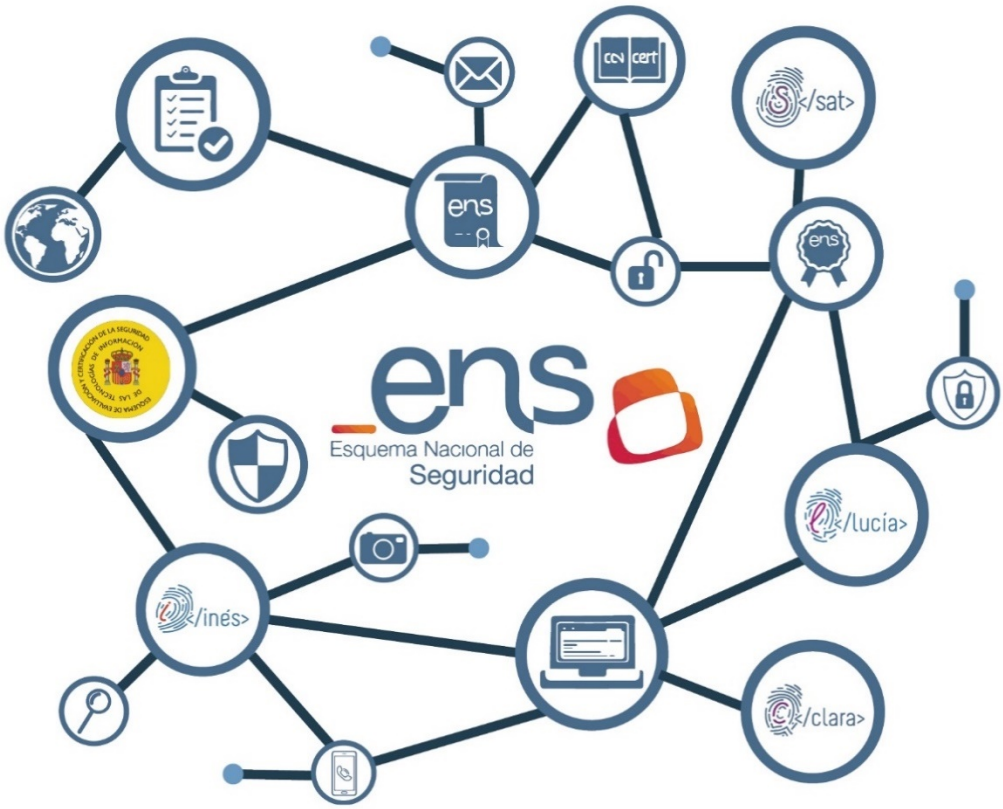
GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC

CCN-STIC 875

Microsoft System Center Configuration Manager 2012 R2 sobre Microsoft Windows Server 2012 R2



Julio 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.07.12 10:16:49 +02'00'

NIPO: 785-17-068-3

Fecha de Edición: julio de 2017
Sidertia Solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

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

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

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

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

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado 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.

Julio de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

Este documento forma parte del conjunto de normas desarrolladas por el Centro Criptológico Nacional para la implementación del Esquema Nacional de Seguridad (CCN-STIC-800) siendo de aplicación para la Administración Pública y teniendo como objeto la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.

Esta guía tiene en consideración la aplicación de plantillas y condiciones de seguridad para la implementación de System Center Configuration Manager 2012 R2 (en adelante SCCM 2012 R2), sobre servidores Microsoft Windows Server 2012 R2 siguiendo las condiciones de seguridad aplicables a través de medidas que se referencian en el RD 3/2010. La aplicación de la seguridad definida en esta guía se ha diseñado de manera incremental, de tal forma que puede ser aplicada bajo diferentes condicionantes. Aunque es factible que se referencien otras guías, especialmente las de la serie CCN-STIC-800, referidas a productos y entornos Microsoft. No será un requisito indispensable partir de ninguna de ellas, tampoco será una necesidad la implementación de otras guías, salvo que las exigencias de seguridad para la organización o el entorno así lo demandaran.

2. OBJETO

El propósito de este documento consiste en, proporcionar plantillas de seguridad para la aplicación de medidas que garanticen dicha seguridad en un escenario de implantación del Esquema Nacional de Seguridad en System Center Configuration Manager 2012 R2 sobre Microsoft Windows Server 2012 R2 y bajo un entorno de servidor miembro de un dominio.

La definición, así como la implementación de las plantillas de seguridad, tiene en consideración las características de seguridad definidas a través del Real Decreto 3/2010 mediante el cual, se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante ENS). La presente guía tiene en consideración la aplicación de plantillas de seguridad en función de los niveles de seguridad que se establecen por la aplicación del Real Decreto.

Se tiene en consideración que los ámbitos de aplicación de este tipo de plantillas son muy variados y, por lo tanto, dependerán de su aplicación las peculiaridades y funcionalidades de los servicios prestados por las diferentes organizaciones. Las plantillas y normas de seguridad se han generado definiendo unas pautas generales de seguridad que permitan el cumplimiento de los mínimos establecidos en el ENS. No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas puedan ser modificadas para adaptarlas a sus necesidades operativas.

3. ALCANCE

La guía se ha elaborado para proporcionar información específica con objeto de realizar una implementación del ENS en MS SCCM 2012 R2 sobre servidores Microsoft Windows Server 2012 R2 y a través de una configuración de seguridad sólida. Se incluyen, además, operaciones básicas de administración para la aplicación de las mismas, así como una serie de recomendaciones para su uso.

Este documento incluye:

a) Descripción del ENS. Se definirán las condiciones de aplicación del ENS, así como los requisitos de seguridad.

b) Descripción de la naturaleza de las medidas. Se referenciarán los marcos de actuación, las dimensiones de seguridad y la aplicación de medidas.

c) Descripción de las plantillas de seguridad. Se definirán las diferentes plantillas de seguridad aplicadas según los niveles que establece el ENS.

d) Mecanismos para la aplicación de configuraciones. Se incorporarán mecanismos para la implementación, de forma automática, de las configuraciones de seguridad susceptibles de ello.

e) Guía paso a paso. Que va a permitir implementar y establecer las configuraciones de seguridad de MS SCCM 2012 R2 en servidores Microsoft Windows Server 2012 R2 para cada uno de los niveles de seguridad.

f) Lista de comprobación. Permitirá verificar el grado de cumplimiento de un servidor con respecto a las condiciones de seguridad que se establecen en esta guía.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender esta guía de seguridad es conveniente explicar, el proceso de refuerzo de la seguridad que describe y los recursos que proporciona. Este procedimiento constará de los siguientes pasos:

Para el escenario de un servidor controlador de dominio, debe asegurarse que existe un sistema operativo Microsoft Windows Server 2012 R2 implementado según las directrices de la guía “CCN-STIC-870A - Implementación del ENS en Windows Server 2012 R2” y “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2” para el servidor controlador de dominio.

Para los escenarios de servidor miembro, sobre los cuales se implementarán las características de MS SCCM 2012 R2 Management Server y MS SCCM 2012 R2 Distribution Point, deberá asegurarse que existe un sistema operativo Microsoft Windows Server 2012 R2 implementado según las directrices de la guía “CCN-STIC-870A - Implementación del ENS en Windows Server 2012 R2” y “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2” para cada servidor miembro implementado.

Para el escenario de servidor miembro sobre el cual se implementará Microsoft SQL Server 2012 deberá asegurarse que existe un sistema operativo Microsoft Windows Server 2012 R2 implementado según las directrices de la guía “CCN-STIC-870A - Implementación del ENS en Windows Server 2012 R2.

Para el escenario de equipo cliente debe asegurarse que existe un sistema operativo Microsoft Windows 7 implementado según las directrices de la guía “CCN-STIC-850A - Implementación del ENS en Windows 7” para equipo cliente.

Prepare el sistema de servidor genérico para que pueda alojar MS SCCM 2012 R2 con los requisitos previos marcados por el fabricante, previos a la implementación del producto.

Se configurará MS SCCM 2012 R2 según se detalla más adelante. Personalizará y aplicará la plantilla de seguridad tal y como se describe en la presente guía.

4.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

Los contenidos de esta guía son de aplicación para servidores con Sistemas Operativos Microsoft Windows Server 2012 R2.

Debido a la importancia, se reitera que se asume que la instalación de System Center Configuration Manager 2012 R2 se realiza sobre un servidor miembro preparado en base a las indicaciones de la guía "CCN-STIC-870A, Implementación del ENS en Windows Server 2012 R2" y "CCN-STIC-873, Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2".

La guía ha sido desarrollada y probada en un entorno de uso de servicios Microsoft, no encontrándose limitación en el uso de los mismos tras la implementación de las plantillas de seguridad. No obstante, debe tener en consideración el escenario en el cual vaya a realizar su implementación para la correcta idoneidad de todos sus sistemas.

Esta guía ha sido diseñada con el fin de reducir la superficie de exposición de los servidores y siguiendo las pautas establecidas por el Esquema Nacional de Seguridad.

La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización, de tipo Hyper-V de Microsoft Windows Server 2012 R2 Datacenter, con las siguientes características técnicas:

a) Servidor Dell PowerEdge™ T320
   i. Intel Pentium Xeon Quad Core.
   ii. HDD 1 TB.
   iii. 32 GB de RAM.
   iv. Interfaz de Red 1 Gb/s.
   v. Sistema de tecnología iSCSI para el almacenamiento compartido.

Esta guía de seguridad no funcionará con hardware que no cumpla con los requerimientos mínimos de hardware de Microsoft Windows Server 2012 R2. Esto quiere decir que se necesitan equipos con procesadores Intel o AMD de 64 bits (x64) a 1,4 GHz o superior, con más de 512 MB de memoria RAM (para ciertas condiciones podría ser necesaria una RAM de 800 MB e incluso 1 GB, como mínimo), 32 GB de espacio libre en disco duro y tarjeta de red con conectividad.

Debe tenerse en cuenta que los valores mínimos pueden diferir de forma significativa respecto a los que serían recomendados para un servicio óptimo. Se debe tener en consideración que estos requerimientos son adicionales a los que se establecen para la instalación de sistema operativo sin SCCM 2012 R2.

La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad mínima, siguiendo las normas descritas en el ENS. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios o características deseados en Microsoft Windows Server 2012 R2.

La guía ha sido desarrollada con objeto de limitar hacia Internet el envío de información al fabricante, limitando a su vez, algunas características que permiten la interrelación del sistema con determinados servicios públicos existentes en Internet. Esto tiene como objeto limitar la posibilidad de envío de datos hacia Internet.

Para garantizar la seguridad de los servidores, deberán instalarse las actualizaciones recomendadas por el fabricante. Éstas están disponibles a través del servicio de Microsoft Update y, por lo general, se liberan el segundo martes de cada mes. No obstante, hay que tener presente que determinadas actualizaciones, debido a su criticidad, pueden ser liberadas en cualquier momento. Se deberá tener en consideración la implementación de las actualizaciones tanto para el sistema operativo, como para los diferentes servicios instalados.

Dependiendo de la naturaleza de estas actualizaciones, el lector podrá encontrarse con algunas diferencias respecto a lo descrito en esta guía. Esto viene motivado por los cambios que se realizan para las distintas actualizaciones de seguridad.

Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado, en el cual se habrán aplicado los test y cambios en la configuración que se ajusten a los criterios específicos de cada organización.

El espíritu de estas guías no está dirigido a reemplazar políticas consolidadas y probadas de las organizaciones, sino servir como la línea base de seguridad que podrá ser adaptada a las necesidades propias de cada organización.

5. INTRODUCCIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

El Esquema Nacional de Seguridad nace desde la necesidad de ofrecer una respuesta a la obligación de las Administraciones Públicas para adoptar medidas de seguridad adecuadas, en función de la naturaleza de la información y los servicios que ofrecen. Se origina para dar cumplimiento a lo establecido en el ámbito de la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos, a través de su artículo 42 punto 2.

"El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información".

Las mejoras introducidas en la Ley 11/2007 sobre la relación entre las Administraciones Públicas y los ciudadanos, así como entre ellas, haciendo uso de la tecnología, requerían de la implementación de unos mecanismos que no solo garantizaran la usabilidad de los servicios sino su seguridad. Ésta se debía hacer extensible tanto al mantenimiento y gestión de la información como a los procesos de comunicación.

El Esquema Nacional de seguridad ve la luz, a través del Boletín Oficial del Estado, el 29 de Enero del año 2010. Entra en vigor el día después, estableciéndose así el cómputo de plazos para la adecuación a la normativa y las condiciones que quedan establecidas.

El ENS se estructura en diez capítulos, una serie de disposiciones y los anexos, siendo estos últimos los significativos para el desarrollo de la presente guía. A modo de introducción, el presente punto analiza las consideraciones necesarias para entender y conocer la necesidad de implementación del ENS. El resto de puntos irá desentrañando aquellas condiciones de índole técnica para aplicar las condiciones de seguridad necesarias.

La finalidad última del ENS consiste en la creación de las condiciones de confianza para el uso de los medios electrónicos. Para ello, se definen las medidas que garantizarán la seguridad de los sistemas, servicios y datos manejados.

Para el cumplimiento del Esquema Nacional de Seguridad, los órganos superiores de las Administraciones Públicas deberán disponer de una política de seguridad. Éstas contarán con unos requisitos mínimos que deberán ser implementados por todos los organismos sujetos al ENS. La política de seguridad tendrá como objetivos fundamentales establecer roles, así como sus funciones y procedimientos de designación. También definirá los criterios para la categorización e identificación de servicios y sistemas, así como plantear los mecanismos de seguridad previstos en el Anexo II.

Para lograr este cumplimiento, se exigen una serie de requisitos mínimos que deberán quedar definidos en la política de seguridad:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de riesgos.
c) Gestión de personal.
d) Autorización y control de los accesos.
e) Protección de las instalaciones.
f) Adquisición de productos.
g) Seguridad por defecto.
h) Integridad y condiciones para mantener los sistemas y servicios actualizados.
i) Confidencialidad de la información almacenada.
j) Registro de actividad.
k) Incidentes de seguridad.
l) Continuidad de la actividad.
m) Mejora continua del proceso de seguridad.

Debe tenerse en consideración que todo proceso de implantación de un sistema de seguridad no es un hecho aislado y puntual. Muy al contrario, mantener la seguridad de una infraestructura requiere de un proceso de mantenimiento continuo, donde existen una serie de factores a tener en consideración para mantener siempre los sistemas en un correcto estado de funcionalidad y garantizando la protección de los mismos.

Debe, pues, entenderse el proceso de gestión del ENS, en una organización, en dos plazos muy bien diferenciados:

El primero consistirá en adecuar e implementar todas las medidas de índole organizativa y técnica para el cumplimiento del ENS.

El segundo consistirá en mantener todas las infraestructuras garantizando el estado de seguridad de sistemas y servicios, así como el adecuado cumplimiento de los procedimientos diseñados.

Uno de los principios fundamentales, en los cuales se basa el ENS, consiste en la seguridad por defecto. A través de este principio, se intenta minimizar el impacto de las amenazas, deshabilitando todos aquellos elementos innecesarios y activando aquellos otros que sean factibles. La presente guía establece este principio como norma. Tiene, no obstante, en consideración que determinadas funcionalidades podrán ser habilitadas por las organizaciones bajo requerimiento de sus servicios, sin menosprecio a lo dispuesto en la presente guía.

5.1 DIMENSIONES DE SEGURIDAD

Para el cumplimiento de los objetivos previstos en el ENS se definen y valoran los fundamentos que van a permitir categorizar sistemas y servicios. Esta categorización es importante puesto que, en función del nivel de los mismos, deberán realizarse unas implementaciones de seguridad u otras. Éstas irán incrementándose en función del nivel exigido.

Cuando se plantea la categorización, se tiene en consideración el impacto que tendría un incidente que pudiera afectar a los sistemas, servicios o a la propia información manejada.

Para ello se establece la repercusión en la capacidad organizativa, en virtud de diferentes aspectos:

Alcanzar sus objetivos. La prestación de un servicio a los ciudadanos, o a la relación entre las propias organizaciones, se plantea a través de la Ley de Acceso Electrónico como la necesidad fundamental de toda Administración Pública. La seguridad definida a través del ENS plantea, por lo tanto, la necesidad de que se cubran todos los objetivos para los que fue diseñado e implantado un determinado servicio.

Proteger los activos a su cargo. El planteamiento de un servicio tiene como premisa el facultar el acceso o proporcionar datos a los ciudadanos, en función de sus necesidades, para la ejecución de un proceso administrativo. La información, por lo tanto, se considera uno de los mayores activos con los que cuenta un usuario de cualquier servicio de la administración pública. Proteger la información y garantizar su integridad se hace factible a través de la implementación del ENS.

Respetar la legalidad vigente. Tomando como premisa la ley para prestación de un servicio, por parte de la Administración Pública, no se podría exigir otra cosa que no sea el respeto a todas las normas vigentes. Si se trataran datos de carácter personal de forma inadecuada o no se atendiera a los derechos “ARCO”, se estaría contraviniendo lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Con el ENS se persigue también que una potencial incidencia de seguridad no conlleve que el servicio o sistema no cumpla con la legalidad vigente.

Respetar los derechos de los ciudadanos. No debe obviarse nunca que, en todo momento, deben darse una serie de garantías y derechos para la protección del ciudadano y que deben ser observados de forma prioritaria. Debe tomarse en consideración qué pasaría si todos aquellos datos sensibles, gestionados por una Administración, se hicieran públicos sin ningún control. Como mínimo, podrían romper algunos de los principios fundamentales regulados en la propia Constitución. Así mismo, se deberá tener en consideración todo el perjuicio que sobre esas personas pudiera recaer debido a una mala práctica.

Atendiendo a la capacidad de la administración pública para establecer mecanismos y controles sobre sus sistemas y servicios, se definió la figura de las dimensiones de seguridad. Éstas diferencian y determinan el impacto que una amenaza podrá realizar sobre los activos de una organización en base a una serie de condiciones. Los términos de dimensiones de seguridad son ampliamente recogidos en todos los aspectos de seguridad de la Tecnología de la Información (TI) y recogen conceptos fundamentales para el tratamiento de sistemas, servicios e información. Las dimensiones de seguridad recogidas en el ENS son cinco:

a) Disponibilidad (D).

b) Autenticidad (A).

c) Integridad (I).

d) Confidencialidad (C).

e) Trazabilidad (T).

Conocidas bien por su nombre o por sus iniciales, cada una de las dimensiones requerirá de la aplicación de una serie de medidas que podrán ser bien de índole técnica, organizativa o procedimental. No todas las medidas deberán ser aplicadas en la misma forma, atendiendo a la criticidad del servicio prestado o la información manejada deberán aplicarse unas u otras medidas.

La consideración de la criticidad se basará en una serie de preceptos que serán descritos a posteriori. A continuación, se detallan las características de las dimensiones de seguridad y los objetivos fundamentales de cada una de ellas.

5.1.1 DISPONIBILIDAD

La disponibilidad establece la necesidad de que la información y los sistemas se encuentren activos para la prestación de los servicios. Éste corresponde, por lo tanto, a uno de los pilares fundamentales cuyo objetivo es garantizar el objetivo estipulado para la Administración pública: ofrecer un servicio. Ante determinadas adversidades, deberán darse condiciones para que este servicio pueda seguir ofreciéndose y, evidentemente, las medidas serán más amplias y necesarias según aumente en criticidad el servicio prestado.

La implementación de mecanismos para garantizar la disponibilidad, no solo tiene sentido en la aplicación de medidas de índole tecnológica, sino que también cobra mucha fuerza la necesidad de implementar procedimientos ante contingencias. Tan importante es la realización de una copia de seguridad como el hecho de haber definido y escrito un mecanismo para recuperar dicha copia de seguridad en sistemas alternativos y ante la posibilidad de que, por un problema severo como pudiera ser un terremoto, se anularan los sistemas originales donde se prestaban los servicios.

Dentro de las necesidades para el cumplimiento efectivo de la disponibilidad, el ENS requiere el establecimiento de medidas que podrían afectar a diferentes condicionantes:

a) Dimensionamiento de los servicios.

b) Usos de sistemas, medios, instalaciones y personal alternativos.

c) Copias de seguridad.

d) Condiciones de mantenimiento del suministro eléctrico.

e) Protección frente a incendios o inundaciones.

Es evidente que la presente guía no cubre todos los aspectos definidos en esta dimensión de seguridad, así como de las otras dimensiones que serán explicadas a continuación. Por lo tanto, además de todas las condiciones de índole técnica dispuestas en la presente guía, la organización deberá atender a todas aquellas otras que siendo de índoles organizativas, estructurales y procedimentales vienen recogidas en RD 3/2010.

5.1.2 AUTENTICIDAD

Dentro del planteamiento de la seguridad en el acceso a los sistemas de la información, uno de los primeros elementos a los que se enfrenta cualquier usuario es la autenticación. "¿Quién eres?" es la pregunta más habitual para el acceso a cualquier servicio. No debería acceder a un sistema quien no hubiera sido autorizado para ello. Esto cobra más sentido ante el hecho de tener que garantizar la privacidad de los datos gestionados por la propia Administración Pública. Por lo tanto, garantizar los procesos de autenticación y control de acceso constituye otras de las máximas de la seguridad, tal y como lo recoge el ENS.

Los procesos de autenticación deben verse siempre como una garantía para la protección de la información y no, en sí mismos, como una incomodidad.

No obstante, aunque el proceso de autenticación es uno de los más evidentes, debe entender la dimensión de "Autenticidad" como un elemento mayor, donde el proceso de autenticación y todo lo que conlleva, presentan una gran relevancia. Existen además otros aspectos como la segregación de funciones o la implementación de mecanismos de bloqueos que quedan también referenciados a través de esta dimensión de seguridad.

El proceso de autenticidad se encuentra, además, totalmente ligado a otra dimensión de seguridad que se verá posteriormente: la trazabilidad. Sin poder saber quién ha hecho tal cosa sería imposible, bien remediar situaciones, o bien establecer las responsabilidades necesarias.

Los sistemas de autenticación, que pueden emplear las organizaciones para llevar a efecto los procedimientos descritos en el ENS, pueden ser de múltiple índole y tipología. Aunque los más básicos están basados en el empleo de contraseñas, ciertas condiciones aplicables por los niveles de seguridad más elevados requerirán de otros sistemas adicionales.

Dentro de los factores para la autenticidad pueden encontrarse los relativos a:

a) Identificación de ciudadanos o usuarios frente a los servicios.

b) Procesos de registros de acceso.

c) Mecanismos que garanticen la segregación de funciones.

d) Establecimiento de mecanismos de autenticación.

e) Implementación de mecanismos de accesos locales o remotos.

f) Implementación de mecanismos de protección de los puestos de trabajo.

Implementación de mecanismos para garantizar la integridad y autenticidad de la información manejada, incluyendo en ellos los procedimientos para documentar y distribuir las credenciales a los usuarios de una organización.

Empleo de mecanismos de Firma Electrónica.

5.1.3 INTEGRIDAD

Este aspecto fundamental, especialmente en la relación con la Administración Pública, consiste en dar validez a documentos y garantizar que los mismos son auténticos. La integridad precisamente valida, como metodología, ese hecho: no dar por hecho que algo es por lo que dice ser, sino porque lo es verdaderamente.

Los mecanismos de integridad validan que un objeto o acción es auténtico y que no ha sido alterado durante el transcurso del tiempo. Un ejemplo significativo corresponde a la implementación de medidas enfocadas a firmar digitalmente documentos administrativos.

5.1.4 CONFIDENCIALIDAD

Garantizar que la información o los propios servicios se encuentran salvaguardados sin que se produzcan accesos indebidos o que, en caso de que estos se produzcan siempre se pueda garantizar que los datos resultan ilegibles, es una máxima que persigue el ENS.

La confidencialidad establece una serie de medidas que aplicarán condicionantes para la salvaguarda de los datos, impidiendo que personas no autorizadas puedan acceder a ellos. Estas medidas son muy variadas y constituyen, en último extremo, la última barrera de protección que se aplicará para garantizar la seguridad de un sistema frente a un atacante.

Los mecanismos empleados para la confidencialidad son muy comunes en la implementación de tecnología y van desde la propia salvaguarda de la contraseña, que se almacena de forma no legible, a la propia implementación de protocolos que emplean cifrados tales como HTTPS. Éstos son la alternativa a protocolos inseguros por el envío de credenciales en claro, como el propio protocolo HTTP.

Los mecanismos que garantizan la confidencialidad han cambiado con el paso del tiempo y debe tenerse en consideración que, aunque se hable de algoritmos de cifrados o protocolos seguros, no todos son tan fiables como se diseñaron en un principio. Deberían utilizarse exclusivamente aquellos que sean más seguros e impedir el uso de los que no lo sean.

La guía CCN-STIC-807 sobre “Criptología de empleo en el Esquema Nacional de Seguridad” detalla la información de qué algoritmos pueden implementarse y cuáles no.

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/807/807-Criptologia_de_empleo_ENS-nov12.pdf

5.1.5 TRAZABILIDAD

A menudo, cuando se ha producido una incidencia, lo que resta es poder determinar qué ha pasado con objeto de aplicar así las medidas correctoras adecuadas. Para que el análisis pueda ser llevado a cabo, será necesario disponer de información. La dimensión de seguridad de trazabilidad, definida en el Esquema Nacional se Seguridad, establece precisamente los procedimientos y mecanismos a emplear por una organización para que ese hecho resulte factible, proporcionando así los datos necesarios que permitan llevar a cabo un análisis de seguridad.

Los mecanismos empleados para garantizar la trazabilidad ofrecerán capacidad analítica a los especialistas, de tal forma que podrán operar en modo preventivo o reactivo, según demande la necesidad. La trazabilidad se prestará a su aplicación a través de las siguientes medidas:

a) Procesos de identificación y control de acceso.
b) Segregación y cumplimiento de funciones.
c) Mecanismos de autenticación.
d) Accesos locales y remotos.

e) Registros de la actividad de los usuarios.

f) Empleo de marcas de tiempo.

Es importante establecer que no basta con garantizar que se produzcan los registros y que éstos se encuentren disponibles, sino también la integridad de los mismos, dándoles validez puesto que no han sido alterados. Es factible, por lo tanto, que múltiples dimensiones de seguridad deban aplicarse sobre una misma medida para que esta cumpla su propósito.

Así, en un rápido ejemplo, se podría entender que el registro resultante de una auditoría de acceso de los usuarios, como parte de los mecanismos de trazabilidad dispuestos, deberá además encontrarse asegurado por medidas de confidencialidad e integridad.

5.2 NIVELES DE DIMENSIONES DE SEGURIDAD

El conjunto de los servicios que presta una Administración Pública lo configuran diferentes componentes que se encontrarán sujetos a diferentes dimensiones de seguridad. Es evidente que no todos los servicios presentan la misma criticidad y, por lo tanto, hay que adaptar la necesidad aplicando las medidas de forma ecuánime en función de dicha criticidad.

Esta criticidad, desde el punto de vista del ENS, se mide atendiendo a una serie de criterios generales aplicables en cada una de las dimensiones de seguridad: disponibilidad (D), autenticidad (A), integridad (I), confidencialidad (C) y trazabilidad (T).

El Esquema de Seguridad establece tres categorías: básica, media y alta.

Un sistema de información será de categoría ALTA si, al menos, una de sus dimensiones de seguridad alcanza el nivel ALTO.

Un sistema de información será de categoría MEDIA si, al menos, una de sus dimensiones de seguridad alcanza el nivel MEDIO y ninguna otra alcanza el nivel superior.

Un sistema de información será de categoría BAJA si, al menos, una de sus dimensiones de seguridad alcanza el nivel BAJO y ninguna otra alcanza el nivel superior.

Los criterios para valorar los niveles aplicables para cada dimensión de seguridad se encuentran totalmente definidos en la guía de seguridad CCN-STIC-803, “Esquema Nacional de Seguridad valoración de los sistemas”.

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf

A efectos de valoración y para determinar cuáles son los niveles de seguridad, tal y como se describe en la propia guía de seguridad CCN-STIC-803, se deberá diferenciar siempre la información del servicio. Ambos son de aplicación, pero se deben valorar de forma independiente.

La información, según establece el ENS, es cualquier dato relevante para el proceso administrativo y puede ser tratado a través de un servicio afectado por la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. Entrarían en este ámbito los datos médicos, expedientes de un ayuntamiento, información de tesorería y un largo etcétera de datos tratados por las diferentes Administraciones Públicas. El ENS no establece la necesidad de valorar directamente aquellos datos que, considerados como auxiliares, no son objeto directo del proceso administrativo. Se encuadrarían dentro de este último epígrafe de datos auxiliares los datos existentes en el Directorio Activo, las claves almacenadas en un puesto de trabajo, etc.

La valoración de la información, la determina el responsable de la misma, teniendo en consideración la naturaleza de la información y la normativa que pudiera serle de aplicación. Esta valoración requiere de un conocimiento legal sobre la materia tratada.

La información suele imponer requisitos relevantes en las dimensiones de confidencialidad, integridad, autenticidad y trazabilidad. No suelen haber requisitos relevantes en la dimensión de disponibilidad.

El nivel de seguridad requerido en el aspecto de CONFIDENCIALIDAD se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

El nivel de seguridad requerido en el aspecto de INTEGRIDAD se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

El nivel de seguridad requerido en el aspecto de AUTENTICIDAD se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.

El nivel de seguridad requerido en el aspecto de TRAZABILIDAD se establecerá en función de las consecuencias que tendría el no poder rastrear, a posteriori, quién ha accedido a, o modificado, una cierta información.

El nivel de seguridad requerido en el aspecto de DISPONIBILIDAD se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.

Se entiende por servicio cada actividad llevada a cabo por la Administración, o bajo un cierto control y regulación de ésta, a través de organización, especializada o no, y destinada a satisfacer necesidades de la colectividad.

El Esquema Nacional de Seguridad se limita a valorar aquellos servicios que son relevantes para el proceso administrativo, estando sometidos a la ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. Algunos de estos servicios pueden estar identificados en algún tipo de ordenamiento general, mientras que otros serán particulares del organismo. En cualquier caso, los servicios aquí contemplados tienen identidad propia, con independencia de los medios que se utilicen para su prestación, asumiendo el organismo que los presta unas obligaciones con respecto a los mismos. No se valoran servicios internos o auxiliares tales como el correo electrónico, ficheros en red, servicios de directorio, de impresión o de copias de respaldo entre otros muchos.

La valoración de un servicio, la determina el responsable del mismo, teniendo en consideración la naturaleza del servicio y la normativa que pudiera serle de aplicación. Esta valoración requiere un conocimiento legal de la materia de que se trate. Habitualmente los servicios establecen requisitos relevantes en términos de disponibilidad. También es habitual que los demás requisitos de seguridad sobre los servicios deriven de los de la información que se maneja.

El nivel de seguridad requerido en el aspecto de DISPONIBILIDAD se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar al servicio cuando lo necesita.

El nivel de seguridad requerido en el aspecto de CONFIDENCIALIDAD se establecerá en función de las consecuencias que tendría su revelación a alguien que no necesita conocer la información.

El nivel de seguridad requerido en el aspecto de AUTENTICIDAD se establecerá en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas; o sea, por personas que no son quienes se cree que son.

El nivel de seguridad requerido en el aspecto de TRAZABILIDAD se establecerá en función de las consecuencias que tendría el no poder rastrear, a posteriori, quién ha accedido al servicio.

A modo de resumen, se describen a continuación los criterios que permiten determinar los niveles de seguridad aplicables a cada dimensión de seguridad. Atendiendo a la criticidad, las siguientes casuísticas determinan los tres niveles existentes:

Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad, que afecte a alguna de las dimensiones de seguridad, supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio limitado:

a) La reducción, de forma apreciable, de la capacidad de la organización para atender eficazmente a sus obligaciones corrientes, aunque estas sigan desempeñándose.
b) El sufrimiento de un daño menor por los activos de la organización.
c) El incumplimiento formal de alguna ley o regulación que tenga carácter de subsanable.
d) Causar un perjuicio menor a algún individuo que, aun siendo molesto, pueda ser fácilmente reparable.
e) Otros de naturaleza análoga.

Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad, que afecte a alguna de las dimensiones de seguridad, supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio grave:

a) La reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque éstas sigan desempeñándose.
b) El sufrimiento de un daño significativo por los activos de la organización.
c) El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
d) Causar un perjuicio significativo, a algún individuo, de difícil reparación.
e) Otros de naturaleza análoga.

Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad, que afecte a alguna de las dimensiones de seguridad, supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio muy grave:

a) La anulación de la capacidad de la organización para atender alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
b) El sufrimiento de un daño muy grave, e incluso irreparable, por parte de los activos de la organización.

c) El incumplimiento grave de alguna ley o regulación.

d) Causar un perjuicio grave, a algún individuo, de difícil o imposible reparación.

e) Otros de naturaleza análoga.

Los criterios para valorar los niveles asociados para cada dimensión de seguridad, en función de si son aplicables sobre la información o sobre los servicios, se encuentran totalmente definidos en la guía de seguridad CCN-STIC-803 "Esquema Nacional de Seguridad valoración de los sistemas".

6. LAS MEDIDAS DE SEGURIDAD

Teniendo en consideración la implementación de seguridad, en función de la naturaleza y los criterios de categorización y aplicables en función de niveles, se hace necesario establecer qué medidas deberán ser aplicadas y en qué modo. Uno de los apartados más extensos del RD 3/2010 radica precisamente en este punto, quedando todos recogidos en el Anexo II.

Además de tomar como referencia el citado Anexo II, las personas encargadas de diseñar, procedimentar, aplicar o gestionar información o servicios sujetos a la normativa, deberán tener en consideración también la guía CCN-STIC-804 "Esquema Nacional de Seguridad - guía de implantación".

La guía de seguridad CCN-STIC-804 establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares. Se espera que cada organización las particularice para adaptarlas a su entorno singular. Si bien el Esquema Nacional de Seguridad establece una serie de medidas de seguridad en su Anexo II, que están condicionadas a la valoración (Anexo III) del nivel de seguridad en cada dimensión y a la categoría (artículo 43) del sistema de información de que se trate, esta guía busca ayudar a los responsables de los sistemas para que puedan implantar rápida y efectivamente las medidas requeridas, sin perjuicio de que utilicen recursos propios o recurran a proveedores y productos externos.

Estas medidas constituyen un mínimo que se debe implementar, o bien deberán justificarse los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.

En la guía para cada medida se proporciona:

a) Una descripción más amplia que la proporcionada en el ENS,

b) Referencias externas que ayudan a su comprensión y realización,

c) Relación con medidas o controles en otros esquemas de seguridad,

d) Relación con los principios básicos recogidos en el ENS,

e) Indicaciones de lo que se considerará evidencia suficiente de cara a una evaluación de la seguridad.

Con objeto de establecer un agrupamiento lógico de las medidas de seguridad en el ENS, éstas se han agrupado atendiendo a criterios de aplicación y usos comunes. Para ello, se han establecido tres categorías denominadas:

a) Marco organizativo.

b) Marco operacional.

c) Medidas de protección.

6.1 MARCO ORGANIZATIVO

Bajo este marco, se agrupan aquellas medidas que, de índole genérica, definen los procedimientos esenciales para la gestión de la seguridad. Estas medidas son de índole no técnica y facultan a la organización para adquirir la capacidad de organizarse y asegurar así el cumplimiento de sus objetivos.

Deben tomarse en consideración dos aspectos fundamentales para el cumplimiento de este marco:

Toda estructura organizativa necesita una evaluación constante y un análisis de la respuesta a los incidentes de forma que se aprenda de la experiencia, se corrijan defectos o debilidades y se busque la excelencia por medio de la mejora continua.

La organización debe estar inexorablemente alineada y servir a la misión global, planteada para el organismo, ajustándose a los servicios que se prestan.

Fruto de las acciones establecidas en esta categoría, se obtendrán una serie de documentos materializando las políticas y normativas de seguridad, junto con los procedimientos básicos de seguridad y de autorización de tareas.

Las subcategorías en las que se divide el marco organizativo son cuatro:

a) Política de seguridad.

b) Normativa de seguridad.

c) Procedimientos de seguridad.

d) Proceso de autorización.

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	B	M	A		
				org	Marco organizativo
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización

Dentro de ellas, la política de seguridad es quizás la fundamental y marcará, en cierto modo, el inicio del proceso de adecuación. Concretada en un documento deberá contener los siguientes elementos:

Los objetivos o misión de la organización. Al marcar sus funciones, se estarán definiendo las obligaciones y con ello las responsabilidades y el alcance para el cumplimiento de objetivos. Será la base fundamental para poder establecer la categorización de niveles en básico, medio o alto.

El marco legal y regulatorio en el que se desarrollarán las actividades. Las acciones de una determinada Administración Pública se verán afectadas, además de por la Ley 11/2007, por otras tales como la necesidad de aplicar medidas que atiendan a todas las normas existentes.

Los roles o funciones de seguridad. Definiendo, para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación. Páginas anteriores definieron los diferentes roles que, con respecto al ENS, deberán existir en una organización. La política definirá quién o en qué condiciones se asumirá cada rol.

La estructura del comité o los comités para la gestión y coordinación de la seguridad. Detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización. La aplicación de determinadas condiciones, como la adquisición de un determinado software, podría ser consensuada a través de un comité. La política dirimirá su proceso de creación, así como las funciones del mismo.

Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso. La política sienta las bases para el establecimiento de las medidas organizativas asociadas a la seguridad del sistema.

Como resulta obvio, la aplicación del resto de medidas dependerá mucho de los resultados obtenidos tras los análisis e implementación de las medidas de índole organizativa.

Puesto que la presente guía se encuadra dentro de la implementación de medidas enfocadas a la protección de servidores Windows Server 2012 R2 y que el alcance de las medidas aplicables dentro del marco organizativo no es específicamente técnico, la implementación de este marco no se abordará en esta guía.

6.2 MARCO OPERACIONAL

Las medidas de tipo operacional se constituyen para proteger la operativa del sistema desde un punto de vista global, así como de sus componentes individuales. La naturaleza de las medidas atiende a diferentes criterios y ha sido estructurada en diferentes subcategorías:

a) Planificación.

b) Control de acceso.

c) Explotación.

d) Servicios externos.

e) Continuidad del servicio.

f) Monitorización del sistema.

				op	Marco operacional
				op.pl	Planificación
categoría	n.a.	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (local logon)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoría	aplica	=	+	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

Algunas de las medidas de seguridad aplicables a través de la presente guía, en una implantación de IIS 8.5 sobre Windows Server 2012 R2, vienen definidas por la aplicación de condiciones a través del marco operacional. En páginas posteriores, se tratará y definirá como realizar su aplicación a través de la aplicación de plantillas y consideraciones que deberán ser tenidas en cuenta.

6.3 MEDIDAS DE PROTECCIÓN

Las medidas de protección constituyen el grueso de aplicación de las medidas de índole técnica. Lo conforman diferentes medidas que tienen como objetivo fundamental la salvaguarda de los activos, bien sean servicio o la propia información. Frente a las medidas previas que tenían una consideración más genérica, estas son más específicas.

Las medidas de protección se encuentran divididas en las siguientes categorías:

a) Protección de las instalaciones e infraestructuras.

b) Gestión de personal.

c) Protección de los equipos.

d) Protección de las comunicaciones.

e) Protección de los soportes de comunicación.

f) Protección de las aplicaciones informáticas.

g) Protección de la información.

h) Protección de los servicios.

				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
I A	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (backup)
				mp.s	Protección de los servicios
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

6.4 RELACIÓN ENTRE LAS DIMENSIONES DE SEGURIDAD, LA NATURALEZA DE LAS MEDIDAS Y LOS NIVELES

En las tres imágenes previas, además de reflejar la información correspondiente a la categorización de las medidas, se establecía la relación entre los diferentes elementos que constituyen el ENS:

a) Dimensiones de seguridad.

b) Niveles de seguridad.

c) Naturaleza de las medidas.

Tal y como ya se ha mencionado en páginas previas, la necesidad de aplicación de una medida concreta viene definida por varios criterios tomados de los tres elementos antes mencionados.

Para tener en consideración la descripción de la tabla, deberá tomarse en referencia el siguiente ejemplo que se dispone, relativo a las medidas asignables a los mecanismos de autenticación que se encuadran dentro del marco operacional.

ICAT	aplica	+	++	op.acc.5	Mecanismo de autenticación

La primera de las columnas referencia las dimensiones de seguridad que son afectadas por la aplicación de la medida de seguridad. La notación de las dimensiones viene definida por la inicial de la misma. En esta circunstancia, corresponden a Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Las tres siguientes columnas representan el nivel al que son aplicables, correspondiendo la primera de las tres al nivel básico, la segunda al nivel medio y la última al nivel alto. El texto que puede aparecer en las columnas son:

La palabra “aplica” especifica que esta medida es de aplicación a partir del nivel para el que se establece.

Las siglas “n.a.” indican que la medida de seguridad para ese control no se aplica a ese nivel.

El símbolo “+” establece que la medida se aplica a nivel medio, incrementándose la seguridad con respecto al anterior nivel.

El símbolo “++” refiere a que la medida se aplica a nivel alto, incrementándose la seguridad con respecto a los anteriores niveles.

El símbolo “=” indica que la medida se aplica con las mismas condiciones de seguridad que el nivel precedente.

Adicionalmente al texto, estas columnas vienen además determinadas por un código de colores. Este código indica si las medidas a aplicar son más severas que las que deberían observarse para las del nivel inferior. Así, la referencia de los colores viene a refrendar de una manera más visual el texto que aparece en las diferentes casillas.

La siguiente de las columnas establece en qué categoría se encuadra la medida definida. Así, en el ejemplo “op.acc.5”, indica que es la medida número 5 de la categoría de control de acceso, dentro del marco operacional.

La última de las columnas hace referencia al texto descriptivo de la medida que deberá ser aplicada. A posteriori de las referidas tablas, en el propio Anexo II del referido Real Decreto, se detalla la información relativa a la medida a aplicar.

7. SYSTEM CENTER CONFIGURATION MANAGER 2012 R2

Microsoft System Center Configuration Manager 2012 R2 continua su evolución como producto líder en el mercado dentro de las soluciones de administración de Microsoft System Center, ayudando a administrar dispositivos y usuarios locales.

Los roles y componentes que forman parte de Microsoft System Center Configuration Manager 2012 R2, en adelante MS SCCM 2012 R2, están estrechamente integrados con Active Directory y dependen de servicios como Internet Information Services o Microsoft SQL Server 2012. Es por ello que es un requerimiento imprescindible planificar adecuadamente la seguridad de estos componentes y aplicar las guías de seguridad correspondientes en las cuales se establecen las bases de seguridad a nivel de Sistema operativo.

MS SCCM 2012 R2 es una herramienta eficaz y compleja para gestionar y administrar usuarios, dispositivos o software. Este producto busca una solución para administrar totalmente los equipos, servidores y dispositivos móviles de una organización.

MS SCCM 2012 R2 aumenta la eficacia y la productividad al reducir las tareas manuales, maximiza las inversiones en hardware y software y fortalece la productividad del usuario al proporcionar el software adecuado en el momento oportuno. A su vez permite la implementación de software seguro y escalable, además de realizar una administración exhaustiva de activos de servidores, escritorios, portátiles y dispositivos móviles.

MS SCCM 2012 R2 emplea los servicios de dominio de Active Directory para la seguridad, la ubicación del servicio, la configuración y detección de los usuarios y dispositivos a administrar en su infraestructura.

Se integra con Microsoft SQL Server como base de datos distribuida de administración de cambios, y utiliza Microsoft SQL Server Reporting Services (SSRS) para la realización de informes con el objetivo de supervisar y hacer seguimiento de las actividades de administración.

Microsoft System Center Configuration Manager se integra con la mayoría de soluciones de Microsoft entre las cuales destacan las siguientes soluciones:

a) Microsoft Intune empleado para administrar una amplia variedad de plataformas de dispositivos móviles.
b) Windows Server Update Services (WSUS) para administrar las actualizaciones de software.
c) Servicios de certificado.
d) Exchange Server y Exchange Online.
e) Directiva de grupo de Windows.
f) DNS.
g) El kit de implementación automatizada de Windows (ADK de Windows) y la herramienta de migración de estado de usuario (USMT).
h) Servicios de implementación de Windows (WDS).
i) Escritorio remoto y Asistencia remota.

8. FUNCIONALIDADES DE SYSTEM CENTER CONFIGURATION MANAGER 2012 R2

Cada funcionalidad de administración principal de MS SCCM 2012 R2 tiene sus propios requisitos previos y funcionalidades las cuales pueden influir en el diseño e implementación de la jerarquía de Configuration Manager. Por ejemplo, si se requiere implementar software en los dispositivos de su organización se deberá disponer de un punto de distribución del sistema de sitio en la organización.

8.1 INVENTARIO DE SOFTWARE Y HARDWARE

Microsoft System Center Configuration Manager 2012 R2 proporciona el inventariado de hardware el cual recopila información sobre la configuración del hardware de los dispositivos cliente de su organización.

Para recopilar el inventario de hardware, es necesario habilitar previamente la opción "Habilitar inventario de hardware en clientes" para que los equipos cliente comiencen a enviar la información solicitada.

Cuando se solicita el inventario de hardware en un equipo cliente, los primeros datos de inventario que se devuelve es un inventario completo. La información del inventario del mismo equipo cliente que se recopila posteriormente contiene únicamente información de inventario diferencial, por lo que únicamente modifica o amplia la información recopilada previamente.

MS SCCM 2012 R2 proporciona compatibilidad limitada con equipos de arranque dual. Es posible detectar equipos de arranque dual, pero únicamente devuelve información de inventario del sistema operativo que estaba activo cuando se ejecutó el ciclo de inventario.

Desde la consola de administración es posible habilitar, deshabilitar, agregar o quitar clases de inventario de hardware personalizado, además se pueden usar archivos NOIDMIF para recopilar información sobre los equipos cliente que Configuration Manager no permite inventariar. Es posible emplear archivos IDMIF para recopilar información acerca de los activos que no están asociados con un cliente de Configuration Manager, por ejemplo, proyectores, impresoras de red o fotocopiadoras.

Es posible inventariar aplicaciones instaladas en dispositivos móviles, las cuales dependerán de si el terminal es propiedad de la empresa o personal, en el caso de dispositivos personales, las únicas aplicaciones inventariadas son las administradas por Microsoft Intune.

La siguiente tabla muestra las aplicaciones que están inventariadas para dispositivos de propiedad personal o de empresa:

Plataforma	Para dispositivos personales	Para dispositivos de la compañía
Windows 10 (sin el cliente de Configuration Manager)	Solo aplicaciones administradas	Solo aplicaciones administradas
Windows 8.1 (sin el cliente de Configuration Manager)	Solo aplicaciones administradas	Solo aplicaciones administradas
Windows Phone 8	Solo aplicaciones administradas	Solo aplicaciones administradas
Windows RT	Solo aplicaciones administradas	Solo aplicaciones administradas
iOS	Solo aplicaciones administradas	Todas las aplicaciones instaladas en el dispositivo
Android	Solo aplicaciones administradas	Todas las aplicaciones instaladas en el dispositivo

Si se precisa obtener más información en referencia a las clases de inventario disponibles para el inventario de hardware en plataformas móviles visite el siguiente enlace: https://docs.microsoft.com/es-es/sccm/mdm/deploy-use/mobile-device-hardware-inventory-hybrid

8.2 ADMINISTRACIÓN Y DISTRIBUCIÓN DE APLICACIONES

En MS SCCM 2012 R2 el termino aplicación hace referencia a uno o varios conjuntos de archivos de instalación de un paquete de software (tipo de implementación).

Los requisitos deciden qué tipo de implementación se instala en los dispositivos cuando la aplicación se implementa.

Microsoft System Center Configuration Manager 2012 R2 permite realizar la implementación de las siguientes aplicaciones:

a) Windows Installer (archivo *.msi)
b) Paquete de aplicación de Windows (*.appx, *.appxbundle)
c) Paquete de aplicación de Windows (en la Tienda Windows)
d) Microsoft Application Virtualization 4
e) Microsoft Application Virtualization 5
f) Archivo .CAB de Windows Mobile
g) MacOS

Es posible administrar dispositivos móviles mediante la administración de dispositivos locales de Microsoft Intune o Configuration Manager, por lo que es posible administrar los siguientes tipos de aplicaciones adicionales:

a) Paquete de aplicación de Windows Phone (archivo *.xap)
b) Paquete de aplicación iOS (archivo *.ipa)
c) Paquete de aplicación de Android (archivo *.apk)
d) Paquete de aplicación para Android en Google Play
e) Paquete de aplicación de Windows Phone (en la Tienda Windows Phone)
f) Windows Installer a través de MDM
g) Aplicación web

Las aplicaciones de MS SCCM 2012 R2 hacen uso de la supervisión basada en estado, por lo que permite hacer un seguimiento del último estado de implementación de una o varias aplicaciones para usuarios y dispositivos.

Las implementaciones de software contienen actualizaciones de software, configuración de cumplimiento, aplicaciones, secuencias de tareas, y paquetes y programas.

Es posible supervisar la implementación de todo el software mediante el área de trabajo “Supervisión” disponible en la consola de administración.

El estado de la implementación de una aplicación puede tener uno de los siguientes estados de cumplimiento:

a) Correcto. La implementación de aplicación se realizó correctamente o ya se encontraba instalada.

b) En curso. La implementación de aplicación está en proceso.

c) Desconocido. No es posible determinar el estado de la implementación de aplicación.

d) Requisitos no cumplidos: la aplicación no se implementó porque no cumple con los requisitos de una dependencia o una regla de requisitos, o porque el sistema operativo en el que se iba a implementar no correspondía.

e) Error: La aplicación no pudo implementarse debido a un error.

MS SCCM 2012 R2 comprueba periódicamente las implementaciones de las aplicaciones mediante el ciclo de evaluación, por lo que, si un usuario desinstala una aplicación, durante el ciclo de evaluación detecta el cambio y que la aplicación no está instalada y vuelve a instalarla de nuevamente.

8.3 ADMINISTRACIÓN Y DISTRIBUCIÓN DE ACTUALIZACIONES

Las actualizaciones de software que suministra MS SCCM 2012 R2 pueden definirse como un conjunto de herramientas y recursos que ayudan en la tarea gestionar y administrar las actualizaciones de software y aplicarlas en equipos cliente de la empresa.

Es recomendable realizar el proceso de actualizaciones de software para subsanar los problemas de seguridad y mantener la estabilidad de la infraestructura de red.

Debido a la naturaleza cambiante de la tecnología y la aparición de nuevas amenazas constantemente la administración de las actualizaciones de software requiere una atención continua y constante.

MS SCCM 2012 R2 se integra con el servicio de Microsoft Update para recuperar los metadatos de actualizaciones de software. El sitio se sincroniza con el servicio de Microsoft Update y cuando finaliza crea una directiva de todo el sitio que proporciona a los clientes la ubicación de los puntos de actualización de software.

Es posible realizar la instalación de varios puntos de actualización de software en un sitio primario. A continuación, se muestran los estados de cumplimiento en relación con las actualizaciones de software.

a) Requerido. Indica que la actualización de software es aplicable y requerida en el equipo cliente.

b) No se requiere. Indica que la actualización de software no es aplicable en el equipo cliente.

c) Instalado. Indica que la actualización se software es aplicable en el equipo y ya está instalada.

d) Desconocida. Indica que el servidor de sitio no recibió el mensaje de estado desde el equipo cliente, por algún error en la comunicación o en el equipo cliente.

8.4 CONFIGURACIÓN DE CUMPLIMIENTO

MS SCCM 2012 R2 proporciona un nuevo rol de seguridad integrado denominado "Administrador de la configuración de cumplimiento", el cual en SCCM 2003 y 2007 se denominaba "Configuración Deseada".

La configuración de cumplimiento contiene las herramientas necesarias para ayudar a evaluar el cumplimiento de los usuarios y equipos cliente para muchas configuraciones, por ejemplo, si están instaladas y configuradas correctamente las versiones correctas de sistema operativo de Windows o si están instaladas y configuradas las aplicaciones necesarias o requeridas por la organización, o si las aplicaciones opcionales están configuradas y si se instalan aplicaciones no permitidas por la organización.

Mediante la configuración de cumplimiento es posible realizar las siguientes tareas:

a) Comparación de la configuración de equipos de escritorio, portátiles, servidores y dispositivos móviles de la organización con configuraciones recomendadas por Microsoft u otros proveedores.

b) Comprobación de la configuración de dispositivos con una o con varias líneas de configuración personalizada ante los equipos de producción.

c) Identificación de las configuraciones de dispositivos mediante los procedimientos de control de cambios no autorizados.

d) Priorización del incumplimiento en cinco niveles de gravedad (ninguno, información, advertencia, crítico y crítico con evento).

e) Informe sobre el cumplimiento con las directivas de las disposiciones legales y directivas de seguridad internas.

f) Identificación de vulnerabilidades de seguridad, como se define por Microsoft u otros proveedores de software.

g) Proporcionar asistencia para detectar las causas más probables de incidencias y problemas comunicados mediante la identificación de las configuraciones no compatibles.

h) Corrección automática de la configuración no compatible para WMI, el registro, las secuencias de comandos y toda la configuración de los dispositivos móviles inscritos en SCCM.

i) Corrección del incumplimiento mediante la implementación de aplicaciones, paquetes, programas o scripts en una colección automática con los equipos que están fuera del cumplimiento de informes.

j) Integración con otros productos de administración que supervisen los eventos de Windows en los equipos para tomar medidas automáticas cuando se notifica una configuración como no conforme.

Para evaluar el cumplimiento de normas se realiza mediante la definición de una línea base de configuración que contiene los elementos de configuración que se quiere evaluar, y las configuraciones y reglas las cuales describen el nivel de cumplimiento que debe cumplir.

Un elemento de configuración se considera un contenedor que puede almacenar la siguiente información:

a) La **información de método de detección** permite detectar si una aplicación está instalada a través de la detección del archivo del programa de instalación de Windows o mediante un script personalizado.

b) La **configuración** representa las condiciones técnicas que se usan para evaluar el cumplimiento en dispositivos cliente.

c) Las **reglas de compatibilidad** especifican las condiciones que definen el cumplimiento del valor de un elemento de configuración.

d) Las **plataformas admitidas** son las plataformas de dispositivo que define en las que se evaluará el elemento de configuración para determinar su cumplimiento.

Los elementos de configuración se clasifican en dos categorías principales:

a) Dispositivos administrados a través del cliente de SCCM. Dispositivos en los que se ha instalado software de cliente de SCCM para su administración.

b) Dispositivos administrados sin el cliente de SCCM: Dispositivos administrados con Microsoft Intune o administración local de SCCM.

Los **perfiles de conexión remota** proveen un conjunto de herramientas y recursos para ayudar a crear, implementar y supervisar la configuración de conexión remota en dispositivos de su organización, minimizando la intervención del usuario final.

8.5 CONTROL REMOTO

En System Center Configuration Manager es posible habilitar la característica de control remoto para administrar de forma remota, dar asistencia o ver todos los equipos cliente.

La característica de control remoto proporciona una herramienta de soporte técnico y permite solucionar problemas de configuración de hardware y software en los equipos cliente.

a) Permite configurar el equipo cliente para ejecutar “Escritorio remoto de Windows” y la asistencia remota desde la consola de administración de Configuration Manager.

b) Permite el control remoto tanto en equipos cliente unidos a un dominio como de un grupo de trabajo.

El control remoto de System Center Configuration Manager tiene dependencias externas y dependencias dentro del producto. En cuanto a las dependencias externas, los dispositivos que ejecutan Windows Embedded, Windows Embedded para punto de servicio (POS) y Windows Fundamentals for Legacy PCs no admiten el visor de control remoto, pero admiten el cliente de control remoto. En cuanto a las dependencias de SCCM el control remoto no está habilitado cuando se instala Configuration Manager por lo que es imprescindible habilitarlo si se desea utilizar.

No es posible usar la característica de control remoto para administrar de forma remota los equipos que ejecuten el cliente de System Management Server 2003 o Configuration Manager 2007.

Se ha de tener en consideración si el permiso "Solicitar al usuario permiso de control remoto" de la configuración de cliente está determinado en "True", la conexión no se iniciara hasta que el usuario en el equipo remoto acepte la solicitud de control remoto.

System Center Configuration Manager permite hacer uso de los informes para obtener la información de auditoria de la característica de control remoto.

A continuación, se muestran los informes que se encuentran disponibles en el apartado informes de SCCM:

a) Control remoto - Todos los equipos controlados remotamente por un usuario específico: muestra un resumen de la actividad de control remoto iniciado por un usuario específico.

b) Control remoto - Toda la información de control remoto: muestra un resumen de los mensajes de estado sobre el control remoto de equipos cliente.

8.6 DESPLIEGUE DE SISTEMAS OPERATIVOS

MS SCCM 2012 R2 dispone de varios métodos con los que es posible realizar la implementación de un sistema operativo, dependiendo de la infraestructura se deberá establecer cuál es el método más adecuada a su entorno.

Las **implementaciones realizadas mediante PXE** (Preboot eXecution Environment), permiten a los equipos cliente solicitar una implementación a través de la red, con este método de despliegue, la imagen de sistema operativo y la imagen de arranque de Windows PE se envía a través de un punto de distribución que está configurado para aceptar solicitudes de arranque de PXE.

Las **implementaciones de multidifusión**, se caracterizan por ahorrar ancho de banda de red al enviar datos a varios clientes a la vez en lugar de enviar una copia de los datos a cada equipo cliente a través conexiones diferentes, la imagen de sistema operativo se envía a un punto de distribución y este a su vez implementa la imagen cuando los equipos cliente solicitan la implementación.

Las **implementaciones de medios de arranque**, permiten implementar el sistema operativo al iniciar el equipo de destino. Cuando se inicia el equipo de destino, recupera la secuencia de tareas, la imagen de sistema operativo y cualquier otro tipo de contenido necesario de la red. Debido a que el contenido no se incluye en los medios, puede actualizar el contenido sin tener que volver a crear los medios.

Las **implementaciones de medios independientes**, permiten implementar sistemas operativos en las condiciones siguientes:

a) Entornos donde no resulta práctico copiar una imagen de sistema operativo u otros paquetes de software grandes a través de la red.

b) Entornos sin conectividad de red o conectividad de red de bajo ancho de banda.

Las **implementaciones de medios preconfigurados** permiten implementar un sistema operativo en un equipo que no está aprovisionado por completo. El medio preconfigurado es un archivo Windows Imaging Format (WIM) que puede ser instalado en un equipo sin sistema operativo por el fabricante o en un centro de configuración empresarial no relacionado con el entorno de Configuration Manager.

Las imágenes de sistema operativo a desplegar son archivos WIM los cuales son una recopilación comprimida de los archivos necesarios para realizar la instalación y configuración correctamente de un equipo.

Existen tres acciones que se deben llevar a cabo para implementar una imagen de sistema operativo.

a) Generar y capturar una imagen y distribuirla en los puntos de distribución.

b) Crear y configurar la secuencia de tareas que instalará la imagen de sistema operativo.

c) Implementar la secuencia de tareas.

MS SCCM 2012 R2 permite importar un catálogo de controladores que contiene referencias de todos los controladores de dispositivos necesarios, por lo que es posible instalar controladores de dispositivos sin incluirlos en la imagen de sistema operativo.

Cuando se implementa un sistema operativo es posible instalar aplicaciones, herramientas de implementación, contenidos de los paquetes de software y actualizaciones de software en el equipo de destino.

Cuando se despliegan sistemas operativos es posible guardar el estado del usuario, implementar el nuevo sistema operativo y posteriormente restaurar el estado del usuario, esta tarea es realizada cuando la operación a realizar es actualizar el sistema operativo.

8.7 ADMINISTRACIÓN DE LICENCIAS DE SOFTWARE

En MS SCCM 2012 R2 se dispone de la herramienta Asset Intelligence el cual permite inventariar y administrar las licencias de uso de software de toda la empresa mediante su catálogo.

El catálogo de Asset Intelligence es un conjunto de tablas de base de datos almacenados que contienen información de categorización e identificación de más de 300.000 títulos de software y sus versiones.

El catálogo de Asset Intelligence provee la información de licencia de software para títulos de software que se utilizan, tanto de software Microsoft como de software de terceros. Asset Intelligence contiene las siguientes secciones:

a) Sincronización de catálogo: Proporciona información sobre si está habilitada la inteligencia de activos y el estado actual del punto de sincronización de Asset Intelligence.

b) Estado del Software en el inventario: Proporciona el número y el porcentaje de inventario de software, las categorías de software y las familias de software.

Asset Intelligence admite las 7 etiquetas de identificación de software obligatorias que se definen en ISO/IEC 19770-2. El estándar ISO/IEC 19770-2 especifica la estructura y el uso básico de identificación de software

Los informes de Asset Intelligence proporcionan información sobre hardware, administración de licencias y software de su organización.

8.8 ADMINISTRACIÓN DE ENDPOINT PROTECTION

El servicio de Endpoint Protection permite gestionar las directivas de prevención de código dañino y la seguridad del Firewall de Windows para equipos cliente. A partir de Windows 10 y Windows Server 2016, los equipos no requieren ningún cliente adicional para la administración de Endpoint Protection, en cambio para los equipos clientes con sistema operativo con versiones Windows 8.1 y anteriores se instala el cliente de Endpoint protection y el cliente de Configuration Manager.

El servicio de Endpoint Protection en SCCM tiene las siguientes características y ventajas:

a) Detección y corrección de código dañino y programas espía.

b) Detección y corrección de rootkit

c) Evaluación y definición automática de vulnerabilidades críticas y actualizaciones del motor

d) Detección de vulnerabilidades de red a través del Sistema de inspección de red

e) Integración con Cloud Protection Service para informar a Microsoft sobre código dañino.

f) Configuración de directivas de protección contra código dañino, configuración del Firewall de Windows y administración de la protección contra amenazas avanzada de Windows Defender en grupos de equipos seleccionados.

g) Actualizaciones de software para la descarga de los archivos de definición de código dañino más recientes.

h) Envío de notificaciones de correo electrónico para mantener a los administradores del entorno informados cuando se detecte código dañino en los equipos cliente.

El servicio de Endpoint Protection permite establecer directivas de protección contra código dañino que contengan opciones de configuración de cliente, además, se pueden implementar estas directivas en los equipos cliente y supervisarlos en el nodo Estado de Endpoint Protection o mediante informes de Configuration Manager.

El servicio de Endpoint Protection permite realizar una administración básica del Firewall de Windows en los equipos cliente, para cada perfil es posible configurar las siguientes opciones:

a) Habilitar o deshabilitar el Firewall de Windows.

b) Bloquear todas las conexiones entrantes, incluidas las de la lista de programas permitidos.

c) Notificar al usuario cuando el Firewall de Windows bloquee un nuevo programa.

Desde la versión 1606, la administración y supervisión de la protección contra amenazas avanzadas de Windows Defender (ATP) proporciona un servicio de apoyo para las empresas en el momento de detectar ataques avanzados para la investigación y respuesta temprana.

System Center Endpoint Protection incluye clientes para Linux y equipos Mac, pero, en estos sistemas a los que no se les suministra el cliente a través de Configuration Manager es necesario realizar la descarga del software, System Center 2012 Endpoint Protection para Mac y System Center 2012 Endpoint Protection para Linux.

Windows Defender o Endpoint Protection incluyen las siguientes características para ayudar a proteger el equipo frente a posibles amenazas:

a) Integración con Firewall de Windows, permitiendo activar o desactivar Firewall de Windows.

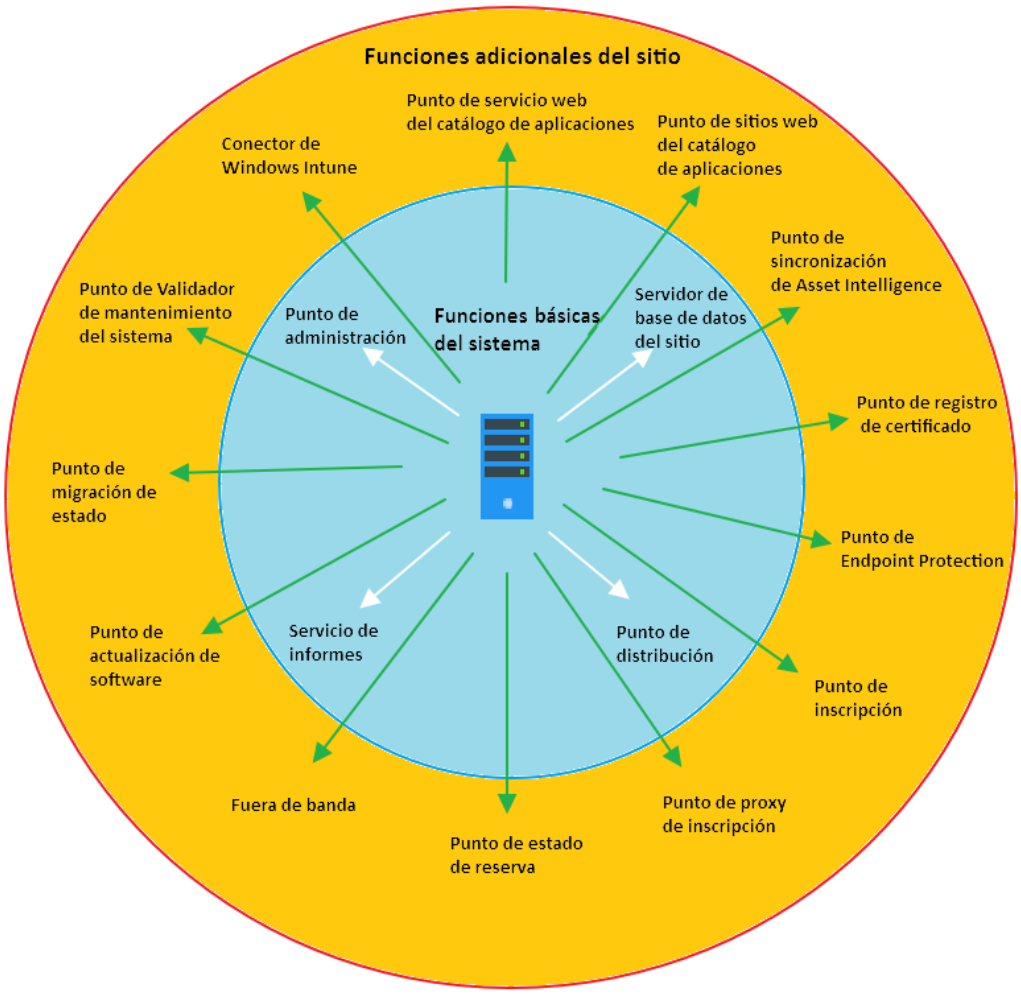
b) Sistema de inspección de redes, mejorando la protección en tiempo real mediante la inspección del tráfico de red.

c) Motor de protección, protección en tiempo real detectando e impidiendo que el código dañino se instale o se ejecute en su equipo.

9. ROLES DEL SISTEMA DE SITIO DE MS SCCM 2012 R2

En cada sitio de MS SCCM 2012 R2, es posible instalar uno o más roles de sistema de sitio para ampliar la funcionalidad de administración del sitio.

El diagrama siguiente muestra los roles básicos y adicionales del sistema de sitio que es posible agregar al equipo del servidor de sitio o distribuir mediante la instalación de servidores adicionales del sistema de sitio:



Los roles del sistema de sitio que proporcionan una funcionalidad de administración básica de la infraestructura, a continuación, se detallan en la siguiente tabla:

Rol de sistema de sitio	Descripción
Servidor de sitio	Equipo desde el que se ejecuta el programa de instalación de Configuration Manager y que proporciona la funcionalidad básica para el sitio.
Servidor de base de datos del sitio	Servidor que se encarga de alojar la base de datos de SQL Server, almacenar la información acerca de los activos y los datos del sitio de Configuration Manager.
Servidor de componentes	Servidor que ejecuta los servicios de Configuration Manager. Cuando se instalan todos los roles del sistema de sitio, excepto el rol de punto de distribución, Configuration Manager instala automáticamente el servidor de componentes.
Punto de administración	Rol del sistema de sitio que proporciona a los clientes información de ubicación de servicio y de directiva y recibe datos de configuración de los clientes.
Punto de distribución	Rol del sistema de sitio que contiene los archivos de origen para ser descargados por los equipos cliente, por ejemplo, imágenes de arranque, contenido de los paquetes de software, actualizaciones de software, imágenes del sistema operativo y contenido de la aplicación.

Los roles adicionales del sistema de sitio que podría necesitar para funcionalidades específicas se enumeran en la tabla siguiente.

Rol de sistema de sitio	Descripción
Punto de servicio web del catálogo de aplicaciones	Rol del sistema de sitio que ofrece información de software al sitio web del catálogo de aplicaciones desde la biblioteca de software.
Punto de sitios web del catálogo de aplicaciones	Rol del sistema de sitio que ofrece a los usuarios una lista de software disponible desde el catálogo de aplicaciones.
Punto de sincronización de Asset Intelligence	Rol de sistema de sitio que se conecta a Microsoft para descargar información del catálogo de Asset Intelligence y para cargar títulos sin categorizar para considerar su futura inclusión en el catálogo.
Punto de registro de certificado	Rol del sistema del sitio que se comunica con un servidor que ejecuta el servicio de inscripción de dispositivos de red para administrar las solicitudes de certificados de dispositivo que utilizan el protocolo de inscripción de certificados Simple (SCEP).
Punto de Endpoint Protection	Rol de sistema de sitio que utiliza Configuration Manager para aceptar los términos de la licencia de Endpoint Protection y para configurar la pertenencia a Microsoft Active Protection Service.
Punto de inscripción	Rol de sistema de sitio que hace uso de certificados PKI para Configuration Manager para inscribir dispositivos móviles y equipos Mac, y aprovisionar equipos basados en Intel AMT.
Punto de proxy de inscripción	Rol de sistema de sitio que administra solicitudes de inscripción de Configuration Manager por parte de dispositivos móviles y equipos Mac.

Rol de sistema de sitio	Descripción
Punto de estado de reserva	Rol de sistema de sitio que ayuda a supervisar la instalación del cliente e identificar a los clientes sin administrar porque no se pueden comunicar con su punto de administración.
Servidor que ejecuta Internet Information Services (IIS)	Rol del sistema de sitio que suministra y gestiona equipos basados en Intel AMT para la administración fuera de banda.
Punto de actualización de software	Rol de sistema de sitio que se integra con Windows Server Update Services (WSUS) para suministrar las actualizaciones de software para los equipos cliente de Configuration Manager.
Punto de migración de estado	Rol de sistema de sitio que almacena datos de estado de usuario cuando se migra un equipo a un nuevo sistema operativo.
Punto de Validador de mantenimiento del sistema	Rol de sistema de sitio que valida las directivas de protección de acceso a redes (NAP) de Configuration Manager. Debe instalarse en un servidor de directivas de mantenimiento NAP.
Punto de servicio de informes	La integración de MS SCCM 2012 R2 con SQL Server Reporting Services proporciona un conjunto de herramientas y recursos para hacer uso de las avanzadas funcionalidades de informes de SQL Server Reporting Services (SSRS).

9.1 SITIOS Y JERARQUIAS DE SYSTEM CENTER CONFIGURATION MANAGER 2012 R2

Una implementación de MS SCCM 2012 R2 debe instalarse en un dominio de Active Directory. La implementación de uno o varios sitios de Configuration Manager forman una jerarquía de sitios.

a) Al implementan varios sitios se establecen relaciones entre los elementos secundarios y los elementos primarios estableciendo una jerarquía.

b) Gracias a la jerarquía es posible administrar de forma centralizada un mayor número de sitios y equipos cliente. Los datos y la información fluyen de forma descendente por la jerarquía hasta llegar a los dispositivos que administra.

c) Toda la información acerca de dispositivos y los resultados de las solicitudes y las tareas de configuración fluyen de forma ascendente en la jerarquía.

d) Aunque la implementación de un único sitio también se denomina una jerarquía.

Cuando se implementa MS SCCM 2012 R2, el primer sitio de Configuration Manager implementado establecerá el ámbito de la jerarquía de los sitios por lo que este primer sitio de Configuration Manager se establece como la base desde la que se administraran los equipos cliente y los usuarios de la infraestructura.

Para implementaciones a gran escala lo recomendado es la creación de un sitio central proporcionando un punto central de administración que aporta la flexibilidad necesaria para admitir equipos cliente distribuidos por una infraestructura de red global.

Para la creación de un sitio de administración central, es necesario instalar uno o varios sitios primarios porque un sitio de administración central no admite directamente la gestión de equipos cliente, cuya función corresponde a un sitio primario.

Un sitio de administración central permite la implementación de varios sitios primarios y secundarios. Los sitios primarios o secundarios se usan para administrar equipos cliente y controlar el ancho de banda de red cuando los equipos que se gestionan estén en ubicaciones geográficas diferentes.

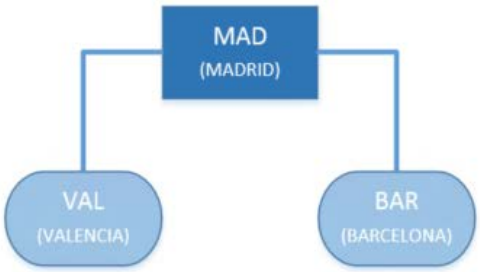
Un sitio de administración central admite hasta 25 sitios primarios o secundarios y cada sitio primario admite hasta 250 sitios secundarios, pero los sitios secundarios no admiten otros sitios secundarios.

Para implementaciones en infraestructuras de menor envergadura es recomendable la instalación de un sitio primario independiente el cual permite gestionar equipos cliente sin disponer de sitios adicionales centralizando y simplificando la arquitectura que se administra.

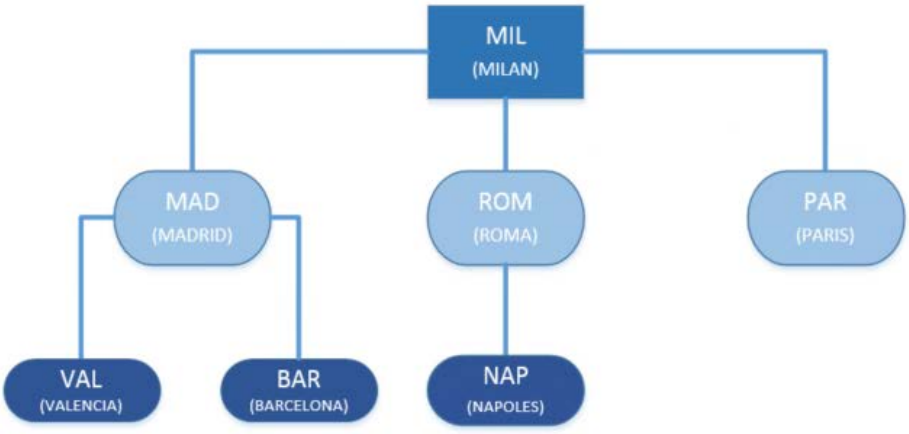
Una vez instalado el primer sitio, es posible instalar sitios adicionales. Además, si el primer sitio es un sitio de administración central, es posible instalar uno o varios sitios primarios o secundarios.

Un sitio secundario solo puede implementarse por debajo de un sitio primario. Estos sitios secundarios facilitan la gestión de equipos clientes ubicados en redes de conexión lenta extendiendo el alcance de un sitio primario.

Ejemplo: Sitio independiente



Ejemplo Jerarquía: Sitio primario con sitios secundarios



Ejemplo Jerarquía: Sitio de administracion central con sitios primarios y sitios secundarios

9.2 PUNTO DE ADMINISTRACIÓN

MS SCCM 2012 R2 proporciona a los clientes la información de ubicación de servicios y directivas, y recibe los datos de configuración de los clientes. El punto de administración facilita las herramientas necesarias para administrar el contenido que se despliega por la infraestructura como, las aplicaciones, los contenidos de los paquetes de software, las actualizaciones de software o implementaciones de sistema operativo.

Es necesario planear previamente la arquitectura que se desea implementar para hacer un uso adecuado de la infraestructura de administración de contenido, por lo que es recomendable conocer todas las opciones y configuraciones disponibles para adaptarlas apropiadamente a su entorno de red y a sus requerimientos de implementación de contenido.

Cada sitio primario admite hasta 15 puntos de administración, y cada sitio secundario admite un solo punto de administración que se debe instalar en el servidor de sitio secundario.

Cada punto de administración puede admitir hasta 25.000 clientes y dispositivos en total en la siguiente proporción:

a) Un máximo de 25000 equipos de escritorio.

b) Un máximo de 10000 dispositivos administrados a través de un MDM local o 10 000 dispositivos que ejecutan clientes Mac y Windows CE 7.0.

   Si desea obtener más información acerca de la escalabilidad de MS SCCM 2012 R2 visite la siguiente URL:

   https://docs.microsoft.com/es-es/sccm/core/plan-design/configs/size-and-scale-numbers.

9.2.1 CUENTAS PARA LA ADMINISTRACIÓN DE CONTENIDO

Antes de implementar el contenido en SCCM es necesario plantear el acceso a ese contenido desde los puntos de distribución.

9.2.1.1 CUENTA DE ACCESO A LA RED

La cuenta de acceso a la red, es usada por los equipos clientes para conectarse a un punto de distribución y acceder al contenido. Esta cuenta también la usan los puntos de distribución de extracción para obtener el contenido de un punto de distribución de origen en un bosque remoto.

Los equipos cliente hacen uso de la cuenta de acceso a la red cuando no es posible usar su cuenta de equipo local para acceder al contenido de los puntos de distribución, esto se aplica a los equipos y clientes del grupo de trabajo de dominios que no son de confianza.

Se recomienda establecer a esta cuenta los permisos mínimos por lo que la cuenta debe tener el permiso de “Tener acceso a este equipo desde la red” en el punto de distribución, pero es importante **no conceder derechos de inicio de sesión**, ni conceder permisos de unir equipos al dominio a la cuenta de acceso a la red. Si fuese necesario unir equipos al dominio durante una secuencia de tareas, se recomienda que utilice la cuenta de unión al dominio del editor de secuencia de tareas.

También se hace uso de la cuenta de acceso a la red cuando se realiza la implementación de un sistema operativo sobre un equipo que está instalando el sistema operativo que no tiene aún una cuenta de equipo en dominio.

a) Los clientes solo usan la cuenta de acceso de red para tener acceso a recursos de la red.

b) Es posible configurar varias cuentas para usar como cuenta de acceso a la red en cada sitio principal.

c) Los clientes intentan obtener el acceso al contenido de un punto de distribución a través la cuenta <NombreDeEquipo>. Si se produce un error en esta cuenta, los clientes intentan usar una cuenta de acceso a la red.

9.2.1.2 CUENTA DE ACCESO AL CONTENIDO DEL PAQUETE DE SOFTWARE

La cuenta de acceso al contenido del paquete de software, concede acceso al contenido de punto de distribución, a las cuentas integradas denominadas “Usuarios y Administradores”. Es posible configurar permisos adicionales para restringir el acceso. Para acceder al contenido del paquete de software, es posible permiten establecer permisos del sistema de archivos NTFS para especificar los usuarios y grupos de usuarios.

MS SCCM 2012 R2 solo concede acceso a las cuentas genéricas “Usuarios y Administradores”, pero es posible controlar el acceso de los equipos cliente mediante el uso de grupos o cuentas de Windows adicionales. Por ejemplo, los dispositivos móviles no utilizan las cuentas de acceso al contenido del paquete de software porque siempre recuperan el contenido del paquete de forma anónima siempre que esté permitido en la configuración.

MS SCCM 2012 R2 copia los archivos de contenido de un paquete en un punto de distribución y este otorga acceso de “Lectura” al grupo local “Usuarios” y “Control total” al grupo “Administradores locales”. Es necesario asegurarse de que la cuenta de acceso de red tiene permisos para acceder al paquete mediante el uso de las cuentas de acceso de paquete definidas.

Si se crea o modifica una cuenta después de haber creado el paquete será necesario redistribuirlo, a su vez, se deberá tener en consideración que la actualización del paquete no modifica los permisos del sistema de archivos NTFS en el paquete.

No es necesario agregar la cuenta de acceso de red como una cuenta de acceso de paquete, ya que la pertenencia al grupo “Usuarios” la agrega automáticamente, por lo que restringir la cuenta de acceso de paquete a solo la cuenta de acceso a la red no impide que los clientes accedan al paquete.

9.2.1.3 CUENTA DE CONEXIÓN MULTIDIFUSIÓN

La cuenta de conexión multidifusión es utilizada para las implementaciones de sistemas operativos. Los puntos de distribución que se encuentran configurados para la multidifusión hacen uso de la cuenta de conexión multidifusión para leer la información de la base de datos del sitio.

Es necesario especificar la cuenta que se debe utilizar al configurar conexiones de base de datos de MS SCCM 2012 R2 para la multidifusión

De forma predeterminada, se emplea la cuenta de equipo del punto de distribución, pero puede configurar una cuenta de usuario en su lugar.

Es obligatorio especificar una cuenta de usuario cada vez que la base de datos del sitio esté en un bosque que no sea de confianza.

La cuenta de conexión de multidifusión debe tener permisos de “Lectura” para la base de datos del sitio.

Es importante **no conceder permisos de inicio de sesión interactivos** a la cuenta de conexión multidifusión, aumentando con ello la seguridad de la infraestructura.

9.3 PUNTOS DE DISTRIBUCIÓN

Los roles de sitio de puntos de distribución alojan el contenido (archivos y software) que se implementa en los equipos cliente y usuarios. Además, es posible crear grupos de puntos de distribución que simplifican la gestión de los puntos de distribución y el cómo se distribuye el contenido de los puntos de distribución.

Algunas opciones de configuración de un punto de distribución únicamente están disponibles una vez implementado el rol y no durante la instalación. Las opciones de configuración disponibles cuando se implementa un punto de distribución son:

a) Permitir que SCCM instale el rol necesario de Internet Information Services en el equipo donde se está implementando el punto de distribución

b) Configurar el espacio de la unidad para el punto de distribución

Las opciones de configuración de un sitio de punto de distribución disponibles cuando se configura posteriormente.

a) Administrar relaciones de grupo de puntos de distribución

b) Ver el contenido implementado en el punto de distribución

c) Configurar los límites de frecuencia de las transferencias de datos a los puntos de distribución

d) Configurar las programaciones de las transferencias de datos a los puntos de distribución

Es necesario establecer un servidor de sistema de sitio como punto de distribución antes de que el contenido pueda estar disponible en los equipos cliente, además es posible agregar el rol de sitio de punto de distribución a un nuevo servidor de sistema de sitio o a uno ya existente.

Antes de implementar un nuevo sitio de punto de distribución, se ha de tener en consideración que debe poseer los permisos necesarios para su implementación y configuración que son los siguientes:

a) Leer en el objeto punto de distribución

b) Copiar en punto de distribución en el objeto punto de distribución

c) Modificar en el objeto Sitio

d) Administrar certificados para implementación de sistema operativo en el objeto Sitio

Los grupos de puntos de distribución proporcionan una agrupación lógica de los puntos de distribución de la organización para la distribución de contenido. Es posible usar estos grupos para administrar y supervisar el contenido desde una ubicación central de puntos de distribución que abarcan varios sitios, pero se ha de tener en consideración lo siguiente:

a) Se permite agregar uno o varios puntos de distribución desde cualquier sitio de la jerarquía a un grupo de puntos de distribución.

b) Se permite agregar un punto de distribución a más de un grupo de puntos de distribución.

c) El contenido que se distribuye a un grupo de puntos de distribución, se distribuye a todos los puntos de distribución que son miembros del grupo de puntos de distribución.

d) Cuando se agrega un punto de distribución al grupo de puntos de distribución después de la distribución de contenido inicial, automáticamente se distribuye el contenido al nuevo miembro del grupo.

e) Es posible asociar una colección a un grupo de puntos de distribución.

Se debe tener en consideración que, si después de distribuir contenido a una colección, asocia la colección a otro grupo de puntos de distribución, es necesario redistribuir el contenido a la colección antes de distribuirlo al nuevo grupo de puntos de distribución

Una vez implementado un punto de distribución es posible configurar los siguientes valores generales:

a) Instalar y configurar IIS si es requerido por Configuration Manager.

b) Habilitar y configurar BranchCache.

c) Configurar la forma en la que los dispositivos cliente se comunican con el punto de distribución (HTTP o HTTPS).

d) Habilitar o deshabilitar las conexiones anónimas de los equipos cliente.

e) Establecer un certificado autofirmado o importar un certificado de cliente de infraestructura de clave pública (PKI) para el punto de distribución.

f) Habilitar el punto de distribución para contenido preconfigurado.

9.3.1 CONFIGURACIÓN DE UNIDAD

Cuando se implementa un punto de distribución es posible realizar la **configuración de la unidad** que permite configurar la prioridad de las unidades de disco y la cantidad de espacio libre en disco que debe quedar en cada unidad de disco

a) Reserva de espacio de unidad (MB), configurando esta opción es posible establecer el espacio libre disponible de la unidad donde se aloja el contenido. El contenido puede ocupar varias unidades.

b) Ubicaciones de contenido, configurando esta opción se establece la ubicación de la librería de contenido y el recurso compartido del contenido.

9.3.2 PXE

Cuando se habilita **PXE**, SCCM instala los Servicios de implementación de Windows en el servidor, el cual realiza el arranque PXE para instalar sistemas operativos, una vez habilitada dicha opción es necesario realizar la configuración de los siguientes valores:

a) Permitir que este punto de distribución responda a solicitudes de PXE entrantes

b) Habilitar compatibilidad de equipos desconocida

c) Requerir una contraseña cuando los equipos usen PXE.

d) Afinidad de dispositivo del usuario.

e) Interfaces de red.

f) Especificar retraso en la respuesta del servidor PXE (segundos).

9.3.3 MULTIDIFUSIÓN

Cuando la **multidifusión** es habilitada, es posible enviar los datos simultáneamente a varios clientes una vez habilitada dicha opción es necesario realizar la configuración de los siguientes valores:

a) Cuenta de conexión de multidifusión

b) Configuración de dirección de multidifusión

c) Intervalo de puertos UDP para multidifusión

d) Velocidad de transferencia de cliente.

e) Número máximo de clientes.

f) Habilitar multidifusión programada.

9.3.4 CONTENIDO Y LIMITES DE FRECUENCIA

La sección de **paquetes de implementación** proporciona una lista de los paquetes distribuidos en los puntos de distribución. A continuación, se detallan las opciones que se pueden realizar en los paquetes de implementación:

a) Validar: Se inicia el proceso para validar la integridad de los archivos de contenido en el paquete.

b) Redistribuir: Copia nuevamente los archivos de contenido en el punto de distribución y sobrescribe los archivos existentes.

c) Quitar: Elimina los archivos de contenido del punto de distribución.

Es posible validar la integridad de los archivos de contenido del punto de distribución, mediante el establecimiento de una programación para realizar la validación.

La sección de **límites de velocidad** permite controlar el ancho de banda de red que se usa cuando se transfiere contenido al punto de distribución, y se puede realizar la siguiente configuración:

a) Ancho de banda ilimitado en los envíos al destino.

b) Modo por pulsos, especificando el tamaño de los bloques de datos que se envían al punto de distribución.

c) Ancho de banda limitado al máximo, especificando velocidades de transferencia por hora

9.3.5 PROGRAMACIÓN Y LIMITE DE ANCHO DE BANDA

La programación y el límite de ancho de banda son opciones que ayudan a controlar cuando se distribuye el contenido de un servidor de sitio en los puntos de distribución, es muy similar a los controles de ancho de banda para la replicación basada en archivos de sitio a sitio.

En MS SCCM 2012 R2 es posible realizar una programación y especificar opciones de límite en puntos de distribución remotos para determinar cómo y cuándo se distribuye el contenido.

9.4 PUNTO DE SERVICIO DE INFORMES

La integración de MS SCCM 2012 R2 con SQL Server Reporting Services proporciona un conjunto de herramientas y recursos para hacer uso de las avanzadas funcionalidades de informes de SQL Server Reporting Services (SSRS) y la amplia experiencia de creación que ofrece el generador de informes de Reporting Services.

Con la generación de informes es posible recopilar, mostrar y categorizar información acerca de toda la infraestructura de una organización, por ejemplo, los usuarios, el inventario de hardware y software, las actualizaciones de software, las aplicaciones y el estado del sitio.

La herramienta de generación de informes ofrece varios informes preestablecidos que pueden usarse sin previa configuración, pero también es posible editarlos para adaptarlo a las necesidades de la organización, y en caso de que no se adapten a las necesidades de la organización, se pueden crear informes completamente personalizados.

La integración entre MS SCCM 2012 R2 y SQL Server Reporting Services proporciona las siguientes ventajas:

a) Utilización de un sistema de informes estándar del sector para consultar la base de datos de SCCM.

b) Los informes se muestran a través del Visor de informes de Configuration Manager o mediante el Administrador de informes, se basa en una conexión al informe basada en web.

c) Proporciona elevada escalabilidad, disponibilidad y alto rendimiento.

d) Provee suscripciones a informes a los que pueden suscribirse los usuarios.

e) Posibilidad de exportar informes que pueden seleccionar los usuarios en una gran variedad de los formatos más usados.

Los servicios de informes son un rol que se implementan en un sitio el cual debe disponer de Microsoft SQL Server Reporting Services.

El punto de servicios de informes copia las definiciones de informes de SCCM en Reporting Services, crea las carpetas de informes basadas en categorías de informes e instaura una directiva de seguridad sobre los informes y las carpetas de informes apoyada en los permisos basados en roles para los usuarios administrativos.

MS SCCM 2012 R2 suministra definiciones de informes para más de 400 informes en más de 50 carpetas de informes, que se copian en la carpeta de informes raíz de SQL Server Reporting Services. El generador de informes incluye las siguientes capacidades:

a) Entorno de creación de informes intuitivo, con un aspecto similar a Microsoft Office.

b) Diseño flexible de informes del lenguaje RDL (Report Definition Language) de SQL Server.

c) Diferentes formas de visualización de datos, incluidos gráficos e indicadores.

d) Proporciona cuadros de texto con formato enriquecido.

e) Exportación a formato de Microsoft Word.

SQL Reporting Services en Configuration Manager utiliza modelos de informe permitiendo a los usuarios con privilegios administrativos incluir elementos de la base de datos en modelos. Los modelos de informes tienen las siguientes características:

a) Es posible dar a los campos y las vistas de la base de datos nombres empresariales lógicos para facilitar la producción de informes.

b) Es posible agrupar los elementos lógicamente.

c) Es posible definir relaciones entre elementos.

d) Es posible proteger los elementos del modelo para que los usuarios administrativos solo puedan ver los datos que tienen permiso para ver.

Es recomendable usar el analizador de consultas y el generador de perfiles de Microsoft SQL Server para optimizar las consultas previniendo con ello posibles retrasos en los informes debido al tiempo de ejecución y recuperación de los resultados.

Si desea conocer los informes que se incluyen en MS SCCM 2012 R2 visite la siguiente URL:

https://docs.microsoft.com/es-es/sccm/core/servers/manage/list-of-reports

9.5 ADMINISTRACIÓN DE CLIENTES

MS SCCM 2012 R2 ofrece varios métodos para la supervisión y administración remota del software de los equipos cliente de la organización una vez que se ha integrado en la consola de administración, permitiendo configurar el equipo cliente para ejecutar el Escritorio remoto de Windows y la asistencia remota desde la propia consola de Configuration Manager.

El control remoto es usado para supervisar los equipos cliente y comprobar el estado de la configuración y en caso de ser necesario es posible realizar una corrección automática según el problema detectado. En la consola de MS SCCM 2012 R2 se ofrecen diversos métodos para administrar clientes de dispositivos individuales o selecciones de dispositivos.

Cuando un cliente de MS SCCM 2012 R2 es instalado y asignado correctamente a un sitio de Configuration Manager, este se muestra en el área de trabajo “Activos y compatibilidad” en el apartado “Dispositivo”. A continuación, se muestran las tareas administrativas posibles para ejecutar en los dispositivos.

a) Administrar la información de afinidad de dispositivo de usuario

b) Agregar el dispositivo a una recopilación nueva o existente

c) Instalar y volver a instalar el cliente mediante el asistente Inserción del cliente

d) Reasignar el sitio

e) Administrar de forma remota el cliente

f) Aprobar un cliente

g) Bloquear o desbloquear un cliente

h) Desactivar una implementación de PXE necesaria

i) Administrar las propiedades del cliente

j) Borrar un dispositivo móvil

k) Retirar un dispositivo móvil

l) Cambiar la propiedad de un dispositivo

La afinidad entre usuario y dispositivo en MS SCCM 2012 R2 vincula un usuario a uno o varios dispositivos. Es posible implementar una aplicación para un usuario sin conocer los nombres de los equipos del usuario. Esa afinidad garantiza que la aplicación se instale en todos los dispositivos asociados a ese usuario. Además, es posible asociar dispositivos primarios que son los catalogados como los más usados por los usuarios.

La caché del cliente almacena los archivos temporales para el momento en que los clientes instalen aplicaciones y programas, en cambio la cache de las actualizaciones de software no está limitada por tamaño de cache configurado. Es importante destacar que no se puede descargar contenido de carpetas cifradas.

A partir de la versión 1606 de MS SCCM se permite especificar el tamaño de la carpeta de caché mediante la configuración del cliente. La ubicación predeterminada de la caché de cliente es “%windir%\ccmcache” y el espacio en disco predeterminado es 5120 MB.

MS SCCM 2012 R2 también se integra con dispositivos con otros sistemas operativos como Linux y UNIX, y mediante los mismos métodos que se usa para ver la información de sistemas clientes basados en Windows permite ver la información la siguiente información:

a) Detalles de estado de los clientes.

b) Detalles sobre los clientes en los informes predeterminados de SCCM.

c) Detalles de inventario en el Explorador de recursos.

También es posible gestionar equipos cliente que se encuentran ubicados fuera de la red corporativa y que están conectados a Internet, sin la necesidad de que los clientes se conecten mediante redes privadas virtuales para conectar con los servidores del sistema de sitio de su empresa. MS SCCM suministra dos maneras de administrar los clientes conectados a Internet:

a) Puerta de enlace de administración en la nube.

b) Administración de cliente basada en Internet.

MS SCCM 2012 R2 desde su versión 1610, presenta la puerta de enlace de administración en la nube, este nuevo método proporciona una administración en base a una combinación de un servicio en la nube implementado en Microsoft Azure y un nuevo rol de sistema que se comunica con dicho servicio. A través de esta configuración se obtienen muchas ventajas como no tener que invertir en la infraestructura o evitar exponer la infraestructura local hacia internet, pero también se observan algunas desventajas como el coste de suscripción en la nube o que los datos se envíen a través del servicio de nube.

Si desea más información sobre la administración de cliente basada en la nube, visite la siguiente URL:

https://docs.microsoft.com/es-es/sccm/core/clients/manage/plan-cloud-management-gateway

La administración de cliente basada en internet, se basa en los servidores de sitio con conexión a internet con los que se comunican los clientes.

Existen ciertas ventajas como la no dependencia de un servicio en la nube, el costo de la suscripción en la nube o el control completo de los servidores, pero también existen desventajas como la necesidad de una gran inversión inicial, los costos generales de la infraestructura y el más importante que es la exposición de su infraestructura a internet.

Si desea más información sobre la administración de cliente basada en internet, visite la siguiente URL:

https://docs.microsoft.com/es-es/sccm/core/clients/manage/plan-internet-based-client-management

10. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN MS SCCM 2012 R2

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de MS SCCM 2012 R2 sobre servidores Windows Server 2012 R2 y que les sea de aplicación el ENS, se establecerán, a través de la presente guía, las condiciones necesarias de aplicación. Éstas 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.

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

a) Aplicación de seguridad en los controladores de dominio Windows Server 2012 R2 que puedan dar soporte a la organización y sobre los que se asientan muchos de los activos tecnológicos de dicha organización. Será además el mecanismo empleado para conducir la centralización y gestión de la seguridad.

b) Aplicación de seguridad en servidores miembro de dominio que sustentarán los diferentes servicios que prestara la organización, sujetos al RD 3/2010 y que se encontrarán implementados con Microsoft Windows Server 2012 R2 siguiendo la guía “CCN-STIC-870A, Implementación del ENS en Windows Server 2012 R2” y “CCN-STIC-873, Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para System Center Configuration Manager, 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, estás van a ser explicadas, y 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, qué mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información, a continuación, se detallarán las diferentes plantillas de seguridad aplicables en función de los diferentes niveles de seguridad.

A continuación, se muestra una tabla con el refuerzo de seguridad recomendado para los roles y las comunicaciones que se han llevado a cabo en la presente guía.

	Nivel Bajo	Nivel Medio	Nivel Alto
Comunicación cliente	Kerberos	PKI	PKI
HTTPS SITE	HTTP	HTTP/ HTTPS	HTTPS
HTTPS MP	HTTP	HTTP	HTTPS
HTTPS DP	HTTP	HTTP	HTTPS
Firma	NO	SI	SI
Cifrado	NO	NO	SI
SHA256	NO	SI	SI
Aprobación clientes	Automáticamente	Automáticamente	Manual
Verificación CRL	NO	NO	SI
Criterio de selección de certificado de cliente	NO	NO	SI (Atributos Subject o SAN)
Cuenta de acceso a la red	Cuenta de equipo cliente	Cuenta de equipo cliente	Cuenta dedicada de servicio
Notificaciones SMTP	SMTP	SMTP	SMTP / TLS
Conexión SUP a WSUS	HTTP	HTTP	HTTPS
App Catalog Service Point	HTTP	HTTP	HTTPS
App Catalog Website Point	HTTP	HTTP	HTTPS
Enrollment Proxy Point	HTTPS	HTTPS	HTTPS

Las comunicaciones entre los servidores que forman parte de la infraestructura de MS SCCM 2012 R2 son comunicaciones internas las cuales deben discurrir siempre por redes seguras, no obstante, es recomendable el empleo de comunicaciones basadas en HTTPS, siempre que la organización presente una infraestructura de PKI adecuada para su integración con MS SCCM 2012 R2.

El envío de notificaciones puede contener información confidencial de usuarios o equipos de la organización por lo que se recomienda el uso de SMTP/TLS siempre que la infraestructura lo permita.

En el caso de que en su infraestructura se disponga del rol de Enrollment Proxy Point el cual facilita la unión de equipos con sistema operativo diferente de Windows que encuentran fuera del dominio, se recomienda que la conexión siempre sea HTTPS, además de contar con un certificado de equipo para la unión con el sitio.

10.1 MARCO OPERACIONAL

El marco operacional está compuesto por las medidas de seguridad a implementar en los sistemas para tratar de proteger la operación del sistema como conjunto integral de componentes para un fin.

10.1.1 CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que, bien preparatorias o ejecutivas, están 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 establecerá 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 comodidad de uso y la protección del sistema, de tal forma que la seguridad se irá incrementando, en base al nivel exigido. Así, en el nivel bajo se primará la comodidad y en los niveles altos se primará la protección.

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

MS SCCM 2012 R2, incluye una amplia variedad de permisos predefinidos basados en cuentas de grupos de usuarios para la concesión de los accesos a los diferentes roles.

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.

Un rol define el conjunto de tareas que un administrador o un usuario pueden realizar, por lo que se deberá asignar los roles en función de las tareas a desempeñar por el usuario teniendo en consideración siempre los principios de mínima funcionalidad y mínimo privilegio, evitando con ello poder dar permisos a determinados usuarios a realizar acciones no autorizadas.

Cuando un rol se asigna a un administrador o usuario, a dicha persona se conceden los permisos que proporciona el rol en cuestión.

Así mismo es importante la creación de grupos de seguridad a la hora de conceder permisos sobre un rol determinado, SCCM se integra con Active Directory para facilitar dicha tarea, lo que permitirá una gestión más global y sencilla evitando modificar los permisos individuales de cada usuario para asignar o quitar permisos.

En MS SCCM 2012 R2 existen grupos de roles predeterminados las cuales establecen las diferentes funciones a realizar en la administración de la consola de SCCM.

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

Este proceso requiere la consolidación de los derechos de acceso, de tal forma que debe tener en consideración:

a) Aplicación del mínimo privilegio. Los privilegios de cada inicio de sesión 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.

MS SCCM 2012 R2 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 visualizar contenido que no es requerido para las funciones que desempeña.

MS SCCM 2012 R2 permite limitar el acceso de determinados equipos a la administración de SCCM aplicando con ello, el principio de mínima funcionalidad, evitando conexiones no permitidas o limitando las conexiones a los equipos autorizados.

10.1.1.3 OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

MS SCCM 2012 R2 usará siempre la autenticación basada en usuarios de Active Directory prevaleciendo la configuración de seguridad establecida mediante las políticas de seguridad según se establece en el Esquema Nacional de Seguridad.

Se permitirá la conexión entre los diferentes servidores con los roles establecidos, así como los propios equipos clientes, mediante HTTP o HTTPS, siendo la conexión HTTPS la más recomendada, debido al cifrado, integridad y autenticación de los datos que se transmiten usando el protocolo HTTPS.

Para el nivel alto del ENS se recomienda realizar la comunicación de los equipos clientes con los servidores o la comunicación de los propios servidores entre sí mediante el uso de certificados aumentando con ello la seguridad en la comunicación y evitando posibles suplantaciones de identidad.

El sistema de autenticación se puede realizar tecnológicamente mediante múltiples mecanismos, siendo el del empleo de usuario y contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes generalidades estos serán:

a) Para el nivel bajo se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, dispositivos físicos (en inglés "Tokens"), sistemas de biometría o certificados digitales entre otros.

b) Para el nivel medio se desaconseja el empleo de passwords o claves concertadas, siendo recomendable el uso de sistemas físicos (Tokens), biométricos o certificados digitales.

c) Para el nivel alto, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige para ello el uso de dispositivos físicos o de biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-807 de criptología de empleo en el ENS.

Conforme a las necesidades establecidas por el Esquema Nacional de Seguridad se deberá tener también en consideración lo establecido en la guía CCN-STIC-804 para los mecanismos de autenticación y que se encuentra recogido en el punto 4.2.5.

10.1.1.4 OP. ACC. 7. ACCESO REMOTO

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

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

MS SCCM 2012 R2 proporciona mecanismos avanzados de seguridad para proteger las conexiones procedentes de fuentes no confiables como es Internet. Dichos mecanismos implementan diferentes modelos de autenticación por certificados, dependiendo de si los extremos forman parte del mismo dominio, forman parte de dominios diferente o equipos clientes que no están unidos a ningún dominio.

La seguridad de nivel de transporte (TLS), es un protocolo estándar que se usa para proporcionar comunicaciones seguras en Internet o en intranets. Permitiendo a los clientes autenticar servidores y, opcionalmente, a los servidores autenticar clientes. También proporciona un canal seguro ya que cifra las comunicaciones. TLS 1.2 es la versión más reciente del protocolo Nivel de sockets seguros (SSL).

MS SCCM 2012 R2 hace uso del rol de IIS 8.5 el cual 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.

10.1.2 EXPLOTACIÓN

Se tienen en consideración todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define, 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.

10.1.2.1 OP. EXP. 1. INVENTARIO DE ACTIVOS

MS SCCM 2012 R2 proporciona una herramienta para mantener el inventario de activos de la organización, así como un control sobre el software y hardware tanto de los equipos cliente, como de los servidores.

MS SCCM 2012 R2 se integra con otras soluciones como Microsoft Intune para gestionar y administrar el inventario de dispositivos móviles conectados en el MDM.

Es posible realizar inventarios personalizados, realizando consultas a medida, que permiten la recopilación de información requerida adaptándose a las necesidades de su organización.

Los datos de inventario son accesibles a través de la consola de MS SCCM 2012 R2 o mediante informes que muestran detalles específicos de los dispositivos inventariados.

10.1.2.2 OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Se considera que MS SCCM 2012 R2 debe configurarse previamente a su entrada en producción teniendo en consideración las siguientes directrices:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

En el ENS se considera indispensable que el sistema no proporcione funcionalidades gratuitas y únicamente presente las estrictamente necesarias para desempeñar la función asignada. Por lo que se eliminarán o desactivarán, mediante el control de la instalación y configuración, todas aquellas funciones que no sean necesarias e incluso aquellas que sean inadecuadas al fin de preservar el principio de mínima funcionalidad establecidas en el ENS.

Para el cumplimiento del ENS, se establecen las diferentes plantillas de seguridad las cuales 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 deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición, 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.

10.1.2.3 OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN

En el ENS se mantiene de forma continua el principio de funcionalidad mínima, ofreciendo el MS SCCM 2012 R2 únicamente los requerimientos necesarios para su correcto funcionamiento, así como los roles necesarios establecidos previamente para ofrecer el servicio deseado.

Se realizará una gestión activa de la configuración permitiendo que el sistema se adapte a las nuevas necesidades de la organización manteniendo en todo momento la regla de seguridad por defecto.

El ENS establece la necesidad de que el sistema reaccione a posibles vulnerabilidades o ante posibles incidentes.

10.1.2.4 OP. EXP. 4 MANTENIMIENTO

Para mantener el equipamiento físico y lógico se deberán atender las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas. Se realizará un seguimiento continuo para garantizar la seguridad de los sistemas. Para ello deberá existir un procedimiento que permita analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación y no de la actualización.

Se tendrán en consideración las especificaciones del fabricante en lo relativo a instalación y mantenimiento de MS SCCM 2012 R2.

Para el cumplimiento del ENS se instalarán las actualizaciones acumulativas publicadas por el fabricante de MS SCCM 2012 R2 las cuales solventan vulnerabilidades detectadas.

10.1.2.5 OP. EXP. 5 GESTIÓN DE CAMBIOS

Tal y como se establece en el ENS se llevará un control continuo de cambios del producto de MS SCCM 2012 R2, así como de los cambios realizados en los equipos clientes gestionados por SCCM.

Se ha de tener en consideración que todos los cambios realizados, deberán ser probados previamente en un entorno de preproducción para comprobar que funcionan correctamente antes de implementar cambios en los equipos de producción.

Una vez que se han comprobado a aplicar en un entorno de preproducción se ha de planificar la intervención en el entorno de producción teniendo en consideración que la aplicación de los cambios afecte lo menos posible en las prestaciones de los servicios afectados.

Con la realización de un análisis de riesgos se podrá predeterminar si los cambios son relevantes para la seguridad del sistema, por lo que aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

10.1.2.6 OP. EXP. 6. PROTECCION FRENTE A CODIGO DAÑINO

MS SCCM 2012 R2 cuenta con la funcionalidad de Endpoint Protection que proporciona la capacidad de administrar las directivas de protección frente a código dañino y la seguridad del Firewall de Windows en los equipos cliente.

Endpoint Protection permite configurar alertas para enviar notificaciones cuando se producen determinados eventos como la infección de código dañino en un equipo, para con ello, prevenir y realizar las acciones necesarias para evitar la infección y difusión por los equipos clientes de la organización.

La directiva frente a código dañino predeterminada controla la configuración para especificar cómo Endpoint Protection protege de código dañino y otras amenazas a toda la organización.

A partir de la versión 1606 de MS SCCM 2012 R2, Endpoint Protection puede ayudar a administrar y supervisar la protección contra amenazas avanzadas de Windows Defender (ATP).

La protección contra amenazas avanzadas de Windows Defender, es un servicio que proporciona apoyo a las organizaciones para detectar ataques avanzados en sus redes, investigarlos y responder a ellos.

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

10.1.2.7 OP. EXP. 7. GESTIÓN DE INCIDENTES

MS SCCM 2012 R2 proporciona la herramienta de configuración de cumplimiento que facilita la gestión y administración de la configuración de seguridad de los equipos cliente de la organización.

La configuración de cumplimiento le ayudara a evaluar el cumplimiento de muchas configuraciones por ejemplo si algún equipo cliente tiene un software no autorizado o incluso si un equipo cliente no tiene una actualización de software critica.

Junto con la configuración de cumplimiento y el inventariado de hardware es posible investigar las causas de los incidentes y analizar las consecuencias de seguridad que dicho incidente puede ocasionar, así como prevenir posibles incidentes futuros.

Es posible comparar la configuración de los equipos cliente de la organización, con el fin de comprobar que cumplan con los requisitos mínimos de seguridad establecidos y la instalación de todos los paquetes de seguridad previamente establecidos por la organización.

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

Aplicable en los niveles bajo, medio y alto de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

a) Quién realiza la actividad, cuándo la realiza y sobre qué.
b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.
c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.
d) La determinación de las actividades y con qué nivel de detalles, se establecerá en base al análisis de riesgos que se haya realizado sobre el sistema.

El nivel alto requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

MS SCCM 2012 R2 implementa mecanismos para la auditoría de los sistemas e infraestructuras. De forma predeterminada, los datos son almacenados localmente, pero se recomienda que los datos sean almacenados en una ubicación diferente a la de la instalación del servicio.

Se establece, por lo tanto, para un nivel bajo de seguridad se activarán los registros de actividad en los servidores, para un nivel medio se revisarán informalmente los registros de actividad buscando patrones anormales y para un nivel alto se dispondrá de un sistema automático de recolección de registros y correlación de datos, es decir, una consola de seguridad centralizada.

En los niveles de seguridad medio y alto del marco operacional del ENS, la trazabilidad de las acciones de los usuarios ha de estar garantizada.

En MS SCCM 2012 R2 se registrará la actividad de los equipos cliente para indicar quien realiza la actividad, cuando la realiza y sobre qué información para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

También se contempla el registro de la actividad de los operadores y administradores en cuanto al acceso, configuración y mantenimiento del MS SCCM 2012 R2.

Para los niveles medio y alto del ENS, es necesario el registro tanto las actividades realizadas con éxito y los intentos fallidos de realizar una acción.

10.1.2.9 OP. EXP. 9. REGISTRO DE LA GESTION DE INCIDENTES

Para los niveles medio y alto de seguridad del ENS se han de registrar todas las actuaciones relacionadas con la gestión de todos incidentes, de tal forma que, se registrara el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

Se registrarán todas aquellas evidencias que posteriormente puedan sustentar una demanda judicial o hacer frente a ella, o cuando el incidente en cuestión pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

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

En el nivel alto del ENS se deberán implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:

a) Determinar el período de retención de los registros.

b) Asegurar fecha y hora del registro de la actividad

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

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

En MS SCCM 2012 R2 existen grupos de roles predeterminados orientados a la protección de la información de los registros de actividad, por lo que, únicamente los usuarios establecidos por la organización tendrán acceso a la información de los registros de actividad.

Se han de definir los periodos de retención de los registros y su almacenamiento para su recuperación, así como asegurar que dichos registros no podrán ser modificados ni eliminados por personal no autorizado.

10.2 MEDIDAS DE PROTECCIÓN

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

Solo estas últimas se tendrán en cuenta para su implementación en la presente guía y de ellas solo un número limitado son de aplicación sobre las funcionalidades del propio producto MS SCCM 2012 R2.

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

10.2.1 PROTECCIÓN DE LAS COMUNICACIONES

Para alcanzar un nivel adecuado de seguridad en las comunicaciones en el entorno de su organización es necesario involucrar tanto a los administradores de la organización, como a los desarrolladores. Consiguiendo con la colaboración de ambos grupos proporcionar un entorno seguro completo.

La formación de seguridad debe centrarse en proporcionar un conocimiento adecuado a administradores y desarrolladores respecto a las vulnerabilidades, las amenazas de seguridad, los diferentes tipos de ataques existentes y los mecanismos de defensa asociados, preferiblemente mediante ejemplos prácticos.

El Real Decreto 3/2010 de 8 de enero de desarrollo del Esquema Nacional de Seguridad, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

10.2.1.1 MP. COM. 2. PROTECCIÓN DE LA CONFIDENCIALIDAD

En aquellos sistemas en que sea de aplicación el nivel medio de seguridad del ENS, tendrán la necesidad de implementar redes virtuales privadas cuando su comunicación se realice a través de redes fuera de la organización o del propio dominio de la seguridad.

Así mismo se emplearán algoritmos de seguridad acreditados por el Centro Criptológico Nacional con el fin de proteger la confidencialidad de las comunicaciones.

Para el nivel alto del ENS se hará uso, preferentemente de dispositivos hardware para el establecimiento de la comunicación y la utilización de la red privada virtual con el fin de aplicar un nivel de seguridad elevado.

Además, se emplearán productos certificados según lo establecido en el apartado “OP.PL 5 Componentes certificados” del ENS.

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

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

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

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

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

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

Se utilizarán los mecanismos de autenticación establecidos anteriormente expuestos en este documento en el apartado “10.1.1.3 OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN”.

En aquellos sistemas en que sea de aplicación el nivel medio de seguridad del ENS, es necesario implementar redes virtuales privadas cuando la comunicación se realice a través de redes fuera de la organización o del propio dominio de la seguridad. Para ello, se deberán tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

Para aquellos entornos con sistemas o información catalogados como de nivel alto, es valorable positivamente el empleo de dispositivos hardware para el establecimiento y utilización de redes virtuales privadas en las comunicaciones, frente a soluciones de tipo software. Se deberá tener en consideración los productos que se encuentran certificados y acreditados.

Se deberán aplicar las últimas actualizaciones de seguridad en cada uno de los elementos software que forman parte de la plataforma de MS SCCM 2012 R2, software de los dispositivos de red, firewalls y sistema operativo de los servidores.

10.2.1.3 MP. COM. 9. MEDIOS ALTERNATIVOS

En el nivel alto de seguridad del ENS se establece que se deberá garantizar la existencia y disponibilidad de medios alternativos en caso de que fallen los medios habituales por ello en MS SCCM 2012 R2 es posible redundar los roles de sistema de sitio importantes.

Los equipos cliente de MS SCCM 2012 R2, si no pueden conectarse con el sitio, almacenan en caché los datos que desean enviar hasta que pueden ponerse en contacto con el sitio de nuevo.

Además, los equipos cliente siguen funcionando con las últimas programaciones conocidas y la información almacenada en caché hasta que pueden conectarse nuevamente con el sitio y recibir nuevas directivas en caso de existir actualizaciones de las mismas.

Los equipos clientes pueden ejecutar inventario, implementaciones de software y acciones programadas similares independientemente del contacto directo con los servidores de sistema de sitio.

Es posible hacer uso de un clúster de SQL Server con la integración de Clúster de conmutación por error integrada en SQL Server para alojar y dar continuidad la base de datos del sitio.

10.2.2 PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN

En el ENS se establecen una serie de pautas a seguir en cuanto a la protección de los soportes que contienen información sensible por lo que se deben etiquetar sin revelar su contenido, además de aplicar mecanismos criptográficos para garantizar la confidencialidad e integridad de la información.

10.2.2.1 MP. SI. 5. BORRADO Y DESTRUCCION

Las medidas de borrado y destrucción de información se aplicarán a todo tipo de equipos susceptibles de almacenar información.

MS SCCM 2012 R2 no permite eliminar una base de datos directamente por lo que será necesario iniciar sesión en el servidor que aloje la base de datos de sitio. Se debe tener en consideración que el usuario que realiza la acción debe tener los permisos adecuados y una vez desvinculado se deberá eliminar físicamente la carpeta contenedora de la información, y si desea eliminar el soporte de dicha información deberá seguir el procedimiento para el borrado y destrucción de soportes físicos que establece el ENS.

Nota: Si desea obtener más información sobre el borrado de bases de datos de Microsoft SQL Server puede visitar el sitio web: https://technet.microsoft.com/es-es/library/ms177419(v=sql.110).aspx

10.2.3 PROTECCIÓN DE LA INFORMACIÓN

10.2.3.1 MP. INFO. 1. DATOS DE CARÁCTER PERSONAL

MS SCCM 2012 R2 tratara la protección de los datos de carácter personal según lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.

La Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos.

10.2.3.2 MP. INFO. 9. COPIAS DE SEGURIDAD (BACKUP)

MS SCCM 2012 R2 ofrece una funcionalidad propia de copias de seguridad, enfocada en evitar la pérdida de datos, permitiendo recuperar sitios y jerarquías con la mínima perdida de datos posibles.

Las copias de seguridad poseerán el mismo nivel de seguridad que los datos originales en cuanto a la integridad, confidencialidad, autenticidad y trazabilidad.

El sistema de copias de seguridad debe ser capaz de garantizar el respaldo de la información de trabajo de la organización, datos de configuración, servicios, aplicaciones, equipos además de implementar las claves necesarias para preservar la seguridad de la confidencialidad de la información.

Se han de contemplar también las copias de las bases de datos de sitios alojadas en MS SQL Server que puede utilizar su propio sistema de copias de seguridad de bases de datos o usar uno de terceros.

10.2.4 PROTECCIÓN DE LOS SERVICIOS

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

MS SCCM 2012 R2 utiliza IIS por lo que todos los sistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que son propias de este entorno como:

a) Ataques directos, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno.

b) Ataques indirectos, dónde cualquiera de los elementos es empleado como herramienta en el ataque.

c) Ataques de denegación de servicio (DoS). Las arquitecturas Web están basadas en tecnologías TCP/IP y por tanto son vulnerables a los ataques de DoS comunes en TCP/IP. Es necesario disponer de contramedidas técnicas y procedimientos de actuación frente a este tipo de ataques.

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

10.2.4.2 MP. S. 9. MEDIOS ALTERNATIVOS

En el nivel alto de seguridad del ENS se establece que se deberán proporcionar medios alternativos para proveer los servicios en caso de fallo de los medios principales, con las mismas garantías de seguridad. La capacidad de MS SCCM 2012 R2 de redundar los roles de sistema de sitio asociados a los servicios activos, permite la tolerancia a fallos requerida.

En los equipos cliente de MS SCCM 2012 R2, existen mecanismos para almacenar los datos hasta la conexión con el servidor. Esto se aplica a las acciones programadas como inventario, instalaciones de software, etc. Que almacenan la información en cache hasta la siguiente comunicación con el sitio y en caso de existir, la recepción de nuevas instrucciones y directivas.

11. RESUMEN Y APLICACIÓN DE MEDIDAS DE MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2

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-800 o bien la aplicación de políticas de seguridad a nivel de dominio o bien localmente.

Control	Medida	Mecanismo de aplicación
OP. ACC. 3	Gestión de derechos de acceso	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. ACC. 5	Mecanismos de autenticación	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 1	Control del inventario de activos	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. EXP. 3	Control de la gestión de la configuración	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 4	Control de cambios y actualizaciones del fabricante.	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 5	Gestión del control de cambios	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 6	Protección frente a código dañino	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 7	Gestión del control de incidentes	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 9	Registro de la gestión de incidentes	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. COM. 2	Protección de la confidencialidad de los datos	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. COM. 3	Protección de la autenticación y de la integridad	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. COM. 9	Medios alternativos	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. SI. 5	Borrado y destrucción de la información	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. INFO. 1	Control y gestión de los datos de carácter personal establecidos en la LOPD	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. INFO. 9	Copia de seguridad	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
MP. S. 2	Protección de servicios y aplicaciones web	Implementación guía CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2. Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.
MP. S. 9	Medios alternativos	Revisión e implementación guía CCN-STIC-875, adaptándolos a la organización.

ANEXO A. CONFIGURACION SEGURA DE MS SCCM 2012 R2 EN EL ENS PARA EL NIVEL BAJO

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de System Center Configuration Manager 2012 R2 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.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para System Center Configuration Manager 2012 R2, 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.

ANEXO A.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL BAJO DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas, a realizar una implementación de seguridad en escenarios donde se tenga que reforzar la seguridad de Microsoft SCCM 2012 R2 sobre MS Windows Server 2012 R2, con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad. Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad, según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran al nivel bajo, 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, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

MS SCCM 2012 R2 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar MS SCCM 2012 R2, en caso de necesitar información sobre los requisitos previos de instalación de MS SCCM 2012 R2, visite el siguiente sitio web:

https://docs.microsoft.com/es-es/sccm/core/plan-design/configs/site-and-site-system-prerequisites

En la presente guía se van a reforzar la seguridad de los principales roles de sitio de MS SCCM 2012 R2.

a) Sistema de sitio
b) Servidor del sitio
c) Punto de distribución

d) Punto de administración

e) Punto de actualización de software

f) Punto de servicios de informes

g) Servidor base de datos del sitio

Nota: Si instala MS SCCM 2012 R2 por primera vez con la guía 870A aplicada previamente debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell, la cual se encuentra deshabilitada por GPO.

Para la implementación de la presente guía se han generado unas plantillas de seguridad que deberán ser aplicada en las unidades organizativas correspondientes donde se encuentren alojados los servidores que vayan a formar parte de MS System Center Configuration Manager 2012 R2.

Hay que tener en consideración que el objetivo de implementación de estos tipos de servidores puede ser para un uso de múltiples roles, por ejemplo, como punto de distribución, punto de actualización de software o punto de servicios de informes., por lo que no existirá una ubicación específica dentro del directorio activo, aunque en la presente guía se intentan agrupar en las unidades organizativas “Servidores SCCM” y “Servidores SQL” para una mejor gestión.

Los detalles de las siguientes plantillas se encuentran exportados en sus ficheros correspondientes con formato HTML en la carpeta “Scripts\Nivel Bajo” que se acompaña junto a este documento.

a) CCN-STIC-875 ENS Incremental Punto de actualización de software bajo

b) CCN-STIC-875 ENS Incremental Punto de administración bajo

c) CCN-STIC-875 ENS Incremental Punto de distribución bajo

d) CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo

e) CCN-STIC-875 ENS Incremental Servidor del sitio bajo

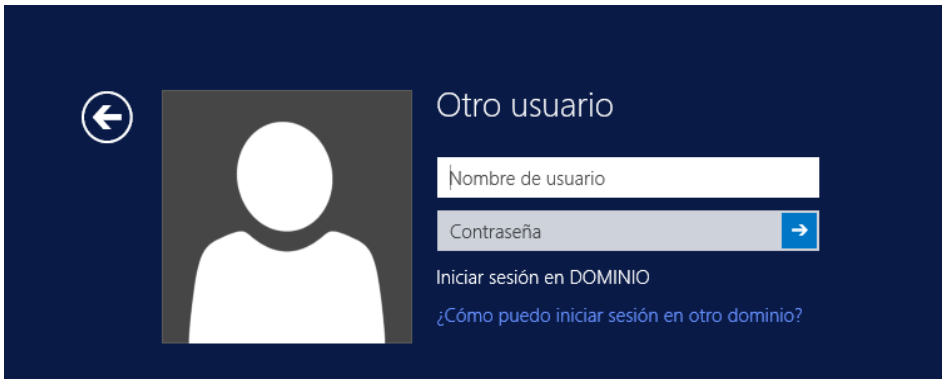
f) CCN-STIC-875 ENS Incremental Punto de -SQL bajo

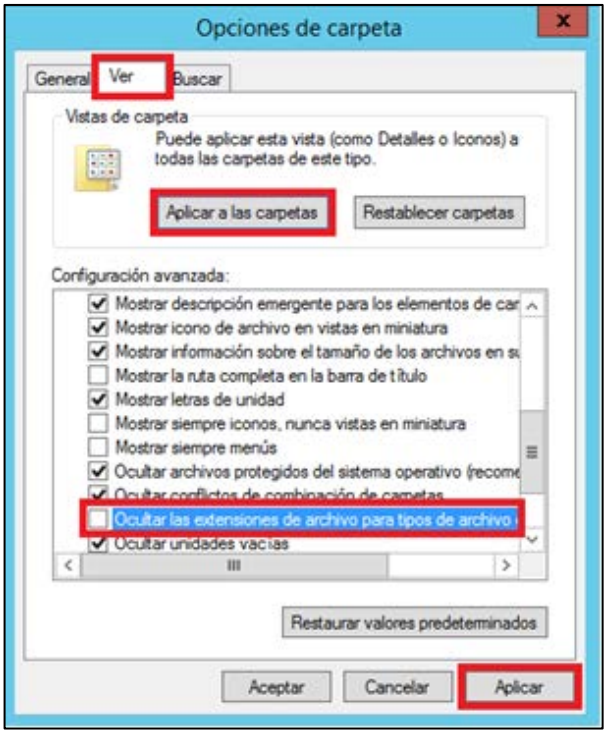
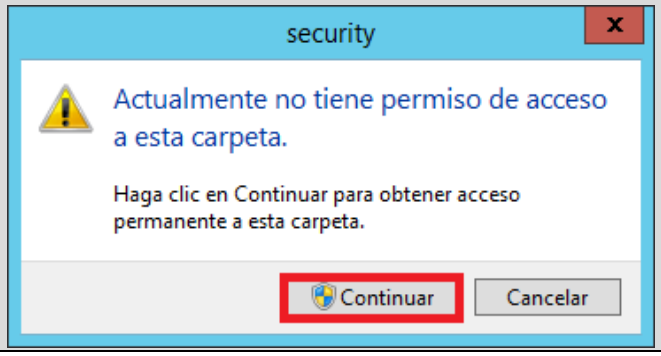
1. REFUERZO DE SEGURIDAD DEL SERVIDOR SQL Y ROL DE SERVIDOR BASE DE DATOS DEL SITIO

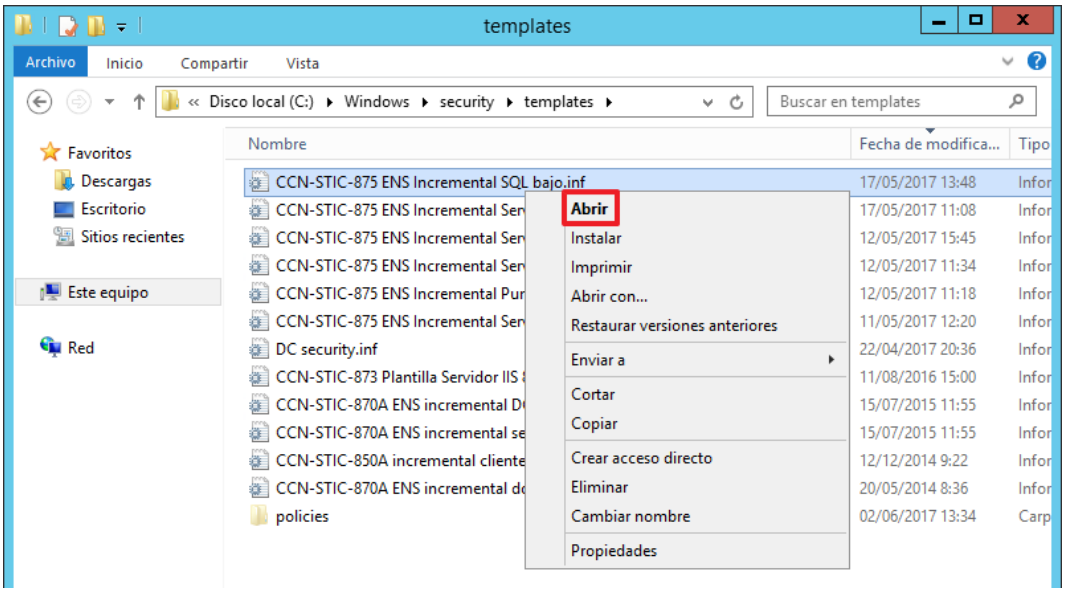
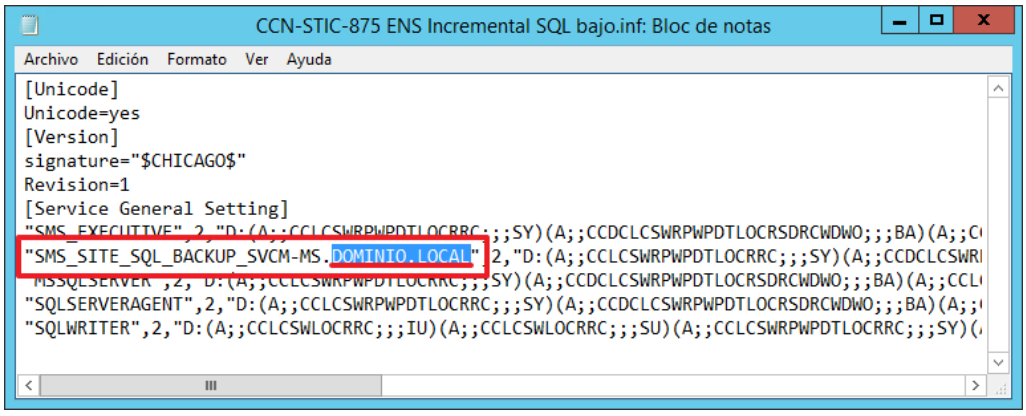
Es necesario dar permisos de inicio de sesión como servicio a los usuarios necesarios para iniciar los servicios de SQL requeridos para el correcto funcionamiento del producto MS SQL server y MS SCCM 2012 R2.

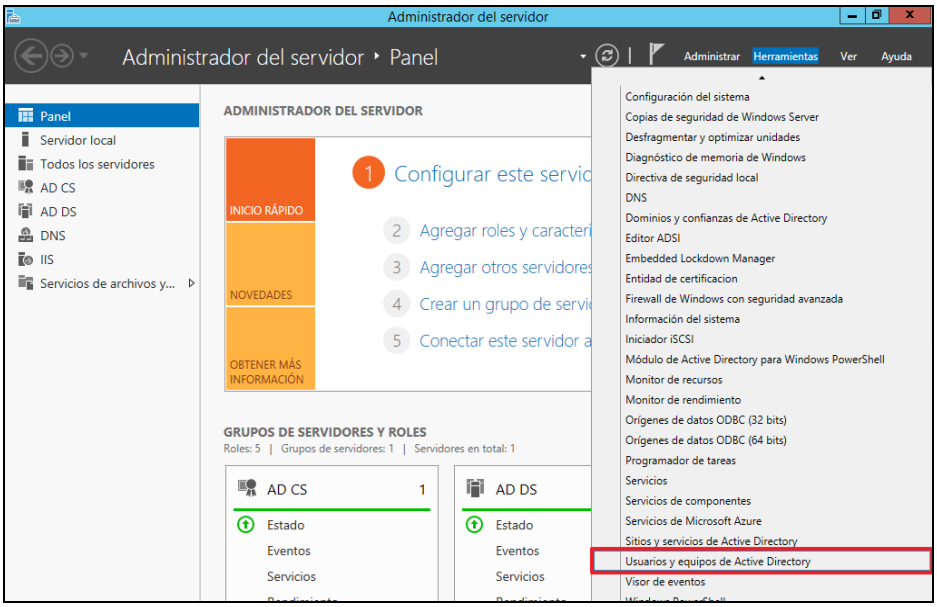
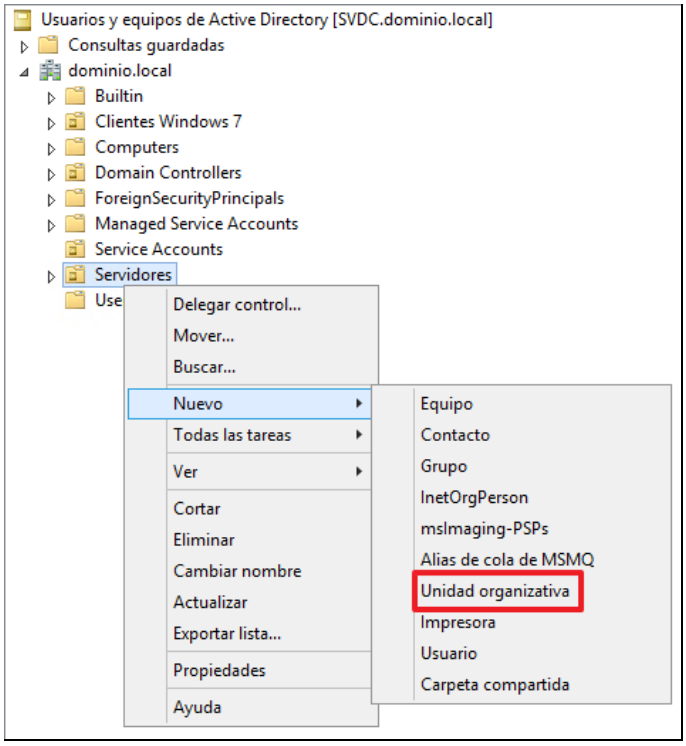
Se ha de tener en consideración que el servidor que aloja el producto de MS SQL Server también contiene Internet Information Services 8.5 para el rol de servicios de informes de SCCM por lo que será necesario aplicar previamente la guía de seguridad “CCN-STIC-873 ENS Incremental IIS 8.5”.

