centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 684

# PUBLICACIÓN SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS


SEPTIEMBRE 2020

Edita:



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


NIPO: 083-20-200-X

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

**LIMITACIÓN DE RESPONSABILIDAD**

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

**AVISO LEGAL**

# PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

septiembre de 2020

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ANEXOS

# ANEXO A. PUBLICACIÓN SEGURA DE APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS EN EL ENS

## ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE APLICACIONES Y ESCRITORIOS VIRTUALES DE CITRIX

### 1. APLICACIÓN DE MEDIDAS PARA LA VIRTUALIZACIÓN DE APLICACIONES Y ESCRITORIOS

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de Citrix Virtual Delivery Agent para la virtualización de aplicaciones y escritorios sobre servidores con Microsoft Windows Server 2016 o equipos Microsoft Windows 10, y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande. 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 "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 los equipos clientes desde los que se realizará la conexión a los recursos de la infraestructura, sujetos al RD 3/2010 y que se encontrarán implementados con los sistemas operativos y guías de seguridad de la serie "CCN-STIC-500 Guías de entornos Windows" que corresponda según las necesidades de implementación de la 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.

d) Aplicación de seguridad en clientes 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 10 implementados siguiendo la guía CCN-STIC-599A19 – Implementación del ENS en Windows 10.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aportan tanto Citrix para el producto Citrix Virtual Apps and Desktops como Microsoft, 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. 2. REQUISITOS DE ACCESO

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

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

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

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

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia. La siguiente dirección URL facilita la información que proporciona el fabricante sobre los controles y vigilancia de acceso para la familia Windows Server y Windows como sistema operativo cliente.

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

#### 1.1.1.3. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS

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

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

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de otra función.

Dichos procesos de segregación son factibles realizarlos a través de los propios mecanismos que proporciona 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 utilización de los recursos desplegados mediante la infraestructura.

#### 1.1.1.4. 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 de utilización de una aplicación virtualizada específica, pero no sobre todas las aplicaciones que despliega un grupo de entrega con varias aplicaciones virtualizadas. Por lo tanto únicamente accederá a aquellos recursos que se le permitan.

#### 1.1.1.5. 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.

### 1.1.2. EXPLOTACIÓN

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

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

#### 1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que 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.

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

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

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

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

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

#### 1.1.2.3. 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.

## 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-684, adaptándolos a la organización. |
| OP. ACC. 2 | Requisitos de acceso | Revisión e implementación de guía CCN-STIC-684, adaptándolos a la organización. |
| OP. ACC. 3 | Segregación de funciones y tareas | Revisión e implementación de guía CCN-STIC-683, adaptándolos a la organización. |
| OP. ACC. 4 | Gestión de derechos de acceso | Revisión e implementación de guía CCN-STIC-684, adaptándolos a la organización. |
| OP. ACC. 7 | Acceso remoto | Revisión e implementación de guía CCN-STIC-684, 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-684, adaptándolos a la organización. |
| OP. EXP. 3 | Gestión de la configuración | Revisión e implementación de guía CCN-STIC-684, adaptándolos a la organización. |
| OP. EXP. 5 | Gestión de cambios | Revisión e implementación de guía CCN-STIC-684, adaptándolos a la organización. |

# ANEXO A.2. CATEGORÍA BÁSICA

## ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS 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 tengan que asegurar aplicaciones y escritorios virtualizados mediante Citrix Virtual Apps and Desktops, 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 los equipos sobre los que implementarán 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.

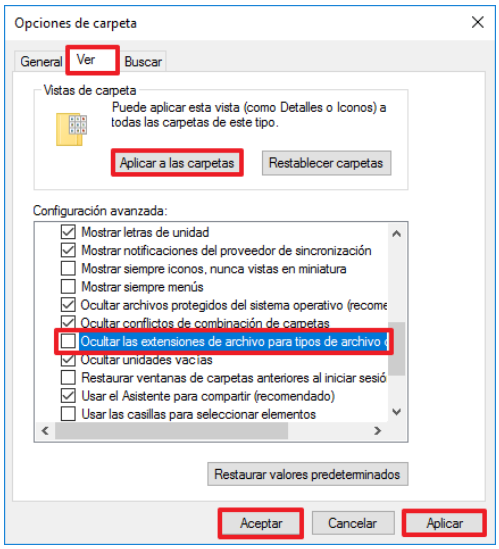
Se asume que ha realizado la implementación de las siguientes guías de seguridad sobre el dominio donde se va a aplicar el siguiente paso a paso:

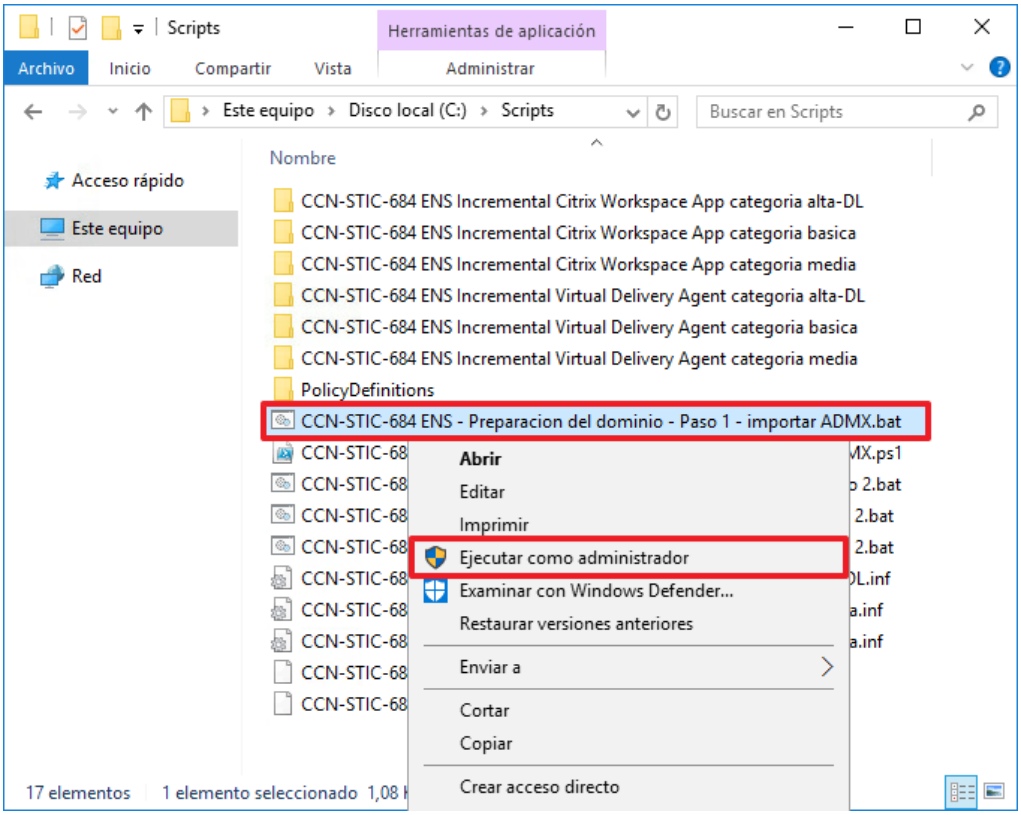
a) CCN-STIC-570A Anexo A Controlador de dominio – Categoría Básica

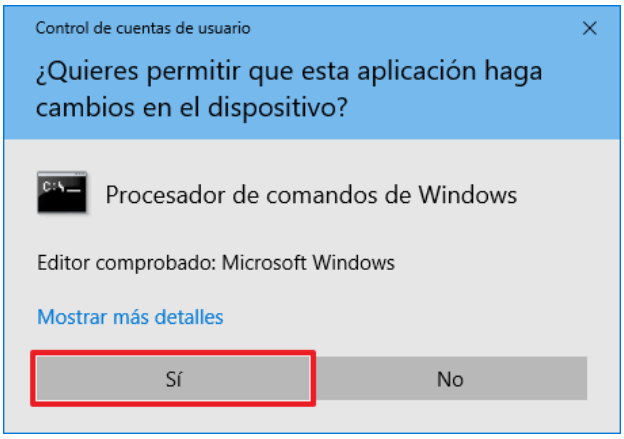
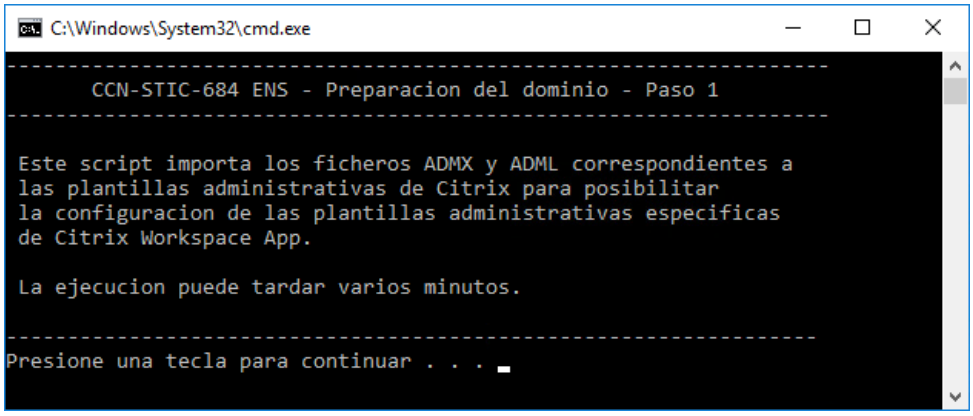
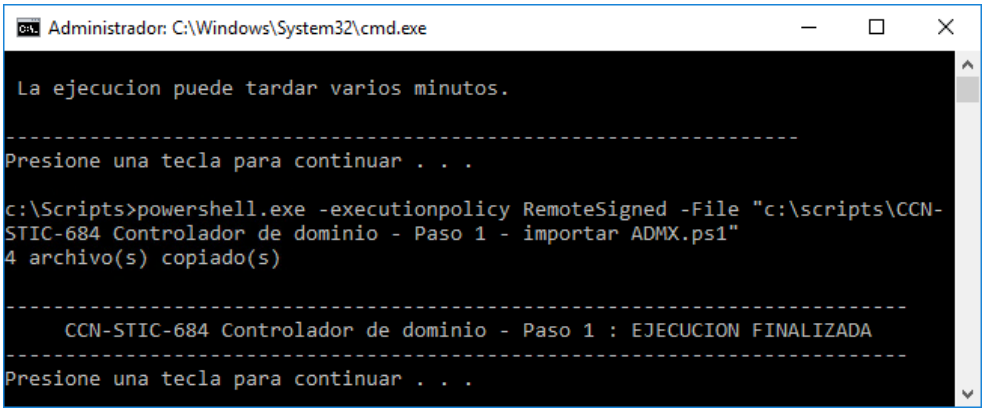
b) CCN-STIC-570A Anexo A Servidor miembro – Categoría Básica

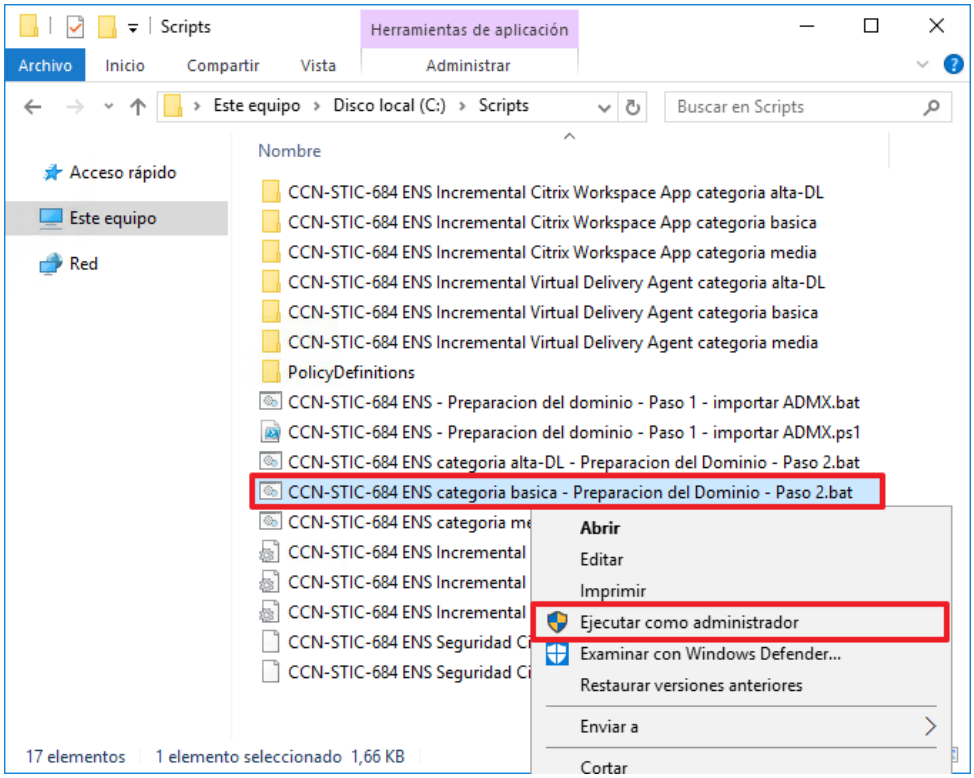
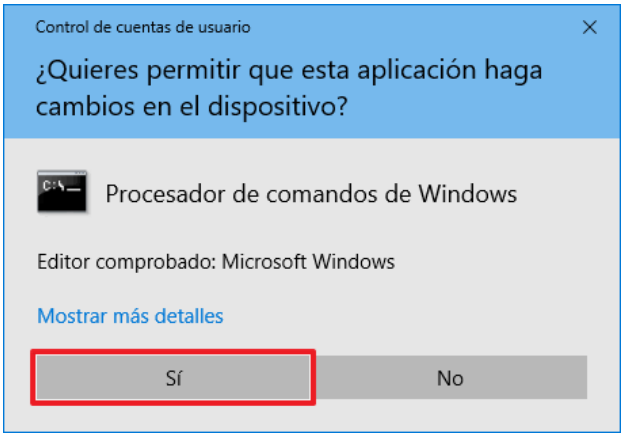
c) CCN-STIC-599A19 Anexo A – Categoría Básica

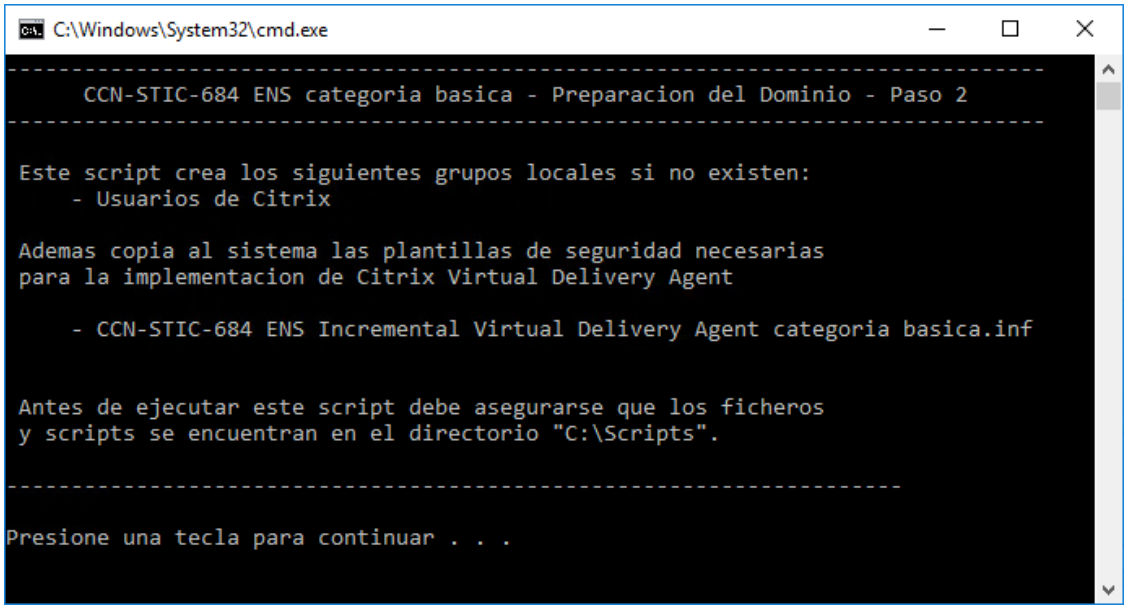
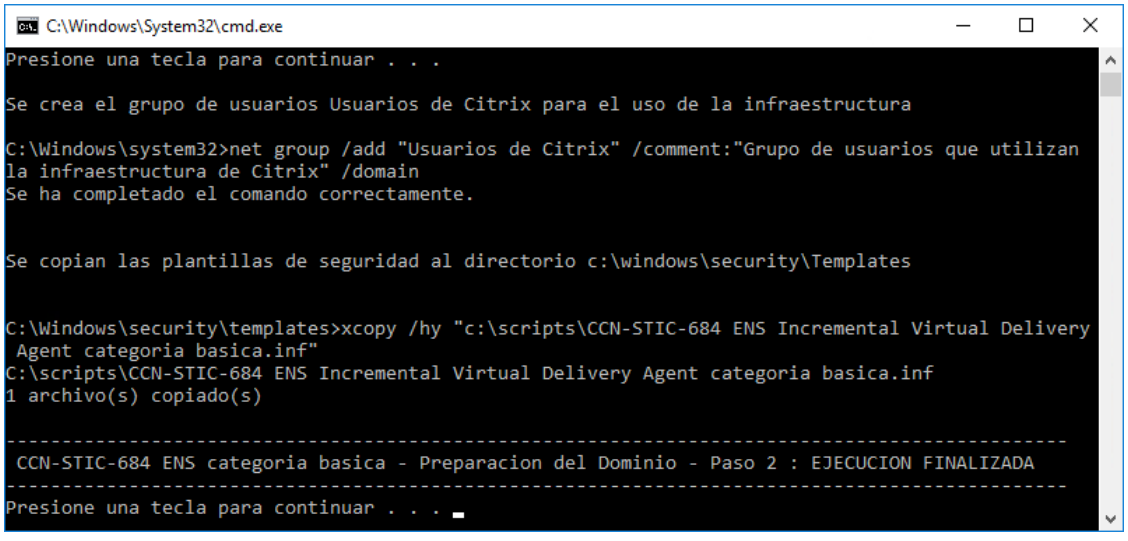
d) CCN-STIC-683 – Categoría Básica

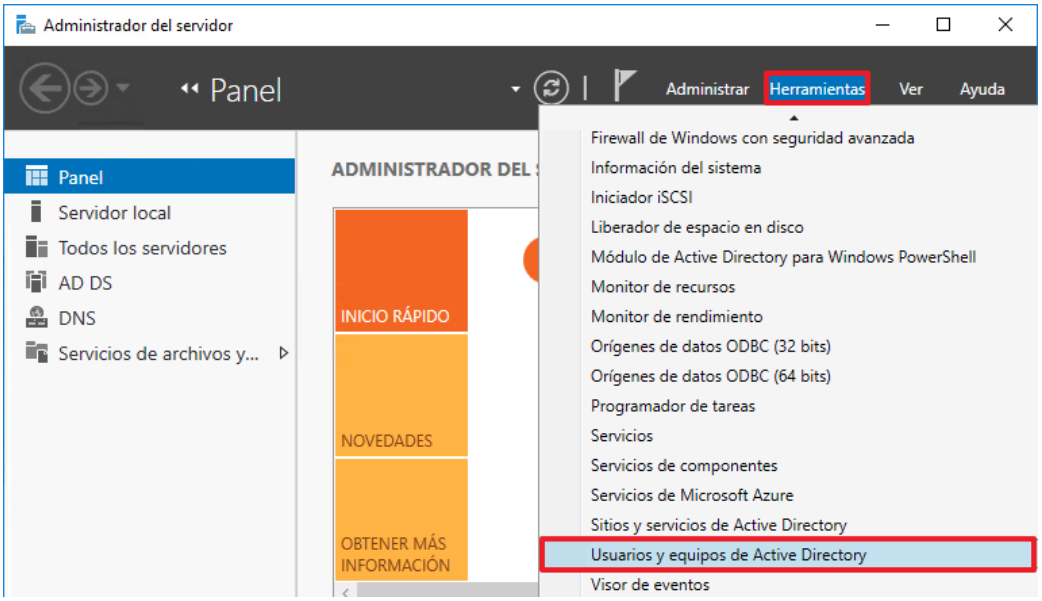
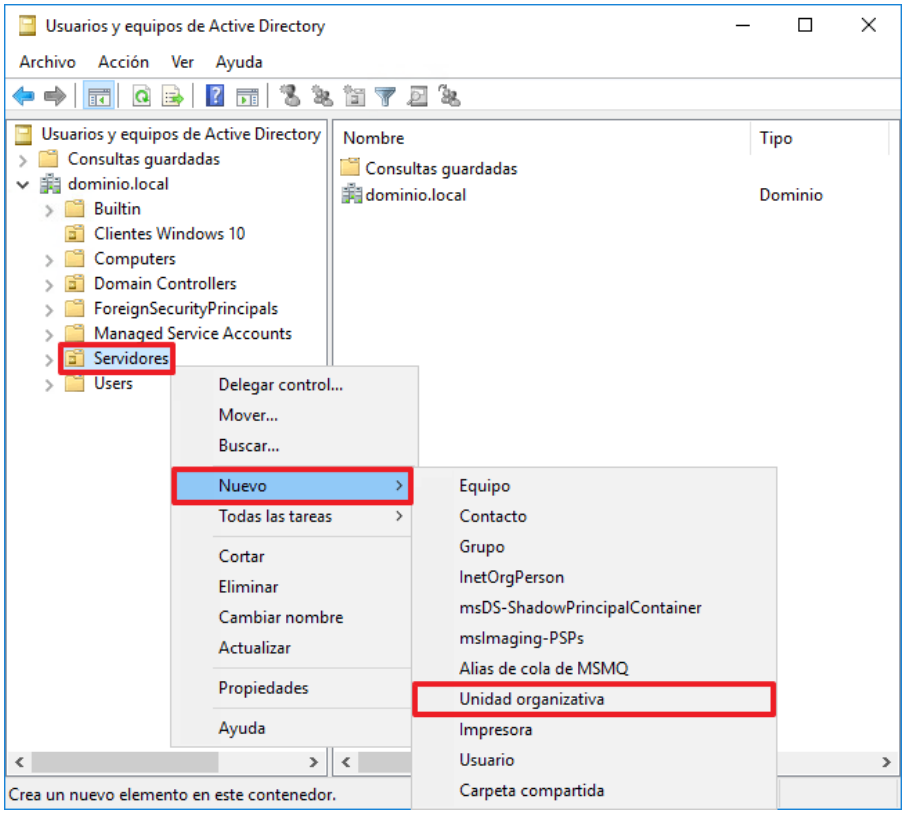
| Paso | Descripción |
|---|---|
| 1. | Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 2. | Cree el directorio “Scripts” en la unidad “C:\”.<br>**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.<br>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:<br>  |
| 5. | Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta". |

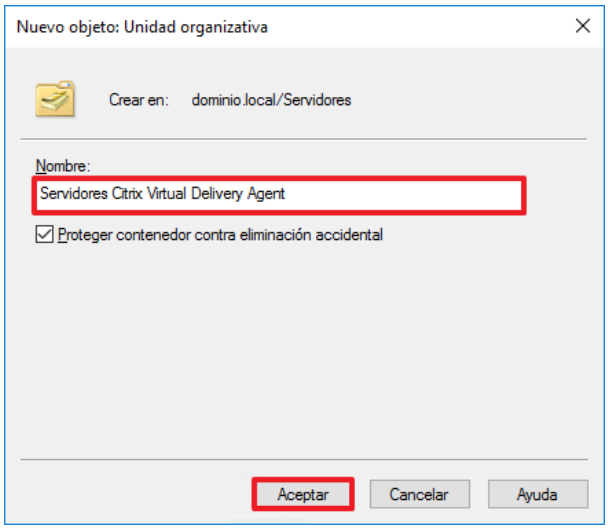
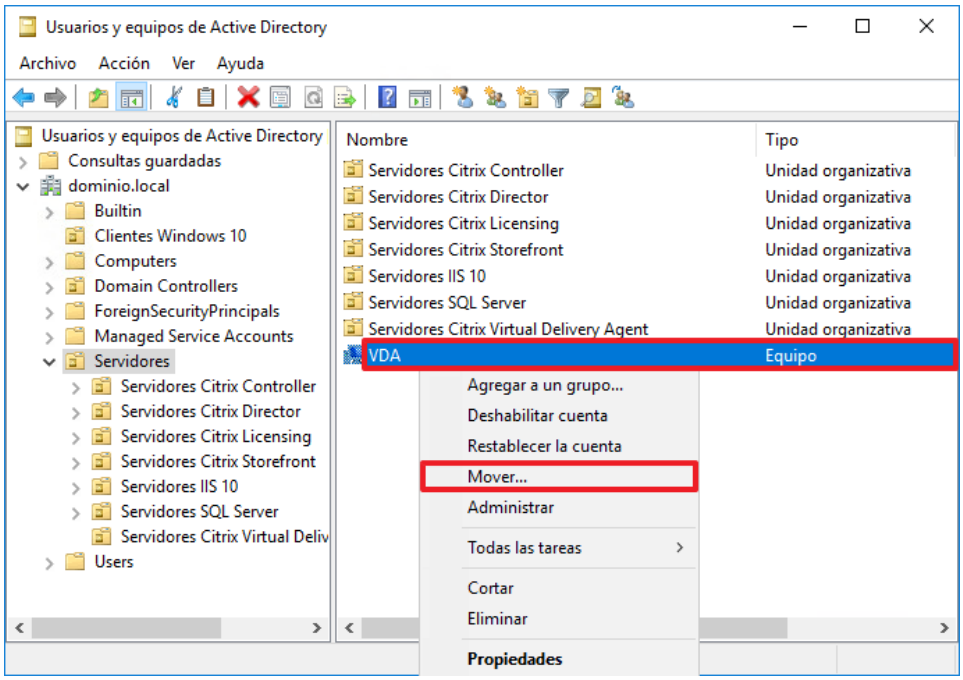
| Paso | Descripción |
|---|---|
| 6. | Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio:<br>– CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica (Directorio)<br>– CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica (Directorio)<br>– PolicyDefinitions (Directorio)<br>– CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.bat<br>– CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.ps1<br>– CCN-STIC-684 ENS categoria basica - Preparacion del Dominio - Paso 2.bat<br>– CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica.inf |
| 7. | Ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.bat". Para ello, visualice la carpeta “C:\Scripts” en el explorador de Windows, marque con el botón derecho el script y seleccione la opción **"Ejecutar como administrador"** del menú contextual, como se muestra en la siguiente figura.<br>  <br>**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.<br>Si el directorio principal de Windows no se encuentra en “C:\Windows”, sustituya "C:\Windows" por la ubicación correspondiente dentro de los archivos de configuración. |

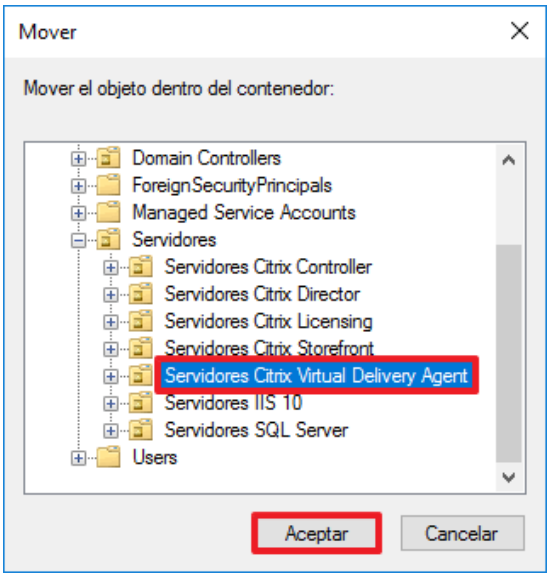
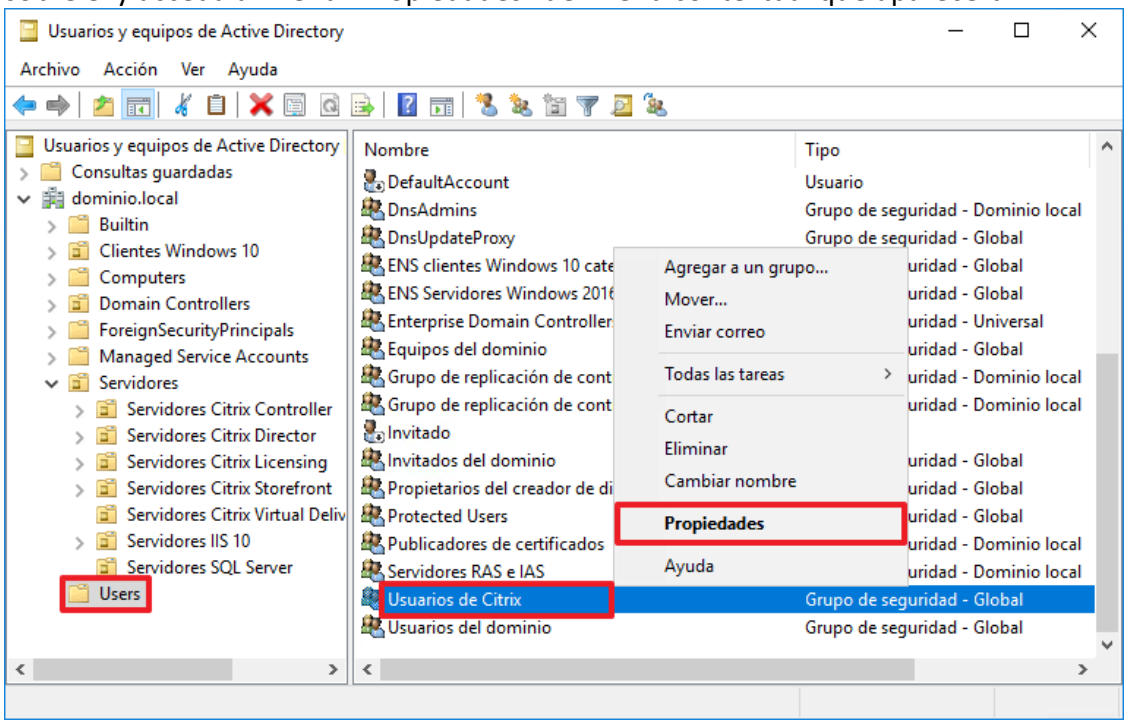
| Paso | Descripción |
|---|---|
| 8. | El sistema solicitará elevación de privilegios, pulse “Si” para continuar.<br>  |
| 9. | Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Citrix Workspace App en el controlador de dominio.<br>  |
| 10. | Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana.<br>  |

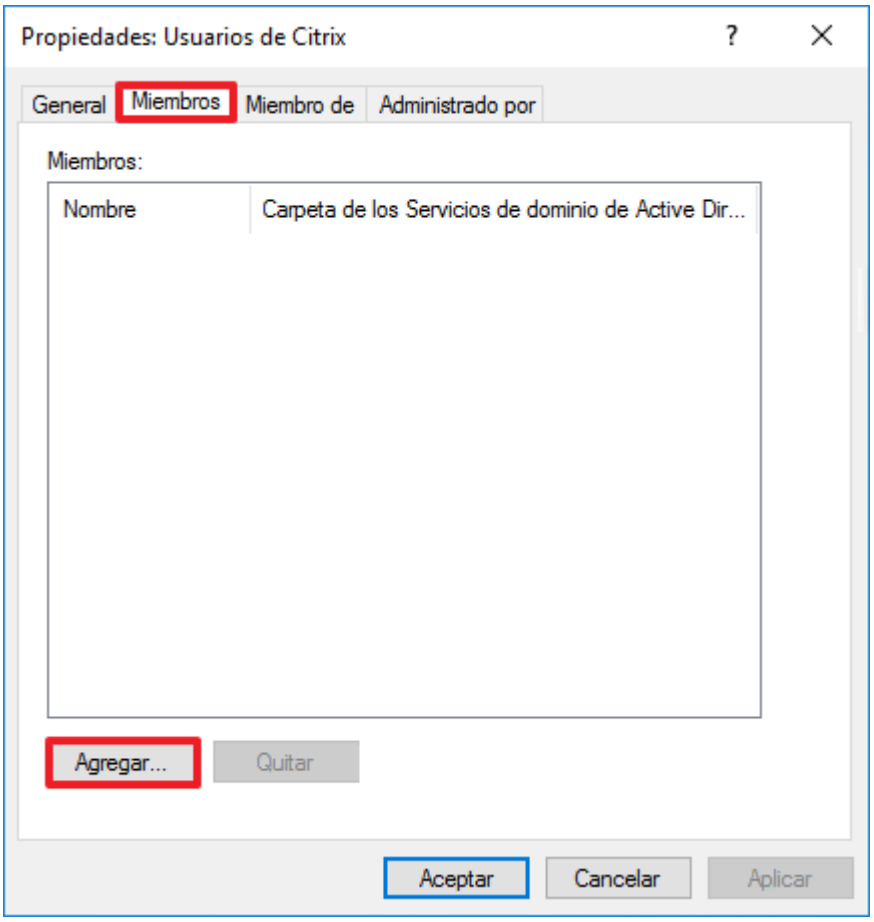
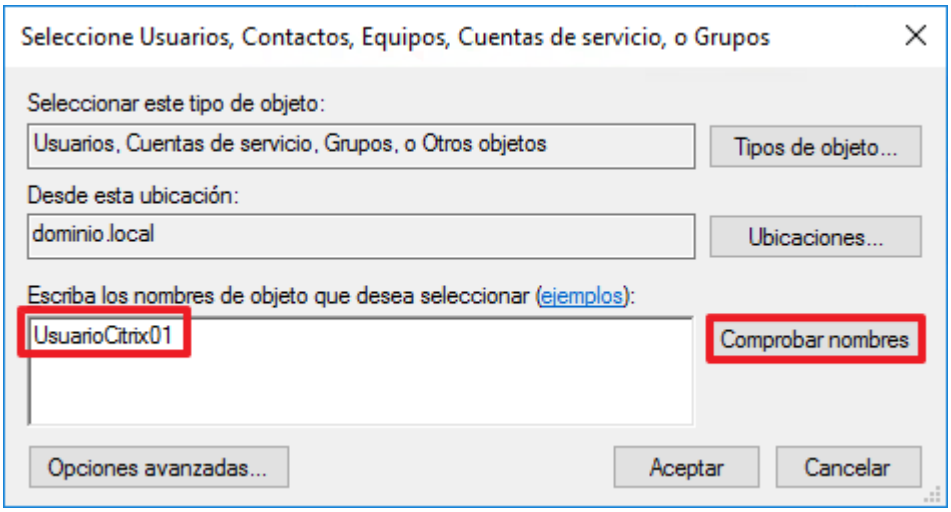
| Paso | Descripción |
|---|---|
| 11. | De igual forma, ejecute con privilegios de administrador (opción “Ejecutar como administrador”) el script “CCN-STIC-684 ENS categoria basica - Preparacion del Dominio - Paso 2.bat”.<br>  |
| 12. | El sistema solicitará elevación de privilegios, pulse “Si” para continuar.<br>  |

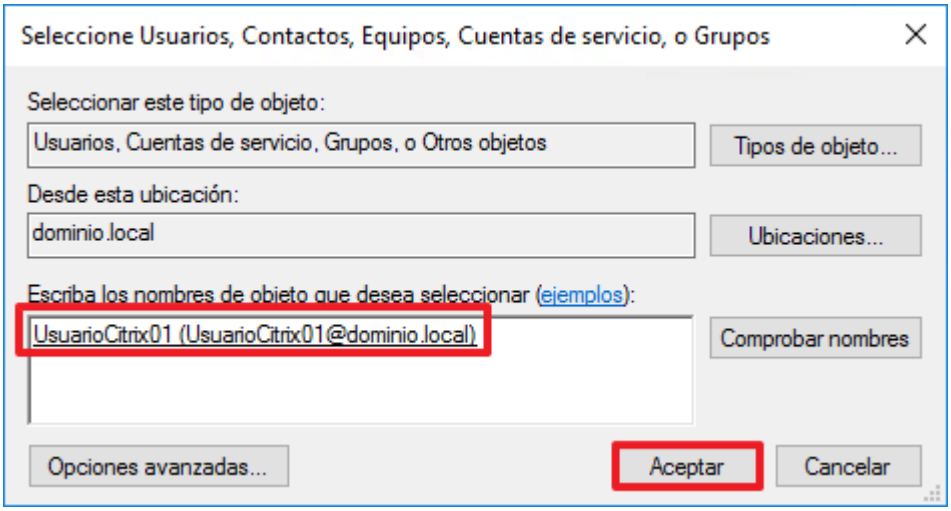
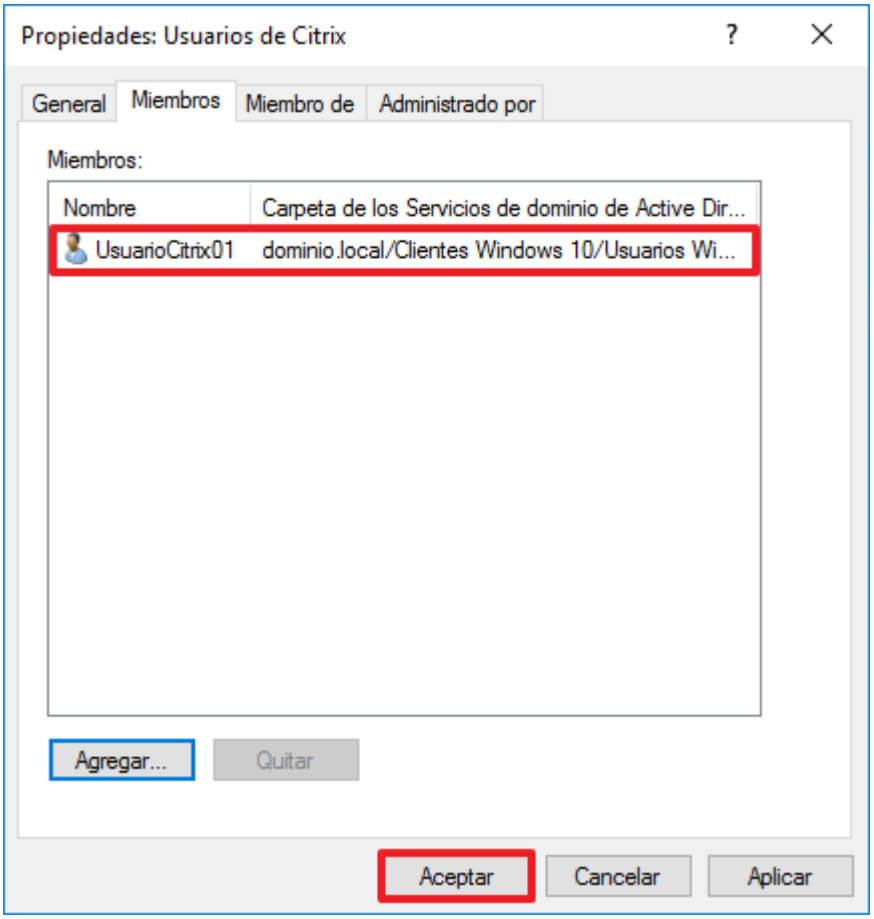
| Paso | Descripción |
|---|---|
| 13. | Se lanzará una ventana del intérprete de comandos “cmd.exe” como la mostrada en la siguiente figura.<br>Este script copia las plantillas de seguridad a la ubicación “C:\Windows\security\templates” y crea el grupo de seguridad “Usuarios de Citrix” si éste no existiese.<br>  |
| 14. | Una vez finalizado pulse una tecla para concluir la ejecución del script.<br>  |

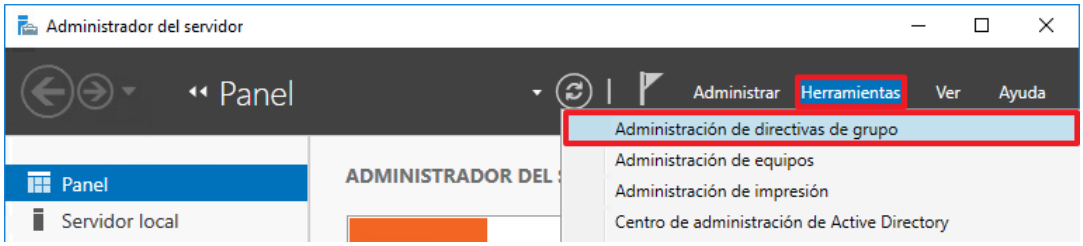
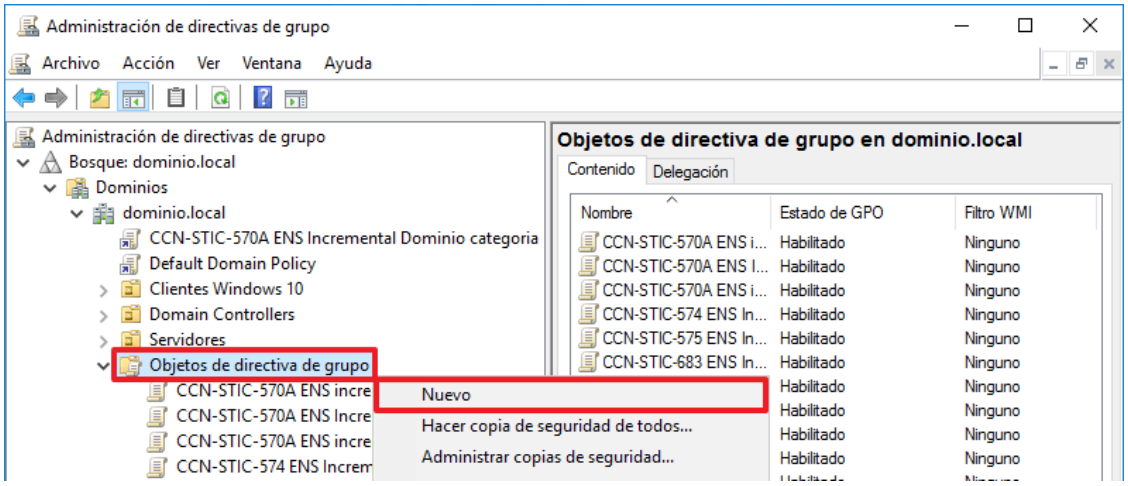
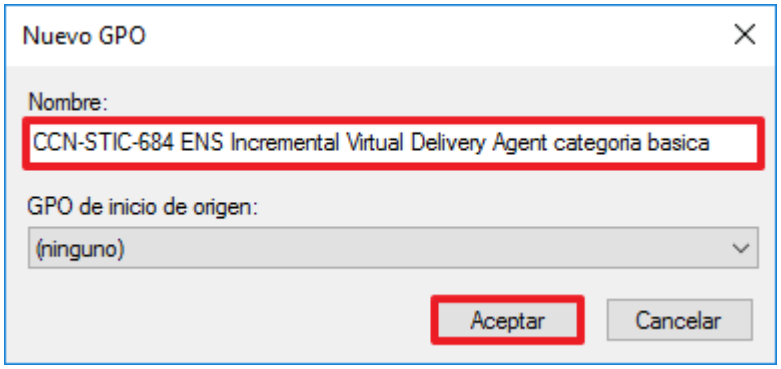
| Paso | Descripción |
|---|---|
| 15. | Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios.<br>  |
| 16. | A continuación, en la herramienta "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.<br>  |

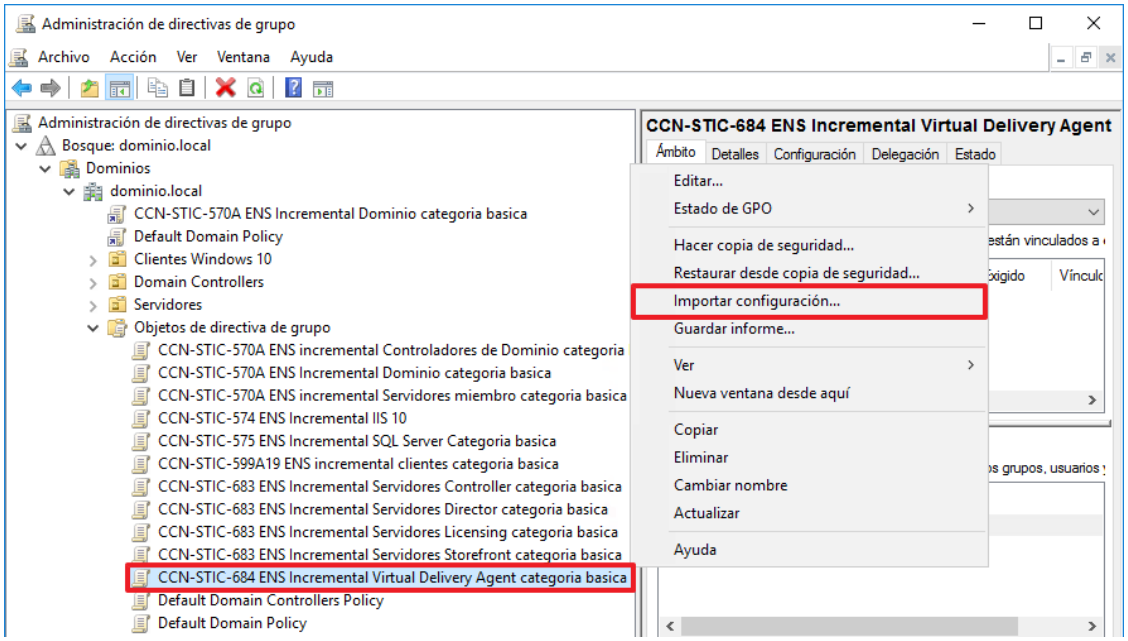
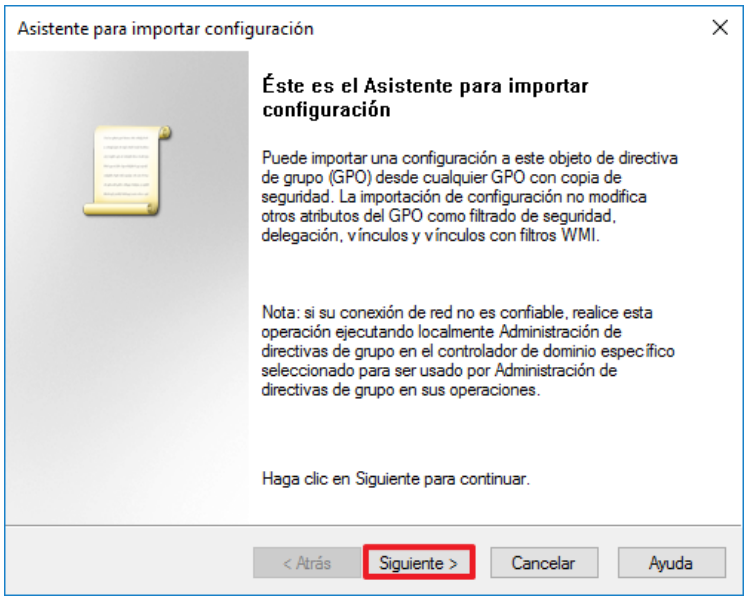
| Paso | Descripción |
|---|---|
| 17. | En la ventana resultante, introduzca como nombre de la nueva unidad organizativa “Servidores Citrix Virtual Delivery Agent” tal y como muestra en la imagen. No desmarque la opción “Proteger contenedores contra eliminación accidental”. Pulse “Aceptar” para crear el nuevo objeto.<br>  <br><br>**Nota:** En este punto deberá crear aquellas unidades organizativas que sean necesarias para la administración de su organización. |
| 18. | Vaya a las unidades organizativas donde se encuentren los equipos que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover…” en cada uno de ellos.<br>  <br><br>**Nota:** En este ejemplo se encuentra bajo la unidad organizativa “Servidores”. |

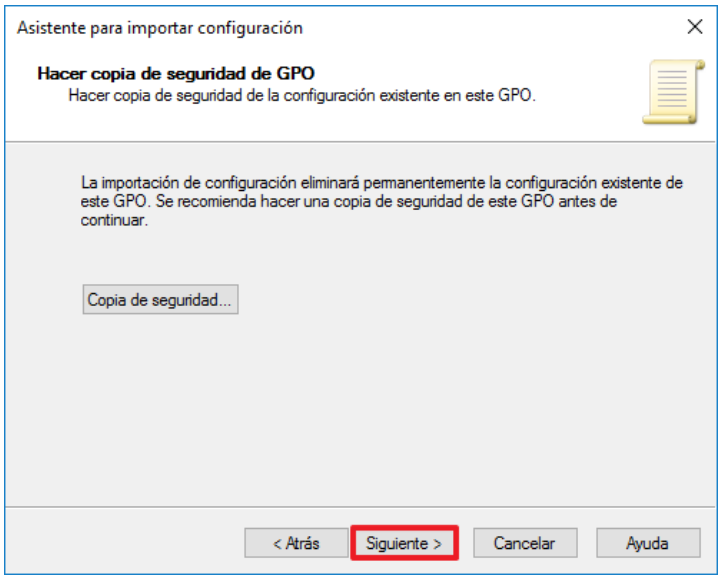
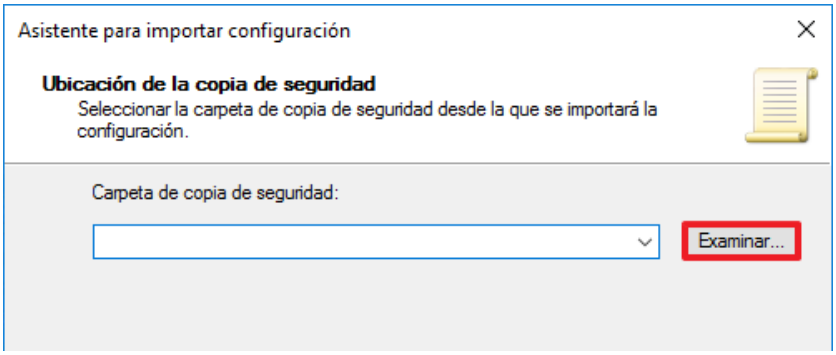
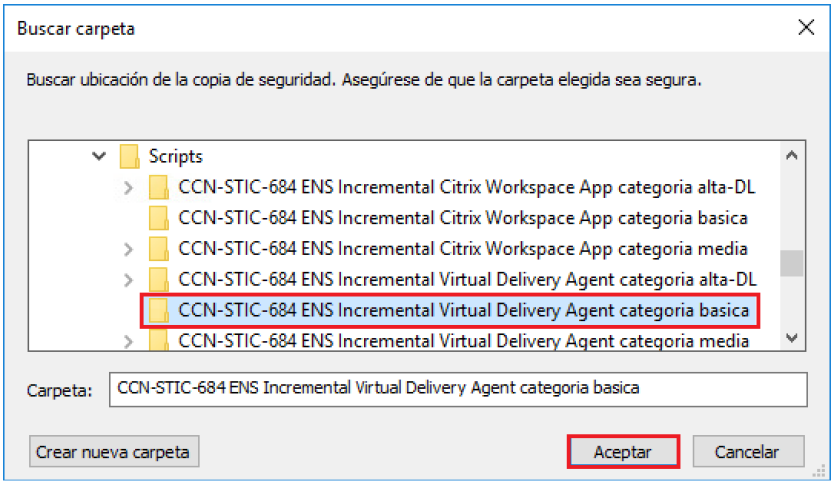
| Paso | Descripción |
|---|---|
| 19. | Seleccione la unidad organizativa “Servidores Citrix Virtual Delivery Agent” creada anteriormente y pulse “Aceptar”.<br>  |
| 20. | A continuación, proceda a incluir a los usuarios que harán uso de la infraestructura de Citrix dentro del grupo de seguridad “Usuarios de Citrix”, para ello expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"** y seleccionando el grupo de seguridad “Usuarios de Citrix” haga clic derecho sobre él y acceda al menú “Propiedades” del menú contextual que aparecerá.<br>  |

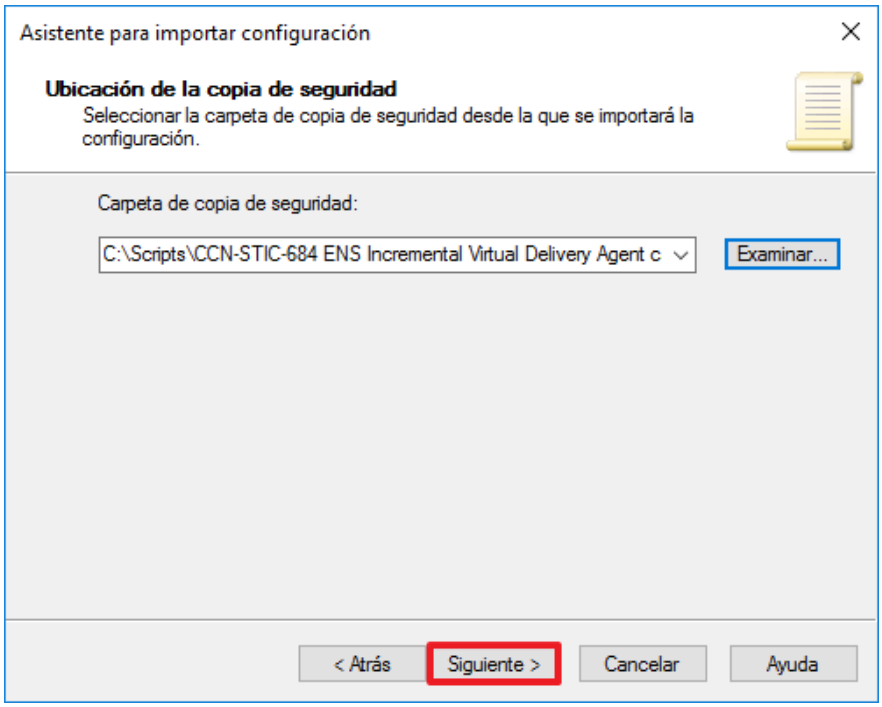
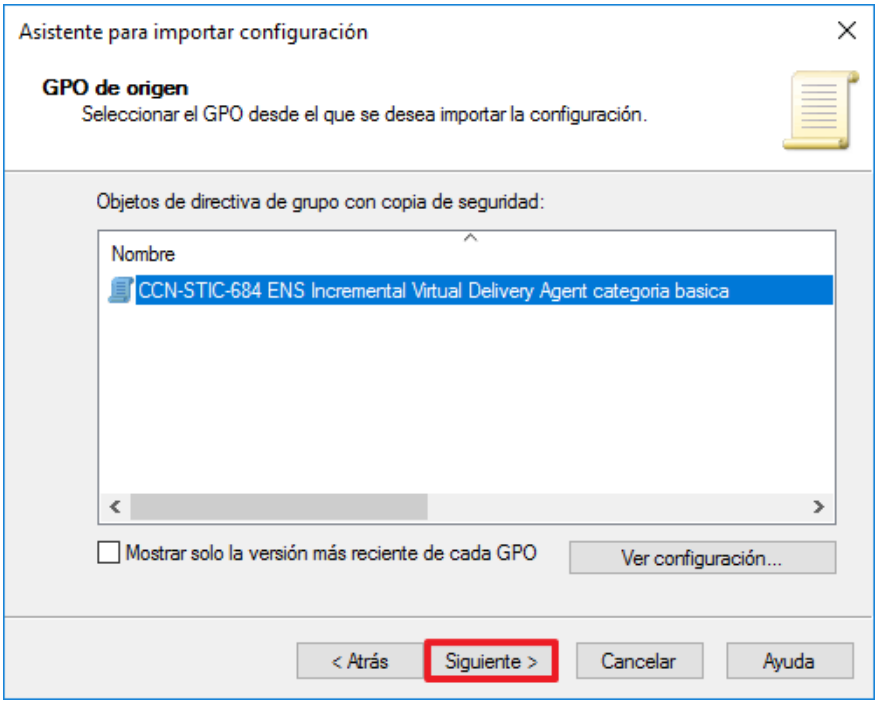
| Paso | Descripción |
|---|---|
| 21. | Dentro de las propiedades del grupo, en la pestaña “Miembros” pulse “Agregar…”.<br>  |
| 22. | Escriba el nombre del usuario que desee agregar al grupo y pulse “Comprobar nombres”.<br>  <br>**Nota:** En este ejemplo se utiliza el usuario “UsuarioCitrix01”. Deberá agregar al grupo “Usuarios de Citrix” los usuarios creados en su organización para hacer uso de los recursos entregados mediante Virtual Delivery Agent. |

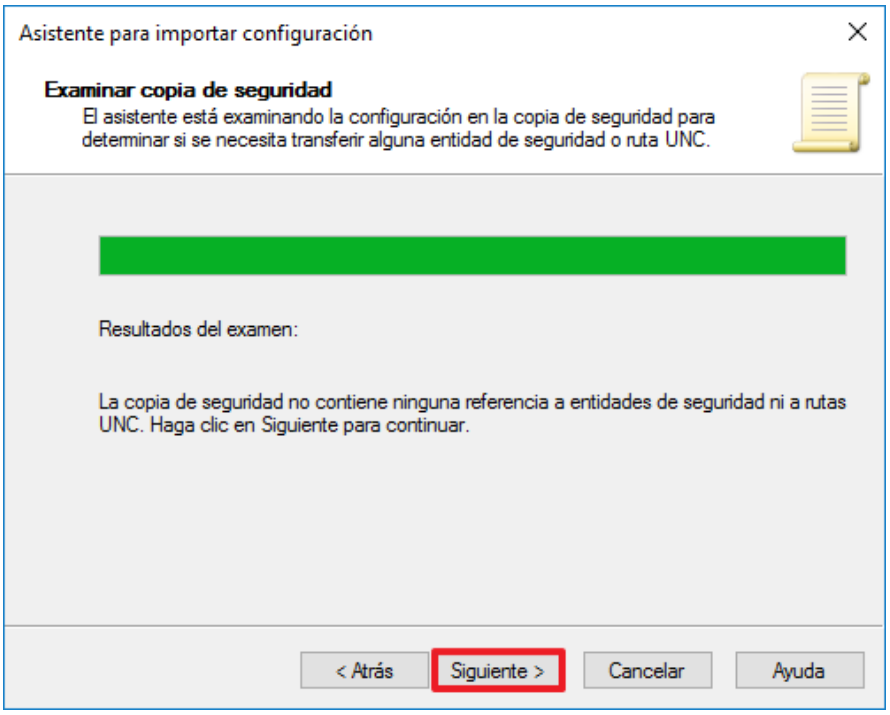
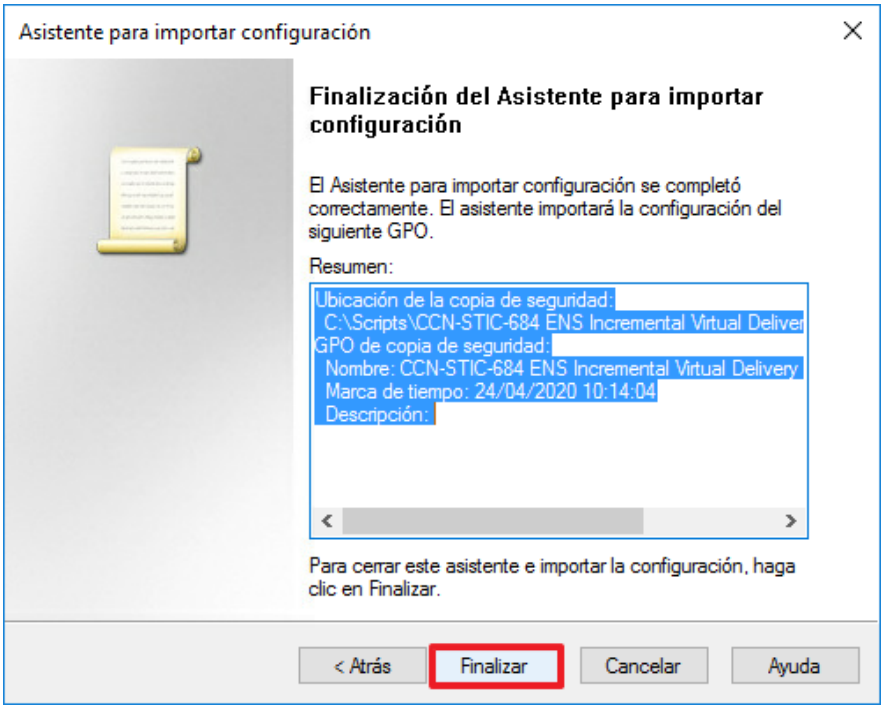
| Paso | Descripción |
|---|---|
| 23. | Compruebe que el usuario sea el correcto y pulse “Aceptar” para agregarlo y cerrar la ventana.<br>  |
| 24. | El usuario aparecerá agregado al grupo “Usuarios de Citrix” pulse “Aceptar” para guardar la configuración y cerrar la ventana. Repita estos pasos para todos aquellos usuarios que desee agregar al grupo.<br>  |
| 25. | Cierre la herramienta “Usuarios y equipos de Directorio Activo”. |

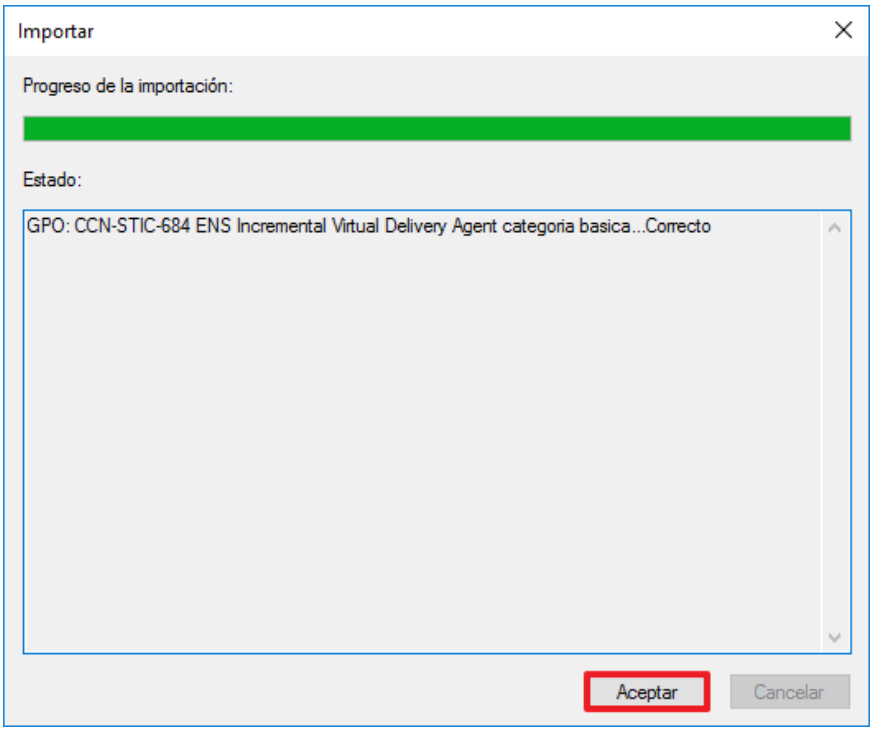
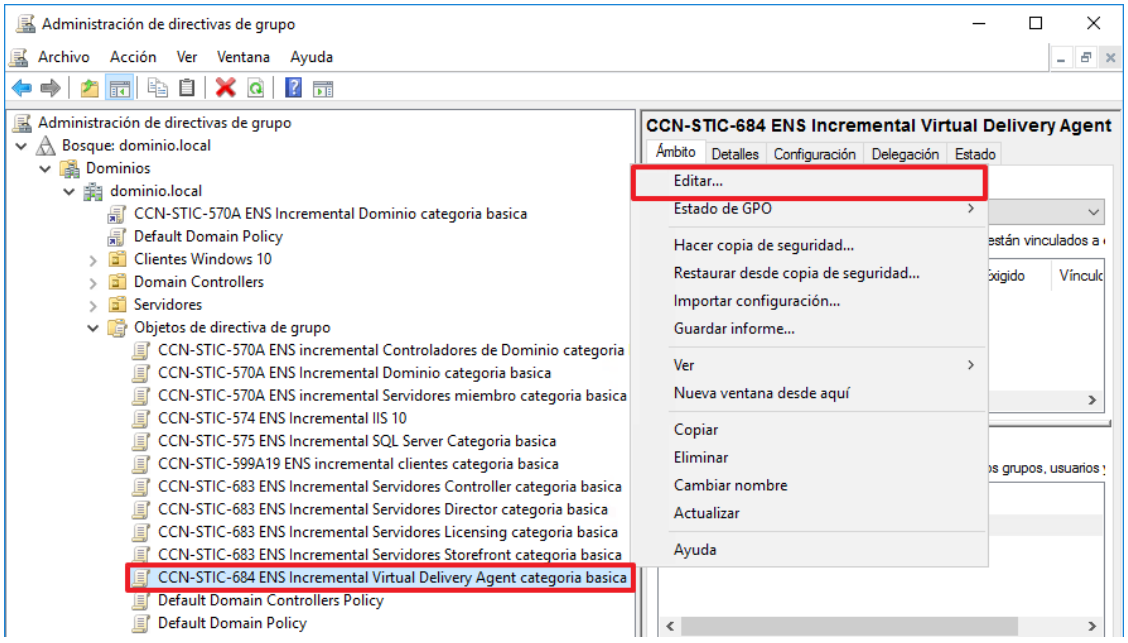
| Paso | Descripción |
|---|---|
| 26. | Utilice la herramienta "Administración de Directivas de grupo" (**Administrador del servidor → Herramientas → Administración de Directivas de grupo**). El sistema solicitará elevación de privilegios.<br>  |
| 27. | Expanda el contenedor **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPOs correspondiente. |
| 28. | 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.<br>  |
| 29. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica" y pulse el botón “Aceptar”.<br>  |

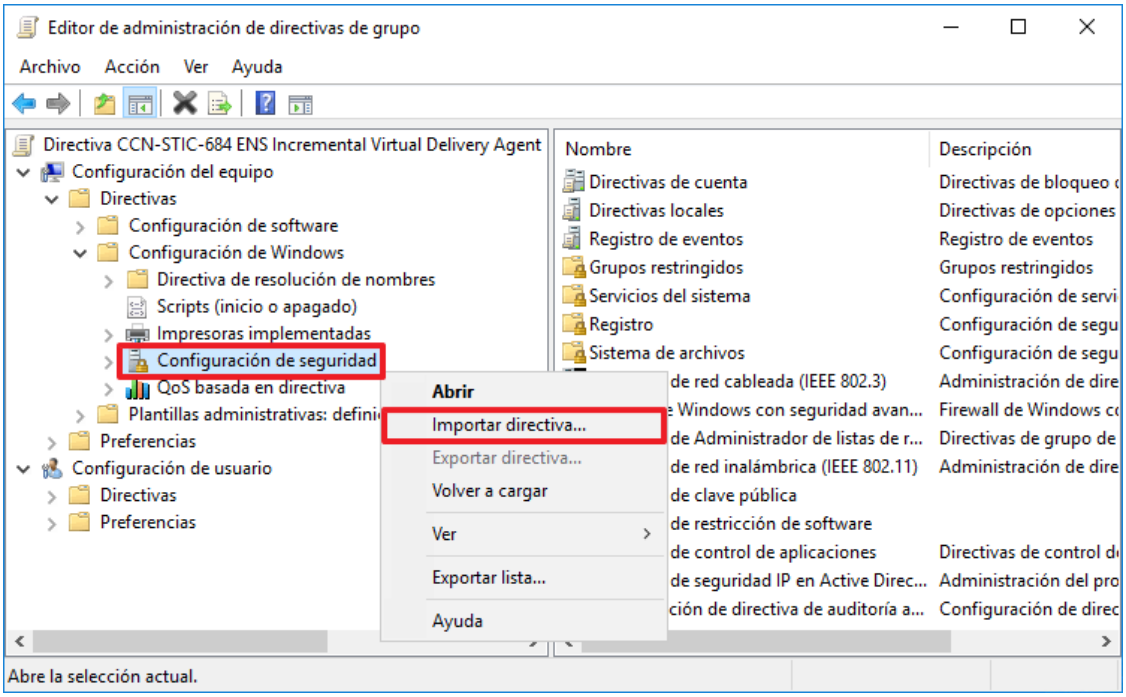
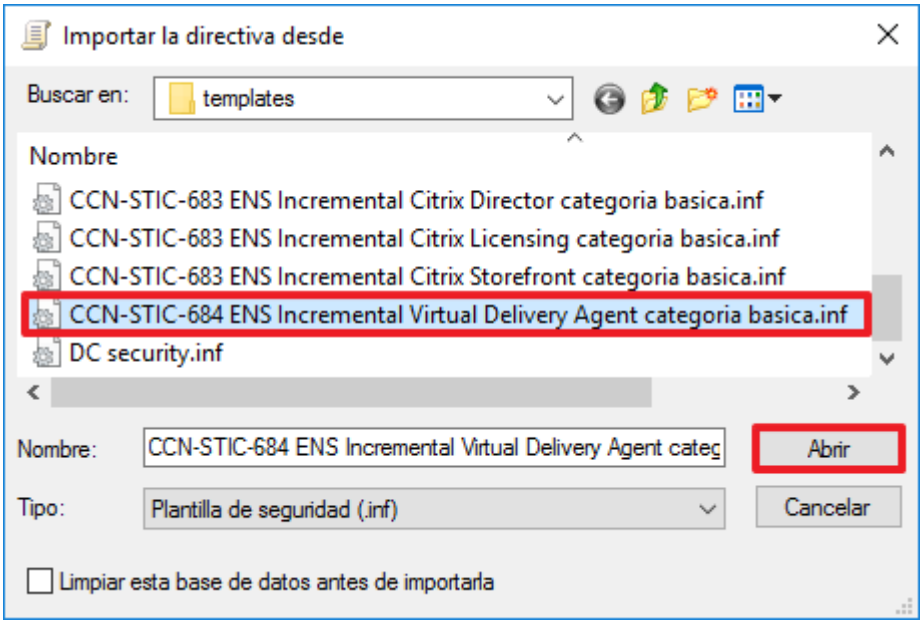
| Paso | Descripción |
|---|---|
| 30. | Seleccione el GPO recién creado, "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica", y marcando con el botón derecho en él, elija la opción "Importar configuración…" del menú contextual que aparecerá.<br>  |
| 31. | En el asistente de importación de configuración, pulse el botón “Siguiente >”.<br>  |

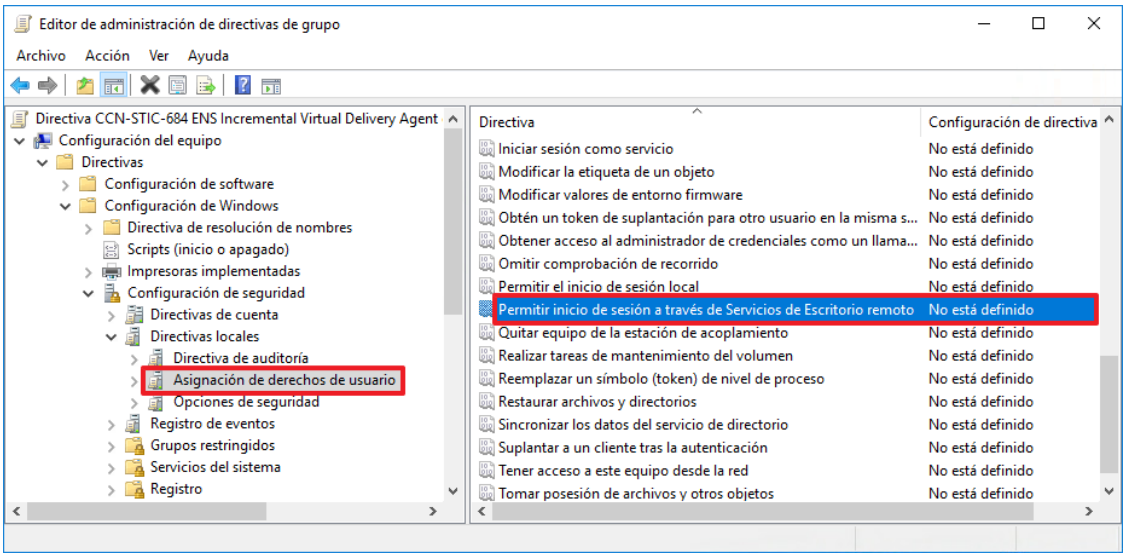
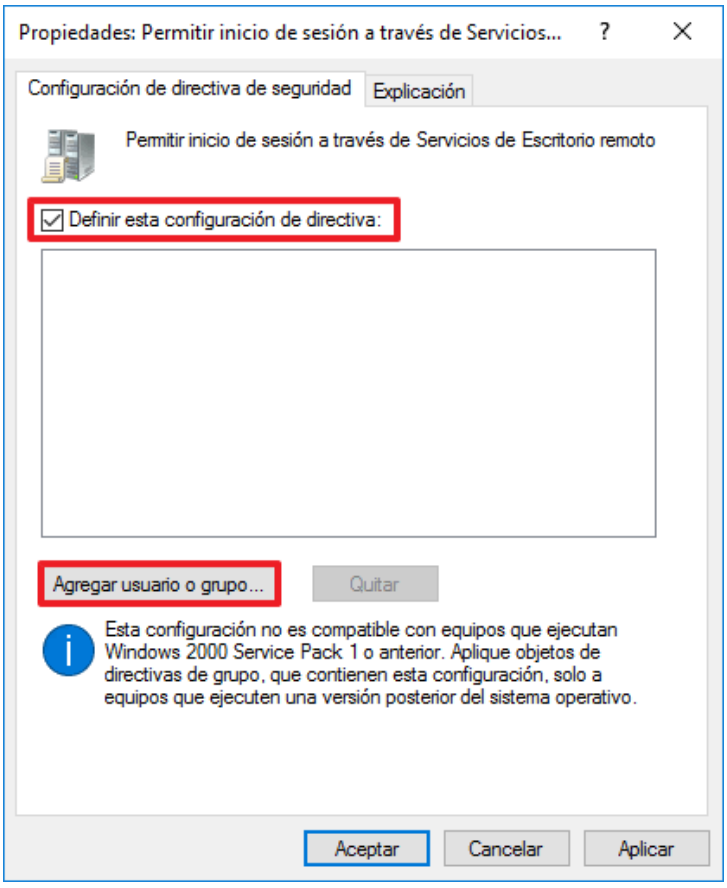
| Paso | Descripción |
|---|---|
| 32. | En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |
| 33. | Pulse el botón “Examinar...” en la ventana “Ubicación de la copia de seguridad”.<br>  |
| 34. | Seleccione la carpeta “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.<br>  |

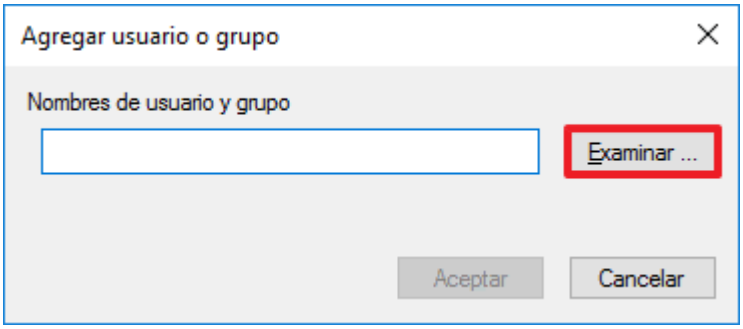
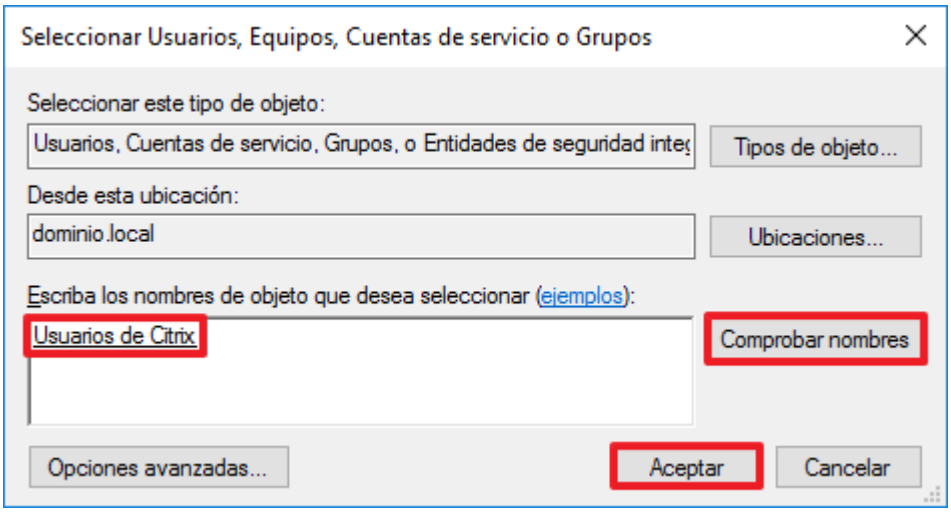
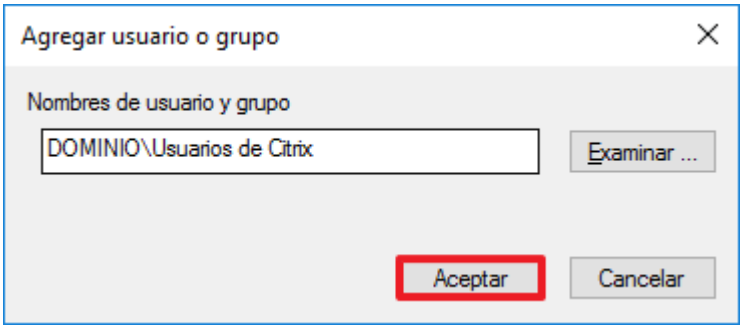
| Paso | Descripción |
|---|---|
| 35. | En la selección de copia de carpeta de seguridad pulse el botón “Siguiente >”.<br>  |
| 36. | En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica” y pulse el botón “Siguiente >”.<br>  |

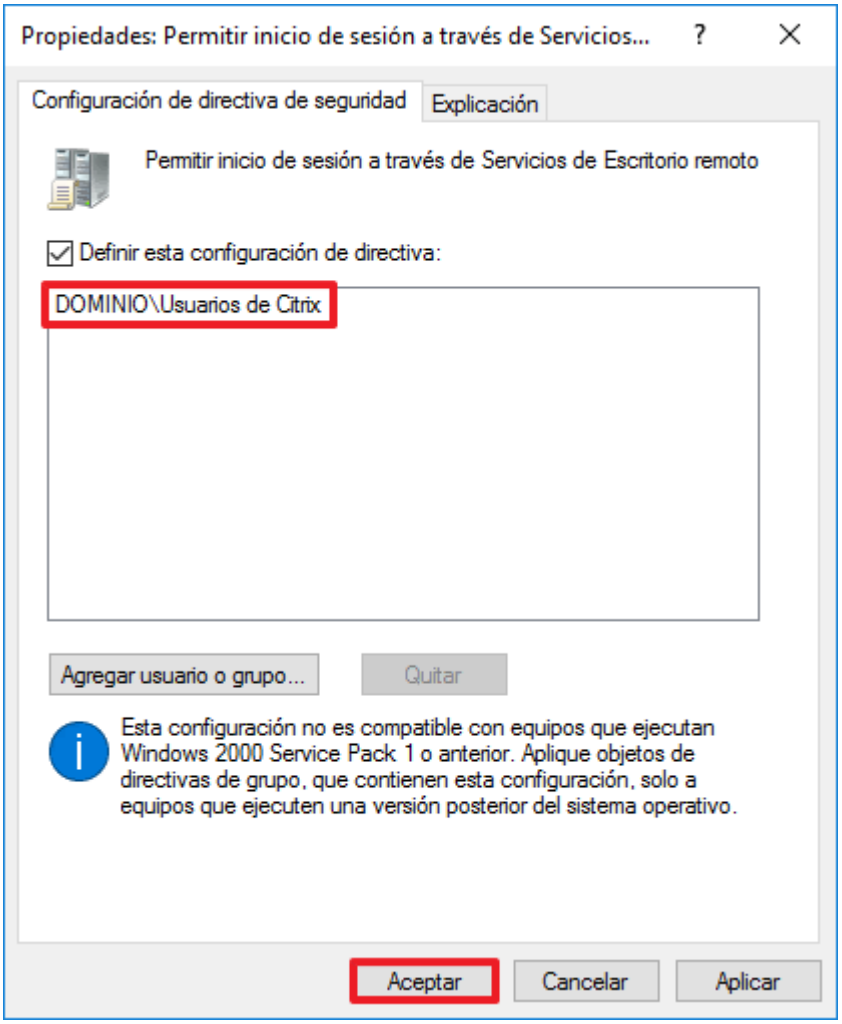
| Paso | Descripción |
|---|---|
| 37. | En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”.<br>  |
| 38. | Para completar el asistente pulse el botón “Finalizar”.<br>  |

