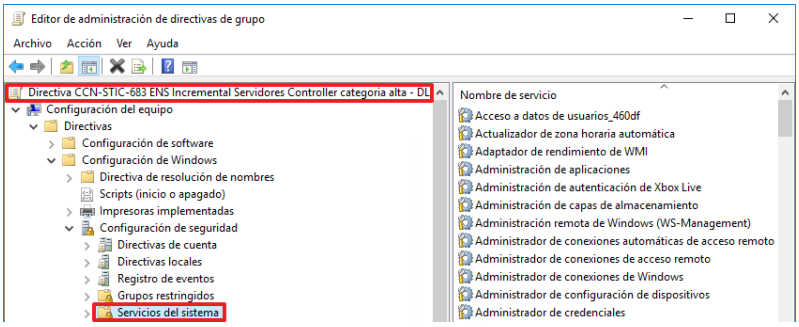
   i. Usuarios y equipos de Active Directory (dsa.msc).

   ii. Administrador de directivas de grupo (gpmc.msc).

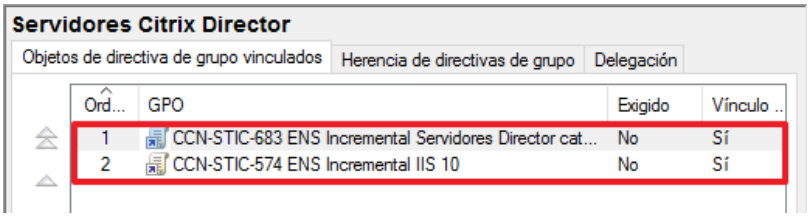
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un servidor controlador de dominio.		En un servidor controlador de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que están creadas las unidades organizativas de Citrix y que alojan sus respectivos servidores.		Ejecute la herramienta "Usuarios y equipos de Active Directory" desde: "**Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**". El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.

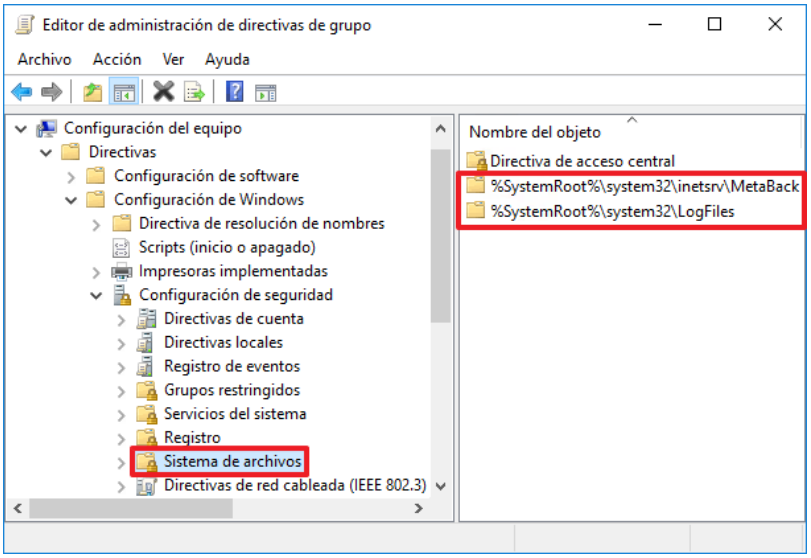
Comprobación	OK/NOK	Cómo hacerlo
3. La unidad organizativa "Servidores Citrix Controller" debe albergar todos los servidores con el rol Citrix Controller de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Controller" en ella, apreciará los servidores correspondientes.  **Nota:** El nombre del servidor de ejemplo es "DDC", en su caso debe figurar el nombre de su equipo.
4. La unidad organizativa "Servidores Citrix Storefront" debe albergar todos los servidores con el rol Citrix Storefront de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Storefront" en ella, apreciará los servidores correspondientes.  **Nota:** El nombre del servidor de ejemplo es "STF", en su caso debe figurar el nombre de su equipo.
5. La unidad organizativa "Servidores Citrix Licensing" debe albergar todos los servidores con el rol Citrix Licensing de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Licensing" en ella, apreciará al menos uno de los servidores.  **Nota:** El nombre del servidor de ejemplo es "LS", en su caso debe figurar el nombre de su equipo.

Comprobación	OK/NOK	Cómo hacerlo
6. La unidad organizativa "Servidores Citrix Director" debe albergar todos los servidores con el rol Citrix Director de la infraestructura.		En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Director" en ella, apreciará los servidores correspondientes.  **Nota:** El nombre del servidor de ejemplo es "DIR", en su caso debe figurar el nombre de su equipo.
7. Verifique que están creadas las directivas de configuración de Citrix.		Ejecute la herramienta "Administración de directivas de grupo" desde: **"Menú inicio → Herramientas administrativas → Administración de directivas de grupo"**. El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio. Seleccione la unidad organizativa "Servidores", situada en **"Bosque → Dominios → [Su dominio] → Servidores"**. 

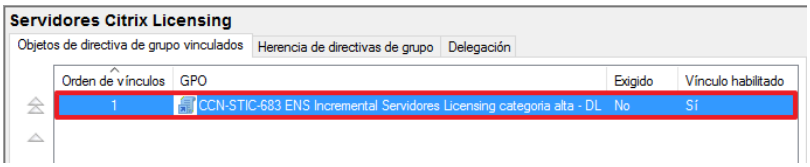
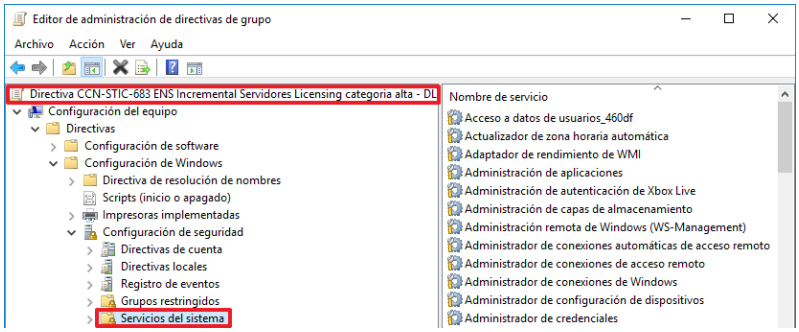
Comprobación	OK/NOK	Cómo hacerlo
8. Verifique las políticas aplicadas a "Servidores Citrix Controller".		Seleccione la unidad organizativa "Servidores Citrix Controller", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Controller"** y revise que, como mínimo, tiene aplicada la siguiente directiva y tiene el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL 
9. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Controller categoria alta - DL" tiene los siguientes valores de servicios de sistema. **"Directiva CCN-STIC-683 ENS Incremental Servidores Controller categoria alta – DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Asignador de extremos de RPC	RpcEptMapper	Automático	
Citrix AD Identity Service	CitrixADIdentityService	Automático	
Citrix Analytics	CitrixAnalytics	Automático	
Citrix App Library	CitrixAppLibrary	Automático	
Citrix Broker Service	CitrixBrokerService	Automático	
Citrix Config Synchronizer Service	CitrixConfigSyncService	Automático	
Citrix Configuration Service	CitrixConfigurationService	Automático	
Citrix Configuration Logging Service	CitrixConfigurationLogging	Automático	