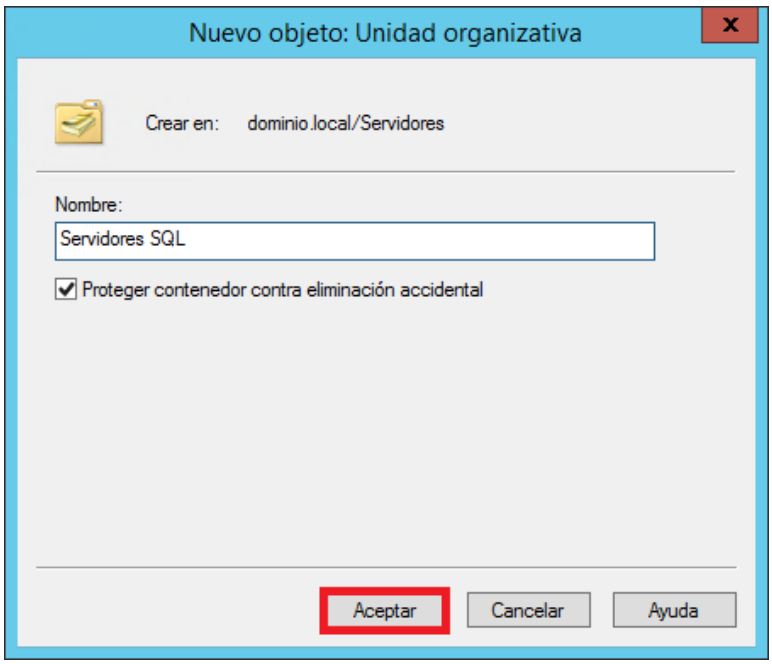
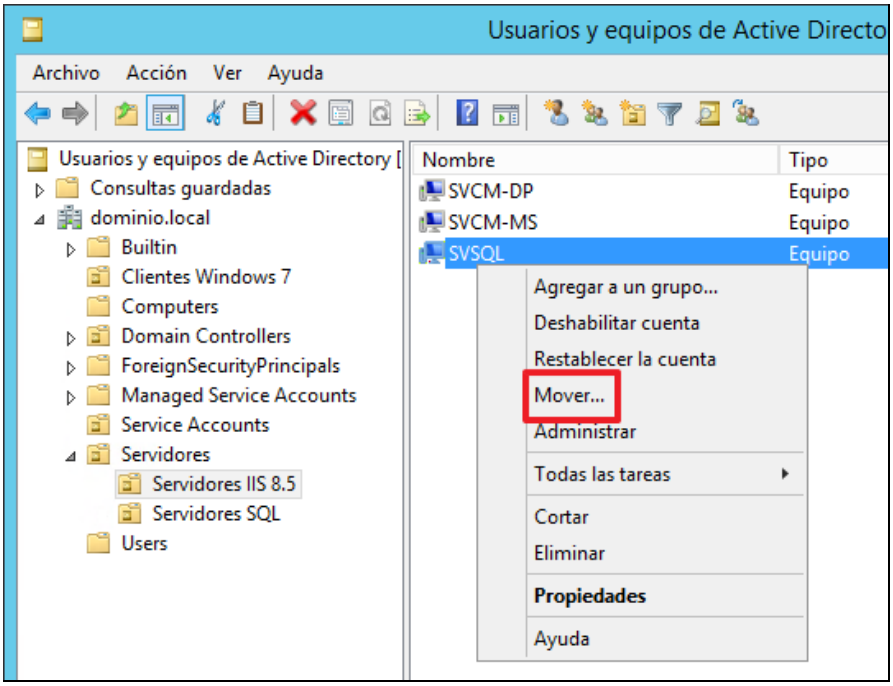
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

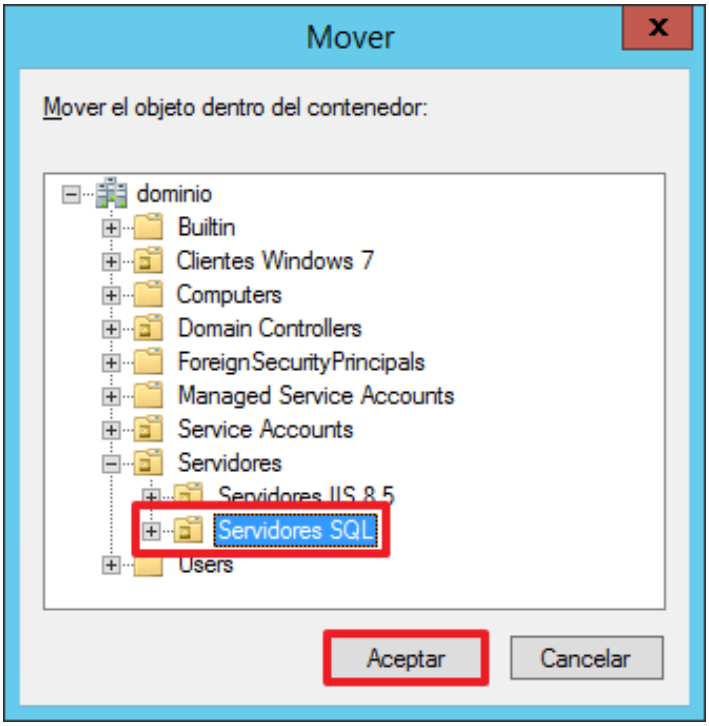
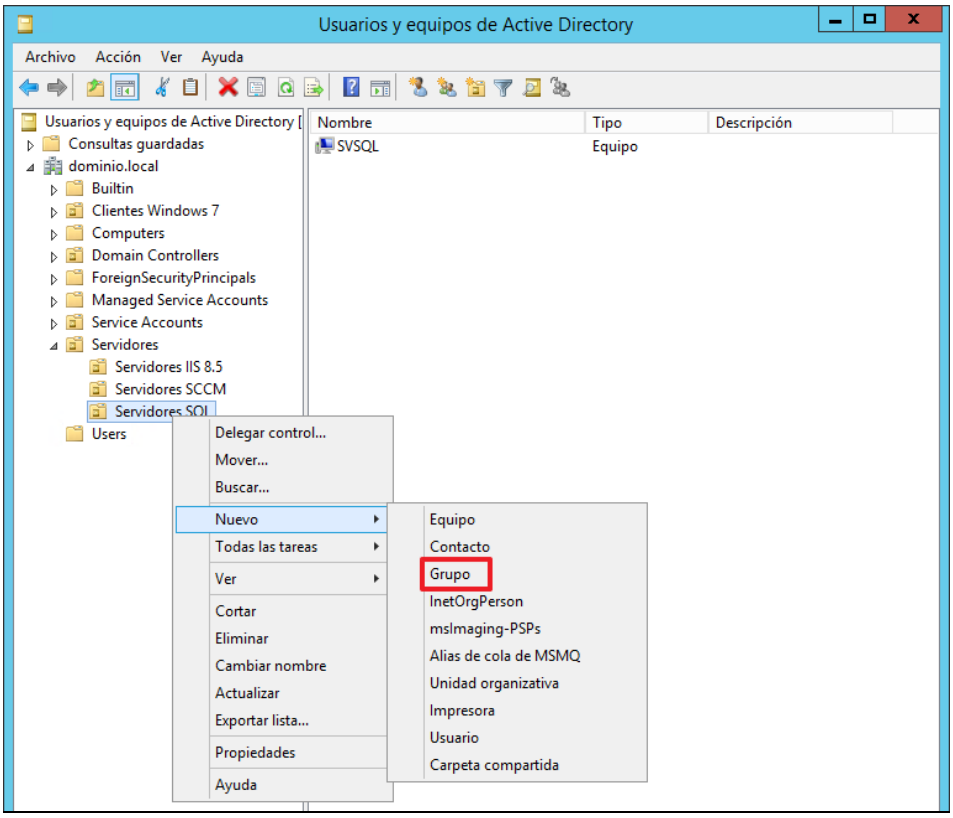
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.

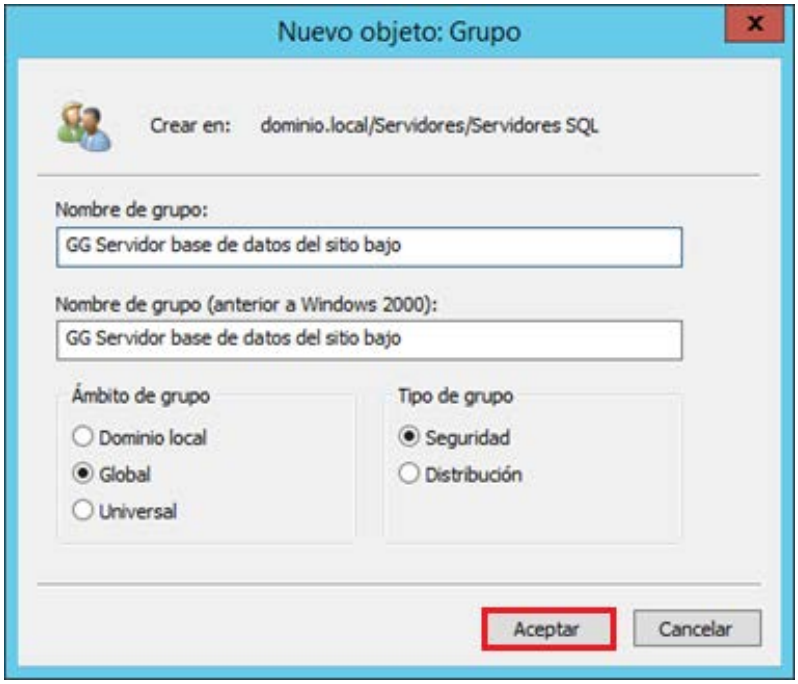
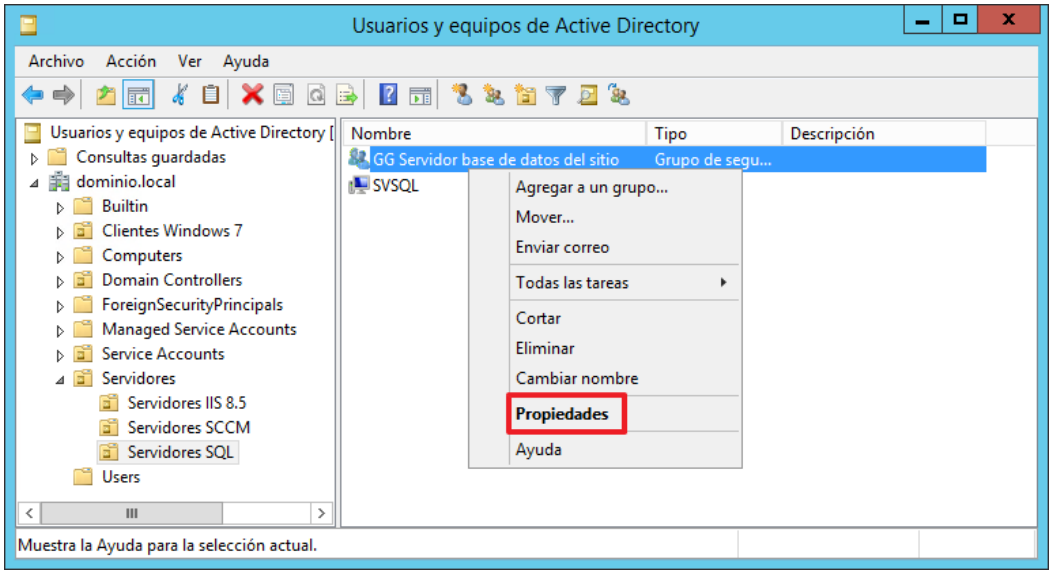
Paso	Descripción
5.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Copie el fichero “CCN-STIC-875 ENS Incremental SQL bajo.inf” que se encuentra en “C:\Scripts\Nivel Bajo” al directorio “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 

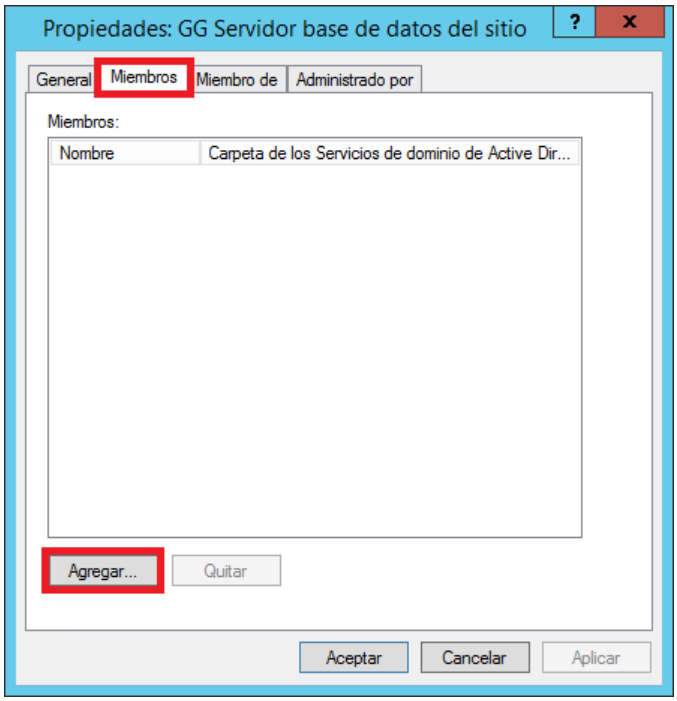
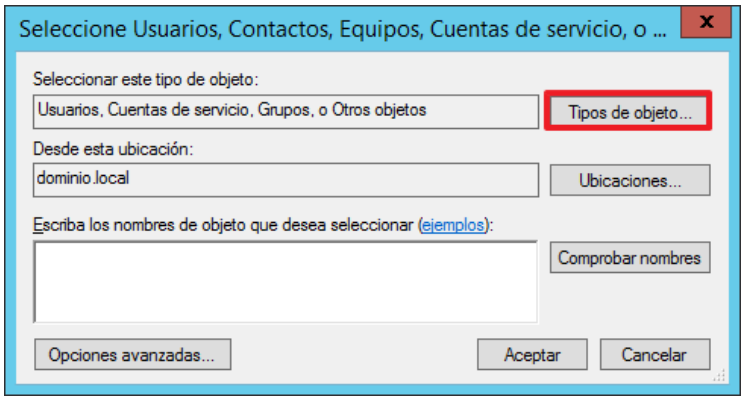
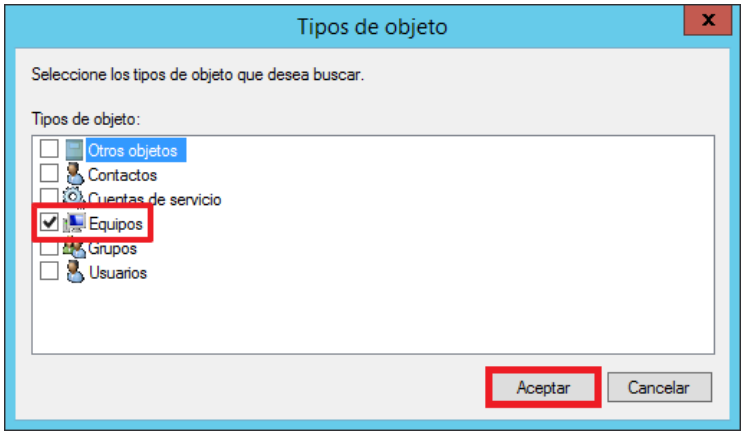
Paso	Descripción
7.	Pulse con el botón derecho sobre el fichero y seleccione la opción “Abrir” del menú contextual. 
8.	A continuación, deberá modificar el fichero para adaptarlo a su organización, para ello localice el servicio “SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL” y modifique el nombre del servicio cambiando el texto “DOMINIO.LOCAL” por el nombre de dominio de su organización.  **Nota:** Si no modifica este fichero el servicio “SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL”, no se reforzará la seguridad según los parámetros establecidos en el documento.
9.	Guarde los cambios realizados y cierre el documento.

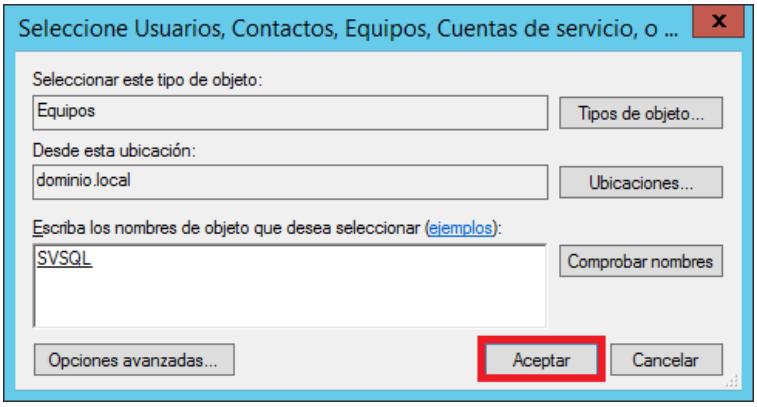
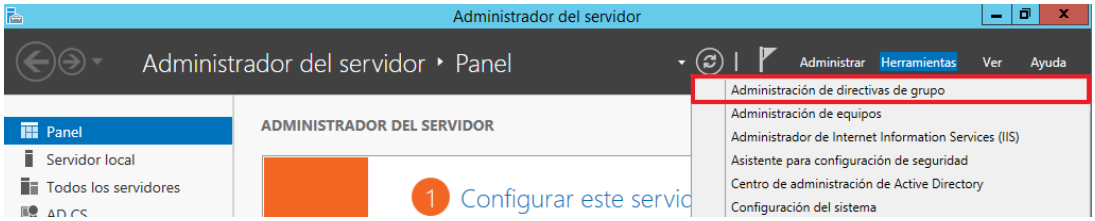
Paso	Descripción
10.	Inicie la herramienta “usuarios y equipos de Active directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
11.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 

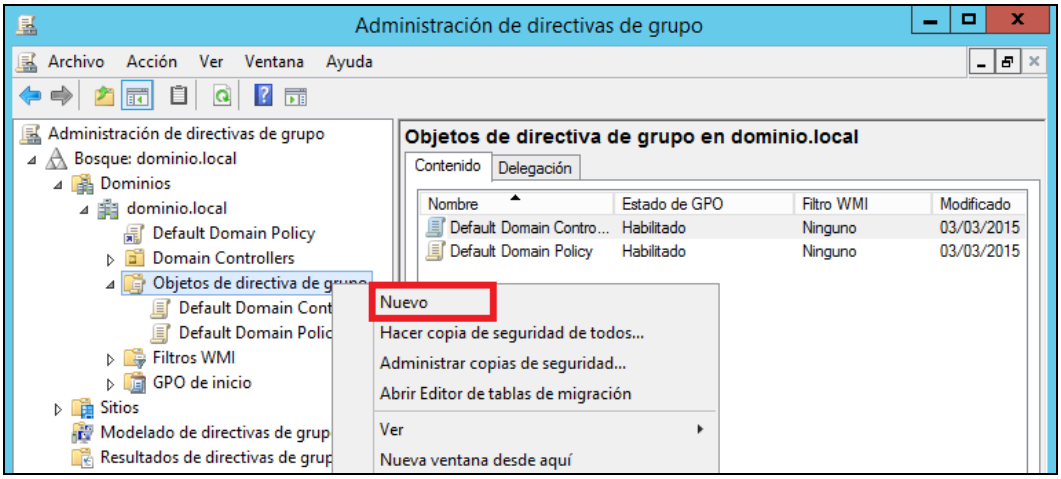
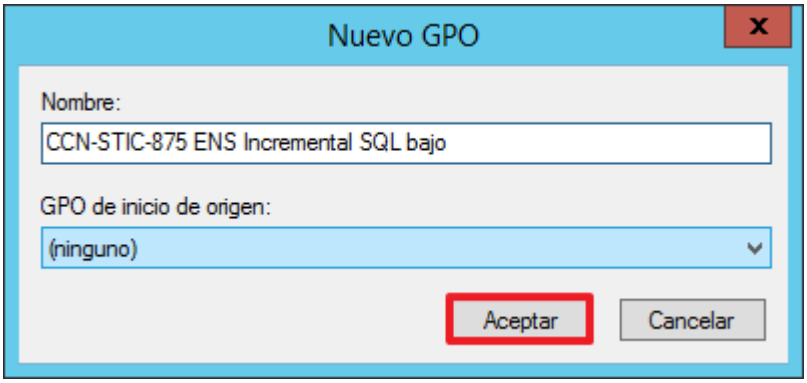
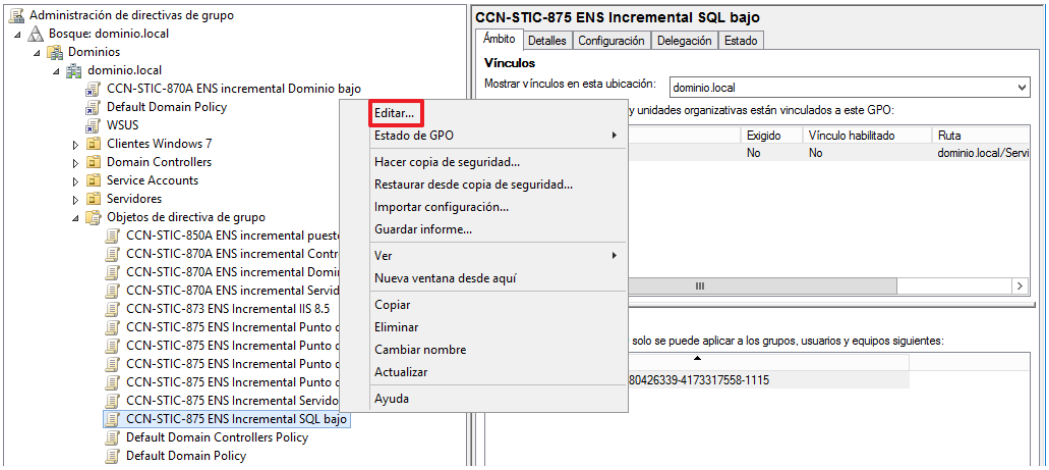
Paso	Descripción
12.	En la consola, cree una unidad organizativa denominada “Servidores SQL” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen. 
13.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores SQL a la unidad organizativa “Servidores SQL”. Para ello, deberá localizar los servidores y hacer clic con el botón derecho sobre el servidor que desee ubicar en la nueva unidad organizativa y marcar en “mover” del menú contextual. 

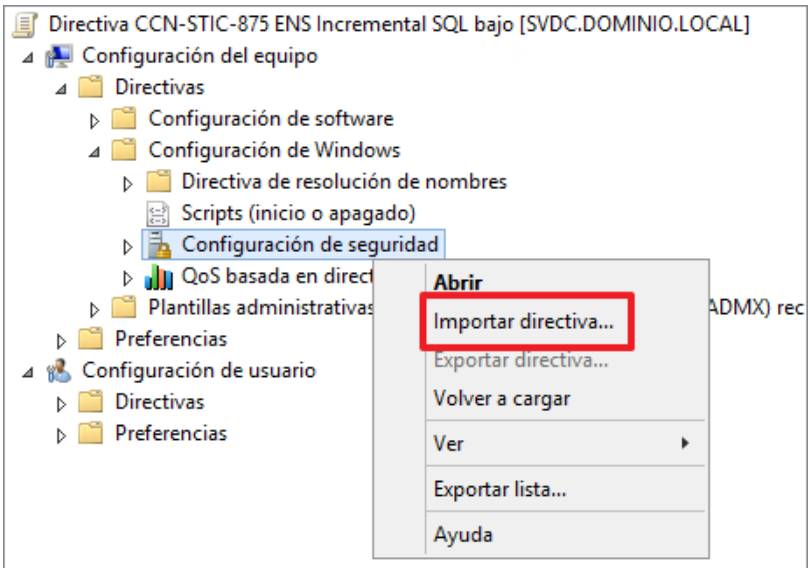
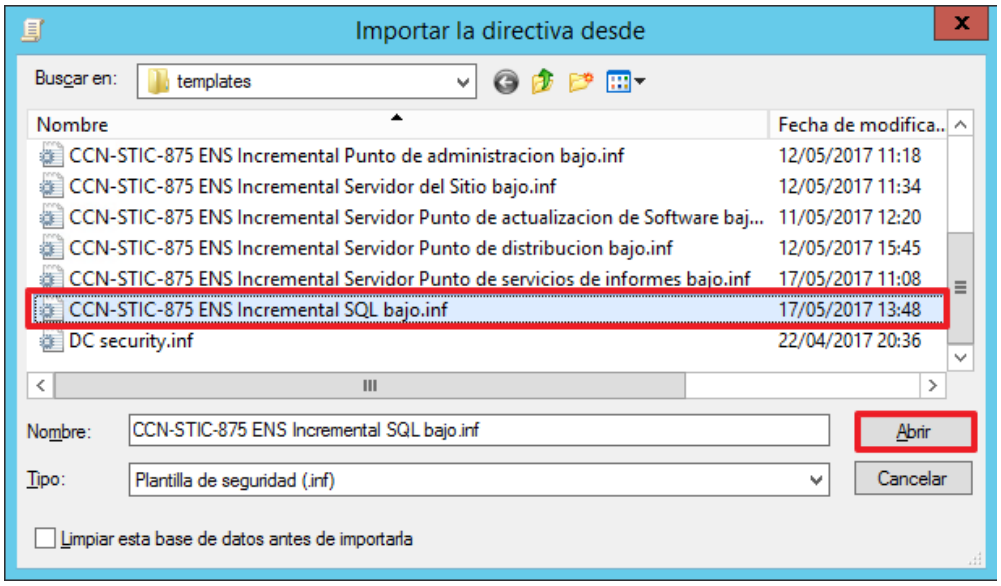
Paso	Descripción
14.	En el árbol de contenedores, seleccione la unidad organizativa “Servidores SQL” y “Aceptar”. 
15.	En el siguiente paso, seleccione la unidad organizativa “Servidores SQL”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 

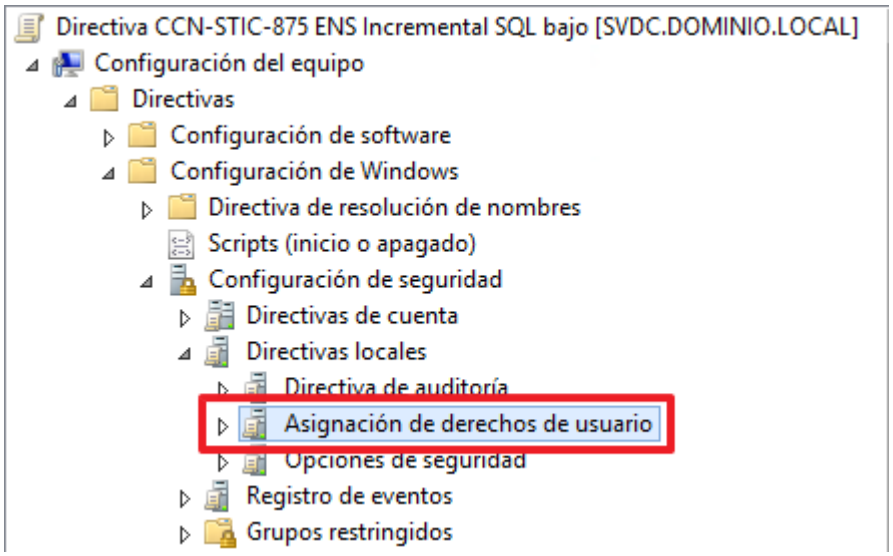
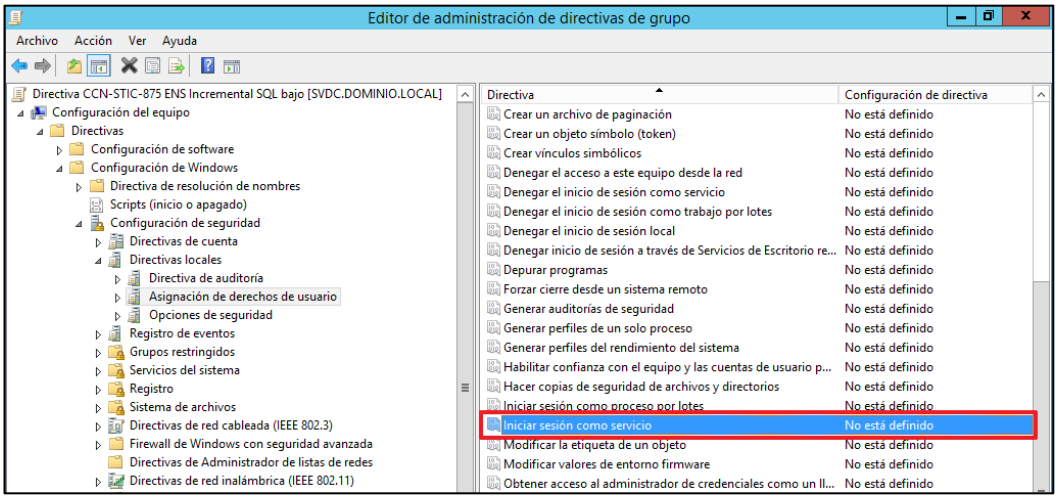
Paso	Descripción
16.	Escriba el nombre “GG Servidor base de datos del sitio bajo” y pulse “Aceptar”. 
17.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 

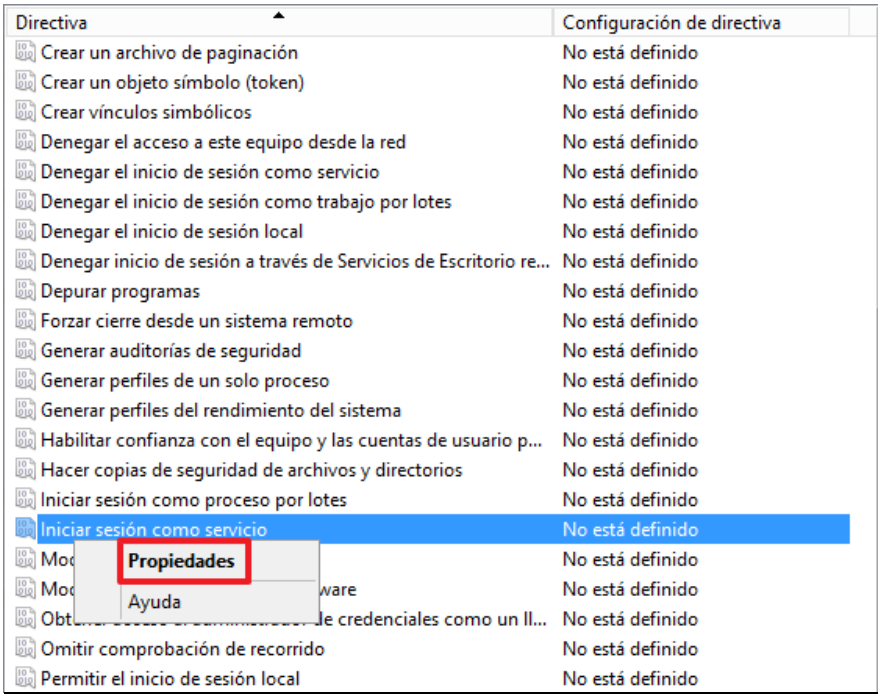
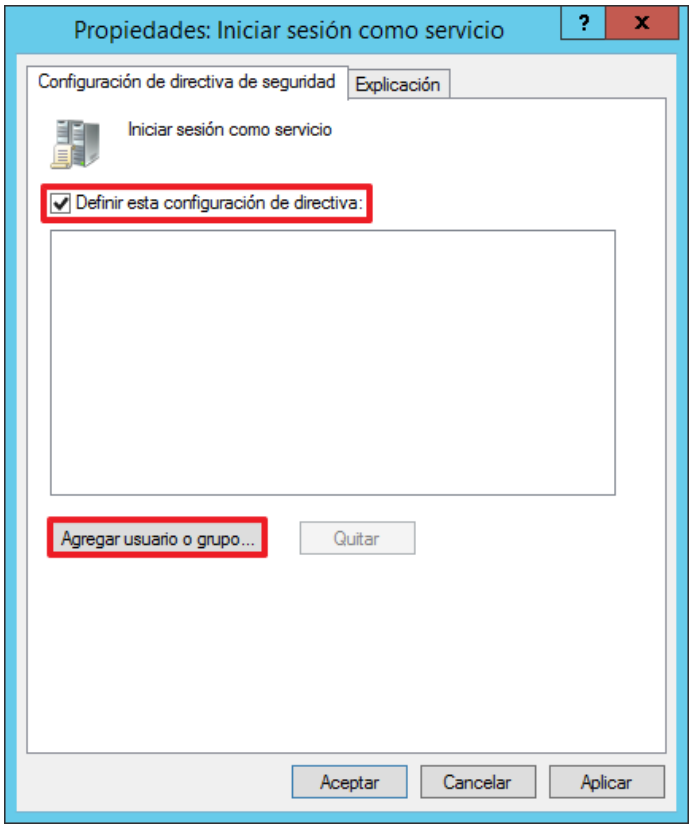
Paso	Descripción
18.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan MS SQL Server al grupo. 
19.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
20.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 

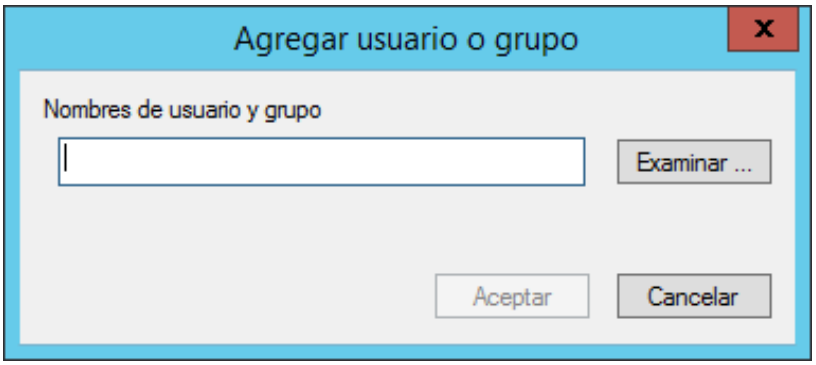
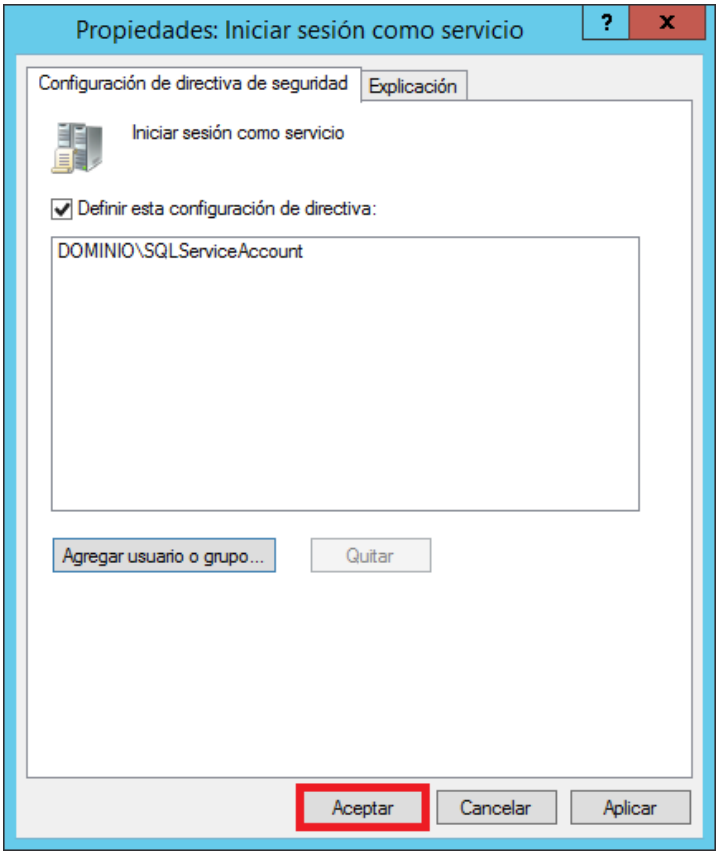
Paso	Descripción
21.	Agregue los equipos y pulse sobre “Aceptar”. 
22.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
23.	Cierre la herramienta de “usuarios y equipos de Active Directory”.
24.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .

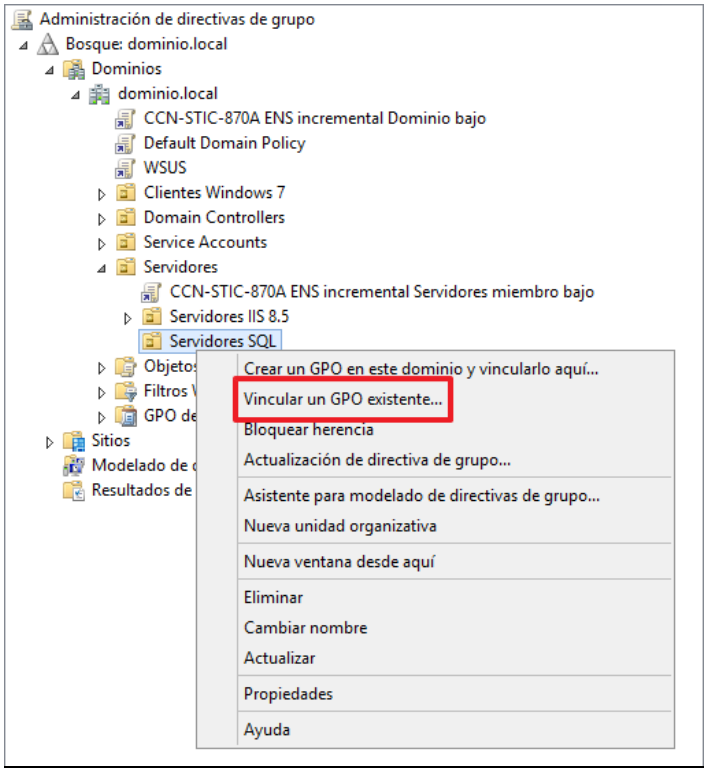
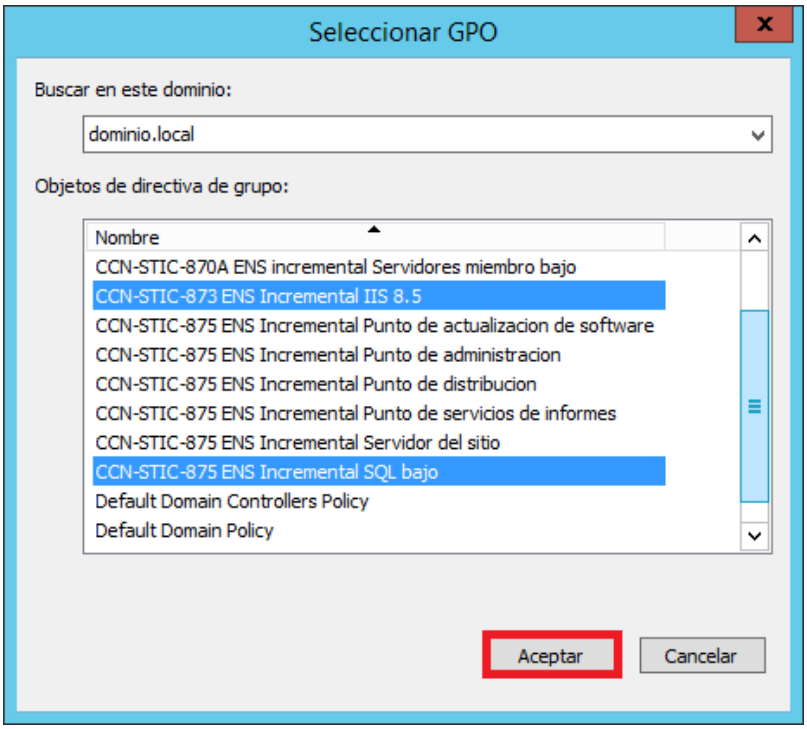
Paso	Descripción
25.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
26.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 
27.	Introduzca como nombre “CCN-STIC-875 ENS Incremental SQL bajo” y pulse el botón “Aceptar”. 
28.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 

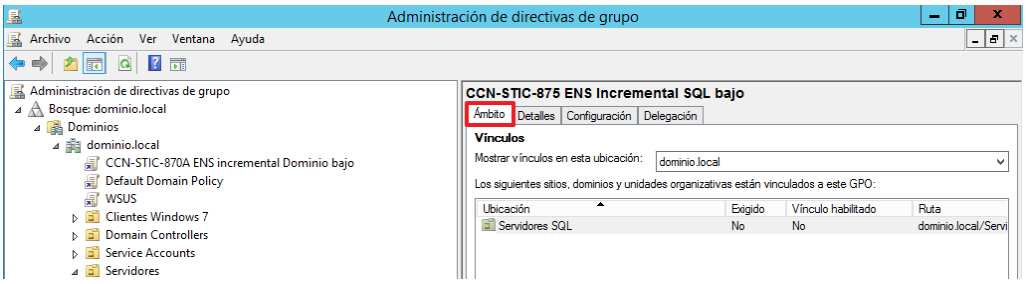
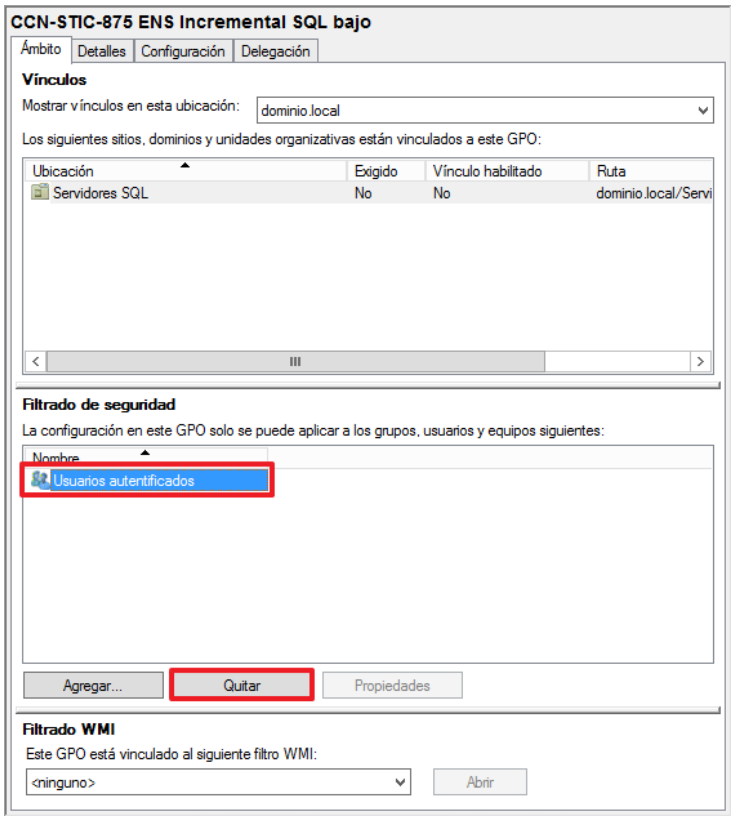
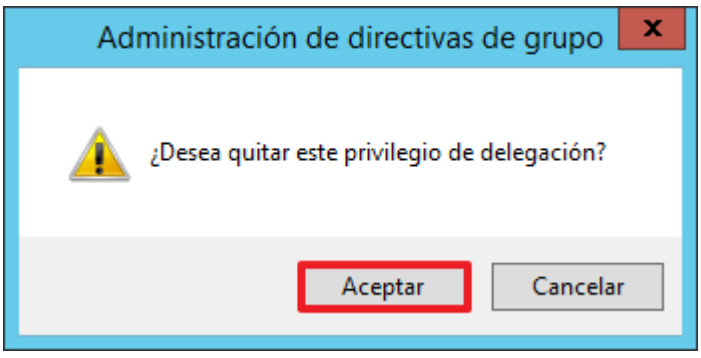
Paso	Descripción
29.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 
30.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental SQL bajo.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 

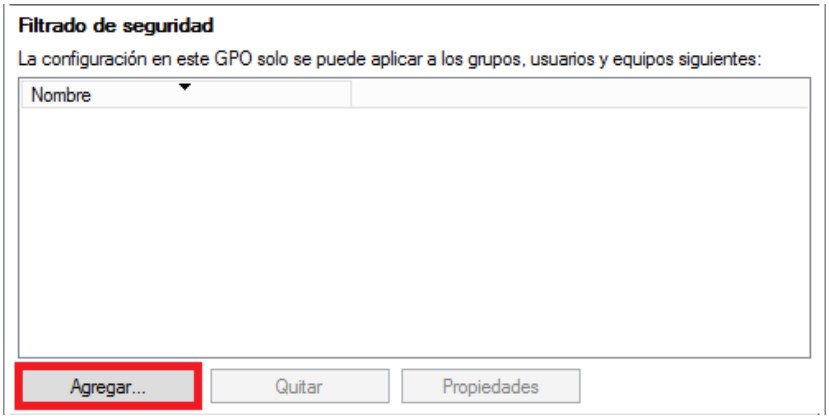
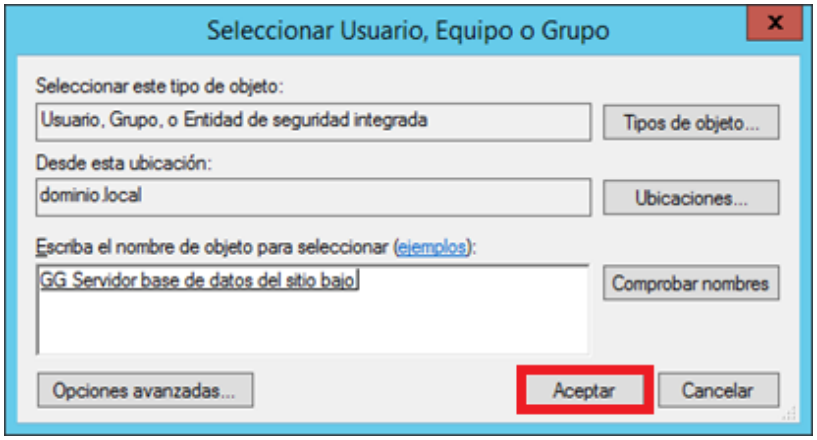
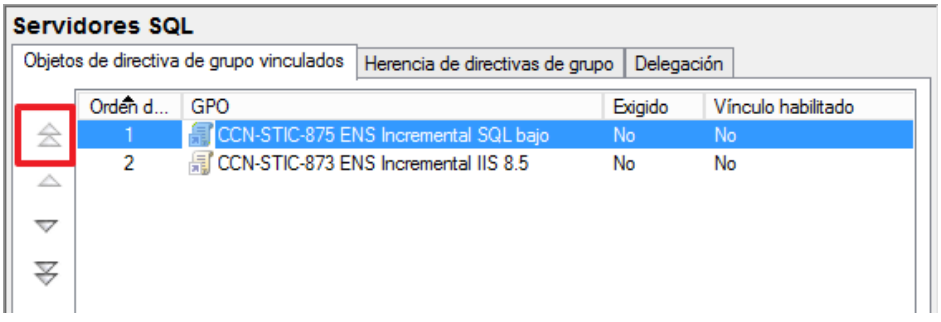
Paso	Descripción
31.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario".** 
32.	A continuación, seleccione la directiva "Iniciar sesión como servicio". 

Paso	Descripción
33.	Pulse con el botón derecho sobre la directiva y seleccione la opción “Propiedades” del menú contextual. 
34.	Seleccione la opción “Definir esta configuración de directiva” y pulse sobre “Agregar usuario o grupo...”. 

Paso	Descripción
35.	Agregue los usuarios necesarios para iniciar correctamente los servicios de SQL requeridos para un correcto funcionamiento del servicio. 
36.	Una vez añadidos los usuarios necesarios pulse “Aceptar”.  **Nota:** Deberá adaptar estos pasos a su organización y añadir únicamente los usuarios necesarios para un correcto funcionamiento del servicio.
37.	Cierre el editor de administración de directivas de grupo para finalizar la configuración.

Paso	Descripción
38.	A continuación, seleccione la unidad organizativa “Servidores SQL” y pulse botón derecho, “Vincular un GPO existente…”. 
39.	Seleccione los objetos de directiva de grupo con nombre, “CCN-STIC-875 ENS Incremental SQL bajo” y “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse aceptar. 

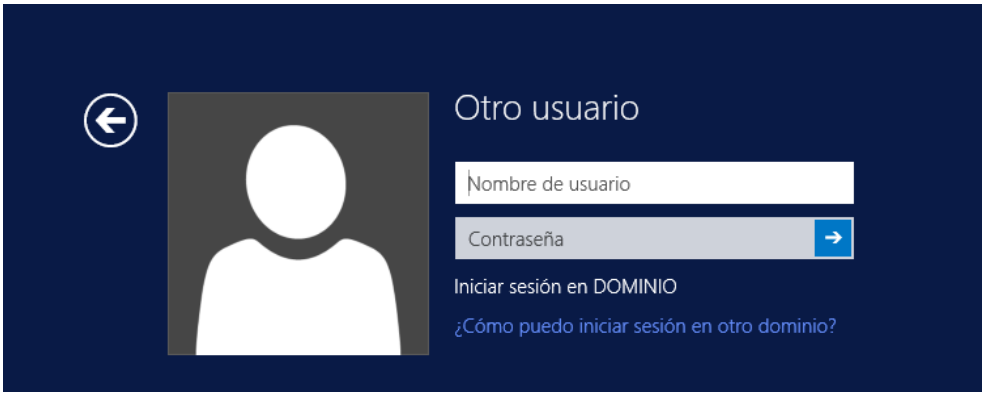
Paso	Descripción
40.	Seleccione la directiva de grupo “CCN-STIC-875 ENS Incremental SQL bajo” y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 
41.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
42.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 

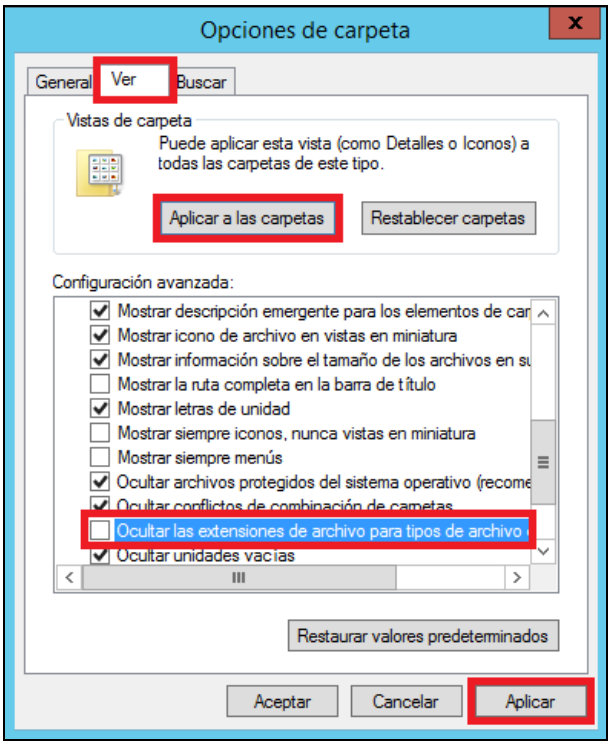
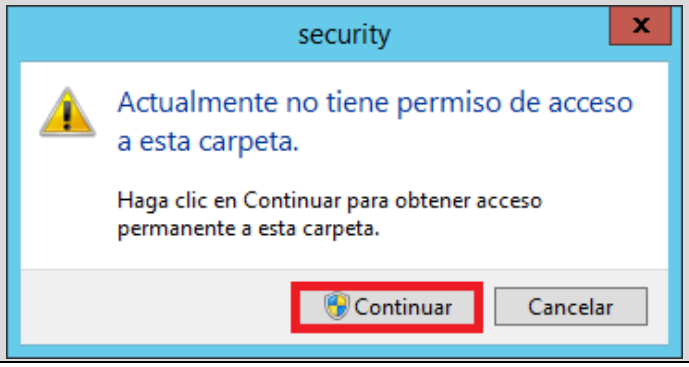
Paso	Descripción
43.	Una vez quitado, pulse el botón “Agregar…”. 
44.	Introduzca como nombre “GG Servidor base de datos del sitio bajo” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
45.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva “CCN-STIC-875 ENS Incremental SQL bajo” aparezca en primer lugar. Para ello seleccione, la unidad organizativa “Servidores SQL” y a continuación, haga clic sobre la fecha doble hacia arriba para que se sitúe con el número 1 de orden vínculos, tal y como se muestra en la imagen. 
46.	Cierre el administrador de directivas de grupo para finalizar con la configuración.

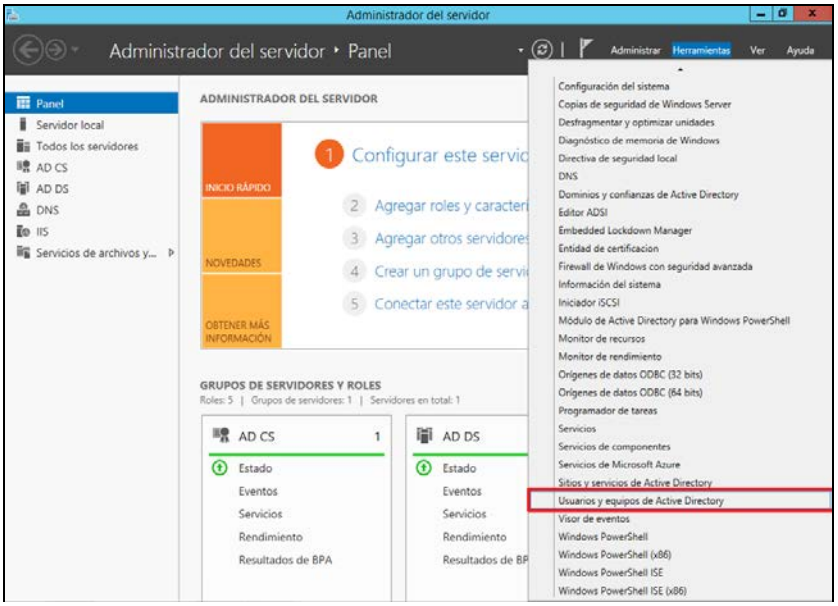
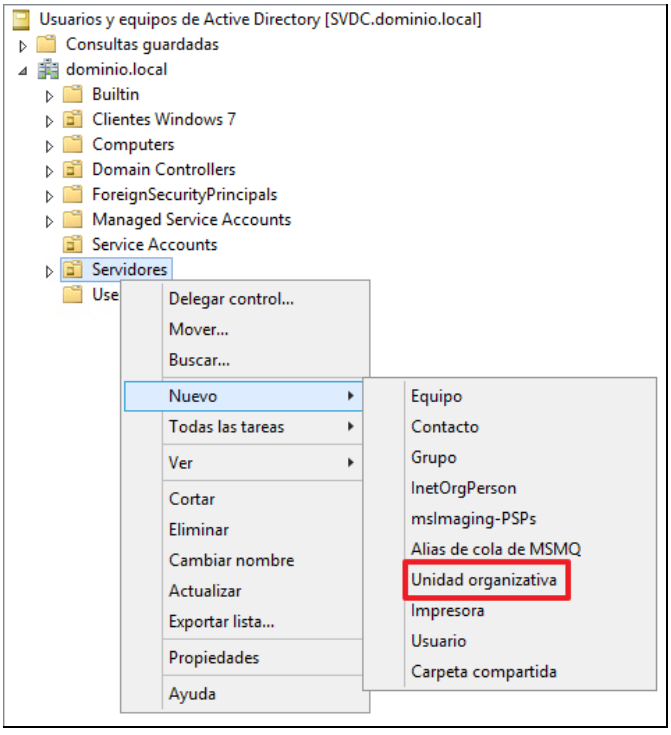
2. REFUERZO DE SEGURIDAD DEL SERVIDOR DEL SITIO

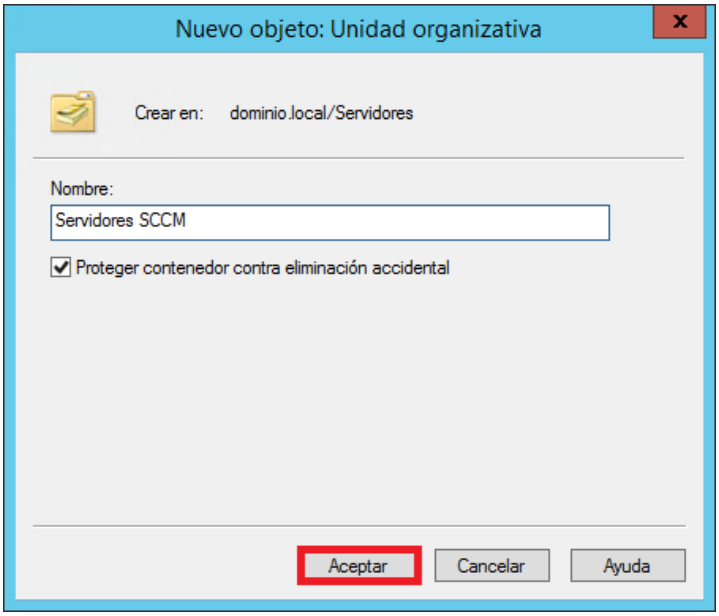
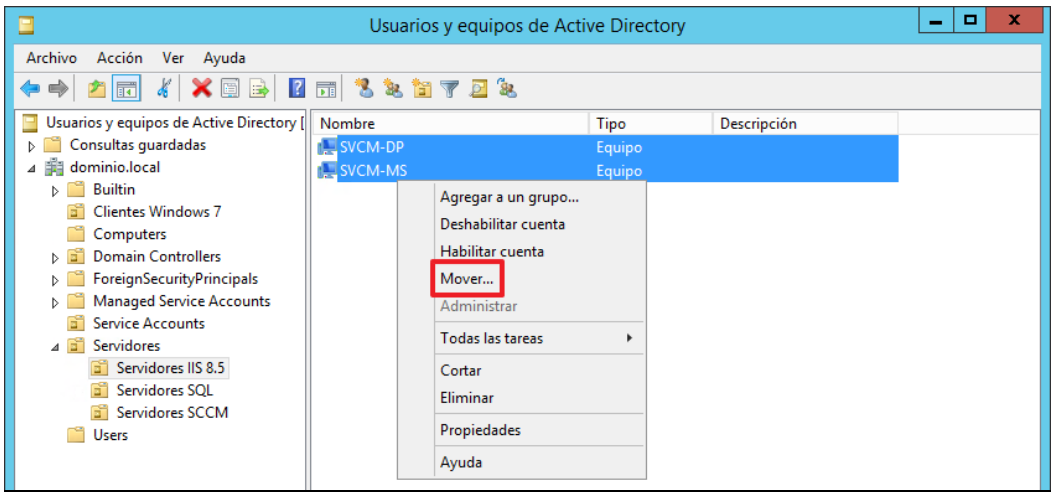
A continuación, se describen los pasos para reforzar la seguridad de un servidor con el rol de servidor de sitio, el cual también incluye el rol de Sistema de sitio y servidor de componentes.

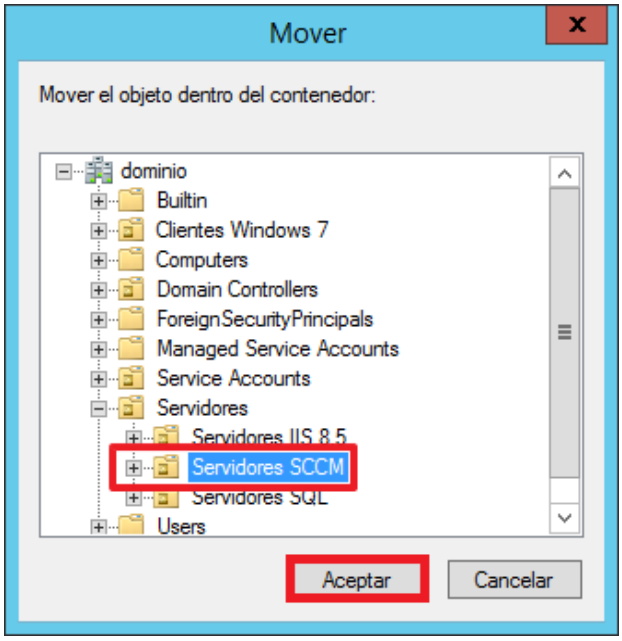
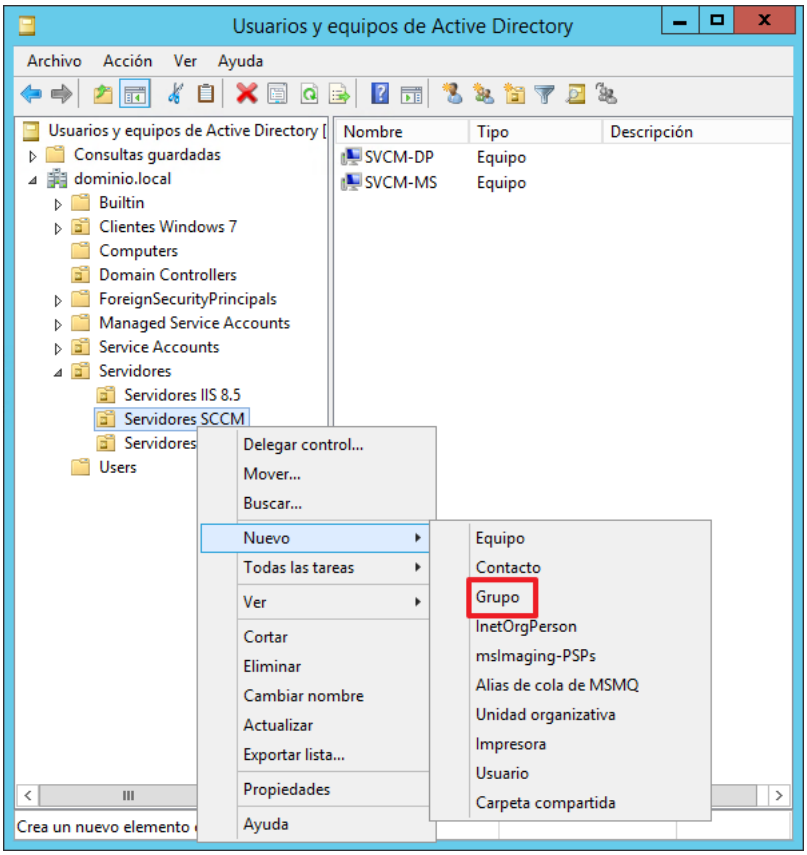
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

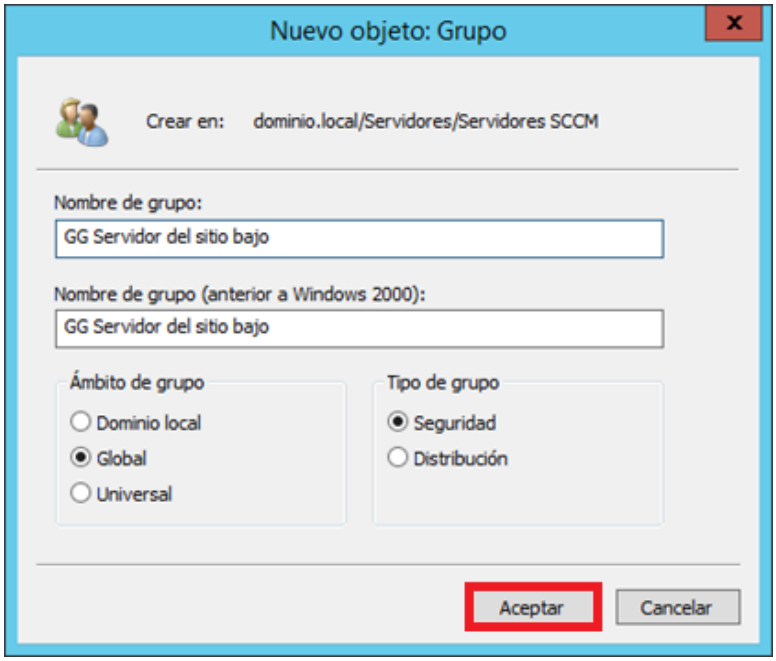
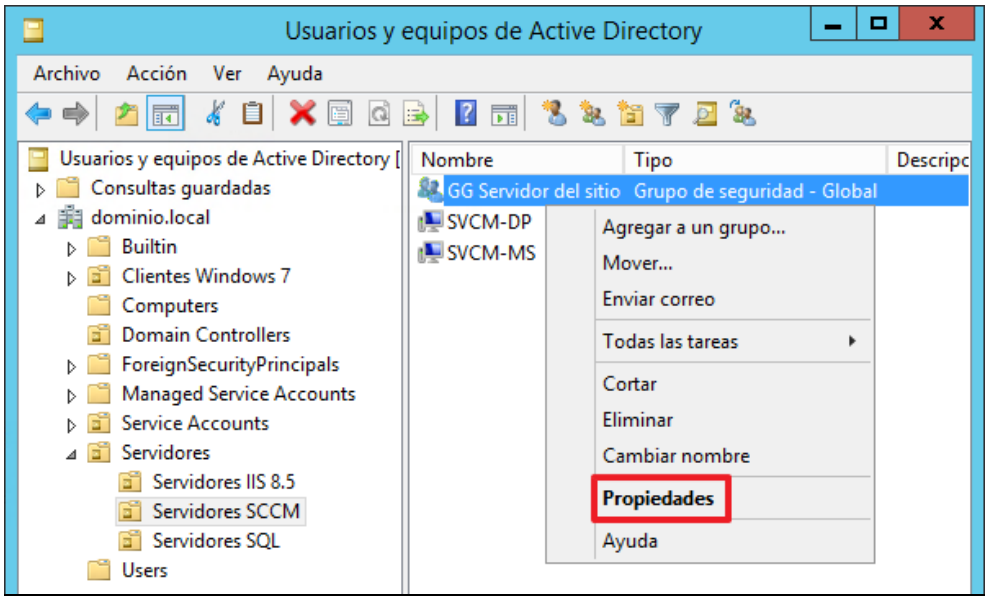
Paso	Descripción
47.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
48.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
49.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
50.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.

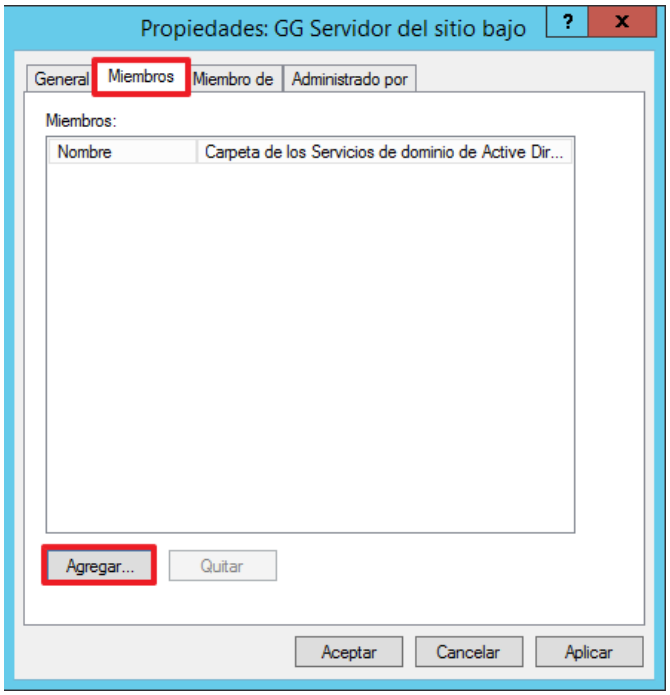
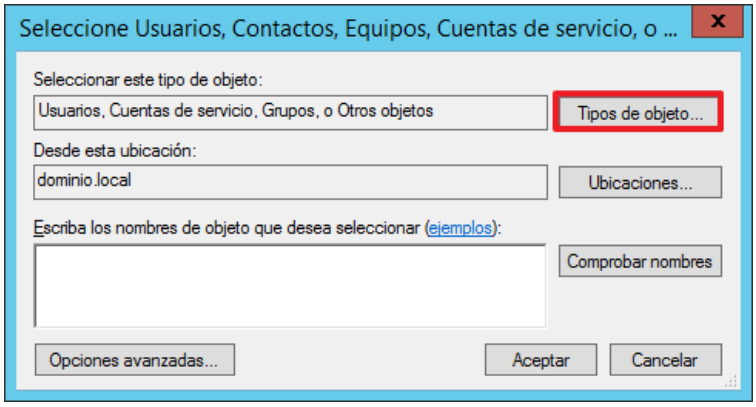
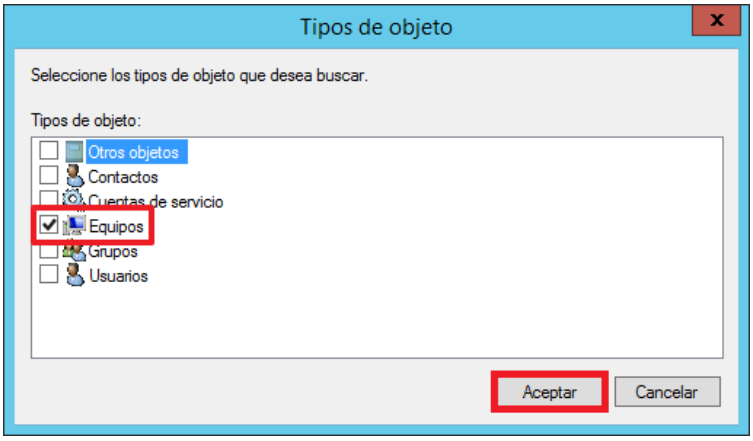
Paso	Descripción
51.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
52.	Copie el fichero “CCN-STIC-875 ENS Incremental Servidor del sitio Bajo.inf” que se encuentra en la ruta “C:\Scripts\Nivel Bajo” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 

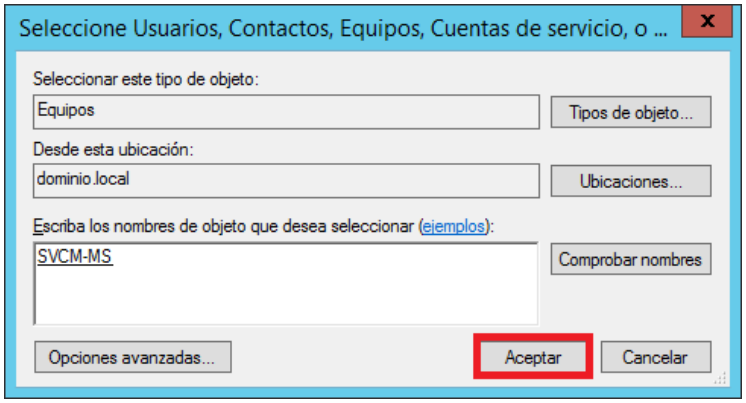
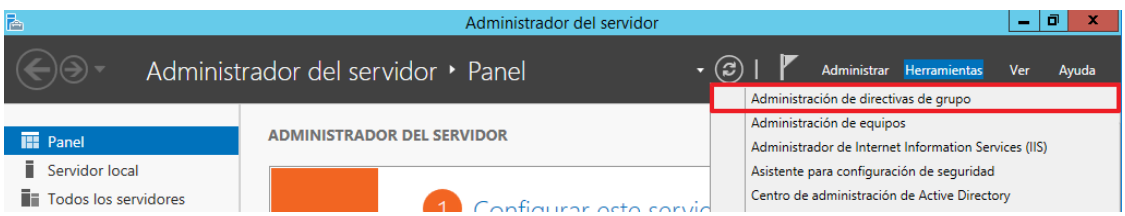
Paso	Descripción
53.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.
54.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 

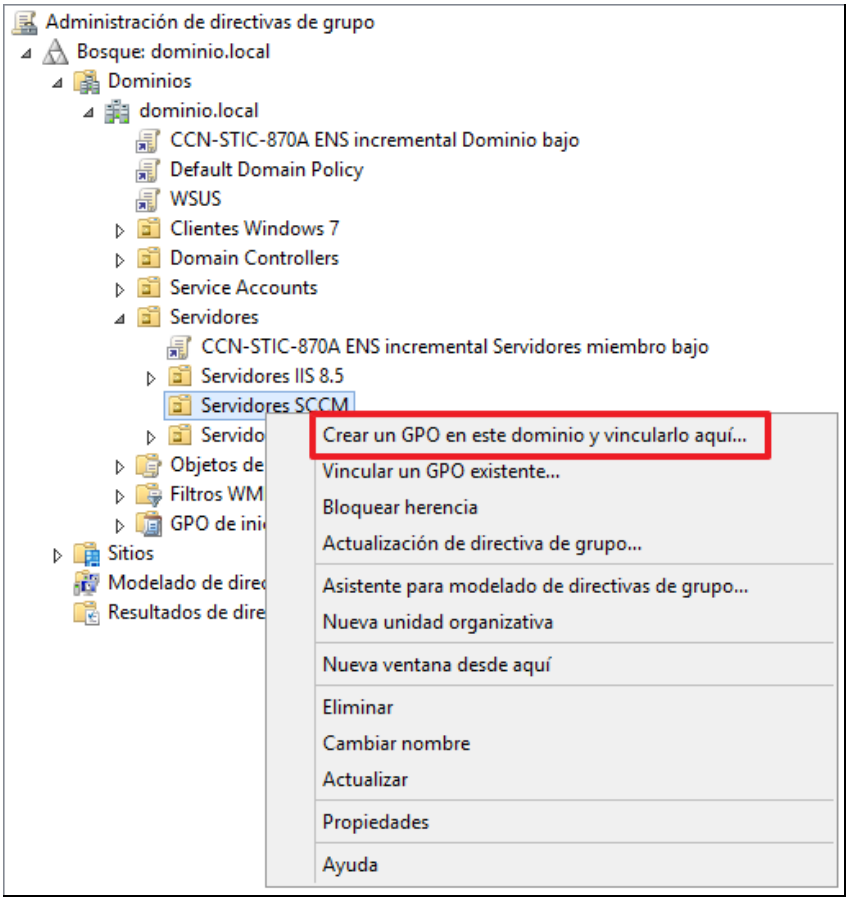
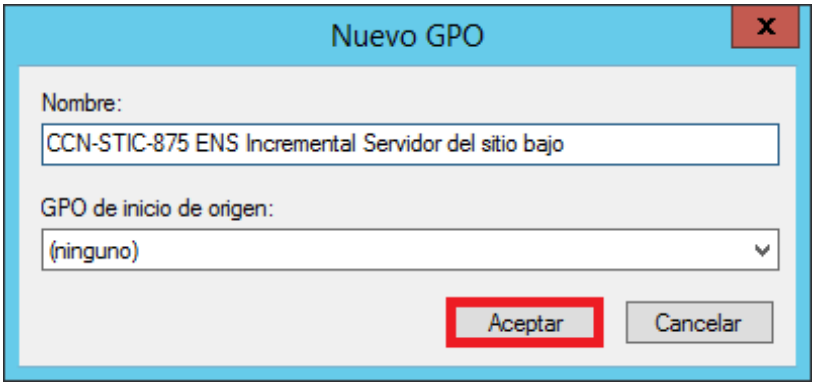
Paso	Descripción
55.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y marque en “Aceptar”. 
56.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.

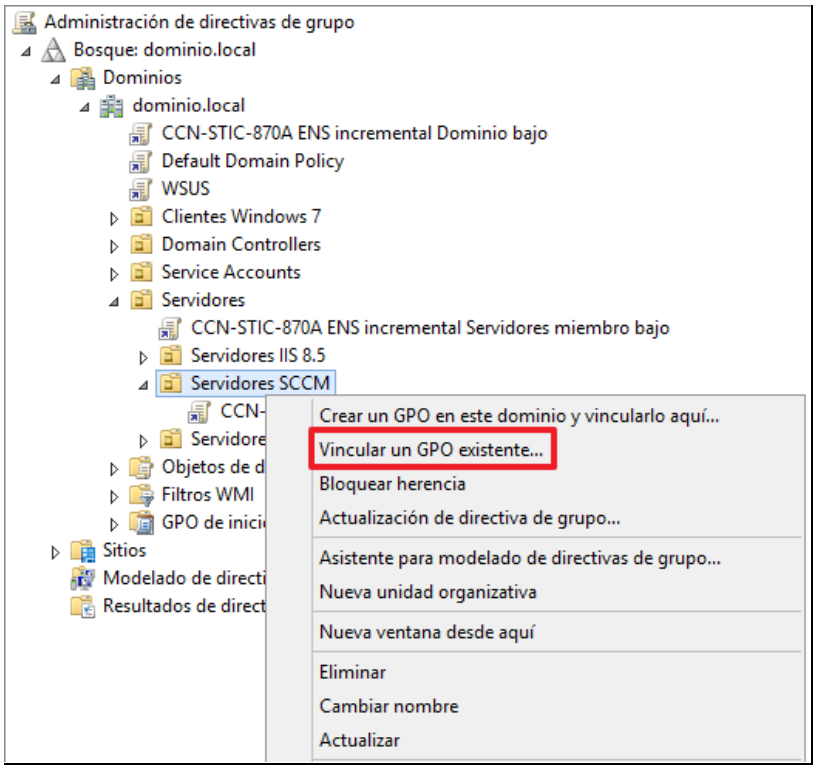
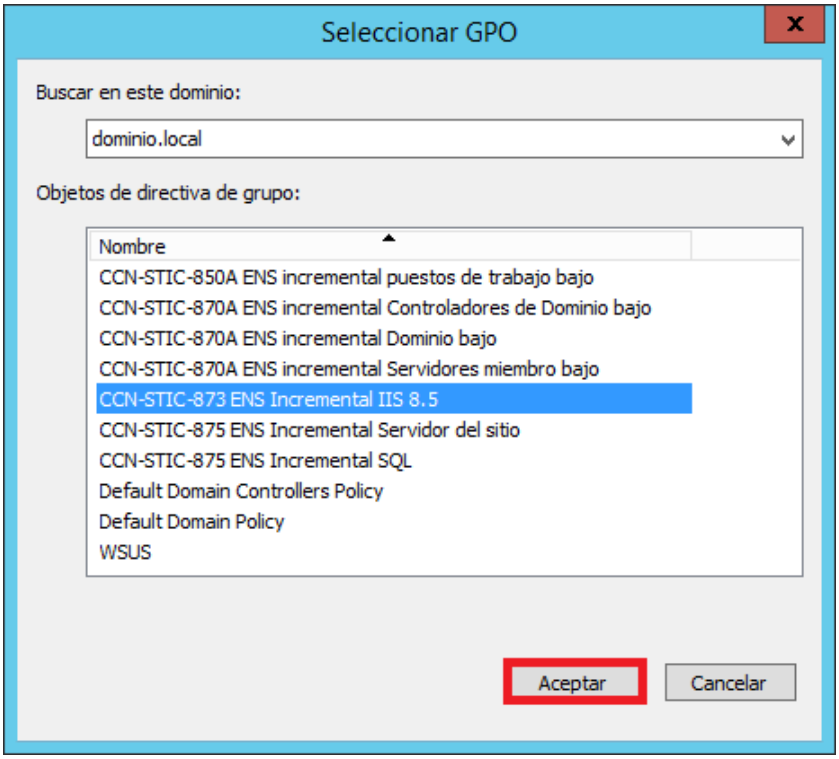
Paso	Descripción
57.	Seleccione la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 
58.	En el siguiente paso, seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 

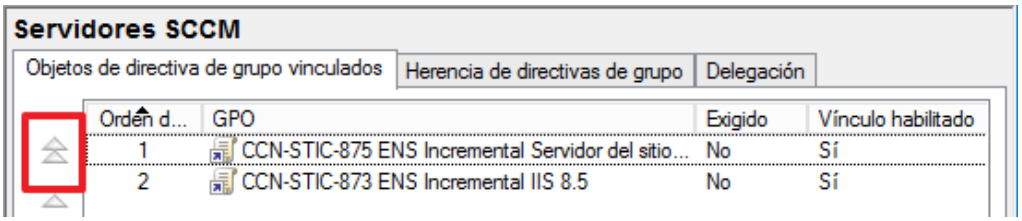
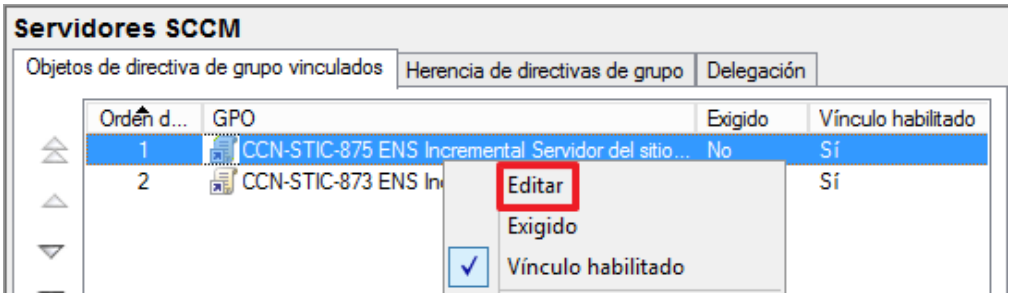
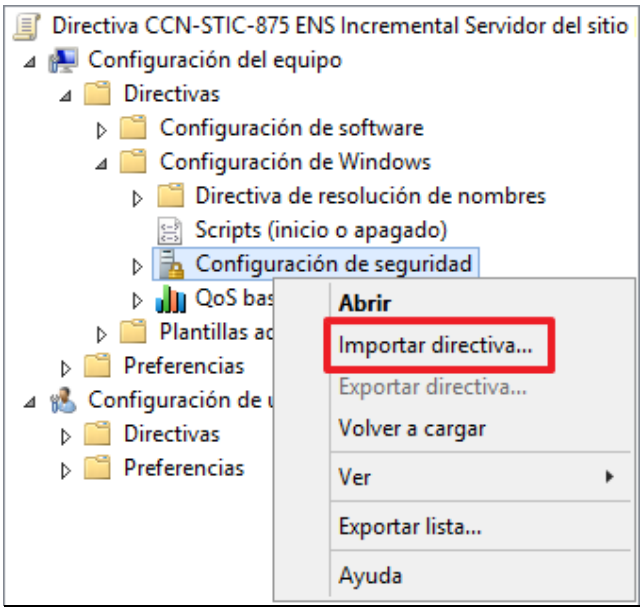
Paso	Descripción
59.	Escriba el nombre “GG Servidor del sitio bajo” y pulse “Aceptar”. 
60.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 

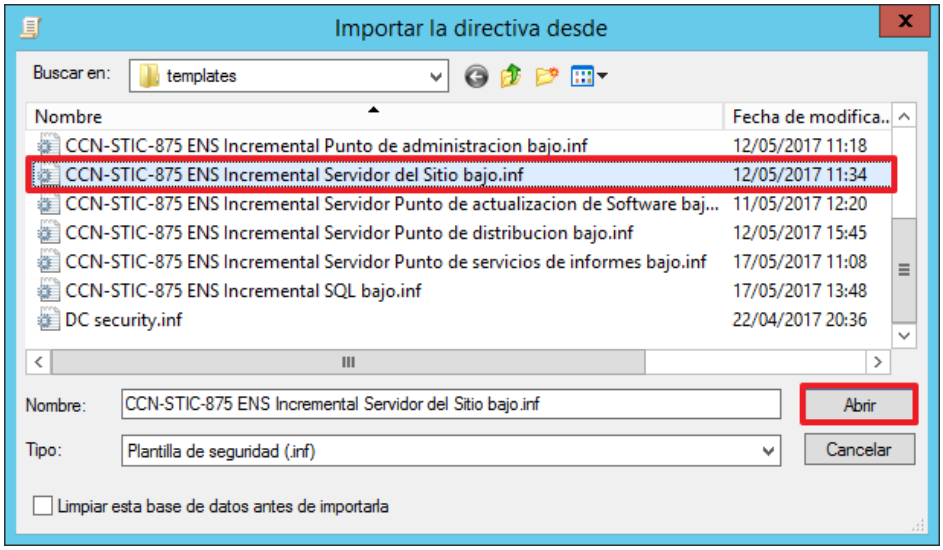
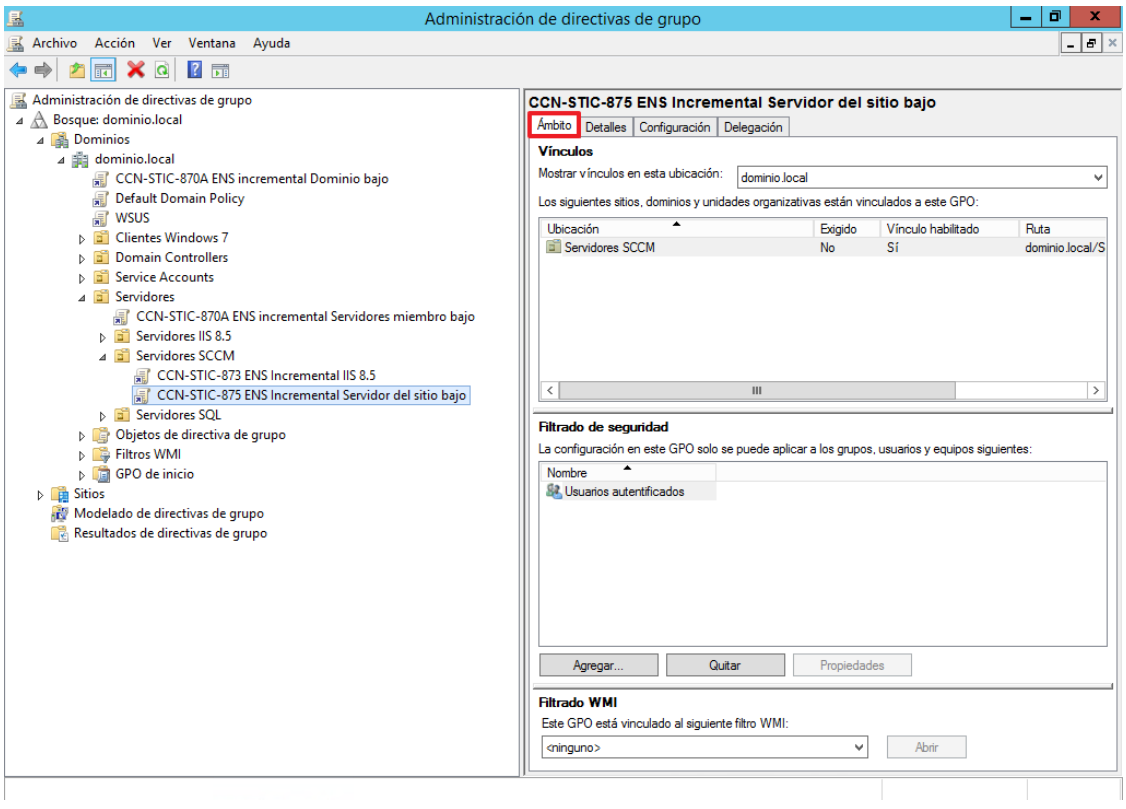
Paso	Descripción
61.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “servidor de sitio” al grupo. 
62.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
63.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 

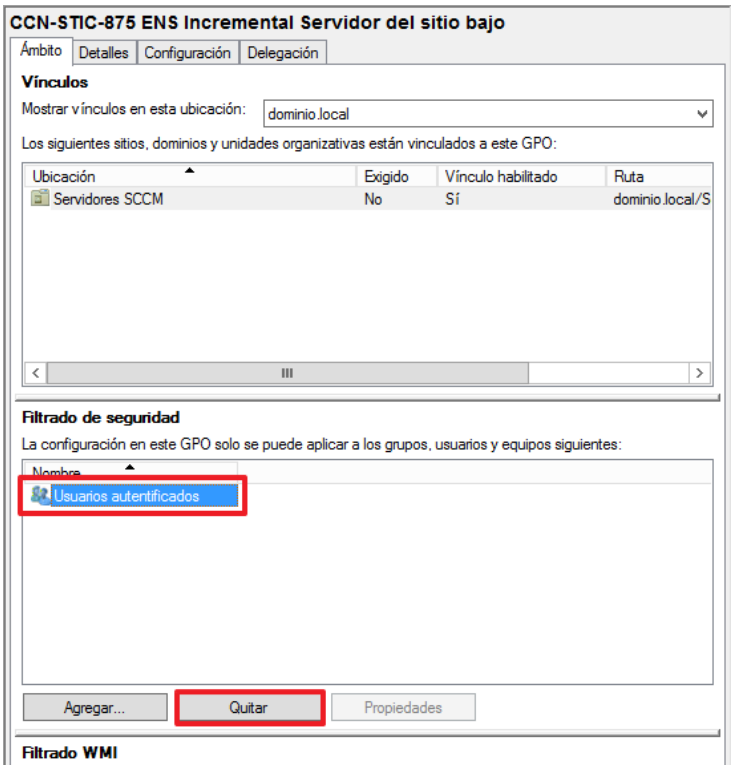
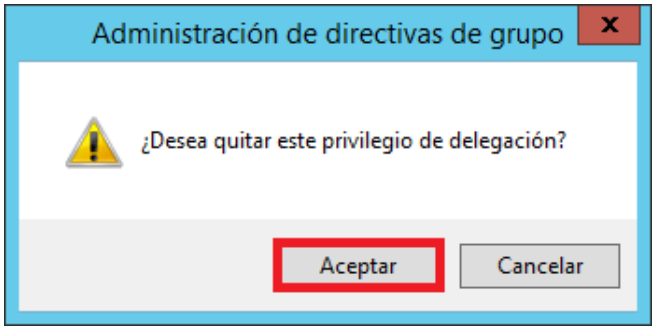
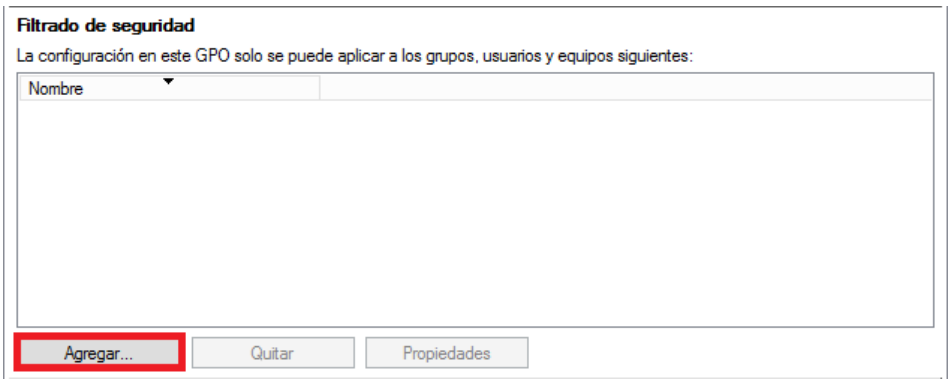
Paso	Descripción
64.	Agregue los equipos y pulse sobre “Aceptar”. 
65.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
66.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
67.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

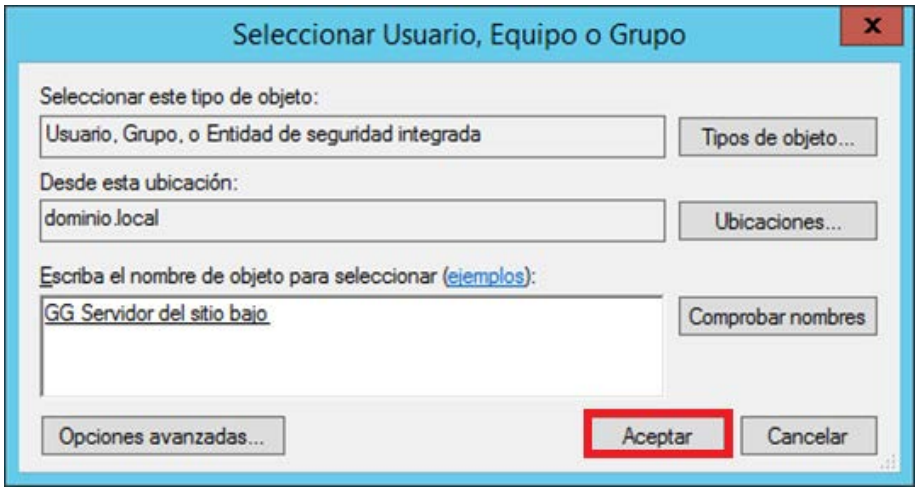
Paso	Descripción
68.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
69.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Servidor del sitio bajo” y haga clic en el botón “Aceptar”. 
70.	Seguidamente, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM.

Paso	Descripción
71.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
72.	A continuación, seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre “Aceptar”. 

Paso	Descripción
73.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Servidor del sitio bajo" aparezca en primer lugar. Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Servidor del sitio bajo" y a continuación, haga clic sobre la fecha doble hacia arriba para que se sitúe con el número 1 de orden vínculos, tal y como se muestra en la imagen. 
74.	Edite la GPO: "CCN-STIC-875 ENS Incremental Servidores del sitio bajo" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
75.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
76.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Servidor del sitio bajo.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
77.	Cierre el “editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
78.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

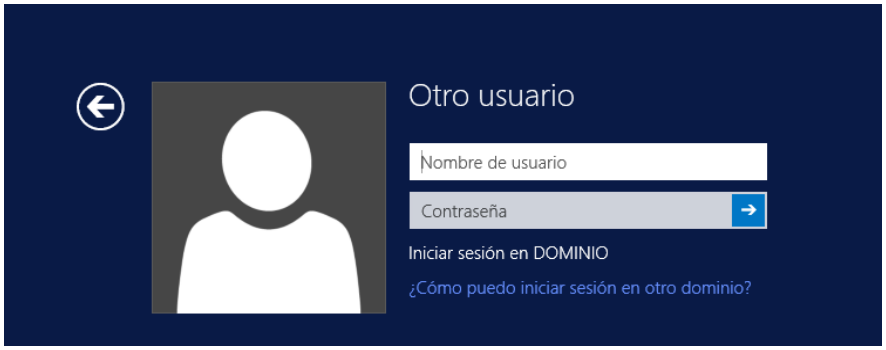
Paso	Descripción
79.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
80.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
81.	Una vez quitado, pulse el botón “Agregar…”. 

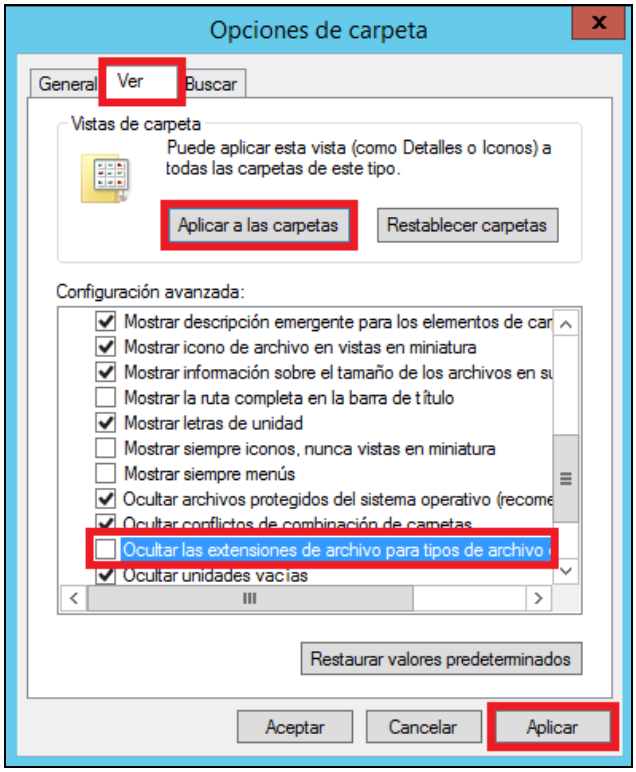
Paso	Descripción
82.	Introduzca como nombre “GG Servidor del sitio bajo”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
83.	Cierre el “Editor de administración de directivas de grupo”.

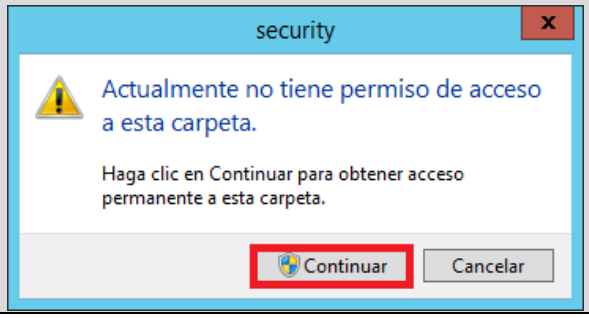
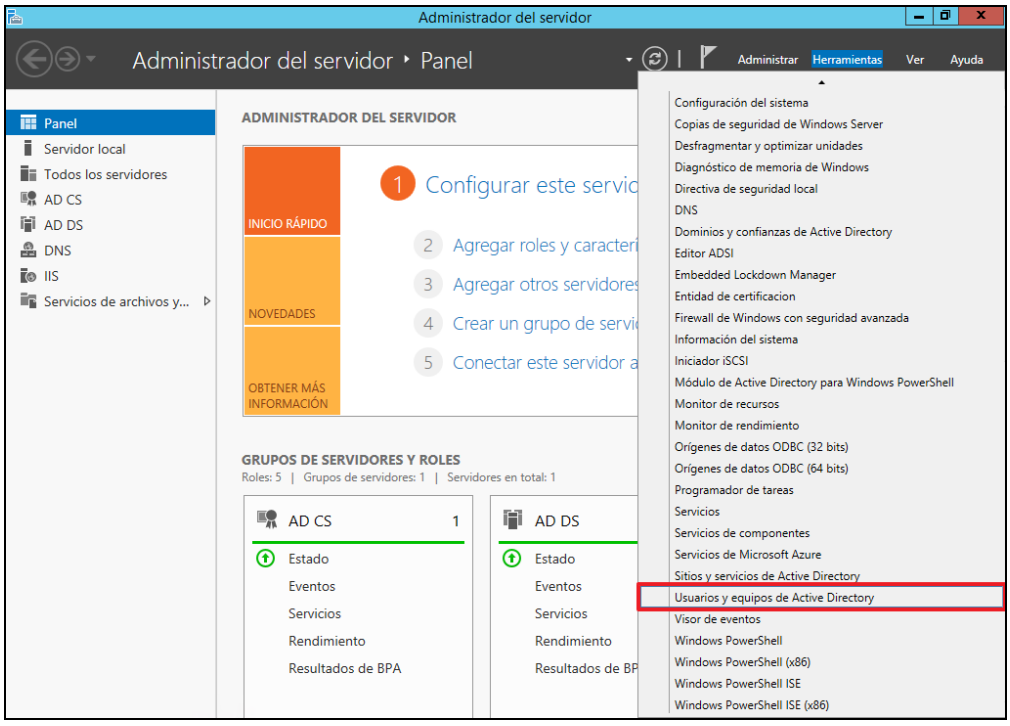
3. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE ADMINISTRACIÓN

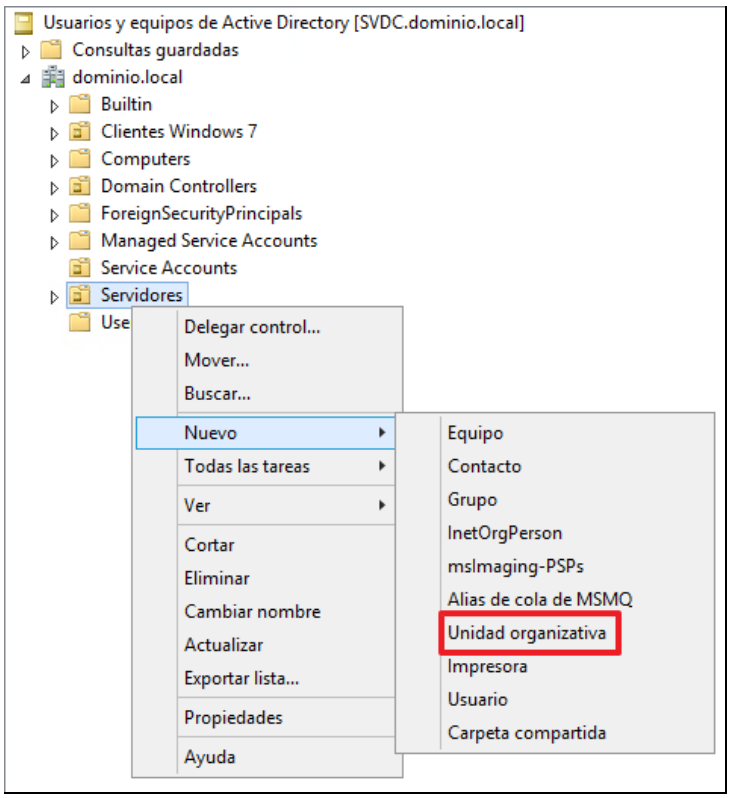
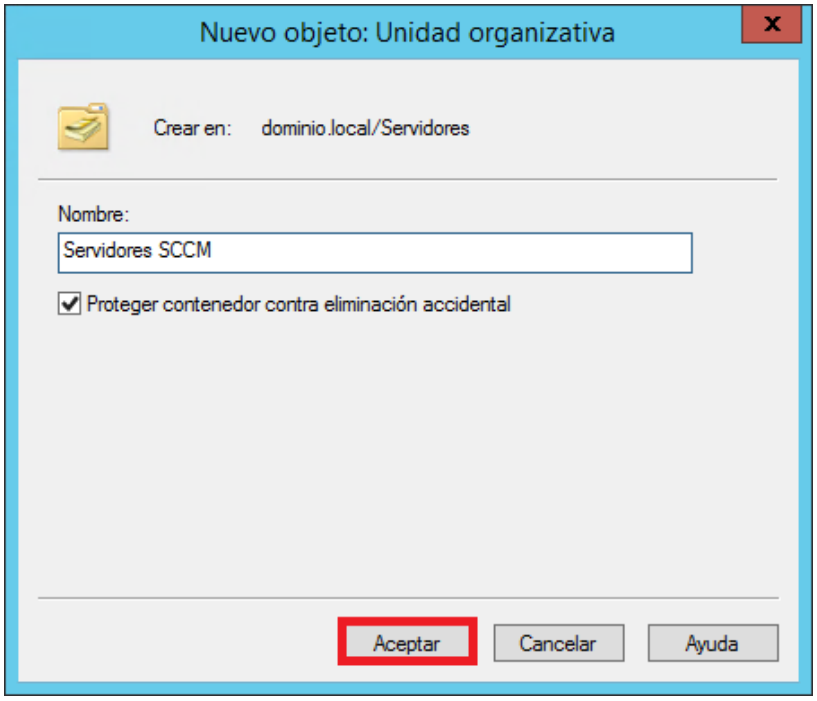
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de administración implementado en el equipo.

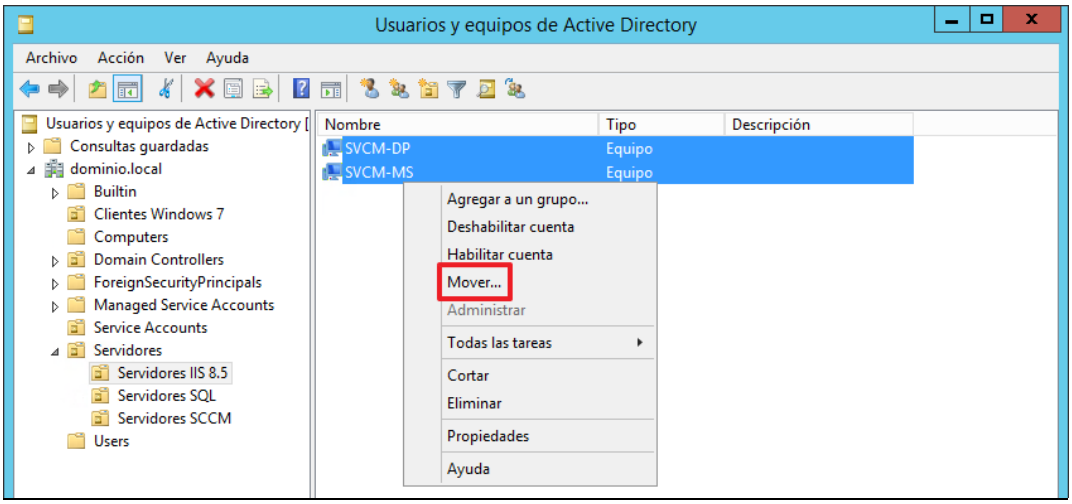
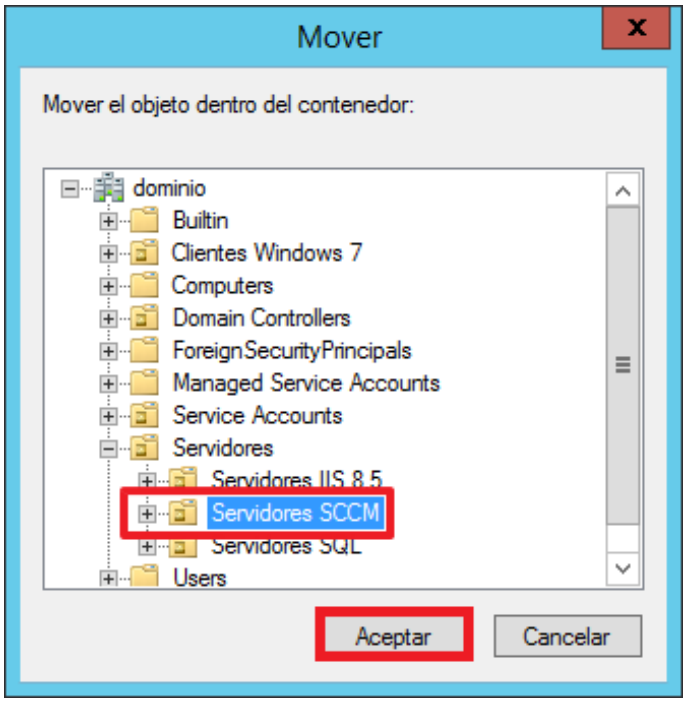
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

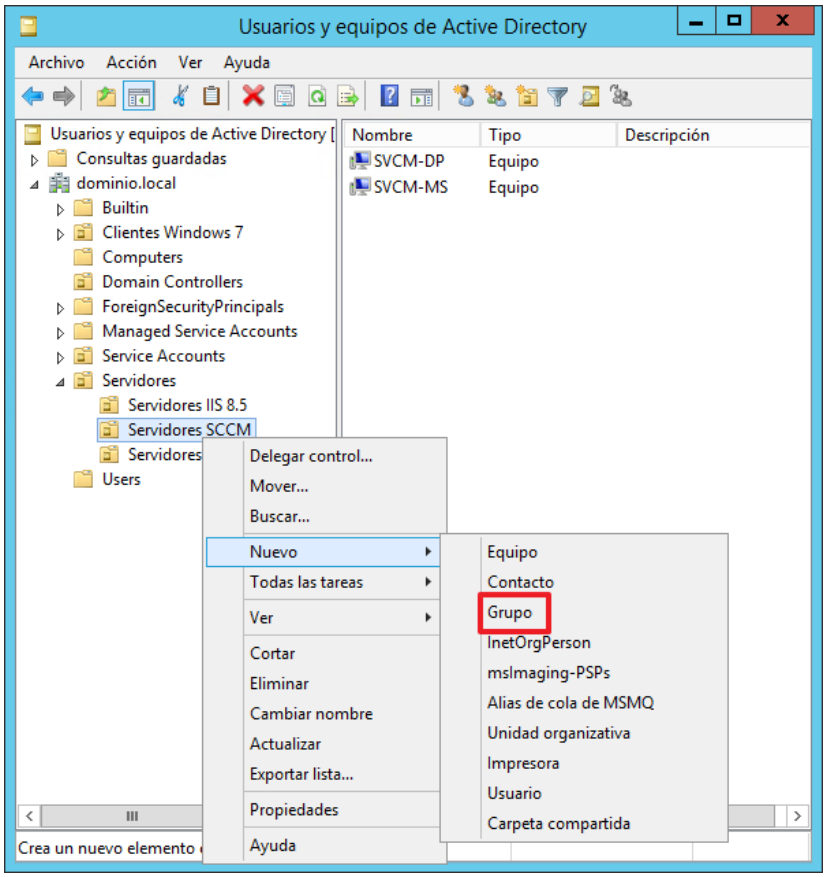
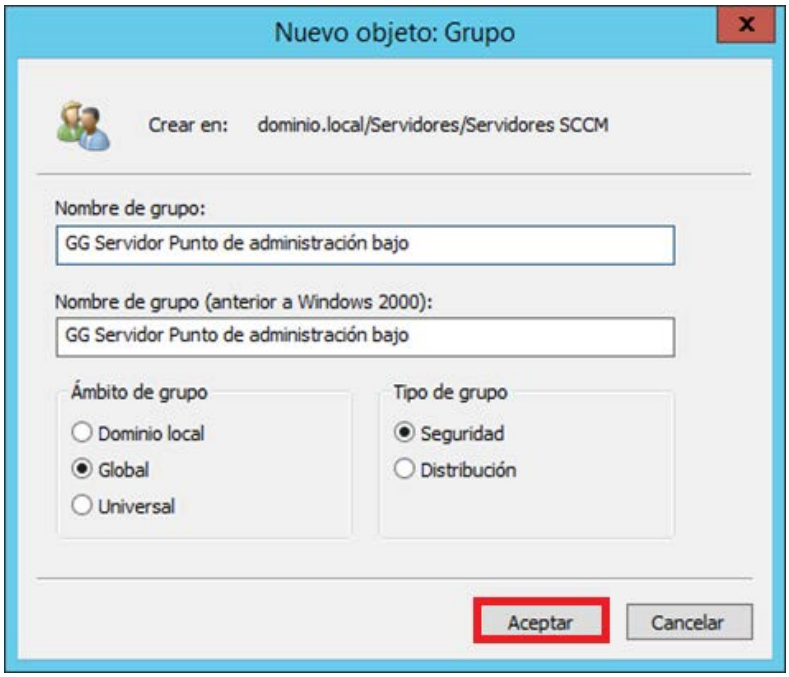
Paso	Descripción
84.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.

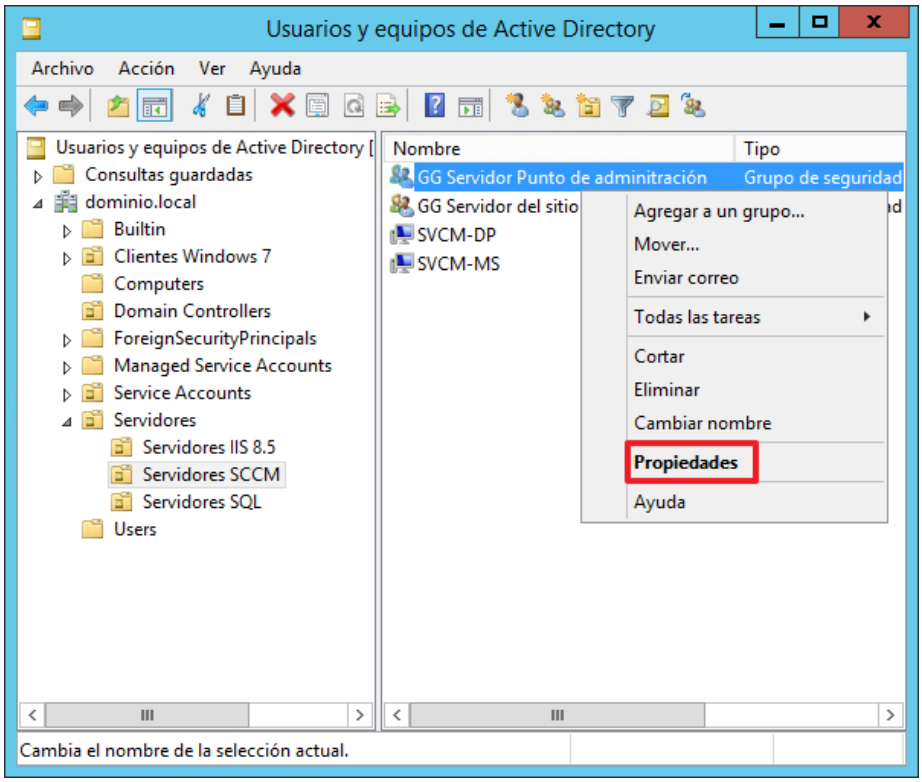
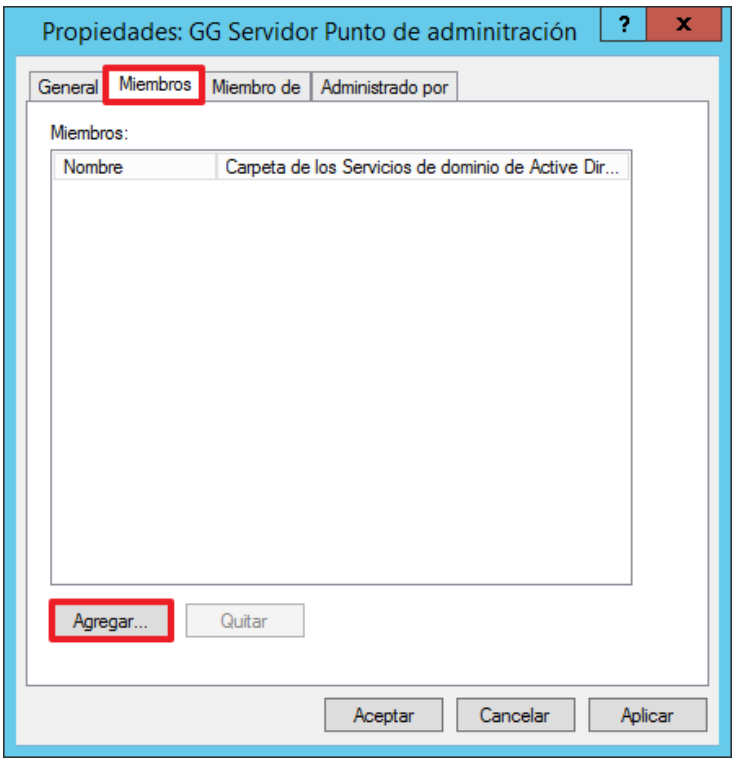
Paso	Descripción
85.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
86.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
87.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
88.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

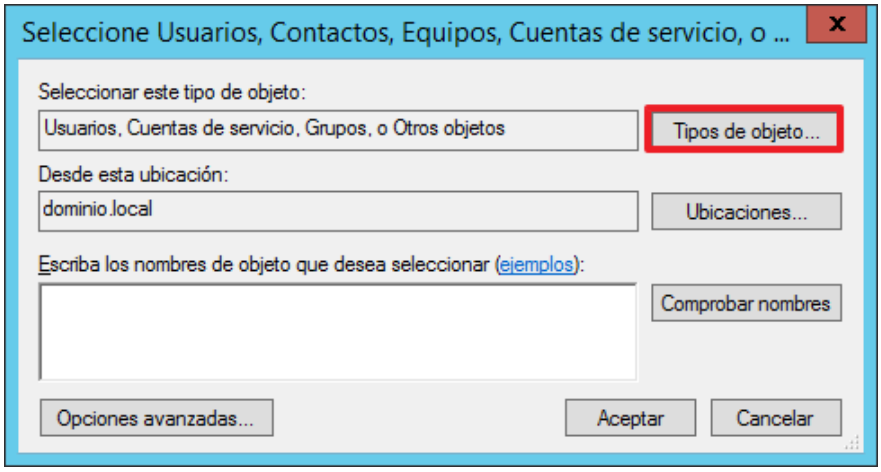
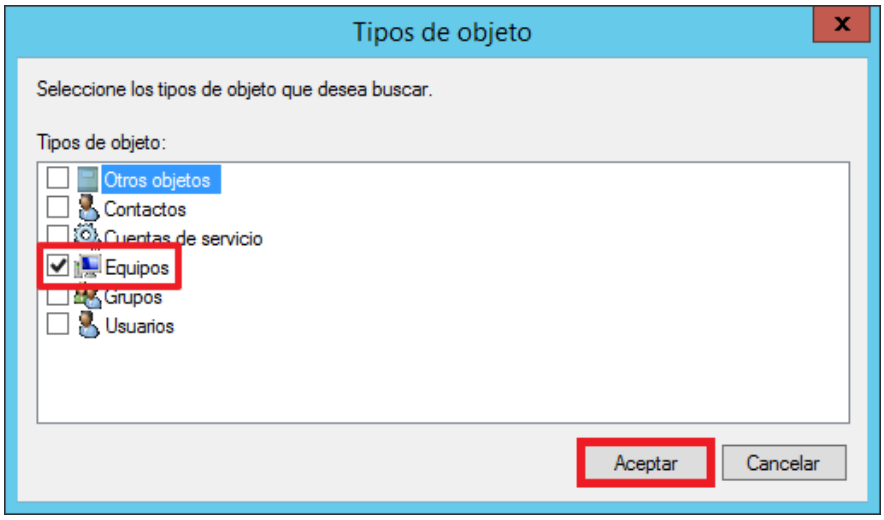
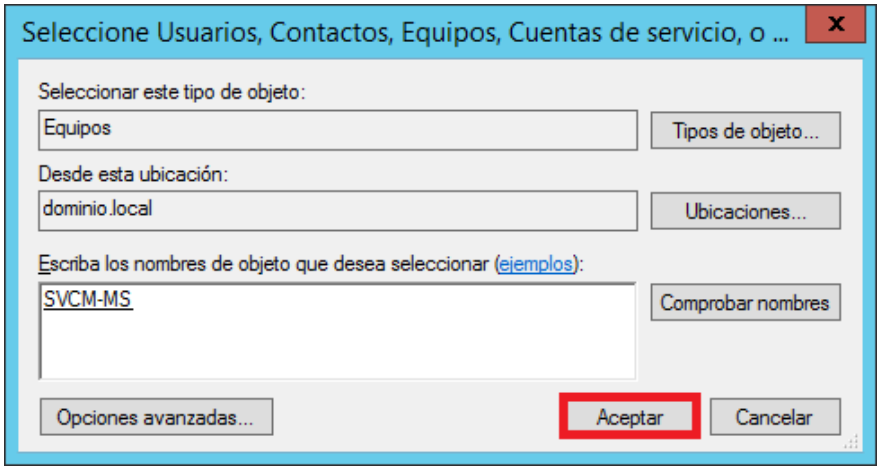
Paso	Descripción
89.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de administración bajo.inf” que se encuentra en la ruta “C:\Scripts\Nivel Bajo” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
90.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
91.	En el siguiente proceso, se va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 96. En caso contrario continúe con el paso a paso.

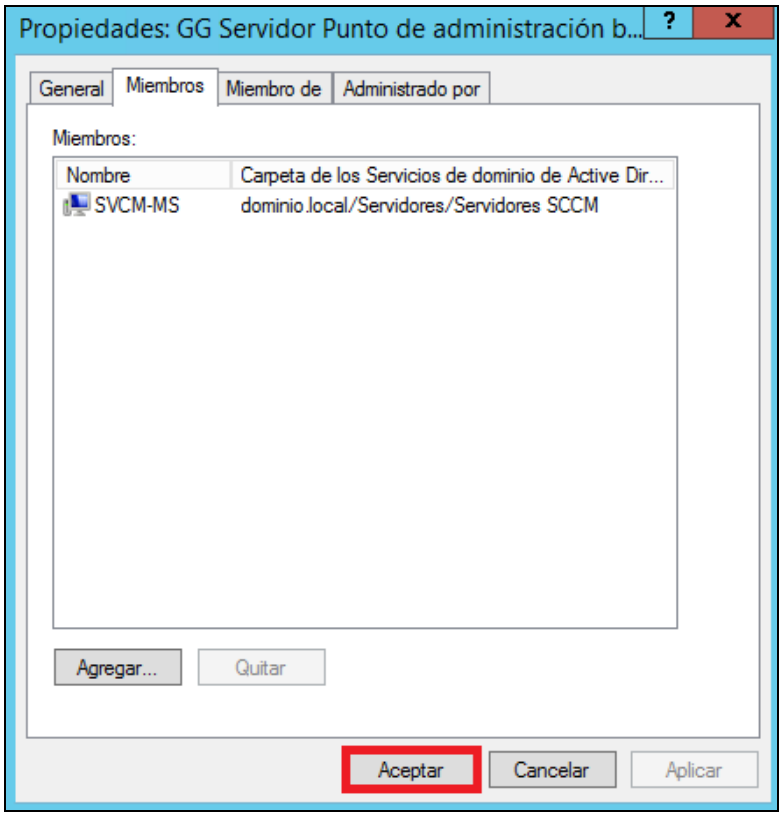
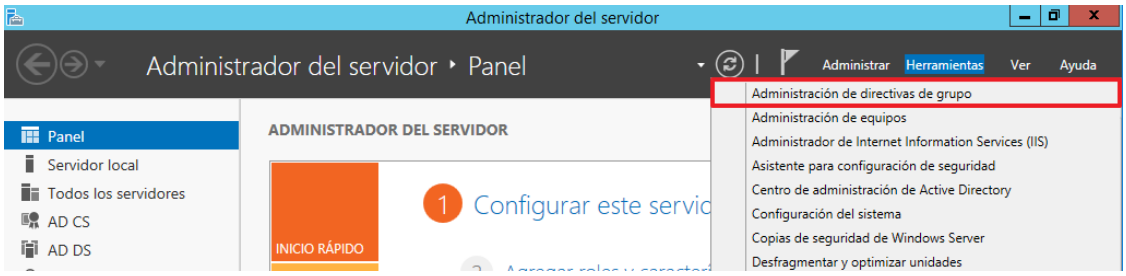
Paso	Descripción
92.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
93.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen, pulse “Aceptar”. 

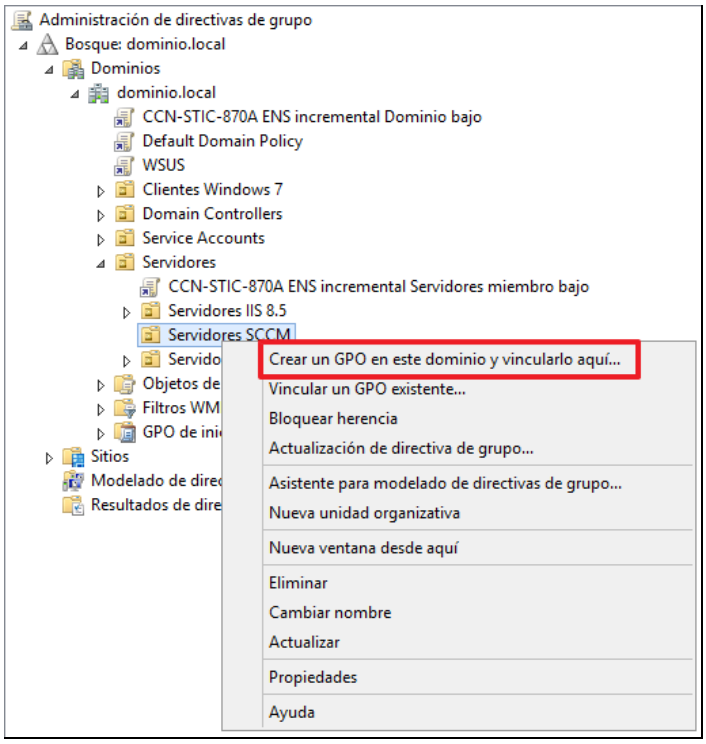
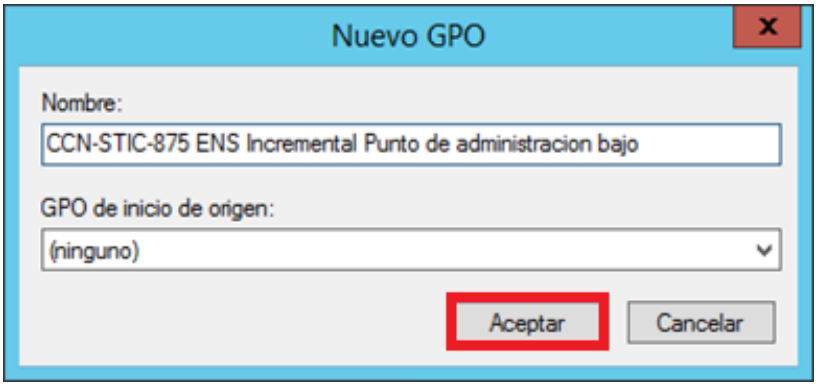
Paso	Descripción
94.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
95.	Seleccione la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

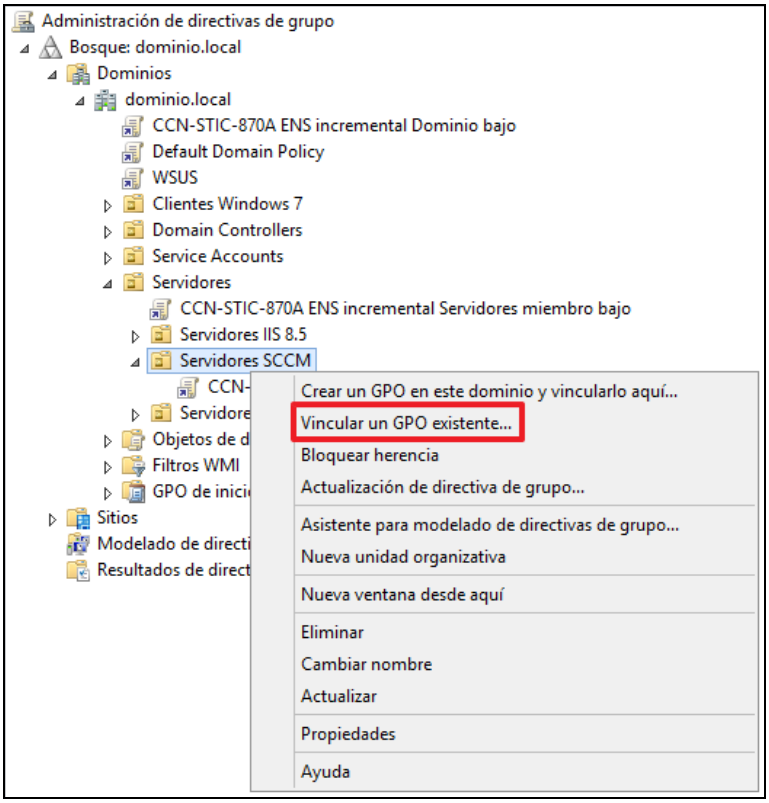
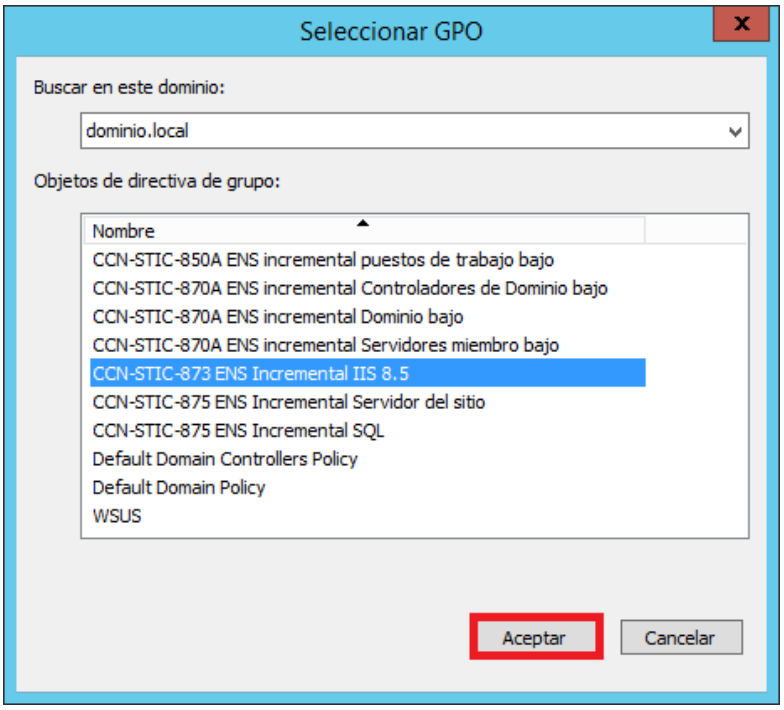
Paso	Descripción
96.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
97.	Escriba el nombre “GG Servidor Punto de administración bajo” y pulse “Aceptar”. 

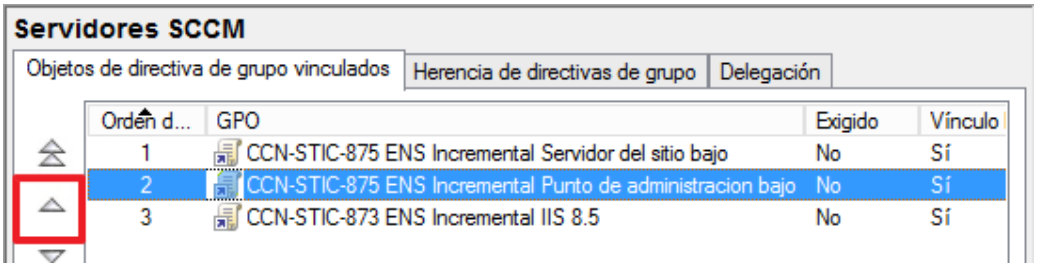
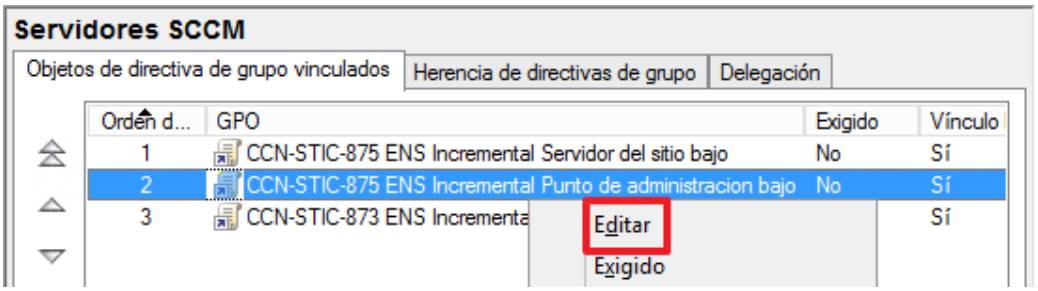
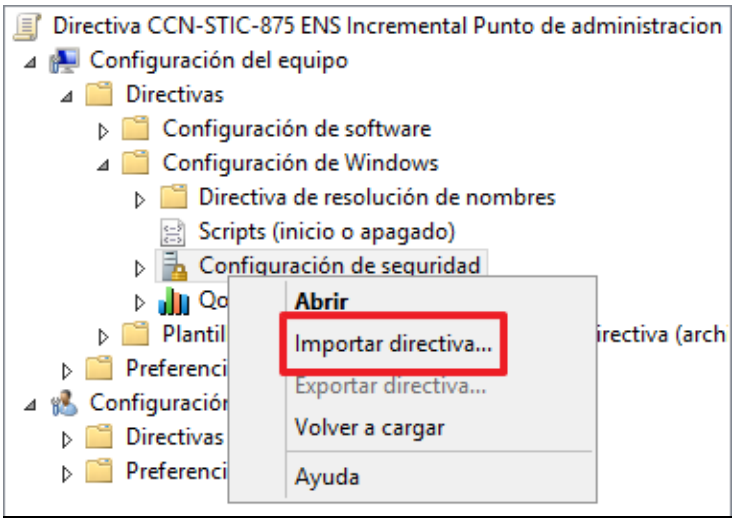
Paso	Descripción
98.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
99.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de administración” al grupo. 

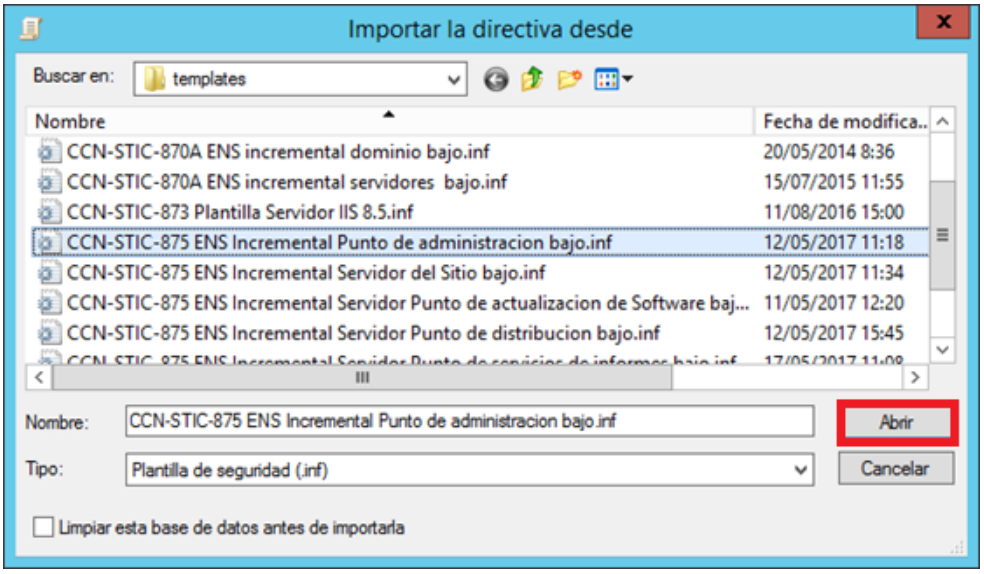
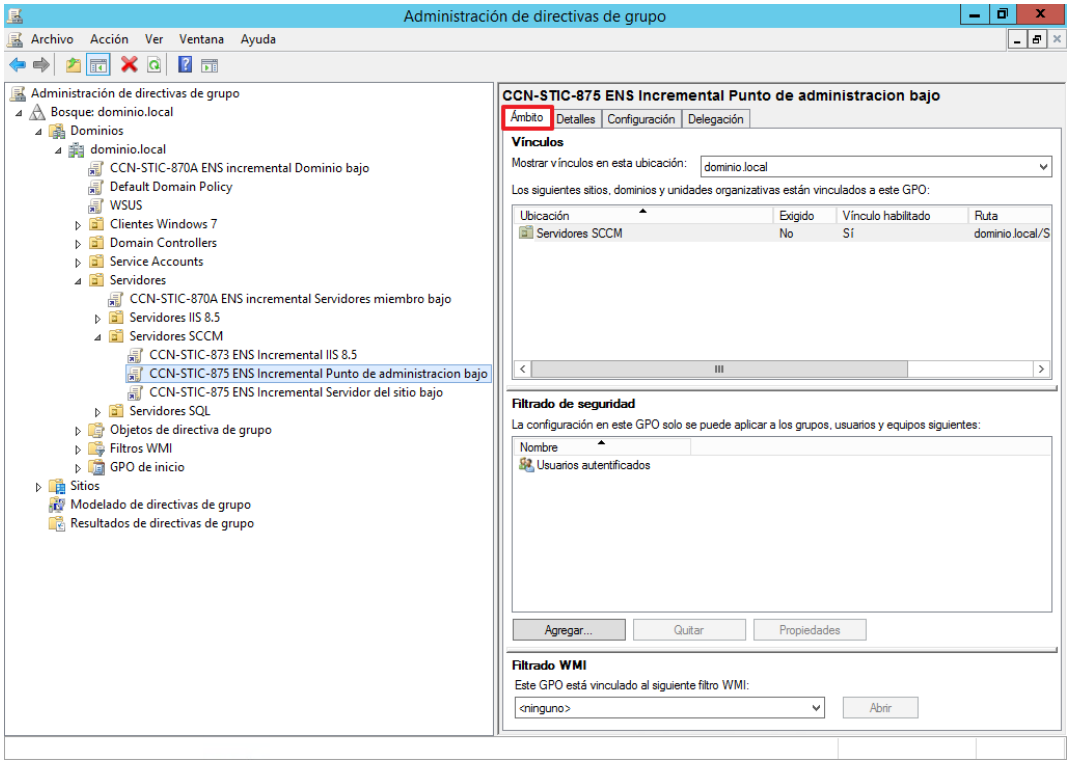
Paso	Descripción
100.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
101.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
102.	Agregue los equipos y pulse sobre “Aceptar”. 