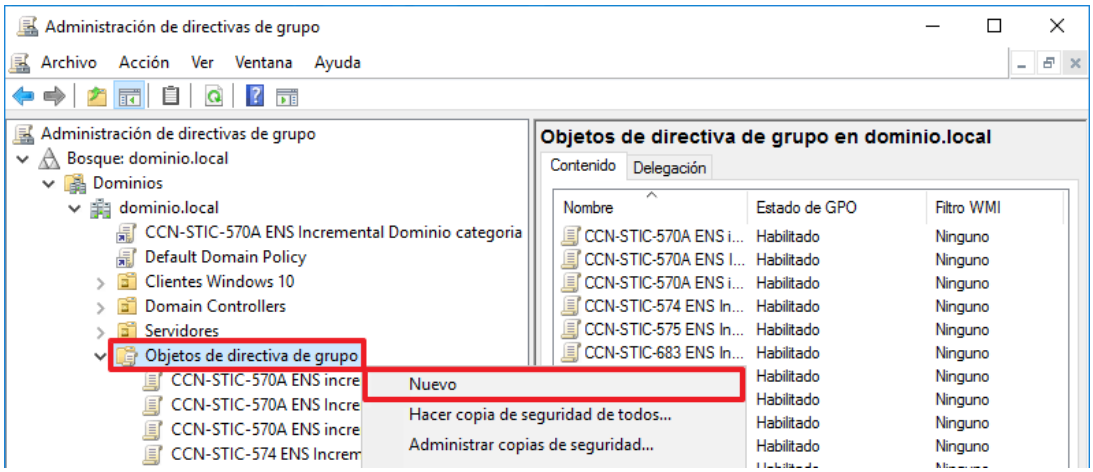
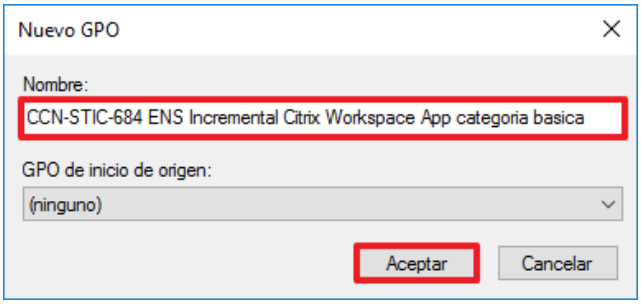
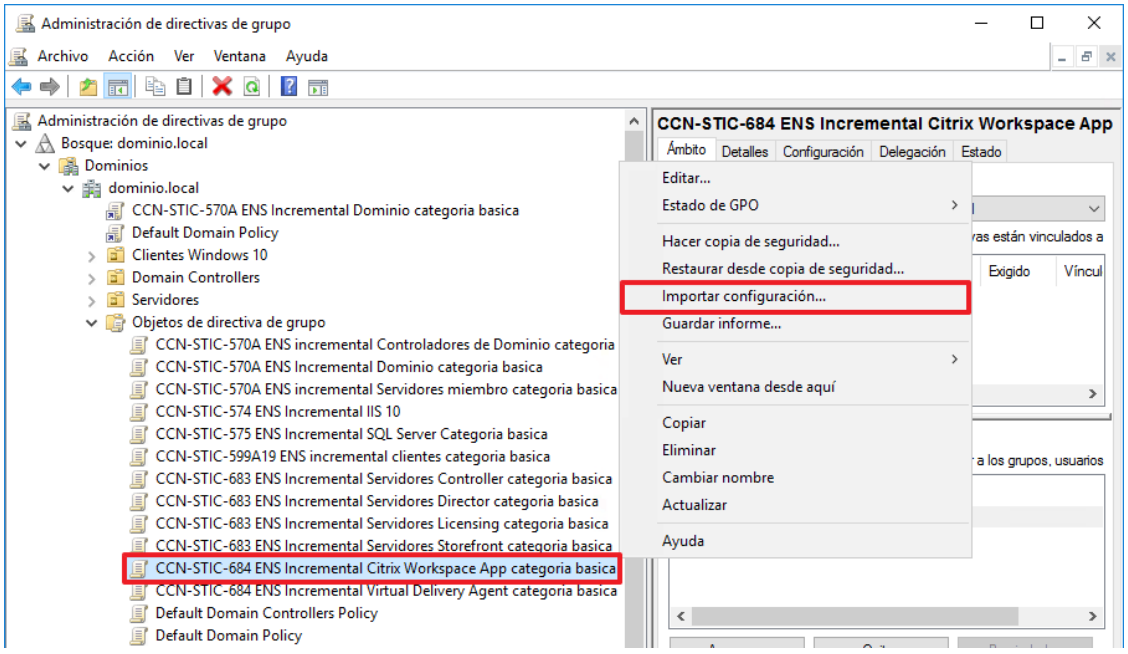
| Paso | Descripción |
|---|---|
| 39. | Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.<br>  |
| 40. | Seleccione de nuevo el GPO, "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica", y marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.<br>  |

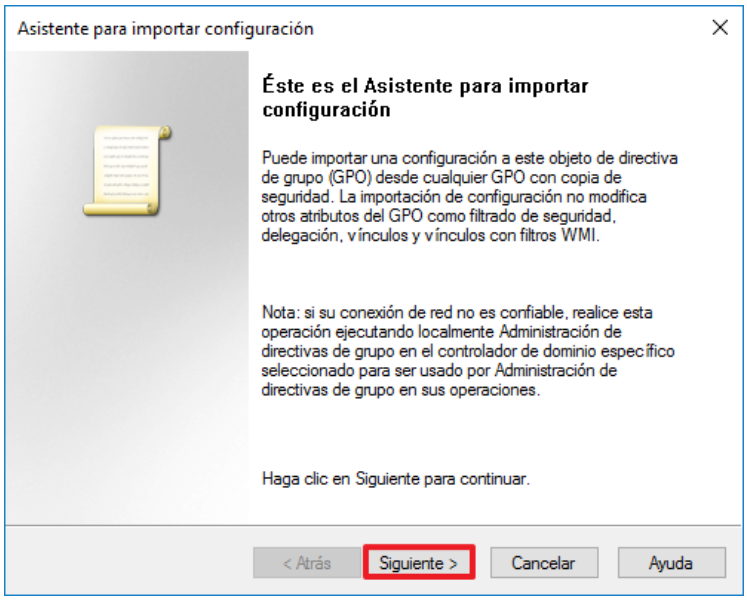
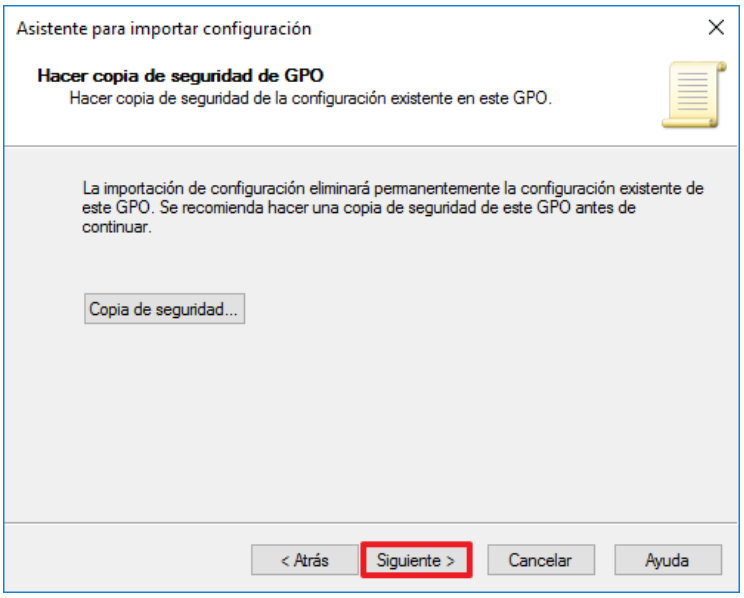
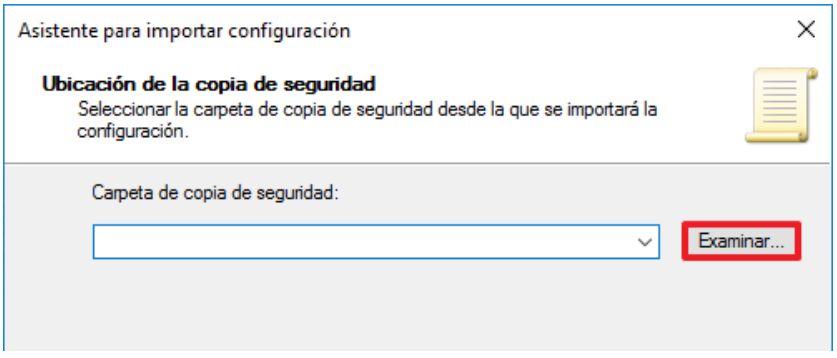
| Paso | Descripción |
|---|---|
| 41. | En la ventana del editor de administración de directivas de grupo, seleccione el nodo **"Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"** y, marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá.   |
| 42. | En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica.inf" y pulse el botón "Abrir". Con eso habrá quedado importada la plantilla de seguridad en el GPO.   |

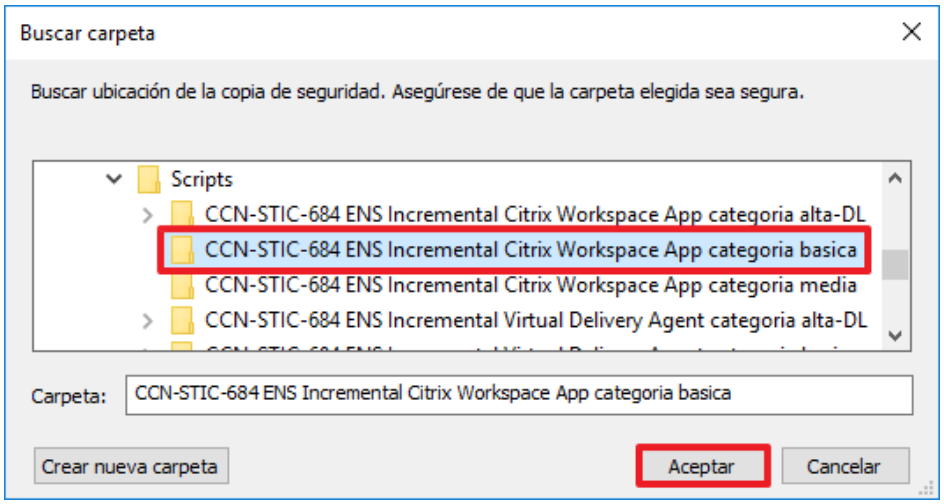
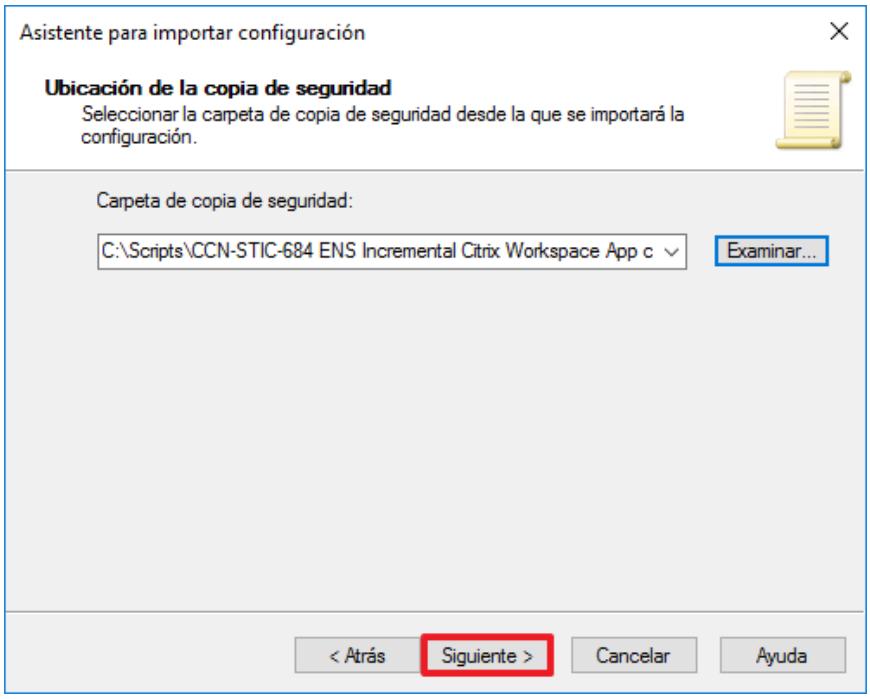
| Paso | Descripción |
|---|---|
| 43. | Continúe editando la directiva de grupo, diríjase al nodo **"Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** y haga doble clic sobre la directiva "Permitir inicio de sesión a través de Escritorio remoto" para proceder a configurarla.<br>  |
| 44. | Marque la casilla "Definir esta configuración de directiva" para habilitar las opciones de configuración. A continuación, pulse sobre "Agregar usuario o grupo".<br>  |

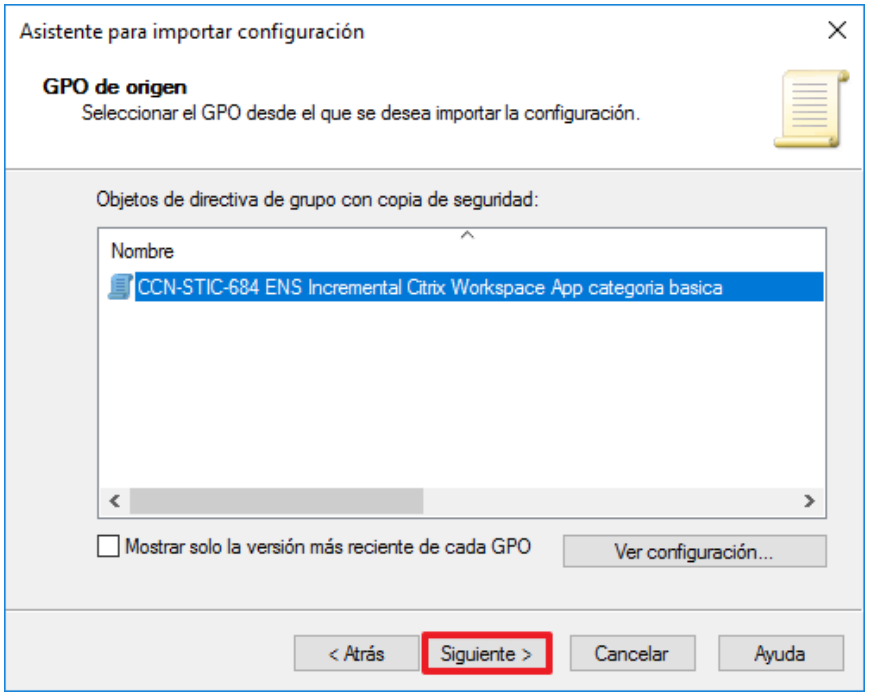
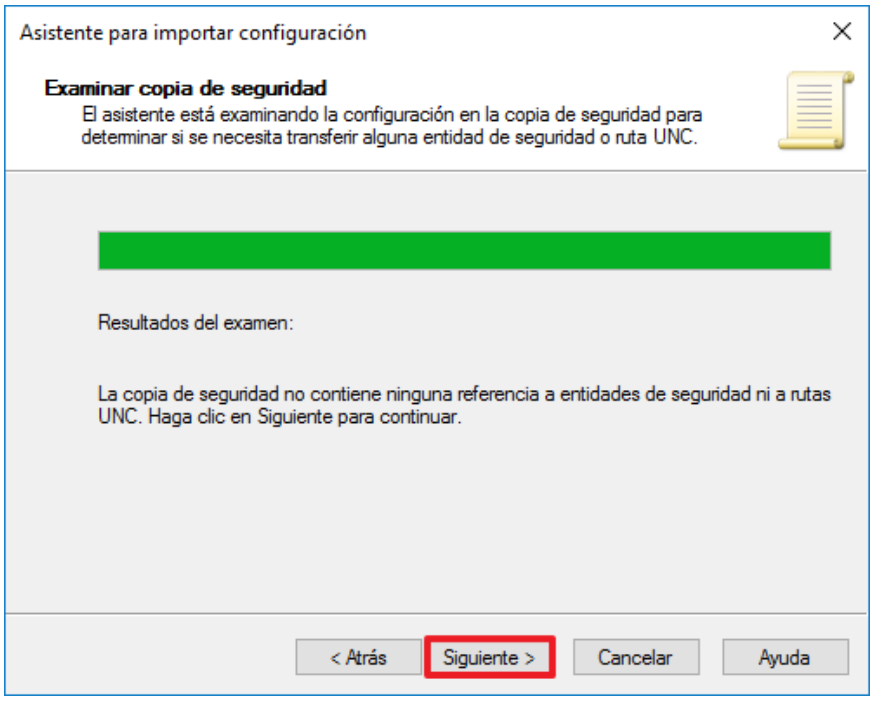
| Paso | Descripción |
|---|---|
| 45. | En la ventana resultante haga clic en “Examinar …”.<br>  |
| 46. | Escriba el nombre del grupo “Usuarios de Citrix” y en este orden pulse en primer lugar sobre “Comprobar nombres” y a continuación sobre “Aceptar”.<br>  <br>**Nota:** El grupo “Usuarios de Citrix” se deberá haber creado al comienzo de esta guía mediante la ejecución del script “CCN-STIC-684 ENS categoria basica - Preparacion del Dominio - Paso 2.bat”. |
| 47. | Pulse “Aceptar” para añadir el grupo “Usuarios de Citrix a la directiva”.<br>  |

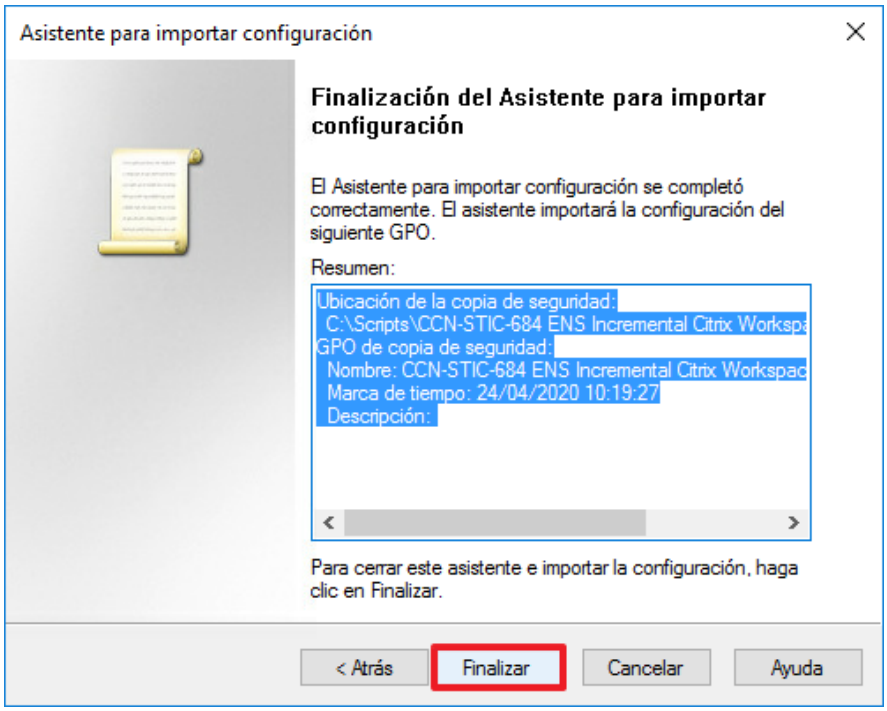
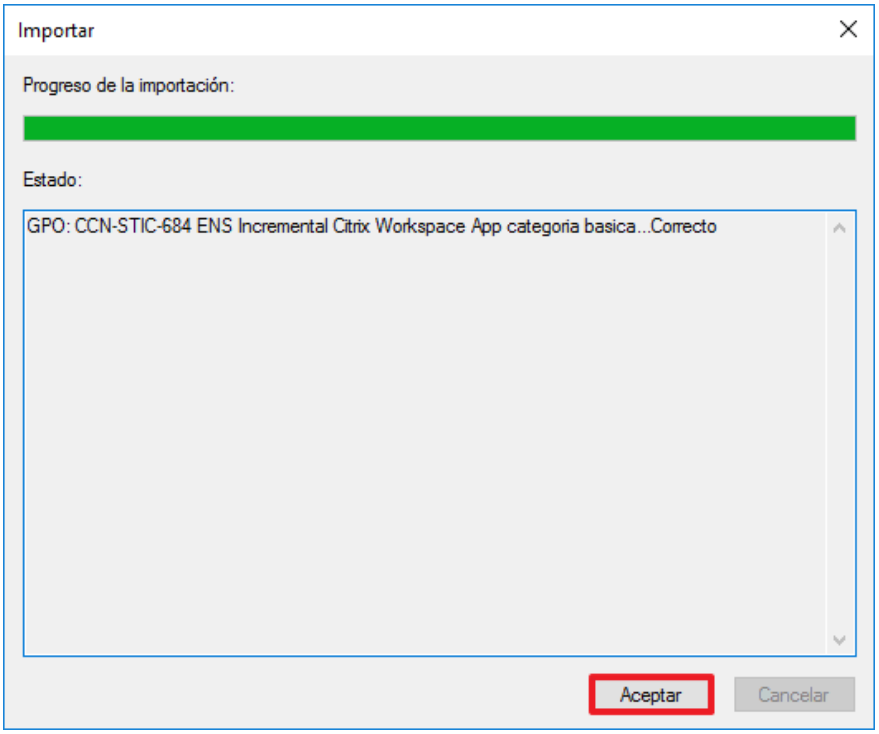
| Paso | Descripción |
|---|---|
| 48. | Aparecerá el grupo “Usuarios de Citrix” definido en la directiva. Pulse “Aceptar” para guardar la configuración y cerrar la ventana.<br>  <br>**Nota:** Ahora sí, cierre la ventana del editor de administración de directivas de grupo. |
| 49. | Con ello este GPO ("CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. |

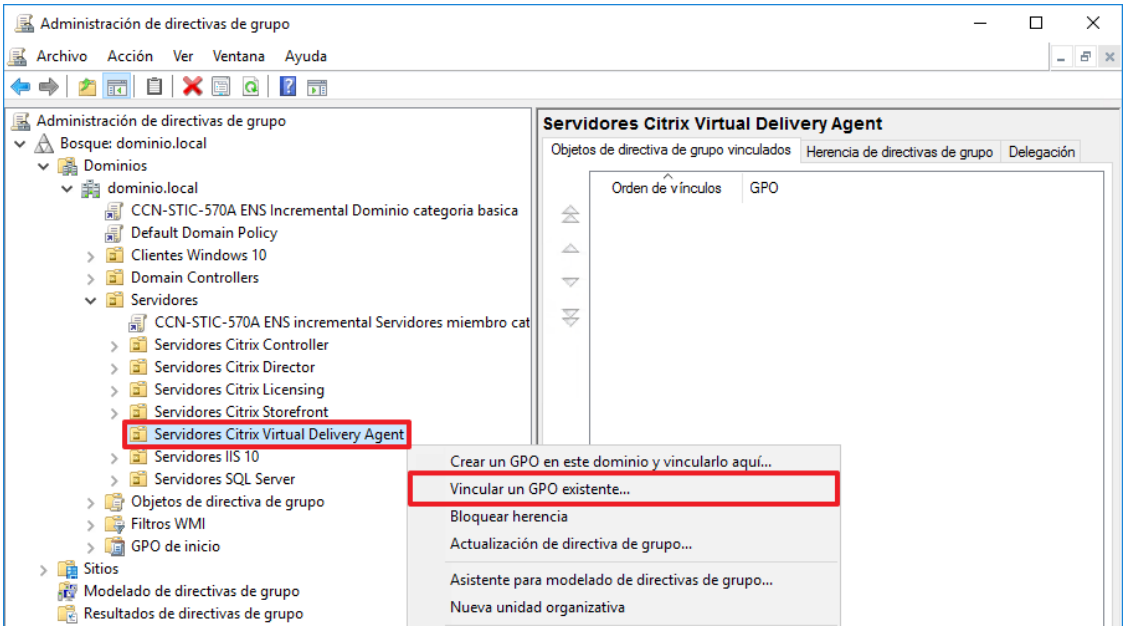
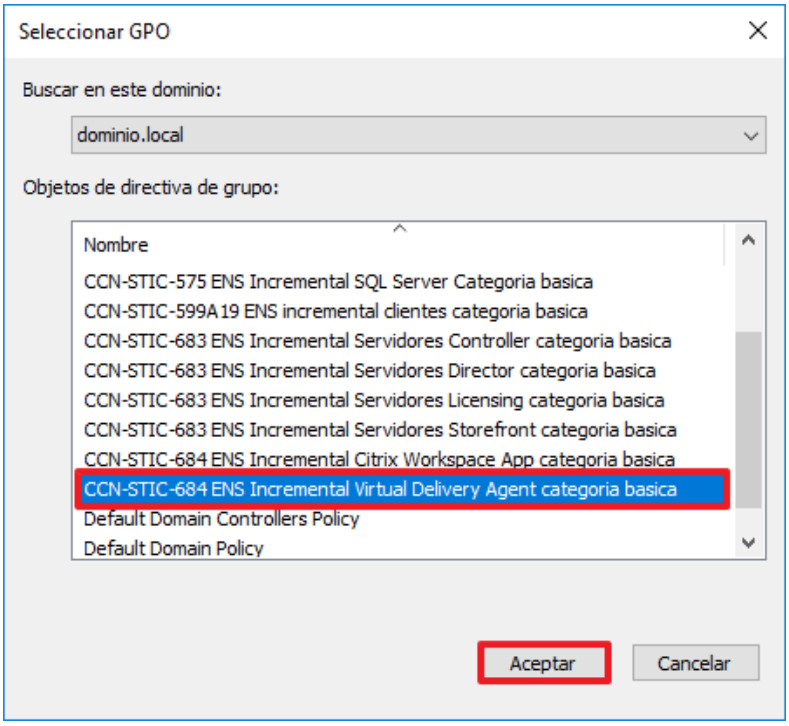
| Paso | Descripción |
|---|---|
| 50. | Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá.<br>  |
| 51. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica" y pulse el botón “Aceptar”.<br>  |
| 52. | Seleccione el GPO recién creado, "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica", y marcando con el botón derecho en él, elija la opción "Importar configuración..." del menú contextual que aparecerá.<br>  |

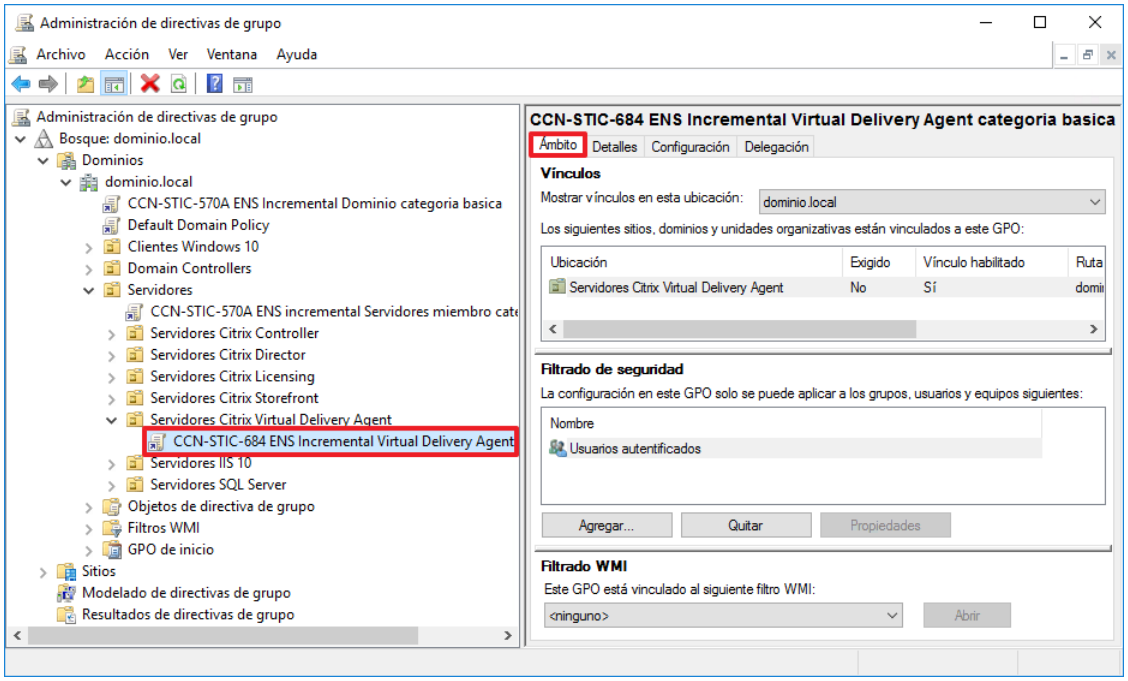
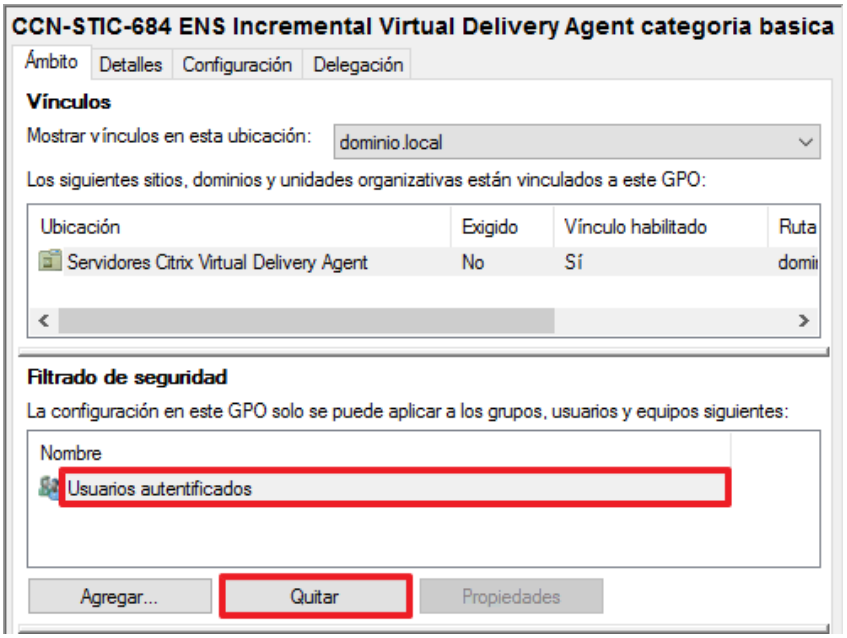
| Paso | Descripción |
|---|---|
| 53. | En el asistente de importación de configuración, pulse el botón “Siguiente >”.<br>  |
| 54. | En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |
| 55. | Pulse el botón “Examinar...” en la ventana “Ubicación de la copia de seguridad”.<br>  |

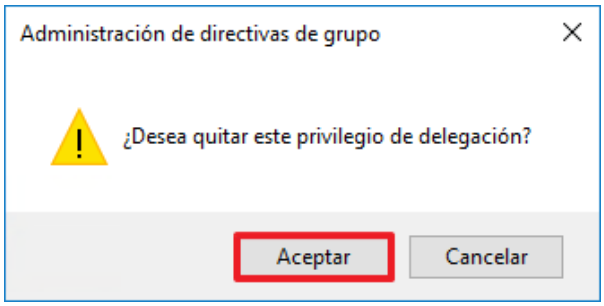
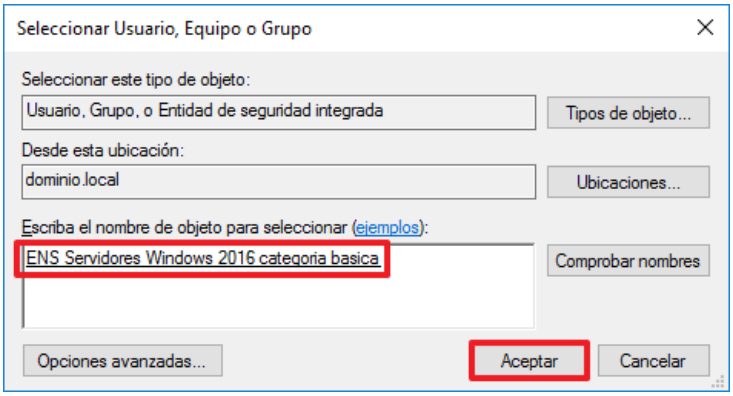
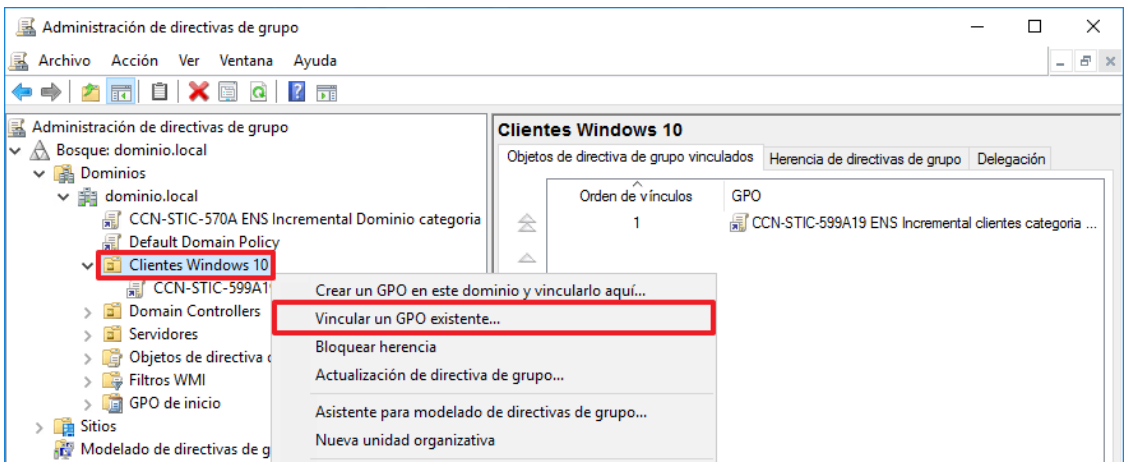
| Paso | Descripción |
|---|---|
| 56. | Seleccione la carpeta “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.<br>  |
| 57. | En la selección de copia de carpeta de seguridad pulse el botón “Siguiente >”.<br>  |

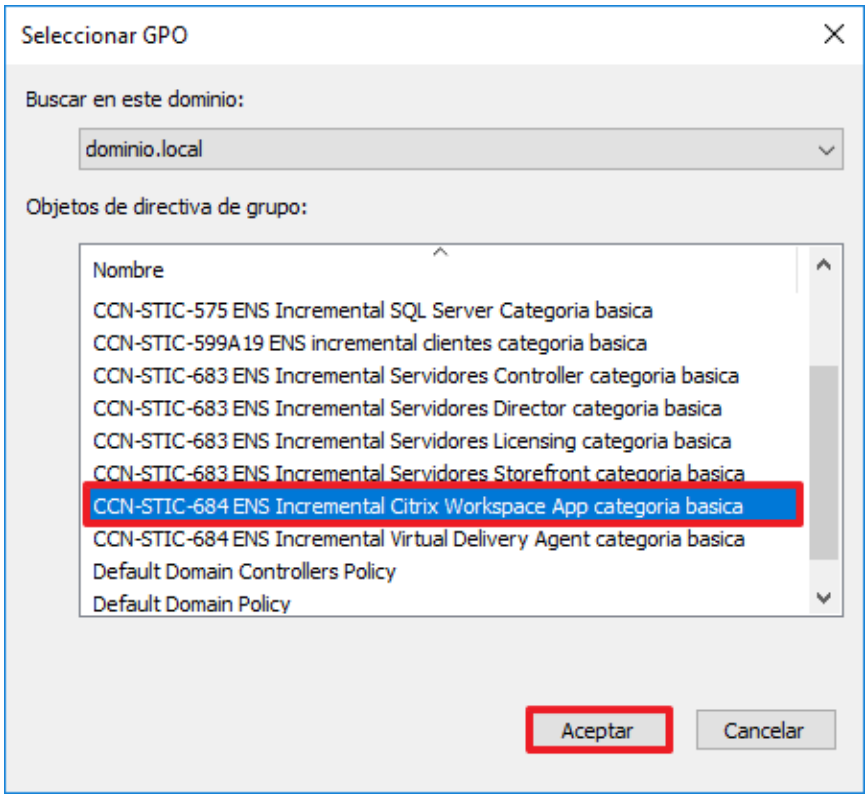
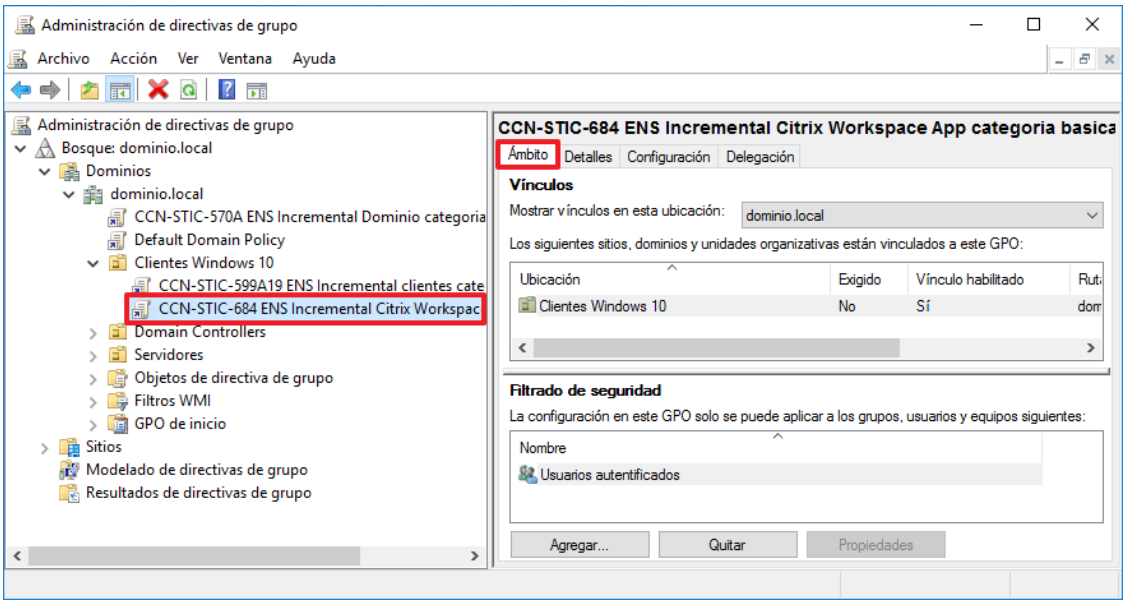
| Paso | Descripción |
|---|---|
| 58. | En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” y pulse el botón “Siguiente >”.<br>  |
| 59. | En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”.<br>  |

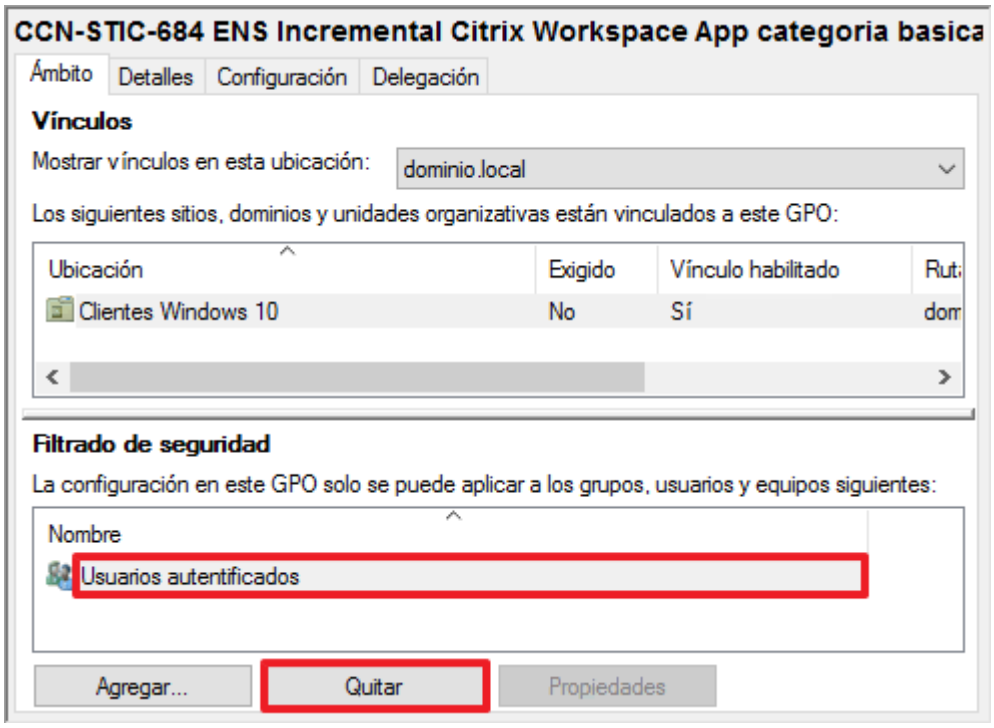
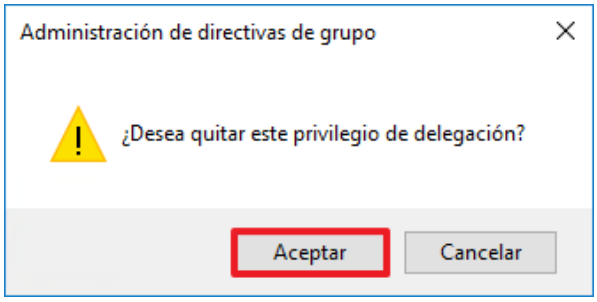
| Paso | Descripción |
|---|---|
| 60. | Para completar el asistente pulse el botón “Finalizar”.<br>  |
| 61. | Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.<br>  |
| 62. | Con ello, este GPO ("CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que la configuración sea aplicada. |

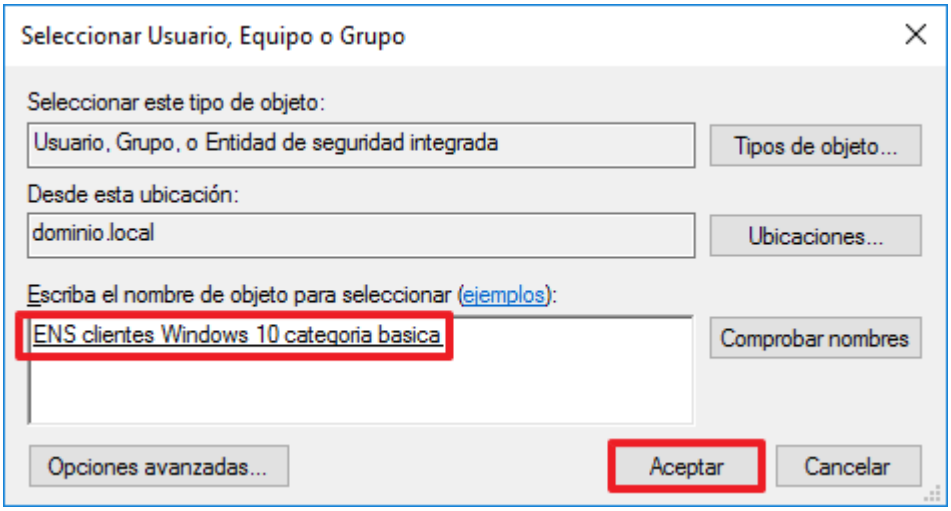
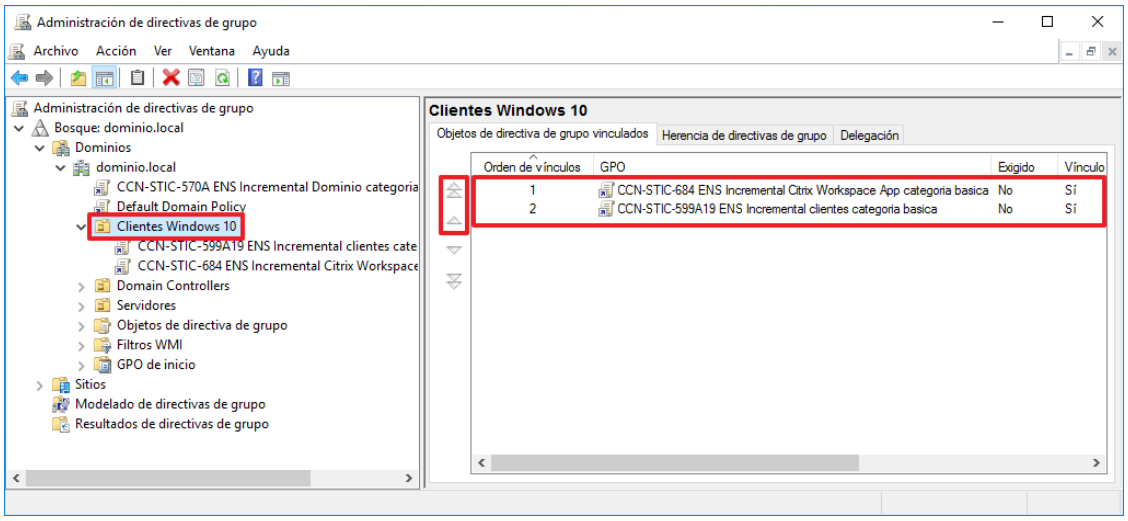
| Paso | Descripción |
|---|---|
| 63. | En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Servidores → Servidores Citrix Virtual Delivery Agent”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá.   |
| 64. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica” y pulse “Aceptar”.   |

| Paso | Descripción |
|---|---|
| 65. | Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.<br>  |
| 66. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.<br>  |

| Paso | Descripción |
|---|---|
| 67. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.<br>  |
| 68. | Una vez quitado, pulse el botón “Agregar…”. |
| 69. | Introduzca como nombre “ENS servidores Windows 2016 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |
| 70. | 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> → Clientes Windows 10”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá.<br>  |

| Paso | Descripción |
|---|---|
| 71. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” y pulse “Aceptar”.<br>  |
| 72. | Seleccione la política de grupo “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.<br>  |

| Paso | Descripción |
|---|---|
| 73. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.<br>  |
| 74. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.<br>  |
| 75. | Una vez quitado, pulse el botón “Agregar…”. |

| Paso | Descripción |
|---|---|
| 76. | Introduzca como nombre “ENS clientes Windows 10 categoria basica”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-599A19”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br><br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |
| 77. | Seleccione el contenedor “Clientes Windows 10” 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.<br>– 1 - CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica<br>– 2 - CCN-STIC-599A19 ENS Incremental clientes categoria basica<br>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.<br>  <br> |

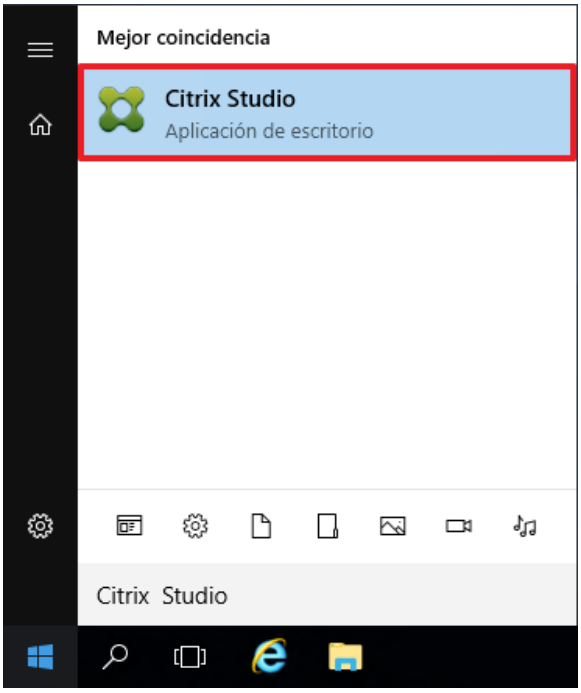
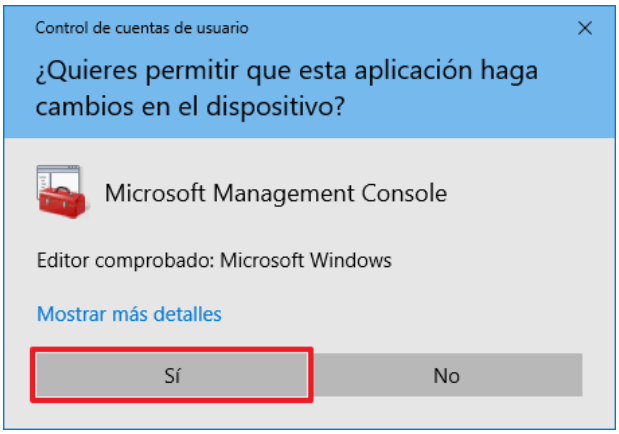
| Paso | Descripción |
|---|---|
| 78. | Compruebe también que el campo "Vínculo habilitado" muestra "Sí" para las GPO recién vinculadas. Si mostrara "No", seleccione el GPO, y marcando con el botón derecho en él, marque la opción "Vínculo habilitado" en el menú contextual que aparecerá. |
| 79. | Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor. |

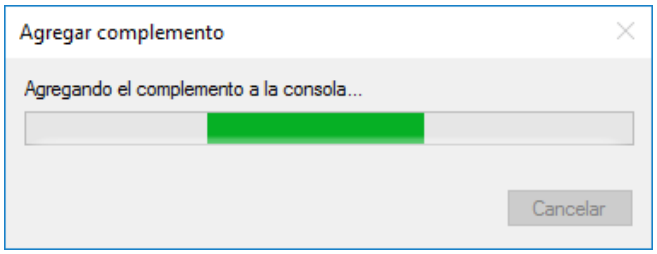
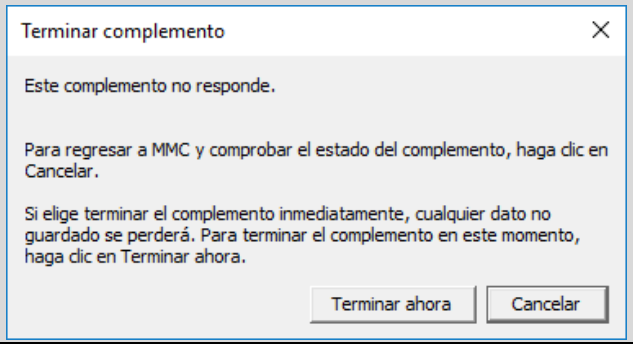
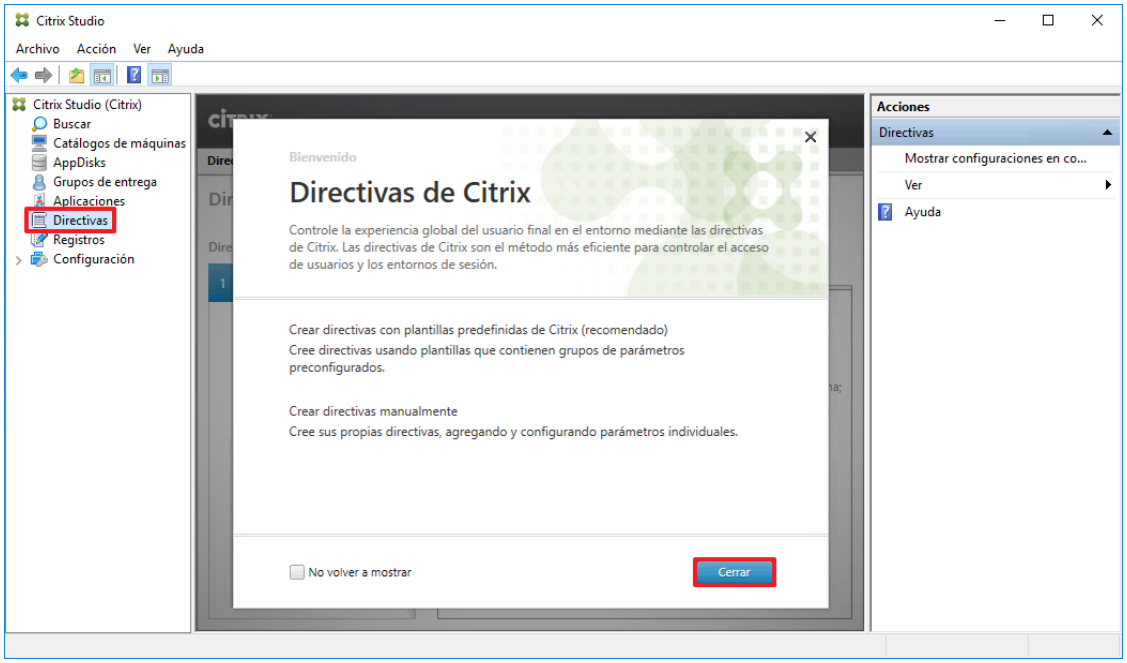
## 2. CONFIGURACIÓN DE SEGURIDAD CITRIX STUDIO

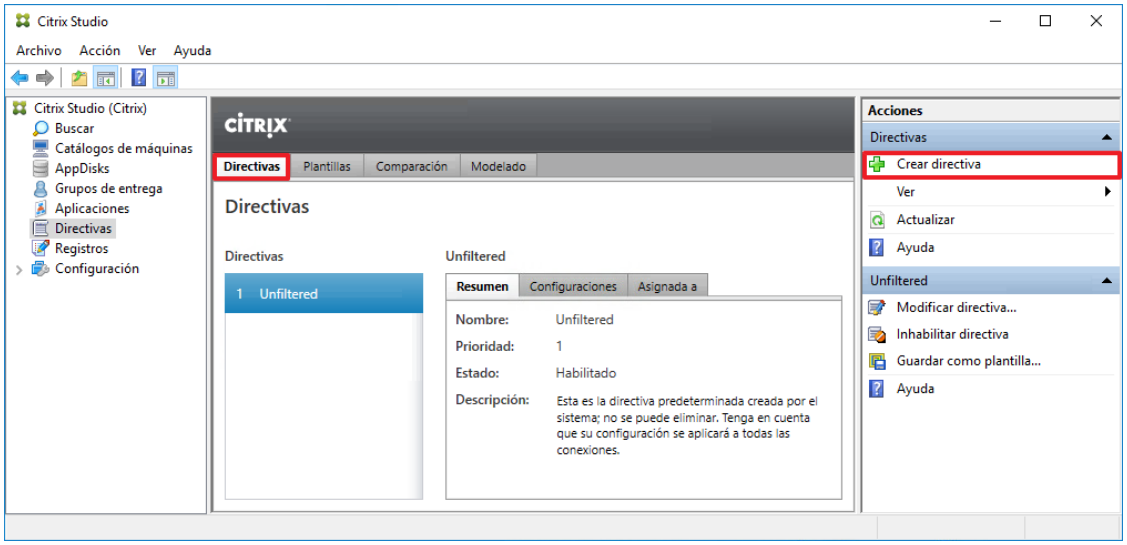
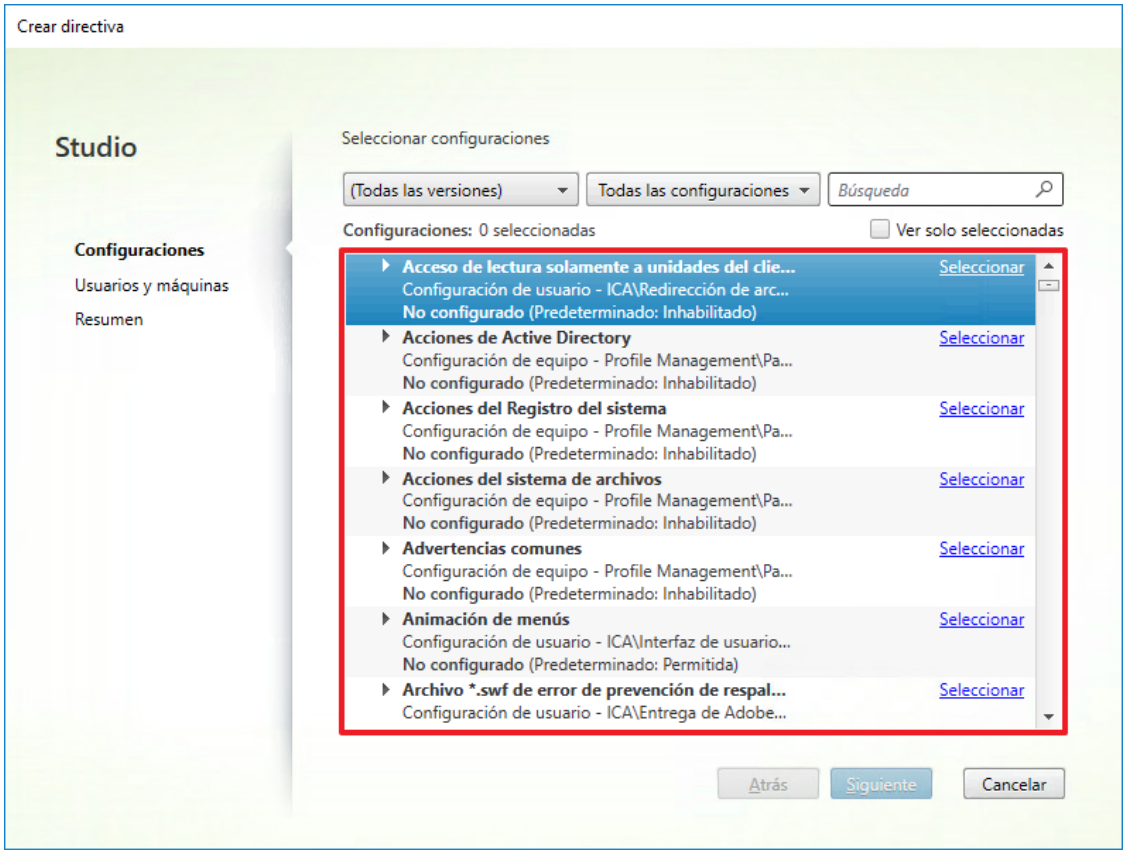
Los pasos que se describen a continuación se realizarán en un servidor con el rol Citrix Controller que haya sido configurado previamente mediante la aplicación de la guía codificada como “CCN-STIC-683 – Categoría Básica”. Los pasos descritos a continuación solo los debe realizar cuando vaya a realizar la primera implementación en el dominio, ya que solo es necesario crear las plantillas de seguridad e incorporarlas en la directiva de seguridad una única vez por infraestructura.

**Nota:** Esta guía asume que al servidor con el rol Citrix Controller se le ha aplicado la configuración descrita en la guía “CCN-STIC-683 Implementación de seguridad en Citrix Virtual Apps and Desktops”. Si no es así, aplique la guía correspondiente antes de continuar con la aplicación de ésta.

| Paso | Descripción |
|---|---|
| 80. | Inicie sesión en un servidor con el rol Citrix Controller, con una cuenta de administrador del dominio.   |

| Paso | Descripción |
|---|---|
| 81. | Ejecute la aplicación “Citrix Studio”.<br>  |
| 82. | El sistema solicitará elevación de privilegios, pulse “Sí” para continuar.<br>  |

| Paso | Descripción |
|---|---|
| 83. | Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.<br>  <br>**Nota:** Ignore cualquier advertencia que le indique que el complemento no responde. Pulse "Cancelar" para continuar.<br>  |
| 84. | Una vez en la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Directivas"**. En la ventana de bienvenida pulse "Cerrar".<br>  <br>**Nota:** Para evitar que la ventana de bienvenida aparezca cada vez que acceda al nodo "Directivas" seleccione la casilla "No volver a mostrar". |

| Paso | Descripción |
|---|---|
| 85. | Proceda en este punto a crear las directivas de seguridad de Citrix Studio que requiera su organización. Para ello, acceda a la opción “Crear directiva” en la ruta **“Citrix Studio → Directivas → Directivas → Acciones → Directivas → Crear directiva”**.<br>  |
| 86. | En la ventana que aparecerá (titulada "Crear directiva"), proceda a configurar aquellas directivas de seguridad que desee implementar en su organización para ofrecer mayor seguridad a los entornos virtualizados.<br>  |

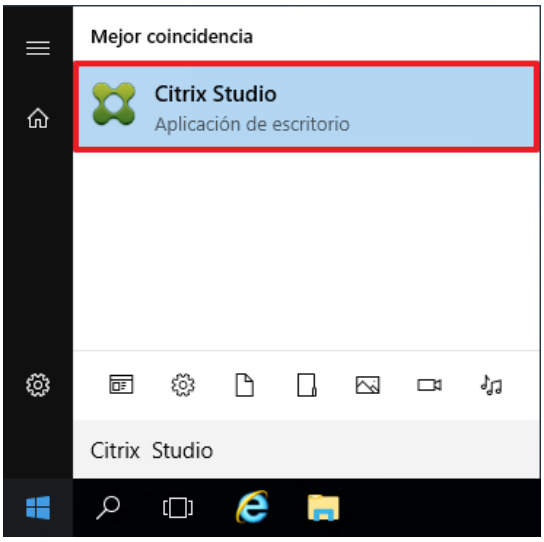
## 3. GESTIÓN DE DERECHOS DE ACCESO

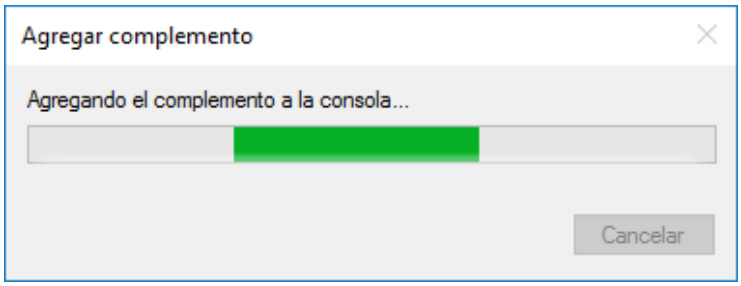
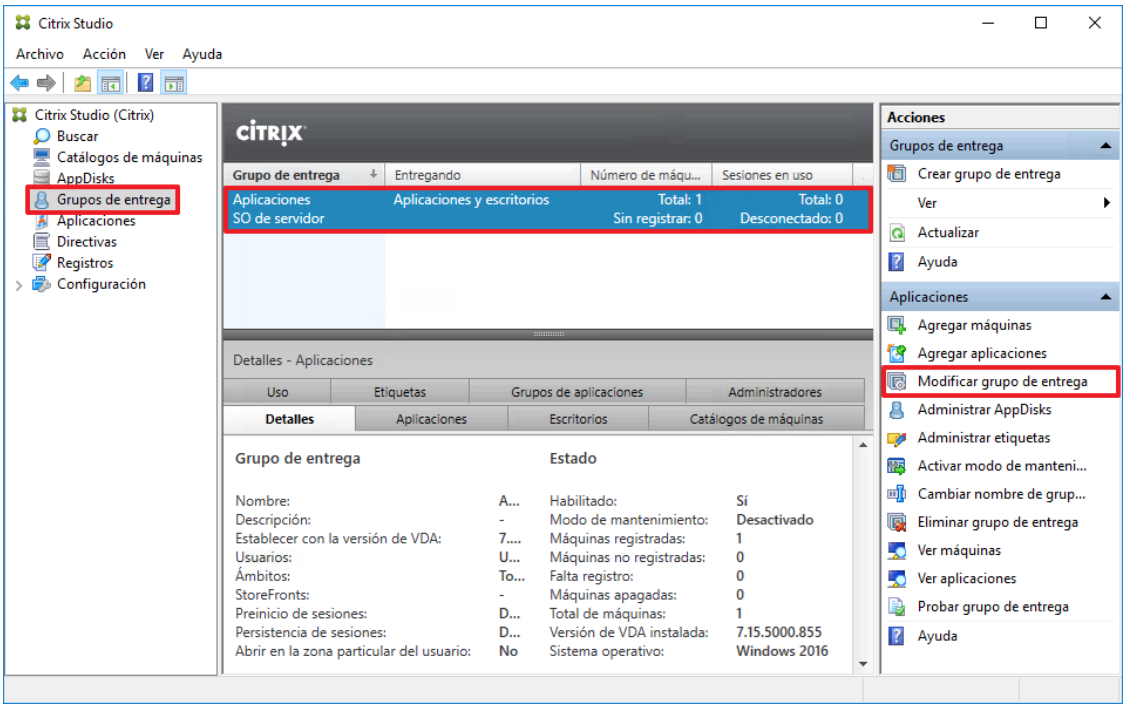
Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

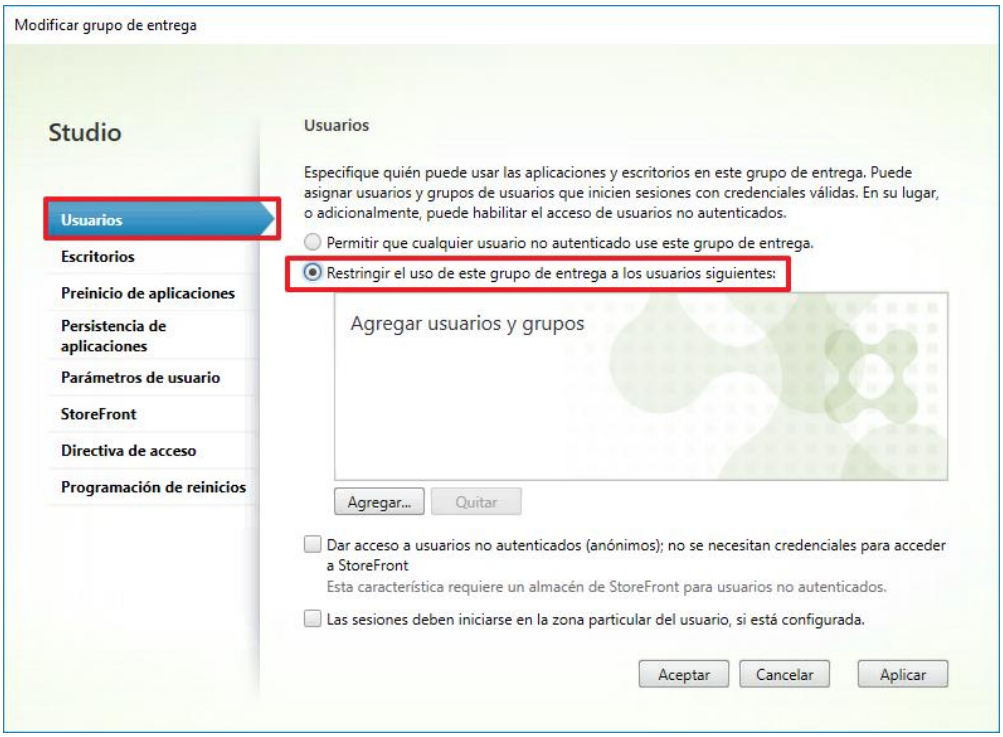
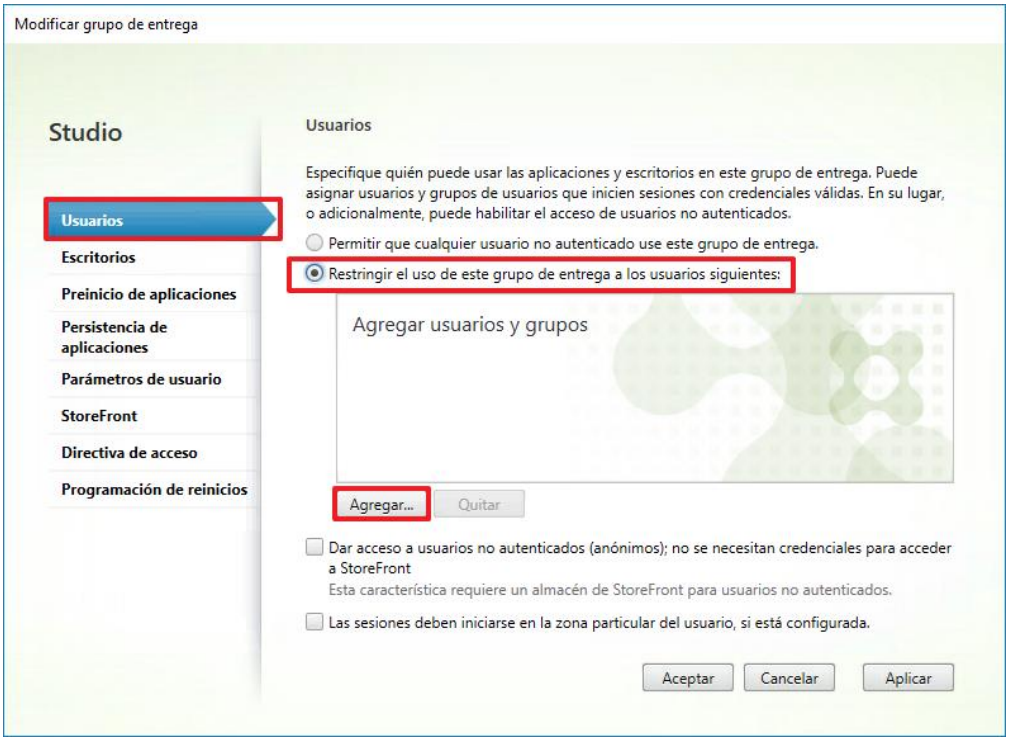
Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda acceder a recursos que no son requeridos para las funciones que desempeña.

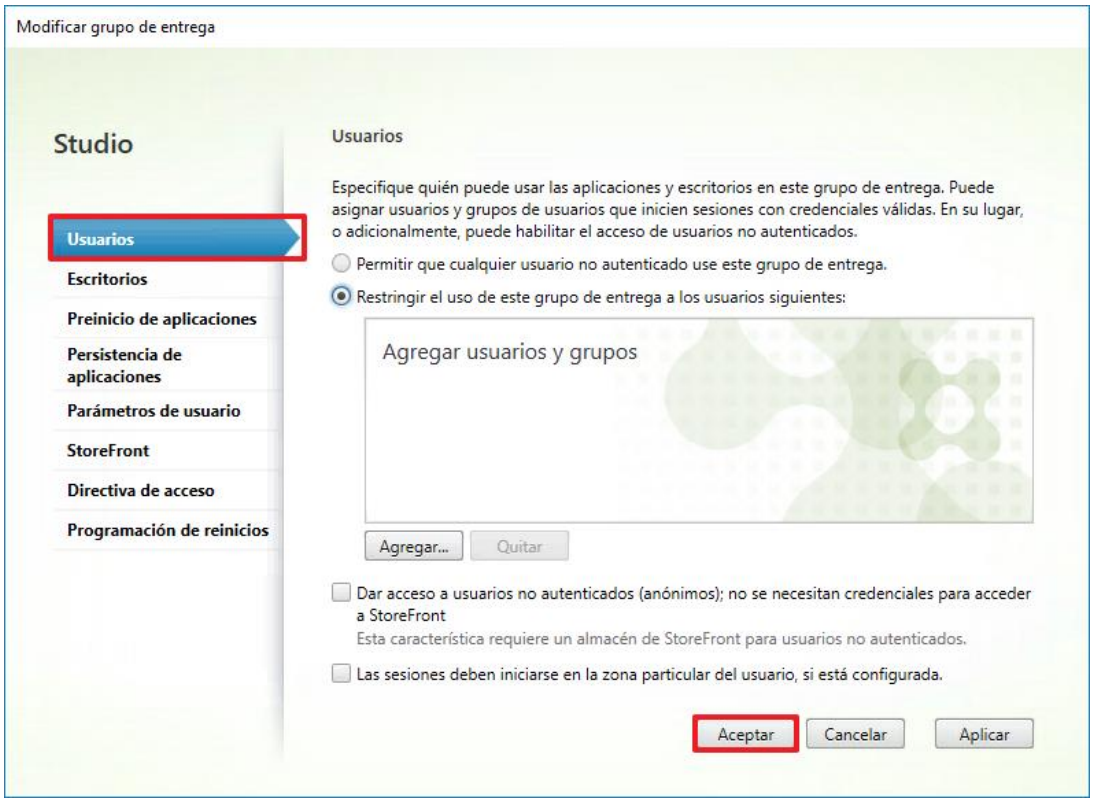
Para tal fin y de acuerdo con el Esquema Nacional de Seguridad se deberán definir, los usuarios que tengan acceso a los recursos de la infraestructura.

Esta configuración será de aplicación en el servidor con el rol Citrix Controller mediante la consola de administración Citrix Studio. Se limitarán, mediante gestión de derechos de acceso, los usuarios con acceso a los diferentes grupos de entrega de la infraestructura de Citrix Virtual Apps and Desktops.

| Paso | Descripción |
|---|---|
| 87. | Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 88. | Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.<br>  <br>**Nota:** El sistema solicitará elevación de privilegios. |

| Paso | Descripción |
|---|---|
| 89. | Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.<br>  |
| 90. | Diríjase al menú de configuración **"Citrix Studio → Grupos de entrega → [Su grupo de entrega]"** y pulse sobre "Modificar grupo de entrega" para modificar los parámetros de su grupo de entrega.<br>  |

| Paso | Descripción |
|---|---|
| 91. | Para el cumplimiento del ENS en su categoría básica, deberá impedir el uso de los recursos a usuarios no autenticados. Para ello, en la ventana "Modificar grupo de entrega", sitúese en la pestaña "Usuarios" y seleccione "Restringir el uso de este grupo de entrega a los usuarios siguientes:".<br>  |
| 92. | Deberá a continuación, mediante el botón "Agregar …", permitir el acceso al grupo de entrega de aquellos usuarios del dominio que requiera su organización.<br>  |

| Paso | Descripción |
|---|---|
| 93. | Pulse “Aceptar” para guardar los cambios realizados en el grupo de entrega.  |



## ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA PUBLICACIÓN DE APLICACIONES Y ESCRITORIOS CON CITRIX VIRTUAL APPS AND DESKTOPS

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los equipos con implementación de seguridad de categoría básica.

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 tanto en el servidor con el rol Citrix Controller como en los equipos con el rol Citrix Virtual Delivery Agent.

**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 EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

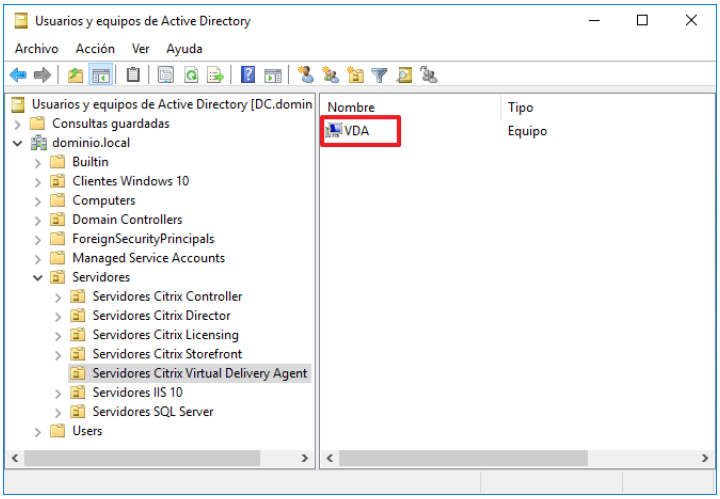
# 1. CONTROLADOR DE DOMINIO

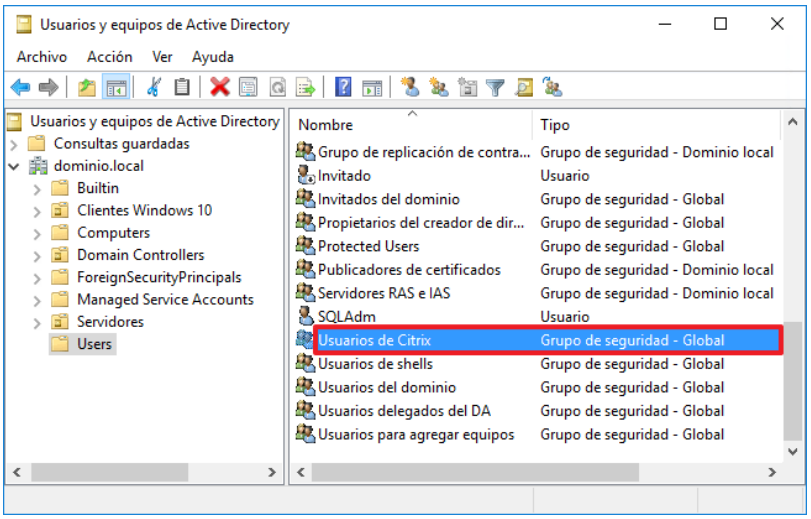
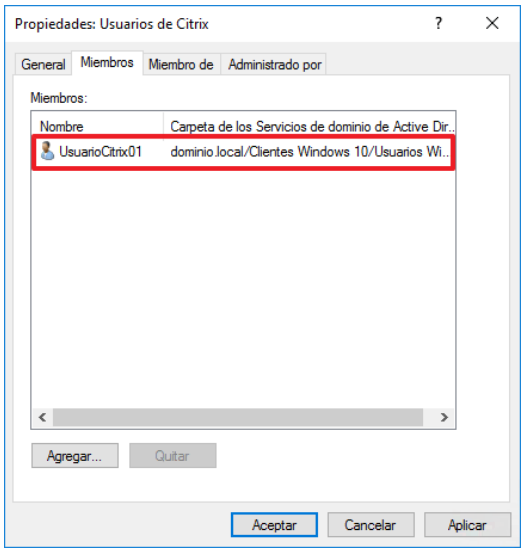
Los siguientes pasos determinan el procedimiento para verificar la configuración del dominio en el que se despliega el sistema de virtualización.

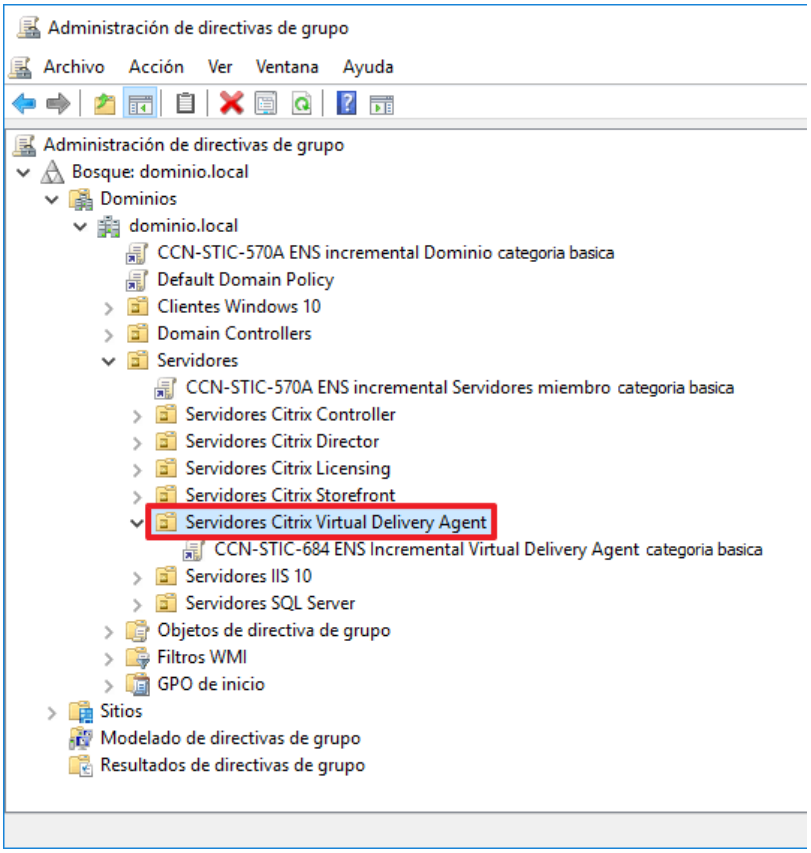
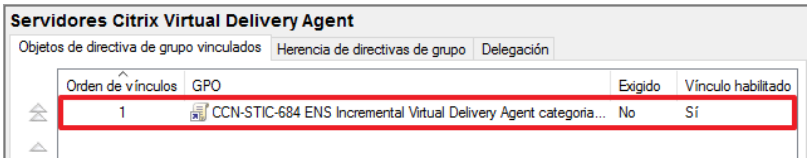
Las consolas y herramientas que se utilizarán son las siguientes:

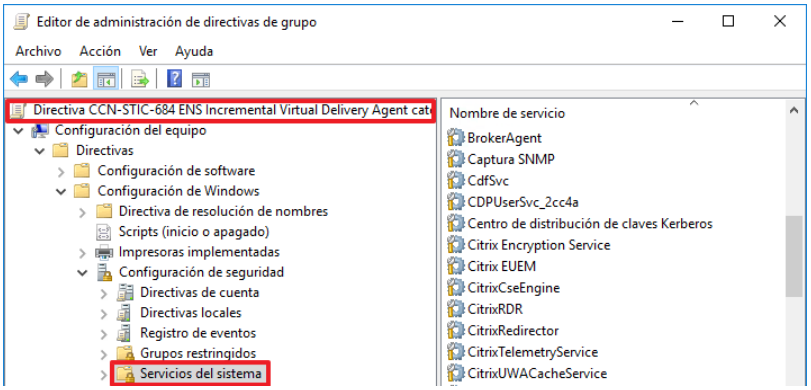
a) Usuarios y equipos de Active Directory (dsa.msc).

b) 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 equipos. | | Ejecute la herramienta "Usuarios y equipos de Active Directory" desde:<br>"**Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**".<br>El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio. |
| 3. La unidad organizativa "Servidores Citrix Virtual Delivery Agent" debe albergar todos los equipos con el rol Virtual Delivery Agent. | | En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Virtual Delivery Agent" En ella, deberá aparecer al menos un equipo.<br>  <br>**Nota:** El nombre del equipo de ejemplo es "VDA", en su caso debe figurar el nombre de su equipo. |

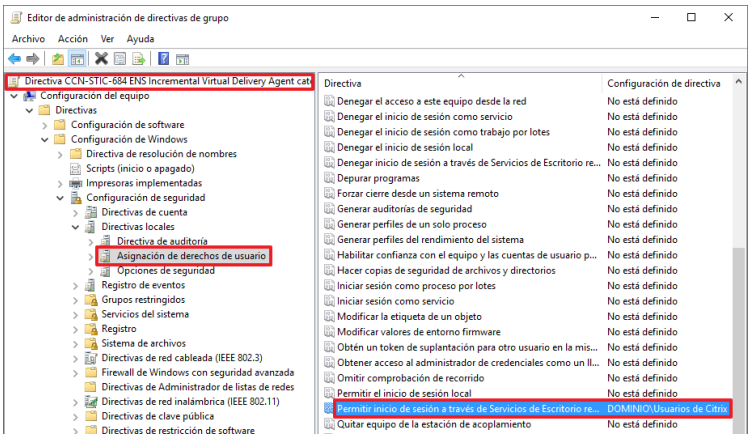
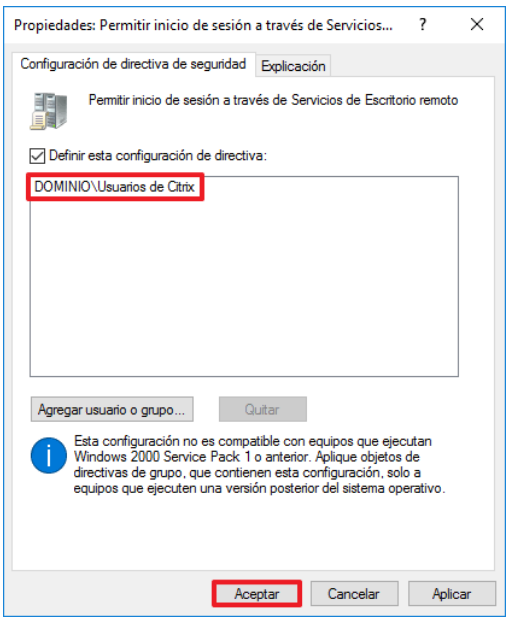
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 4. Verifique que está creado el grupo de seguridad “Usuarios de Citrix”. | | En la consola “Usuarios y equipos de Active Directory”, localice la unidad organizativa “Users” en ella, deberá aparecer el grupo de seguridad “Usuarios de Citrix”.   |
| 5. Compruebe que el grupo de seguridad “Usuarios de Citrix” aloja sus respectivos usuarios. | | Compruebe que en la pestaña “Miembros” de las propiedades del grupo de seguridad “Usuarios de Citrix” se encuentran aquellos usuarios que harán uso de la infraestructura.   |

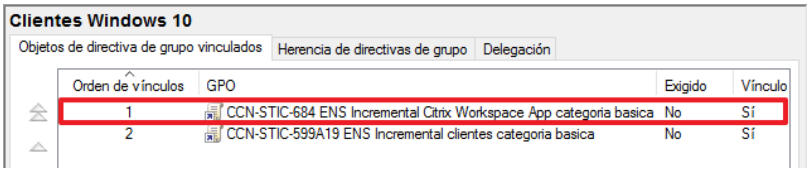
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 6. Verifique que están creadas las directivas de configuración de Citrix Virtual Delivery Agent. | | Ejecute la herramienta "Administración de directivas de grupo" desde: **"Menú inicio → Herramientas administrativas → Administración de directivas 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 Citrix Virtual Delivery Agent", situada en **"Bosque [Su bosque] → Dominios → [Su dominio] → Servidores → Servidores Citrix Virtual Delivery Agent"**.   |
| 7. Verifique las políticas aplicadas a "Servidores Citrix Virtual Delivery Agent". | | Revise que la unidad organizativa "Servidores Citrix Virtual Delivery Agent", como mínimo, tiene aplicada la siguiente directiva y tiene el vínculo habilitado.<br>– "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica"<br>   |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 8. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica". | | Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica" tiene los siguientes valores de servicios de sistema.<br>**"CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**.<br>  <br>**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 Audio Redirection Service | CtxAudioSrv | Automático | |
| Citrix Audio Redirection Service | CtxAudioSvc | Automático | |
| Citrix CEIP Service for Vda | CitrixVdaCeipService | Deshabilitado | |
| Citrix Desktop Service | BrokerAgent | Automático | |
| Citrix Device Redirector Service | CitrixRDR | Automático | |
| Citrix Device Redirector Service | CitrixRedirector | Automático | |
| Citrix Diagnostic Facility COM Server | CdfSvc | Automático | |
| Citrix Dynamic Virtual Channel Service | PicaDvcControllerSvc | Automático | |
| Citrix Encryption Service | Citrix Encryption Service | Automático | |
| Citrix End User Experience Monitoring Service | Citrix EUEM | Automático | |
| Citrix Group Policy Engine | CitrixCseEngine | Automático | |
| Citrix HDX HTML5 Video Redirection Service | CtxHdxWebSocketService | Automático | |
| Citrix ICA Service | PorticaService | Automático | |
| Citrix Location and Sensor Virtual Channel Service | CtxSensVcSvc | Automático | |
| Citrix Mobile Receiver Virtual Channel Service | MRVCSvc | Automático | |

| Comprobación | OK/NOK | Cómo hacerlo | | | |
|---|---|---|---|---|---|
| **Servicio (nombre largo)** | | **Servicio (nombre corto)** | | **Inicio** | **OK/NOK** |
| Citrix Multi Touch Redirection Service | | CtxMultiTouchSvc | | Automático | |
| Citrix Print Manager Service | | cpsvc | | Automático | |
| Citrix Profile Management | | CtxProfile | | Automático | |
| Citrix Pvs for VMs agent | | PvsVmAgent | | Automático | |
| Citrix Services Manager | | ServicesManager | | Automático | |
| Citrix Smart Card Certificate Propagation Service | | CtxSCardCertPropSvc | | Automático | |
| Citrix Smart Card Removal Policy Service | | CtxScardRemovalPolicySvc | | Automático | |
| Citrix Smart Card Service | | CtxSmartCardSvc | | Automático | |
| Citrix Stack Control Service | | StackControlService | | Automático | |
| Citrix Telemetry Service | | CitrixTelemetryService | | Deshabilitado | |
| Citrix UWA Cache Service | | CitrixUWACacheService | | Automático | |
| Cola de Impresión | | Spooler | | Automático | |
| Estación de trabajo | | LanmanWorkstation | | Automático | |
| Iniciador de procesos de servidor DCOM | | DcomLaunch | | Automático | |
| Llamada a procedimiento remoto (RPC) | | RpcSs | | Automático | |
| Servicio Citrix HDX MediaStream para Flash | | CtxFlashSvc | | Automático | |
| Servicio Informe de errores de Windows | | WerSvc | | Automático | |
| Servicio Interfaz de almacenamiento en red | | nsi | | Automático | |
| Servicios de Escritorio Remoto | | TermService | | Manual | |
| Solicitante de instantaneas de volumen de Hyper-V | | vmicvss | | Manual | |
| 9. Verifique los valores de asignación de derechos de usuario de la directiva “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica”. | | Pulse botón derecho sobre el objeto de directiva de grupo “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica” y seleccione “Editar” en el menú desplegado. Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica” tiene configurados los valores de asignación de derechos de usuario. **“CCN-STIC-684 Incremental Virtual Delivery Agent categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad →Directivas locales → Asignación de derechos de usuario”**. | | | |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| | |  <br>Compruebe que la directiva “Permitir inicio de sesión a través de Servicios de Escritorio remoto” se encuentra definida y que al menos muestra el grupo “Usuarios de Citrix”.<br>  <br>Cierre el “Editor de Administración de directivas de grupo”. |
| 10. Verifique los valores de Opciones de inicio de sesión de Windows de la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica". | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-684 Incremental Virtual Delivery Agent" tiene los siguientes valores en la siguiente ubicación:<br>**“Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”** |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario.</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>11. Verifique las políticas aplicadas a “Clientes Windows 10”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Clientes Windows 10”, situada en “Bosque [Su bosque] → Dominios → [Su dominio] → Clientes Windows 10” y revise que, como mínimo, tiene aplicada la siguiente directiva, tiene el vínculo habilitado y se encuentra situada en primer lugar.<br>– “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica”<br> 
</td></tr>
<tr><td rowspan="2">12. Verifique los valores para Actualizaciones de Citrix Workspace de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica”.</td><td></td><td colspan="3">Pulse botón derecho sobre el objeto de directiva de grupo “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” y seleccione “Editar” en el menú desplegado. Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Actualizaciones de Citrix Workspace”.</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Actualizaciones de Citrix Workspace</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>13. Verifique los valores para autoservicio de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Autoservicio”.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">EnableFTU</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir a los usuarios agregar o quitar cuentas</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir/impedir que los usuarios publiquen contenido no seguro</td><td>Habilitada (Impedir)</td><td></td></tr>
<tr><td rowspan="4">14. Verifique los valores para CEIP de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → CEIP”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Configuración de CEIP</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar CEIP</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="3">15. Verifique los valores para Conformidad de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Conformidad”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Inhabilitar el envío de datos a terceros</td><td>Habilitada</td><td></td></tr>
</table>

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 16. Verifique los valores para Diagnóstico de la directiva "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica". | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica" tiene los siguientes valores en la siguiente ubicación: **"Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria basica → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Diagnóstico"**. |

| Directiva | Valor | OK/NOK |
|---|---|---|
| Seguimiento permanente | Habilitada | |

## 2. CITRIX CONTROLLER

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el servidor con el rol Citrix Controller de la infraestructura.