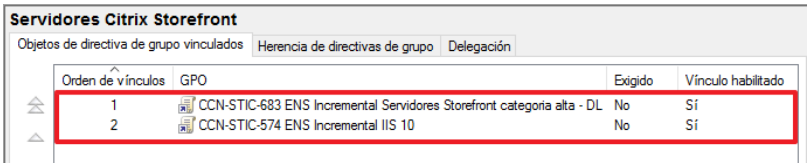
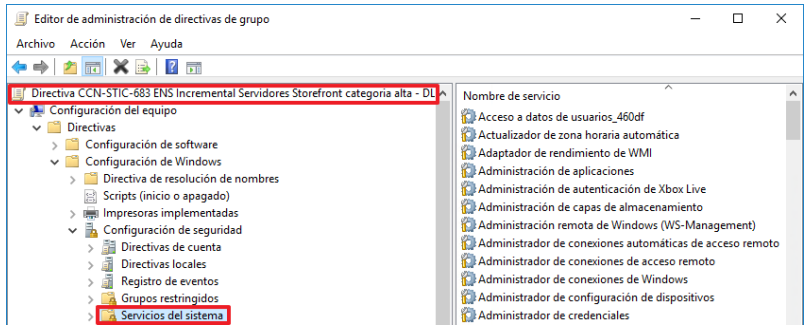
<table>
<tr><th colspan="2">Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td colspan="3">Servicio (nombre largo)</td><td>Servicio (nombre corto)</td><td>Inicio</td><td>OK/NOK</td></tr>
<tr><td colspan="3">Citrix Smart Tools Agent Service</td><td>CitrixConnector</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="3">Citrix Delegated Administration Service</td><td>CitrixDelegatedAdmin</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Enviroment Test Service</td><td>CitrixEnvTest</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix High Availability Service</td><td>CitrixHighAvailabilityService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Host Service</td><td>CitrixHostService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Machine Creation Service</td><td>CitrixMachineCreationService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Monitor Service</td><td>CitrixMonitor</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Orchestration Service</td><td>CitrixOrchestration</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Storefront Privileged Administration Service</td><td>CitrixPrivilegedService</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Storefront Service</td><td>CitrixStorefront</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Telemetry Service</td><td>CitrixTelemetryService</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="3">Citrix Trust Service</td><td>CitrixTrust</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Estación de trabajo</td><td>LanmanWorkstation</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Iniciador de procesos de servidor DCOM</td><td>DcomLaunch</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Llamada a procedimiento remoto (RPC)</td><td>RpcSs</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Servicio Interfaz de almacenamiento en red</td><td>nsi</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Remote Broker Provider</td><td>XaXdCloudProxy</td><td>Automático</td><td></td></tr>
<tr><td colspan="3">Citrix Smart Tools Monitor Service</td><td>Monitor Agent</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">10. Verifique las políticas aplicadas a “Servidores Citrix Director”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Servidores Citrix Director”, situada en “Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Director” y revise que, como mínimo, la unidad organizativa “Servidores Citrix Director” tiene aplicadas las siguientes directivas en el orden adecuado y tienen el vínculo habilitado.
– CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL
– CCN-STIC-574 ENS Incremental Servidores IIS 10
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique los valores de los permisos del sistema de archivos de la directiva "CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL".		Utilizando el "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL" tiene los siguientes valores de permisos de sistema de archivos. **"Directiva CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos"**.  **Nota:** Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...". Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\inetsrv\MetaBack	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	
%SystemRoot%\system32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	

Comprobación	OK/NOK	Cómo hacerlo
12. Verifique las políticas aplicadas a "Servidores Citrix Licensing".		Seleccione la unidad organizativa "Servidores Citrix Licensing", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Licensing"** y revise que, como mínimo, la unidad organizativa "Servidores Citrix Licensing" tiene aplicada la siguiente directiva y tiene el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL 
13. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL" tiene los siguientes valores de servicios de sistema. **"Directiva CCN-STIC-683 ENS Incremental Servidores Licensing categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Licensing	Citrix Licensing	Automático	
Citrix Web Services for Licensing	CitrixWebServicesforLicensing	Automático	
Citrix Licensing Support Service	CtxLSPortSvc	Automático	
Citrix Licensing WMI	Citrix_GTLicensingProv	Manual	

Comprobación	OK/NOK	Cómo hacerlo
14. Verifique las políticas aplicadas a "Servidores Citrix Storefront".		Seleccione la unidad organizativa "Servidores Citrix Storefront", situada en **"Bosque → Dominios → [Su dominio] → Servidores → Servidores Citrix Storefront"** y revise que, como mínimo, la unidad organizativa "Servidores Citrix Storefront" tiene aplicadas las siguientes directivas en el orden adecuado y tienen el vínculo habilitado. – CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL – CCN-STIC-574 ENS Incremental IIS 10 
15. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL".		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL" tiene los siguientes valores de servicios de sistema. **"Directiva CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	
Citrix Peer Resolution Service	Citrix Peer Resolution Service	Automático	
Citrix Configuration Replication	CitrixConfigurationReplication	Automático	
Citrix Credential Wallet	CitrixCredentialWallet	Automático	
Citrix Default Domain Service	CitrixDefaultDomainService	Automático	
Citrix Service Monitor	CitrixServiceMonitor	Automático	
Citrix Subscriptions Store	CitrixSubscriptionsStore	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	

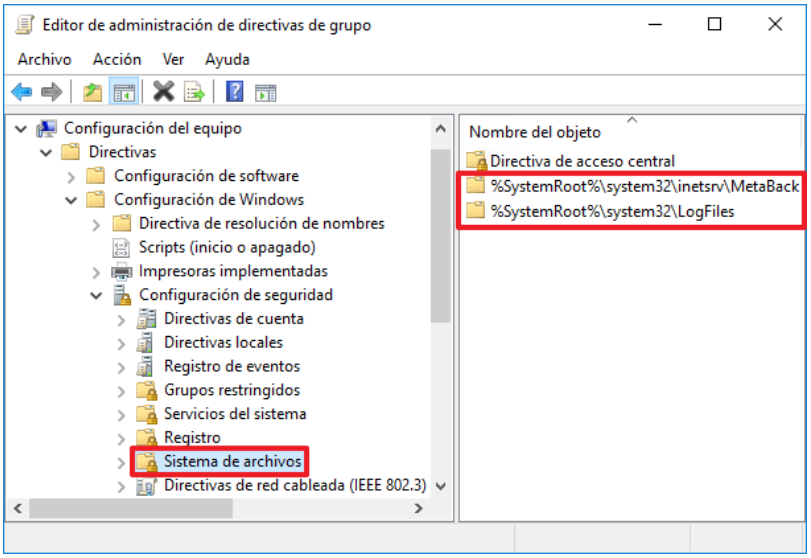
Comprobación	OK/NOK	Cómo hacerlo

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Automático	
Servidor	LanmanServer	Automático	
Citrix Cluster Service	CitrixClusterService	Deshabilitado	

16. Verifique los valores de los permisos del sistema de archivos de la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL".

Utilizando el "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL" tiene los siguientes valores de permisos de sistema de archivos.

"Directiva CCN-STIC-683 ENS Incremental Servidores Storefront categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos".



Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción Propiedades del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá marcar el botón "Modificar seguridad...".
Deberá tener cuidado para no realizar cambios sobre la directiva de grupo. Para cerrar las ventanas de propiedades y de permisos sin guardar los cambios marque la opción "Cancelar".

Archivo	Usuario	Permiso	OK/NOK
%SystemRoot%\system32\inetsrv\MetaBack	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	
%SystemRoot%\system32\LogFiles	Administradores	Control Total	
	SYSTEM	Control Total	
	CREATOR OWNER	Control Total	

2. CITRIX CONTROLLER

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Controller, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

a) En el servidor miembro Citrix Controller:

i. Servicios (services.msc).

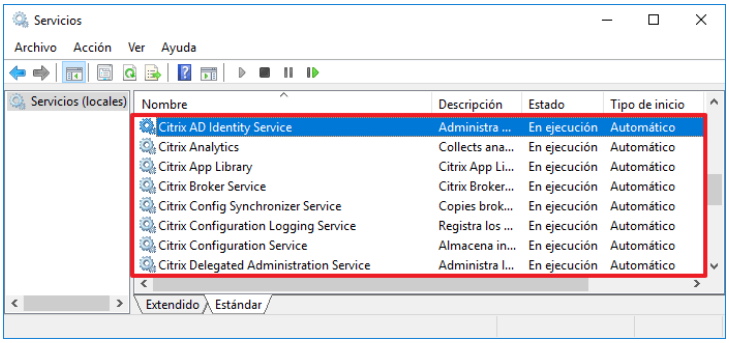
ii. Consola de administración de Microsoft (mmc.exe).

iii. Consola de comandos (cmd.exe).

iv. Consola de Citrix Studio.