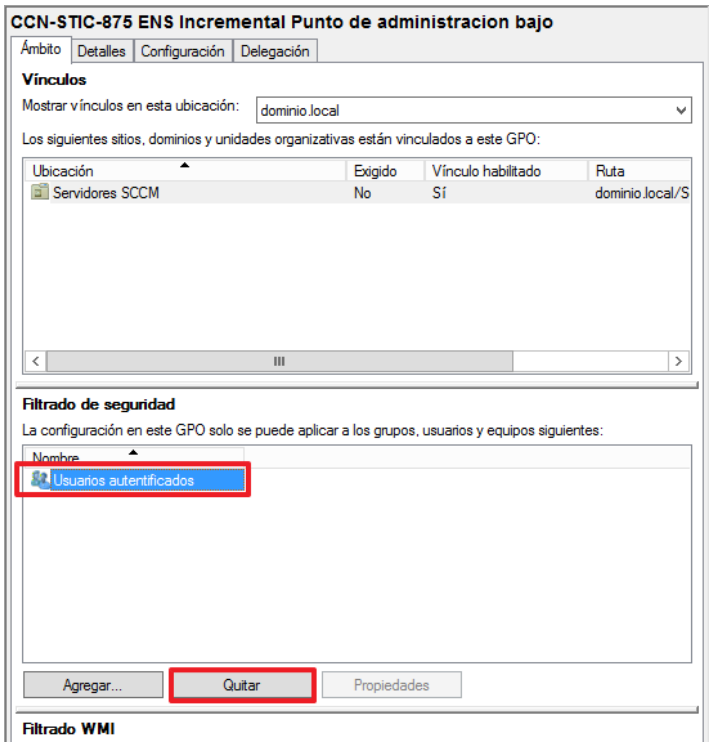
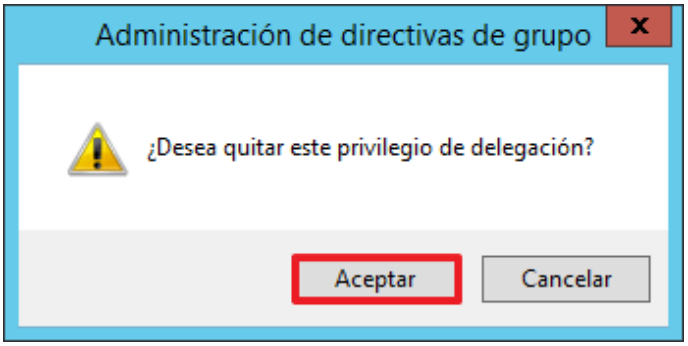
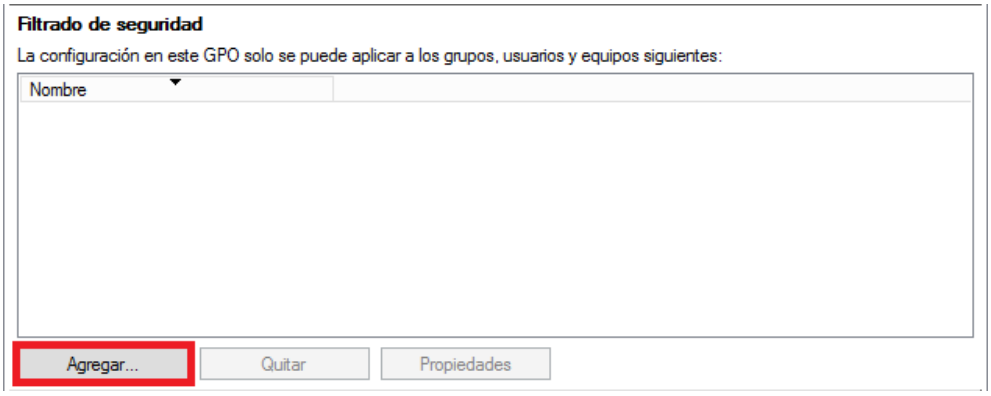
Paso	Descripción
103.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
104.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
105.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

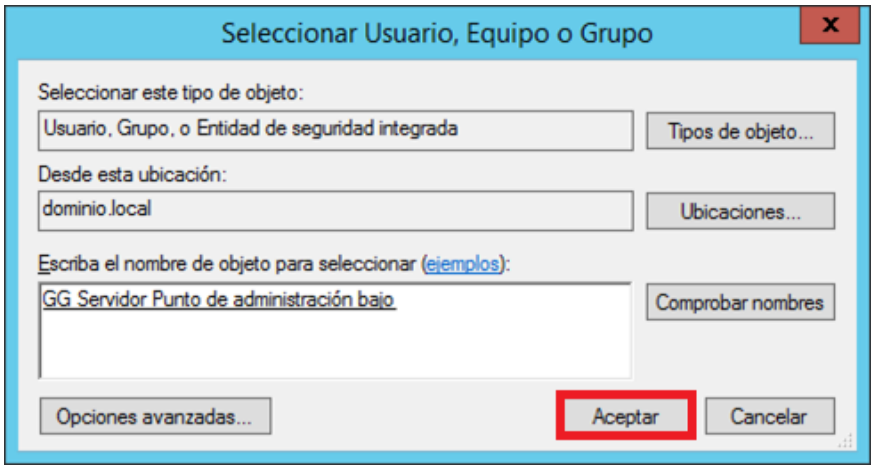
Paso	Descripción
106.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
107.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de administración bajo” y haga clic en el botón “Aceptar”. 
108.	En los siguientes pasos, se va a asociar la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” en la unidad organizativa “Servidores SCCM”, en caso de que ya haya vinculado la directiva en algún paso anterior, continúe con el paso 113, en caso contrario continúe con el siguiente paso.
109.	A continuación, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM.

Paso	Descripción
110.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
111.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre “Aceptar”. 

Paso	Descripción
112.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de administración bajo" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de administración bajo" y a continuación, haga clic sobre la flecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
113.	Edite la GPO: "CCN-STIC-875 ENS Incremental Punto de administración bajo" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
114.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
115.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Punto de administración bajo.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
116.	Cierre el “editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
117.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

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

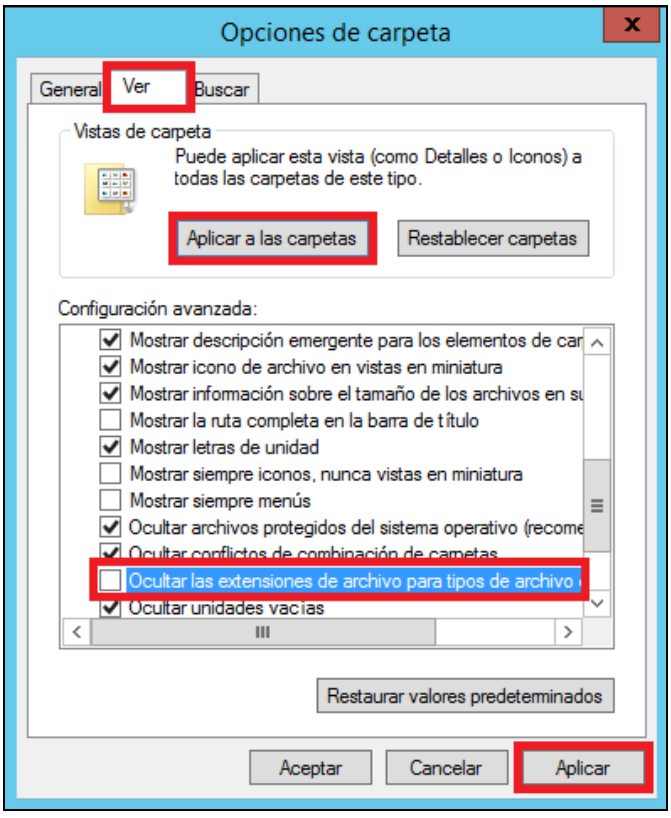
Paso	Descripción
121.	Introduzca como nombre “GG Servidor Punto de administración bajo” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
122.	Cierre el “Editor de administración de directivas de grupo”.

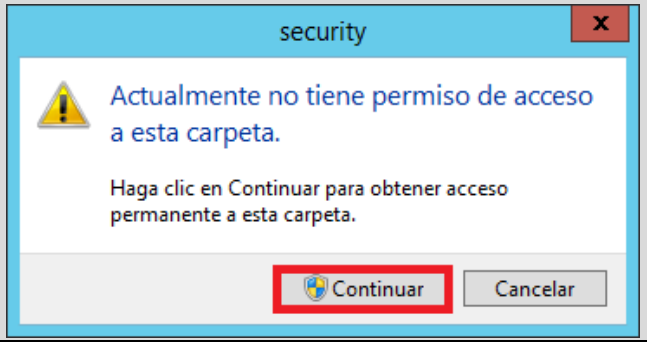
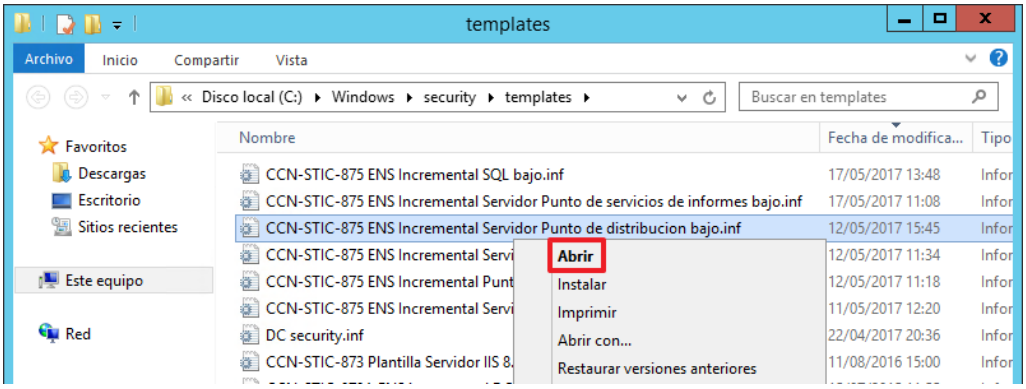
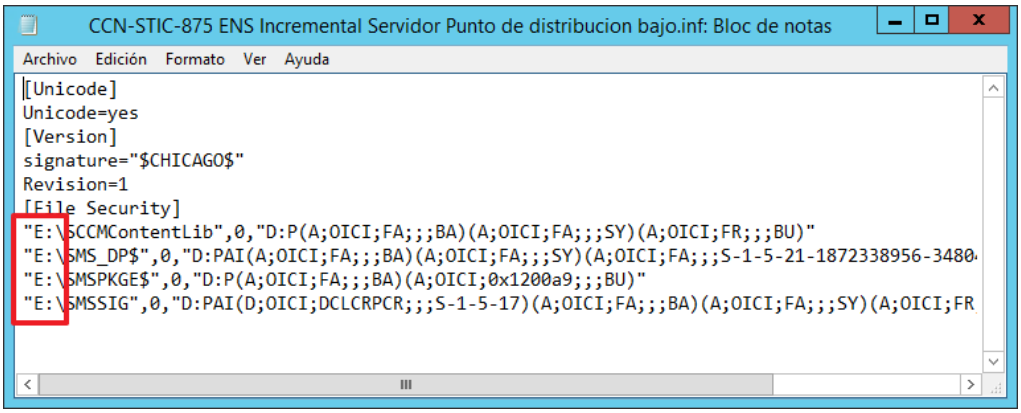
4. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE DISTRIBUCIÓN

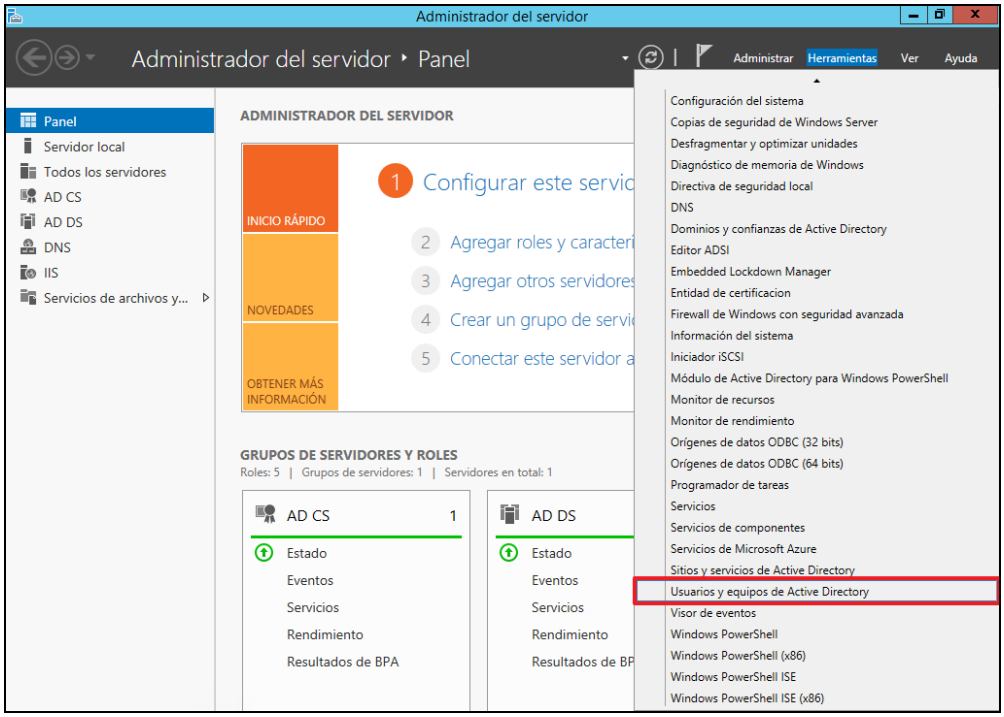
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de distribución implementado en el equipo.

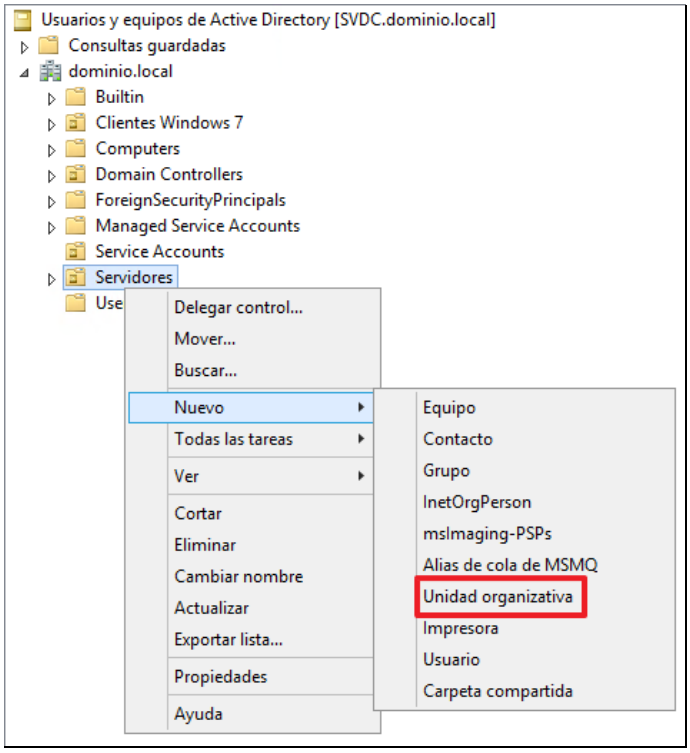
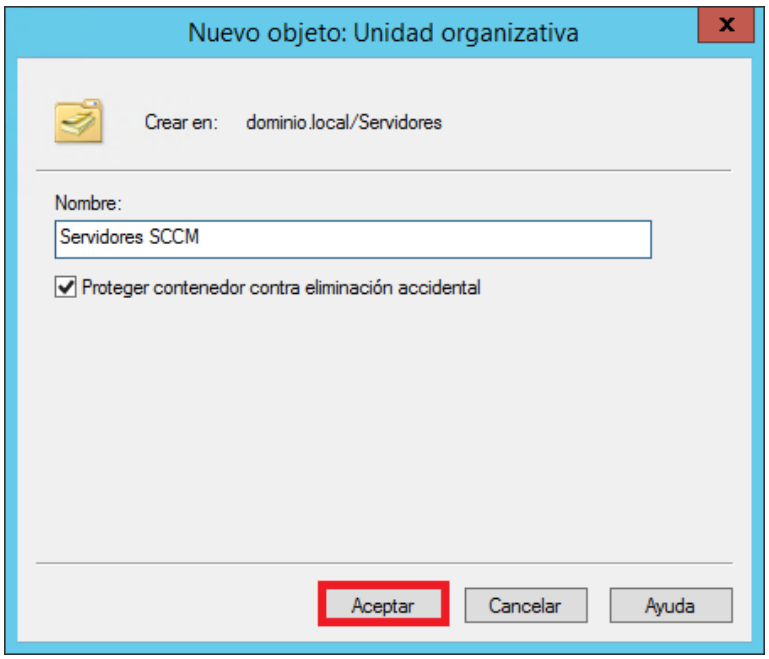
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

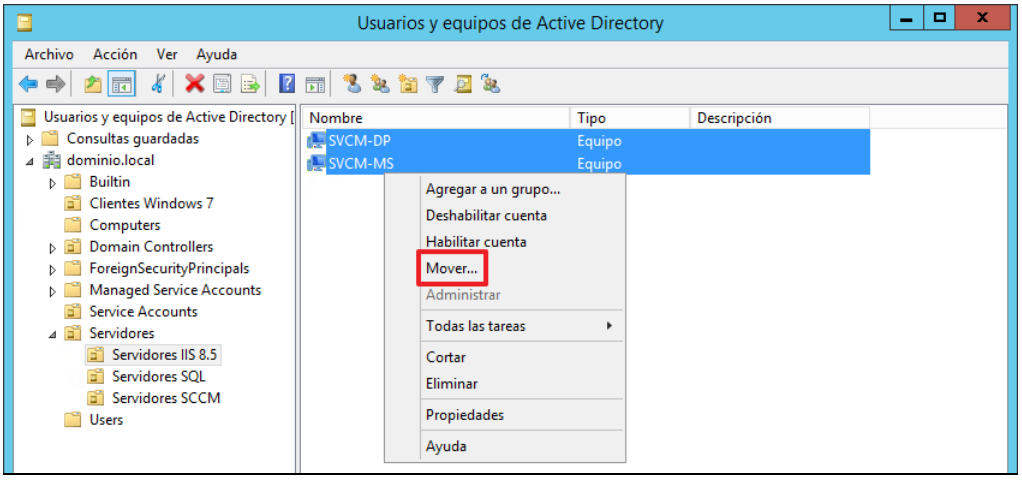
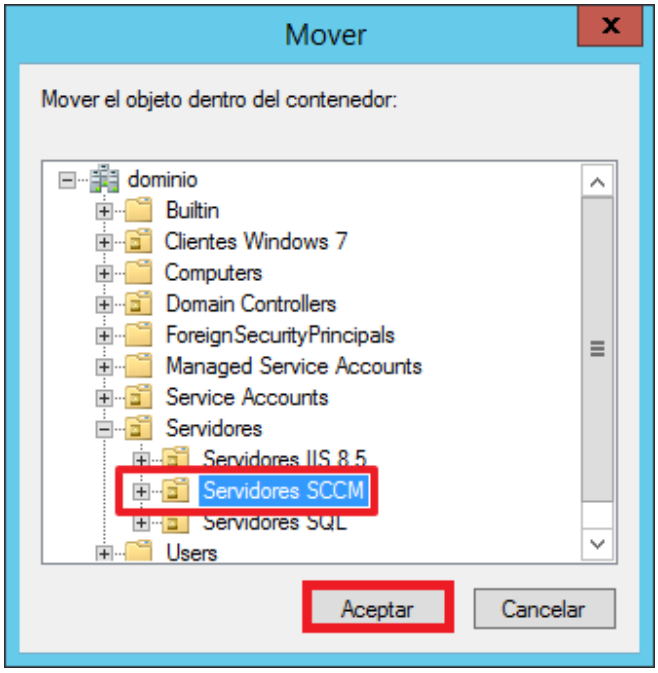
Paso	Descripción
123.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.

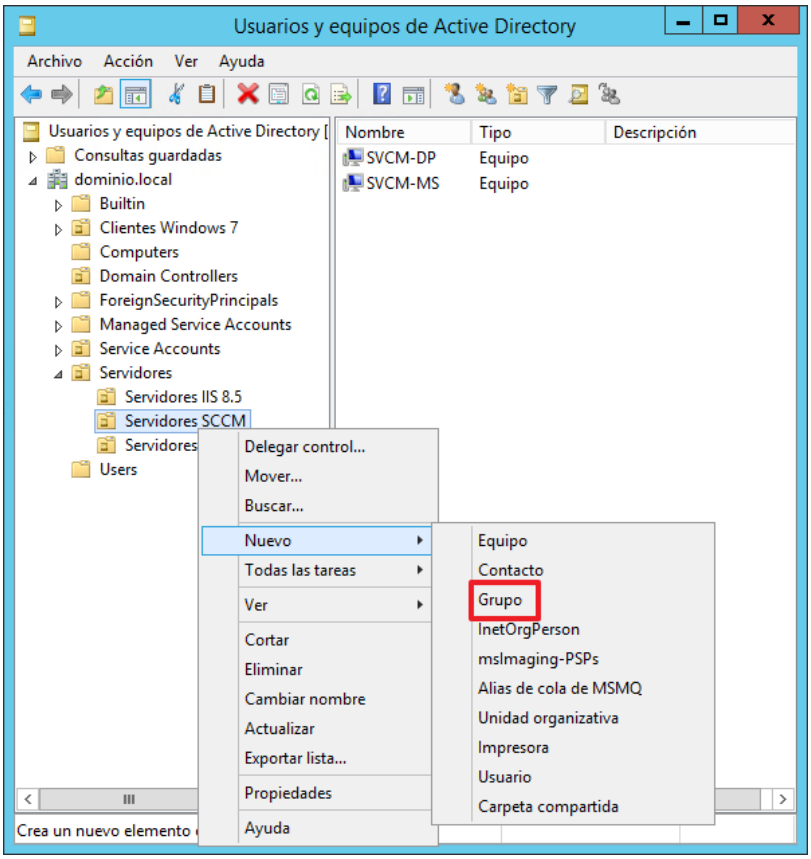
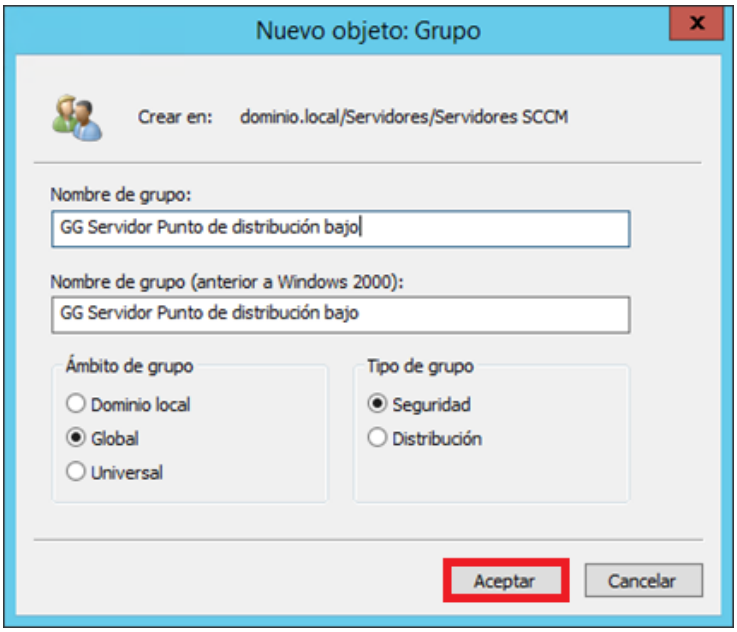
Paso	Descripción
124.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
125.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
126.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
127.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

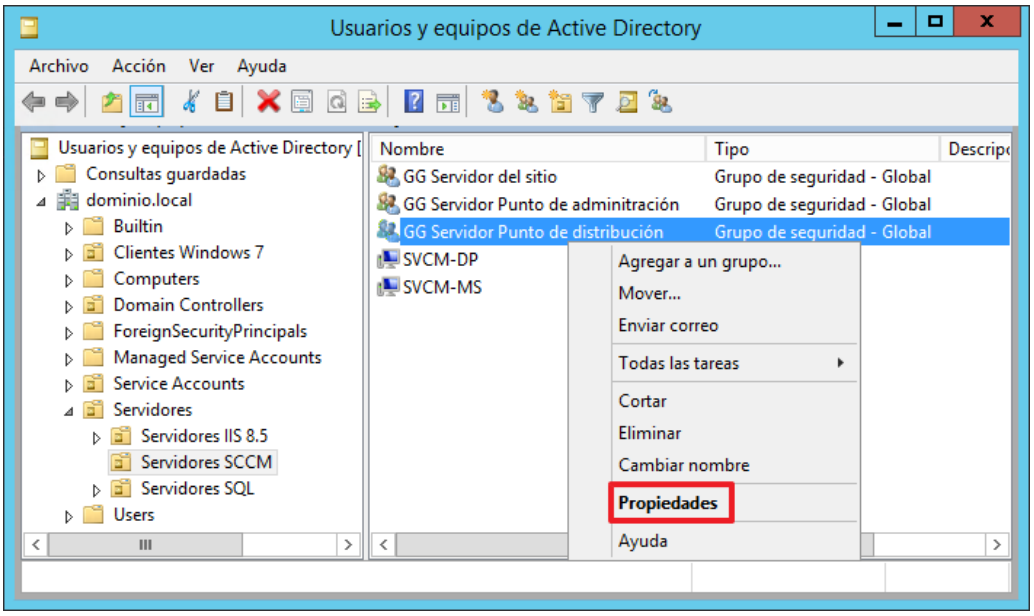
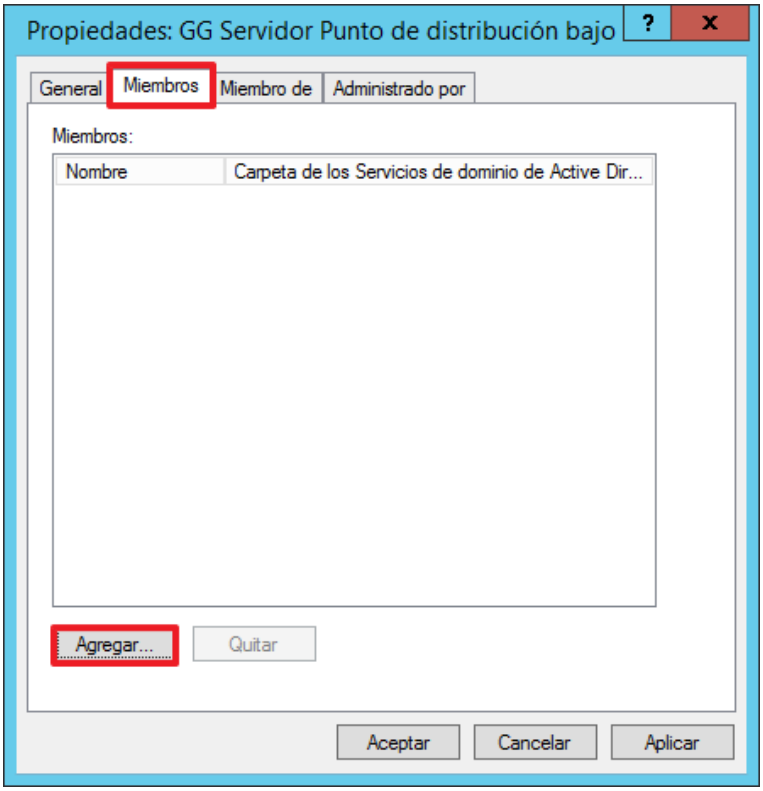
Paso	Descripción
128.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de distribución bajo.inf” que se encuentra en la ruta “C:\Scripts\Nivel Bajo” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
129.	Pulse con el botón derecho sobre el fichero y seleccione la opción “Abrir” del menú contextual. 
130.	Deberá modificar la ruta del fichero para adaptarlo a su organización, para ello localice la ruta de las carpetas sobre las que desea aplicar seguridad y modifíquela en función de la ruta de directorios de su organización.  **Nota:** Si no modifica este fichero los permisos establecidos en la presente guía no se aplicarán correctamente.

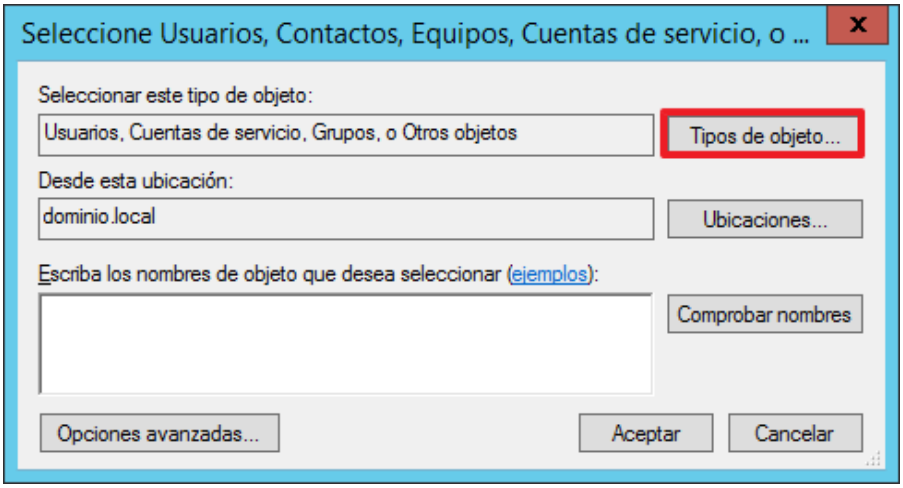
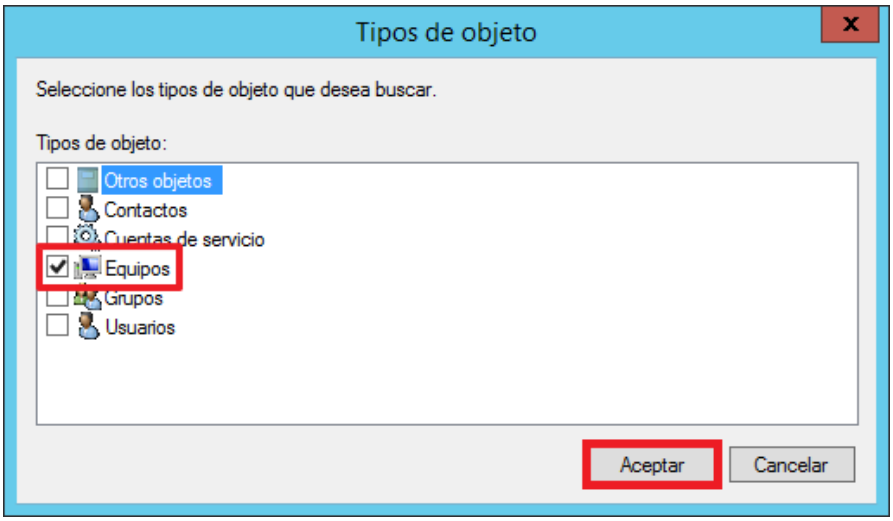
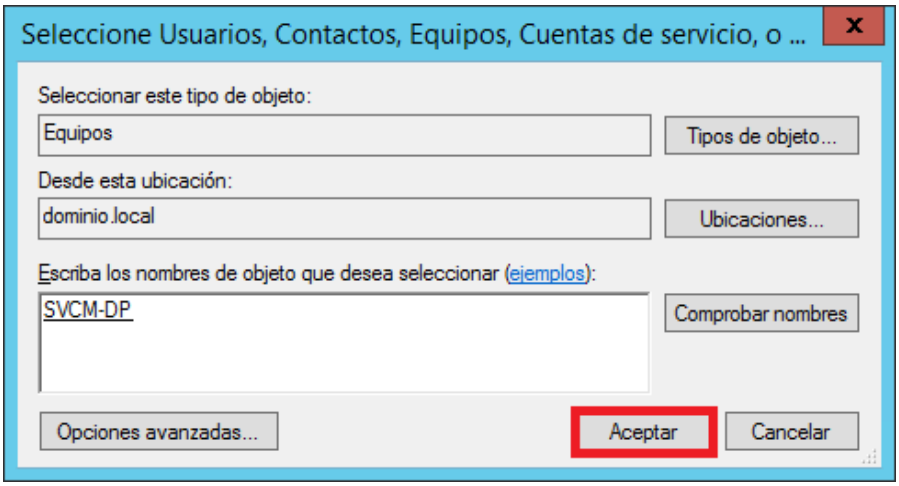
Paso	Descripción
131.	Guarde los cambios realizados y cierre el documento.
132.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**.  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .
133.	El siguiente proceso va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 138. En caso contrario continúe con el paso a paso.

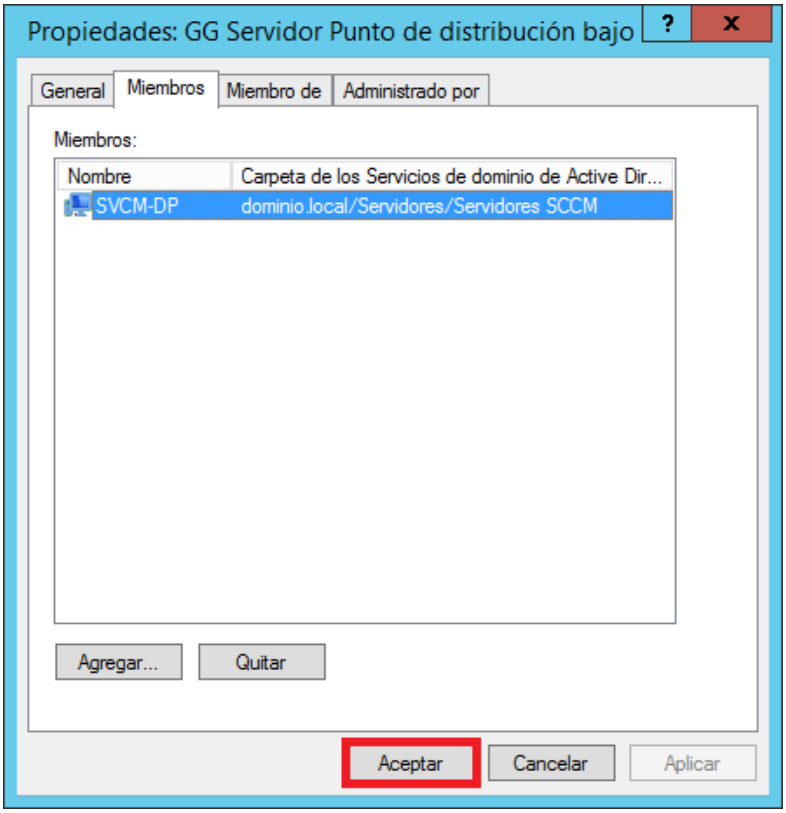
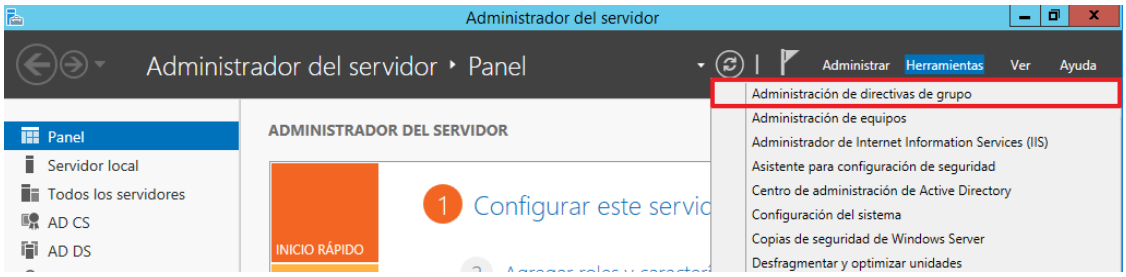
Paso	Descripción
134.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
135.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen, maque en “Aceptar”. 

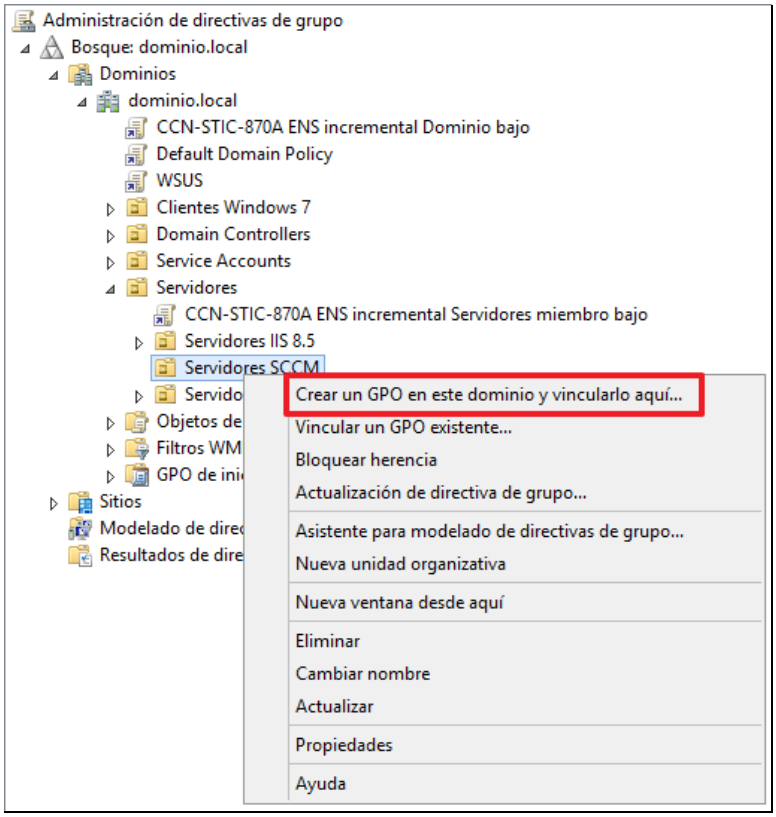
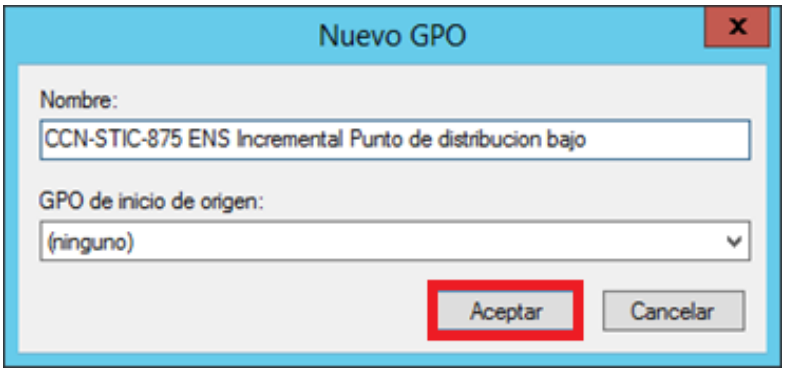
Paso	Descripción
136.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
137.	Marque sobre la unidad organizativa “Servidores SCCM” y pulse en “Aceptar”. 

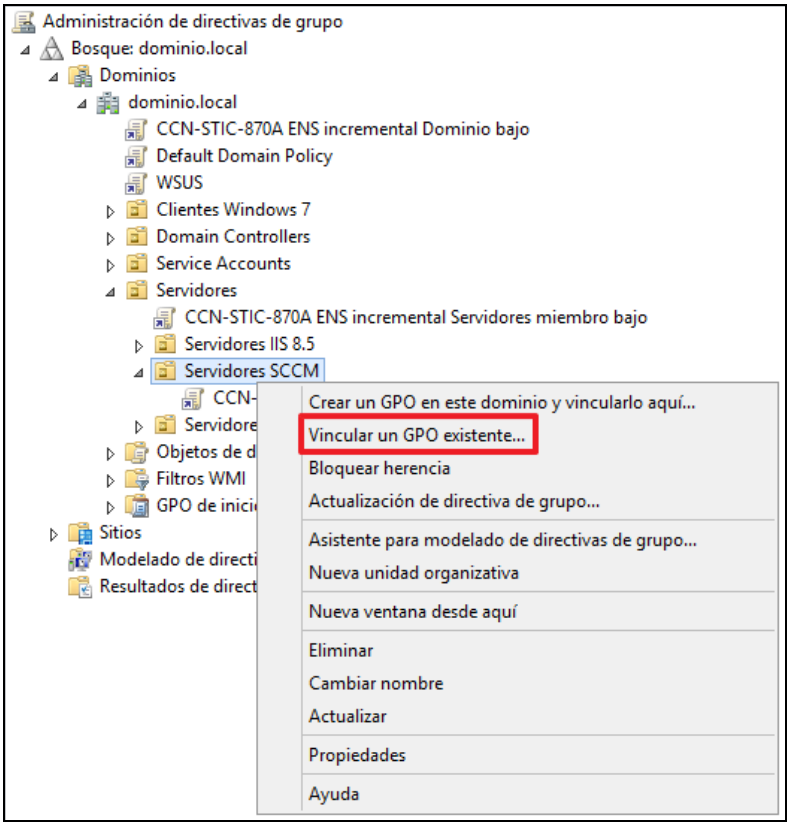
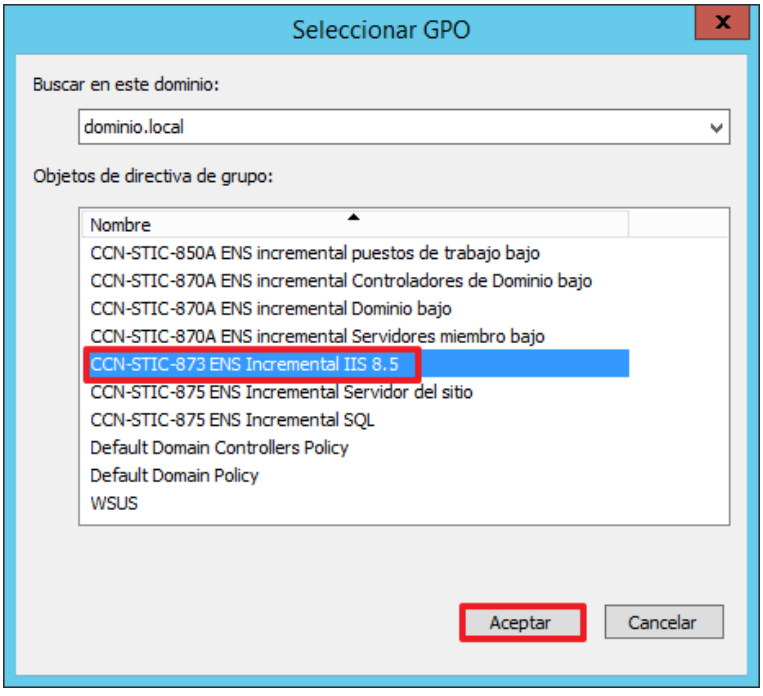
Paso	Descripción
138.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
139.	Escriba el nombre “GG Servidor Punto de distribución bajo” y pulse “Aceptar”. 

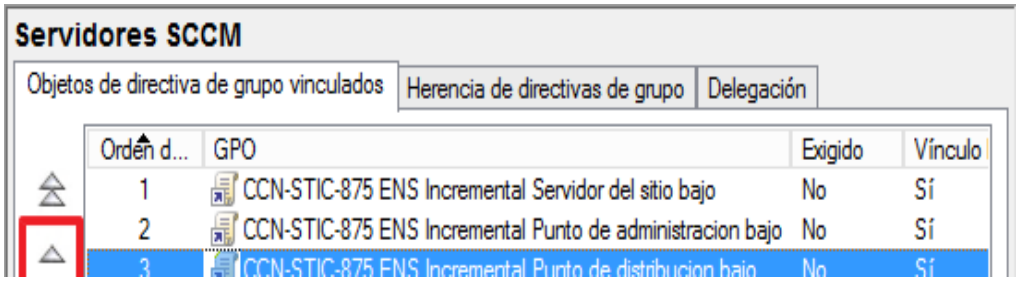
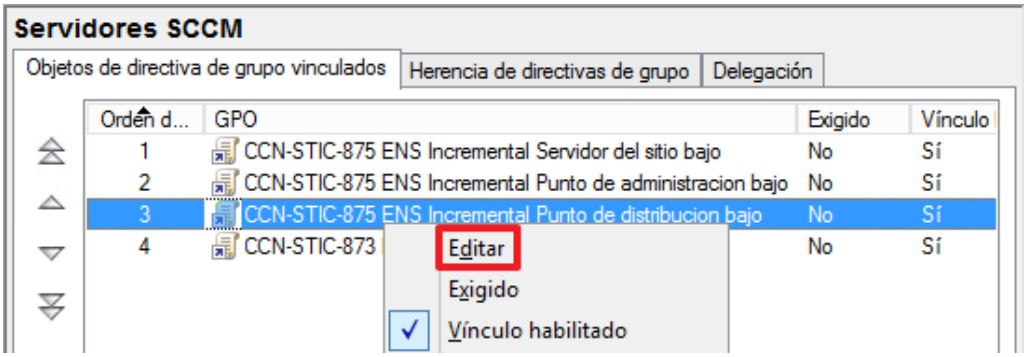
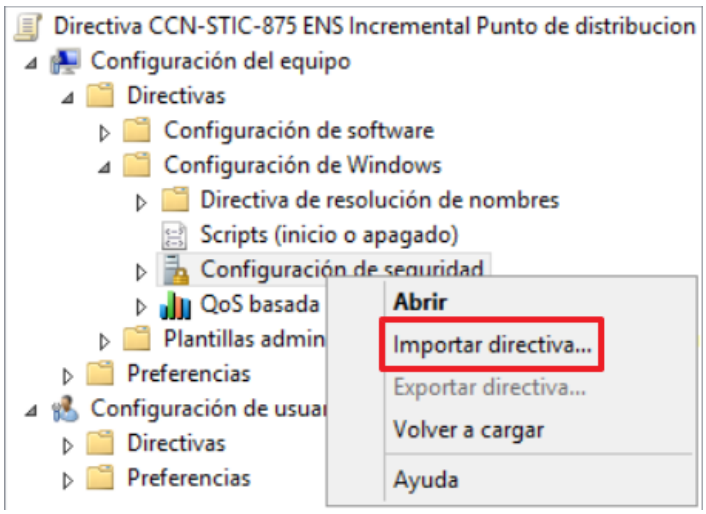
Paso	Descripción
140.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
141.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de distribución” al grupo. 

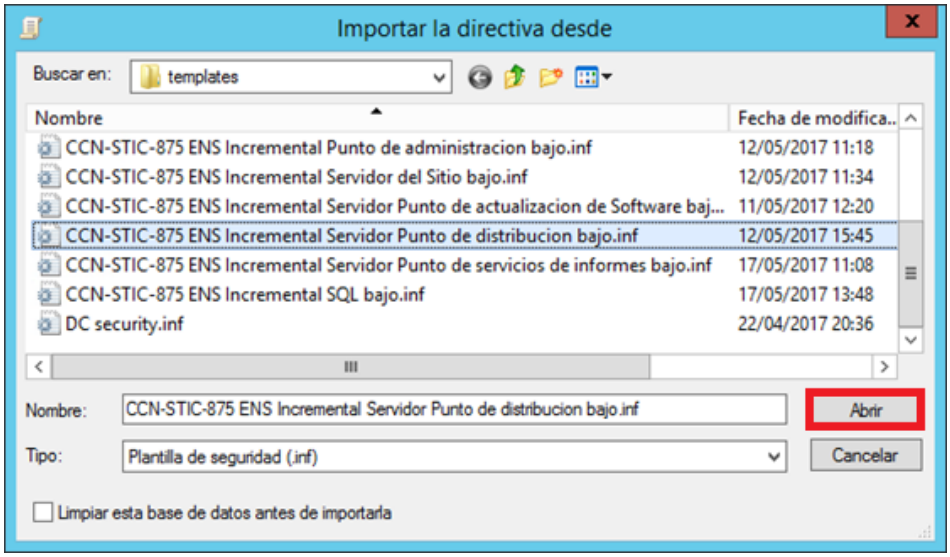
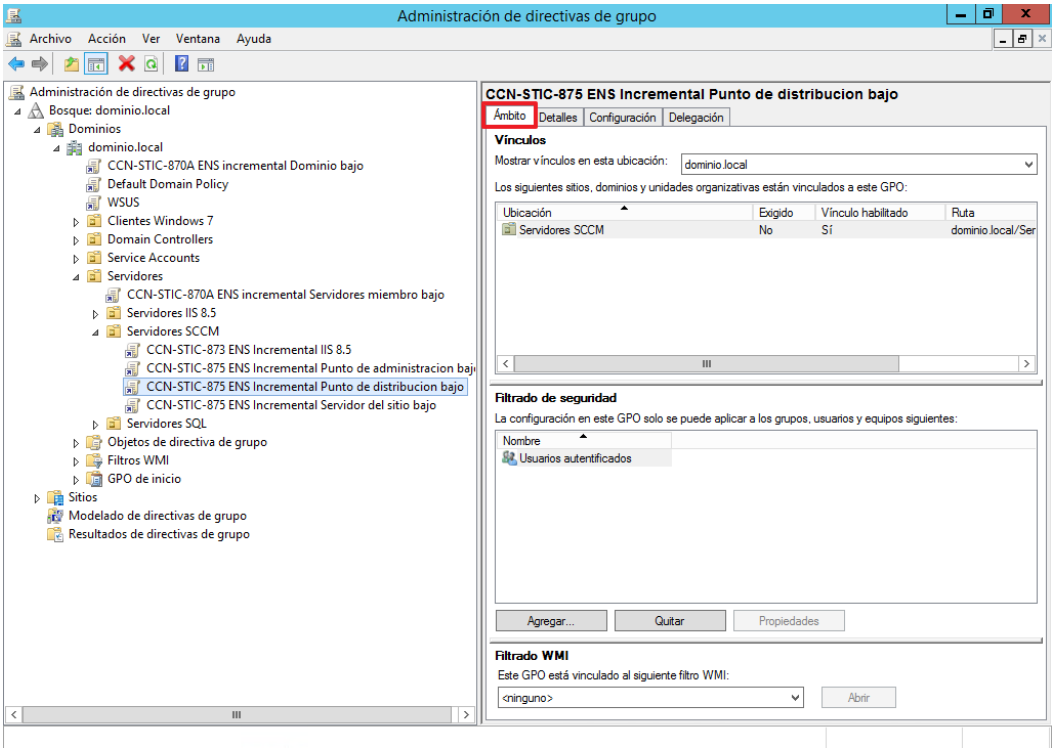
Paso	Descripción
142.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
143.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
144.	Agregue los equipos y pulse sobre “Aceptar”. 

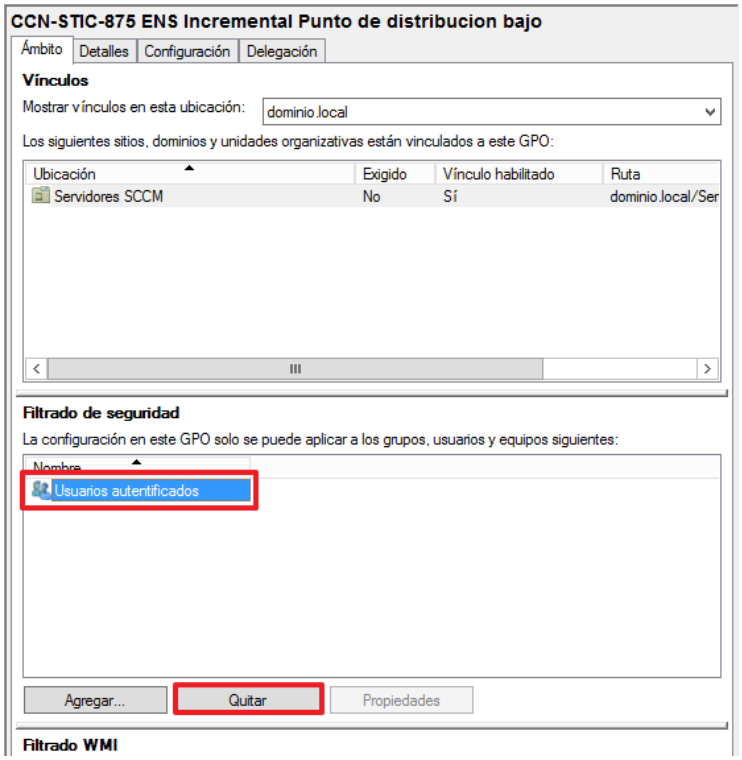
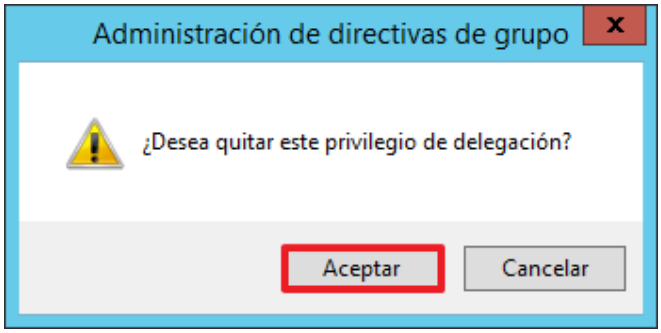
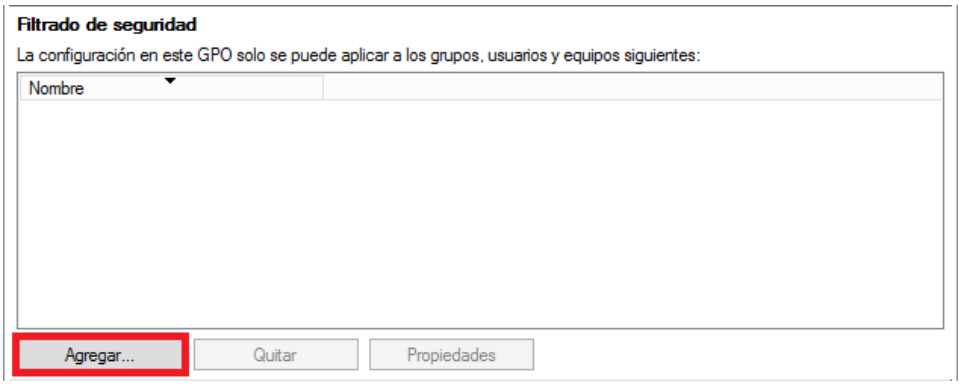
Paso	Descripción
145.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
146.	Cierre la herramienta de “Usuarios y equipos de Active Directory”.
147.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”.**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

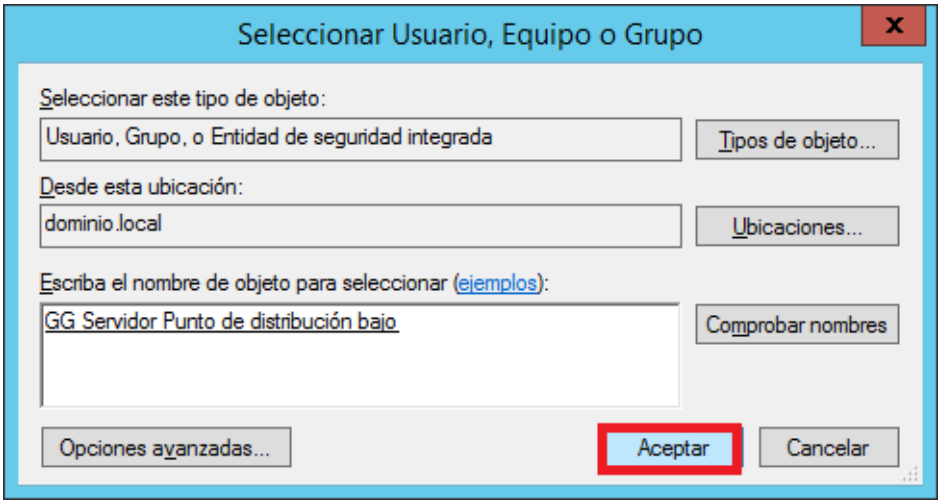
Paso	Descripción
148.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
149.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de distribución bajo” y haga clic en el botón “Aceptar”. 
150.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”. En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 155, en caso contrario continúe con el paso a paso.
151.	A continuación, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM.

Paso	Descripción
152.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
153.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
154.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de distribución bajo" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de distribución bajo" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
155.	Edite la GPO: "CCN-STIC-875 ENS Incremental Punto de distribución bajo" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
156.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
157.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de distribución bajo.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
158.	Cierre el "Editor de administración de directivas de grupo" una vez que se haya realizado la importación de la configuración de seguridad.
159.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

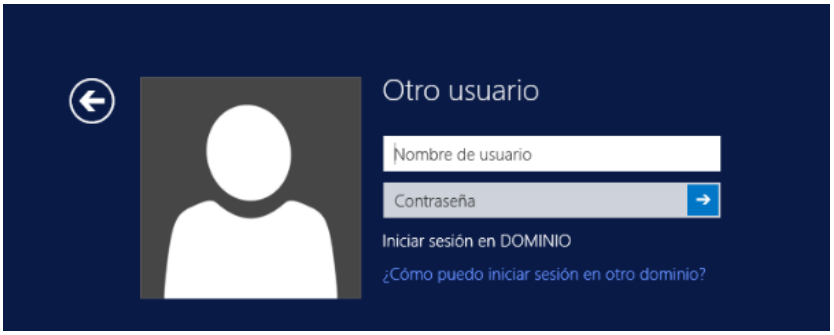
Paso	Descripción
160.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
161.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
162.	Una vez quitado, pulse el botón “Agregar…”. 

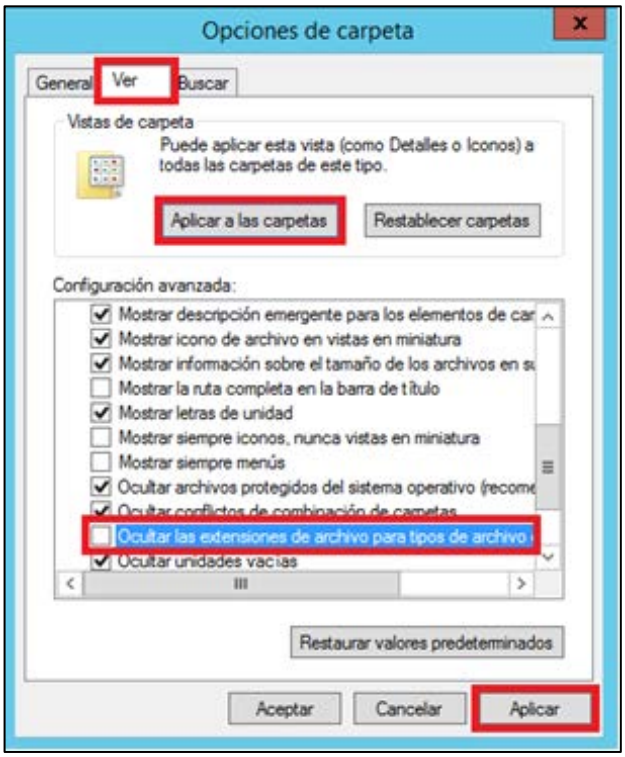
Paso	Descripción
163.	Introduzca como nombre “GG Servidor Punto de distribución bajo” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
164.	Cierre el “Editor de administración de directivas de grupo”.

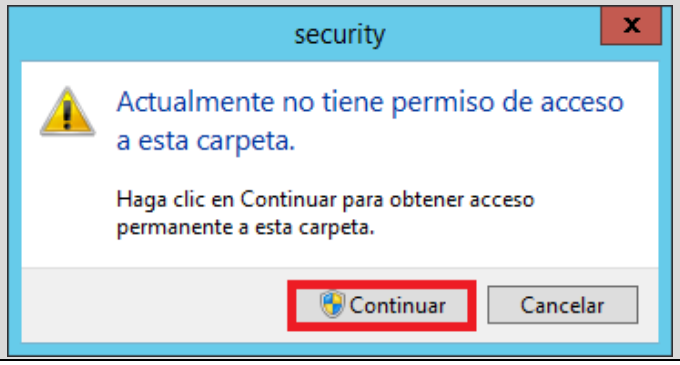
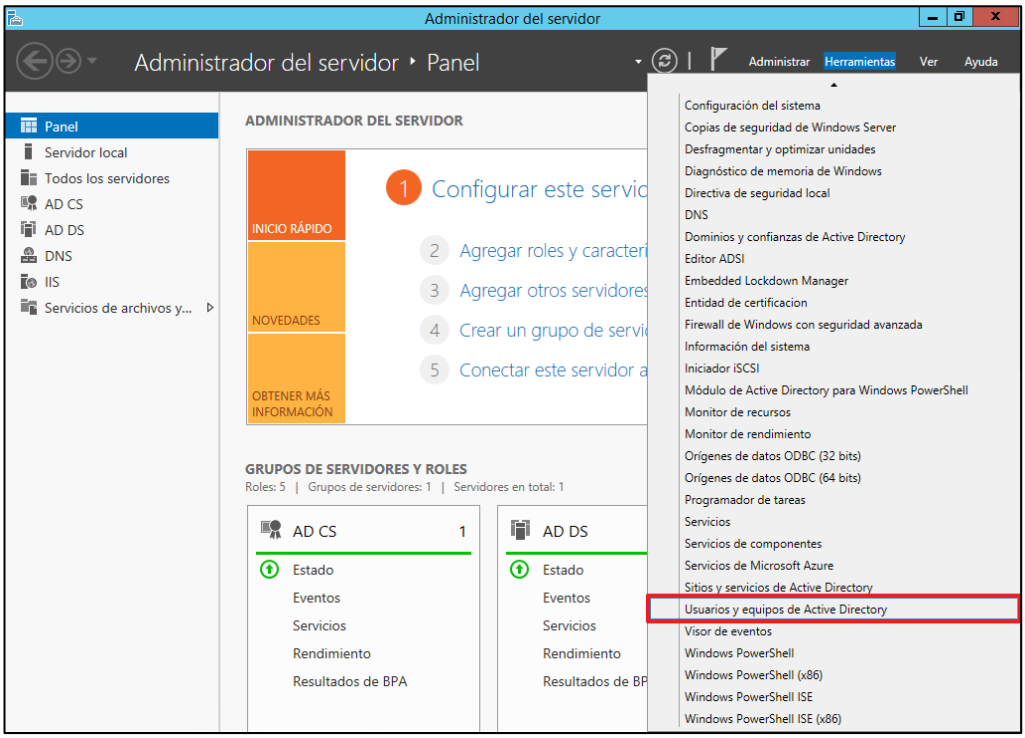
5. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE ACTUALIZACIÓN DE SOFTWARE

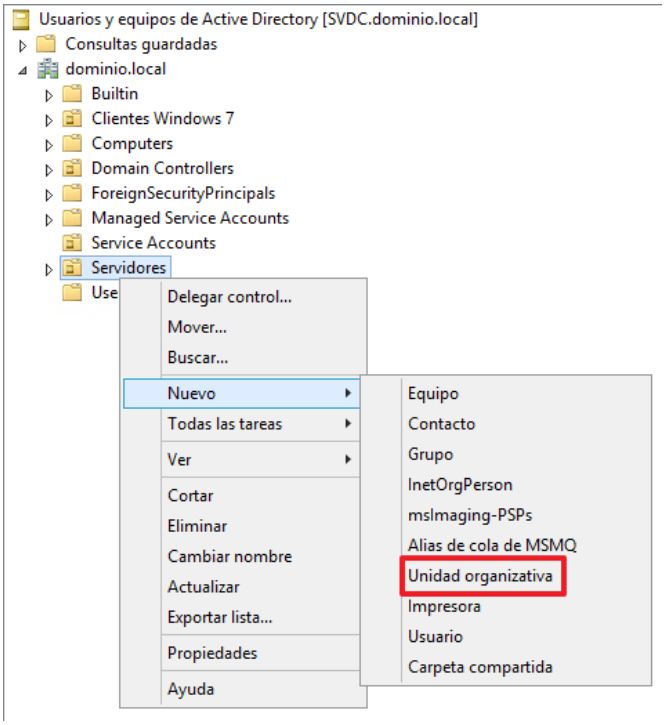
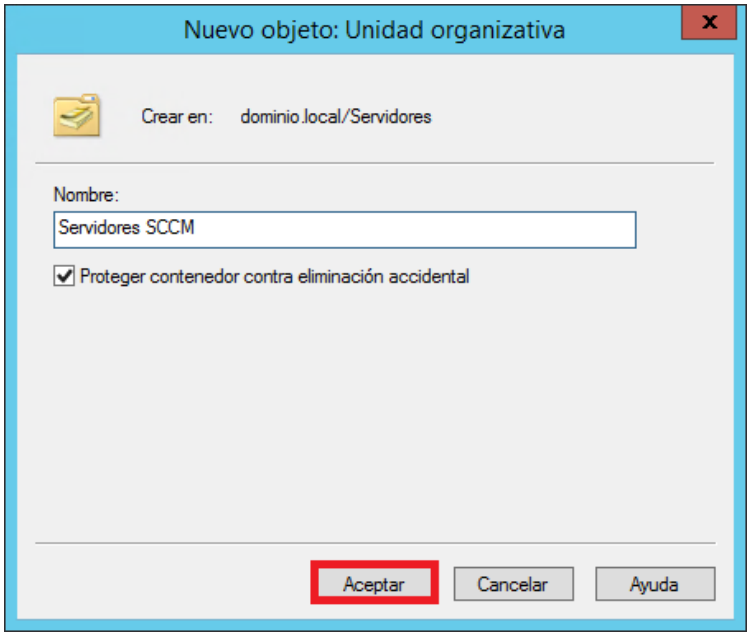
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de actualización de software implementado en el equipo.

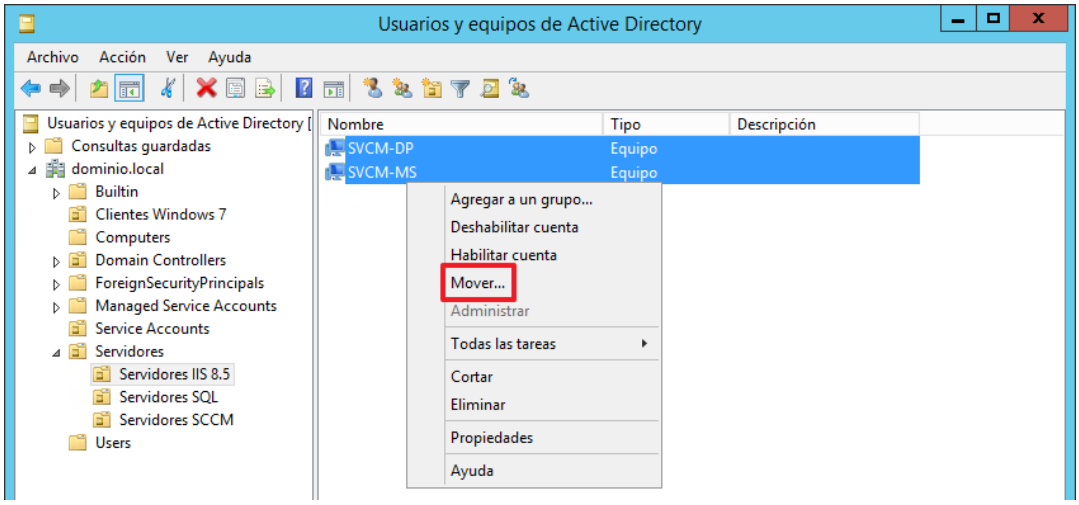
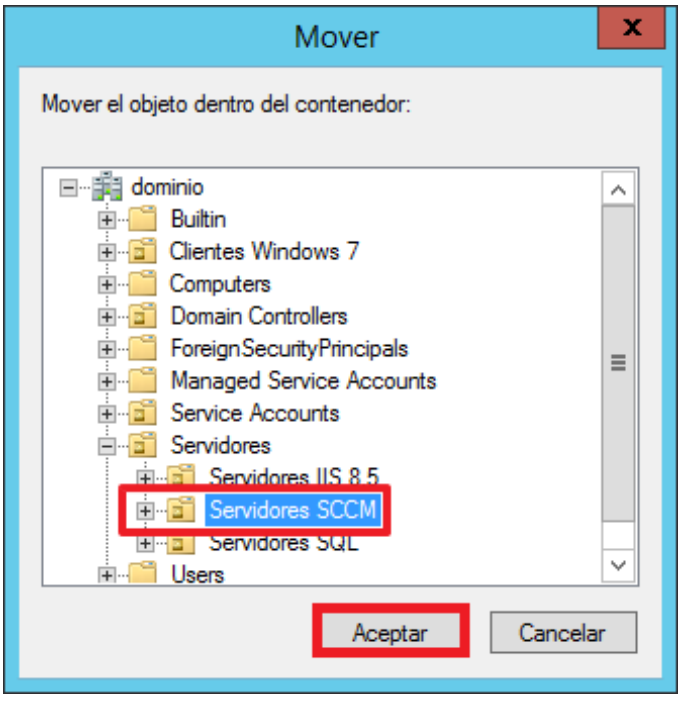
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

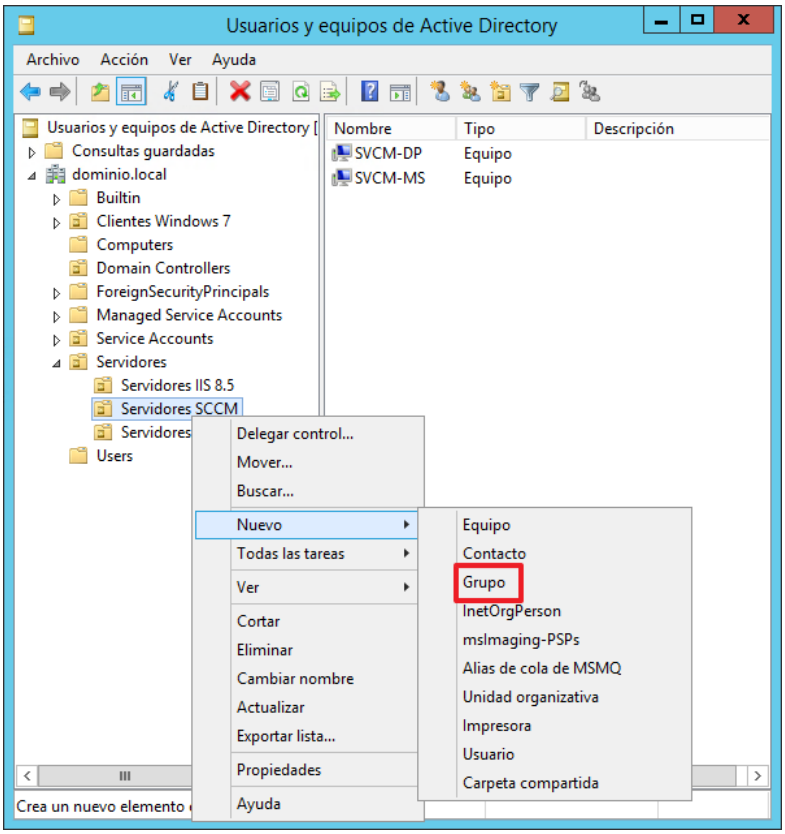
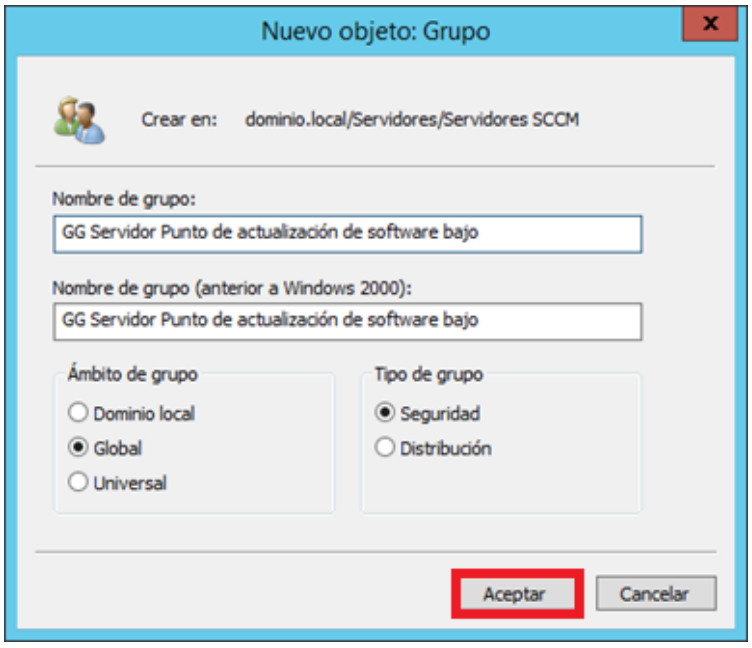
Paso	Descripción
165.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.

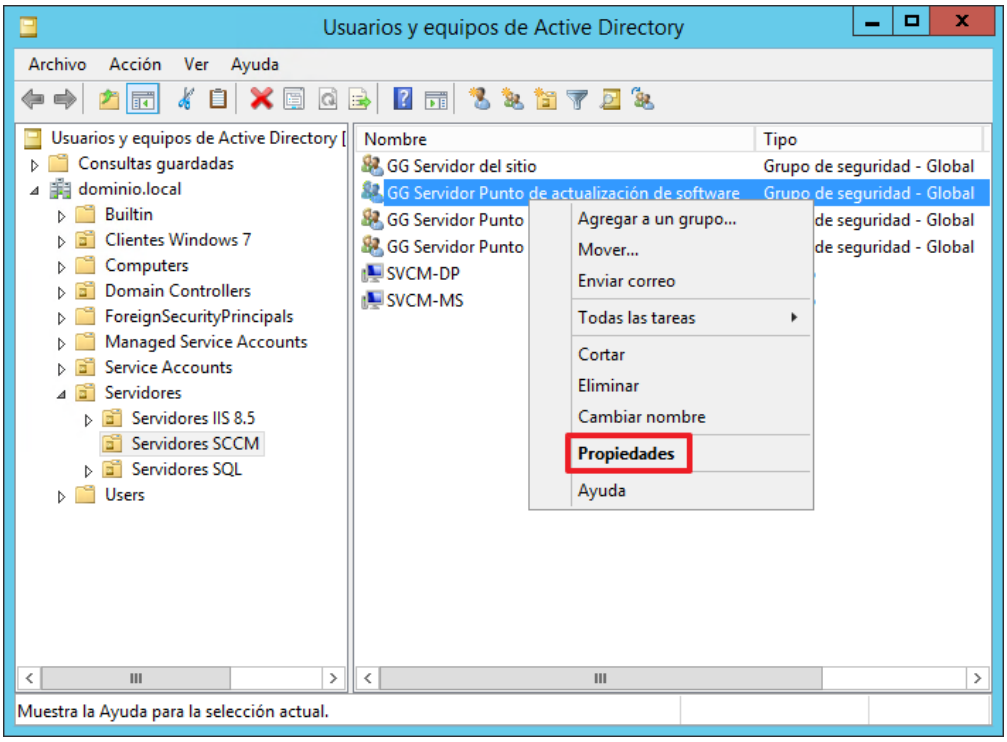
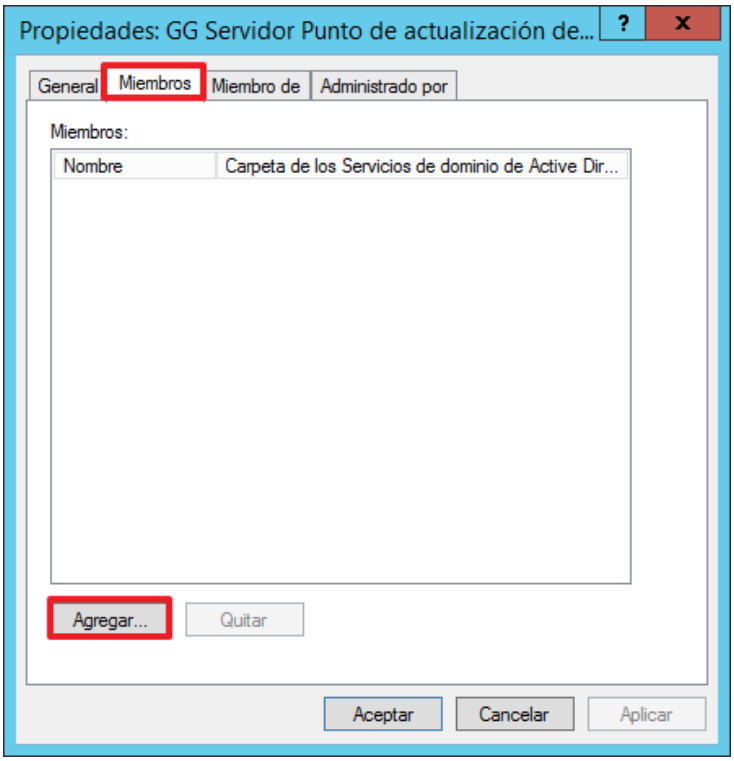
Paso	Descripción
166.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
167.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
168.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
169.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

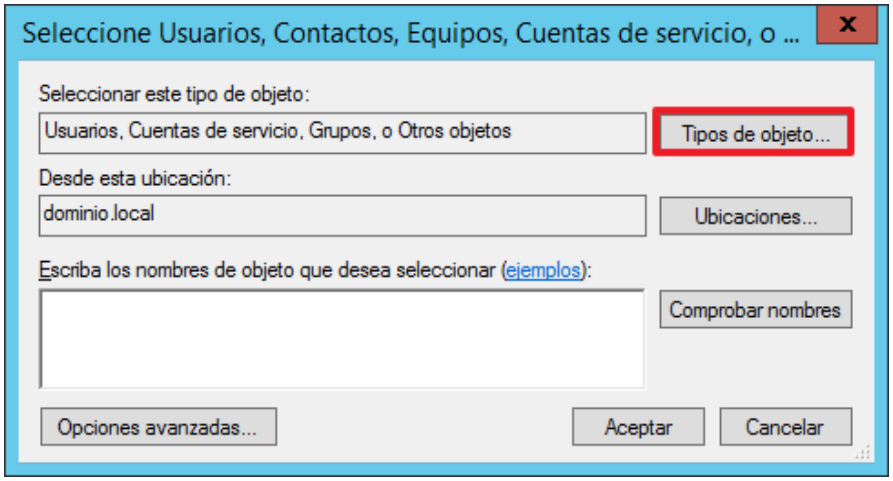
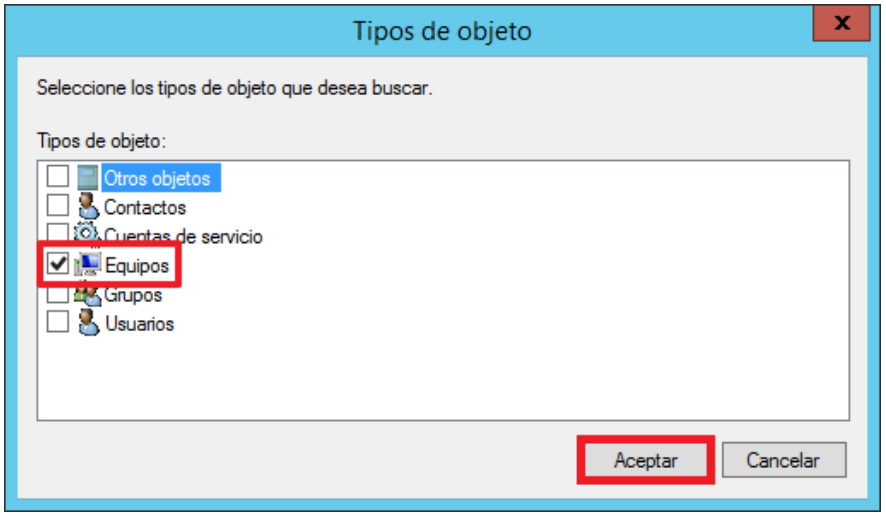
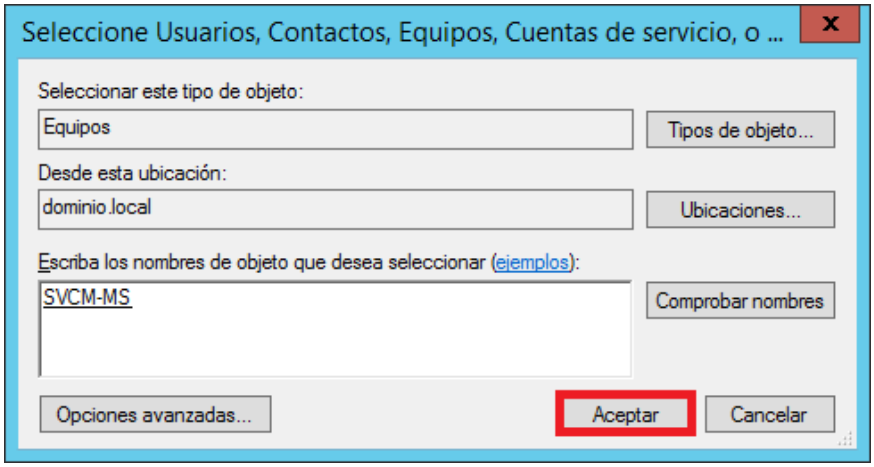
Paso	Descripción
170.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de actualización de software bajo.inf” que se encuentra en la ruta “C:\Scripts\Nivel Bajo” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
171.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

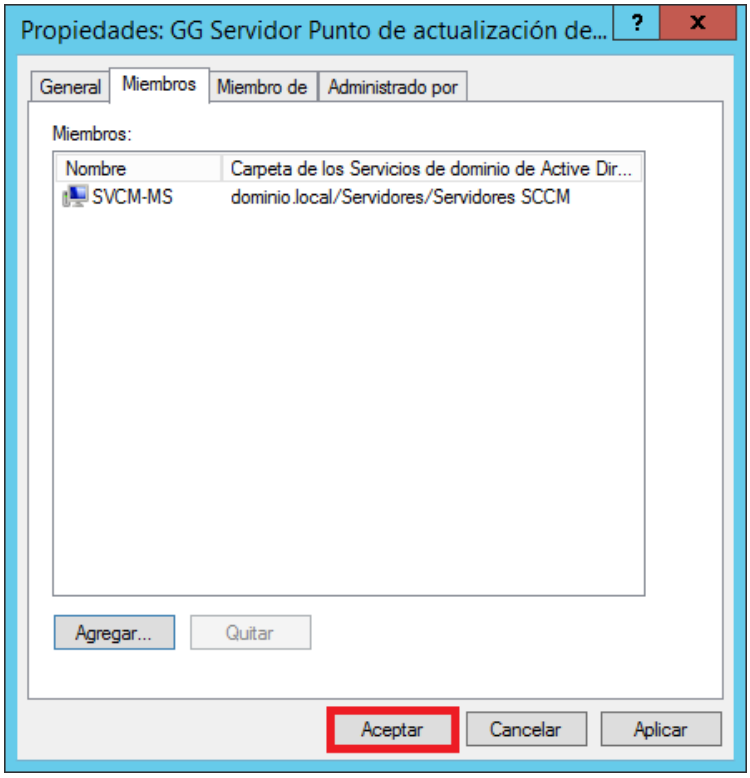
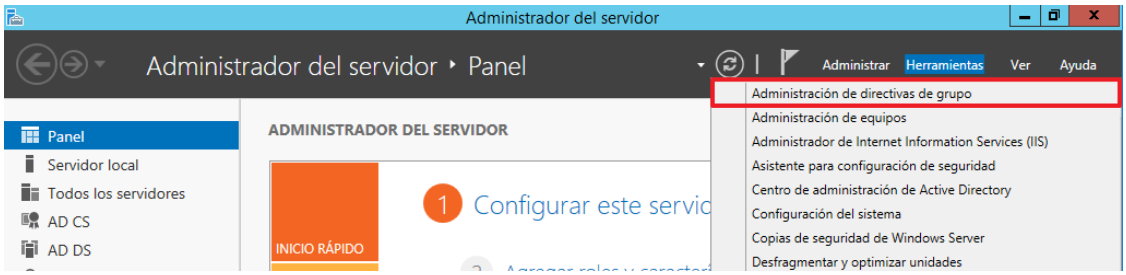
Paso	Descripción
172.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 177. En caso contrario continúe con el paso a paso.
173.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
174.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen, marque en el botón “Aceptar”. 

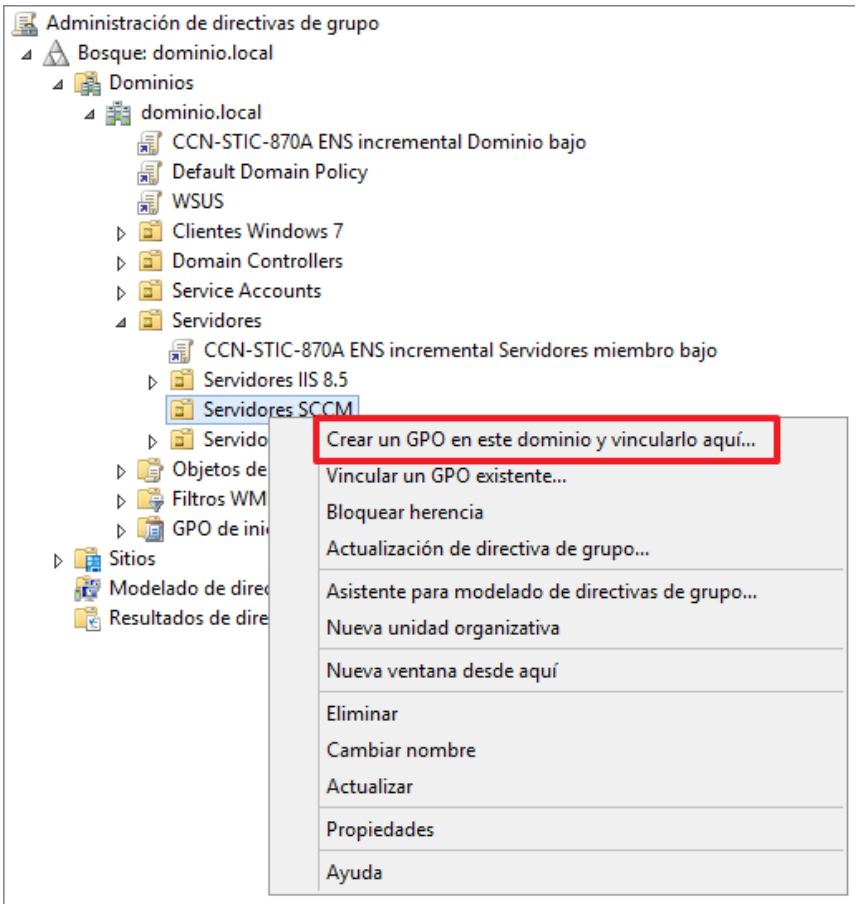
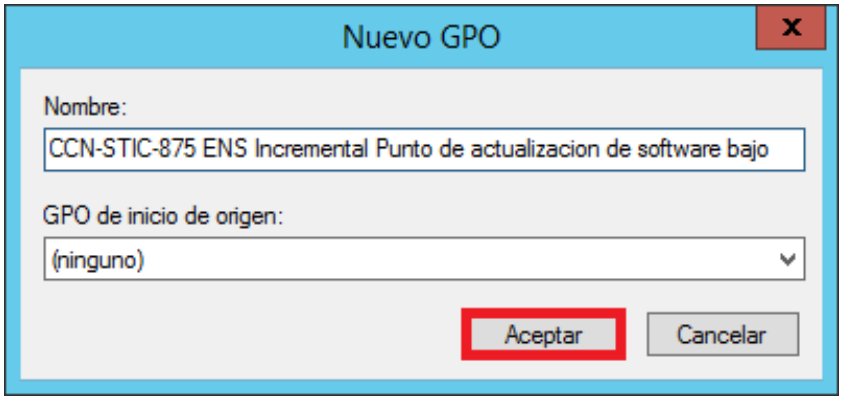
Paso	Descripción
175.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
176.	Marque sobre la unidad organizativa “Servidores SCCM” y pulse en “Aceptar”. 

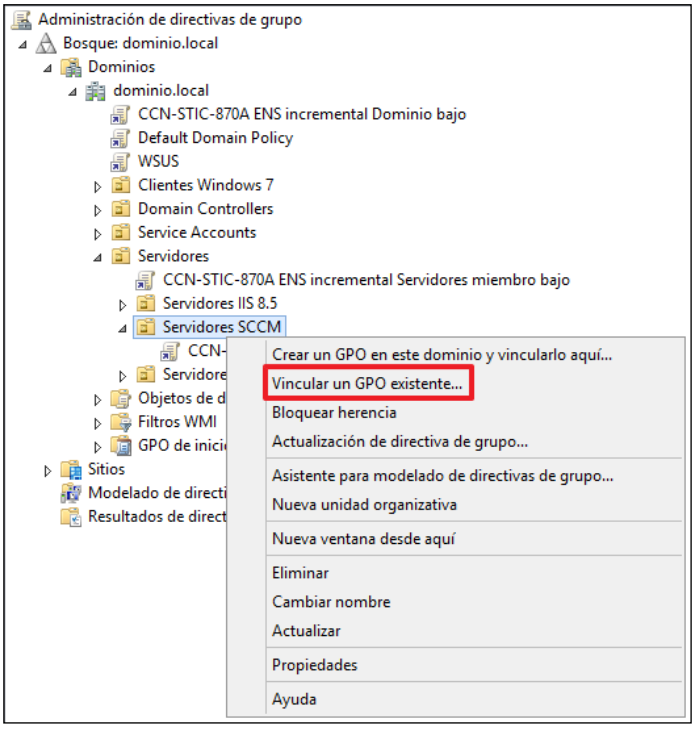
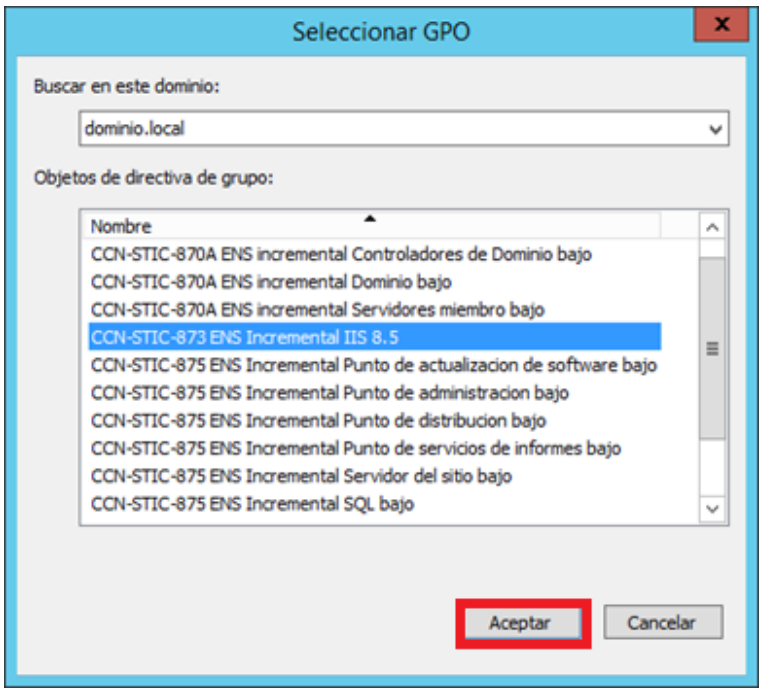
Paso	Descripción
177.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
178.	Escriba el nombre “GG Servidor Punto de actualización de software bajo” y pulse “Aceptar”. 

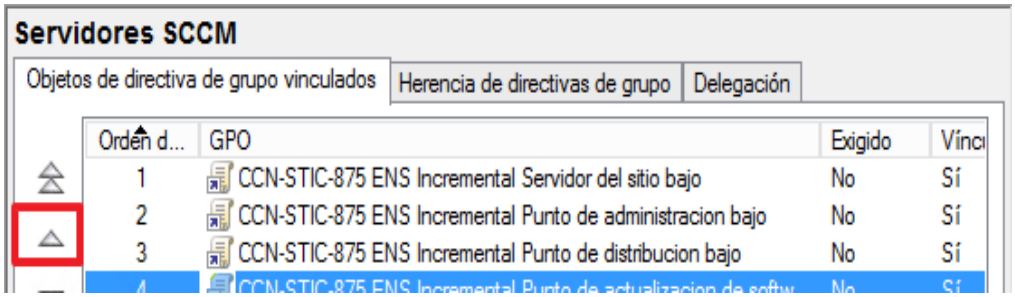
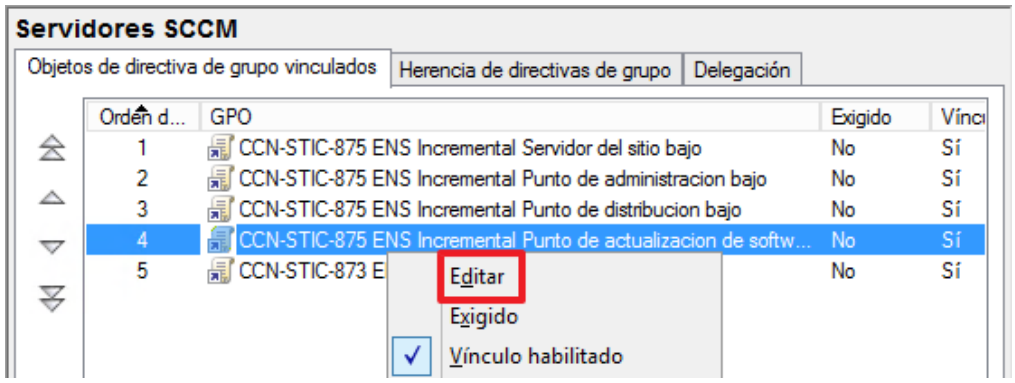
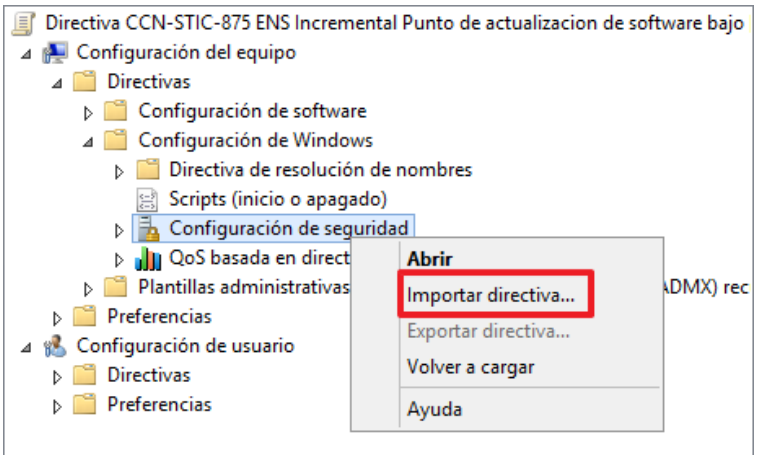
Paso	Descripción
179.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
180.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de actualización de software” al grupo. 

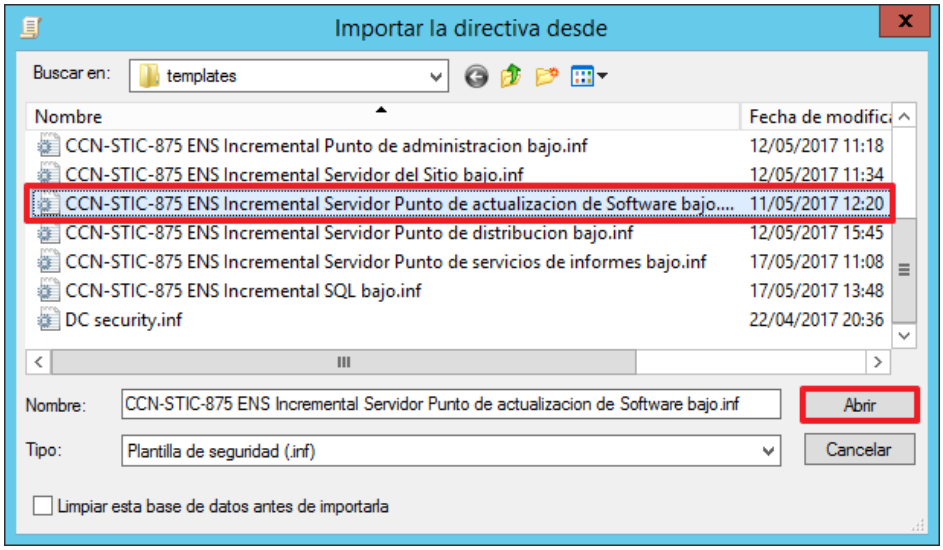
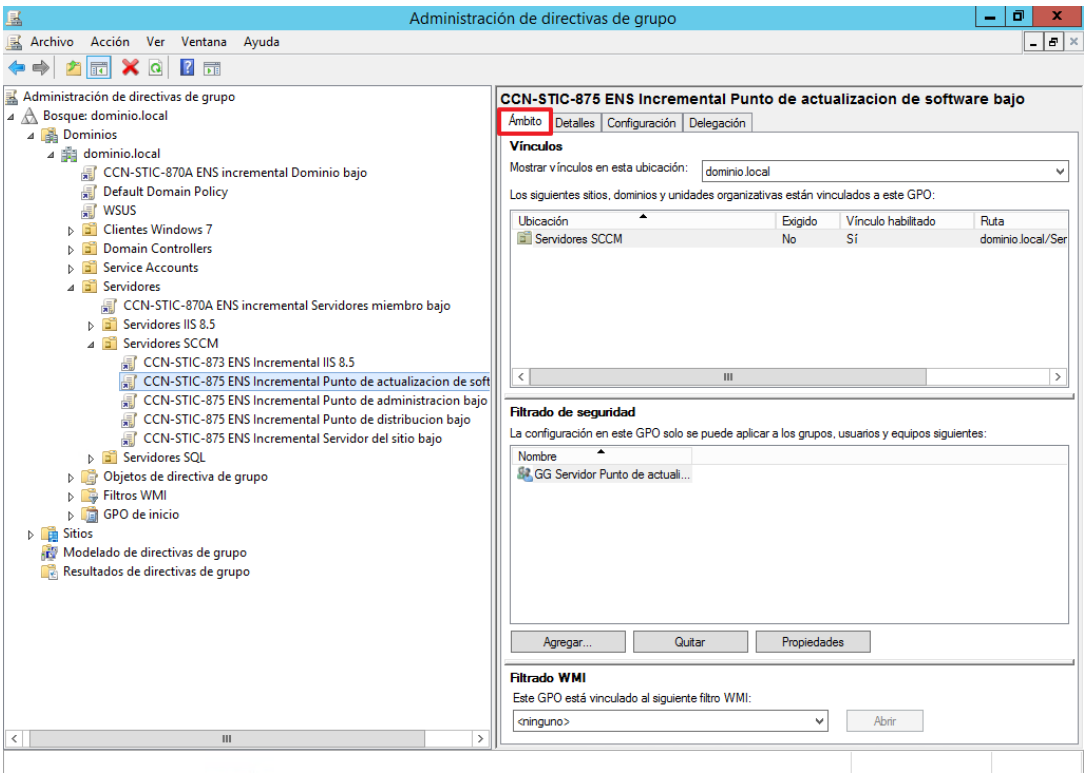
Paso	Descripción
181.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
182.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
183.	Agregue los equipos y pulse sobre “Aceptar”. 

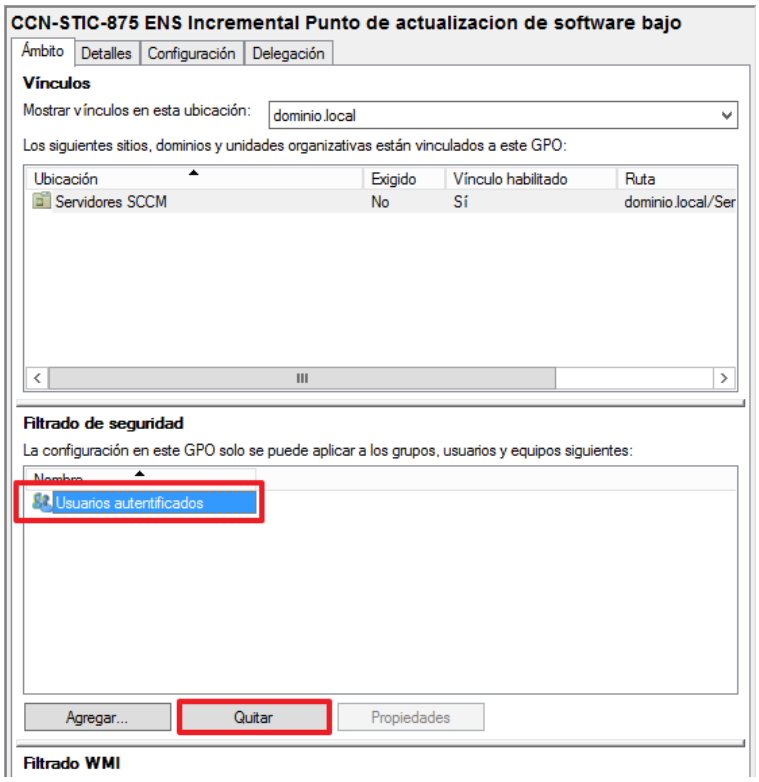
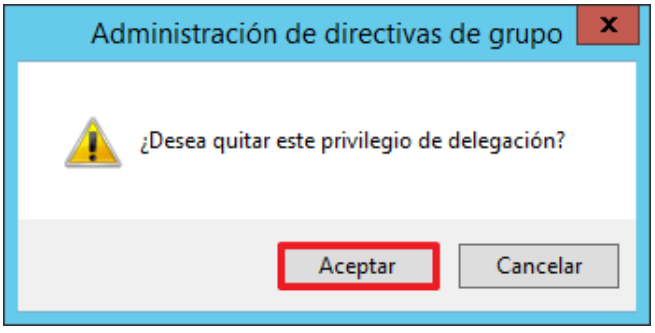
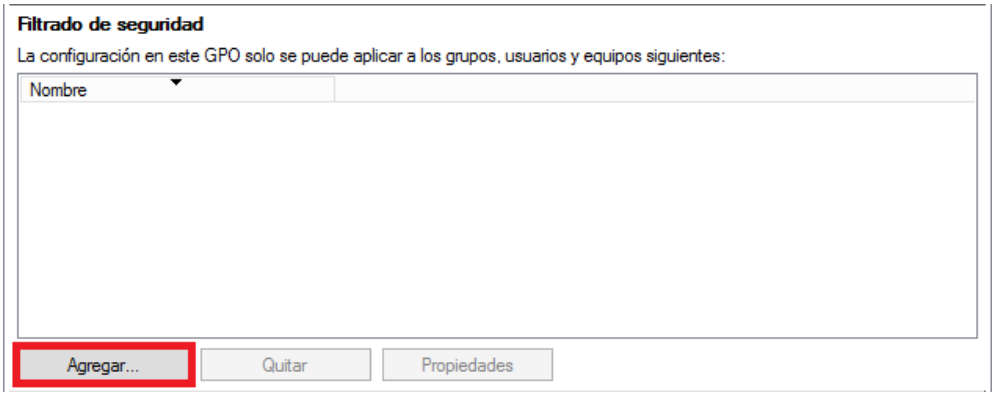
Paso	Descripción
184.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
185.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
186.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

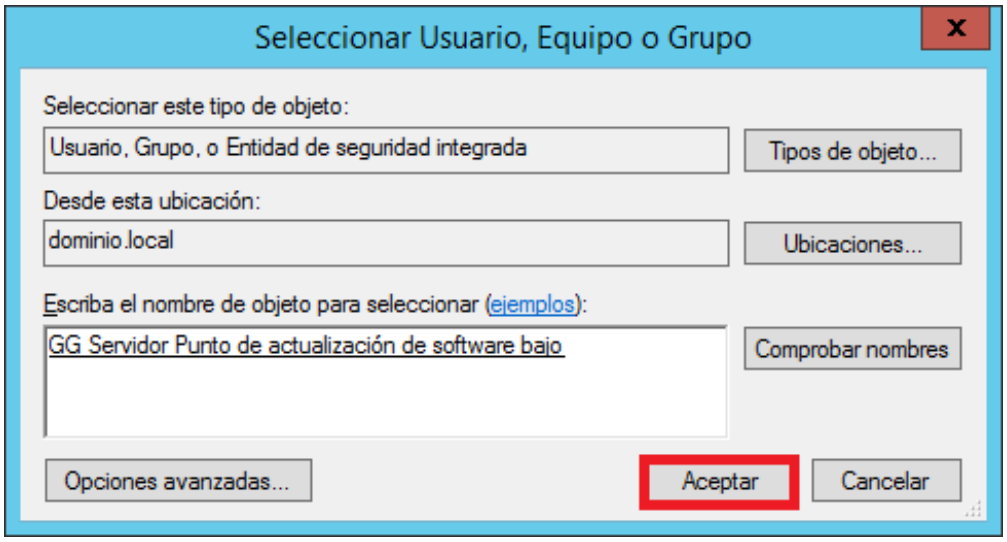
Paso	Descripción
187.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
188.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de actualización de software bajo” y haga clic en el botón “Aceptar”. 
189.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”, En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 194193, en caso contrario continúe con el paso a paso.

Paso	Descripción
190.	A continuación, se asociará la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.
191.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
192.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
193.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de actualización de software bajo" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de actualización de software bajo" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
194.	Para editar la GPO: "CCN-STIC-875 ENS Incremental Punto de actualización de software bajo" creada anteriormente, haga clic con el botón derecho y seleccione la opción "Editar" del menú contextual. 
195.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
196.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de actualización de software bajo.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
197.	Cierre el "Editor de administración de directivas de grupo" una vez que se haya realizado la importación de la configuración de seguridad.
198.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

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

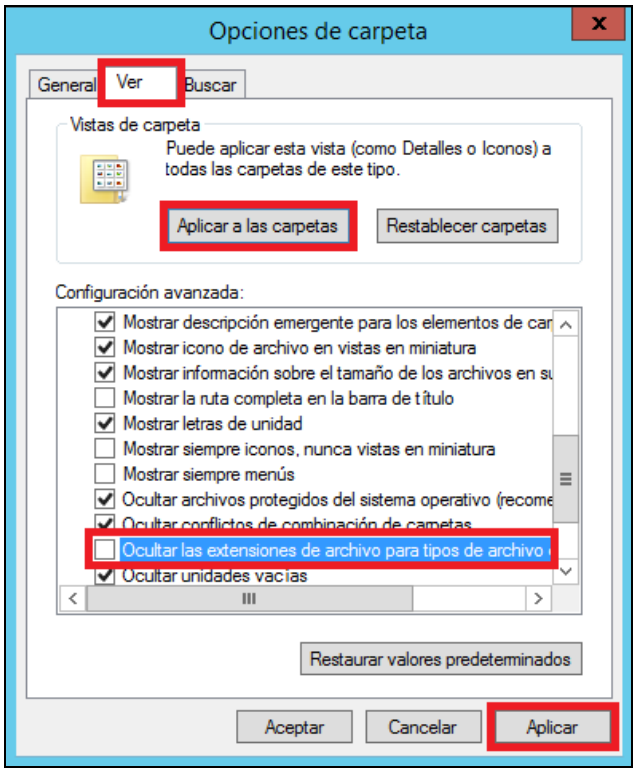
Paso	Descripción
202.	Introduzca como nombre “GG Servidor Punto de actualización de software bajo”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
203.	Cierre el “Editor de administración de directivas de grupo”.

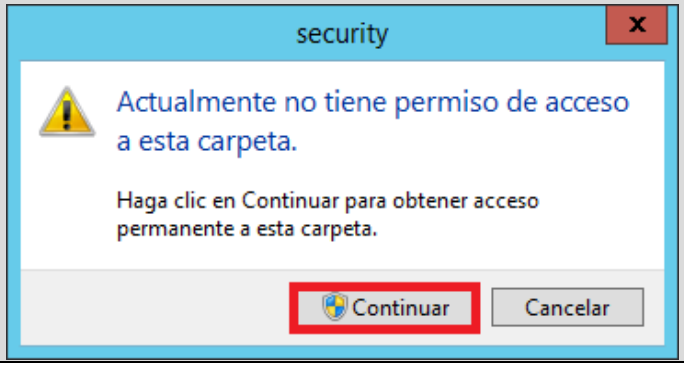
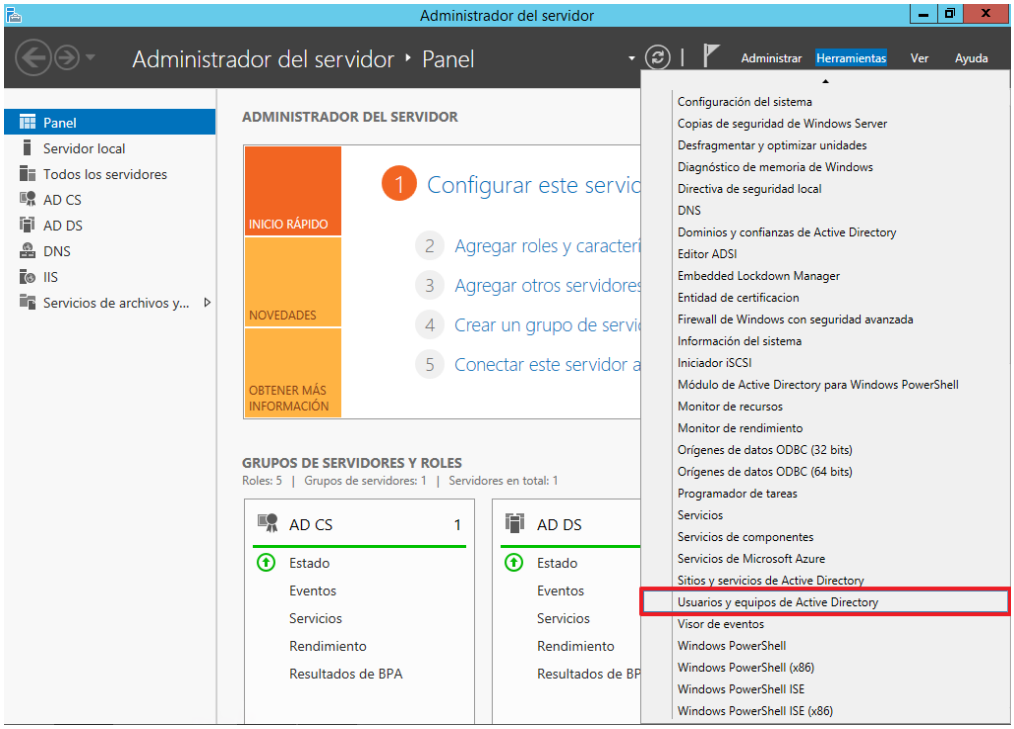
6. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE SERVICIOS DE INFORME

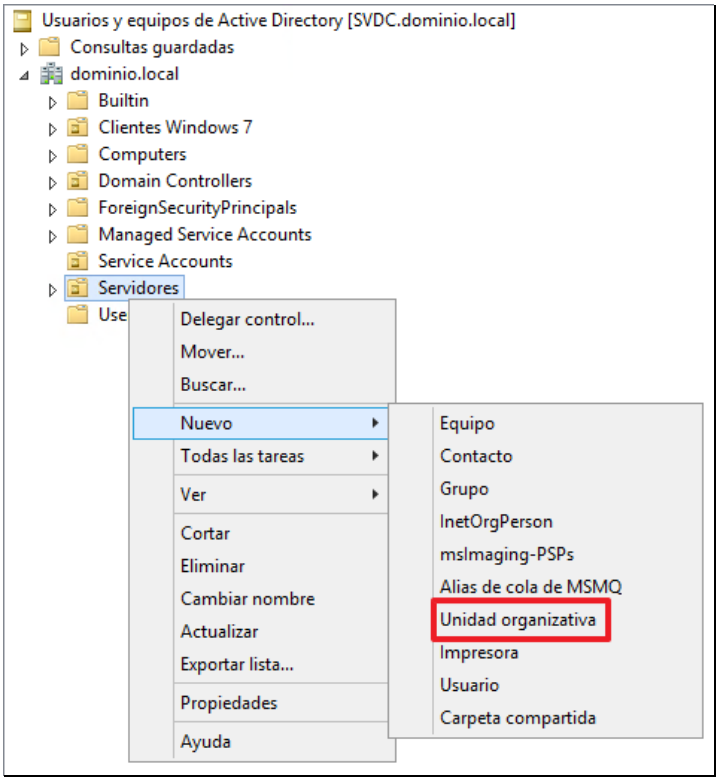
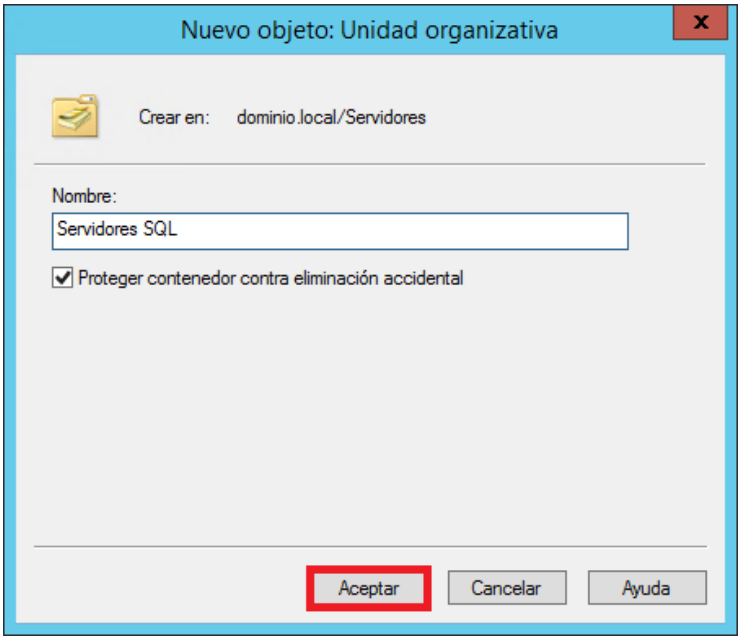
A continuación, se describen los pasos para reforzar la seguridad de los servidores que tienen del rol de punto de servicios de informes implementado en el equipo.

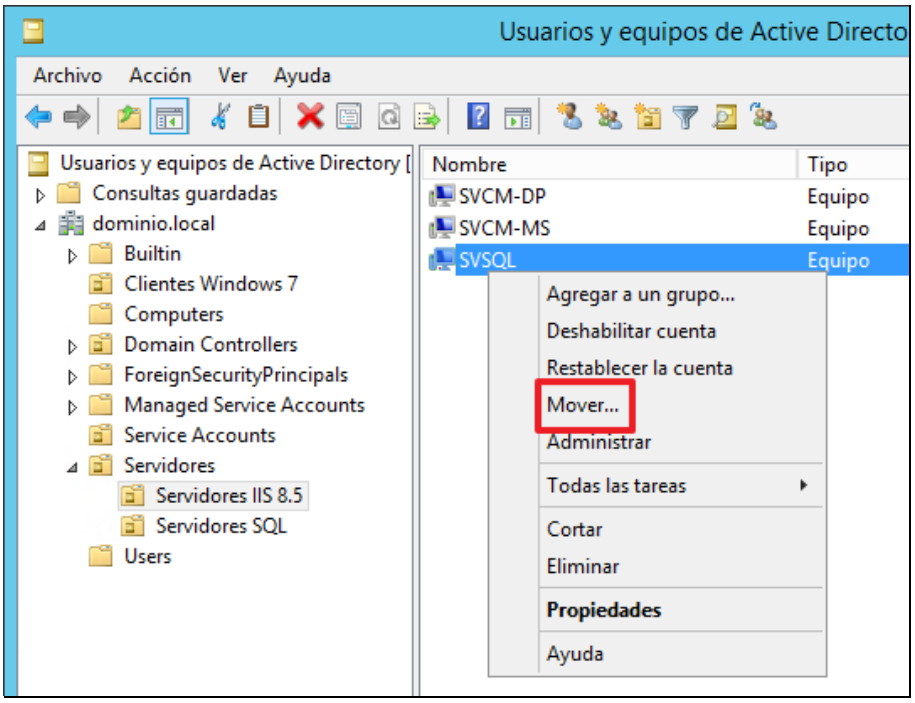
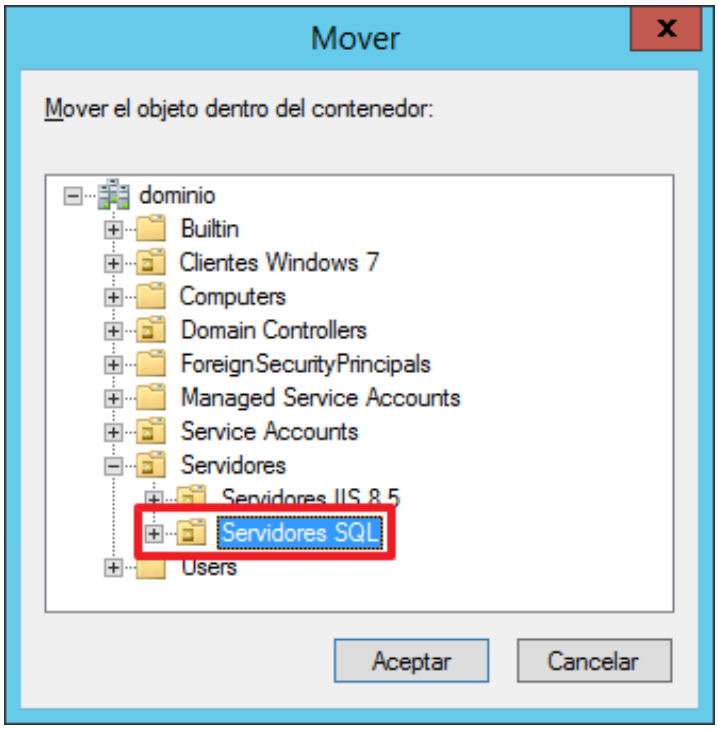
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

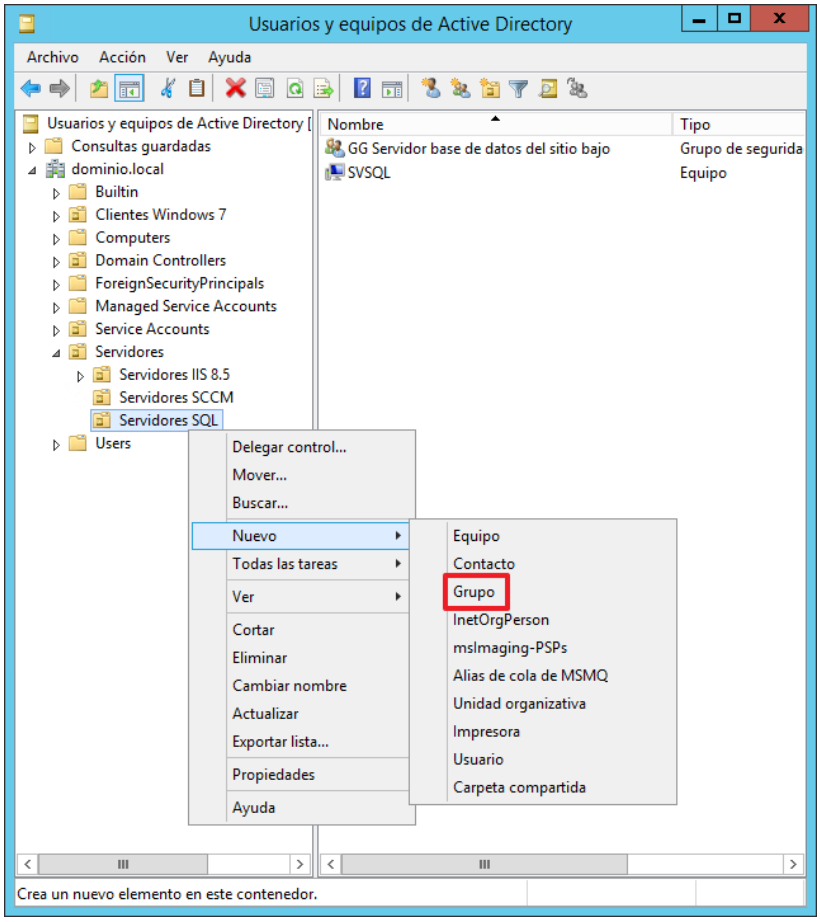
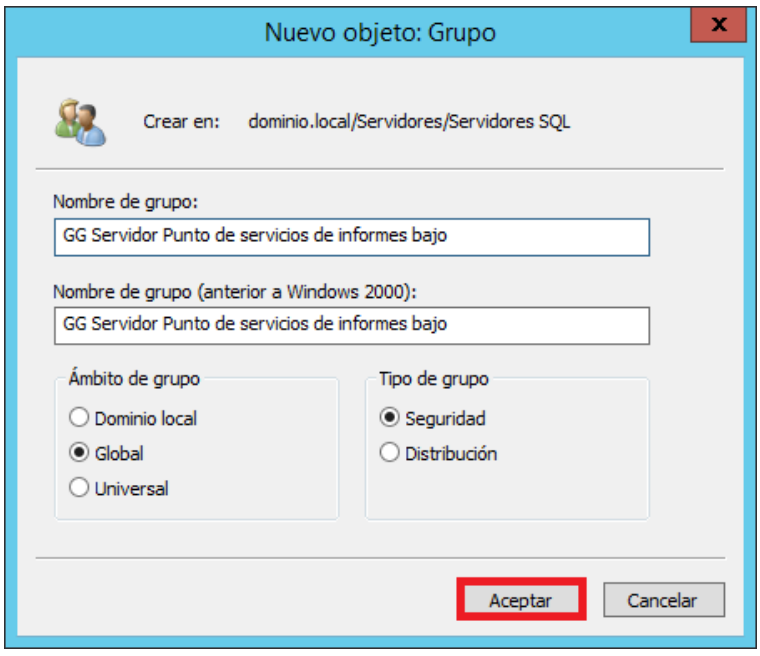
Paso	Descripción
204.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.

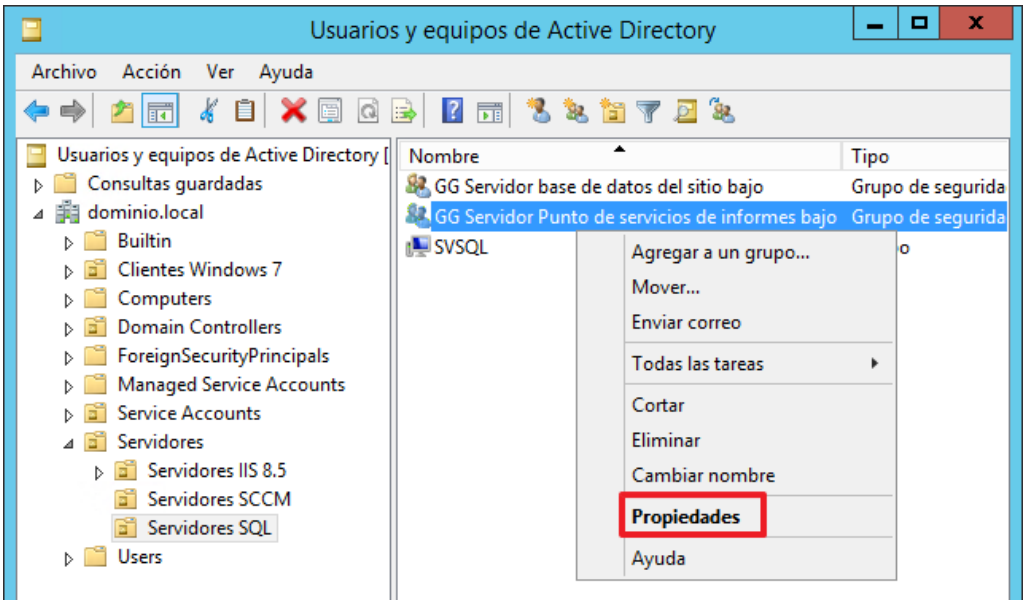
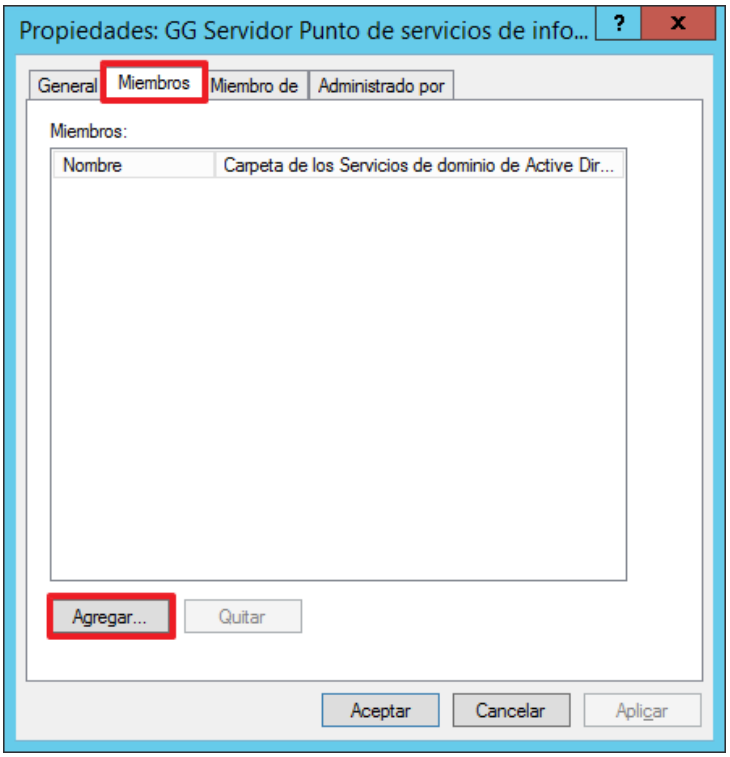
Paso	Descripción
205.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
206.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
207.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
208.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

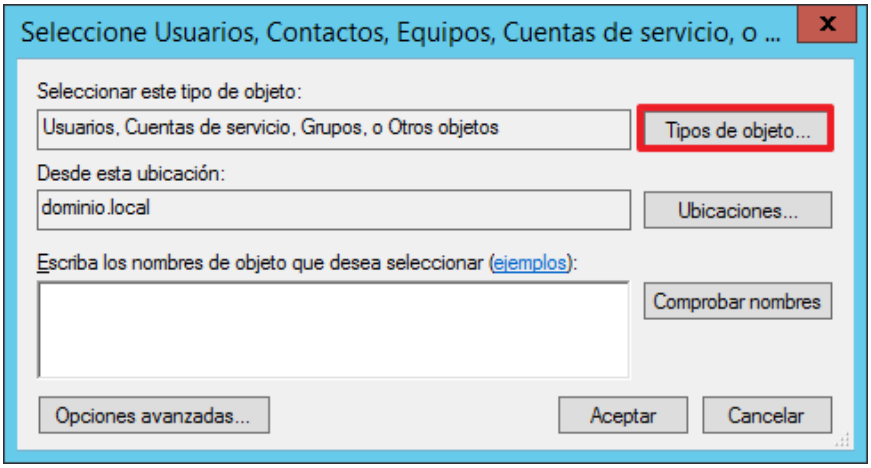
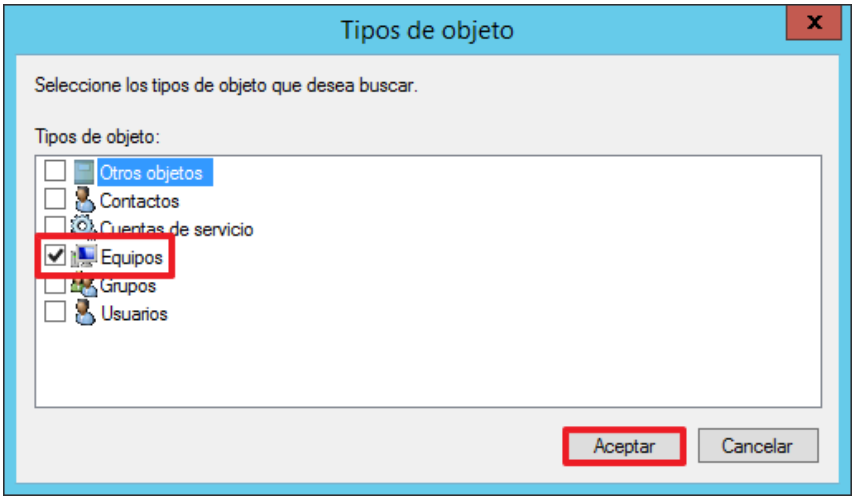
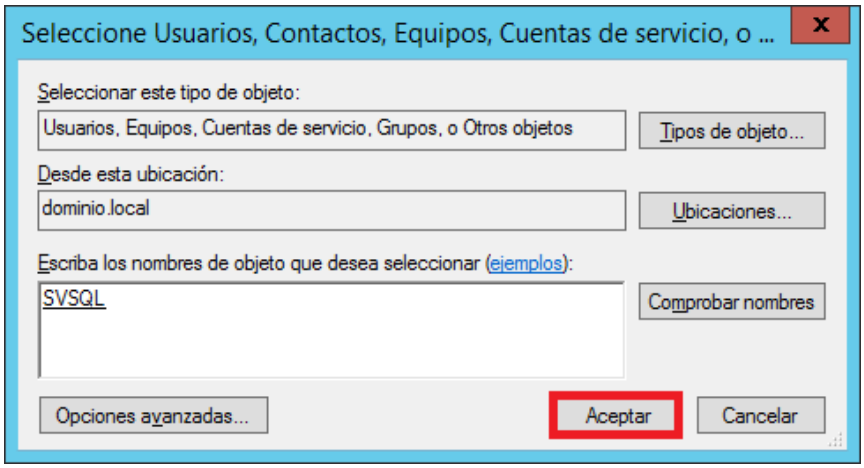
Paso	Descripción
209.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo.inf” que se encuentra en la ruta “C:\Scripts\Nivel Bajo” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
210.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .
211.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SQL, si ya ha realizado esta tarea, vaya directamente al paso 216. En caso contrario continúe con el paso a paso.

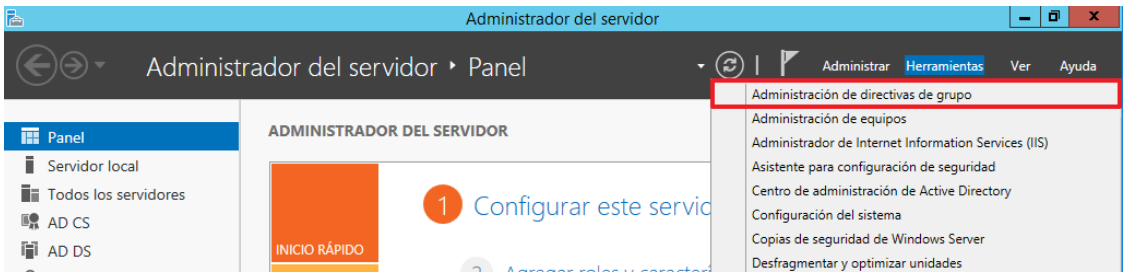
Paso	Descripción
212.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
213.	En la consola, cree una unidad organizativa denominada “Servidores SQL” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen. 