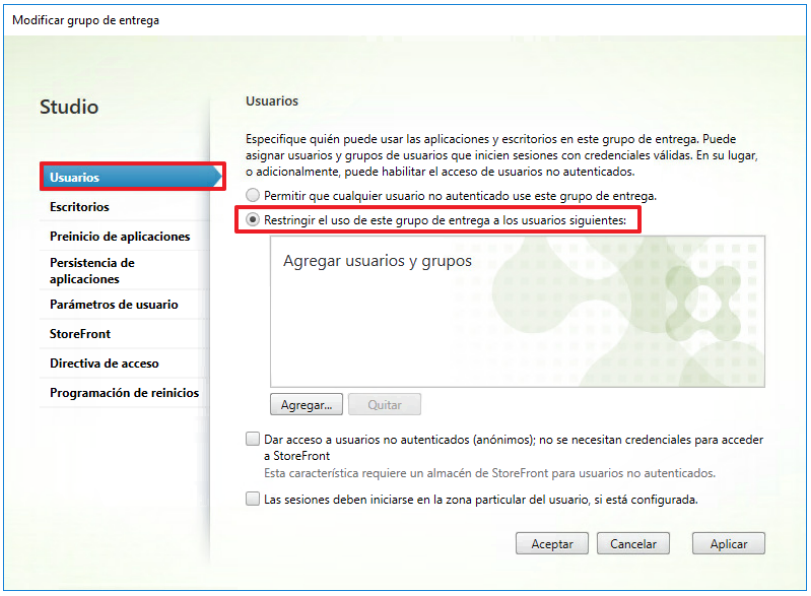
Las consolas y herramientas que se utilizarán son las siguientes:

a) Citrix Studio.

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

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

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 17. Inicie sesión en un servidor con el rol Citrix Controller | | Inicie sesión en un servidor con el rol Citrix Controller, con una cuenta de administrador del dominio. |
| 18. Verifique que están creadas las directivas de seguridad de Citrix Studio. | | Ejecute la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Directivas"** y compruebe que se hayan creado las directivas de seguridad necesarias para su organización. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 19. Verifique los derechos de acceso a los recursos. | | Ejecute la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Grupos de entrega"** y sobre cada uno de los grupos de entrega verifique que se encuentra restringido el uso de estos. Para ello, pulse el botón derecho del ratón sobre cada uno de los grupos de entrega y seleccione "Modificar Grupo de entrega" en el menú desplegable.<br>  <br>Ina vez comprobado, pulse "Cancelar" para cerrar la ventana emergente. |

## 3. CLIENTE CON INSTALACIÓN DE VIRTUAL DELIVERY AGENT

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el equipo en el que se ha desplegado el agente Virtual Delivery Agent, y las configuraciones propias implementadas sobre este equipo.

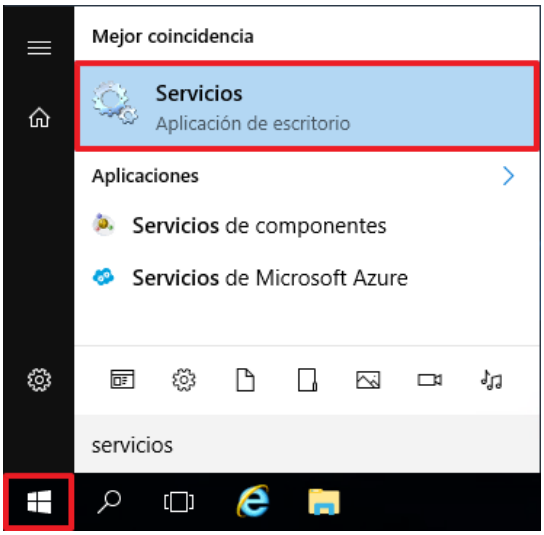
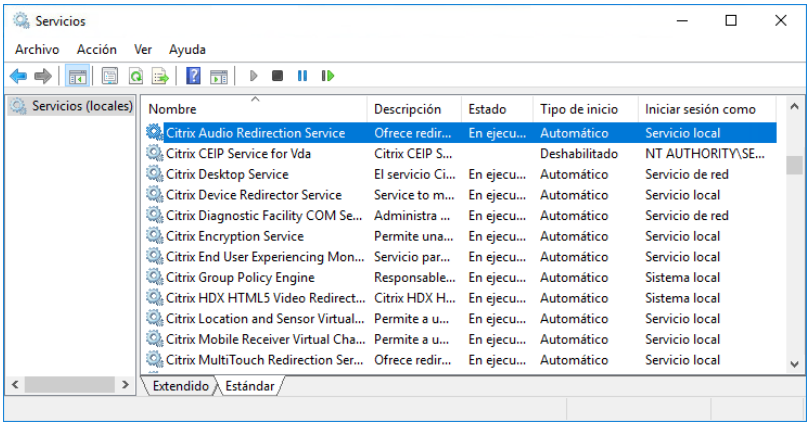
Las consolas y herramientas que se utilizarán son las siguientes:

a) Servicios (services.msc).

El siguiente procedimiento verifica la configuración del equipo con el rol Virtual Delivery Agent.

**Nota:** Deberá ejecutar los siguientes pasos de comprobación en el equipo con el rol Virtual Delivery Agent que haya sido preparado e instalado siguiendo esta guía de seguridad.

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 20. Inicie sesión en un equipo con el rol Virtual Delivery Agent. | | En un equipo con el rol Virtual Delivery Agent, inicie sesión con una cuenta que tenga privilegios de administración del dominio. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 21. Ejecución de la consola de servicios. | | Pulse sobre el botón de "Inicio" o el botón de búsqueda y teclee "Servicios". Pulse sobre el icono que aparece. El sistema solicitará elevación de privilegios. Pulse "Sí" para continuar.<br>  |
| 22. Sobre cada uno de los equipos con el rol Virtual Delivery Agent revise los servicios implementados y su estado. | | Compruebe que el valor de inicio de los servicios se ha configurado correctamente.<br>  <br>**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. Debido a esto, es posible que algunos servicios de la lista no aparezcan. Por tanto, compruebe que los que aparezcan se encuentran en el estado correcto. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|

| Servicio (nombre largo) | Servicio (nombre corto) | Inicio | OK/NOK |
|---|---|---|---|
| Asignador de extremos de RPC | RpcEptMapper | Automático | |
| Citrix Audio Redirection Service | CtxAudioSrv | Automático | |
| Citrix Audio Redirection Service | CtxAudioSvc | Automático | |
| Citrix CEIP Service for Vda | CitrixVdaCeipService | Deshabilitado | |
| Citrix Desktop Service | BrokerAgent | Automático | |
| Citrix Device Redirector Service | CitrixRDR | Automático | |
| Citrix Device Redirector Service | CitrixRedirector | Automático | |
| Citrix Diagnostic Facility COM Server | CdfSvc | Automático | |
| Citrix Dynamic Virtual Channel Service | PicaDvcControllerSvc | Automático | |
| Citrix Encryption Service | Citrix Encryption Service | Automático | |
| Citrix End User Experience Monitoring Service | Citrix EUEM | Automático | |
| Citrix Group Policy Engine | CitrixCseEngine | Automático | |
| Citrix HDX HTML5 Video Redirection Service | CtxHdxWebSocketService | Automático | |
| Citrix ICA Service | PorticaService | Automático | |
| Citrix Location and Sensor Virtual Channel Service | CtxSensVcSvc | Automático | |
| Citrix Mobile Receiver Virtual Channel Service | MRVCSvc | Automático | |
| Citrix Multi Touch Redirection Service | CtxMultiTouchSvc | Automático | |
| Citrix Print Manager Service | cpsvc | Automático | |
| Citrix Profile Management | CtxProfile | Automático | |
| Citrix Pvs for VMs agent | PvsVmAgent | Automático | |
| Citrix Services Manager | ServicesManager | Automático | |
| Citrix Smart Card Certificate Propagation Service | CtxSCardCertPropSvc | Automático | |
| Citrix Smart Card Removal Policy Service | CtxScardRemovalPolicySvc | Automático | |
| Citrix Smart Card Service | CtxSmartCardSvc | Automático | |
| Citrix Stack Control Service | StackControlService | Automático | |
| Citrix Telemetry Service | CitrixTelemetryService | Deshabilitado | |
| Citrix UWA Cache Service | CitrixUWACacheService | Automático | |
| Cola de Impresión | Spooler | Automático | |
| Estación de trabajo | LanmanWorkstation | Automático | |
| Iniciador de procesos de servidor DCOM | DcomLaunch | Automático | |
| Llamada a procedimiento remoto (RPC) | RpcSs | Automático | |
| Servicio Citrix HDX MediaStream para Flash | CtxFlashSvc | Automático | |
| Servicio Informe de errores de Windows | WerSvc | Automático | |
| Servicio Interfaz de almacenamiento en red | nsi | Automático | |
| Servicios de Escritorio Remoto | TermService | Manual | |
| Solicitante de instantaneas de volumen de Hyper-V | vmicvss | Manual | |

# ANEXO A.3. CATEGORÍA MEDIA

## ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS 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 tengan que asegurar aplicaciones y escritorios virtualizados mediante Citrix Virtual Apps and Desktops, 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 los equipos sobre los que implementarán 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.

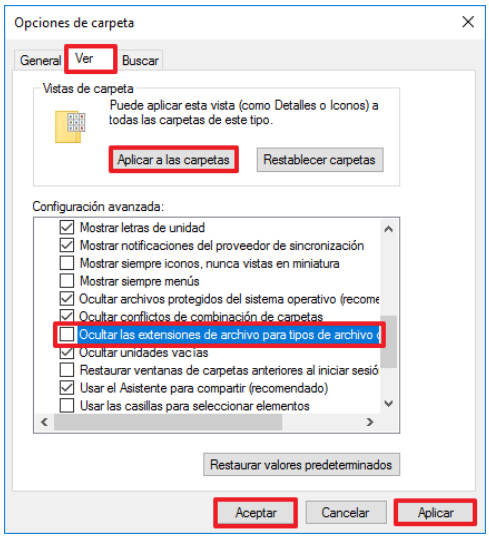
Se asume que ha realizado la implementación de las siguientes guías de seguridad sobre el dominio donde se va a aplicar el siguiente paso a paso:

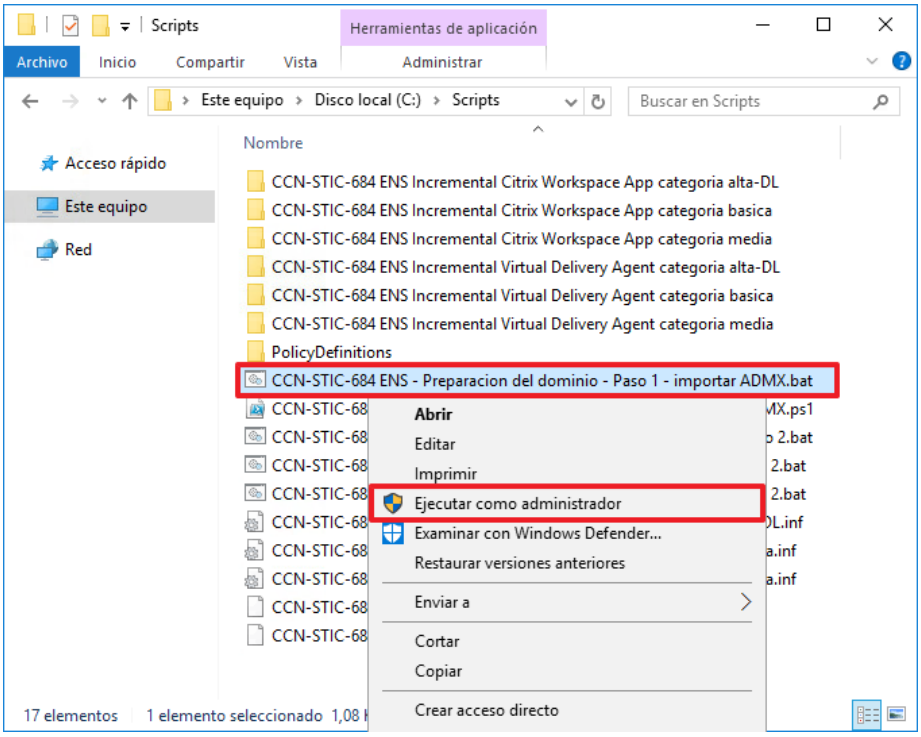
a) CCN-STIC-570A Anexo A Controlador de dominio – Categoría Media

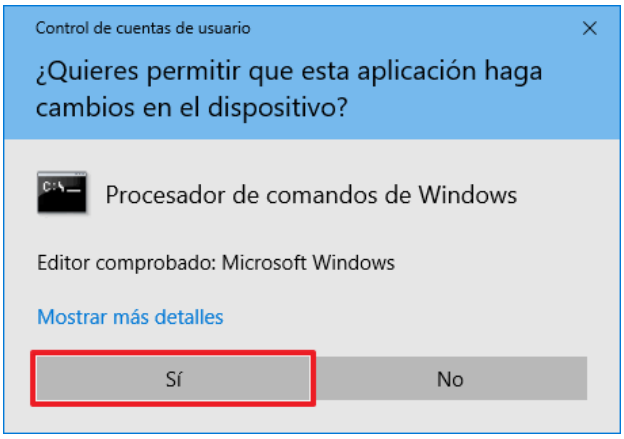
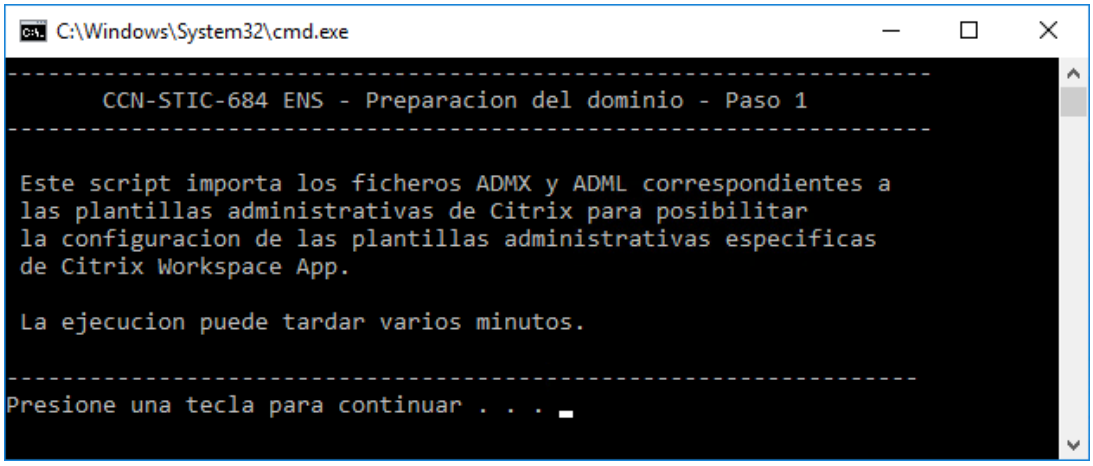
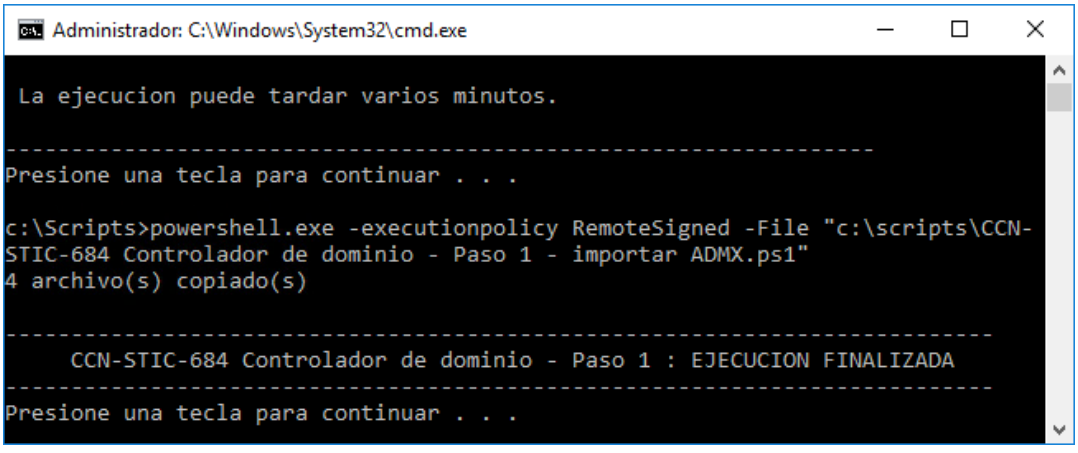
b) CCN-STIC-570A Anexo A Servidor miembro – Categoría Media

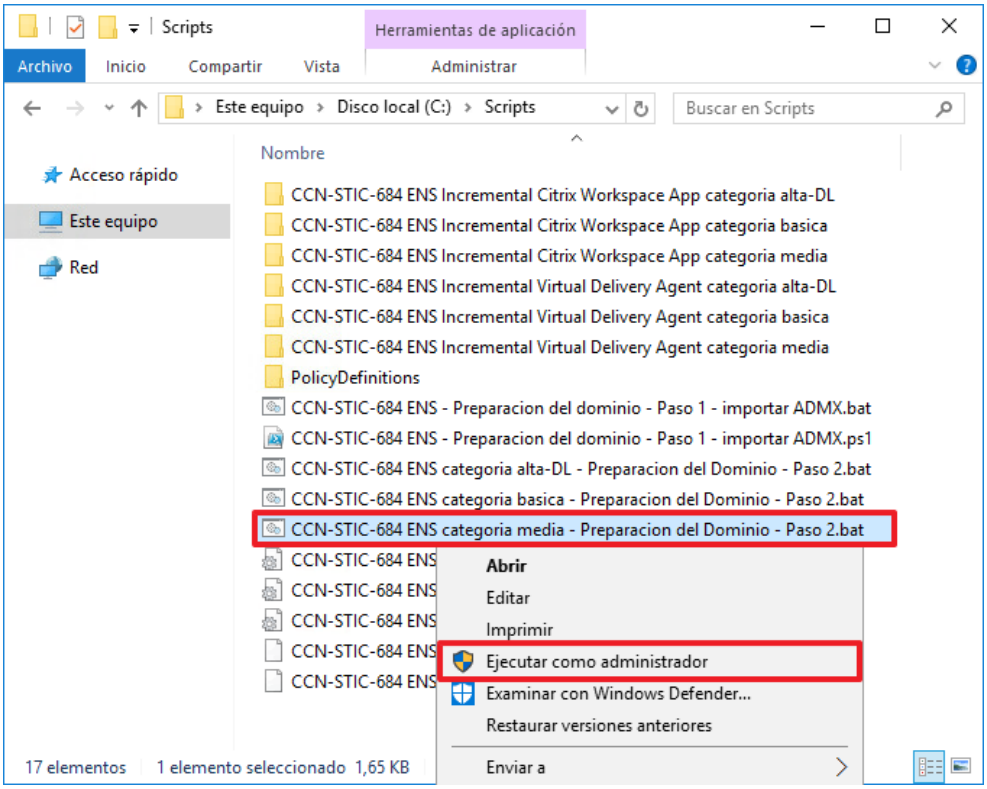
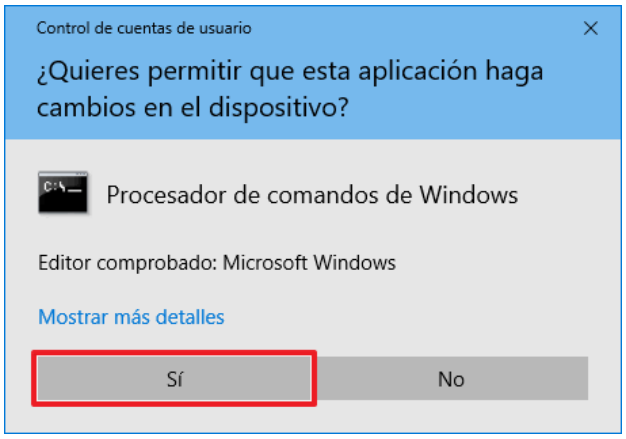
c) CCN-STIC-599A19 Anexo A – Categoría Media

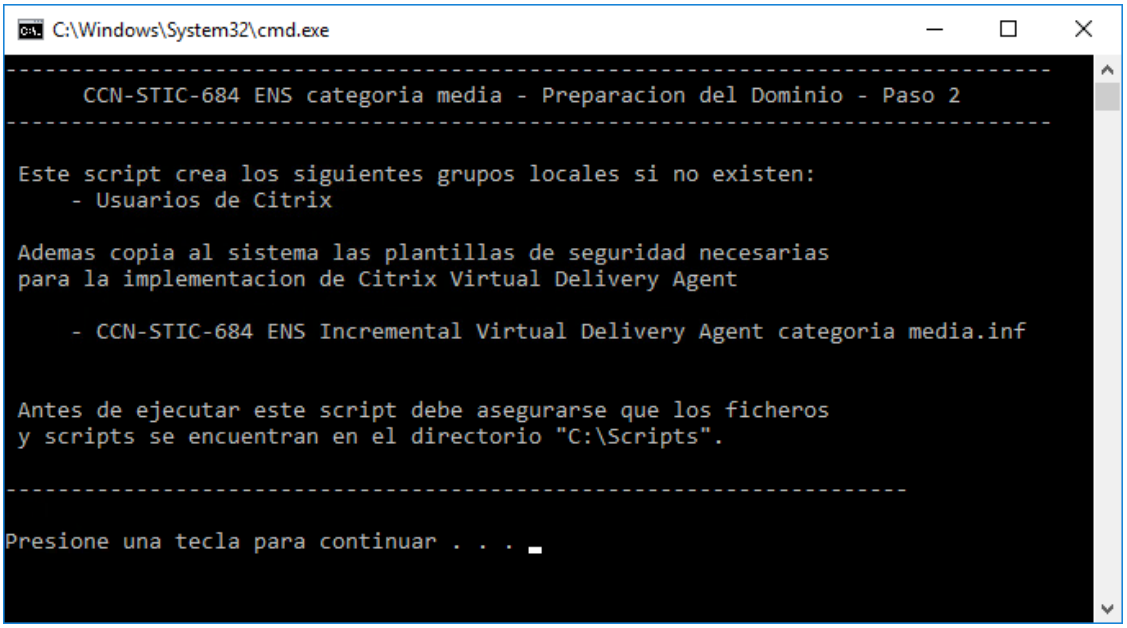
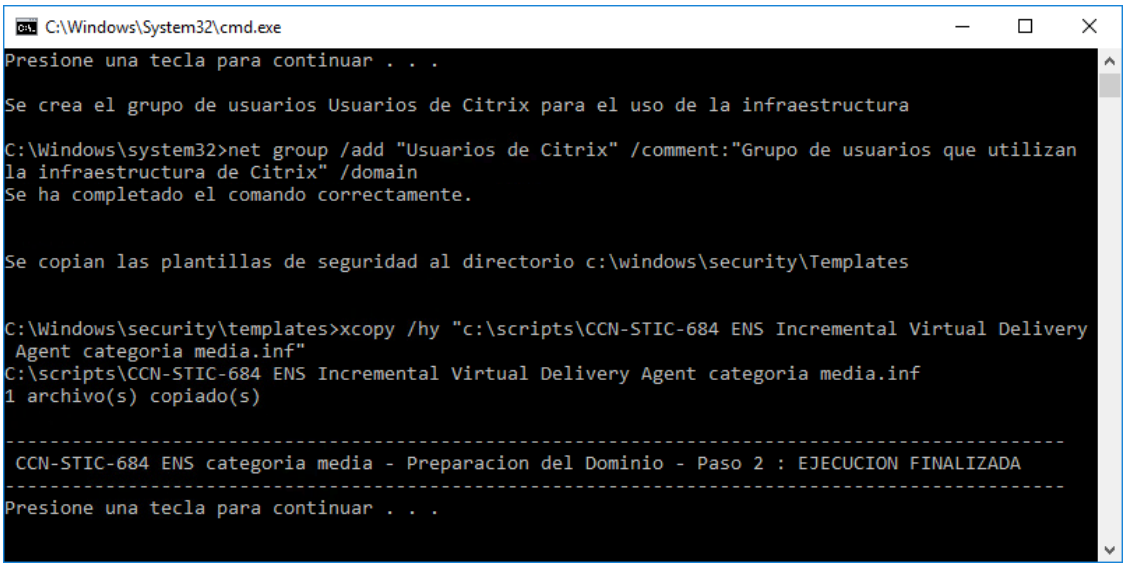
d) CCN-STIC-683 – Categoría Media

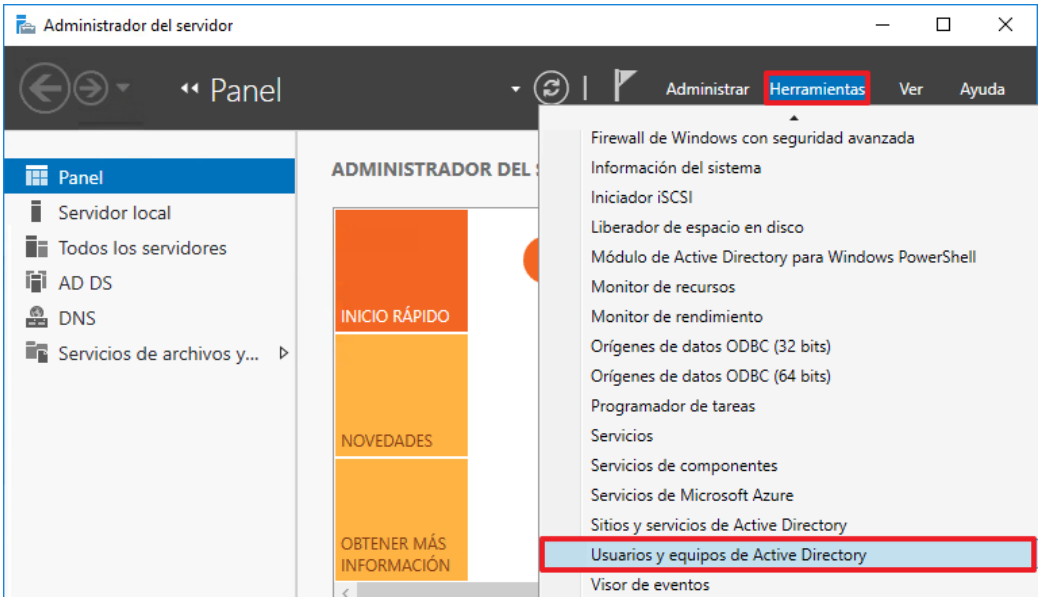
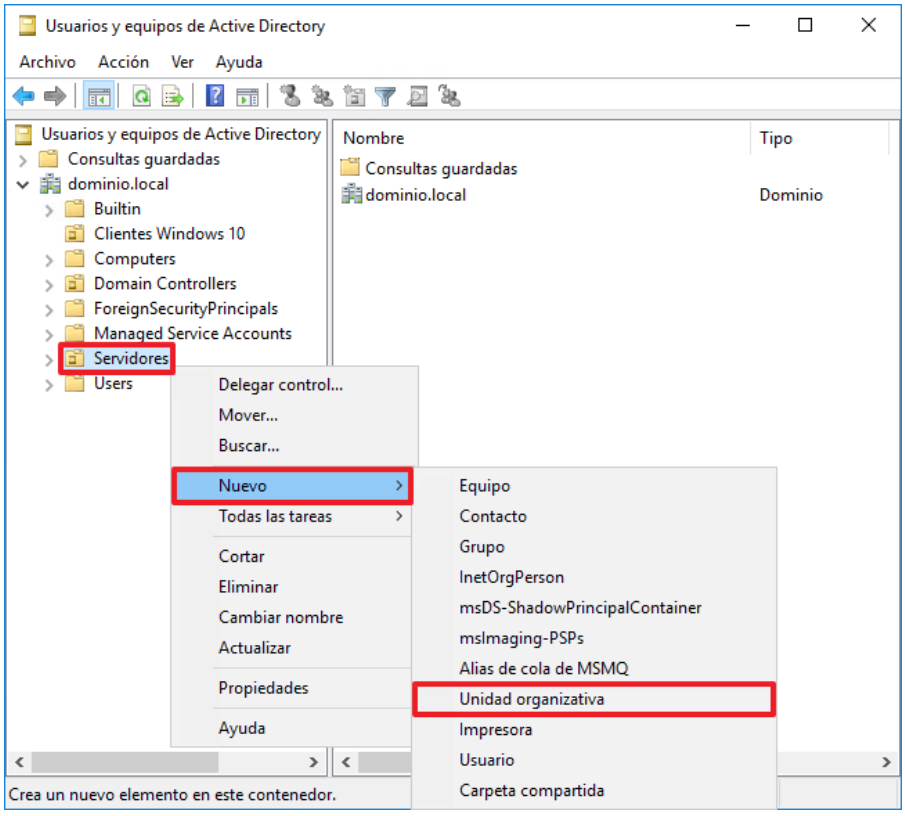
| Paso | Descripción |
|---|---|
| 1. | Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 2. | Cree el directorio “Scripts” en la unidad “C:\”.<br>**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.<br>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:<br>  |
| 5. | Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta". |

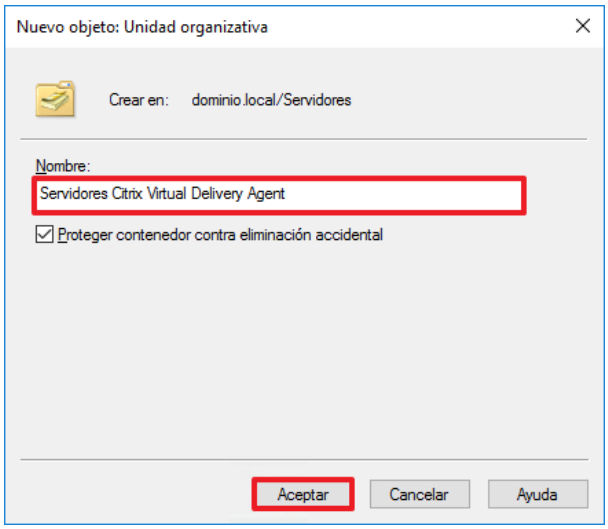
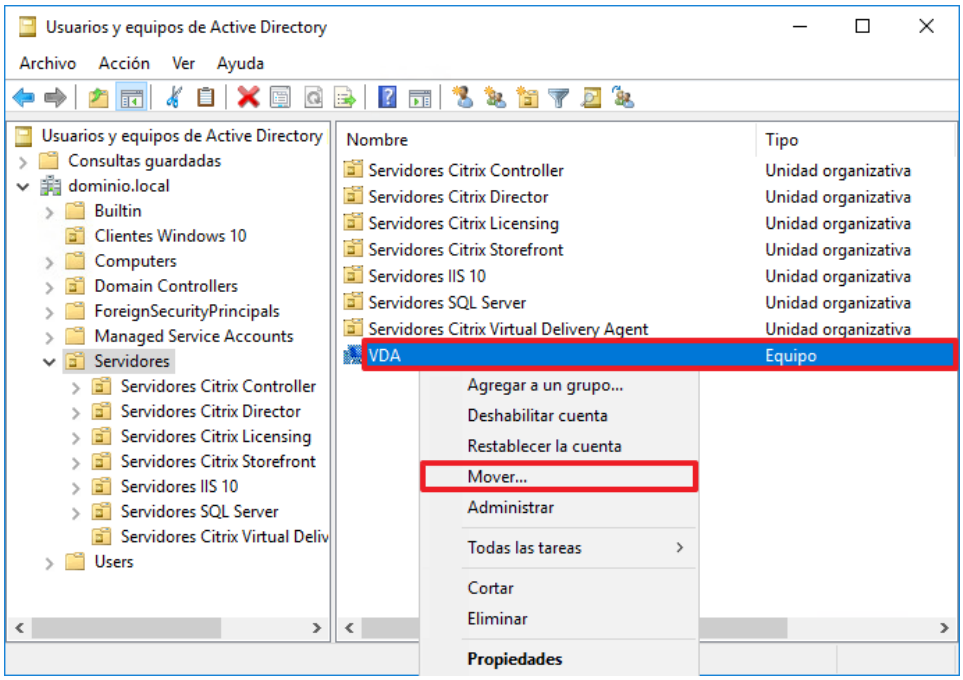
| Paso | Descripción |
|---|---|
| 6. | Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio:<br>– CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media (Directorio)<br>– CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media (Directorio)<br>– PolicyDefinitions (Directorio)<br>– CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.bat<br>– CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.ps1<br>– CCN-STIC-684 ENS categoria media - Preparacion del Dominio - Paso 2.bat<br>– CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media.inf |
| 7. | Ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.bat". Para ello, visualice la carpeta “C:\Scripts” en el explorador de Windows, marque con el botón derecho el script y seleccione la opción **"Ejecutar como administrador"** del menú contextual, como se muestra en la siguiente figura.<br>  <br>**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.<br>Si el directorio principal de Windows no se encuentra en “C:\Windows”, sustituya "C:\Windows" por la ubicación correspondiente dentro de los archivos de configuración. |

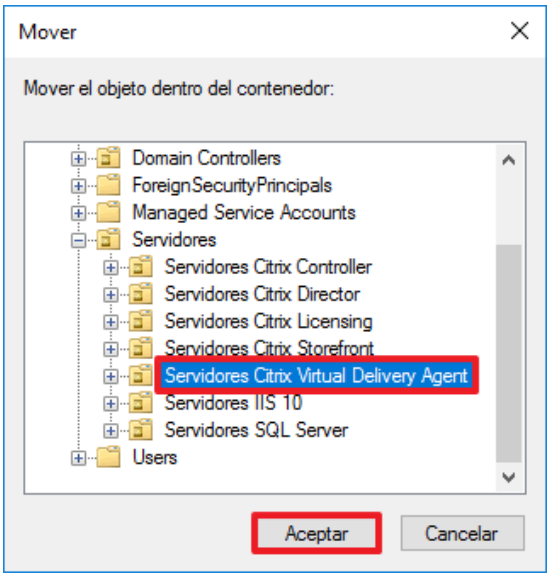
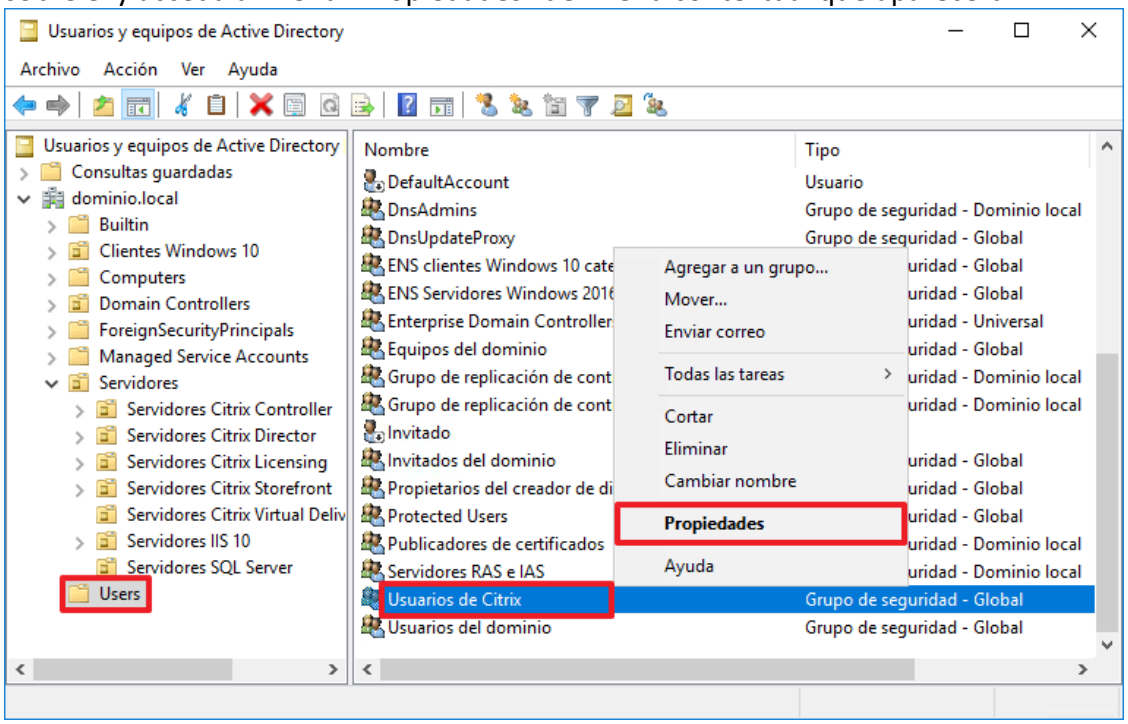
| Paso | Descripción |
|---|---|
| 8. | El sistema solicitará elevación de privilegios, pulse “Si” para continuar.<br>  |
| 9. | Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Citrix Workspace App en el controlador de dominio.<br>  |
| 10. | Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana.<br>  |

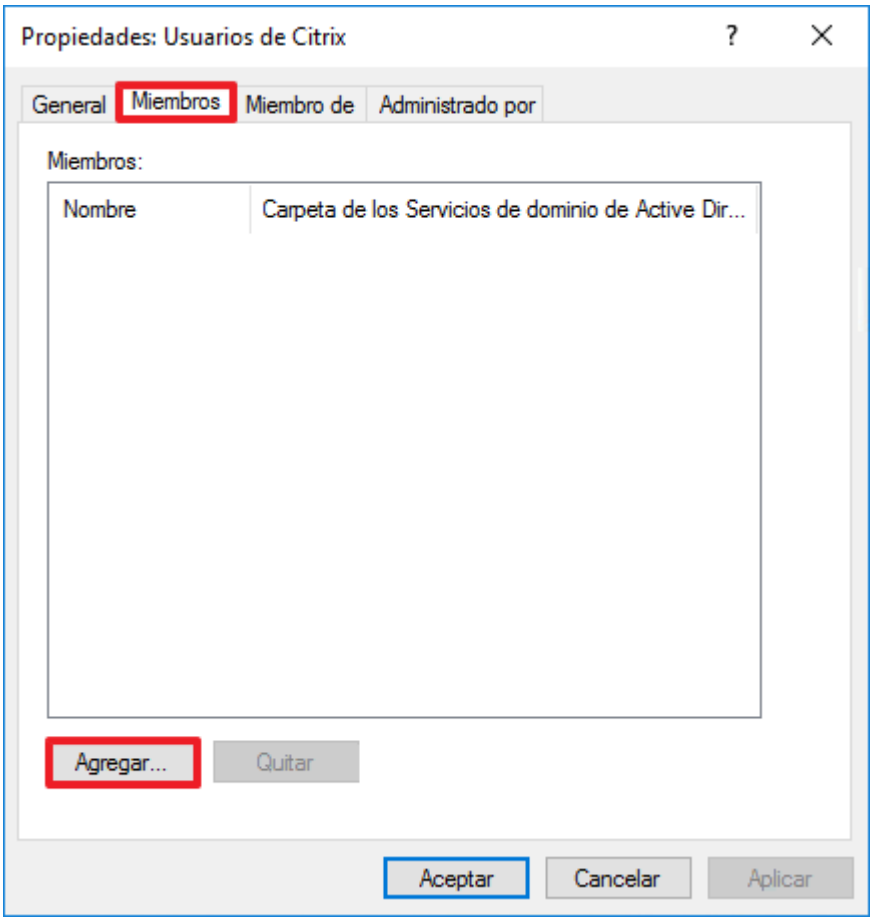
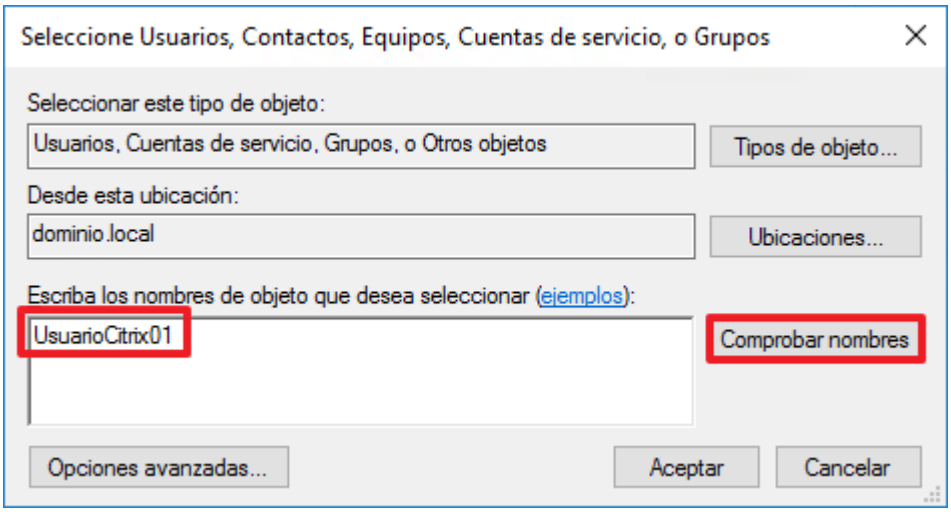
| Paso | Descripción |
|---|---|
| 11. | De igual forma, ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-684 ENS categoria media - Preparacion del Dominio - Paso 2.bat".   |
| 12. | El sistema solicitará elevación de privilegios, pulse "Si" para continuar.   |

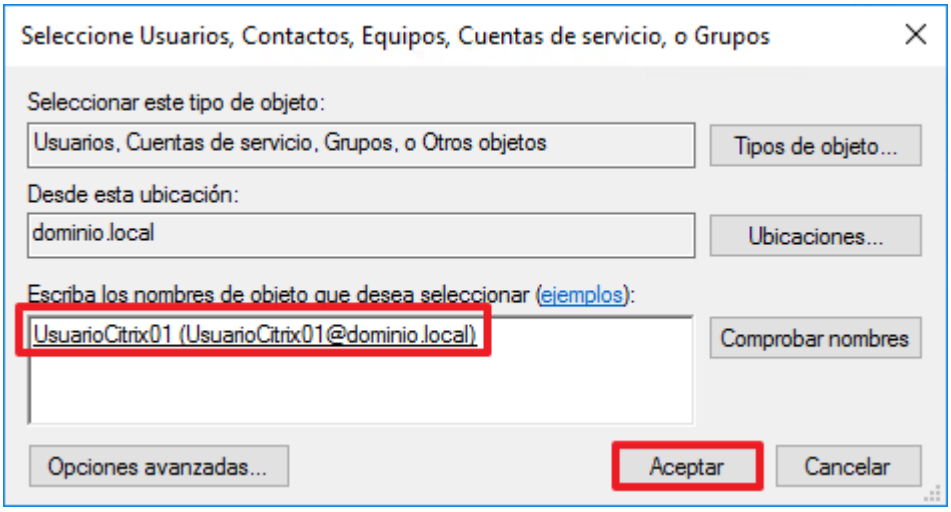
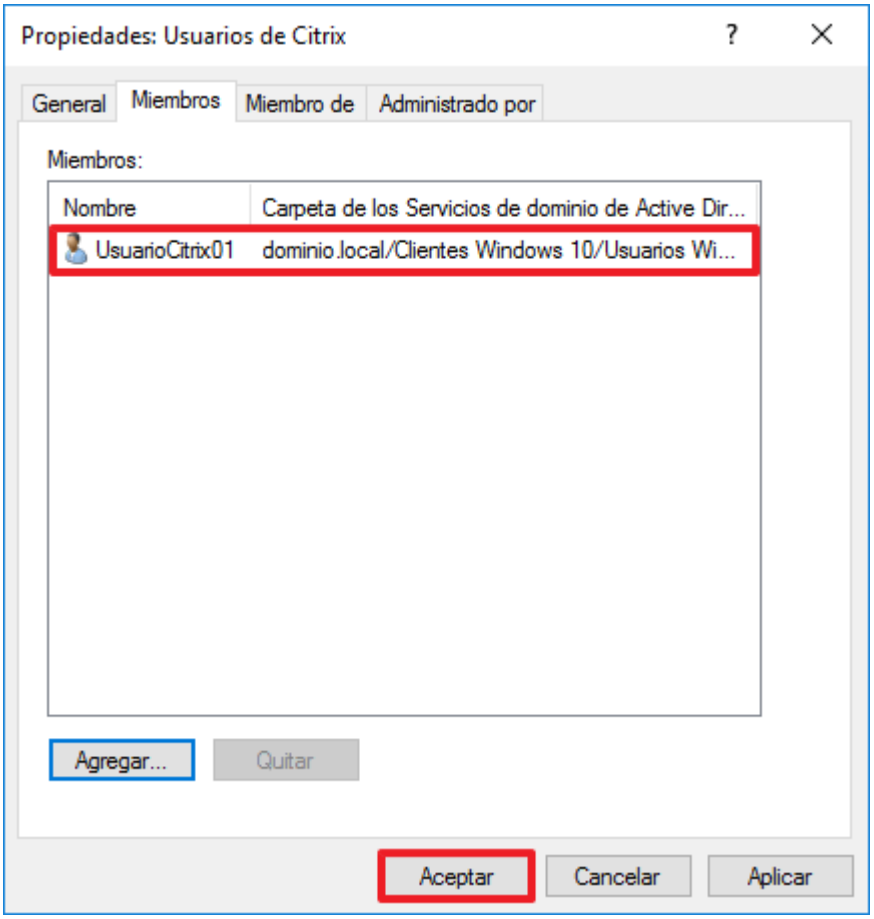
| Paso | Descripción |
|---|---|
| 13. | Se lanzará una ventana del intérprete de comandos “cmd.exe” como la mostrada en la siguiente figura.<br>Este script copia las plantillas de seguridad a la ubicación “C:\Windows\security\templates” y crea el grupo de seguridad “Usuarios de Citrix” si éste no existiese.<br>  |
| 14. | Una vez finalizado pulse una tecla para concluir la ejecución del script.<br>  |

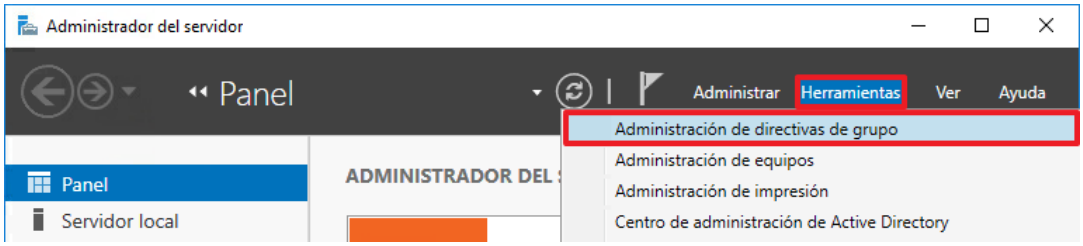
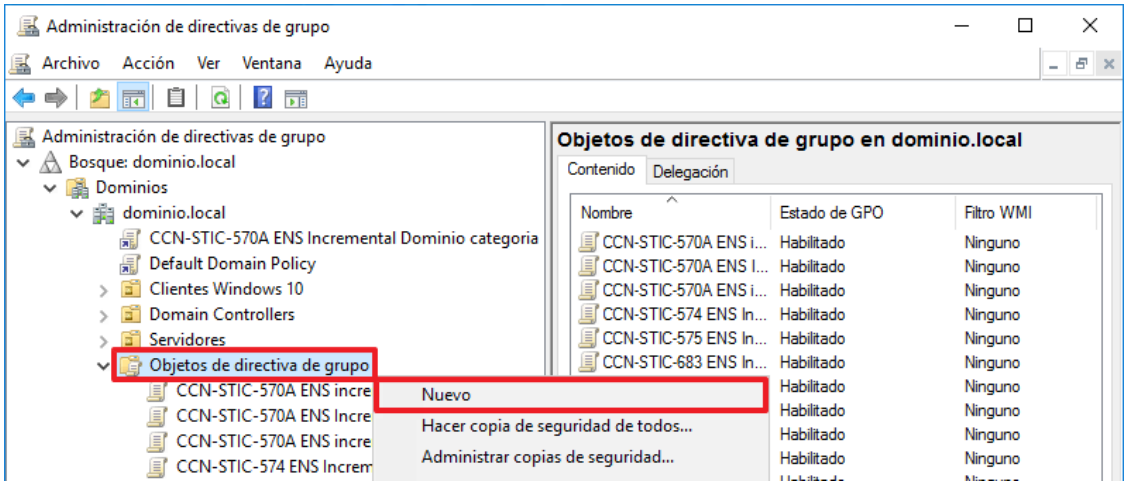
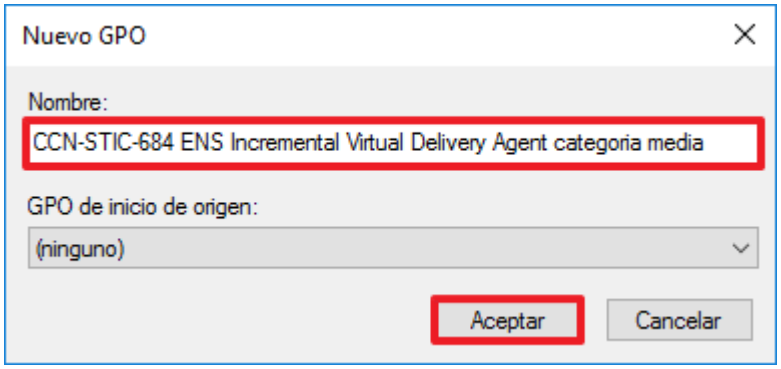
| Paso | Descripción |
|---|---|
| 15. | Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios.<br>  |
| 16. | A continuación, en la herramienta "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.<br>  |

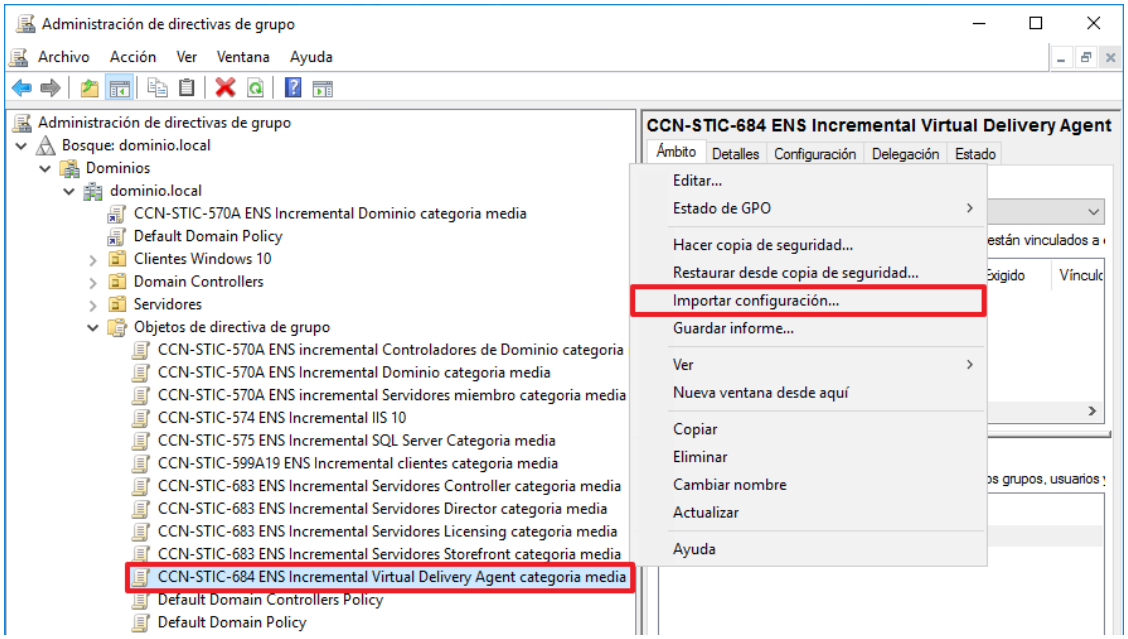
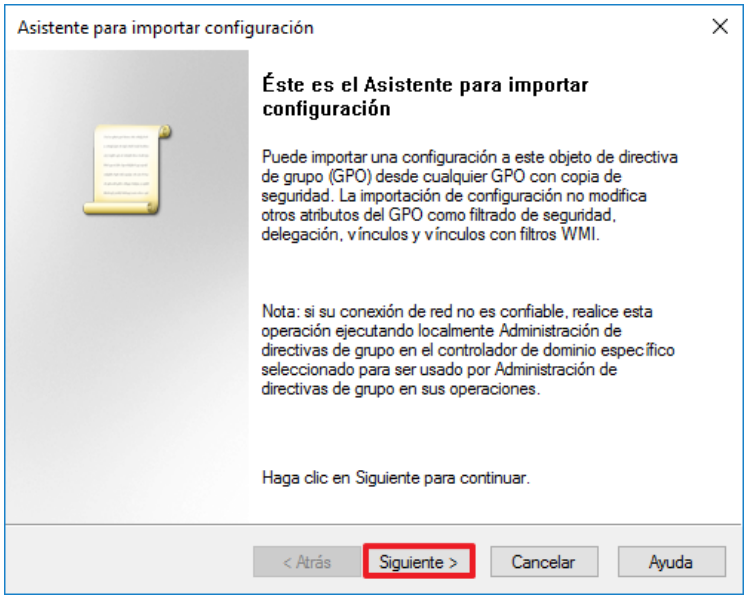
| Paso | Descripción |
|---|---|
| 17. | En la ventana resultante, introduzca como nombre de la nueva unidad organizativa “Servidores Citrix Virtual Delivery Agent” tal y como muestra en la imagen. No desmarque la opción “Proteger contenedores contra eliminación accidental”. Pulse “Aceptar” para crear el nuevo objeto.<br>  <br>**Nota:** En este punto deberá crear aquellas unidades organizativas que sean necesarias para la administración de su organización. |
| 18. | Vaya a las unidades organizativas donde se encuentren los equipos que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover…” en cada uno de ellos.<br>  <br>**Nota:** En este ejemplo se encuentra bajo la unidad organizativa “Servidores”. |

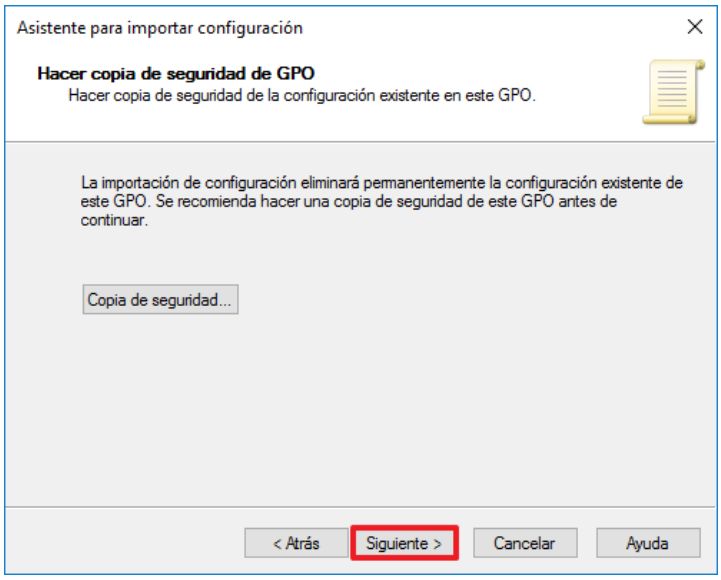
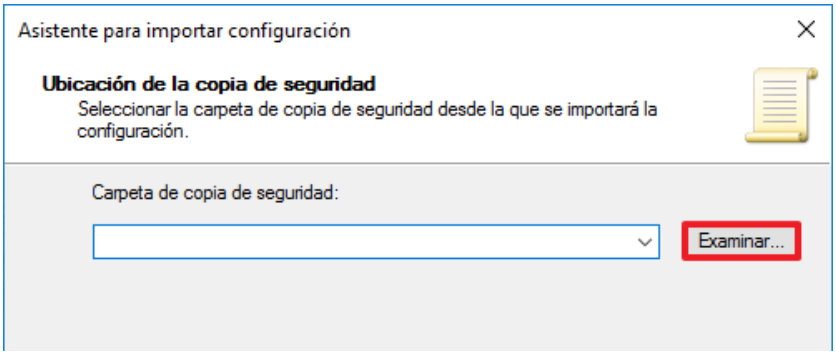
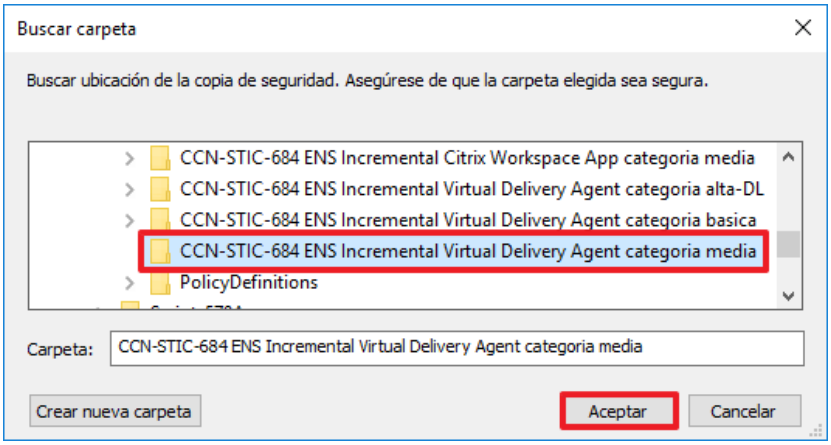
| Paso | Descripción |
|---|---|
| 19. | Seleccione la unidad organizativa “Servidores Citrix Virtual Delivery Agent” creada anteriormente y pulse “Aceptar”.<br>  |
| 20. | A continuación proceda a incluir a los usuarios que harán uso de la infraestructura de Citrix dentro del grupo de seguridad “Usuarios de Citrix”, para ello expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"** y seleccionando el grupo de seguridad “Usuarios de Citrix” haga clic derecho sobre él y acceda al menú “Propiedades” del menú contextual que aparecerá.<br>  |

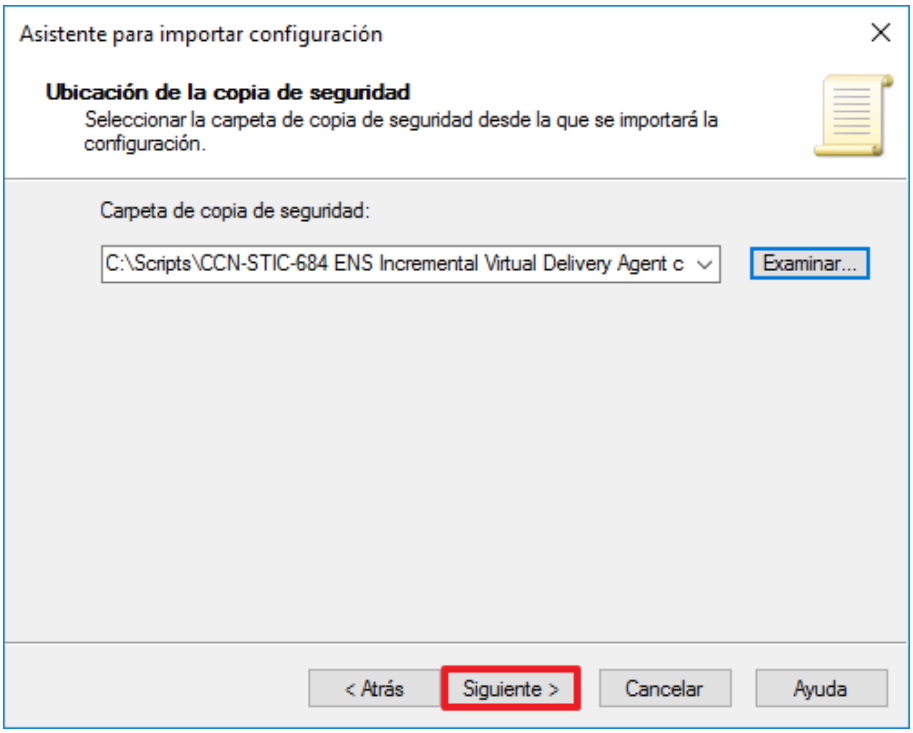
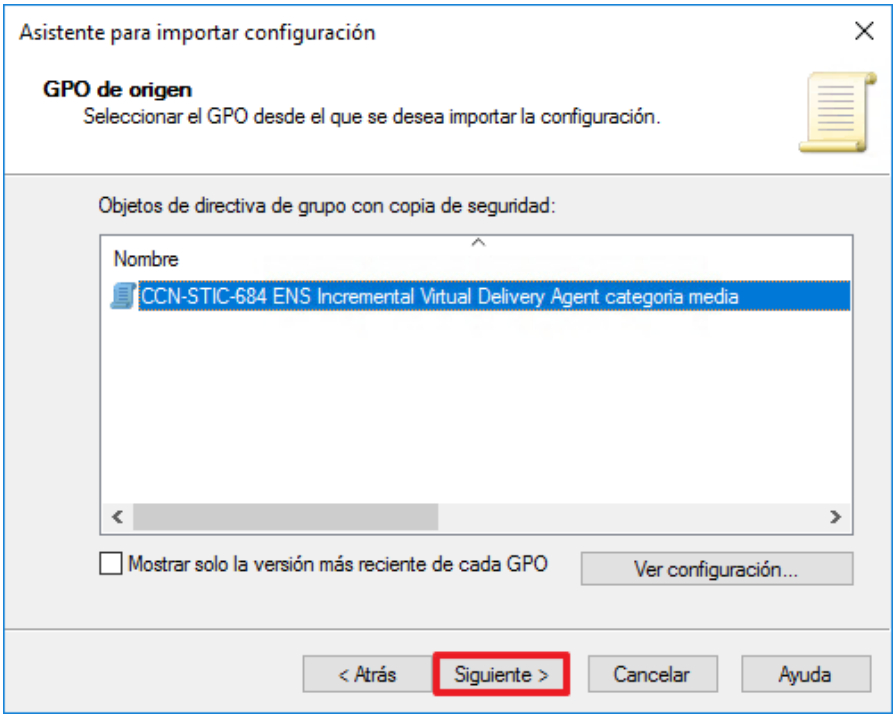
| Paso | Descripción |
|---|---|
| 21. | Dentro de las propiedades del grupo, en la pestaña “Miembros” pulse “Agregar…”.<br>  |
| 22. | Escriba el nombre del usuario que desee agregar al grupo y pulse “Comprobar nombres”.<br>  <br>**Nota:** En este ejemplo se utiliza el usuario “UsuarioCitrix01”. Deberá agregar al grupo “Usuarios de Citrix” los usuarios creados en su organización para hacer uso de los recursos entregados mediante Virtual Delivery Agent. |

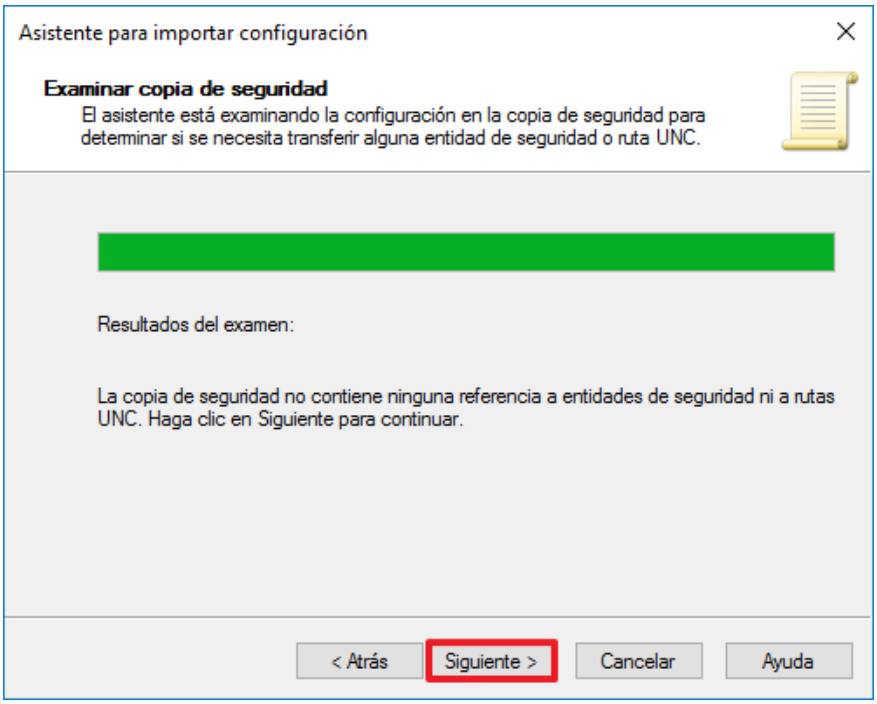
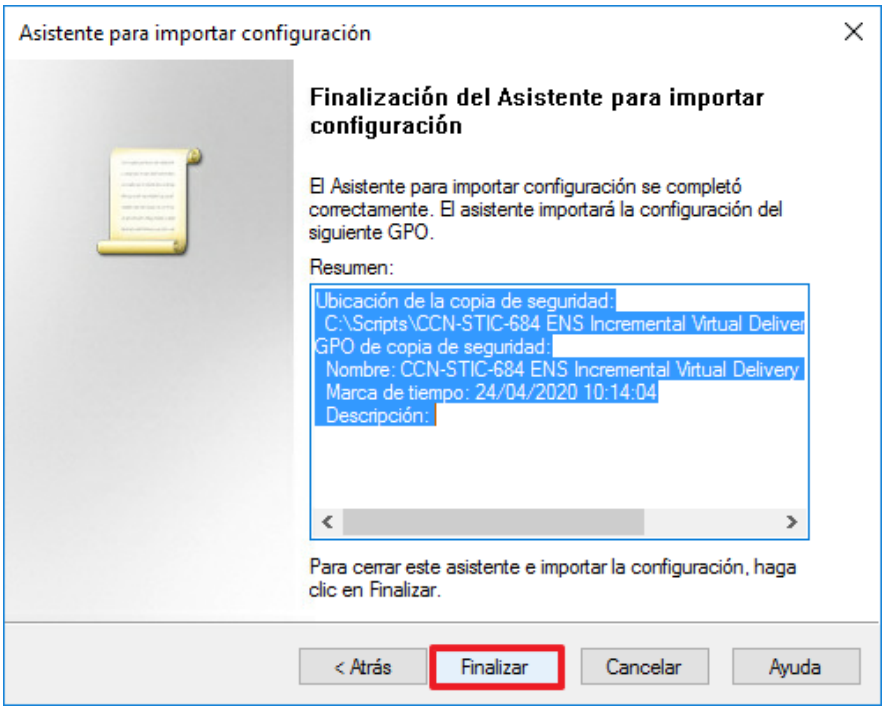
| Paso | Descripción |
|---|---|
| 23. | Compruebe que el usuario sea el correcto y pulse “Aceptar” para agregarlo y cerrar la ventana.<br>  |
| 24. | El usuario aparecerá agregado al grupo “Usuarios de Citrix” pulse “Aceptar” para guardar la configuración y cerrar la ventana. Repita estos pasos para todos aquellos usuarios que desee agregar al grupo.<br>  |
| 25. | Cierre la herramienta “Usuarios y equipos de Directorio Activo”. |

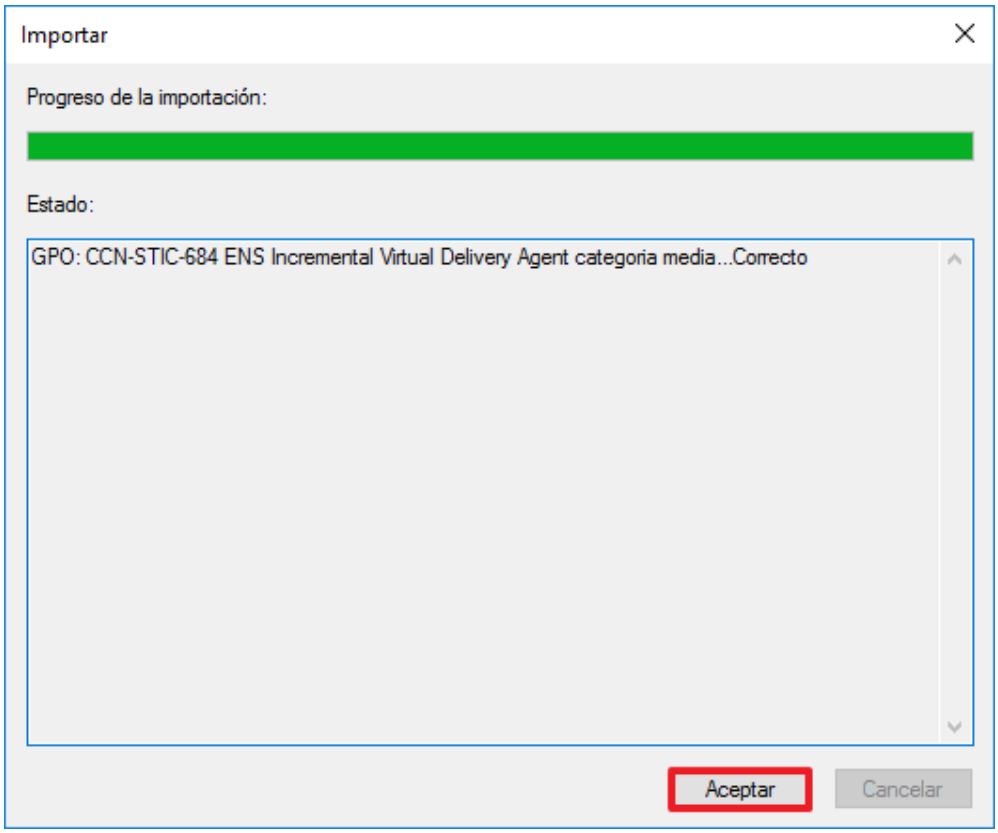
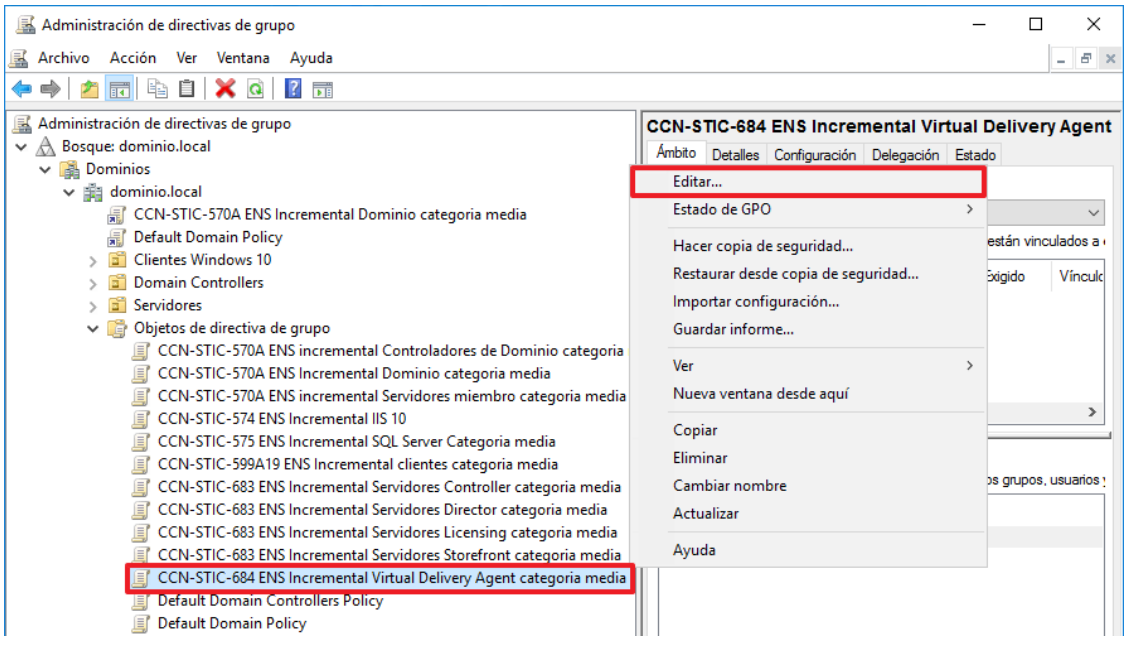
| Paso | Descripción |
|---|---|
| 26. | Utilice la herramienta "Administración de Directivas de grupo" (**Administrador del servidor → Herramientas → Administración de Directivas de grupo**). El sistema solicitará elevación de privilegios.<br>  |
| 27. | Expanda el contenedor **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>"**. A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPOs correspondientes. |
| 28. | 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.<br>  |
| 29. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media" y pulse el botón “Aceptar”.<br>  |

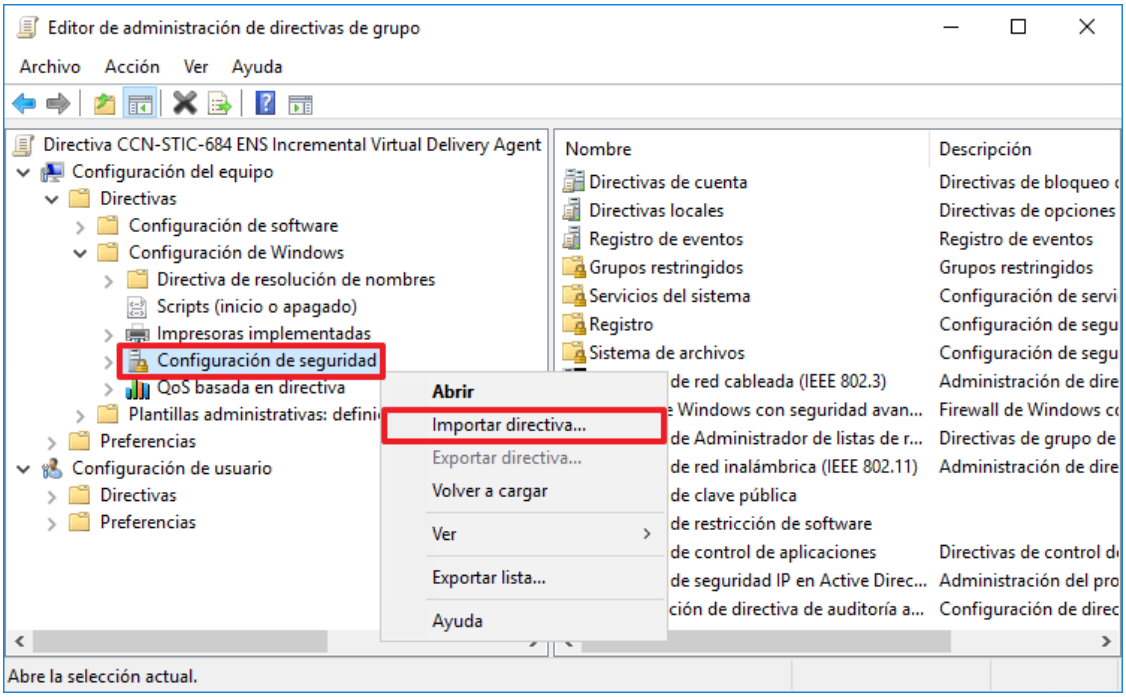
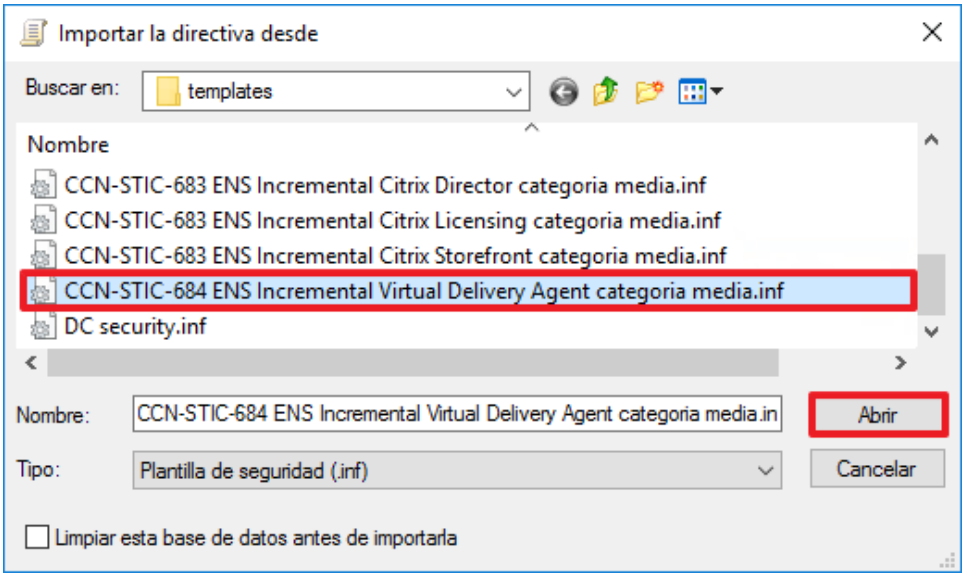
| Paso | Descripción |
|---|---|
| 30. | Seleccione el GPO recién creado, "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media", y marcando con el botón derecho en él, elija la opción "Importar configuración…" del menú contextual que aparecerá.   |
| 31. | En el asistente de importación de configuración, pulse el botón “Siguiente >”.   |