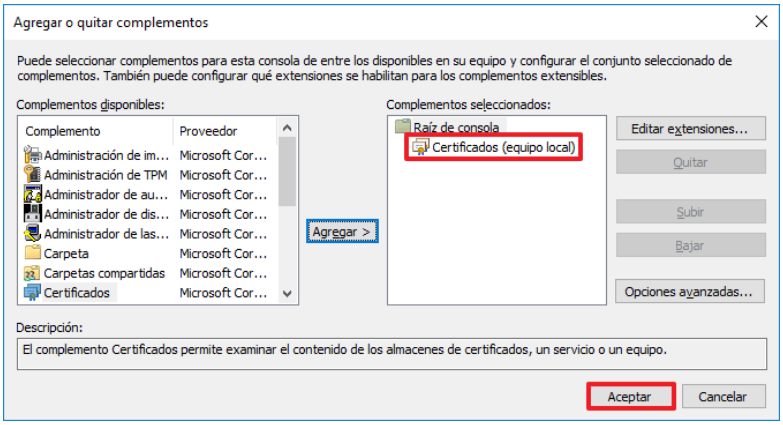
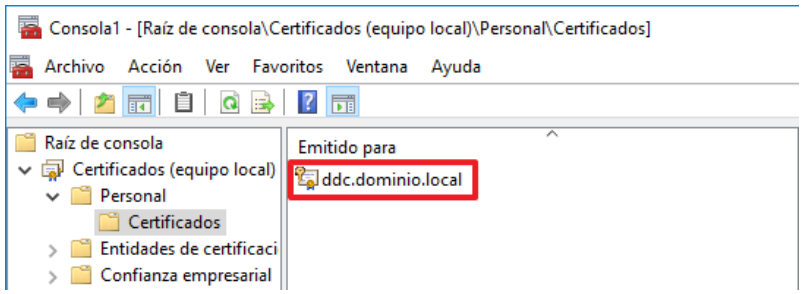
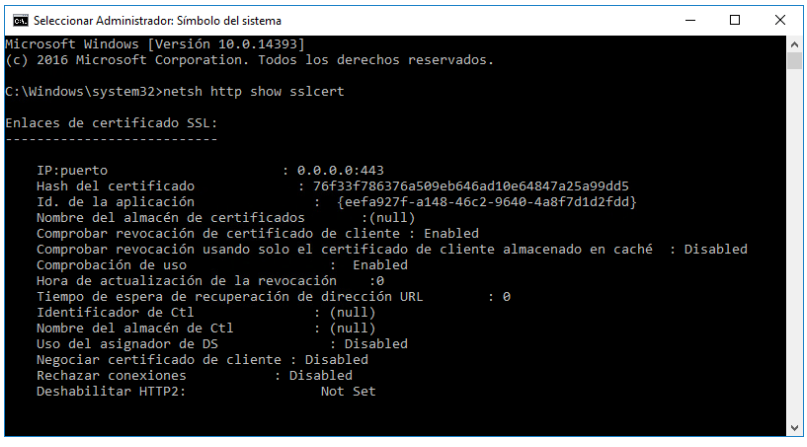
v. Registro del sistema (regedit.exe).

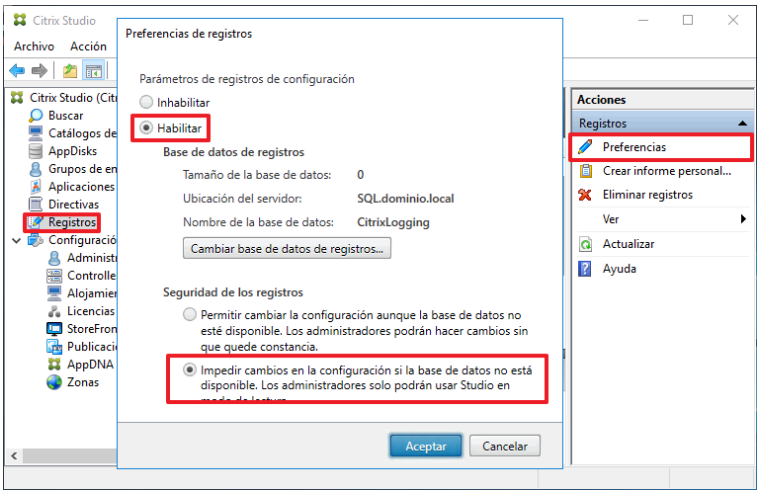
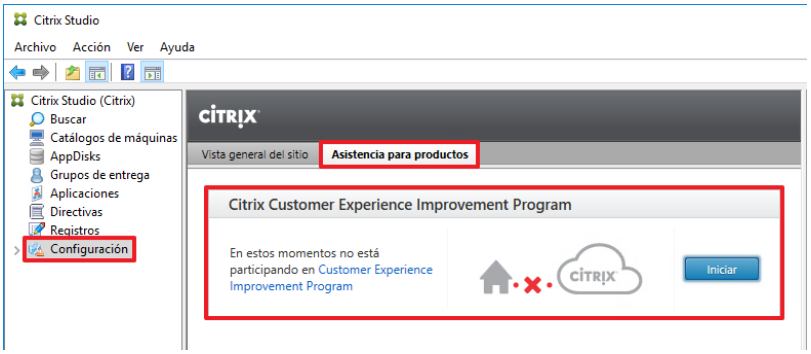
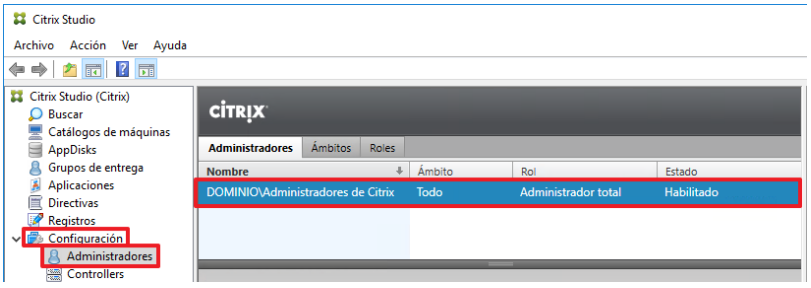
vi. Windows PowerShell.

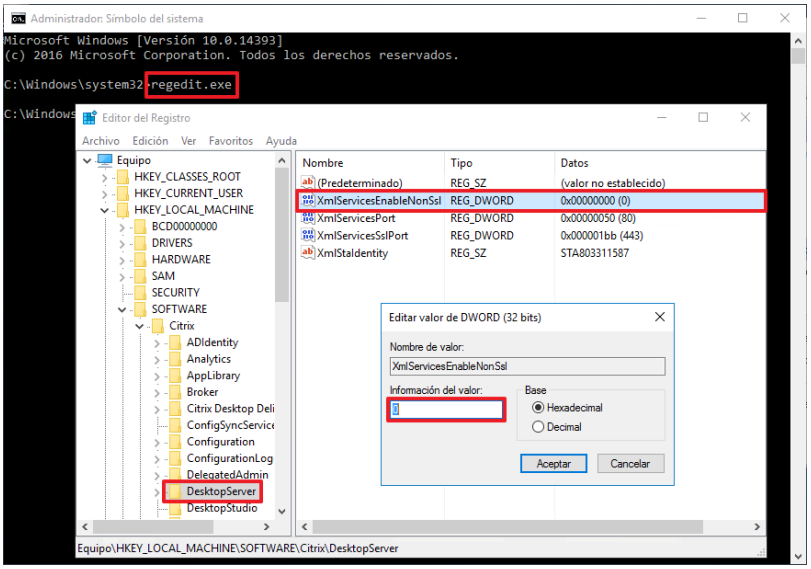
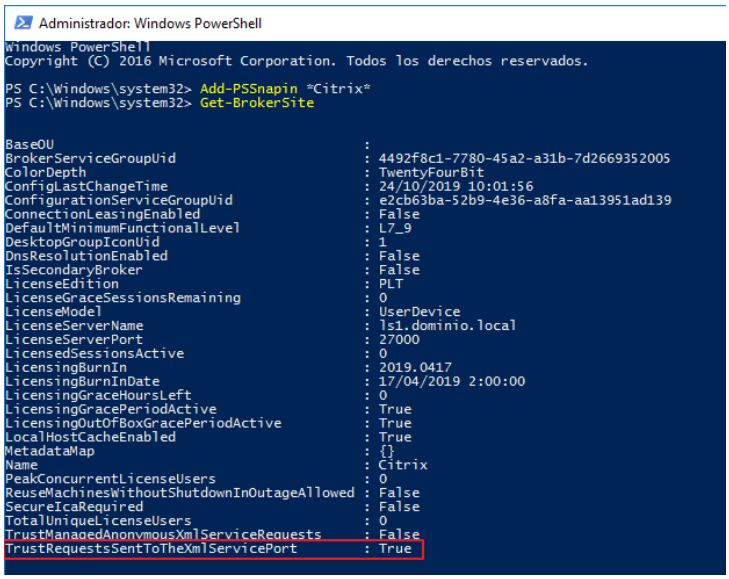
Comprobación	OK/NOK	Cómo hacerlo
17. Inicie sesión en un servidor con el rol Citrix Controller.		En un servidor con el rol Citrix Controller, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
18. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios.
19. Sobre cada uno de los servidores con el rol Citrix Controller revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Comprobación	OK/NOK	Cómo hacerlo