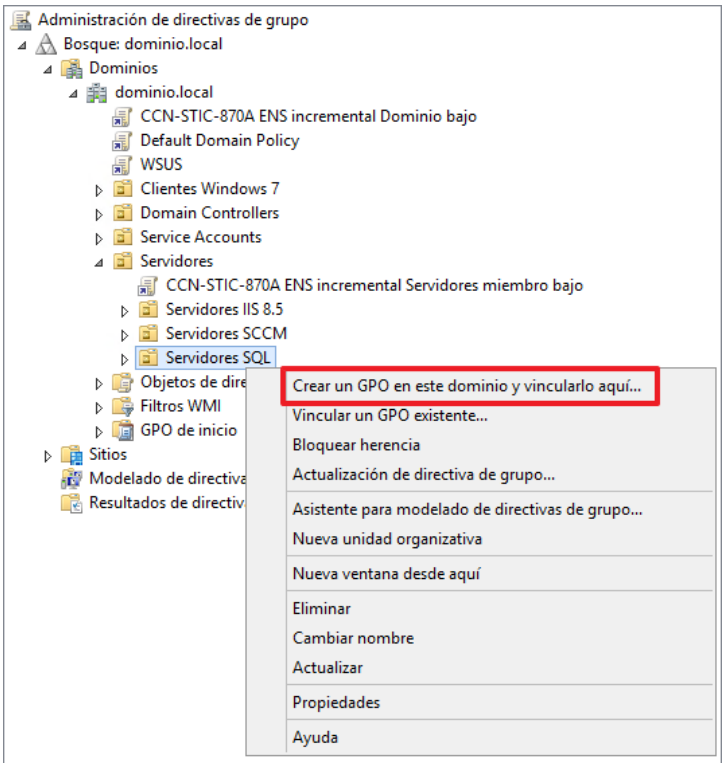
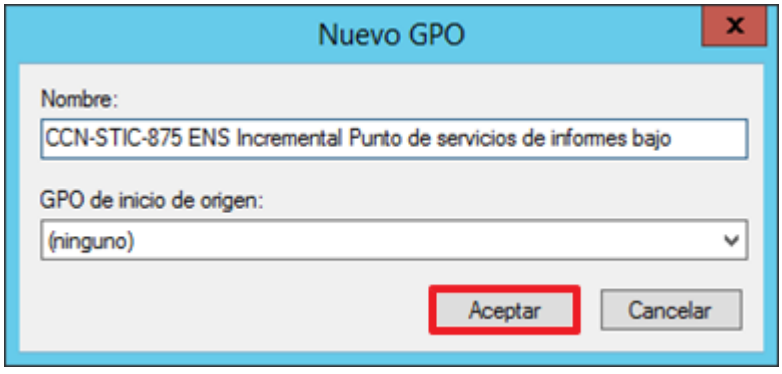
Paso	Descripción
214.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores SQL a la unidad organizativa “Servidores SQL”. Para ello, deberá localizar los servidores y hacer clic con el botón derecho sobre “mover” en el servidor que desee ubicar en la nueva unidad organizativa. 
215.	Seleccione la unidad organizativa “Servidores SQL” y pulse “Aceptar”. 

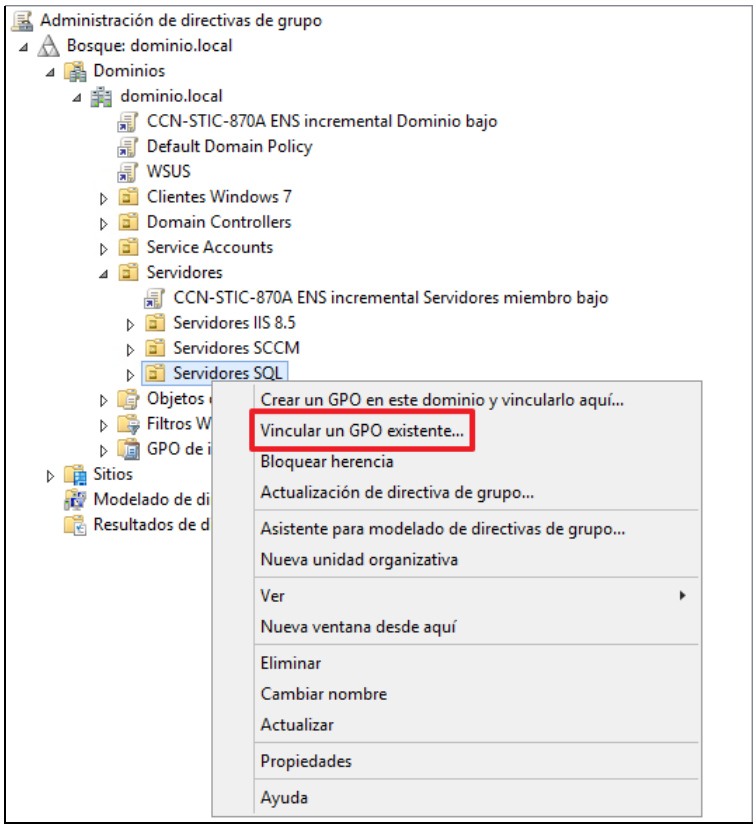
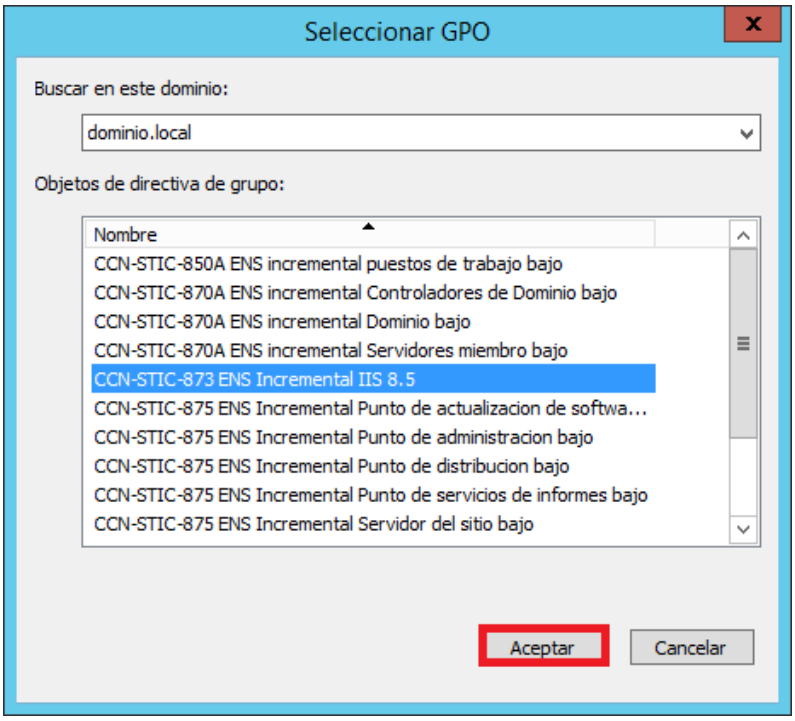
Paso	Descripción
216.	En el siguiente paso, seleccione la unidad organizativa “Servidores SQL”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
217.	Escriba el nombre “GG Servidor Punto de servicios de informes bajo” y pulse “Aceptar”. 

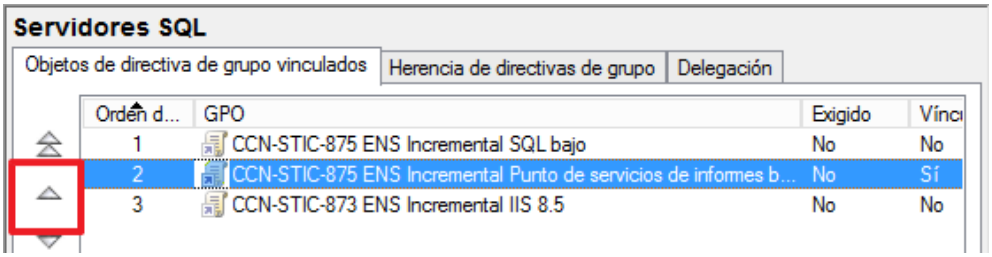
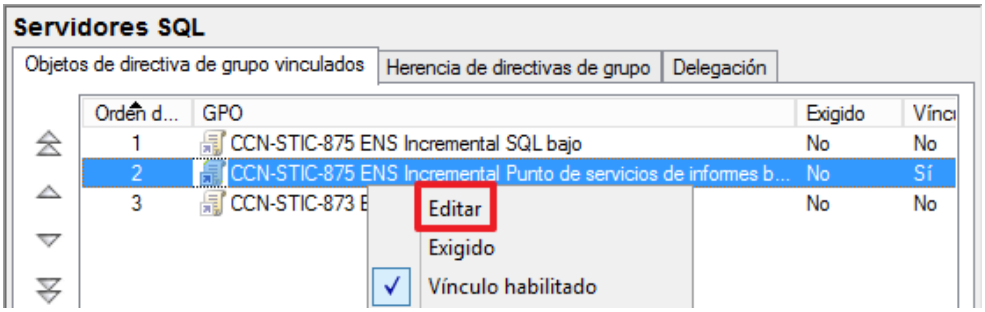
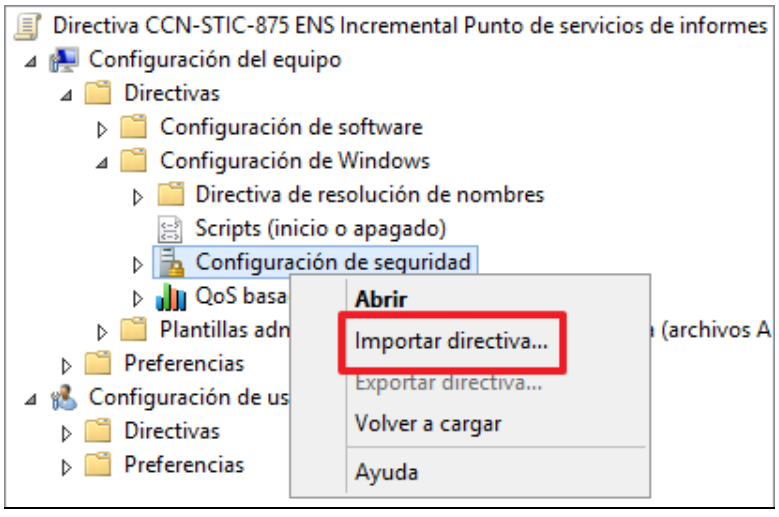
Paso	Descripción
218.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
219.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de Servicios de informes” al grupo. 

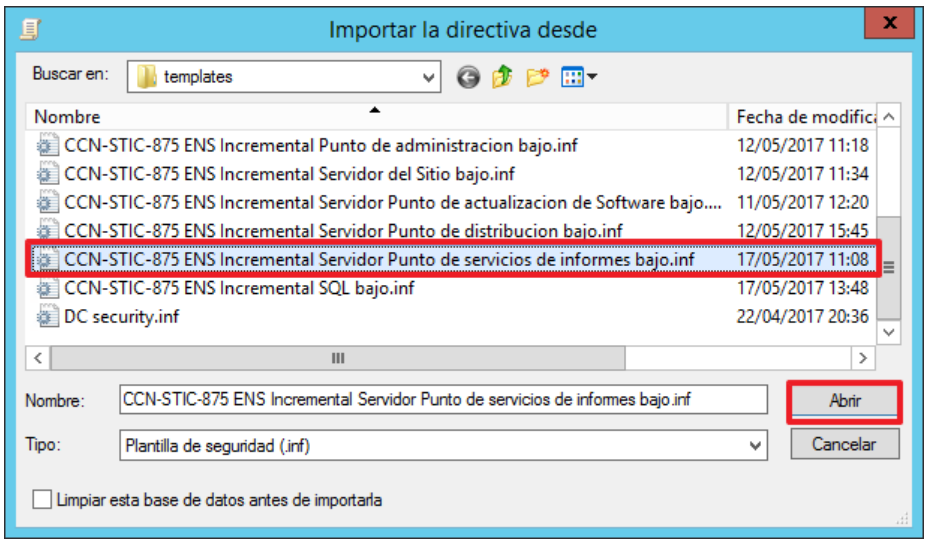
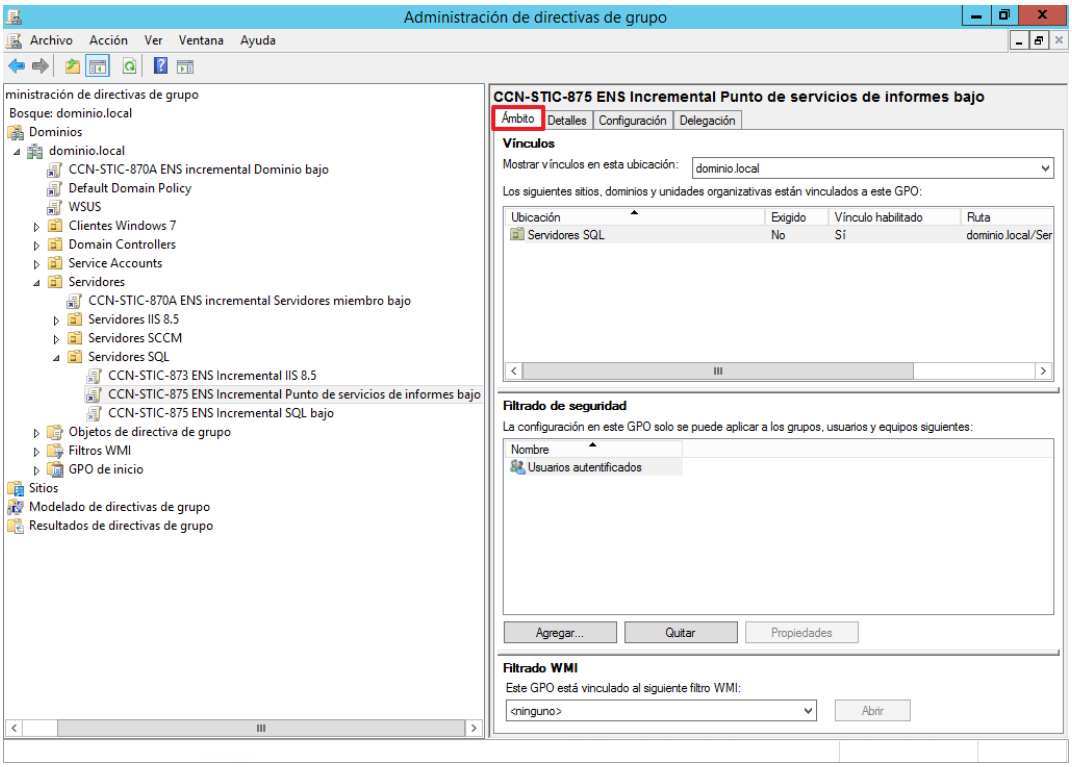
Paso	Descripción
220.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
221.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
222.	Agregue los equipos y pulse sobre “Aceptar”. 

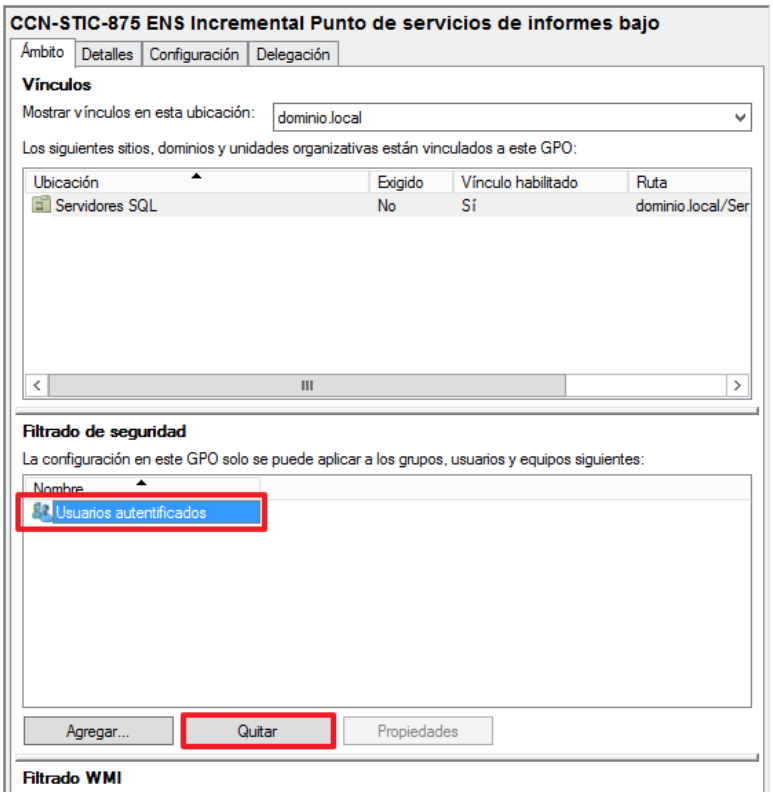
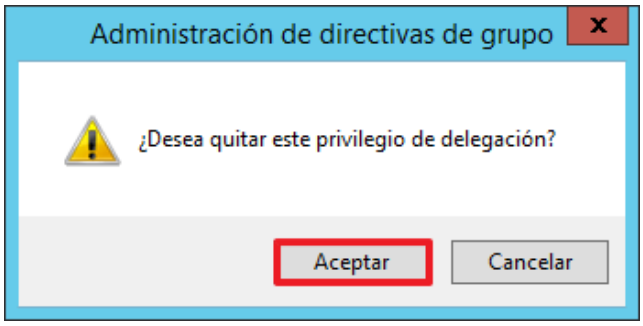
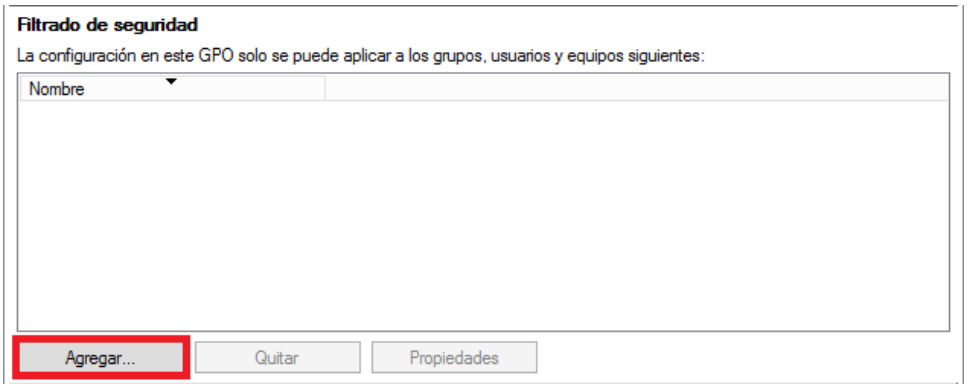
Paso	Descripción
223.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
224.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
225.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

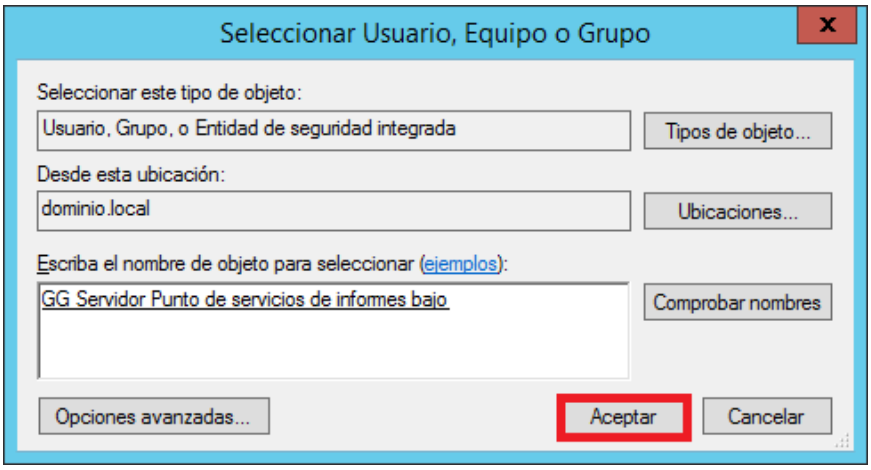
Paso	Descripción
226.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SQL”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”.  **Nota:** Deberá adaptar estos pasos a su organización seleccionando la Unidad Organizativa que aloje los roles en los que está reforzando la seguridad.
227.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de Servicios de Informes bajo” y haga clic en el botón “Aceptar”. 
228.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”. En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 233, en caso contrario continúe con el paso a paso.
229.	A continuación, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SQL.

Paso	Descripción
230.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SQL” y haga clic sobre “Vincular un GPO existente…” 
231.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
232.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de Servicios de informes bajo" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SQL", la directiva "CCN-STIC-875 ENS Incremental Punto de Servicios de informes bajo" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
233.	Edite la GPO: "CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
234.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
235.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
236.	Cierre el “Editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
237.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

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

Paso	Descripción
241.	Introduzca como nombre “GG Servidor Punto de servicios de informes bajo” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
242.	Cierre el “Administrador de directivas de grupo”.

7. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

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

En la presente guía la conexión con el servidor que tiene implementado SCCM se efectúa a través de escritorio remoto, debido a la aplicación de los refuerzos de seguridad que se van a realizar, en caso que los usuarios administrativos solo requieran de acceso para administrar SCCM se recomienda que la conexión se realice a través de la consola de administración de SCCM desde su puesto de trabajo y no mediante escritorio remoto, evitando con ello otorgar más permisos de los estrictamente necesarios.

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

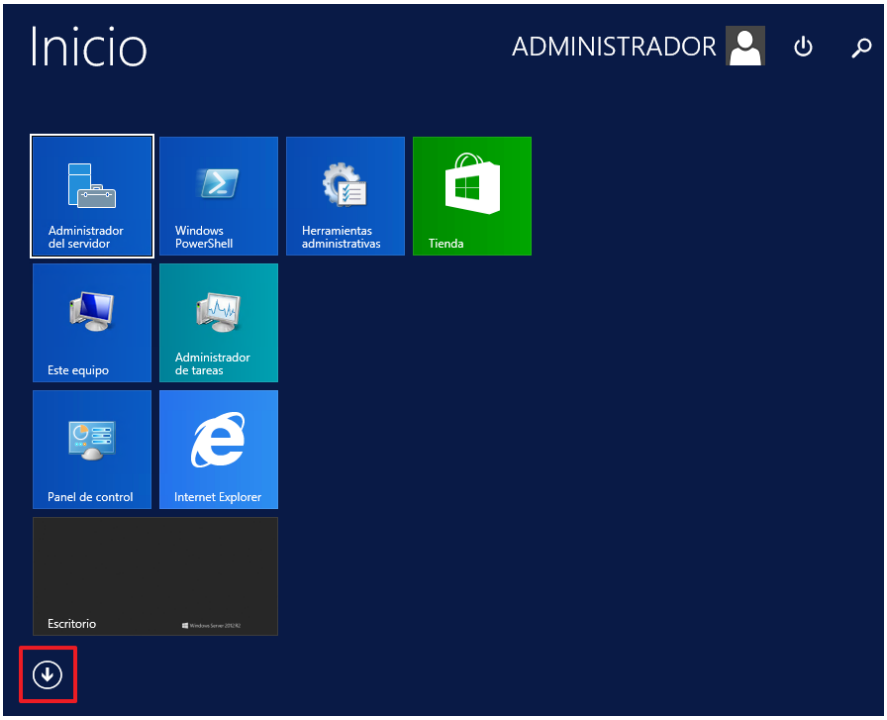
Nota: Todas las recomendaciones de seguridad indicadas en la presente guía deben ser adaptadas al entorno de su organización. Se aconseja realizar las pruebas pertinentes en un entorno de preproducción antes de ser incluidas en su entorno de producción.

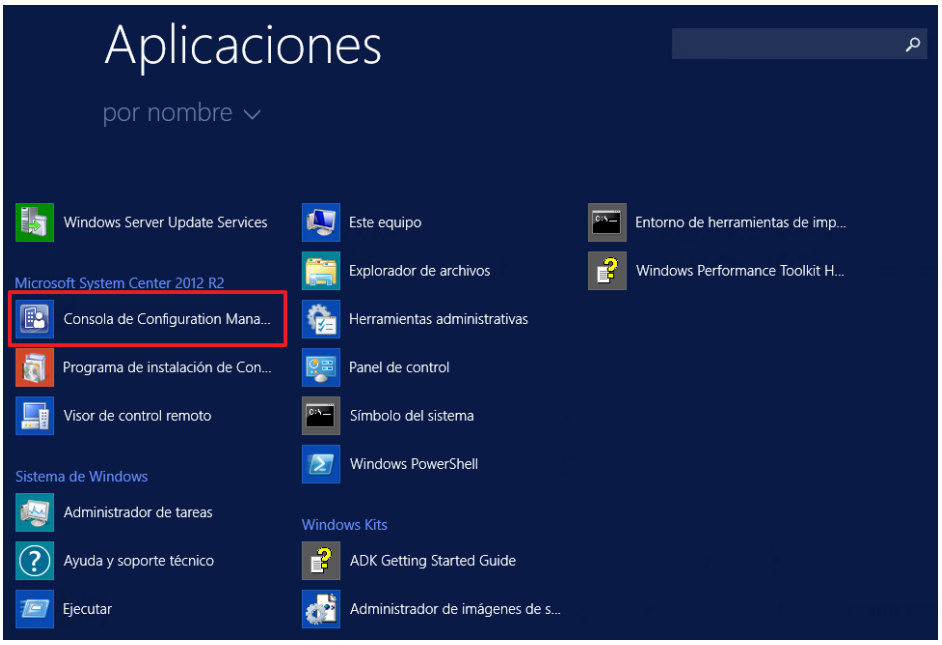
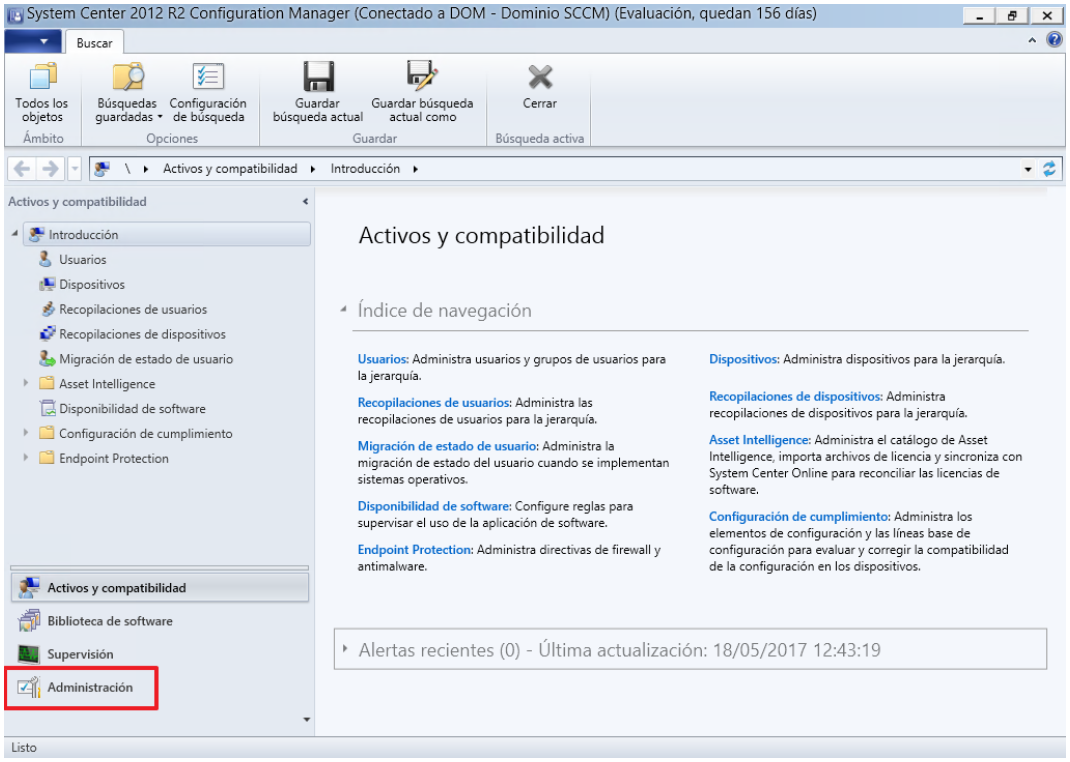
7.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

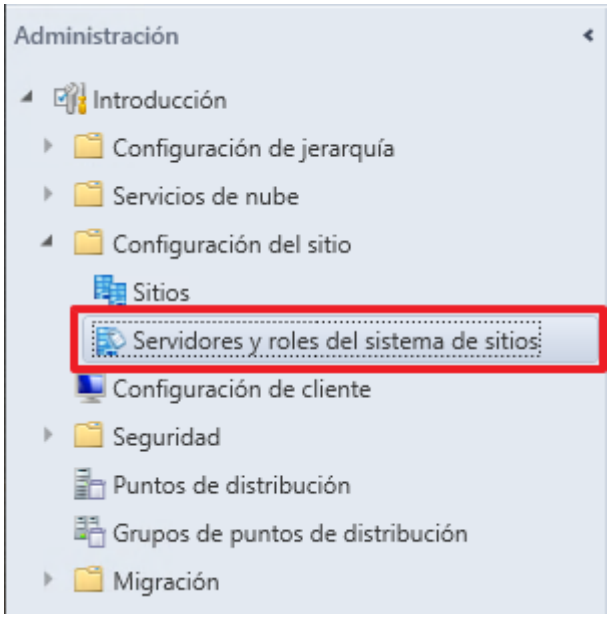
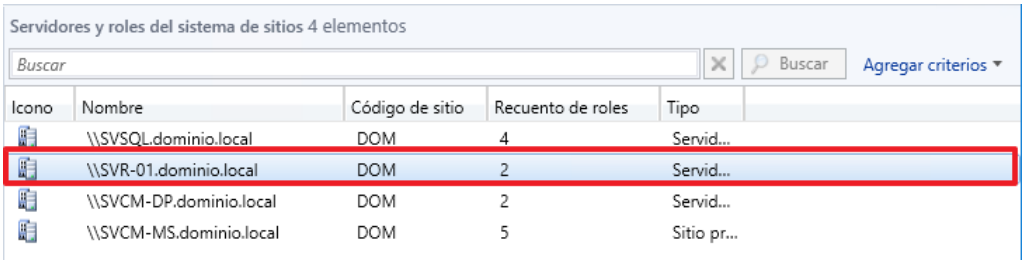
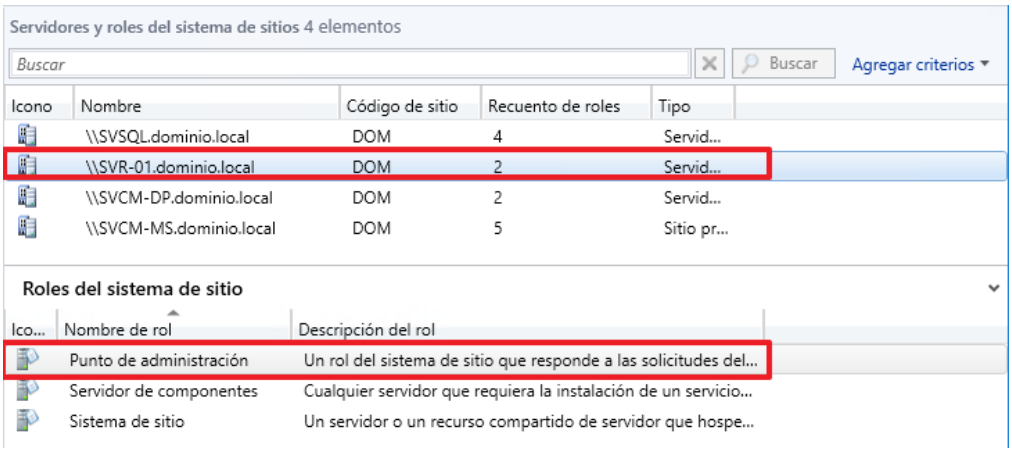
Uno de los aspectos que marca el ENS, desde su requisito de nivel bajo en el Marco Operacional, es la mínima funcionalidad y mínima exposición evitando con ello posibles vulnerabilidades minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

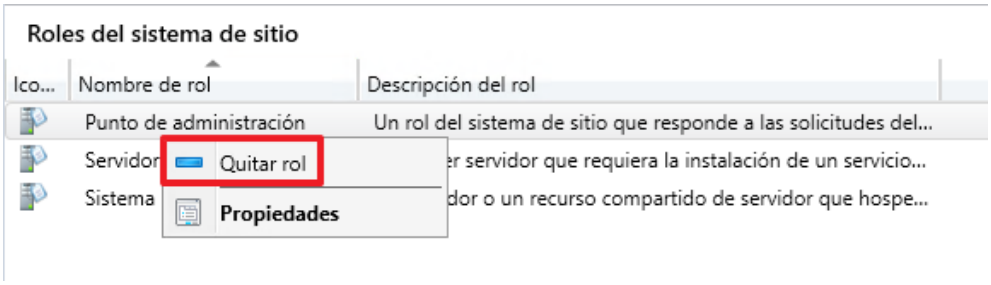
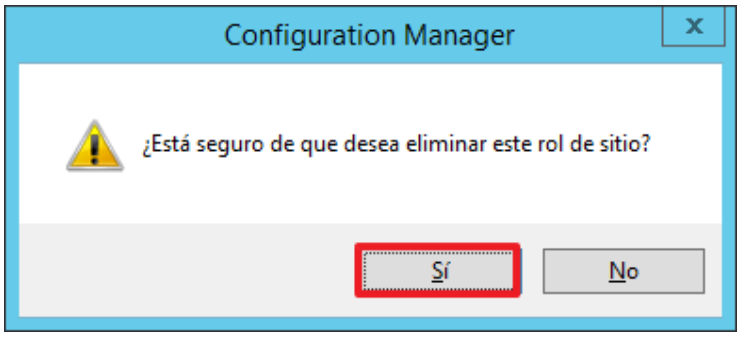
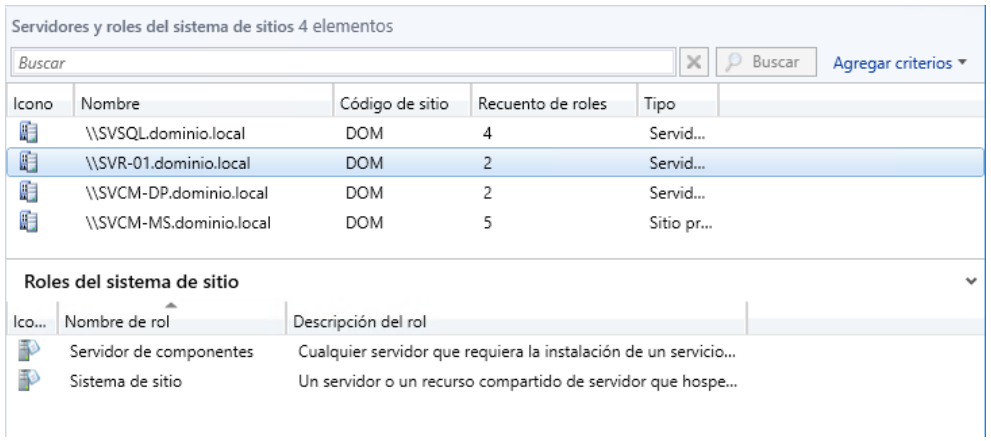
Microsoft SCCM 2012 R2 permite el añadir o quitar roles en los servidores función de la tarea a desempeñar por el servidor, por ejemplo, un servidor destinado únicamente a la distribución de paquetes, el cual tiene instalado el rol de punto de distribución, no es necesario que tenga otro rol para el cual el servidor no está destinado.

Seguidamente, se muestra un ejemplo de cómo desinstalar un rol especifico implementado en un servidor, el siguiente paso a paso da por hecho que ya instalado previamente un rol y que por necesidades de la organización dicho rol se ha de desinstalar del servidor, aplicando con ello el principio de mínima funcionalidad quitando características que ya no son necesarias de un servidor de su organización.

Paso	Descripción
243.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
244.	Pulse sobre el menú inicio. 
245.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
246.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
247.	Seleccione el apartado “Administración”. 

Paso	Descripción
248.	Despliegue "**Configuración del sitio > Servidores y roles del sistema de sitios**". 
249.	Marque en el menú derecho el servidor del que quiere quitar un rol de sistema de sitios.  **Nota:** Deberá adaptar estos pasos a su organización seleccionando el servidor que contenga implementado el rol que desea quitar.
250.	En este ejemplo se va a quitar el rol de "Punto de administración" el cual ha sido implementado previamente. Asegúrese que selecciona el servidor correcto y en la parte inferior seleccione el rol que desea desinstalar. 

Paso	Descripción
251.	Una vez seleccionado el rol que desea quitar, pulse con el botón derecho y seleccione la opción “Quitar rol” del menú contextual. 
252.	Pulse “Sí” sobre la advertencia que aparece cuando está intentando quitar el rol. 
253.	Verifique que ha quitado el rol correctamente. 

7.2. SEGREGACIÓN DE ROLES Y FUNCIONES

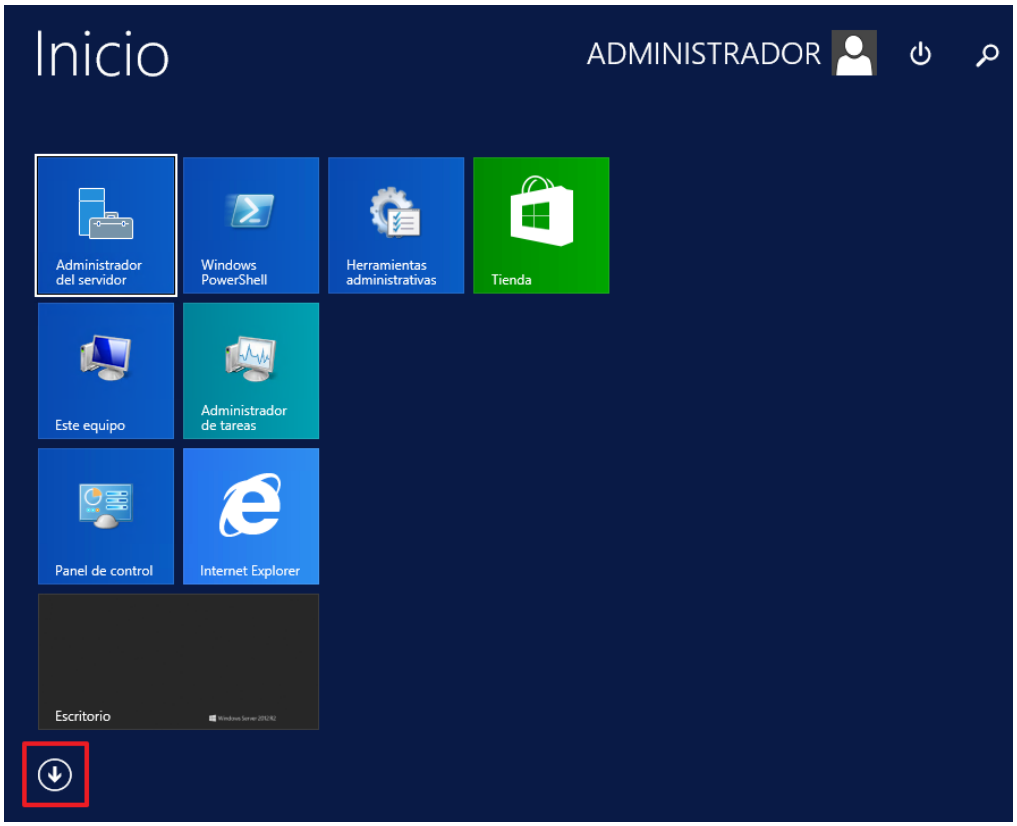
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y a la aplicación de directivas sobre dichos grupos.

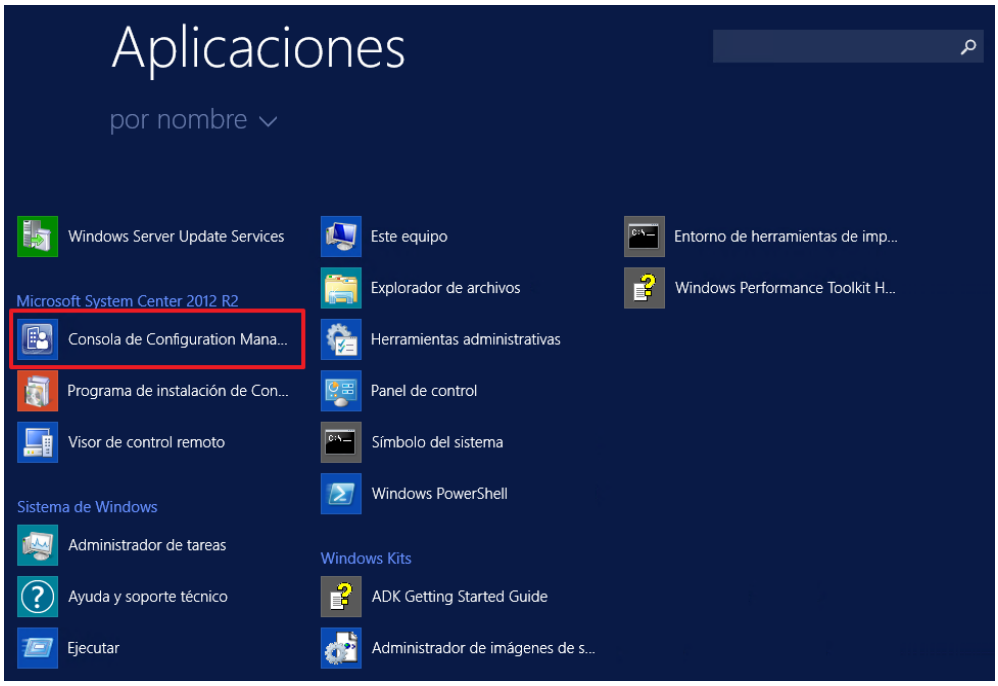
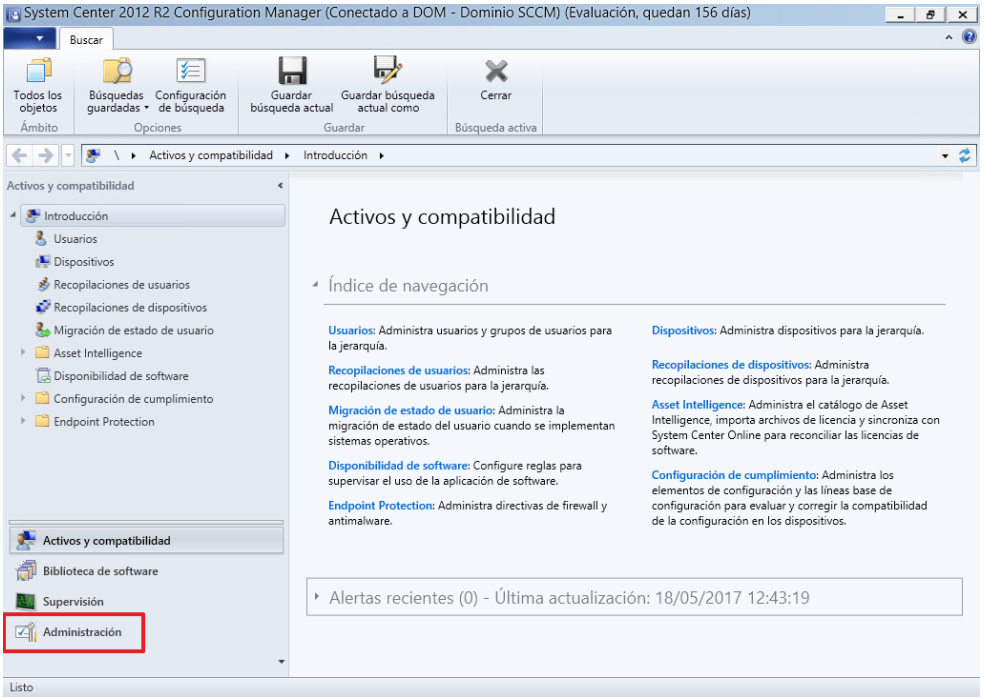
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración, a la vez que otros pueden asumir la funcionalidad de auditores.

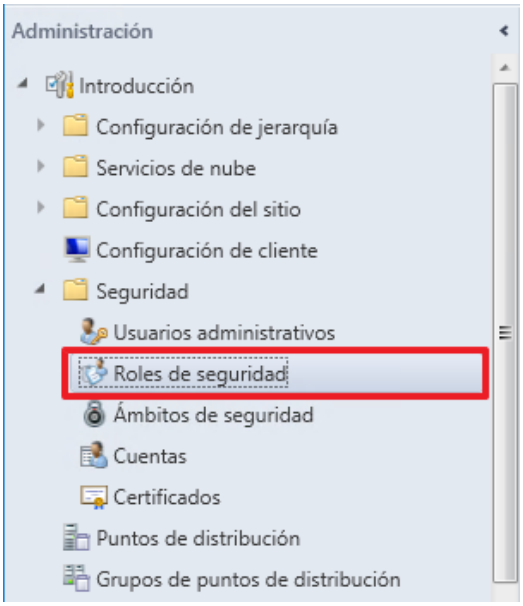
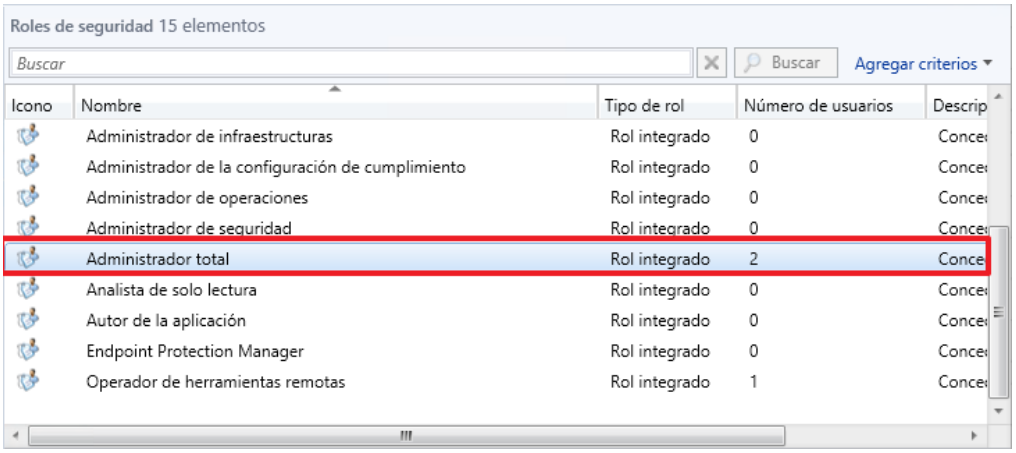
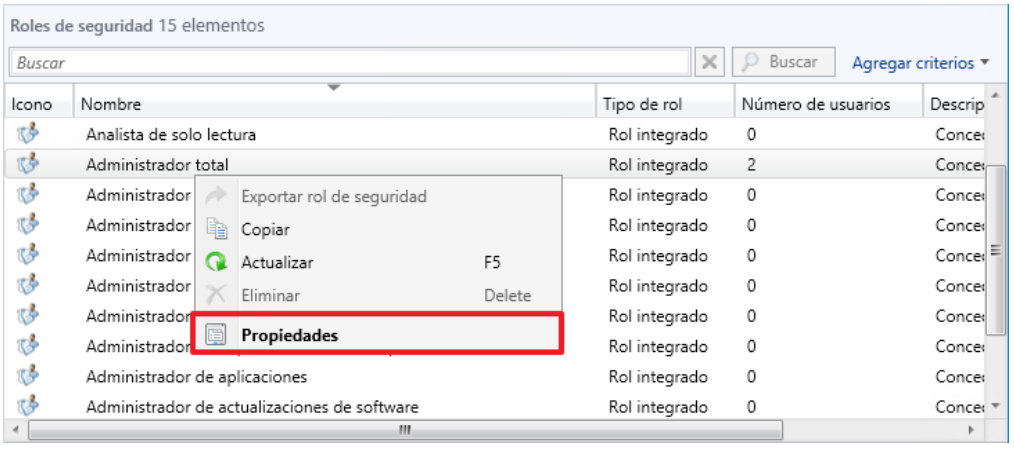
La administración de roles de seguridad y permisos se puede realizar a través de la consola principal de Configuration Manager o bien a través de cmdlets de PowerShell.

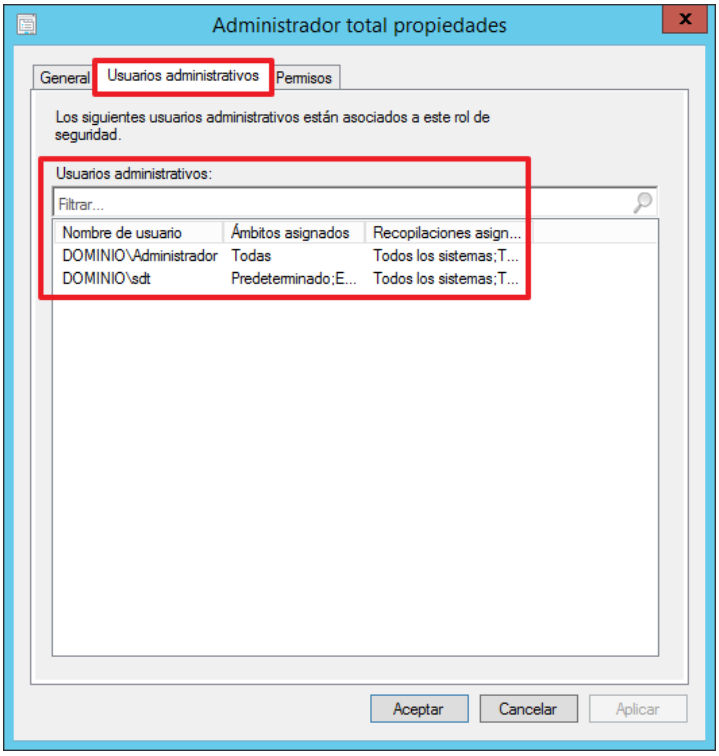
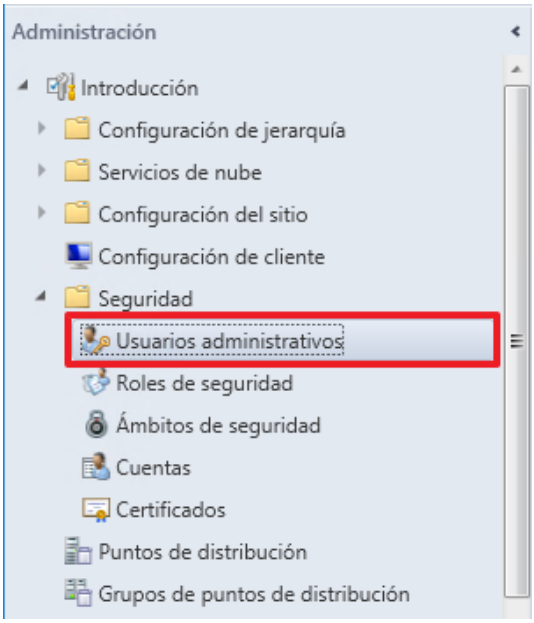
A continuación, se muestra un ejemplo de cómo comprobar los roles de seguridad que tiene asignado un usuario al igual que el procedimiento para asignar un rol de seguridad concreto a un usuario determinado.

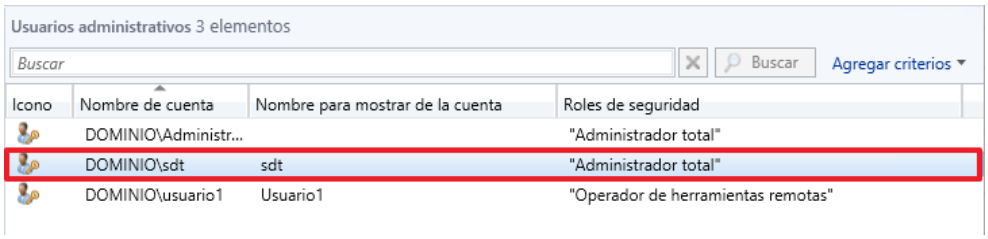
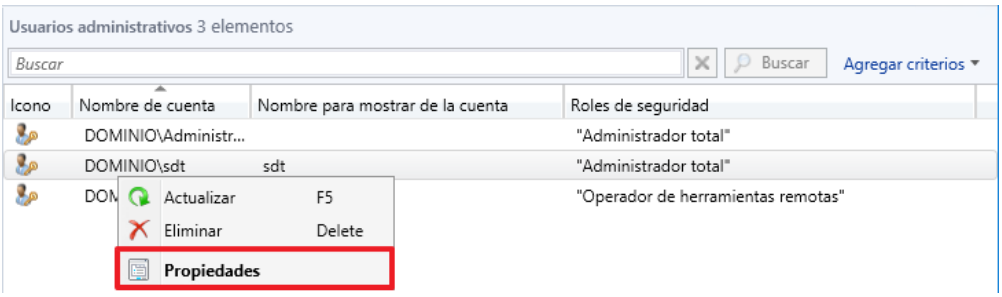
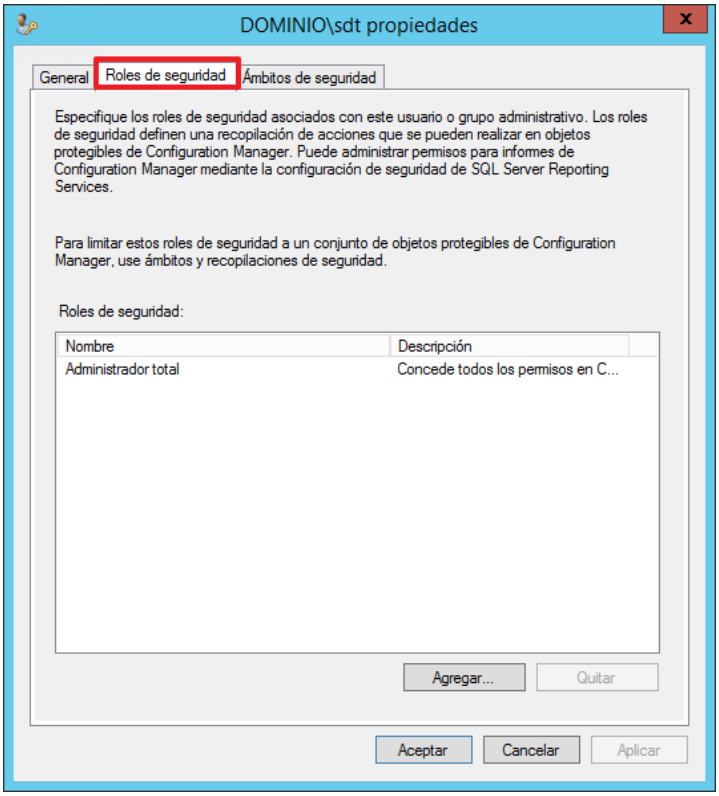
Nota: Si desea crear más información sobre la administración de roles y permisos visite la siguiente web: https://technet.microsoft.com/en-us/library/gg682106.aspx.

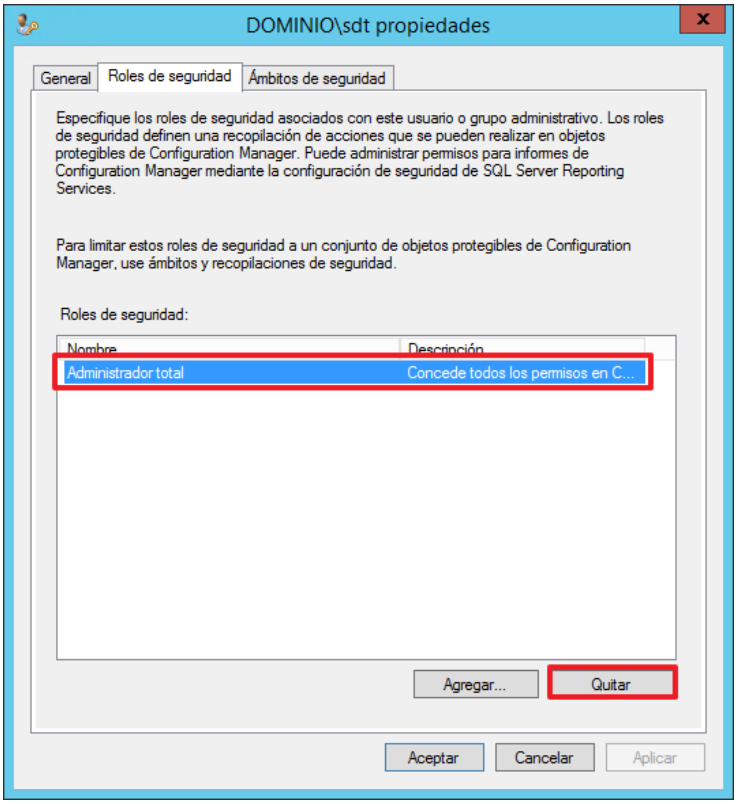
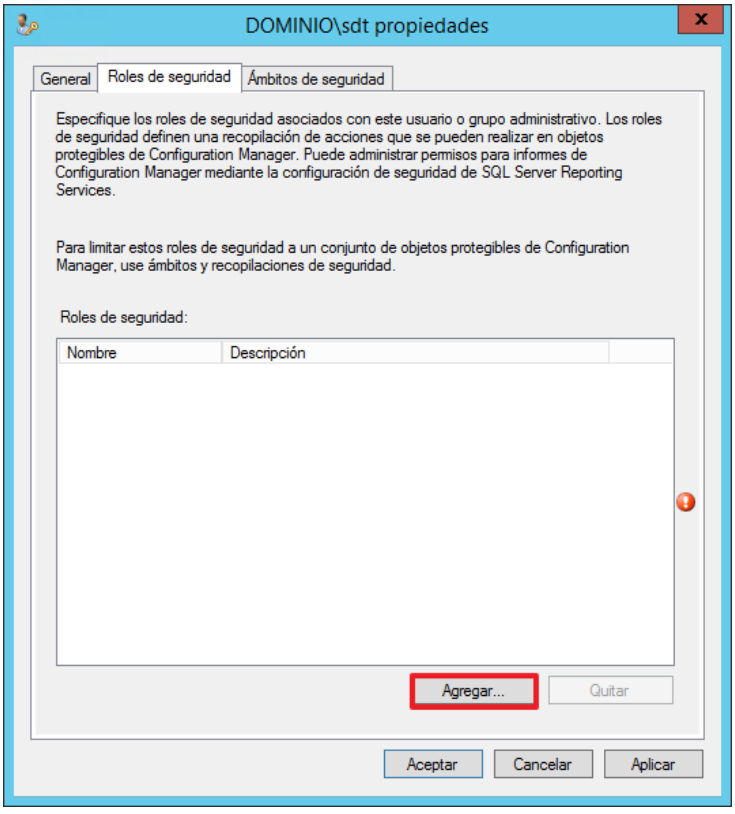
Paso	Descripción
254.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
255.	Pulse sobre el menú inicio. 
256.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

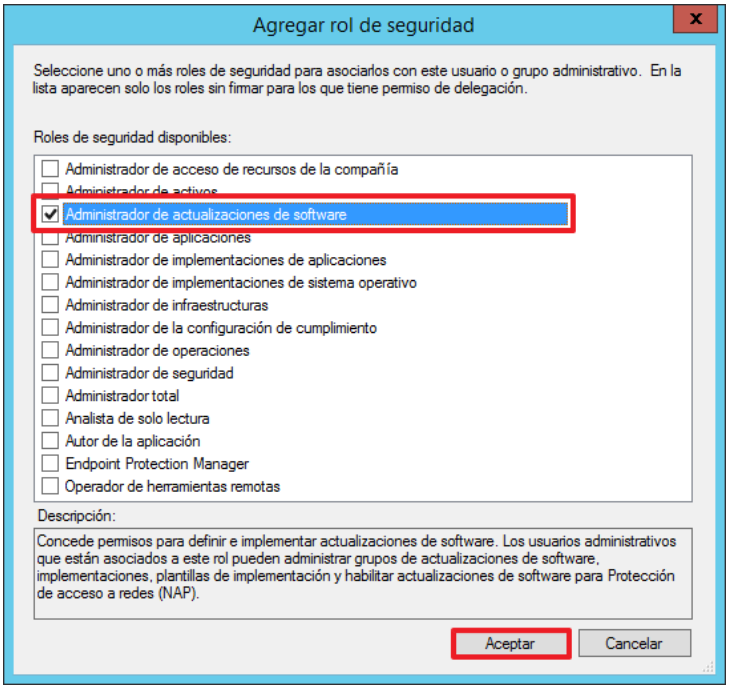
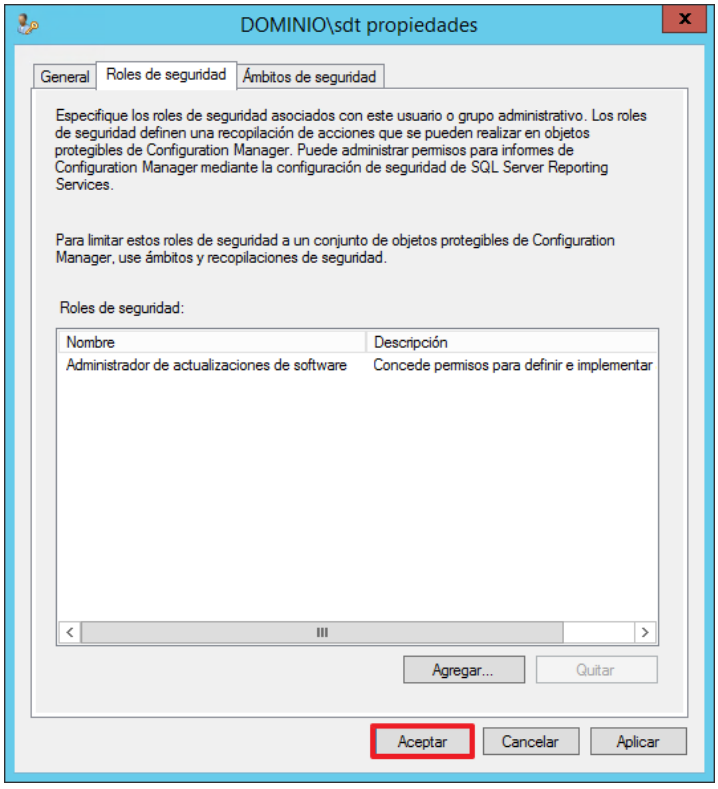
Paso	Descripción
257.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
258.	Seleccione el apartado “Administración”. 

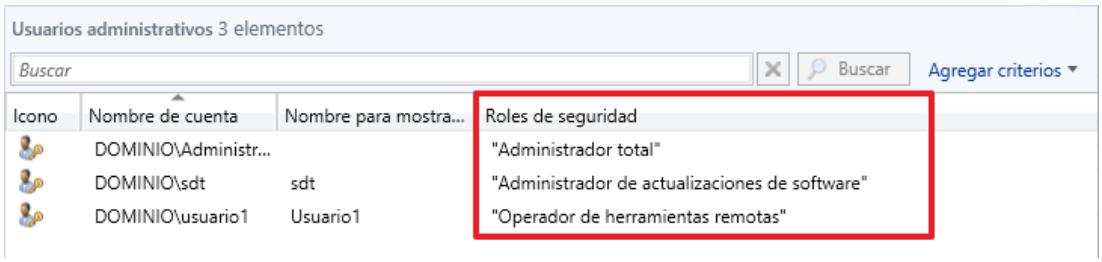
Paso	Descripción
259.	Despliegue “**Seguridad > Roles de seguridad**”. 
260.	Localice el rol de seguridad “Administrador total”. 
261.	Una vez seleccionado el rol de seguridad “Administrador total”, pulse con el botón derecho y marque la opción “Propiedades” del menú contextual. 

Paso	Descripción
262.	Seleccione la pestaña “Usuarios administrativos” y compruebe que los usuarios administrativos que aparecen son correctos ya que el rol de “Administrador total” concede todos los permisos en Configuration Manager. Una vez finalizada la comprobación pulse “Aceptar” para cerrar la ventana. 
263.	En el caso que requiera quitar el rol de seguridad “Administrador total” de un usuario y agregarle otro rol de seguridad deberá seleccionar la pestaña “Usuarios administrativos”. 

Paso	Descripción
264.	Localice el usuario administrativo que desea cambiar la configuración de roles de seguridad.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización. La presente guía no detalla como añadir usuarios administrativos a la consola de Configuration Manager.
265.	Una vez seleccionado el usuario al cual quiere modificar los roles de seguridad, pulse con el botón derecho y seleccione la opción “Propiedades” del menú contextual. 
266.	Seleccione la pestaña “Roles de seguridad”. 

Paso	Descripción
267.	Seleccione el rol que desea quitar y pulse sobre el botón “Quitar”. 
268.	Seleccione “Agregar” para añadir el rol de seguridad que desee aplicar sobre el usuario seleccionado anteriormente. 

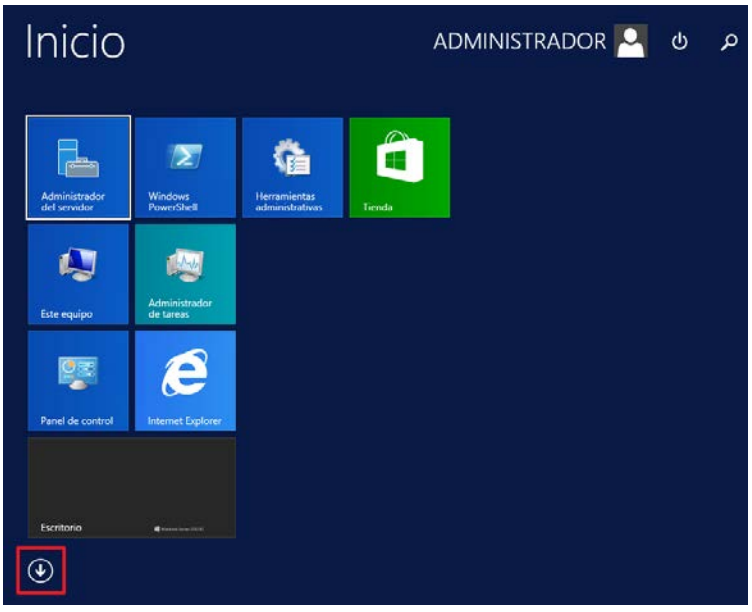
Paso	Descripción
269.	Seleccione el rol que desea asignar y pulse “Aceptar”.  **Nota:** En este ejemplo se agrega el rol de seguridad “Administrador de actualizaciones de software”, deberá adaptar estos pasos a sus requerimientos.
270.	Pulse sobre “Aceptar” para confirmar la configuración y cerrar la ventana de propiedades del usuario. 

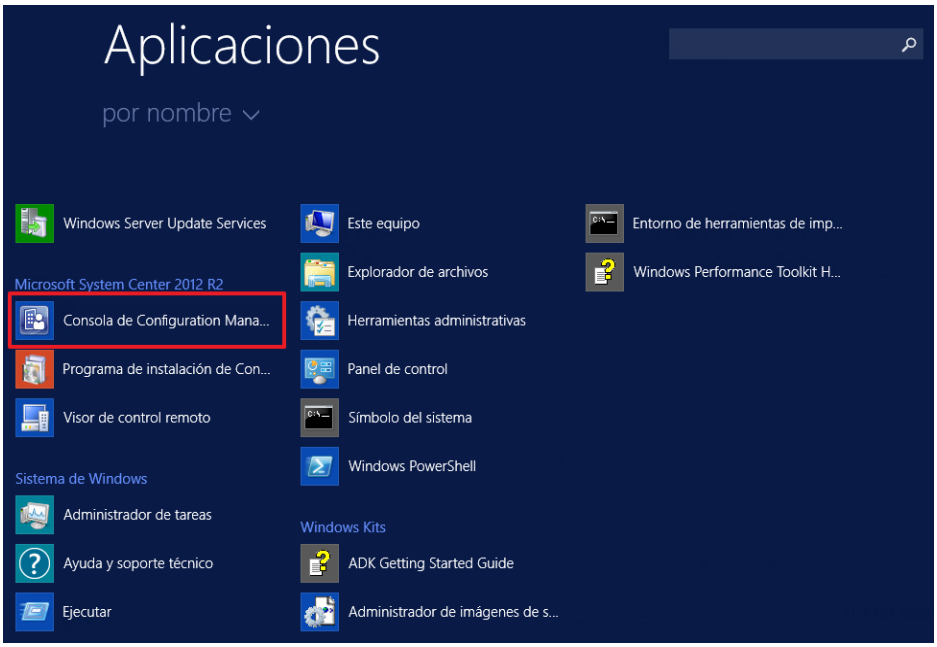
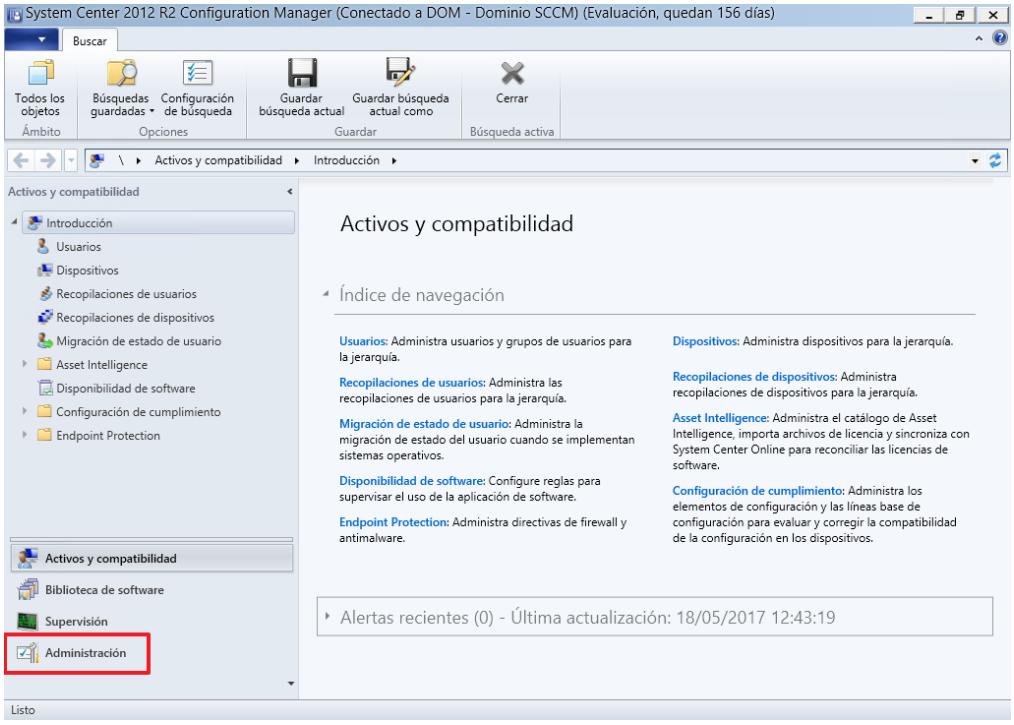
Paso	Descripción
271.	Es posible comprobar el rol asignado a un usuario desde la propia ventana de "usuarios administrativos.  **Nota:** Es posible que un usuario tenga varios roles de seguridad, pero en la presente guía no se contempla esta casuística.

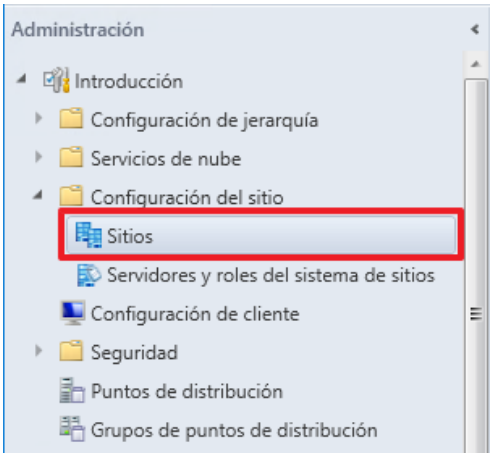
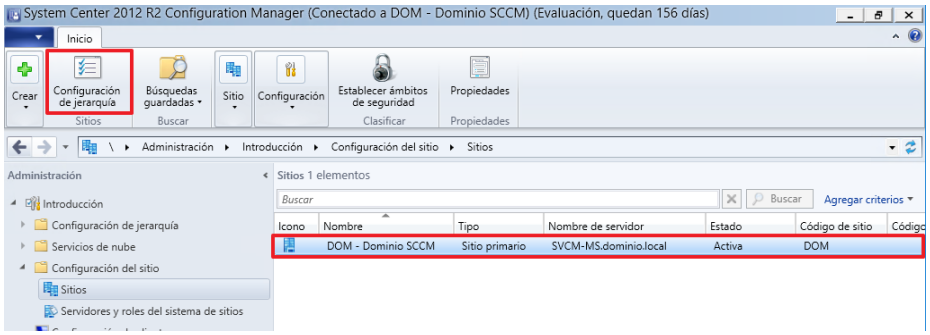
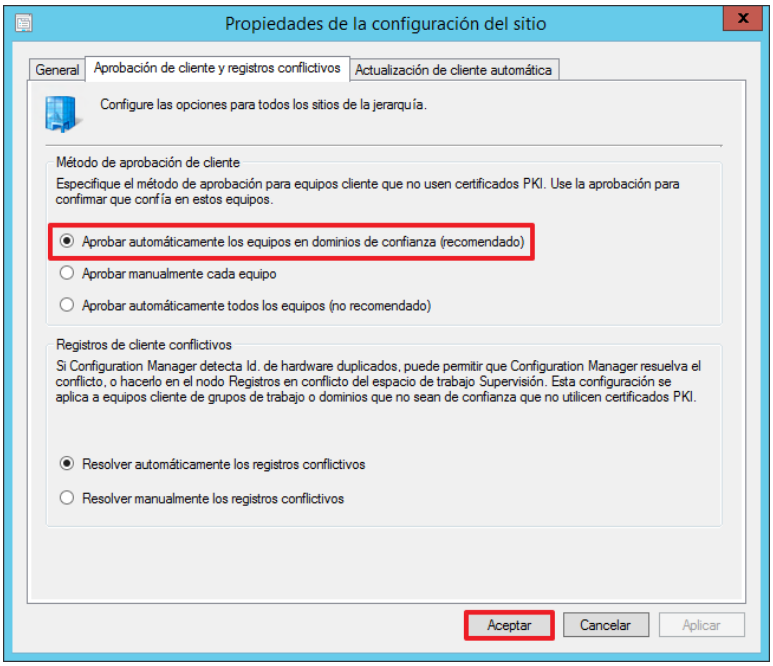
7.3. GESTIÓN DE DERECHOS DE ACCESO

Microsoft SCCM 2012 R2 permite el establecer el método de aprobación de los clientes evitando con ello que equipos cliente no autorizados conecten con SCCM.

En el proceso siguiente, se describe como establecer la aprobación de clientes en SCCM.

Paso	Descripción
272.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
273.	Pulse sobre el menú inicio. 
274.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
275.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
276.	Seleccione el apartado “Administración”. 

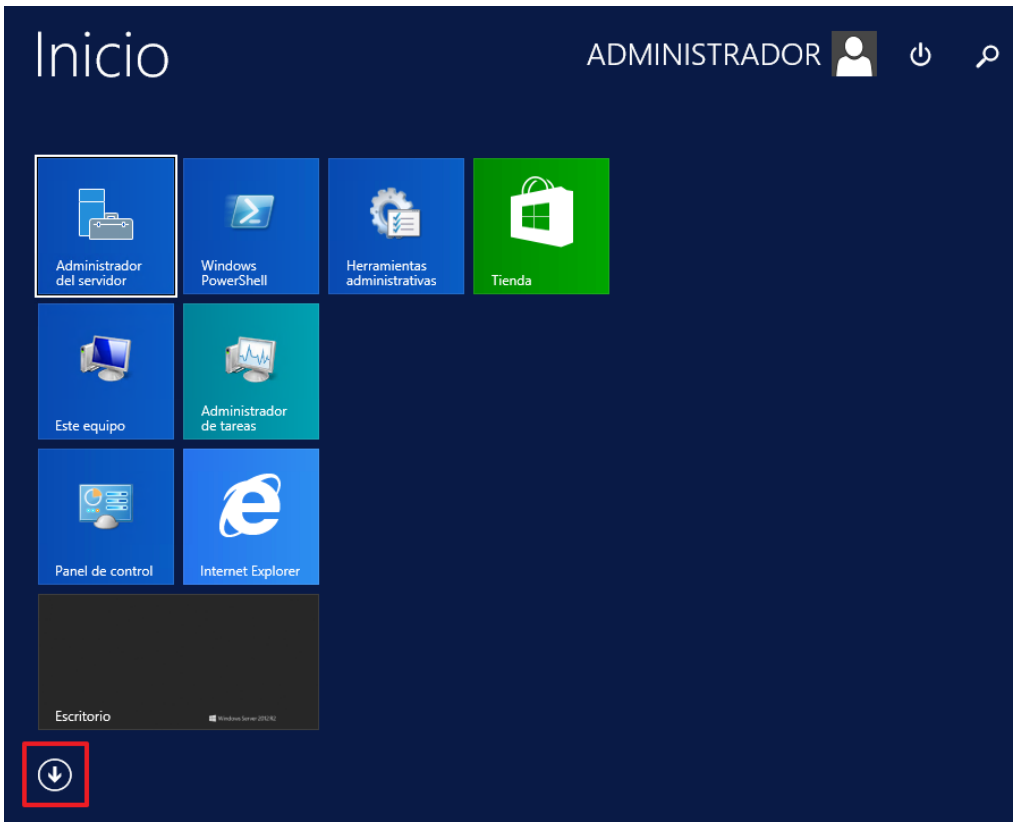
Paso	Descripción
277.	Despliegue “**Configuración del sitio > Sitios**”. 
278.	Seleccione el sitio que desea configurar y pulse sobre la opción “Configuración de jerarquía”. 
279.	Localice la pestaña “Aprobación de cliente y registros conflictivos”, marque la opción “**Aprobar automáticamente los equipos en dominio de confianza (recomendado)**” y pulse “**Aceptar**” para validar la configuración. 

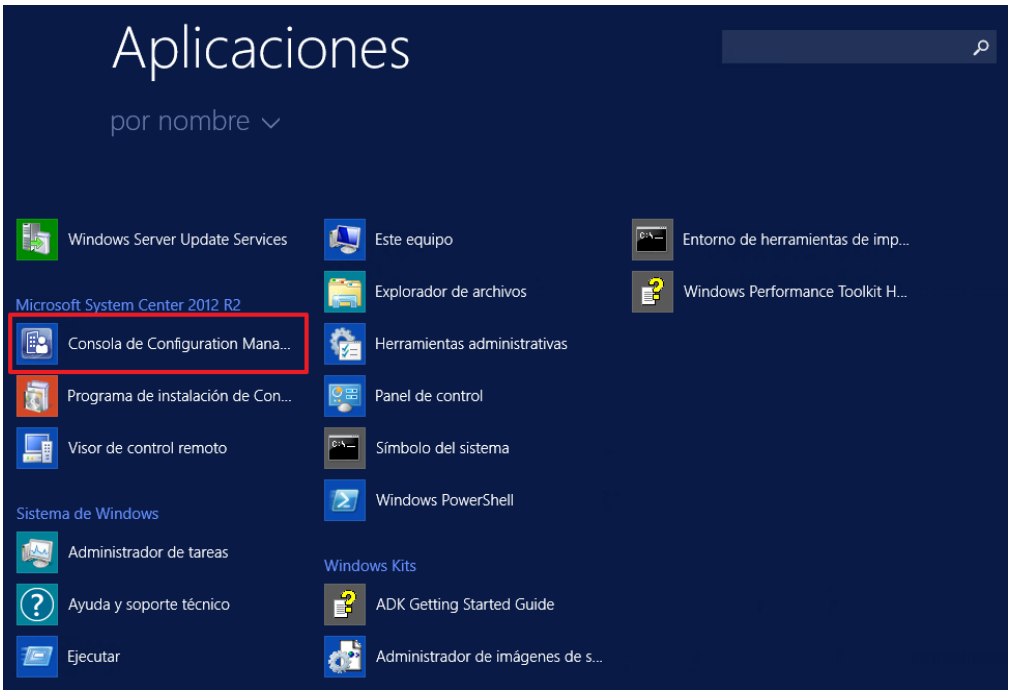
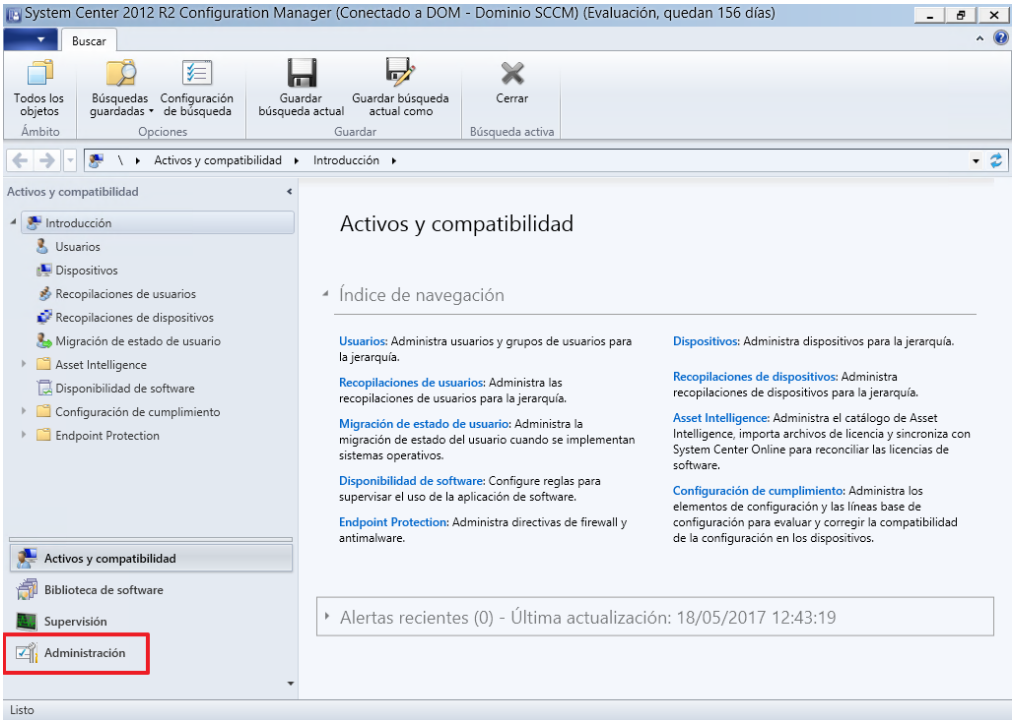
7.4. COMUNICACIÓN CON MS SCCM 2012 R2

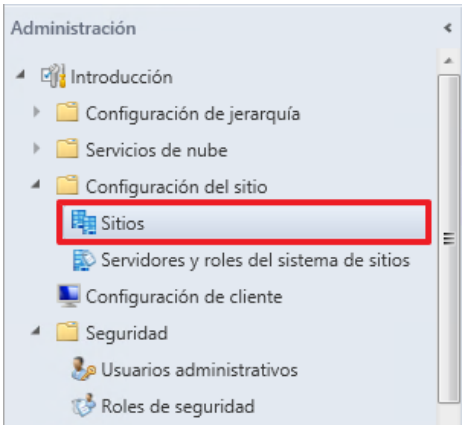
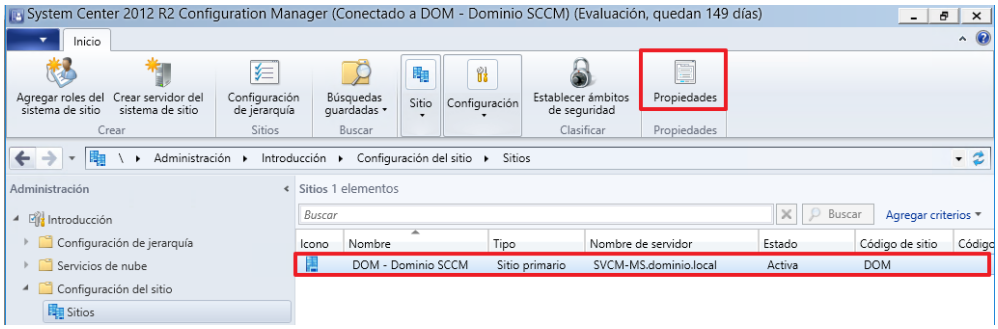
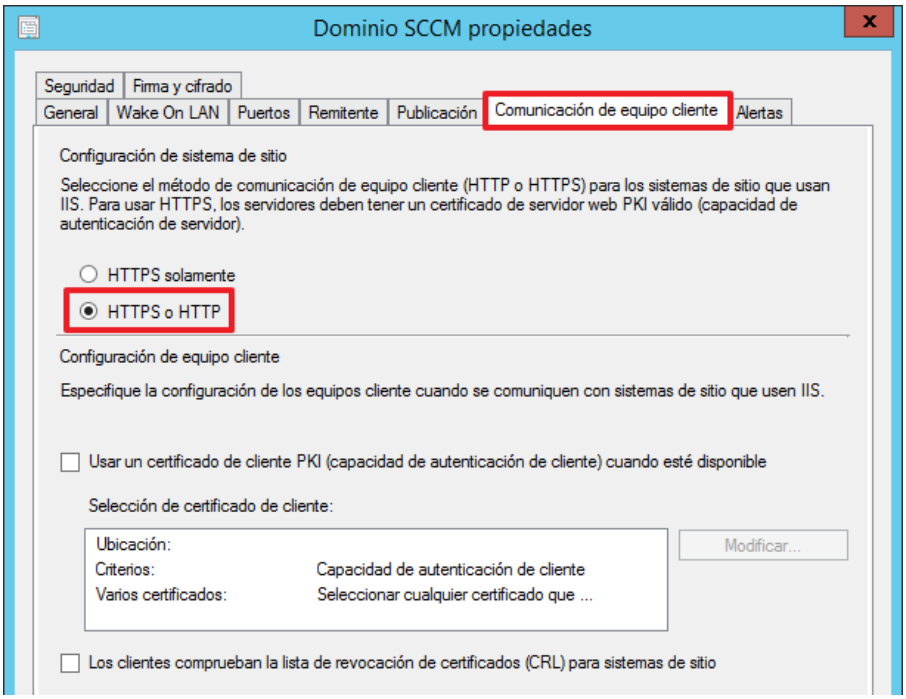
Microsoft SCCM 2012 R2 permite el establecer el método de comunicación de los equipos cliente estableciéndose en función del nivel de seguridad que se establezca en el ENS.

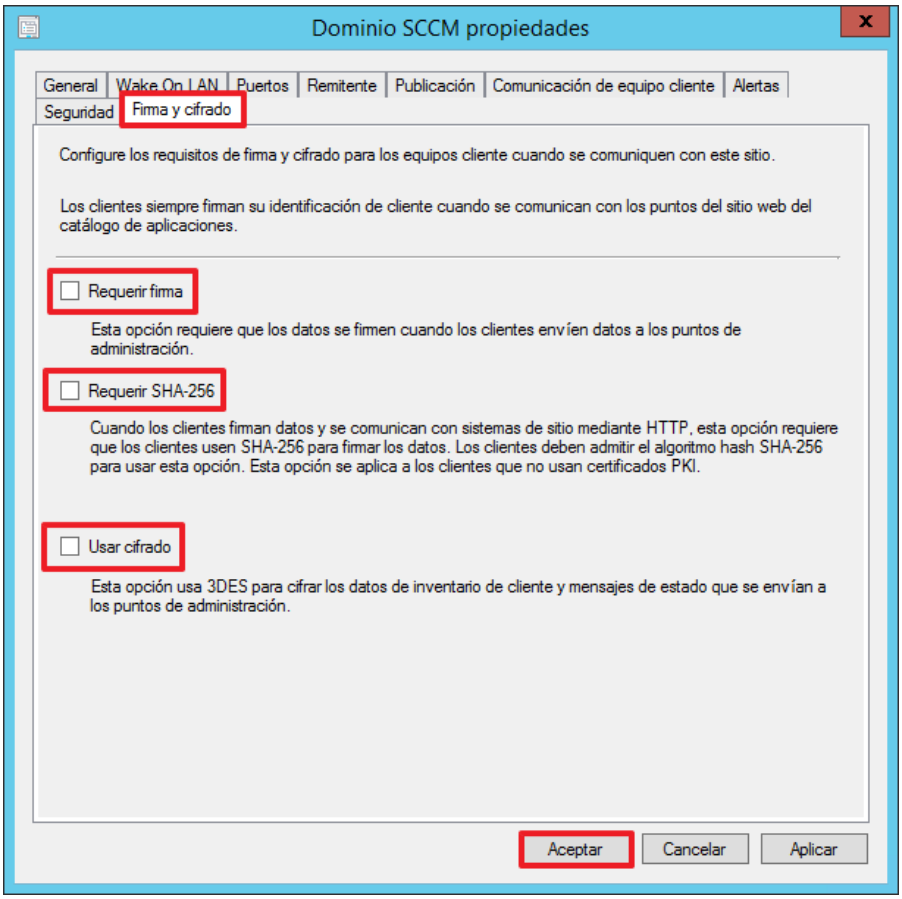
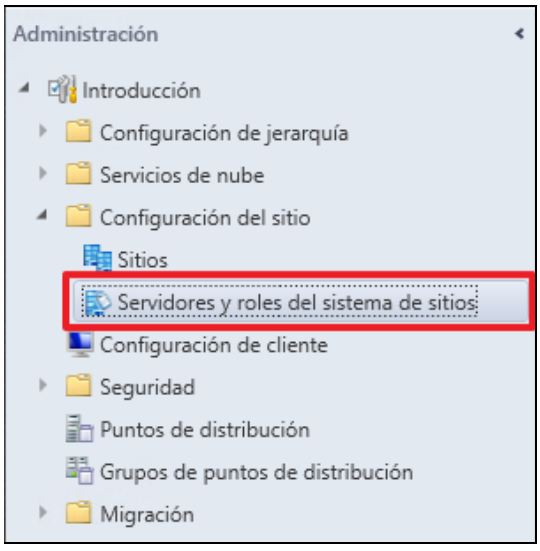
A continuación, se describe un paso a paso para reforzar la seguridad de las comunicaciones de MS SCCM 2012 R2.

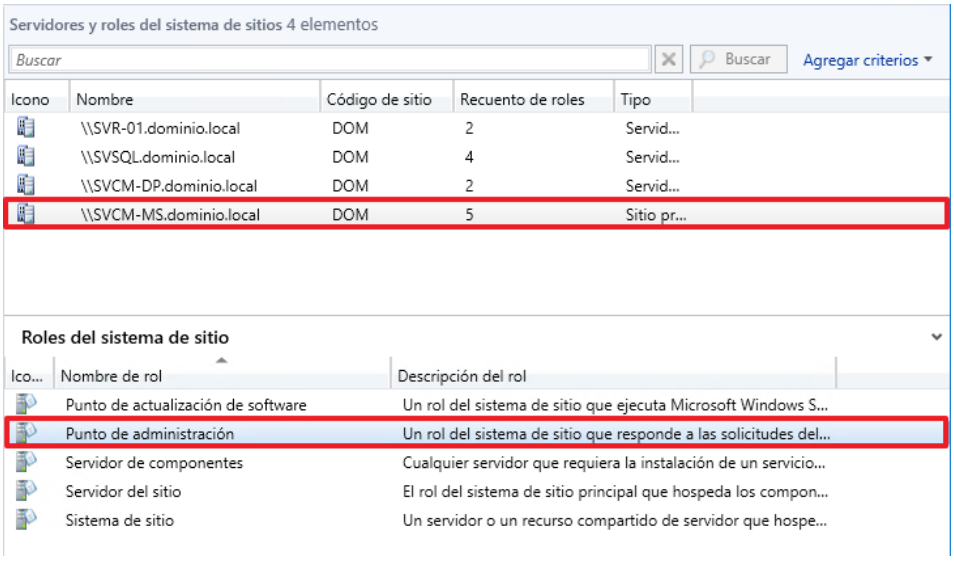
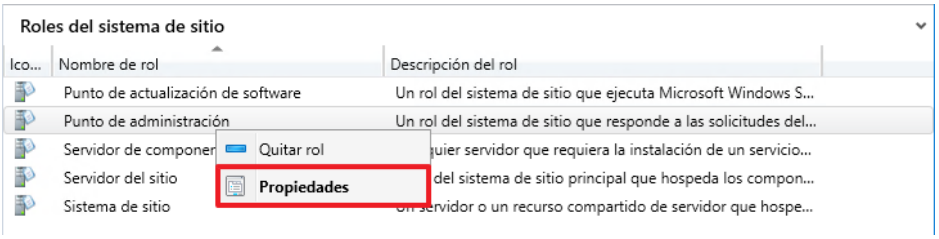
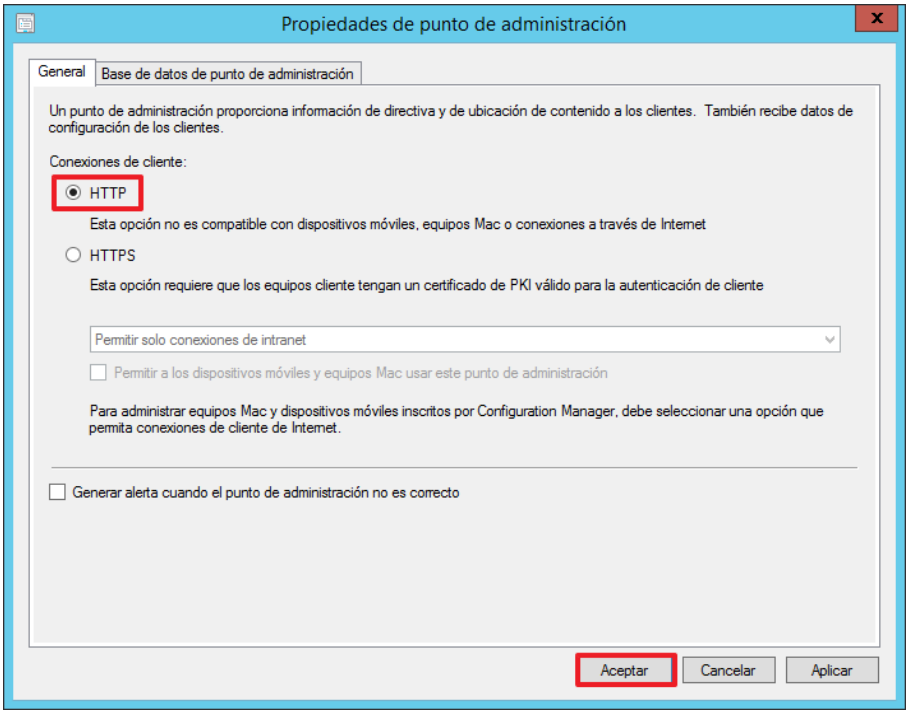
Nota: Si requiere aumentar la seguridad de las comunicaciones internas mediante comunicaciones basadas en HTTPS, puede aplicar el paso a paso 7.4 COMUNICACIÓN CON MS SCCM 2012 R2 correspondiente al ANEXO C.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL ALTO DEL ENS, siempre que la organización presente una infraestructura de PKI adecuada para su integración con MS SCCM 2012 R2.

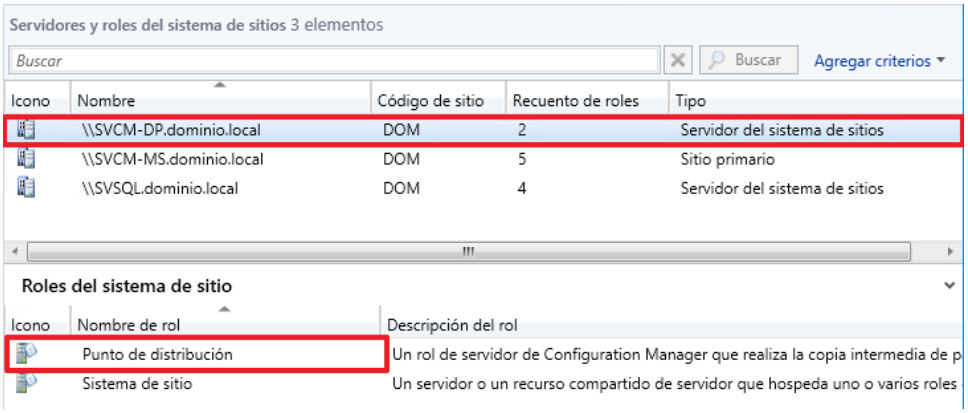
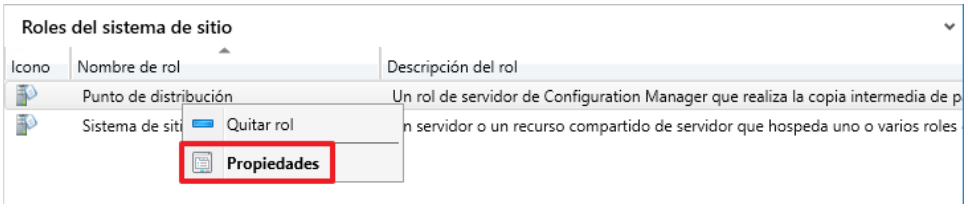
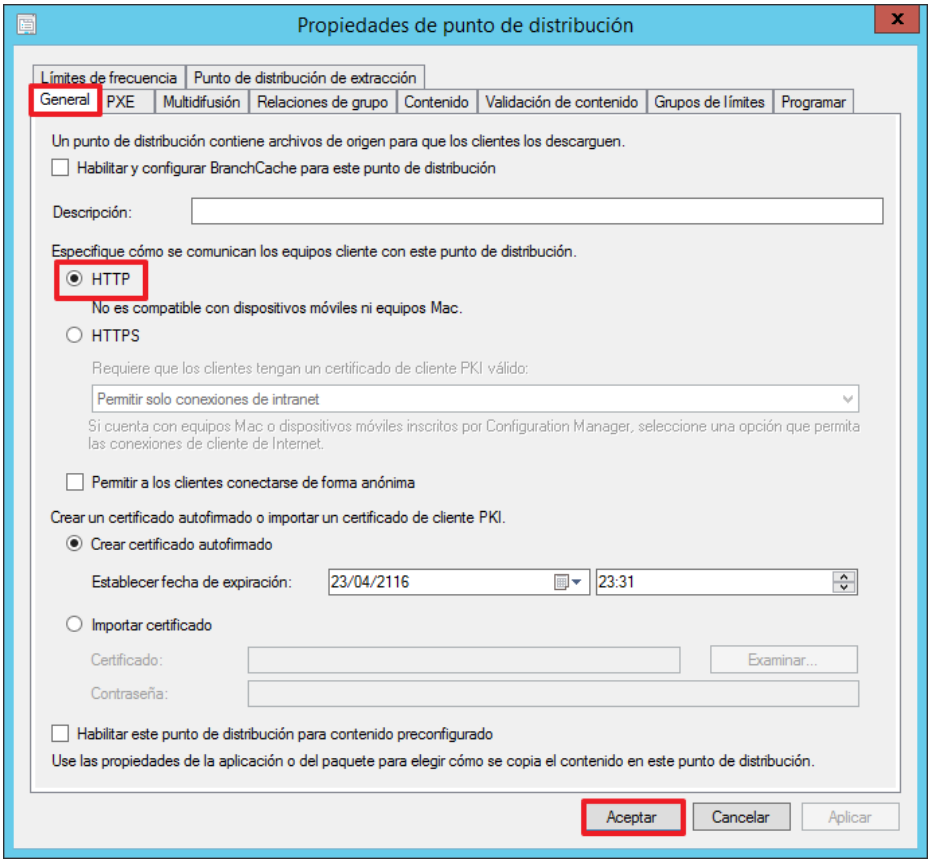
Paso	Descripción
280.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
281.	Pulse sobre el menú inicio. 
282.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
283.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
284.	Seleccione el apartado “Administración”. 

Paso	Descripción
285.	Despliegue “**Configuración del sitio > Sitios**”. 
286.	Seleccione el sitio que desea configurar y pulse sobre el botón “Propiedades” ubicado en la barra superior. 
287.	Seleccione la pestaña “Comunicación de equipo cliente” y marque la opción “HTTPS o HTTP. 

Paso	Descripción
288.	Sitúese en la pestaña “Firma y cifrado”, desmarque las siguientes opciones disponibles y pulse “Aceptar” para finalizar la configuración. En el caso que se quiera reforzar la seguridad en este apartado, marque alguna de las tres opciones disponibles. 
289.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 

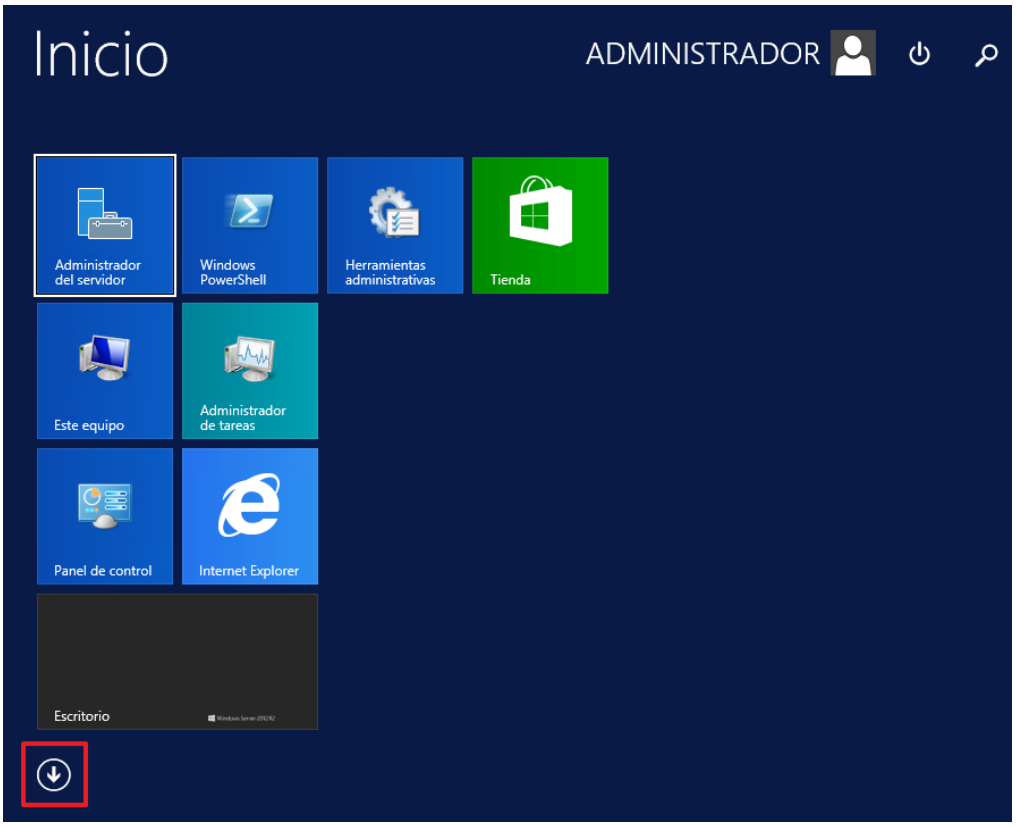
Paso	Descripción
290.	Seleccione el servidor que contiene el rol de “Punto de administración”. 
291.	Localice el rol de “Punto de administración” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 
292.	En la pestaña “General”, seleccione en “Conexiones de cliente:” la opción “HTTP” y pulse “Aceptar” para validar los cambios. 

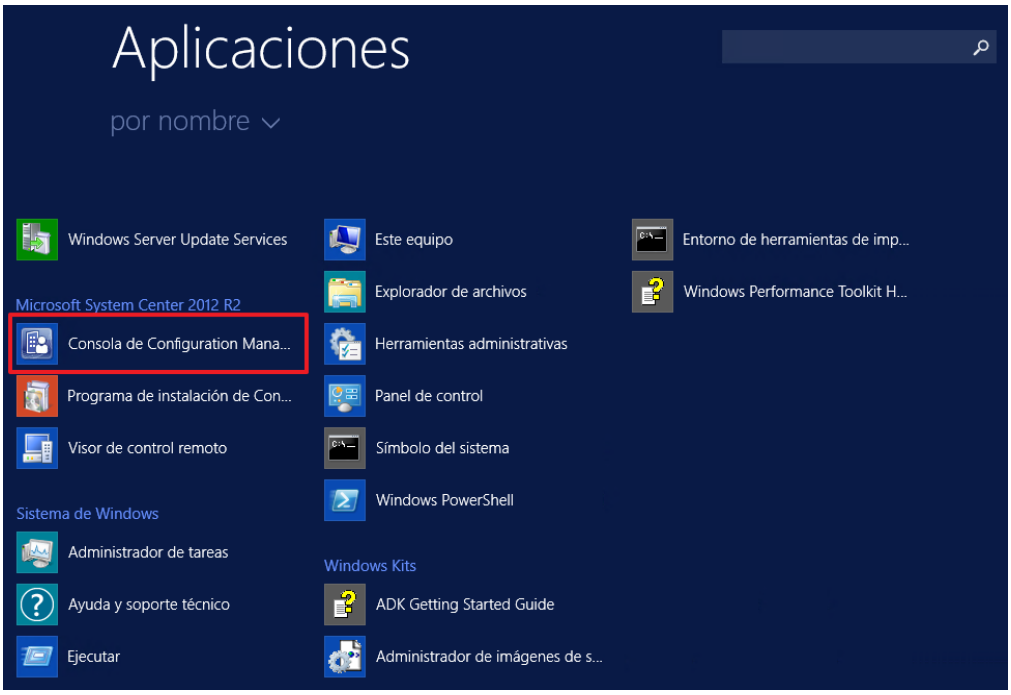
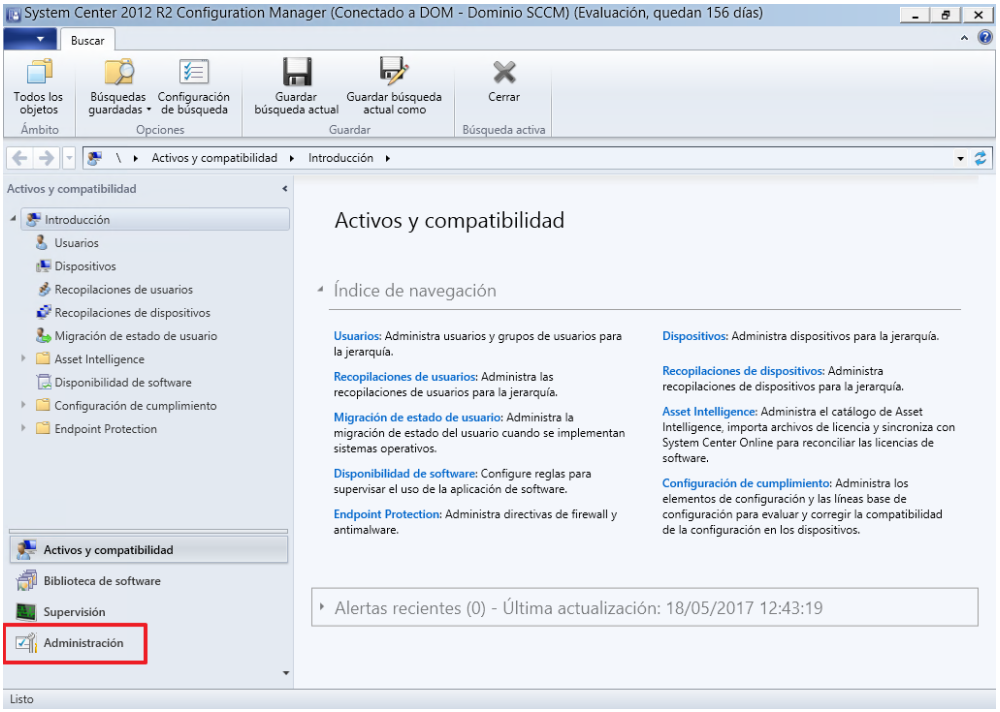
Paso	Descripción
293.	Seleccione el servidor que contiene el rol de “Punto de distribución”. 
294.	Localice el rol de “Punto de distribución” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 
295.	Seleccione en “General:” la opción “HTTP” y pulse “Aceptar” para validar los cambios. 

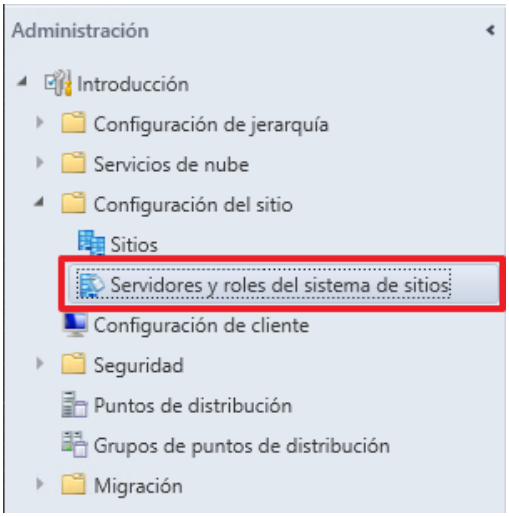
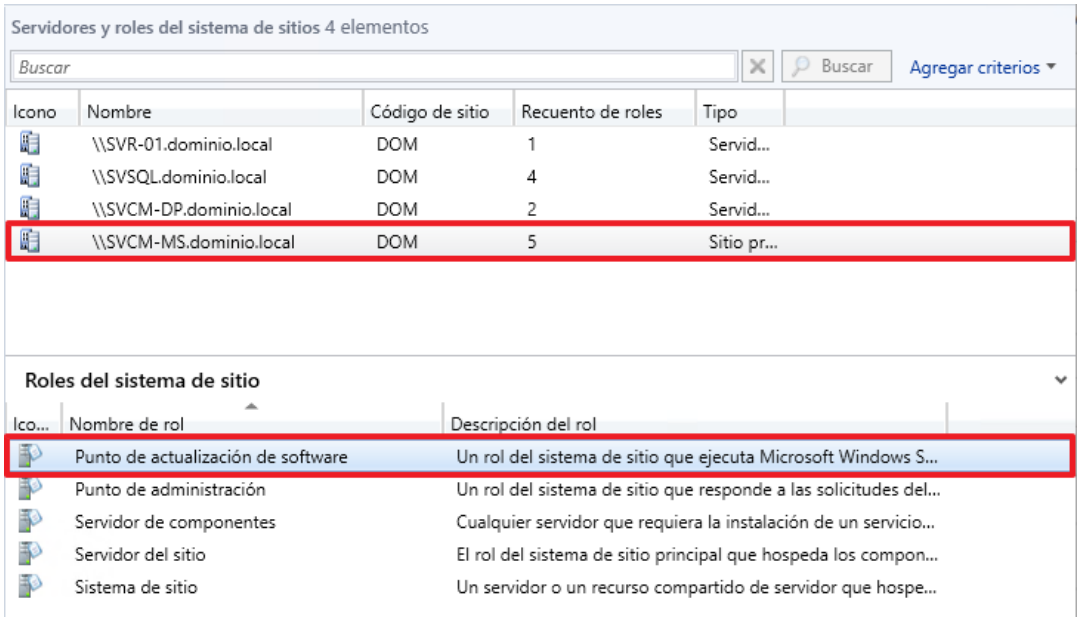
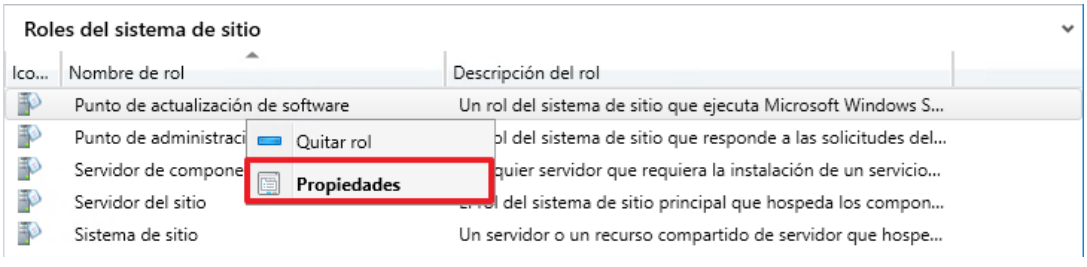
7.5. MANTENIMIENTO ACTUALIZACIONES DE SEGURIDAD

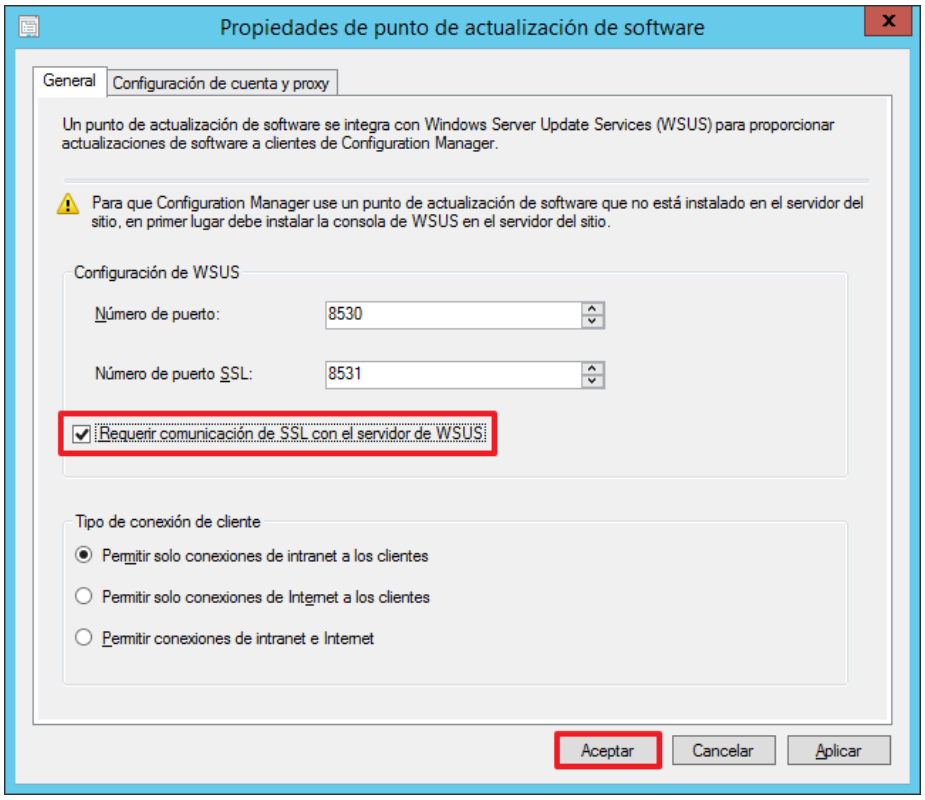
Microsoft SCCM 2012 R2 permite el administrar las actualizaciones de seguridad de clientes mediante el rol de "**Punto de actualización de software**", estableciendo y desplegando las actualizaciones publicadas por el fabricante.

A continuación, se describe un paso a paso para configurar la comunicación con el servidor que contiene el rol de WSUS es cual es necesario para el correcto funcionamiento del rol de "**Punto de actualización de software**".

Paso	Descripción
296.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
297.	Pulse sobre el menú inicio. 
298.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
299.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
300.	Seleccione el apartado “Administración”. 

Paso	Descripción
301.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 
302.	Seleccione el servidor que contiene el rol de “Punto de actualización de software”. 
303.	Localice el rol de “Punto de actualización de software” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 

Paso	Descripción
304.	Seleccione en la pestaña “General” la opción “Requerir comunicación SSL con el servidor de WSUS” y pulse “Aceptar” para validar los cambios. 

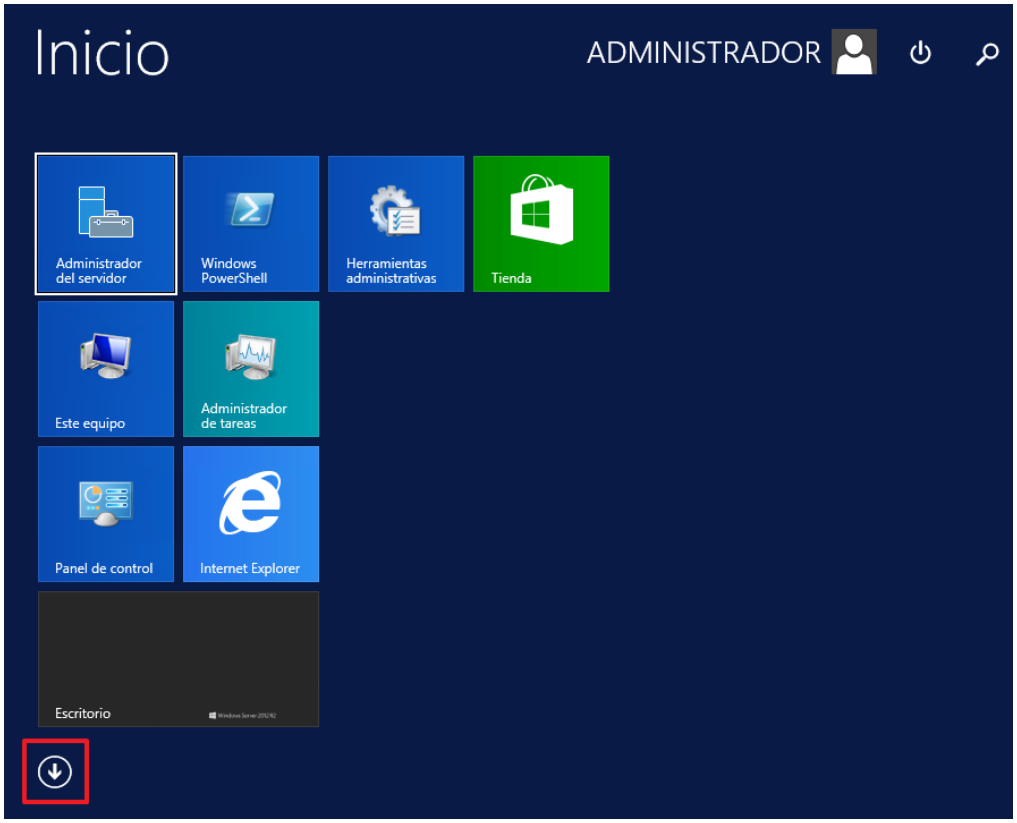
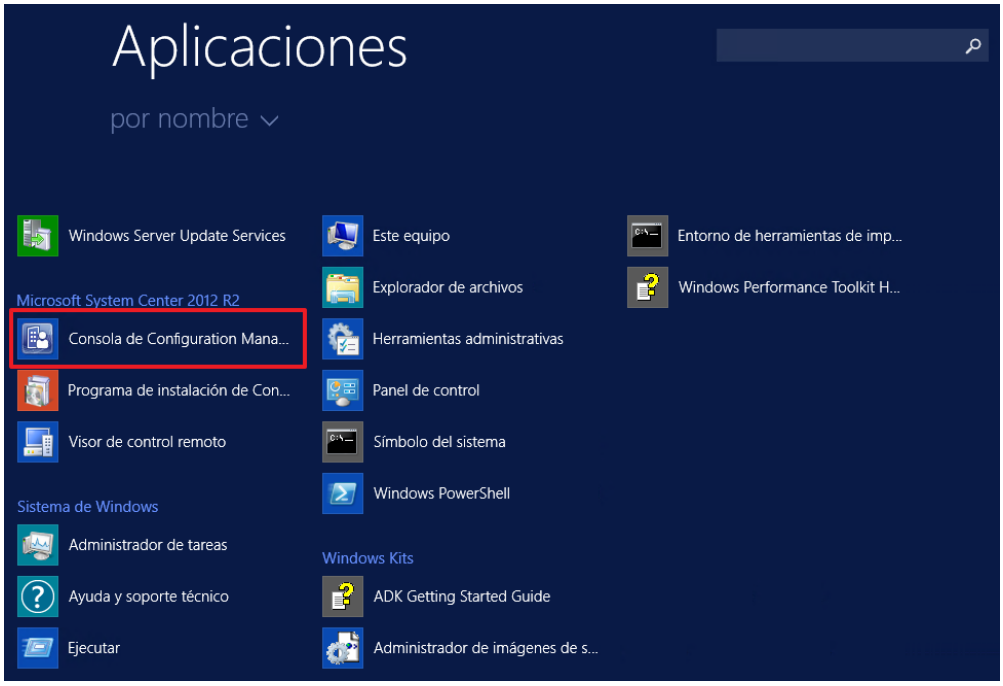
7.6. CONFIGURACIÓN HERRAMIENTAS REMOTAS

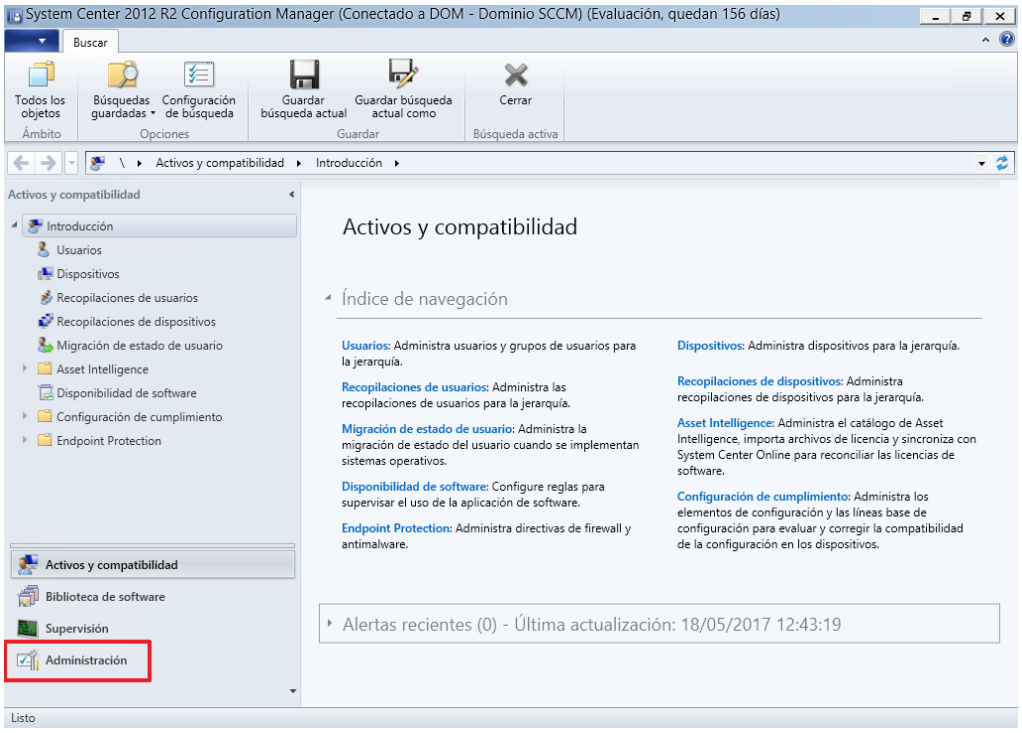
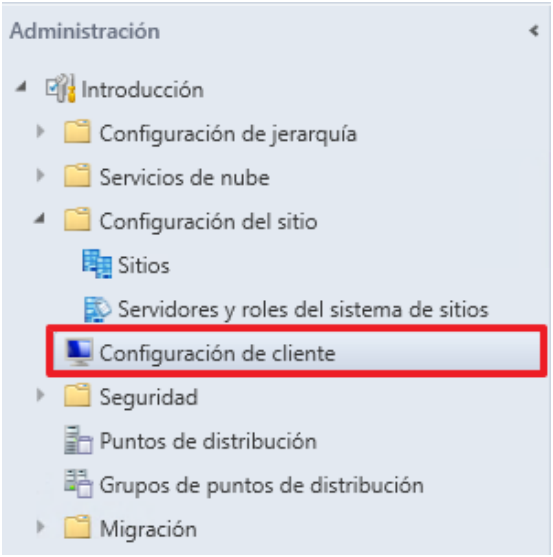
Microsoft SCCM 2012 R2 permite establecer la configuración de control remoto en equipos clientes que se aplica a todos los clientes de la jerarquía.

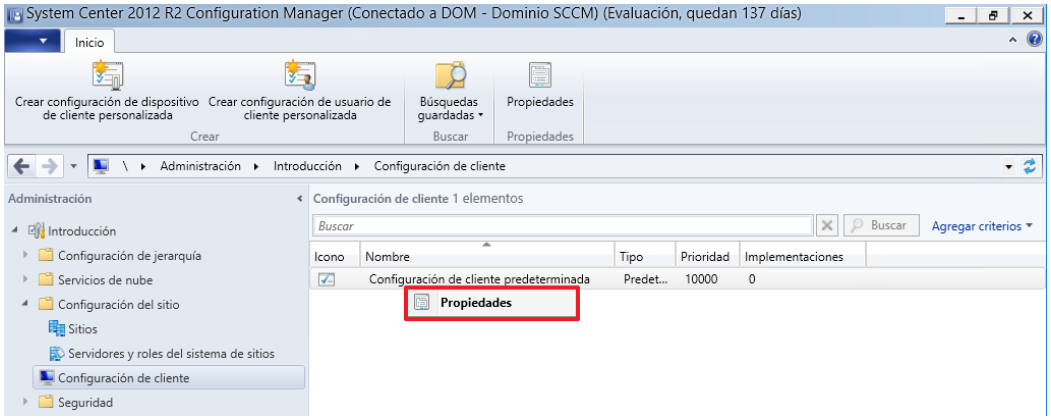
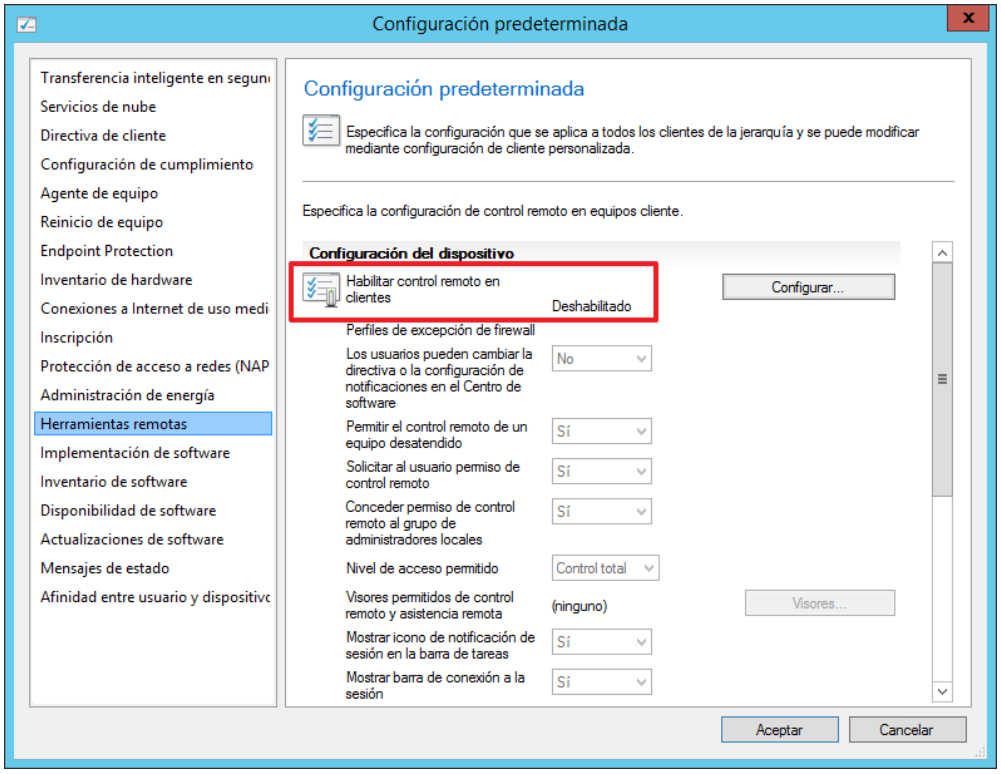
Se recomienda que esta herramienta, siempre que no sea un requisito de la organización, este en estado deshabilitado y en caso de estar habilitada, asegurarse que está configurada correctamente para que únicamente los usuarios con privilegios tengan acceso a esta característica de control remoto de equipos cliente.

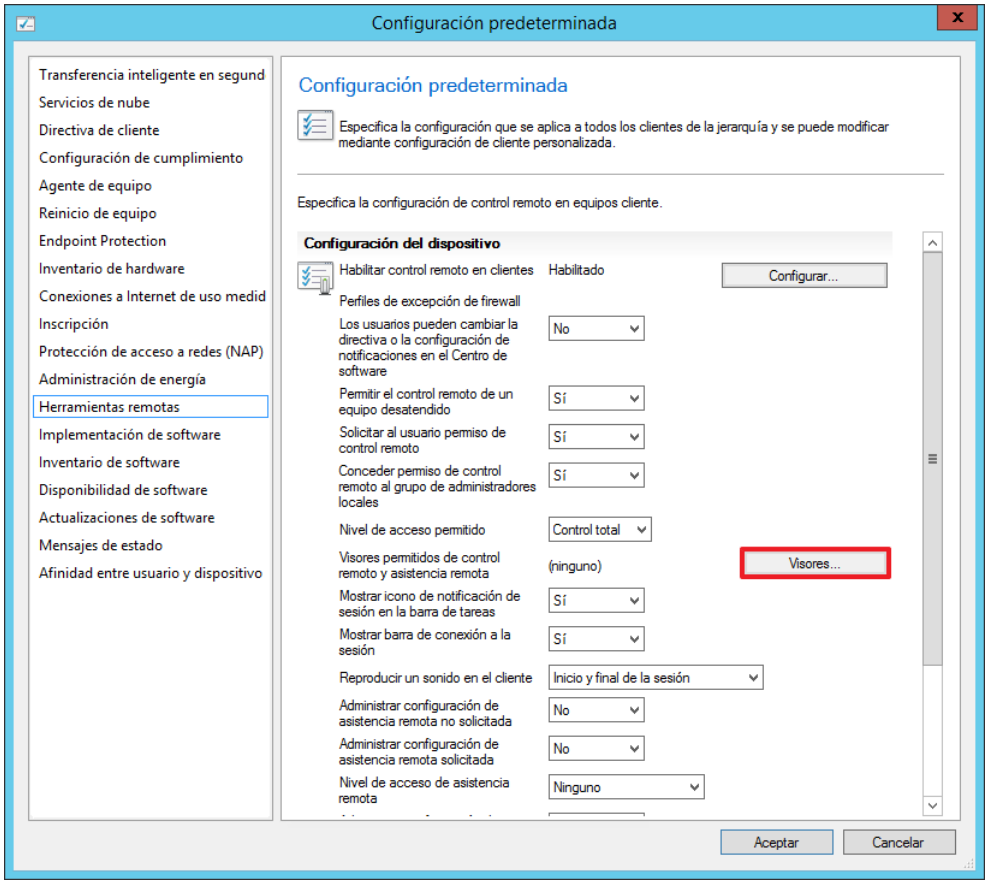
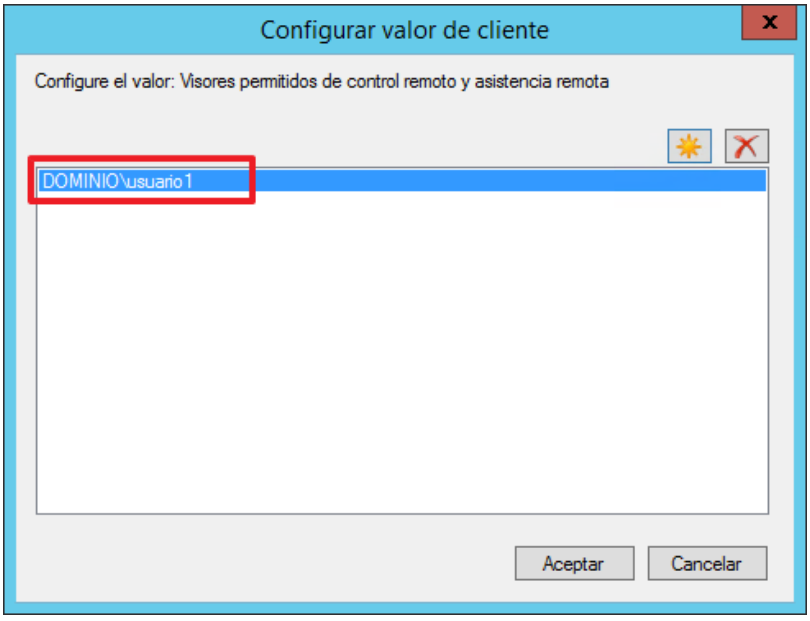
A continuación, se describe como establecer la configuración de control remoto en equipos clientes.