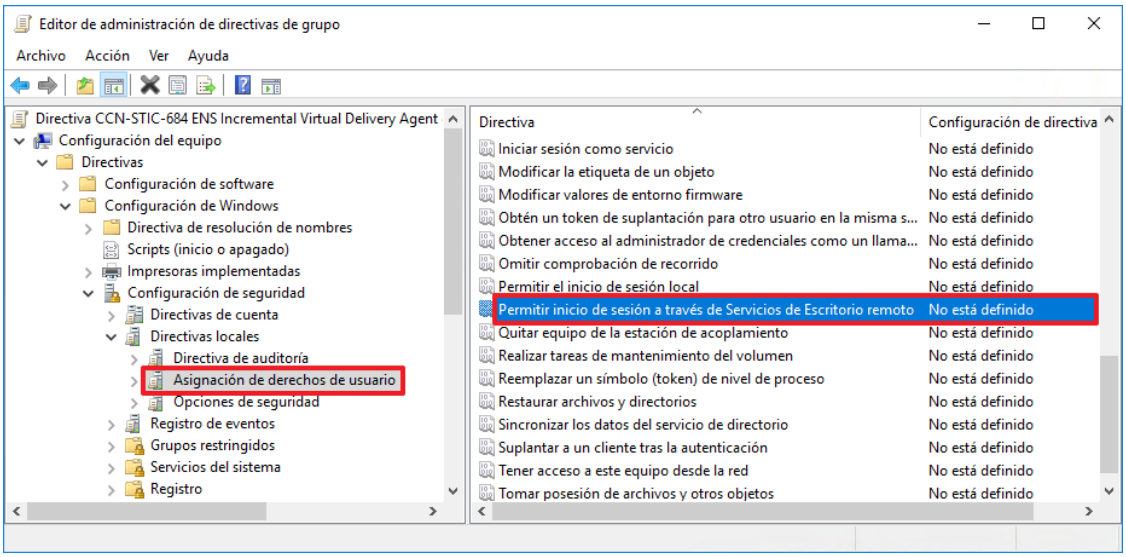
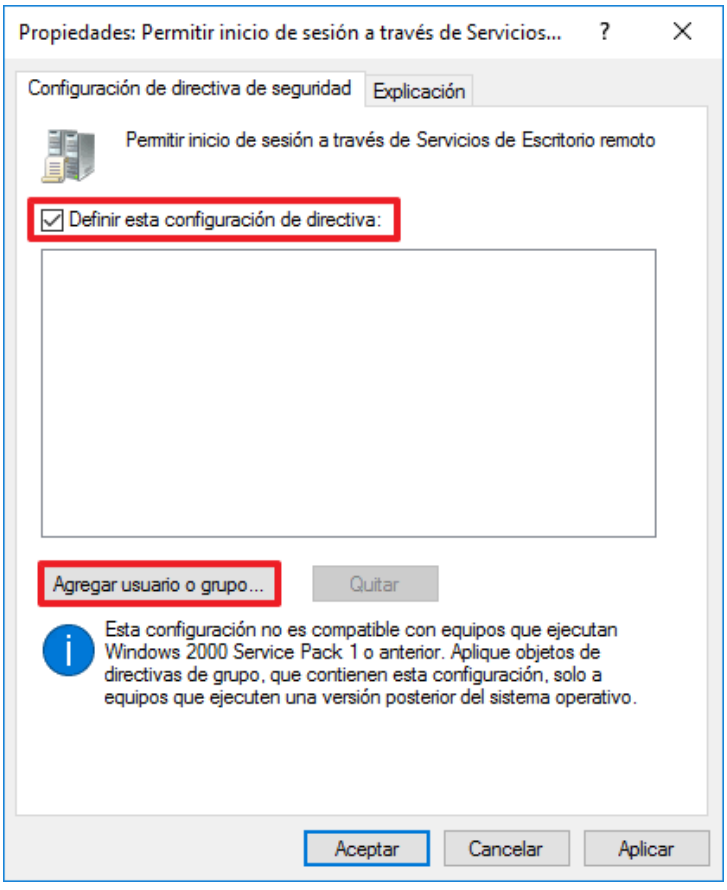
| Paso | Descripción |
|---|---|
| 32. | En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |
| 33. | Pulse el botón “Examinar...” en la ventana “Ubicación de la copia de seguridad”.<br>  |
| 34. | Seleccione la carpeta “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.<br>  |

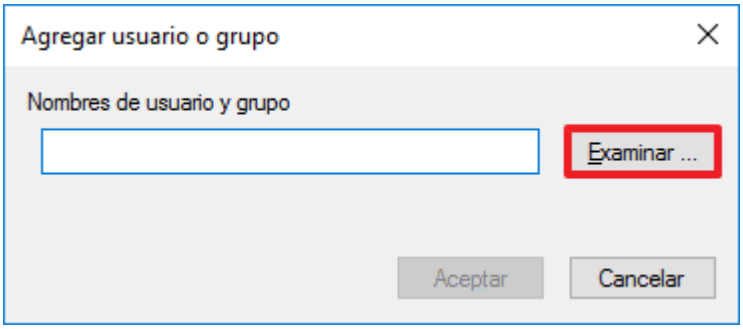
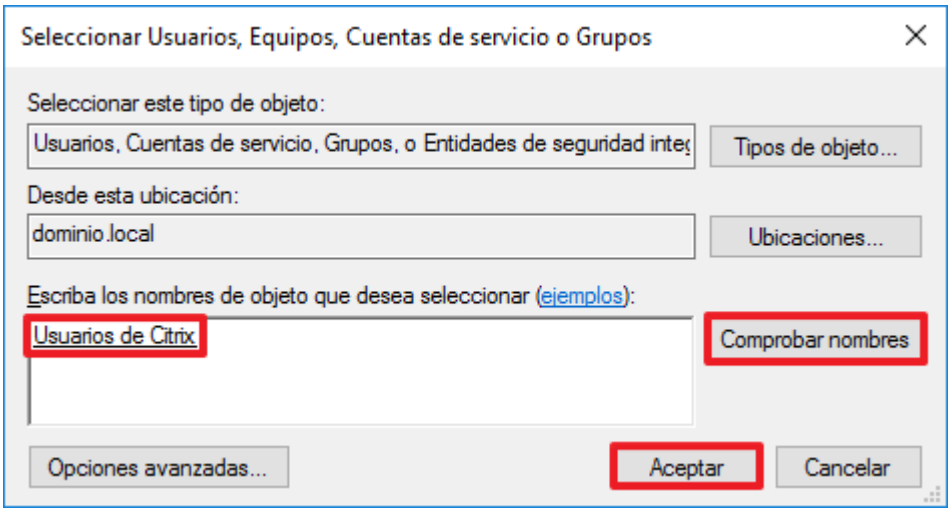
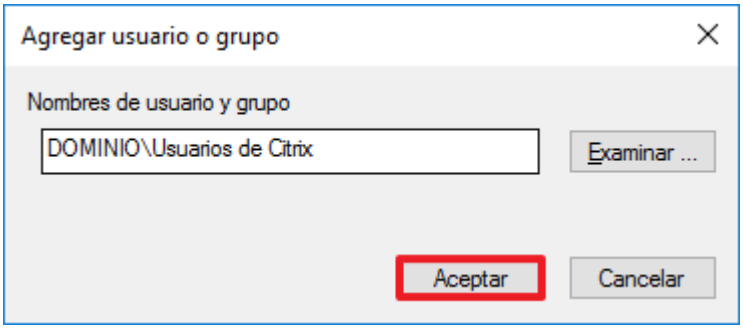
| Paso | Descripción |
|---|---|
| 35. | En la selección de copia de carpeta de seguridad pulse el botón “Siguiente >”.<br>  |
| 36. | En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media” y pulse el botón “Siguiente >”.<br>  |

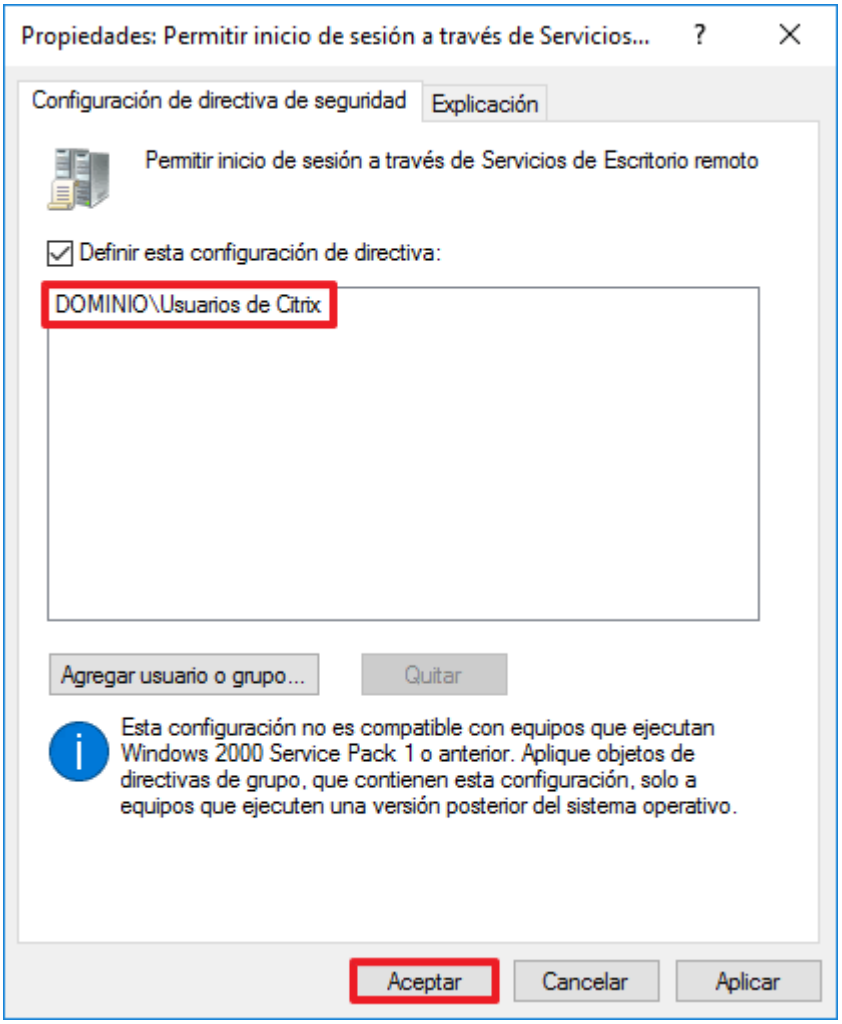
| Paso | Descripción |
|---|---|
| 37. | En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”.<br>  |
| 38. | Para completar el asistente pulse el botón “Finalizar”.<br>  |

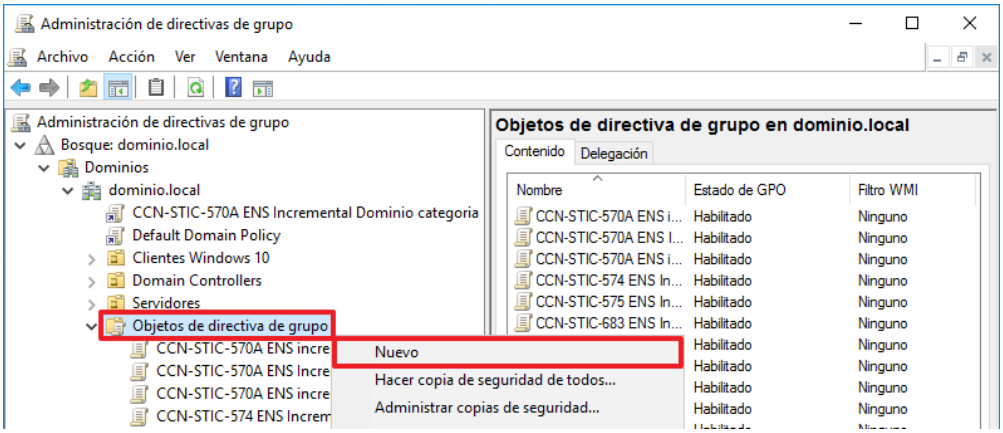
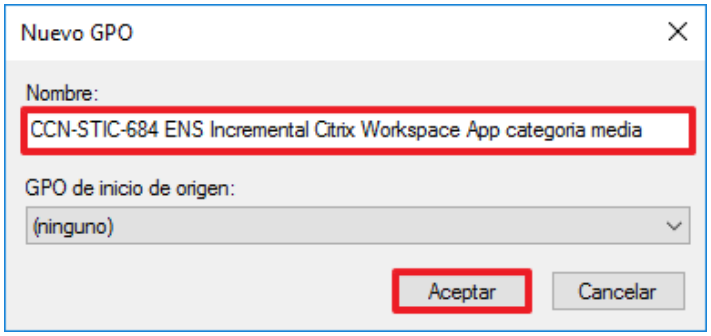
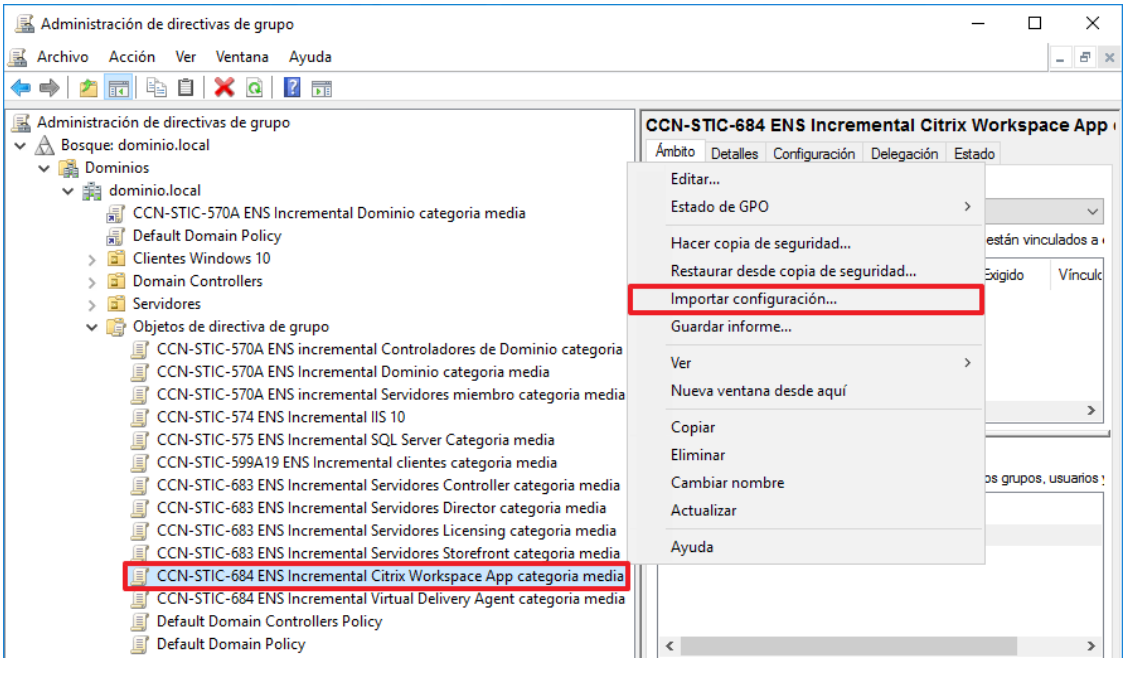
| Paso | Descripción |
|---|---|
| 39. | Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.<br>  |
| 40. | Seleccione de nuevo el GPO, "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media", y marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.<br>  |

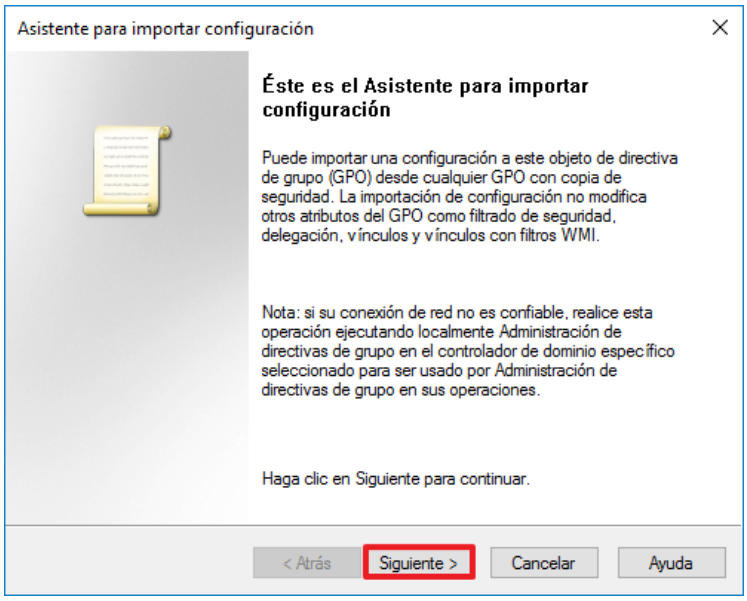
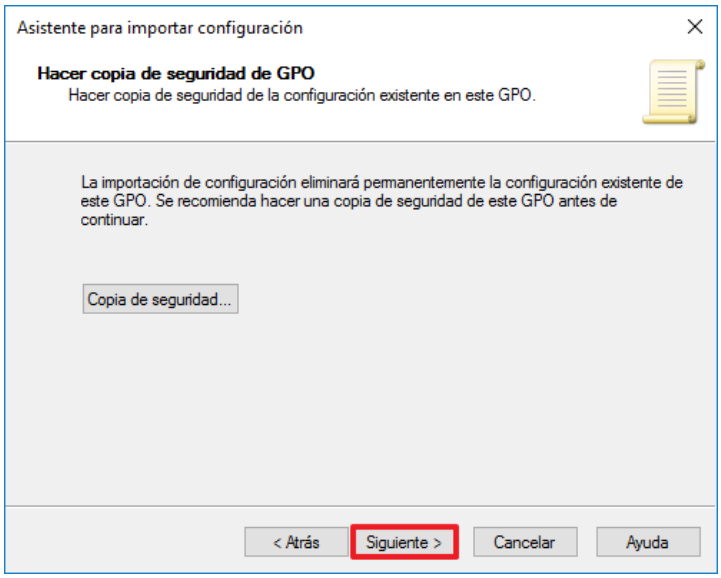
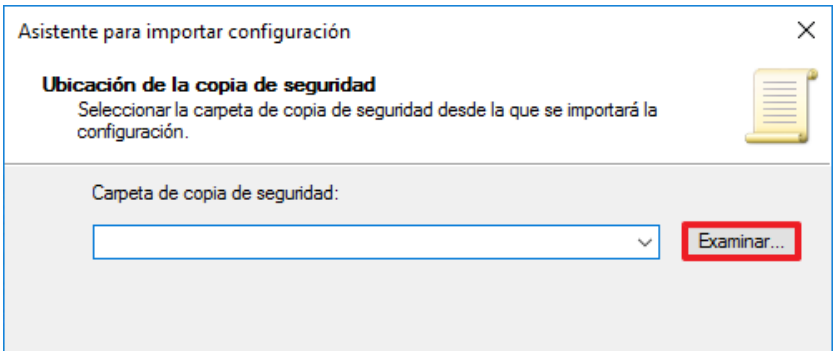
| Paso | Descripción |
|---|---|
| 41. | En la ventana del editor de administración de directivas de grupo, seleccione el nodo **"Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria basica → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad"**, y marcando con el botón derecho en él, elija la opción "Importar directiva..." del menú contextual que aparecerá.<br>  |
| 42. | En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media.inf" y pulse el botón "Abrir". Con eso habrá quedado importada la plantilla de seguridad en el GPO.<br>  |

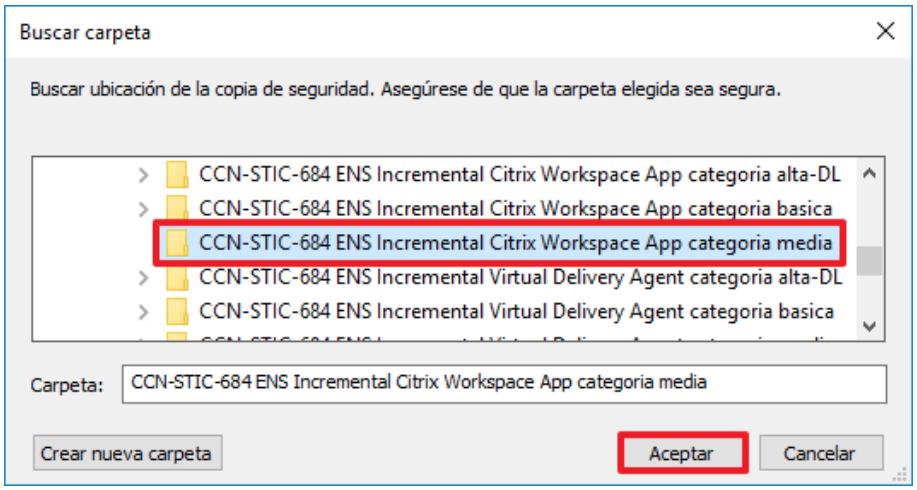
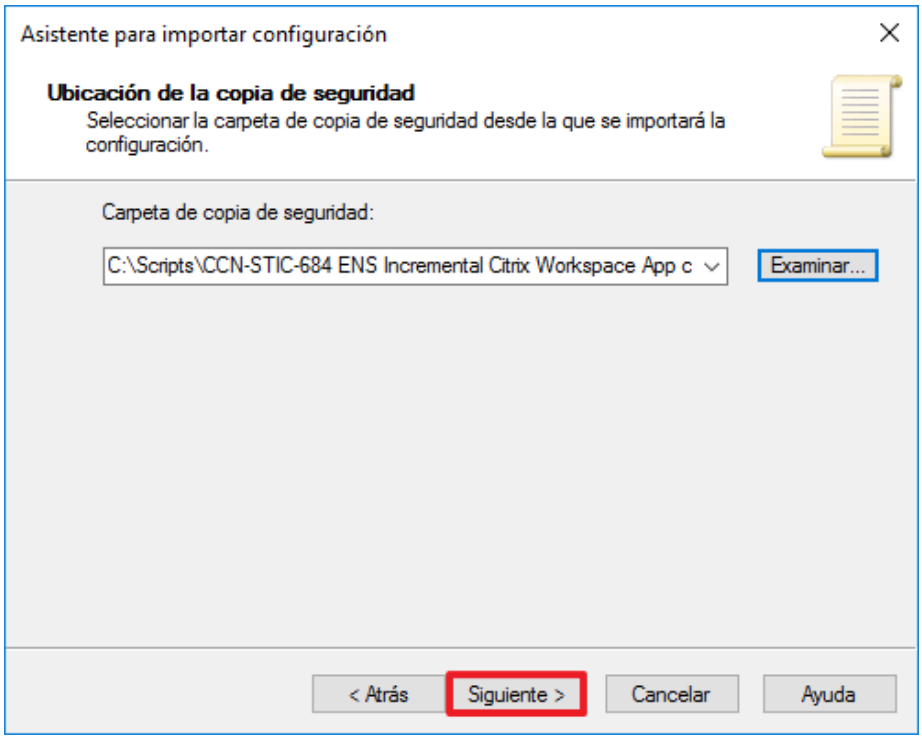
| Paso | Descripción |
|---|---|
| 43. | Continúe editando la directiva de grupo, diríjase al nodo **"Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** y haga doble clic sobre la directiva "Permitir inicio de sesión a través de Escritorio remoto" para proceder a configurarla.<br>  |
| 44. | Marque la casilla "Definir esta configuración de directiva" para habilitar las opciones de configuración. A continuación, pulse sobre "Agregar usuario o grupo".<br>  |

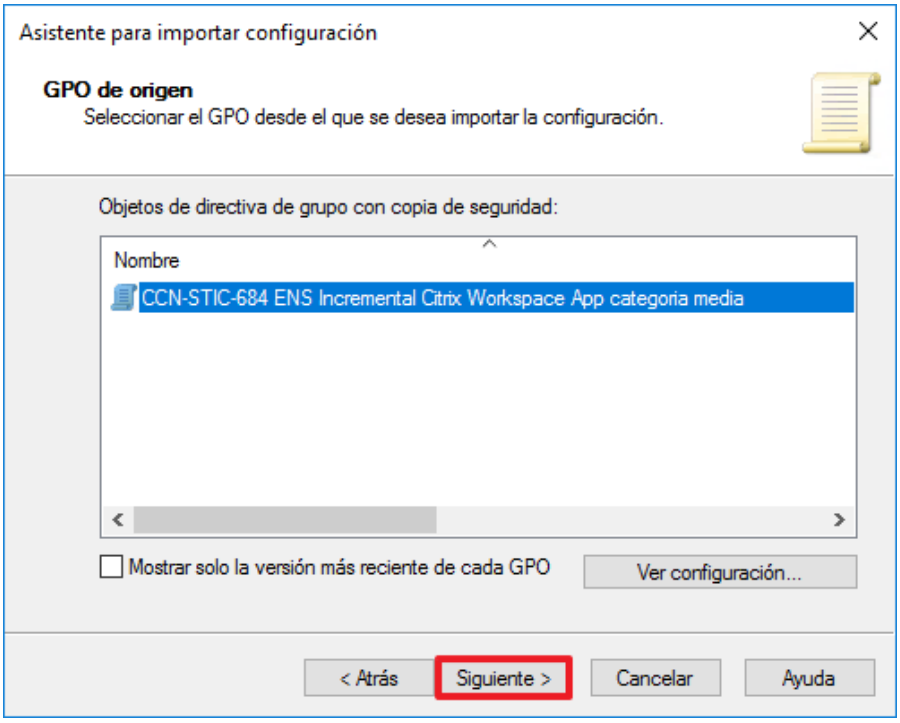
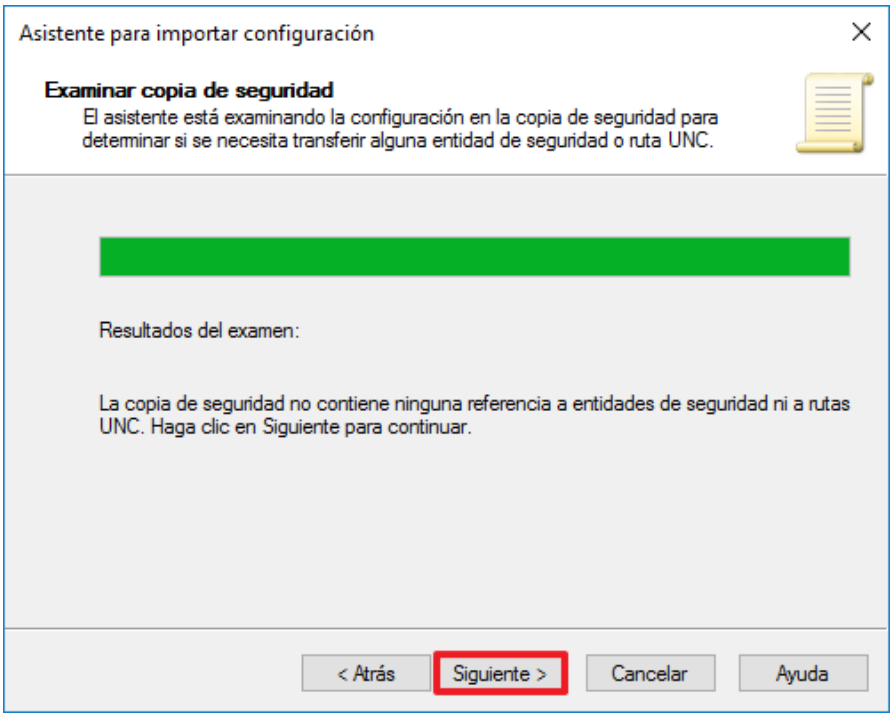
| Paso | Descripción |
|---|---|
| 45. | En la ventana resultante haga clic en “Examinar …”.<br>  |
| 46. | Escriba el nombre del grupo “Usuarios de Citrix” y en este orden pulse en primer lugar sobre “Comprobar nombres” y a continuación sobre “Aceptar”.<br>  <br>**Nota:** El grupo “Usuarios de Citrix” se deberá haber creado al comienzo de esta guía mediante la ejecución del script “CCN-STIC-684 ENS categoria media - Preparacion del Dominio - Paso 2.bat”. |
| 47. | Pulse “Aceptar” para añadir el grupo “Usuarios de Citrix a la directiva”.<br>  |

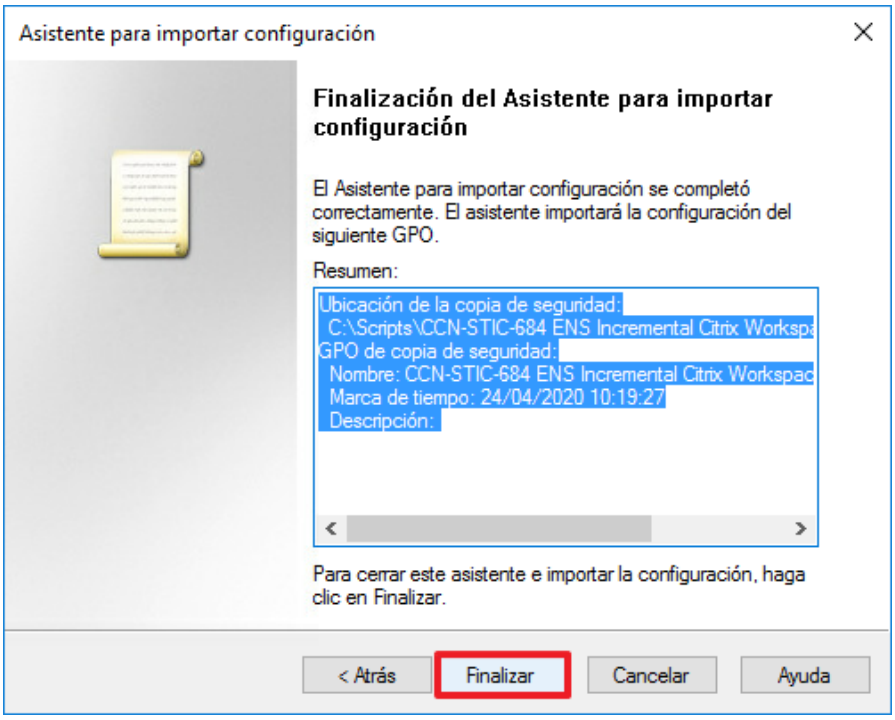
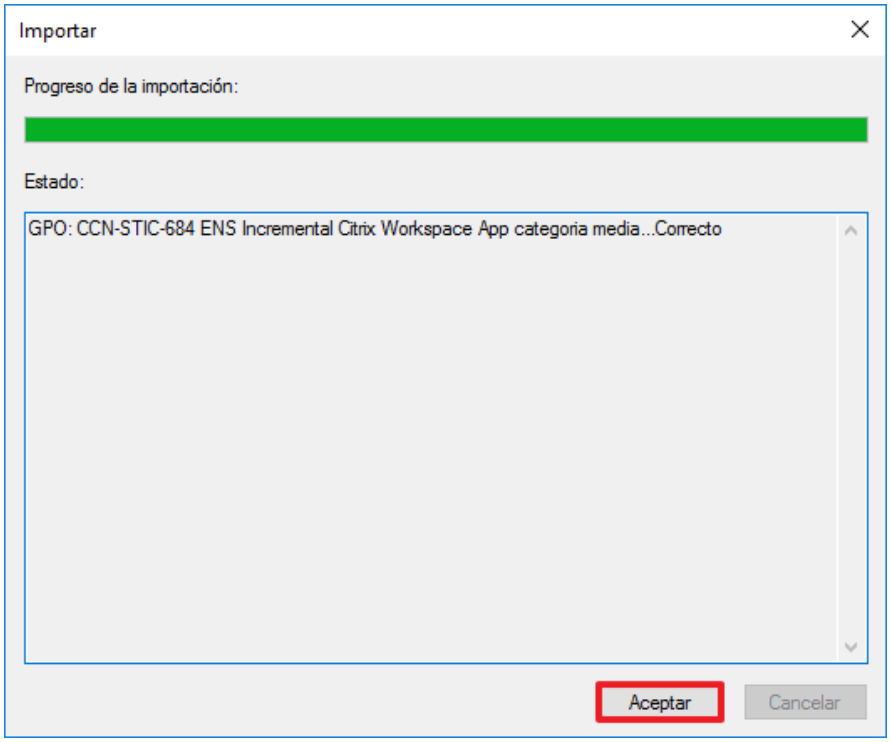
| Paso | Descripción |
|---|---|
| 48. | Aparecerá el grupo “Usuarios de Citrix” definido en la directiva. Pulse “Aceptar” para guardar la configuración y cerrar la ventana.<br>  <br>**Nota:** Ahora sí, cierre la ventana del editor de administración de directivas de grupo. |
| 49. | Con ello este GPO ("CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. |

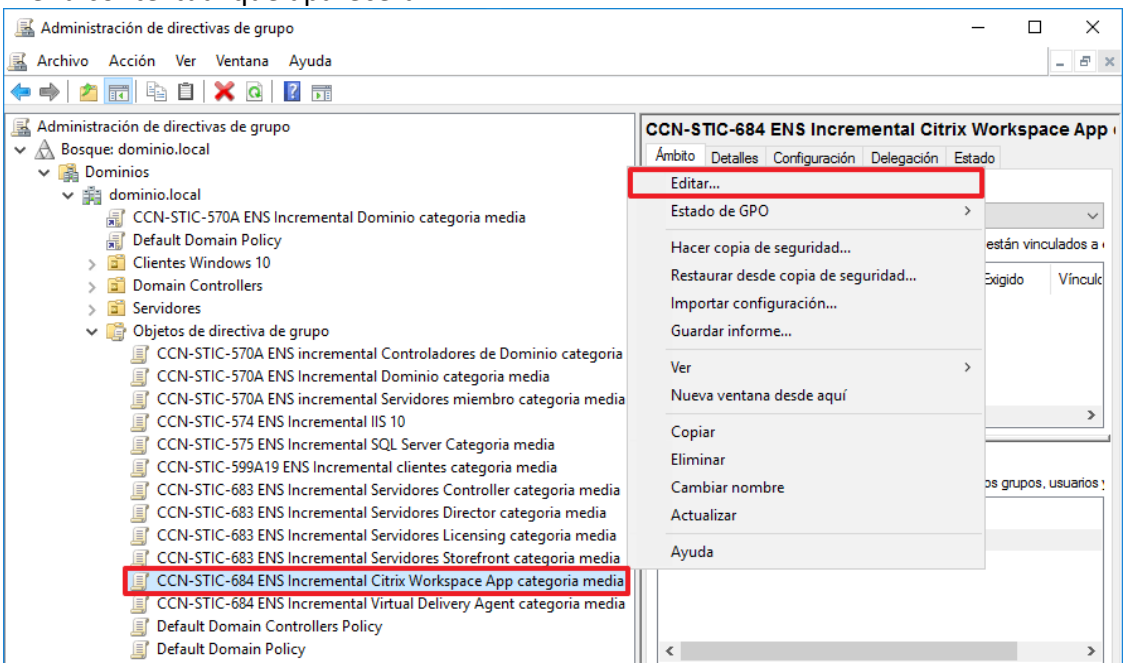
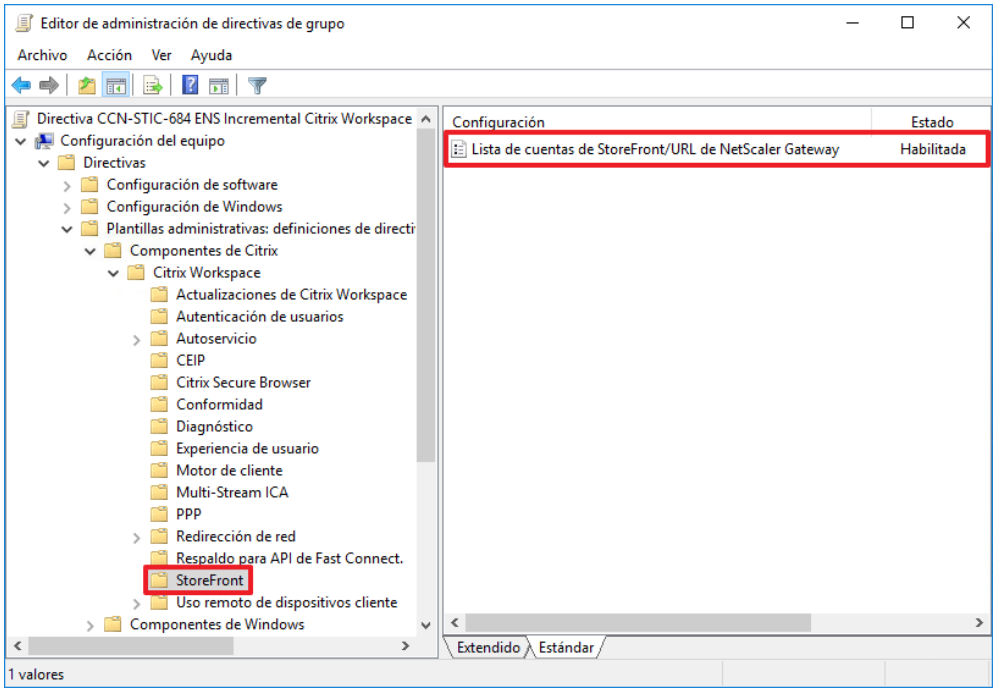
| Paso | Descripción |
|---|---|
| 50. | Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá.   |
| 51. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media" y pulse el botón “Aceptar”.   |
| 52. | Seleccione el GPO recién creado, "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media", y marcando con el botón derecho en él, elija la opción "Importar configuración..." del menú contextual que aparecerá.   |

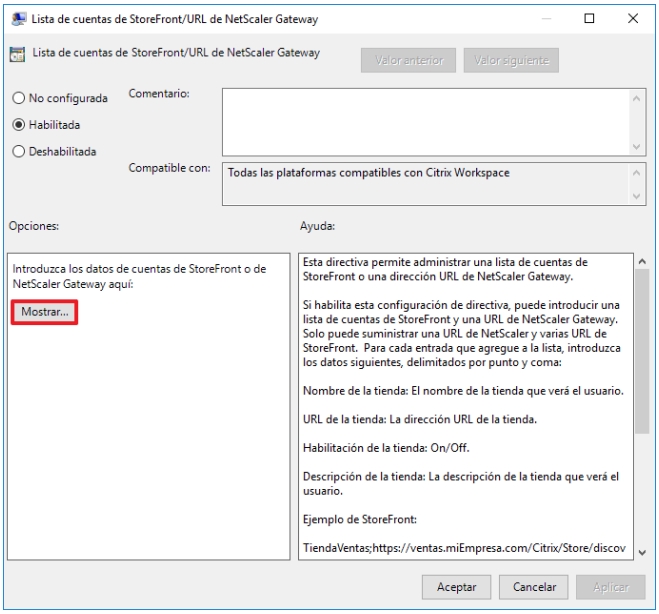
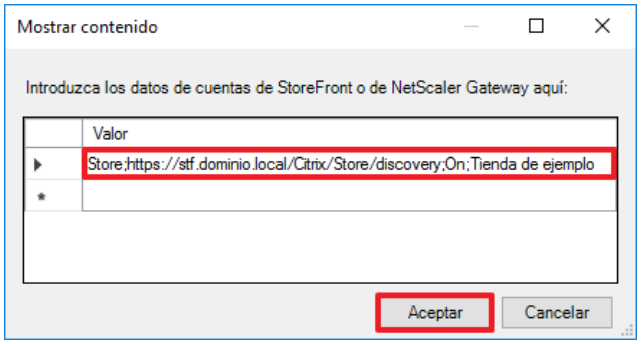
| Paso | Descripción |
|---|---|
| 53. | En el asistente de importación de configuración, pulse el botón “Siguiente >”.<br>  |
| 54. | En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |
| 55. | Pulse el botón “Examinar...” en la ventana “Ubicación de la copia de seguridad”.<br>  |

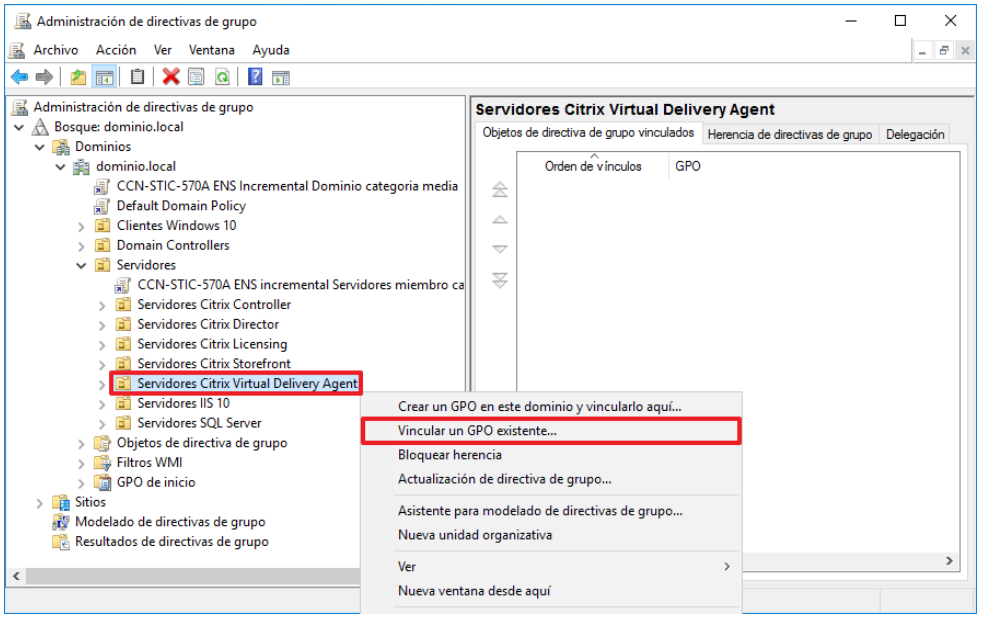
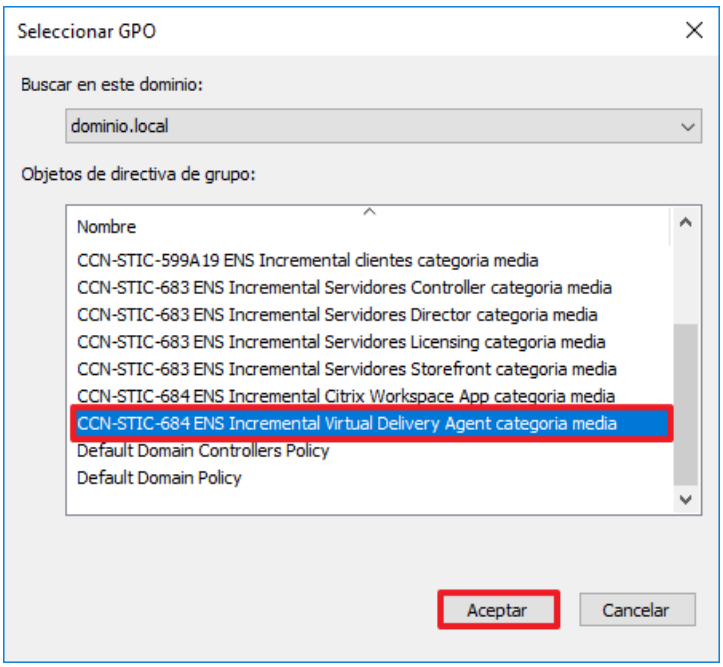
| Paso | Descripción |
|---|---|
| 56. | Seleccione la carpeta “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.<br>  |
| 57. | En la selección de copia de carpeta de seguridad pulse el botón “Siguiente >”.<br>  |

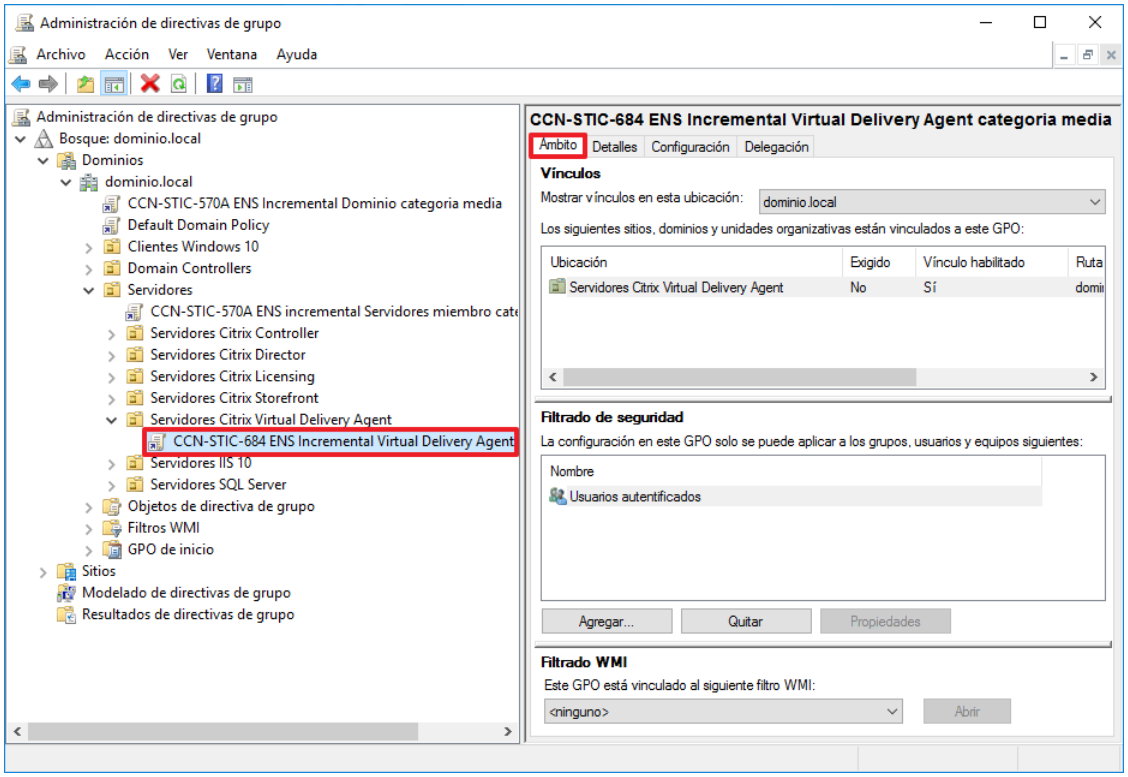
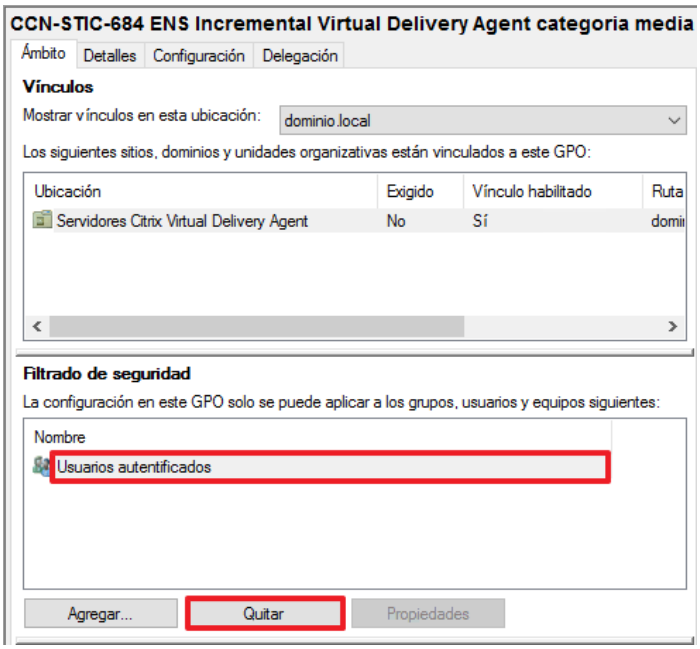
| Paso | Descripción |
|---|---|
| 58. | En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” y pulse el botón “Siguiente >”.<br>  |
| 59. | En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”.<br>  |

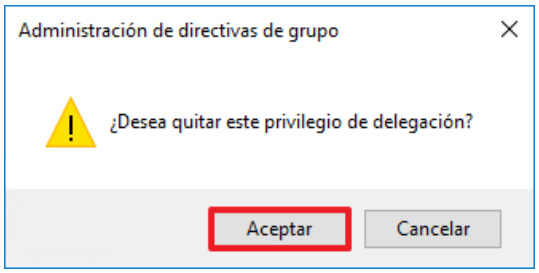
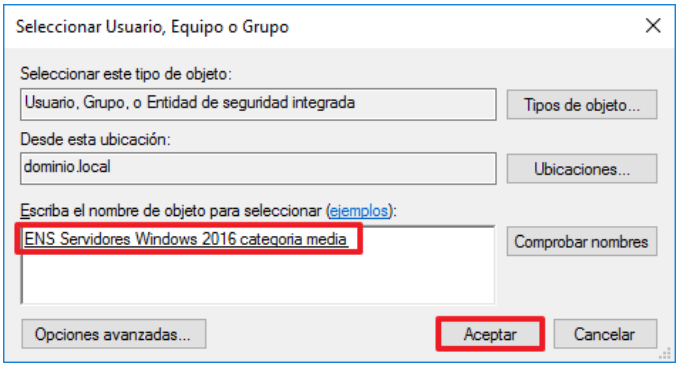
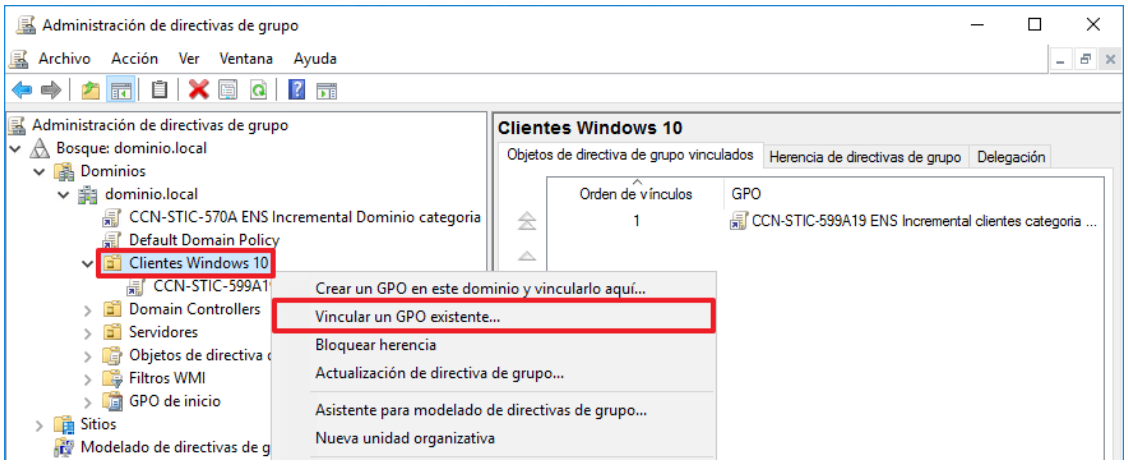
| Paso | Descripción |
|---|---|
| 60. | Para completar el asistente pulse el botón “Finalizar”.<br>  |
| 61. | Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.<br>  |

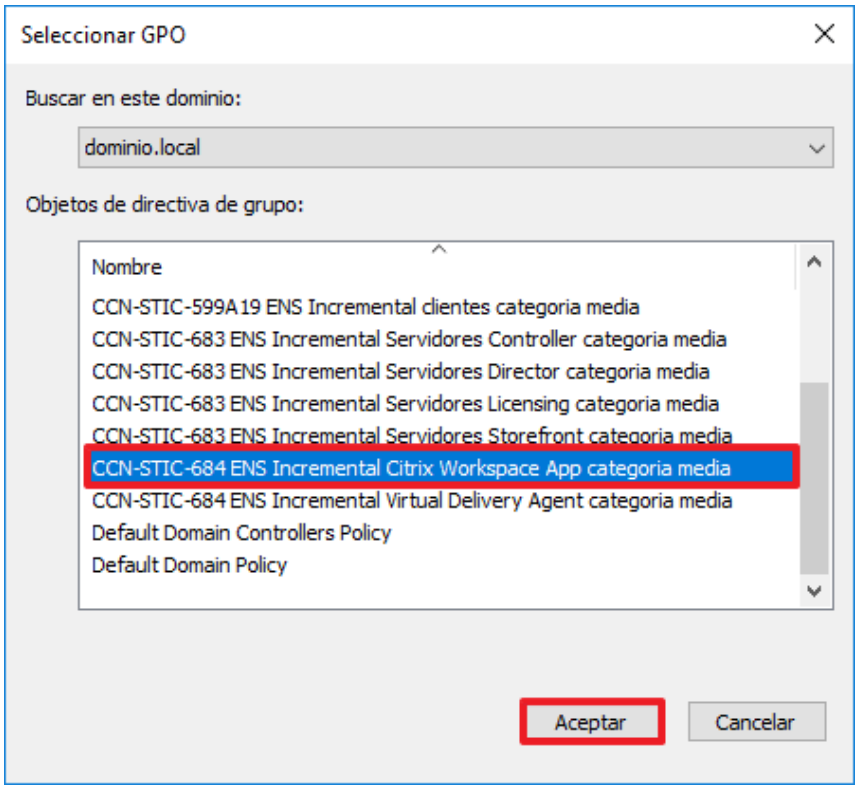
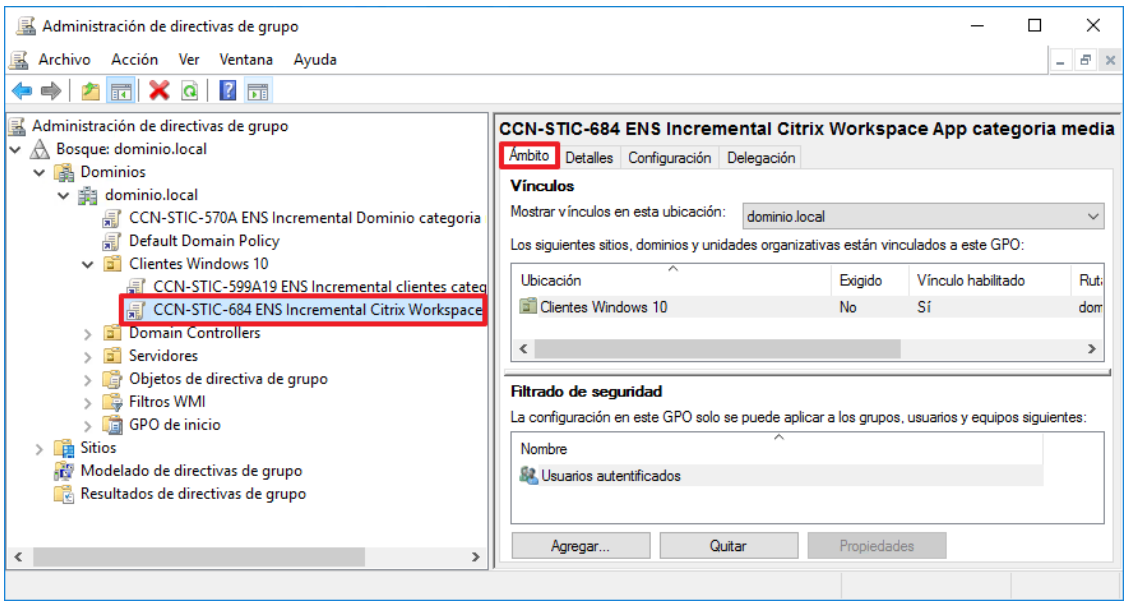
| Paso | Descripción |
|---|---|
| 62. | Seleccione el GPO "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media" de nuevo, y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.<br>  |
| 63. | En la ventana del editor de administración de directivas de grupo, seleccione el nodo **"Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Storefront"**, y haciendo doble clic sobre la directiva "Lista de cuentas de Storefront/URL de Netscaler Gateway" acceda a la configuración de la misma.<br>  |

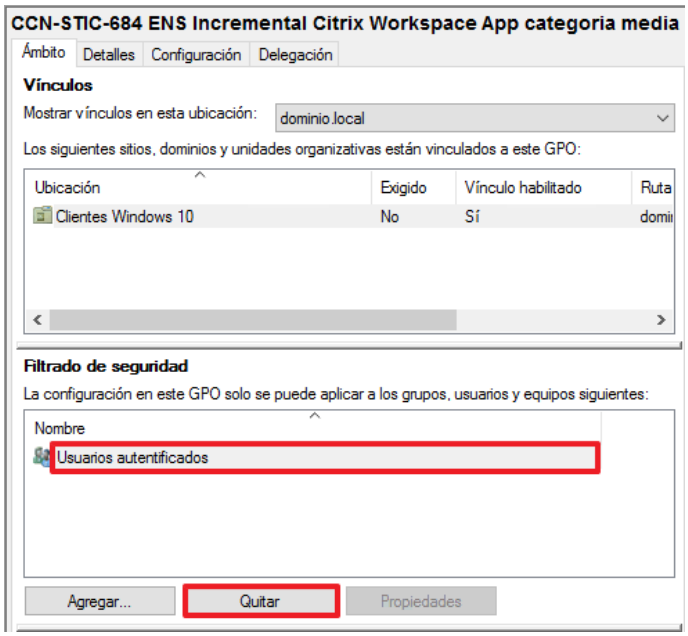
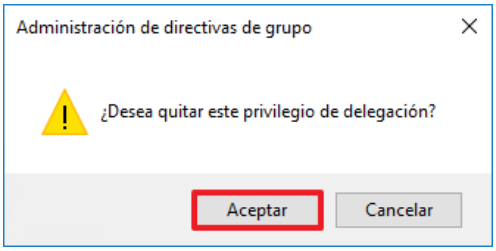
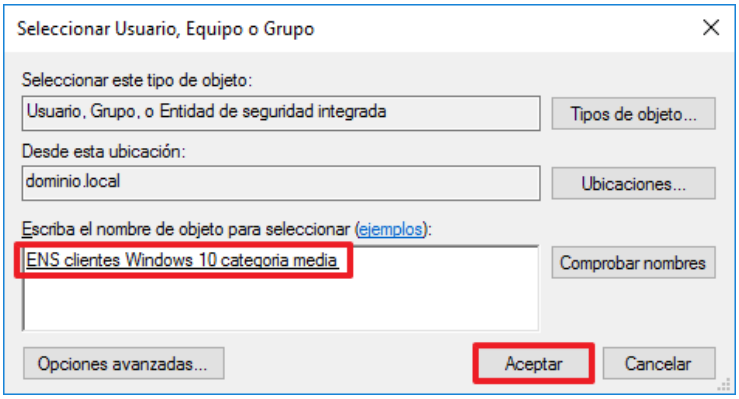
| Paso | Descripción |
|---|---|
| 64. | La directiva se entrega habilitada pero con los valores en blanco. Deberá en este momento configurar la directiva con los valores necesarios para el correcto funcionamiento de su infraestructura. Para ello, haga clic en “Mostrar…”.<br>  <br> |
| 65. | En la ventana resultante, en el campo “Valor”, deberá indicar los datos de la cuenta de Storefront configurado durante la aplicación de la guía CCN-STIC-683. Para cada entrada que agregue a la lista, introduzca los siguientes datos, delimitados por punto y coma:<br>– Nombre de la tienda: El nombre de la tienda que verá el usuario.<br>– URL de la tienda: La dirección URL de la tienda.<br>– Habilitación de la tienda: On/Off.<br>– Descripción de la tienda: La descripción de la tienda que verá el usuario.<br>Pulse “Aceptar” para cerrar la ventana y nuevamente en “Aceptar” para guardar la configuración de la directiva.<br>  <br><br>**Nota:** En esta guía se utiliza la URL “https://stf.dominio.local/Citrix/Store/discovery” así como el resto de configuraciones a modo de ejemplo. Deberá en su caso, adaptar este valor a los configurados por su organización durante la aplicación de la guía “CCN-STIC-683” y los requisitos de la misma.<br>Para el descubrimiento de la tienda será necesario incluir “/Discovery” al final de la URL independientemente de la dirección utilizada. |

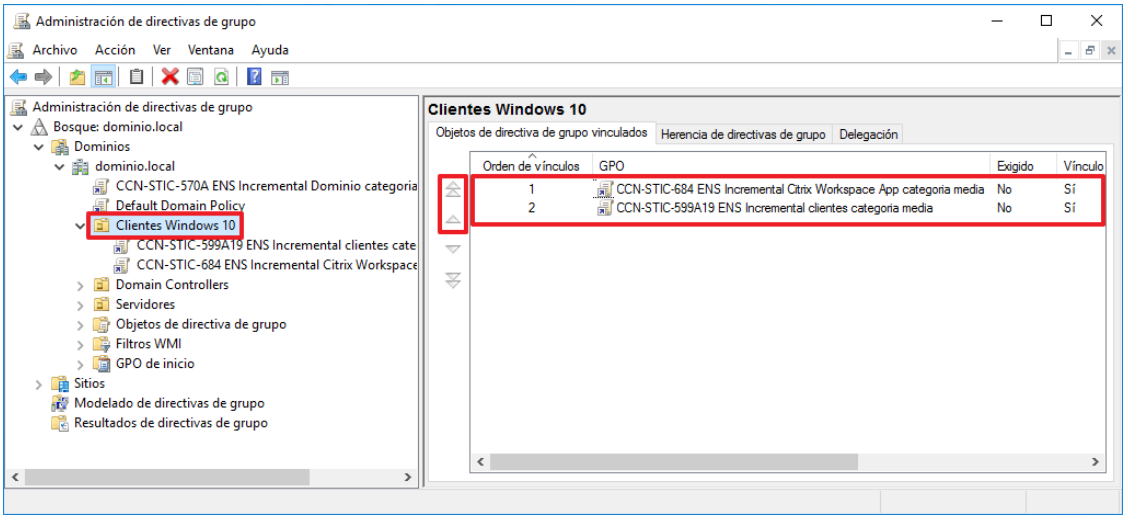
| Paso | Descripción |
|---|---|
| 66. | Con ello, este GPO ("CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que la configuración sea aplicada. |
| 67. | Cierre el “Editor de administración de directivas de grupo”. |
| 68. | 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 Virtual Delivery Agent”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá.   |
| 69. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media” y pulse “Aceptar”.   |

| Paso | Descripción |
|---|---|
| 70. | Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.   |
| 71. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.   |

| Paso | Descripción |
|---|---|
| 72. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.<br>  |
| 73. | Una vez quitado, pulse el botón “Agregar…”. |
| 74. | Introduzca como nombre “ENS servidores Windows 2016 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |
| 75. | 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> → Clientes Windows 10”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá.<br>  |

| Paso | Descripción |
|---|---|
| 76. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” y pulse “Aceptar”.<br>  |
| 77. | Seleccione la política de grupo “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.<br>  |

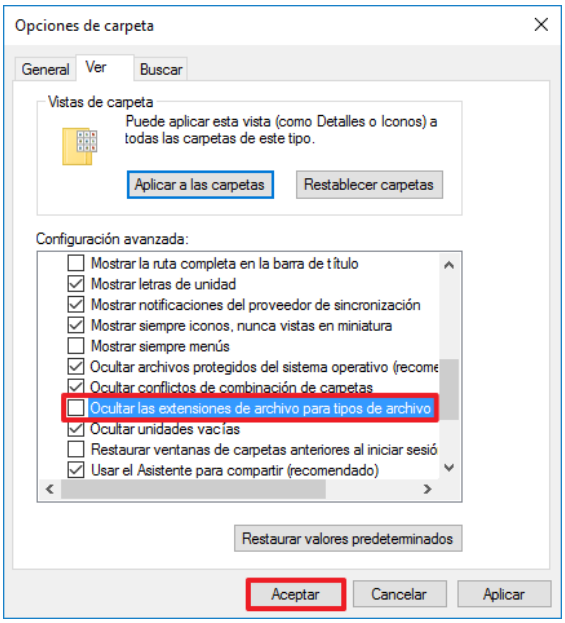
| Paso | Descripción |
|---|---|
| 78. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.<br>  |
| 79. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.<br>  |
| 80. | Una vez quitado, pulse el botón “Agregar…”. |
| 81. | Introduzca como nombre “ENS clientes Windows 10 categoria media”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-599A19”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |

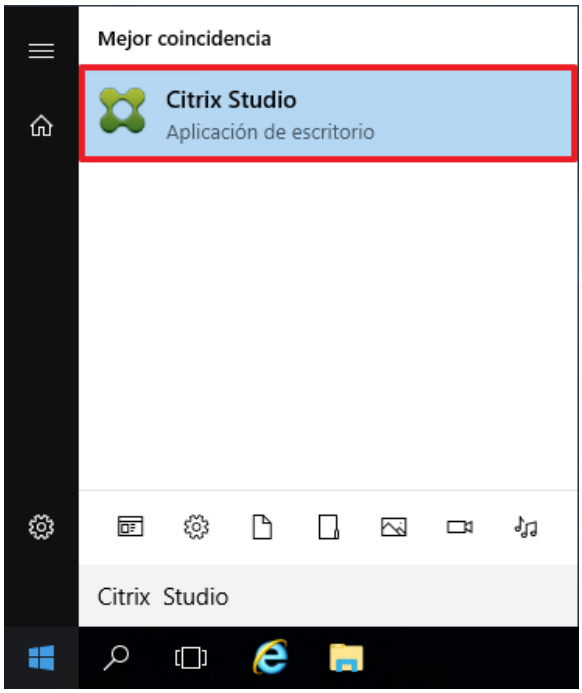
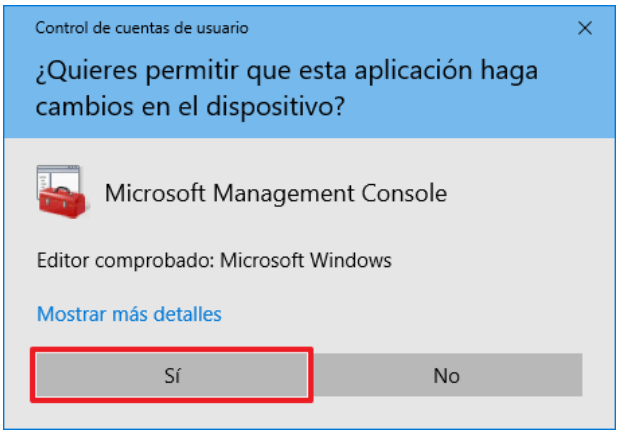
| Paso | Descripción |
|---|---|
| 82. | Seleccione el contenedor “Clientes Windows 10” y compruebe en la parte central de la ventana, en la pestaña "Objetos de directiva de grupo vinculados", que el orden de los vínculos es el siguiente, tal y como se muestra en la figura.<br>– 1 - CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media<br>– 2 - CCN-STIC-599A19 ENS Incremental clientes categoria media<br>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.<br>  |
| 83. | 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. |
| 84. | Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor. |

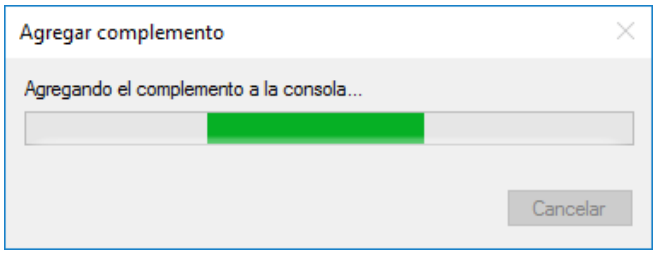
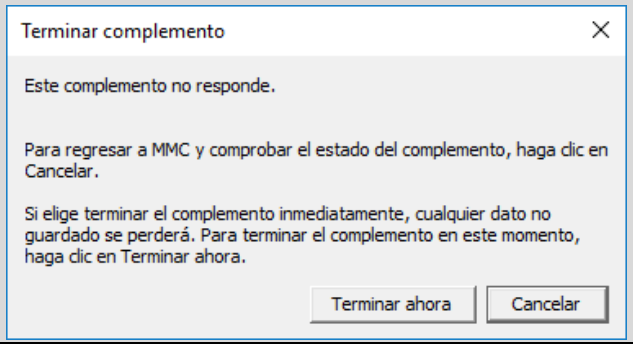
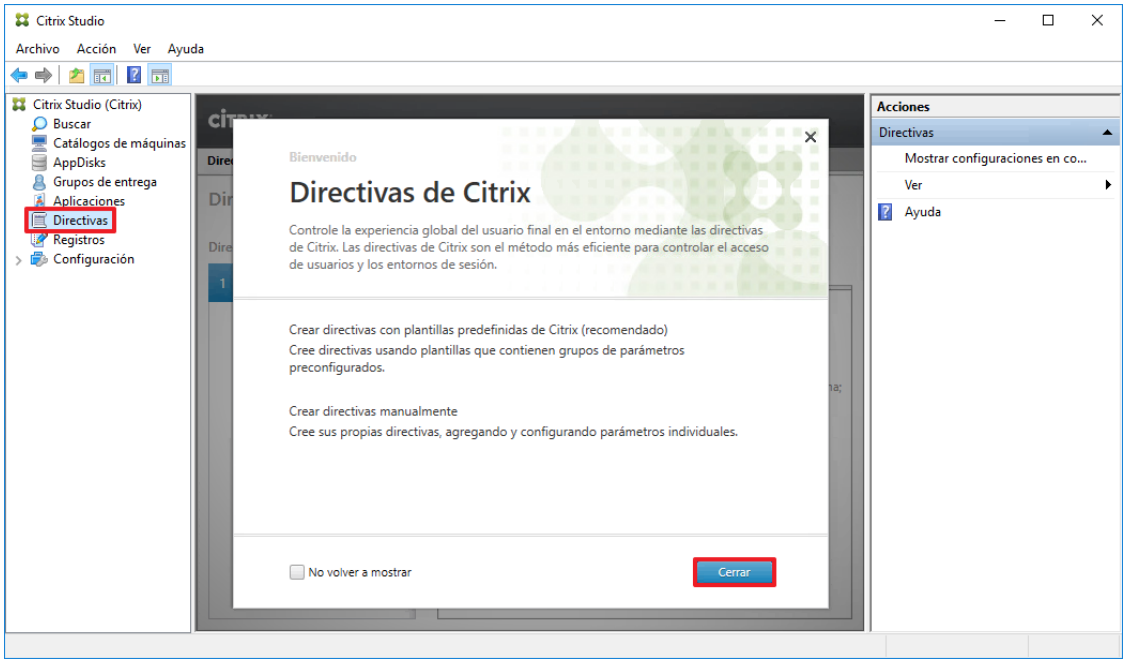
## 2. CONFIGURACIÓN DE SEGURIDAD CITRIX STUDIO

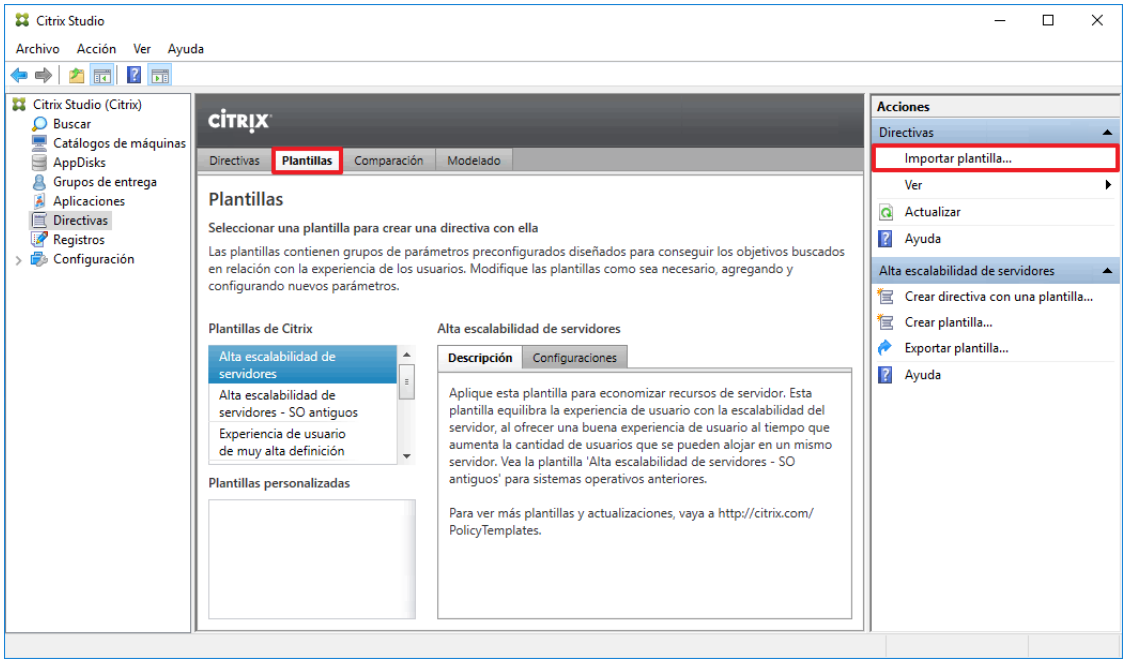
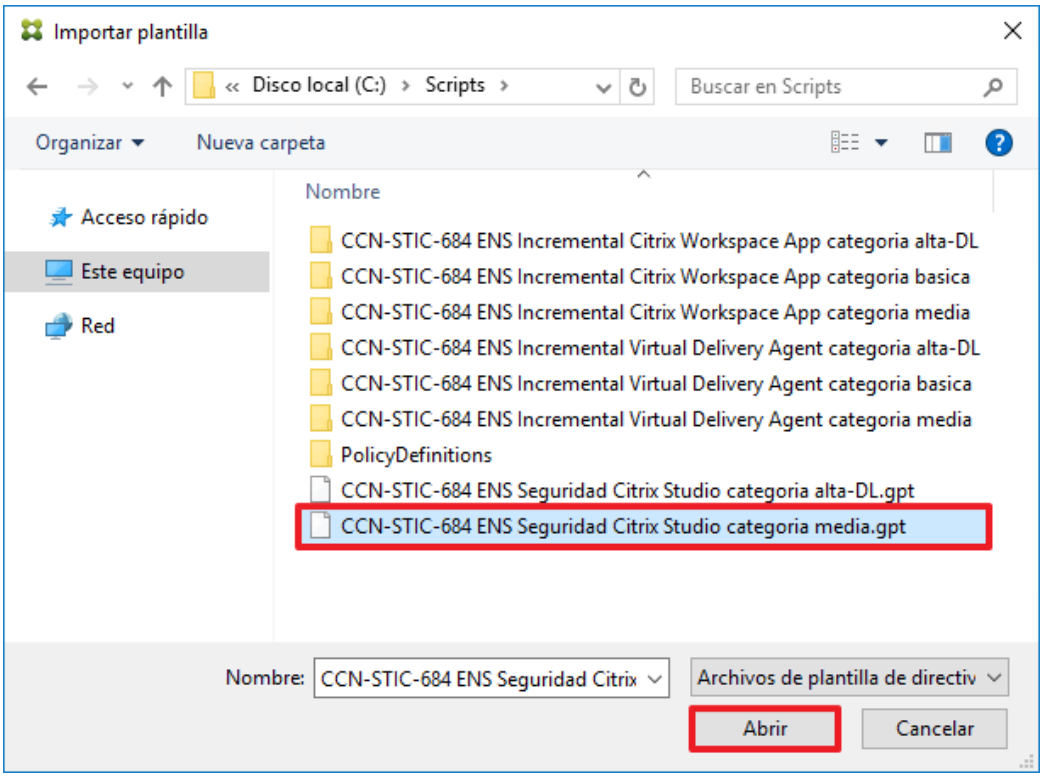
Los pasos que se describen a continuación se realizarán en un servidor con el rol Citrix Controller que haya sido configurado previamente mediante la aplicación de la guía codificada como “CCN-STIC-683 – Categoría Media”. Los pasos descritos a continuación solo los debe realizar cuando vaya a realizar la primera implementación en el dominio, ya que solo es necesario crear las plantillas de seguridad e incorporarlas en la directiva de seguridad una única vez por infraestructura.

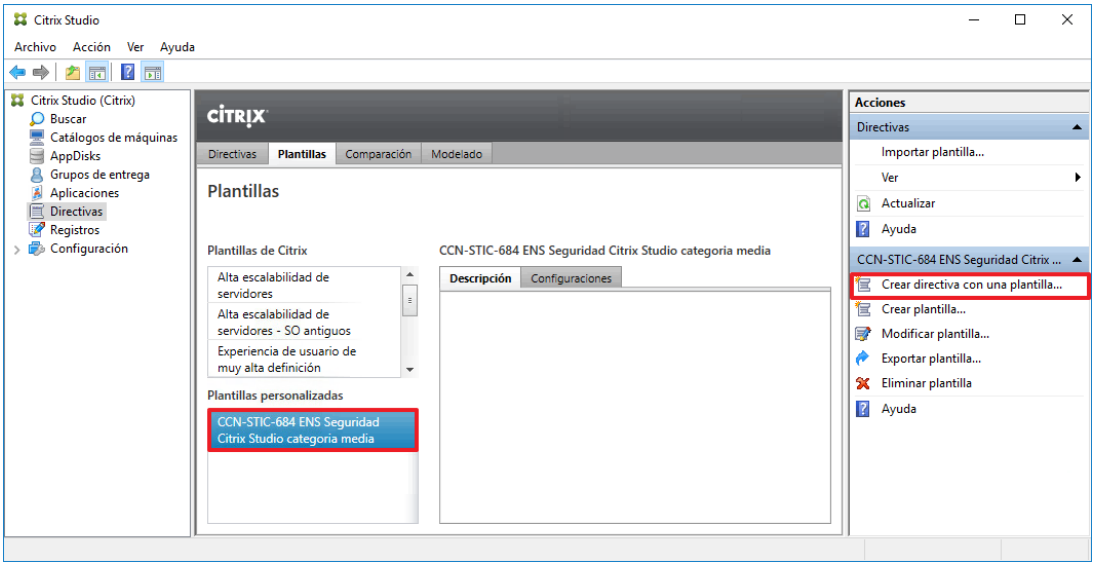
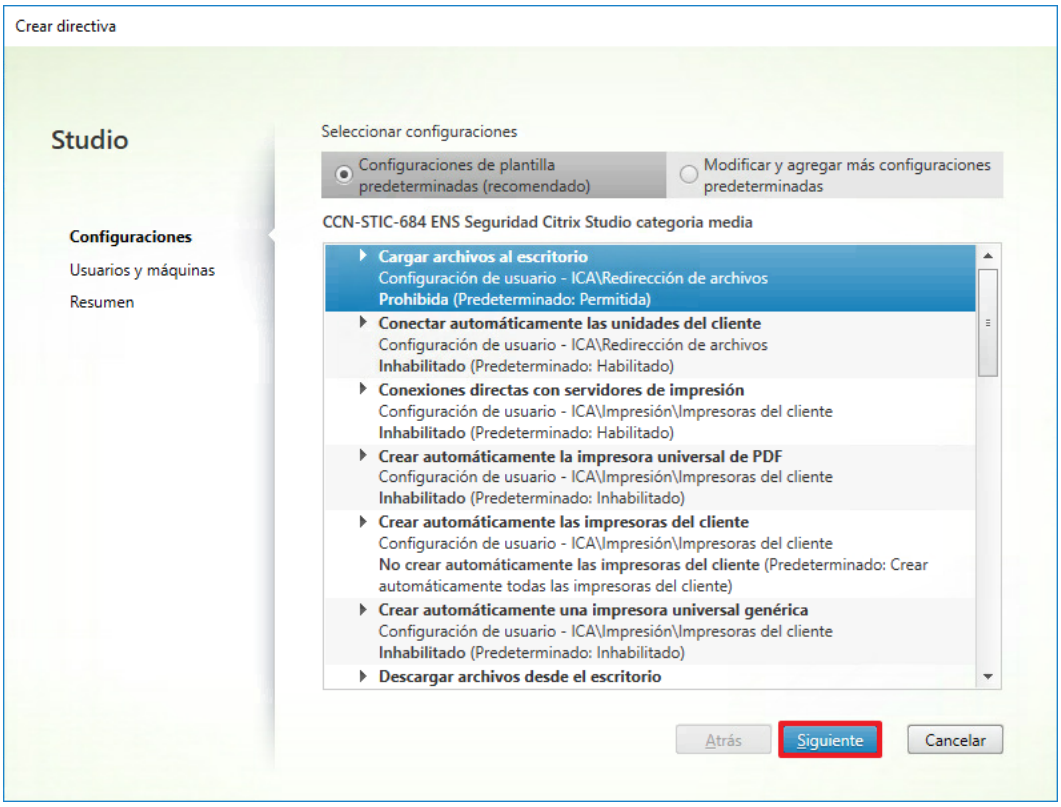
**Nota:** Esta guía asume que al servidor con el rol Citrix Controller se le ha aplicado la configuración descrita en la guía “CCN-STIC-683 Implementación de seguridad en Citrix Virtual Apps and Desktops”. Si no es así, aplique la guía correspondiente antes de continuar con la aplicación de ésta.