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Asignador de extremos de RPC	RpcEptMapper	Automático	
Citrix AD Identity Service	CitrixADIdentityService	Automático	
Citrix Analytics	CitrixAnalytics	Automático	
Citrix App Library	CitrixAppLibrary	Automático	
Citrix Broker Service	CitrixBrokerService	Automático	
Citrix Config Synchronizer Service	CitrixConfigSyncService	Automático	
Citrix Configuration Service	CitrixConfigurationService	Automático	
Citrix Configuration Logging Service	CitrixConfigurationLogging	Automático	
Citrix Smart Tools Agent Service	CitrixConnector	Deshabilitado	
Citrix Delegated Administration Service	CitrixDelegatedAdmin	Automático	
Citrix Enviroment Test Service	CitrixEnvTest	Automático	
Citrix High Availability Service	CitrixHighAvailabilityService	Automático	
Citrix Host Service	CitrixHostService	Automático	
Citrix Machine Creation Service	CitrixMachineCreationService	Automático	
Citrix Monitor Service	CitrixMonitor	Automático	
Citrix Orchestration Service	CitrixOrchestration	Automático	
Citrix Storefront Privileged Administration Service	CitrixPrivilegedService	Automático	
Citrix Storefront Service	CitrixStorefront	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Citrix Trust Service	CitrixTrust	Automático	
Estación de trabajo	LanmanWorkstation	Automático	
Iniciador de procesos de servidor DCOM	DcomLaunch	Automático	
Llamada a procedimiento remoto (RPC)	RpcSs	Automático	
Servicio Interfaz de almacenamiento en red	nsi	Automático	
Citrix Remote Broker Provider	XaXdCloudProxy	Automático	
Citrix Smart Tools Monitor Service	Monitor Agent	Deshabilitado	

Comprobación	OK/NOK	Cómo hacerlo
20. Verifique la instalación del certificado local para cada uno de los servidores Citrix Controller.		Acceda a la consola “mmc.exe” desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado “Ctrl + M”. 
21. Verifique la instalación del certificado local para cada uno de los servidores Citrix Controller.		Compruebe que bajo el almacén “Personal” deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo “Emitido para” variará dependiendo del nombre de su servidor.
22. Sobre un terminal cmd revise la vinculación del certificado con el puerto 443.		Abra un terminal “cmd.exe” con privilegios de administrador y ejecute el comando **“netsh http show sslcert”**. Deberá estar vinculado el certificado con la dirección 0.0.0.0:443. 

Comprobación	OK/NOK	Cómo hacerlo
23. Bajo la consola Citrix Studio revise la configuración de registro.		Acceda a la consola "Citrix Studio" y bajo el apartado **"Registros → Preferencias"** verifique que en "Parámetros de registros de configuración" se encuentra marcada la opción **"Habilitar"** y tiene aplicada la configuración **"Impedir cambios en la configuración si la base de datos no está disponible. Los administradores solo podrán utilizar Studio en modo de lectura"**. 
24. Compruebe la no participación en Citrix CEIP.		Sobre la consola "Citrix Studio" diríjase al nodo **"Citrix Studio → Configuración → Asistencia para productos"**. Compruebe que el "Citrix Customer Experience Improvement Program" se encuentra detenido. 
25. Revisión permisos administrativos		Dirjase al menú de configuración **"Citrix Studio → Configuración → Administradores"** y compruebe que se han restringido los permisos administrativos a los necesarios en función de su organización. 

Comprobación	OK/NOK	Cómo hacerlo
26. Verifique que las comunicaciones utilizando el puerto 80 no están permitidas en el sistema.		Abra con permisos administrativos la consola "regedit.exe" mediante una consola de comandos con privilegios de administrador. y localice la clave "HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer" encontrará el valor DWORD "XmlServicesEnableNonSsl" datos "0". 
27. Compruebe que están configuradas las peticiones hacia el servicio XML.		Abra una consola de Powershell con privilegios de administrador en cada uno de los servidores con el rol Citrix Controller instalado y ejecute los comandos "Add-PSSnapin *Citrix*" y "Get-BrokerSite". Verifique que el parámetro **"TrustRequestSentToTheXmlServicePort"** se encuentra con valor "True" como en la siguiente figura. 

3. CITRIX STOREFRONT

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Storefront, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

a) En el servidor miembro Citrix Storefront:

i. Servicios (services.msc).

ii. Consola de administración de Microsoft (mmc.exe).

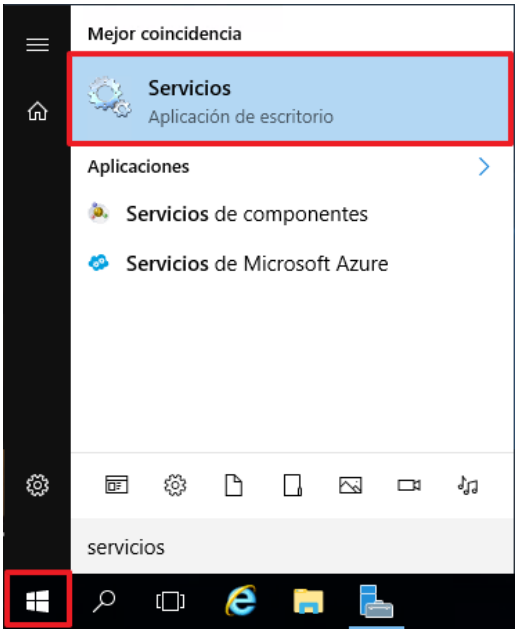
iii. Administrador de Internet Information Service (IIS).

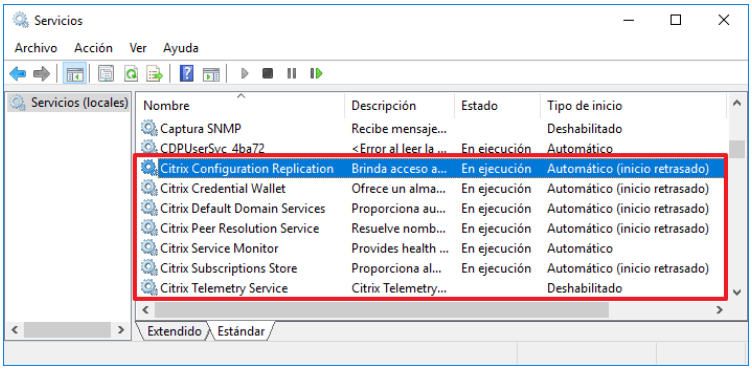
iv. Consola de comandos (cmd.exe).

v. Consola de Citrix Storefront.

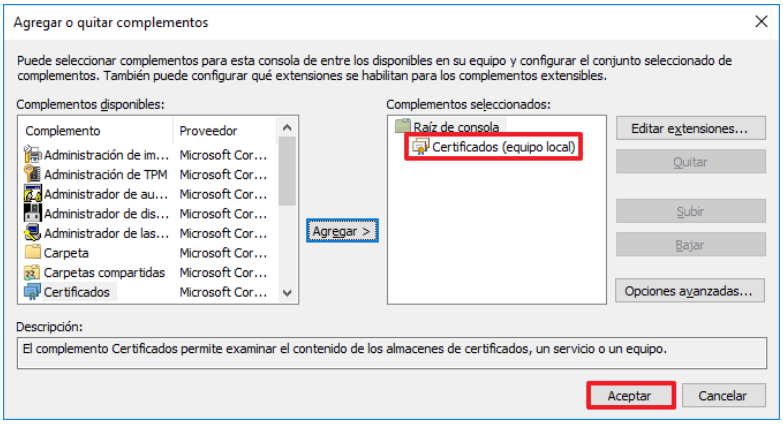
El siguiente procedimiento verifica la configuración del servidor con el rol Citrix Storefront.