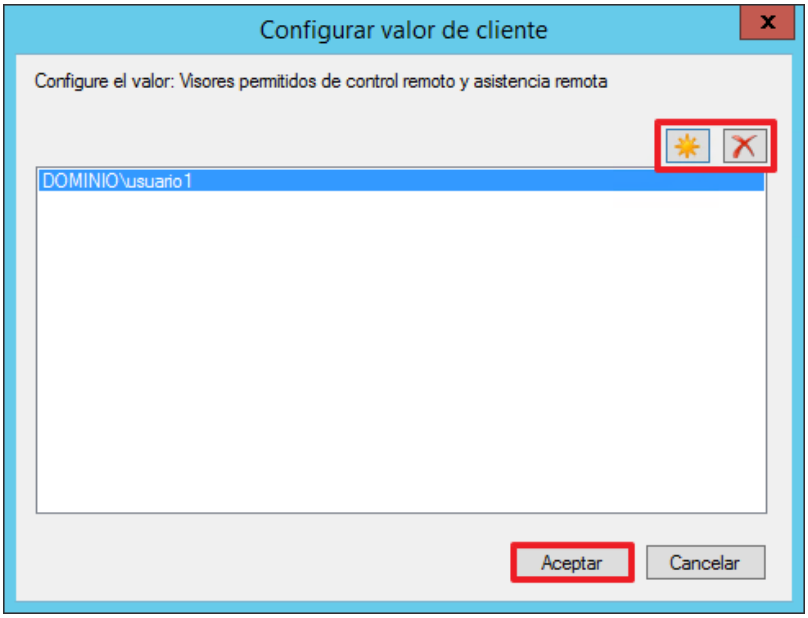
Paso	Descripción
305.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
306.	Pulse sobre el menú inicio. 

Paso	Descripción
307.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
308.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
309.	Seleccione el apartado “Administración”. 
310.	Despliegue “**Configuración del sitio > Configuración de cliente**”. 

Paso	Descripción
311.	Seleccione “Configuración de cliente predeterminada”, pulse con el botón derecho, y seleccione la opción “Propiedades” del menú contextual.  **Nota:** Deberá adaptar los pasos a su organización y seleccionar la configuración de cliente que se esté aplicado a sus equipos cliente.
312.	Localice la pestaña “Herramientas remotas” en la ventana de Configuración predeterminada y a continuación, verifique que la opción “Habilitar control remoto en clientes” esta deshabilitado.  **Nota:** En caso que en su organización se esté haciendo uso de esta característica, y aparezca “habilitado”, deberá corroborar los usuarios que tienen permisos para usar la característica.

Paso	Descripción
313.	Para comprobar los usuarios que tienen permiso de acceso remoto, pulse el botón “Visores…”. 
314.	Compruebe en el listado los usuarios que tienen permisos de control remoto. 

Paso	Descripción
315.	En caso de requerir añadir o eliminar algún usuario o grupos de usuarios seleccione los dos botones situados en la parte derecha de la imagen en función de la acción que desee realizar. Pulse “Aceptar” una vez haya finalizado la configuración. 

7.7. REGISTRO DE LA ACTIVIDAD

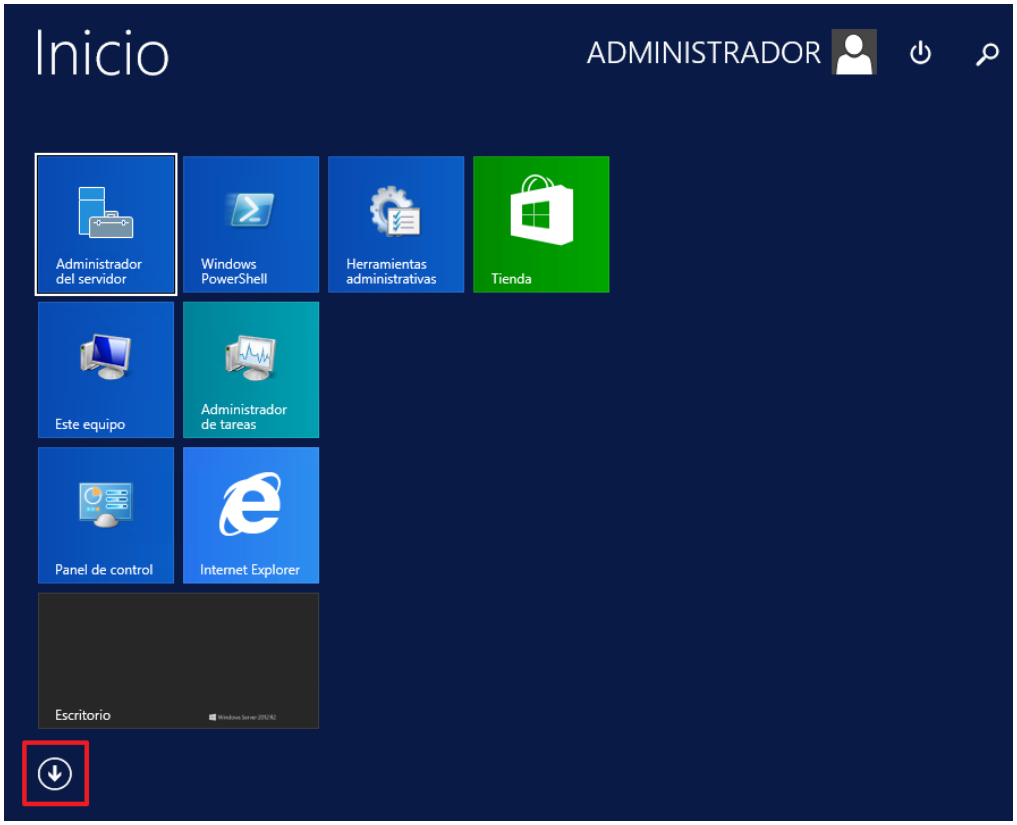
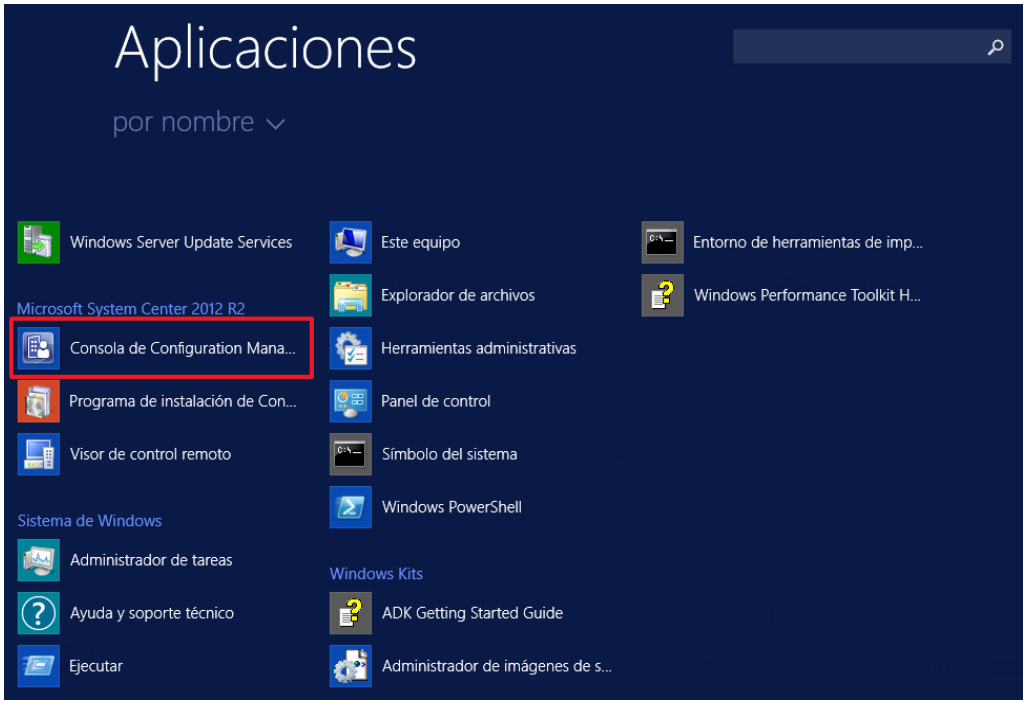
Según el ENS “Se registrará toda aquella evidencia que pueda, respaldar una demanda judicial, o hacer frente a ella, cuando el suceso pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos”.

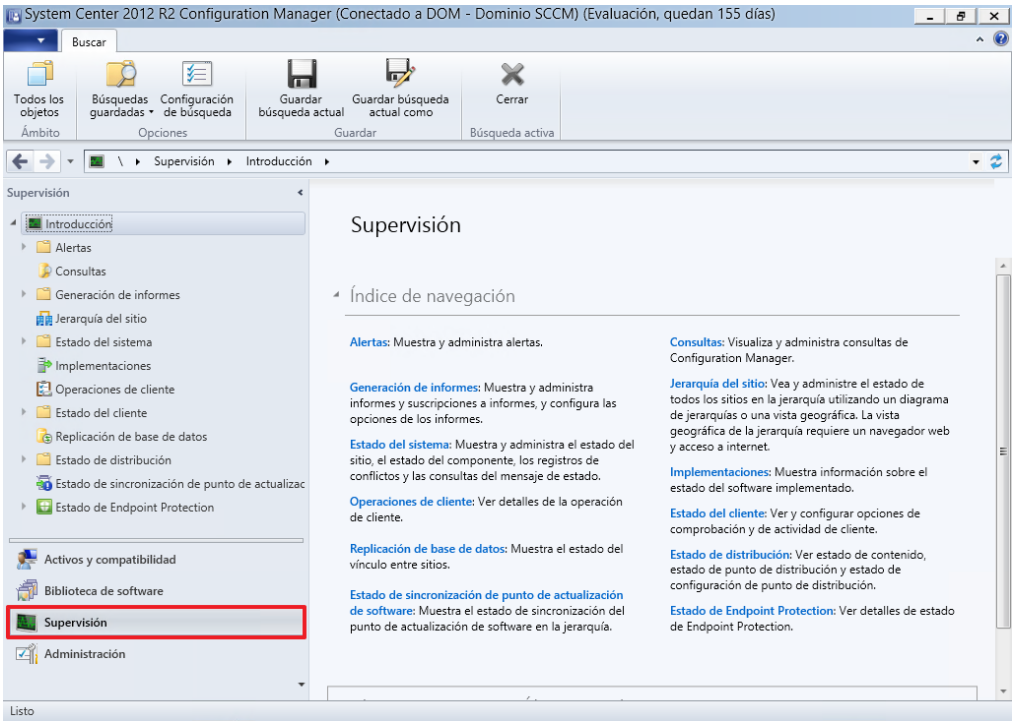
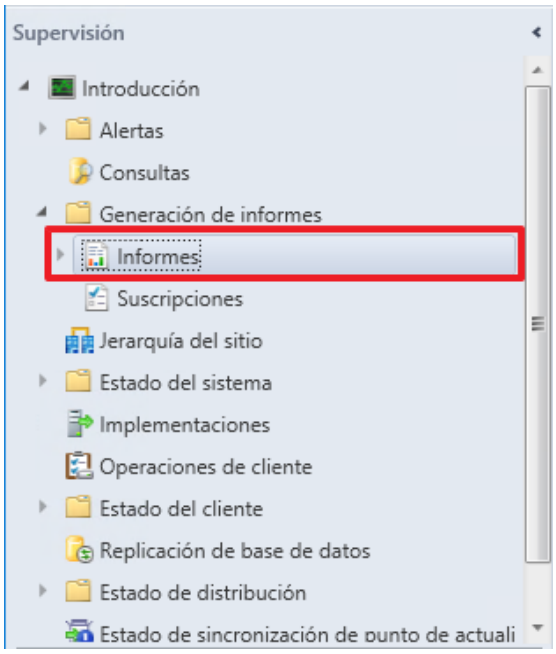
Además, se incluirá la actividad de los usuarios y, con especial atención, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

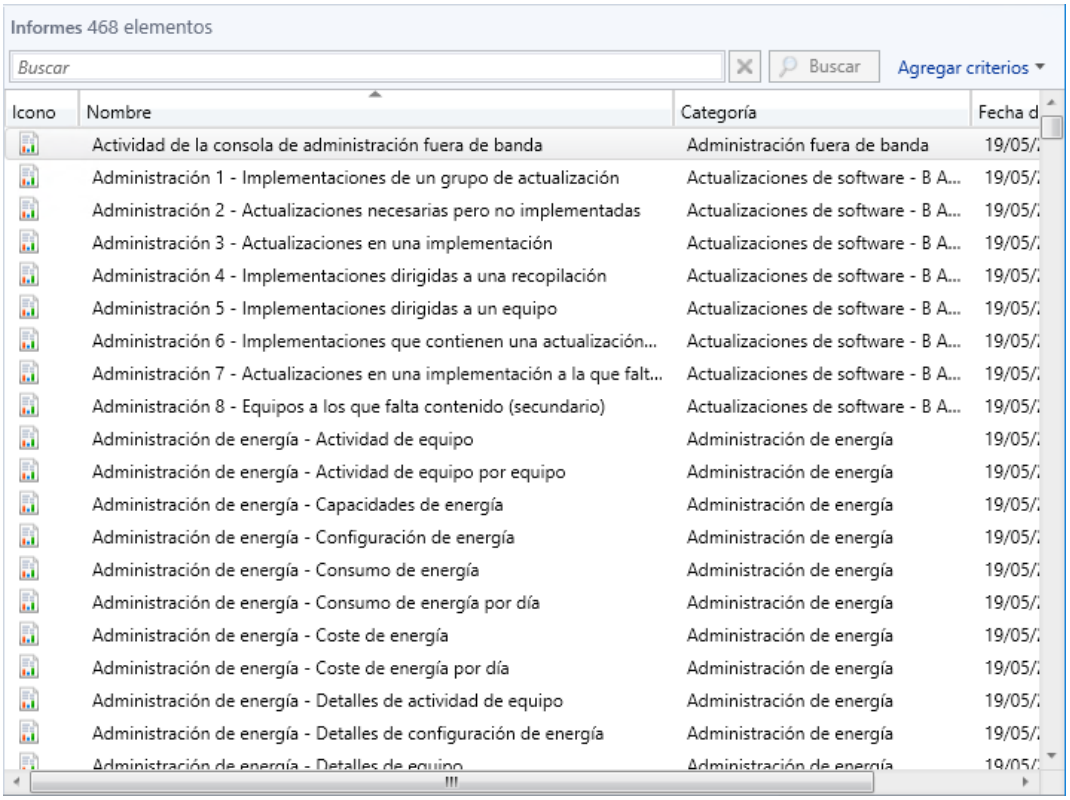
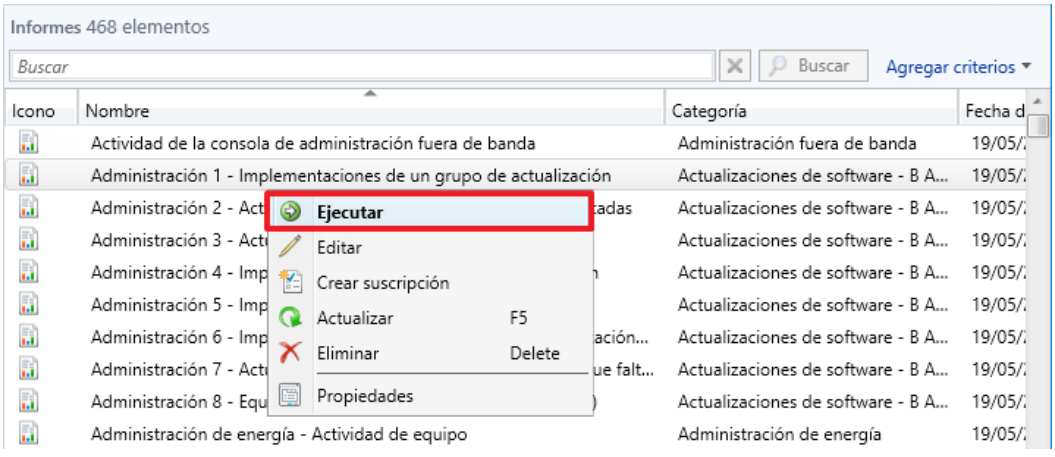
Se ha de tener en consideración que la primera medida para reforzar la seguridad es el mantenimiento y aplicación correcta de la segregación de roles y funciones descrito en el punto 7.2 de la presente guía, limitando con ello el campo de acción de los usuarios administrativos.

A continuación, se muestra un paso a paso para ver los informes de actividad de MS SCCM 2012 R2.

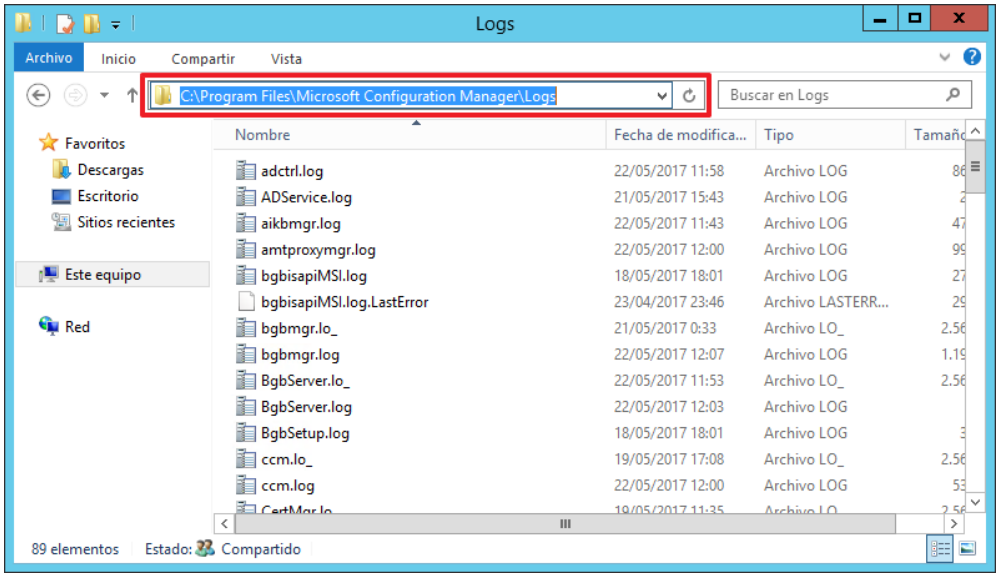
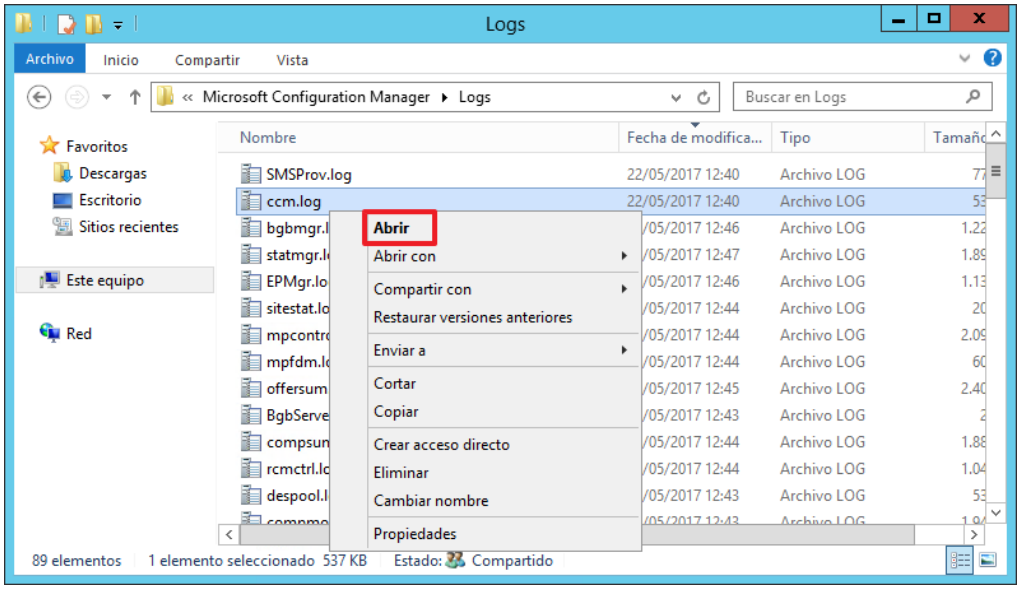
Paso	Descripción
316.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
317.	Pulse sobre el menú inicio. 

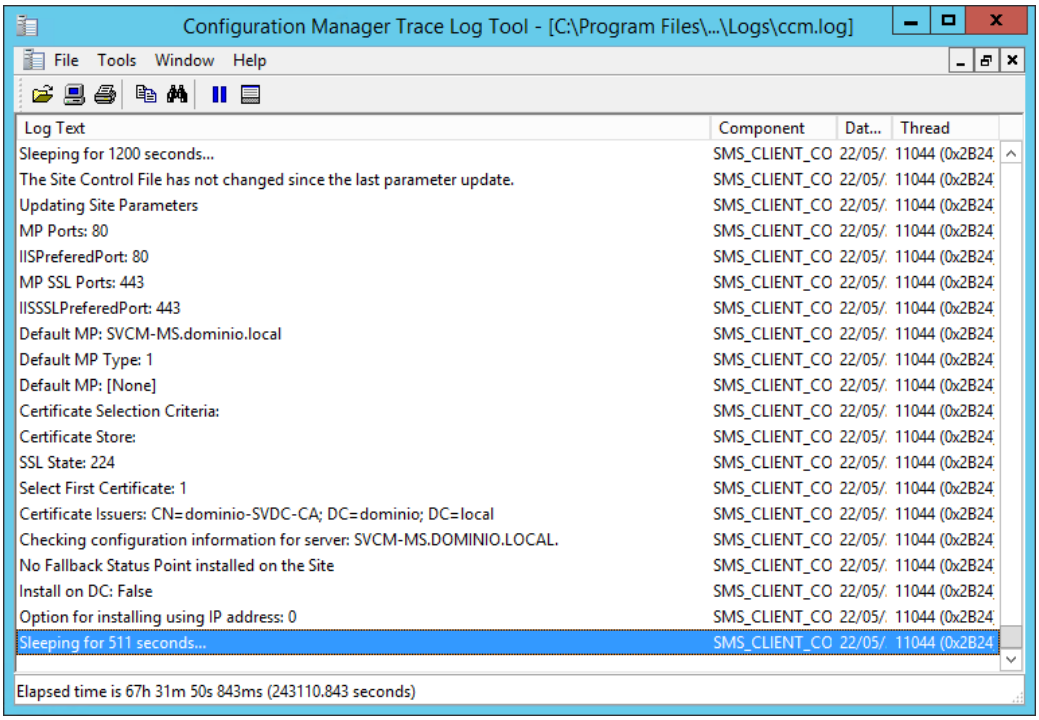
Paso	Descripción
318.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
319.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
320.	Seleccione el apartado “Supervisión”. 
321.	Despliegue “**Generación de informes > Informes**”. 

Paso	Descripción
322.	Seleccione de entre todos los informes disponibles el que más se adecue a sus necesidades. 
323.	Una vez localizado, pulse con el botón derecho y seleccione la opción “Ejecutar” del menú contextual para visualizar los datos del informe seleccionado.  **Nota:** En este ejemplo se selecciona el informe “Administración 1 – Implementaciones de un grupo de actualización” por lo que deberá adaptar los pasos a las necesidades de su organización.

Además de los informes presentados en MS SCCM 2012 R2 es posible consultar la actividad del servicio a través de los registros los cuales ofrecen una información más detallada de lo que puede estar sucediendo o buscar evidencias de acciones realizadas.

Paso	Descripción
324.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
325.	Pulse sobre el menú inicio y seleccione el icono “Explorador de archivos”. 
326.	Localice la ruta “C:\Program Files\Microsoft Configuration Manager\Logs”.  **Nota:** La ruta que contiene los registros puede variar en función de la ubicación de la instalación del producto MS SCCM 2012 R2.
327.	Seleccione el archivo.log que más se adecue a sus necesidades y haga clic botón derecho, y seleccione la opción “Abrir” del menú contextual. 

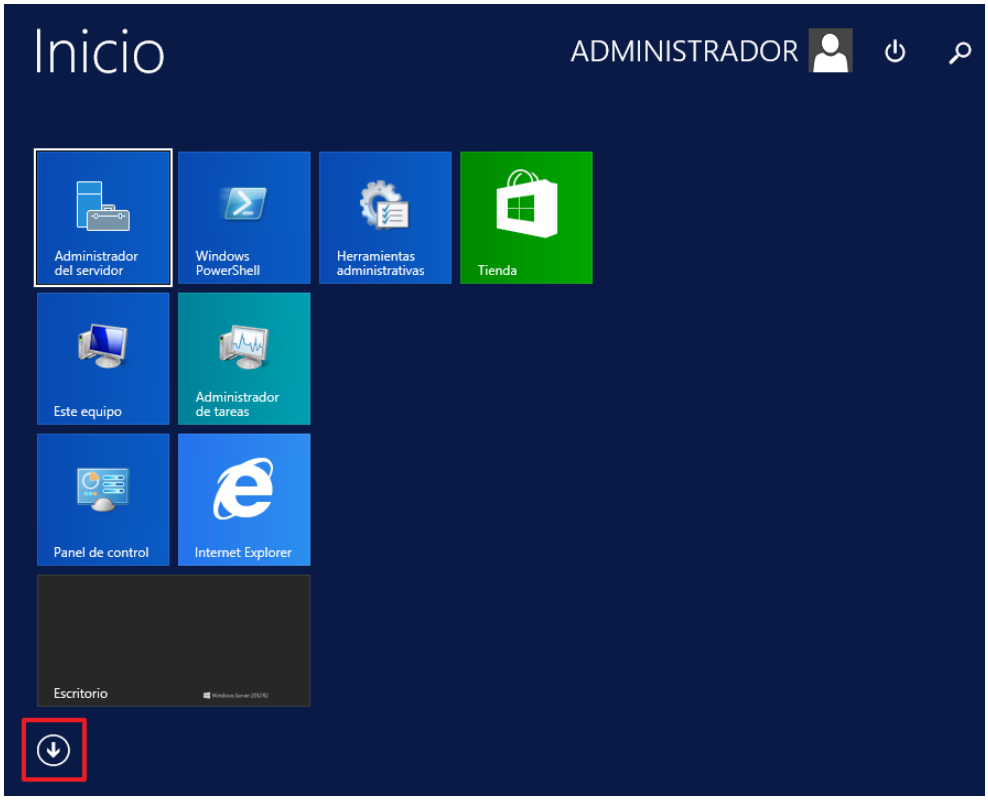
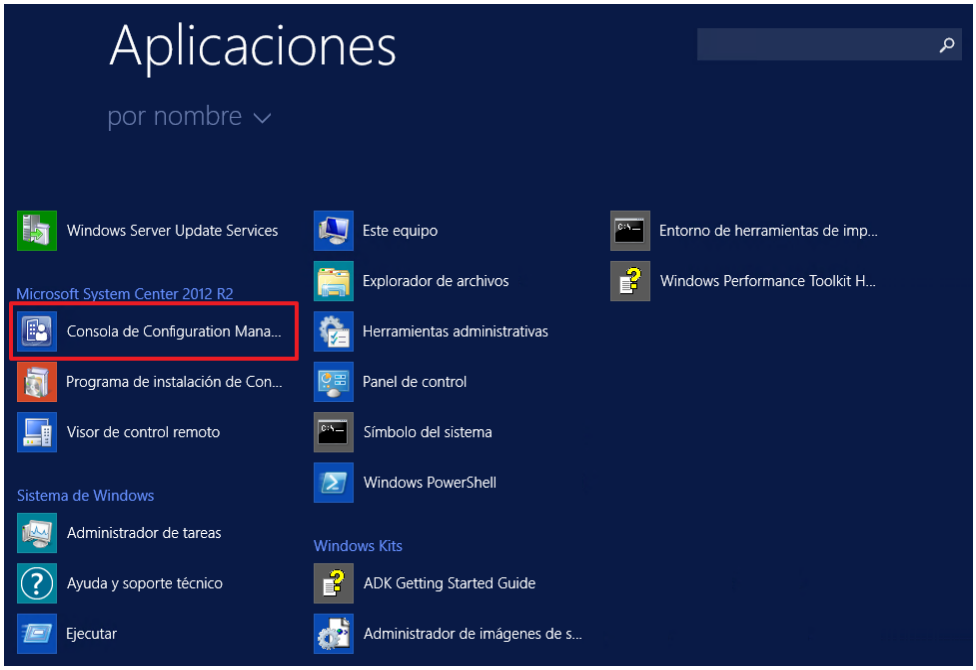
Paso	Descripción
328.	En la siguiente imagen, se muestra un ejemplo del fichero “ccm.log”.  **Nota:** En la imagen se visualiza el log mediante la herramienta propia de Configuration Manager Trace log tool, siendo posible utilizar cualquier editor de textos para su lectura.

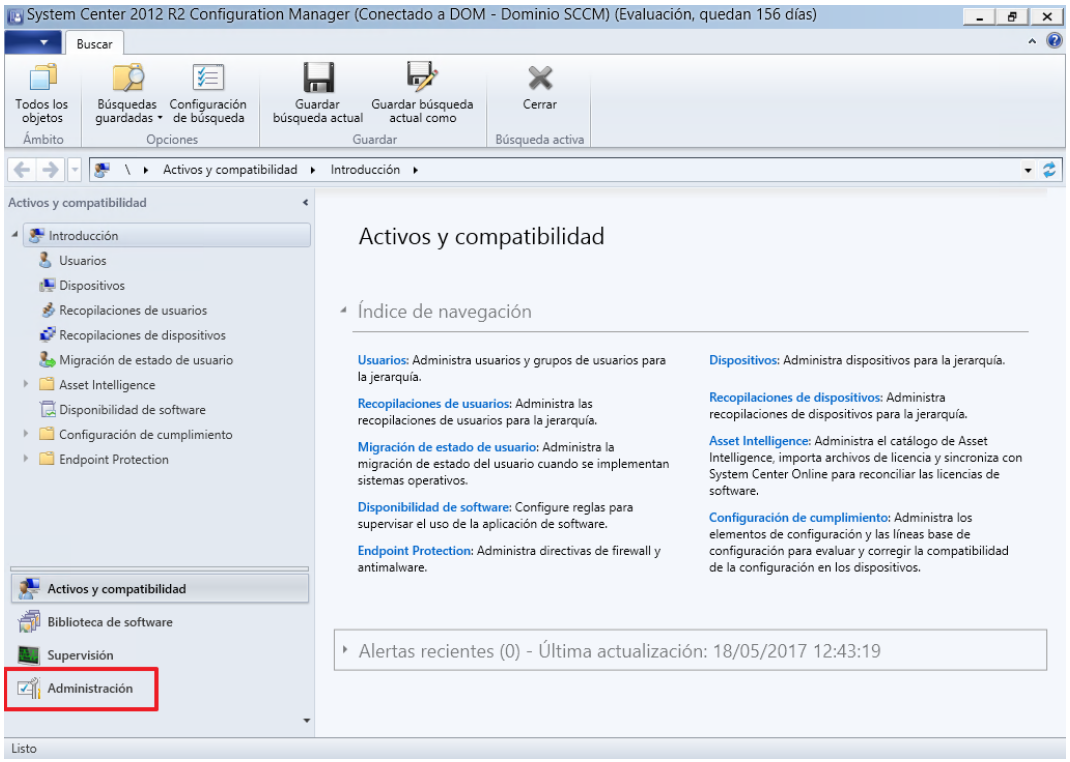
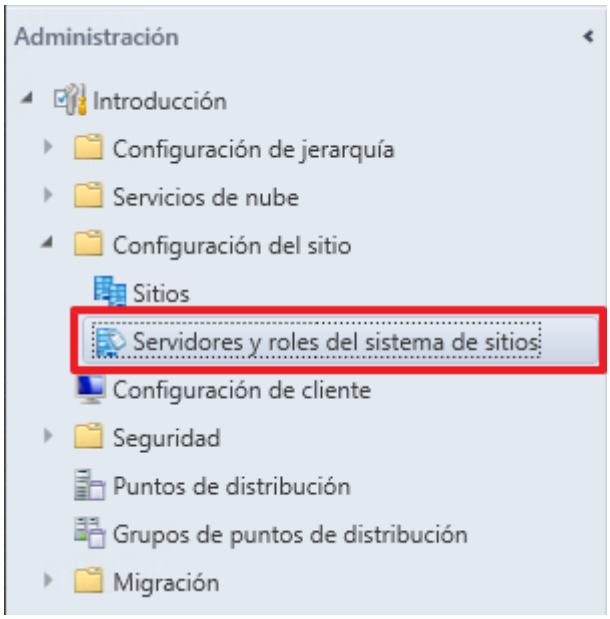
7.8. IMPLEMENTACIÓN DE SERVIDORES Y ROLES DEL SISTEMA DE SITIO

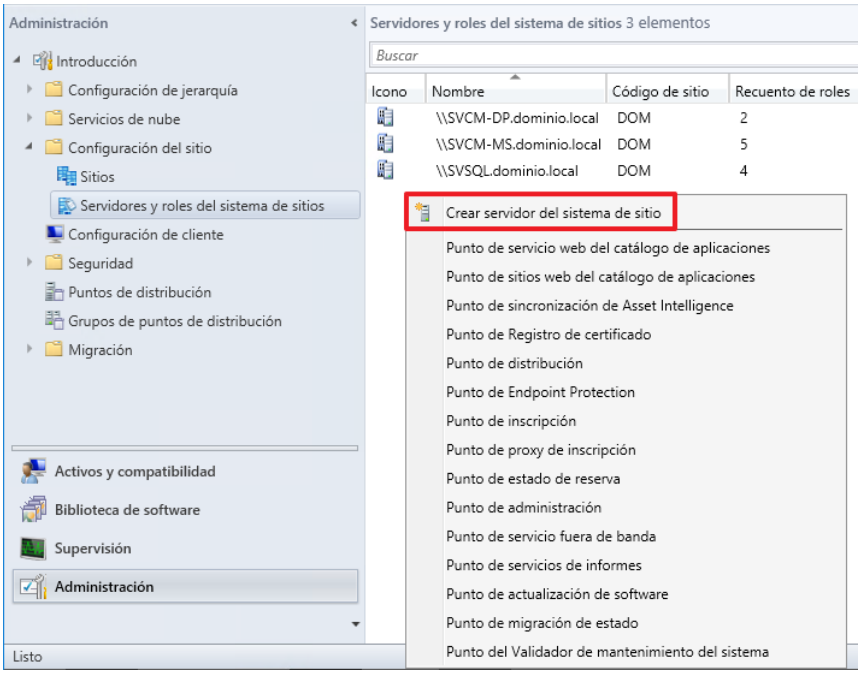
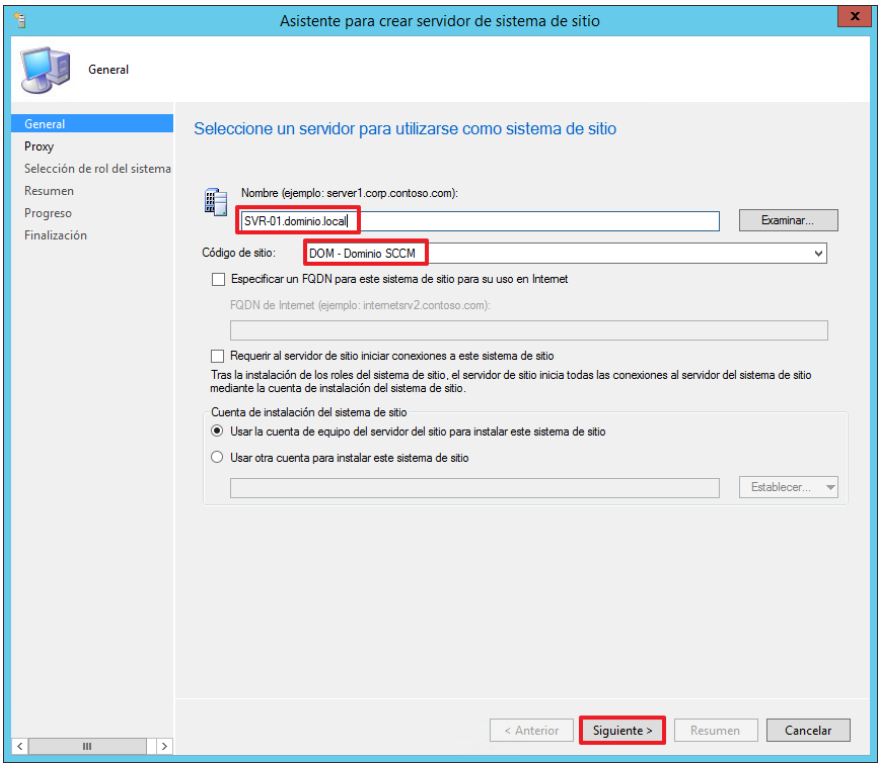
En MS SCCM 2012 R2 es posible agregar múltiples servidores que contengan varios roles para garantizar un servicio de alta disponibilidad, para en caso de que fallen los medios habituales de comunicación existan alternativas que garanticen el servicio.

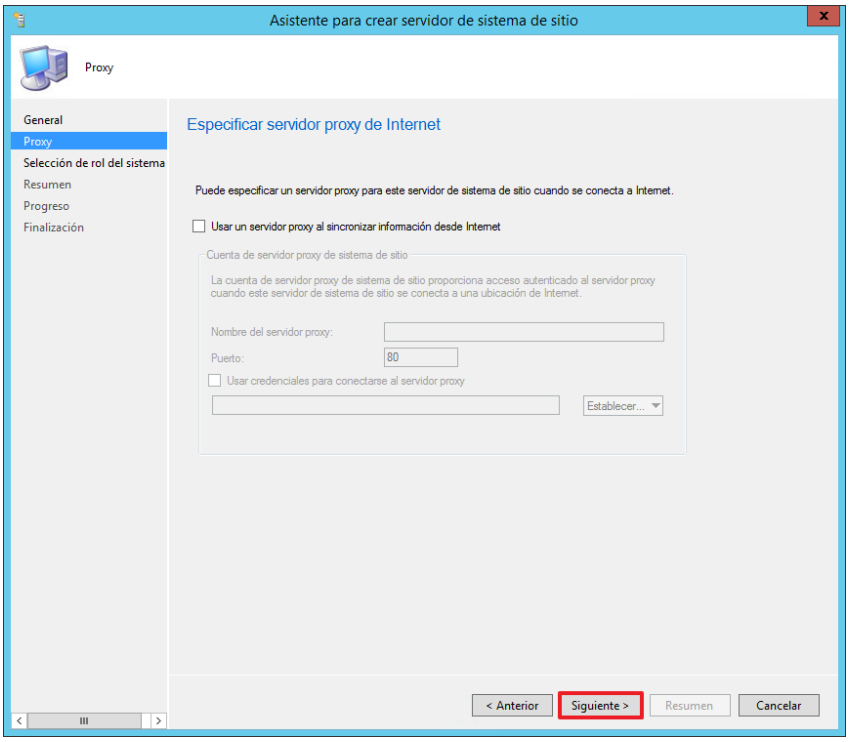
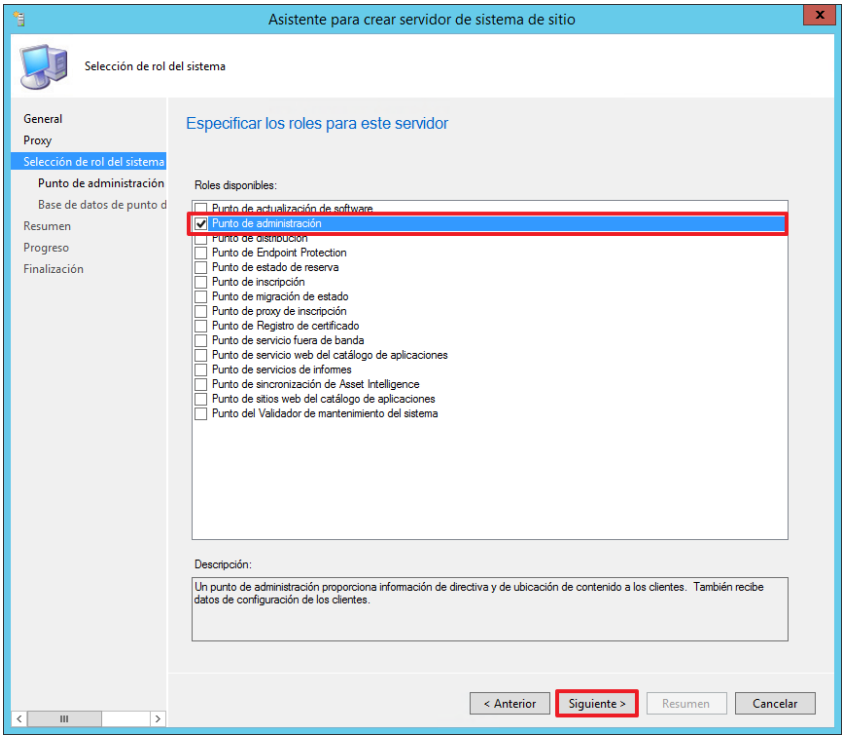
A continuación, se muestra un paso a paso en el que se detalla como agregar un servidor y a su vez como agregar un rol de sitio de MS SCCM 2012 R2.

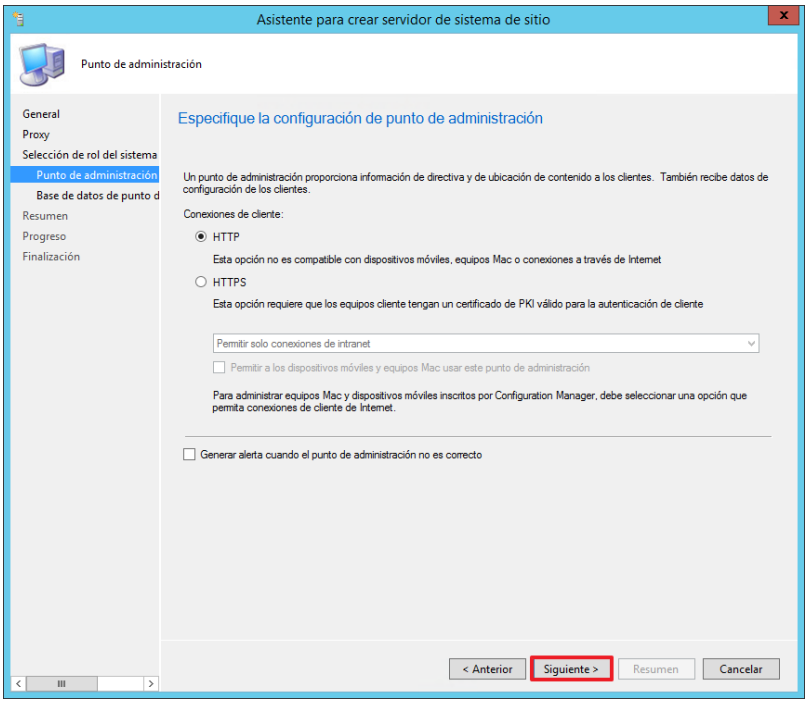
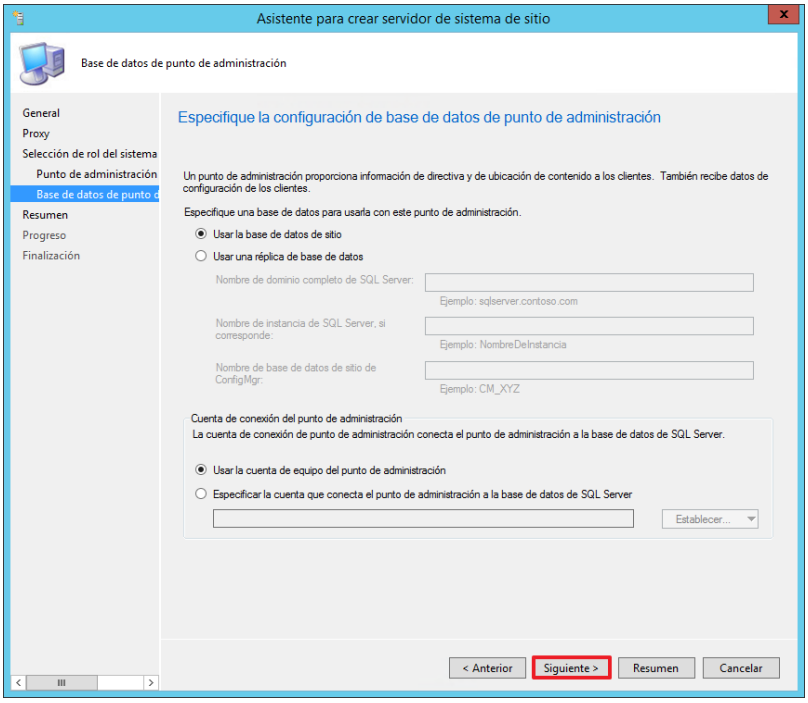
Paso	Descripción
329.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
330.	Pulse sobre el menú inicio. 

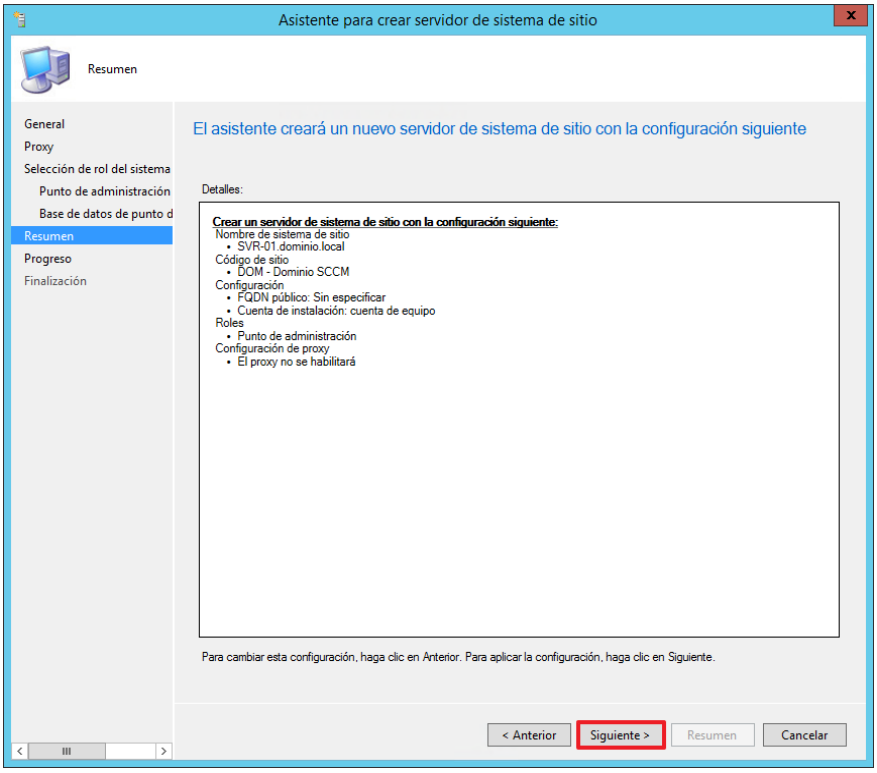
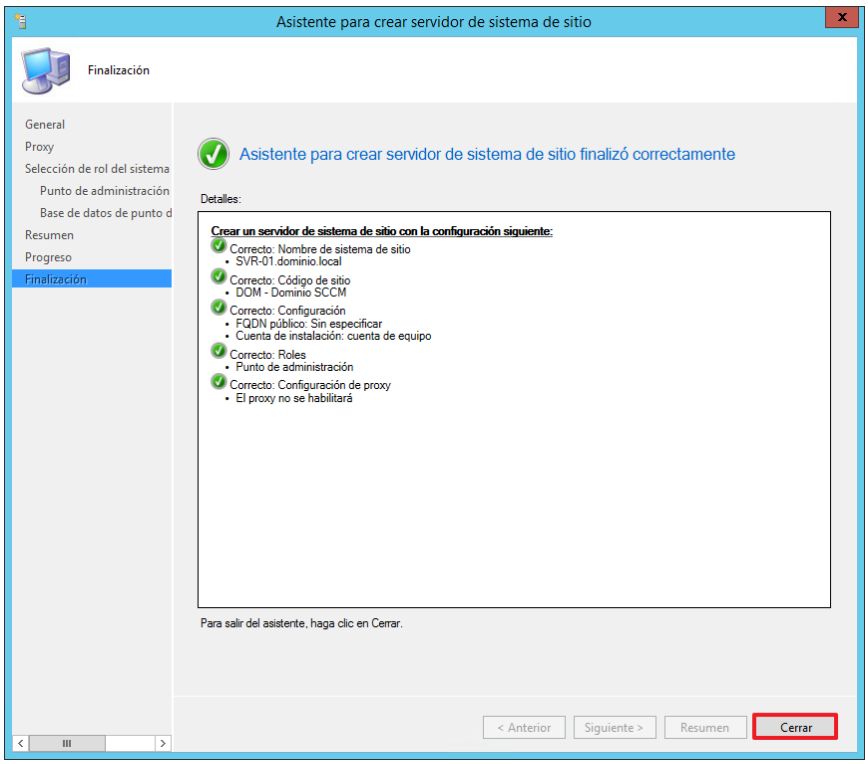
Paso	Descripción
331.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
332.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

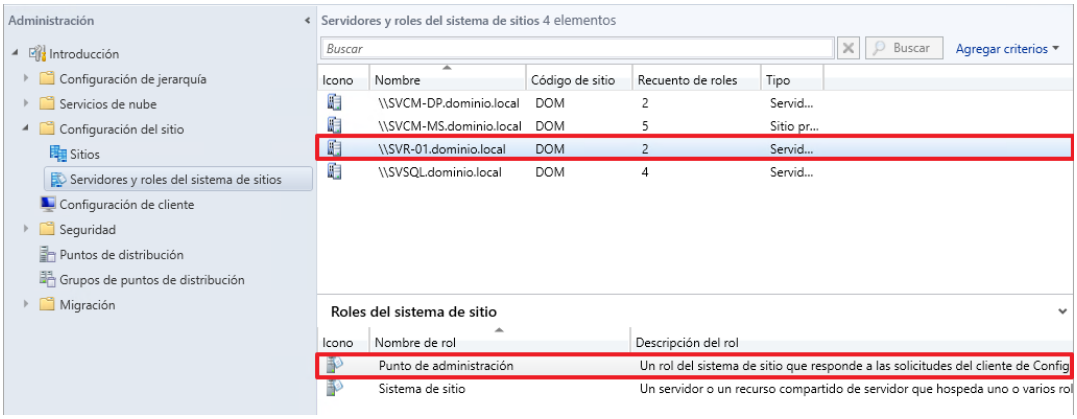
Paso	Descripción
333.	Seleccione el apartado “Administración”. 
334.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 

Paso	Descripción
335.	Pulse con el botón derecho sobre un espacio en blanco y seleccione la opción “crear servidor del sistema de sitio” para agregar un nuevo servidor al sitio ya creado.  **Nota:** Este paso contempla que usted ya tiene un sitio creado anteriormente y un servidor preparado para ser unido al sitio de Configuration Manager.
336.	Seleccione el nombre del servidor que desea añadir y el sitio y pulse “Siguiente >”  **Nota:** Tanto el nombre del servidor como el del sitio han sido creados para elaborar la presente guía por lo que deberá adaptar estos pasos a su organización.

Paso	Descripción
337.	En caso de que su servidor se conecte a internet a través de un proxy deberá configurar la presente pantalla, y pulsar “Siguiente >” para continuar. 
338.	A continuación, seleccione el rol del sistema de sitio que quiere implementar en dicho servidor y pulse “Siguiente >”.  **Nota:** En el presente ejemplo se implementa el rol de “Punto de administración”, deberá adaptar estos pasos a los requerimientos de su organización.

Paso	Descripción
339.	En los siguientes pasos, se va a establecer una configuración específica para el rol de “Punto de administración”, en caso de haber seleccionado otro rol del sistema de sitio deberá adaptar estos pasos a su organización. Pulse “Siguiente >” para continuar. 
340.	Para avanzar con la configuración del rol del sistema de sitio. Pulse “Siguiente >” para continuar. 

Paso	Descripción
341.	Pulse “Siguiente >” para continuar con la implementación. 
342.	Compruebe que se ha creado el servidor de sitio correctamente y pulse “Cerrar” para finalizar el asistente. 

Paso	Descripción
343.	Una vez realizada la implementación del servidor y del rol del sistema de sitio, verifique que el proceso ha sido correcto. 

7.9. BORRADO Y DESTRUCCIÓN

Las medidas de borrado y destrucción de información se aplicarán a todo tipo de equipos susceptibles de almacenar información.

MS SCCM 2012 R2 no permite eliminar una base de datos directamente por lo que será necesario iniciar sesión en el servidor que aloje la base de datos de sitio. Se debe tener en consideración que el usuario que realiza la acción debe tener los permisos adecuados y una vez desvinculada la base de datos, se deberá eliminar físicamente la carpeta contenedora de la información, y si desea eliminar el soporte de dicha información deberá proceder siguiendo el procedimiento marcado en el borrado y destrucción de soportes físicos que establece el ENS.

Nota: Si desea obtener más información sobre el borrado de bases de datos de Microsoft SQL Server puede visitar el sitio web: https://technet.microsoft.com/es-es/library/ms177419(v=sql.110).aspx

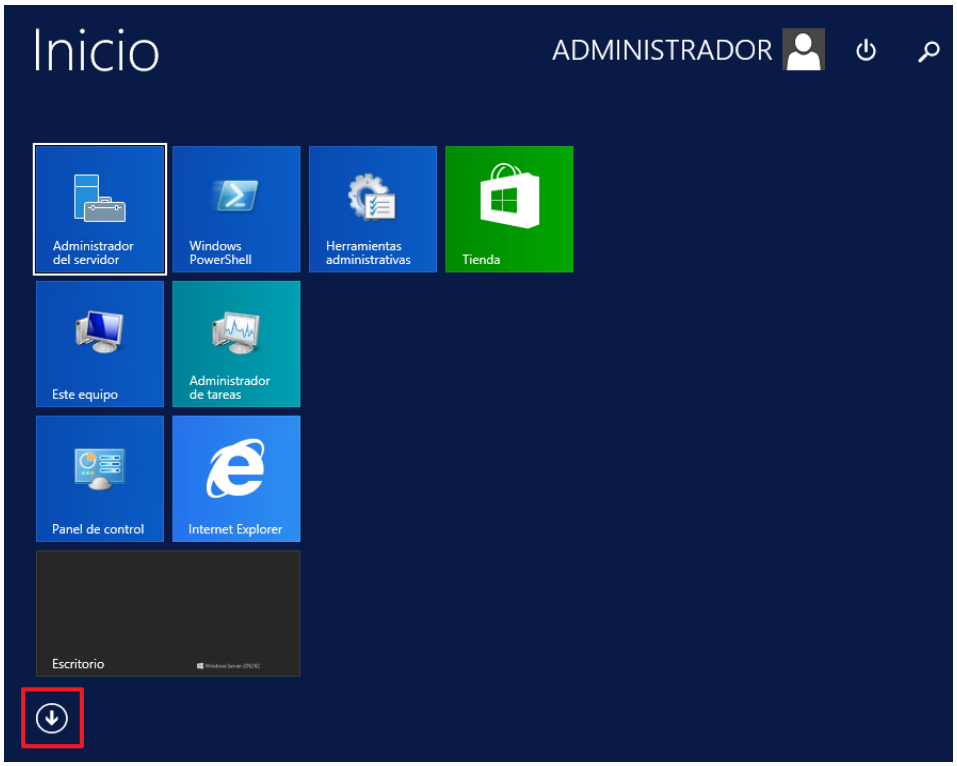
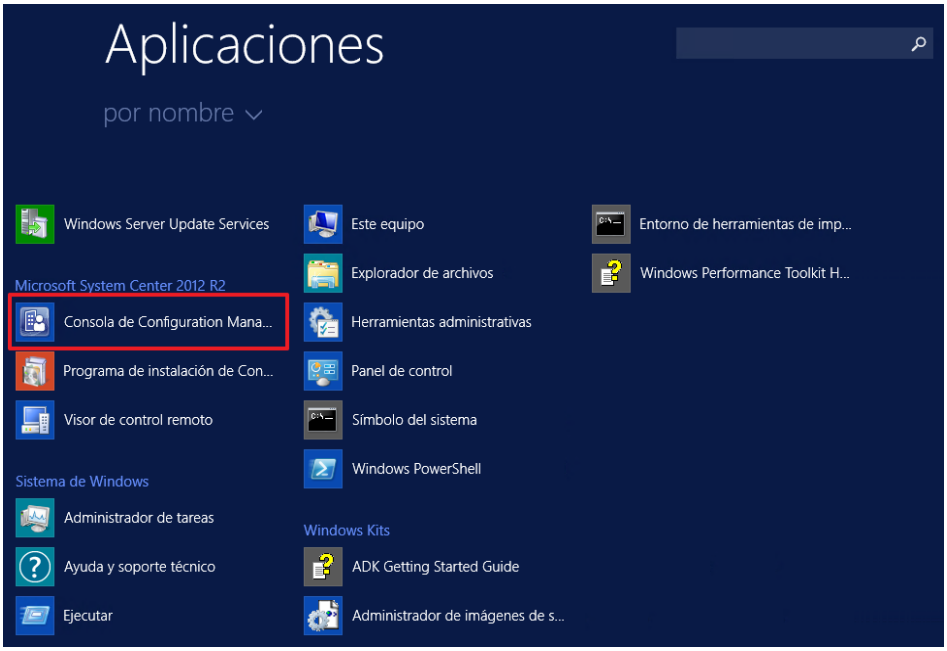
7.10. COPIAS DE SEGURIDAD

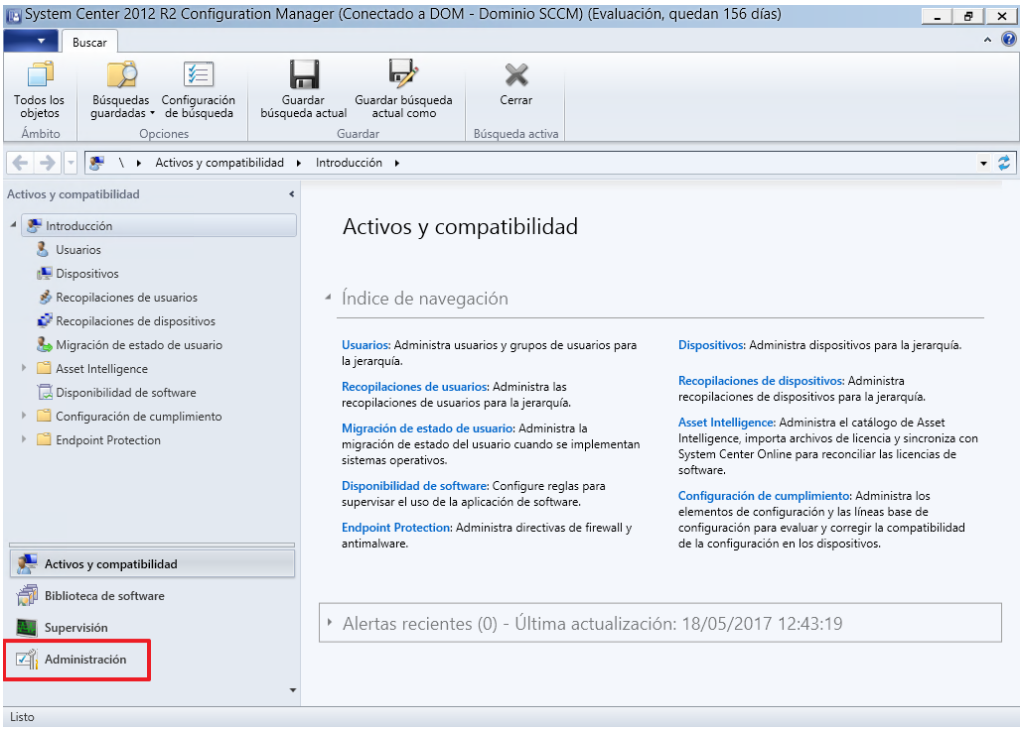
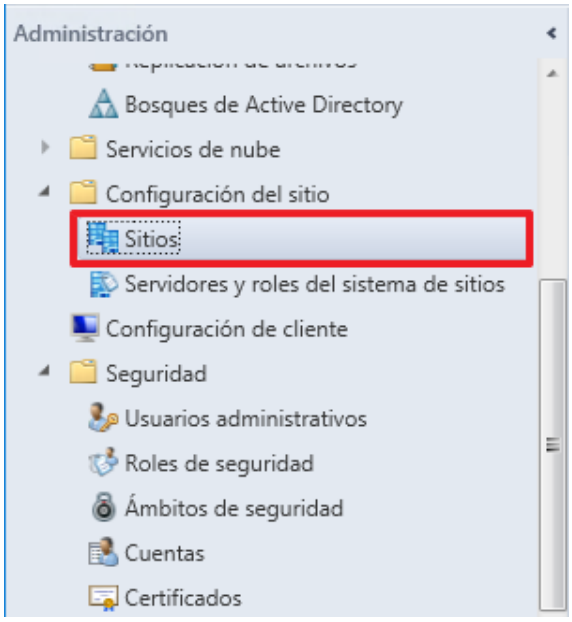
MS SCCM 2012 R2 permite realizar copias de seguridad de los sitios, así como de las bases de datos de los sitios, para en caso de desastre, tener la posibilidad de restaurar el sistema en el menor tiempo posible y minimizar al máximo una posible pérdida de información.

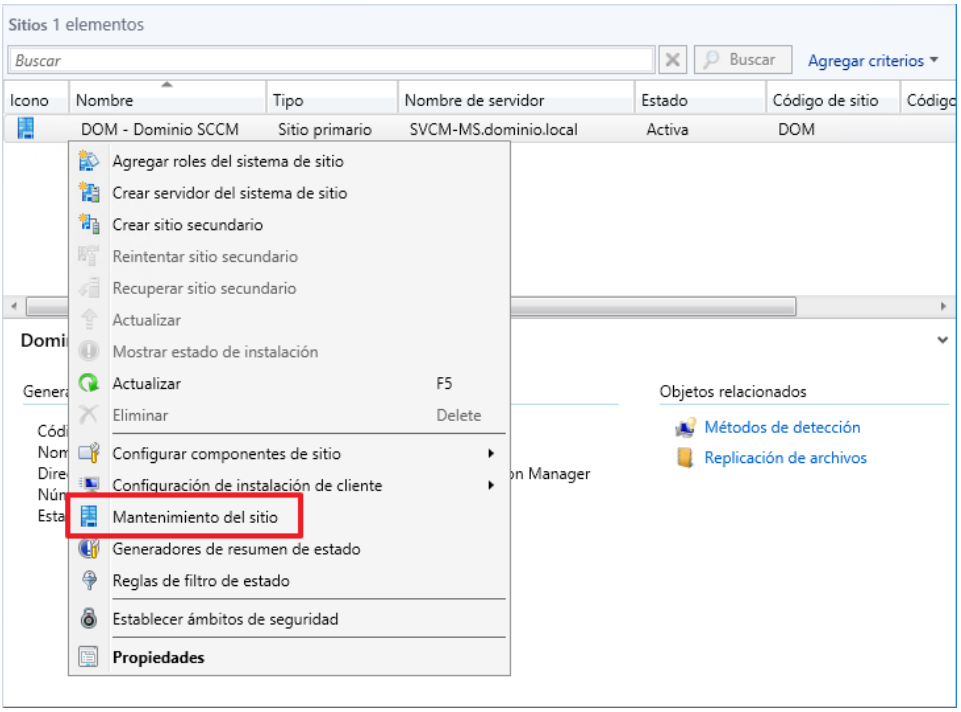
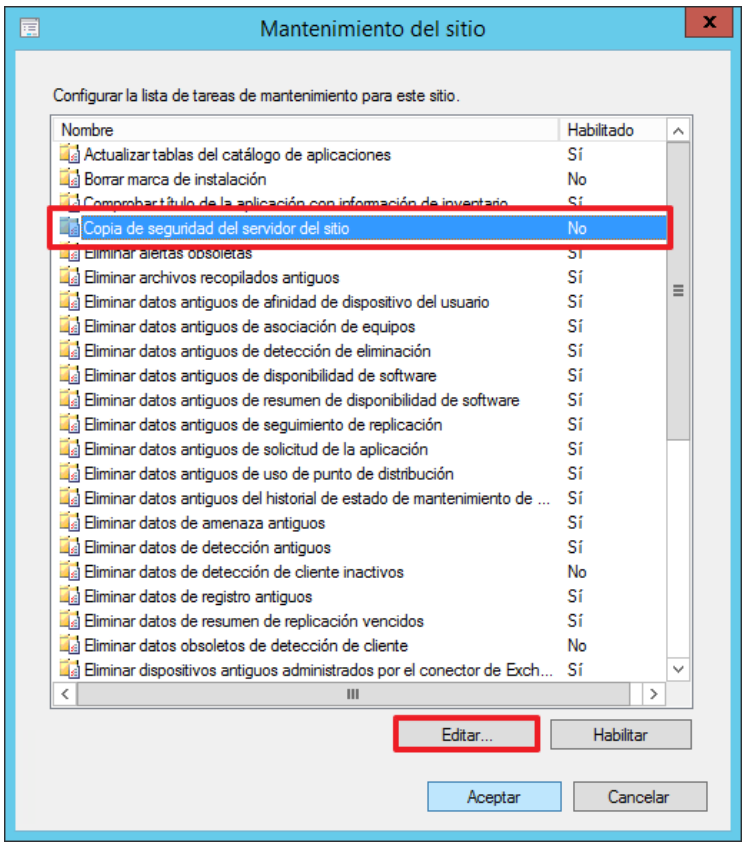
Tal y como se establece en el ENS las copias de seguridad conservarán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.

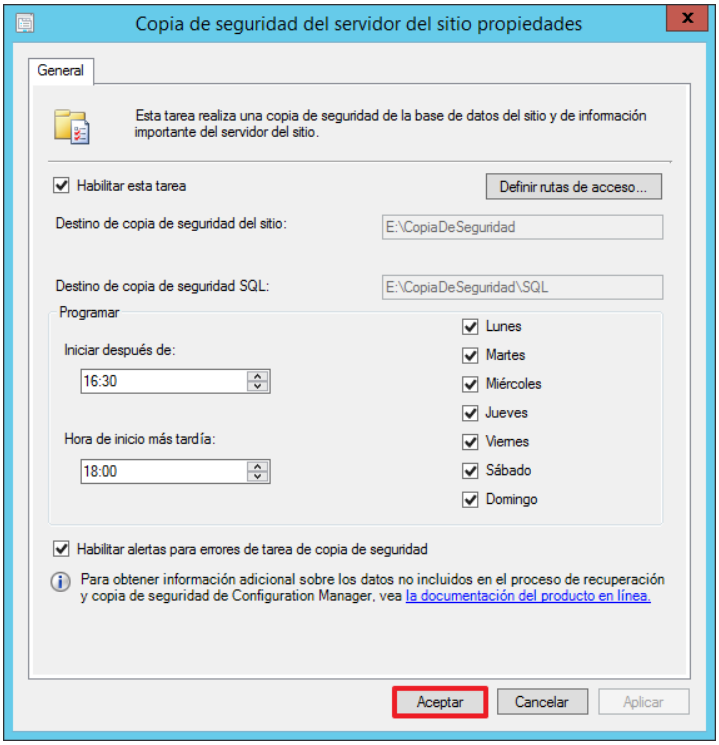
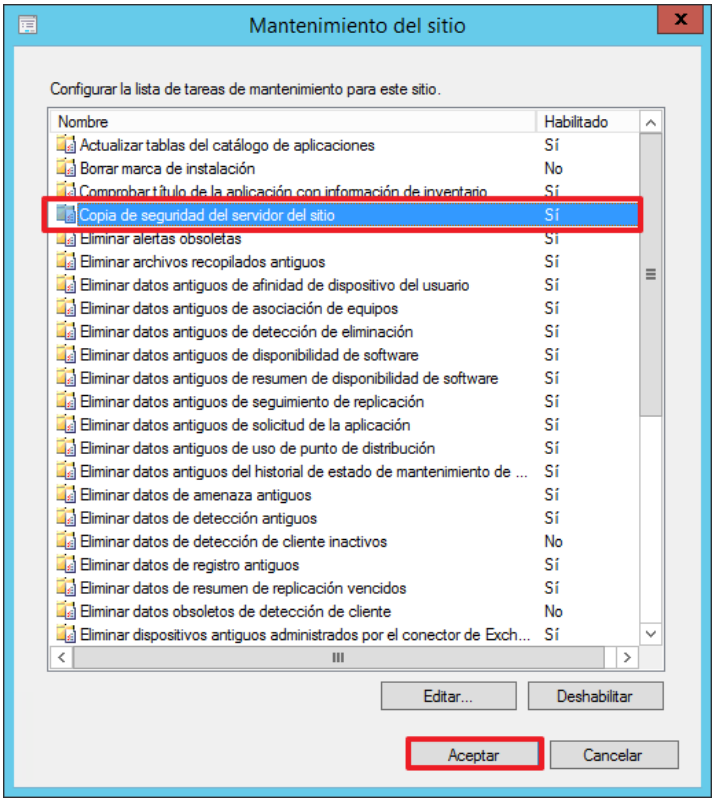
A continuación, se muestra un paso a paso de como habilitar las copias de seguridad de un sitio.

Paso	Descripción
344.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.

Paso	Descripción
345.	Pulse sobre el menú inicio. 
346.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
347.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
348.	Seleccione el apartado “Administración”. 
349.	Despliegue “**Configuración del sitio > Sitios**”. 

Paso	Descripción
350.	Localice el sitio sobre el que desea habilitar las copias de seguridad, pulse con el botón derecho sobre el sitio y seleccione la opción “Mantenimiento del sitio” del menú contextual. 
351.	Localice la opción “Copia de seguridad del servidor del sitio” y pulse sobre el botón “Editar”. 

Paso	Descripción
352.	Configure los parámetros adecuándolos a su organización y pulse “Aceptar” para guardar la configuración. 
353.	Confirme que la opción “Copia de seguridad del servidor del sitio” está habilitada y pulse “Aceptar” para cerrar las opciones de mantenimiento del sitio. 

ANEXO A.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL BAJO DEL ENS

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores MS SCCM 2012 R2 sobre Microsoft Windows Server 2012 R2 con implementación de seguridad de nivel bajo del ENS.

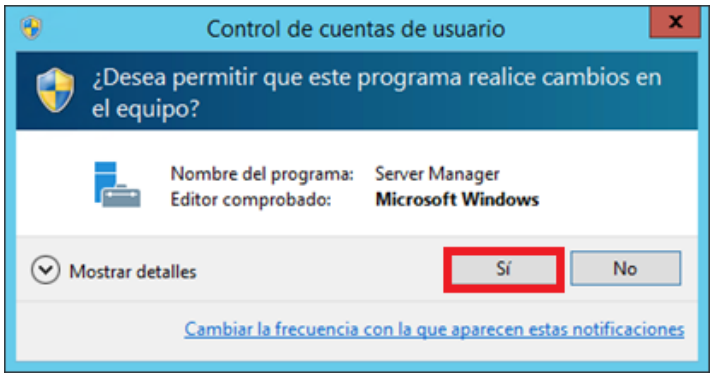
Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

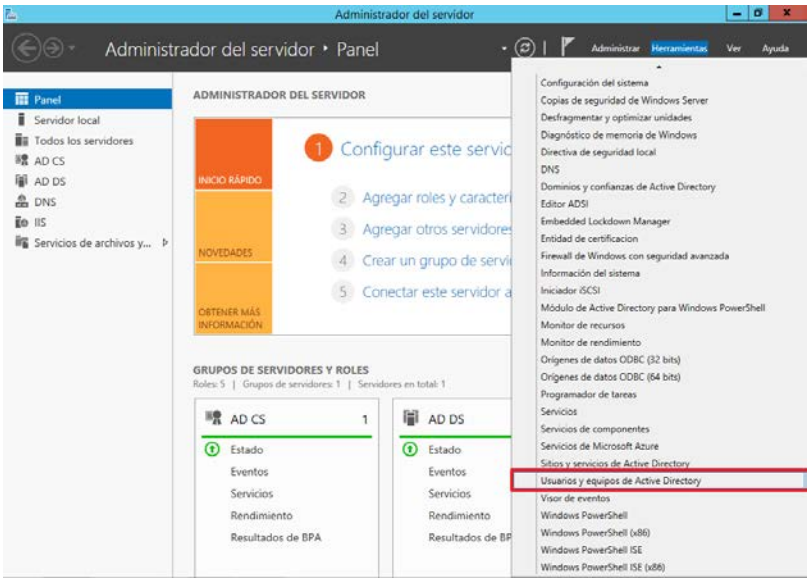
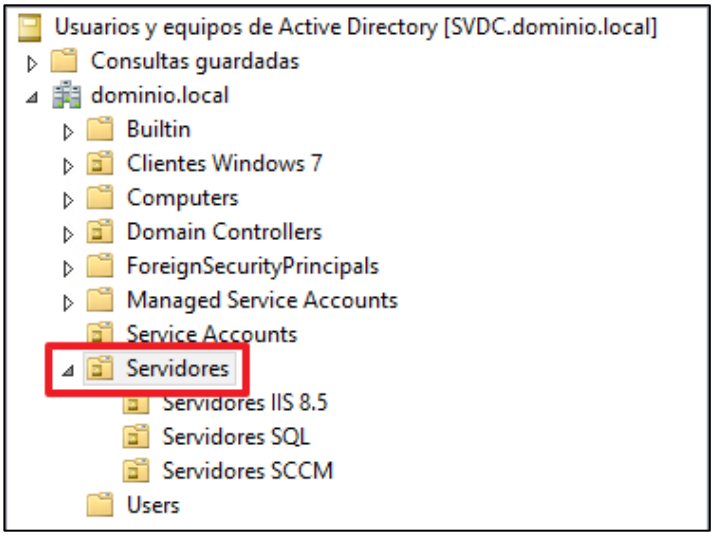
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

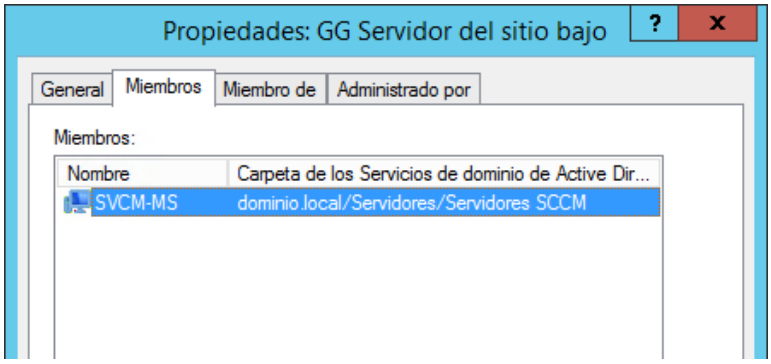
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

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

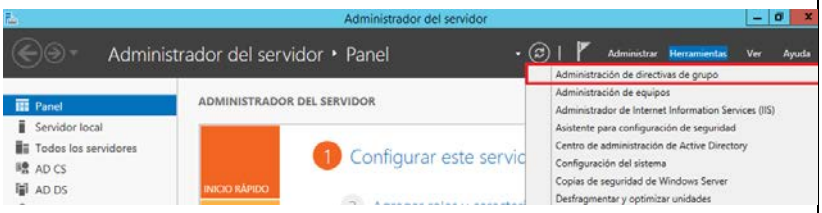
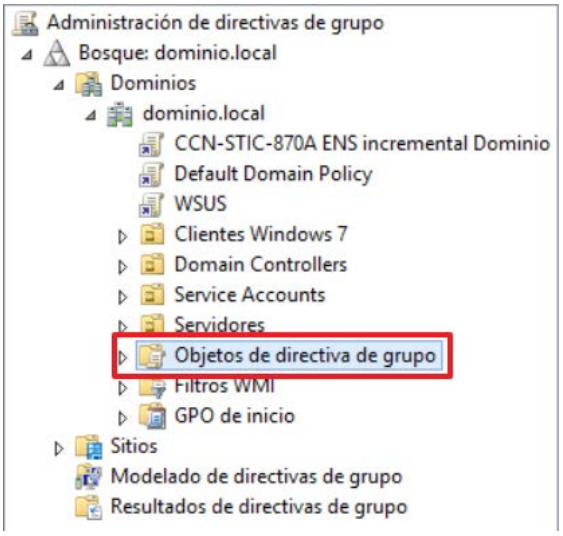
b) Usuarios y equipos de Active Directory (dsa.msc)

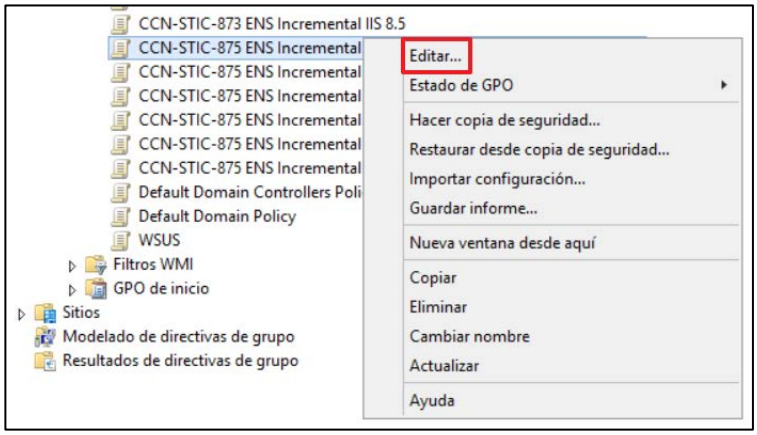
Comprobación	OK/NOK	Como hacerlo
1. Inicie sesión en un controlador de dominio		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana que se muestra a continuación. 

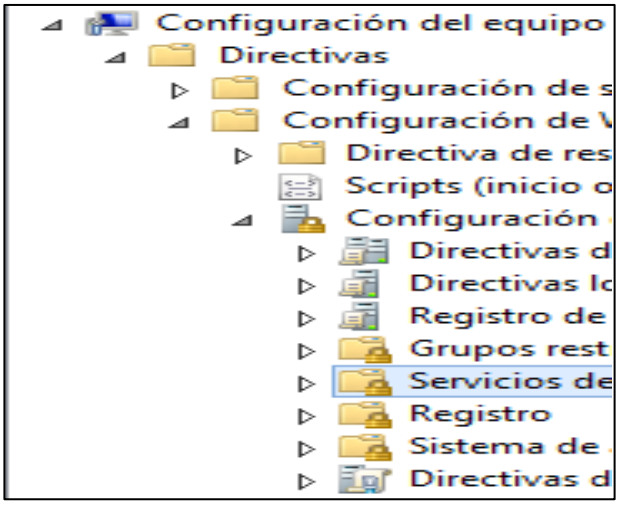
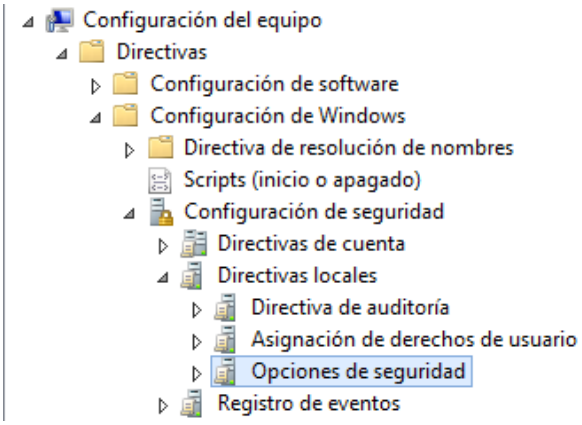
Comprobación	OK/NOK	Como hacerlo
2. Verifique que están creados los grupos de seguridad global		Ejecute la herramienta "Usuarios y equipos de Active Directory". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio. Seleccione el contenedor "Servidores SCCM" y "Servidores SQL", situados en la siguiente ruta: "**Usuarios y equipos de Active Directory → [Su dominio] → Servidores**". Verifique que están creados los grupos de seguridad en función de los roles de sistema de sitio que ha reforzado la seguridad. 

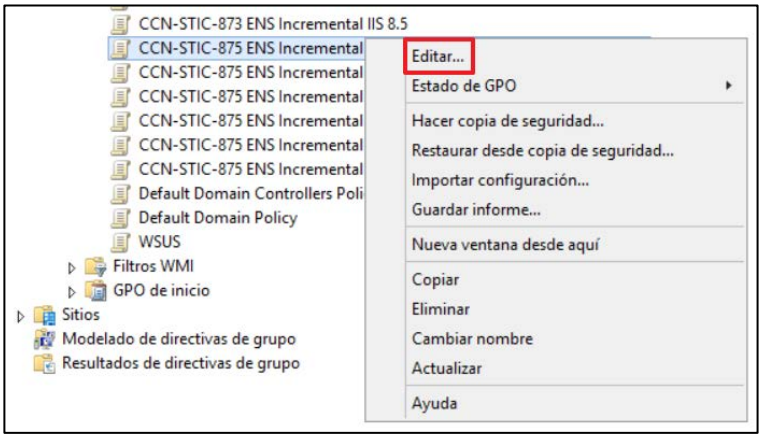
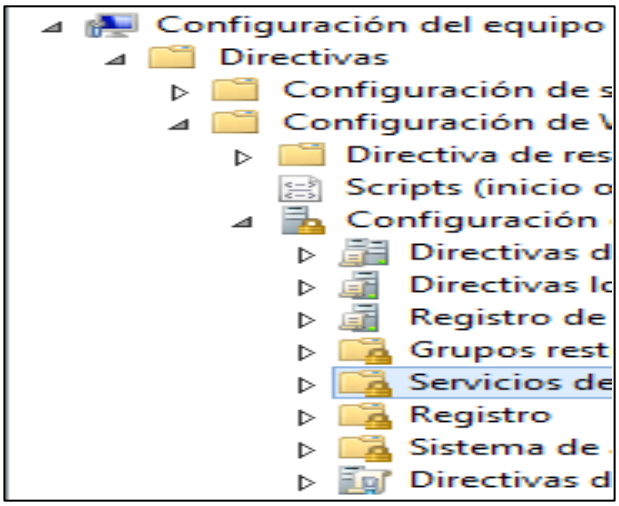
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="2">Como hacerlo</th></tr>
<tr><td></td><td colspan="2">Grupo de seguridad</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">GG Servidor Base de datos del sitio bajo</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de servicios de informes bajo</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor del sitio bajo</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de administración bajo</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de distribución bajo</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de actualización de software bajo</td><td></td></tr>
<tr><td>3. Verifique que los servidores que han sido catalogados correctamente</td><td></td><td colspan="2">Pulse doble clic sobre cada grupo de seguridad y seleccione la pestaña “Miembros” para verificar que los servidores que corresponden a este grupo de seguridad aparecen en el listado.
 

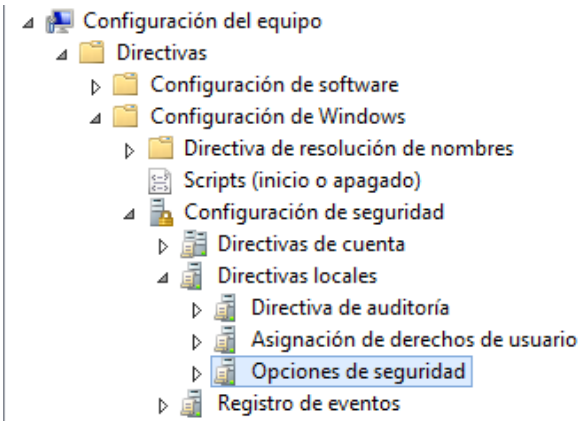
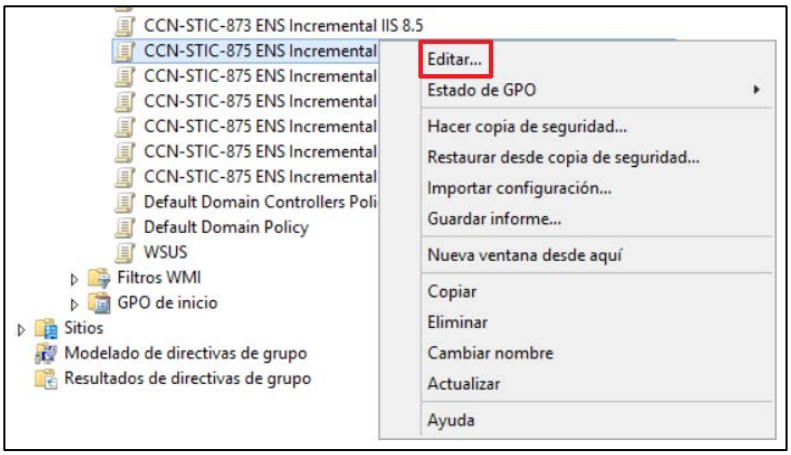
Nota: La imagen mostrada anteriormente corresponde a un ejemplo de los miembros del grupo de seguridad “GG Servidor del sitio bajo”, deberá realizar esta comprobación en todos los grupos de seguridad correspondientes y verificar que aparecen los servidores que pertenecen a cada grupo.</td></tr>
</table>

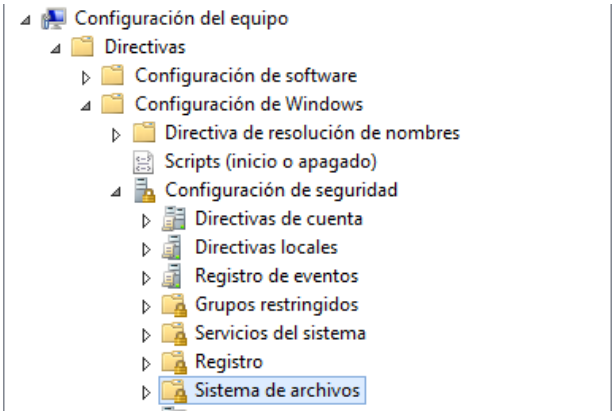
Comprobación	OK/NOK	Como hacerlo
4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.		Ejecute la herramienta "Administrador de directivas de grupo". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: "**Herramientas → Administración de directivas de grupo".**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio. Dentro de la consola diríjase a los "Objetos de directiva de grupo": **"Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo".** Verifique que están creados los objetos de directiva de grupo en función de los roles de sistema de sitio que ha reforzado la seguridad y que en la columna "Estado de GPO" figuran como habilitadas. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Como hacerlo</th></tr>
<tr><td rowspan="7"></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">CCN-STIC-875 ENS Incremental Punto de actualización de software bajo</td><td>Habilitado</td><td></td></tr>
<tr><td colspan="2">CCN-STIC-875 ENS Incremental Punto de administración bajo</td><td>Habilitado</td><td></td></tr>
<tr><td colspan="2">CCN-STIC-875 ENS Incremental Punto de distribución bajo</td><td>Habilitado</td><td></td></tr>
<tr><td colspan="2">CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo</td><td>Habilitado</td><td></td></tr>
<tr><td colspan="2">CCN-STIC-875 ENS Incremental Servidor del sitio bajo</td><td>Habilitado</td><td></td></tr>
<tr><td colspan="2">CCN-STIC-875 ENS Incremental Punto de -SQL bajo</td><td>Habilitado</td><td></td></tr>
<tr><td>5. Verifique la configuración de la directiva</td><td></td><td colspan="3">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de actualización de software bajo” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>6. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”.
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>Administración remota de Windows (WS-Management)</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>Servicio de transferencia inteligente en segundo plano (BITS)</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>Servidor</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>WSusCertServer</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>WsusService</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
</table>

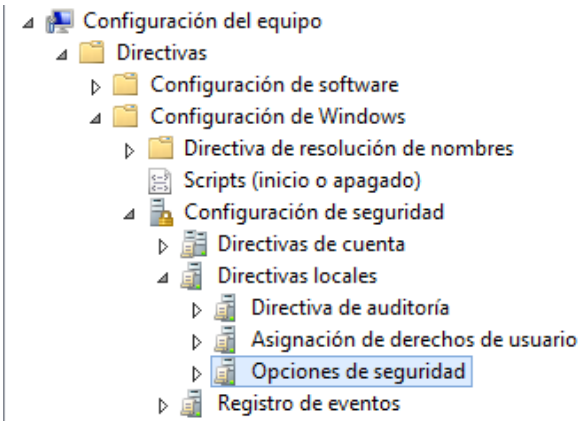
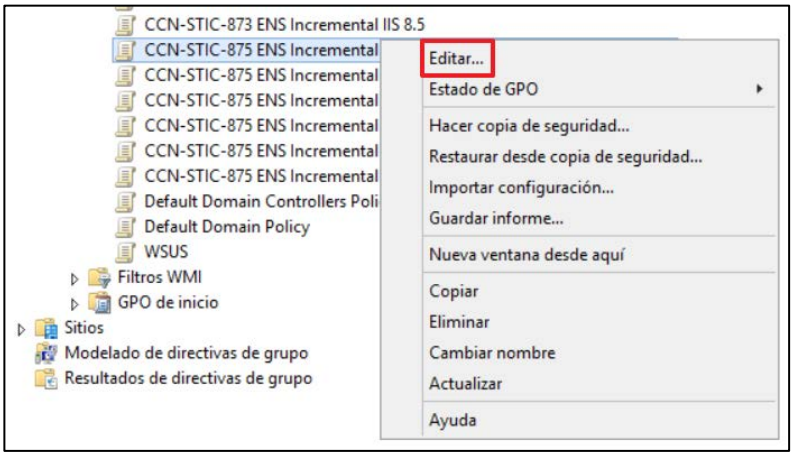
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Como hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>8. Verifique la configuración de la directiva</td><td></td><td colspan="3">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de administración bajo” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>9. Verifique los servicios del sistema.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 
</td></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
</table>

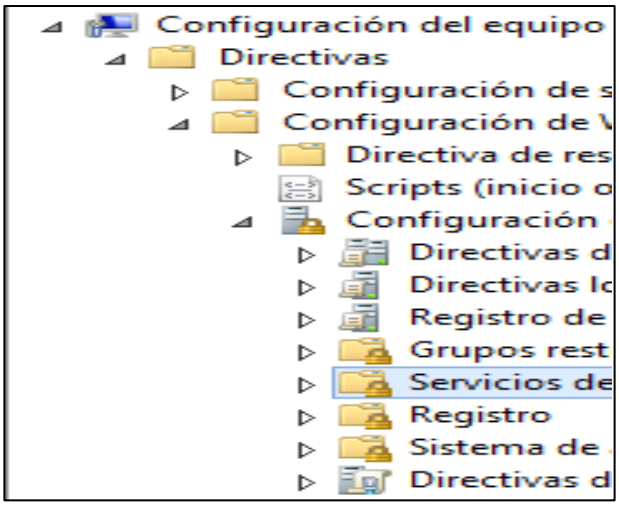
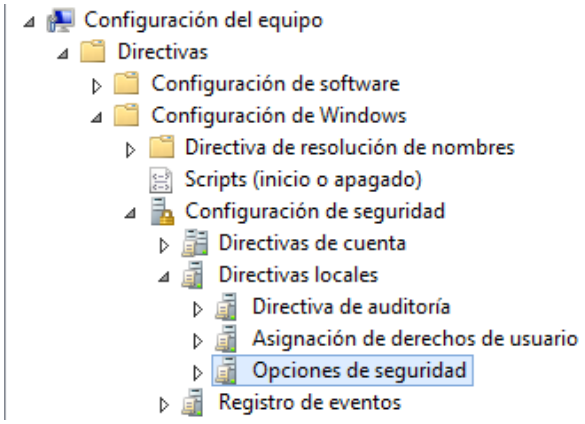
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td rowspan="4">10. Verifique las opciones de seguridad</td><td></td><td colspan="2">Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
<tr><td>11. Verifique la configuración de la directiva</td><td></td><td colspan="2">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución bajo” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

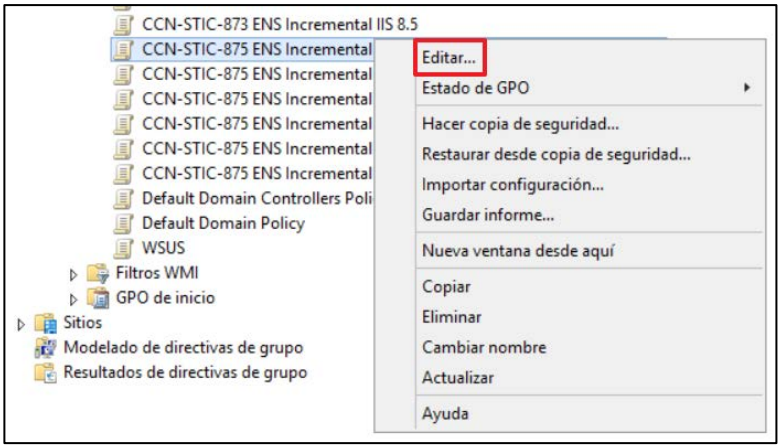
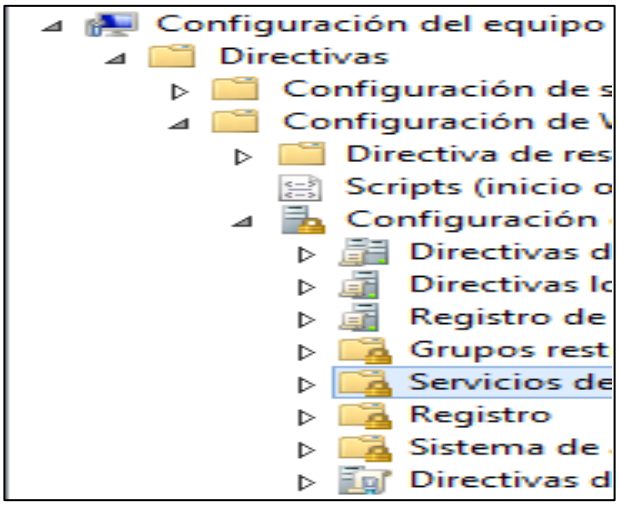
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>12. Compruebe que se ha aplicado correctamente los permisos sobre los siguientes directorios</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos”.
 

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

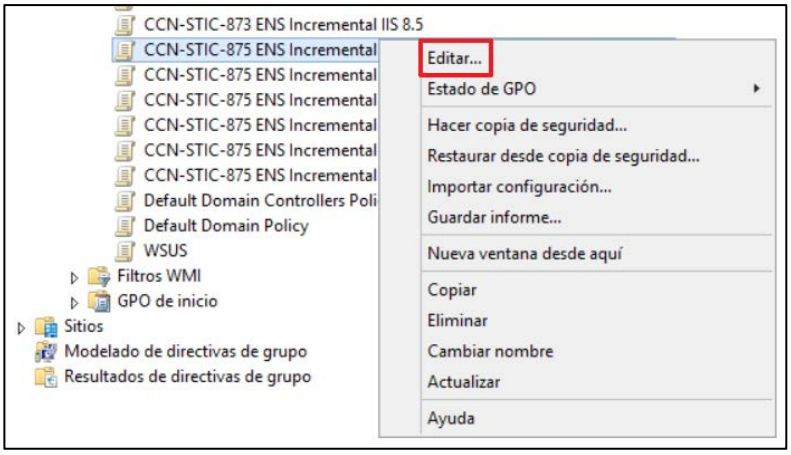
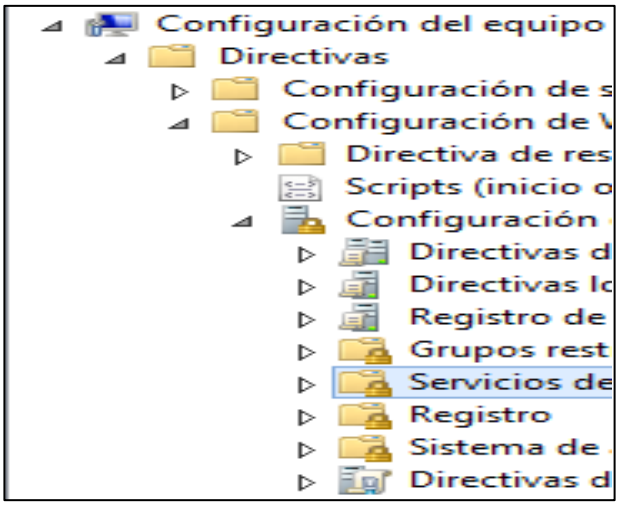
Archivo	Usuario	Permiso	OK/NOK
E:\SCCMContentLib	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer	
E:\SMS_DP$	SYSTEM	Control total	
	Administradores	Control total	
	Administrador	Control total	
E:\SMSPKGE$	Administradores	Control total	
	Usuarios	Leer y ejecutar	
E:\SMSSIG	IUSR	Escribir (Denegar)	
	SYSTEM	Control total	
	Administradores	Control total	
	Usuarios	Leer	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td rowspan="4">13. Verifique las opciones de seguridad</td><td></td><td colspan="2">Seleccione el siguiente nodo. “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">Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
<tr><td>14. Verifique la configuración de la directiva</td><td></td><td colspan="2">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

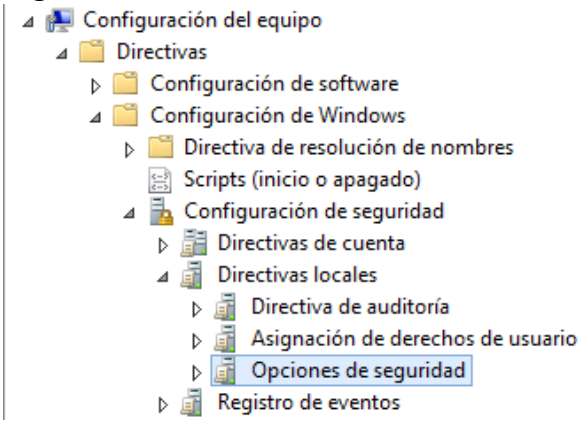
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>15. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
<tr><td>16. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
</table>

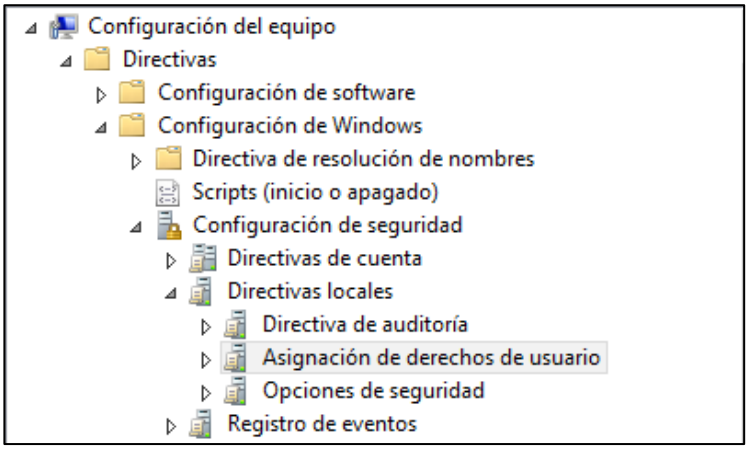
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>17. Verifique la configuración de la directiva</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental servidor del sitio bajo” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>18. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_SITE_VSS_WRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_COMPONENT_MANAGER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>CcmExec</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_NOTIFICATION_SERVER</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_BACKUP</td><td>Manual</td><td>Configurado</td><td></td></tr>
</table></td></tr>
</table>

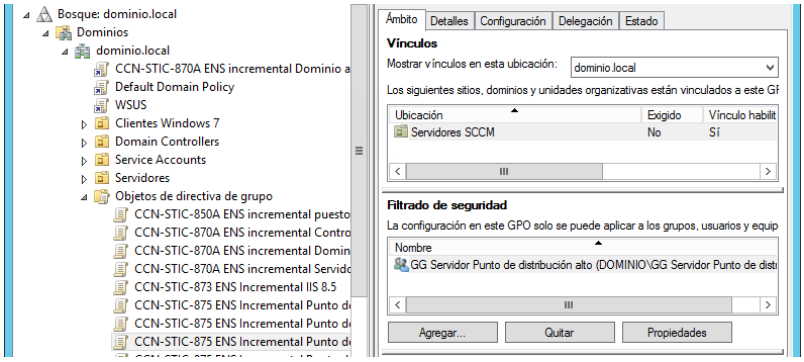
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>19. Verifique la configuración de la directiva</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental SQL bajo” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>20. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>MSSQLSERVER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLSERVERAGENT</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLWRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table>
Nota: Deberá adaptar el servicio SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL, por el servicio configurado con el nombre de dominio de su organización.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>21. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>22. Verifique la asignación de derechos de usuario</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos usuario”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Inicio de sesión como servicio</td><td>DOMINIO\SQLServiceAccount</td><td></td></tr>
</table>
Nota: Deberá adaptar estos pasos a su organización y comprobar que el usuario con permisos de inicio de sesión como servicio es el adecuado.ario con permisos de inicio de sesión como servicio es el adecuado.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>23. Verifique que cada objeto de directiva de tiene definido el filtro de seguridad correspondiente</td><td></td><td>En el árbol de la izquierda, pulse doble clic sobre el objeto de directiva de grupo: “Bosques [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo”
Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo seguridad correspondiente a cada objeto de directiva de grupo.
 

Nota: La imagen mostrada anteriormente corresponde a un ejemplo del filtro de seguridad del objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución bajo” al que corresponde el filtro de seguridad “GG Servidor punto de distribución bajo”, deberá realizar esta comprobación en todos los objetos de directivas de grupo correspondientes y verificar que están vinculados los grupos de seguridad que pertenecen a cada directiva.</td></tr>
</table>

Directiva	Grupo de seguridad	OK/NOK
CCN-STIC-875 ENS Incremental Punto de actualización de software bajo	GG Servidor Punto de actualización de software bajo	
CCN-STIC-875 ENS Incremental Punto de administración bajo	GG Servidor Punto de administración bajo	
CCN-STIC-875 ENS Incremental Punto de distribución bajo	GG Servidor Punto de distribución bajo	
CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo	GG Servidor Punto de servicios de informes bajo	
CCN-STIC-875 ENS Incremental Servidor del sitio bajo	GG Servidor del sitio bajo	
CCN-STIC-875 ENS Incremental Punto de -SQL bajo	GG Servidor Base de datos del sitio bajo	

2. COMPROBACIONES EN SERVIDOR MIEMBRO

Para realizar las comprobaciones pertinentes en los servidores miembros, se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

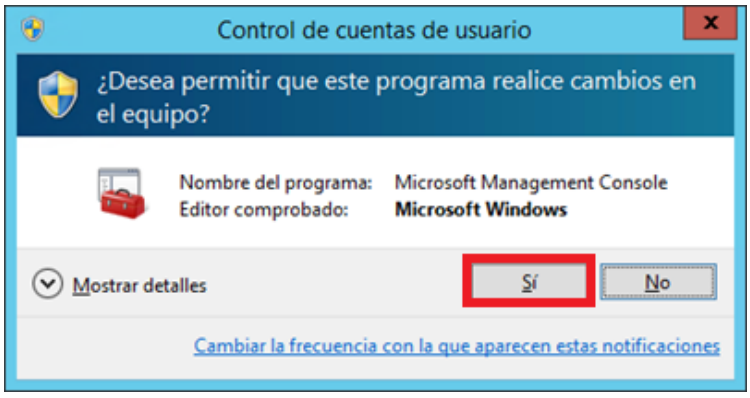
a) Administrador del Servidor

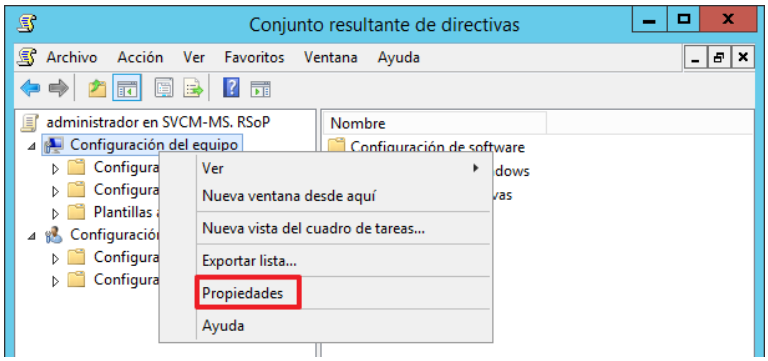
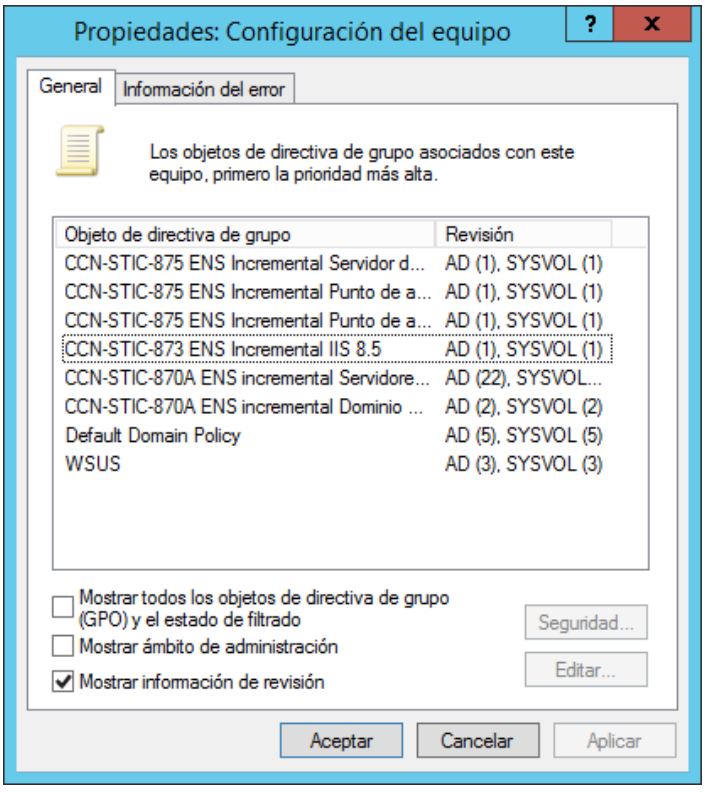
b) Conjunto resultante de directivas (rsop.msc)

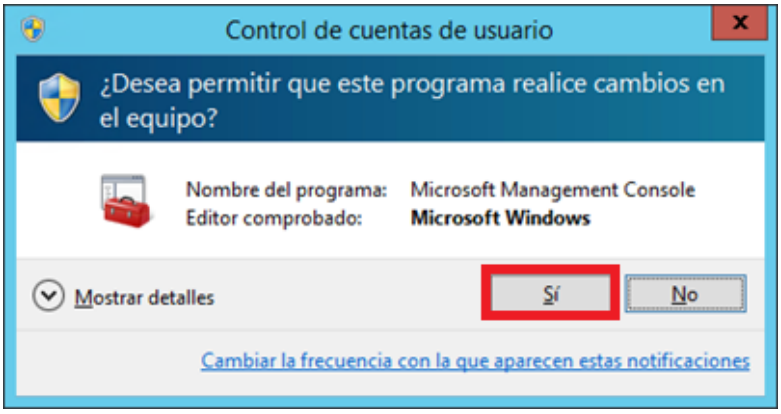
c) Consola de servicios (services.msc)

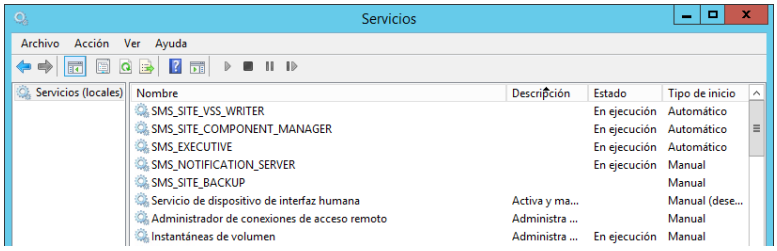
d) Editor de registro (regedit.exe)

e) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Como hacerlo
24. Inicie sesión en un servidor miembro del dominio		En uno de los servidores miembro del dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
25. Verifique que el equipo ha recibido la directiva de grupo correspondiente con el rol de sistema de sitio que esta implementado		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): “Tecla Windows+R → rsop.msc” El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” en la ventana que se muestra a continuación: 

Comprobación	OK/NOK	Como hacerlo
		Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo". Verifique que en dicha sección aparecen listados, los objetos de directiva de grupo correspondientes con el servidor miembro que está comprobando.  **Nota:** Se debe tener en consideración que el listado de objetos de directivas de grupo variara en función del servidor miembro que este comprobando y de los roles de sistema de sitio que dicho servidor tenga implementado.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>26. Verifique que los servicios del sistema están correctamente configurados</td><td></td><td>Usando la consola de servicios (el sistema solicitará elevación de privilegios): “Windows+R → services.msc”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” en la ventana que se muestra a continuación:
 

Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:
 

Nota: Dependiendo del servidor miembro que este comprobando y del rol del sistema de sitio implementado, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.</td></tr>
</table>

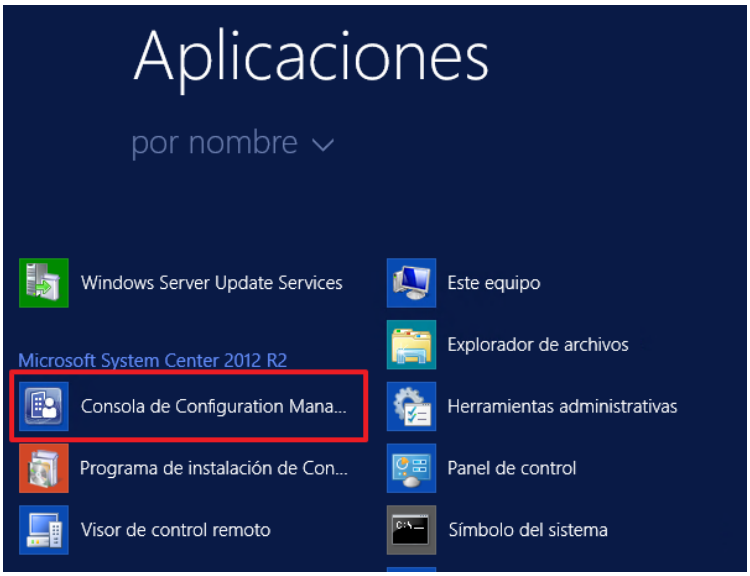
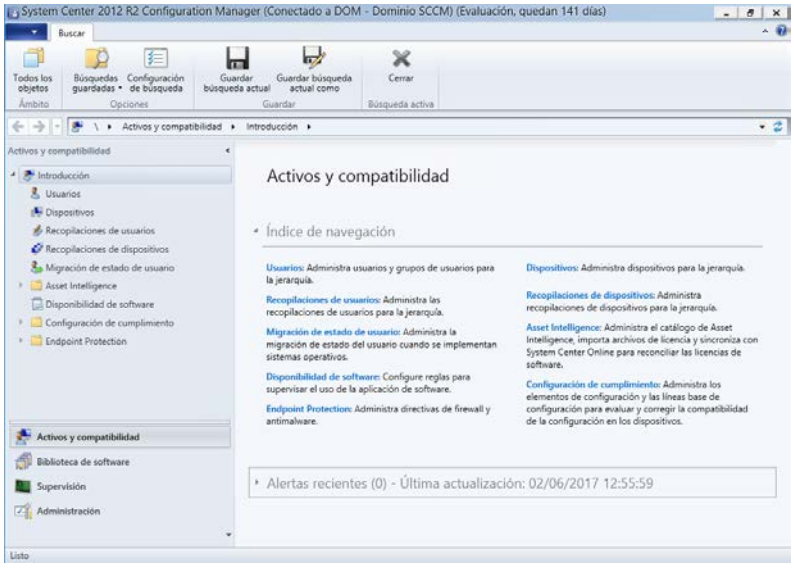
Directiva	Servicio	Iniciado	Permiso	OK/NOK
CCN-STIC-875 ENS Incremental Punto de actualización de software bajo	Administración remota de Windows (WS-Management)	Automático	Configurado	
	Servicio de transferencia inteligente en segundo plano (BITS)	Automático	Configurado	
	Servidor	Automático	Configurado	
	WSusCertServer	Automático	Configurado	
	WsusService	Automático	Configurado	

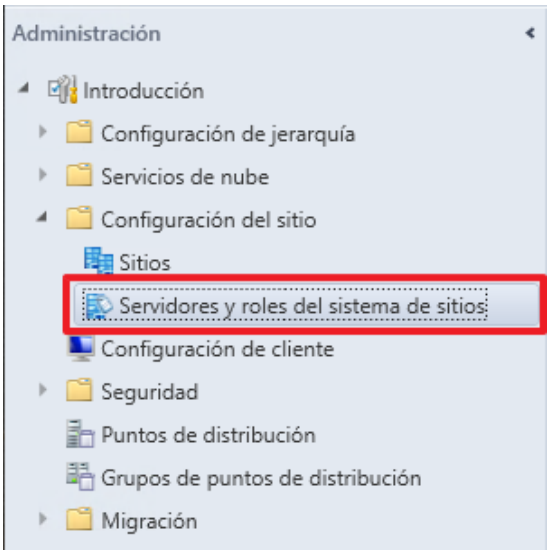
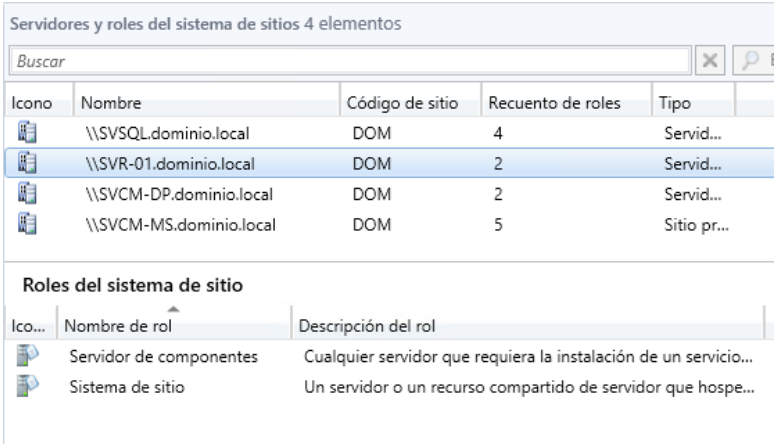
Comprobación	OK/NOK	Como hacerlo			
	Directiva	Servicio	Iniciado	Permiso	OK/NOK
	CCN-STIC-875 ENS Incremental Punto de administración bajo	SMS_EXECUTIVE	Automático	Configurado	
	CCN-STIC-875 ENS Incremental Punto de servicios de informes bajo	SMS_EXECUTIVE	Automático	Configurado	
	CCN-STIC-875 ENS Incremental servidor del sitio bajo	SMS_SITE_VSS_WRITER	Automático	Configurado	
		SMS_SITE_COMPONENT_MANAGER	Automático	Configurado	
		CcmExec	Automático	Configurado	
		SMS_NOTIFICATION_SERVER	Manual	Configurado	
		SMS_SITE_BACKUP	Manual	Configurado	
	CCN-STIC-875 ENS Incremental SQL bajo	MSSQLSERVER	Automático	Configurado	
		SMS_EXECUTIVE	Automático	Configurado	
		SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL	Automático	Configurado	
		SQLSERVERAGENT	Automático	Configurado	
		SQLWRITER	Automático	Configurado	
	Nota: Deberá adaptar el servicio SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL, por el servicio configurado con el nombre de dominio de su organización.				

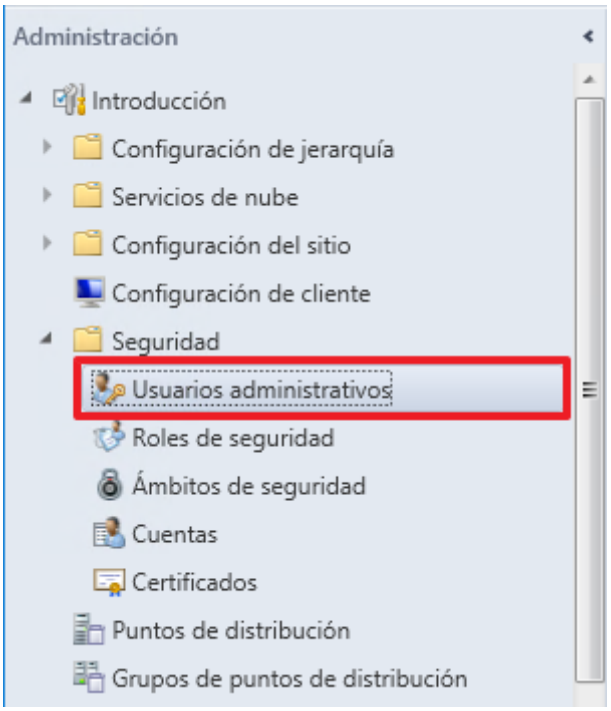
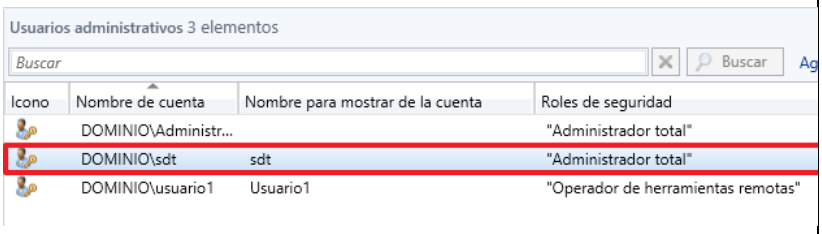
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>27. Verifique que se han asignado los permisos correctos en el sistema de archivos.</td><td></td><td>En los servidores miembro donde tenga implementado el rol de sistema de sitio de Punto de distribución y se le esté aplicando la directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución bajo”. Verifique los permisos asignados utilizando el Explorador de Windows: “Windows+R → Explorer”.
En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada.

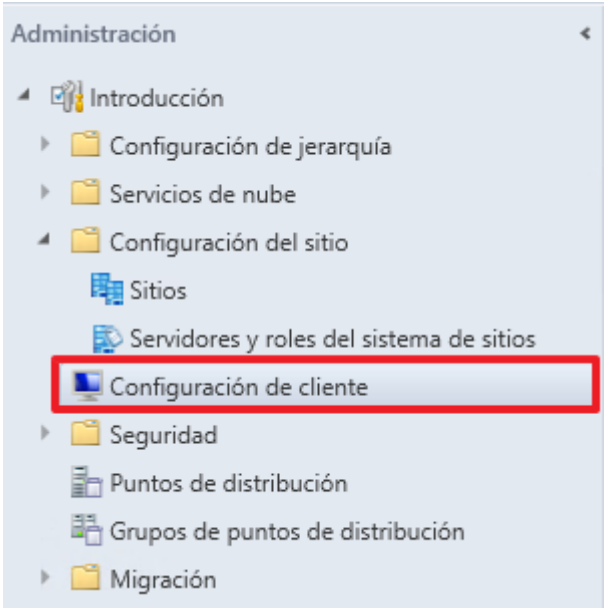
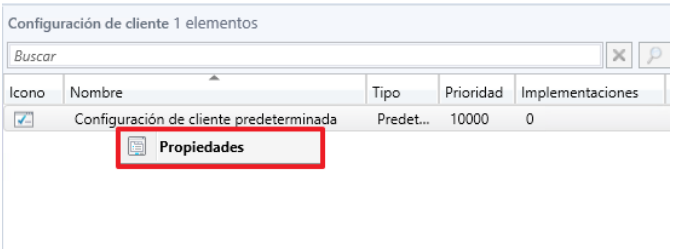
Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña “Seguridad”. En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados</td></tr>
</table>

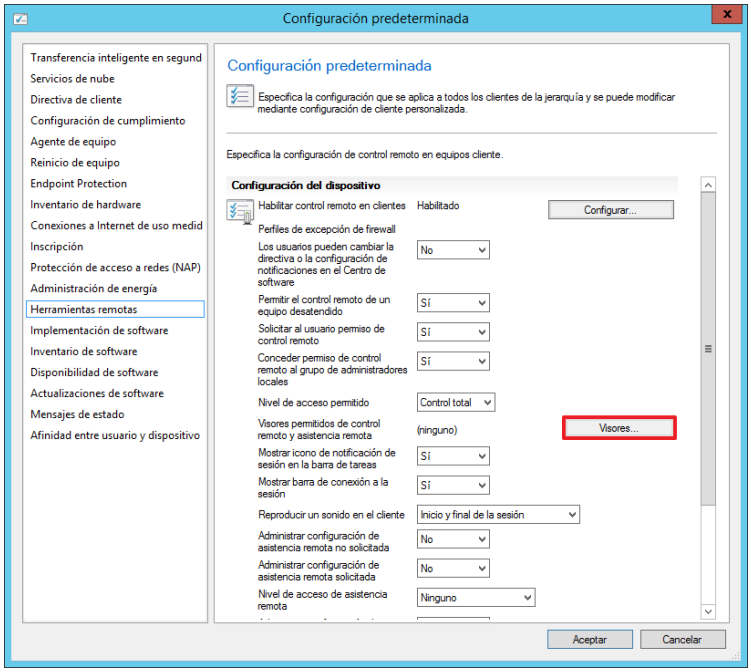
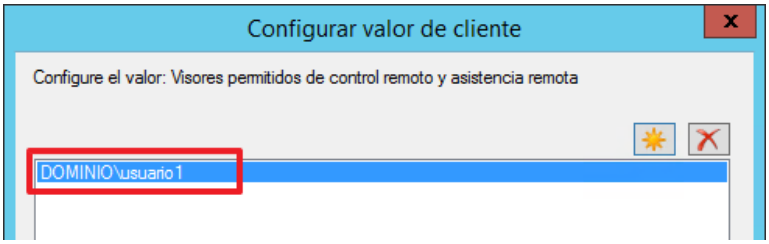
Archivo	Usuario	Permiso	OK/NOK
E:\SCCMContentLib	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer	
E:\SMS_DP$	SYSTEM	Control total	
	Administradores	Control total	
	Administrador	Control total	
E:\SMSPKGE$	Administradores	Control total	
	Usuarios	Leer y ejecutar	
E:\SMSSIG	IUSR	Escribir (Denegar)	
	SYSTEM	Control total	
	Administradores	Control total	
	Usuarios	Leer	

Comprobación	OK/NOK	Como hacerlo
28. Inicie sesión en el servidor miembro donde tiene instalada la consola de administración de MS SCCM 2012 R2, verifique que accede correctamente		Inicie sesión en la consola de administración de Configuration Manager desde el menú "Inicio > Todas las aplicaciones > Microsoft System Center 2012 R2 > Consola de Configuration Manager". 
29. Verifique que tiene acceso a la Consola de Configuración		Compruebe que accede correctamente a la consola de configuración de MS SCCM 2012 R2. 

Comprobación	OK/NOK	Como hacerlo
30. Verifique que los roles de sistema de sitio están implementados en los servidores correspondientes		Despliegue "**Configuración del sitio > Servidores y roles del sistema de sitios**".  Verifique seleccionando cada servidor, que tiene implementados los roles de sistema de sitio correspondientes.  **Nota:** Tanto los nombres de los servidores como el del sitio han sido creados para elaborar la presente guía por lo que deberá adaptar estos pasos a su organización.

Comprobación	OK/NOK	Como hacerlo
31. Verifique los permisos asignados a los usuarios administrativos.		Despliegue "**Introducción > Seguridad > Usuarios administrativos**".  Compruebe que los usuarios tienen asignados los roles de seguridad correctamente.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización.

Comprobación	OK/NOK	Como hacerlo
32. Verifique los permisos asignados a los usuarios con permisos de control remoto.		Despliegue "**Introducción > Configuración del sitio > Configuración de cliente**".  Compruebe que los usuarios tienen asignados los permisos correctamente. Para ello pulse con el botón derecho sobre "Configuración de cliente predeterminada" y pulse botón derecho, y seleccione la opción "Propiedades" del menú contextual. 

Comprobación	OK/NOK	Como hacerlo
33. Verifique los usuarios que tienen permisos.		Pulse sobre el botón “Visores…”.  Compruebe en el listado los usuarios que tienen permisos de control remoto.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización.

ANEXO B. CONFIGURACION SEGURA DE MS SCCM 2012 R2 EN EL ENS PARA EL NIVEL MEDIO

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de System Center Configuration Manager 2012 R2 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.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para System Center Configuration Manager 2012 R2, 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.

ANEXO B.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL MEDIO DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas, a realizar una implementación de seguridad en escenarios donde se tenga que reforzar la seguridad de Microsoft SCCM 2012 R2 sobre MS Windows Server 2012 R2, 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 al nivel medio, 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, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

MS SCCM 2012 R2 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar MS SCCM 2012 R2, en caso de necesitar información sobre los requisitos previos de instalación de MS SCCM 2012 R2, visite el siguiente sitio web:

https://docs.microsoft.com/es-es/sccm/core/plan-design/configs/site-and-site-system-prerequisites

En la presente guía se van a reforzar la seguridad de los principales roles de sitio de MS SCCM 2012 R2.

a) Sistema de sitio
b) Servidor del sitio
c) Punto de distribución

d) Punto de administración

e) Punto de actualización de software

f) Punto de servicios de informes

g) Servidor base de datos del sitio

Nota: Si instala MS SCCM 2012 R2 por primera vez con la guía 870A aplicada previamente debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell, la cual se encuentra deshabilitada por GPO.

Para la implementación de la presente guía se han generado unas plantillas de seguridad que deberán ser aplicada en las unidades organizativas correspondientes donde se encuentren alojados los servidores que vayan a formar parte de MS System Center Configuration Manager 2012 R2.

Hay que tener en consideración que el objetivo de implementación de estos tipos de servidores puede ser para un uso de múltiples roles, por ejemplo, como punto de distribución, punto de actualización de software o punto de servicios de informes., por lo que no existirá una ubicación específica dentro del directorio activo, aunque en la presente guía se intentan agrupar en las unidades organizativas “Servidores SCCM” y “Servidores SQL” para una mejor gestión.

Los detalles de las siguientes plantillas se encuentran exportados en sus ficheros correspondientes con formato HTML en la carpeta “Scripts\Nivel Medio” que se acompaña junto a este documento.

a) CCN-STIC-875 ENS Incremental Punto de actualización de software medio

b) CCN-STIC-875 ENS Incremental Punto de administración medio

c) CCN-STIC-875 ENS Incremental Punto de distribución medio

d) CCN-STIC-875 ENS Incremental Punto de servicios de informes medio

e) CCN-STIC-875 ENS Incremental Servidor del sitio medio

f) CCN-STIC-875 ENS Incremental Punto de -SQL medio.

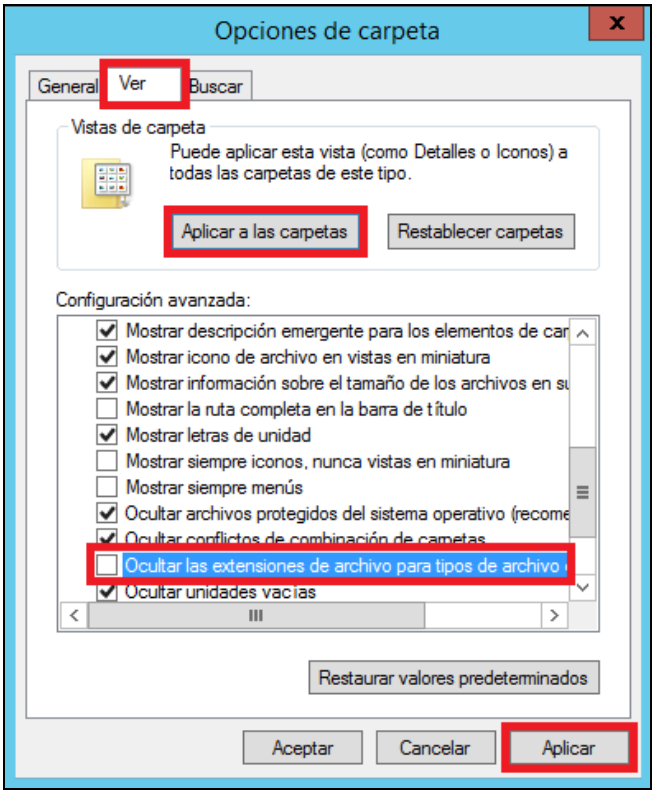
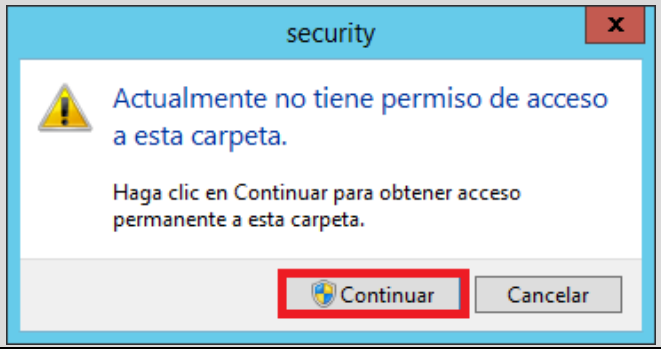
1. REFUERZO DE SEGURIDAD DEL SERVIDOR SQL Y ROL DE SERVIDOR BASE DE DATOS DEL SITIO

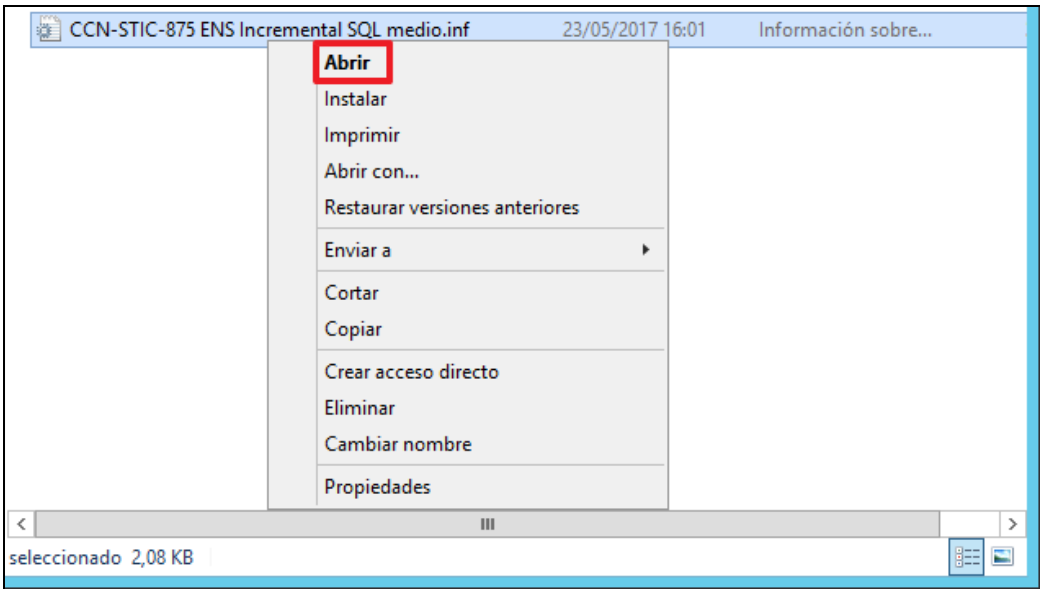
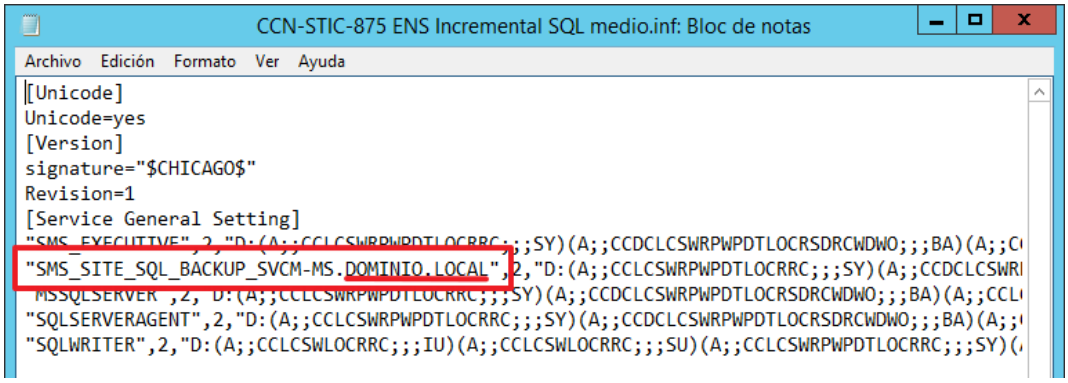
Es necesario dar permisos de inicio de sesión como servicio a los usuarios necesarios para iniciar los servicios de SQL requeridos para el correcto funcionamiento del producto MS SQL server y MS SCCM 2012 R2.