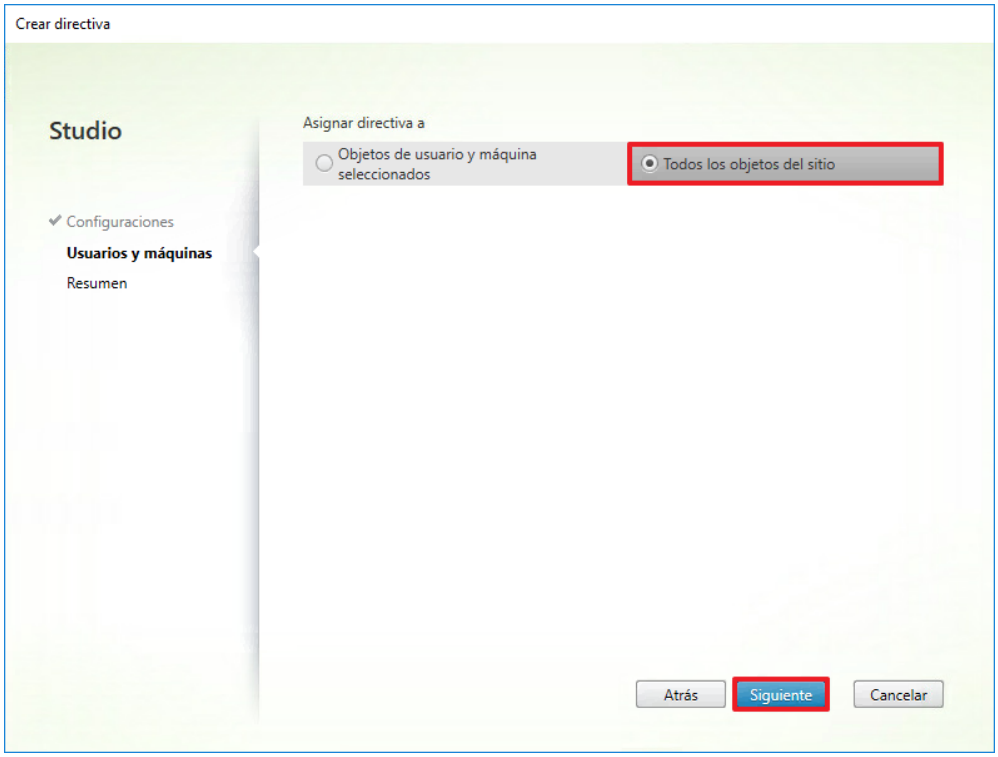
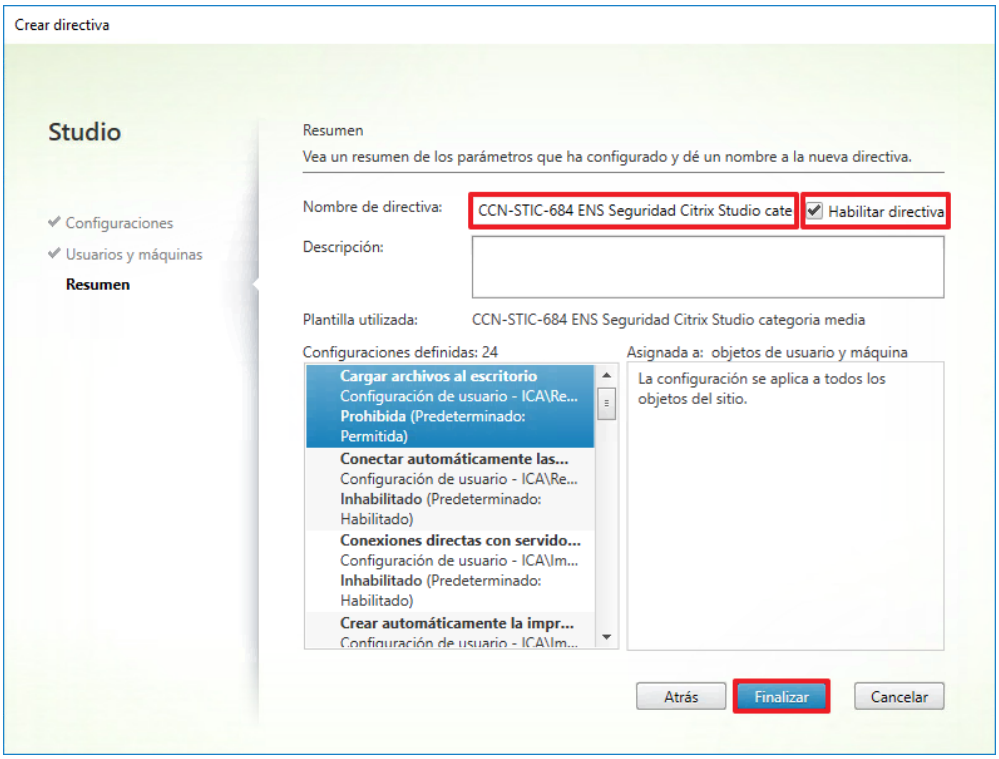
| Paso | Descripción |
|---|---|
| 85. | Inicie sesión en un servidor con el rol Citrix Controller, con una cuenta de administrador del dominio.<br>  |
| 86. | Cree el directorio “Scripts” en la unidad “C:\”. |
| 87. | Copie los ficheros y carpetas que acompañan a esta guía en el directorio “C:\Scripts”. El sistema solicitará elevación de privilegios. Como mínimo deben aparecer los siguientes ficheros y carpetas.<br>– CCN-STIC-684 ENS Seguridad Citrix Studio categoria media.gpt |
| 88. | Si no lo ha realizado durante la implementación de la guía CCN-STIC-570A, configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que Explorador de Windows sí muestra las extensiones de los archivos.<br>Para configurar Explorador de Windows para 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.<br>  |

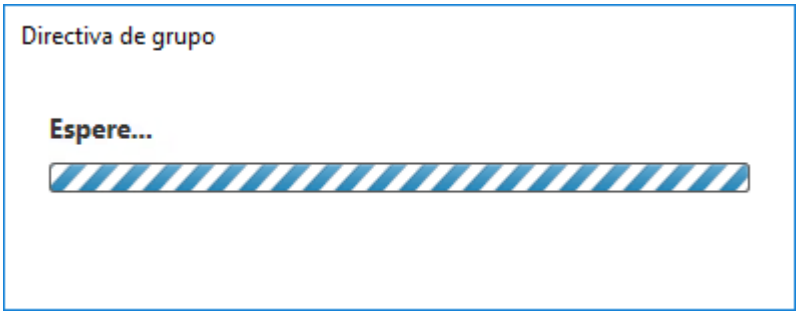
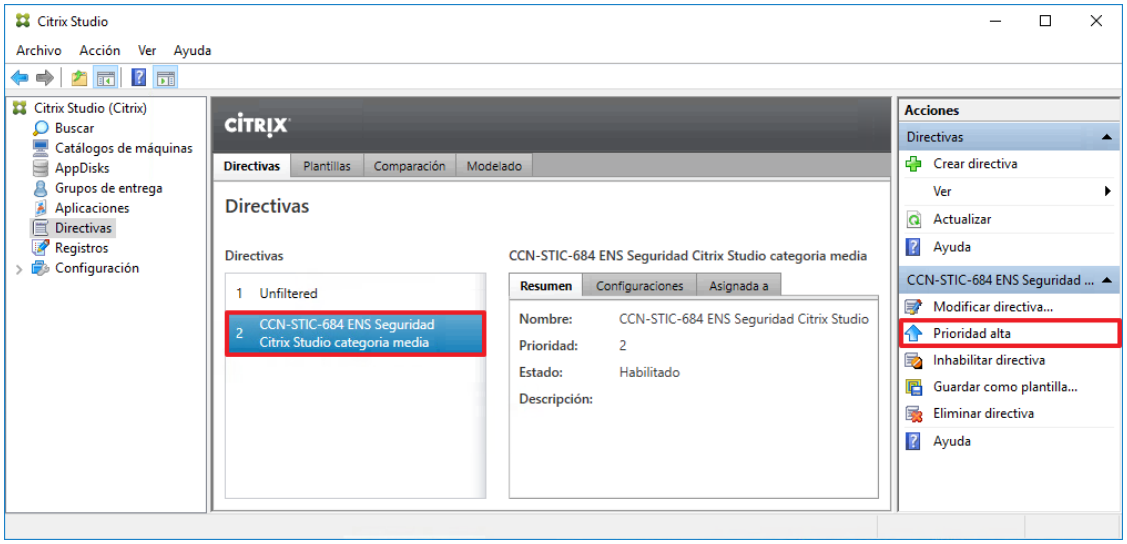
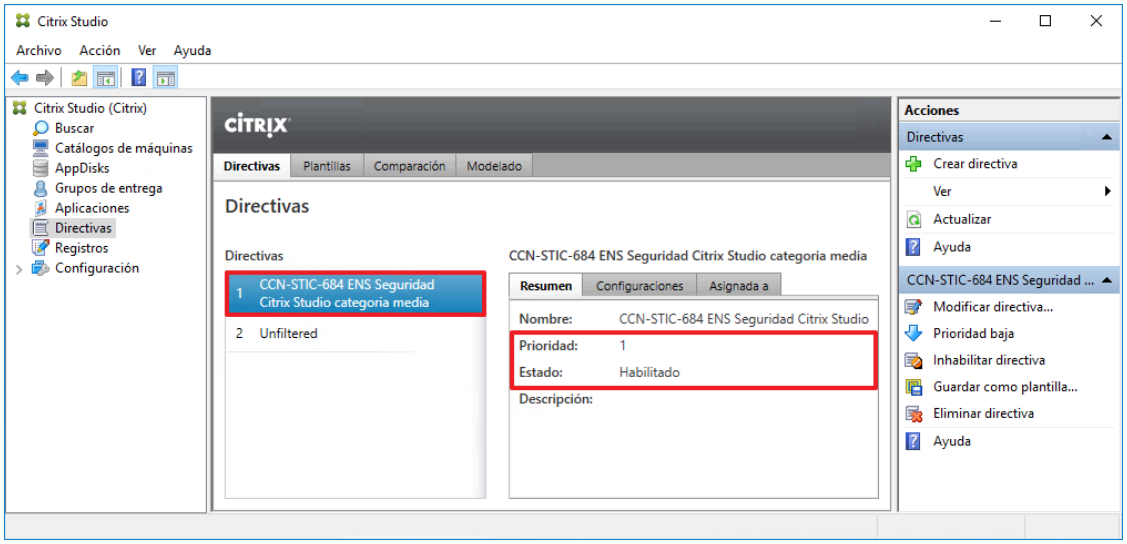
| Paso | Descripción |
|---|---|
| 89. | Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá "¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?", y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta". |
| 90. | Ejecute la aplicación "Citrix Studio".<br>  |
| 91. | El sistema solicitará elevación de privilegios, pulse "Sí" para continuar.<br>  |

| Paso | Descripción |
|---|---|
| 92. | Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.<br>  <br>**Nota:** Ignore cualquier advertencia que le indique que el complemento no responde. Pulse "Cancelar" para continuar.<br>  |
| 93. | Una vez en la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Directivas"**. En la ventana de bienvenida pulse "Cerrar".<br>  <br>**Nota:** Para evitar que la ventana de bienvenida aparezca cada vez que acceda al nodo "Directivas" seleccione la casilla "No volver a mostrar". |

| Paso | Descripción |
|---|---|
| 94. | Proceda en este punto a importar la plantilla de seguridad de Citrix Studio. Para ello, acceda a la opción "Importar plantilla…" en la ruta **"Citrix Studio → Directivas → Plantillas → Acciones → Directivas → Importar plantillas…"**.<br>  |
| 95. | En el cuadro de diálogo que aparecerá (titulado "Importar plantilla"), seleccione la directiva "C:\Scripts\CCN-STIC-684 ENS Seguridad Citrix Studio categoria media.gpt" y pulse el botón "Abrir".<br>Con eso habrá quedado importada la plantilla de seguridad.<br>  |

| Paso | Descripción |
|---|---|
| 96. | Aparecerá la plantilla recién importada en el apartado “Plantillas personalizadas”. Seleccione la plantilla y haga clic en “Crear directiva con una plantilla…”.   |
| 97. | Se abrirá el asistente de creación de directivas de Citrix Studio. Puesto que con la importación de la plantilla en pasos anteriores se asignan las configuraciones necesarias no modifique ningún parámetro. Pulse “Siguiente” para continuar.   |

| Paso | Descripción |
|---|---|
| 98. | En la ventana “Asignar directiva a” seleccione “Todos los objetos del sitio”. Pulse “Siguiente” para continuar.<br>  |
| 99. | Por último, asigne el nombre “CCN-STIC-684 ENS Seguridad Citrix Studio categoria media” a la directiva recién creada. Marque la opción “Habilitar directiva” y pulse “Finalizar” para completar la creación de la directiva.<br>  |

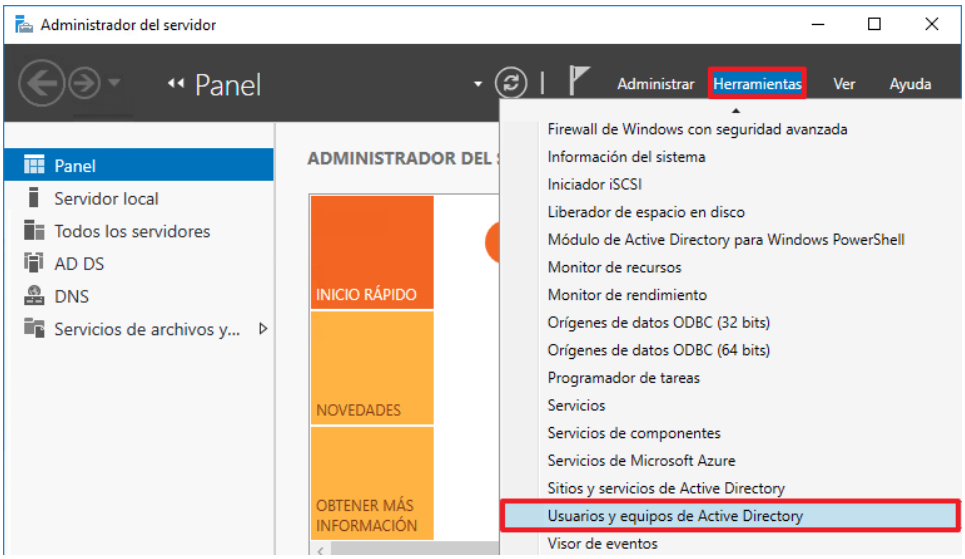
| Paso | Descripción |
|---|---|
| 100. | Espere a que finalice el proceso de creación de la directiva.<br>  |
| 101. | Para finalizar la configuración de la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria media” diríjase al nodo de configuración **“Citrix Studio → Directivas”** y seleccionando la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria media” sitúela con el mayor nivel de prioridad haciendo uso de la opción “Prioridad alta”.<br>  |
| 102. | Verifique que la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria media” ha quedado configurada con la prioridad 1 y que es estado de la misma es “Habilitado”.<br>  |

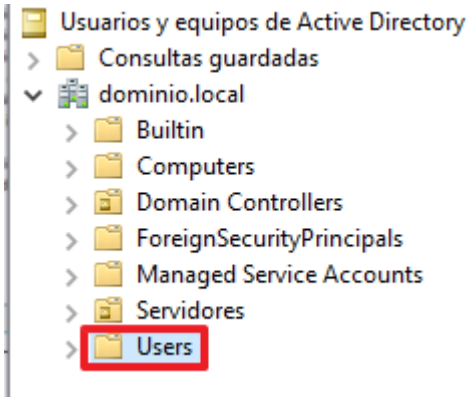
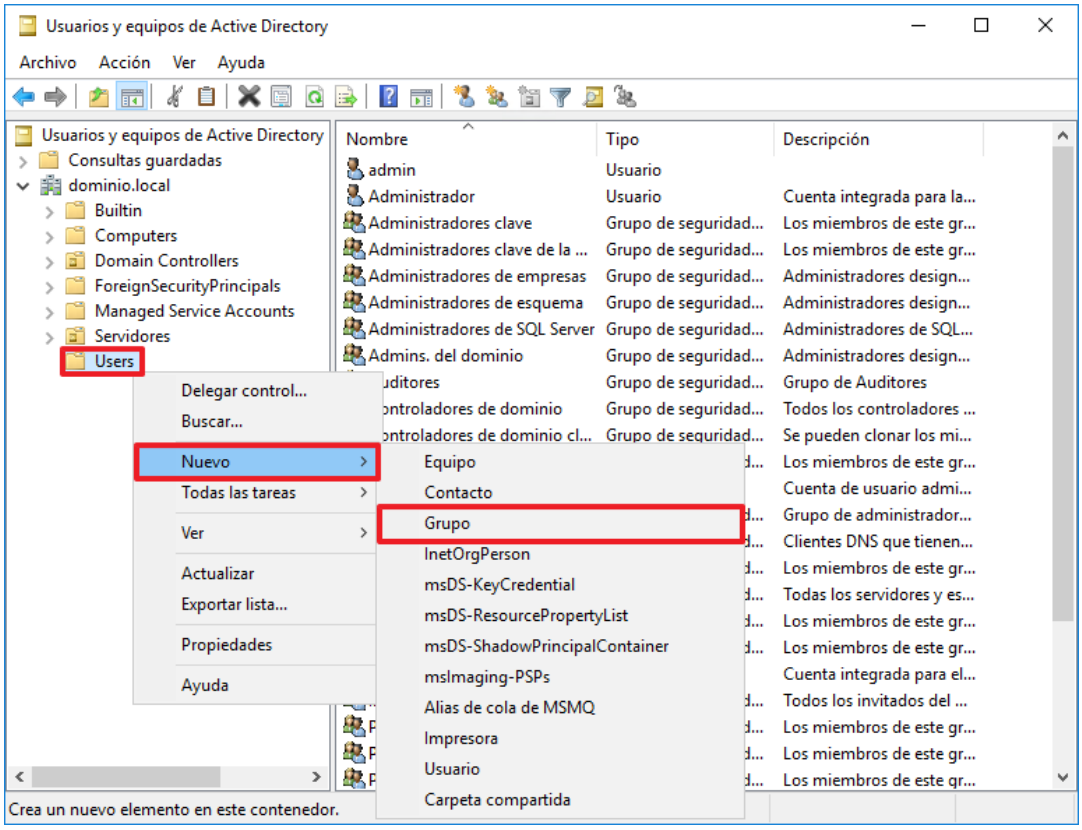
| Paso | Descripción |
|---|---|
| 103. | En este punto se encuentran configuradas las directivas de seguridad de Citrix Studio que serán de aplicación a los recursos que se publiquen desde la infraestructura. |
| 104. | Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor. |

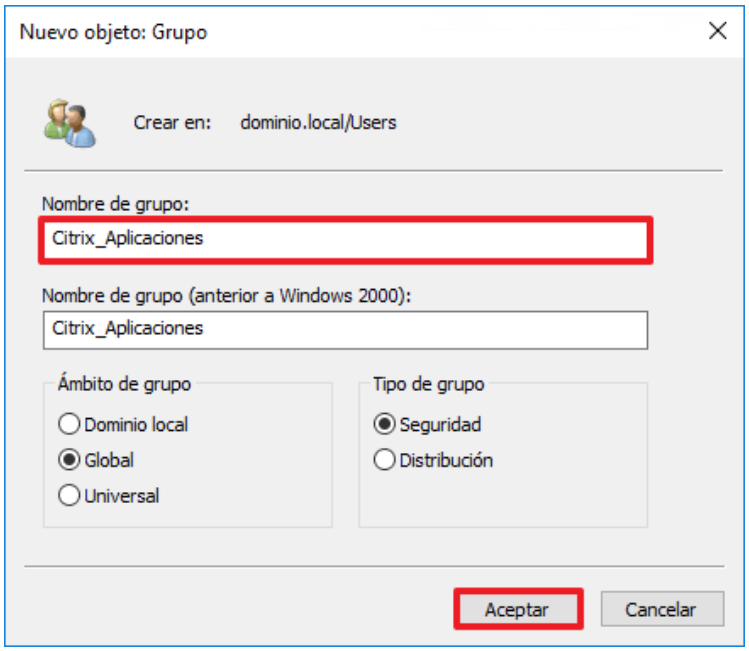
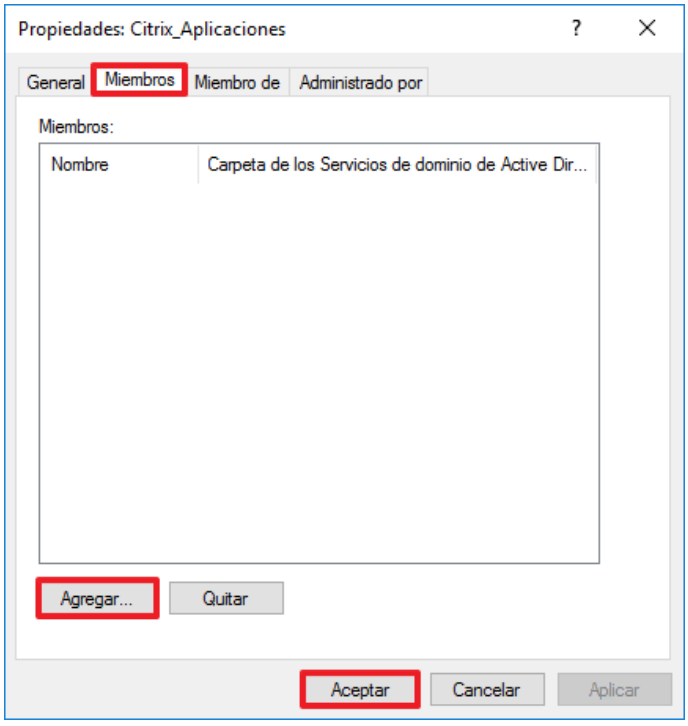
## 3. SEGREGACIÓN DE ROLES

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.

En los siguientes pasos se procederá a crear, a modo de ejemplo, un grupo de usuarios a los que se les concederá el acceso a un determinado recurso de la infraestructura.

| Paso | Descripción |
|---|---|
| 105. | Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 106. | 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.<br>  |

| Paso | Descripción |
|---|---|
| 107. | Expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"**, como se muestra en la siguiente figura.   |
| 108. | Pulsando con el botón derecho sobre "Users" diríjase al apartado de configuración **"Nuevo → Grupo"**.   |

| Paso | Descripción |
|---|---|
| 109. | Sobre la ventana emergente para la creación del nuevo grupo introduzca “Citrix_Aplicaciones” y pulse sobre “Aceptar” como se indica en la siguiente imagen.<br>  |
| 110. | A continuación, deberá agregar los usuarios que tendrán acceso al grupo de entrega de “Aplicaciones” al grupo de seguridad “Citrix_Aplicaciones”. 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”.<br>  |

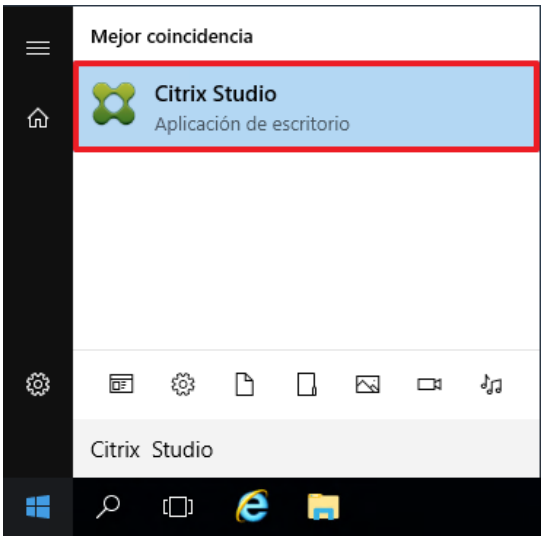
## 4. GESTIÓN DE DERECHOS DE ACCESO

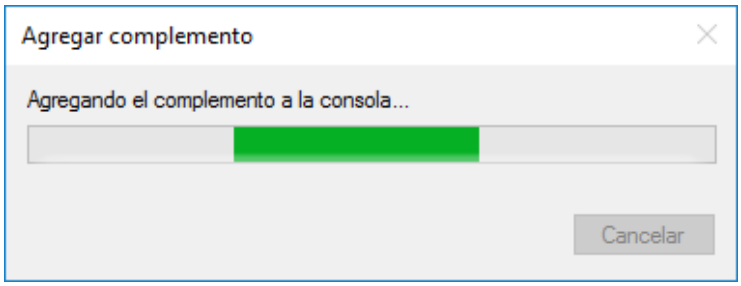
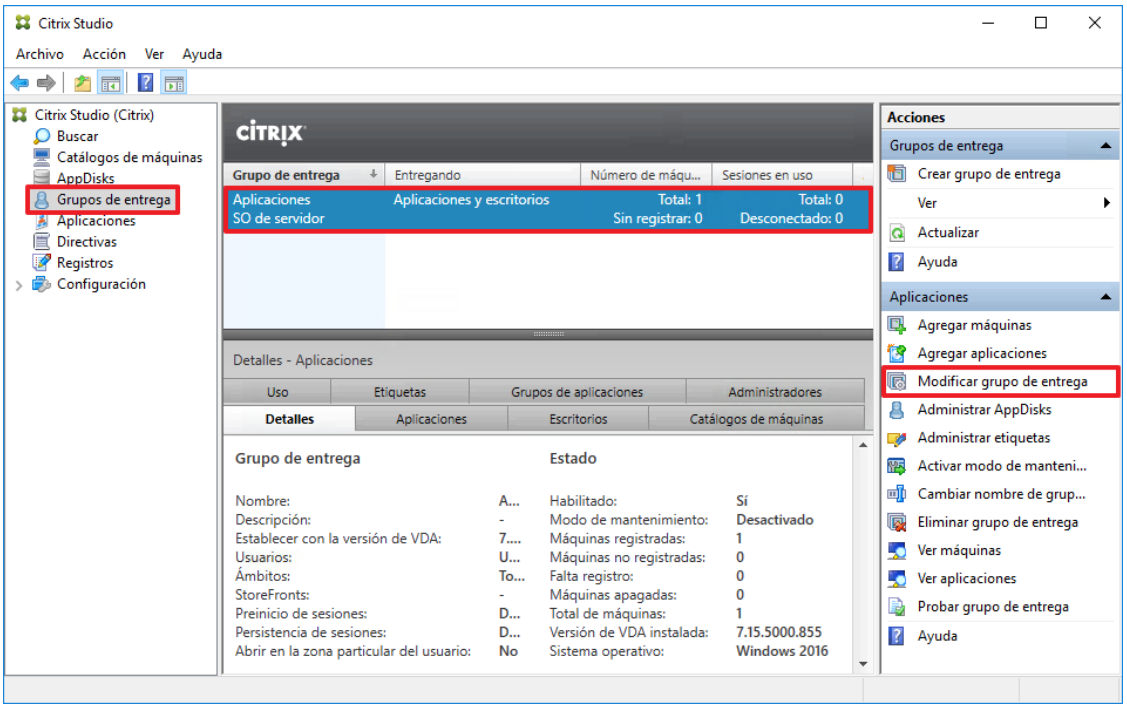
Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

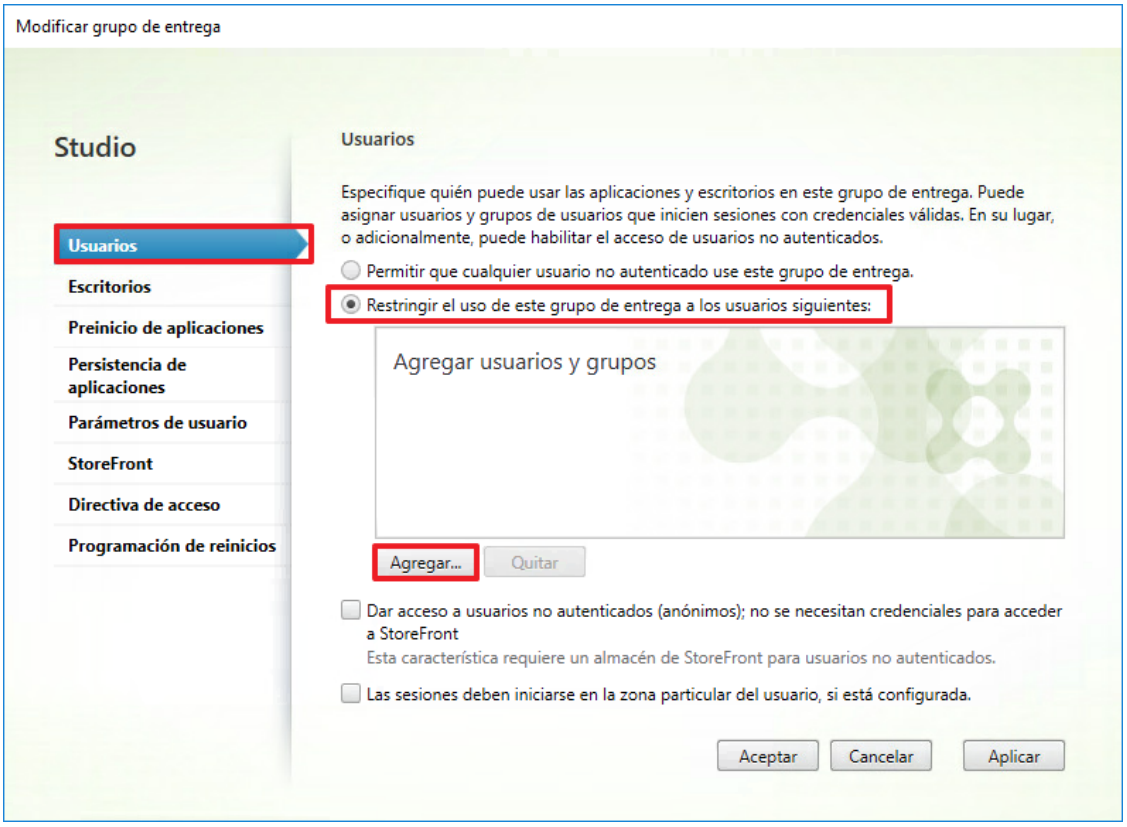
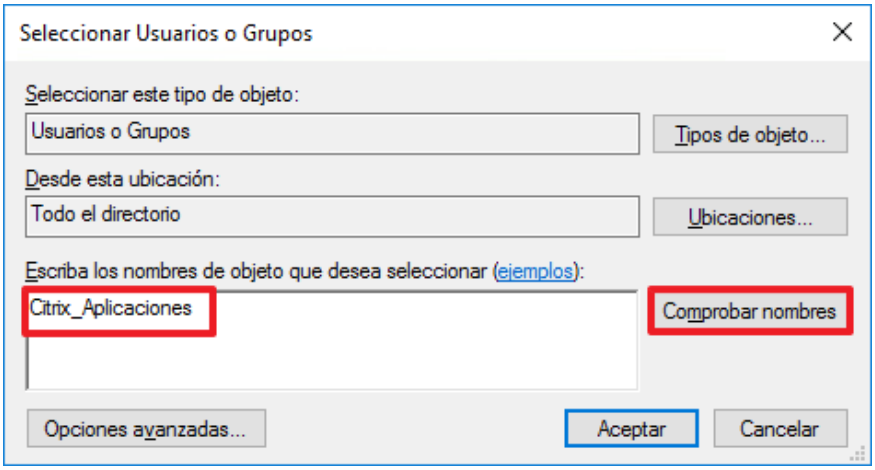
Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda acceder a recursos que no son requeridos para las funciones que desempeña.

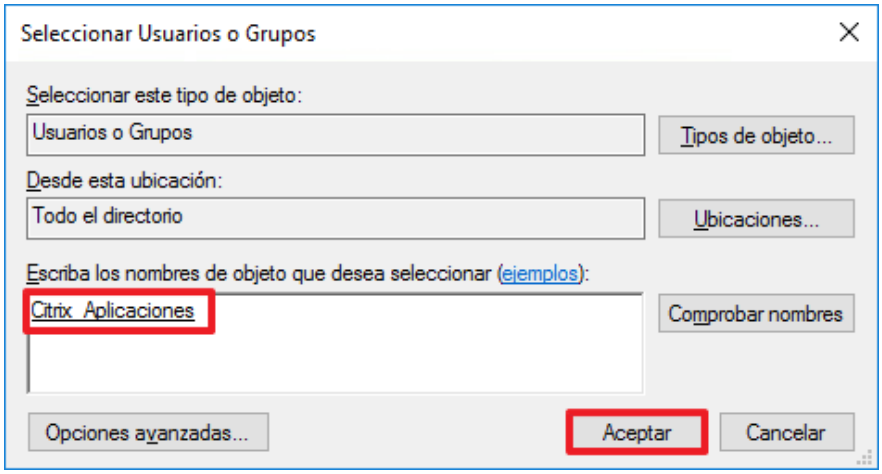
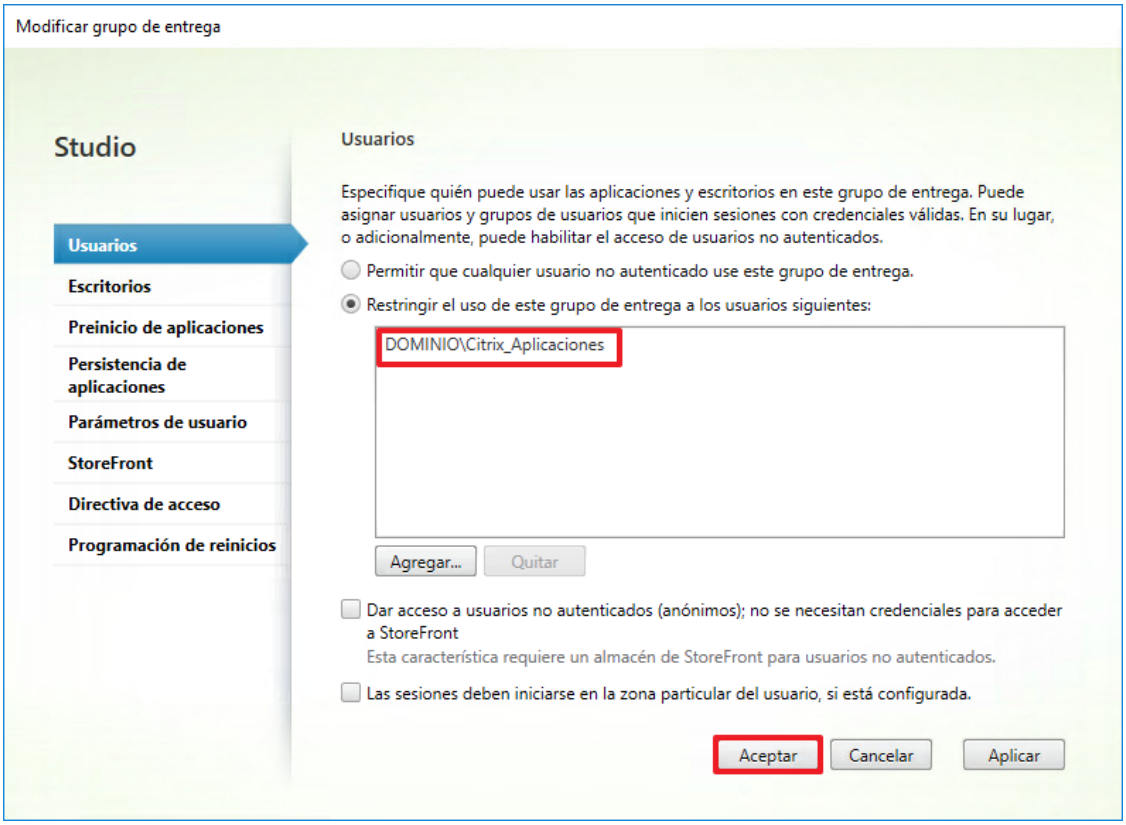
Para tal fin y de acuerdo con el Esquema Nacional de Seguridad se deberán definir, mediante grupos de seguridad, los usuarios que tengan acceso a los recursos de la infraestructura.

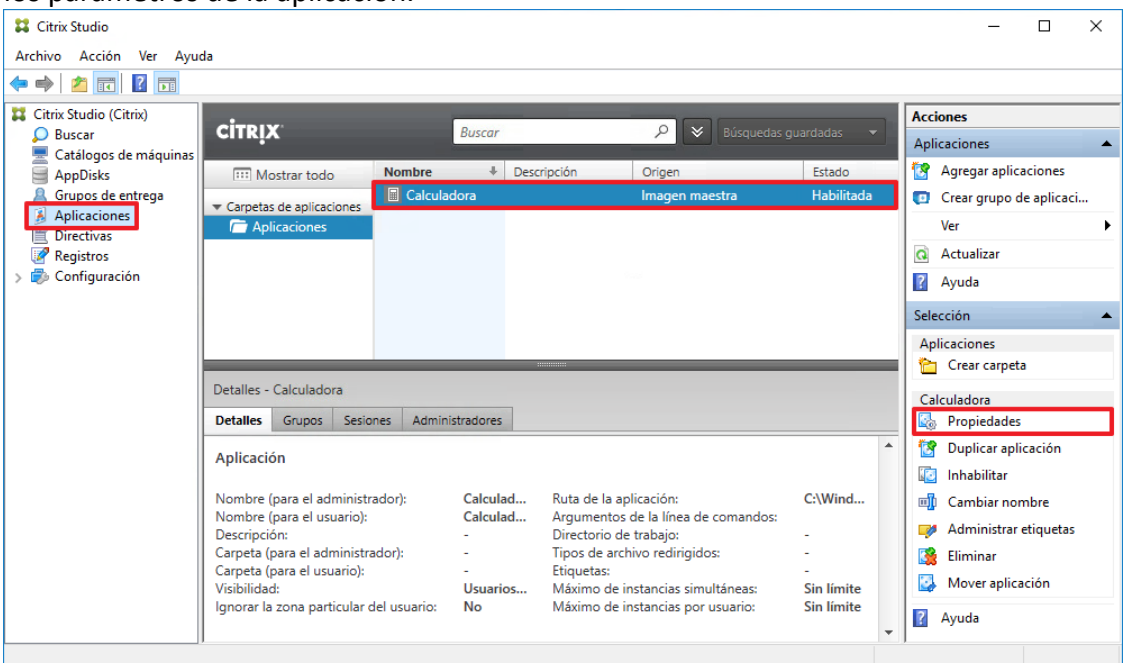
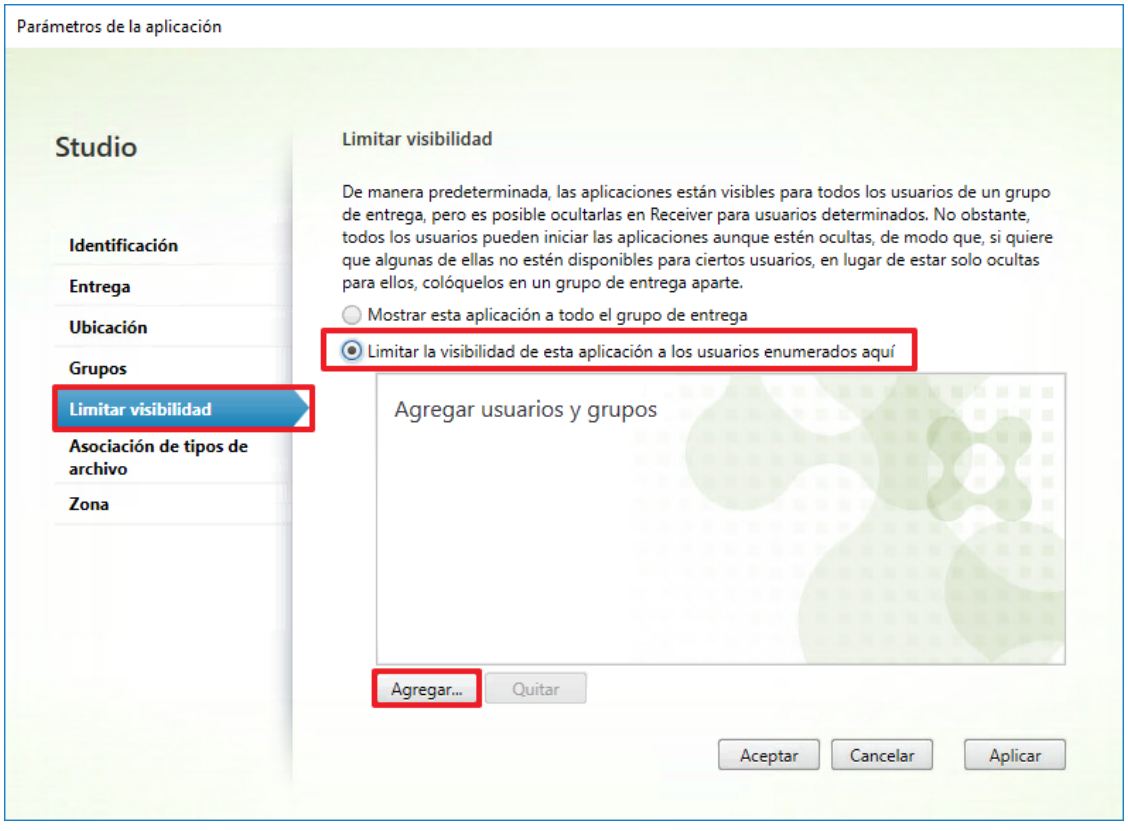
Esta configuración será de aplicación en el servidor con el rol Citrix Controller mediante la consola de administración Citrix Studio. Se limitarán, mediante grupos de seguridad, los usuarios con acceso a los diferentes grupos de entrega de la infraestructura de Citrix Virtual Apps and Desktops.

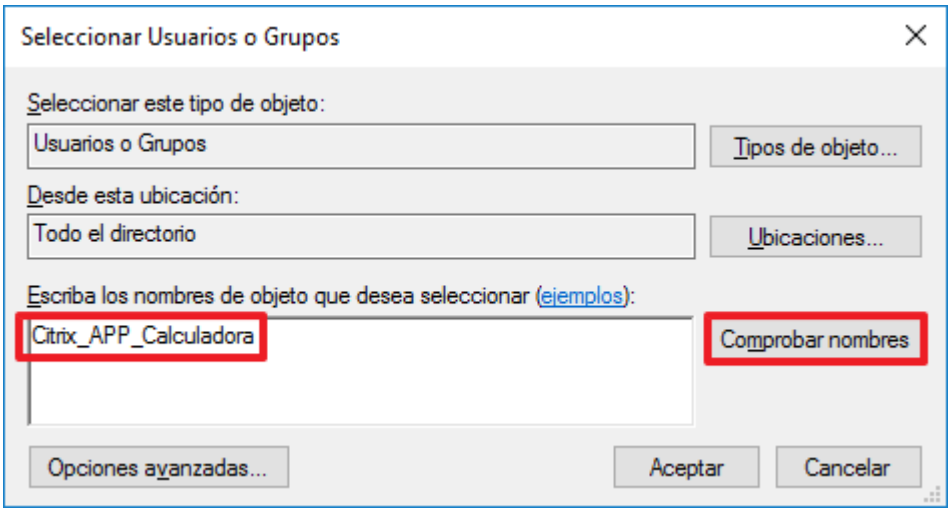
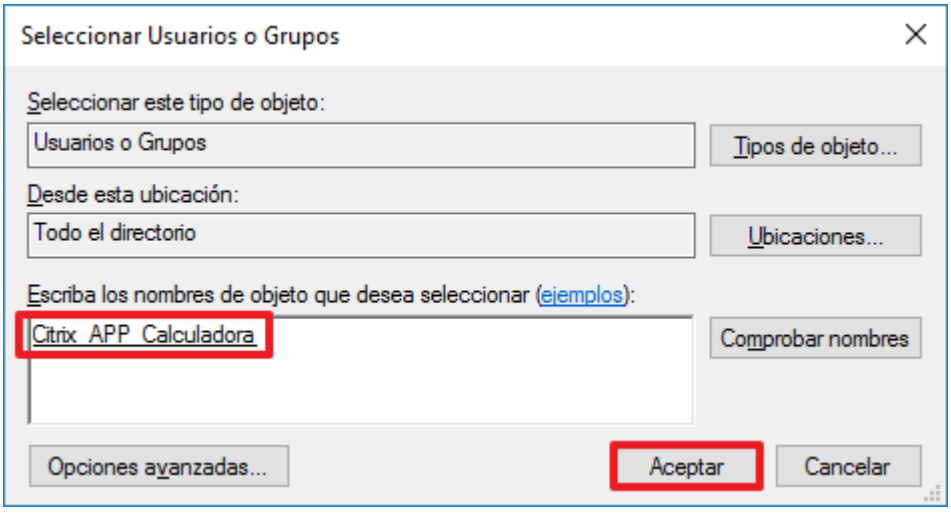
| Paso | Descripción |
|---|---|
| 111. | Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 112. | Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.<br>  <br>**Nota:** El sistema solicitará elevación de privilegios. |

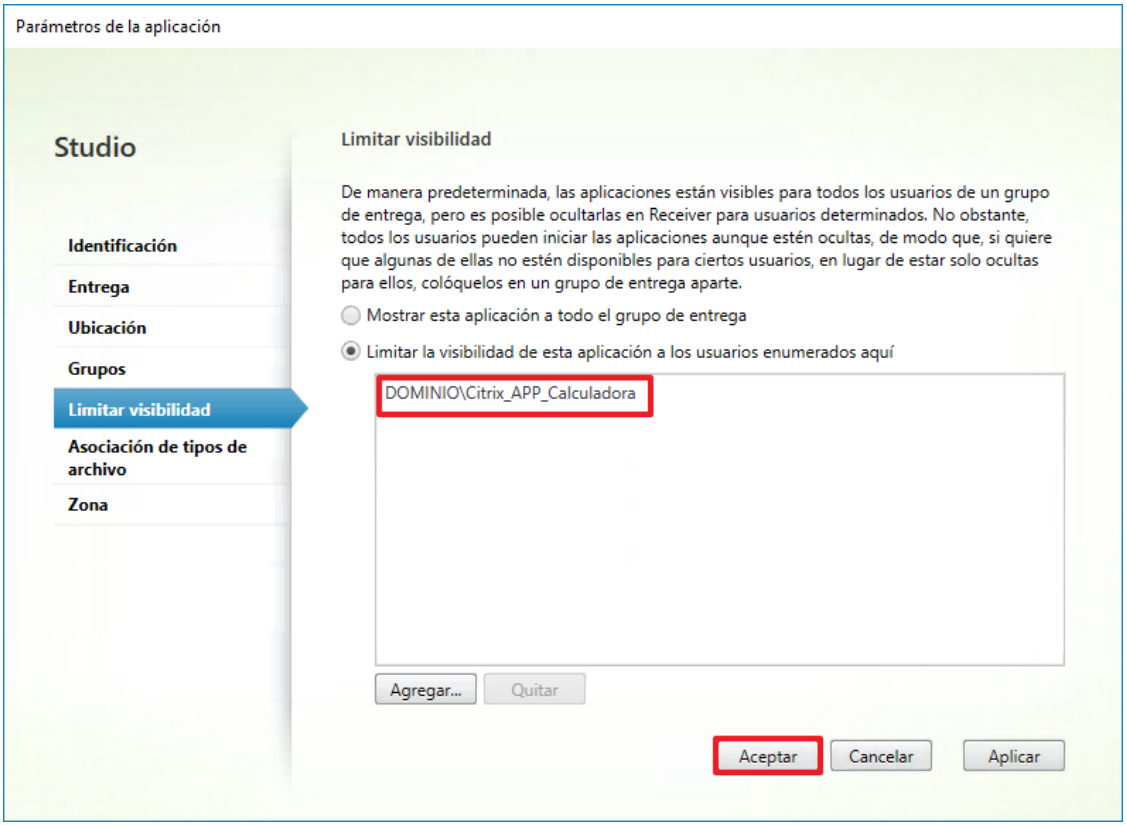
| Paso | Descripción |
|---|---|
| 113. | Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.<br>  |
| 114. | Diríjase al menú de configuración **"Citrix Studio → Grupos de entrega → [Su grupo de entrega]"** y pulse sobre "Modificar grupo de entrega" para modificar los parámetros de su grupo de entrega.<br>  |

| Paso | Descripción |
|---|---|
| 115. | En la ventana “Modificar grupo de entrega” sitúese en la pestaña “Usuarios” y seleccionando “Restringir el uso de este grupo de entrega a los usuarios siguientes:” seleccione la opción “Agregar…”.<br>  |
| 116. | Introduzca el nombre del objeto “Citrix_Aplicaciones” y pulse sobre “Comprobar nombres”.<br>  <br>**Nota:** En esta guía se usa de ejemplo el grupo de seguridad “Citrix_Aplicaciones” adapte este paso a los requisitos de su organización. |

| Paso | Descripción |
|---|---|
| 117. | Compruebe que el objeto “Citrix_Aplicaciones” ha sido añadido correctamente. Pulse “Aceptar” para añadir el objeto y cerrar la ventana.<br>  |
| 118. | El objeto aparecerá añadido. Pulse “Aceptar” para guardar los cambios. Desde este momento, únicamente los usuarios especificados en el grupo de seguridad que acaba de añadir podrán acceder al recurso publicado.<br>  |
| 119. | Para el cumplimiento del ENS en su categoría media, será necesario así mismo restringir la visibilidad de cada una de las aplicaciones, a grupos específicos de usuarios que harán uso de las mismas. |

| Paso | Descripción |
|---|---|
| 120. | A continuación, se procederá a limitar la visibilidad de una aplicación entregada a únicamente el grupo de usuarios que harán uso de esa aplicación. Para ello, acceda al nodo **"Citrix Studio → Aplicaciones → [Su aplicación] → Propiedades"** para modificar los parámetros de la aplicación.   |
| 121. | En la ventana "Parámetros de la aplicación", sitúese en la pestaña "Limitar visibilidad", y seleccionando "Limitar la visibilidad de esta aplicación a los usuarios enumerados aquí" seleccione la opción "Agregar…".   |

| Paso | Descripción |
|---|---|
| 122. | En la ventana resultante introduzca el grupo de seguridad que engloba a los usuarios que harán uso de esta aplicación y pulse en “Comprobar nombres”.<br>  <br>**Nota:** En esta guía se usa de ejemplo el grupo de seguridad “Citrix_App_Calculadora” adapte este paso a los requisitos de su organización. |
| 123. | Una vez comprobado que el objeto existe pulse “Aceptar”.<br>  |

| Paso | Descripción |
|---|---|
| 124. | El objeto aparecerá añadido. Pulse “Aceptar” para guardar los cambios. Desde este momento, únicamente los usuarios especificados en el grupo de seguridad que acaba de añadir podrán ver la aplicación publicada.<br>  |
| 125. | En este punto los recursos se encuentran configurados para la entrega de los mismos a los usuarios de forma segura. |

## ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA PUBLICACIÓN DE APLICACIONES Y ESCRITORIOS CON CITRIX VIRTUAL APPS AND DESKTOPS

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los equipos con implementación de seguridad de categoría media.

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 tanto en el servidor con el rol Citrix Controller como en los equipos con el rol Citrix Virtual Delivery Agent.

**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 EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA”.

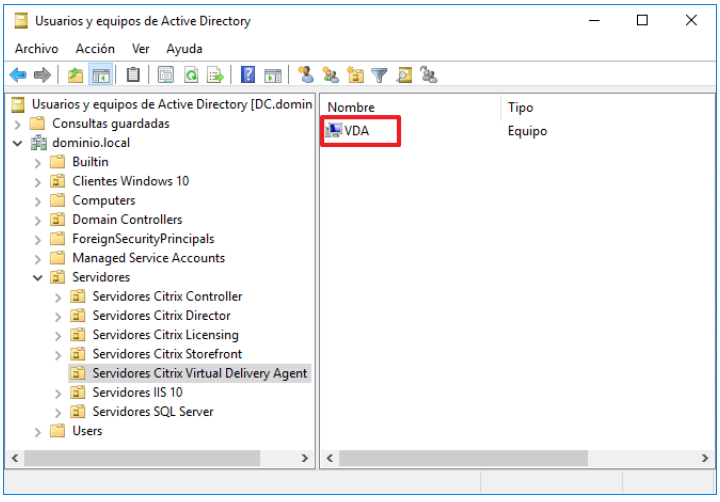
# 1. CONTROLADOR DE DOMINIO

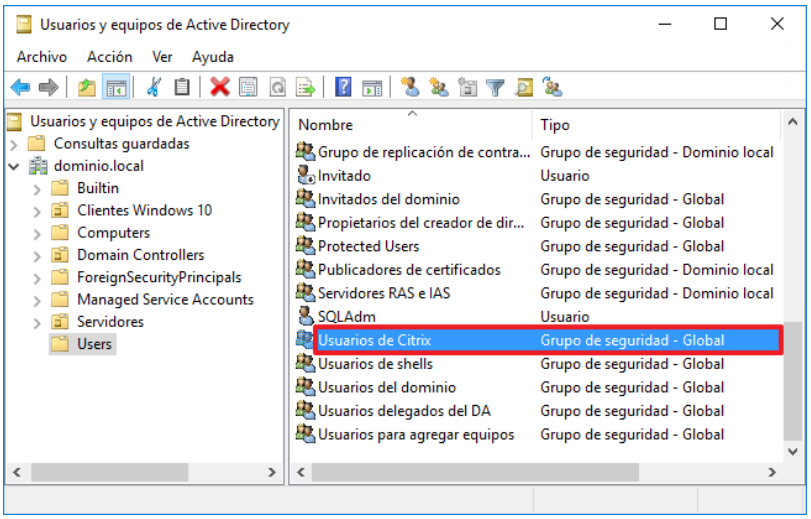
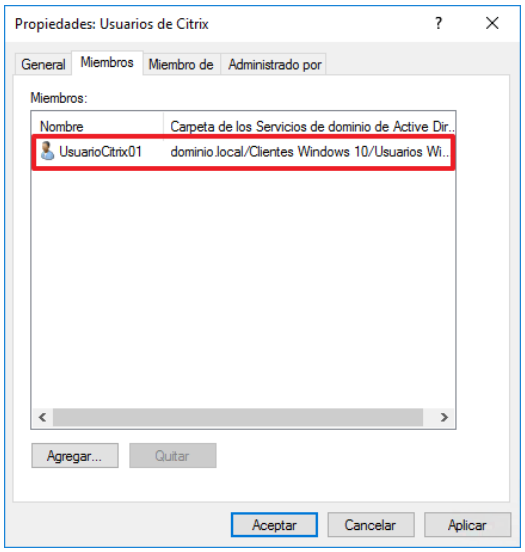
Los siguientes pasos determinan el procedimiento para verificar la configuración del dominio en el que se despliega el sistema de virtualización.

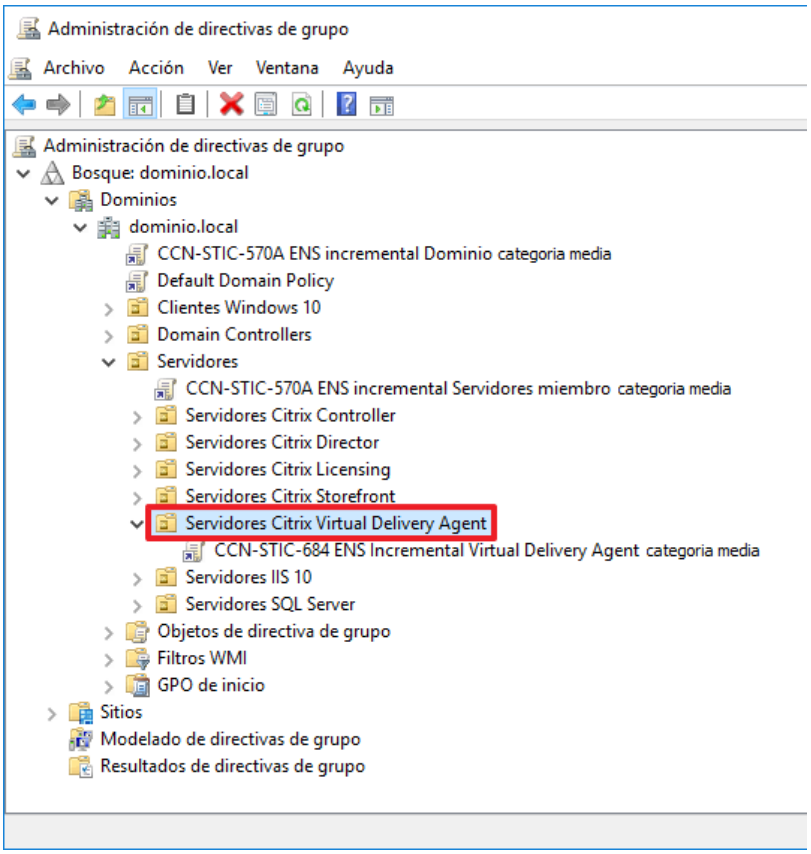
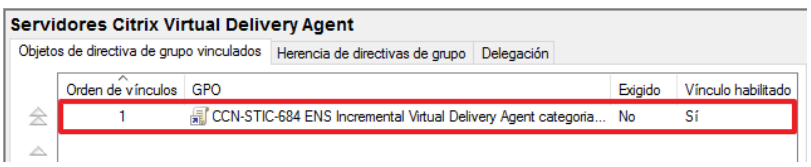
Las consolas y herramientas que se utilizarán son las siguientes:

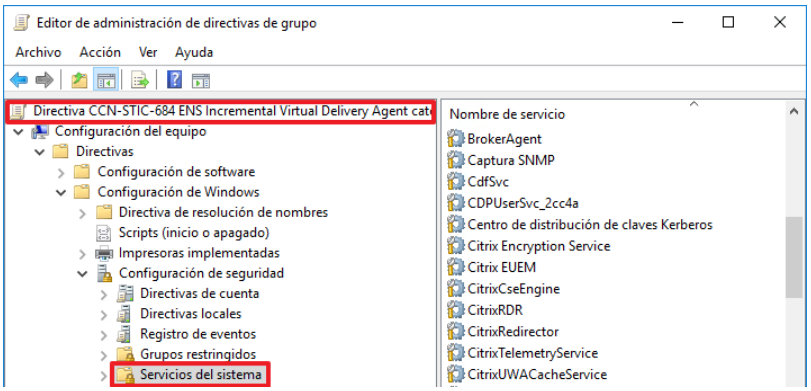
a) Usuarios y equipos de Active Directory (dsa.msc).

b) 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 equipos. | | Ejecute la herramienta "Usuarios y equipos de Active Directory" desde:<br>"**Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**".<br>El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio. |
| 3. La unidad organizativa "Servidores Citrix Virtual Delivery Agent" debe albergar todos los equipos con el rol Virtual Delivery Agent. | | En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Virtual Delivery Agent" En ella, deberá aparecer al menos un equipo.<br>  <br>**Nota:** El nombre del equipo de ejemplo es "VDA", en su caso debe figurar el nombre de su equipo. |

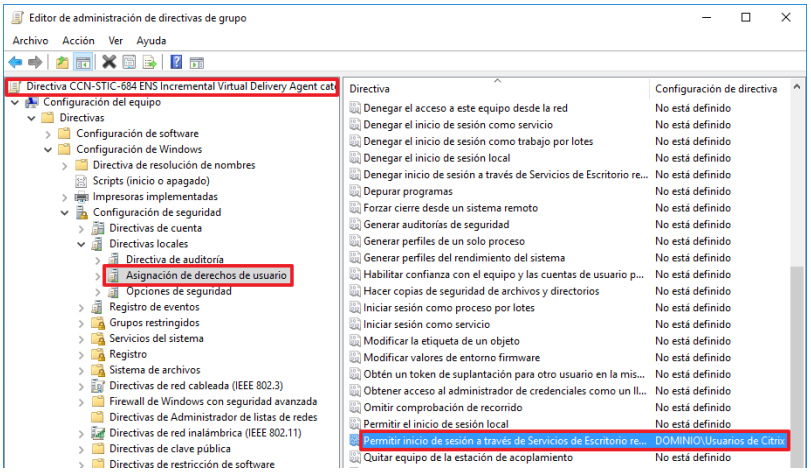
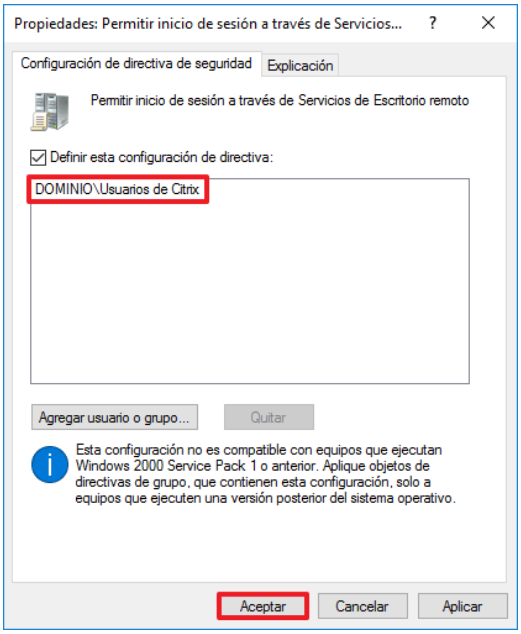
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 4. Verifique que está creado el grupo de seguridad “Usuarios de Citrix”. | | En la consola “Usuarios y equipos de Active Directory”, localice la unidad organizativa “Users” en ella, deberá aparecer el grupo de seguridad “Usuarios de Citrix”.<br>  |
| 5. Compruebe que el grupo de seguridad “Usuarios de Citrix” aloja sus respectivos usuarios. | | Compruebe que en la pestaña “Miembros” de las propiedades del grupo de seguridad “Usuarios de Citrix” se encuentran aquellos usuarios que harán uso de la infraestructura.<br>  |

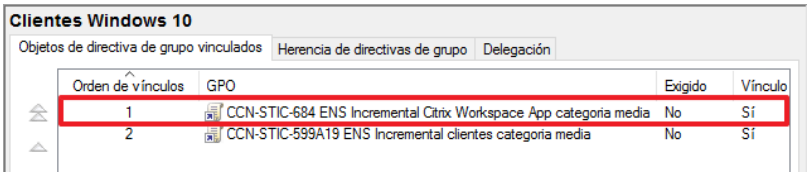
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 6. Verifique que están creadas las directivas de configuración de Citrix Virtual Delivery Agent. | | Ejecute la herramienta "Administración de directivas de grupo" desde:<br>**"Menú inicio → Herramientas administrativas → Administración de directivas de grupo"**.<br>El sistema le solicitará elevación de privilegios para acceder a la consola de administración, pulse "Sí" para continuar.<br>Seleccione la unidad organizativa "Servidores Citrix Virtual Delivery Agent", situada en **"Bosque [Su bosque] → Dominios → [Su dominio] → Servidores → Servidores Citrix Virtual Delivery Agent"**.<br>  |
| 7. Verifique las políticas aplicadas a "Servidores Citrix Virtual Delivery Agent". | | Revise que la unidad organizativa "Servidores Citrix Virtual Delivery Agent", como mínimo, tiene aplicada la siguiente directiva y tiene el vínculo habilitado.<br>– "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media"<br>  |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 8. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media". | | Pulse con el botón derecho del ratón sobre la directiva y seleccione "Editar" en el menú que se ha desplegado. Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media" tiene los siguientes valores de servicios de sistema.<br>**"CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**.<br>  <br>**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 Audio Redirection Service | CtxAudioSrv | Automático | |
| Citrix Audio Redirection Service | CtxAudioSvc | Automático | |
| Citrix CEIP Service for Vda | CitrixVdaCeipService | Deshabilitado | |
| Citrix Desktop Service | BrokerAgent | Automático | |
| Citrix Device Redirector Service | CitrixRDR | Automático | |
| Citrix Device Redirector Service | CitrixRedirector | Automático | |
| Citrix Diagnostic Facility COM Server | CdfSvc | Automático | |
| Citrix Dynamic Virtual Channel Service | PicaDvcControllerSvc | Automático | |
| Citrix Encryption Service | Citrix Encryption Service | Automático | |
| Citrix End User Experience Monitoring Service | Citrix EUEM | Automático | |
| Citrix Group Policy Engine | CitrixCseEngine | Automático | |
| Citrix HDX HTML5 Video Redirection Service | CtxHdxWebSocketService | Automático | |
| Citrix ICA Service | PorticaService | Automático | |
| Citrix Location and Sensor Virtual Channel Service | CtxSensVcSvc | Automático | |

| Comprobación | OK/NOK | Cómo hacerlo | | | |
|---|---|---|---|---|---|
| **Servicio (nombre largo)** | | **Servicio (nombre corto)** | | **Inicio** | **OK/NOK** |
| Citrix Mobile Receiver Virtual Channel Service | | MRVCSvc | | Automático | |
| Citrix Multi Touch Redirection Service | | CtxMultiTouchSvc | | Automático | |
| Citrix Print Manager Service | | cpsvc | | Automático | |
| Citrix Profile Management | | CtxProfile | | Automático | |
| Citrix Pvs for VMs agent | | PvsVmAgent | | Automático | |
| Citrix Services Manager | | ServicesManager | | Automático | |
| Citrix Smart Card Certificate Propagation Service | | CtxSCardCertPropSvc | | Automático | |
| Citrix Smart Card Removal Policy Service | | CtxScardRemovalPolicySvc | | Automático | |
| Citrix Smart Card Service | | CtxSmartCardSvc | | Automático | |
| Citrix Stack Control Service | | StackControlService | | Automático | |
| Citrix Telemetry Service | | CitrixTelemetryService | | Deshabilitado | |
| Citrix UWA Cache Service | | CitrixUWACacheService | | Automático | |
| Cola de Impresión | | Spooler | | Automático | |
| Estación de trabajo | | LanmanWorkstation | | Automático | |
| Iniciador de procesos de servidor DCOM | | DcomLaunch | | Automático | |
| Llamada a procedimiento remoto (RPC) | | RpcSs | | Automático | |
| Servicio Citrix HDX MediaStream para Flash | | CtxFlashSvc | | Automático | |
| Servicio Informe de errores de Windows | | WerSvc | | Automático | |
| Servicio Interfaz de almacenamiento en red | | nsi | | Automático | |
| Servicios de Escritorio Remoto | | TermService | | Manual | |
| Solicitante de instantaneas de volumen de Hyper-V | | vmicvss | | Manual | |
| 9. Verifique los valores de asignación de derechos de usuario de la directiva “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media”. | | Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media” tiene configurados los valores de asignación de derechos de usuario. **“CCN-STIC-684 Incremental Virtual Delivery Agent categoria media → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad →Directivas locales → Asignación de derechos de usuario”**. | | | |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| | |  <br>Compruebe que la directiva “Permitir inicio de sesión a través de Servicios de Escritorio remoto” se encuentra definida y que al menos muestra el grupo “Usuarios de Citrix”.<br>  |
| 10. Verifique los valores de Opciones de inicio de sesión de Windows de la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media". | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-684 Incremental Virtual Delivery Agent" tiene los siguientes valores en la siguiente ubicación:<br>**“Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”.**<br>Tras la comprobación, cierre el “Editor de administración de directivas de grupo”. |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario.</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>11. Verifique las políticas aplicadas a “Clientes Windows 10”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Clientes Windows 10”, situada en “Bosque [Su bosque] → Dominios → [Su dominio] → Clientes Windows 10” y revise que, como mínimo, tiene aplicada la siguiente directiva, tiene el vínculo habilitado y se encuentra situada en primer lugar.<br>– “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”<br> 
</td></tr>
<tr><td rowspan="3">12. Verifique los valores para Actualizaciones de Citrix Workspace de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td colspan="3">Pulse con el botón derecho del ratón sobre la directiva y seleccione “Editar” en el menú que se ha desplegado. Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Actualizaciones de Citrix Workspace”.</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Actualizaciones de Citrix Workspace</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>13. Verifique los valores para autoservicio de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Autoservicio”.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">EnableFTU</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir a los usuarios agregar o quitar cuentas</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir/impedir que los usuarios publiquen contenido no seguro</td><td>Habilitada (Impedir)</td><td></td></tr>
<tr><td rowspan="4">14. Verifique los valores para CEIP de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → CEIP”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Configuración de CEIP</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar CEIP</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="3">15. Verifique los valores para Conformidad de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Conformidad”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Inhabilitar el envío de datos a terceros</td><td>Habilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="3">16. Verifique los valores para Diagnóstico de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Diagnóstico”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Seguimiento permanente</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="9">17. Verifique los valores para Uso remoto de dispositivos del cliente de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Uso remoto de dispositivos del cliente”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Acceso al hardware del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Asignación de unidades del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Captura de imágenes</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Dispositivos Plug-n-Play USB</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Impresoras del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Micrófono del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Portapapeles</td><td>Deshabilitada</td><td></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>18. Verifique los valores para Uso remoto de USB genérico de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media”.</td><td></td><td>Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria media → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Uso remoto de dispositivos del cliente → Uso remoto de USB genérico”.<br>Tras la comprobación, cierre el “Editor de administración de directivas de grupo”.</td></tr>
<tr><td colspan="3">
<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Dispositivos USB existentes</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Dispositivos USB nuevos</td><td>Deshabilitado</td><td></td></tr>
<tr><td>EnableUSBForceRedirection</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Lista de dispositivos USB en Desktop Viewer</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Quitar en bloqueo</td><td>Habilitado</td><td></td></tr>
<tr><td>Redirigir dispositivos USB desconocidos</td><td>Deshabilitado</td><td></td></tr>
</table>
</td></tr>
</table>

## 2. CITRIX CONTROLLER

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el servidor con el rol Citrix Controller de la infraestructura.

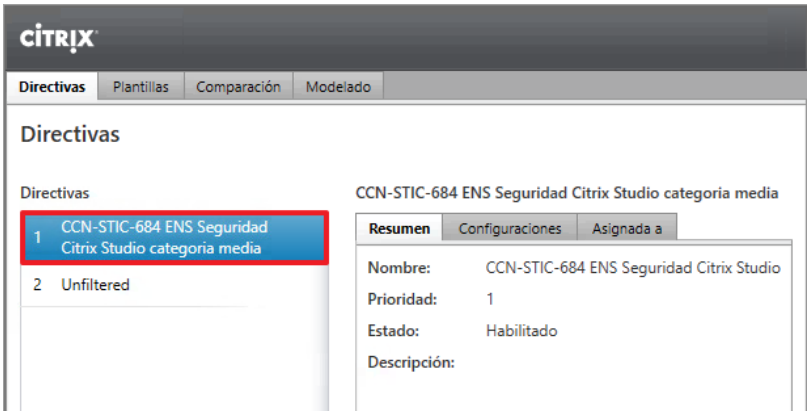
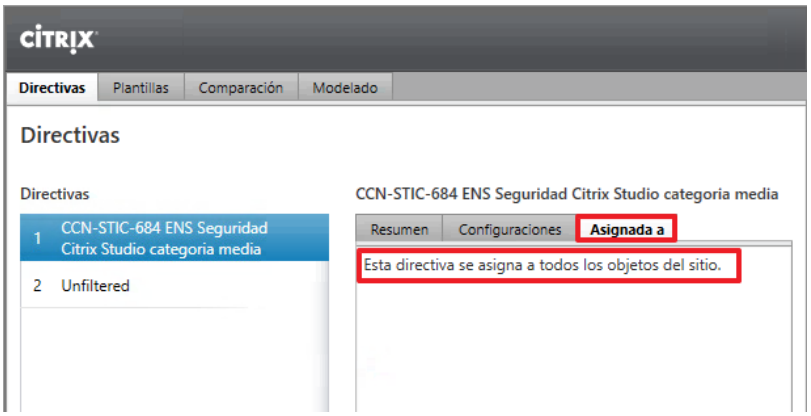
Las consolas y herramientas que se utilizarán son las siguientes:

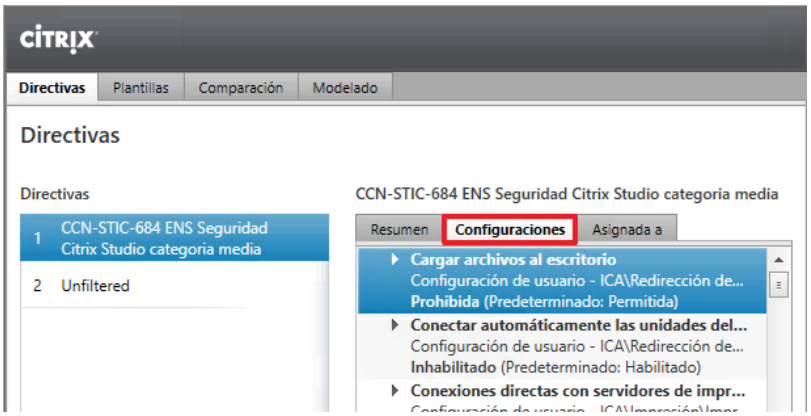
a) Citrix Studio.

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

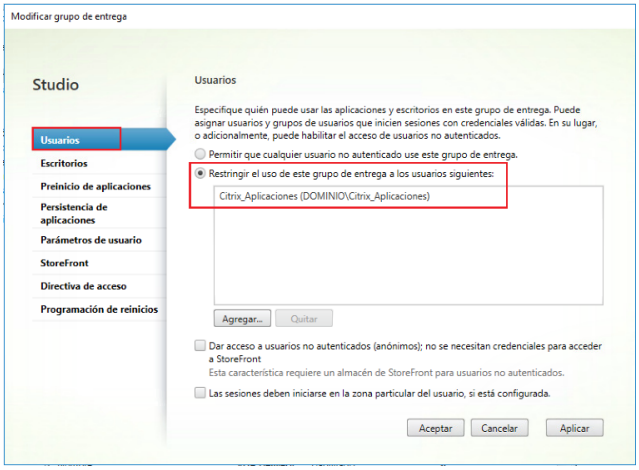
**Nota:** Deberá ejecutar los siguientes pasos de comprobación en el servidor con el rol Citrix Controller que haya sido preparado siguiendo esta guía de seguridad.

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 19. Inicie sesión en un servidor con el rol Citrix Controller | | Inicie sesión en un servidor con el rol Citrix Controller, con una cuenta de administrador del dominio. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 20. Verifique que están creadas las directivas de seguridad de Citrix Studio. | | Ejecute la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Directivas"** y compruebe que la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria media" está creada.<br>  |
| 21. Verifique la configuración de la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria media". | | Verifique que la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria media" se encuentra configurada con la prioridad 1 y que el estado de la misma es "Habilitado".<br>  |
| 22. Verifique la asignación de la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria media". | | Verifique que la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria media" se encuentra asignada a todos los objetos del sitio.<br>  |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>23. Verifique las configuraciones de la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria media”.</td><td></td><td>Verifique que la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria media” tiene los siguientes valores configurados.<br> 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cargar archivos al escritorio</td><td>Prohibida</td><td></td></tr>
<tr><td>Conectar automáticamente las unidades del cliente</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Conexiones directas con servidores de impresión</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Crear automáticamente la impresora universal de PDF</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Crear automáticamente las impresoras del cliente</td><td>No crear automáticamente las impresoras del cliente</td><td></td></tr>
<tr><td>Crear automáticamente una impresora universal genérica</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Descargar archivos desde el escritorio</td><td>Prohibida</td><td></td></tr>
<tr><td>Impresoras del cliente retenidas o restauradas</td><td>Prohibida</td><td></td></tr>
<tr><td>Instalación automática de controladores de impresora</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Permitir transferencia de archivos entre escritorio y cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de dispositivos TWAIN del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de dispositivos USB del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de dispositivos USB Plug and Play del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de impresoras del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de puertos COM del cliente</td><td>Prohibida</td><td></td></tr>
</table></td></tr>
</table>

| Comprobación | OK/NOK | Cómo hacerlo | | |
|---|---|---|---|---|
| | | Directiva | Valor | OK/NOK |
| | | Redirección de puertos LPT del cliente | Prohibida | |
| | | Redirección de unidades del cliente | Prohibida | |
| | | Redirección del host al cliente | Inhabilitado | |
| | | Redirección del portapapeles del cliente | Prohibida | |
| | | Unidades de disco flexibles del cliente | Prohibida | |
| | | Unidades de red del cliente | Prohibida | |
| | | Unidades extraíbles del cliente | Prohibida | |
| | | Unidades fijas del cliente | Prohibida | |
| | | Unidades ópticas del cliente | Prohibida | |
| 24. Verifique los derechos de acceso a los recursos. | | Ejecute la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Grupos de entrega"** y sobre cada uno de los grupos de entrega verifique que se encuentra restringido el uso de estos a los grupos de seguridad definidos por su organización. Para ello, pulse el botón derecho sobre cada grupo de entrega y seleccione "Modificar Grupo de entrega".   | | |

## 3. CLIENTE CON INSTALACIÓN DE VIRTUAL DELIVERY AGENT

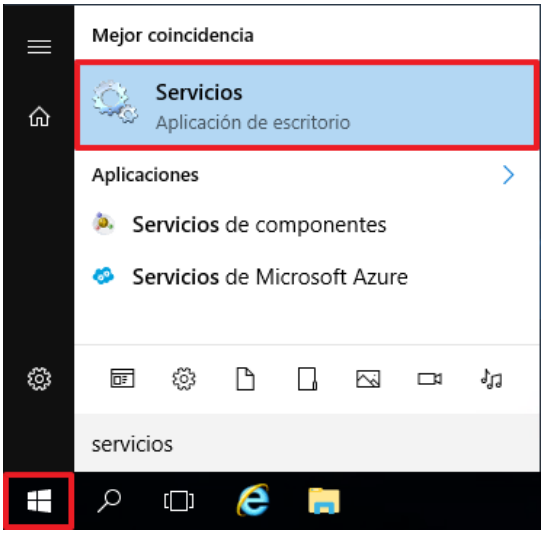
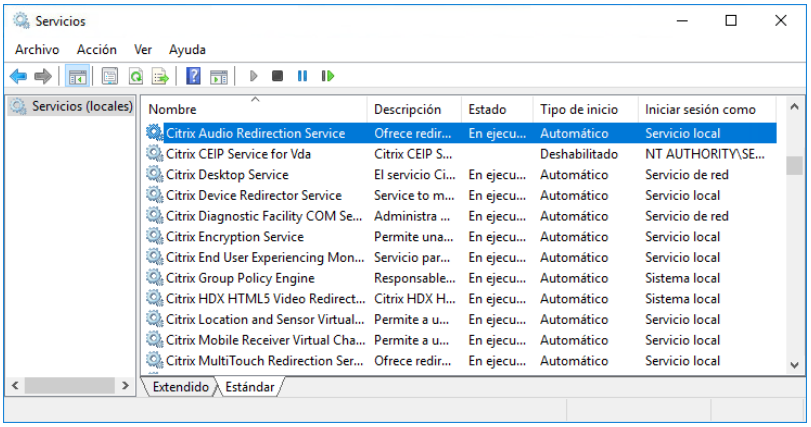
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el equipo en el que se ha desplegado el agente Virtual Delivery Agent, y las configuraciones propias implementadas sobre este equipo.

Las consolas y herramientas que se utilizarán son las siguientes:

a) Servicios (services.msc).

El siguiente procedimiento verifica la configuración del equipo con el rol Virtual Delivery Agent.

**Nota:** Deberá ejecutar los siguientes pasos de comprobación en el equipo con el rol Virtual Delivery Agent que haya sido preparado e instalado siguiendo esta guía de seguridad.

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 25. Inicie sesión en un equipo con el rol Virtual Delivery Agent. | | En un equipo con el rol Virtual Delivery Agent, inicie sesión con una cuenta que tenga privilegios de administración del dominio. |
| 26. Ejecución de la consola de servicios. | | Pulse sobre el botón de "Inicio" o el buscador y teclee "Servicios", seleccione la herramienta que aparece. El sistema solicitará elevación de privilegios. Pulse "Sí" para continuar.<br>  |
| 27. Sobre cada uno de los equipos con el rol Virtual Delivery Agent revise los servicios implementados y su estado. | | Compruebe que el valor de inicio de los servicios se ha configurado correctamente.<br>  <br>**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. Por tanto, es posible que alguno de los servicios no figure. Compruebe que el estado de los que figuran sea el indicado en la siguiente tabla. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|

| Servicio (nombre largo) | Servicio (nombre corto) | Inicio | OK/NOK |
|---|---|---|---|
| Asignador de extremos de RPC | RpcEptMapper | Automático | |
| Citrix Audio Redirection Service | CtxAudioSrv | Automático | |
| Citrix Audio Redirection Service | CtxAudioSvc | Automático | |
| Citrix CEIP Service for Vda | CitrixVdaCeipService | Deshabilitado | |
| Citrix Desktop Service | BrokerAgent | Automático | |
| Citrix Device Redirector Service | CitrixRDR | Automático | |
| Citrix Device Redirector Service | CitrixRedirector | Automático | |
| Citrix Diagnostic Facility COM Server | CdfSvc | Automático | |
| Citrix Dynamic Virtual Channel Service | PicaDvcControllerSvc | Automático | |
| Citrix Encryption Service | Citrix Encryption Service | Automático | |
| Citrix End User Experience Monitoring Service | Citrix EUEM | Automático | |
| Citrix Group Policy Engine | CitrixCseEngine | Automático | |
| Citrix HDX HTML5 Video Redirection Service | CtxHdxWebSocketService | Automático | |
| Citrix ICA Service | PorticaService | Automático | |
| Citrix Location and Sensor Virtual Channel Service | CtxSensVcSvc | Automático | |
| Citrix Mobile Receiver Virtual Channel Service | MRVCSvc | Automático | |
| Citrix Multi Touch Redirection Service | CtxMultiTouchSvc | Automático | |
| Citrix Print Manager Service | cpsvc | Automático | |
| Citrix Profile Management | CtxProfile | Automático | |
| Citrix Pvs for VMs agent | PvsVmAgent | Automático | |
| Citrix Services Manager | ServicesManager | Automático | |
| Citrix Smart Card Certificate Propagation Service | CtxSCardCertPropSvc | Automático | |
| Citrix Smart Card Removal Policy Service | CtxScardRemovalPolicySvc | Automático | |
| Citrix Smart Card Service | CtxSmartCardSvc | Automático | |
| Citrix Stack Control Service | StackControlService | Automático | |
| Citrix Telemetry Service | CitrixTelemetryService | Deshabilitado | |
| Citrix UWA Cache Service | CitrixUWACacheService | Automático | |
| Cola de Impresión | Spooler | Automático | |
| Estación de trabajo | LanmanWorkstation | Automático | |
| Iniciador de procesos de servidor DCOM | DcomLaunch | Automático | |
| Llamada a procedimiento remoto (RPC) | RpcSs | Automático | |
| Servicio Citrix HDX MediaStream para Flash | CtxFlashSvc | Automático | |
| Servicio Informe de errores de Windows | WerSvc | Automático | |
| Servicio Interfaz de almacenamiento en red | nsi | Automático | |
| Servicios de Escritorio Remoto | TermService | Manual | |
| Solicitante de instantaneas de volumen de Hyper-V | vmicvss | Manual | |

# ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

## ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS 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 tengan que asegurar aplicaciones y escritorios virtualizados mediante Citrix Virtual Apps and Desktops, 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 los equipos sobre los que implementarán 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.