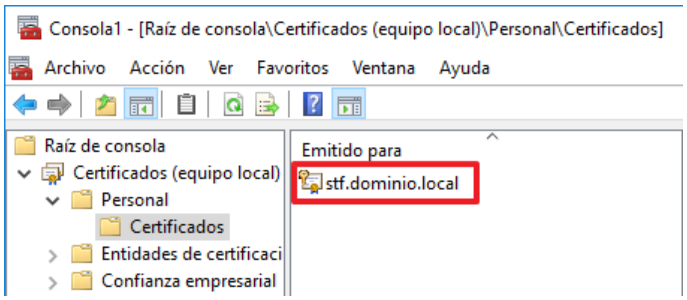
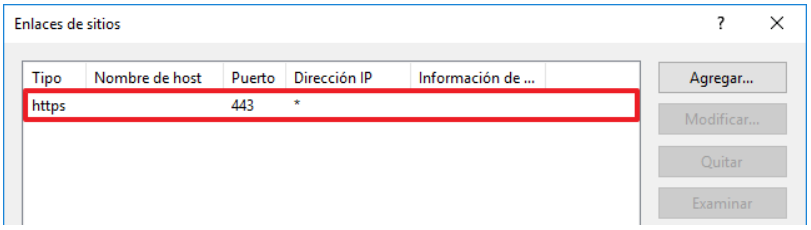
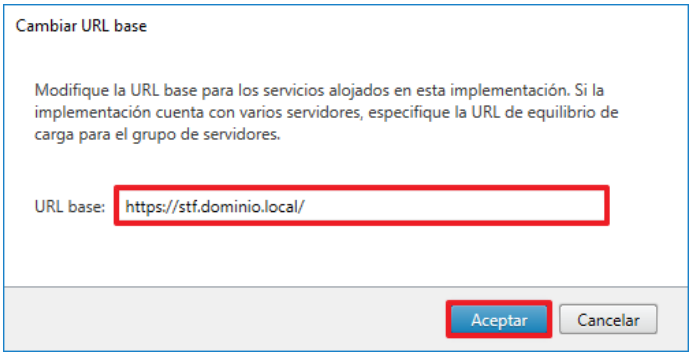
Nota: Deberá ejecutar los siguientes pasos de comprobación en el servidor con el rol Citrix Storefront que haya sido preparado siguiendo esta guía de seguridad.

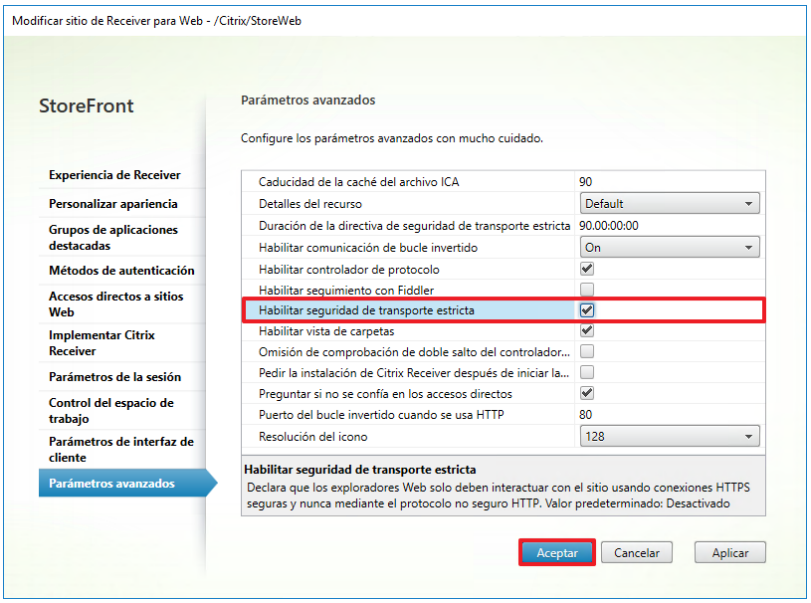
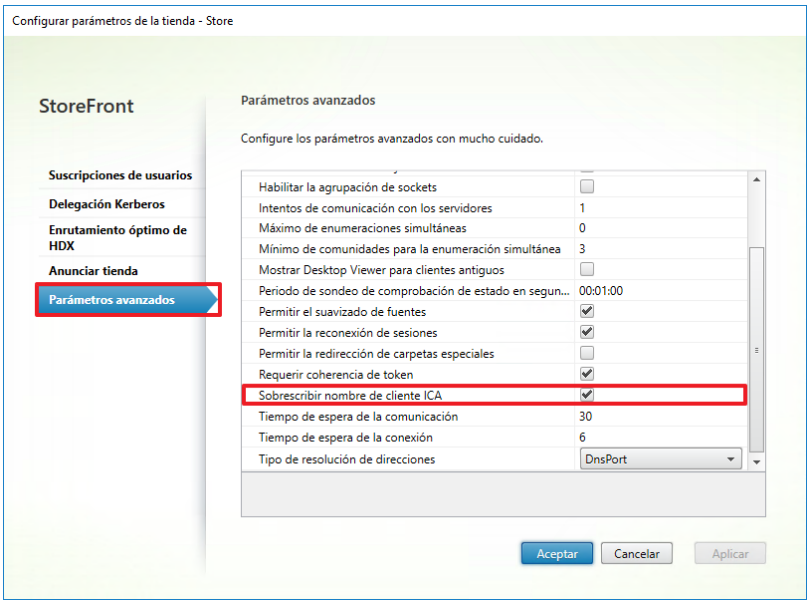
Comprobación	OK/NOK	Cómo hacerlo
28. Inicie sesión en un servidor con el rol Citrix Storefront.		En un servidor con el rol Citrix Storefront, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
29. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios. 

Comprobación	OK/NOK	Cómo hacerlo
30. Sobre cada uno de los servidores con el rol Citrix Storefront revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Aislamiento de claves CNG	KeyIso	Automático	
Citrix Peer Resolution Service	Citrix Peer Resolution Service	Automático	
Citrix Configuration Replication	CitrixConfigurationReplication	Automático	
Citrix Credential Wallet	CitrixCredentialWallet	Automático	
Citrix Default Domain Service	CitrixDefaultDomainService	Automático	
Citrix Service Monitor	CitrixServiceMonitor	Automático	
Citrix Subscriptions Store	CitrixSubscriptionsStore	Automático	
Citrix Telemetry Service	CitrixTelemetryService	Deshabilitado	
Servicio de uso compartido de puertos Net.Tcp	NetTcpPortSharing	Automático	
Servidor	LanmanServer	Automático	
Citrix Cluster Service	CitrixClusterService	Deshabilitado	

31. Verifique la instalación del certificado local para cada uno de los servidores Citrix Storefront.		Acceda a la consola “mmc.exe” desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado “Ctrl + M”. 

Comprobación	OK/NOK	Cómo hacerlo
32. Verifique la instalación del certificado local para cada uno de los servidores Citrix Storefront.		Despliegue el nodo **"Personal → Certificados"**. Deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo "Emitido para" variará dependiendo del nombre de su servidor.
33. Ejecute la consola de administración de IIS.		Ejecute la herramienta "Administrador de Internet Information Services (IIS)" desde: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)"**. El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.
34. Enlaces de sitios configurado para HTTPS.		Abra el nodo de configuración **"Su servidor (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"** Compruebe que únicamente se encuentra configurado el tipo "https" con el puerto 443. 
35. URL base del sitio configurada para HTTPS.		Ejecute la consola Citrix Storefront. Desde la pestaña **"Grupo de servidores"**, acceda a la opción "Cambiar URL base", compruebe que la URL de la tienda incluye el protocolo seguro HTTPS como se muestra en la siguiente figura. 

Comprobación	OK/NOK	Cómo hacerlo
36. Seguridad de transporte estricta habilitada.		Continúe con las comprobaciones accediendo a la consola "Citrix Storefront" y diríjase al menú de configuración **"Tiendas → Store → Administrar sitios de Receiver para Web"**, en la configuración de su sitio web, dentro del apartado de parámetros avanzados compruebe que se encuentra marcada la opción "Habilitar seguridad de transporte estricta". 
37. Configuración de parámetros avanzados de la tienda.		Continúe con las comprobaciones de la consola "Citrix Storefront" y diríjase al menú de configuración **"Tiendas → Store → Configurar parámetros de la tienda → Parámetros avanzados"**. Compruebe que se encuentra marcada la opción "Sobrescribir nombre de cliente ICA". 