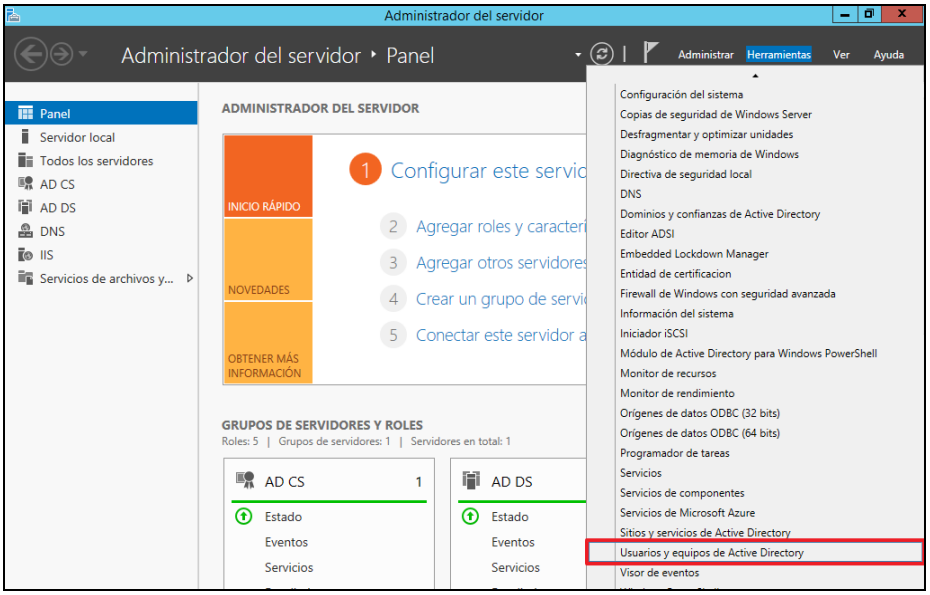
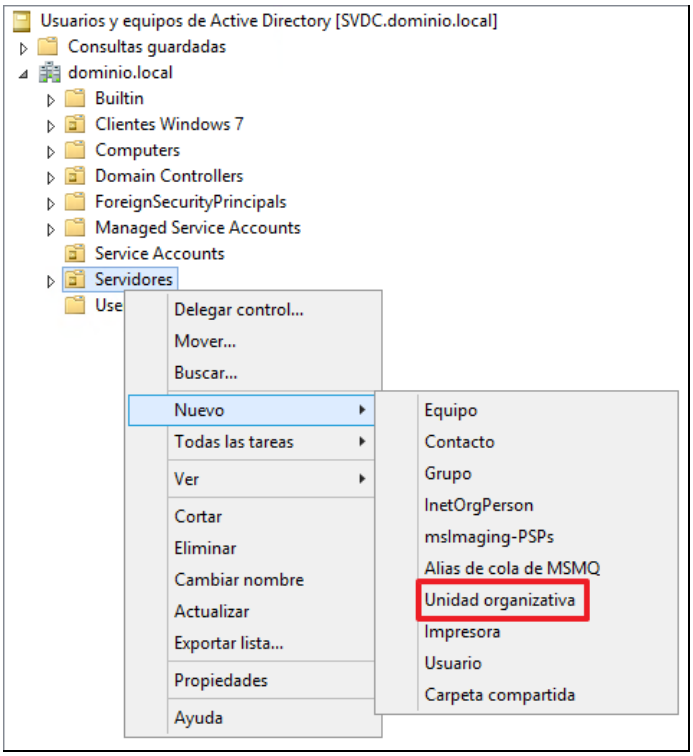
Se ha de tener en consideración que el servidor que aloja el producto de MS SQL Server también contiene Internet Information Services 8.5 para el rol de servicios de informes de SCCM por lo que será necesario aplicar previamente la guía de seguridad “CCN-STIC-873 ENS Incremental IIS 8.5”.

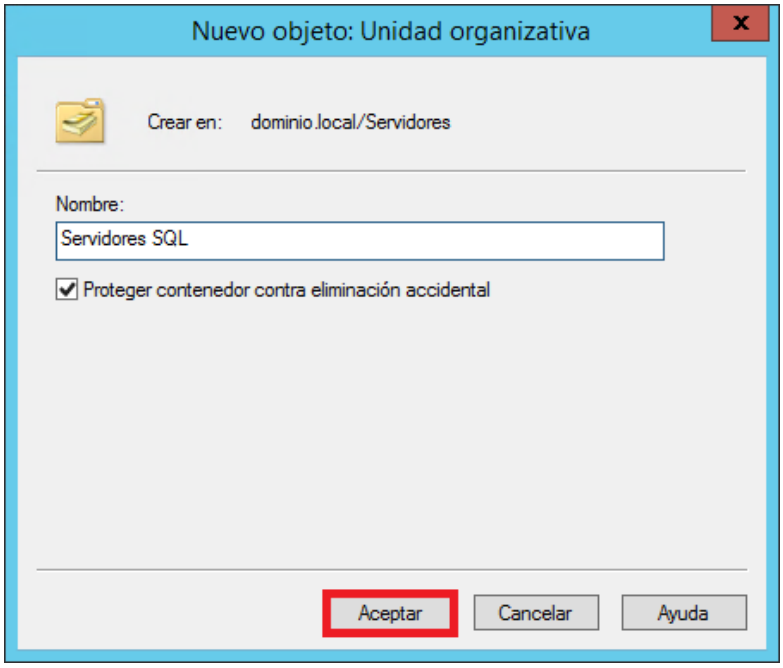
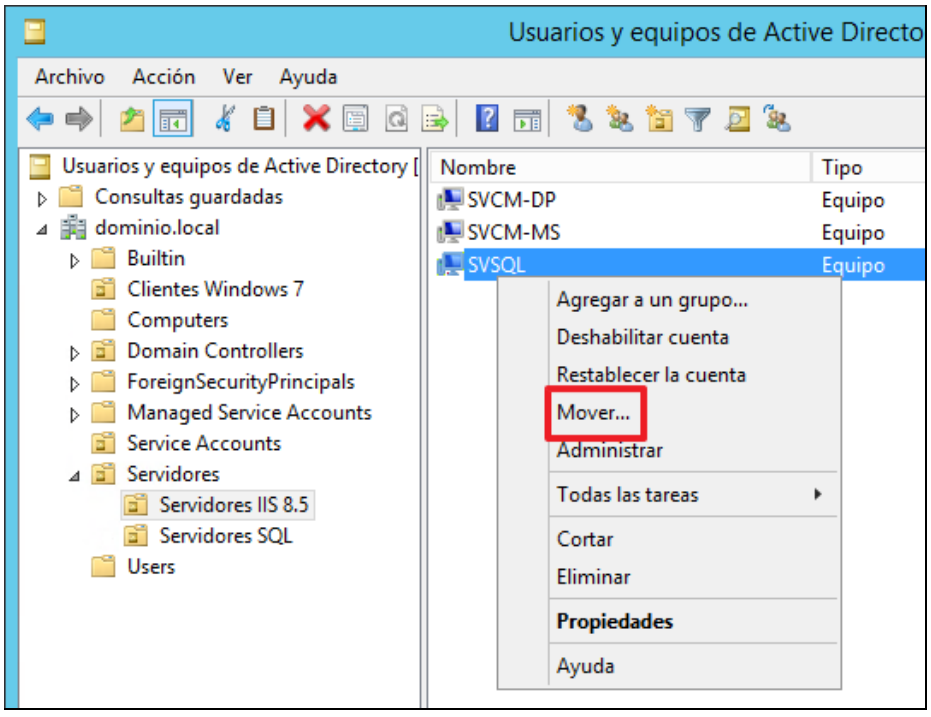
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

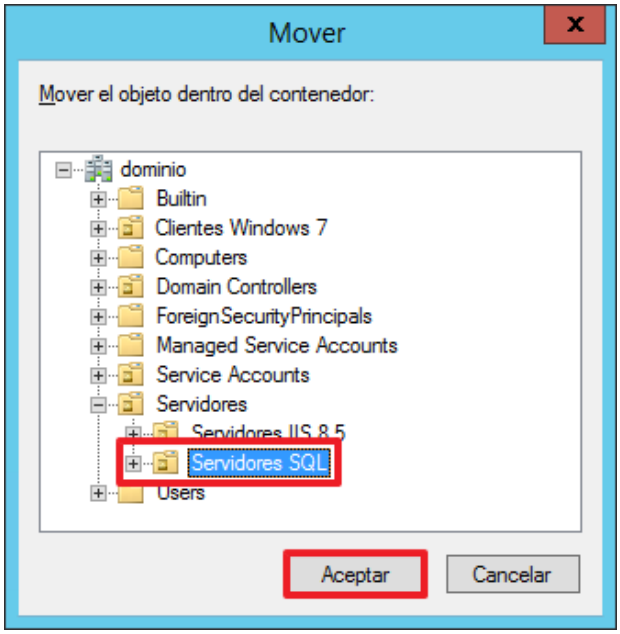
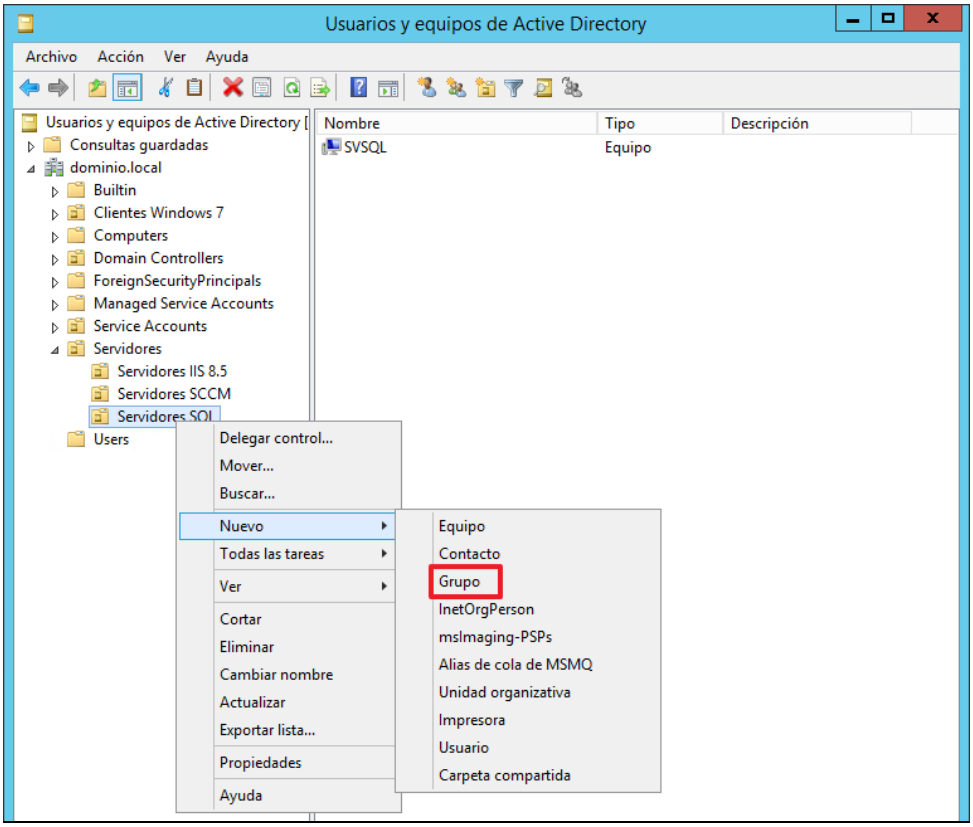
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.

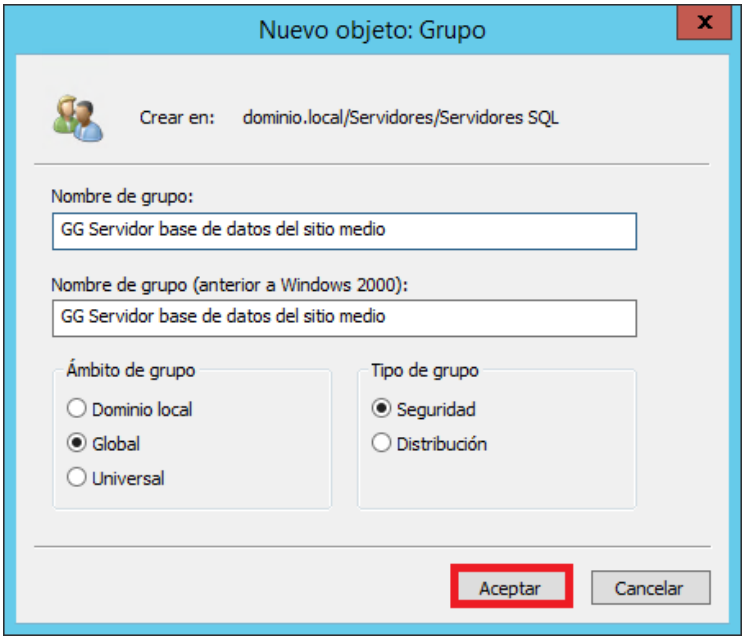
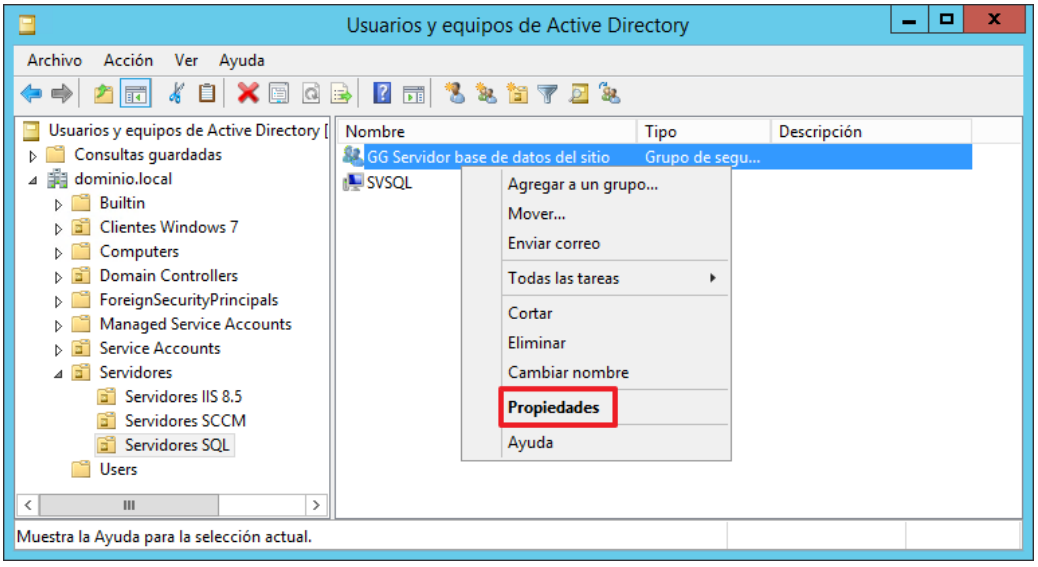
Paso	Descripción
5.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Copie el fichero “CCN-STIC-875 ENS Incremental SQL medio.inf” que se encuentra en “C:\Scripts\Nivel Medio” al directorio “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 

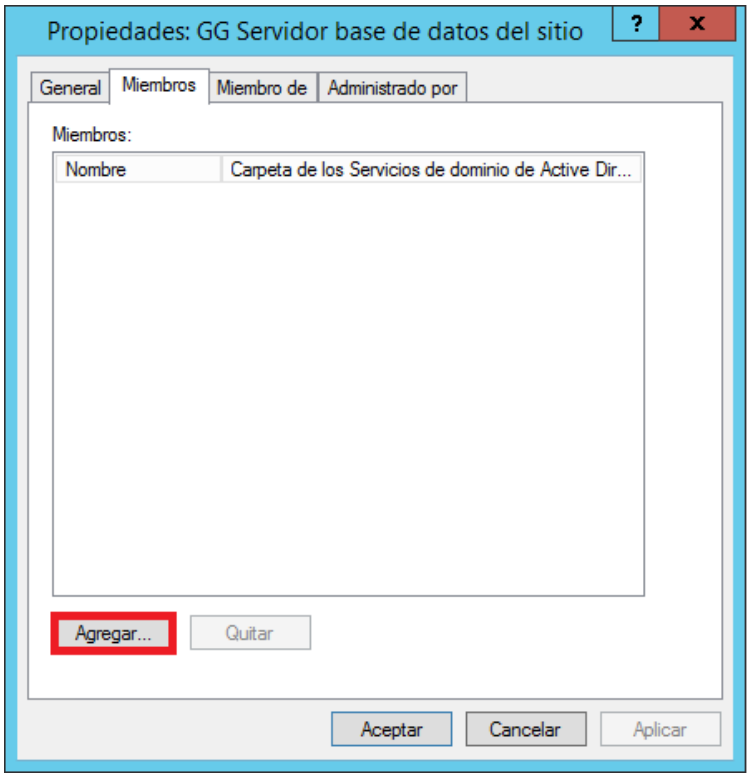
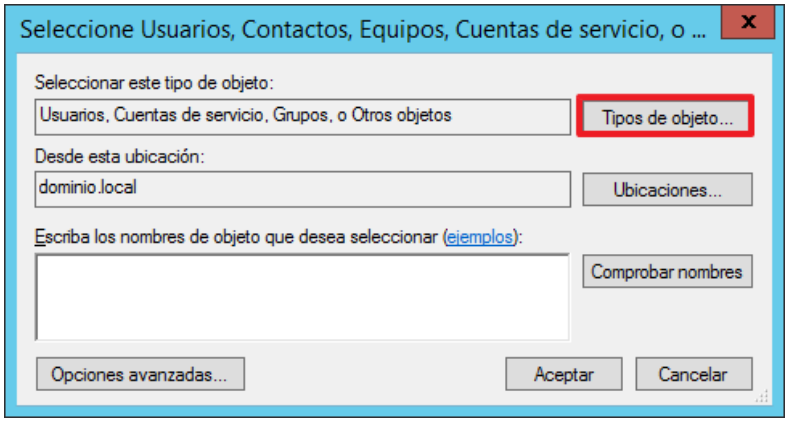
Paso	Descripción
7.	Pulse con el botón derecho sobre el fichero y seleccione la opción “Abrir” del menú contextual. 
8.	A continuación, deberá modificar el fichero para adaptarlo a su organización, para ello localice el servicio “SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL” y modifique el nombre del servicio cambiando el texto “DOMINIO.LOCAL” por el nombre de dominio de su organización.  **Nota:** Si no modifica este fichero el servicio “SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL”, no se reforzará la seguridad según los parámetros establecidos en el documento.
9.	Guarde los cambios realizados y cierre el documento.

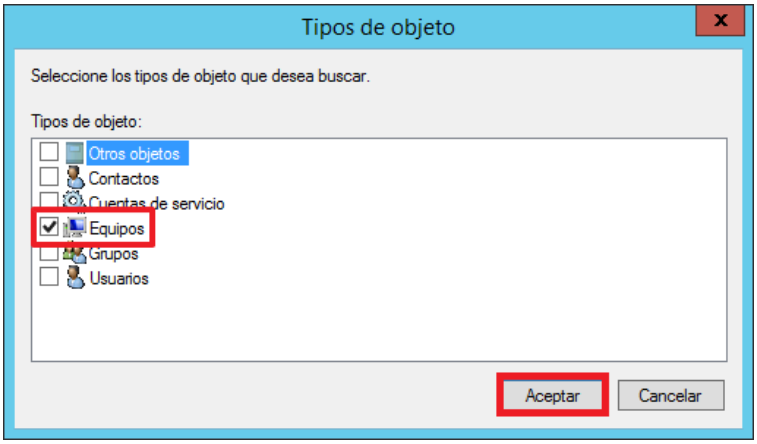
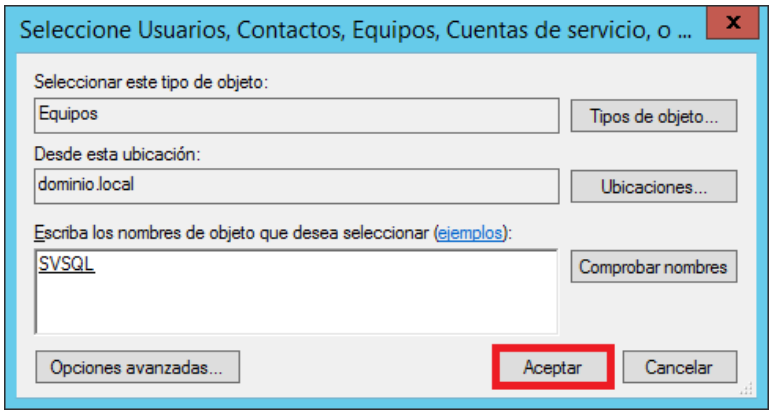
Paso	Descripción
10.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .
11.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 

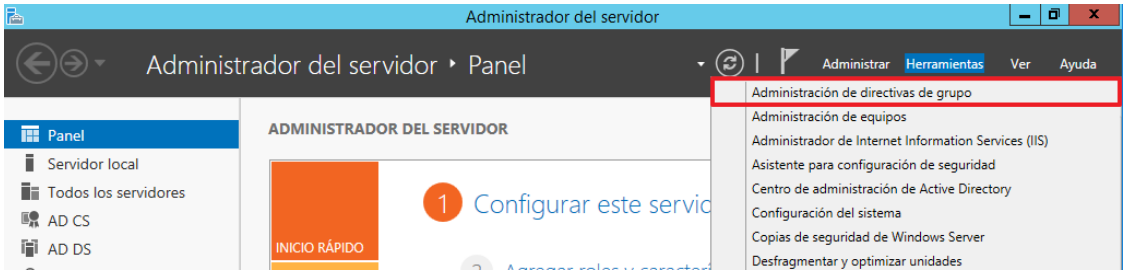
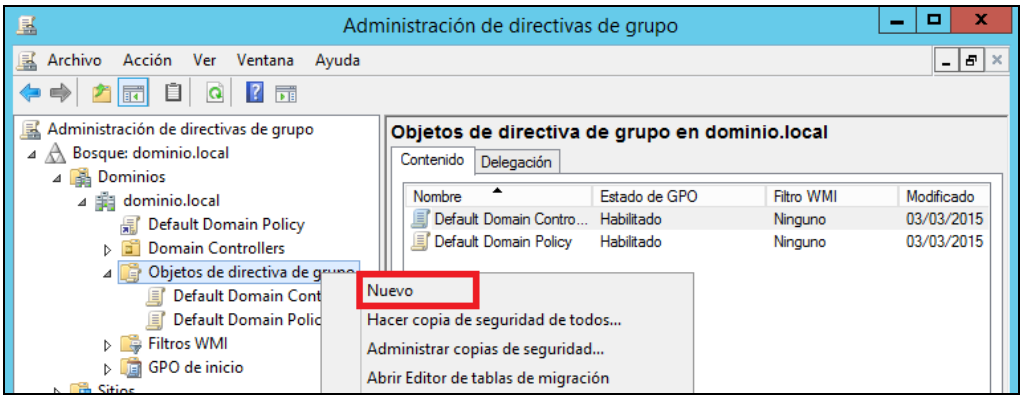
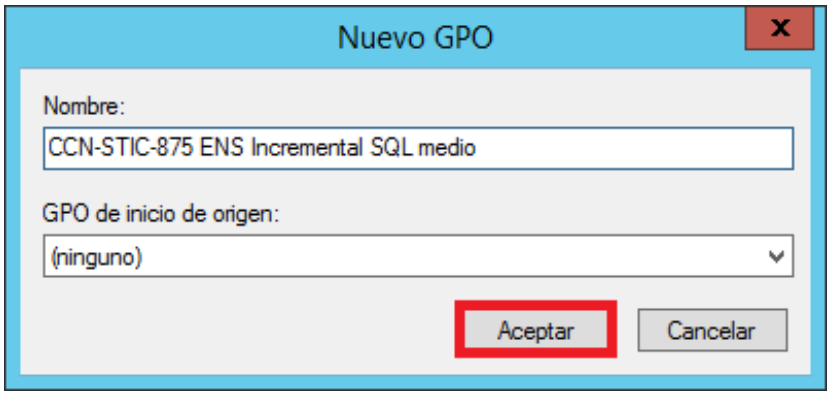
Paso	Descripción
12.	En la consola, cree una unidad organizativa denominada “Servidores SQL” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar”. 
13.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores SQL a la unidad organizativa “Servidores SQL”. Para ello, deberá localizar los servidores y hacer clic con el botón derecho sobre el servidor que desee ubicar en la nueva unidad organizativa y marcar en “mover” del menú contextual. 

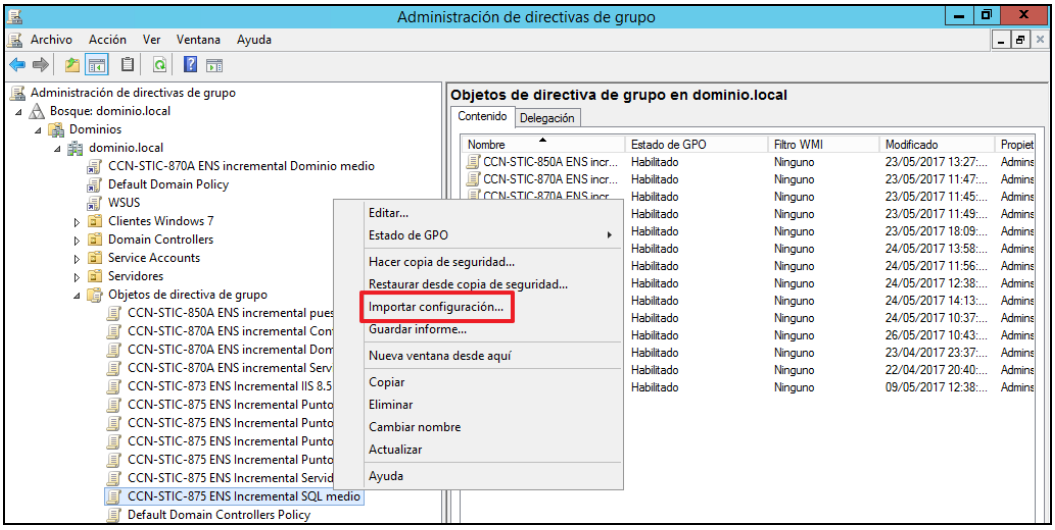
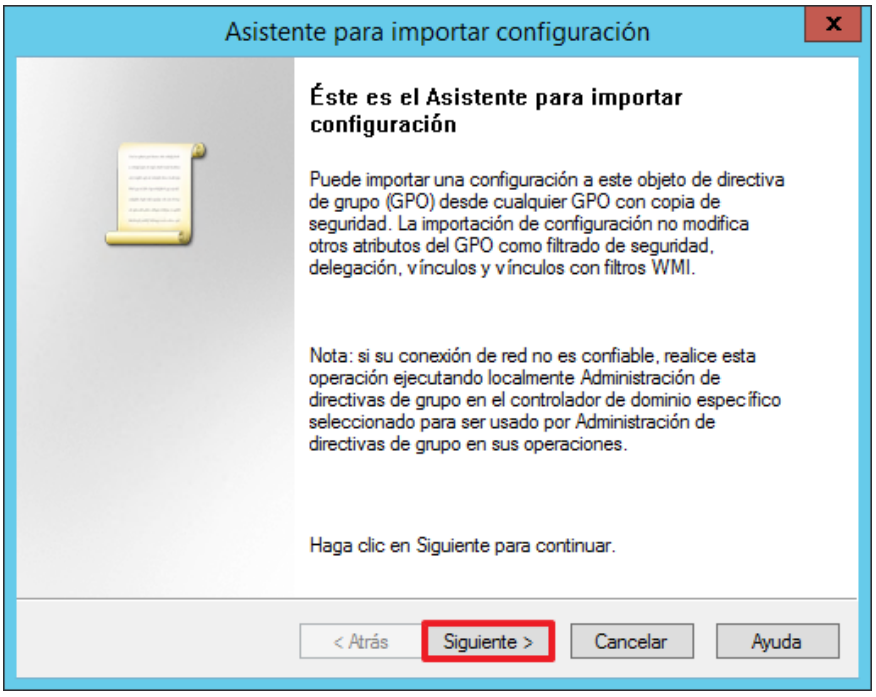
Paso	Descripción
14.	En el árbol de contenedores, seleccione la unidad organizativa “Servidores SQL” y “Aceptar”. 
15.	En el siguiente paso, seleccione la unidad organizativa “Servidores SQL”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 

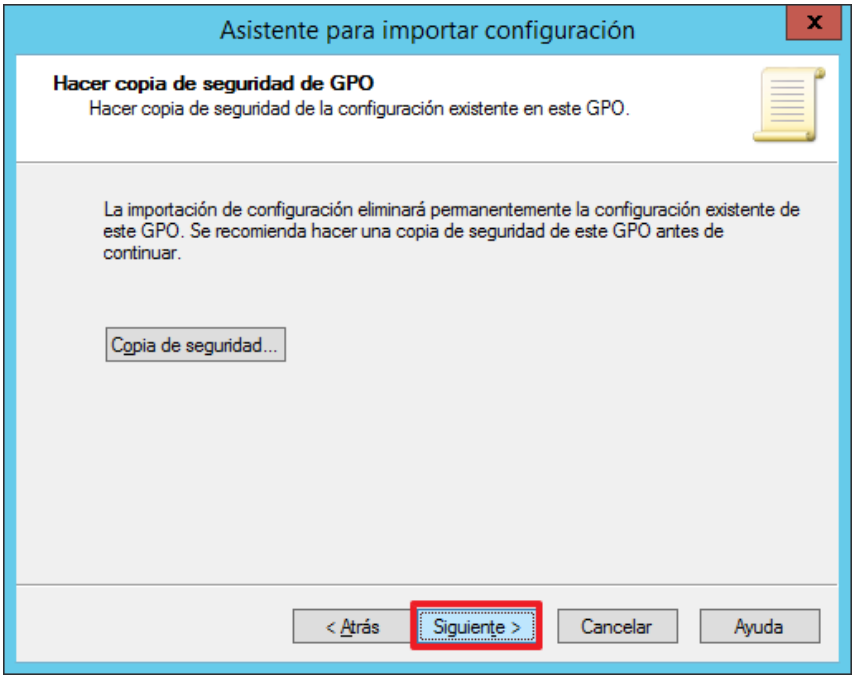
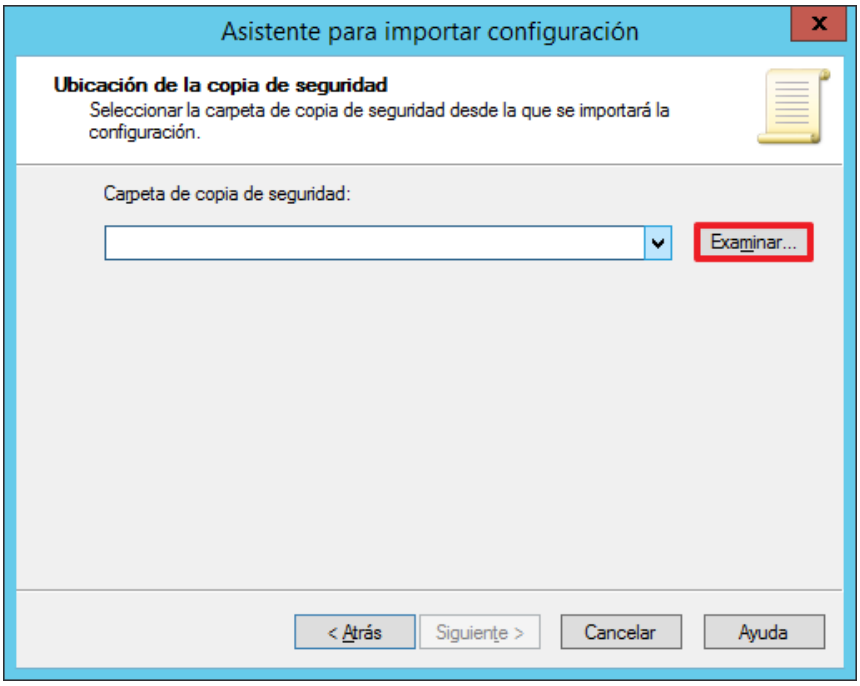
Paso	Descripción
16.	Escriba el nombre “GG Servidor base de datos del sitio medio” y pulse “Aceptar”. 
17.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 

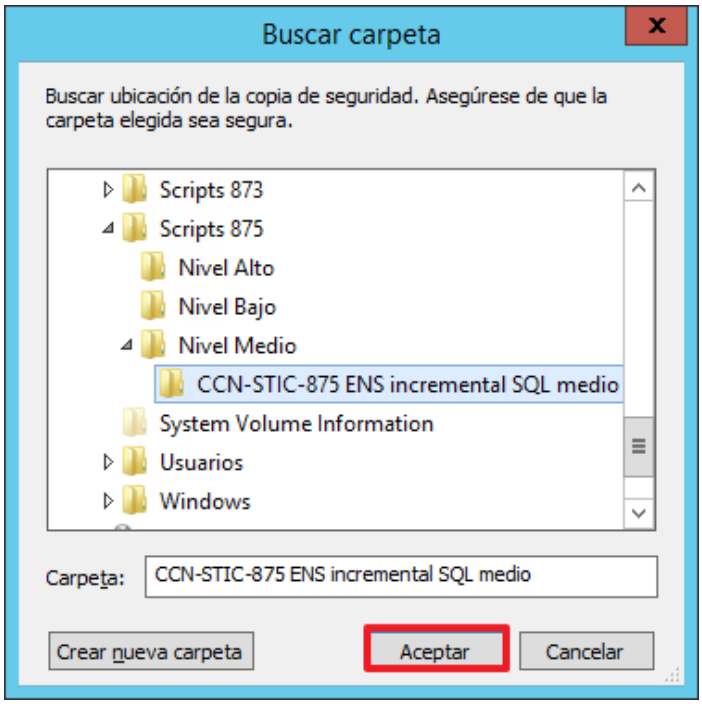
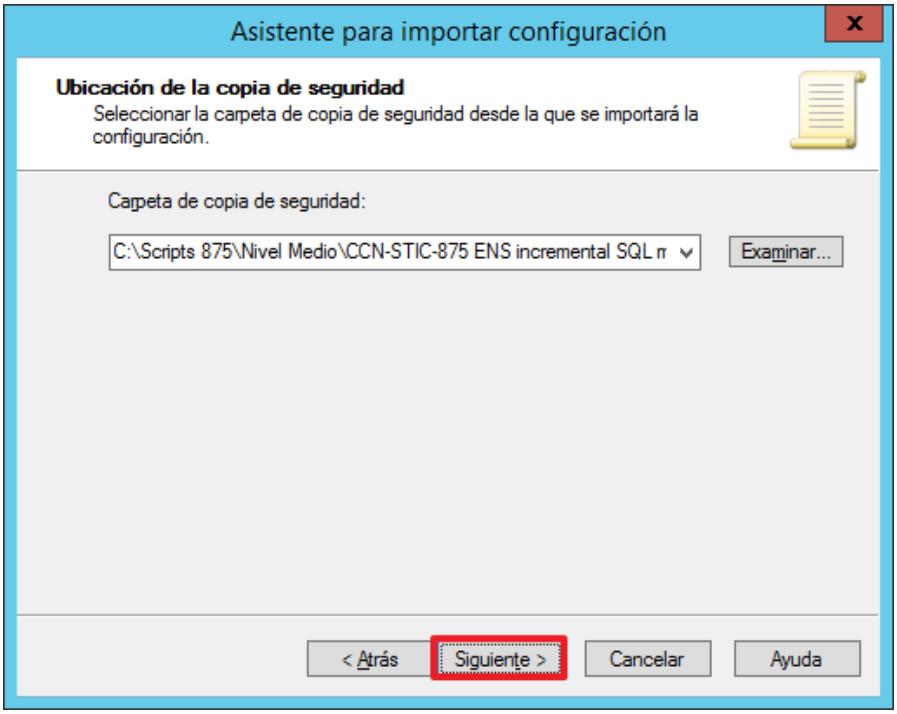
Paso	Descripción
18.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan MS SQL Server al grupo. 
19.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 

Paso	Descripción
20.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
21.	Agregue los equipos y pulse sobre “Aceptar”. 
22.	Pulse “Aceptar” para cerrar las propiedades del grupo. 

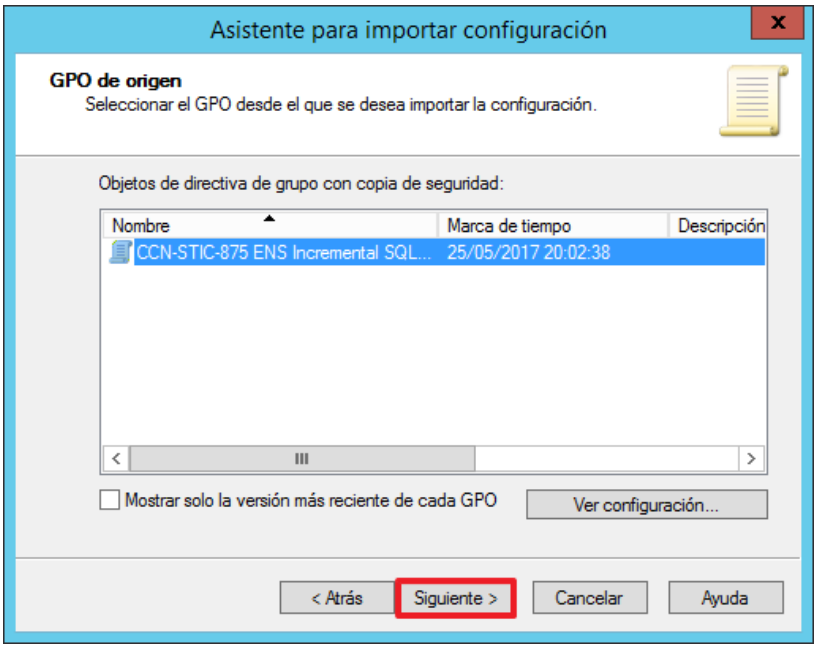
Paso	Descripción
23.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
24.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
25.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.
26.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 
27.	Introduzca como nombre “CCN-STIC-875 ENS Incremental SQL medio” y pulse el botón “Aceptar”.  **Nota:** Se debe tener en consideración que en esta directiva de seguridad se va a habilitar el protocolo SSL 3.0 para el correcto funcionamiento del servicio de SQL, en caso de que exista algún inconveniente deberá adaptar estos pasos a su organización.

Paso	Descripción
28.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
29.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 

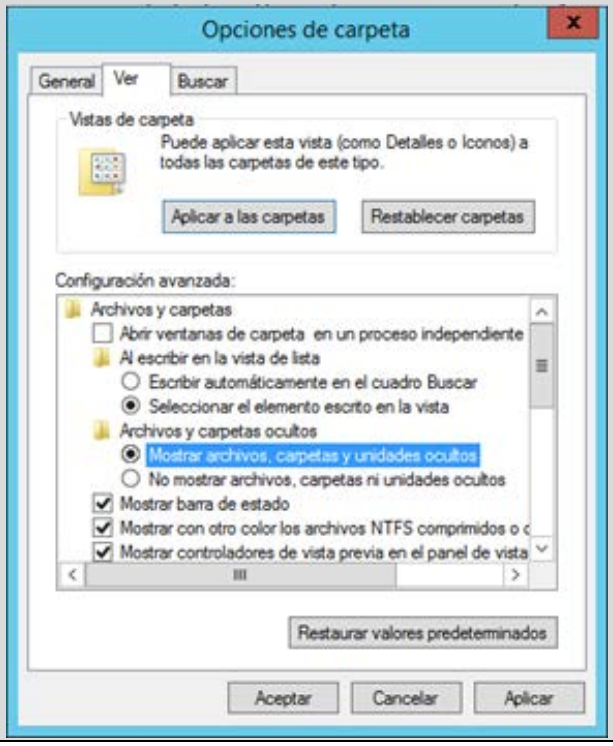
Paso	Descripción
30.	En la selección de copia de seguridad pulse el botón “Siguiente >”.  **Nota:** No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
31.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 

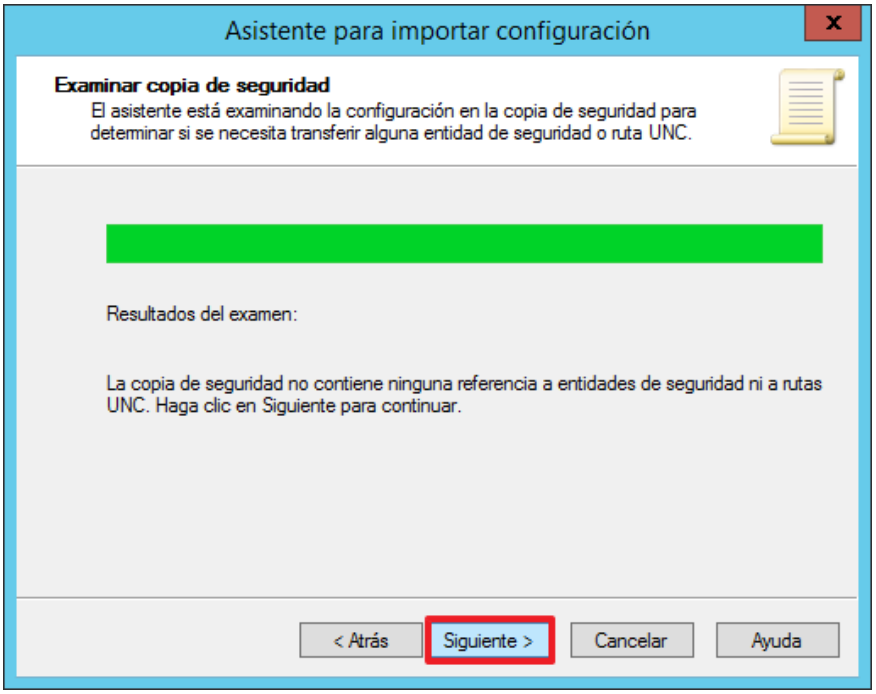
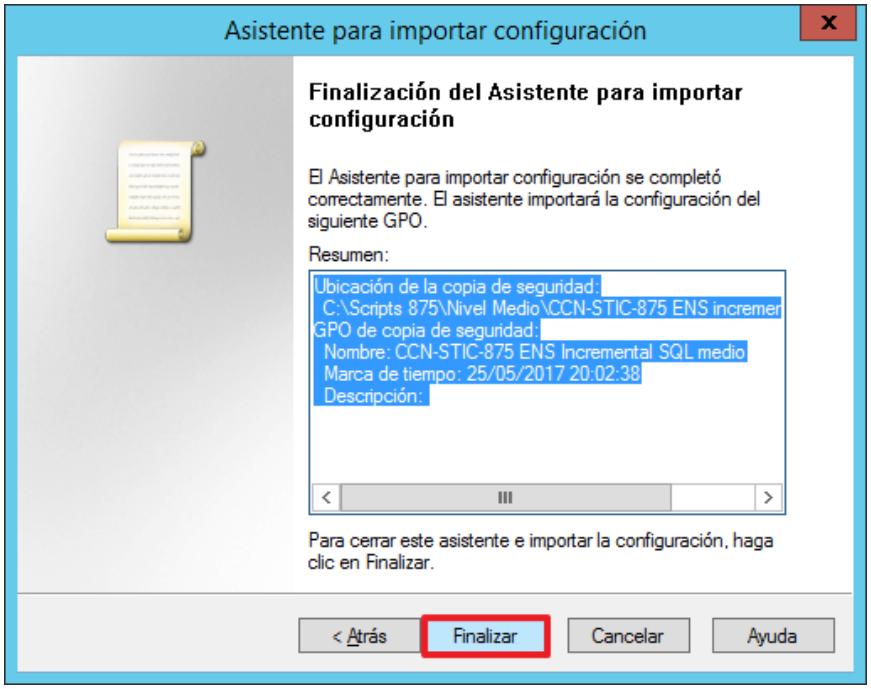
Paso	Descripción
32.	Seleccione la carpeta “CCN-STIC-875 ENS Incremental SQL medio” que encontrará en la carpeta “C:\Scripts\Nivel Medio” y pulse el botón “Aceptar”. 
33.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

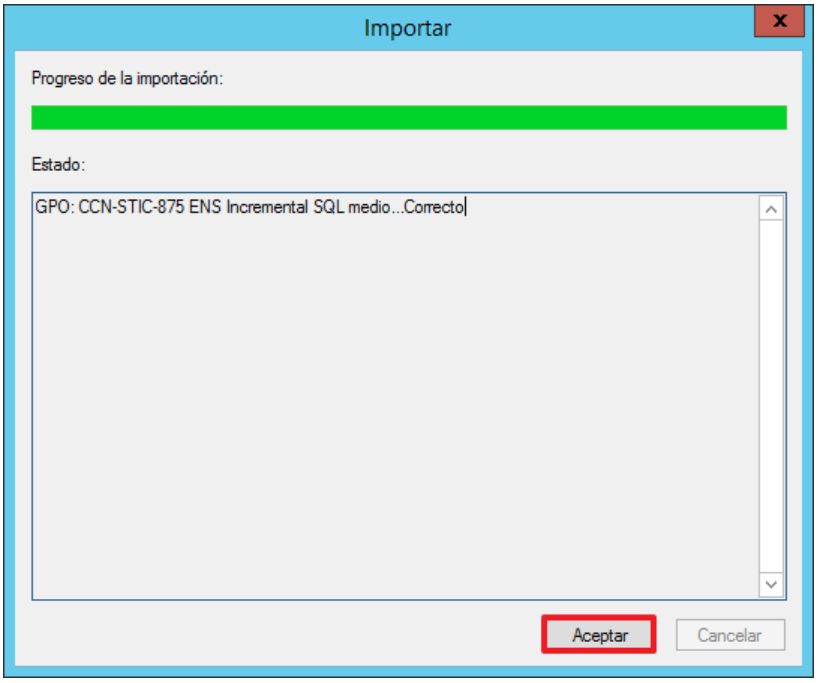
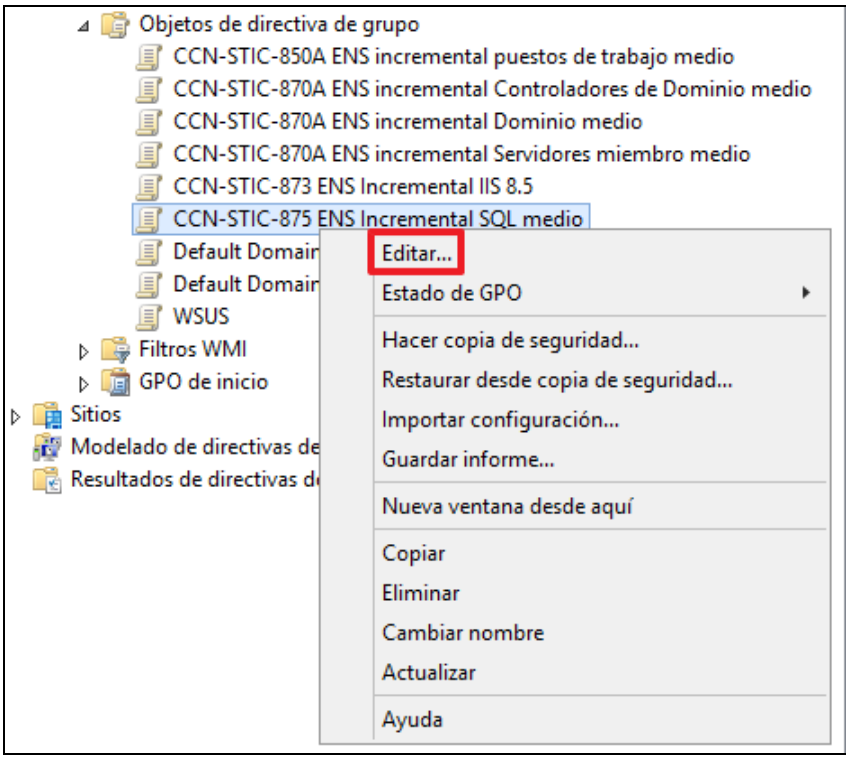
Paso	Descripción
34.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-875 Incremental SQL medio” y pulse el botón “Siguiente >”.

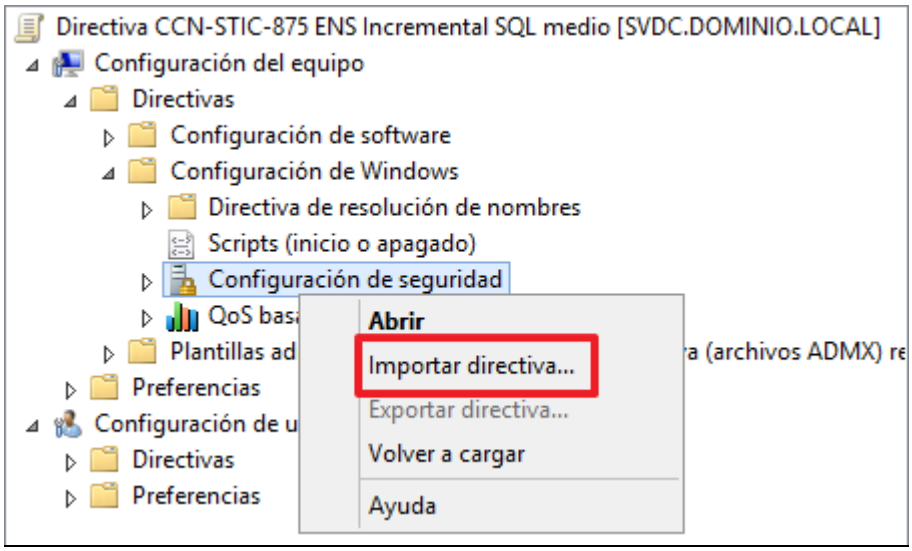
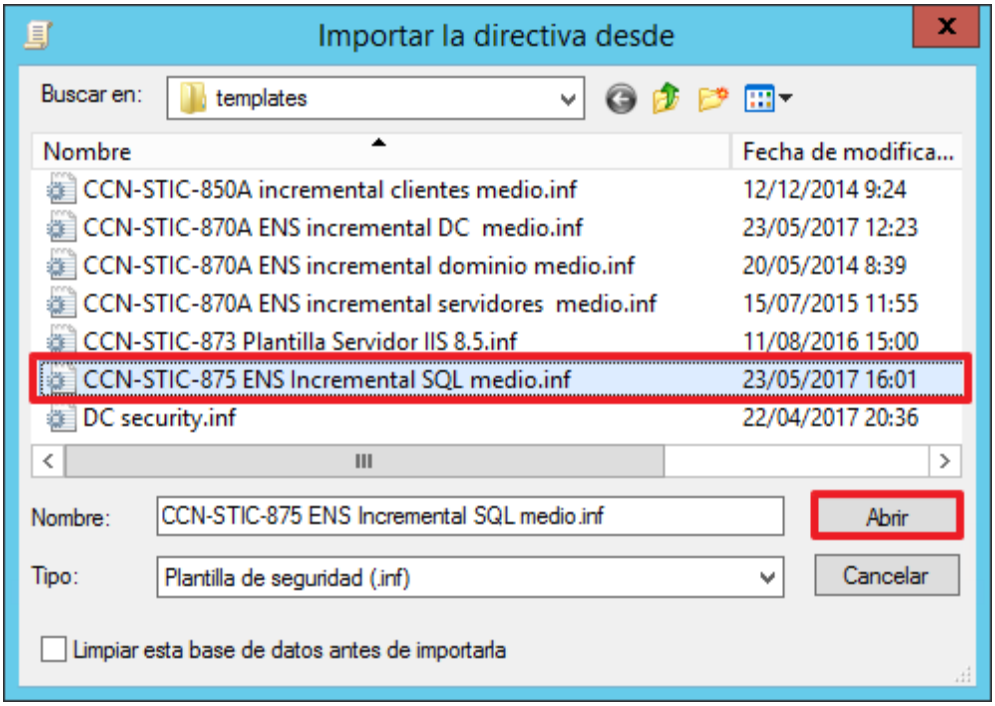


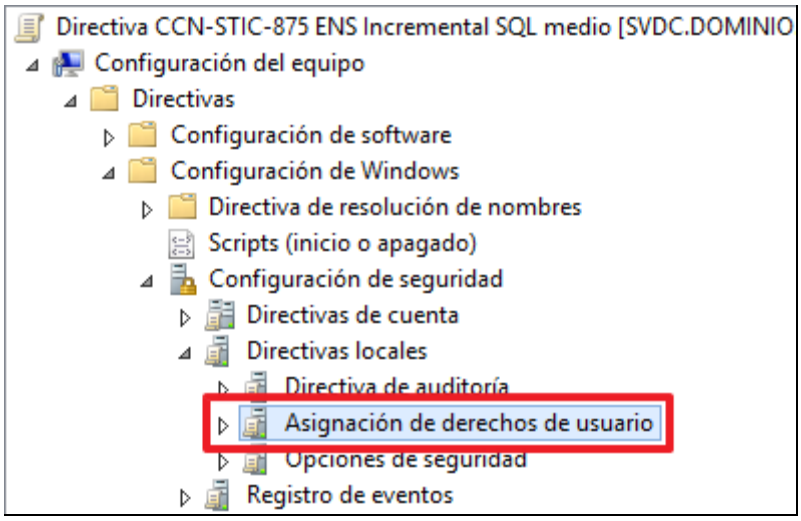
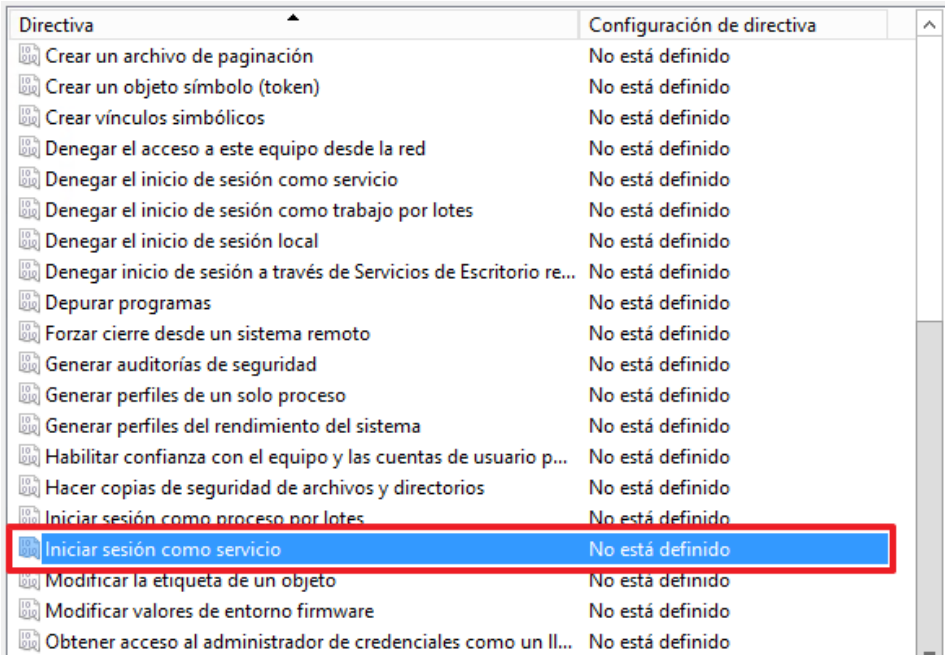
Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe activar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”.

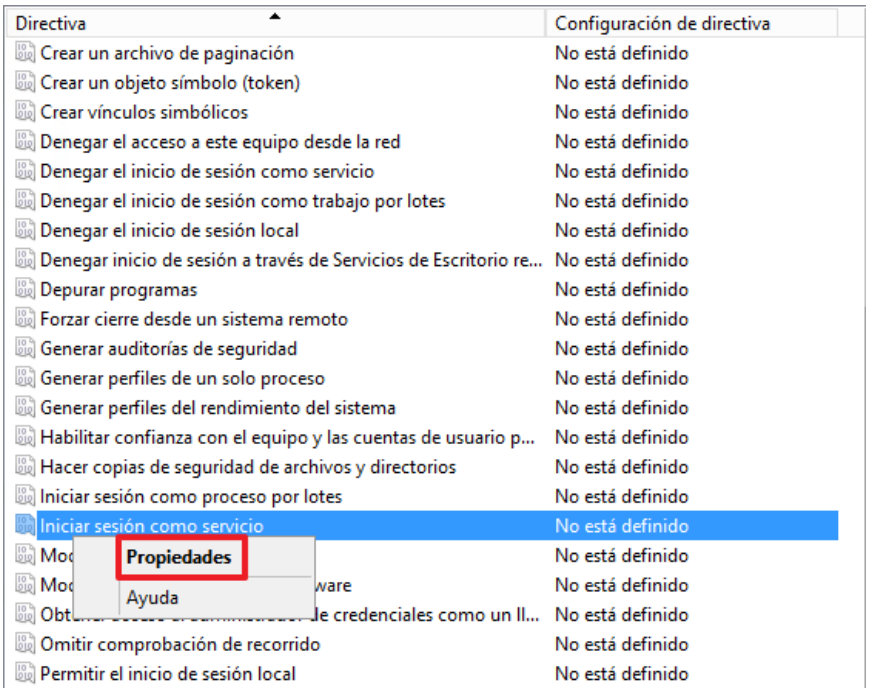
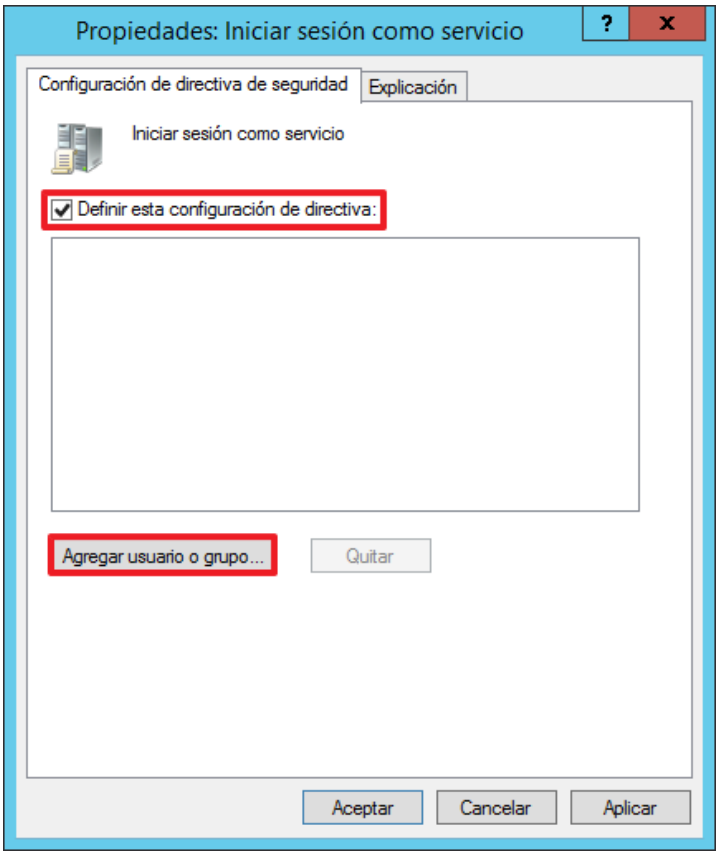


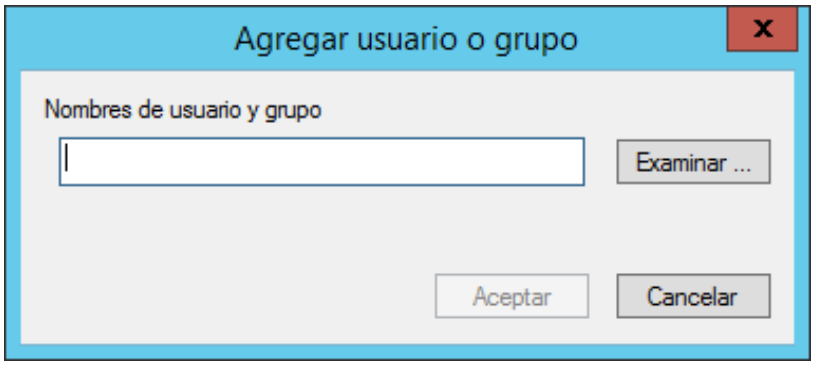
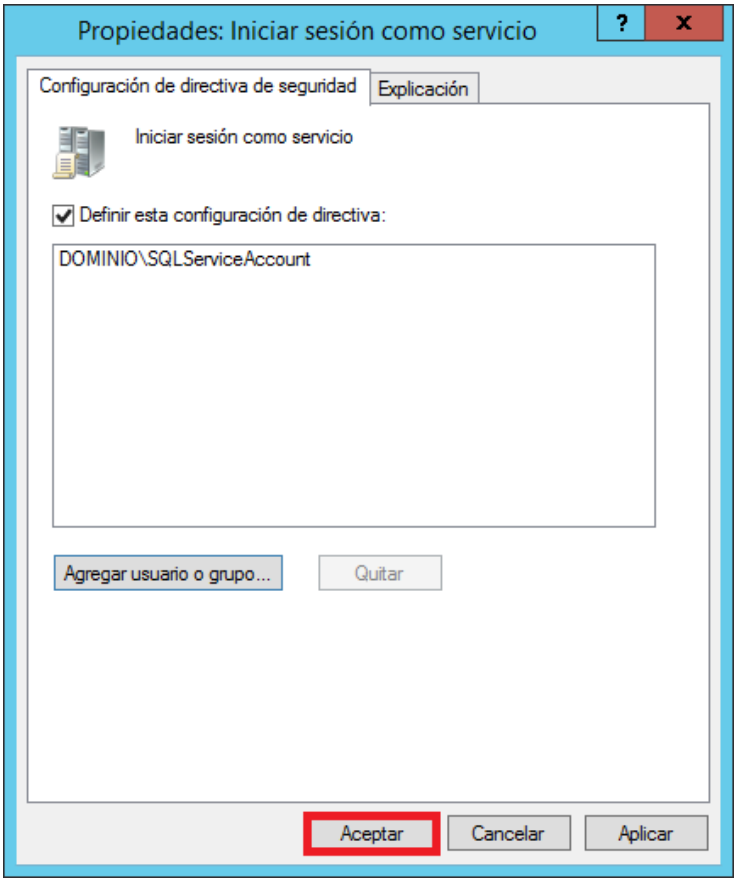
Paso	Descripción
35.	En la pantalla de “Examinar copia de seguridad”, pulse el botón “Siguiente >”. 
36.	Si apareciera la ventana “Migrar referencias”, mantenga las opciones y pulse el botón “Siguiente >”.
37.	Para finalizar el asistente pulse el botón “Finalizar”. 

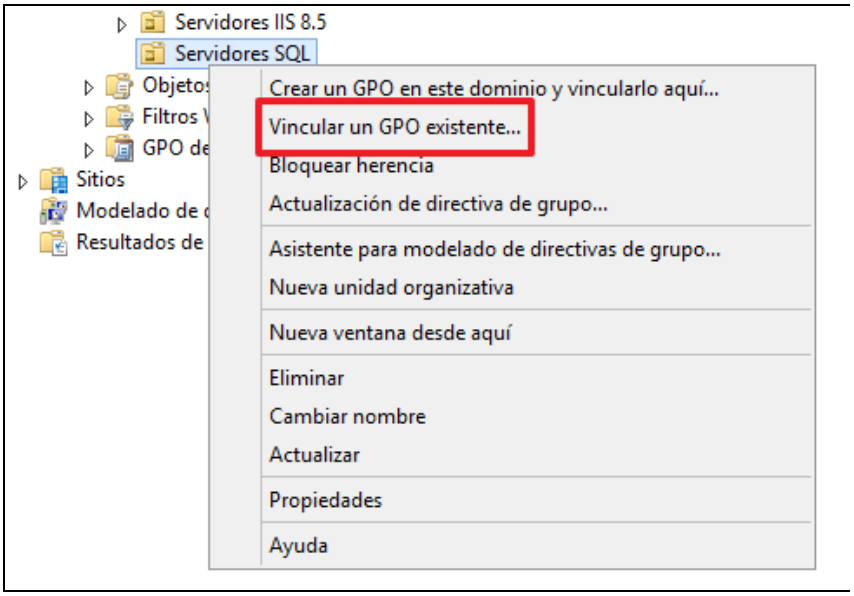
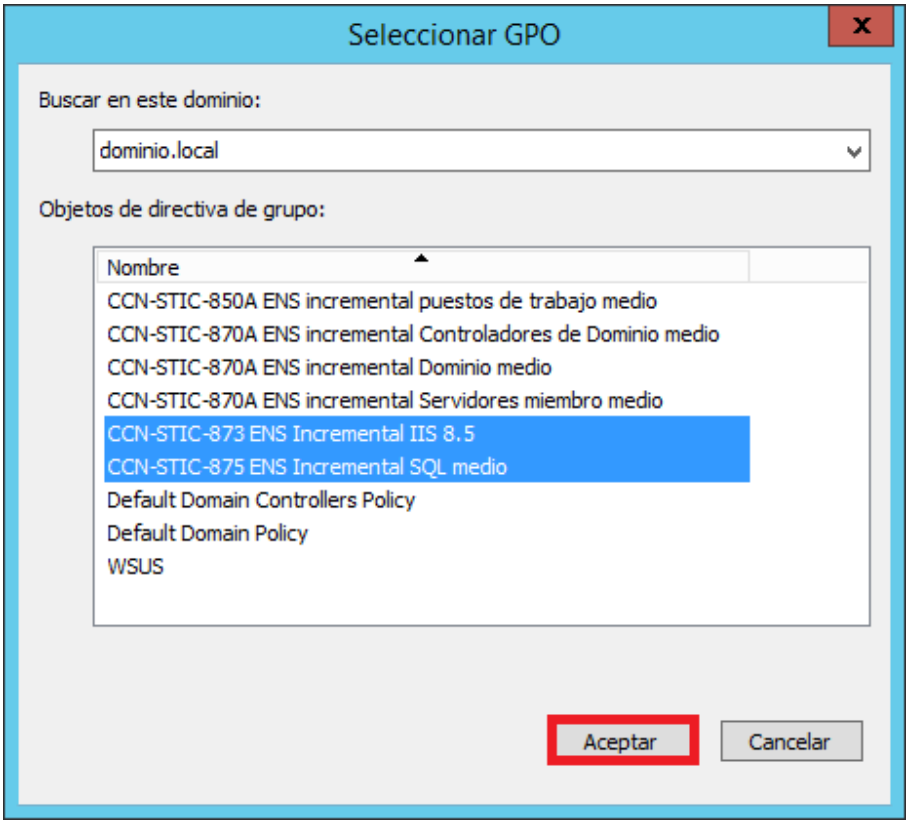
Paso	Descripción
38.	Para cerrar el asistente pulse el botón “Aceptar”. 
39.	A continuación, seleccione la política recién configurada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 

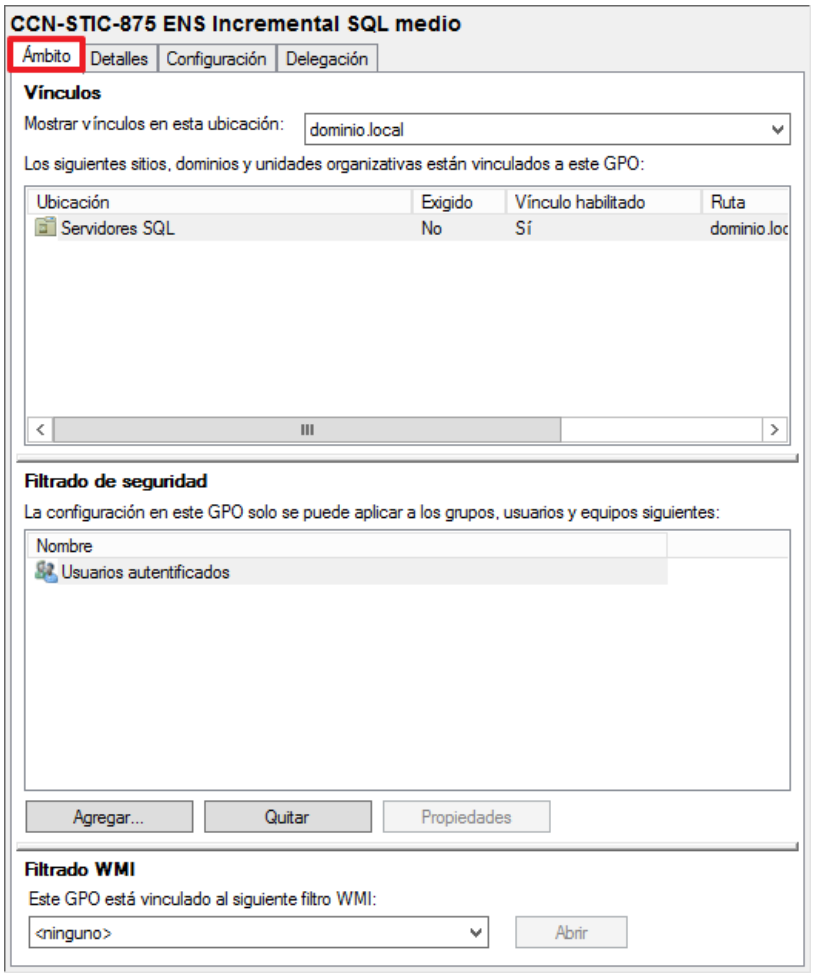
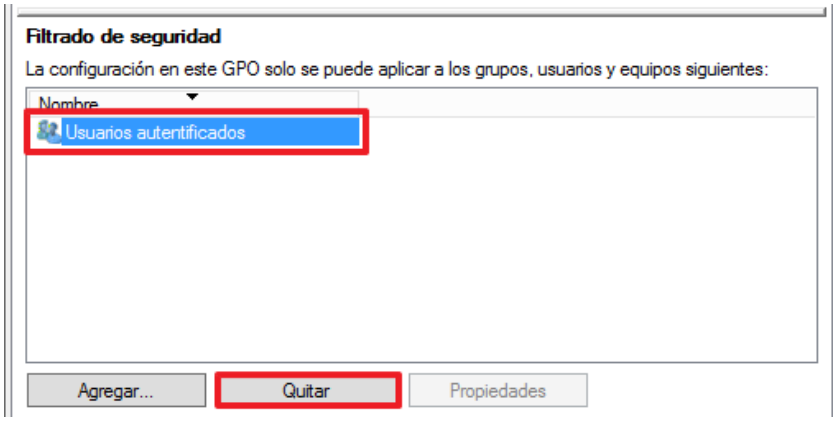
Paso	Descripción
40.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 
41.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental SQL medio.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en el botón "Abrir". 

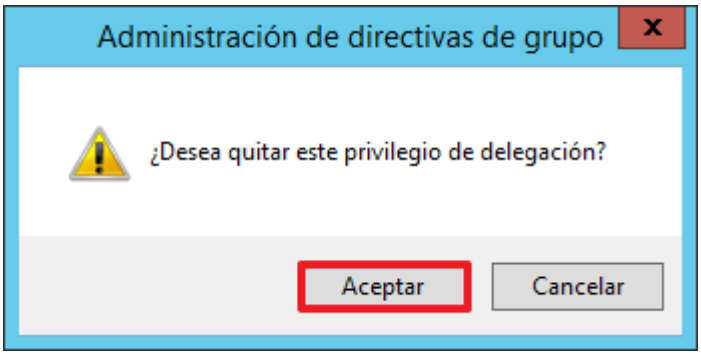
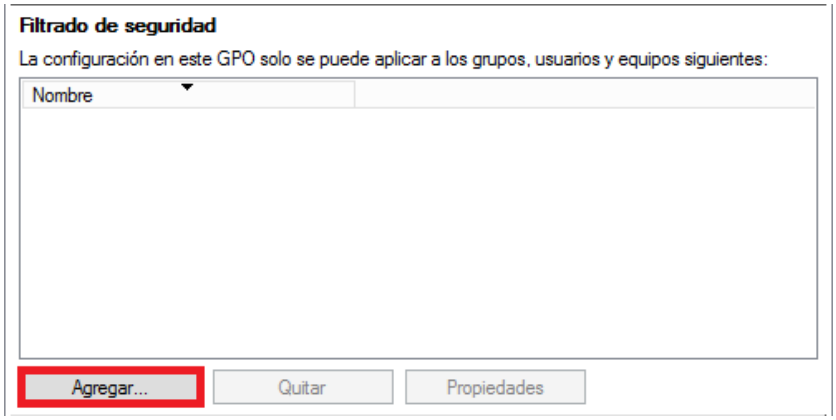
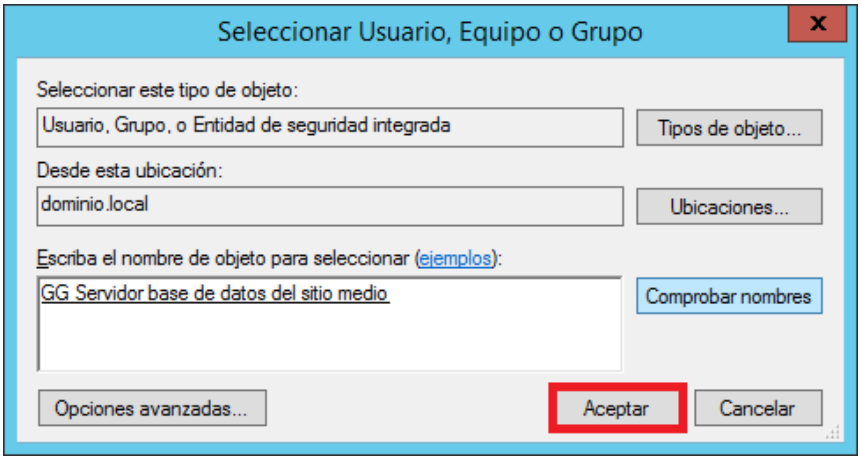
Paso	Descripción
42.	Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario".** 
43.	A continuación, seleccione la directiva "Iniciar sesión como servicio". 

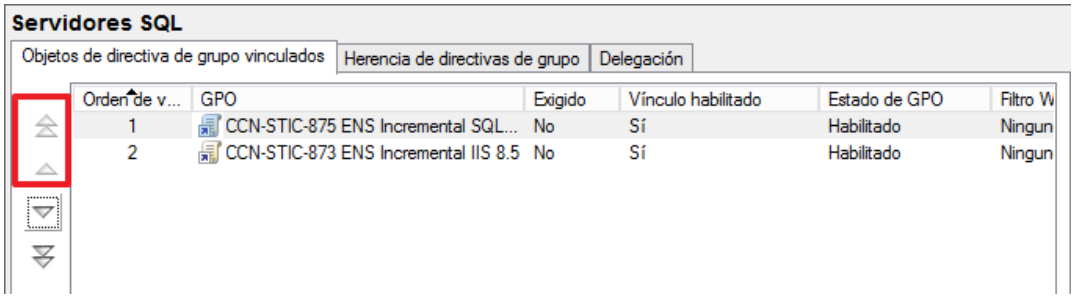
Paso	Descripción
44.	Pulse con el botón derecho sobre la directiva y seleccione la opción “Propiedades” del menú contextual. 
45.	Seleccione la opción “Definir esta configuración de directiva” y pulse sobre “Agregar usuario o grupo...”. 

Paso	Descripción
46.	Agregue los usuarios necesarios para iniciar los servicios de SQL requeridos para un correcto funcionamiento del servicio. 
47.	Una vez añadidos los usuarios necesarios pulse “Aceptar”.  **Nota:** Deberá adaptar estos pasos a su organización y añadir únicamente los usuarios necesarios para un correcto funcionamiento del servicio.
48.	Cierre el editor de administración de directivas de grupo para finalizar la configuración.

Paso	Descripción
49.	A continuación, seleccione la unidad organizativa “Servidores SQL” y pulse botón derecho, “Vincular un GPO existente…”. 
50.	Seleccione los objetos de directiva de grupo con nombre, “*CCN-STIC-875 ENS Incremental SQL medio*” y “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse aceptar. 

Paso	Descripción
51.	Seleccione la directiva de grupo "*CCN-STIC-875 ENS Incremental SQL medio*" y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 
52.	En la opción de filtrado de seguridad, seleccione "Usuarios autentificados" y pulse la opción "Quitar". 

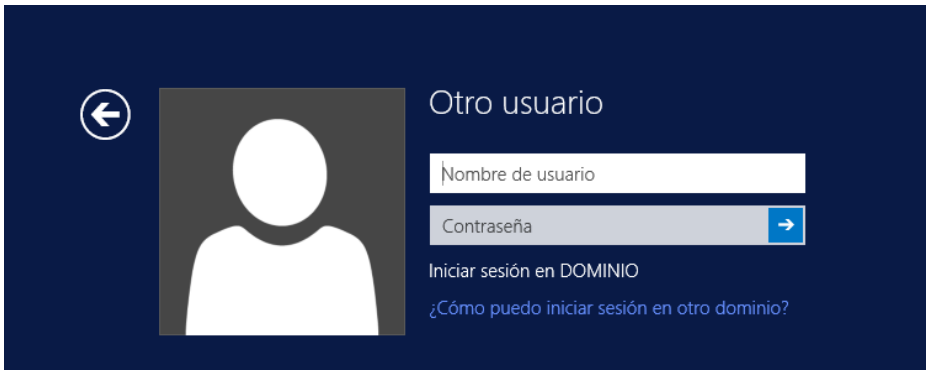
Paso	Descripción
53.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
54.	Una vez quitado, pulse el botón “Agregar…”. 
55.	Introduzca como nombre “GG Servidor base de datos del sitio medio” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.

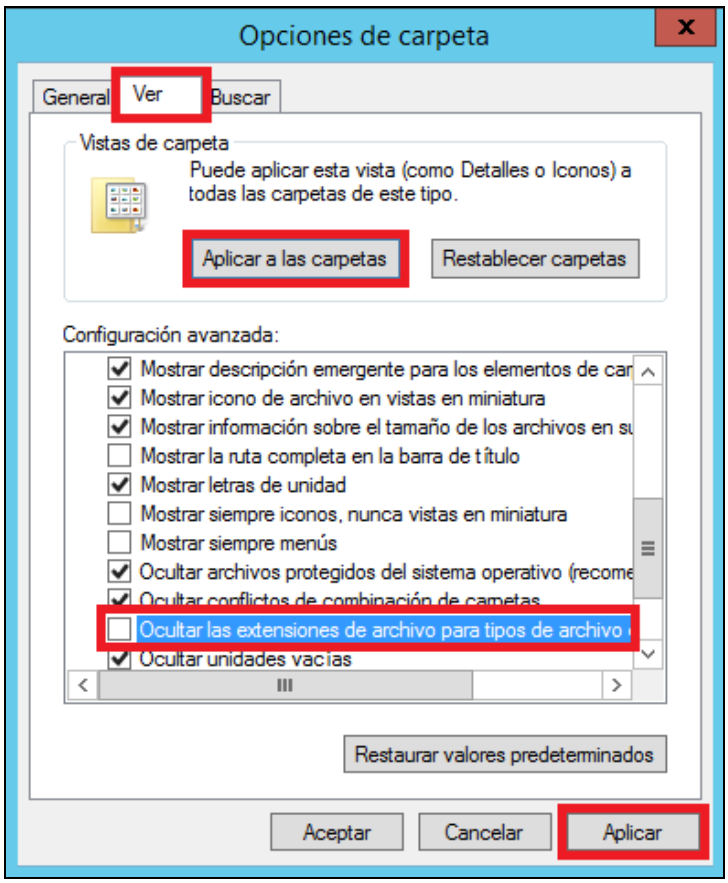
Paso	Descripción
56.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva “CCN-STIC-875 ENS Incremental SQL medio” aparezca en primer lugar. Para ello despliegue, la unidad organizativa “Servidores SQL” y a continuación seleccione la directiva y haga clic sobre la fecha doble hacia arriba para que se sitúe con el número 1 de orden vínculos, tal y como se muestra en la imagen. 
57.	Cierre el administrador de directivas de grupo para finalizar con la configuración.

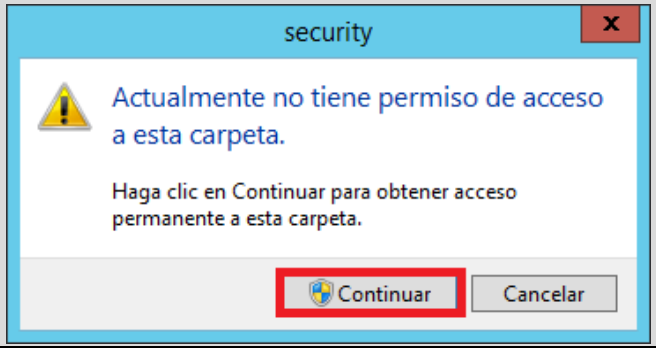
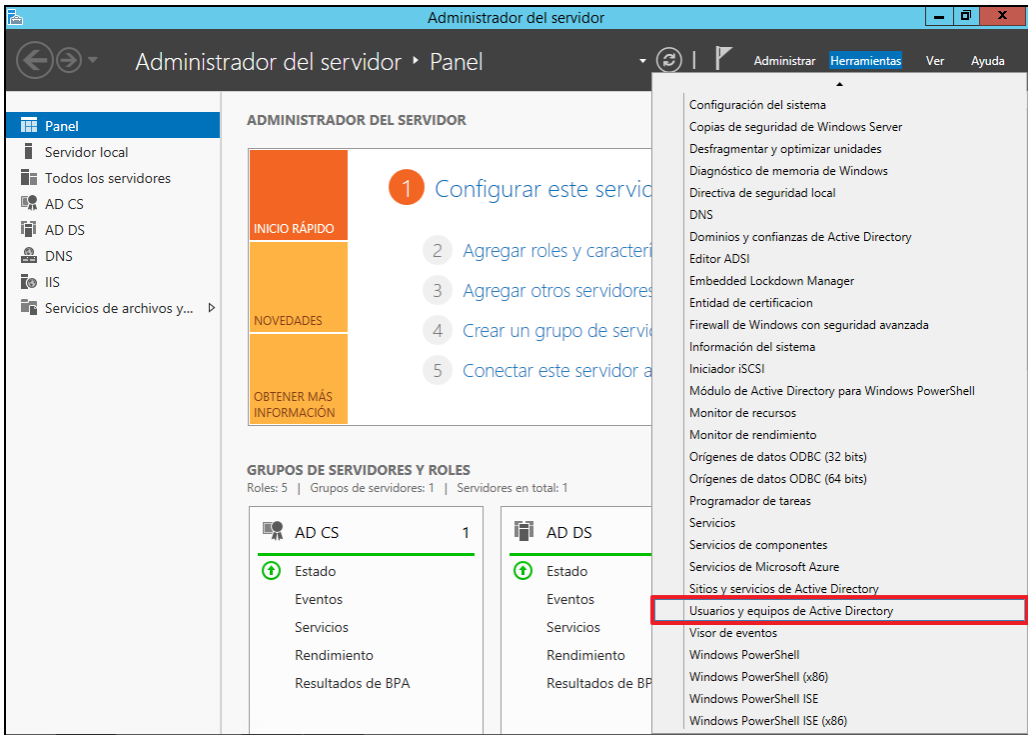
2. REFUERZO DE SEGURIDAD DEL SERVIDOR DEL SITIO

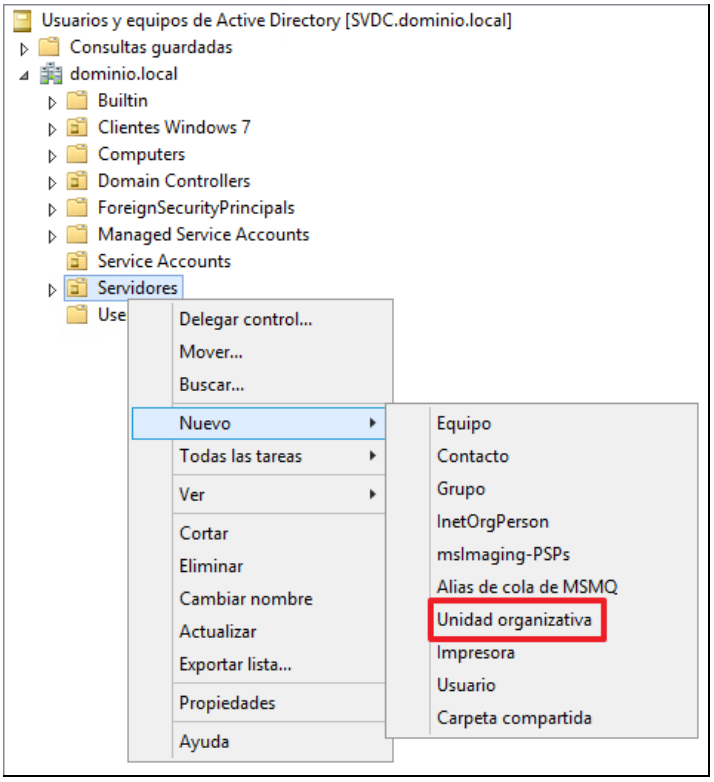
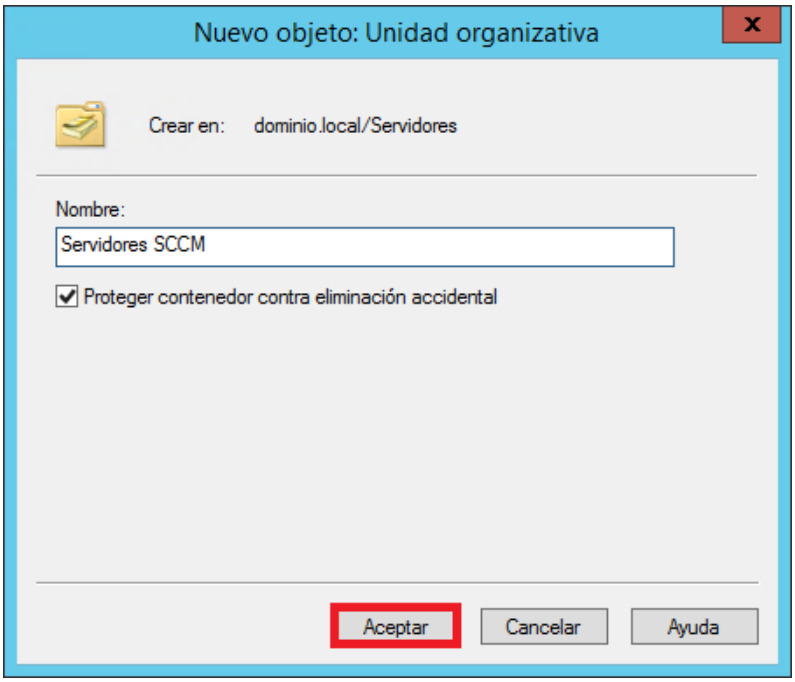
A continuación, se describen los pasos para reforzar la seguridad de un servidor con el rol de servidor de sitio, el cual también incluye el rol de Sistema de sitio y servidor de componentes.

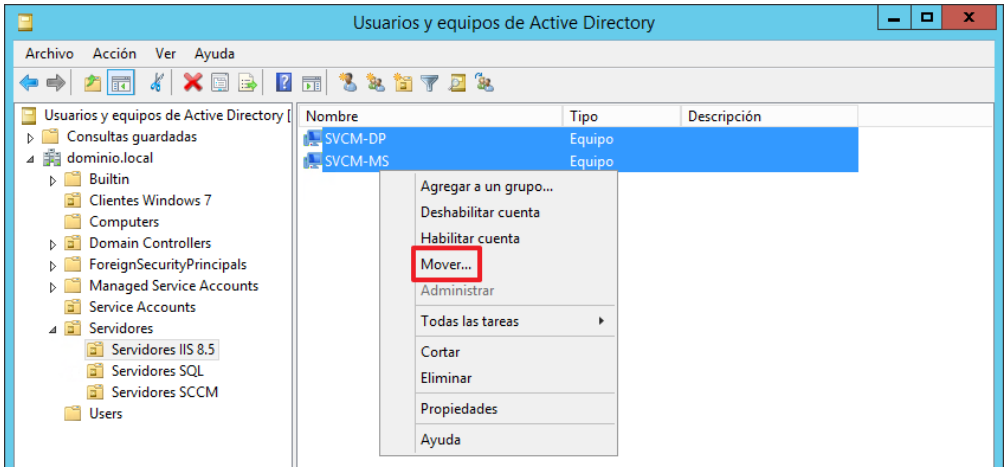
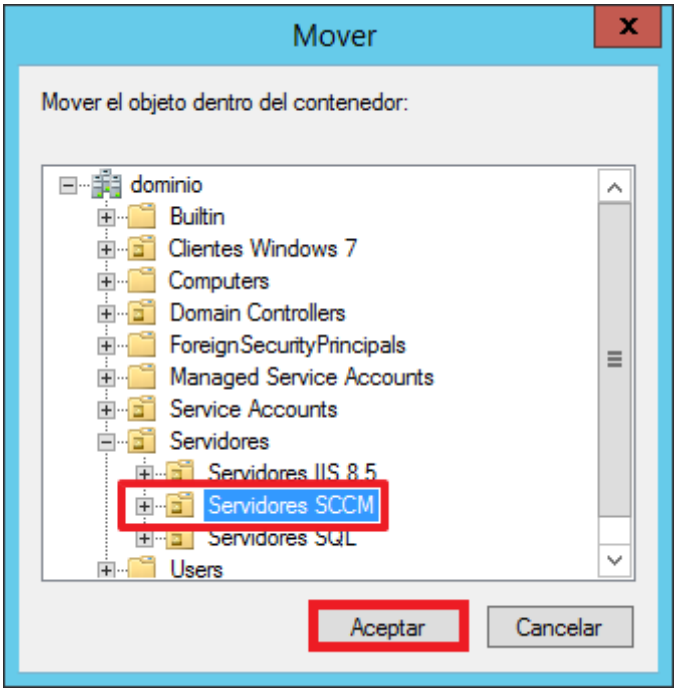
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

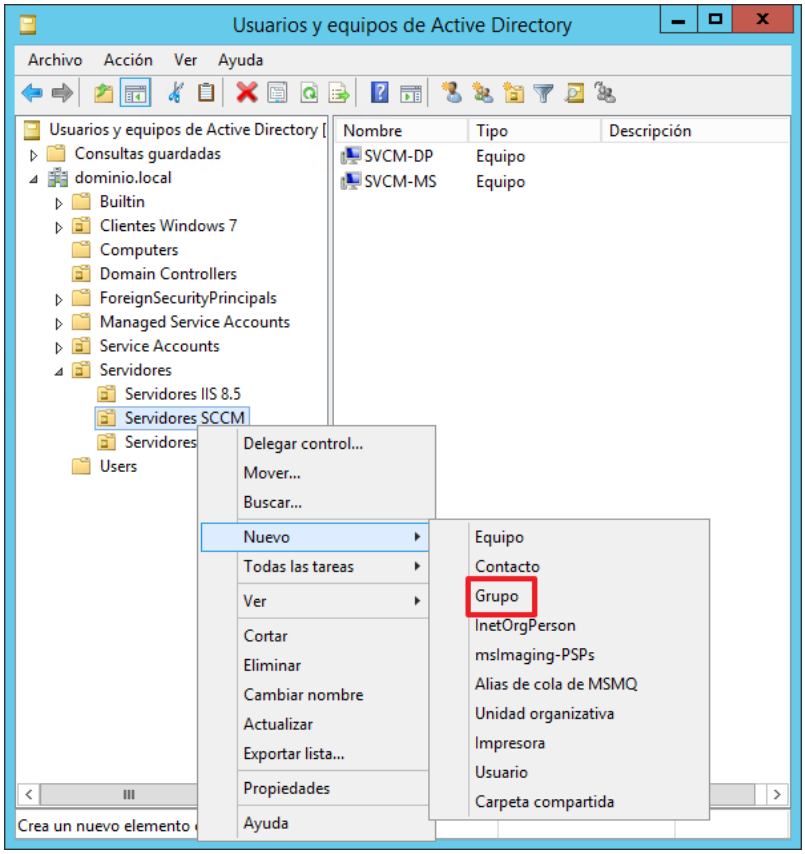
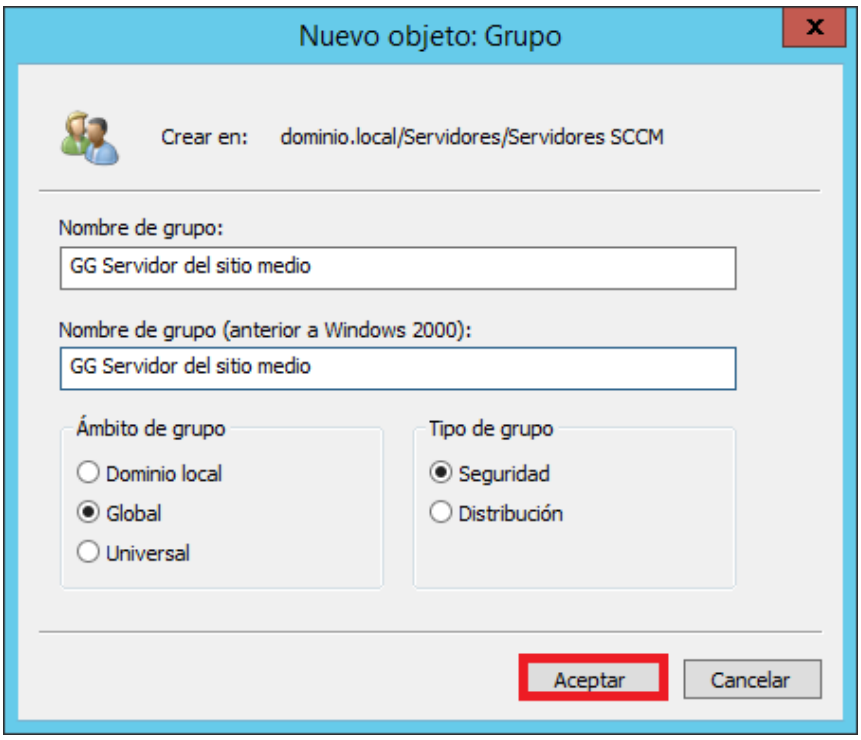
Paso	Descripción
58.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
59.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
60.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.

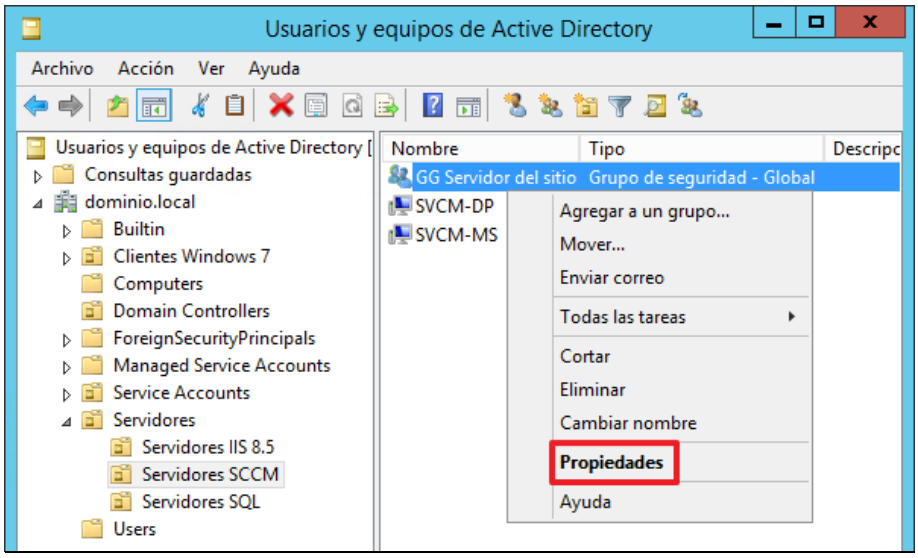
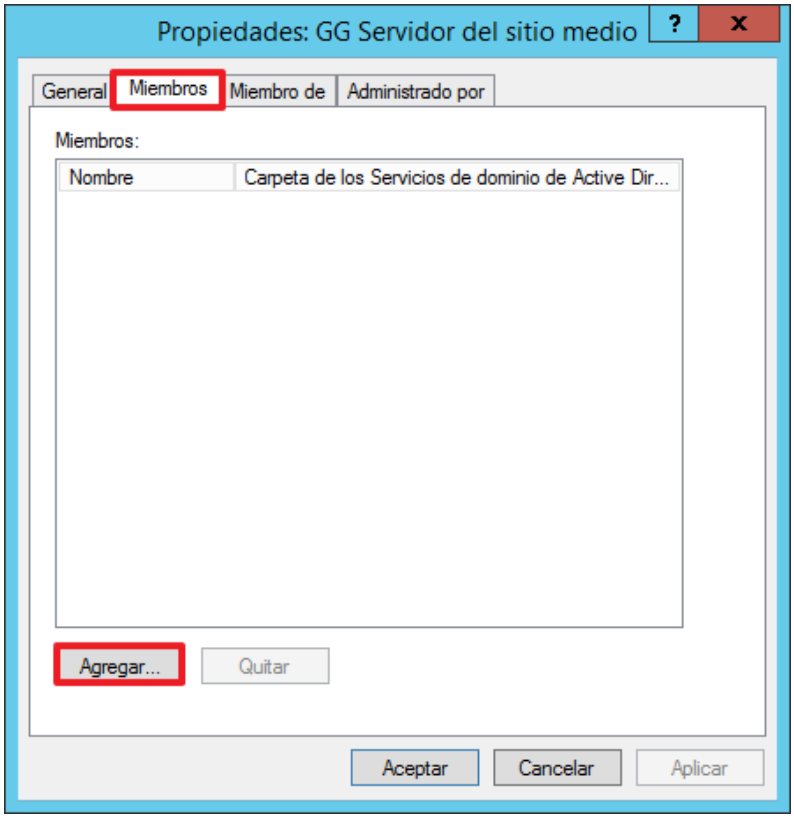
Paso	Descripción
61.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
62.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

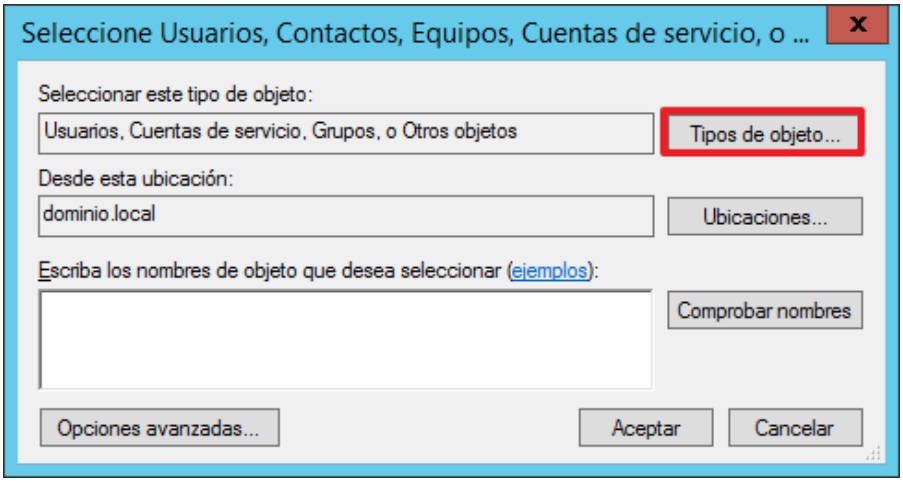
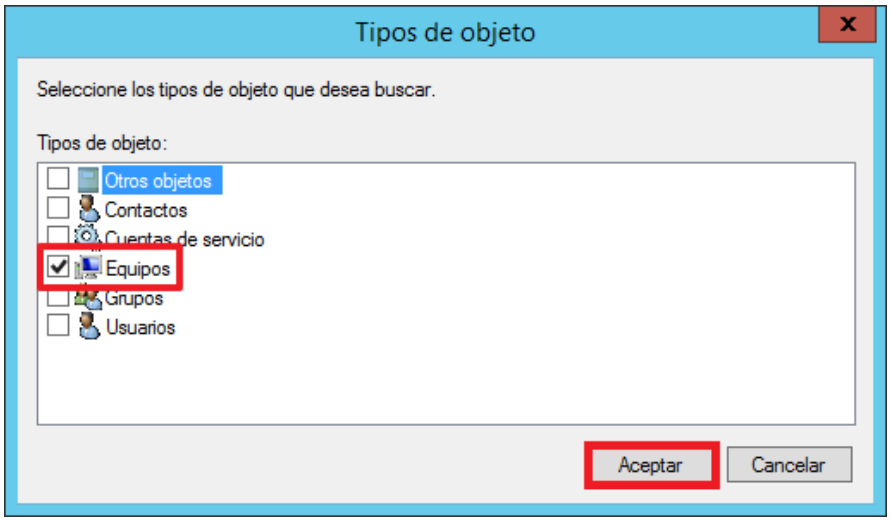
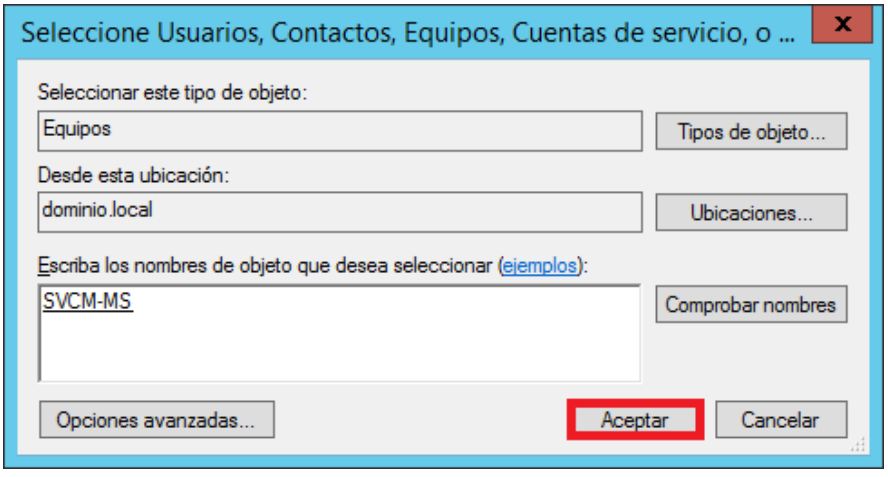
Paso	Descripción
63.	Copie el fichero “CCN-STIC-875 ENS Incremental Servidor del sitio medio.inf” que se encuentra en la ruta “C:\Scripts\Nivel Medio” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
64.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

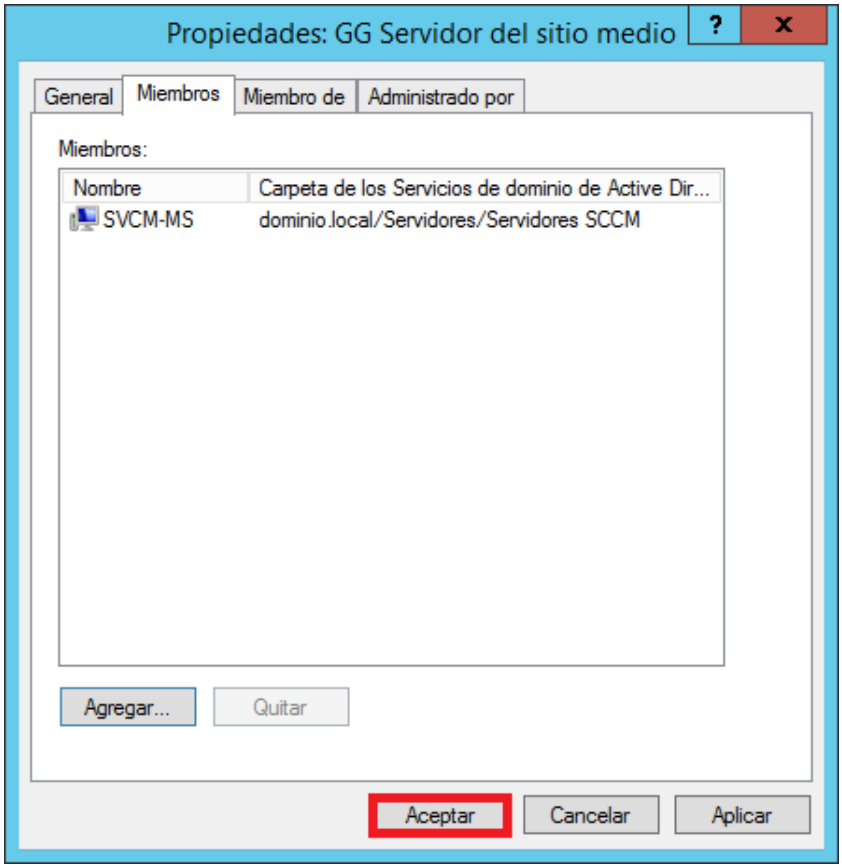
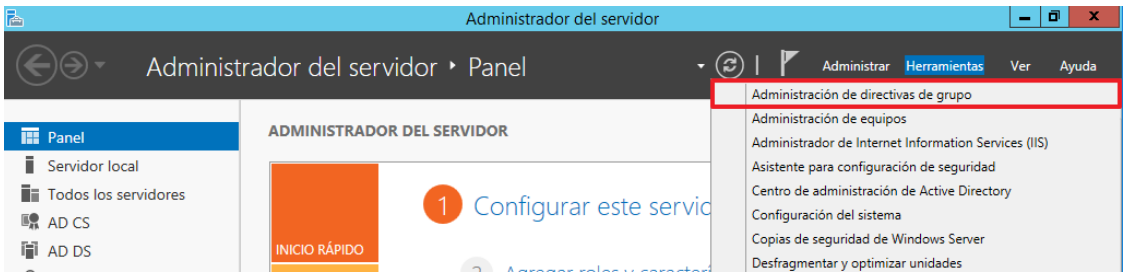
Paso	Descripción
65.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
66.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y marque en “Aceptar”. 

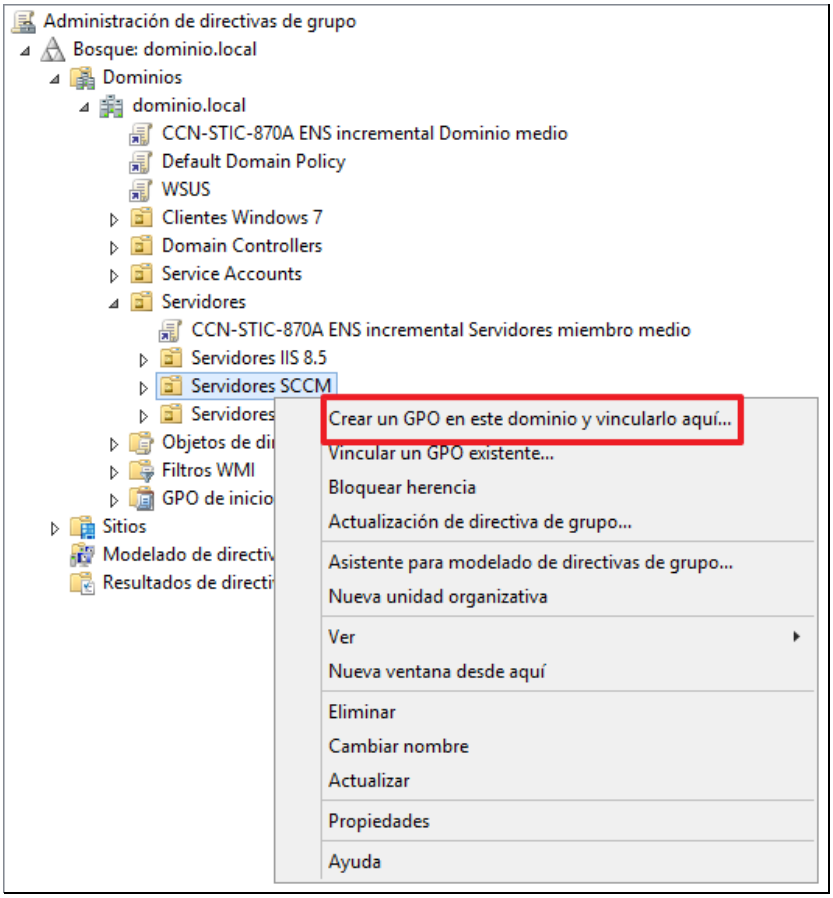
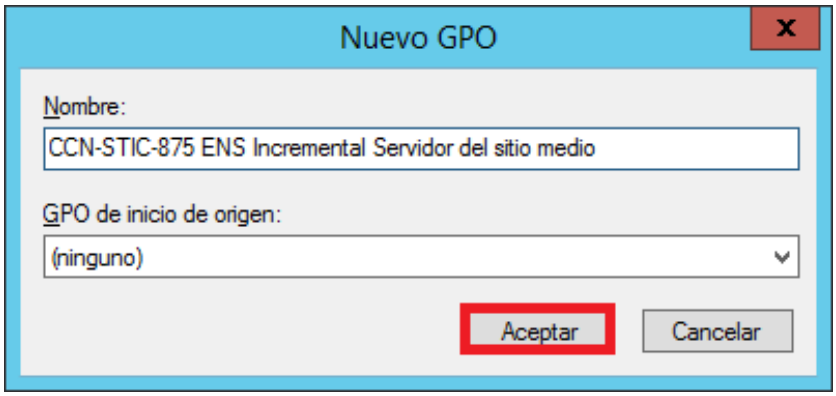
Paso	Descripción
67.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
68.	Seleccione la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

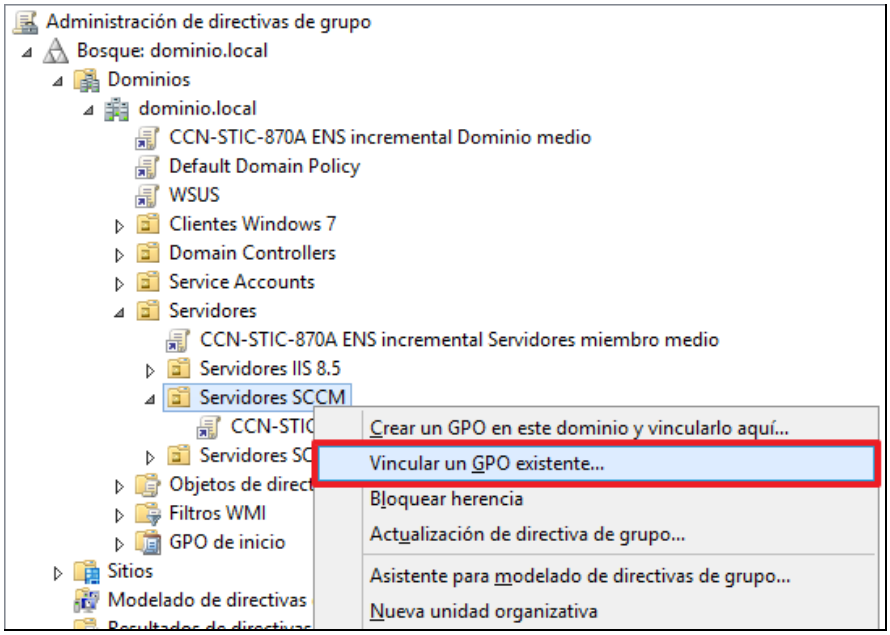
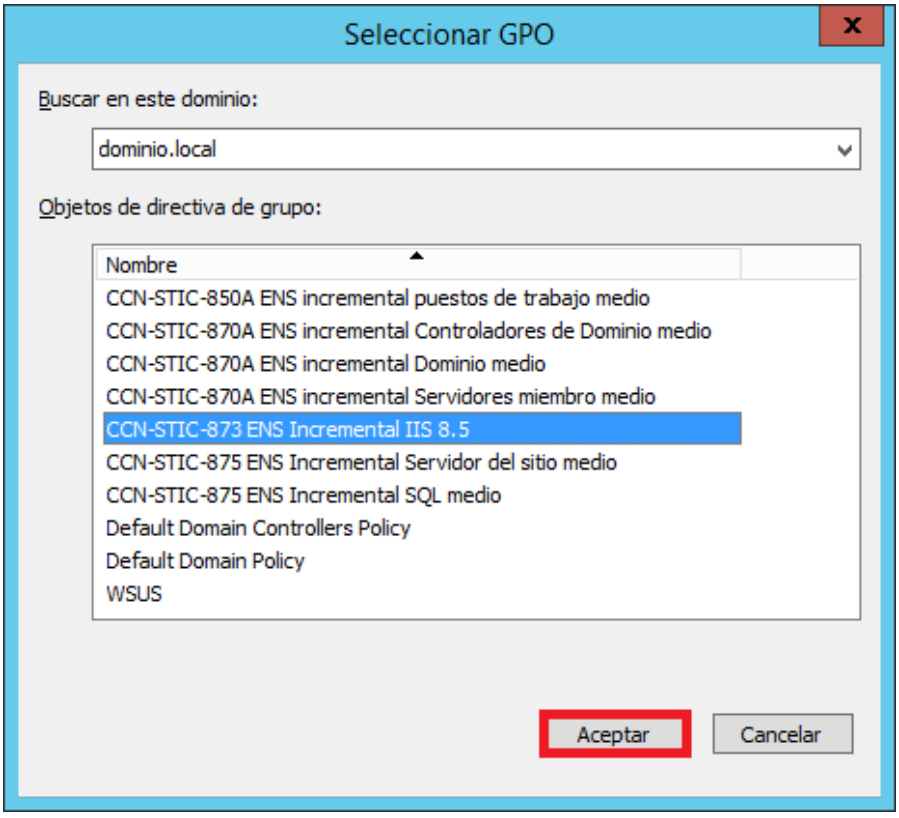
Paso	Descripción
69.	En el siguiente paso, seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
70.	Escriba el nombre “GG Servidor del sitio medio” y pulse “Aceptar”. 

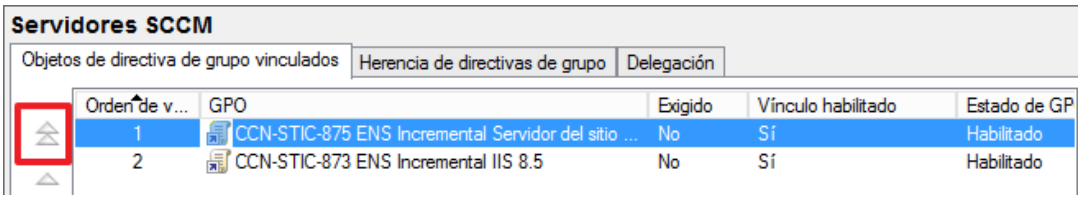
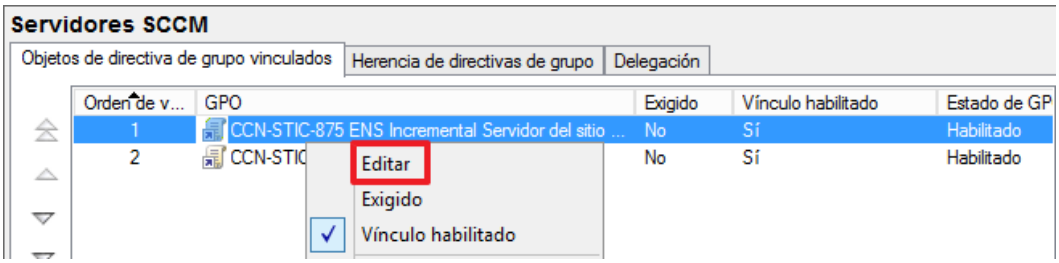
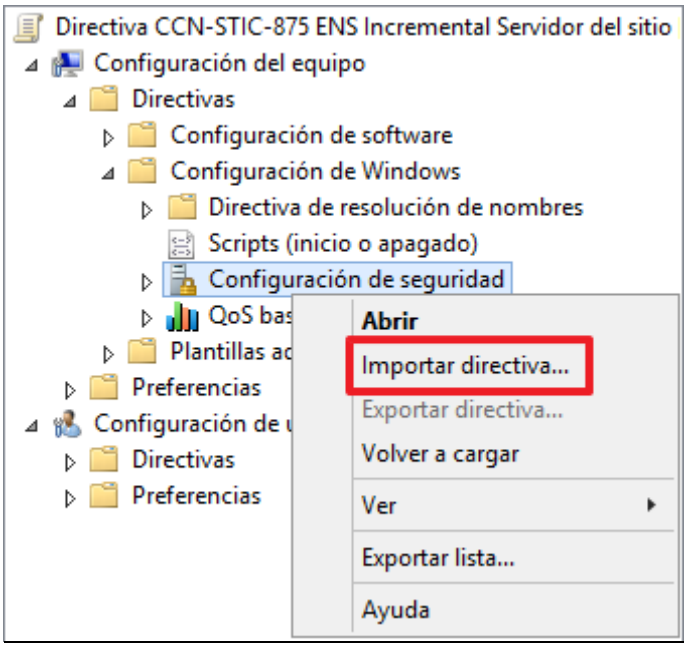
Paso	Descripción
71.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
72.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “servidor de sitio” al grupo. 

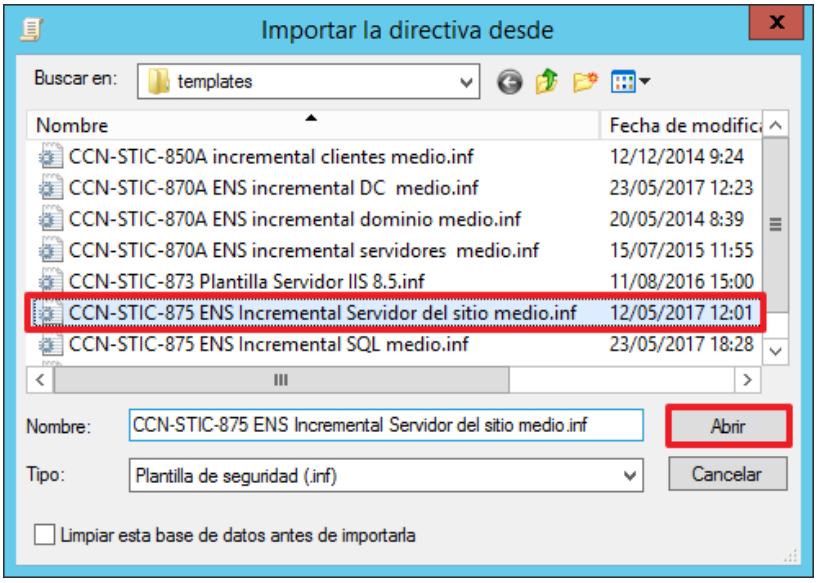
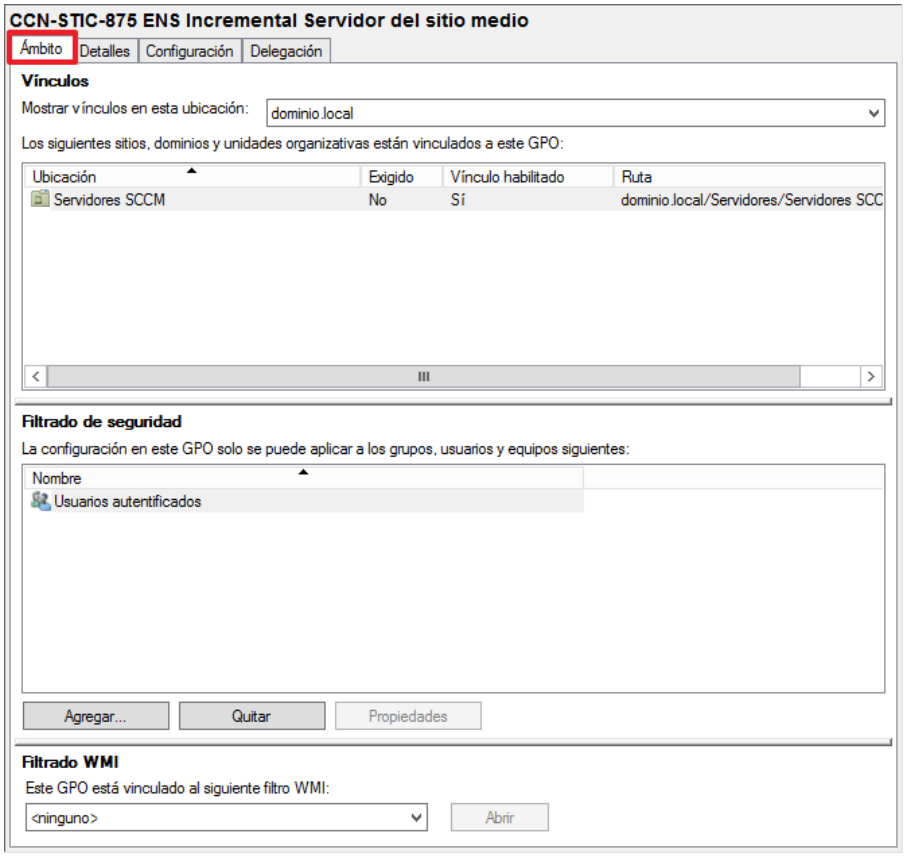
Paso	Descripción
73.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
74.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
75.	Agregue los equipos y pulse sobre “Aceptar”. 

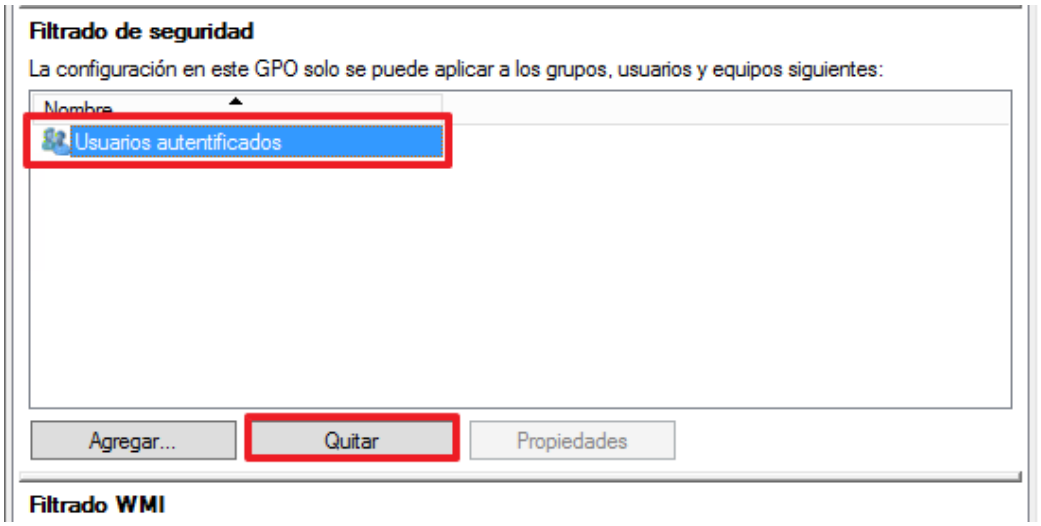
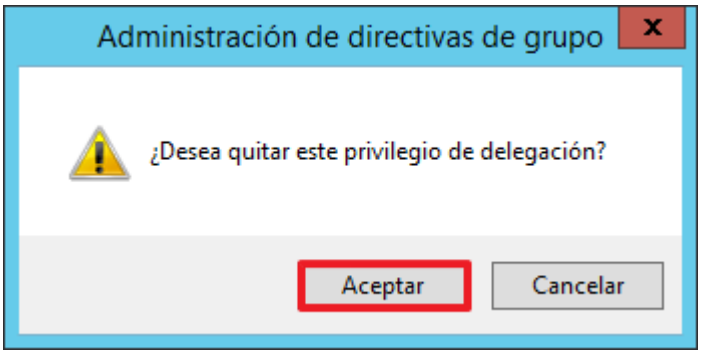
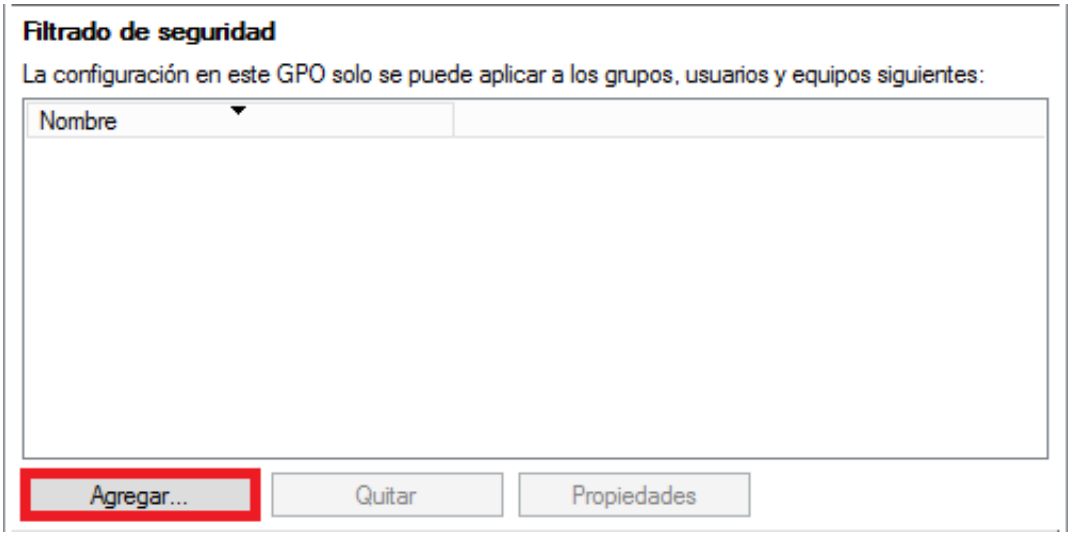
Paso	Descripción
76.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
77.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
78.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

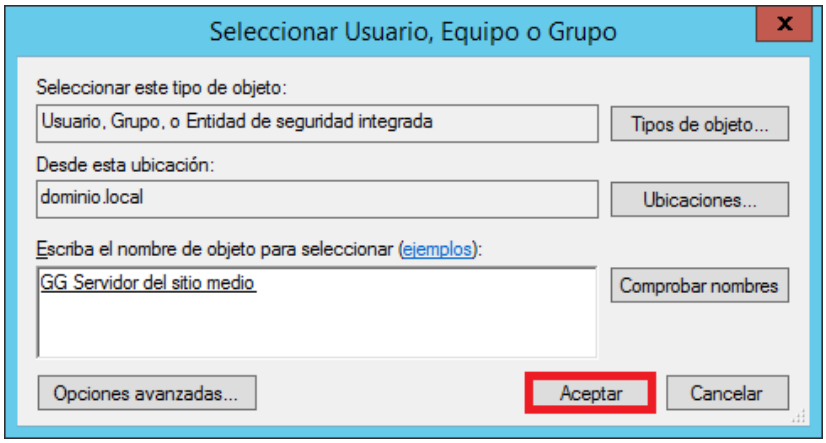
Paso	Descripción
79.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
80.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Servidor del sitio medio” y haga clic en el botón “Aceptar”. 
81.	Seguidamente, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM.

Paso	Descripción
82.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
83.	A continuación, seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre “Aceptar”. 

Paso	Descripción
84.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva “CCN-STIC-875 ENS Incremental Servidor del sitio medio” aparezca en primer lugar. Para ello seleccione, dentro de la unidad organizativa “Servidores SCCM”, la directiva “CCN-STIC-875 ENS Incremental Servidor del sitio medio” y a continuación, haga clic sobre la fecha doble hacia arriba para que se sitúe con el número 1 de orden vínculos, tal y como se muestra en la imagen. 
85.	Edite la GPO: “CCN-STIC-875 ENS Incremental Servidores del sitio medio” creada anteriormente haciendo clic con el botón derecho y seleccionando la opción “Editar” del menú contextual. 
86.	Expanda el nodo “**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**” y haga clic con el botón derecho sobre “Configuración de seguridad” y seleccione en el menú contextual la opción “Importar directiva…”. 

Paso	Descripción
87.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Servidor del sitio medio.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
88.	Cierre el “editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
89.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

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

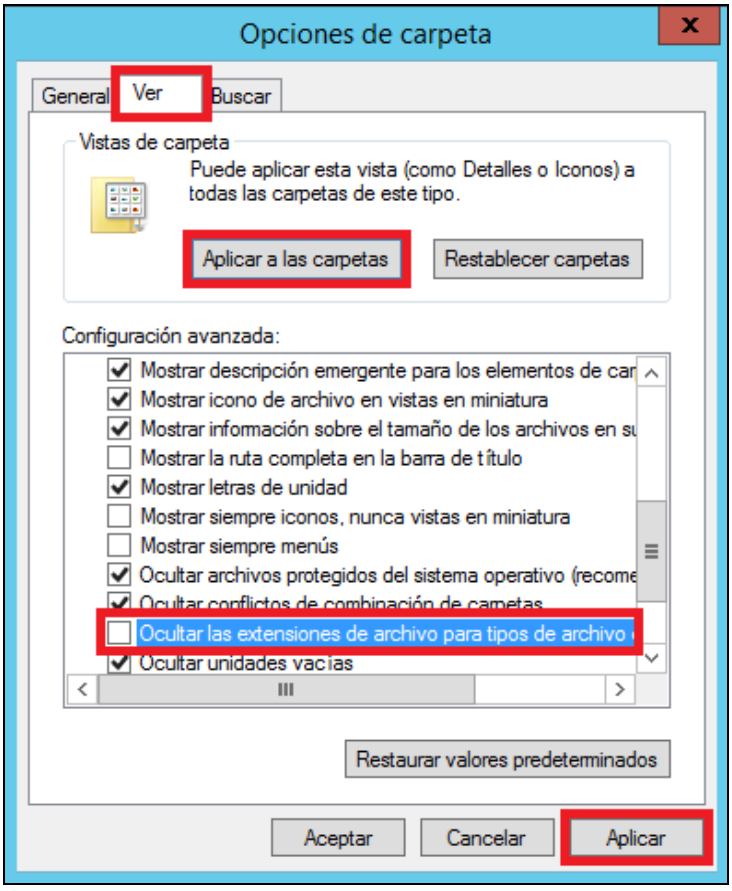
Paso	Descripción
93.	Introduzca como nombre “GG Servidor del sitio medio”. A continuación, sobre el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
94.	Cierre el “Editor de administración de directivas de grupo”.

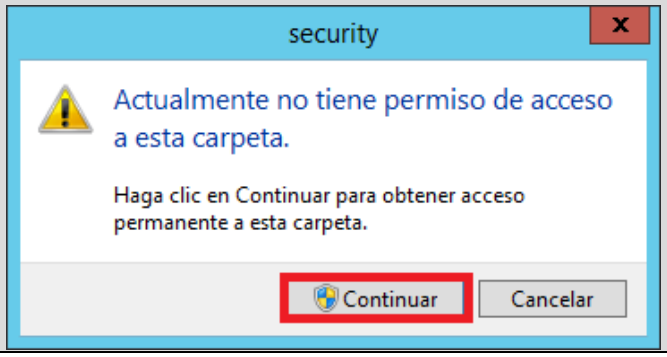
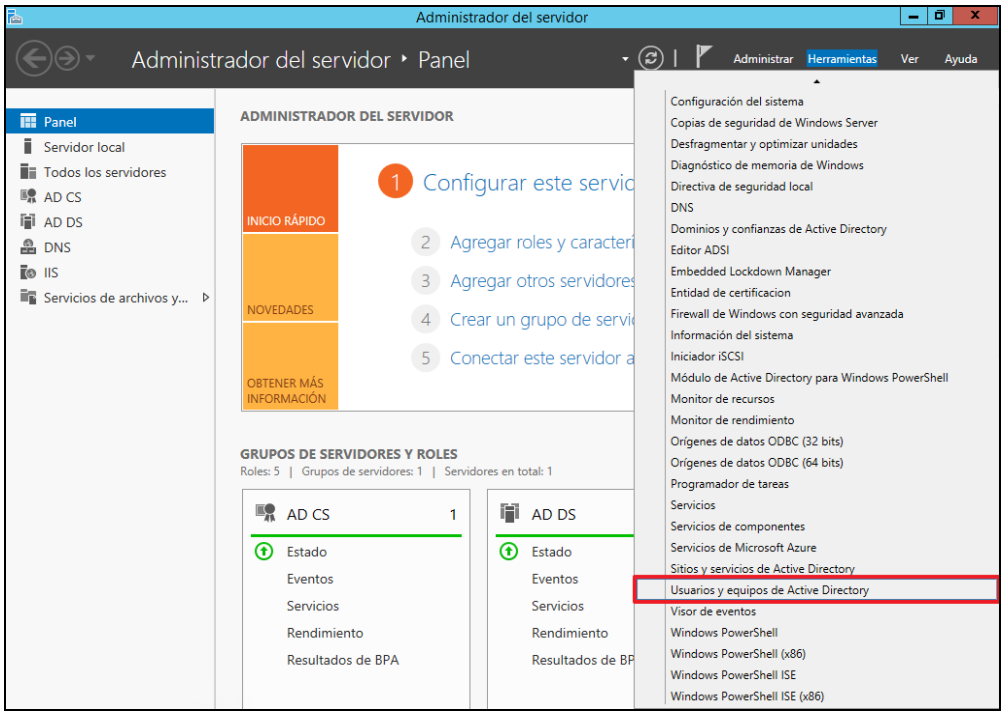
3. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE ADMINISTRACIÓN

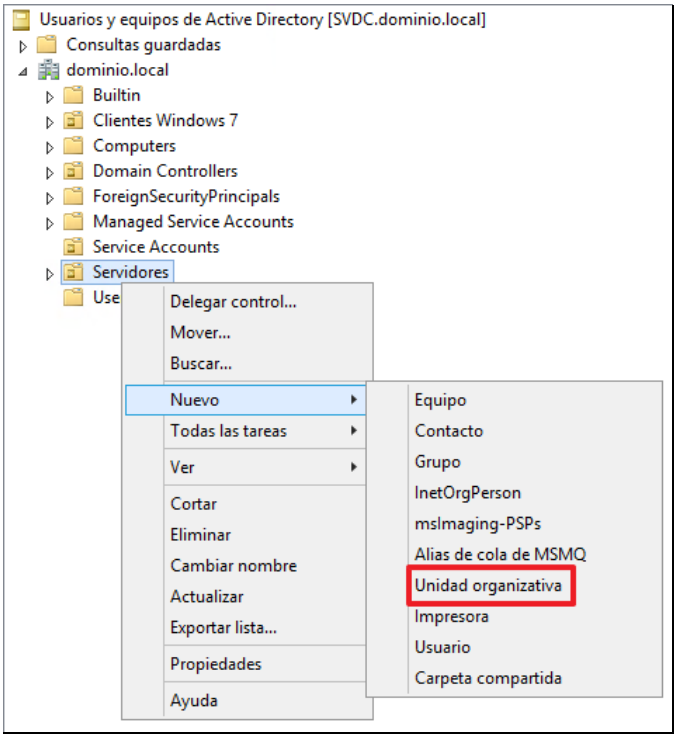
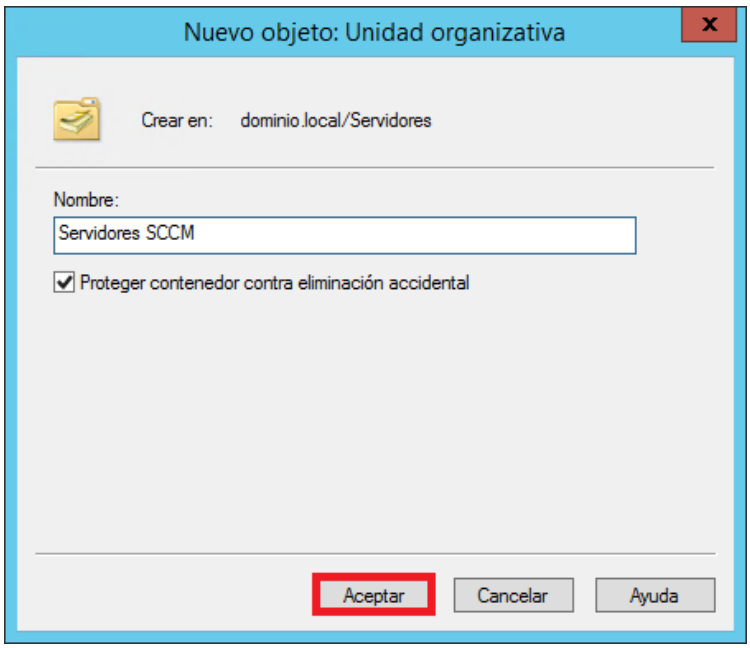
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de administración implementado en el equipo.