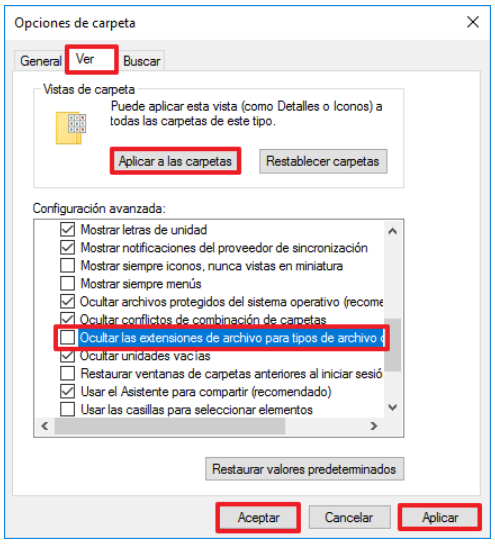
Se asume que ha realizado la implementación de las siguientes guías de seguridad sobre el dominio donde se va a aplicar el siguiente paso a paso:

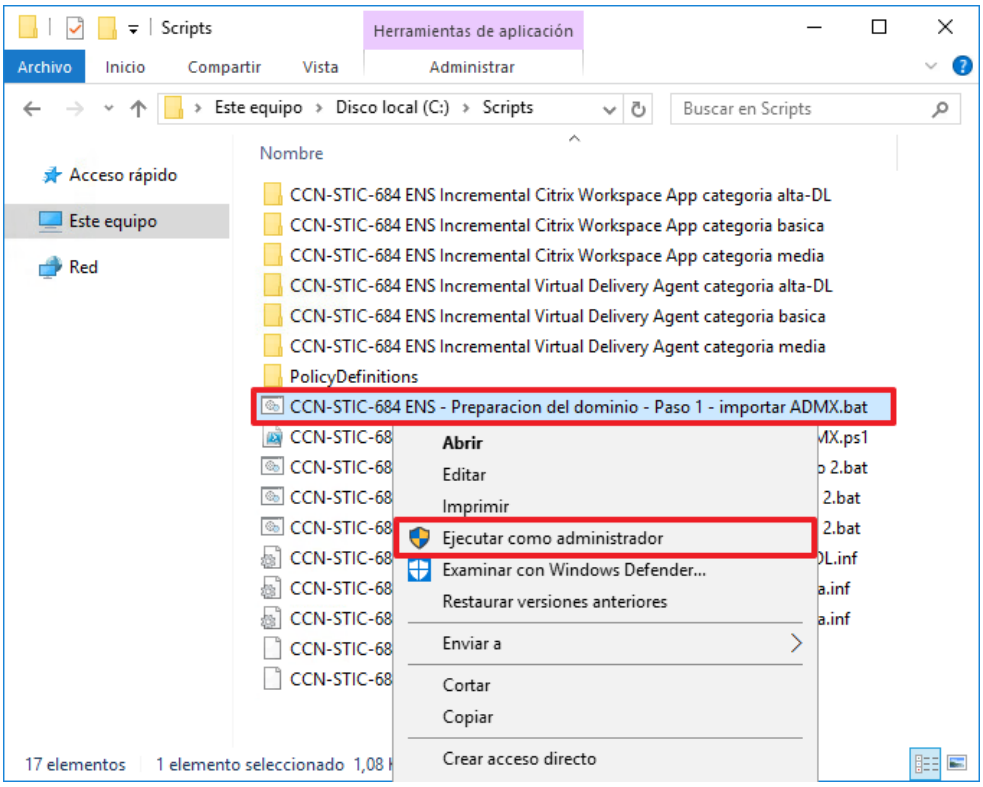
a) CCN-STIC-570A Anexo A Controlador de dominio – Categoría Alta / Difusión Limitada

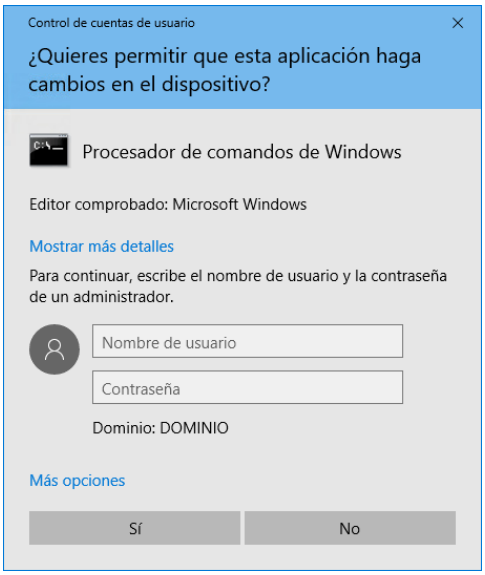
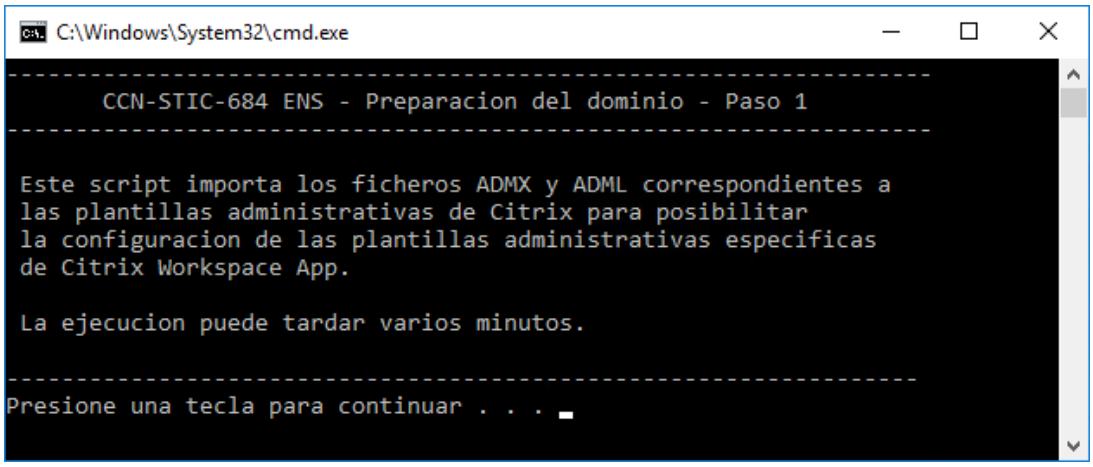
b) CCN-STIC-570A Anexo A Servidor miembro – Categoría Alta / Difusión Limitada

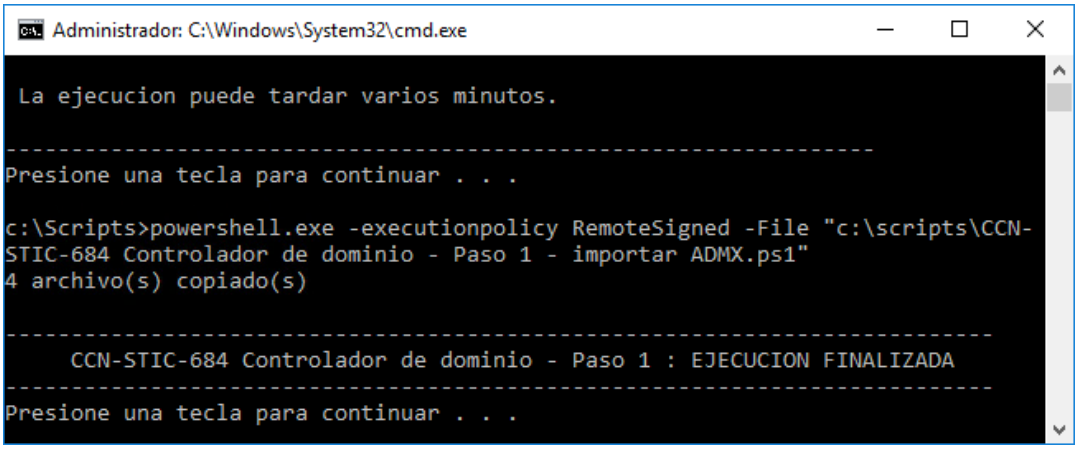
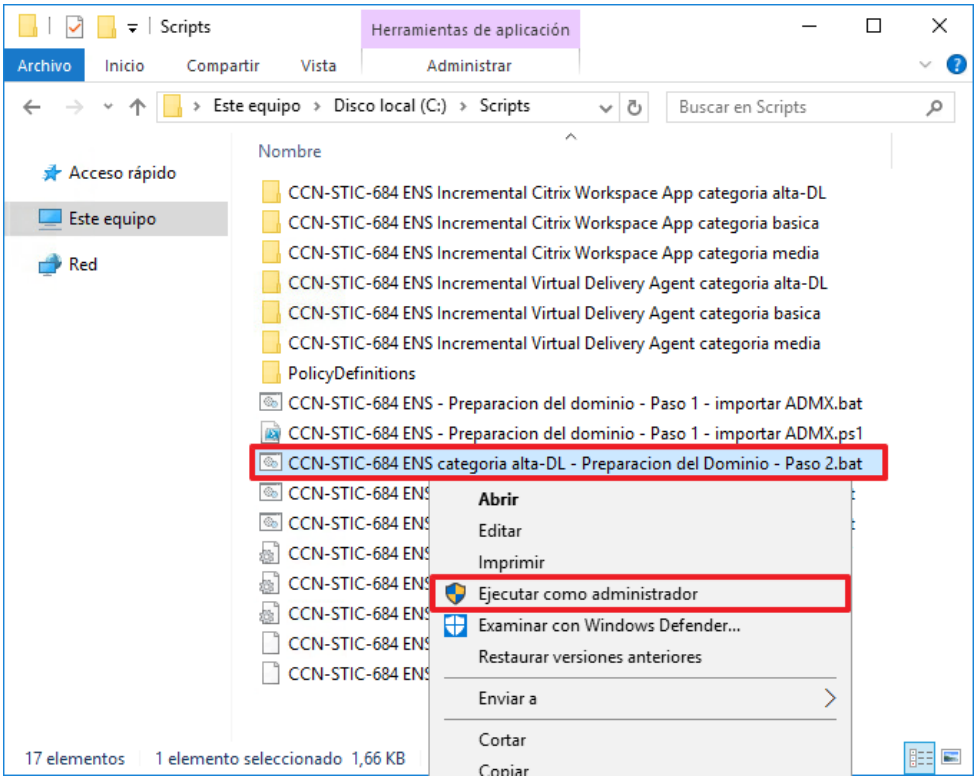
c) CCN-STIC-599A19 Anexo A – Categoría Alta / Difusión Limitada

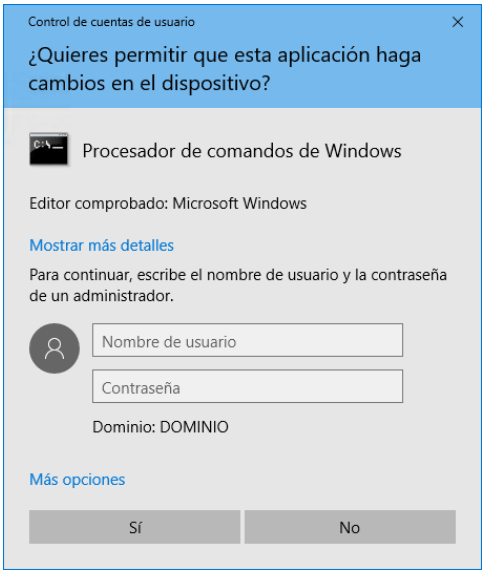
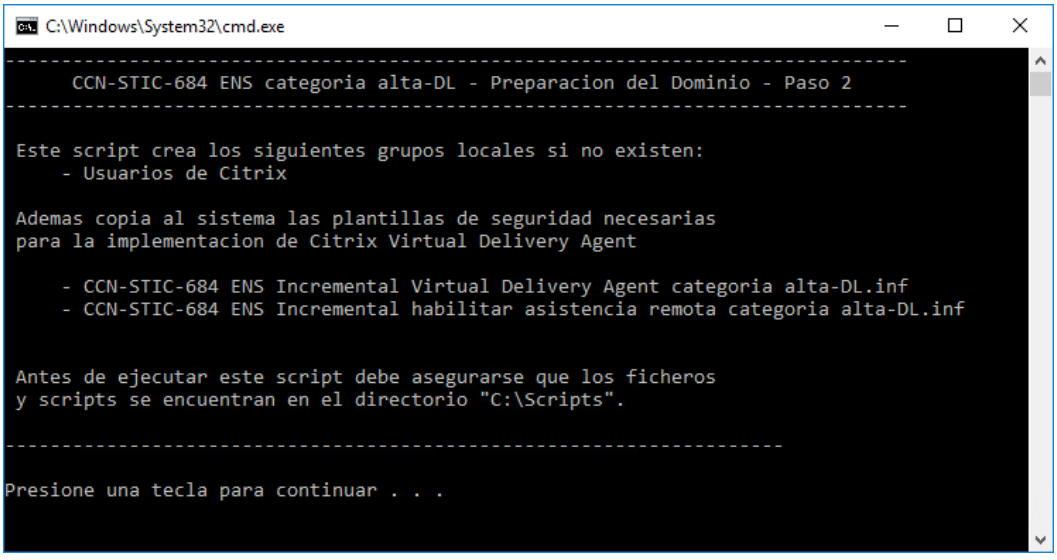
d) CCN-STIC-683 – Categoría Alta / Difusión Limitada

| Paso | Descripción |
|---|---|
| 1. | Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 2. | Cree el directorio “Scripts” en la unidad “C:\”.<br>**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.<br>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:<br>  |
| 5. | Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta". |

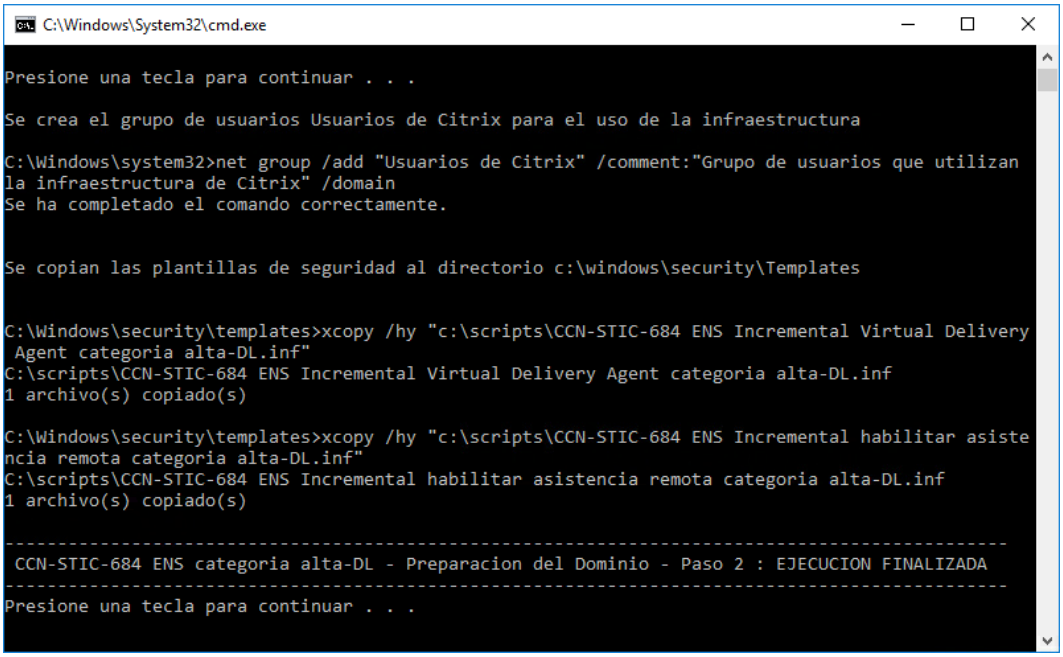
| Paso | Descripción |
|---|---|
| 6. | Asegúrese de que al menos los siguientes ficheros hayan sido copiados al directorio “C:\Scripts” del controlador de dominio:<br>– CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta-DL (Directorio)<br>– CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta-DL (Directorio)<br>– PolicyDefinitions (Directorio)<br>– CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.bat<br>– CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.ps1<br>– CCN-STIC-684 ENS categoria alta-DL - Preparacion del Dominio - Paso 2.bat<br>– CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta-DL.inf<br>– CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta-DL.inf |
| 7. | Ejecute con privilegios de administrador (opción "Ejecutar como administrador") el script "CCN-STIC-684 ENS - Preparacion del dominio - Paso 1 - importar ADMX.bat". Para ello, visualice la carpeta “C:\Scripts” en el explorador de Windows, marque con el botón derecho el script y seleccione la opción **"Ejecutar como administrador"** del menú contextual, como se muestra en la siguiente figura.<br>  <br>**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.<br>Si el directorio principal de Windows no se encuentra en “C:\Windows”, sustituya "C:\Windows" por la ubicación correspondiente dentro de los archivos de configuración. |

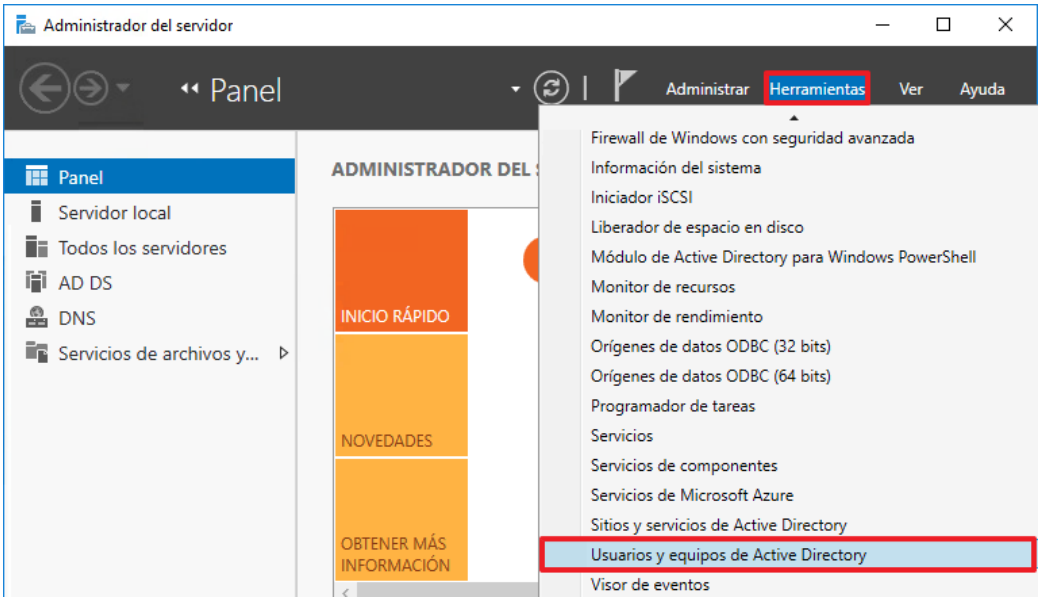
| Paso | Descripción |
|---|---|
| 8. | El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración del dominio y pulse “Sí” para continuar.<br>  |
| 9. | Pulse una tecla para ejecutar el script que añadirá las definiciones de las plantillas administrativas relativas a Citrix Workspace App en el controlador de dominio.<br>  |

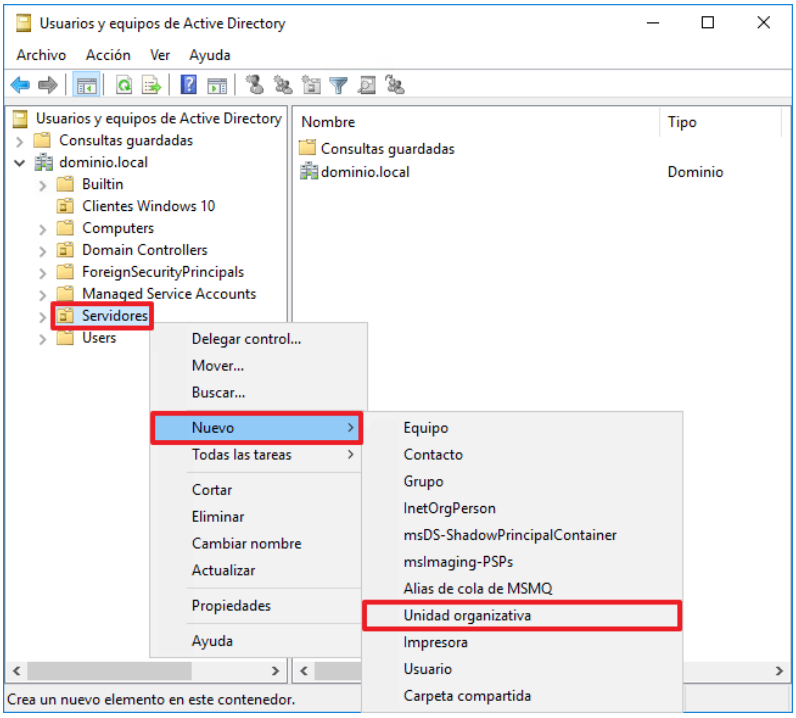
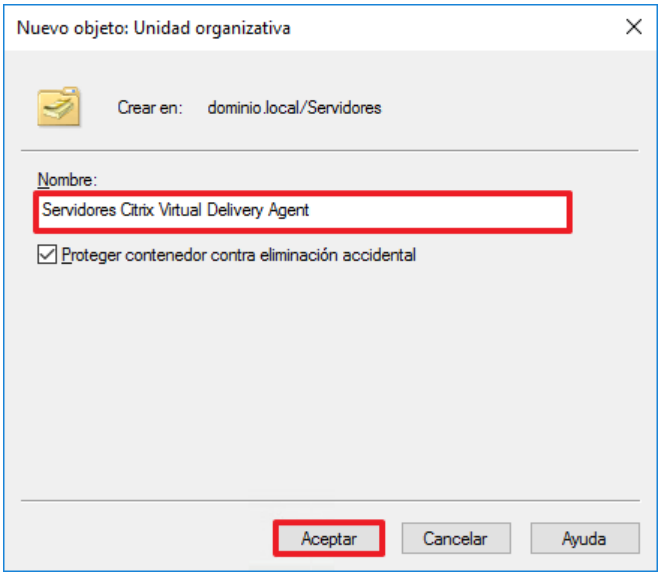
| Paso | Descripción |
|---|---|
| 10. | Una vez termine la ejecución del script, pulse una tecla para cerrar la ventana.<br>  |
| 11. | De igual forma, ejecute con privilegios de administrador (opción “Ejecutar como administrador”) el script “CCN-STIC-684 ENS categoria alta-DL - Preparacion del Dominio - Paso 2.bat.<br>  |

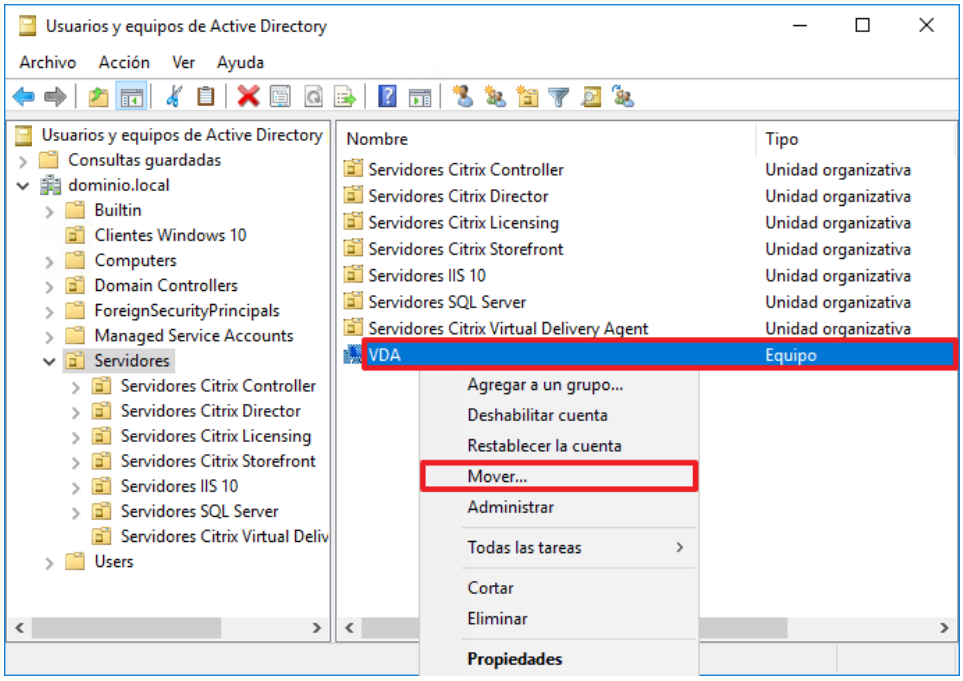
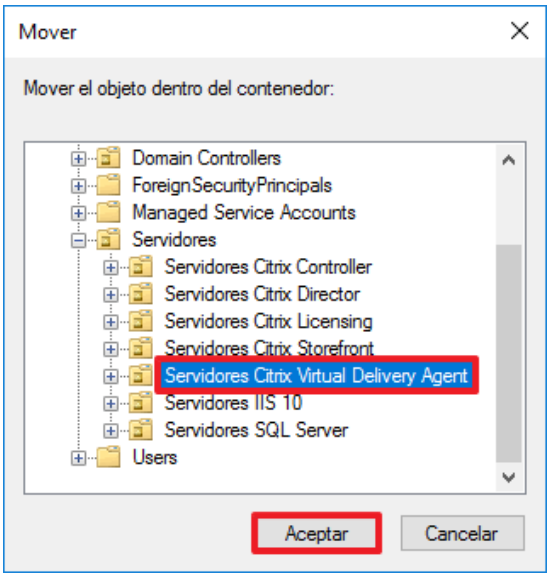
| Paso | Descripción |
|---|---|
| 12. | El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administración del dominio y pulse “Sí” para continuar.<br>  |
| 13. | Se lanzará una ventana del intérprete de comandos “cmd.exe” como la mostrada en la siguiente figura.<br>Este script copia las plantillas de seguridad a la ubicación “C:\Windows\security\templates” y crea el grupo de seguridad “Usuarios de Citrix” si éste no existiese.<br>  |

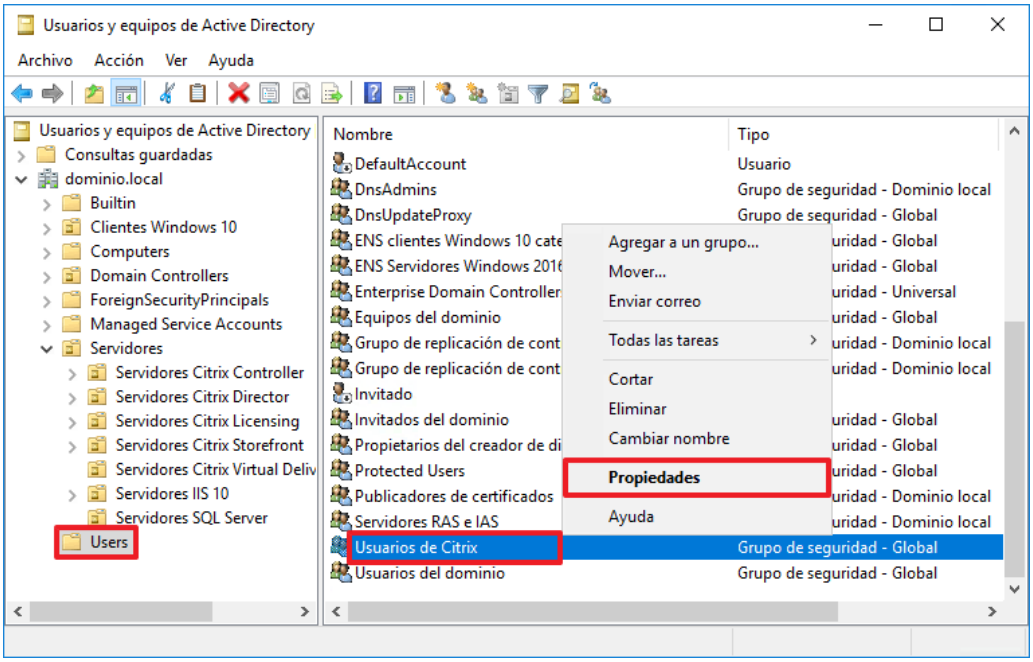
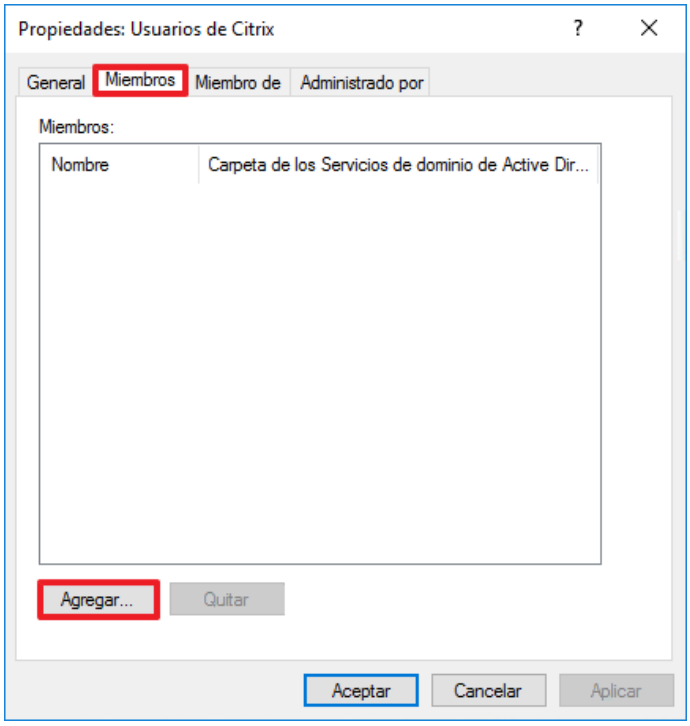
| Paso | Descripción |
|---|---|
| 14. | Pulse una tecla al finalizar la ejecución del script para cerrar la ventana. |
| 15. | Abra la herramienta "Administrador del servidor" y a continuación seleccione **"Herramientas → Usuarios y equipos de Active Directory"** en el menú superior derecho. El sistema solicitará elevación de privilegios. |

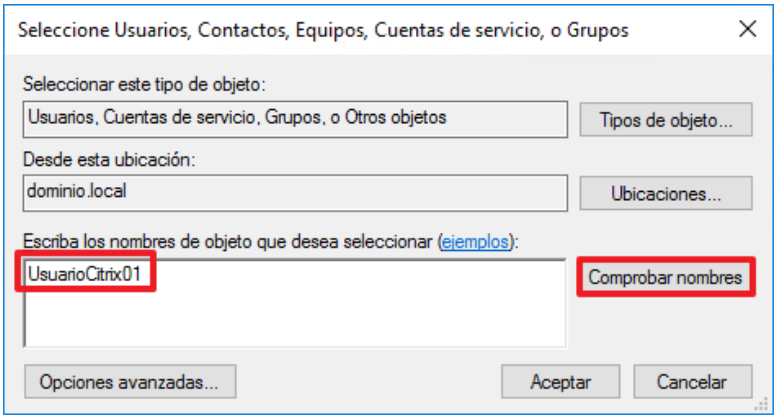
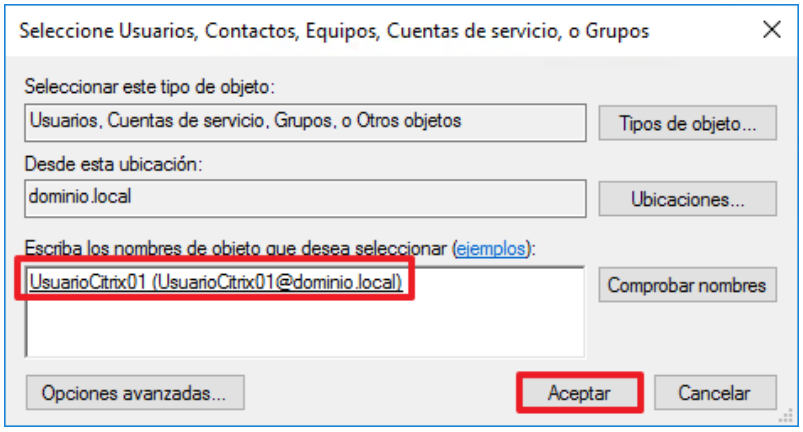


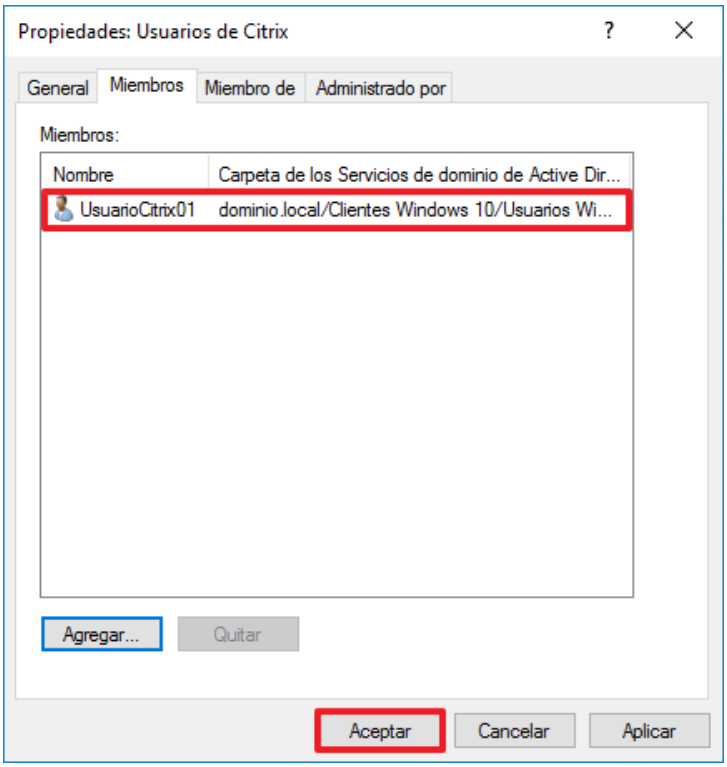
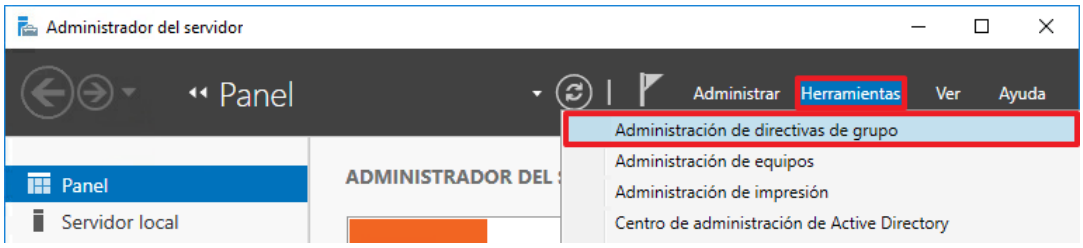



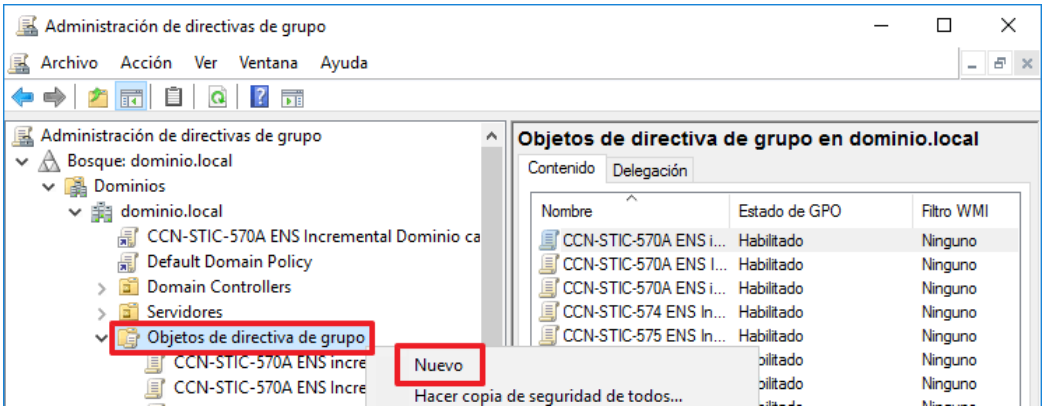
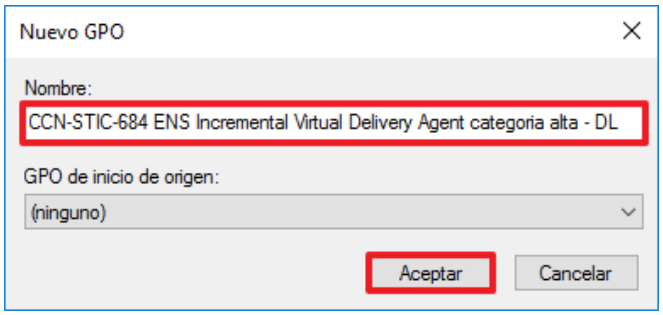
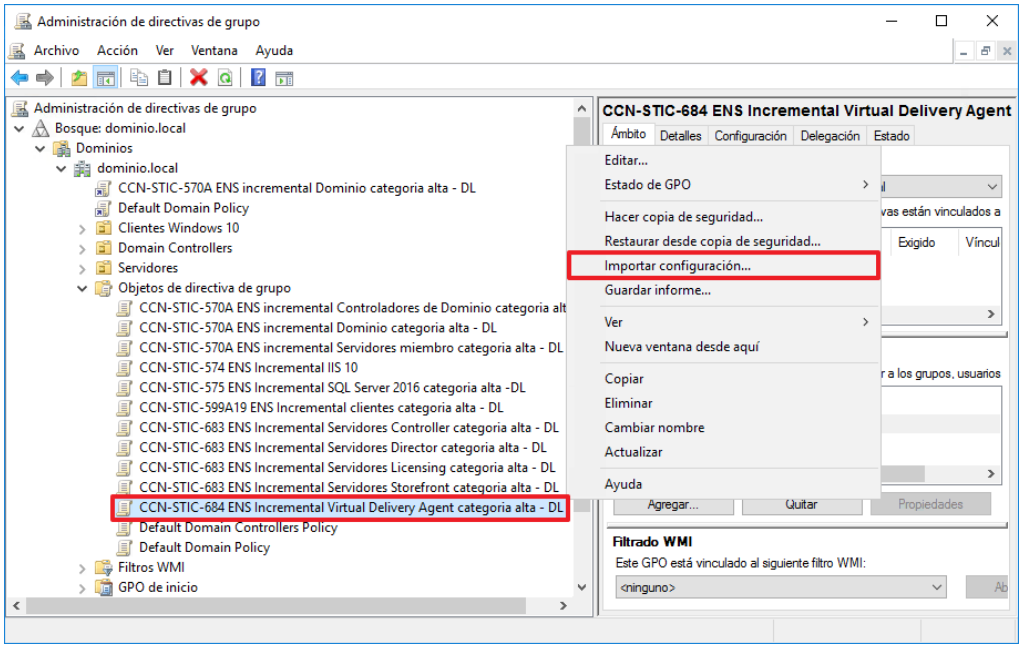
| Paso | Descripción |
|---|---|
| 16. | A continuación, en la herramienta “Usuarios y equipos de Active Directory” expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio>" → Servidores”**, y marcándolo con el botón derecho del ratón, seleccione la opción **"Nuevo → Unidad organizativa"** del menú contextual que aparecerá, como se muestra en la siguiente figura.<br>  |
| 17. | En la ventana resultante, introduzca como nombre de la nueva unidad organizativa “Servidores Citrix Virtual Delivery Agent” tal y como muestra en la imagen. No desmarque la opción “Proteger contenedores contra eliminación accidental”. Pulse “Aceptar” para crear el nuevo objeto.<br>  <br>**Nota:** En este punto deberá crear aquellas unidades organizativas que sean necesarias para la administración de su organización. |

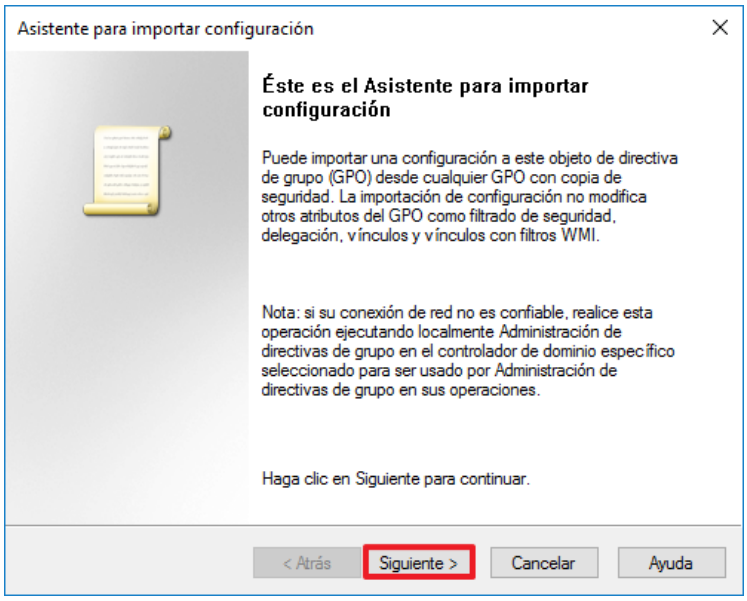
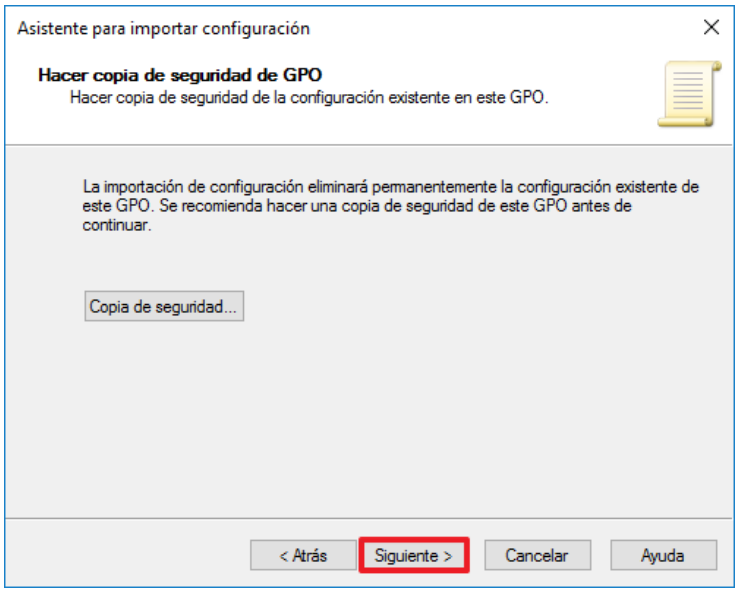
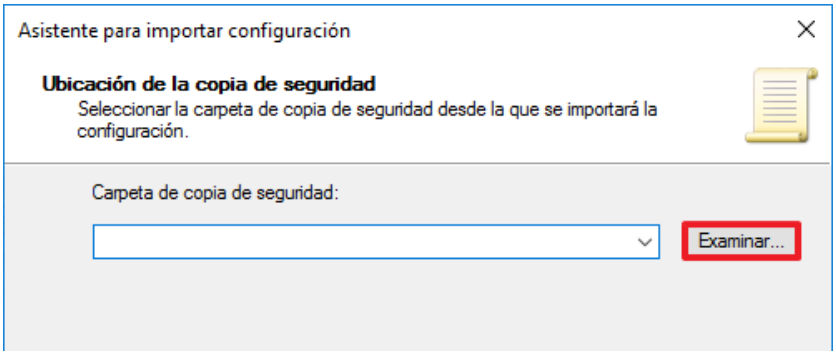
| Paso | Descripción |
|---|---|
| 18. | Vaya a las unidades organizativas donde se encuentren los equipos que les sea de aplicación el ENS, pulse con botón derecho sobre ellos y seleccione “Mover…” en cada uno de ellos.<br>  <br><br>**Nota:** En este ejemplo se encuentra bajo la unidad organizativa “Servidores”. |
| 19. | Seleccione la unidad organizativa “Servidores Citrix Virtual Delivery Agent” creada anteriormente y pulse “Aceptar”.<br>  <br> |

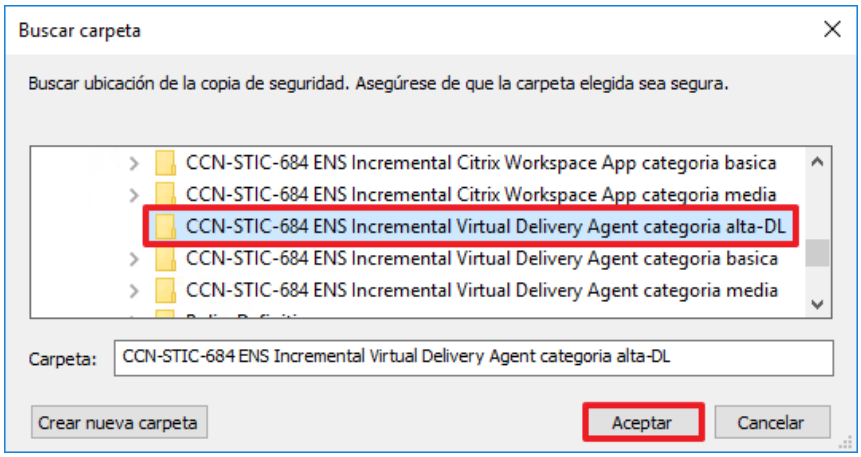
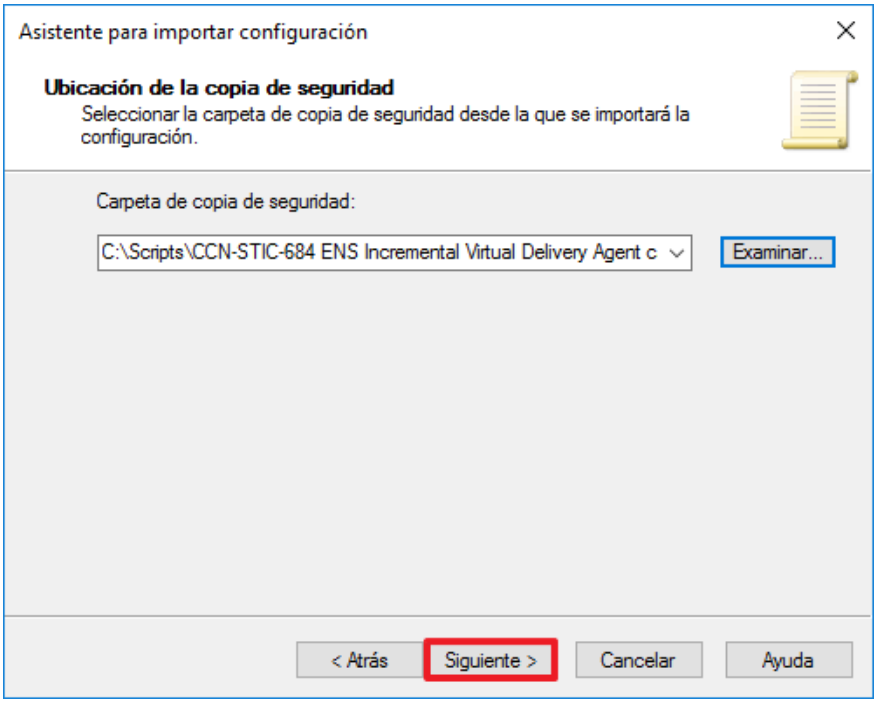
| Paso | Descripción |
|---|---|
| 20. | A continuación proceda a incluir a los usuarios que harán uso de la infraestructura de Citrix dentro del grupo de seguridad "Usuarios de Citrix", para ello expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"** y seleccionando el grupo de seguridad "Usuarios de Citrix" haga clic derecho sobre él y acceda al menú "Propiedades" del menú contextual que aparecerá.   |
| 21. | Dentro de las propiedades del grupo, en la pestaña "Miembros" pulse "Agregar…".   |

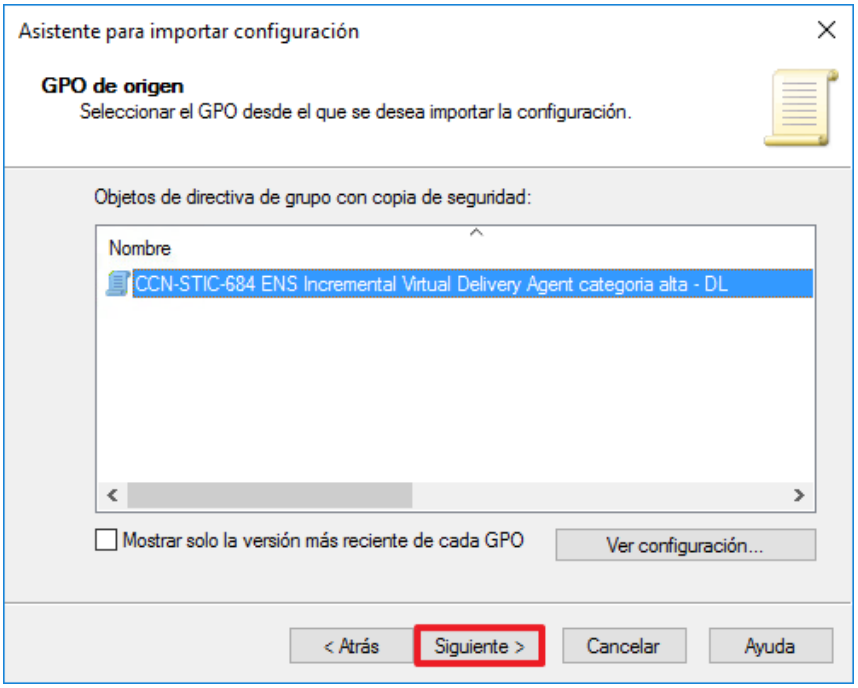
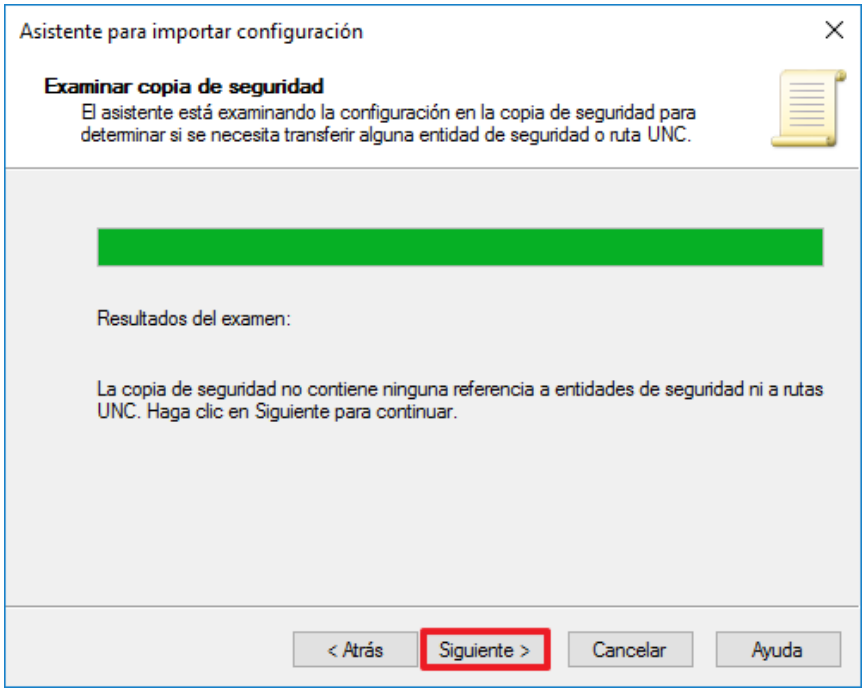
| Paso | Descripción |
|---|---|
| 22. | Escriba el nombre del usuario que desee agregar al grupo y pulse “Comprobar nombres”.<br>  <br>**Nota:** En este ejemplo se utiliza el usuario “UsuarioCitrix01” deberá, en este paso, agregar al grupo “Usuarios de Citrix” los usuarios creados en su organización para hacer uso de los recursos entregados mediante Virtual Delivery Agent. |
| 23. | Compruebe que el usuario sea el correcto y pulse “Aceptar” para agregarlo y cerrar la ventana.<br>  |

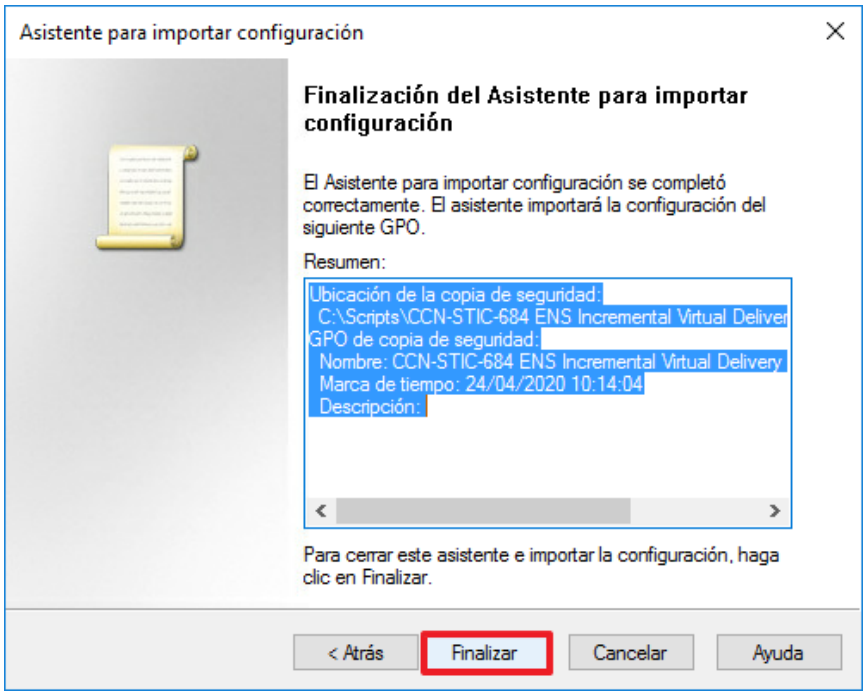
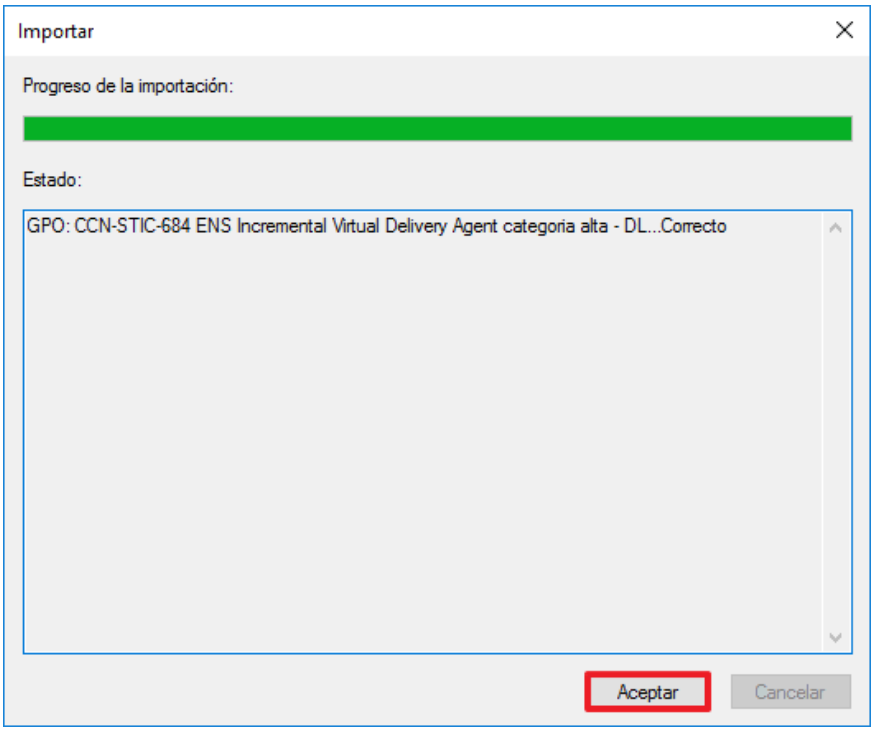
| Paso | Descripción |
|---|---|
| 24. | El usuario aparecerá agregado al grupo “Usuarios de Citrix” pulse “Aceptar” para guardar la configuración y cerrar la ventana. Repita estos pasos para todos aquellos usuarios que desee agregar al grupo.<br>  |
| 25. | Cierre la herramienta “Usuarios y equipos de Directorio Activo”. |
| 26. | Utilice la herramienta "Administración de Directivas de grupo" (**Administrador del servidor → Herramientas → Administración de Directivas de grupo**). El sistema solicitará elevación de privilegios.<br>  |
| 27. | Expanda el contenedor **"Bosque:<nombre de su bosque> → Dominios → <nombre de su dominio>”**. A continuación, proceda a realizar los pasos siguientes para crear, configurar y asignar las GPOs correspondiente. |

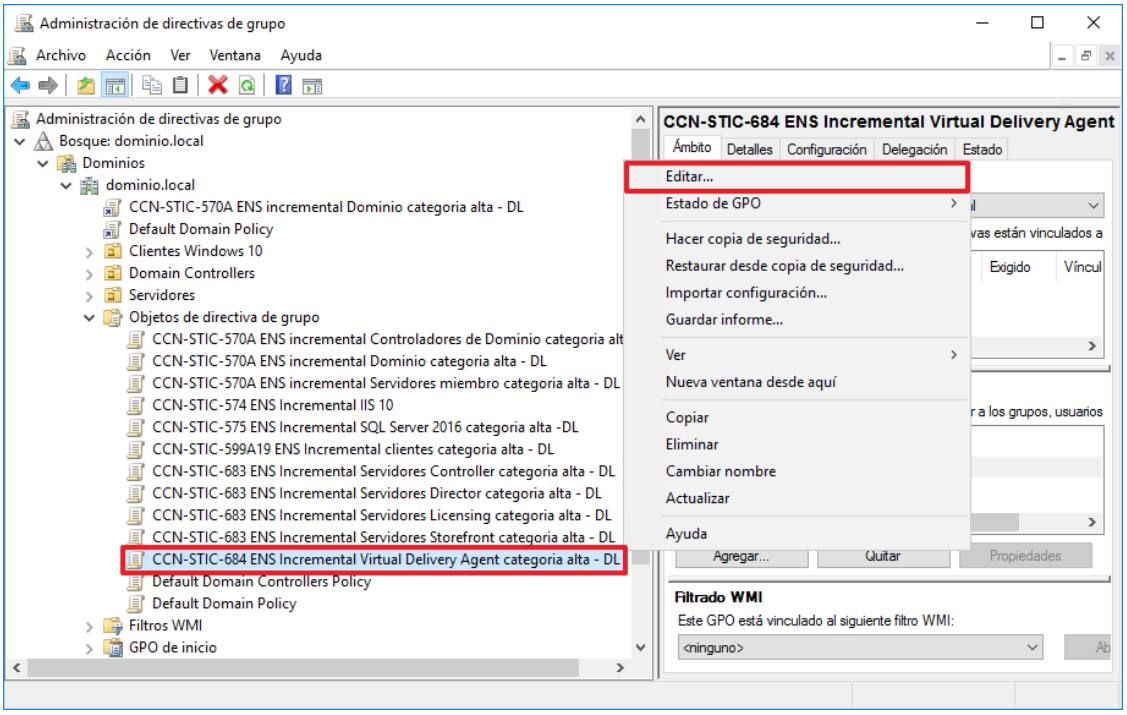
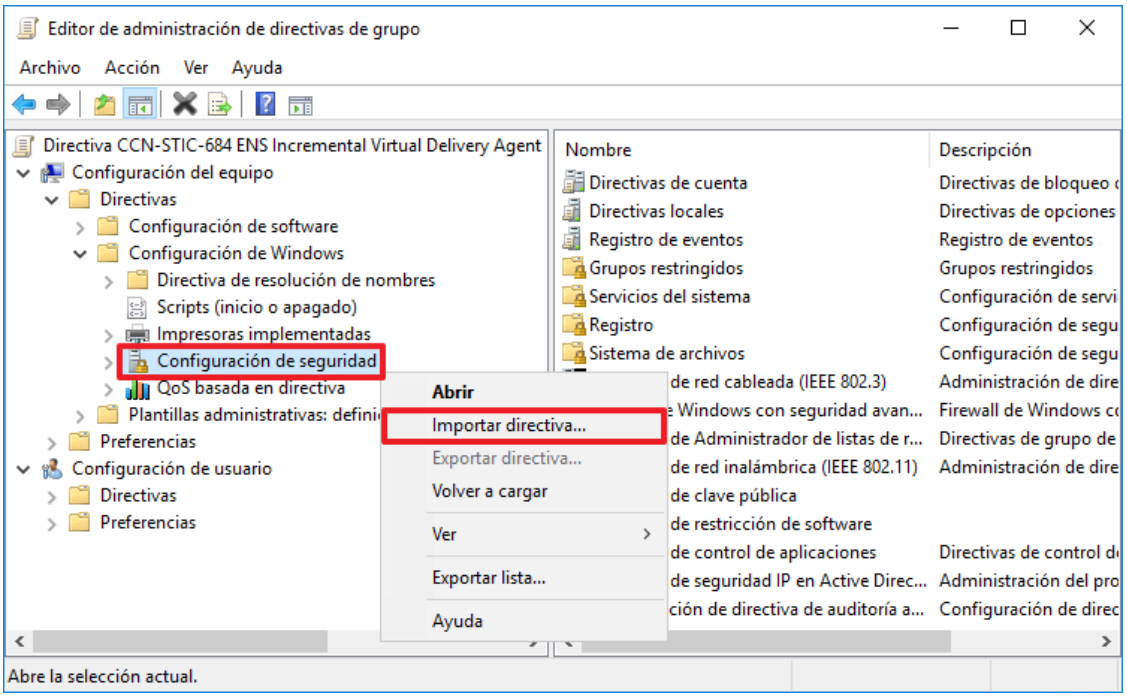
| Paso | Descripción |
|---|---|
| 28. | Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá.<br>  |
| 29. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL" y pulse el botón “Aceptar”.<br>  |
| 30. | Seleccione el GPO recién creado, "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Importar configuración…" del menú contextual que aparecerá.<br>  |

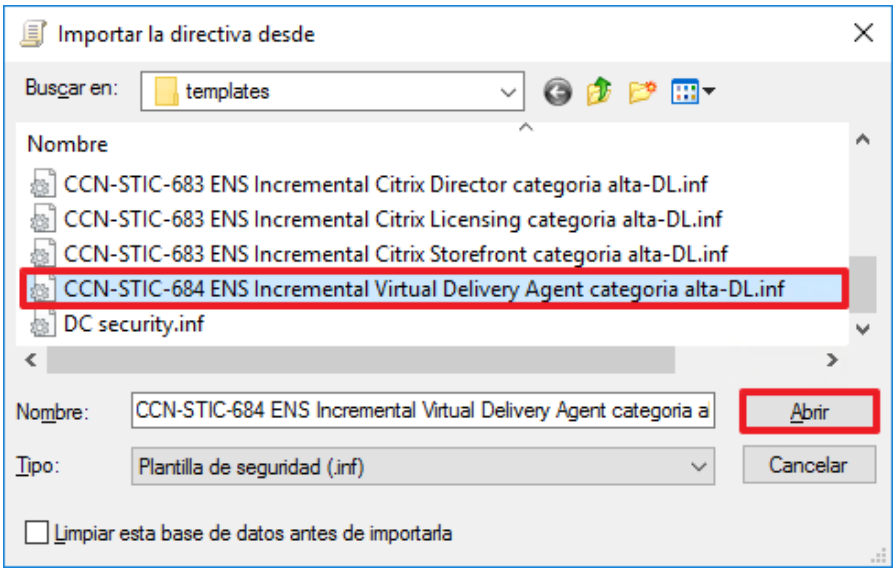
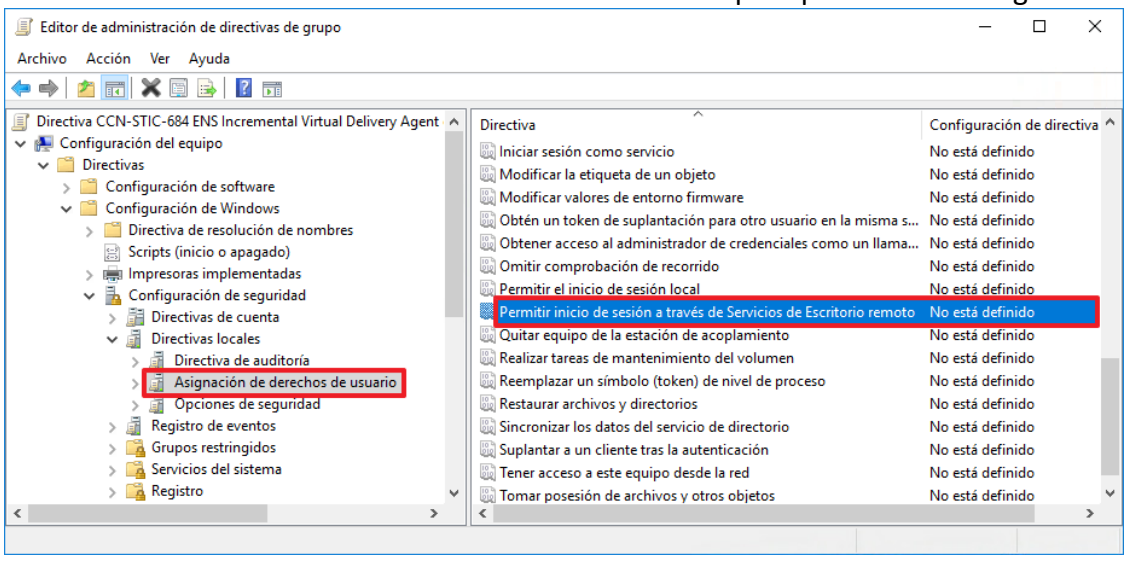
| Paso | Descripción |
|---|---|
| 31. | En el asistente de importación de configuración, pulse el botón “Siguiente >”.<br>  |
| 32. | En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |
| 33. | Pulse el botón “Examinar...” en la ventana “Ubicación de la copia de seguridad”.<br>  |

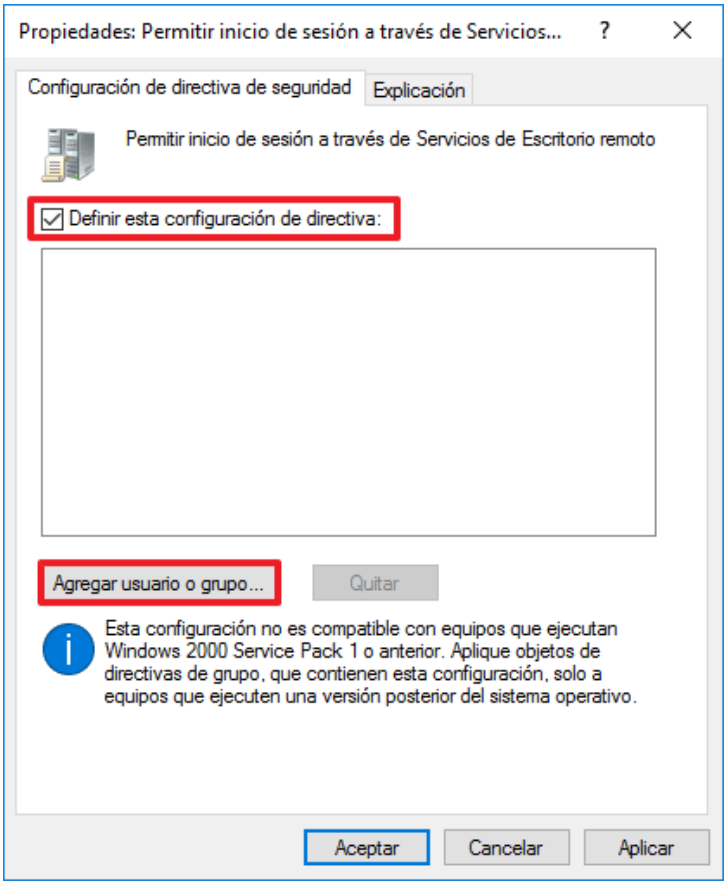
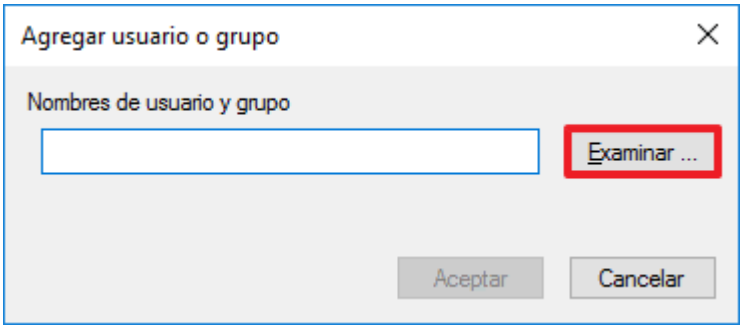
| Paso | Descripción |
|---|---|
| 34. | Seleccione la carpeta “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.<br>  |
| 35. | En la selección de copia de carpeta de seguridad pulse el botón “Siguiente >”.<br>  |

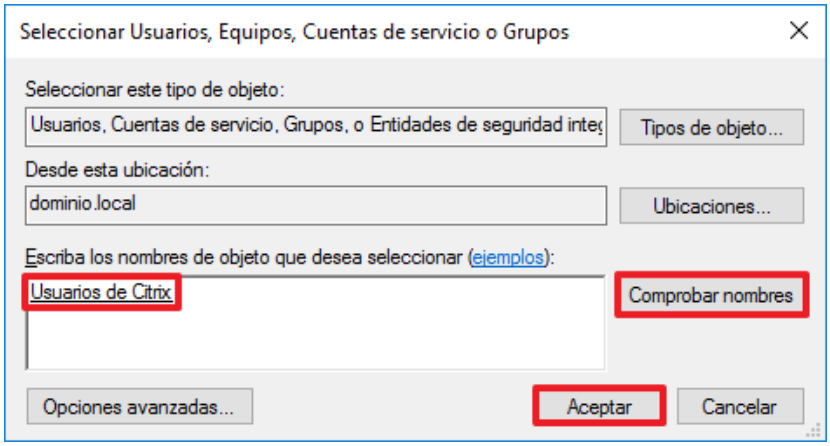
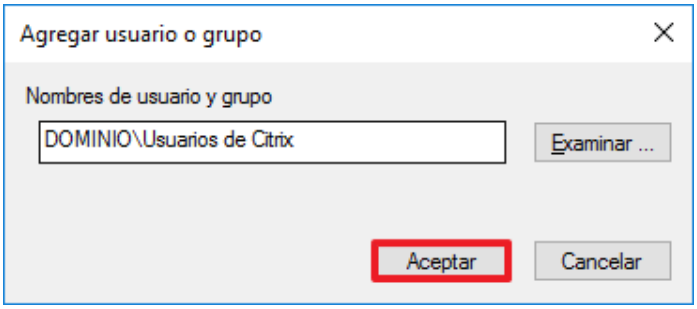
| Paso | Descripción |
|---|---|
| 36. | En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL” y pulse el botón “Siguiente >”.<br>  |
| 37. | En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”.<br>  |

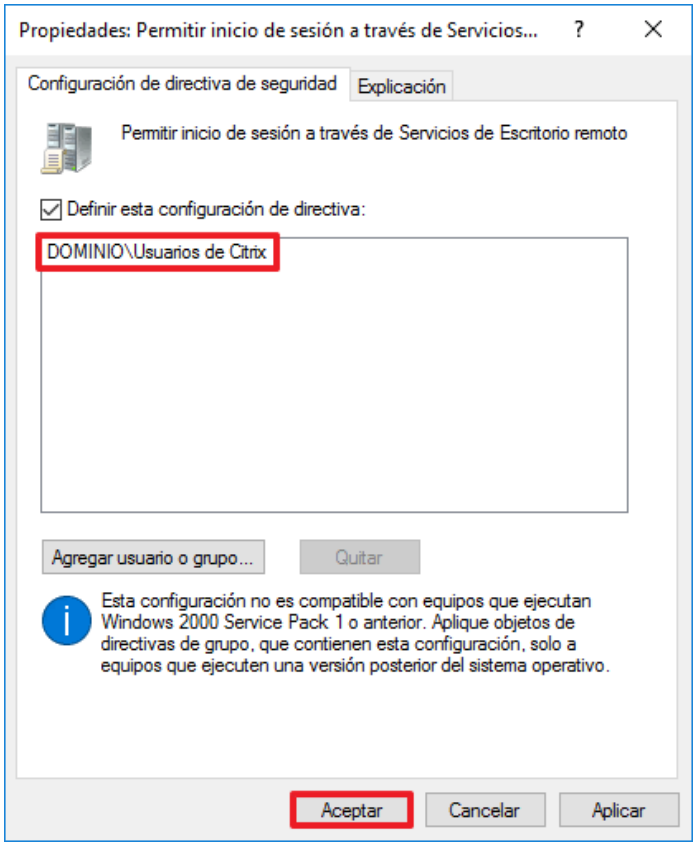
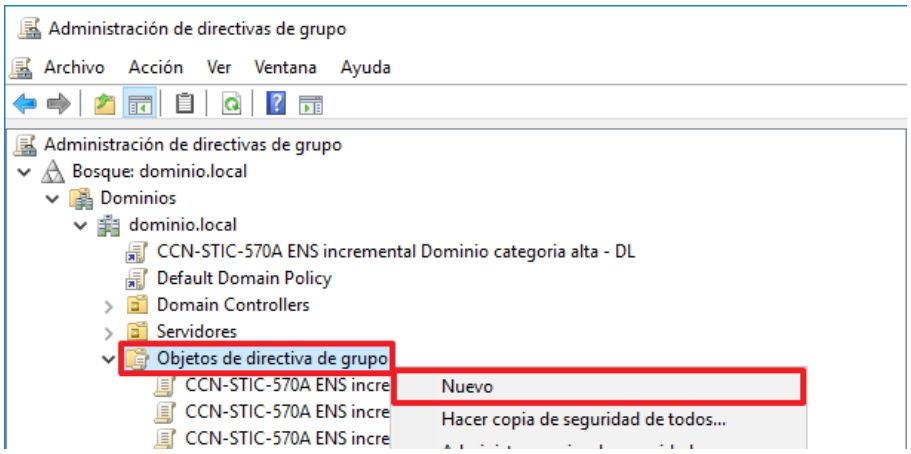
| Paso | Descripción |
|---|---|
| 38. | Para completar el asistente pulse el botón “Finalizar”.<br>  |
| 39. | Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.<br>  |

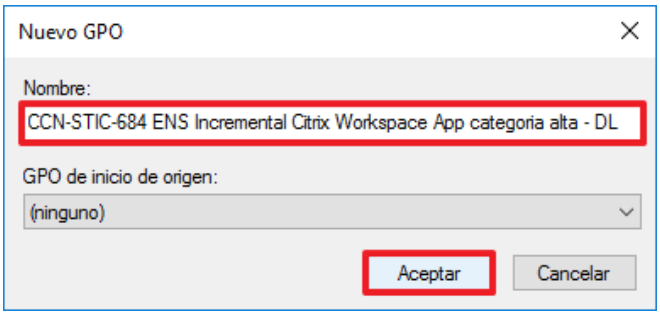
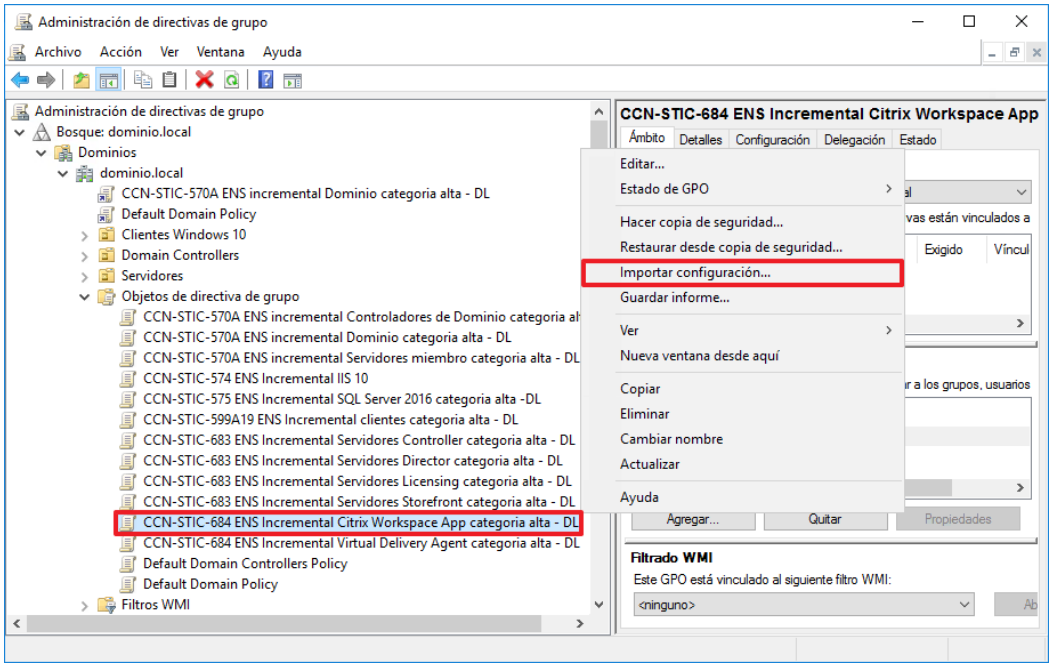
| Paso | Descripción |
|---|---|
| 40. | Seleccione de nuevo el GPO, "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.<br>  |
| 41. | En la ventana del editor de administración de directivas de grupo, seleccione el nodo **“Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL → 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.<br>  |

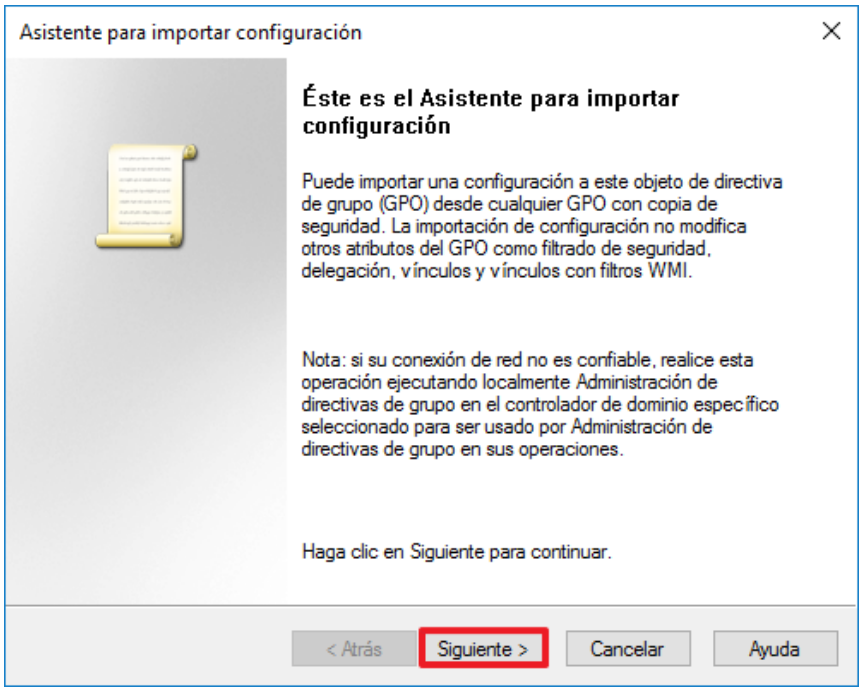
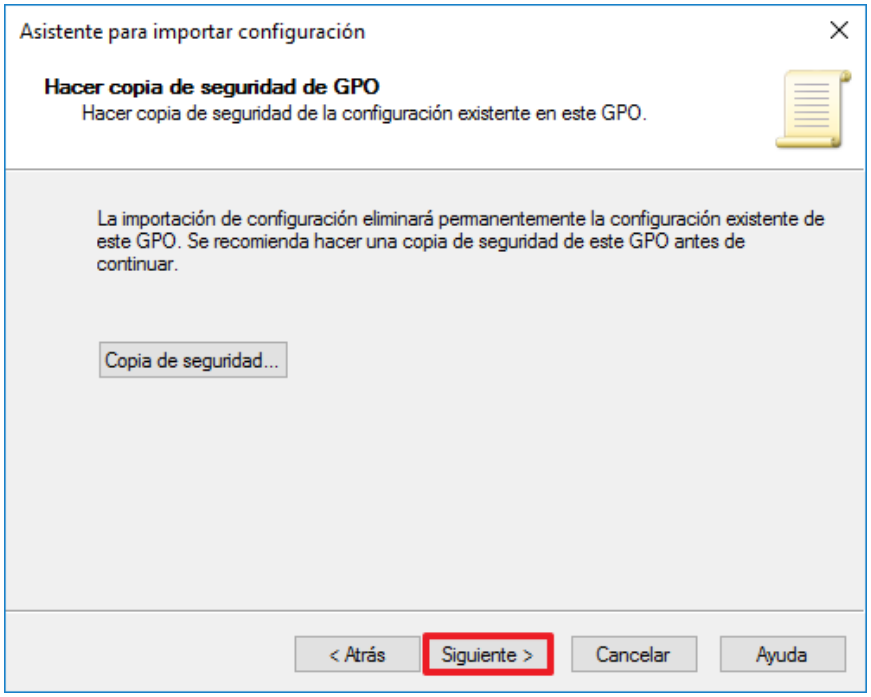
| Paso | Descripción |
|---|---|
| 42. | En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta-DL.inf" y pulse el botón "Abrir". Con eso habrá quedado importada la plantilla de seguridad en el GPO.   |
| 43. | Continúe editando la directiva de grupo, diríjase al nodo **"Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL→ Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario"** y haga doble clic sobre la directiva "Permitir inicio de sesión a través de Escritorio remoto" para proceder a configurarla.   |

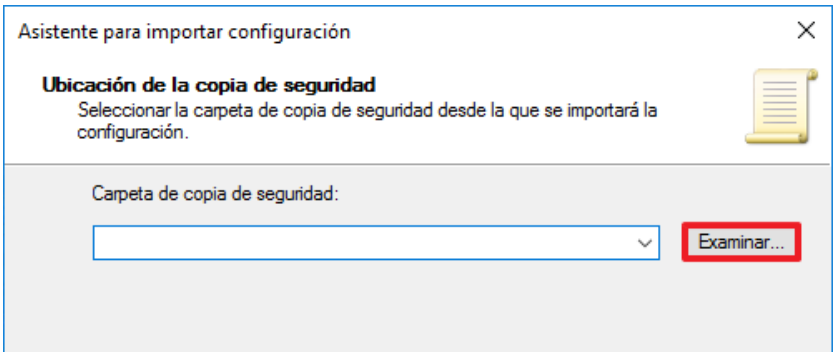
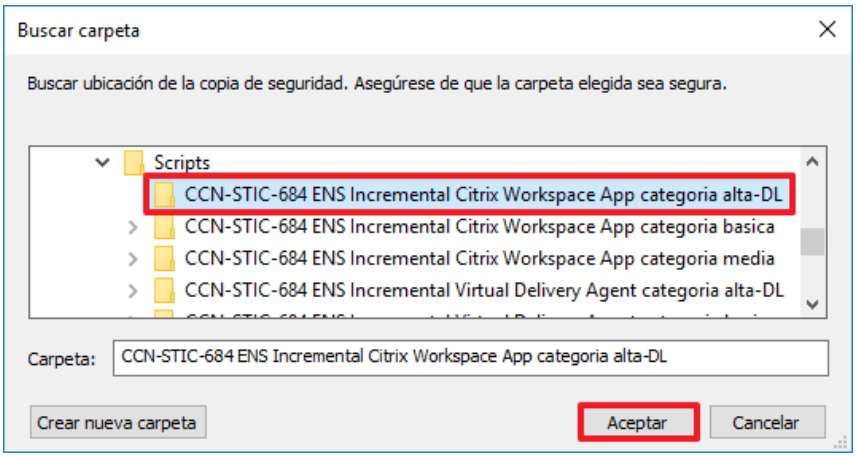
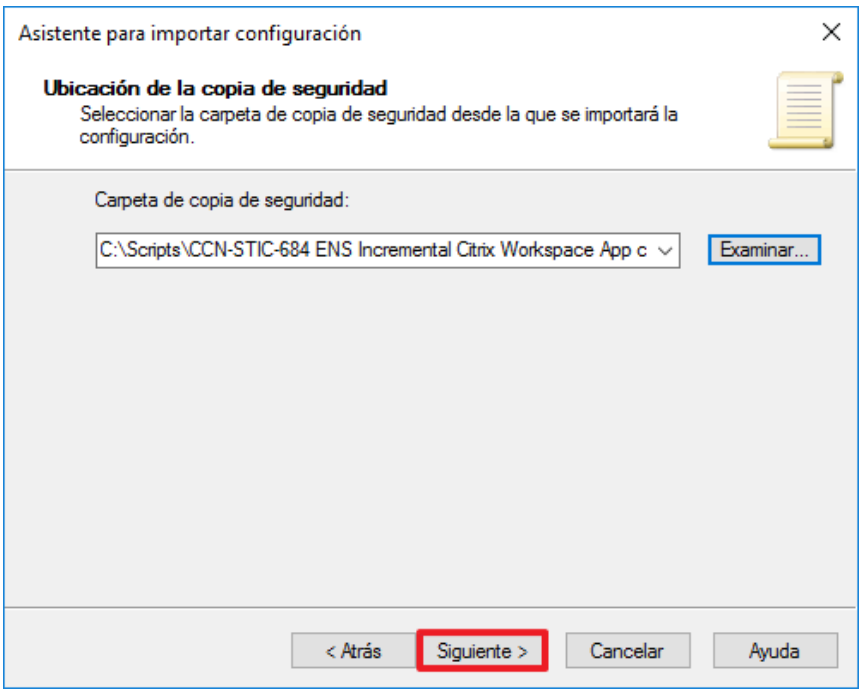
| Paso | Descripción |
|---|---|
| 44. | Marque la casilla “Definir esta configuración de directiva” para habilitar las opciones de configuración. A continuación, pulse sobre “Agregar usuario o grupo”.<br>  |
| 45. | En la ventana resultante haga clic en “Examinar …”.<br>  |