4. CITRIX LICENSING

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Licensing, y las configuraciones propias implementadas sobre este servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

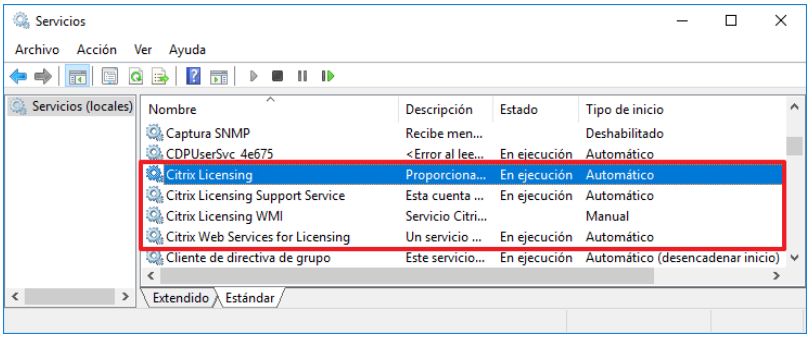
a) En el servidor miembro Citrix Licensing:

i. Servicios (services.msc).

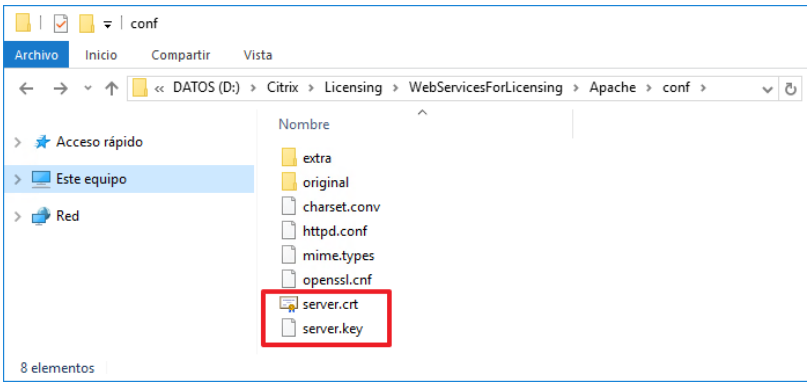
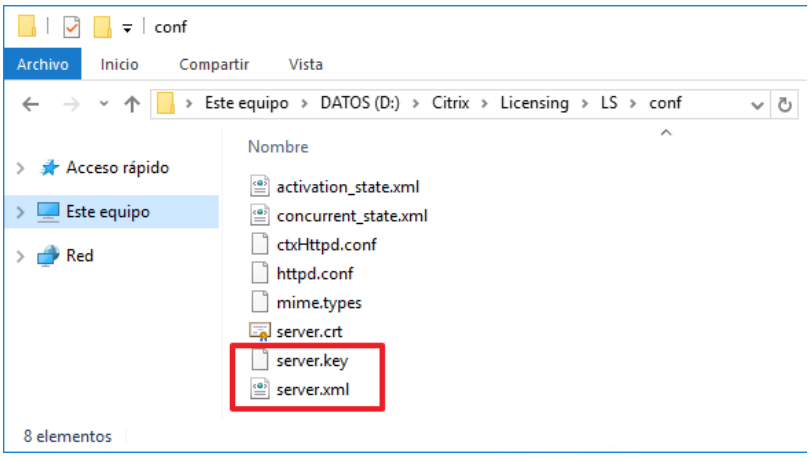
ii. Explorador de archivos de Windows

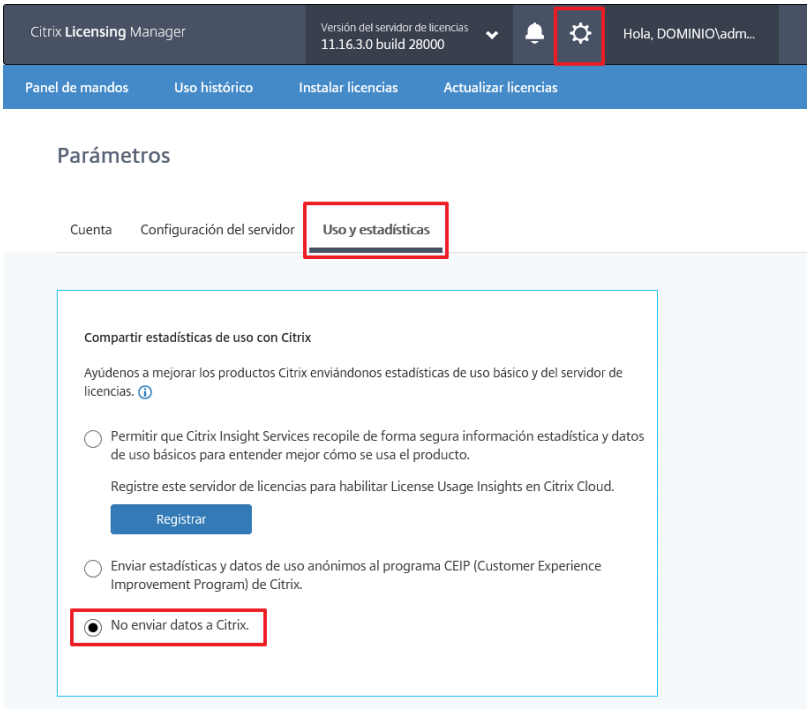
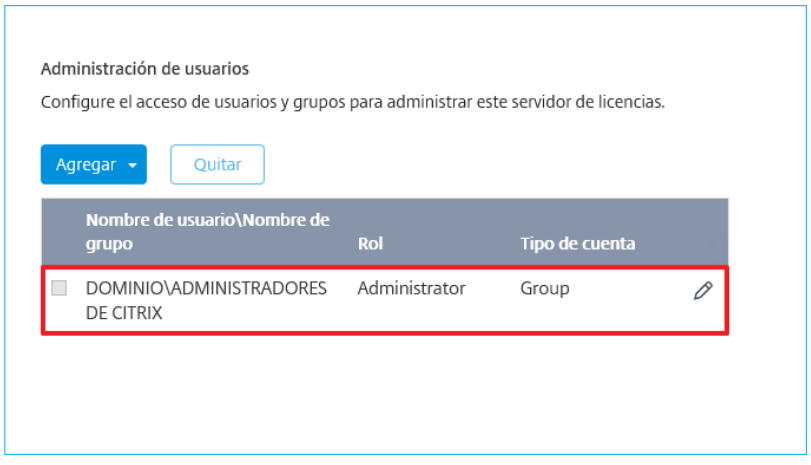
iii. Consola de comandos (cmd.exe).

iv. Consola de Citrix Licensing.

Comprobación	OK/NOK	Cómo hacerlo
38. Inicie sesión en un servidor con el rol Citrix Licensing.		En un servidor con el rol Citrix Licensing, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
39. Ejecución de la consola de servicios.		Pulse sobre el botón de "Inicio" y ejecute la herramienta "Servicios". El sistema solicitará elevación de privilegios.
40. Sobre cada uno de los servidores con el rol Citrix Licensing revise los servicios implementados y su estado.		Compruebe que el valor de inicio de los servicios se ha configurado correctamente.  **Nota:** Que un servicio se encuentre definido en una directiva no implica necesariamente que luego esté disponible en el servidor, ya que dependerá de si se ha instalado o no. Solo afectará el valor cuando el servicio esté disponible.

Servicio (nombre largo)	Servicio (nombre corto)	Inicio	OK/NOK
Citrix Licensing	Citrix Licensing	Automático	
Citrix Web Services for Licensing	CitrixWebServicesforLicensing	Automático	
Citrix Licensing Support Service	CtxLSPortSvc	Automático	
Citrix Licensing WMI	Citrix_GTLicensingProv	Manual	

Comprobación	OK/NOK	Cómo hacerlo
41. Comprobar archivos de certificados.		Compruebe que los archivos “server.crt” y “server.key” se encuentren en la ruta “C:\Pogram Files (x86)\Citrix\Licensing\WebServicesForLicensing\Apache\conf”.  **Nota:** En esta guía la instalación del rol Citrix Licensing se ha efectuado sobre la unidad “C:\”. Deberá copiar los archivos de certificados adaptando este paso a la ruta de instalación del rol Citrix Licensing en su organización.
42. Comprobar archivos de certificados.		Compruebe que los archivos “server.crt” y “server.key” se encuentren en la ruta: “C:\Pogram Files (x86)\Citrix\Licensing\LS\conf”.  **Nota:** En esta guía la instalación del rol Citrix Licensing se ha efectuado sobre la unidad “C:\”. Deberá copiar los archivos de certificados adaptando este paso a la ruta de instalación del rol Citrix Licensing en su organización.