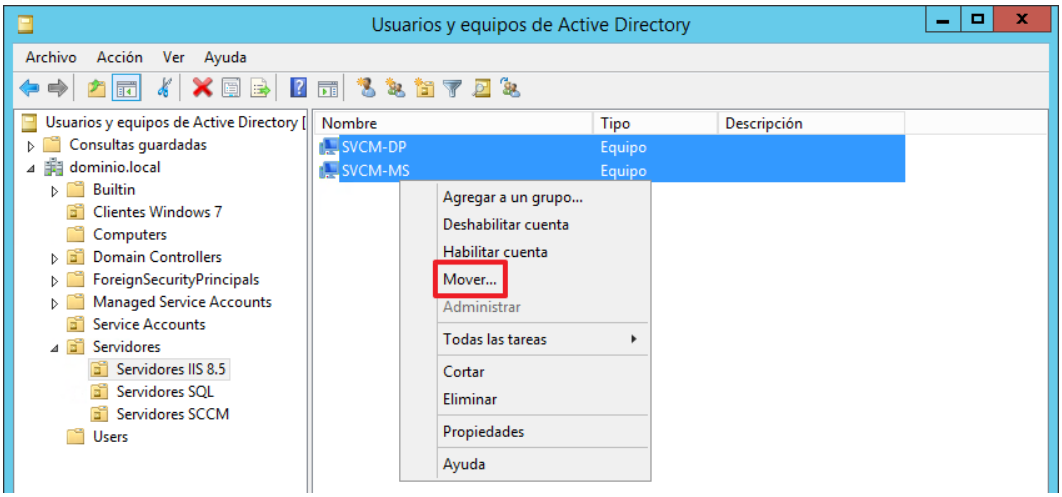
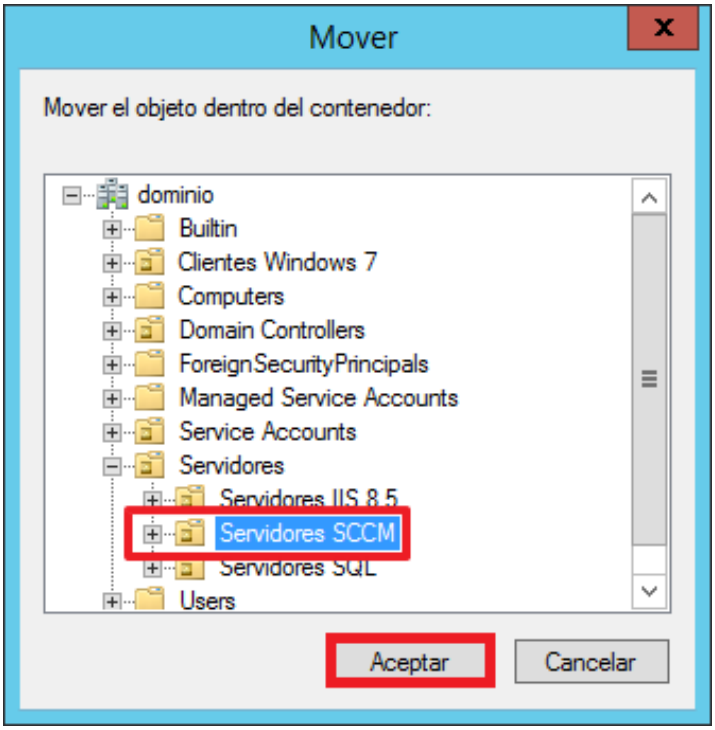
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

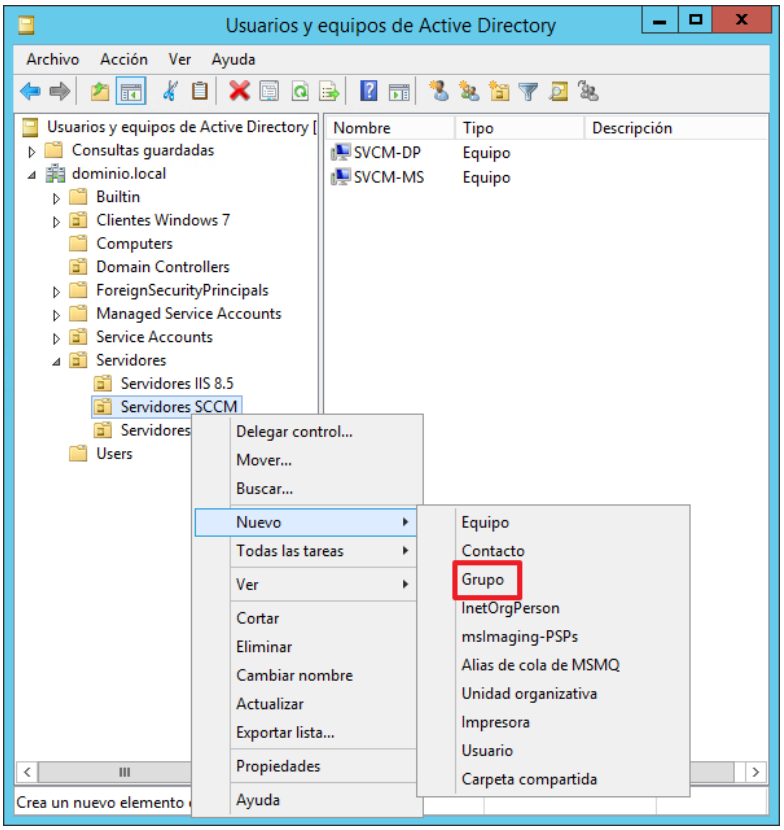
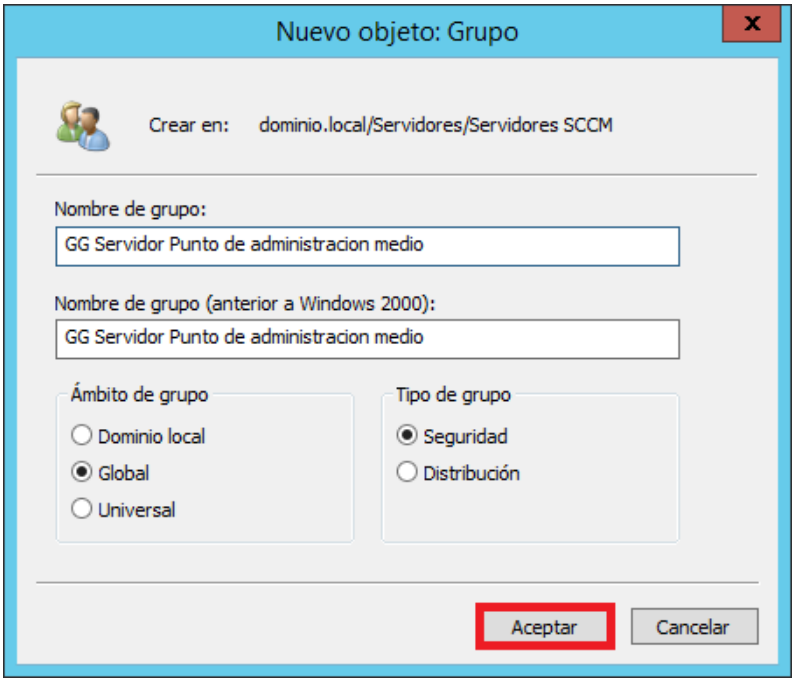
Paso	Descripción
95.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
96.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

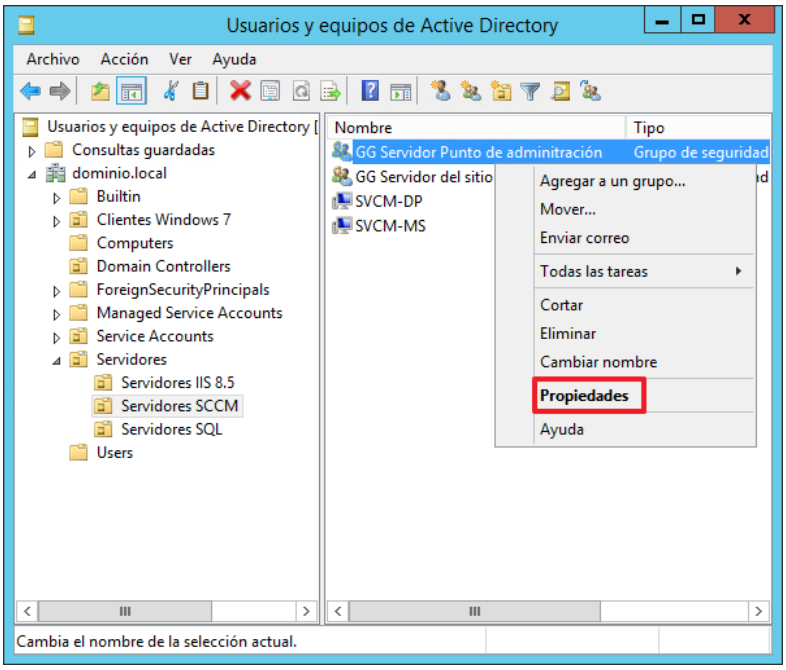
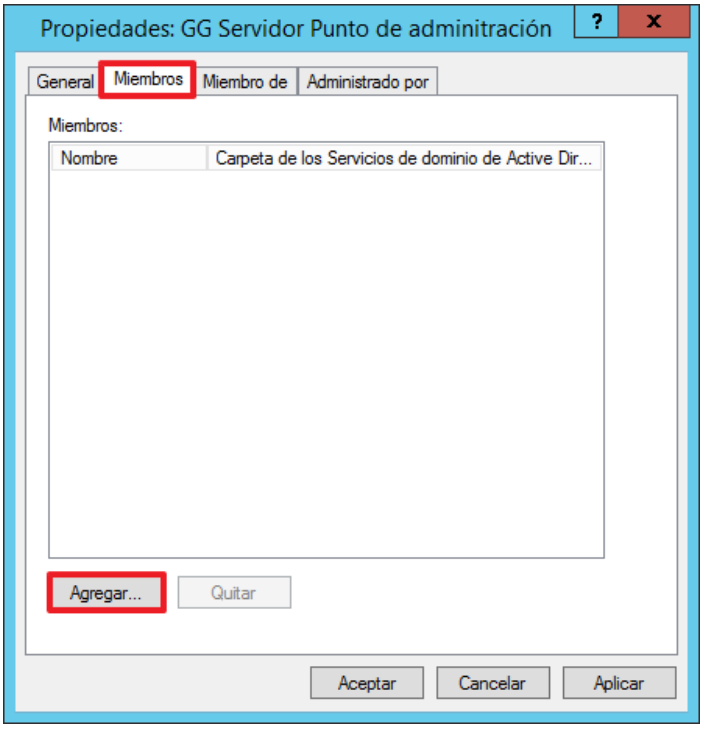
Paso	Descripción
97.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
98.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
99.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

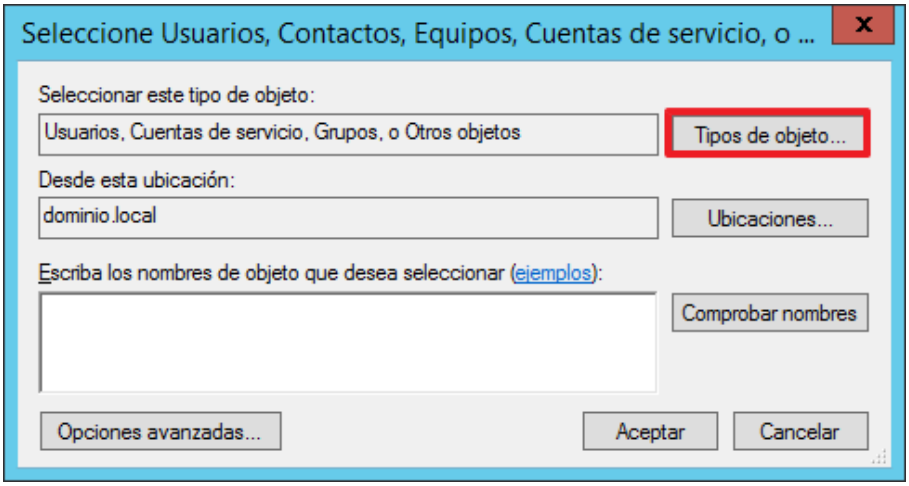
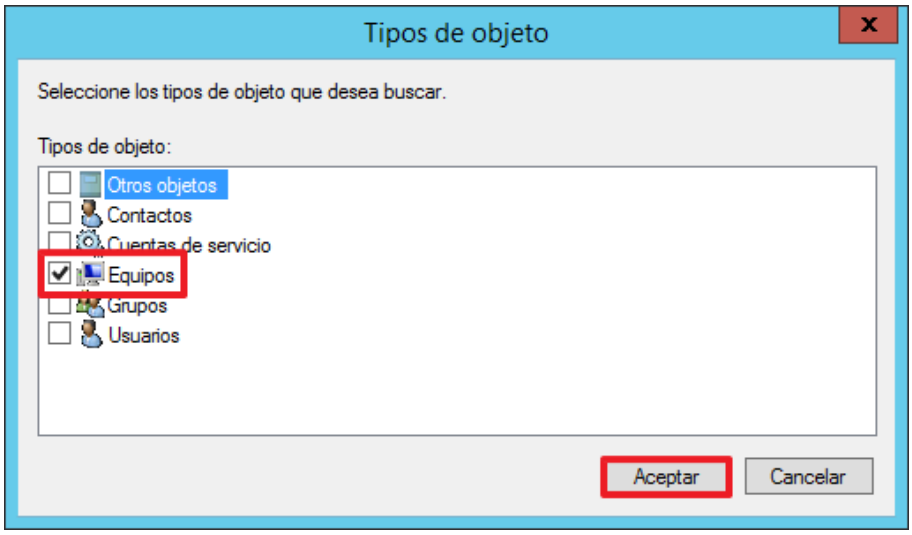
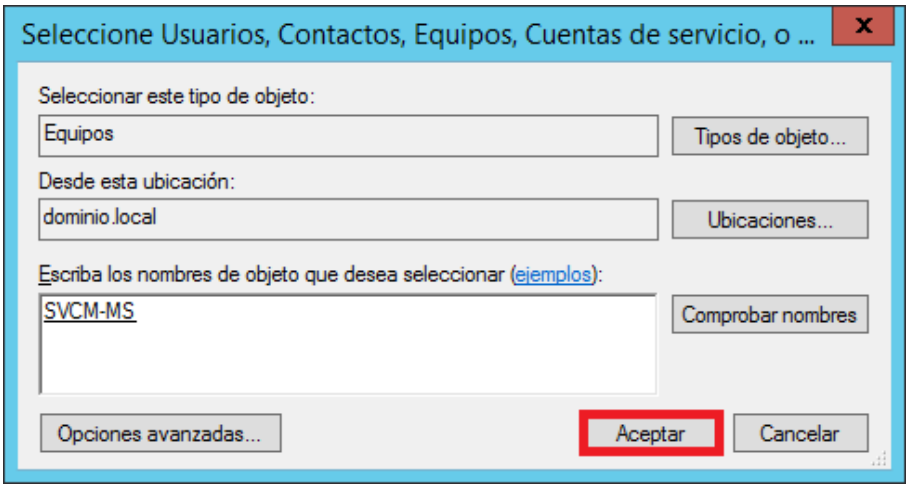
Paso	Descripción
100.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de administración medio.inf” que se encuentra en la ruta “C:\Scripts\Nivel Medio” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
101.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .
102.	En el siguiente proceso, se va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 107. En caso contrario continúe con el paso a paso.

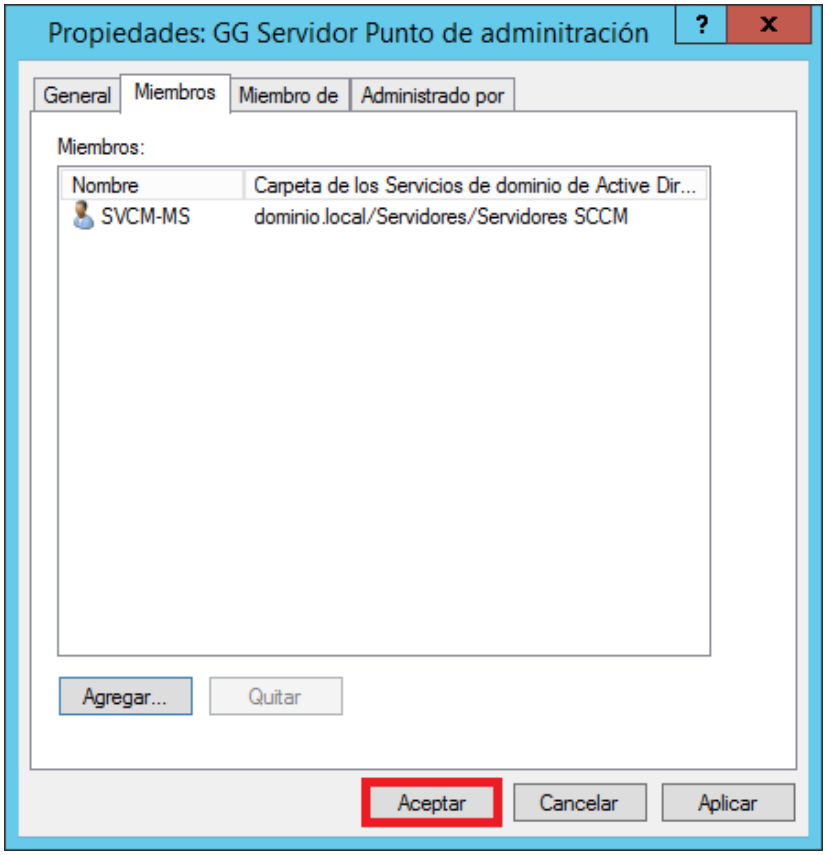
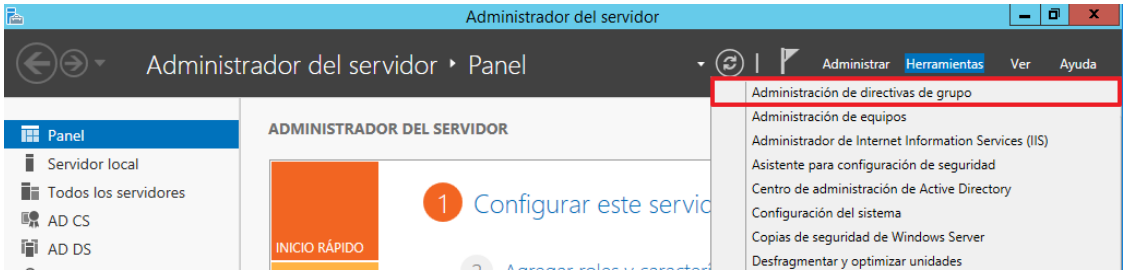
Paso	Descripción
103.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
104.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar”. 

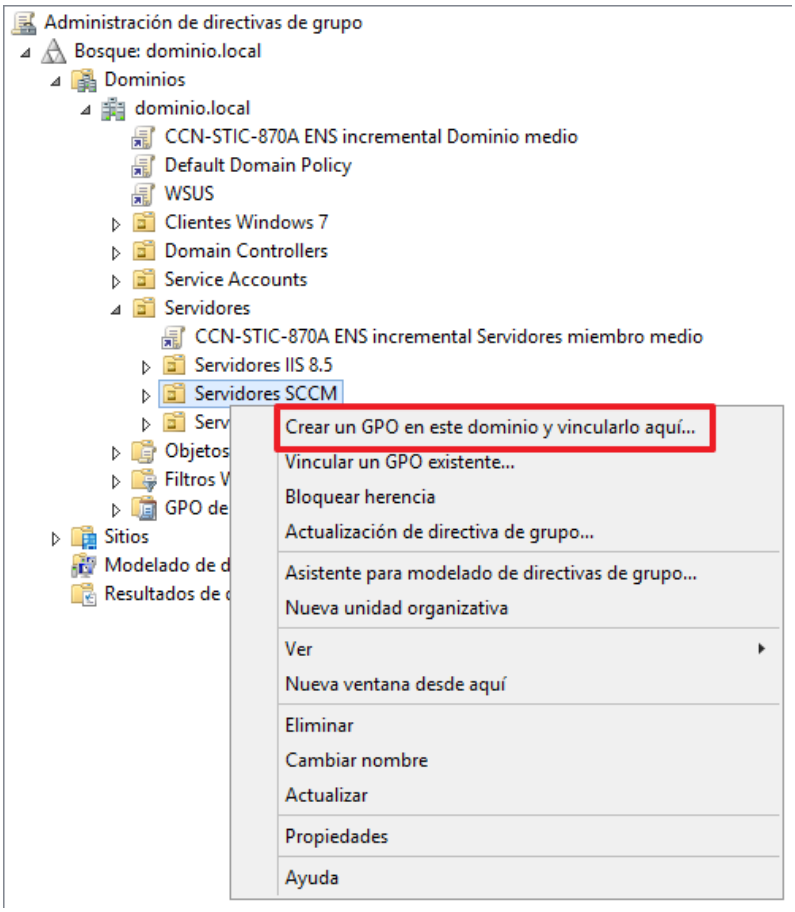
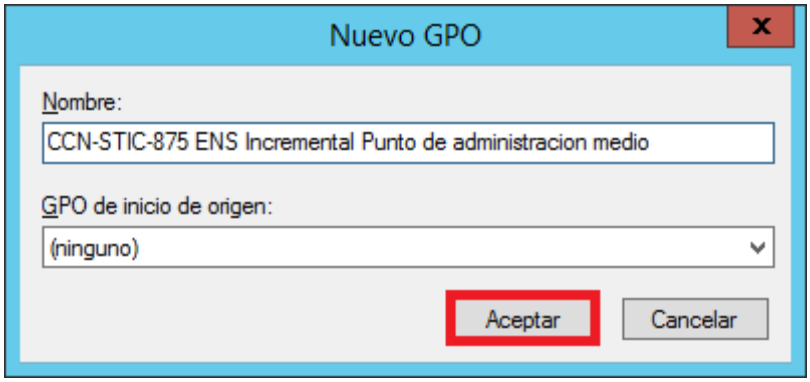
Paso	Descripción
105.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
106.	Seleccione la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

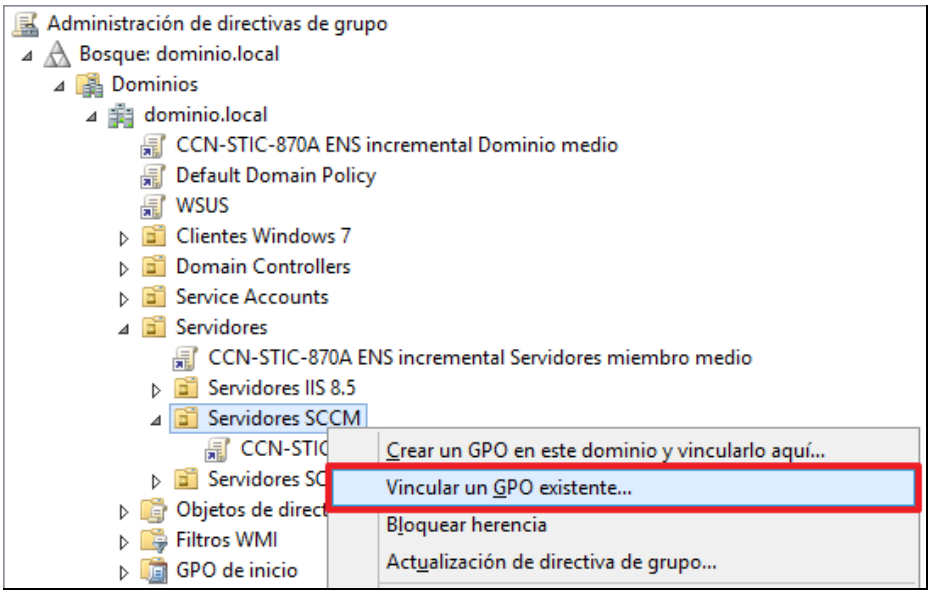
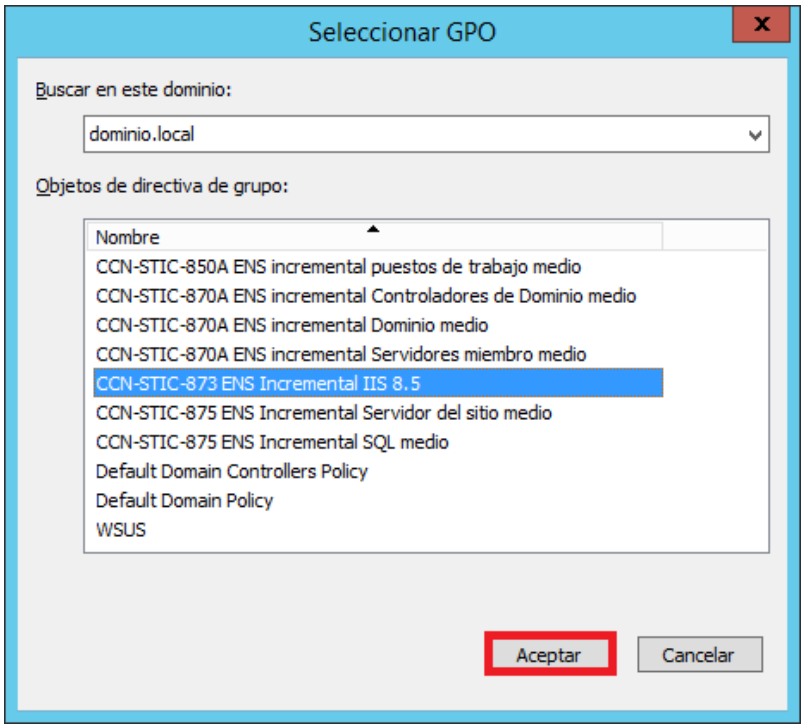
Paso	Descripción
107.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
108.	Escriba el nombre “GG Punto de administración medio” y pulse “Aceptar”. 

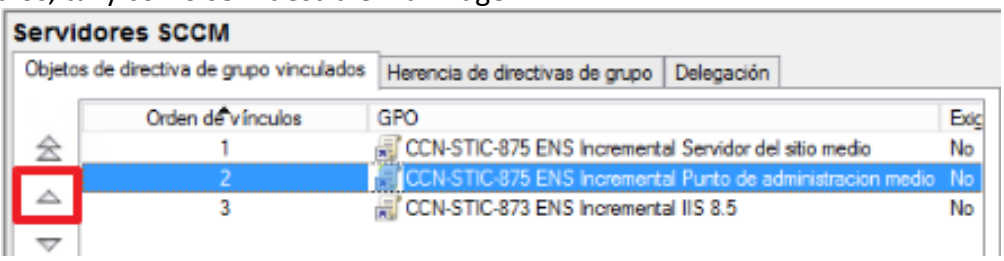
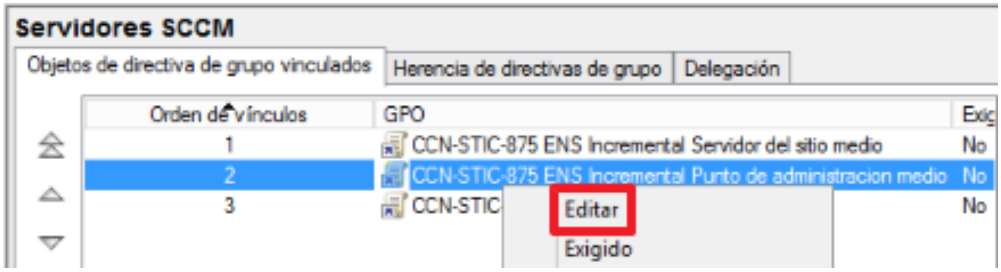
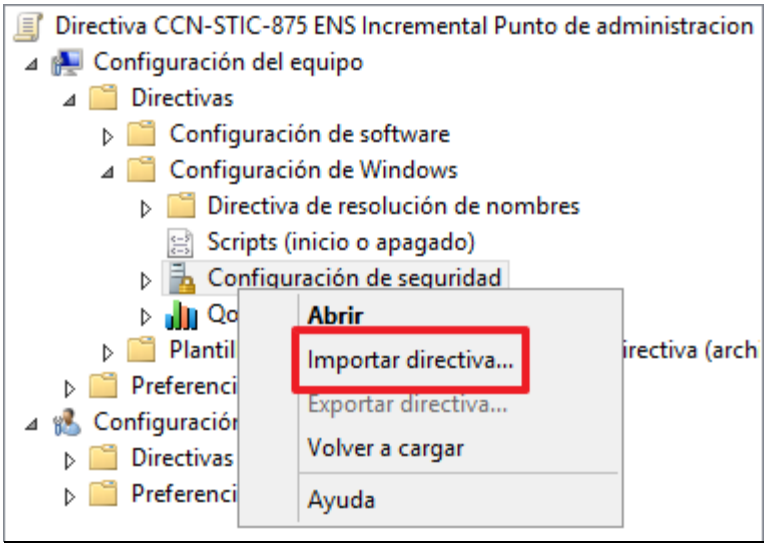
Paso	Descripción
109.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
110.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de administración” al grupo. 

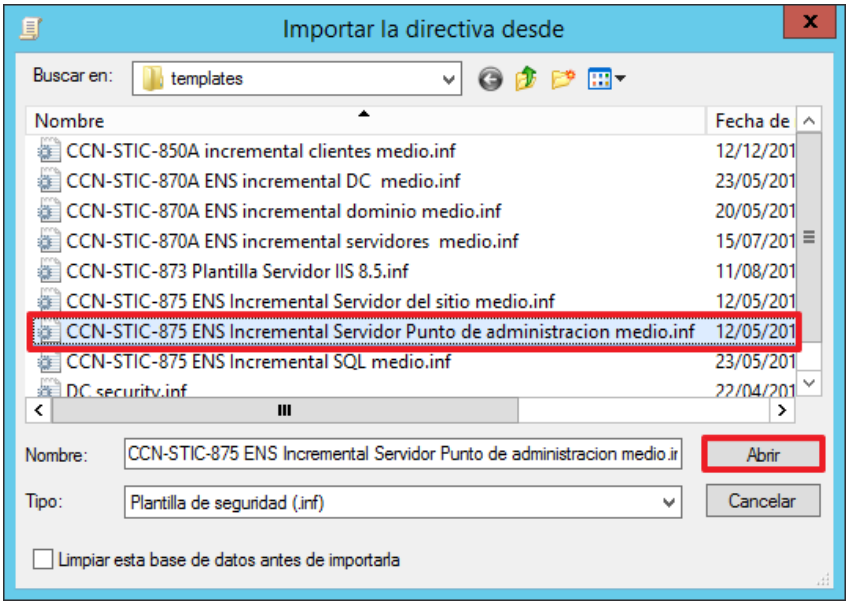
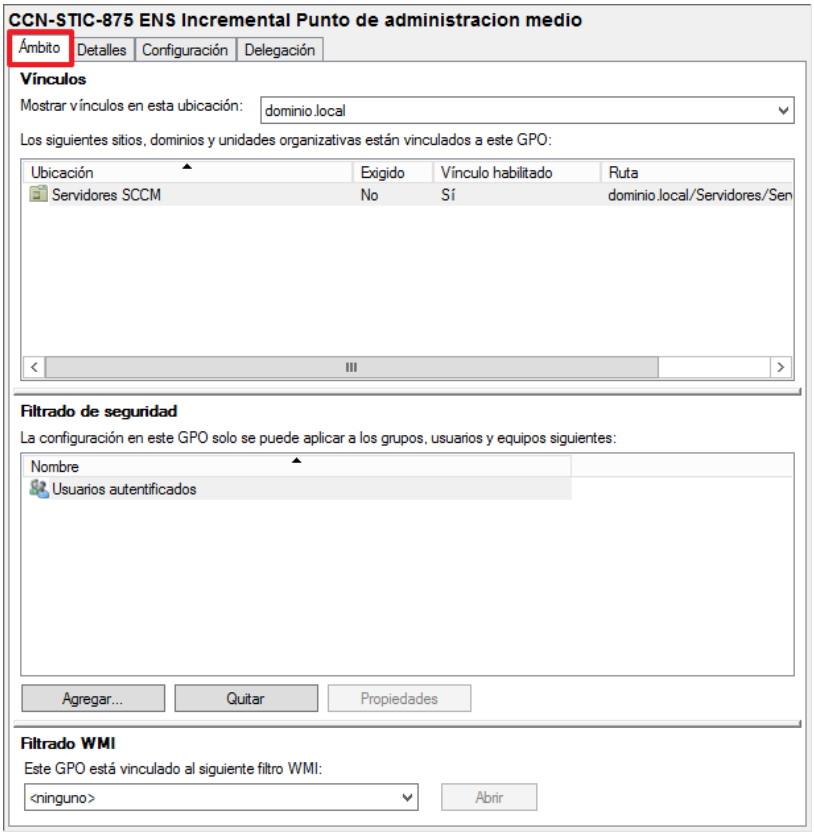
Paso	Descripción
111.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
112.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
113.	Agregue los equipos y pulse sobre “Aceptar”. 

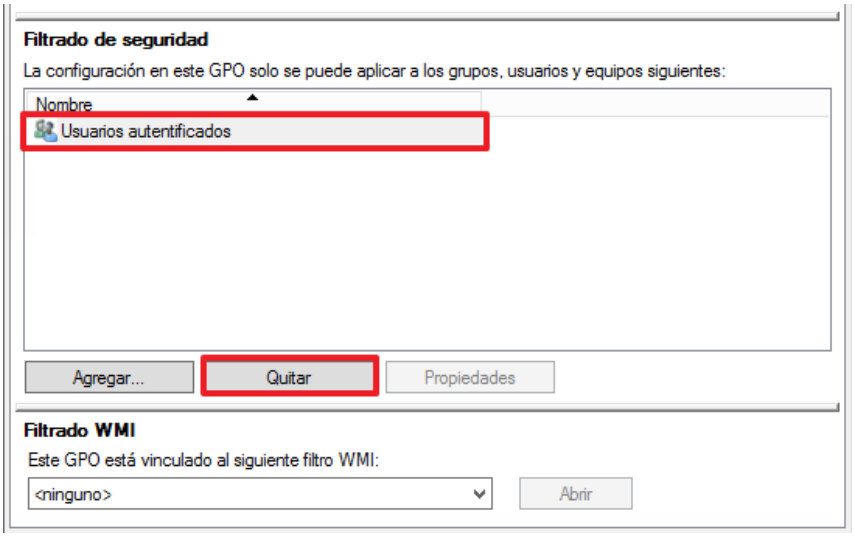
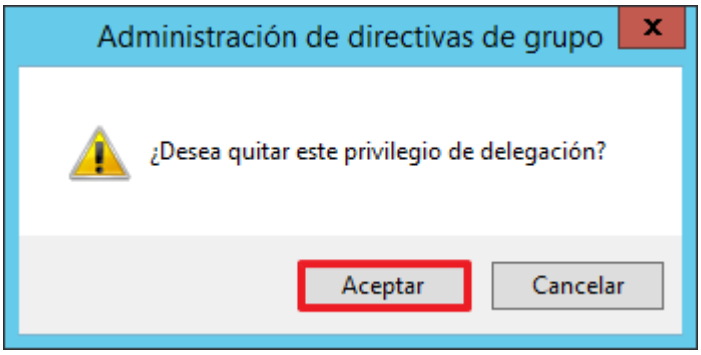
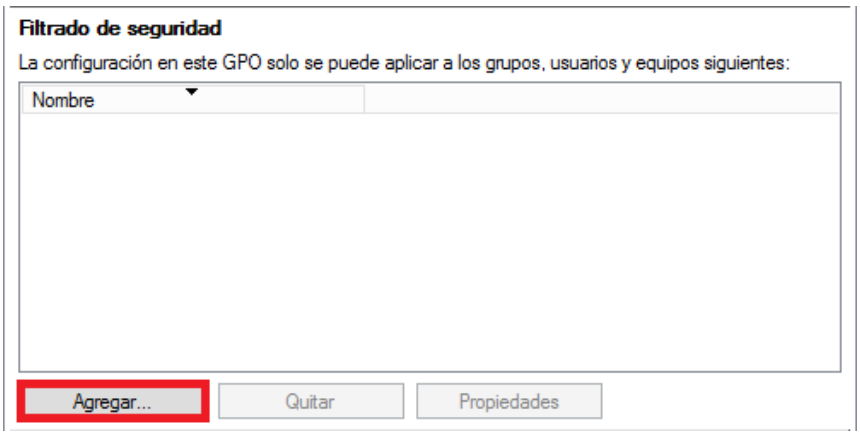
Paso	Descripción
114.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
115.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
116.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .

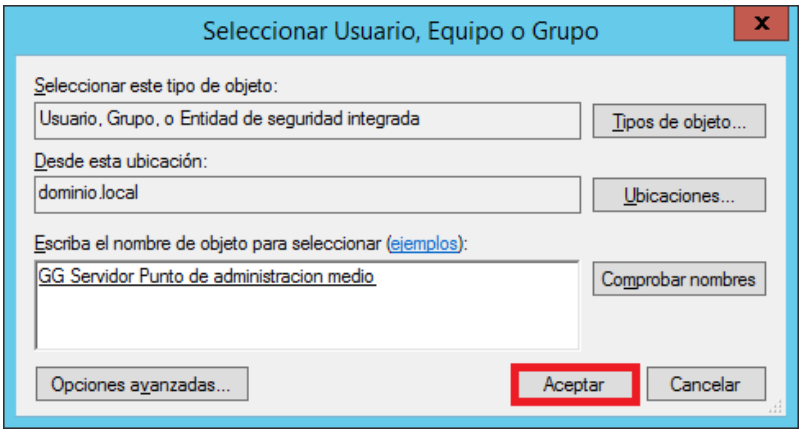
Paso	Descripción
117.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
118.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de administración medio” y haga clic en el botón “Aceptar”. 
119.	En los siguientes pasos, se va a asociar la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” en la unidad organizativa “Servidores SCCM”, en caso de que ya haya vinculado la directiva en algún paso anterior, continúe con el paso 124 , en caso contrario continúe con el siguiente paso.

Paso	Descripción
120.	A continuación, se vinculará la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM.
121.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
122.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
123.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva “CCN-STIC-875 ENS Incremental Punto de administración medio” aparezca posicionada por encima de la directiva “CCN-STIC-873 ENS Incremental IIS 8.5”. Para ello seleccione, dentro de la unidad organizativa “Servidores SCCM”, la directiva “CCN-STIC-875 ENS Incremental Punto de administración medio” y a continuación, haga clic sobre la flecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
124.	Edite la GPO: “CCN-STIC-875 ENS Incremental Punto de administración medio” creada anteriormente haciendo clic con el botón derecho y seleccionando la opción “Editar” del menú contextual. 
125.	Expanda el nodo “**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**” y haga clic con el botón derecho sobre “Configuración de seguridad” y seleccione en el menú contextual la opción “Importar directiva…”. 

Paso	Descripción
126.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de administración medio.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
127.	Cierre el "editor de administración de directivas de grupo" una vez que se haya realizado la importación de la configuración de seguridad.
128.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

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

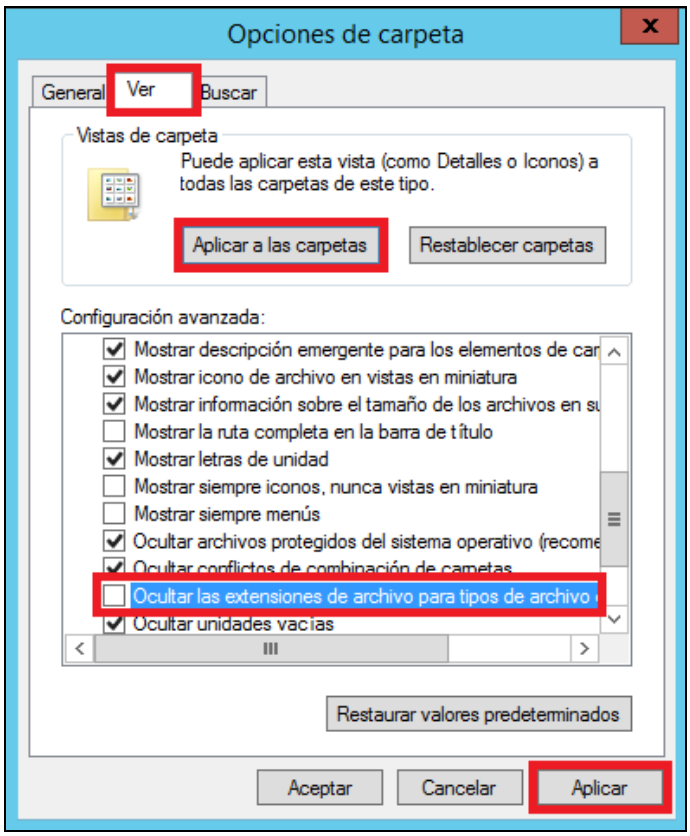
Paso	Descripción
132.	Introduzca como nombre “GG Servidor Punto de administración medio” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
133.	Cierre el “Editor de administración de directivas de grupo”.

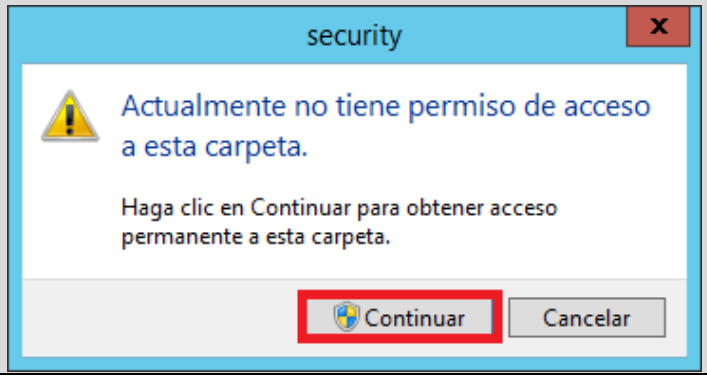
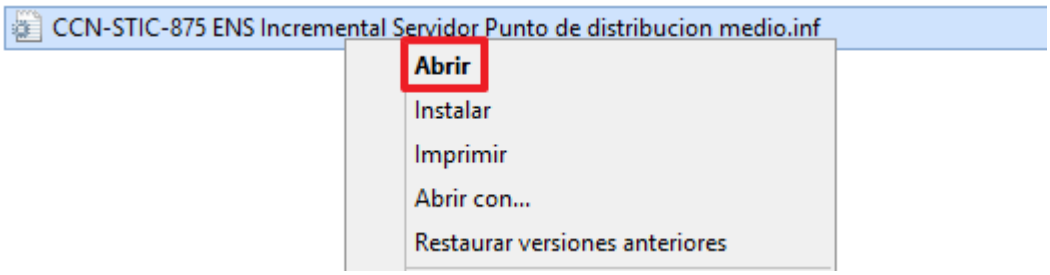
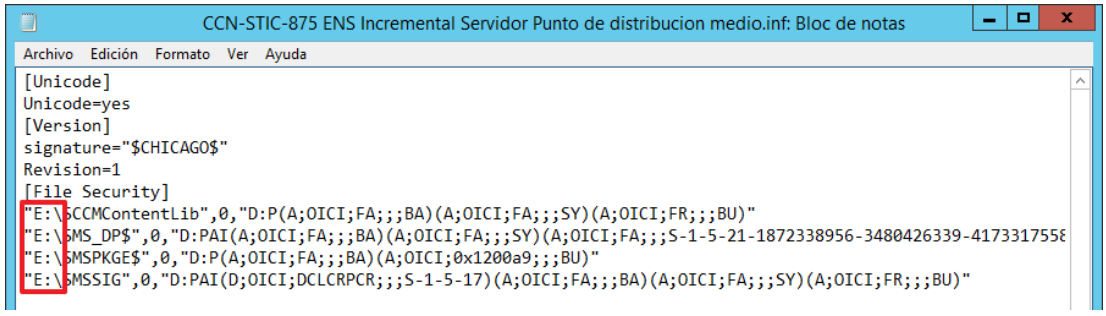
4. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE DISTRIBUCIÓN

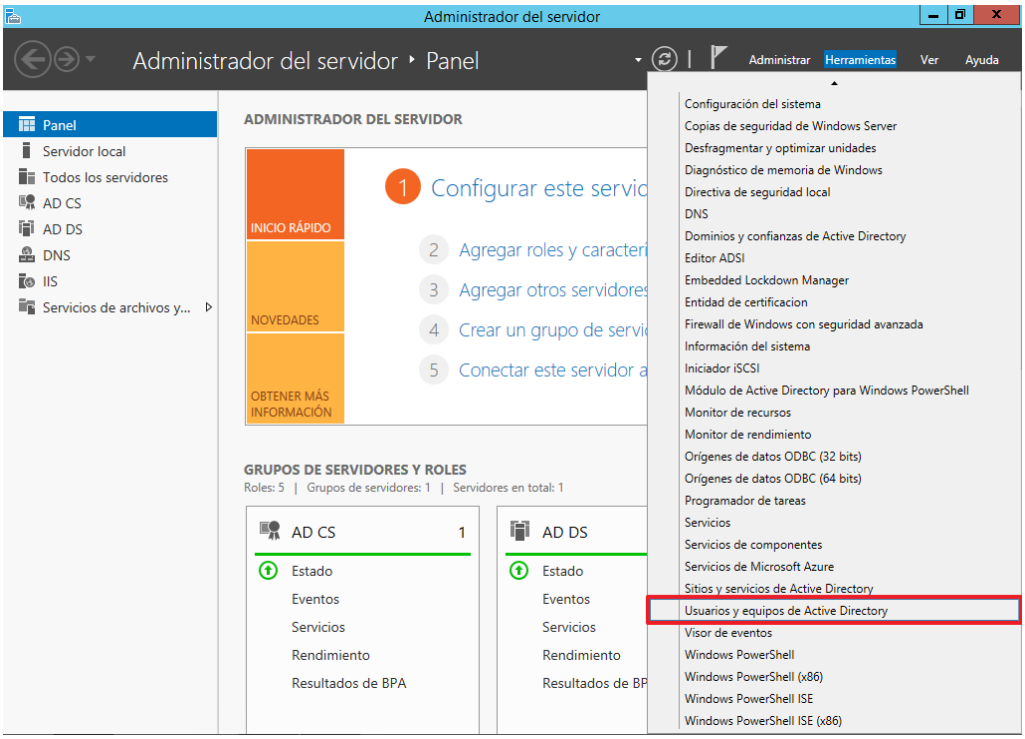
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de distribución implementado en el equipo.

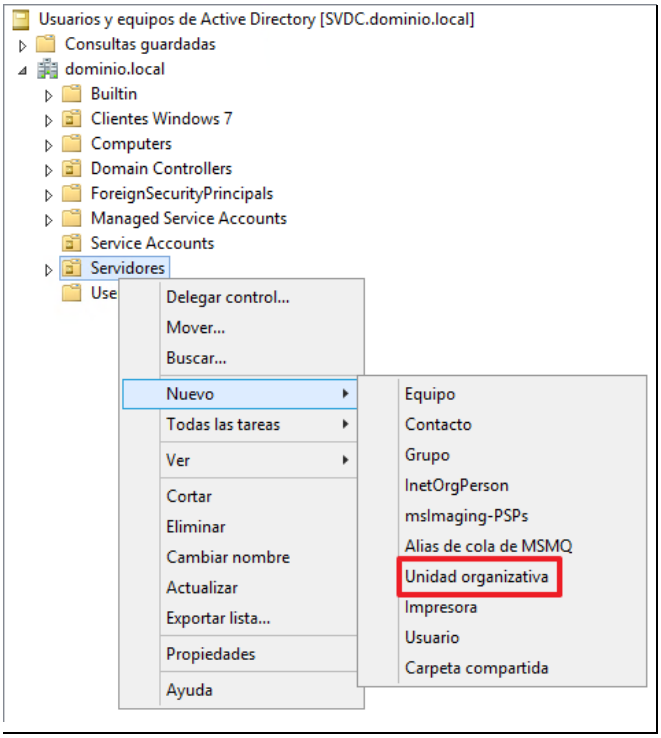
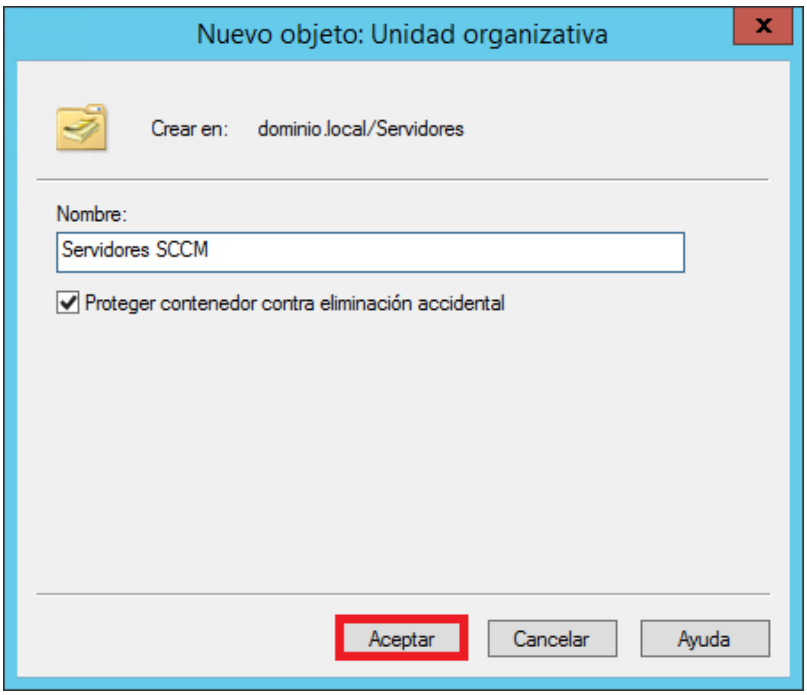
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

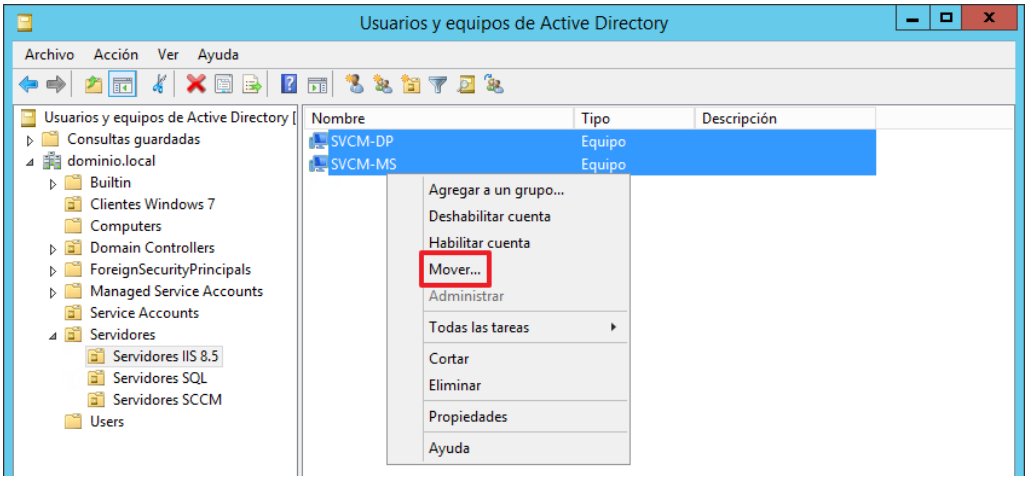
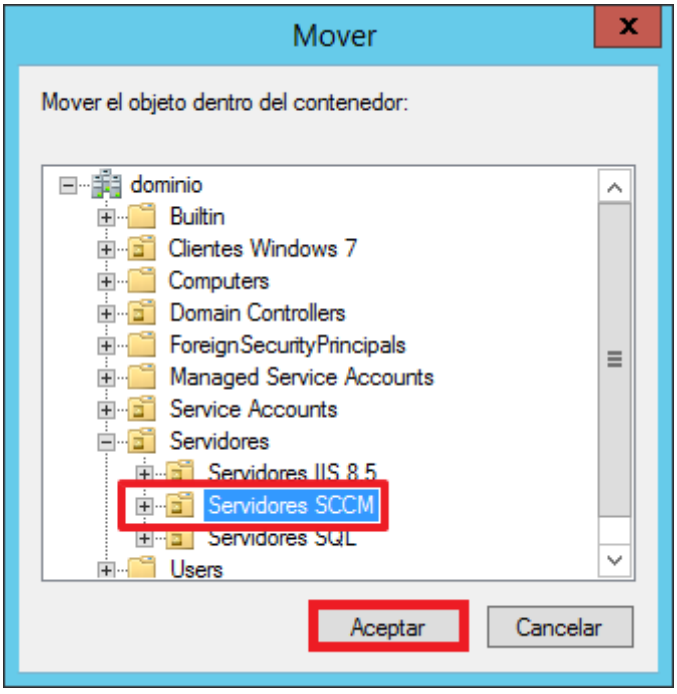
Paso	Descripción
134.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
135.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

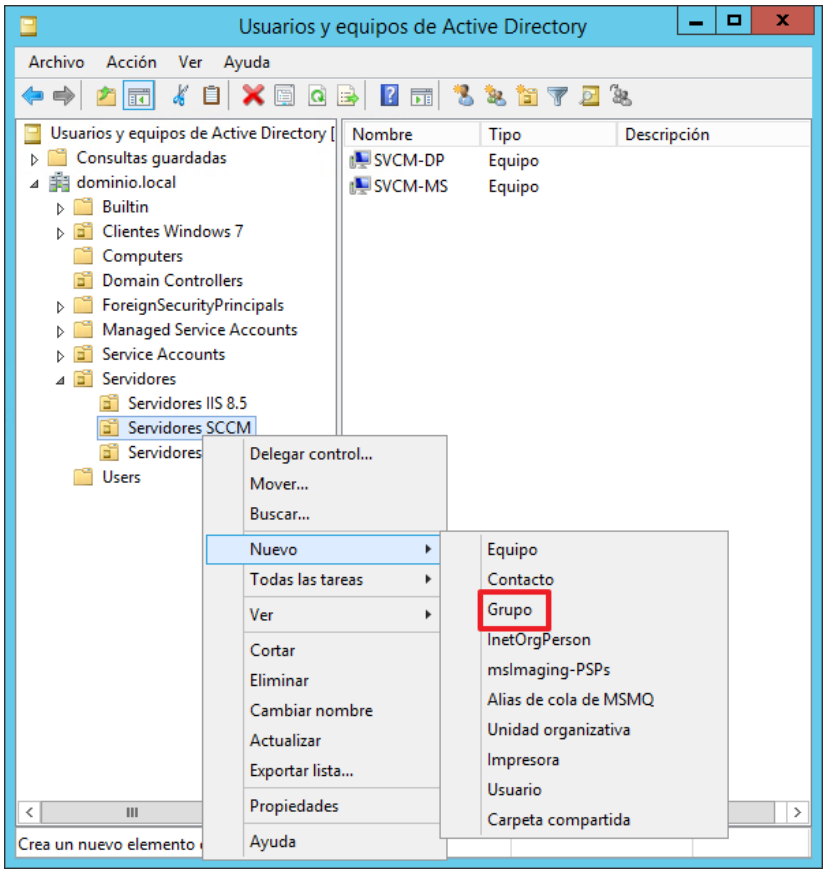
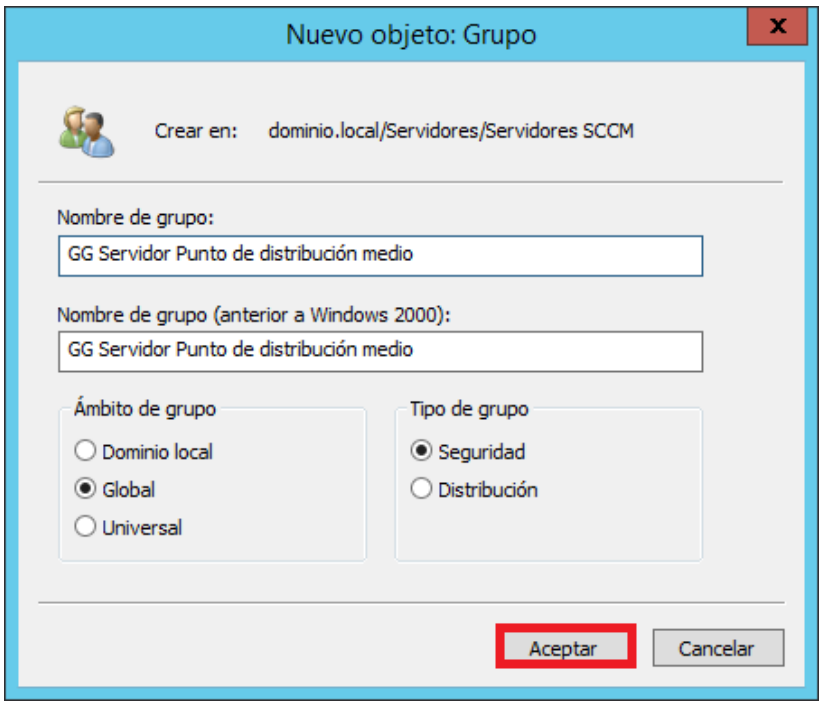
Paso	Descripción
136.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
137.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
138.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

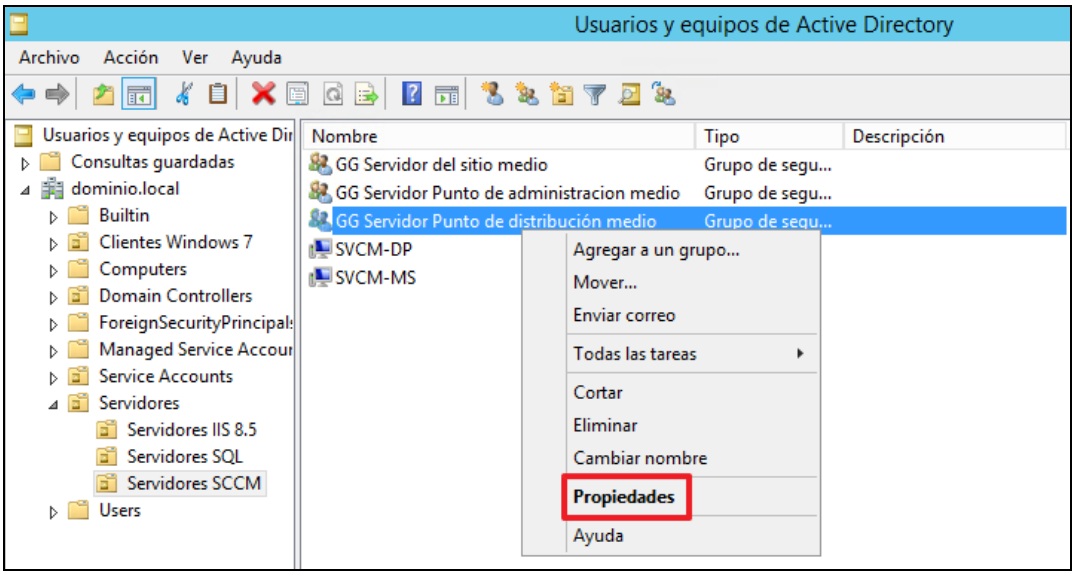
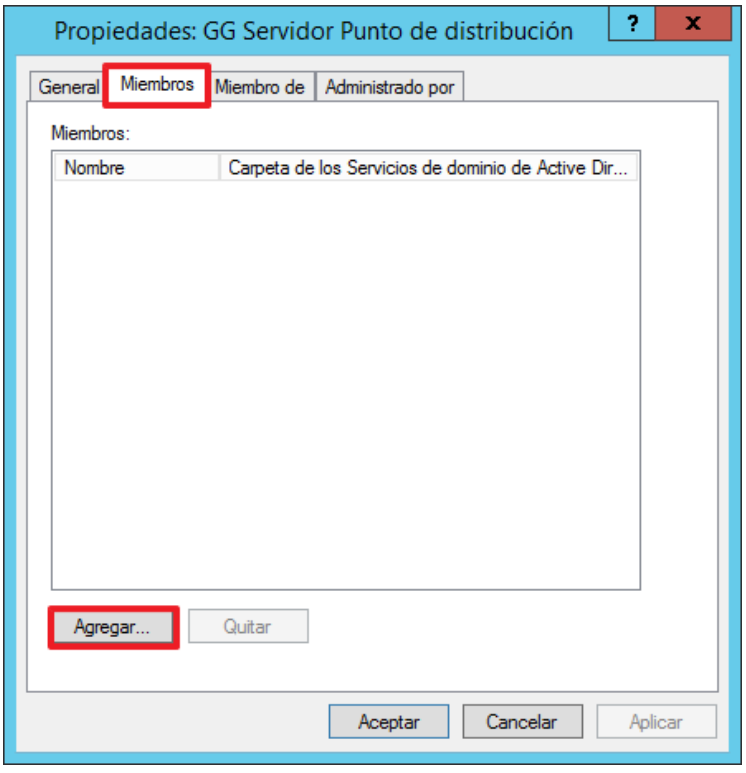
Paso	Descripción
139.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de distribución medio.inf” que se encuentra en la ruta “C:\Scripts\Nivel Medio” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
140.	Pulse con el botón derecho sobre el fichero y seleccione la opción “Abrir” del menú contextual. 
141.	Deberá modificar la ruta del fichero para adaptarlo a su organización, para ello localice la ruta de las carpetas sobre las que desea aplicar seguridad y modifíquela en función de la ruta de directorios de su organización.  **Nota:** Si no modifica este fichero los permisos establecidos en la presente guía no se aplicarán correctamente sobre las carpetas que se quiere reforzar la seguridad.
142.	Guarde los cambios realizados y cierre el documento.

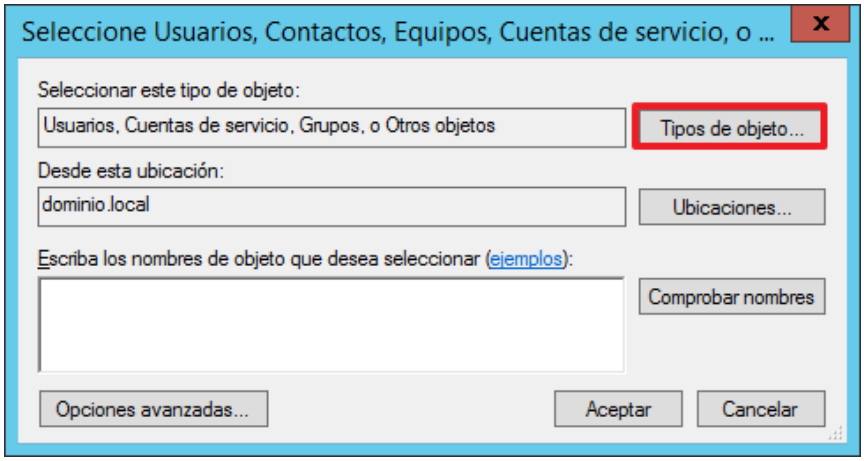
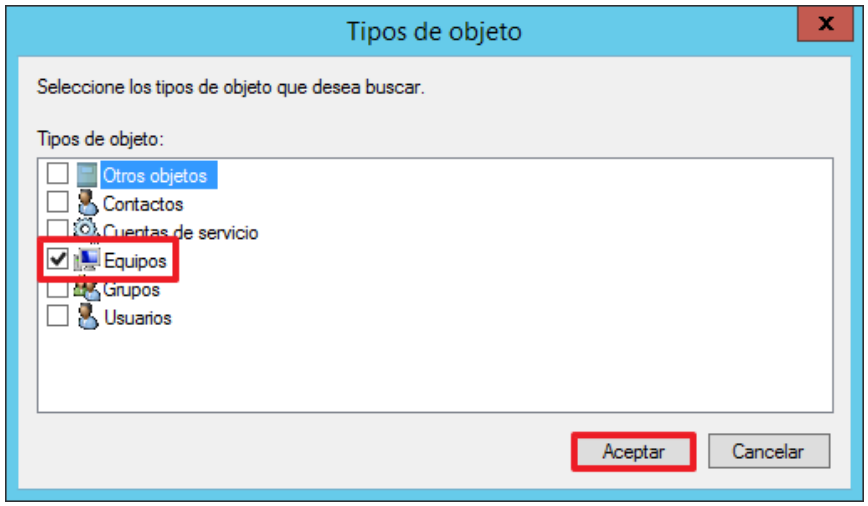
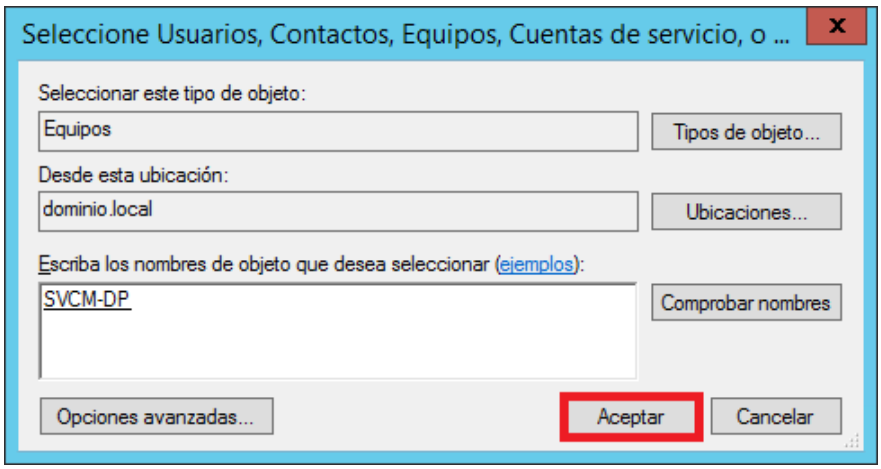
Paso	Descripción
143.	Inicie la herramienta "Usuarios y equipos de Active Directory". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
144.	El siguiente proceso va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 149. En caso contrario continúe con el paso a paso.

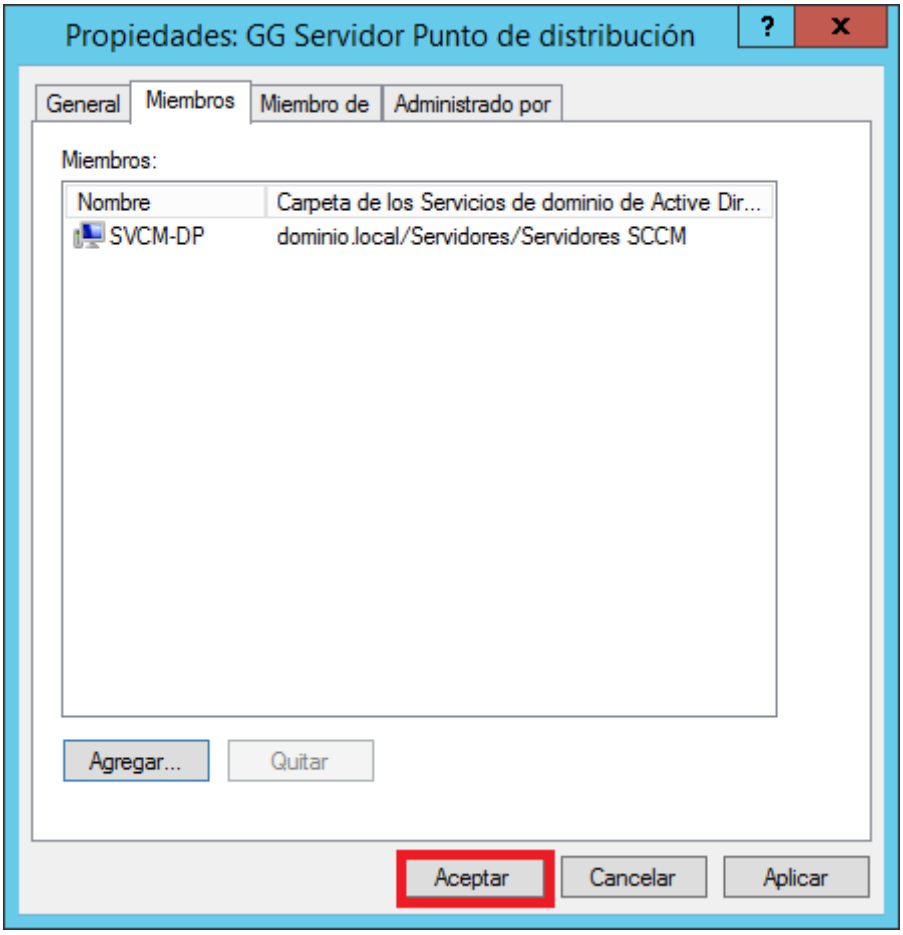
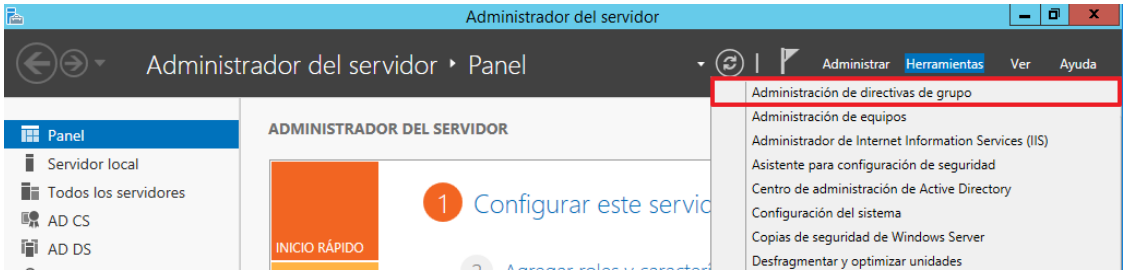
Paso	Descripción
145.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
146.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar”. 

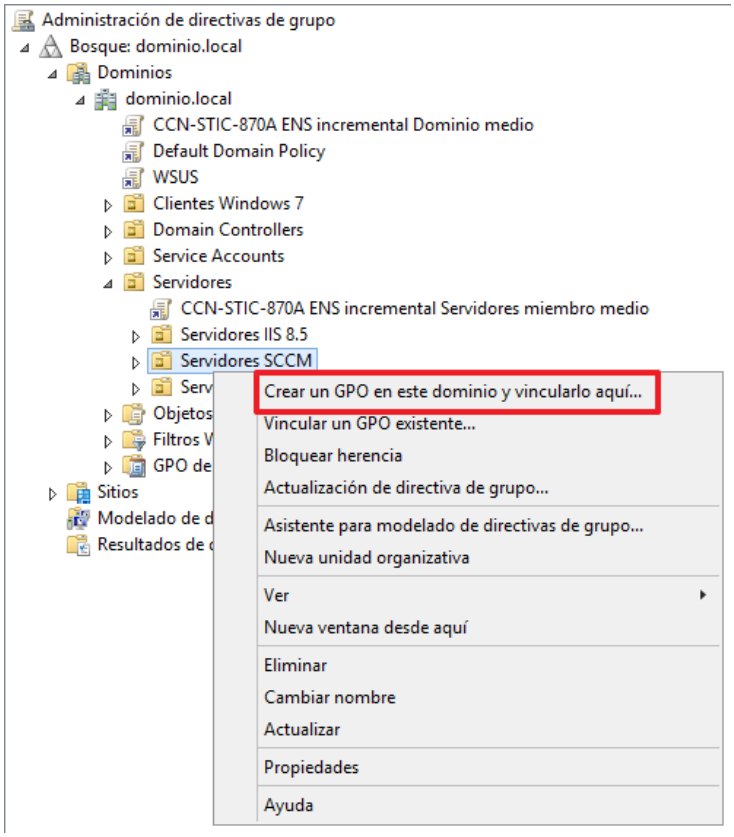
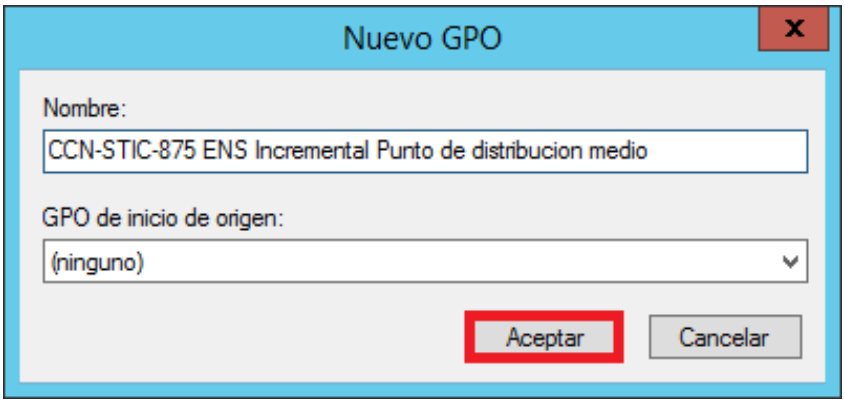
Paso	Descripción
147.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
148.	Marque sobre la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

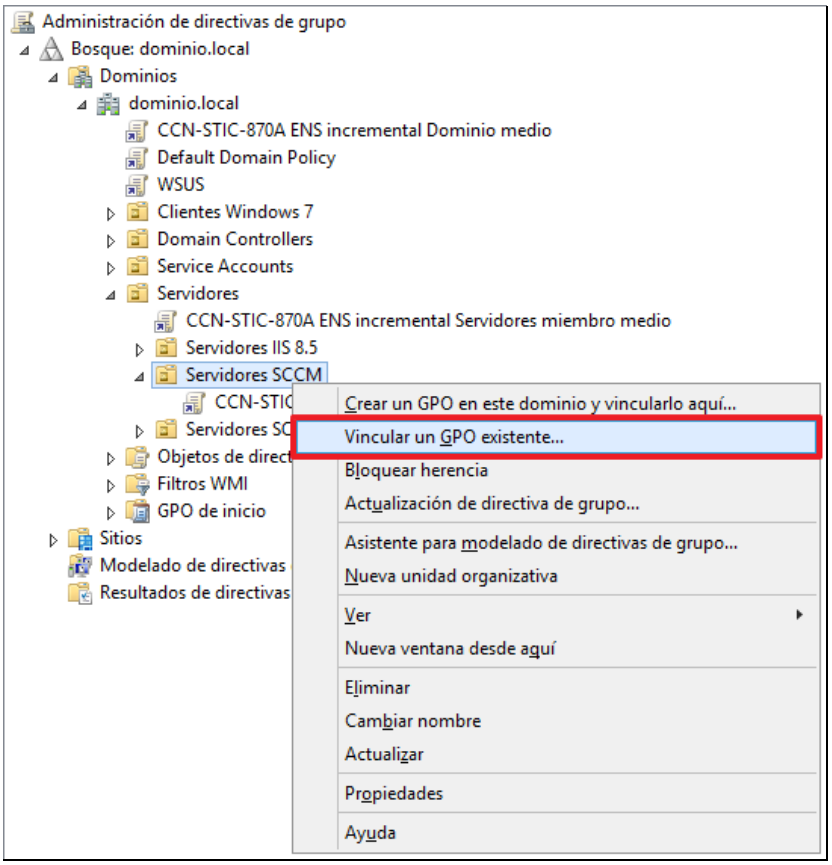
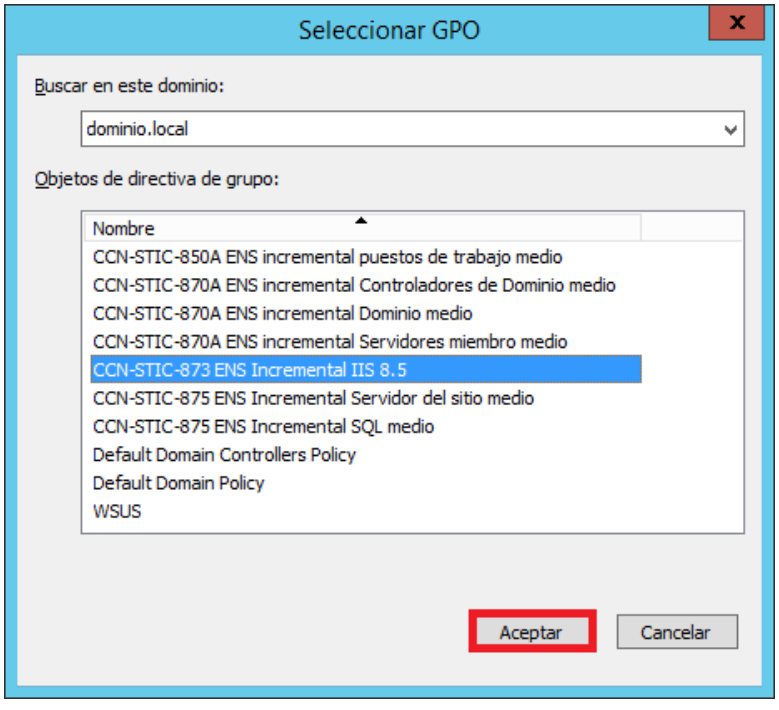
Paso	Descripción
149.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
150.	Escriba el nombre “GG Servidor Punto de distribución medio” y pulse “Aceptar”. 

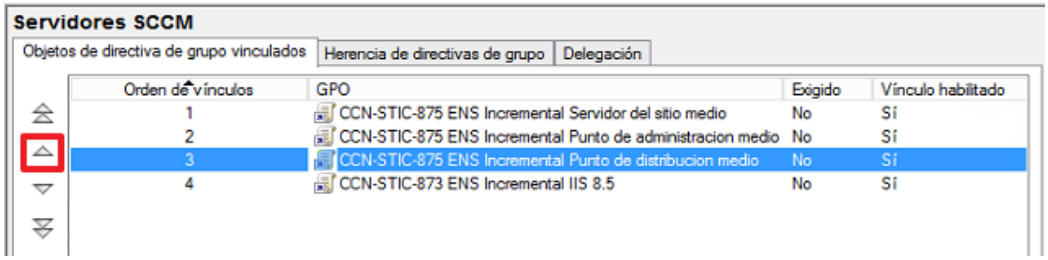
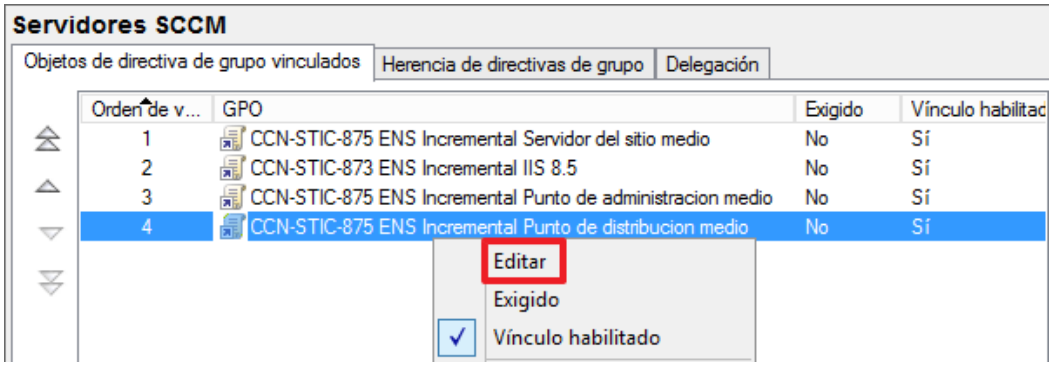
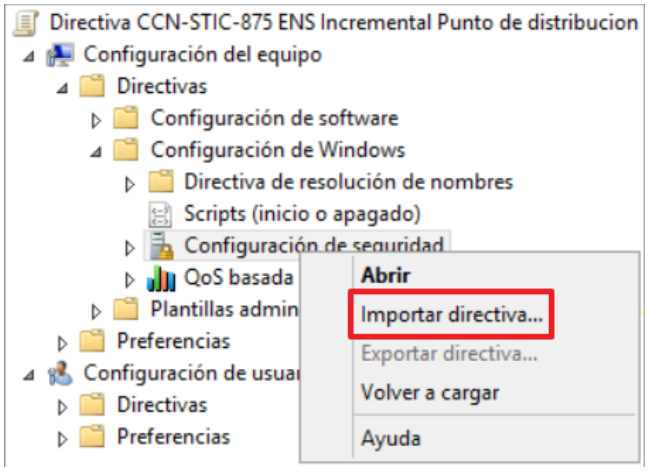
Paso	Descripción
151.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
152.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de distribución” al grupo. 

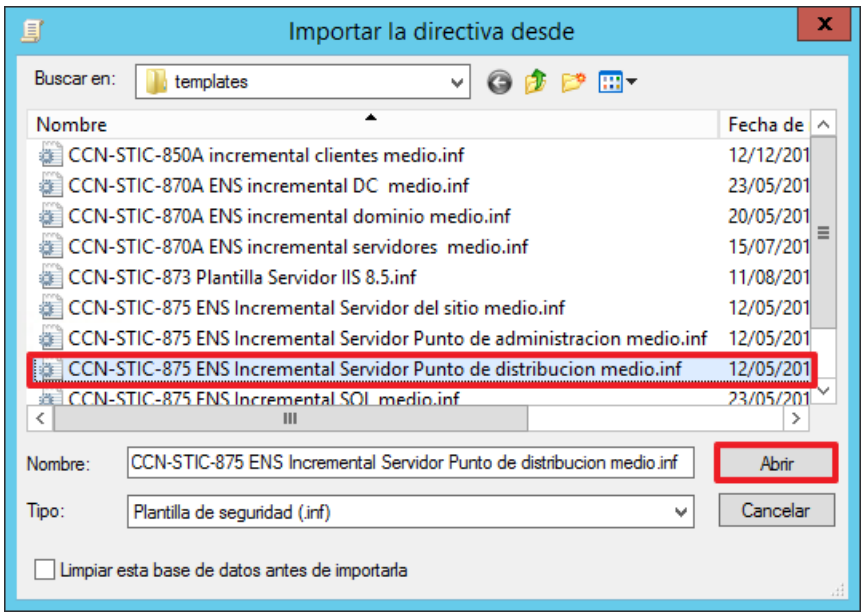
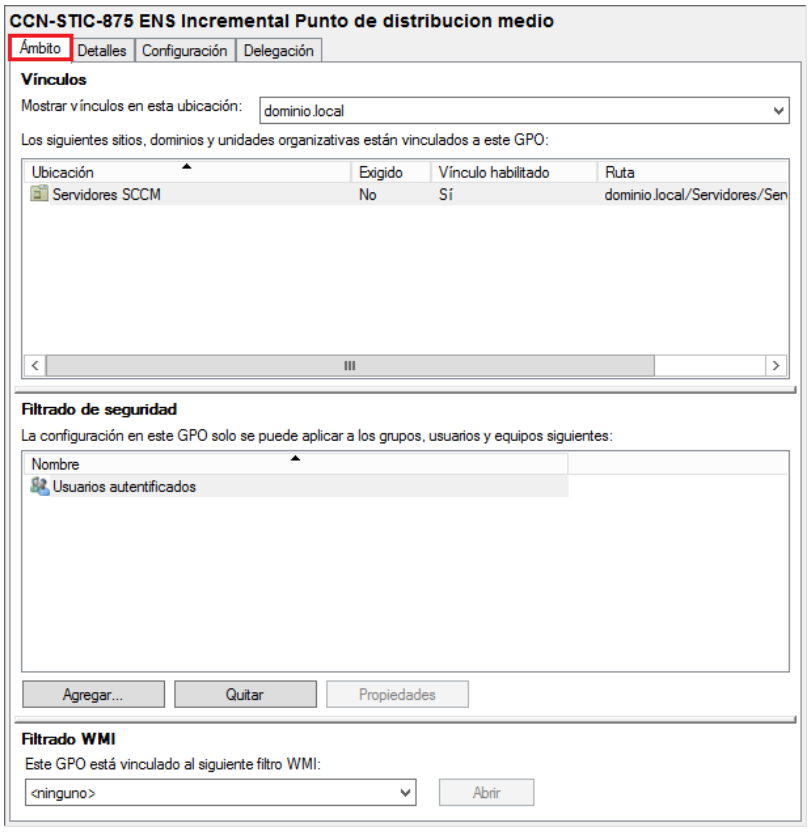
Paso	Descripción
153.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
154.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
155.	Agregue los equipos y pulse sobre “Aceptar”. 

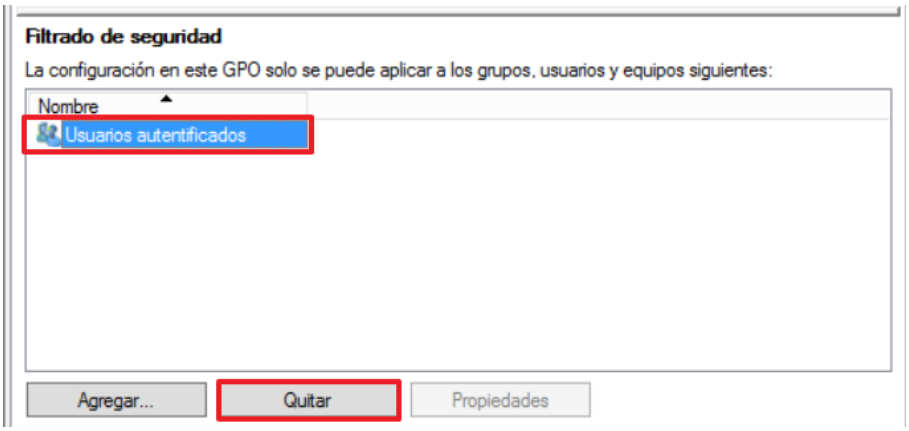
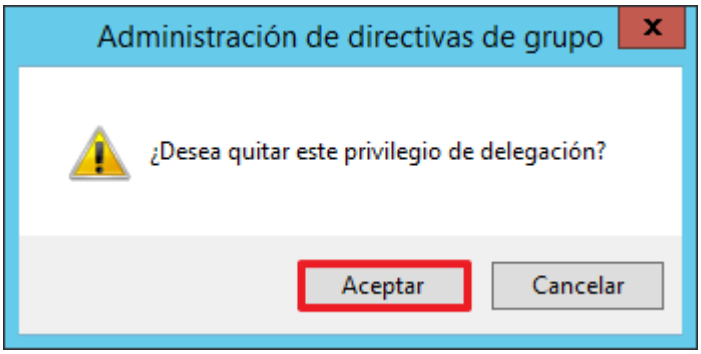
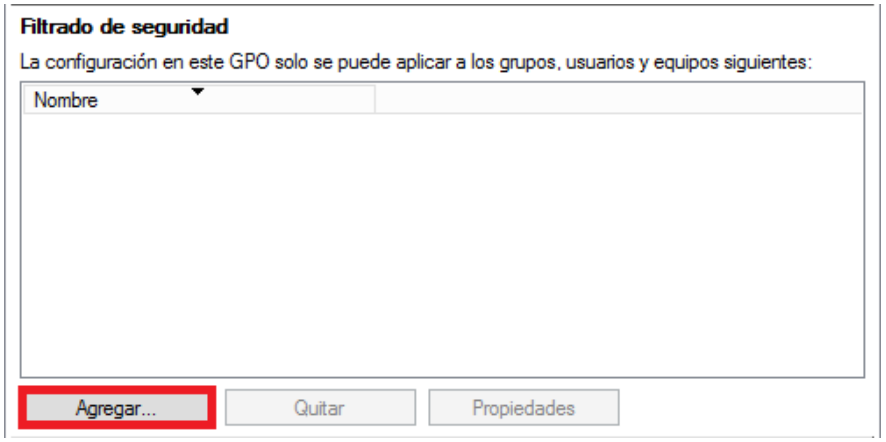
Paso	Descripción
156.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
157.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
158.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

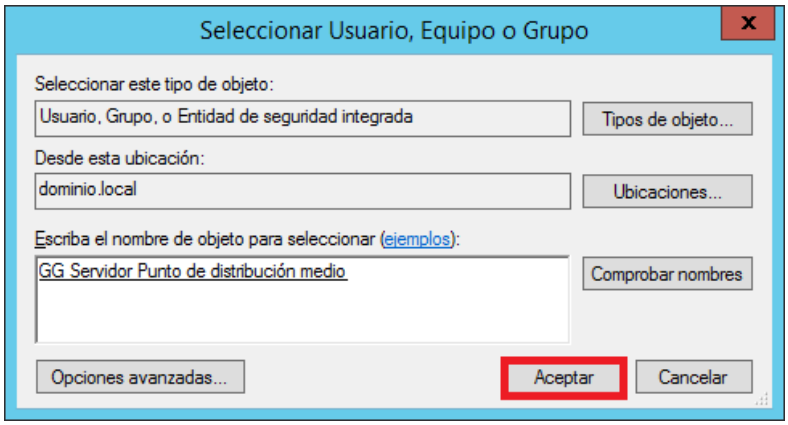
Paso	Descripción
159.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
160.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de distribución medio” y haga clic en el botón “Aceptar”. 
161.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”. En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 166, en caso contrario continúe con el paso a paso.
162.	A continuación, se va a asociar la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.

Paso	Descripción
163.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
164.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
165.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de distribución medio" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de distribución medio" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
166.	Edite la GPO: "CCN-STIC-875 ENS Incremental Punto de distribución medio" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
167.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
168.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de distribución medio.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
169.	Cierre el "Editor de administración de directivas de grupo" una vez que se haya realizado la importación de la configuración de seguridad.
170.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

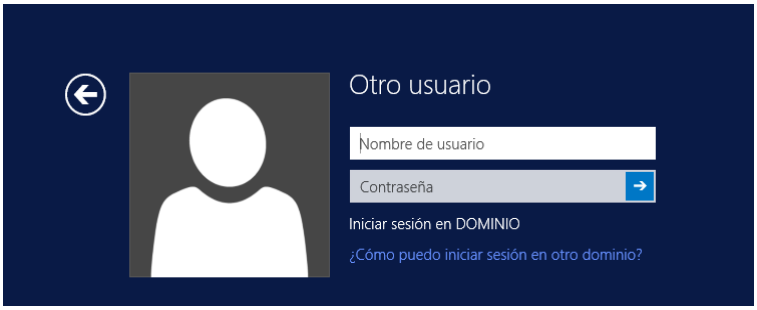
Paso	Descripción
171.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
172.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
173.	Una vez quitado, pulse el botón “Agregar…”. 

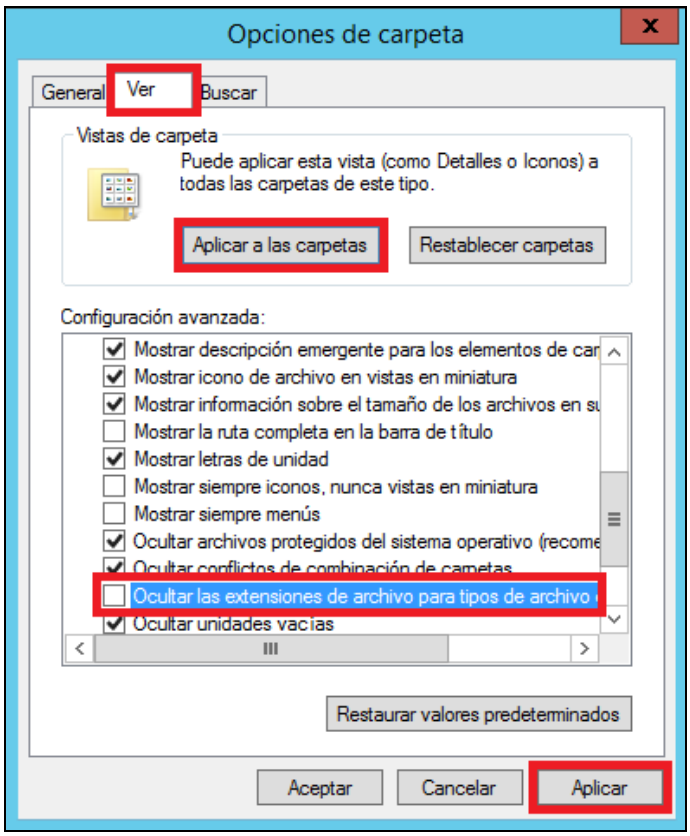
Paso	Descripción
174.	Introduzca como nombre “GG Servidor Punto de distribución medio” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
175.	Cierre el “Editor de administración de directivas de grupo”.

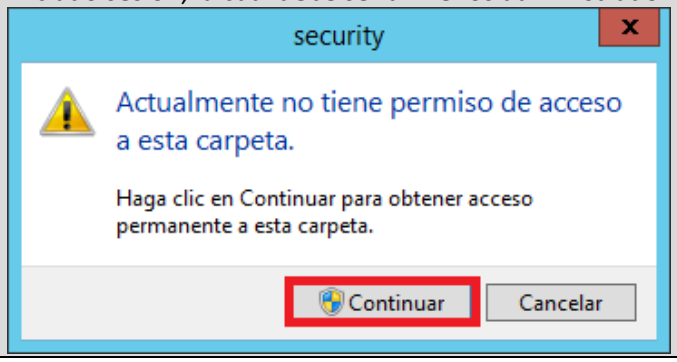
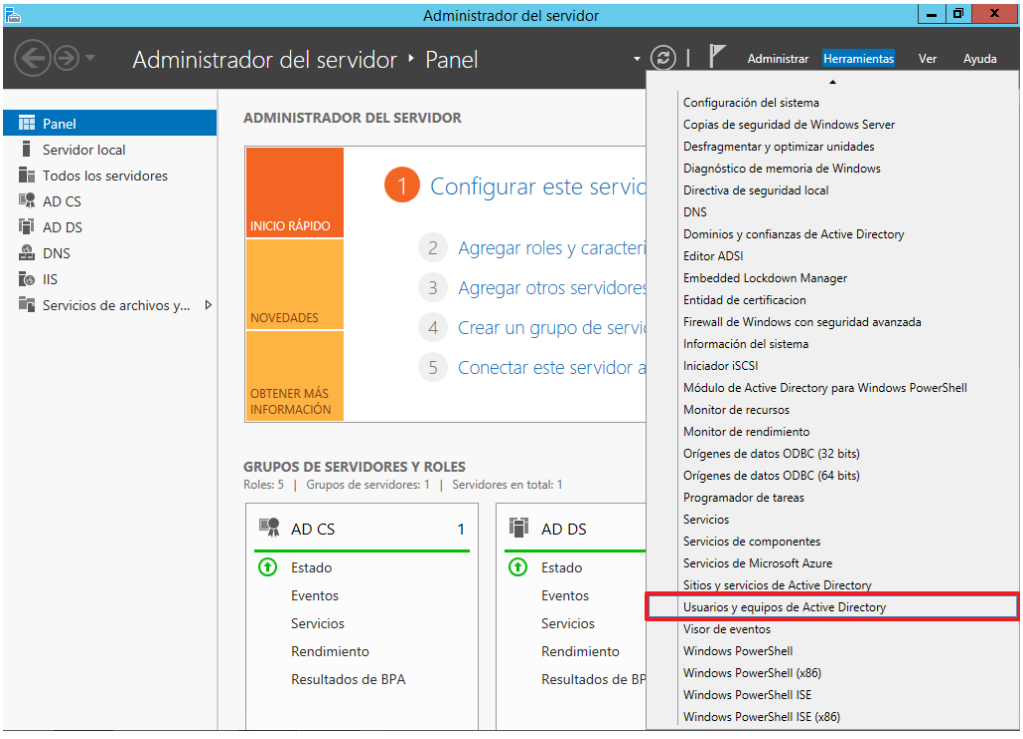
5. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE ACTUALIZACIÓN DE SOFTWARE

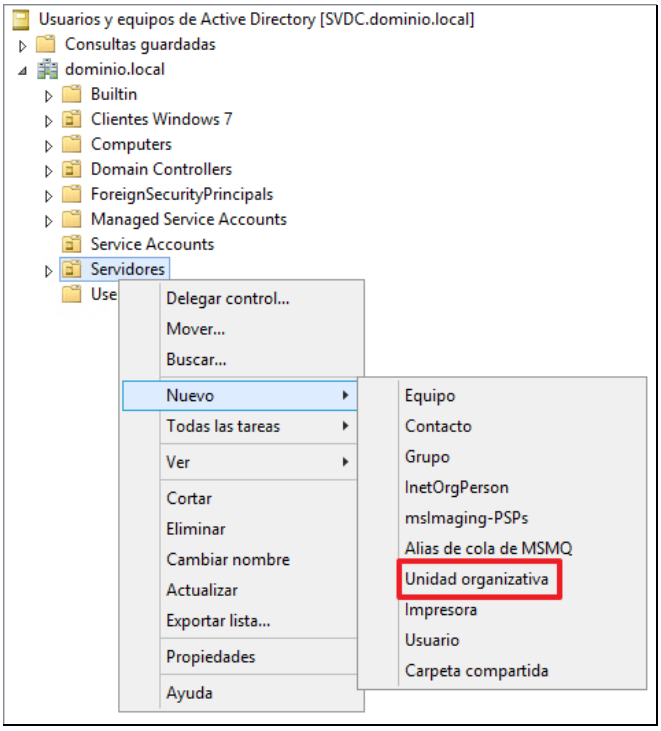
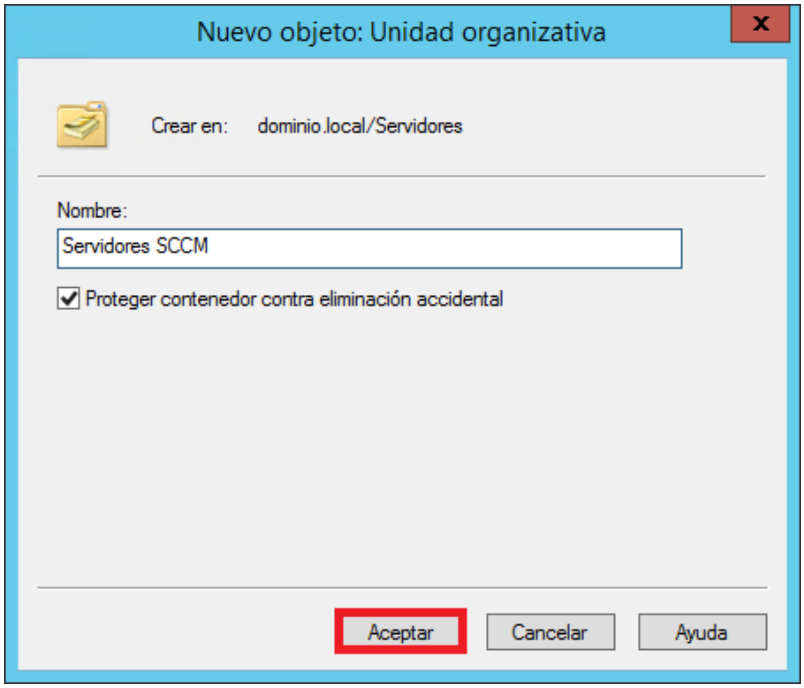
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de actualización de software implementado en el equipo.

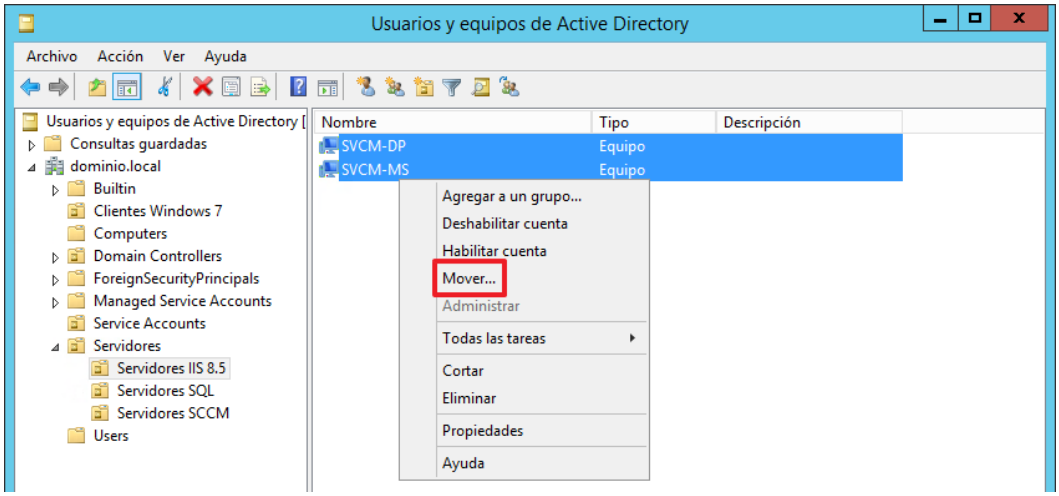
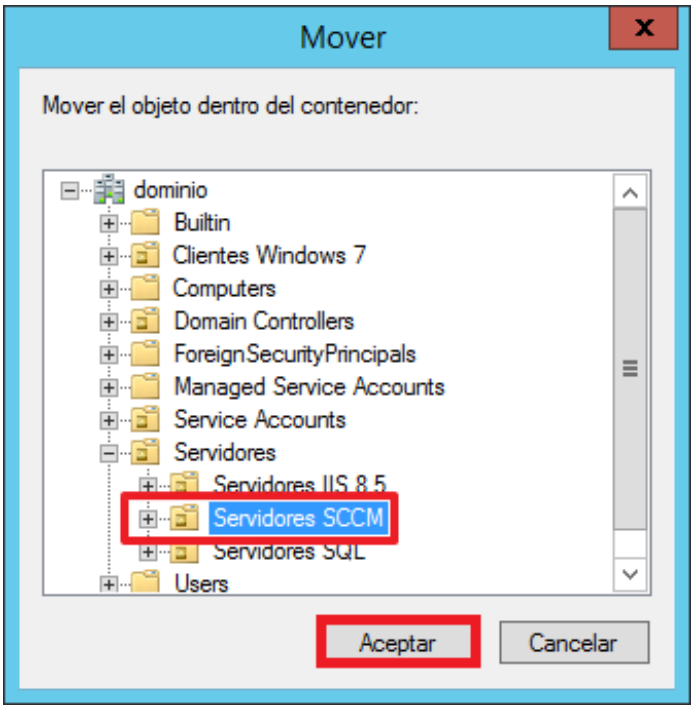
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

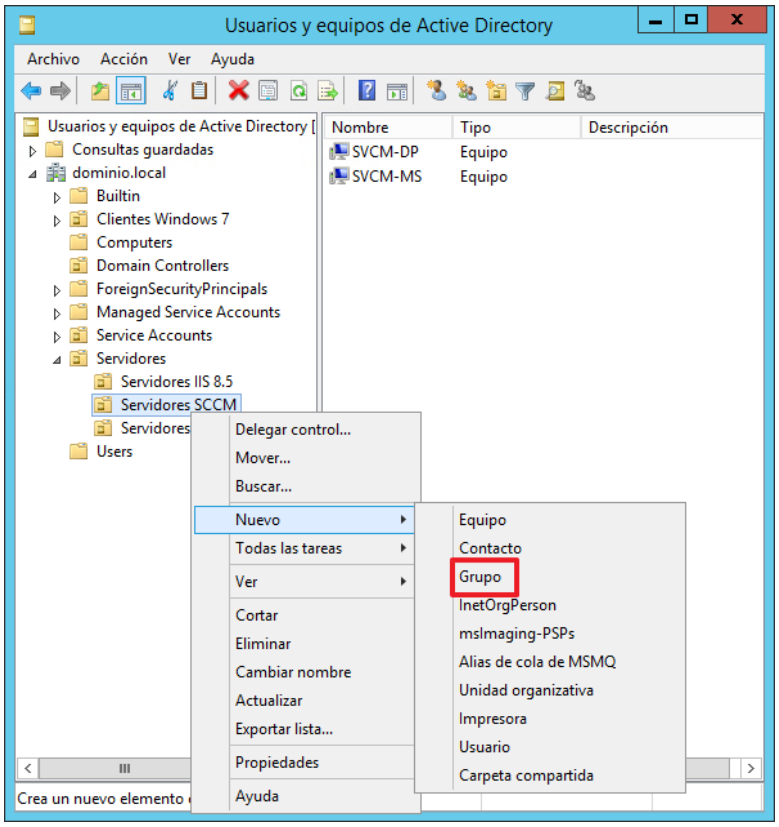
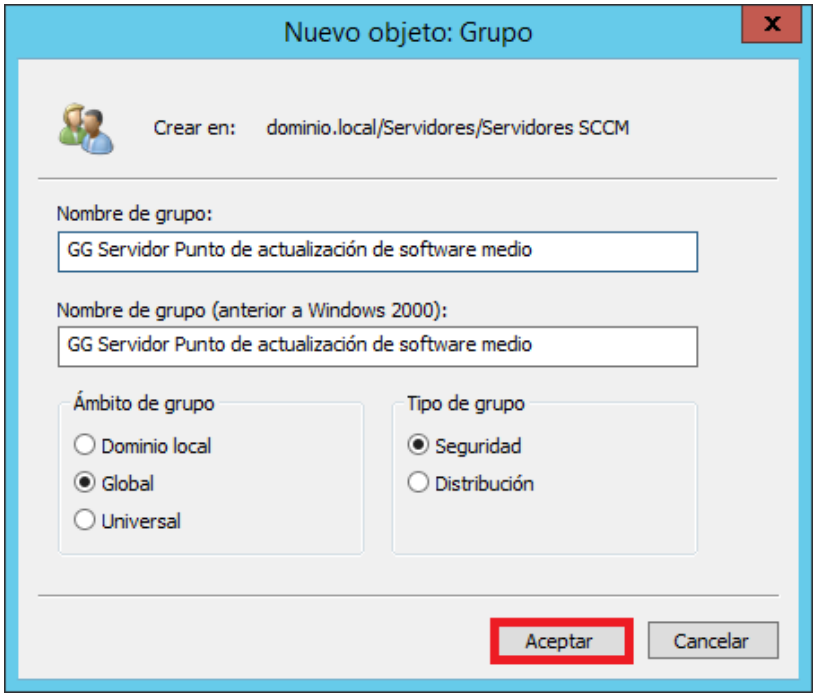
Paso	Descripción
176.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
177.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

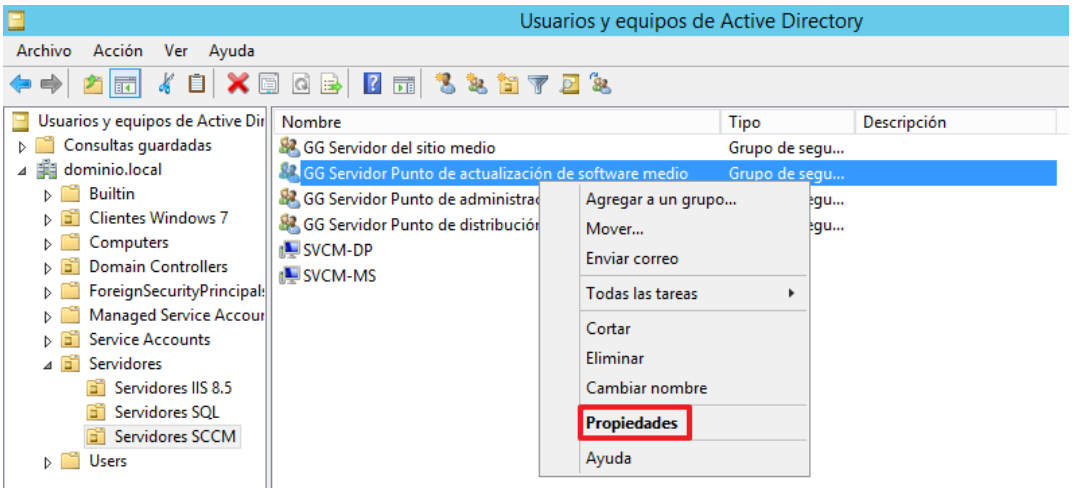
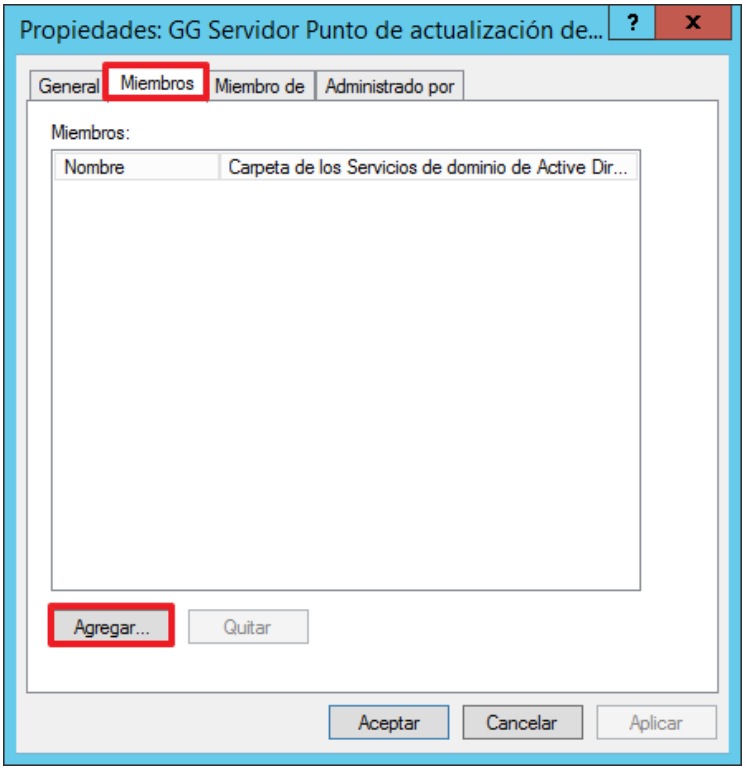
Paso	Descripción
178.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
179.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
180.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

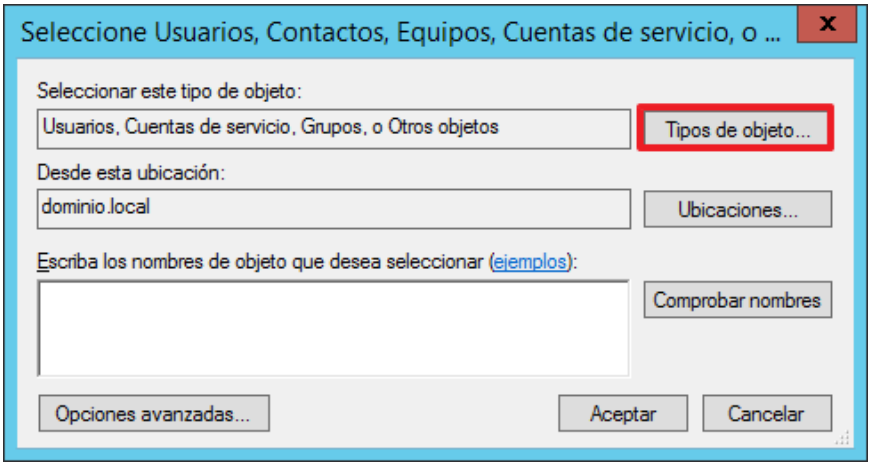
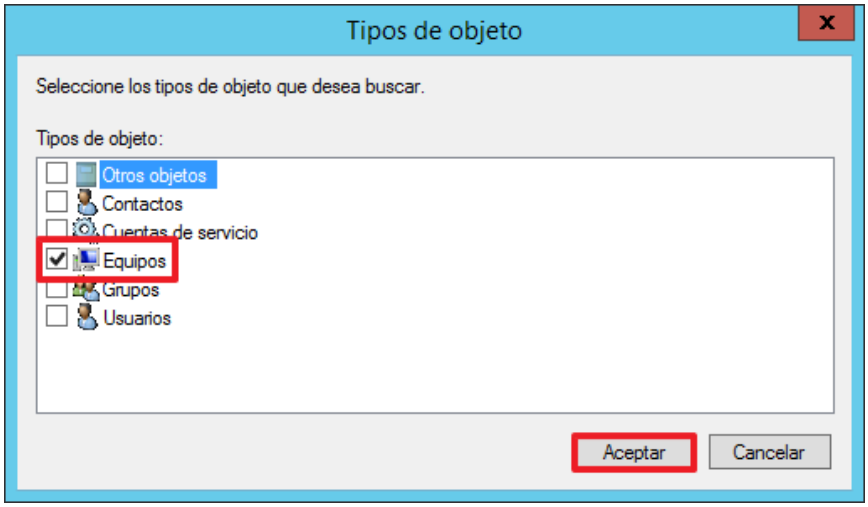
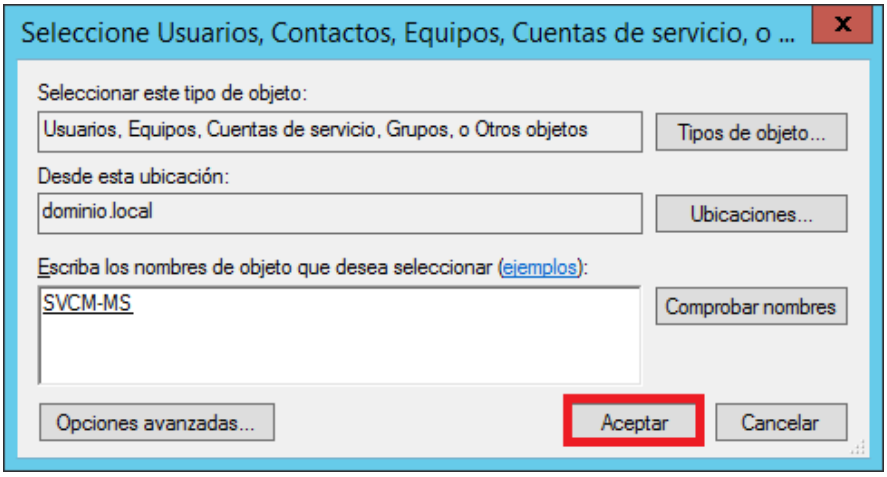
Paso	Descripción
181.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de actualización de software medio.inf” que se encuentra en la ruta “C:\Scripts\Nivel Medio” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
182.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.
183.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SCCM, si ya ha realizado esta tarea, vaya directamente al paso 188. En caso contrario continúe con el paso a paso.

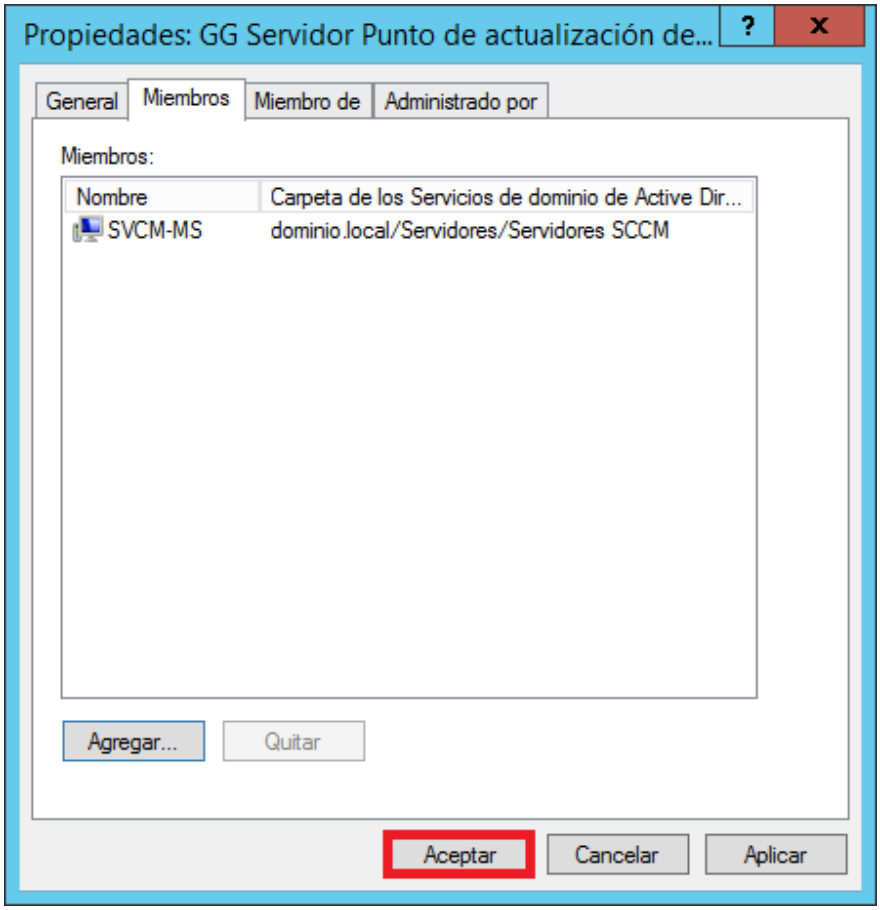
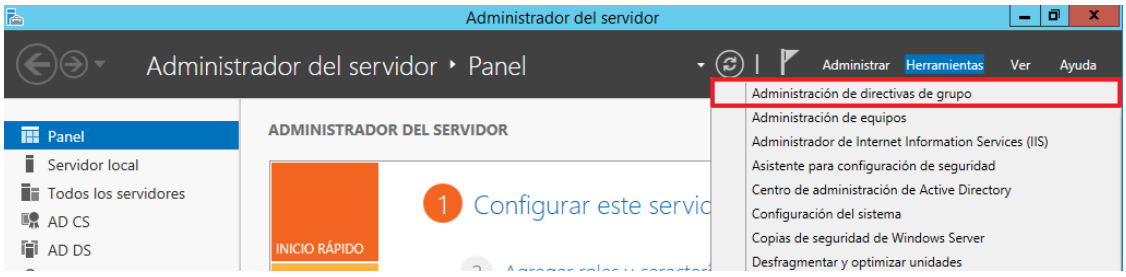
Paso	Descripción
184.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
185.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse en el botón “Aceptar”. 

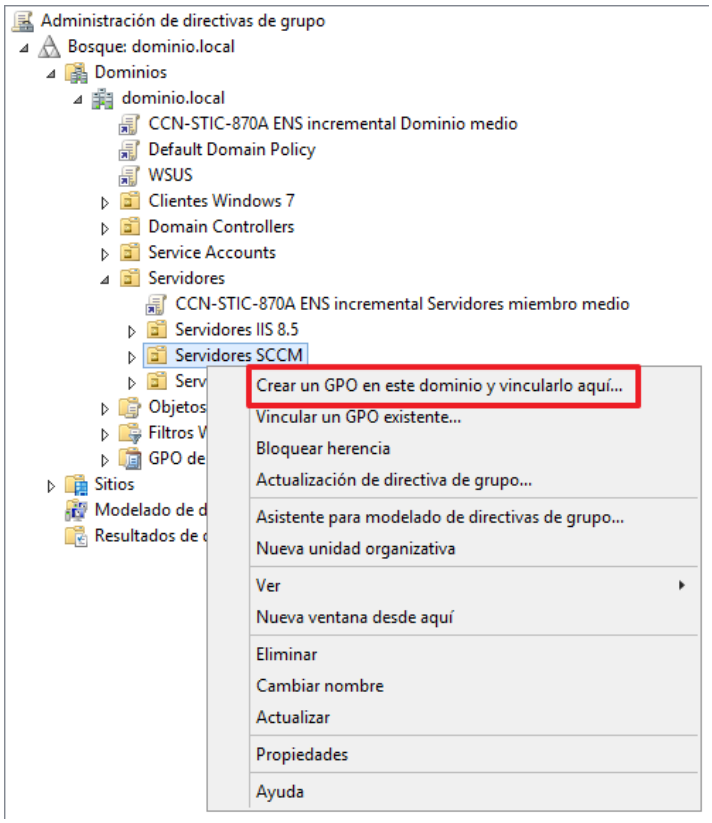
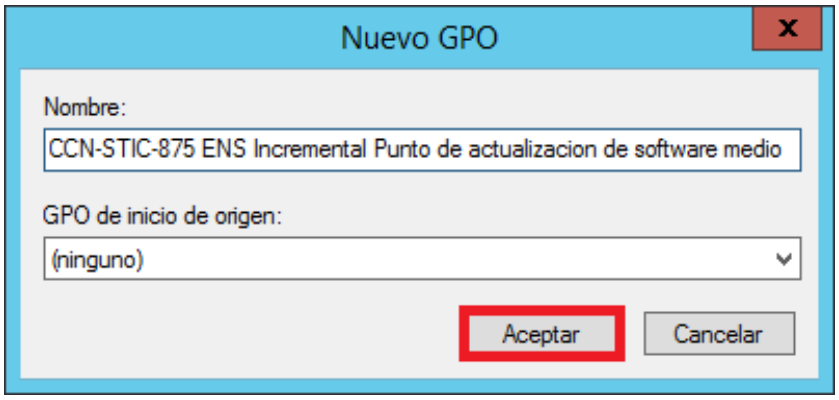
Paso	Descripción
186.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
187.	Marque sobre la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

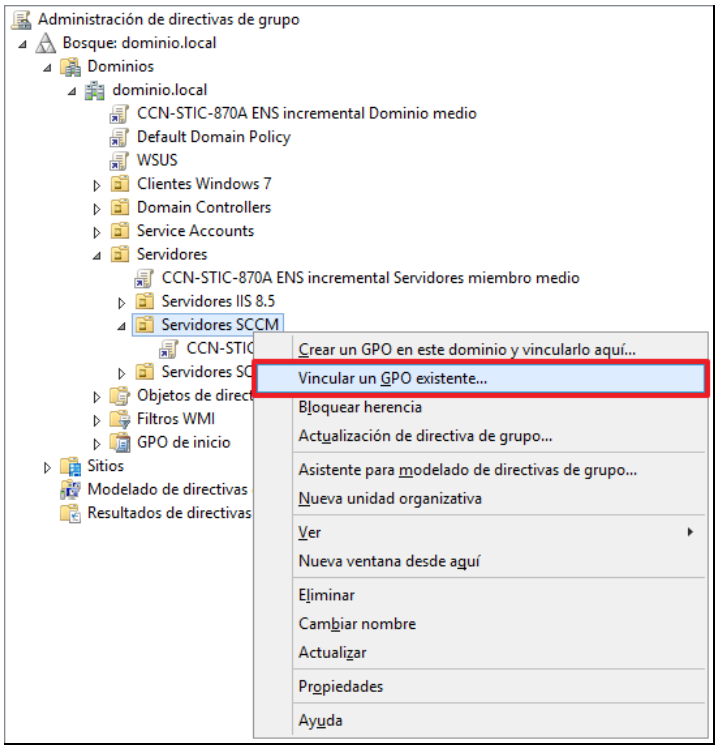
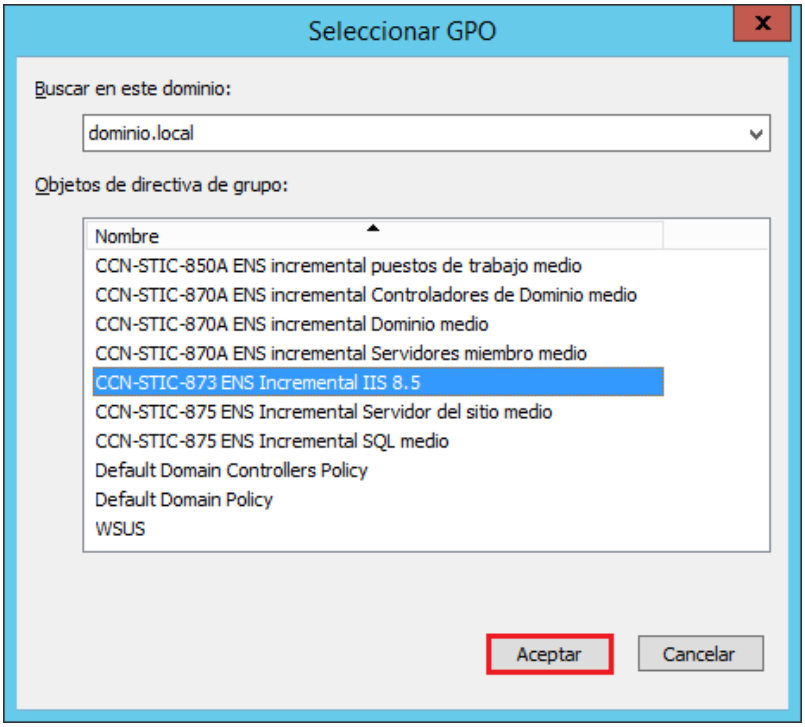
Paso	Descripción
188.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
189.	Escriba el nombre “GG Servidor Punto de actualización de software medio” y pulse “Aceptar”. 

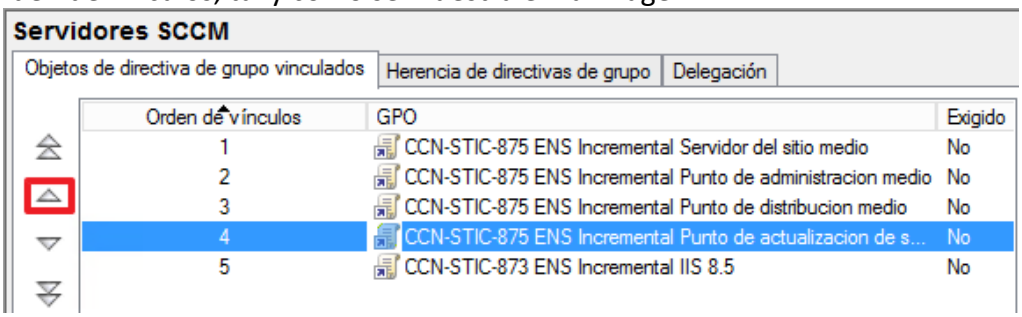
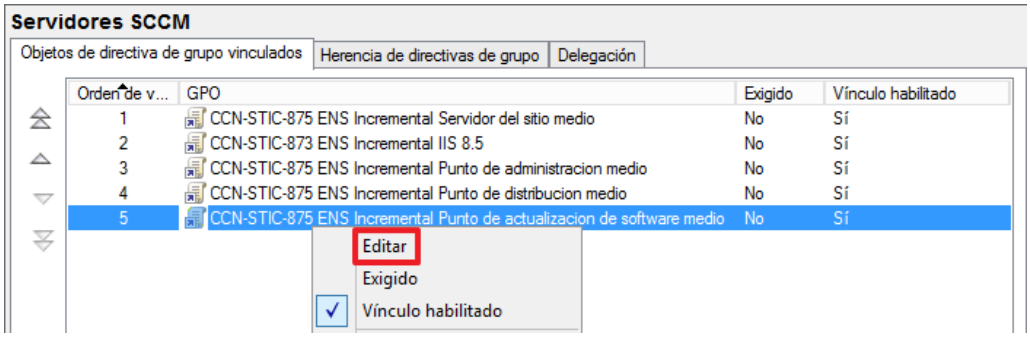
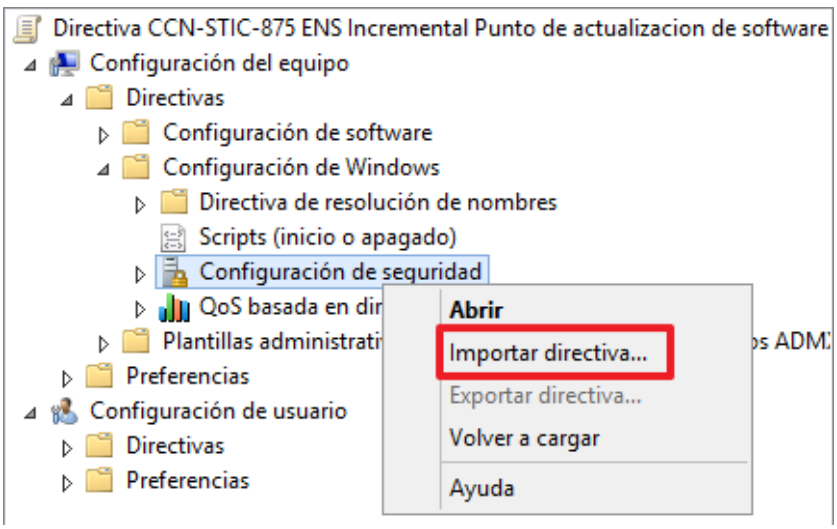
Paso	Descripción
190.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
191.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de actualización de software” al grupo. 

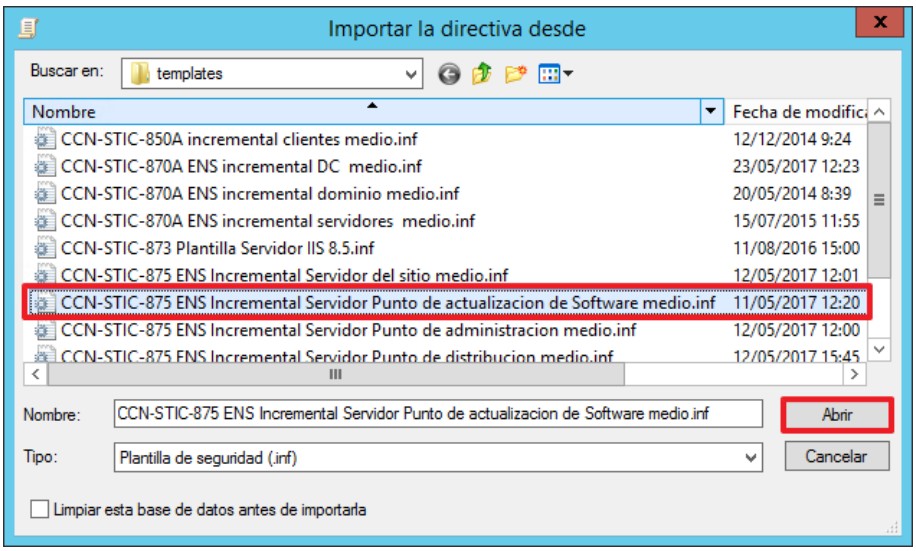
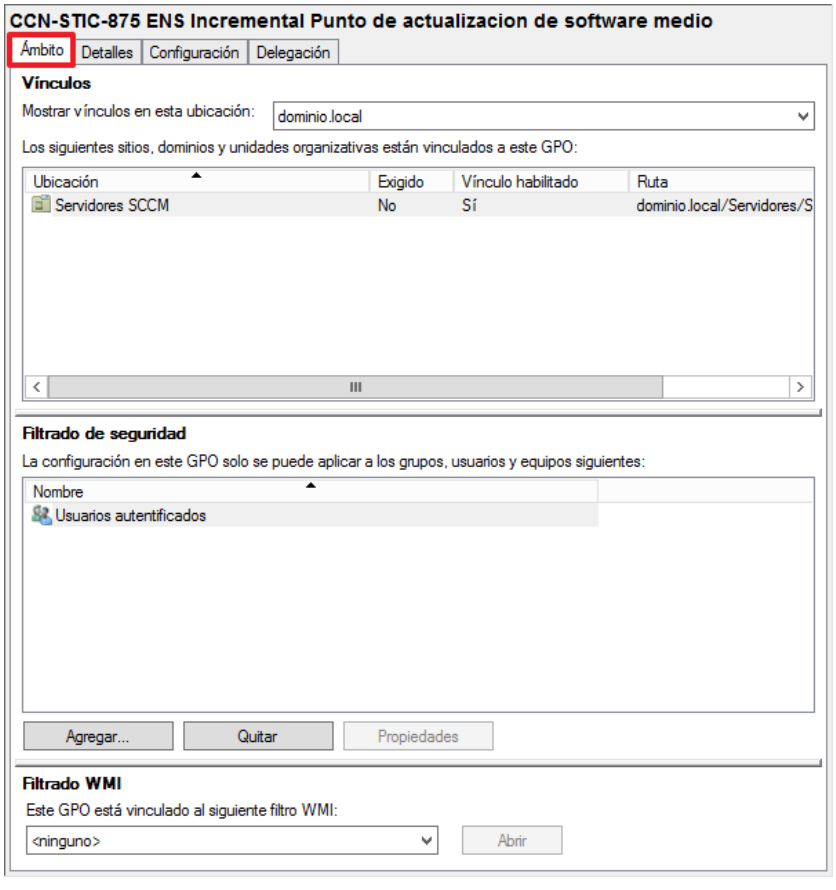
Paso	Descripción
192.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
193.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
194.	Agregue los equipos y pulse sobre “Aceptar”. 