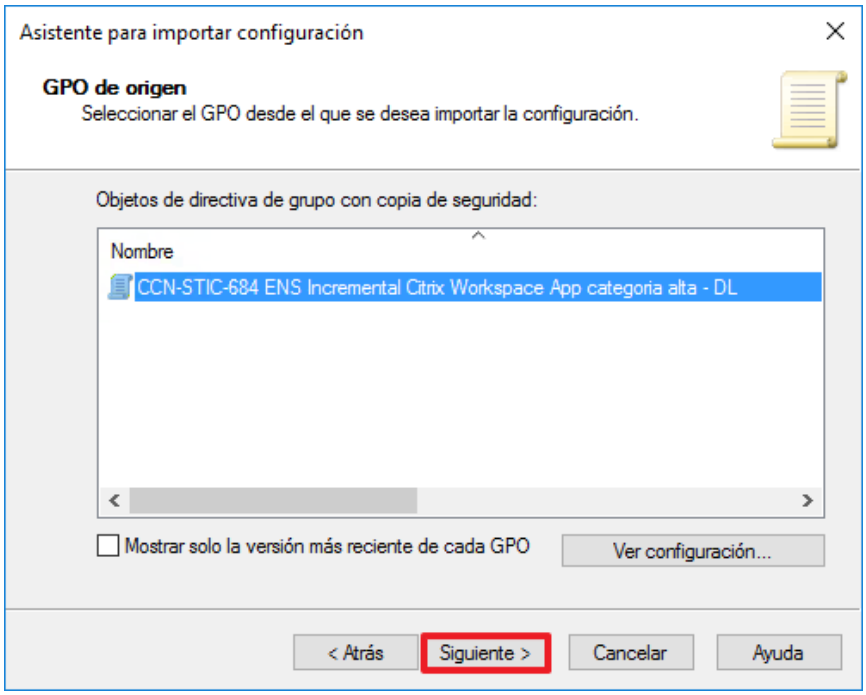
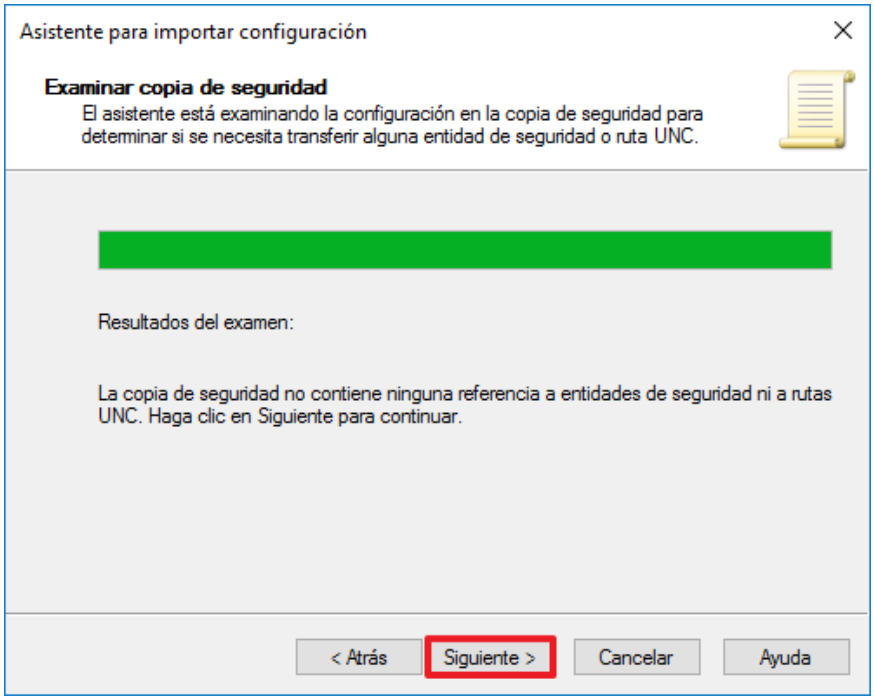
| Paso | Descripción |
|---|---|
| 46. | Escriba el nombre del grupo “Usuarios de Citrix” y en este orden pulse en primer lugar sobre “Comprobar nombres” y a continuación sobre “Aceptar”.<br>  <br>**Nota:** El grupo “Usuarios de Citrix” se deberá haber creado al comienzo de esta guía mediante la ejecución del script “CCN-STIC-684 ENS categoria alta-DL - Preparacion del Dominio - Paso 2.bat”. |
| 47. | Pulse “Aceptar” para añadir el grupo “Usuarios de Citrix a la directiva”.<br>  |

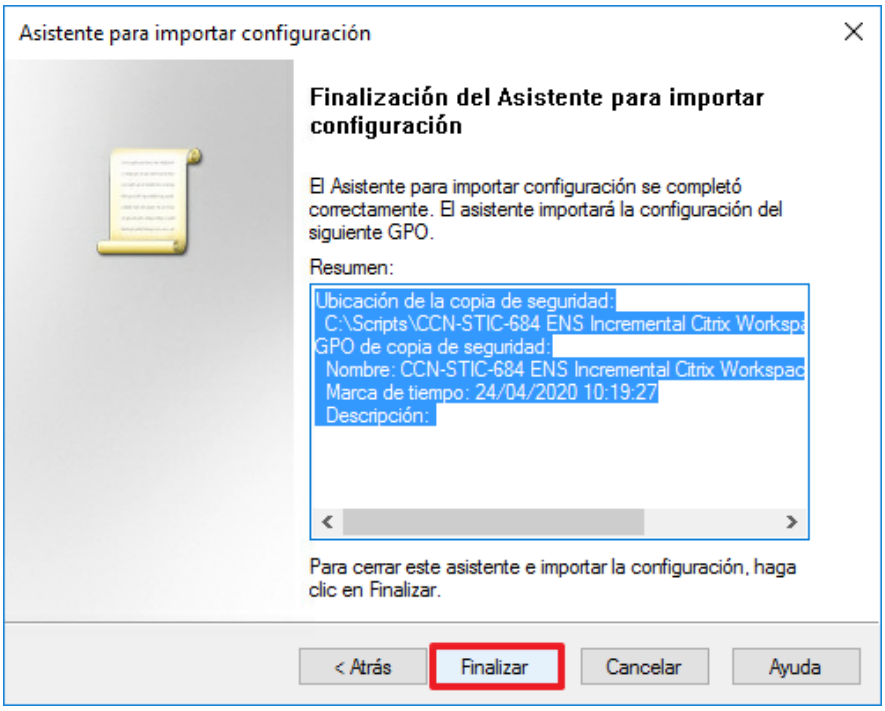
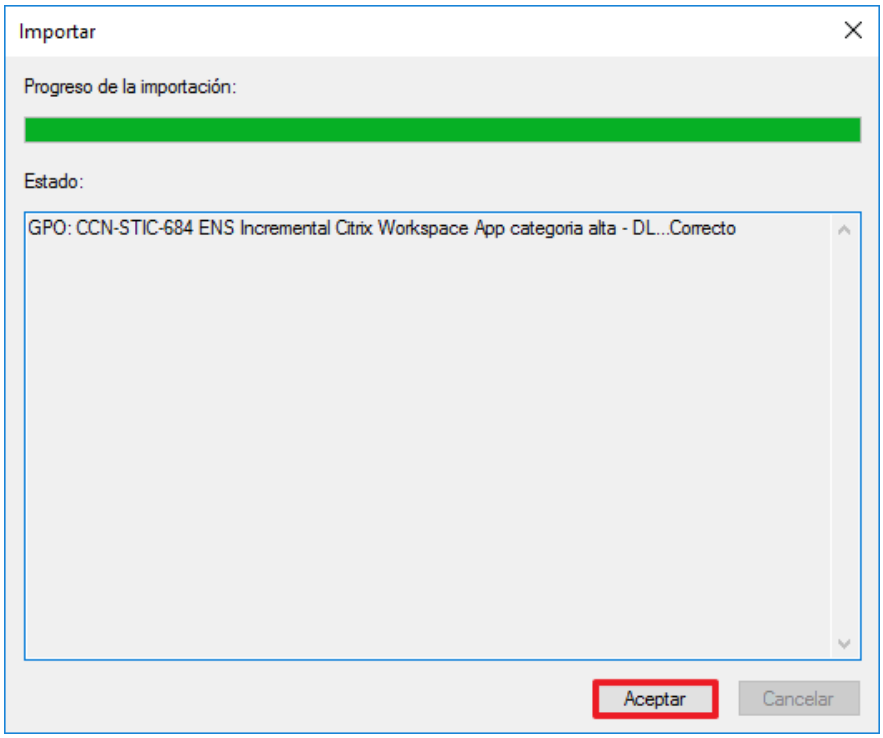
| Paso | Descripción |
|---|---|
| 48. | Aparecerá el grupo “Usuarios de Citrix” definido en la directiva. Pulse “Aceptar” para guardar la configuración y cerrar la ventana.<br>  <br>**Nota:** Ahora sí, cierre la ventana del editor de administración de directivas de grupo. |
| 49. | Con ello este GPO ("CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que su configuración sea aplicada. |
| 50. | 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.<br>  |

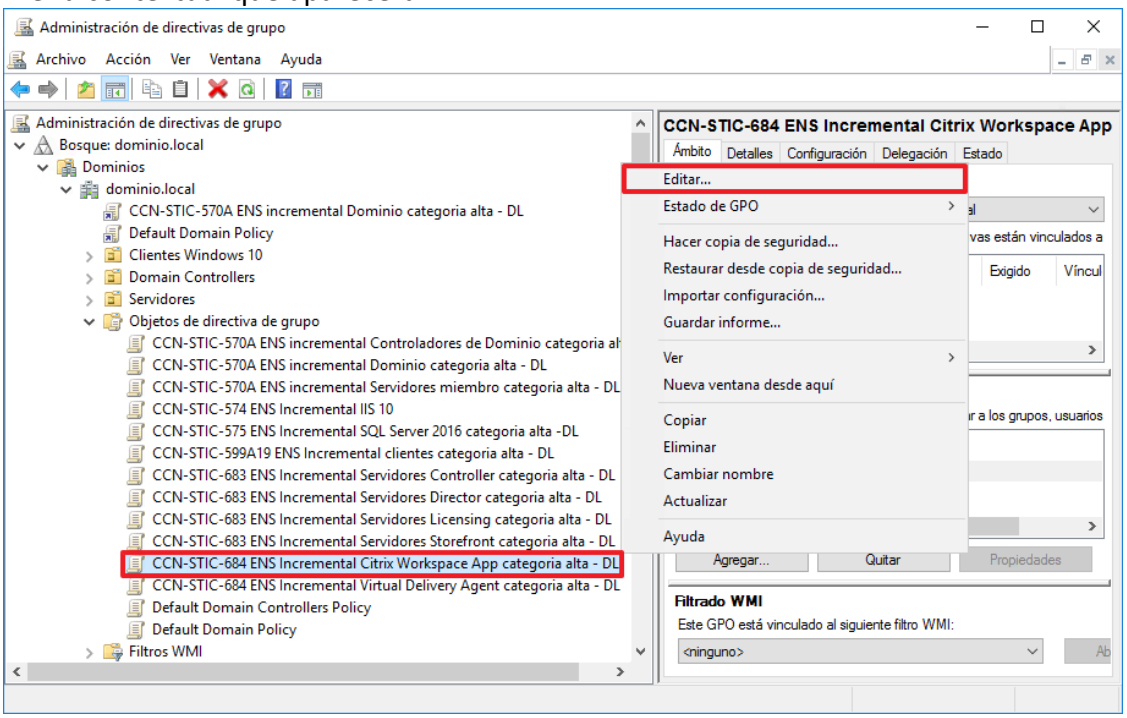
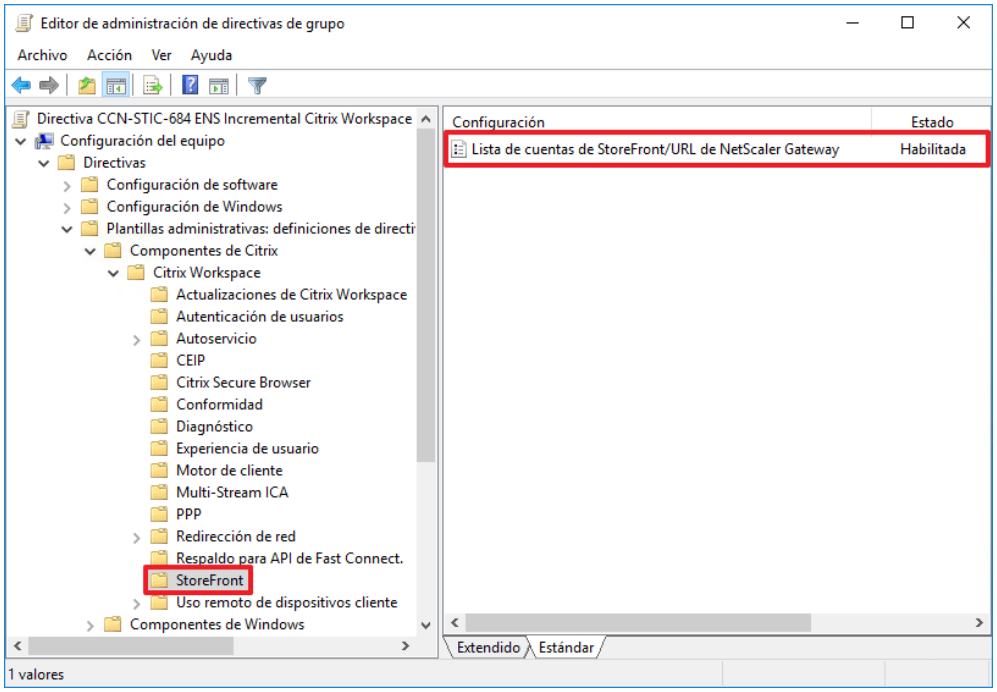
| Paso | Descripción |
|---|---|
| 51. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL" y pulse el botón “Aceptar”.<br>  |
| 52. | Seleccione el GPO recién creado, "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Importar configuración…" del menú contextual que aparecerá.<br>  |

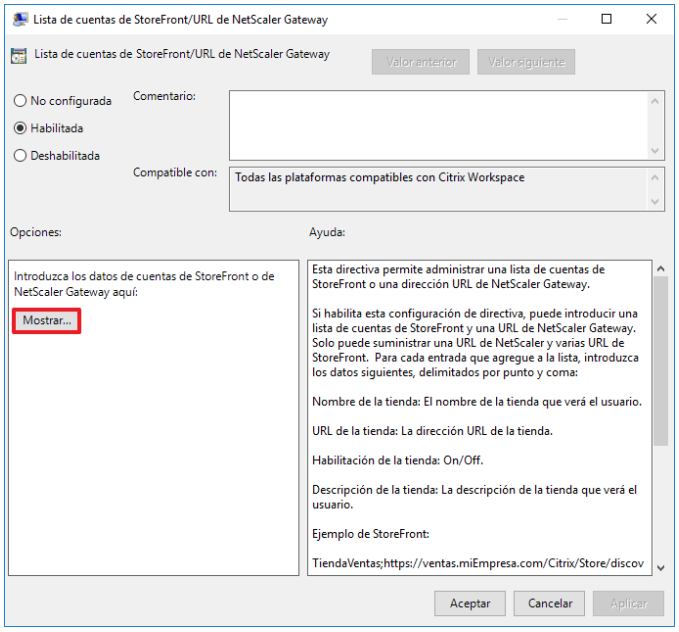
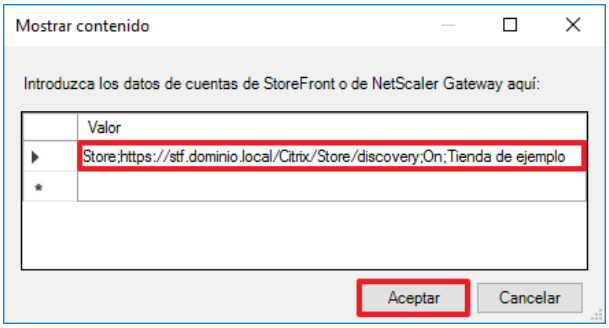
| Paso | Descripción |
|---|---|
| 53. | En el asistente de importación de configuración, pulse el botón “Siguiente >”.<br>  |
| 54. | En la selección de copia de seguridad pulse el botón “Siguiente >”. No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.<br>  |

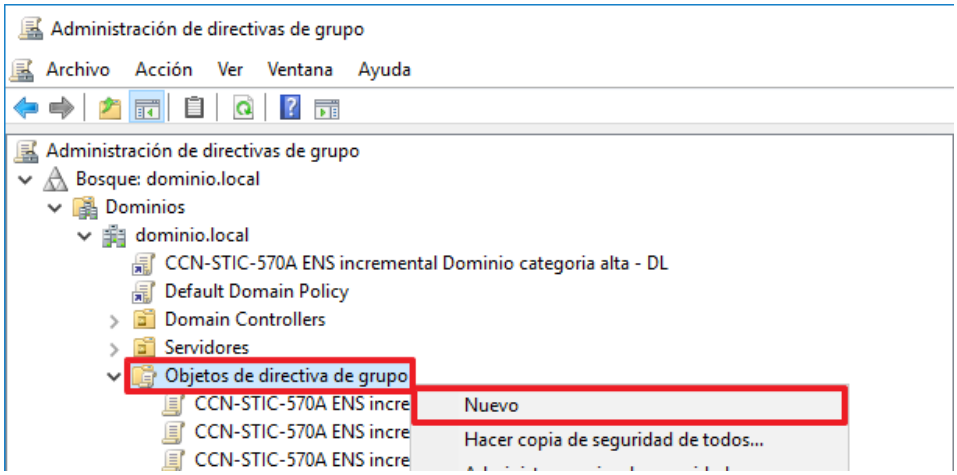
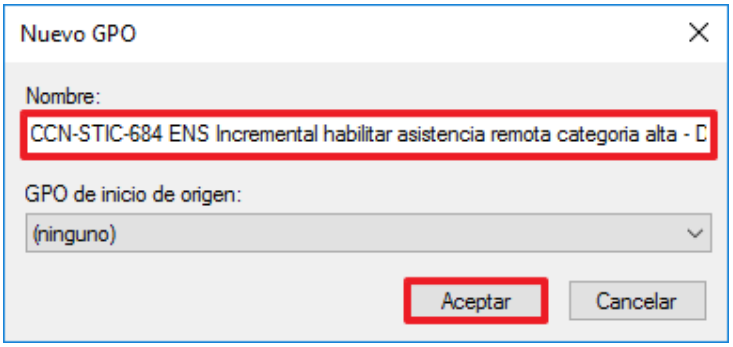
| Paso | Descripción |
|---|---|
| 55. | Pulse el botón “Examinar...” en la ventana “Ubicación de la copia de seguridad”.<br>  |
| 56. | Seleccione la carpeta “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.<br>  |
| 57. | En la selección de copia de carpeta de seguridad pulse el botón “Siguiente >”.<br>  |

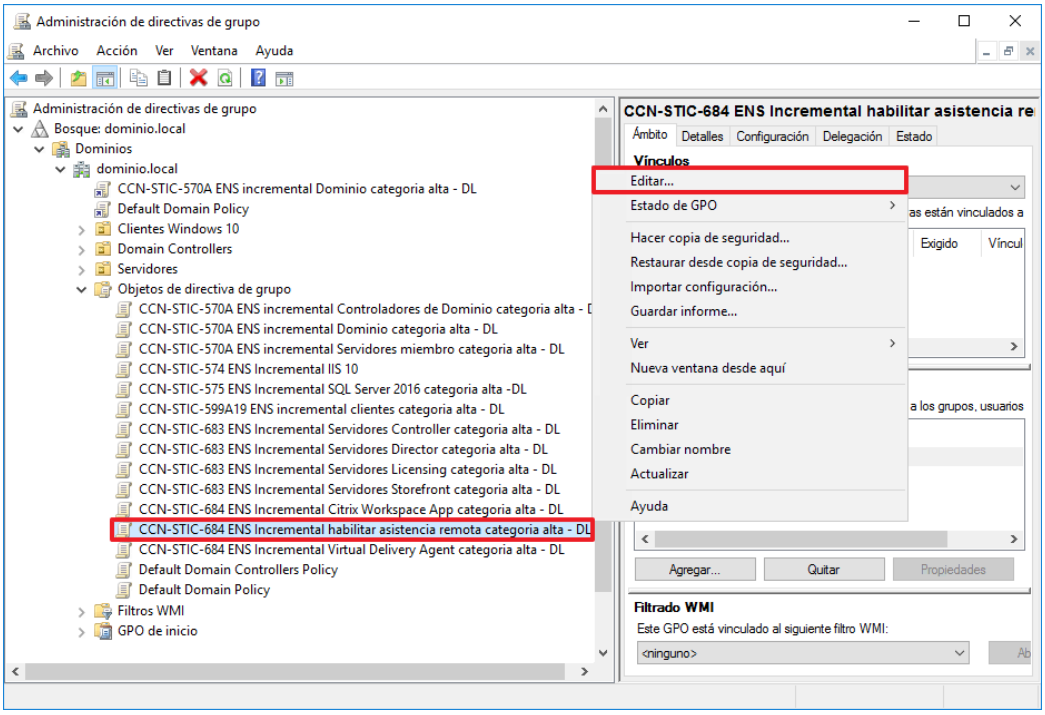
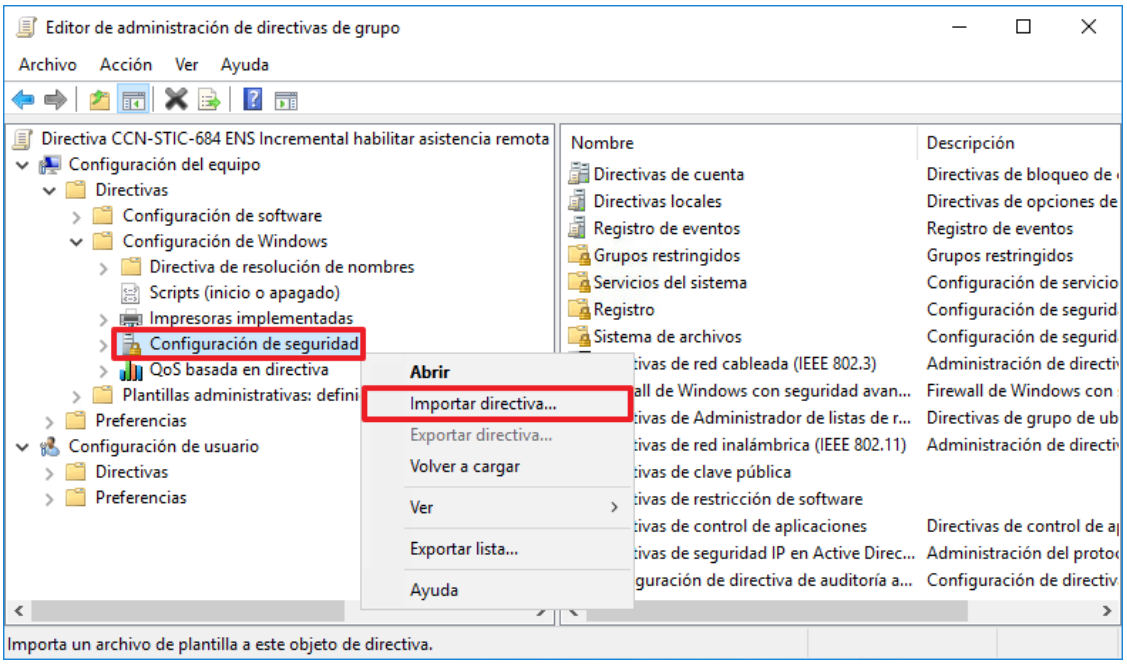
| Paso | Descripción |
|---|---|
| 58. | En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” y pulse el botón “Siguiente >”.<br>  |
| 59. | En la pantalla “Examinar copia de seguridad”, pulse el botón “Siguiente >”.<br>  |

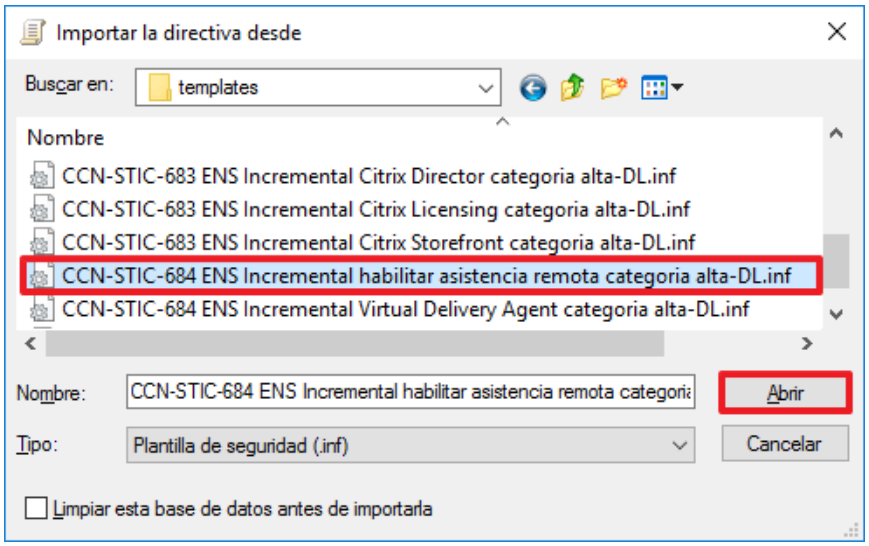
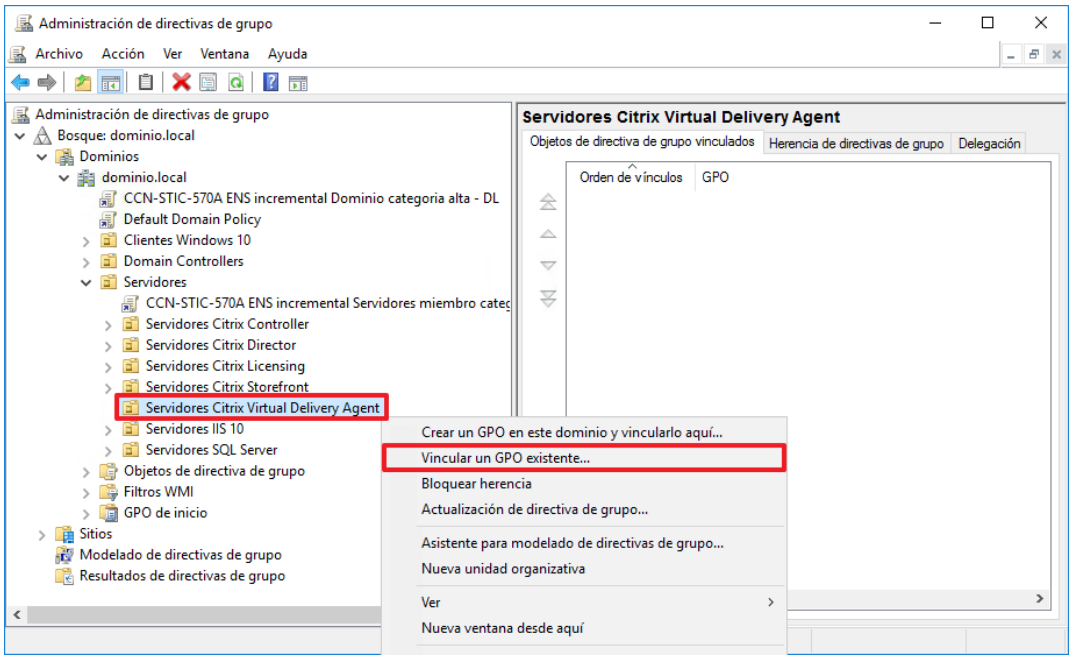
| Paso | Descripción |
|---|---|
| 60. | Para completar el asistente pulse el botón “Finalizar”.<br>  |
| 61. | Pulse el botón “Aceptar” para finalizar el proceso de importación. Si aparece alguna advertencia de resolución de identificadores, no la tenga en consideración.<br>  |

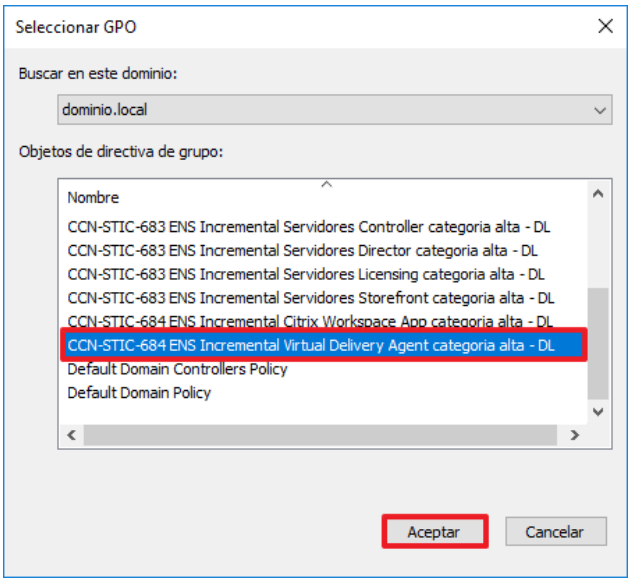
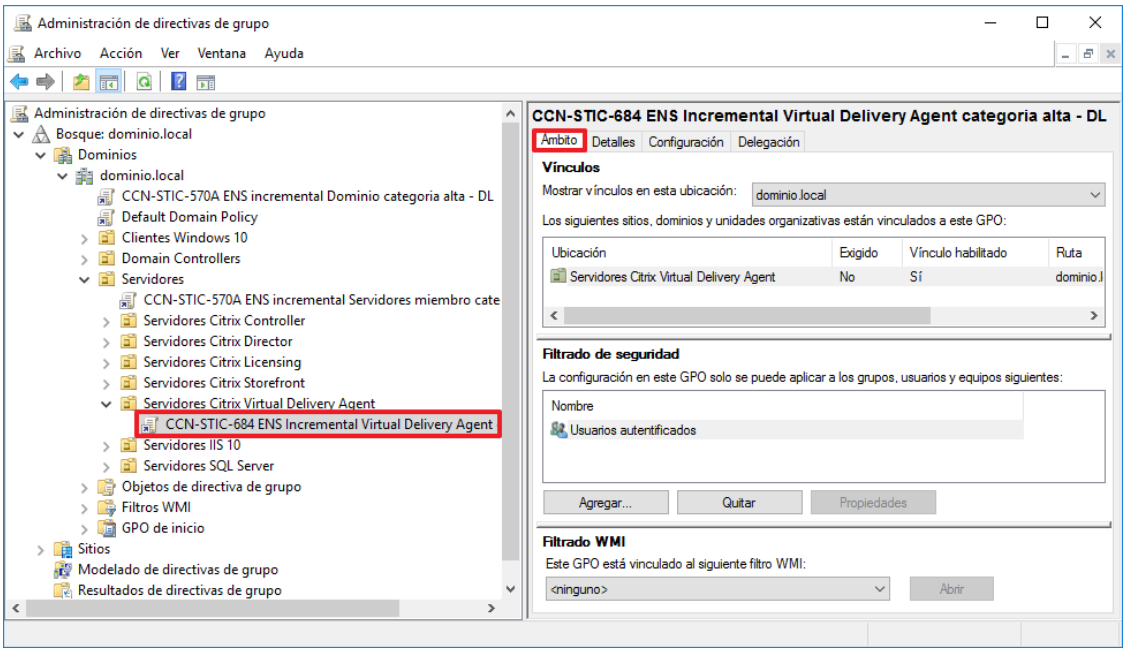
| Paso | Descripción |
|---|---|
| 62. | Seleccione el GPO "CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL " de nuevo, y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.<br>  |
| 63. | En la ventana del editor de administración de directivas de grupo, seleccione el nodo **"Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Storefront"**, y haciendo doble clic sobre la directiva “Lista de cuentas de Storefront/URL de Netscaler Gateway” acceda a la configuración de la misma.<br>  |

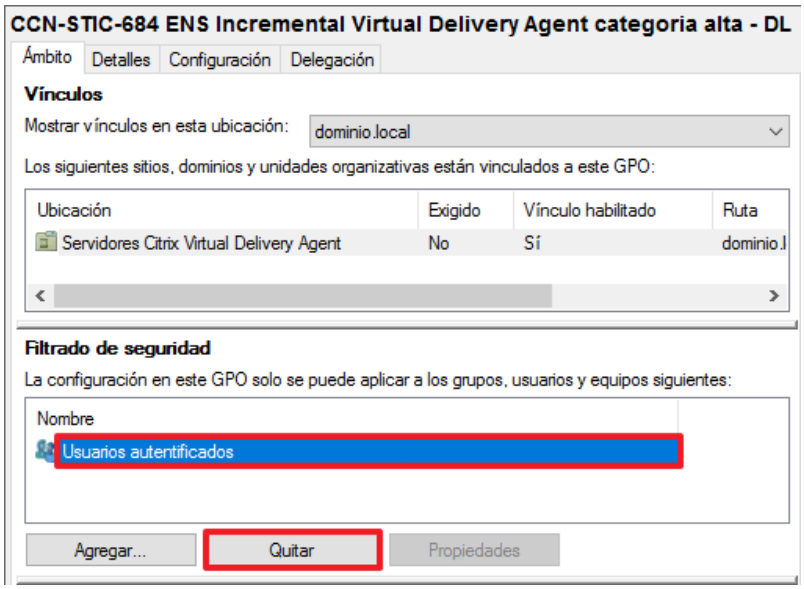
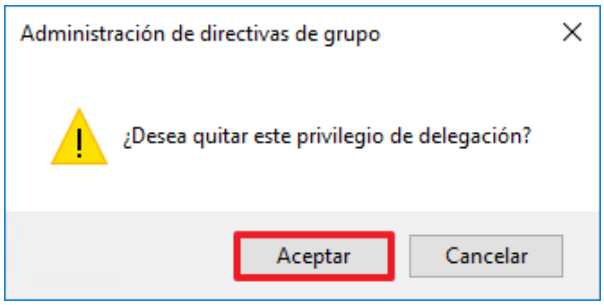
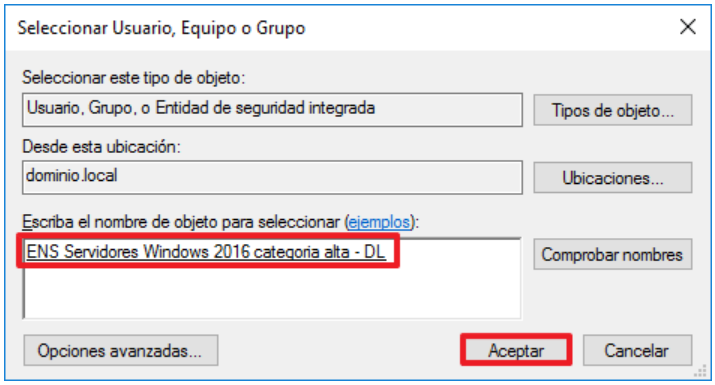
| Paso | Descripción |
|---|---|
| 64. | La directiva se entrega habilitada pero con los valores en blanco. Deberá en este momento configurar la directiva con los valores necesarios para el correcto funcionamiento de su infraestructura. Para ello, haga clic en “Mostrar…”.<br>  <br> |
| 65. | En la ventana resultante, en el campo “Valor”, deberá indicar los datos de la cuenta de Storefront configurado durante la aplicación de la guía CCN-STIC-683. Para cada entrada que agregue a la lista, introduzca los siguientes datos, delimitados por punto y coma:<br>– Nombre de la tienda: El nombre de la tienda que verá el usuario.<br>– URL de la tienda: La dirección URL de la tienda.<br>– Habilitación de la tienda: On/Off.<br>– Descripción de la tienda: La descripción de la tienda que verá el usuario.<br>Pulse “Aceptar” para cerrar la ventana y nuevamente en “Aceptar” para guardar la configuración de la directiva.<br>  <br><br>**Nota:** En esta guía se utiliza la URL “https://stf.dominio.local/Citrix/Store/discovery” así como el resto de configuraciones a modo de ejemplo. Deberá en su caso, adaptar este valor a los configurados por su organización durante la aplicación de la guía “CCN-STIC-683” y los requisitos de la misma.<br>Para el descubrimiento de la tienda será necesario incluir “/Discovery” al final de la URL independientemente de la dirección utilizada. |

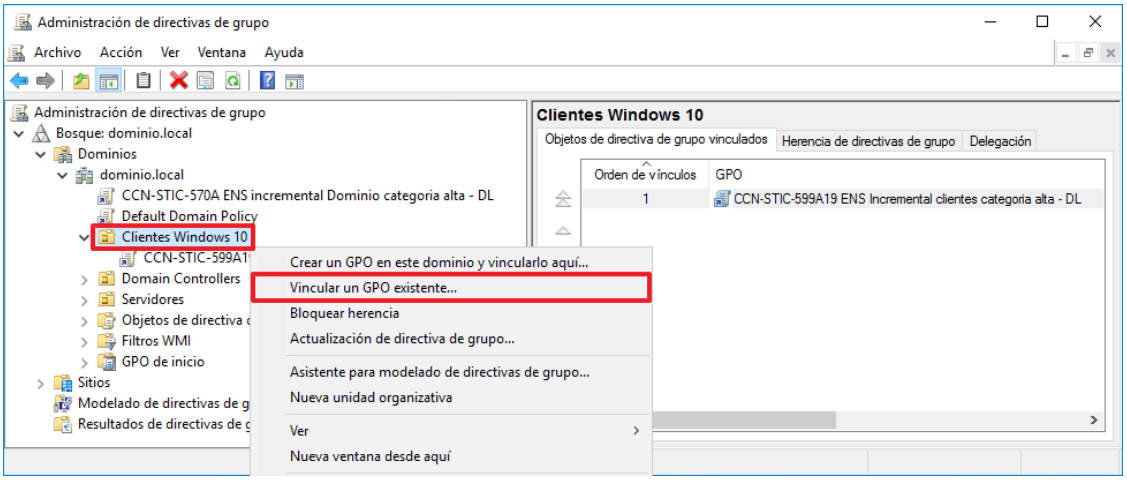
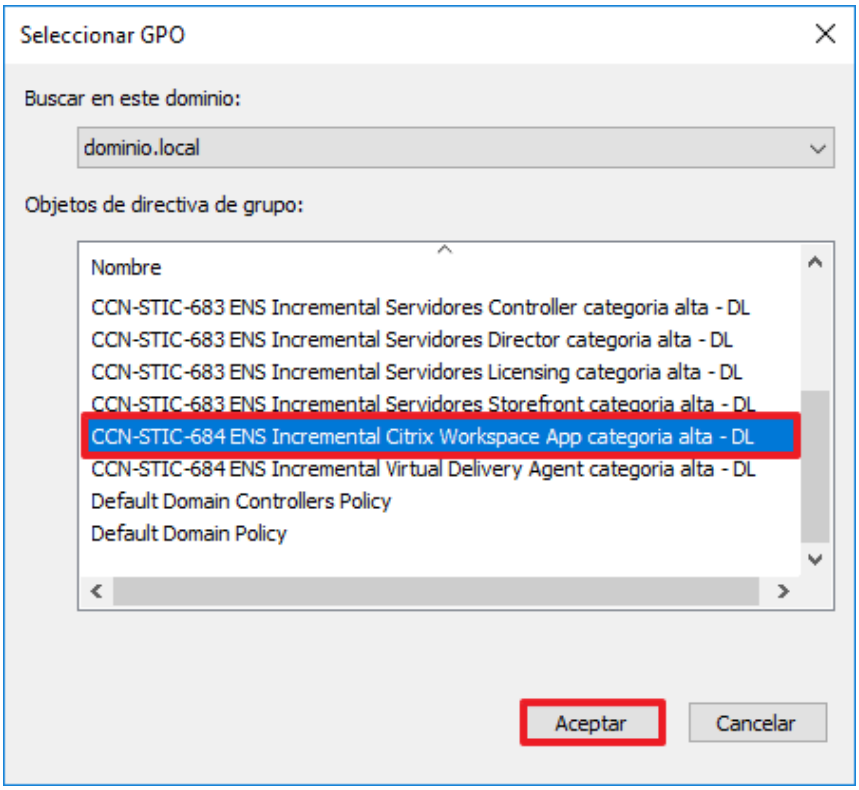
| Paso | Descripción |
|---|---|
| 66. | Con ello, este GPO ("CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que la configuración sea aplicada. |
| 67. | Expanda y seleccione el contenedor "Objetos de directiva de grupo", y marcando con el botón derecho en él, elija la opción "Nuevo" del menú contextual que aparecerá.   |
| 68. | Asigne el siguiente nombre al nuevo GPO: "CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL" y pulse el botón “Aceptar”.   |

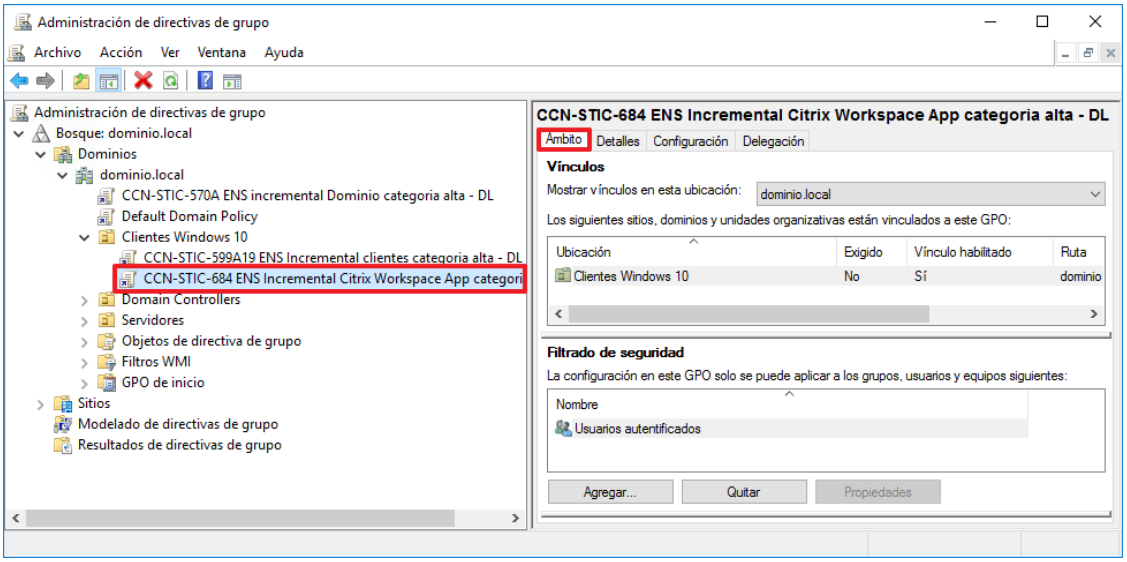
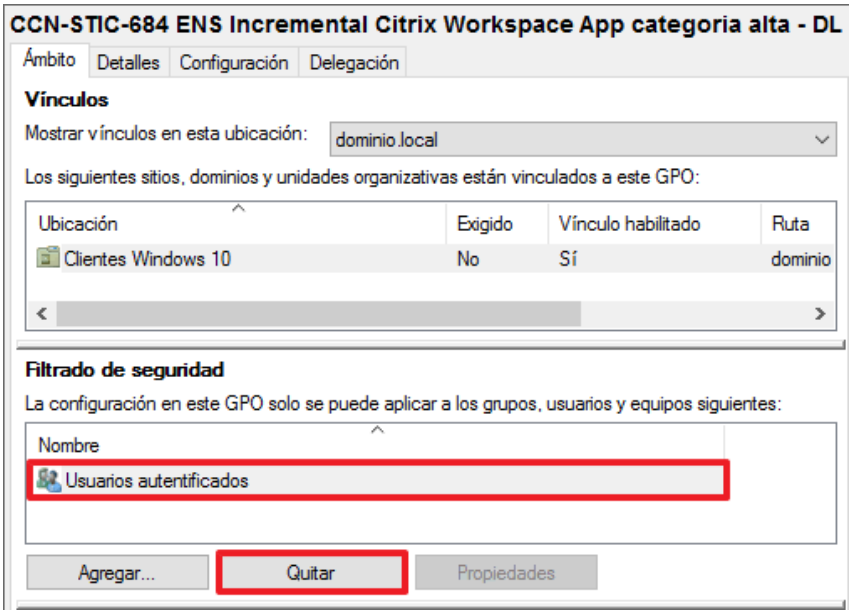
| Paso | Descripción |
|---|---|
| 69. | Seleccione de nuevo el GPO, "CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.   |
| 70. | En la ventana del editor de administración de directivas de grupo, seleccione el nodo **“Directiva CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL → 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.   |

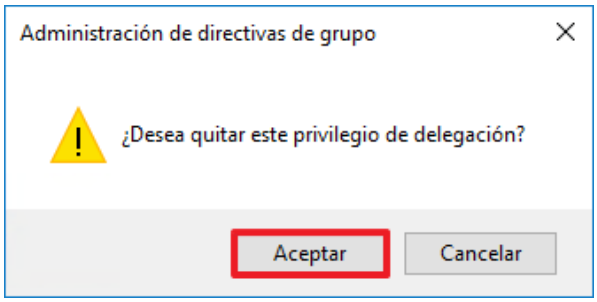
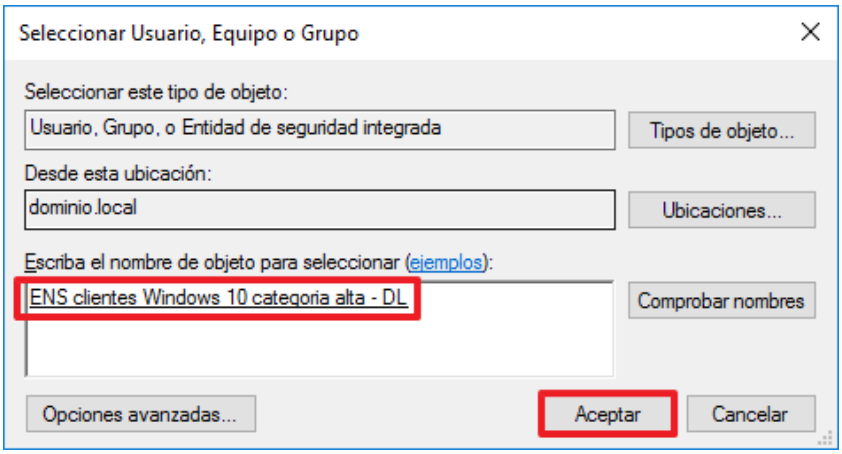
| Paso | Descripción |
|---|---|
| 71. | En el cuadro de diálogo que aparecerá (titulado "Importar la directiva desde"), seleccione la directiva "C:\Windows\security\templates\ CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta-DL.inf" y pulse el botón "Abrir". Con eso habrá quedado importada la plantilla de seguridad en el GPO.   |
| 72. | Con ello, este GPO ("CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL") habrá quedado configurado. En un paso posterior se enlazará al contenedor adecuado de Active Directory para que la configuración sea aplicada. |
| 73. | Cierre el “Editor de administración de directivas de grupo”. |
| 74. | 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 Virtual Delivery Agent”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá.   |

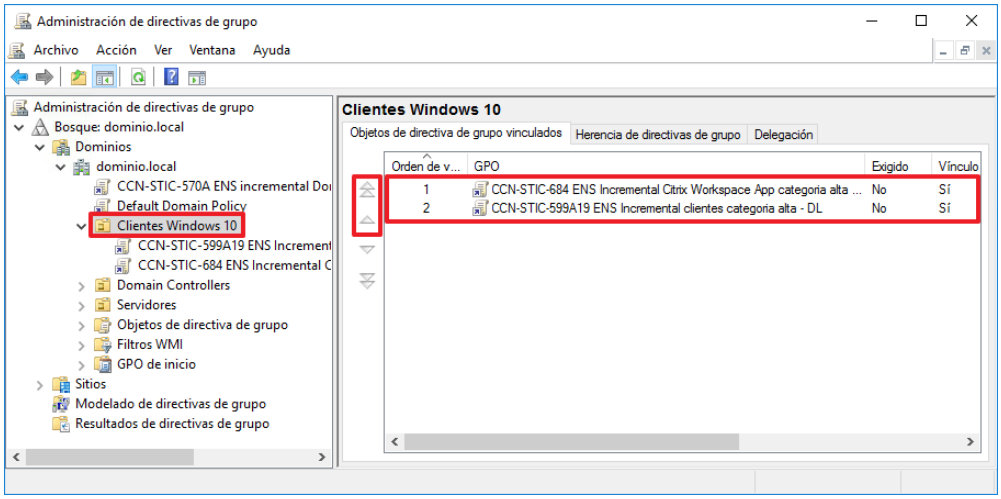
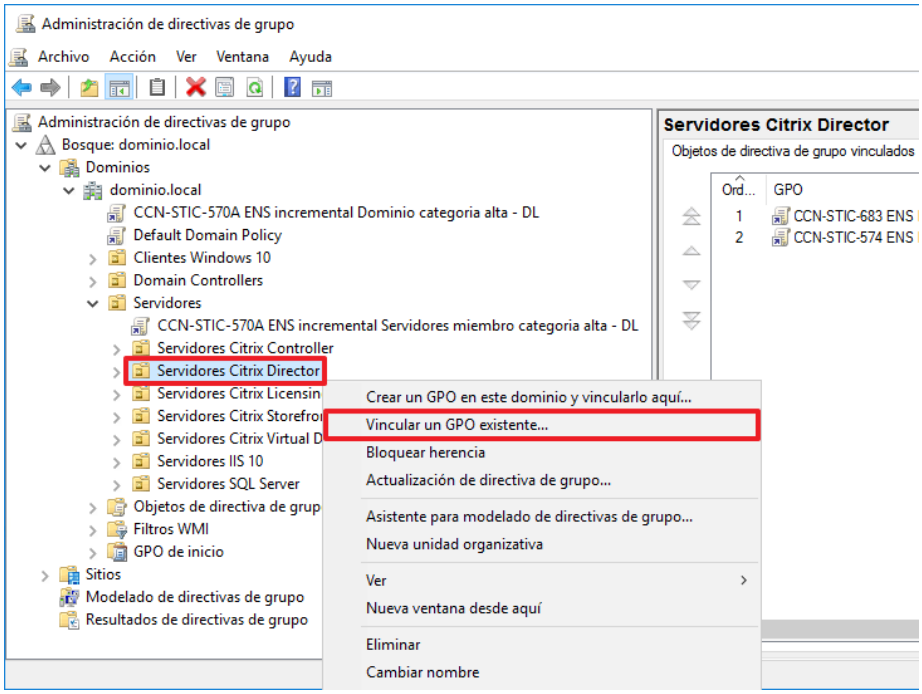
| Paso | Descripción |
|---|---|
| 75. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL” y pulse “Aceptar”.<br>  |
| 76. | Seleccione la política de grupo recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.<br>  |

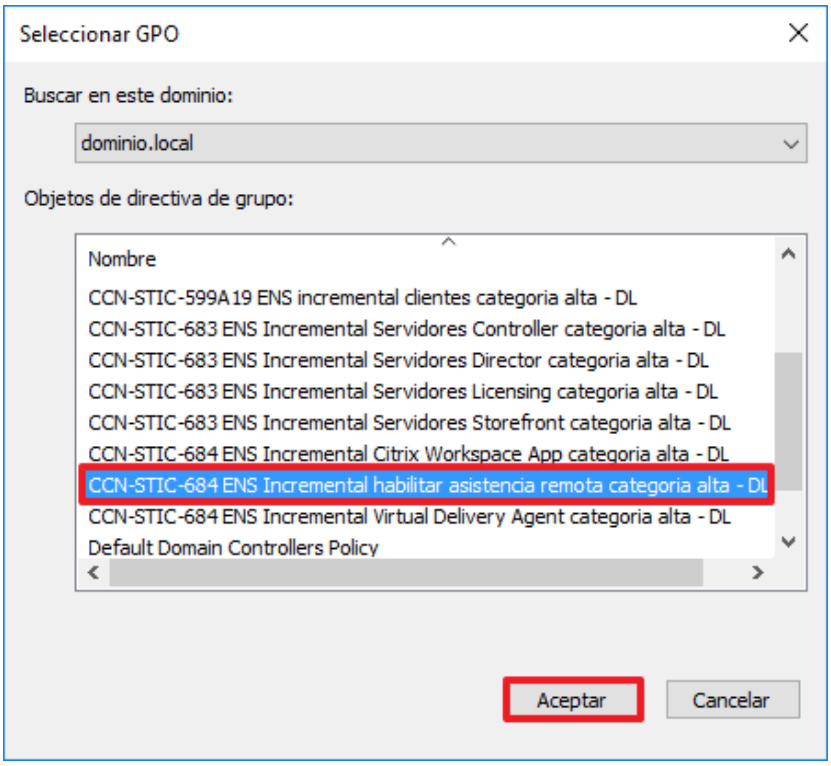
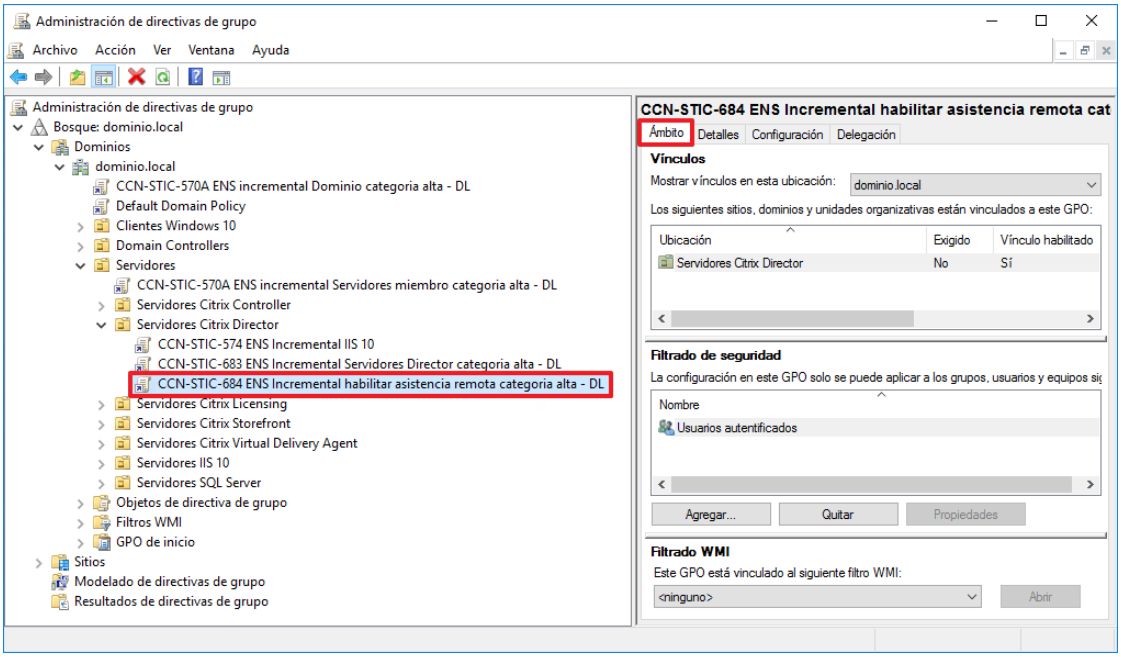
| Paso | Descripción |
|---|---|
| 77. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.<br>  |
| 78. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.<br>  |
| 79. | Una vez quitado, pulse el botón “Agregar…”. |
| 80. | 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”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |

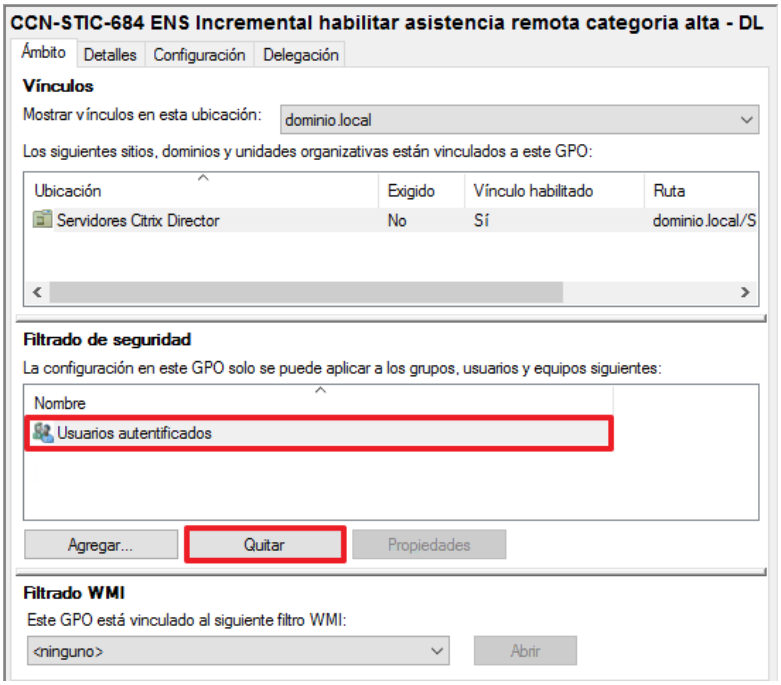
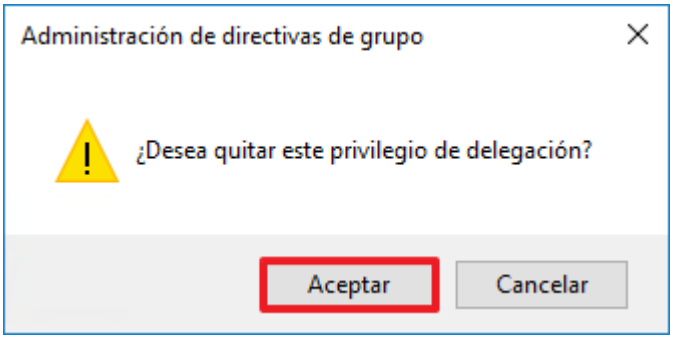
| Paso | Descripción |
|---|---|
| 81. | En la ventana “Administración de directivas de grupo”, expanda y seleccione el contenedor **“Administración de directivas de grupo → Bosque: <nombre de su bosque> → Dominios → <nombre de su dominio> → Clientes Windows 10”**, y marcando con el botón derecho en él, elija la opción "Vincular un GPO existente..." del menú contextual que aparecerá.   |
| 82. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” y pulse “Aceptar”.   |

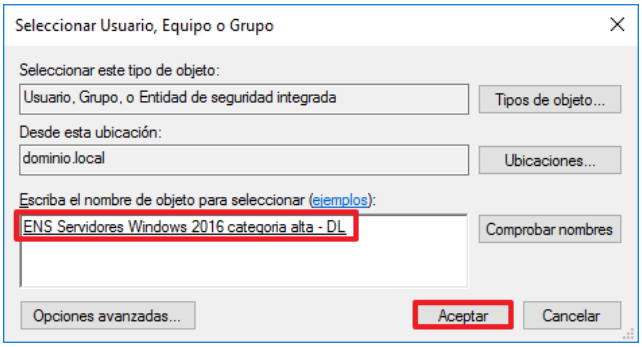
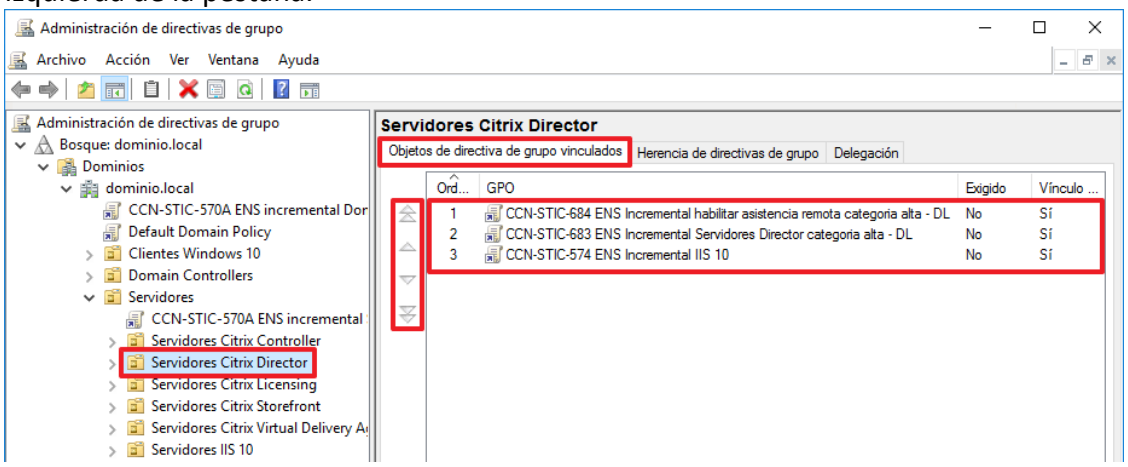
| Paso | Descripción |
|---|---|
| 83. | Seleccione la política de grupo “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.<br>  |
| 84. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.<br>  |

| Paso | Descripción |
|---|---|
| 85. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.<br>  |
| 86. | Una vez quitado, pulse el botón “Agregar…”. |
| 87. | Introduzca como nombre “ENS clientes Windows 10 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-599A19”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |

| Paso | Descripción |
|---|---|
| 88. | Seleccione el contenedor “Clientes Windows 10” 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.<br>– 1 - CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL<br>– 2 - CCN-STIC-599A19 ENS Incremental clientes categoria alta - DL<br>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.<br>  |
| 89. | 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.<br>  |

| Paso | Descripción |
|---|---|
| 90. | En la ventana “Seleccionar GPO” que aparecerá, seleccione el GPO “CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL”.   |
| 91. | Seleccione la política de grupo “CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL” recién vinculada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho.   |

| Paso | Descripción |
|---|---|
| 92. | En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”.   |
| 93. | Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.   |
| 94. | Una vez quitado, pulse el botón “Agregar…”. |

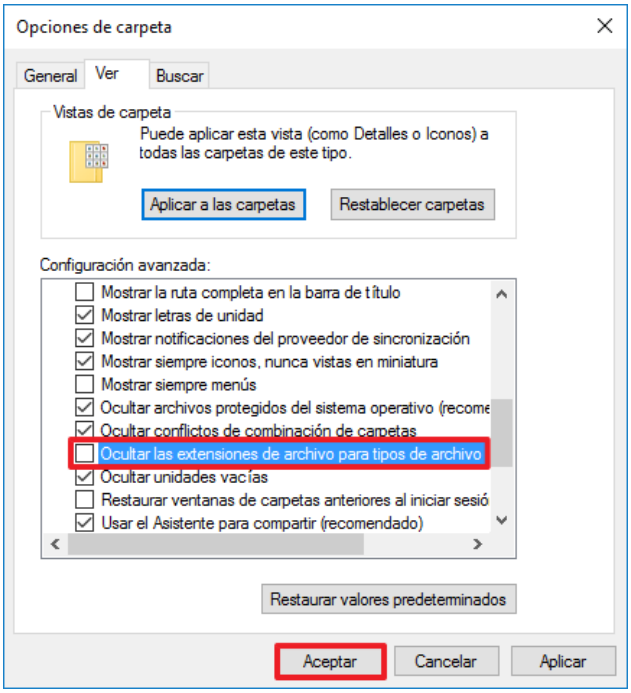
| Paso | Descripción |
|---|---|
| 95. | Introduzca como nombre “ENS servidores Windows 2016 categoria alta - DL”. Este grupo corresponde con el generado en la aplicación de la guía “CCN-STIC-570A”.<br>A continuación, pulse el botón “Aceptar”.<br>  <br>**Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización. |
| 96. | 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.<br>– 1 - CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL<br>– 2 - CCN-STIC-683 ENS Incremental Servidores Director categoria alta - DL<br>– 3 - CCN-STIC-574 ENS Incremental IIS 10<br>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.<br>  |
| 97. | 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. |
| 98. | Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor. |

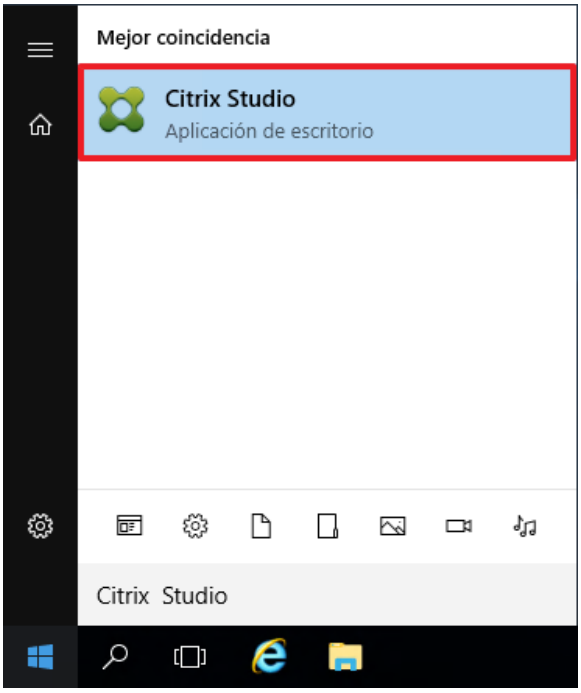
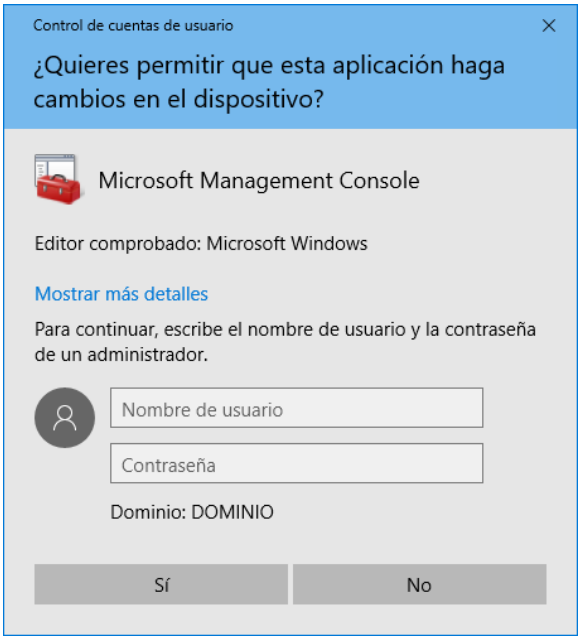
## 2. CONFIGURACIÓN DE SEGURIDAD CITRIX STUDIO

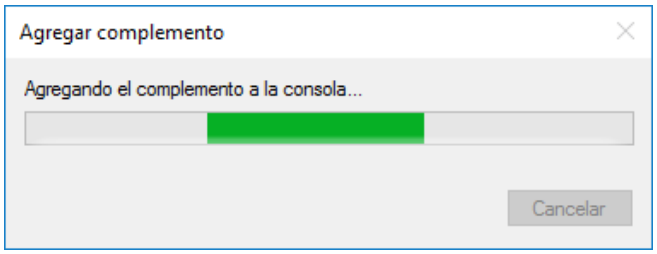
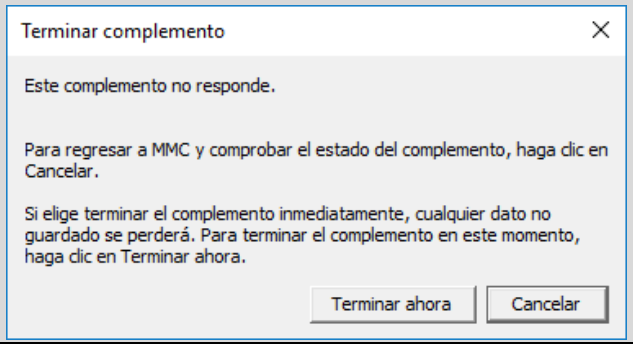
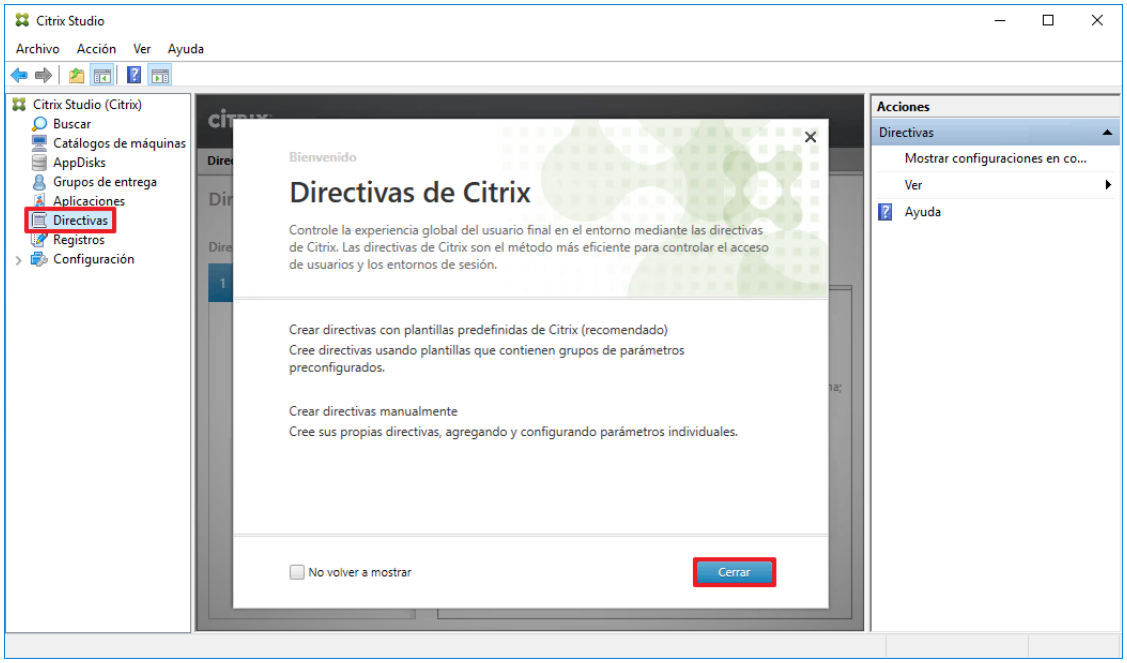
Los pasos que se describen a continuación se realizarán en un servidor con el rol Citrix Controller que haya sido configurado previamente mediante la aplicación de la guía codificada como "CCN-STIC-683 – Categoría Alta / Difusión Limitada". Los pasos descritos a continuación solo los debe realizar cuando vaya a realizar la primera implementación en el dominio, ya que solo es necesario crear las plantillas de seguridad e incorporarlas en la directiva de seguridad una única vez por infraestructura.

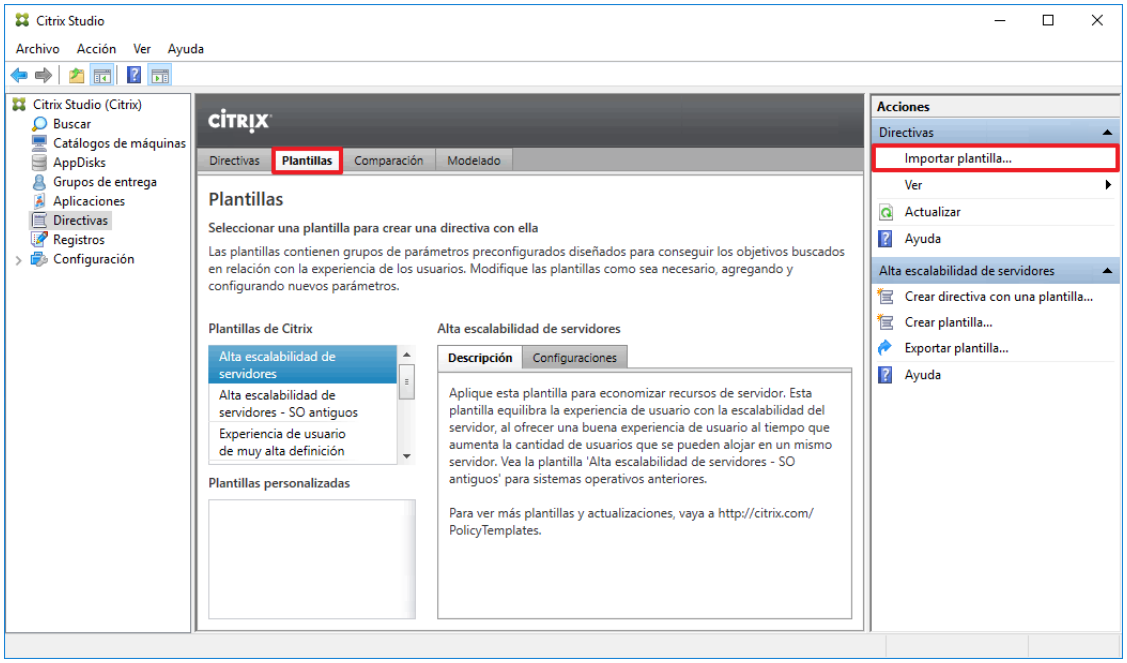
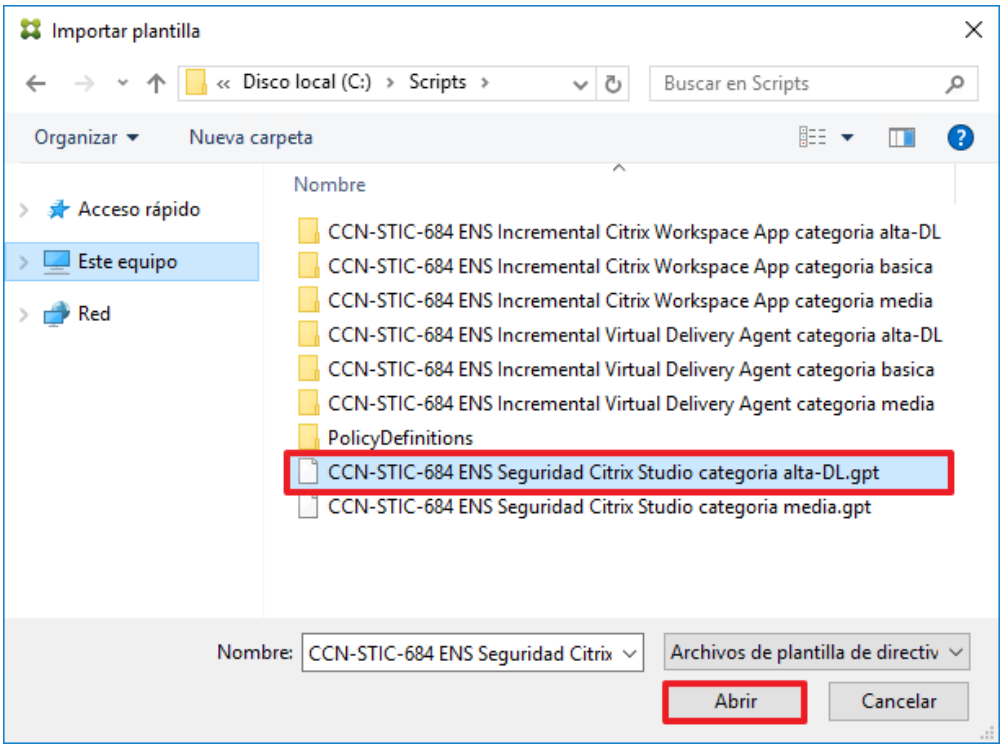
**Nota:** Esta guía asume que al servidor con el rol Citrix Controller se le ha aplicado la configuración descrita en la guía "CCN-STIC-683 Implementación de seguridad en Citrix Virtual Apps and Desktops". Si no es así, aplique la guía correspondiente antes de continuar con la aplicación de ésta.