Comprobación	OK/NOK	Cómo hacerlo
43. Restringir envío de información a Citrix.		Acceda a la dirección URL https://ls.dominio.local:8083 adaptándolo a su entorno. Una vez abierto correctamente el portal, acceda al menú de configuración pulsando sobre el botón de configuración en la parte superior derecha. Acceda al apartado "Uso y estadísticas". Compruebe que está marcada la opción "No enviar datos a Citrix". 
44. Restricción permisos Citrix Licensing.		A continuación, acceda al nodo de configuración "Cuenta". Verifique que se han restringido los permisos administrativos a los necesarios en función de su organización. 

5. CITRIX DIRECTOR

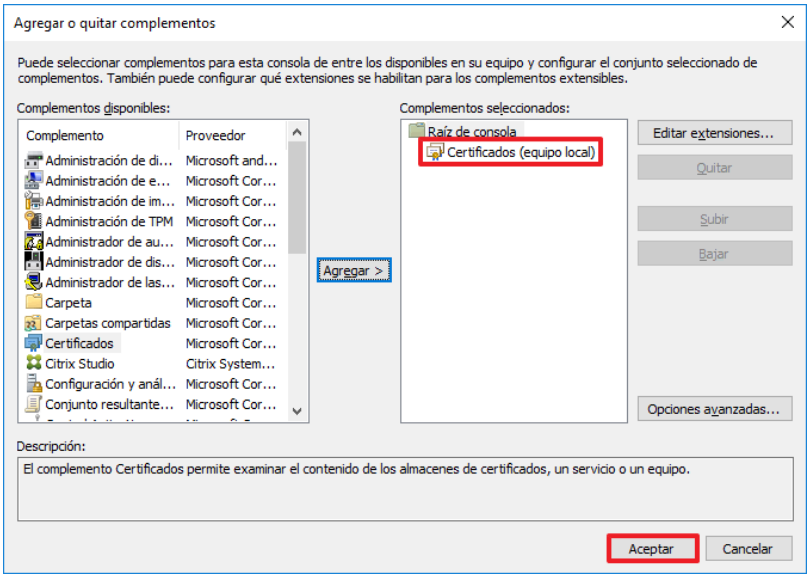
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el controlador de dominio del dominio en el que se ha desplegado el servidor donde se ha implementado el rol Citrix Director, y las configuraciones propias implementadas sobre este servidor.

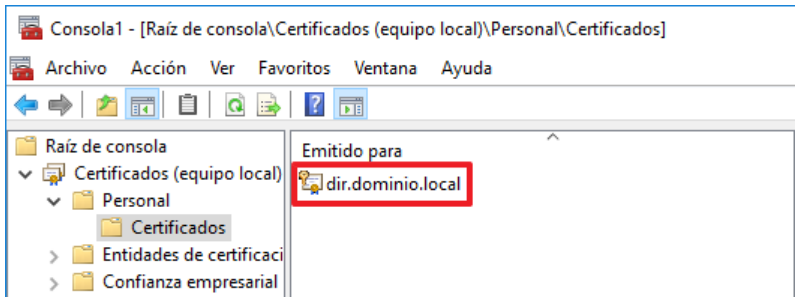
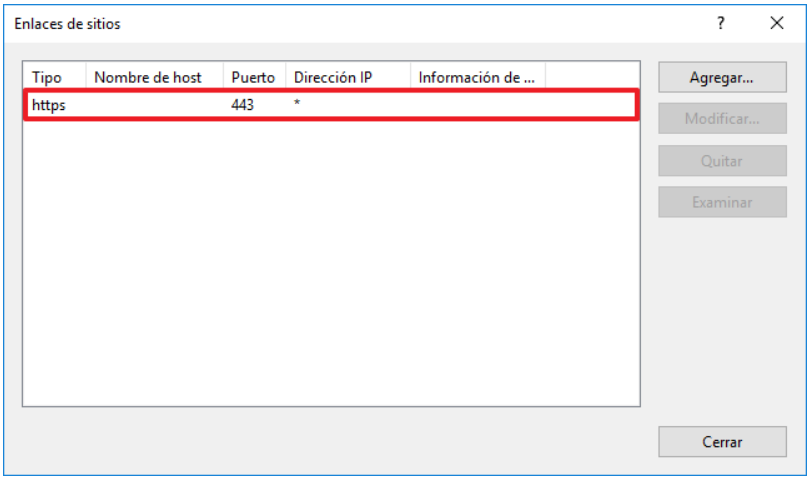
Las consolas y herramientas que se utilizarán son las siguientes:

a) En el servidor miembro Citrix Director:

i. Consola de administración de Microsoft (mmc.exe).

ii. Administrador de Internet Information Service (IIS).

Comprobación	OK/NOK	Cómo hacerlo
45. Inicie sesión en un servidor con el rol Citrix Director.		En un servidor con el rol Citrix Director, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
46. Verifique la instalación del certificado local para cada uno de los servidores Citrix Director.		Acceda a la consola "mmc.exe" desde el menú de inicio. El sistema solicitará elevación de privilegios. Agregue el complemento certificados de equipo mediante el atajo de teclado "Ctrl + M". 

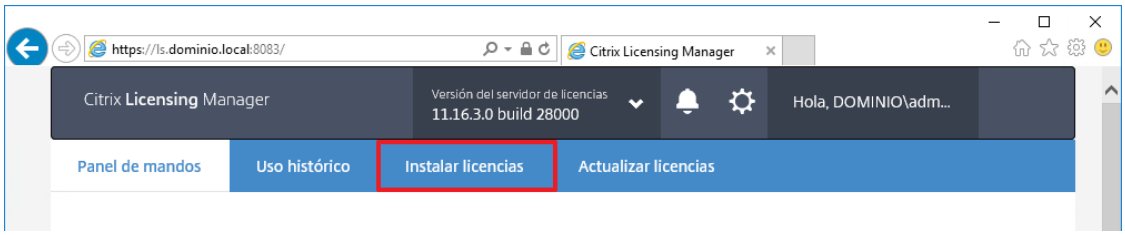
Comprobación	OK/NOK	Cómo hacerlo
47. Verifique la instalación del certificado local para cada uno de los servidores Citrix Director.		Despliegue el nodo **"Personal → Certificados"**. Deberá encontrar instalado un certificado cuyo CN coincida con el nombre completo del servidor.  **Nota:** El campo "Emitido para" variará dependiendo del nombre de su servidor.
48. Ejecute la consola de administración de IIS.		Ejecute la herramienta "Administrador de Internet Information Services (IIS)" desde: **"Menú inicio → Herramientas administrativas → Administrador de Internet Information Services (IIS)"**. El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.
49. Enlaces de sitios configurado para HTTPS.		Abra el nodo de configuración **"Su servidor (Dominio\Administrador) → Sitios → Default Web Site"** y pulsando con el botón derecho entre en **"Modificar enlaces…"** Compruebe que únicamente se encuentra configurado el tipo "https" con el puerto 443. 