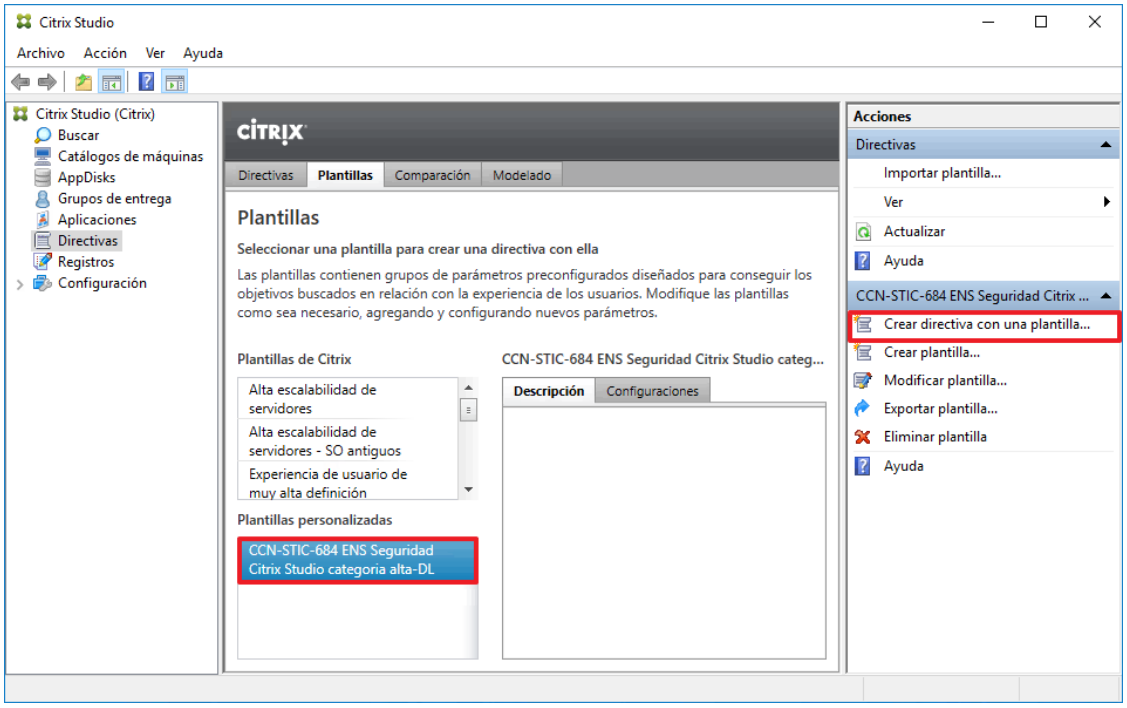
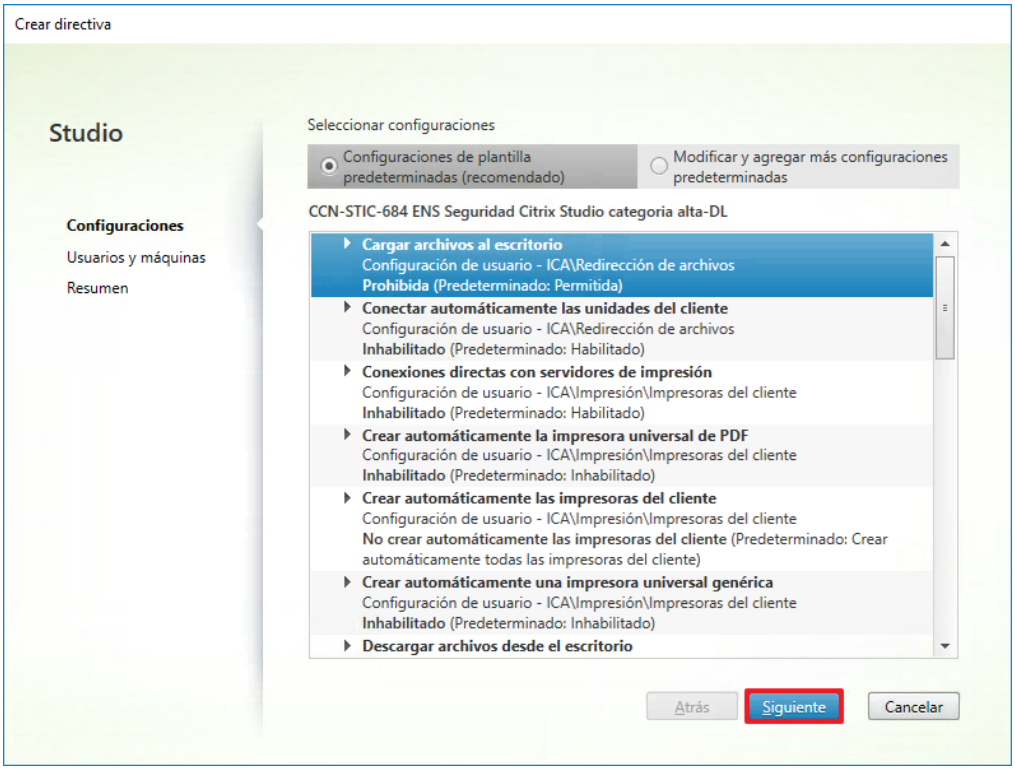
| Paso | Descripción |
|---|---|
| 99. | Inicie sesión en un servidor con el rol Citrix Controller, con una cuenta de administrador del dominio.<br>  |
| 100. | Cree el directorio "Scripts" en la unidad "C:\". |
| 101. | Copie los ficheros y carpetas que acompañan a esta guía en el directorio "C:\Scripts". El sistema solicitará elevación de privilegios. Como mínimo deben aparecer los siguientes ficheros y carpetas.<br>– CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta-DL.gpt |

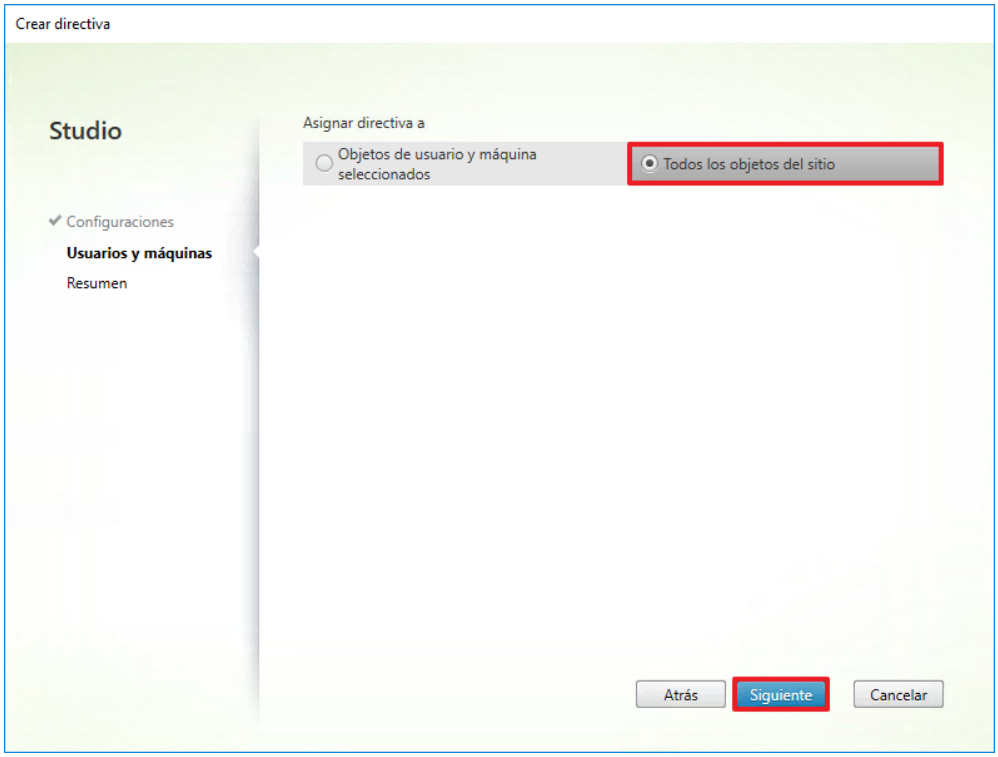
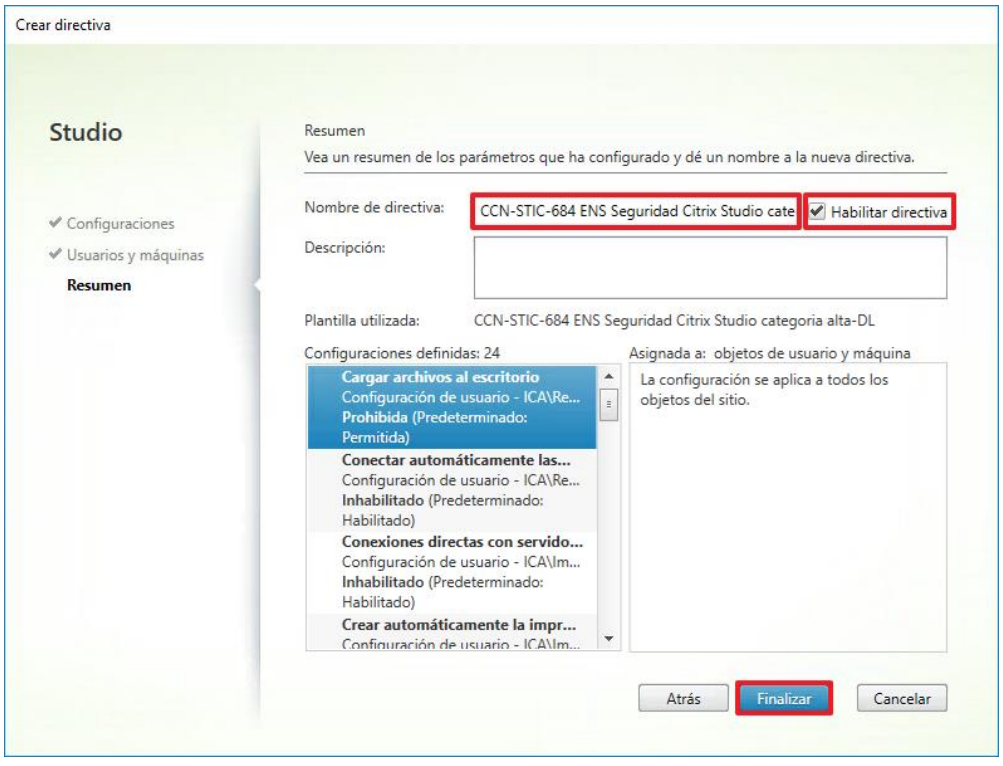
| Paso | Descripción |
|---|---|
| 102. | Si no lo ha realizado durante la implementación de la guía CCN-STIC-570A, configure el Explorador de Windows para que muestre las extensiones de los archivos. Por defecto, Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que Explorador de Windows sí muestra las extensiones de los archivos.<br>Para configurar Explorador de Windows para 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.<br>  |
| 103. | 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". |

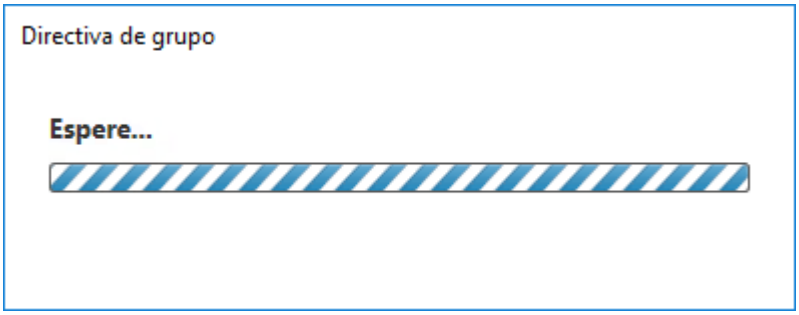
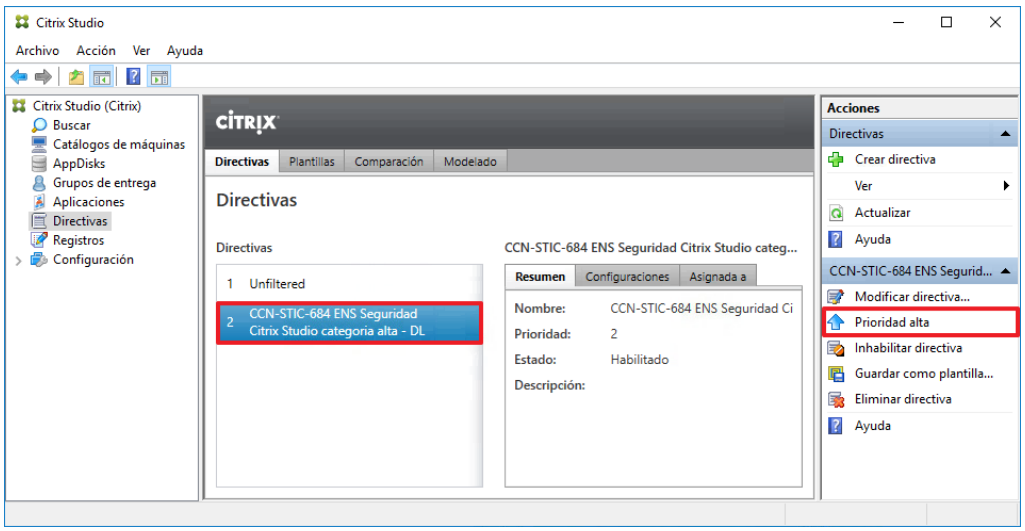
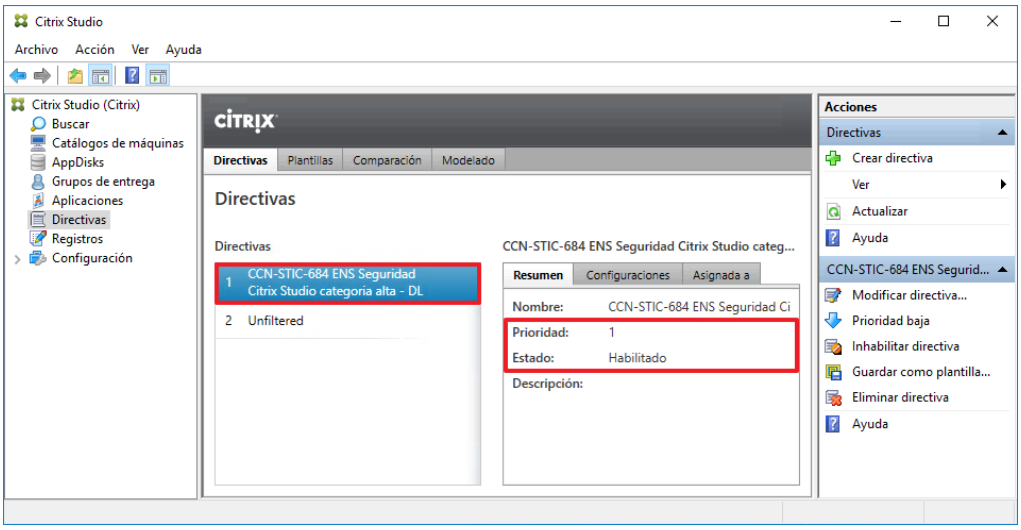
| Paso | Descripción |
|---|---|
| 104. | Ejecute la aplicación “Citrix Studio”.<br>  |
| 105. | El “Control de cuentas de usuario” solicitará que introduzca el nombre de usuario y la contraseña de un administrador. Introduzca el nombre de usuario y contraseña de un administrador que sea miembro del grupo **“Administradores de Citrix”** y pulse “Sí” para continuar.<br>  |

| Paso | Descripción |
|---|---|
| 106. | Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.<br>  <br>**Nota:** Ignore cualquier advertencia que le indique que el complemento no responde. Pulse "Cancelar" para continuar.<br>  |
| 107. | Una vez en la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Directivas"**. En la ventana de bienvenida pulse "Cerrar".<br>  <br>**Nota:** Para evitar que la ventana de bienvenida aparezca cada vez que acceda al nodo "Directivas" seleccione la casilla "No volver a mostrar". |

| Paso | Descripción |
|---|---|
| 108. | Proceda en este punto a importar la plantilla de seguridad de Citrix Studio. Para ello, acceda a la opción "Importar plantilla…" en la ruta **"Citrix Studio → Directivas → Plantillas → Acciones → Directivas → Importar plantillas…"**.<br>  |
| 109. | En el cuadro de diálogo que aparecerá (titulado "Importar plantilla"), seleccione la directiva "C:\Scripts\CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta-DL.gpt" y pulse el botón "Abrir".<br>Con eso habrá quedado importada la plantilla de seguridad.<br>  |

| Paso | Descripción |
|---|---|
| 110. | Aparecerá la plantilla recién importada en el apartado “Plantillas personalizadas”. Seleccione la plantilla y haga clic en “Crear directiva con una plantilla…”.   |
| 111. | Se abrirá el asistente de creación de directivas de Citrix Studio. Puesto que con la importación de la plantilla en pasos anteriores se asignan las configuraciones necesarias no modifique ningún parámetro. Pulse “Siguiente” para continuar.   |

| Paso | Descripción |
|---|---|
| 112. | En la ventana “Asignar directiva a” seleccione “Todos los objetos del sitio”. Pulse “Siguiente” para continuar.<br>  |
| 113. | Por último, asigne el nombre “CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL” a la directiva recién creada. Marque la opción “Habilitar directiva” y pulse “Finalizar” para completar la creación de la directiva.<br>  |

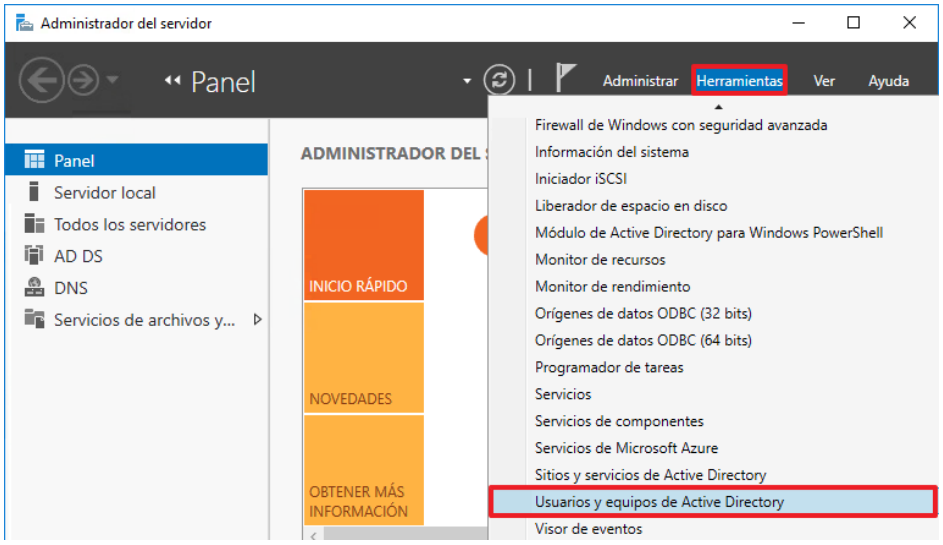
| Paso | Descripción |
|---|---|
| 114. | Espere a que finalice el proceso de creación de la directiva.<br>  |
| 115. | Para finalizar la configuración de la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL” diríjase al nodo de configuración **“Citrix Studio → Directivas”** y seleccionando la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL” sitúela con el mayor nivel de prioridad haciendo uso de la opción “Prioridad alta”.<br>  |
| 116. | Verifique que la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL” ha quedado configurada con la prioridad 1 y que es estado de la misma es “Habilitado”.<br>  |

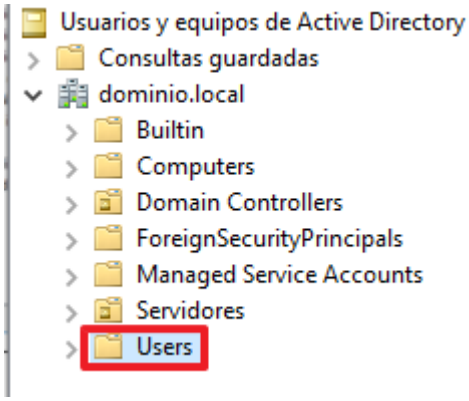
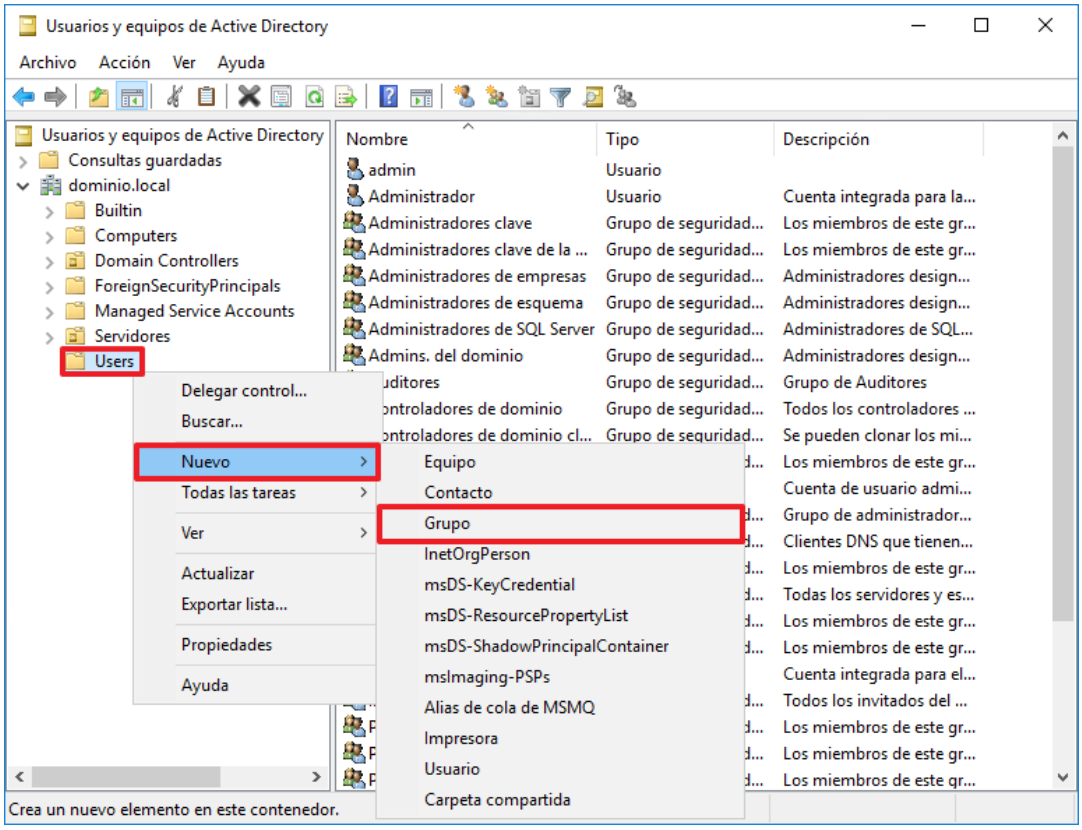
| Paso | Descripción |
|---|---|
| 117. | En este punto se encuentran configuradas las directivas de seguridad de Citrix Studio que serán de aplicación a los recursos que se publiquen desde la infraestructura. |
| 118. | Ya puede cerrar todas las consolas abiertas y eliminar la carpeta “C:\Scripts” del servidor. |

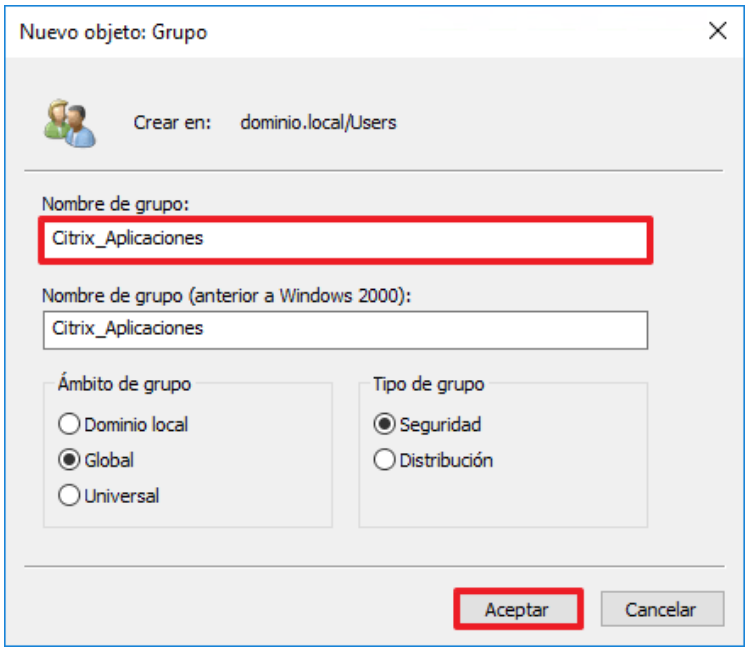
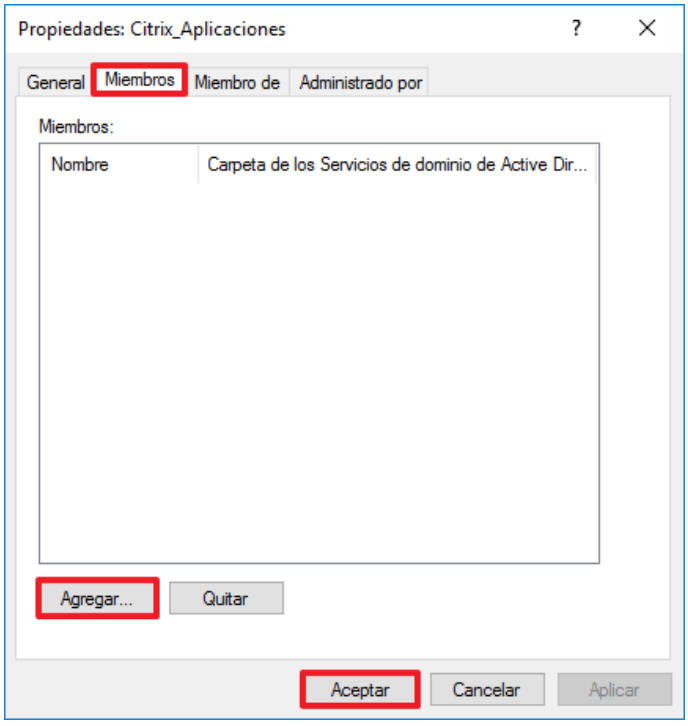
## 3. SEGREGACIÓN DE ROLES

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.

En los siguientes pasos se procederá a crear, a modo de ejemplo, un grupo de usuarios a los que se les concederá el acceso a un determinado recurso de la infraestructura.

| Paso | Descripción |
|---|---|
| 119. | Inicie sesión en un servidor Controlador de Dominio del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 120. | 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.<br>  |

| Paso | Descripción |
|---|---|
| 121. | Expanda el contenedor **"Usuarios y equipos de Active Directory → <nombre de su dominio> → Users"**, como se muestra en la siguiente figura.   |
| 122. | Pulsando con el botón derecho sobre "Users" diríjase al apartado de configuración **"Nuevo → Grupo"**.   |

| Paso | Descripción |
|---|---|
| 123. | Sobre la ventana emergente para la creación del nuevo grupo introduzca “Citrix_Aplicaciones” y pulse sobre “Aceptar” como se indica en la siguiente imagen.<br>  |
| 124. | A continuación, deberá agregar los usuarios que tendrán acceso al grupo de entrega de “Aplicaciones” al grupo de seguridad “Citrix_Aplicaciones”. 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”.<br>  |

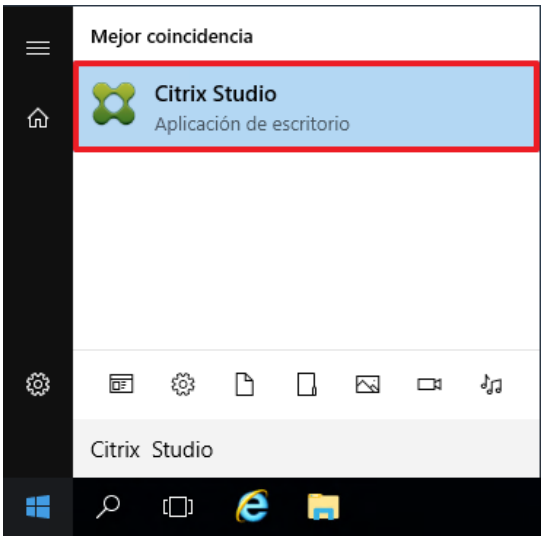
## 4. GESTIÓN DE DERECHOS DE ACCESO

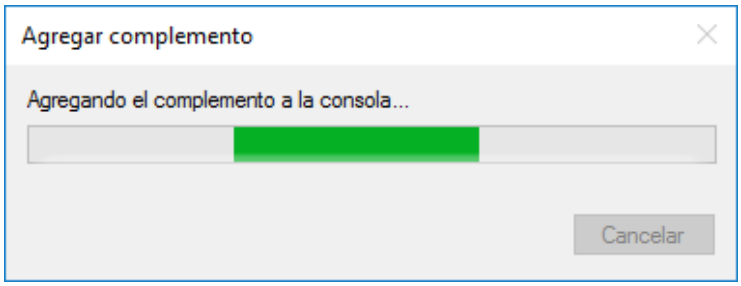
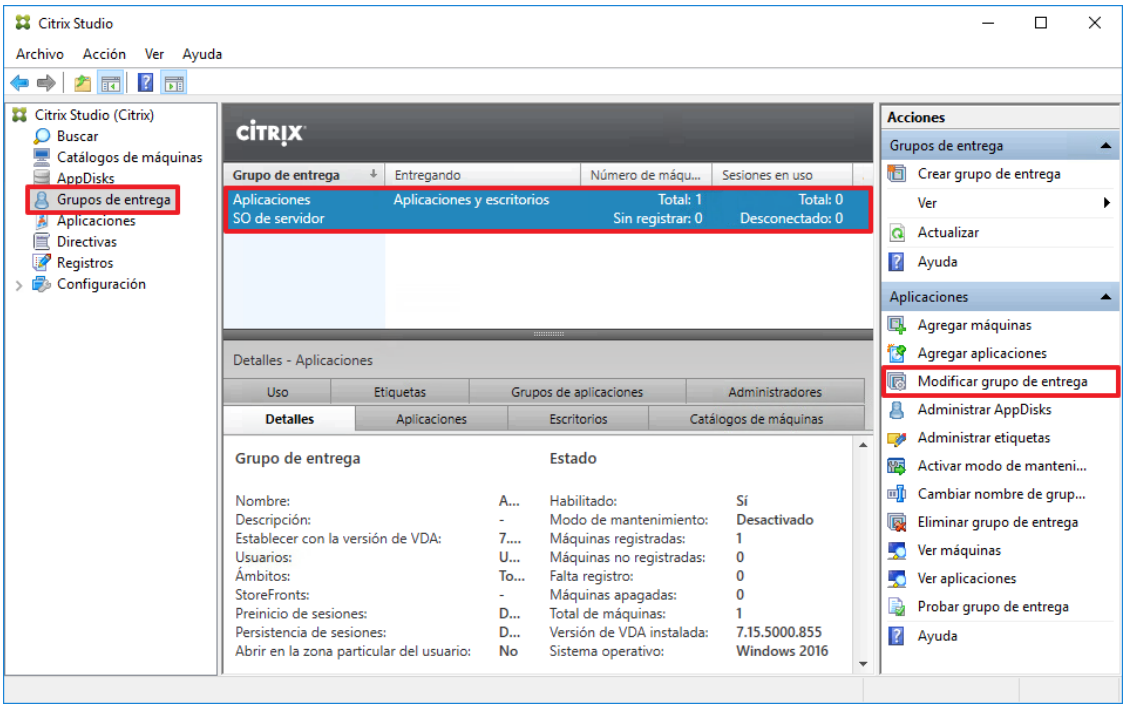
Citrix Virtual Apps and Desktops se encuentra facultado para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

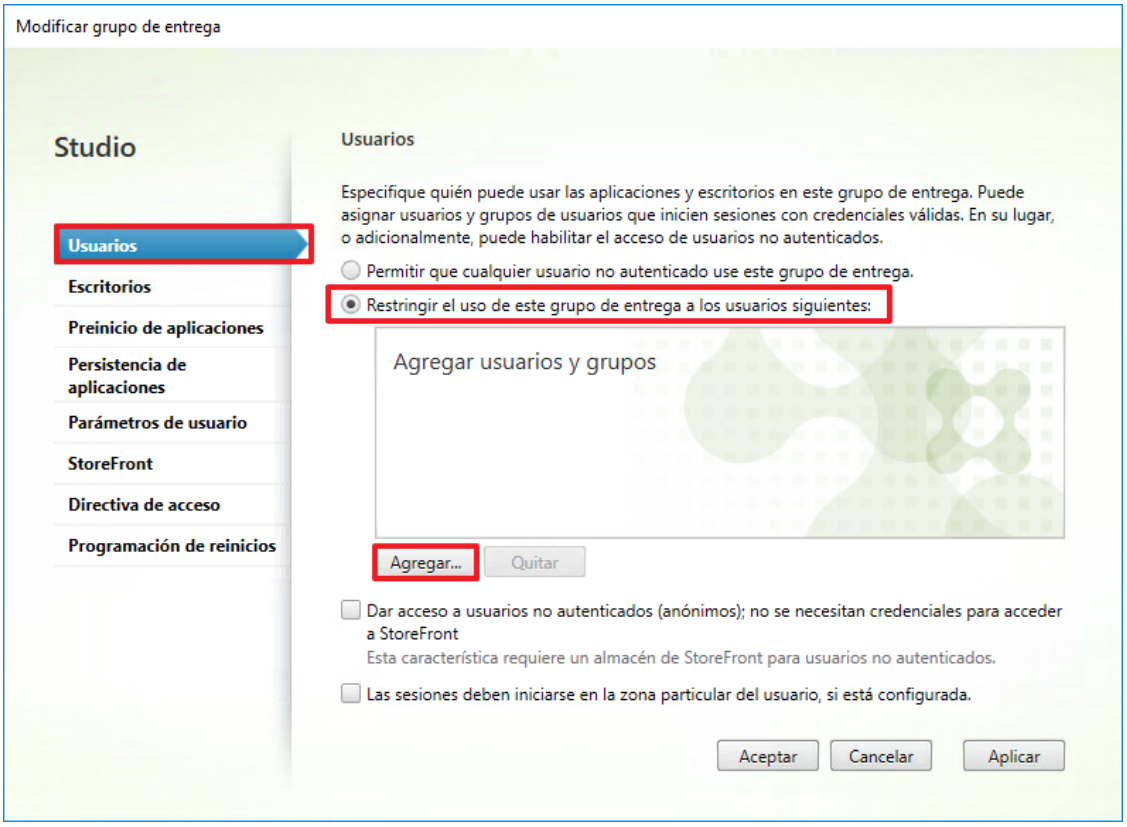
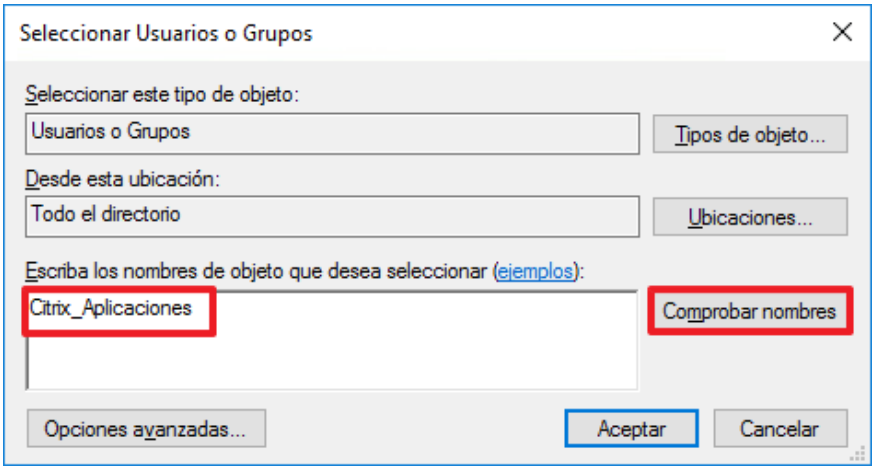
Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda acceder a recursos que no son requeridos para las funciones que desempeña.

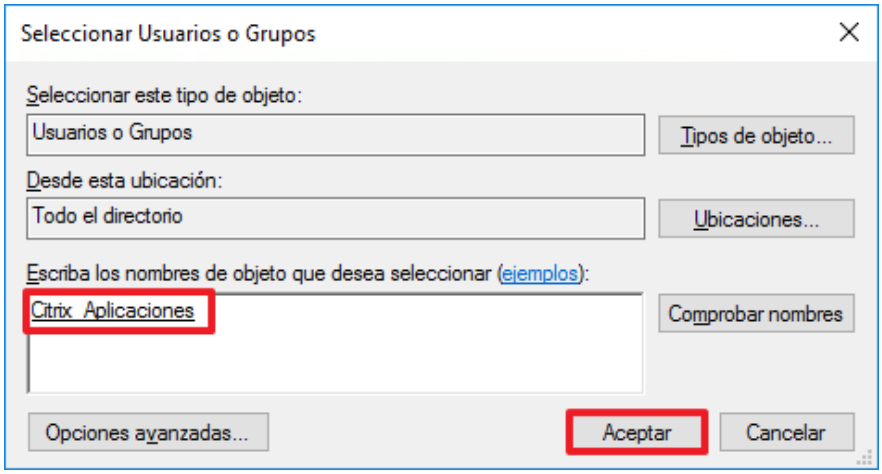
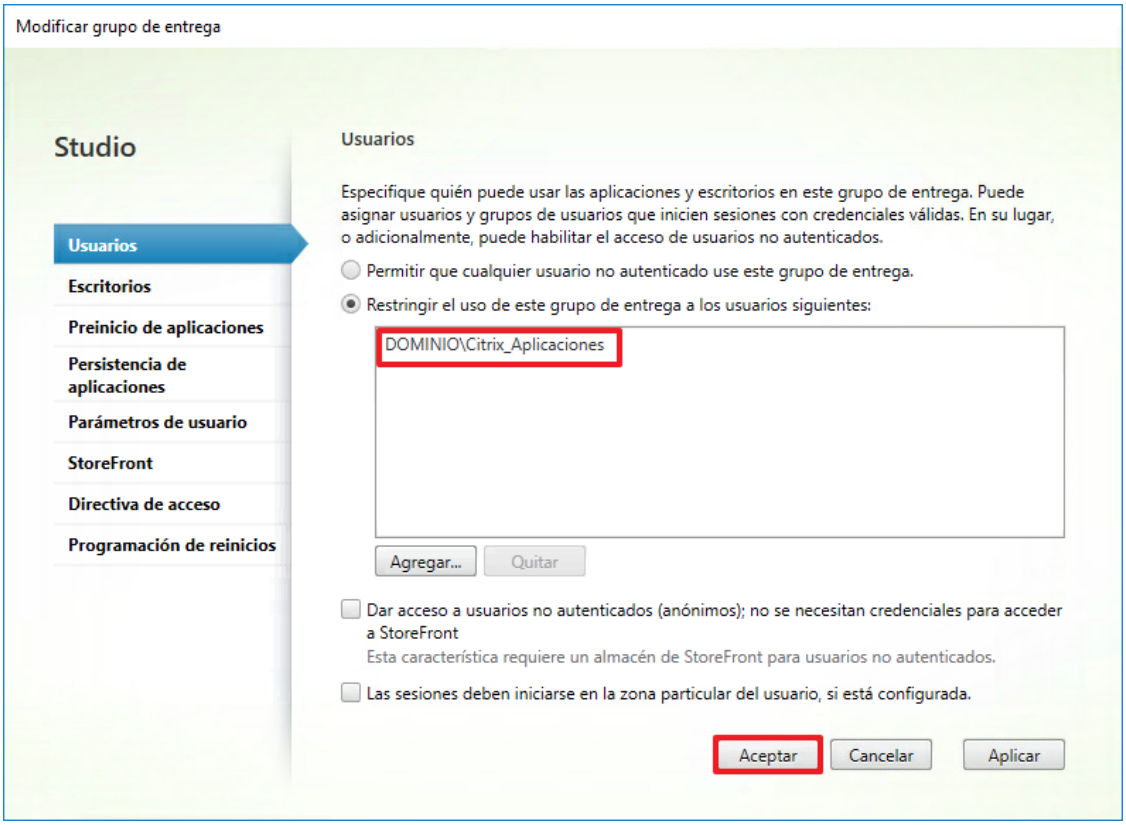
Para tal fin y de acuerdo con el Esquema Nacional de Seguridad se deberán definir, mediante grupos de seguridad, los usuarios que tengan acceso a los recursos de la infraestructura.

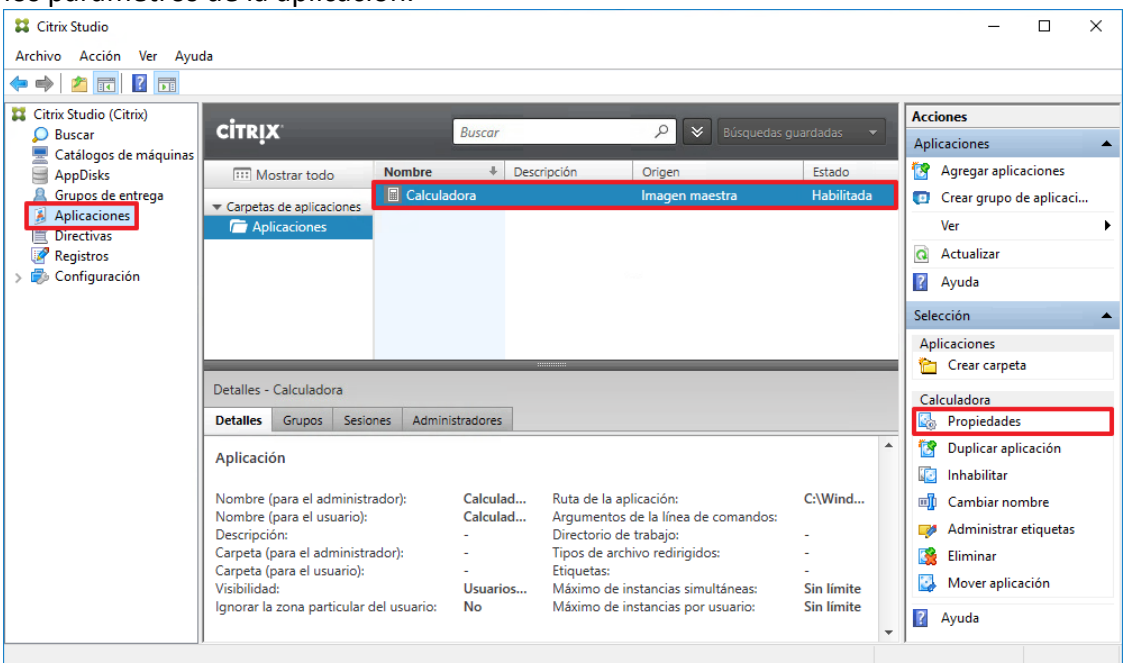
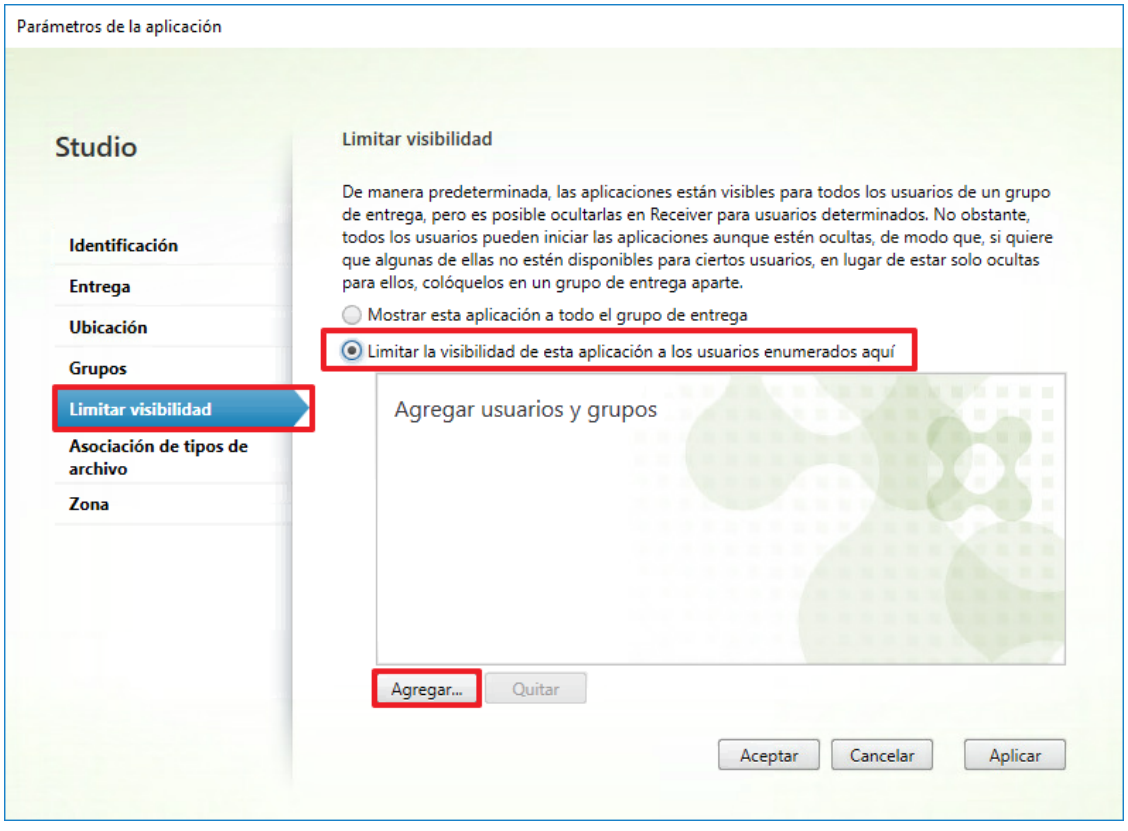
Esta configuración será de aplicación en el servidor con el rol Citrix Controller mediante la consola de administración Citrix Studio. Se limitarán, mediante grupos de seguridad, los usuarios con acceso a los diferentes grupos de entrega de la infraestructura de Citrix Virtual Apps and Desktops.

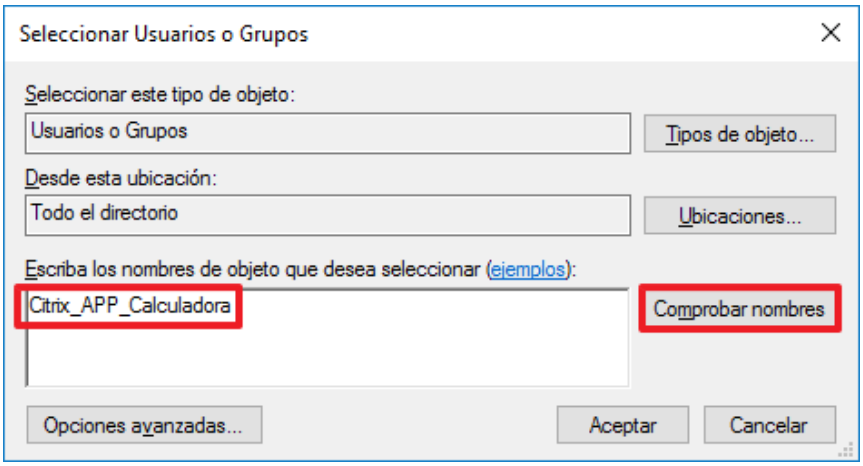
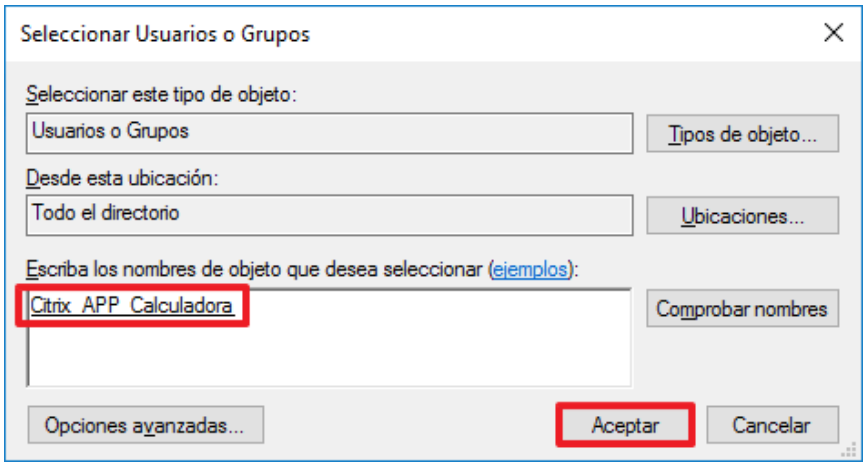
| Paso | Descripción |
|---|---|
| 125. | Inicie sesión en un servidor con el rol Citrix Controller del dominio donde se va a aplicar seguridad según criterios de ENS.<br>  <br>**Nota:** Deberá iniciar sesión con una cuenta que sea administrador del dominio. |
| 126. | Si no lo ha hecho todavía, busque e inicie la aplicación Citrix Studio.<br>  <br>**Nota:** El sistema solicitará elevación de privilegios. |

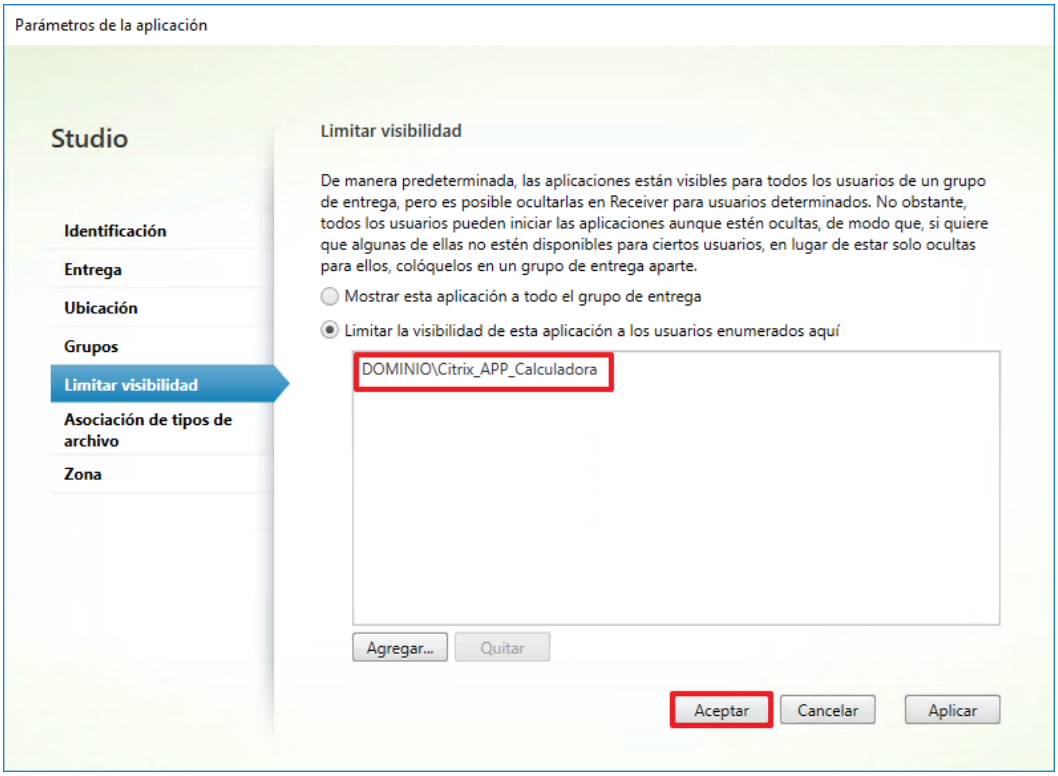
| Paso | Descripción |
|---|---|
| 127. | Espere a que la consola abra completamente, puede demorarse dependiendo del entorno.<br>  |
| 128. | Diríjase al menú de configuración **"Citrix Studio → Grupos de entrega → [Su grupo de entrega]"** y pulse sobre "Modificar grupo de entrega" para modificar los parámetros de su grupo de entrega.<br>  |

| Paso | Descripción |
|---|---|
| 129. | En la ventana “Modificar grupo de entrega” sitúese en la pestaña “Usuarios” y seleccionando “Restringir el uso de este grupo de entrega a los usuarios siguientes:” seleccione la opción “Agregar…”.<br>  |
| 130. | Introduzca el nombre del objeto “Citrix_Aplicaciones” y pulse sobre “Comprobar nombres”.<br>  <br>**Nota:** En esta guía se usa de ejemplo el grupo de seguridad “Citrix_Aplicaciones” adapte este paso a los requisitos de su organización. |

| Paso | Descripción |
|---|---|
| 131. | Compruebe que el objeto “Citrix_Aplicaciones” ha sido añadido correctamente. Pulse “Aceptar” para añadir el objeto y cerrar la ventana.<br>  |
| 132. | El objeto aparecerá añadido. Pulse “Aceptar” para guardar los cambios. Desde este momento, únicamente los usuarios especificados en el grupo de seguridad que acaba de añadir podrán acceder al recurso publicado.<br>  |
| 133. | Para el cumplimiento del ENS en su categoría alta - DL, será necesario así mismo restringir la visibilidad de cada una de las aplicaciones, a grupos específicos de usuarios que harán uso de las mismas. |

| Paso | Descripción |
|---|---|
| 134. | A continuación, se procederá a limitar la visibilidad de una aplicación entregada a únicamente el grupo de usuarios que harán uso de esa aplicación. Para ello, acceda al nodo **"Citrix Studio → Aplicaciones → [Su aplicación] → Propiedades"** para modificar los parámetros de la aplicación.   |
| 135. | En la ventana "Parámetros de la aplicación", sitúese en la pestaña "Limitar visibilidad", y seleccionando "Limitar la visibilidad de esta aplicación a los usuarios enumerados aquí" seleccione la opción "Agregar…".   |

| Paso | Descripción |
|---|---|
| 136. | En la ventana resultante introduzca el grupo de seguridad que engloba a los usuarios que harán uso de esta aplicación y pulse en “Comprobar nombres”.<br>  <br>**Nota:** En esta guía se usa de ejemplo el grupo de seguridad “Citrix_App_Calculadora” adapte este paso a los requisitos de su organización. |
| 137. | Una vez comprobado que el objeto existe pulse “Aceptar”.<br>  |

| Paso | Descripción |
|---|---|
| 138. | El objeto aparecerá añadido. Pulse “Aceptar” para guardar los cambios. Desde este momento, únicamente los usuarios especificados en el grupo de seguridad que acaba de añadir podrán ver la aplicación publicada.<br>  |
| 139. | En este punto los recursos se encuentran configurados para la entrega de los mismos a los usuarios de forma segura. |

## ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA PARA PUBLICACIÓN DE APLICACIONES Y ESCRITORIOS CON CITRIX VIRTUAL APPS AND DESKTOPS

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los equipos 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 tanto en el servidor con el rol Citrix Controller como en los equipos con el rol Citrix Virtual Delivery Agent.

**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 EN APLICACIONES Y ESCRITORIOS VIRTUALES CON CITRIX VIRTUAL APPS AND DESKTOPS QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS/DIFUSIÓN LIMITADA”.

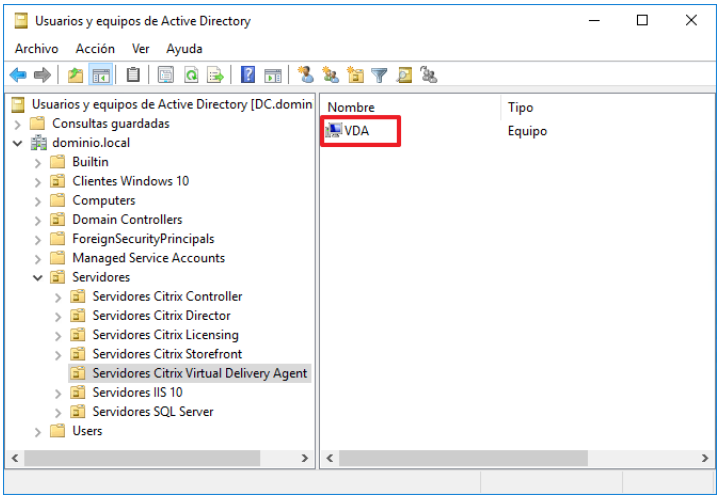
# 1. CONTROLADOR DE DOMINIO

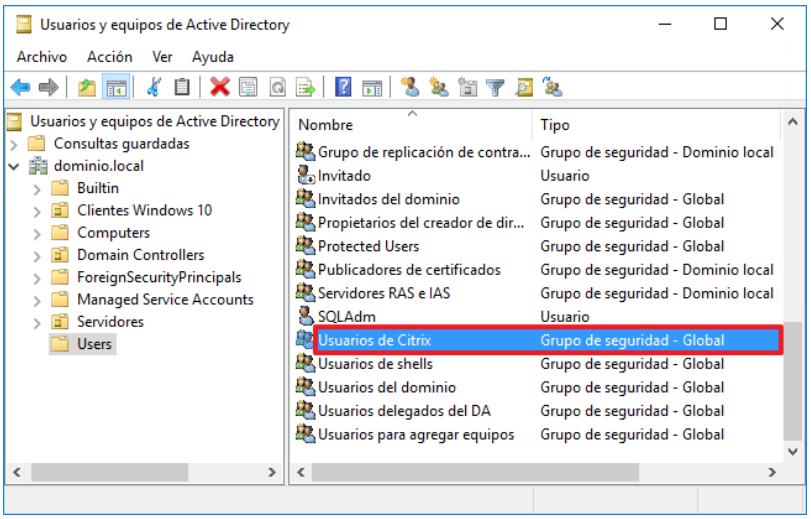
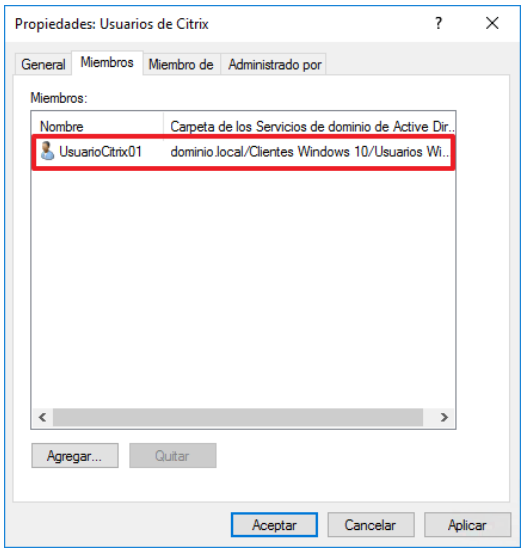
Los siguientes pasos determinan el procedimiento para verificar la configuración del dominio en el que se despliega el sistema de virtualización.

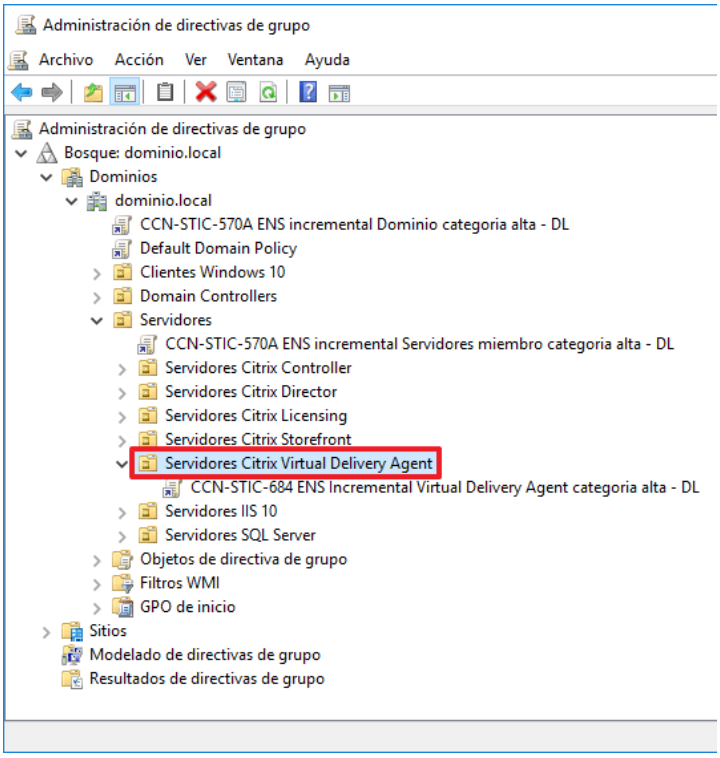
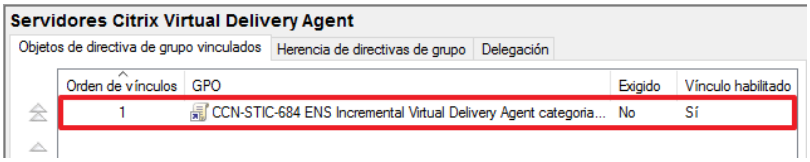
Las consolas y herramientas que se utilizarán son las siguientes:

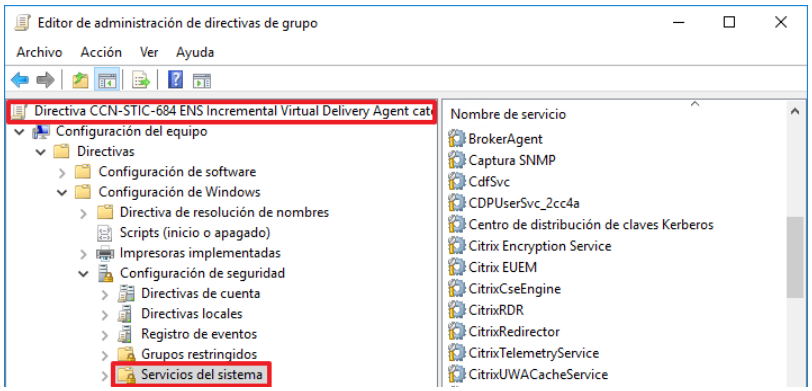
a) Usuarios y equipos de Active Directory (dsa.msc).

b) 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 equipos. | | Ejecute la herramienta "Usuarios y equipos de Active Directory" desde:<br>"**Menú inicio → Herramientas administrativas → Usuarios y equipos de Active Directory**".<br>El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio. |
| 3. La unidad organizativa "Servidores Citrix Virtual Delivery Agent" debe albergar todos los equipos con el rol Virtual Delivery Agent. | | En la consola "Usuarios y equipos de Active Directory", localice la unidad organizativa "Servidores Citrix Virtual Delivery Agent" En ella, deberá aparecer al menos un equipo.<br>  <br>**Nota:** El nombre del equipo de ejemplo es "VDA", en su caso debe figurar el nombre de su equipo. |

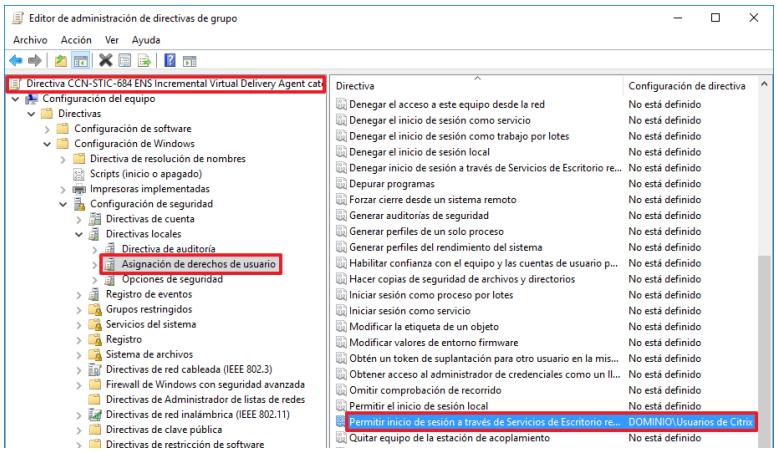
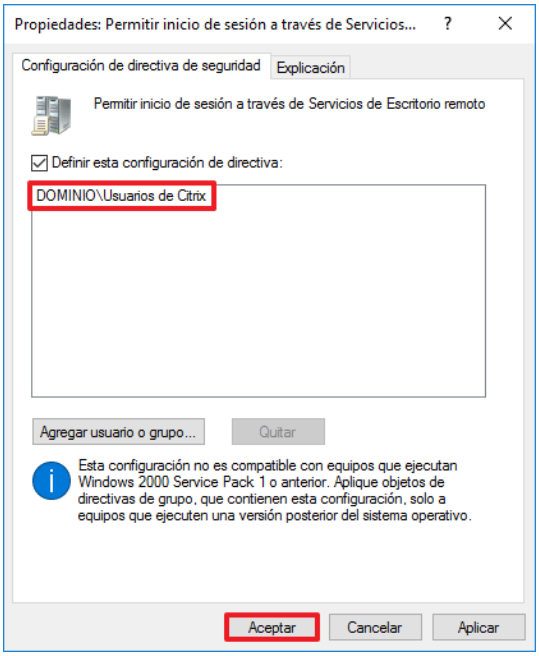
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 4. Verifique que está creado el grupo de seguridad “Usuarios de Citrix”. | | En la consola “Usuarios y equipos de Active Directory”, localice la unidad organizativa “Users” en ella, deberá aparecer el grupo de seguridad “Usuarios de Citrix”.<br>  |
| 5. Compruebe que el grupo de seguridad “Usuarios de Citrix” aloja sus respectivos usuarios. | | Compruebe que en la pestaña “Miembros” de las propiedades del grupo de seguridad “Usuarios de Citrix” se encuentran aquellos usuarios que harán uso de la infraestructura.<br>  |

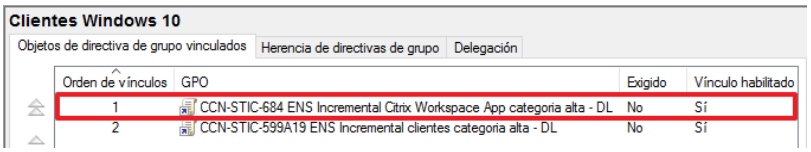
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 6. Verifique que están creadas las directivas de configuración de Citrix Virtual Delivery Agent. | | Ejecute la herramienta "Administración de directivas de grupo" desde:<br>**"Menú inicio → Herramientas administrativas → Administración de directivas de grupo"**.<br>El sistema le solicitará elevación de privilegios para acceder a la consola de administración, introduzca el nombre y contraseña de un administrador del dominio.<br>Seleccione la unidad organizativa "Servidores Citrix Virtual Delivery Agent", situada en **"Bosque [Su bosque] → Dominios → [Su dominio] → Servidores → Servidores Citrix Virtual Delivery Agent"**.<br>  |
| 7. Verifique las políticas aplicadas a "Servidores Citrix Virtual Delivery Agent". | | Revise que la unidad organizativa "Servidores Citrix Virtual Delivery Agent", como mínimo, tiene aplicada la siguiente directiva y tiene el vínculo habilitado.<br>– "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL"<br>  |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 8. Verifique los valores de los servicios del sistema de la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL". | | Seleccione la directiva y, con el botón derecho del ratón, despliegue el menú y seleccione "Editar". Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL" tiene los siguientes valores de servicios de sistema.<br>**"CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema"**.<br>  <br>**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 Audio Redirection Service | CtxAudioSrv | Automático | |
| Citrix Audio Redirection Service | CtxAudioSvc | Automático | |
| Citrix CEIP Service for Vda | CitrixVdaCeipService | Deshabilitado | |
| Citrix Desktop Service | BrokerAgent | Automático | |
| Citrix Device Redirector Service | CitrixRDR | Automático | |
| Citrix Device Redirector Service | CitrixRedirector | Automático | |
| Citrix Diagnostic Facility COM Server | CdfSvc | Automático | |
| Citrix Dynamic Virtual Channel Service | PicaDvcControllerSvc | Automático | |
| Citrix Encryption Service | Citrix Encryption Service | Automático | |
| Citrix End User Experience Monitoring Service | Citrix EUEM | Automático | |
| Citrix Group Policy Engine | CitrixCseEngine | Automático | |
| Citrix HDX HTML5 Video Redirection Service | CtxHdxWebSocketService | Automático | |
| Citrix ICA Service | PorticaService | Automático | |
| Citrix Location and Sensor Virtual Channel Service | CtxSensVcSvc | Automático | |

| Comprobación | OK/NOK | Cómo hacerlo | | |
|---|---|---|---|---|
| **Servicio (nombre largo)** | | **Servicio (nombre corto)** | **Inicio** | **OK/NOK** |
| Citrix Mobile Receiver Virtual Channel Service | | MRVCSvc | Automático | |
| Citrix Multi Touch Redirection Service | | CtxMultiTouchSvc | Automático | |
| Citrix Print Manager Service | | cpsvc | Automático | |
| Citrix Profile Management | | CtxProfile | Automático | |
| Citrix Pvs for VMs agent | | PvsVmAgent | Automático | |
| Citrix Services Manager | | ServicesManager | Automático | |
| Citrix Smart Card Certificate Propagation Service | | CtxSCardCertPropSvc | Automático | |
| Citrix Smart Card Removal Policy Service | | CtxScardRemovalPolicySvc | Automático | |
| Citrix Smart Card Service | | CtxSmartCardSvc | Automático | |
| Citrix Stack Control Service | | StackControlService | Automático | |
| Citrix Telemetry Service | | CitrixTelemetryService | Deshabilitado | |
| Citrix UWA Cache Service | | CitrixUWACacheService | Automático | |
| Cola de Impresión | | Spooler | Automático | |
| Estación de trabajo | | LanmanWorkstation | Automático | |
| Iniciador de procesos de servidor DCOM | | DcomLaunch | Automático | |
| Llamada a procedimiento remoto (RPC) | | RpcSs | Automático | |
| Servicio Citrix HDX MediaStream para Flash | | CtxFlashSvc | Automático | |
| Servicio Informe de errores de Windows | | WerSvc | Automático | |
| Servicio Interfaz de almacenamiento en red | | nsi | Automático | |
| Servicios de Escritorio Remoto | | TermService | Manual | |
| Solicitante de instantaneas de volumen de Hyper-V | | vmicvss | Manual | |
| 9. Verifique los valores de asignación de derechos de usuario de la directiva “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL”. | | Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL” tiene configurados los valores de asignación de derechos de usuario. **“CCN-STIC-684 Incremental Virtual Delivery Agent categoria alta – DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad →Directivas locales → Asignación de derechos de usuario”**. | | |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| | |  <br>Compruebe que la directiva “Permitir inicio de sesión a través de Servicios de Escritorio remoto” se encuentra definida y que al menos muestra el grupo “Usuarios de Citrix”.<br>  |
| 10. Verifique los valores de Opciones de inicio de sesión de Windows de la directiva "CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL". | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva "CCN-STIC-684 Incremental Virtual Delivery Agent" tiene los siguientes valores en la siguiente ubicación:<br>**“Directiva CCN-STIC-684 ENS Incremental Virtual Delivery Agent categoria alta - DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Windows → Opciones de inicio de sesión de Windows”.**<br>Una vez comprobado, cierre el “Editor de administración de directivas de grupo”. |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario.</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>11. Verifique las políticas aplicadas a “Clientes Windows 10”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Clientes Windows 10”, situada en “Bosque [Su bosque] → Dominios → [Su dominio] → Clientes Windows 10” y revise que, como mínimo, tiene aplicada la siguiente directiva, tiene el vínculo habilitado y se encuentra situada en primer lugar.<br>– “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”<br> 
</td></tr>
<tr><td rowspan="2">12. Verifique los valores para Actualizaciones de Citrix Workspace de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”.</td><td></td><td colspan="3">Pulse el botón derecho sobre la directiva y seleccione “Editar” en el menú que se ha desplegado. Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Actualizaciones de Citrix Workspace”.</td></tr>
<tr><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Actualizaciones de Citrix Workspace</td><td>Deshabilitada</td><td></td></tr>
</table></td></tr>
<tr><td>13. Verifique los valores para autoservicio de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Autoservicio”.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="4"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">EnableFTU</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir a los usuarios agregar o quitar cuentas</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Permitir/impedir que los usuarios publiquen contenido no seguro</td><td>Habilitada (Impedir)</td><td></td></tr>
<tr><td rowspan="9">14. Verifique los valores para Opciones de preferencias avanzadas de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Autoservicio → Opciones de Preferencias avanzadas”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Ocultar Central de conexiones</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar Citrix Casting</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar Citrix Files</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar Eliminar contraseñas guardadas</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar información de asistencia</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar parámetros de PPP</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Ocultar recopilación de datos</td><td>Habilitada</td><td></td></tr>
<tr><td rowspan="5">15. Verifique los valores para CEIP de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → CEIP”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Configuración de CEIP</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Habilitar CEIP</td><td>Deshabilitada</td><td></td></tr>
</table>

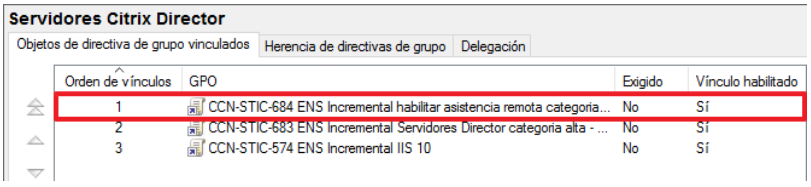
| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 16. Verifique los valores para Conformidad de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”. | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación: **“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Conformidad”**. |

| Directiva | Valor | OK/NOK |
|---|---|---|
| Inhabilitar el envío de datos a terceros | Habilitada | |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 17. Verifique los valores para Diagnóstico de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”. | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación: **“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Diagnóstico”**. |

| Directiva | Valor | OK/NOK |
|---|---|---|
| Seguimiento permanente | Habilitada | |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 18. Verifique los valores para Uso remoto de dispositivos del cliente de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”. | | Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación: **“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Uso remoto de dispositivos del cliente”**. |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td rowspan="8"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Acceso al hardware del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Asignación de unidades del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Captura de imágenes</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Dispositivos Plug-n-Play USB</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Impresoras del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Micrófono del cliente</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Portapapeles</td><td>Deshabilitada</td><td></td></tr>
<tr><td rowspan="9">19. Verifique los valores para Uso remoto de USB genérico de la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL”.</td><td></td><td colspan="3">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta - DL” tiene los siguientes valores en la siguiente ubicación:<br>“Directiva CCN-STIC-684 ENS Incremental Citrix Workspace App categoria alta – DL → Configuración del equipo → Directivas → Plantillas administrativas → Componentes de Citrix → Citrix Workspace → Uso remoto de dispositivos del cliente → Uso remoto de USB genérico”.<br>Cuando termine de realizar la comprobación, cierre el “Editor de administración de directivas de grupo”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Dispositivos USB existentes</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Dispositivos USB nuevos</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">EnableUSBForceRedirection</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Lista de dispositivos USB en Desktop Viewer</td><td>Deshabilitada</td><td></td></tr>
<tr><td colspan="2">Quitar en bloqueo</td><td>Habilitada</td><td></td></tr>
<tr><td colspan="2">Redirigir dispositivos USB desconocidos</td><td>Deshabilitada</td><td></td></tr>
<tr><td>20. Verifique las políticas aplicadas a “Servidores Citrix Director”.</td><td></td><td colspan="3">Seleccione la unidad organizativa “Clientes Windows 10”, situada en “Bosque [Su bosque] → Dominios → [Su dominio] → Servidores → Servidores Citrix Director” y revise que, como mínimo, tiene aplicada la siguiente directiva, tiene el vínculo habilitado y se encuentra situada en primer lugar.<br>– “CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL”<br> 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td rowspan="3">21. Verifique los valores para Opciones de seguridad de la directiva “CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL”.</td><td></td><td colspan="2">Utilizando la herramienta "Editor de administración de directivas de grupo", verifique que la directiva “CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta - DL” tiene los siguientes valores en la siguiente ubicación: “Directiva CCN-STIC-684 ENS Incremental habilitar asistencia remota categoria alta – DL → Configuración del equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Criptografía del sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash</td><td>Deshabilitada</td><td></td></tr>
</table>

## 2. CITRIX CONTROLLER

Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el servidor con el rol Citrix Controller de la infraestructura.

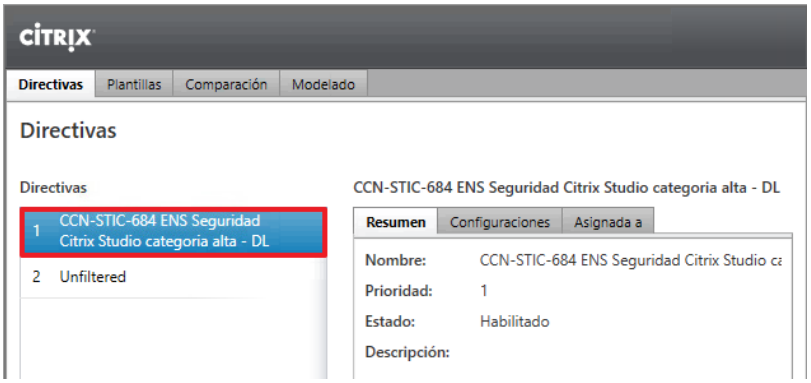
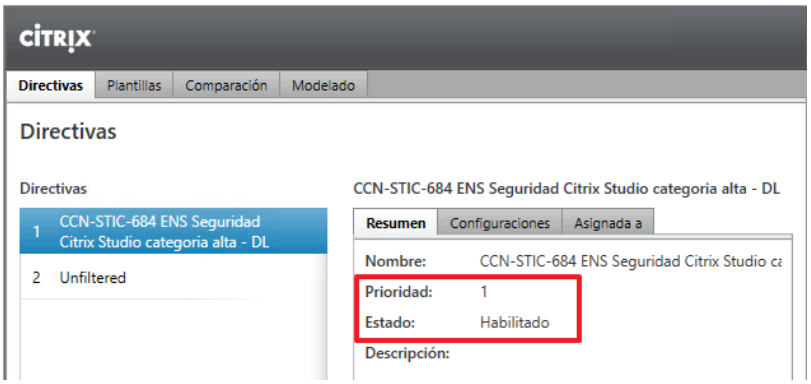
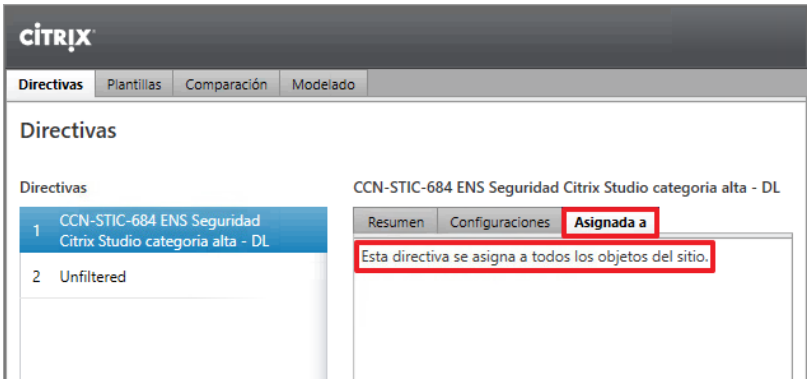
Las consolas y herramientas que se utilizarán son las siguientes:

a) Citrix Studio.

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

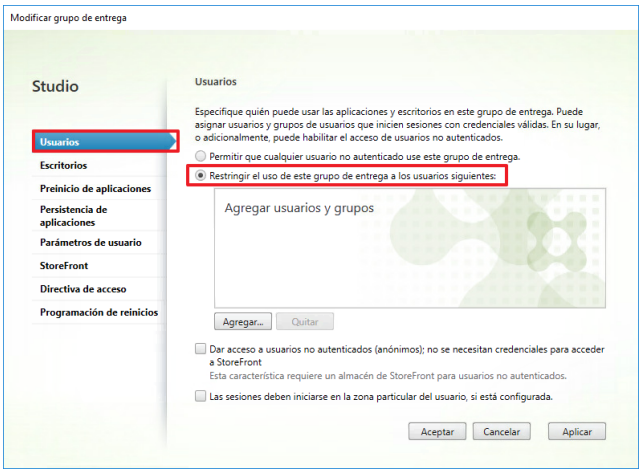
**Nota:** Deberá ejecutar los siguientes pasos de comprobación en el servidor con el rol Citrix Controller que haya sido preparado siguiendo esta guía de seguridad.

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 22. Inicie sesión en un servidor con el rol Citrix Controller | | Inicie sesión en un servidor con el rol Citrix Controller, con una cuenta de administrador del dominio. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 23. Verifique que están creadas las directivas de seguridad de Citrix Studio. | | Ejecute la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Directivas"** y compruebe que la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL" está creada.<br>  |
| 24. Verifique la configuración de la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL". | | Verifique que la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL" se encuentra configurada con la prioridad 1 y que el estado de la misma es "Habilitado".<br>  |
| 25. Verifique la asignación de la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL". | | Verifique que la directiva "CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL" se encuentra asignada a todos los objetos del sitio.<br>  |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>26. Verifique las configuraciones de la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL”.</td><td></td><td>Verifique que la directiva “CCN-STIC-684 ENS Seguridad Citrix Studio categoria alta - DL” tiene los siguientes valores configurados.<br> 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cargar archivos al escritorio</td><td>Prohibida</td><td></td></tr>
<tr><td>Conectar automáticamente las unidades del cliente</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Conexiones directas con servidores de impresión</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Crear automáticamente la impresora universal de PDF</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Crear automáticamente las impresoras del cliente</td><td>No crear automáticamente las impresoras del cliente</td><td></td></tr>
<tr><td>Crear automáticamente una impresora universal genérica</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Descargar archivos desde el escritorio</td><td>Prohibida</td><td></td></tr>
<tr><td>Impresoras del cliente retenidas o restauradas</td><td>Prohibida</td><td></td></tr>
<tr><td>Instalación automática de controladores de impresora</td><td>Inhabilitado</td><td></td></tr>
<tr><td>Permitir transferencia de archivos entre escritorio y cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de dispositivos TWAIN del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de dispositivos USB del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de dispositivos USB Plug and Play del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de impresoras del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de puertos COM del cliente</td><td>Prohibida</td><td></td></tr>
<tr><td>Redirección de puertos LPT del cliente</td><td>Prohibida</td><td></td></tr>
</table></td></tr>
</table>

| Comprobación | OK/NOK | Cómo hacerlo | | |
|---|---|---|---|---|
| | | Directiva | Valor | OK/NOK |
| | | Redirección de unidades del cliente | Prohibida | |
| | | Redirección del host al cliente | Inhabilitado | |
| | | Redirección del portapapeles del cliente | Prohibida | |
| | | Unidades de disco flexibles del cliente | Prohibida | |
| | | Unidades de red del cliente | Prohibida | |
| | | Unidades extraíbles del cliente | Prohibida | |
| | | Unidades fijas del cliente | Prohibida | |
| | | Unidades ópticas del cliente | Prohibida | |
| 27. Verifique los derechos de acceso a los recursos. | | Ejecute la consola Citrix Studio, diríjase al nodo de configuración **"Citrix Studio → Grupos de entrega"** y sobre cada uno de los grupos de entrega verifique que se encuentra restringido el uso de los mismos a los grupos de seguridad definidos por su organización. Para ello, pulse con el botón derecho del ratón sobre cada uno de ellos y seleccione "Modificar grupo de entrega" en el menú que se ha desplegado.<br>Pulse "Cancelar" una vez realizada la comprobación.<br>  | | |

## 3. CLIENTE CON INSTALACIÓN DE VIRTUAL DELIVERY AGENT

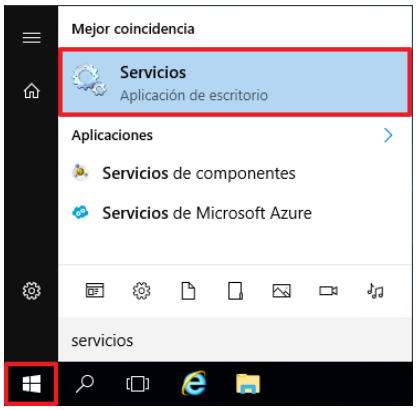
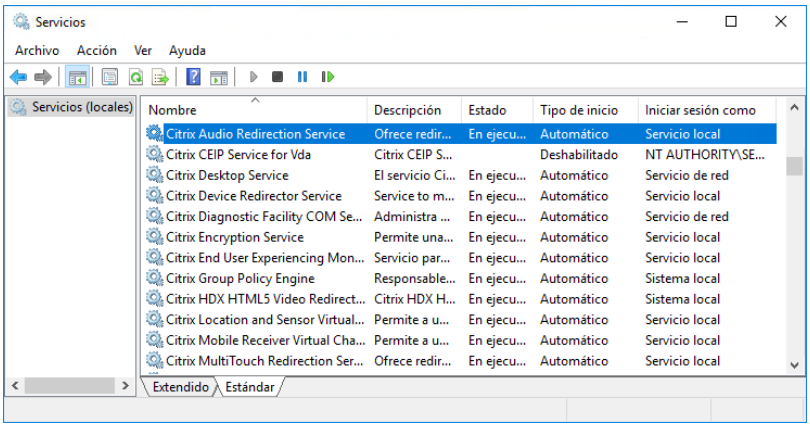
Los siguientes pasos ayudan a verificar la correcta configuración que se ha implementado en el equipo en el que se ha desplegado el agente Virtual Delivery Agent, y las configuraciones propias implementadas sobre este equipo.

Las consolas y herramientas que se utilizarán son las siguientes:

a) Servicios (services.msc).

El siguiente procedimiento verifica la configuración del equipo con el rol Virtual Delivery Agent.

**Nota:** Deberá ejecutar los siguientes pasos de comprobación en el equipo con el rol Virtual Delivery Agent que haya sido preparado e instalado siguiendo esta guía de seguridad.

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|
| 28. Inicie sesión en un equipo con el rol Virtual Delivery Agent. | | En un equipo con el rol Virtual Delivery Agent, 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"o sobre el buscador y teclee "servicios". Ejecute la herramienta "Servicios" que ha aparecido. El sistema solicitará elevación de privilegios, introduzca las credenciales de un usuario con privilegios y pulse "Sí" para continuar.<br>  |
| 30. Sobre cada uno de los equipos con el rol Virtual Delivery Agent revise los servicios implementados y su estado. | | Compruebe que el valor de inicio de los servicios se ha configurado correctamente.<br>  <br>**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. Por tanto, es posible que varios servicios no aparezcan. Compruebe que el estado de los que aparecen coincide con lo definido en la tabla del paso siguiente. |

| Comprobación | OK/NOK | Cómo hacerlo |
|---|---|---|

| Servicio (nombre largo) | Servicio (nombre corto) | Inicio | OK/NOK |
|---|---|---|---|
| Asignador de extremos de RPC | RpcEptMapper | Automático | |
| Citrix Audio Redirection Service | CtxAudioSrv | Automático | |
| Citrix Audio Redirection Service | CtxAudioSvc | Automático | |
| Citrix CEIP Service for Vda | CitrixVdaCeipService | Deshabilitado | |
| Citrix Desktop Service | BrokerAgent | Automático | |
| Citrix Device Redirector Service | CitrixRDR | Automático | |
| Citrix Device Redirector Service | CitrixRedirector | Automático | |
| Citrix Diagnostic Facility COM Server | CdfSvc | Automático | |
| Citrix Dynamic Virtual Channel Service | PicaDvcControllerSvc | Automático | |
| Citrix Encryption Service | Citrix Encryption Service | Automático | |
| Citrix End User Experience Monitoring Service | Citrix EUEM | Automático | |
| Citrix Group Policy Engine | CitrixCseEngine | Automático | |
| Citrix HDX HTML5 Video Redirection Service | CtxHdxWebSocketService | Automático | |
| Citrix ICA Service | PorticaService | Automático | |
| Citrix Location and Sensor Virtual Channel Service | CtxSensVcSvc | Automático | |
| Citrix Mobile Receiver Virtual Channel Service | MRVCSvc | Automático | |
| Citrix Multi Touch Redirection Service | CtxMultiTouchSvc | Automático | |
| Citrix Print Manager Service | cpsvc | Automático | |
| Citrix Profile Management | CtxProfile | Automático | |
| Citrix Pvs for VMs agent | PvsVmAgent | Automático | |
| Citrix Services Manager | ServicesManager | Automático | |
| Citrix Smart Card Certificate Propagation Service | CtxSCardCertPropSvc | Automático | |
| Citrix Smart Card Removal Policy Service | CtxScardRemovalPolicySvc | Automático | |
| Citrix Smart Card Service | CtxSmartCardSvc | Automático | |
| Citrix Stack Control Service | StackControlService | Automático | |
| Citrix Telemetry Service | CitrixTelemetryService | Deshabilitado | |
| Citrix UWA Cache Service | CitrixUWACacheService | Automático | |
| Cola de Impresión | Spooler | Automático | |
| Estación de trabajo | LanmanWorkstation | Automático | |
| Iniciador de procesos de servidor DCOM | DcomLaunch | Automático | |
| Llamada a procedimiento remoto (RPC) | RpcSs | Automático | |
| Servicio Citrix HDX MediaStream para Flash | CtxFlashSvc | Automático | |
| Servicio Informe de errores de Windows | WerSvc | Automático | |
| Servicio Interfaz de almacenamiento en red | nsi | Automático | |
| Servicios de Escritorio Remoto | TermService | Manual | |
| Solicitante de instantaneas de volumen de Hyper-V | vmicvss | Manual | |