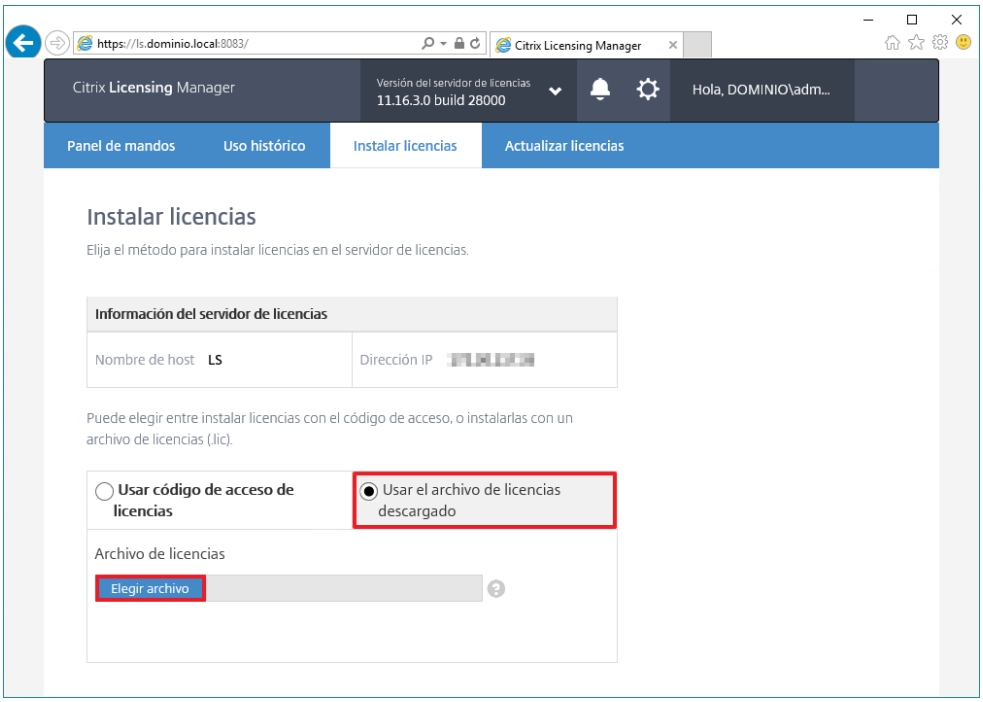
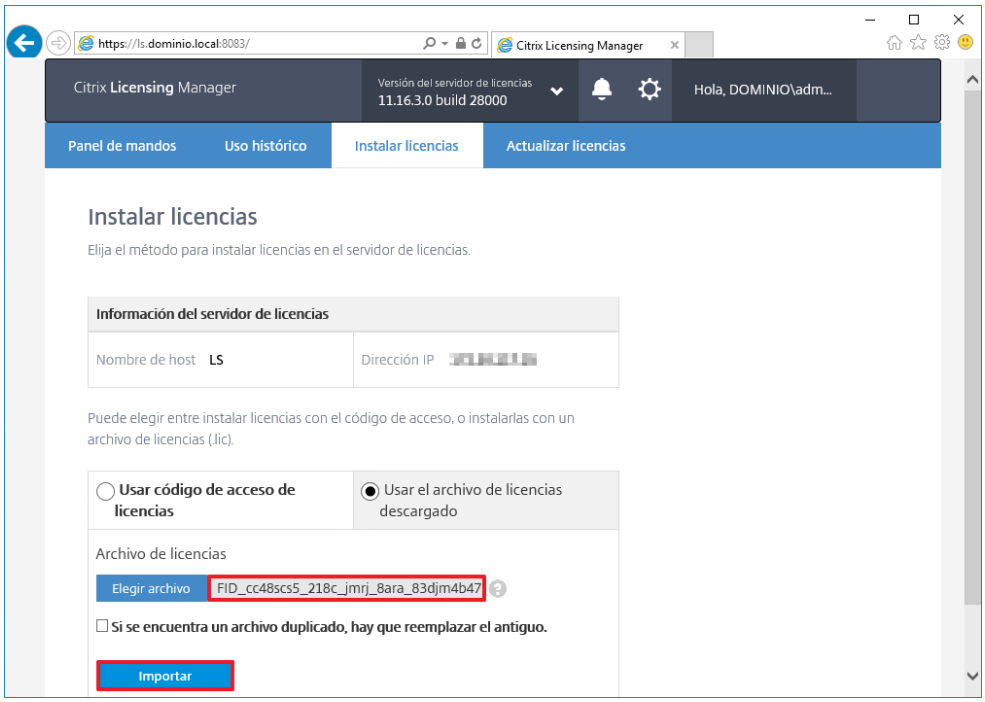
ANEXO A.5. TAREAS ADICIONALES

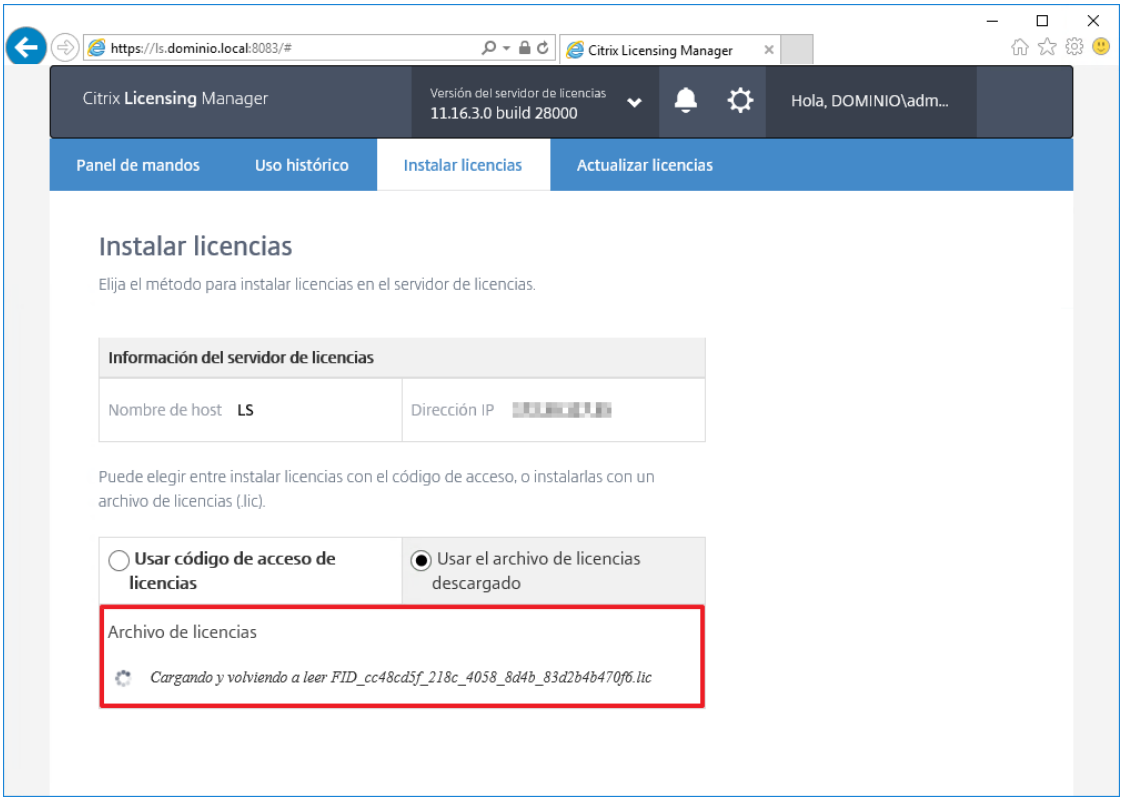
ANEXO A.5.1. INSTALACIÓN DE LICENCIAS EN CITRIX LICENSING

A continuación, se realizará la instalación de licencias válidas para su uso en un entorno de Citrix Virtual Apps and Desktops. Para proceder con los siguientes pasos, deberá asignar las licencias obtenidas al nombre de máquina de su servidor de licencias y posteriormente descargar la licencia en un archivo con formato "FID_XXXXXXXXXXXXXXXXXXXXXXX.lic" que se importará desde la consola Citrix Licensing Manager.

Se asume en el siguiente paso a paso que dispone de un licenciamiento válido proporcionado por el fabricante y que dispone de suficientes licencias para su organización.

Paso	Descripción
1.	Inicie sesión en un servidor con el rol Citrix Licensing del dominio donde se va a realizar el proceso de instalación de licencias.  **Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio.
2.	Acceda a la dirección URL https://ls.dominio.local:8083 adaptándolo a su entorno para acceder al portal Citrix Licensing Manager.
3.	Una vez en el portal de administración seleccione "Instalar licencias". 

Paso	Descripción
4.	Marque la opción “Usar el archivo de licencias descargado” y a continuación, a través del botón “Elegir archivo” seleccione el archivo “FID_XXXXXXXXXXXXXXXXXXXXXXX.lic” de su archivo de licencias. 
5.	Una vez seleccionado el archivo de licencias pulse “Importar”.  **Nota:** En caso de que su organización ya tuviera un archivo de licencias vinculado anteriormente que coincida con el nombre del nuevo archivo de licencias a importar, deberá seleccionar la opción **“Si se encuentra un archivo duplicado, hay que reemplazar el antiguo”** y posteriormente proceder a la importación.

Paso	Descripción
6.	Citrix Licensing Manager procederá a la importación del archivo de licencias definido en el paso anterior. 
7.	Una vez importado el fichero de licencias, Citrix Licensing Manager devolverá un mensaje indicando que el fichero ha sido cargado correctamente.