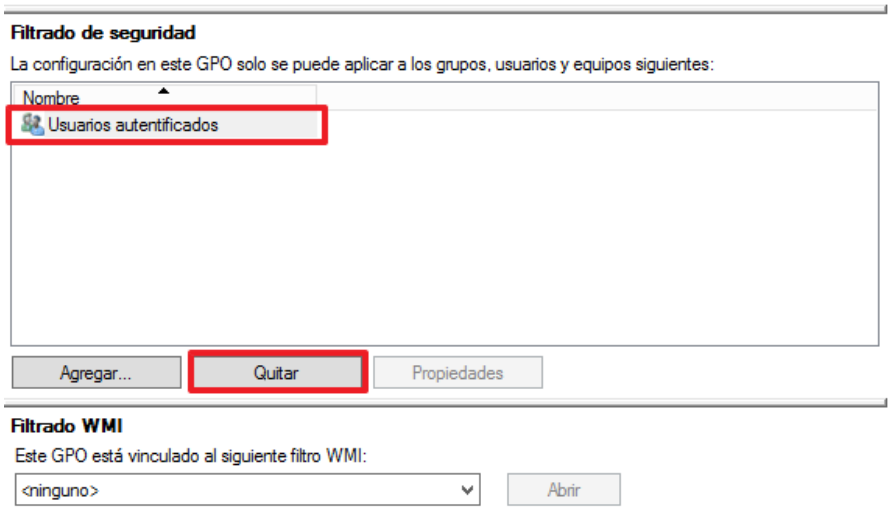
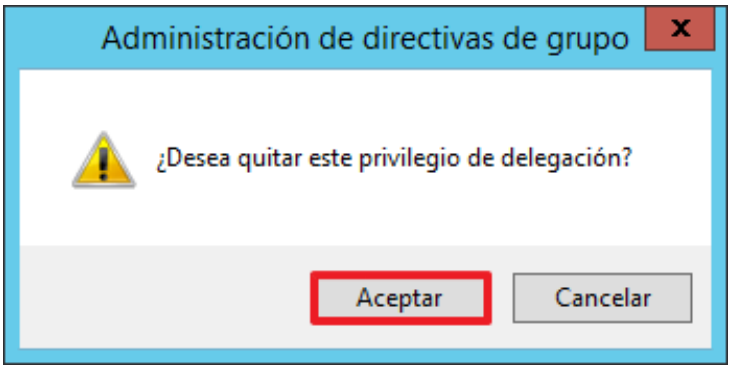
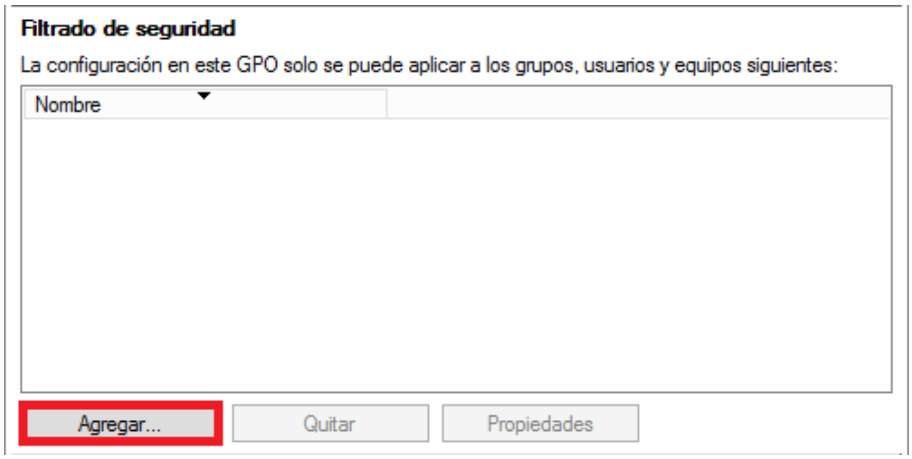
Paso	Descripción
195.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
196.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
197.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

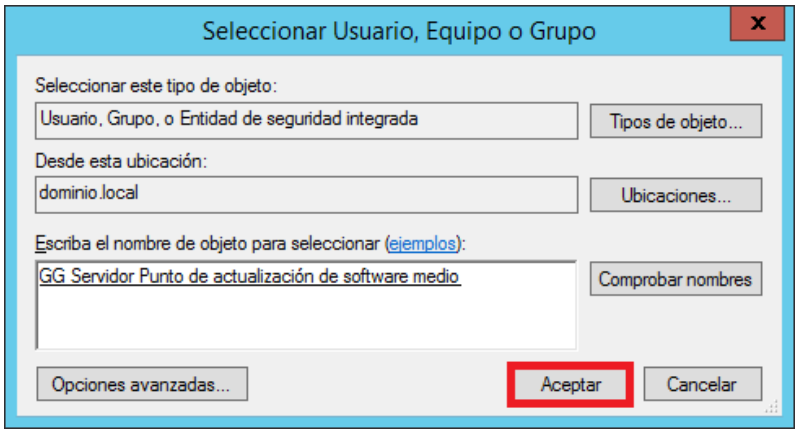
Paso	Descripción
198.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
199.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de actualización de software medio” y haga clic en el botón “Aceptar”. 
200.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”, En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 205, en caso contrario continúe con el paso a paso.
201.	A continuación, se asociará la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.

Paso	Descripción
202.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
203.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
204.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de actualización de software medio" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de actualización de software medio" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
205.	Para editar la GPO: "CCN-STIC-875 ENS Incremental Punto de actualización de software medio" creada anteriormente, haga clic con el botón derecho y seleccione la opción "Editar" del menú contextual. 
206.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". Y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
207.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de actualización de software medio.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
208.	Cierre el "Editor de administración de directivas de grupo" una vez que se haya realizado la importación de la configuración de seguridad.
209.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

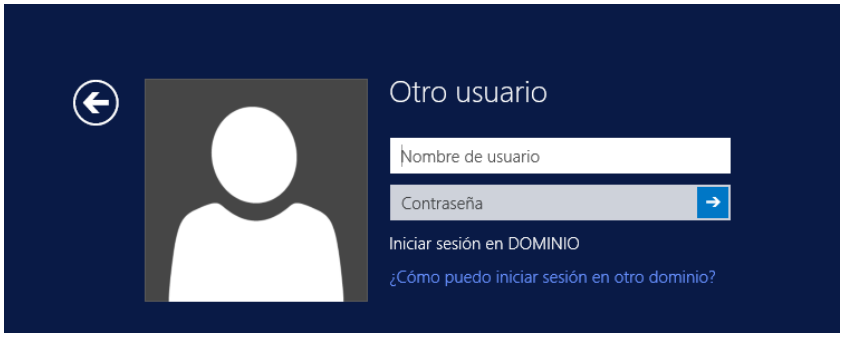
Paso	Descripción
210.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
211.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
212.	Una vez quitado, pulse el botón “Agregar…”. 

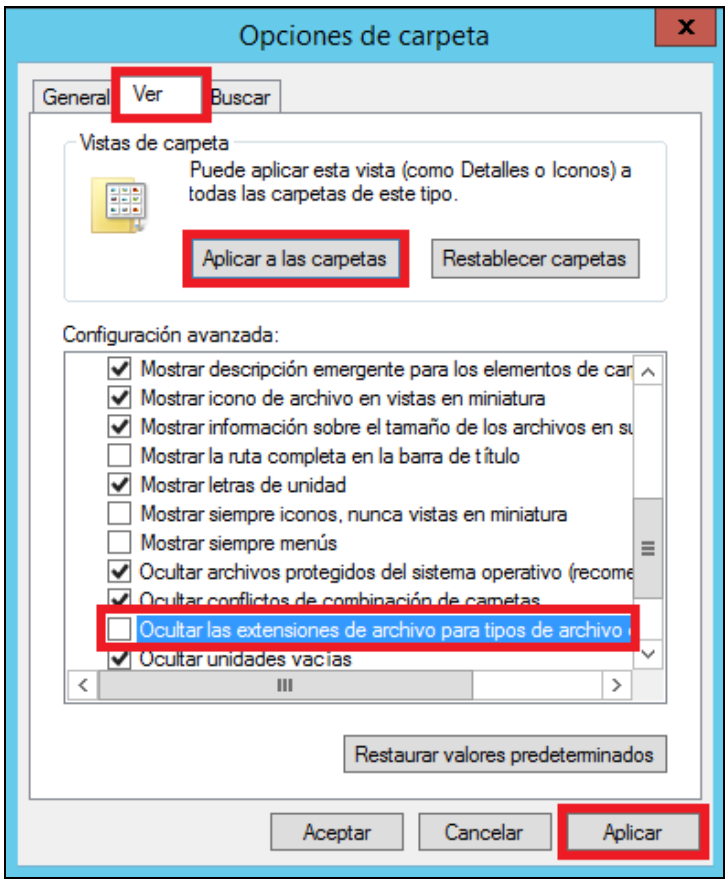
Paso	Descripción
213.	Introduzca como nombre “GG Servidor Punto de actualización de software medio”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
214.	Cierre el “Editor de administración de directivas de grupo”.

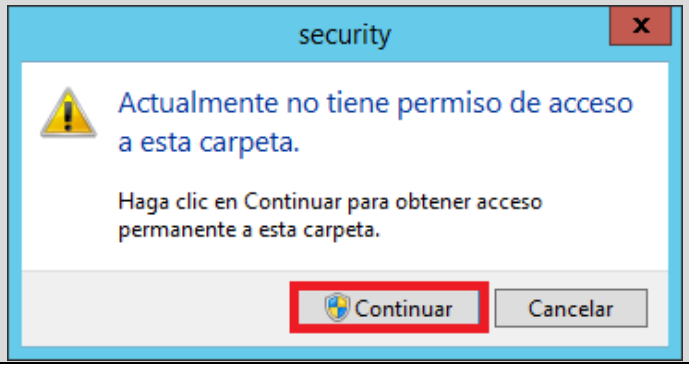
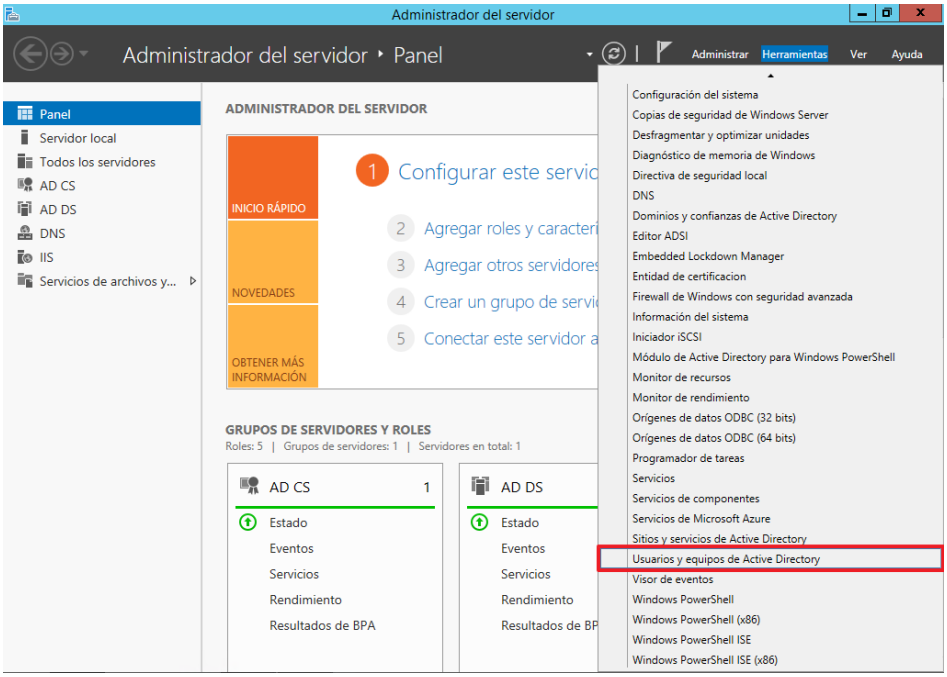
6. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE SERVICIOS DE INFORME

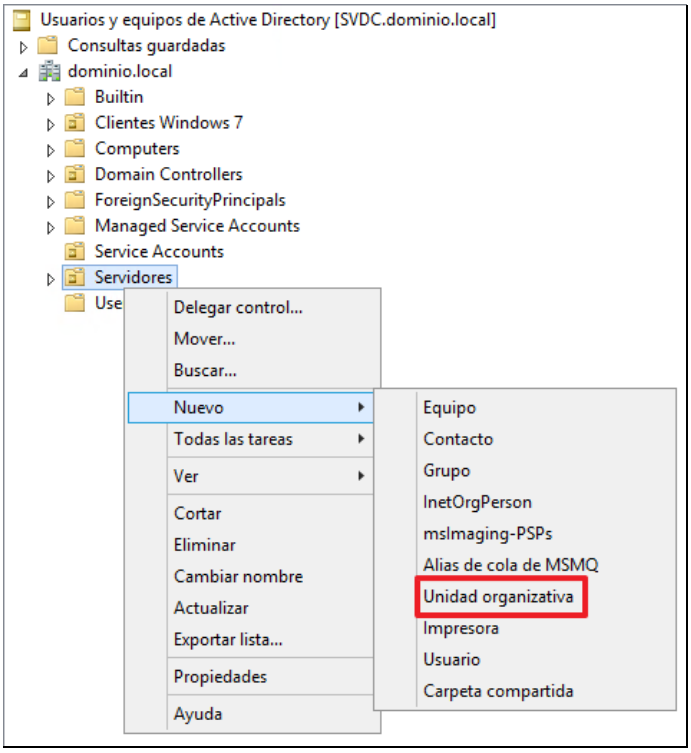
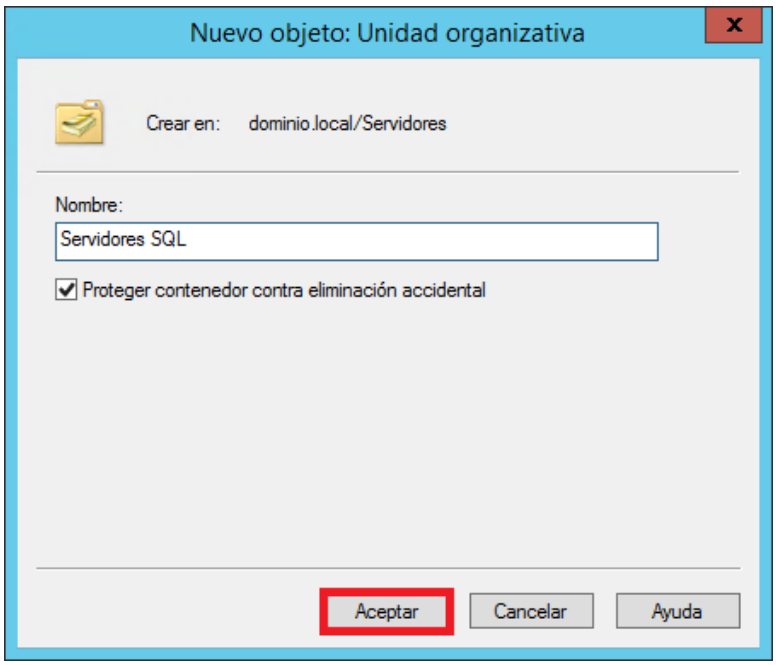
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de servicios de informes implementado en el equipo.

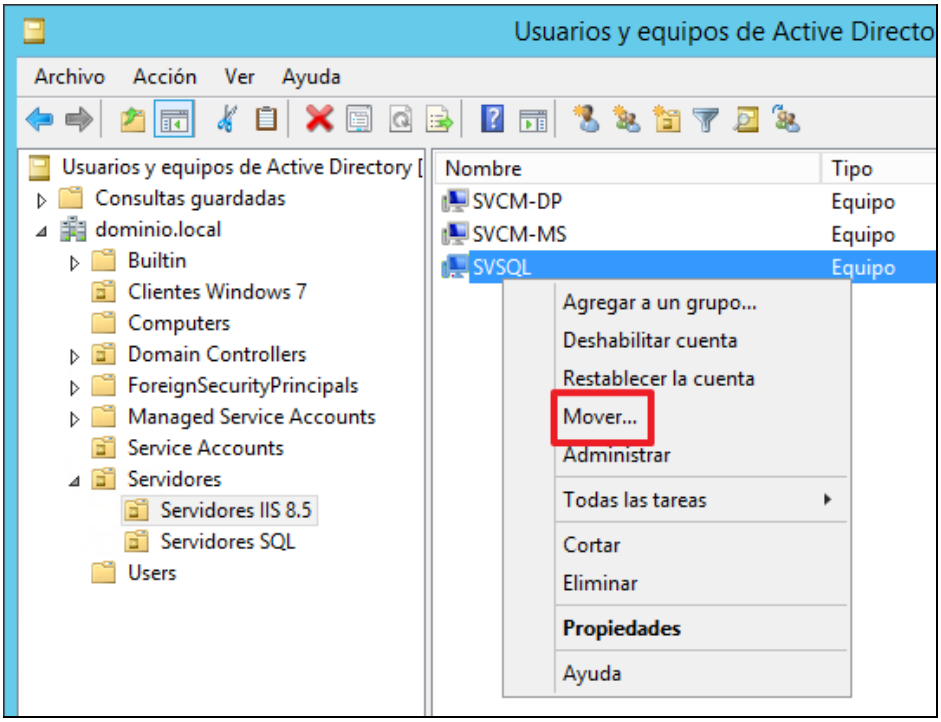
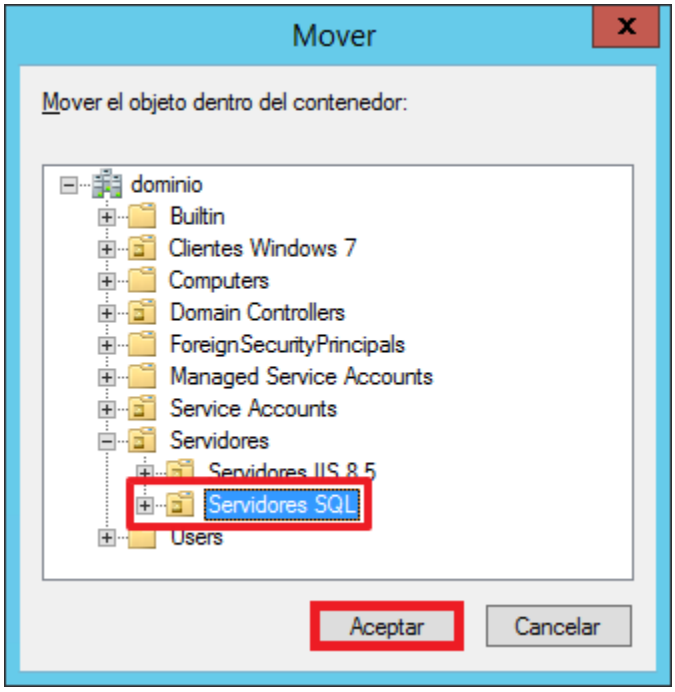
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

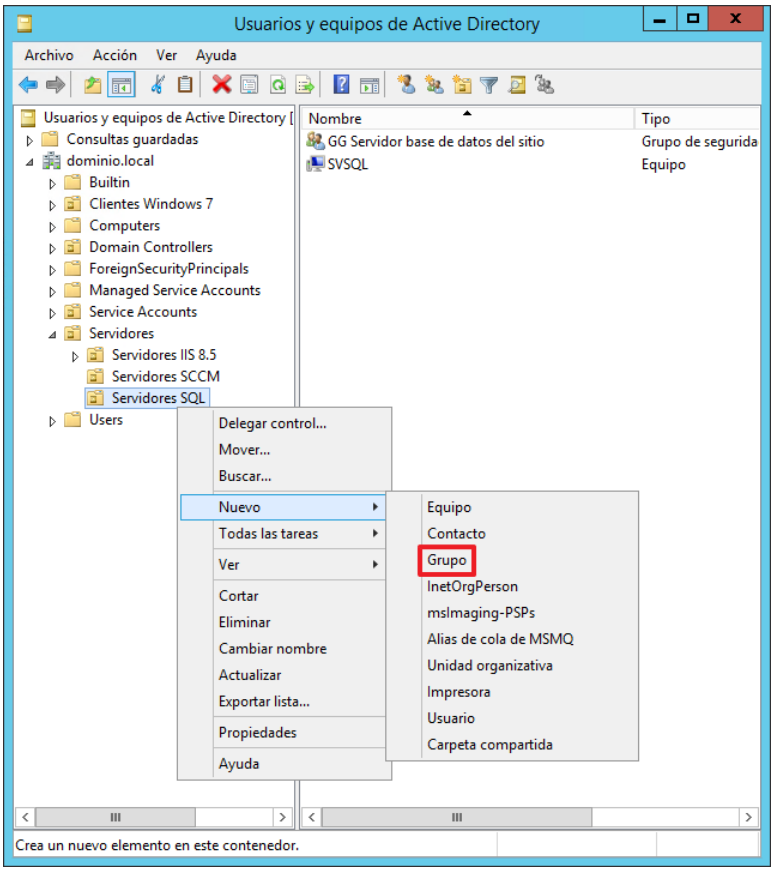
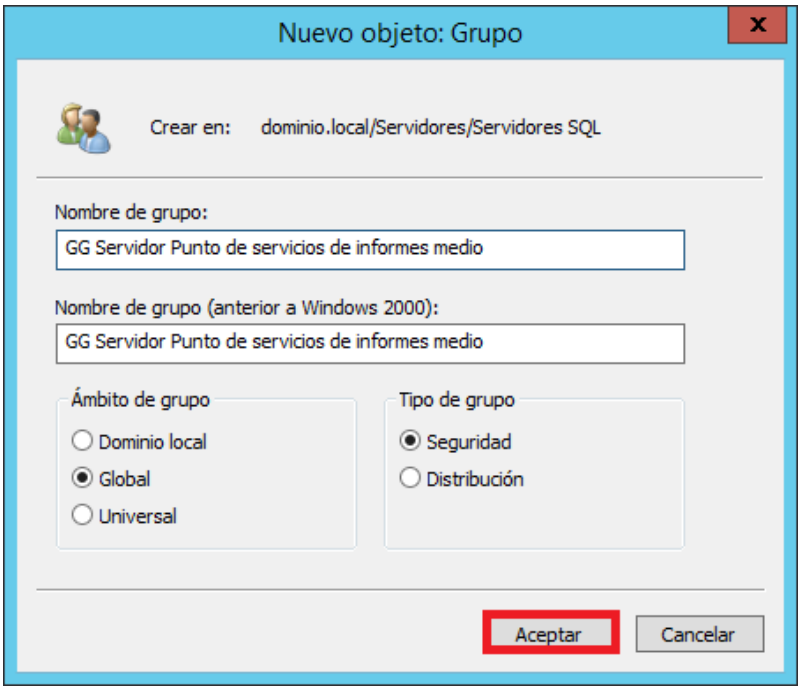
Paso	Descripción
215.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
216.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

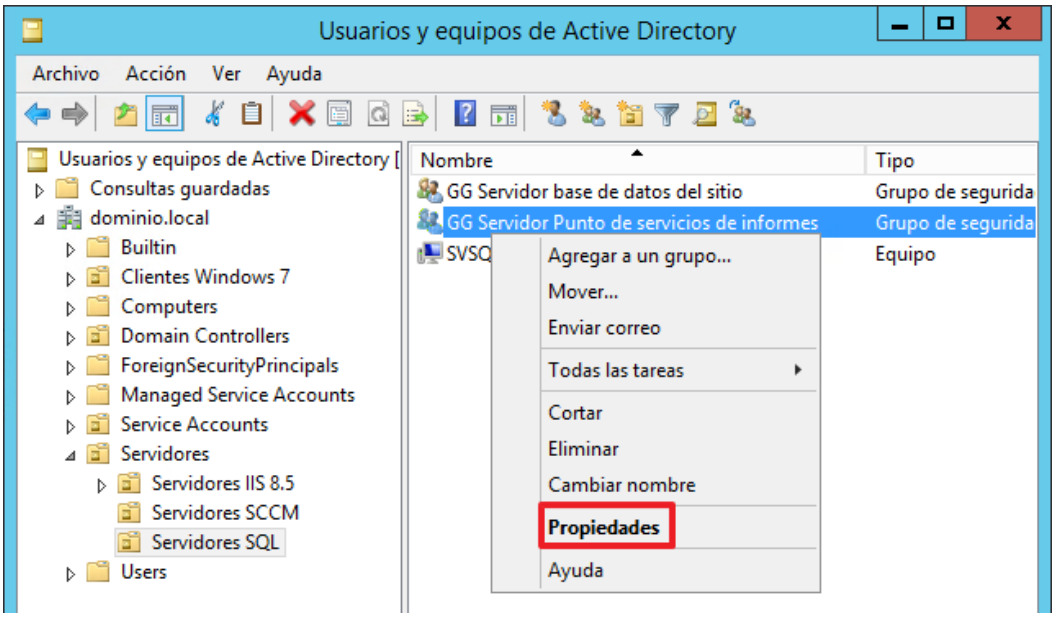
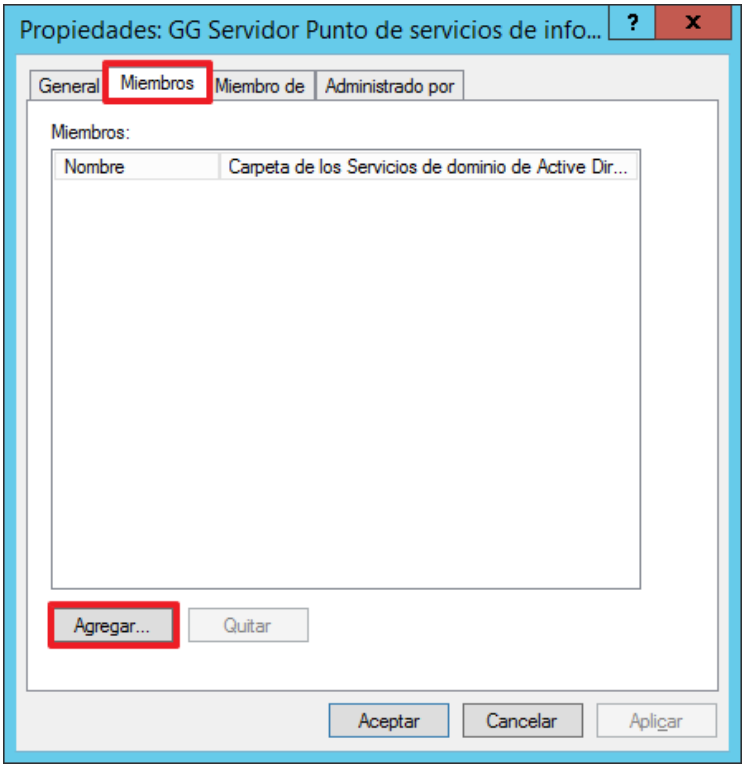
Paso	Descripción
217.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
218.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
219.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

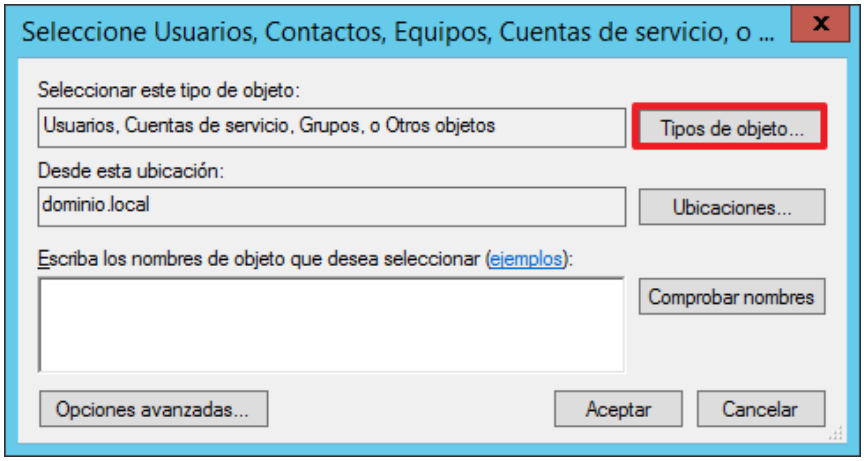
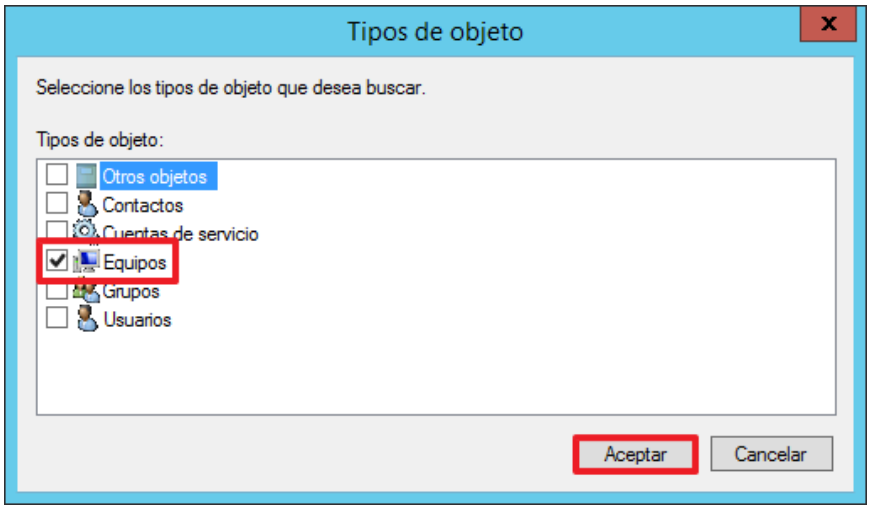
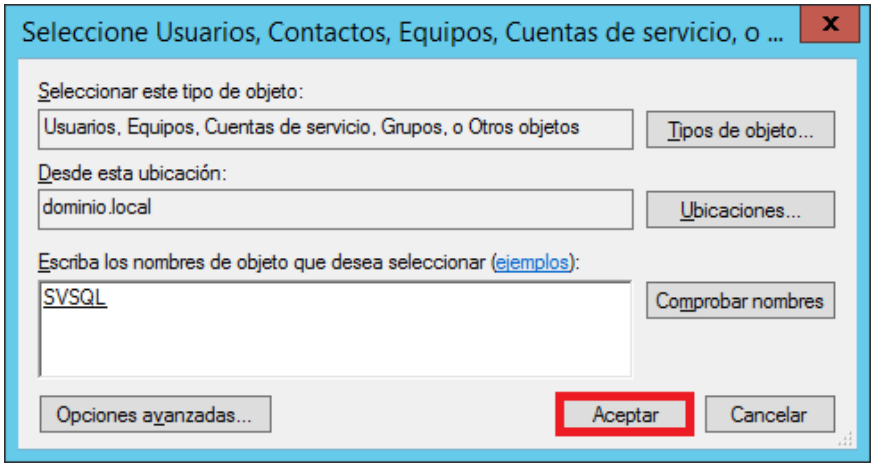
Paso	Descripción
220.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de servicios de informes medio.inf” que se encuentra en la ruta “C:\Scripts\Nivel Medio” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
221.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
222.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SQL, si ya ha realizado esta tarea, vaya directamente al paso 227. En caso contrario continúe con el paso a paso.

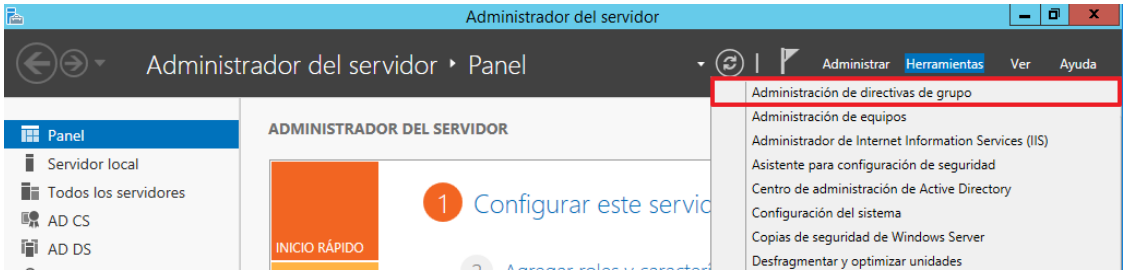
Paso	Descripción
223.	Para la creación de la nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
224.	En la consola, cree una unidad organizativa denominada “Servidores SQL” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse en el botón “Aceptar”. 

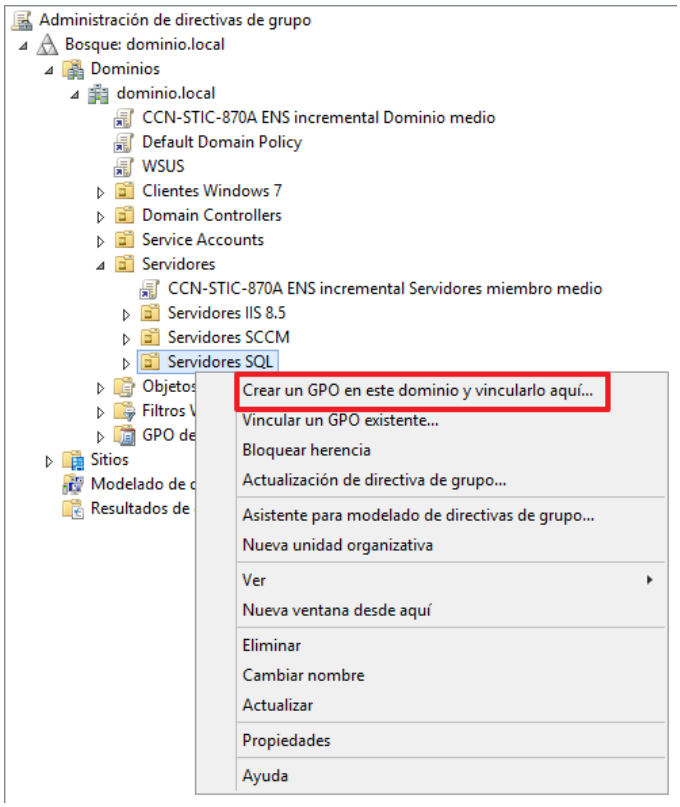
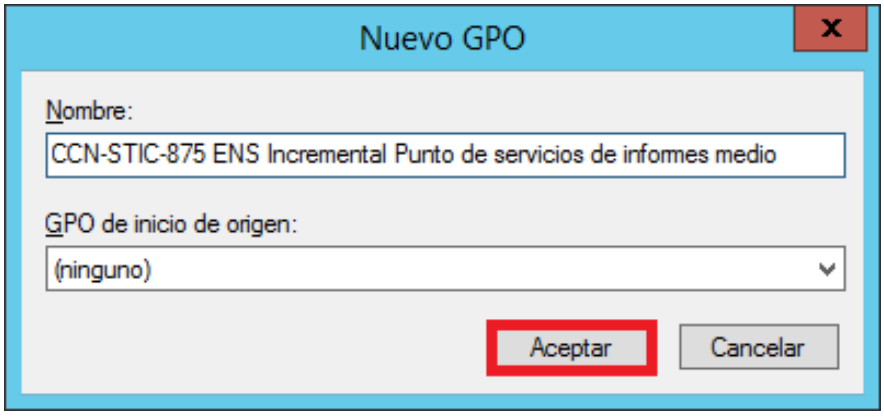
Paso	Descripción
225.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores SQL a la unidad organizativa "Servidores SQL". Para ello, deberá localizar los servidores y hacer clic con el botón derecho sobre "mover" en el servidor que desee ubicar en la nueva unidad organizativa. 
226.	Seleccione la unidad organizativa "Servidores SQL" y pulse "Aceptar". 

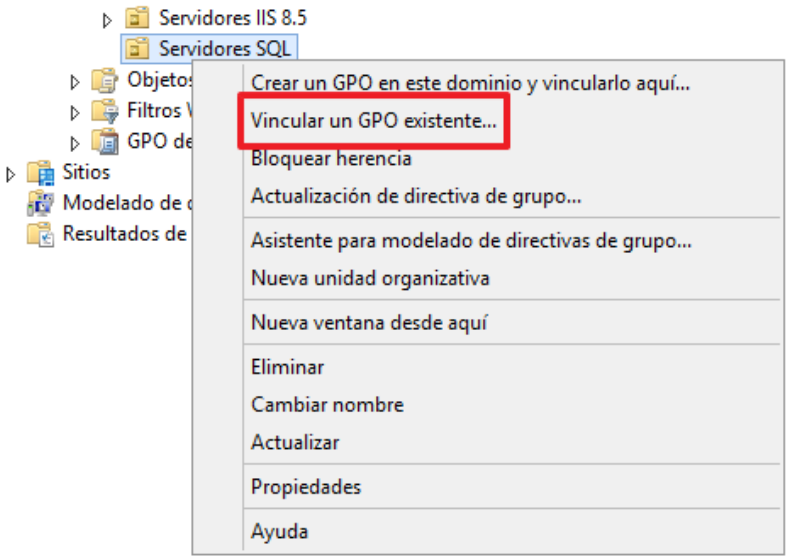
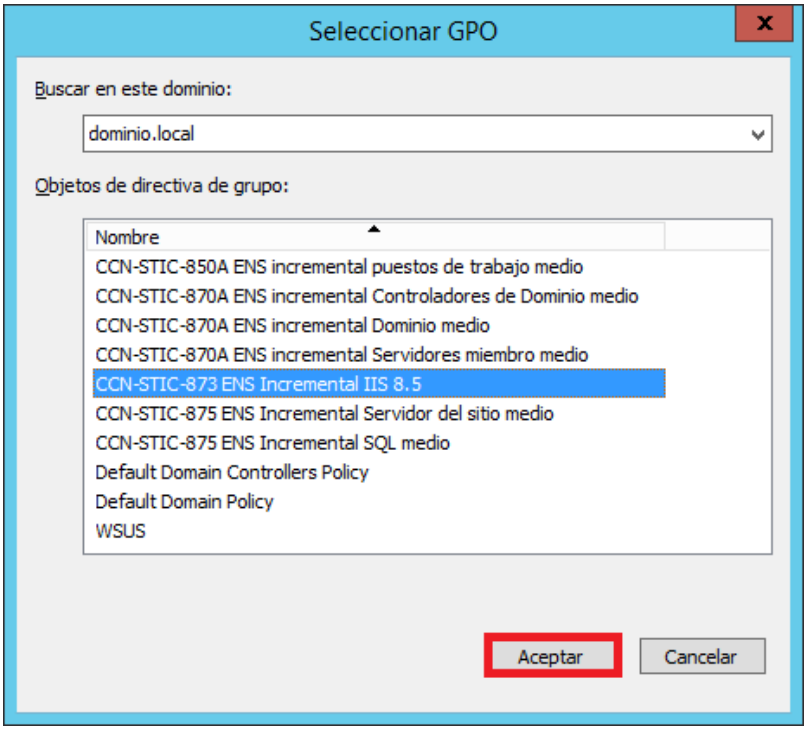
Paso	Descripción
227.	En el siguiente paso, seleccione la unidad organizativa “Servidores SQL”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
228.	Escriba el nombre “GG Servidor Punto de servicios de informes medio” y pulse “Aceptar”. 

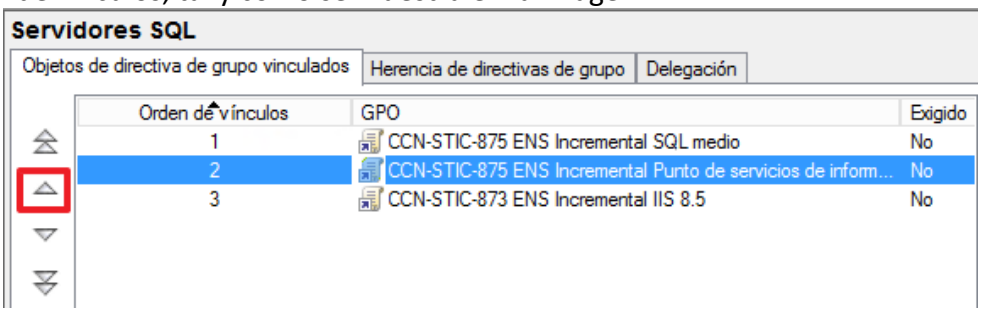
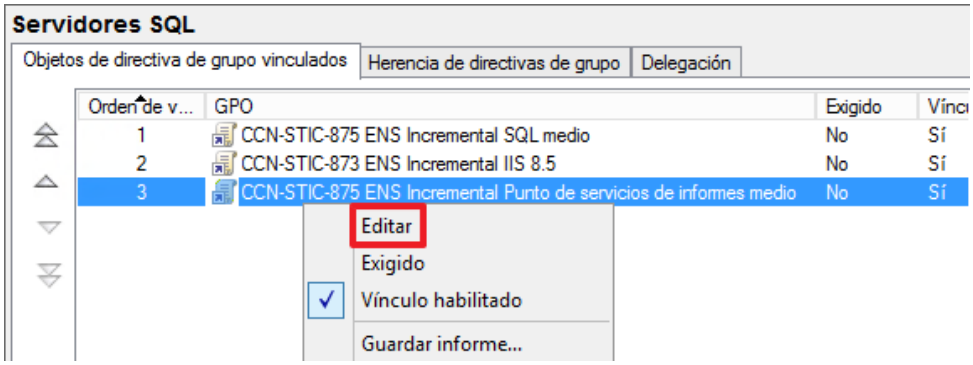
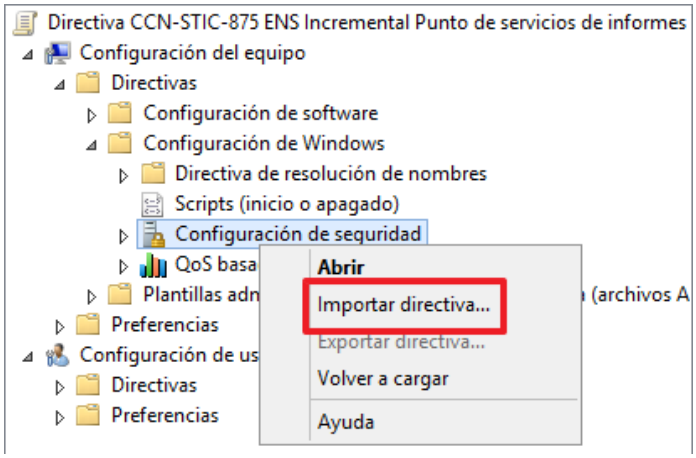
Paso	Descripción
229.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
230.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de Servicios de informes” al grupo. 

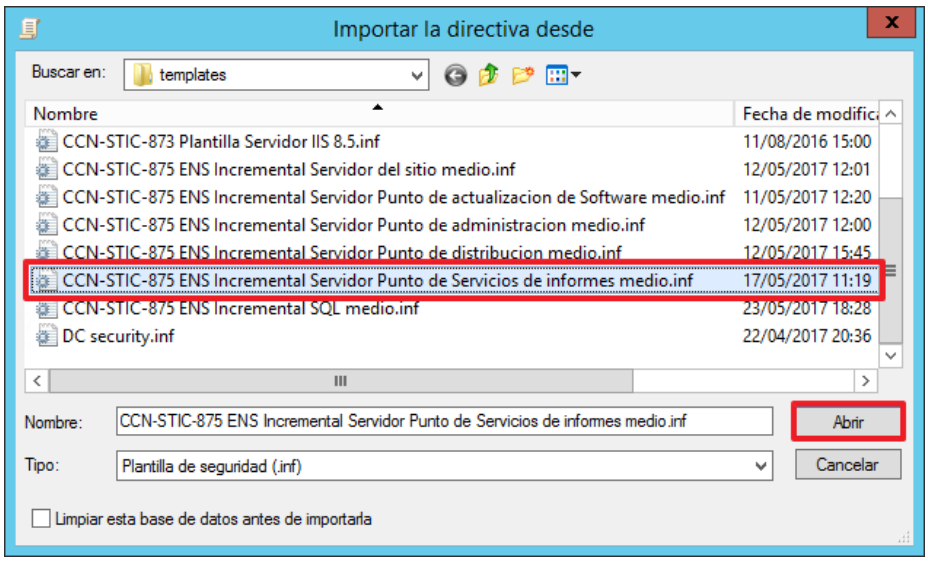
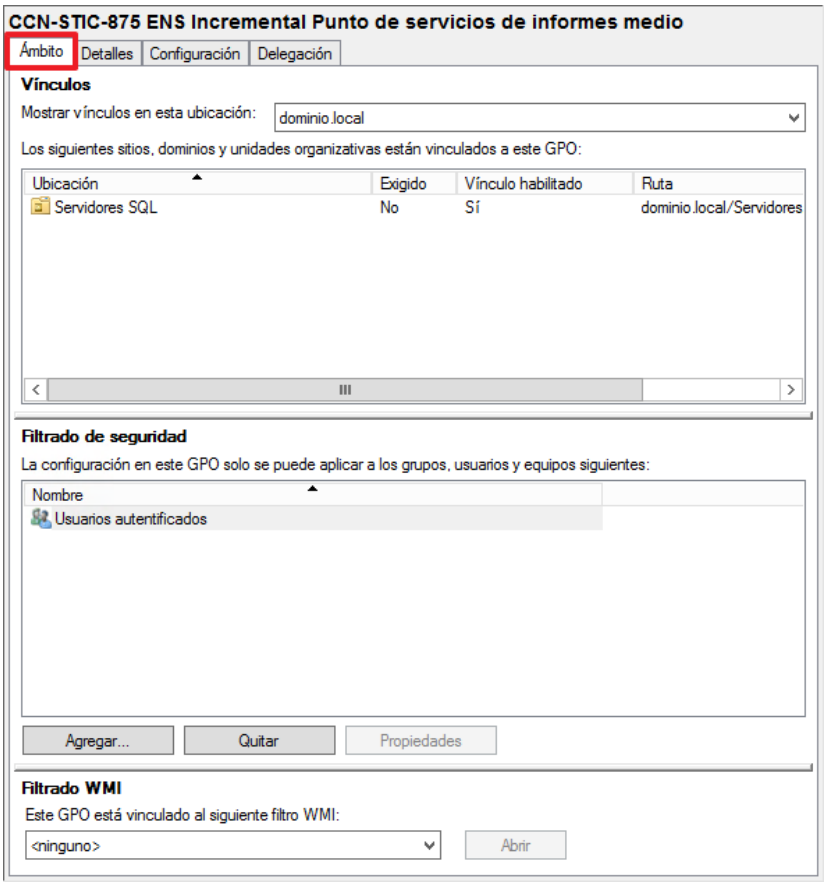
Paso	Descripción
231.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
232.	Deje marcado únicamente el tipo de objeto “Equipos” y pulse “Aceptar”. 
233.	Agregue los equipos y pulse sobre “Aceptar”. 

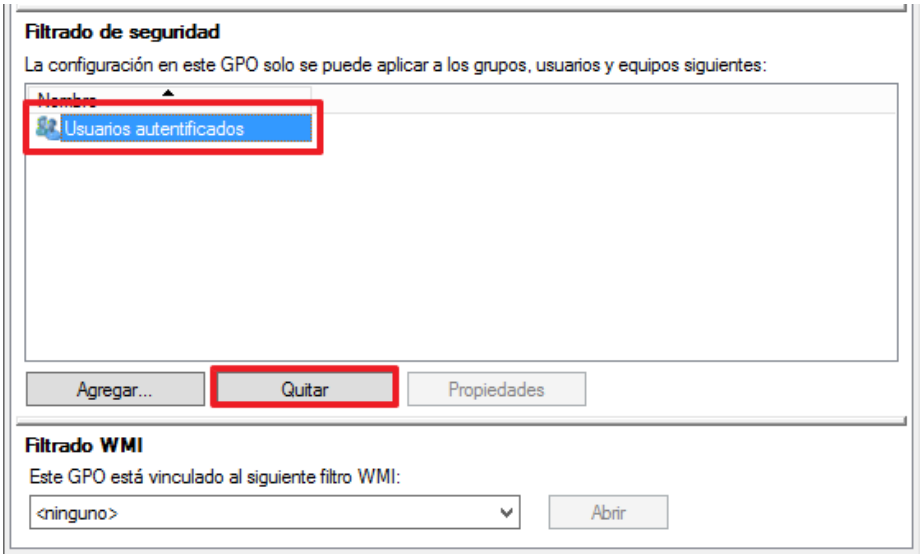
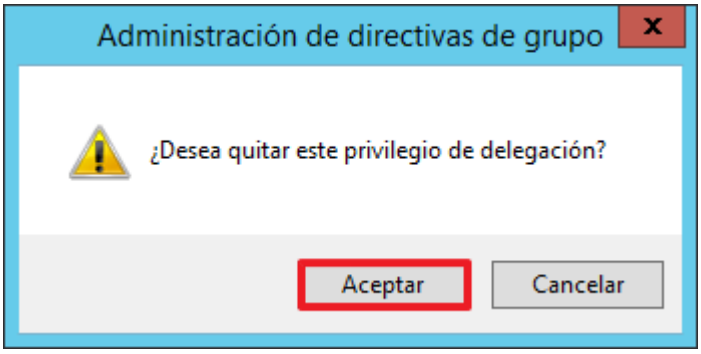
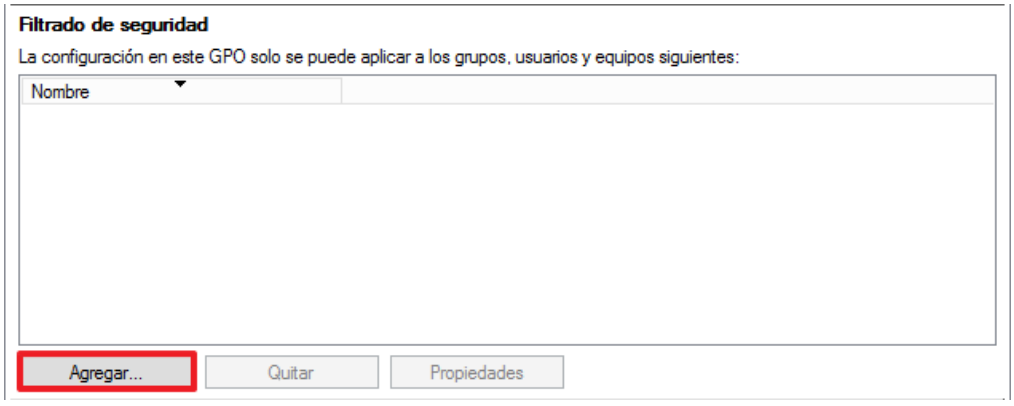
Paso	Descripción
234.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
235.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
236.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

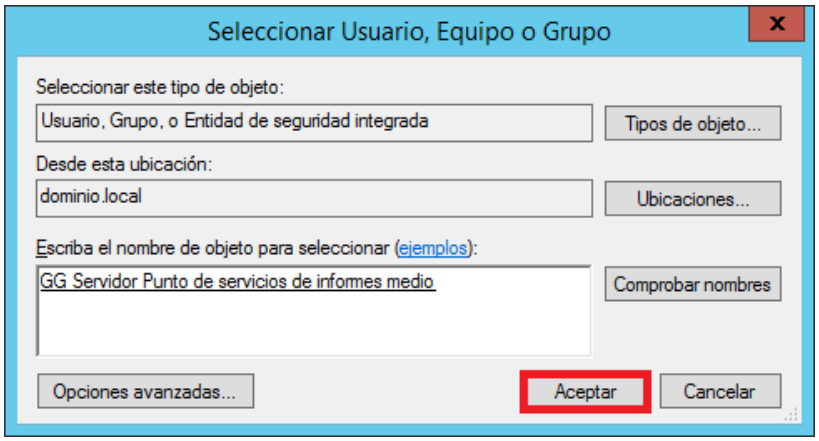
Paso	Descripción
237.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SQL”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”.  **Nota:** Deberá adaptar estos pasos a su organización seleccionando la Unidad Organizativa que aloje los roles en los que está reforzando la seguridad.
238.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de Servicios de Informes medio” y haga clic en el botón “Aceptar”. 
239.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”. En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 244, en caso contrario continúe con el paso a paso.

Paso	Descripción
240.	A continuación, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SQL.
241.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SQL” y haga clic sobre “Vincular un GPO existente…” 
242.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
243.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de Servicios de informes medio" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SQL", la directiva "CCN-STIC-875 ENS Incremental Punto de Servicios de informes medio" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
244.	Edite la GPO: "CCN-STIC-875 ENS Incremental Punto de servicios de informes medio" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
245.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
246.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Punto de servicios de informes medio.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
247.	Cierre el “Editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
248.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

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

Paso	Descripción
252.	Introduzca como nombre “GG Servidor Punto de servicios de informes medio” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
253.	Cierre el “Administrador de directivas de grupo”.

7. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

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

En la presente guía la conexión con el servidor que tiene implementado SCCM se efectúa a través de escritorio remoto, debido a la aplicación de los refuerzos de seguridad que se van a realizar, en caso que los usuarios administrativos solo requieran de acceso para administrar SCCM se recomienda que la conexión se realice a través de la consola de administración de SCCM desde su puesto de trabajo y no mediante escritorio remoto, evitando con ello otorgar más permisos de los estrictamente necesarios.

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

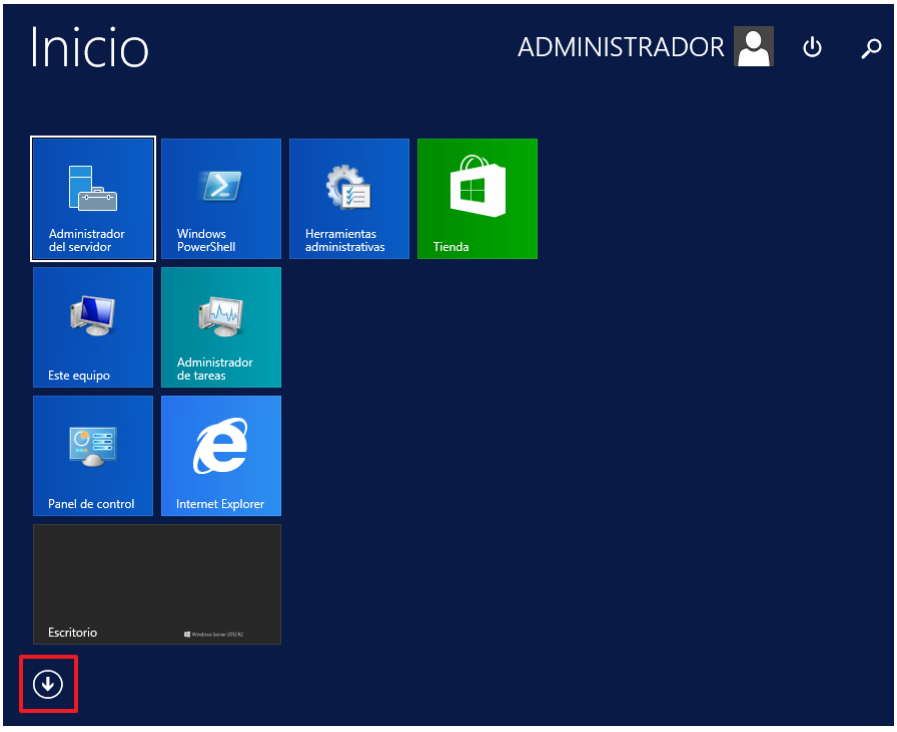
Nota: Todas las recomendaciones de seguridad indicadas en la presente guía deben ser adaptadas al entorno de su organización. Se aconseja realizar las pruebas pertinentes en un entorno de preproducción antes de ser incluidas en su entorno de producción.

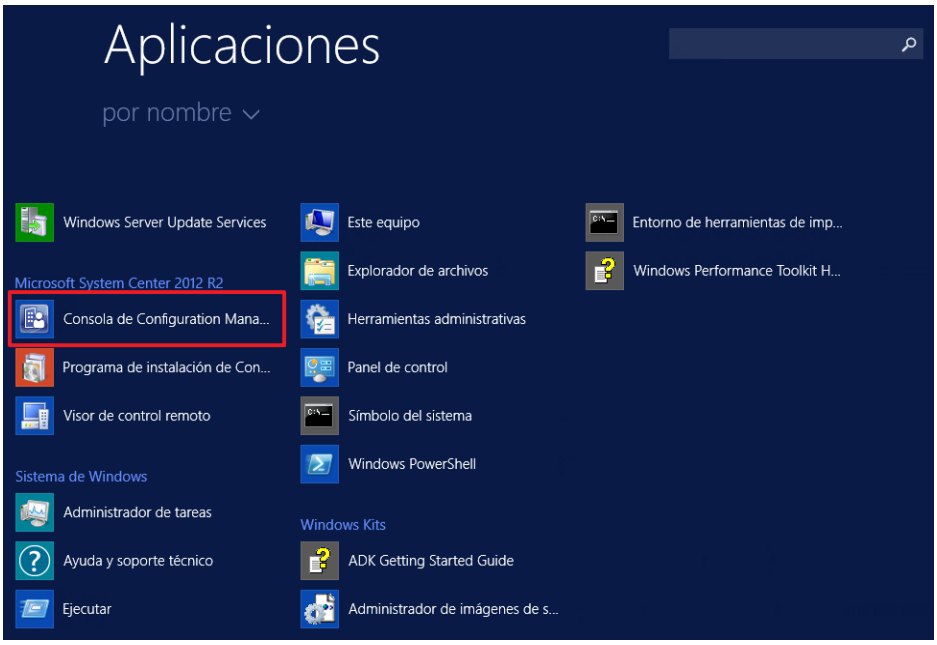
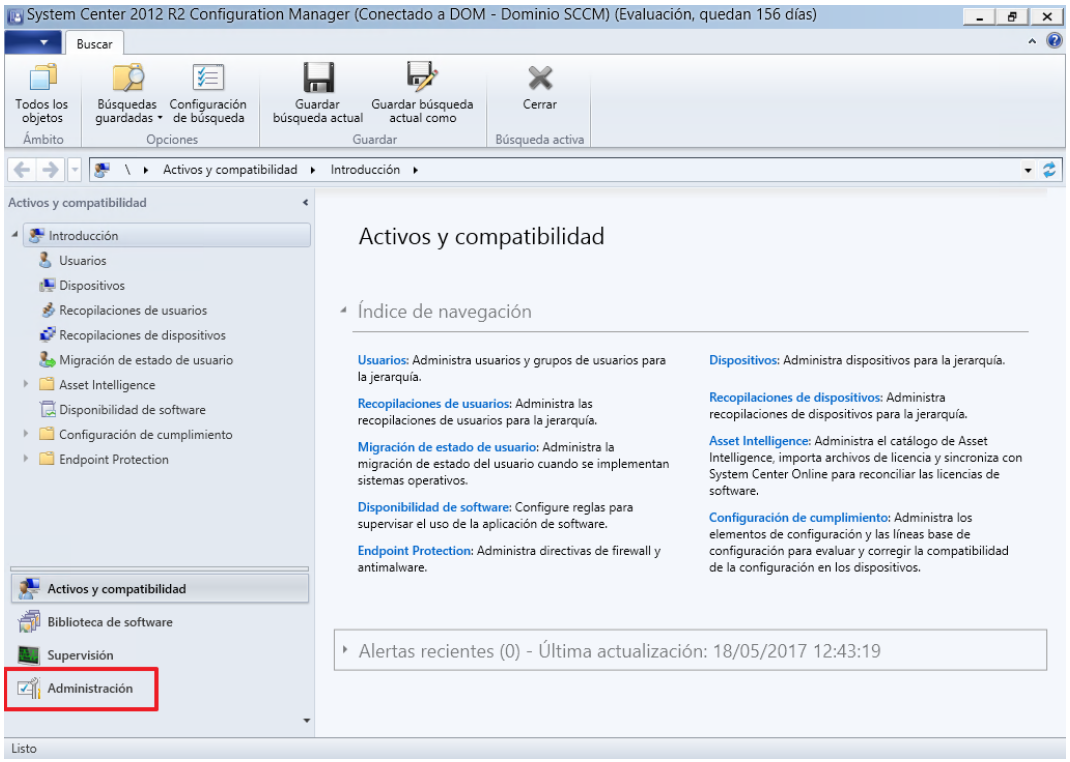
7.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

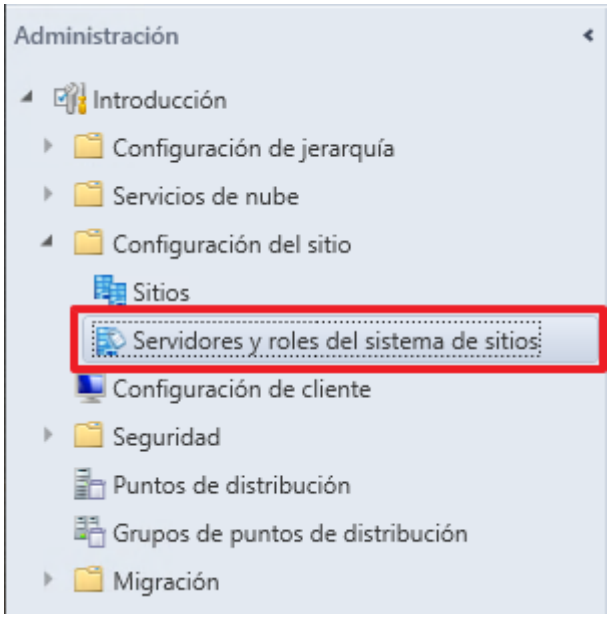
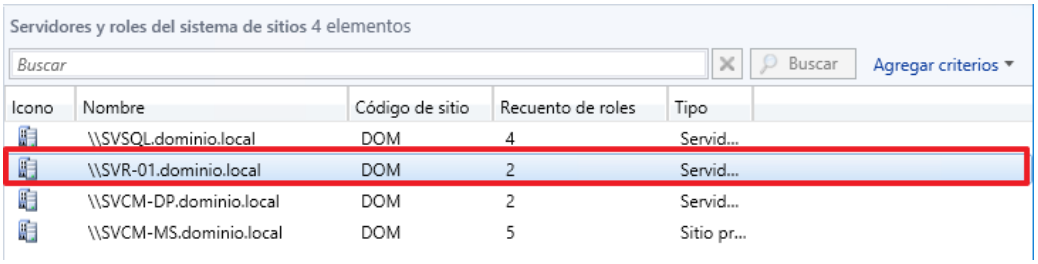
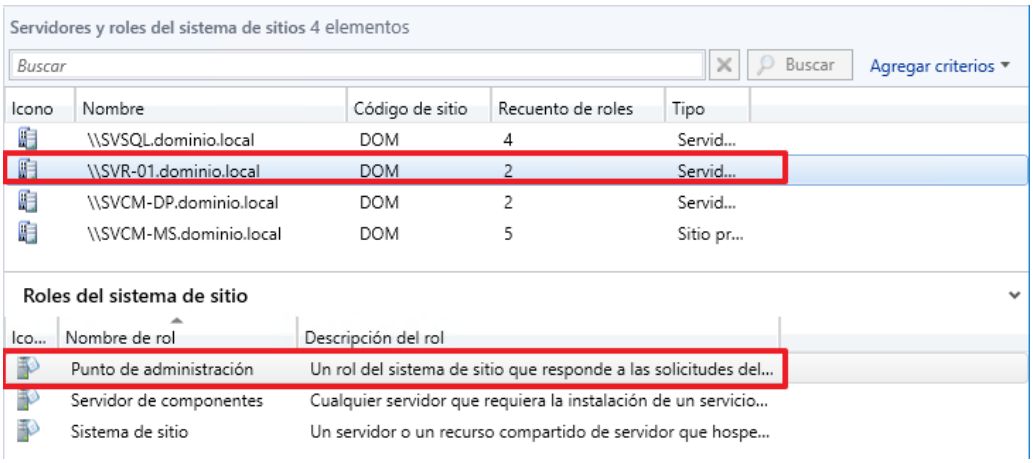
Uno de los aspectos que marca el ENS, desde su requisito de nivel bajo en el Marco Operacional, es la mínima funcionalidad y mínima exposición evitando con ello posibles vulnerabilidades minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

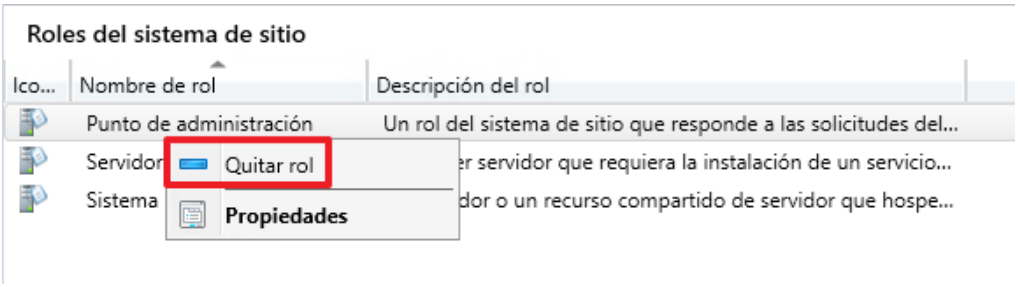
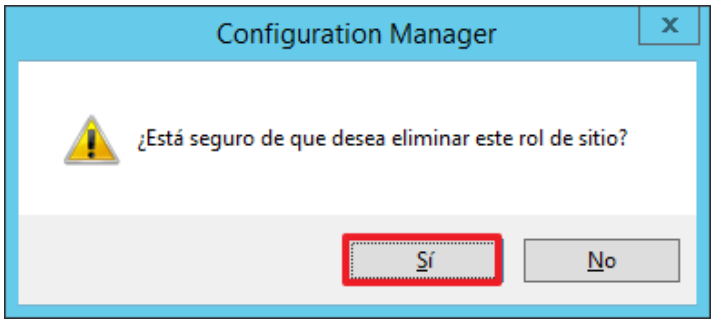
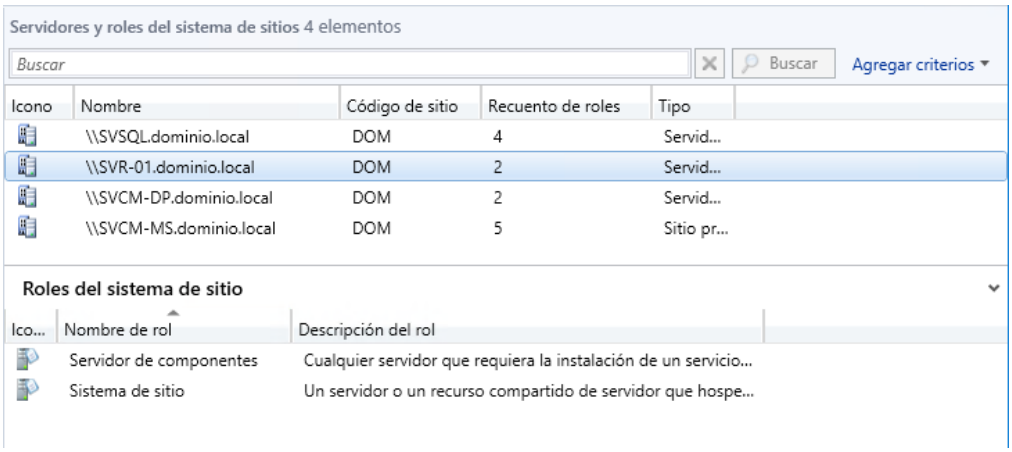
Microsoft SCCM 2012 R2 permite el añadir o quitar roles en los servidores función de la tarea a desempeñar por el servidor, por ejemplo, un servidor destinado únicamente a la distribución de paquetes, el cual tiene instalado el rol de punto de distribución, no es necesario que tenga otro rol para el cual el servidor no está destinado.

Seguidamente, se muestra un ejemplo de cómo desinstalar un rol específico implementado en un servidor. El siguiente paso a paso da por hecho que ya instalado previamente un rol y que por necesidades de la organización dicho rol se ha de desinstalar del servidor, aplicando con ello el principio de mínima funcionalidad quitando características que ya no son necesarias de un servidor de su organización.

Paso	Descripción
254.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
255.	Pulse sobre el menú inicio. 
256.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
257.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
258.	Seleccione el apartado “Administración”. 

Paso	Descripción
259.	Despliegue "**Configuración del sitio > Servidores y roles del sistema de sitios**". 
260.	Marque en el menú derecho el servidor del que quiere quitar un rol de sistema de sitios.  **Nota:** Deberá adaptar estos pasos a su organización seleccionando el servidor que contenga implementado el rol que desea quitar.
261.	En este ejemplo se va a quitar el rol de "Punto de administración" el cual ha sido implementado previamente. Asegúrese que selecciona el servidor correcto y en la parte inferior seleccione el rol que desea desinstalar. 

Paso	Descripción
262.	Una vez seleccionado el rol que desea quitar, pulse con el botón derecho y seleccione la opción “Quitar rol” del menú contextual. 
263.	Pulse “Sí” sobre la advertencia que aparece cuando está intentando quitar el rol. 
264.	Verifique que ha quitado el rol correctamente. 

7.2. SEGREGACIÓN DE ROLES Y FUNCIONES

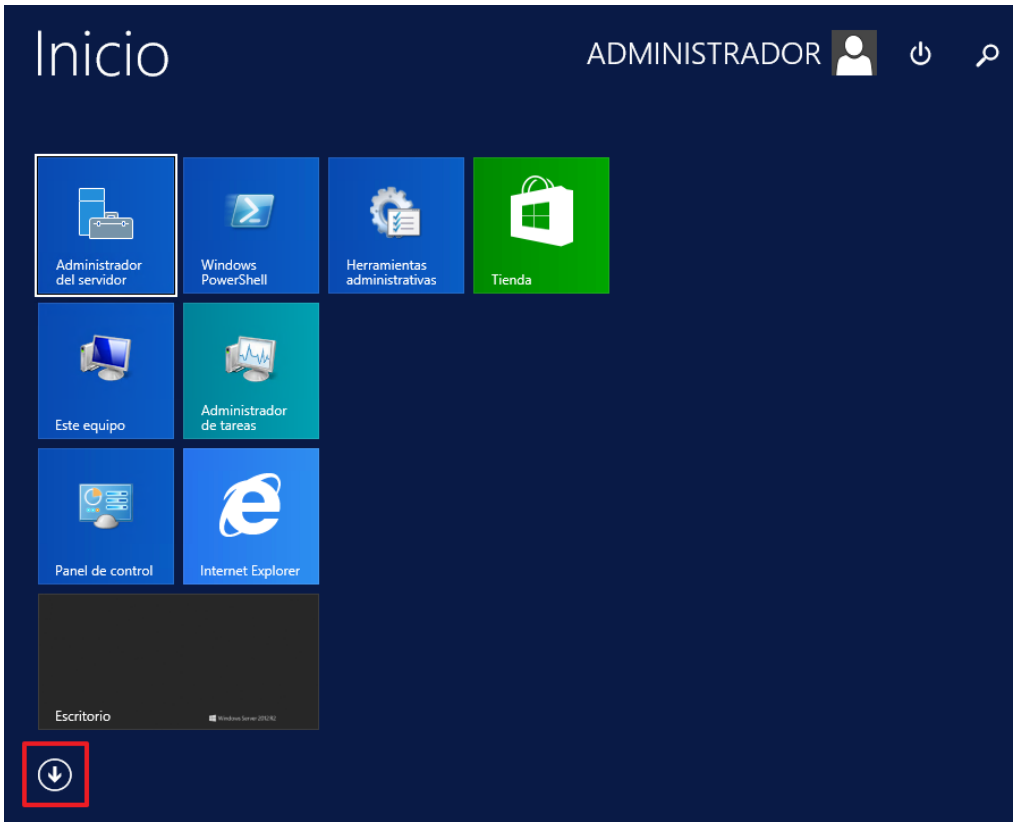
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y a la aplicación de directivas sobre dichos grupos.

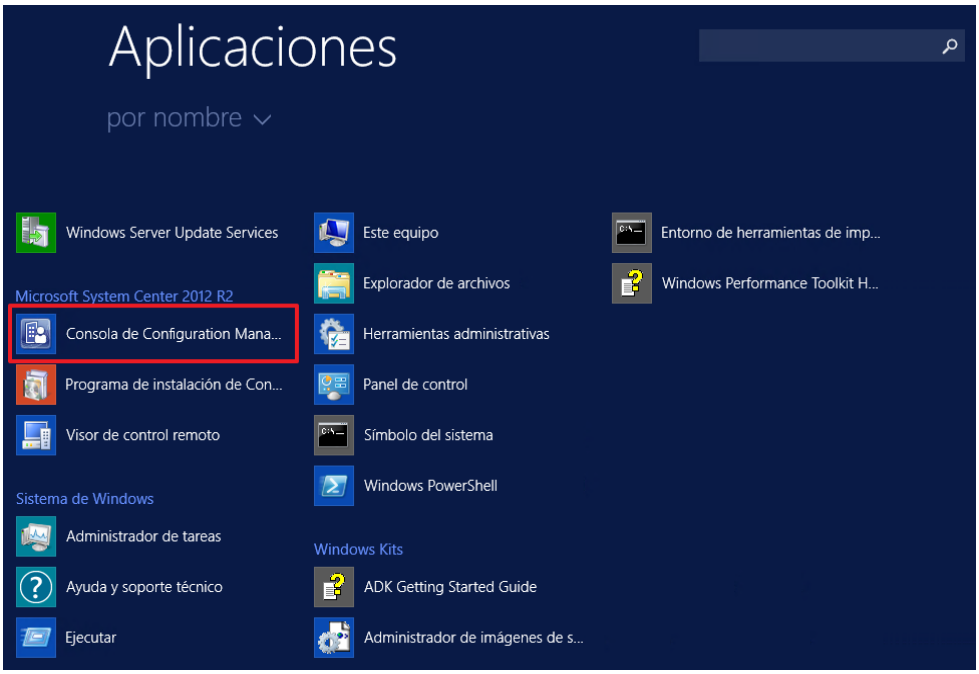
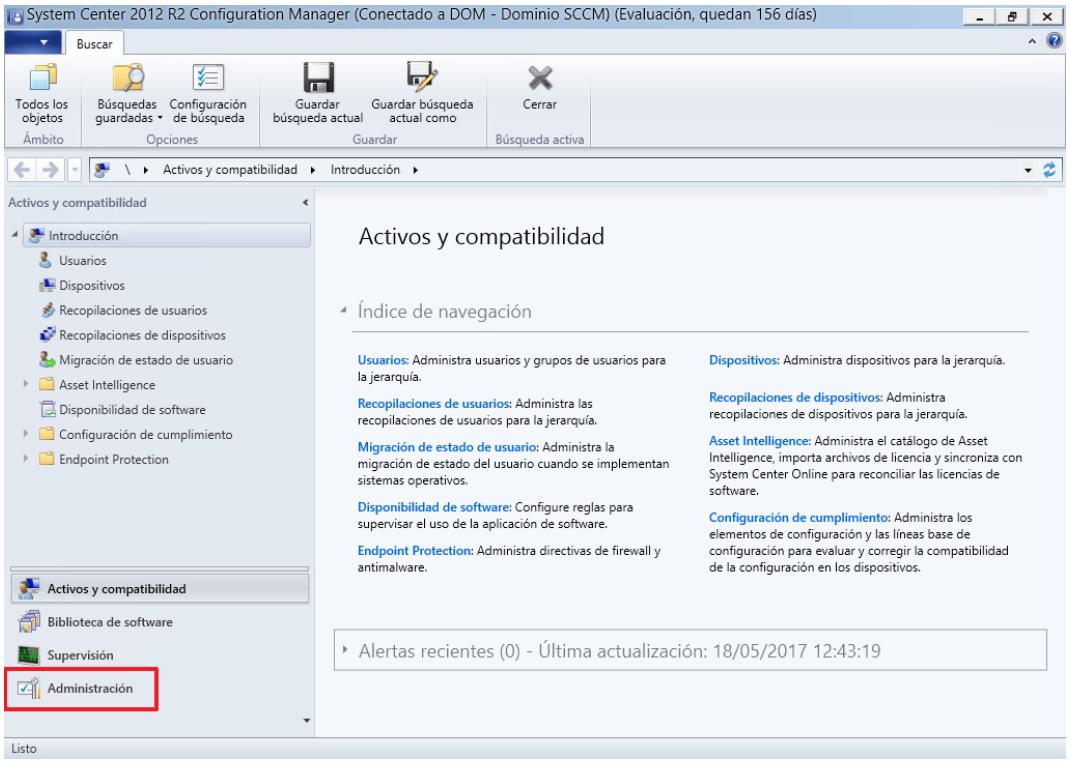
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración, a la vez que otros pueden asumir la funcionalidad de auditores.

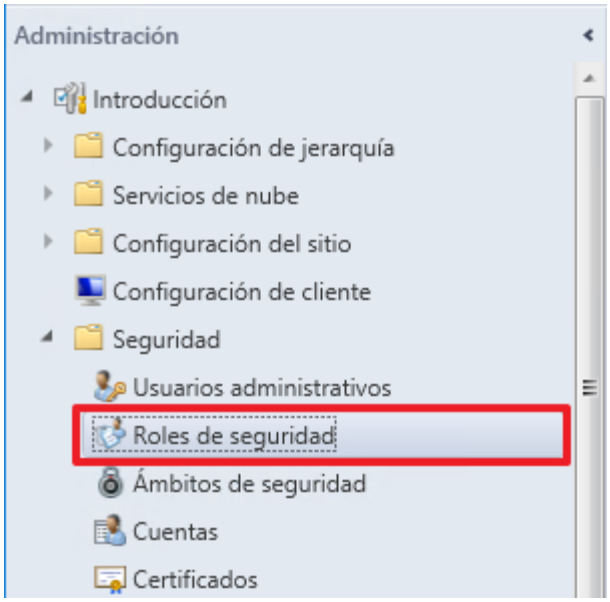
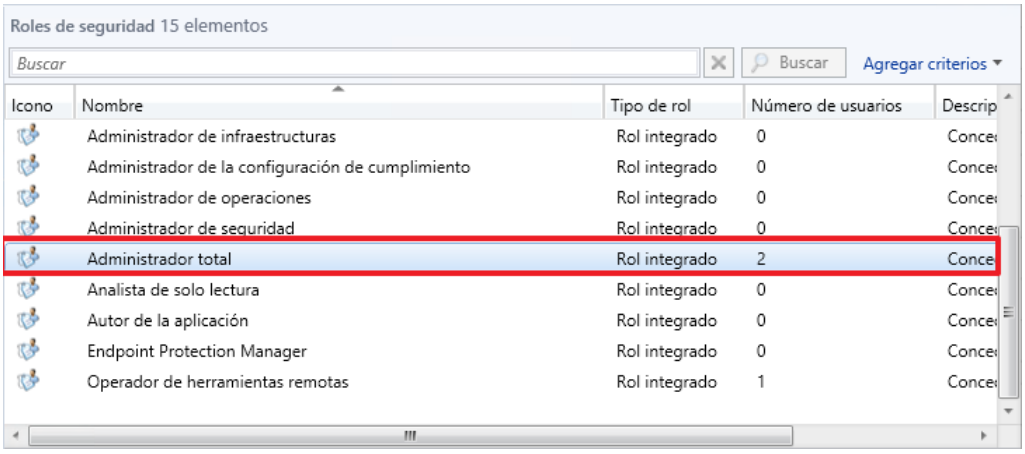
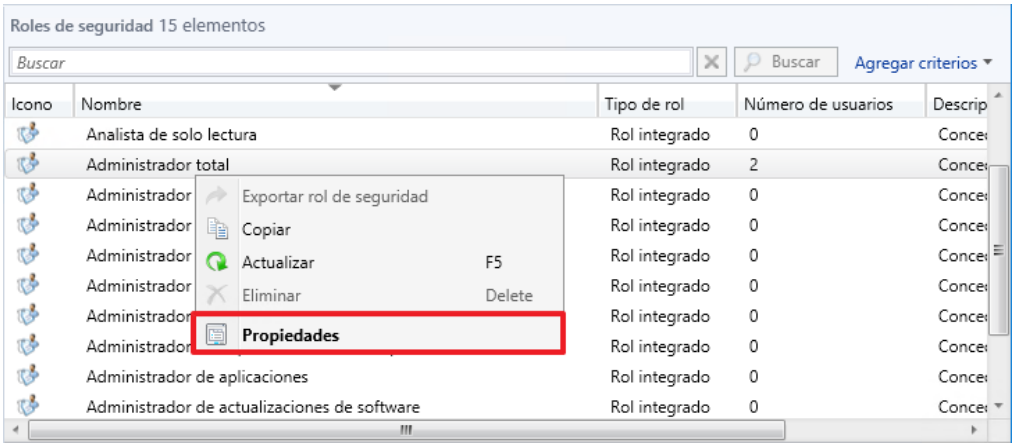
La administración de roles de seguridad y permisos se puede realizar a través de la consola principal de Configuration Manager o bien a través de cmdlets de PowerShell.

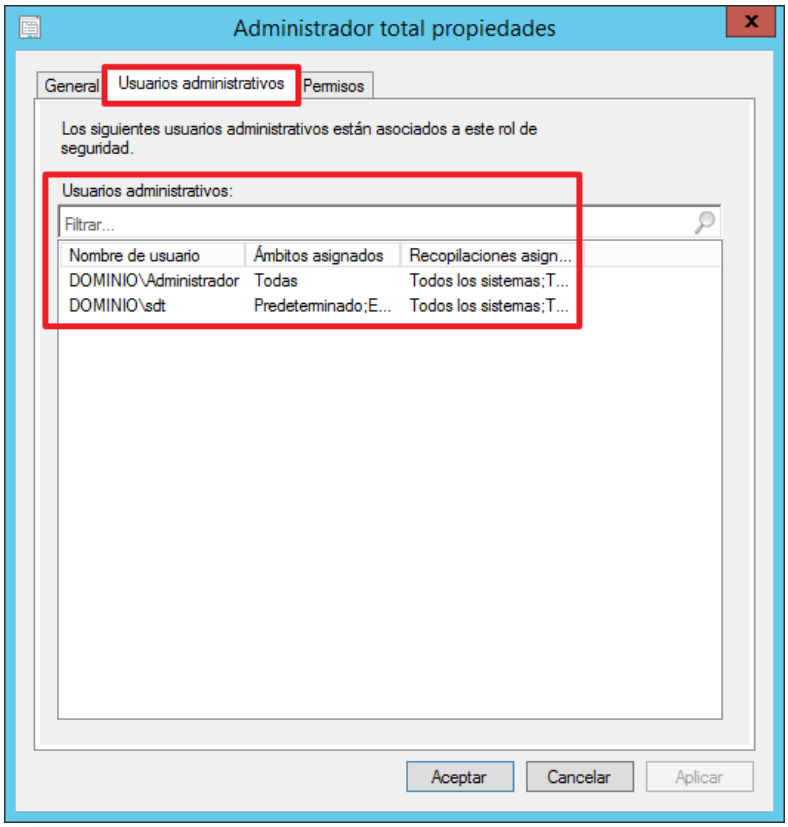
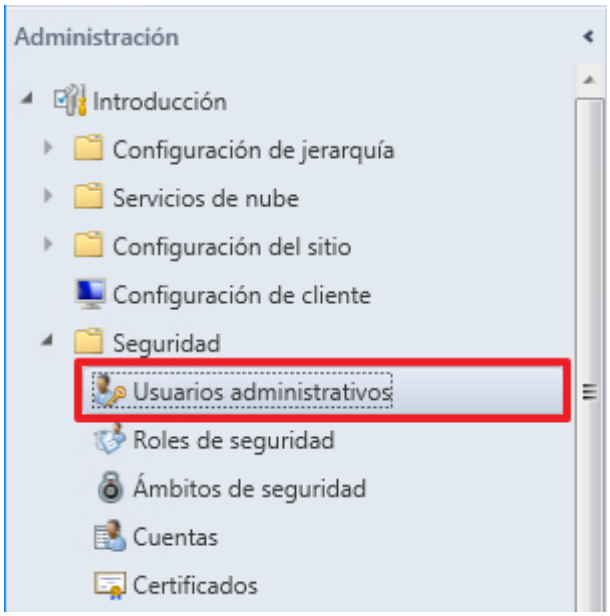
A continuación, se muestra un ejemplo de cómo comprobar los roles de seguridad que tiene asignado un usuario al igual que el procedimiento para asignar un rol de seguridad concreto a un usuario determinado.

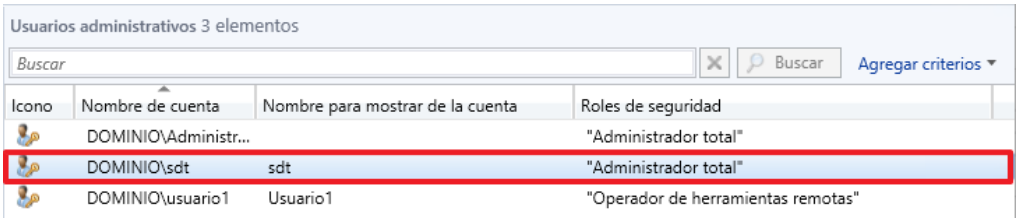
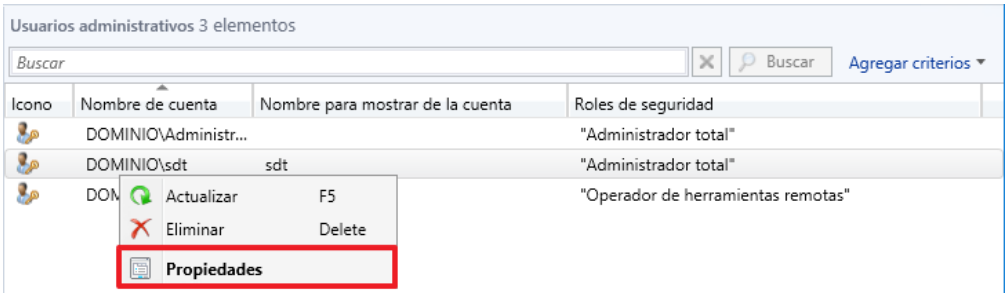
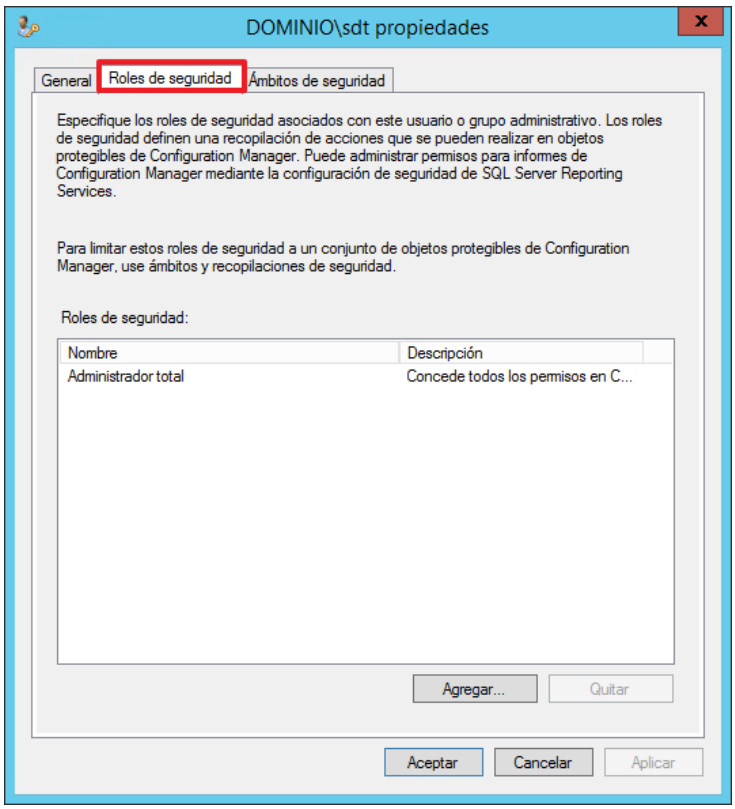
Nota: Si desea crear más información sobre la administración de roles y permisos visite la siguiente web: https://technet.microsoft.com/en-us/library/gg682106.aspx.

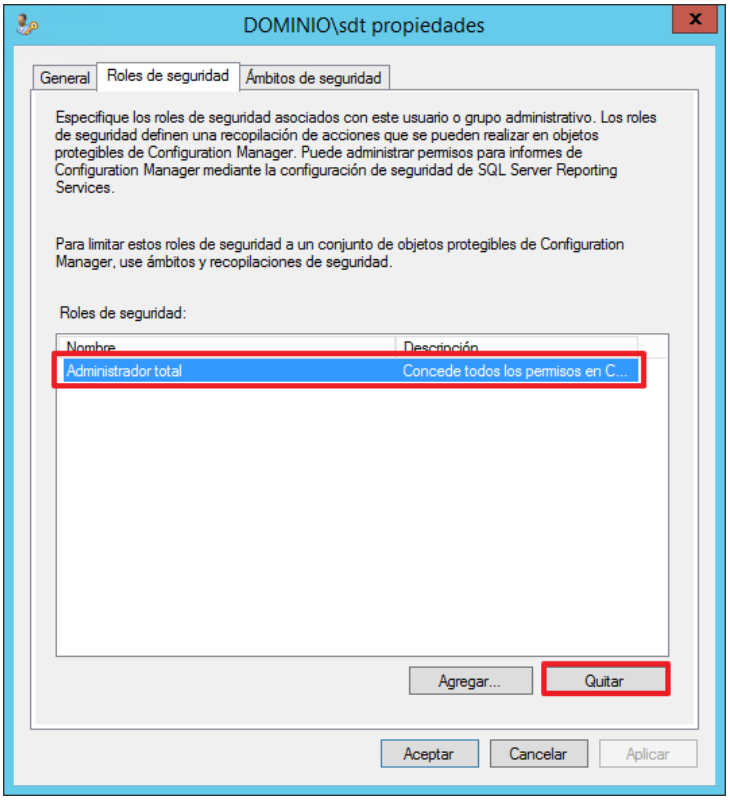
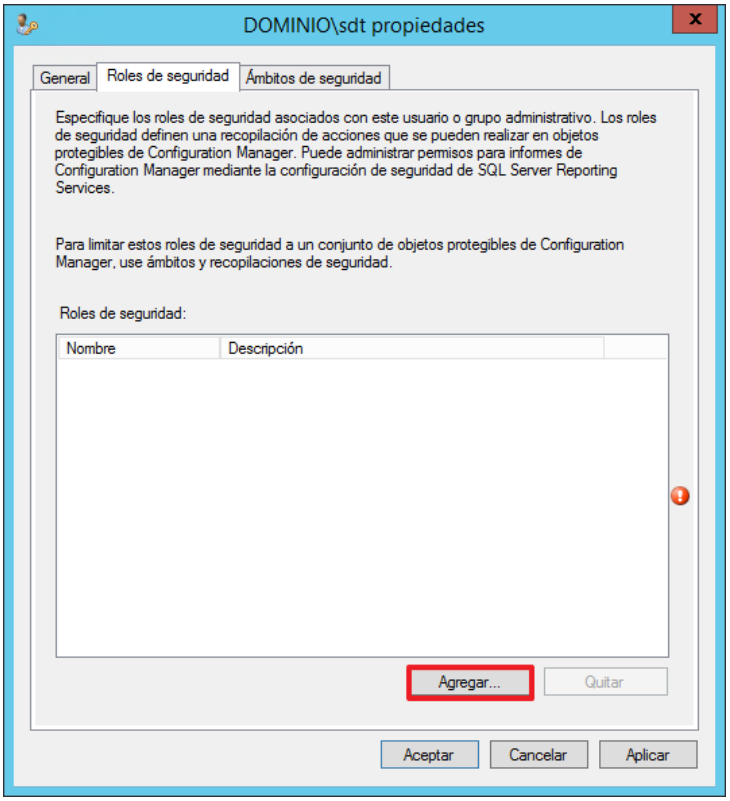
Paso	Descripción
265.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
266.	Pulse sobre el menú inicio. 
267.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

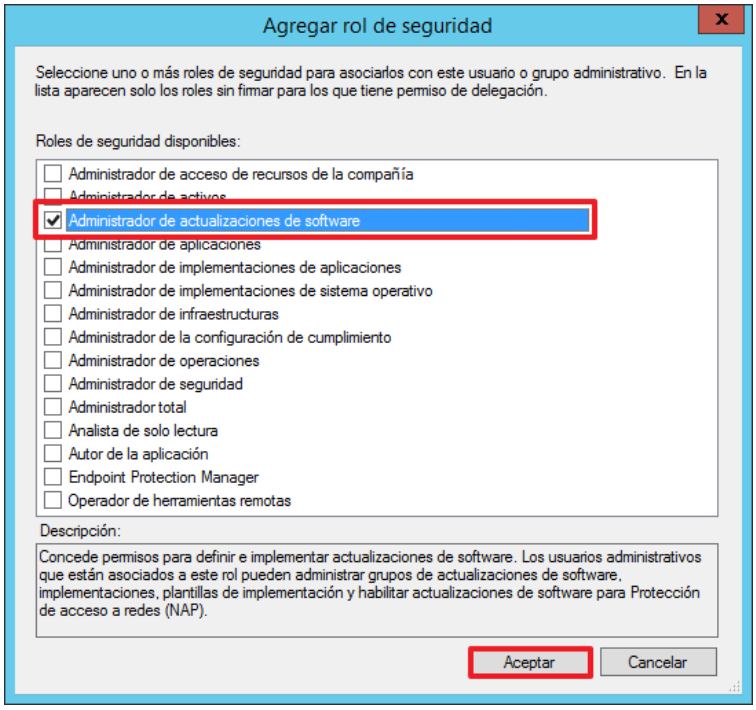
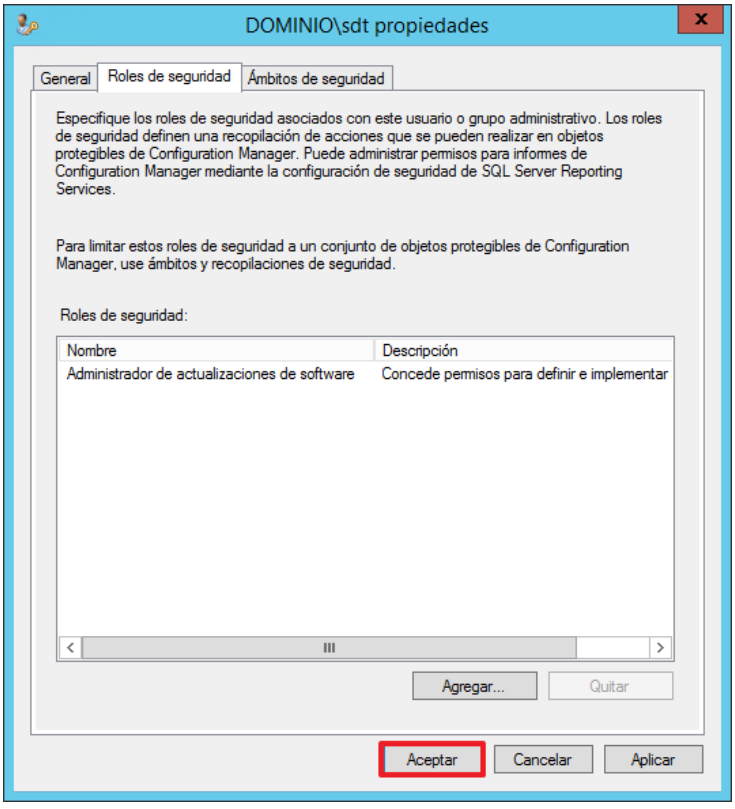
Paso	Descripción
268.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
269.	Seleccione el apartado “Administración”. 

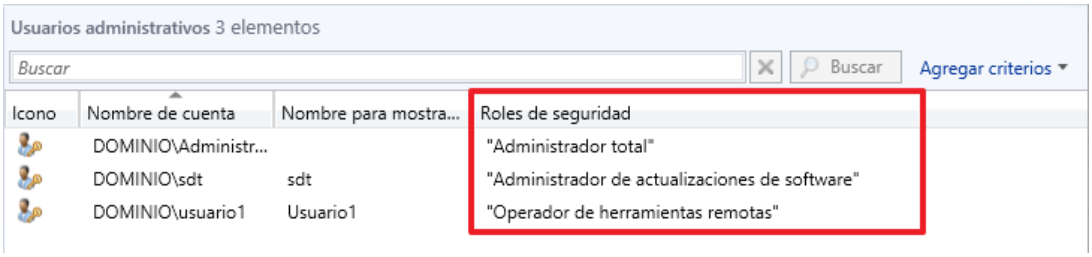
Paso	Descripción
270.	Despliegue “**Seguridad > Roles de seguridad**”. 
271.	Localice el rol de seguridad “Administrador total”. 
272.	Una vez seleccionado el rol de seguridad “Administrador total”, pulse con el botón derecho y marque la opción “Propiedades” del menú contextual. 

Paso	Descripción
273.	Seleccione la pestaña “Usuarios administrativos” y compruebe que los usuarios administrativos que aparecen son correctos ya que el rol de “Administrador total” concede todos los permisos en Configuration Manager. Una vez finalizada la comprobación pulse “Aceptar” para cerrar la ventana. 
274.	En el caso que requiera quitar el rol de seguridad “Administrador total” de un usuario y agregarle otro rol de seguridad deberá seleccionar la pestaña “Usuarios administrativos”. 

Paso	Descripción
275.	Localice el usuario administrativo que desea cambiar la configuración de roles de seguridad.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización. La presente guía no detalla como añadir usuarios administrativos a la consola de Configuration Manager.
276.	Una vez seleccionado el usuario al cual quiere modificar los roles de seguridad, pulse con el botón derecho y marque la opción “Propiedades” del menú contextual. 
277.	Seleccione la pestaña “Roles de seguridad”. 

Paso	Descripción
278.	Seleccione el rol que desea quitar y pulse sobre el botón “Quitar”. 
279.	Seleccione “Agregar” para añadir el rol de seguridad que desee aplicar sobre el usuario seleccionado anteriormente. 

Paso	Descripción
280.	Seleccione el rol que desea asignar y pulse “Aceptar”.  **Nota:** En este ejemplo se agrega el rol de seguridad “Administrador de actualizaciones de software”, deberá adaptar estos pasos a sus requerimientos.
281.	Pulse sobre “Aceptar” para confirmar la configuración y cerrar la ventana de propiedades del usuario. 

Paso	Descripción
282.	Es posible comprobar el rol asignado a un usuario desde la propia ventana de "usuarios administrativos.  **Nota:** Es posible que un usuario tenga varios roles de seguridad, pero en la presente guía no se contempla esta casuística.

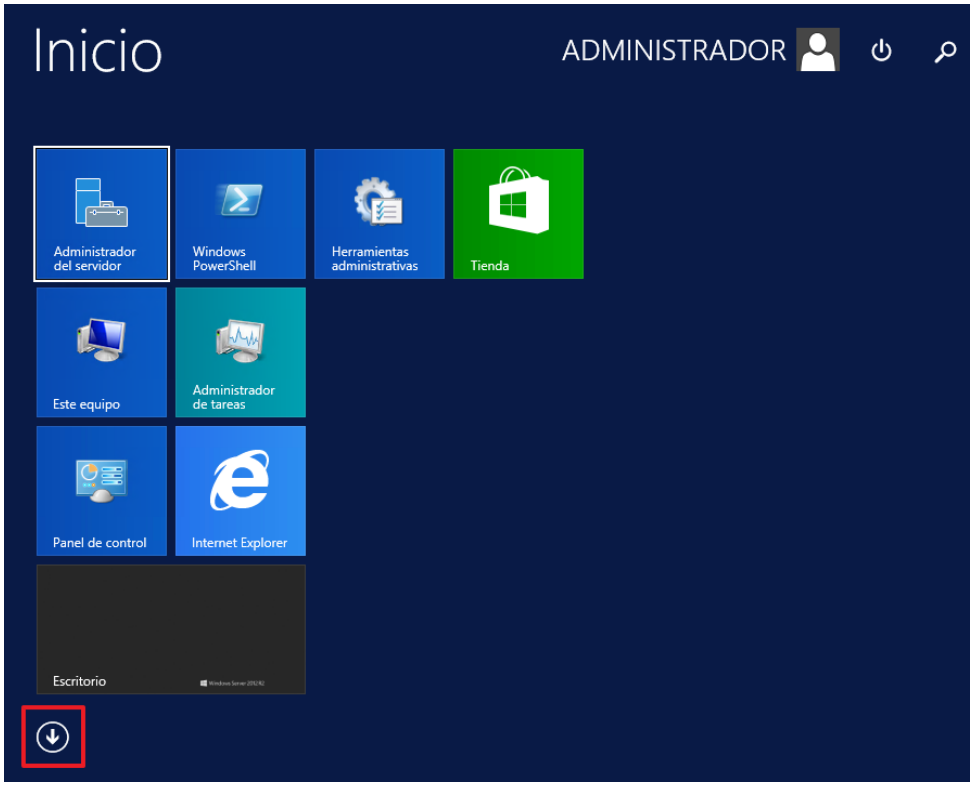
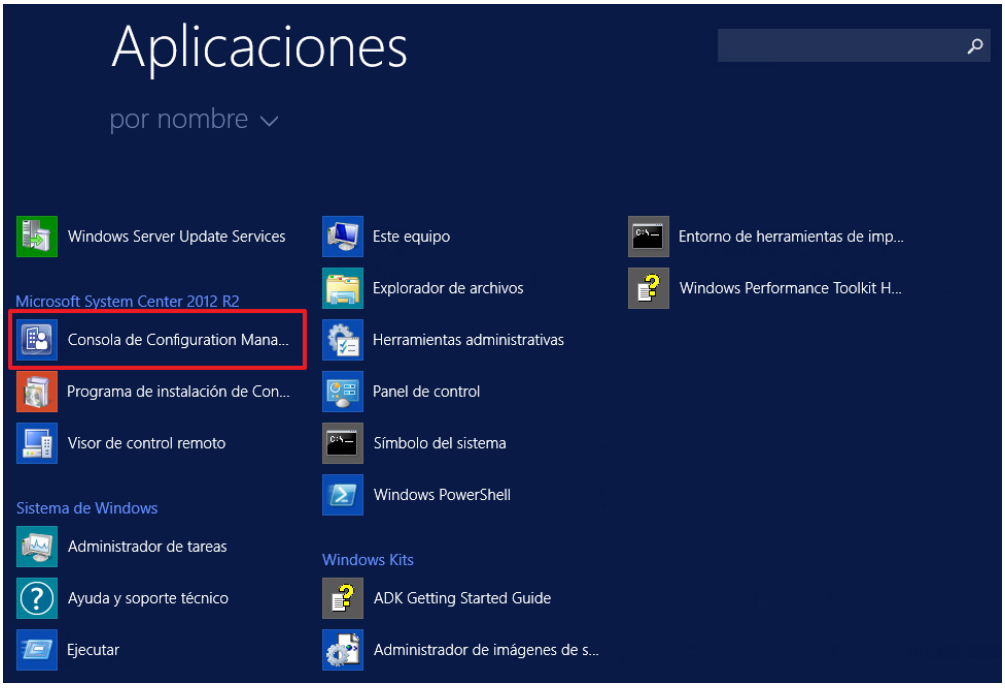
7.3. GESTIÓN DE DERECHOS DE ACCESO

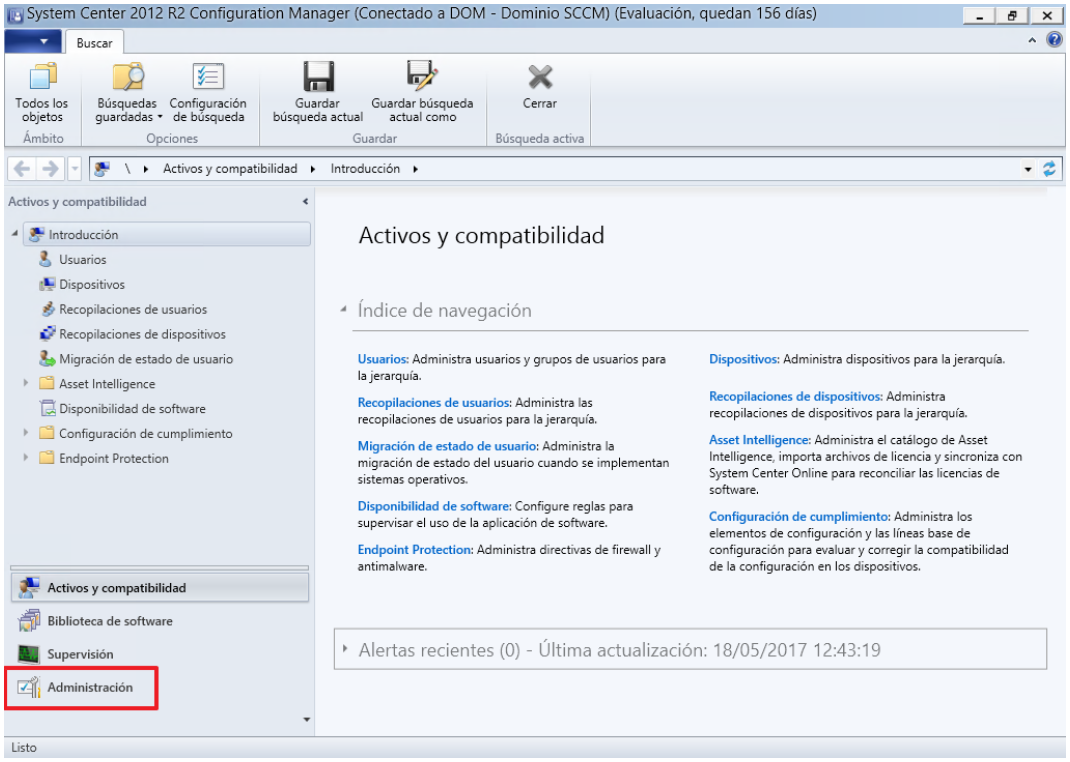
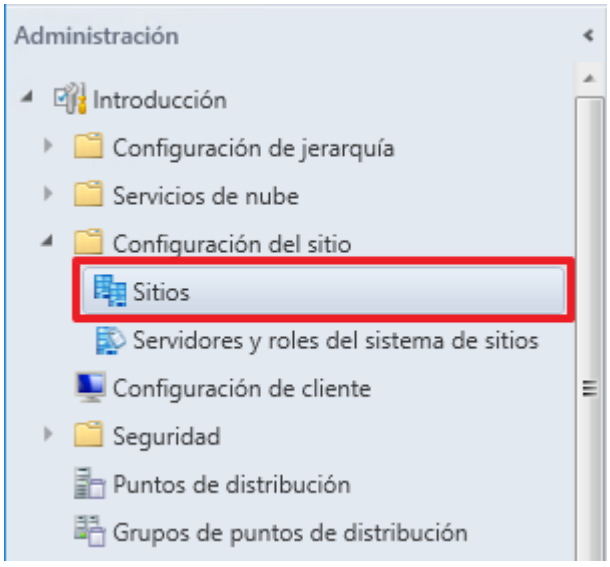
Microsoft SCCM 2012 R2 permite el establecer el método de aprobación de los clientes evitando con ello que equipos cliente no autorizados conecten con SCCM.

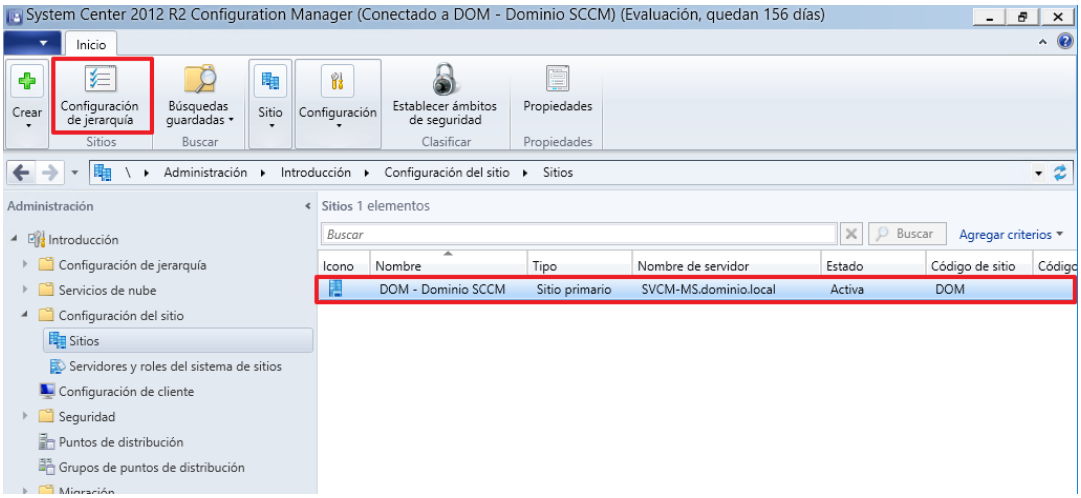
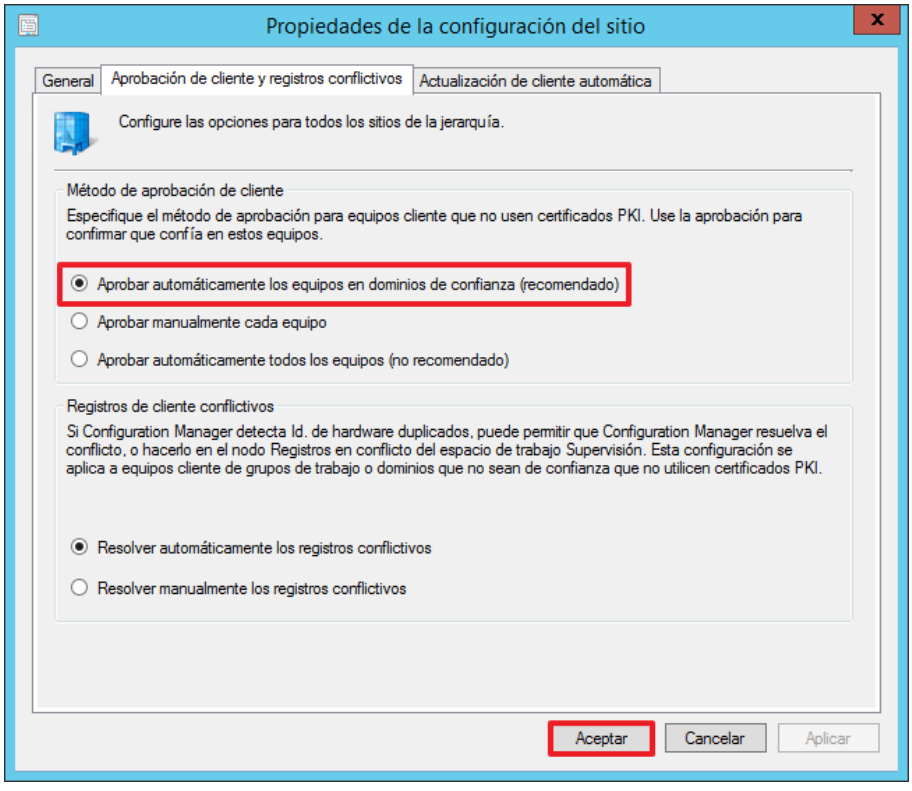
Para los niveles de seguridad medio y alto del ENS se recomienda que el derecho de acceso de los equipos cliente de MS SCCM 2012 R2 no se realice de forma automatizada si no que se requiera de la intervención de personal autorizado que permita la conexión del equipo cliente con MS SCCM 2012 R2.

En el proceso siguiente, se describe como establecer la aprobación de clientes en SCCM.

Paso	Descripción
283.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
284.	Pulse sobre el menú inicio. 

Paso	Descripción
285.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
286.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
287.	Seleccione el apartado “Administración”. 
288.	Despliegue “**Configuración del sitio > Sitios**”. 

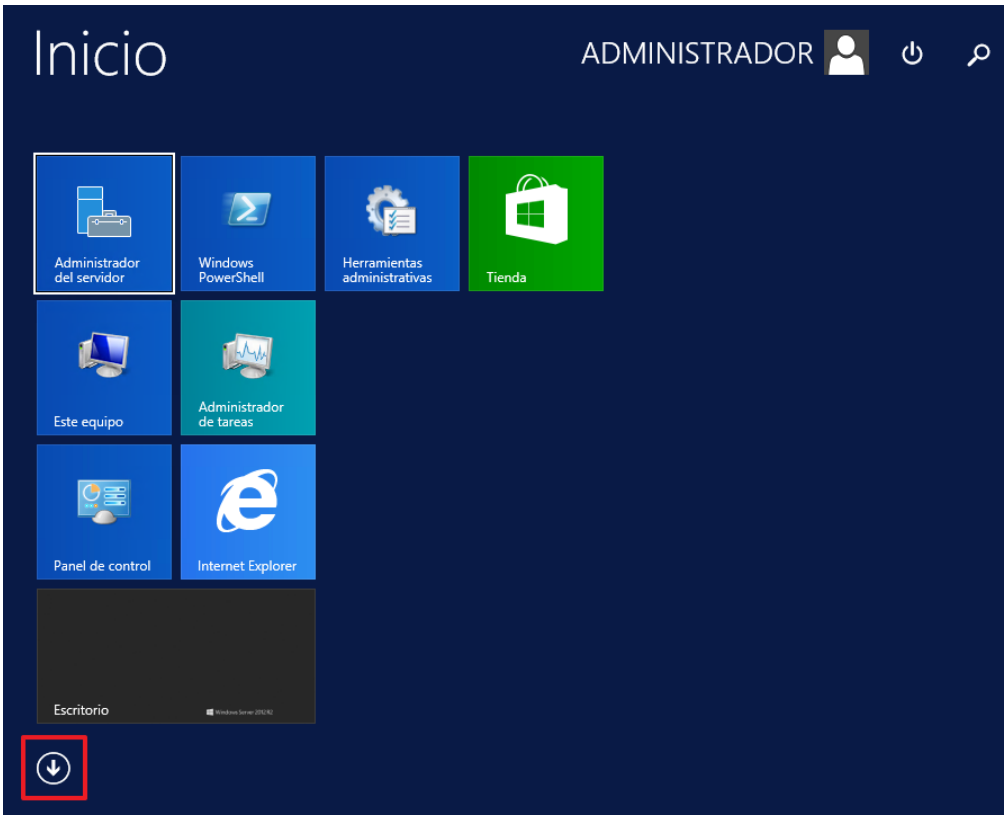
Paso	Descripción
289.	Seleccione el sitio que desea configurar y pulse sobre la opción “Configuración de jerarquía”. 
290.	Localice la pestaña “Aprobación de cliente y registros conflictivos”, marque la opción “**Aprobar automáticamente los equipos en dominio de confianza (recomendado)**” y pulse “**Aceptar**” para validar la configuración. 

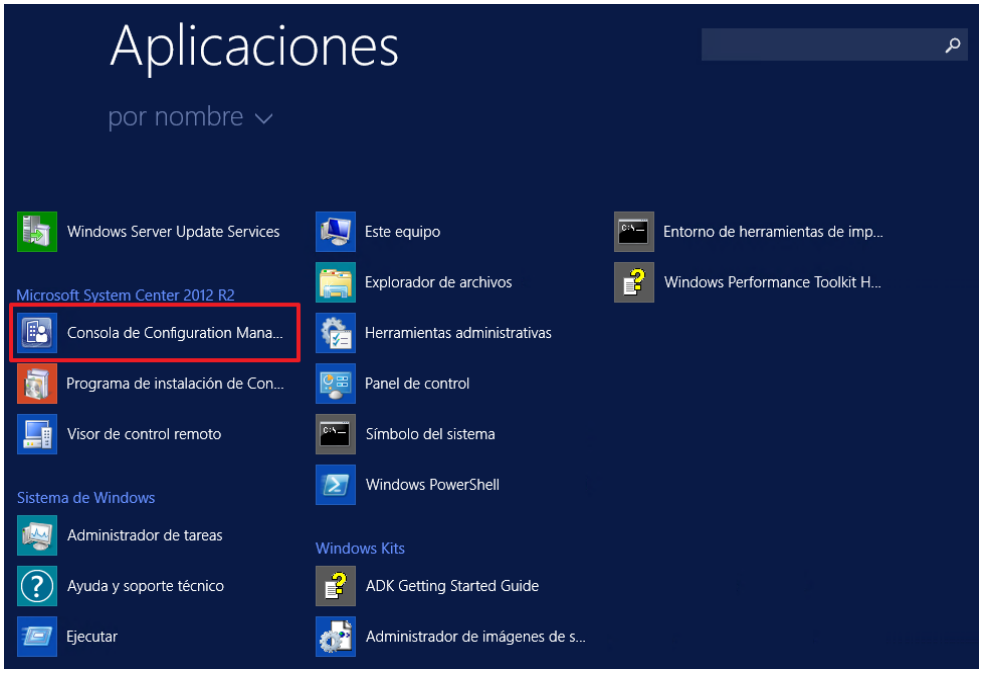
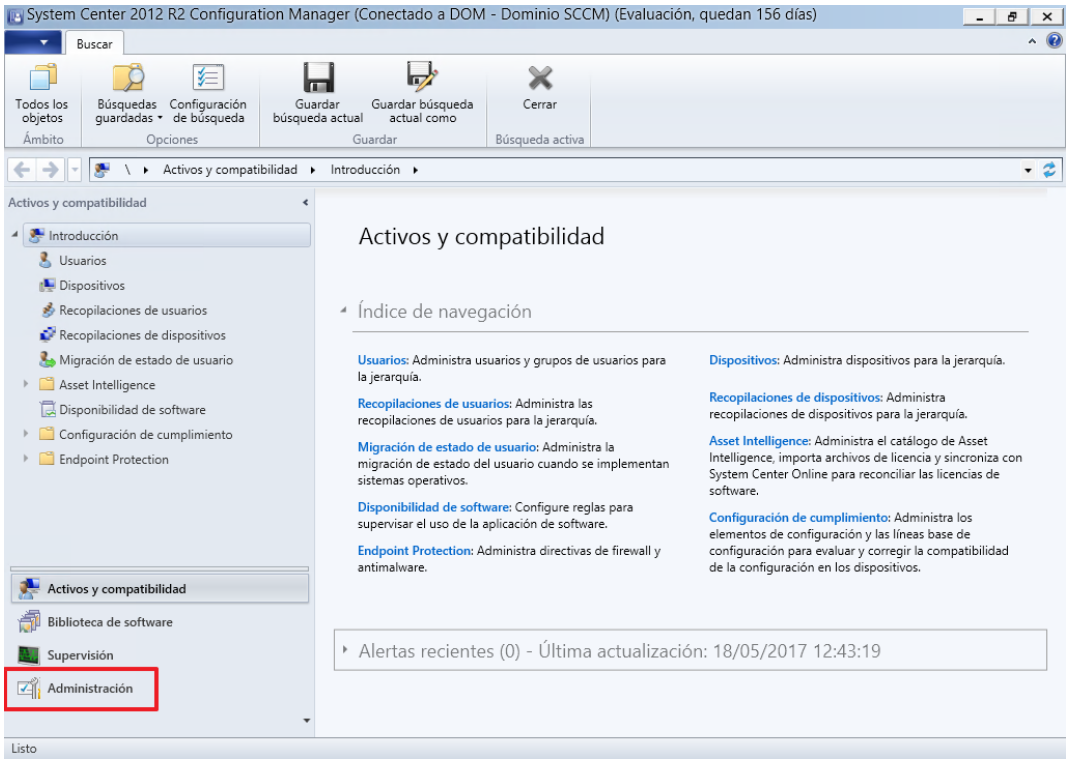
7.4. COMUNICACIÓN CON MS SCCM 2012 R2

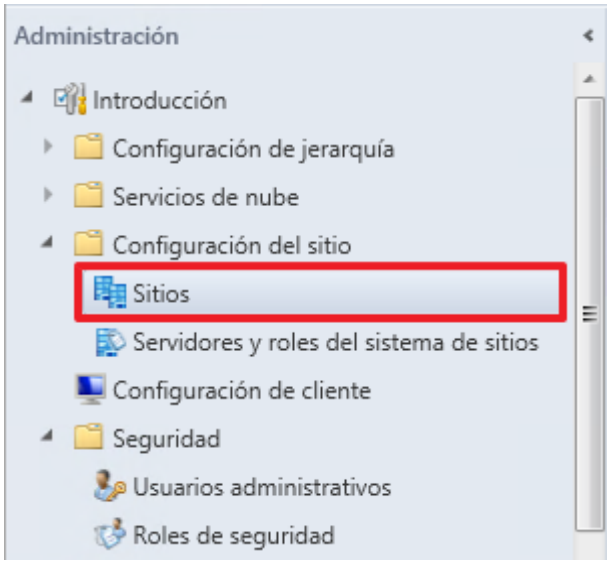
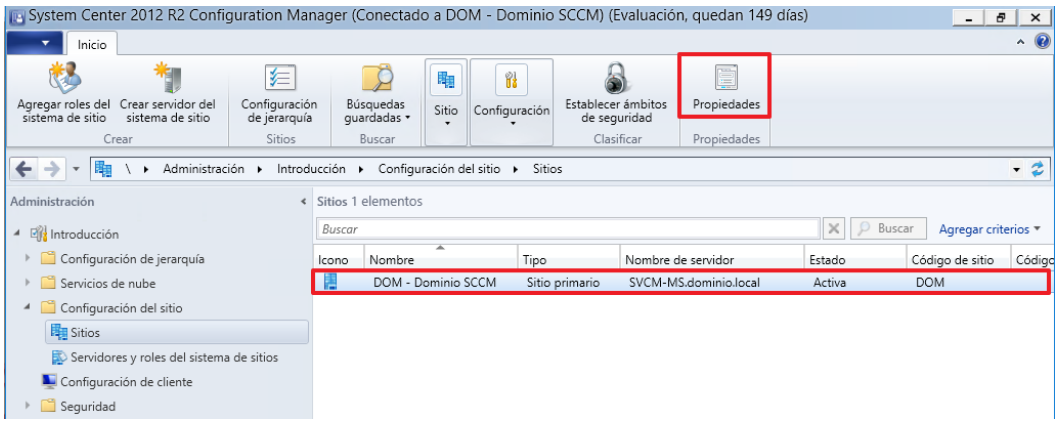
Microsoft SCCM 2012 R2 permite el establecer el método de comunicación de los equipos cliente estableciéndose en función del nivel de seguridad que se establezca en el ENS.

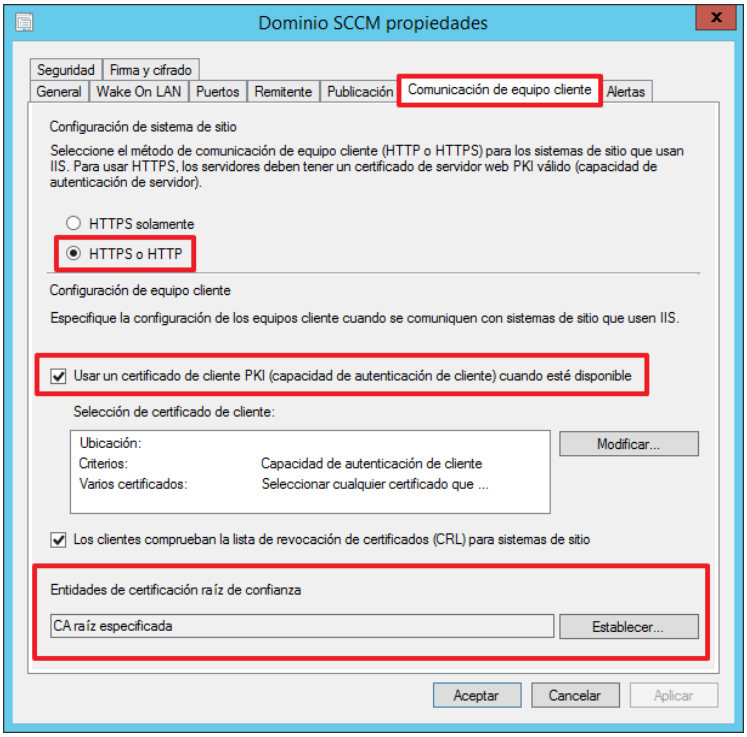
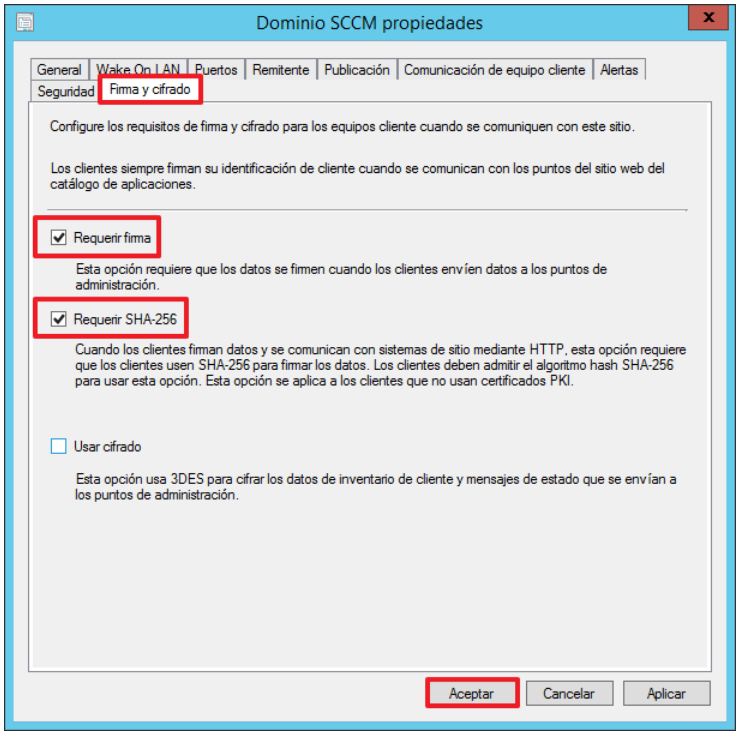
A continuación, se describe un paso a paso para reforzar la seguridad de las comunicaciones de MS SCCM 2012 R2.

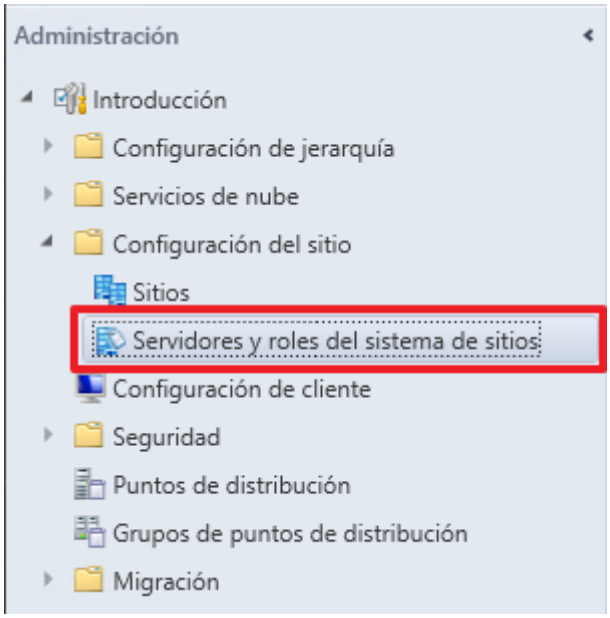
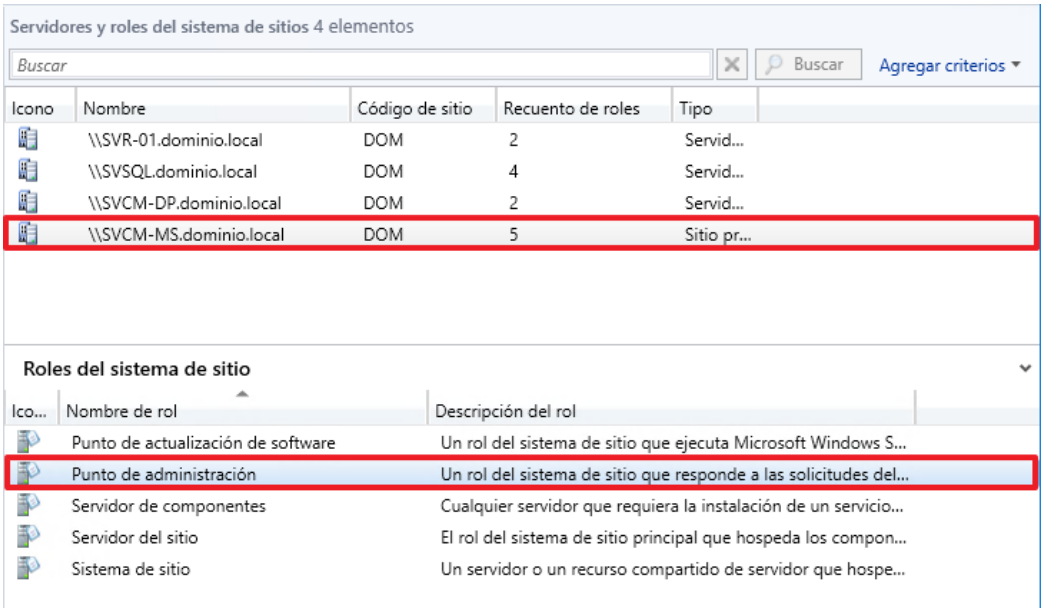
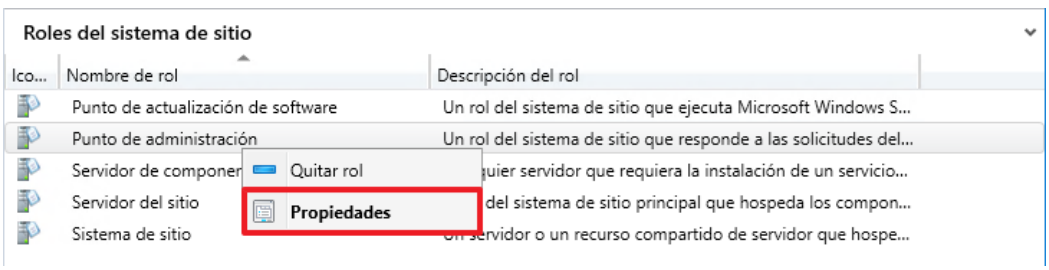
Nota: Si requiere aumentar la seguridad de las comunicaciones internas mediante comunicaciones basadas en HTTPS, puede aplicar el paso a paso 7.4 COMUNICACIÓN CON MS SCCM 2012 R2 correspondiente al ANEXO C.1 IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL ALTO DEL ENS, siempre que la organización presente una infraestructura de PKI adecuada para su integración con MS SCCM 2012 R2.

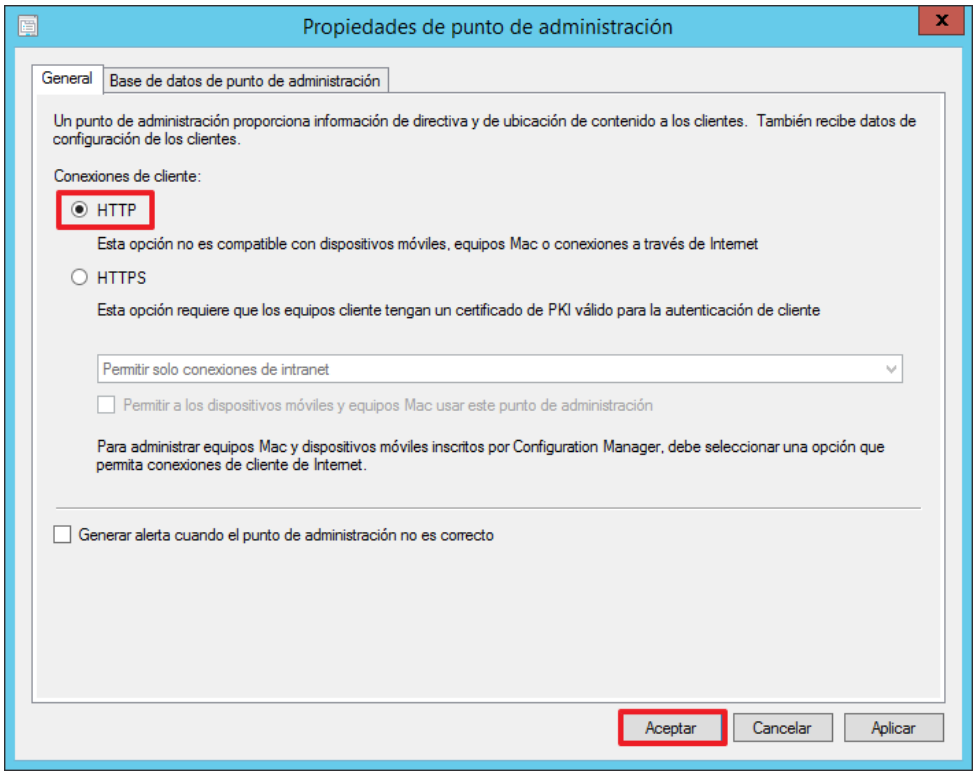
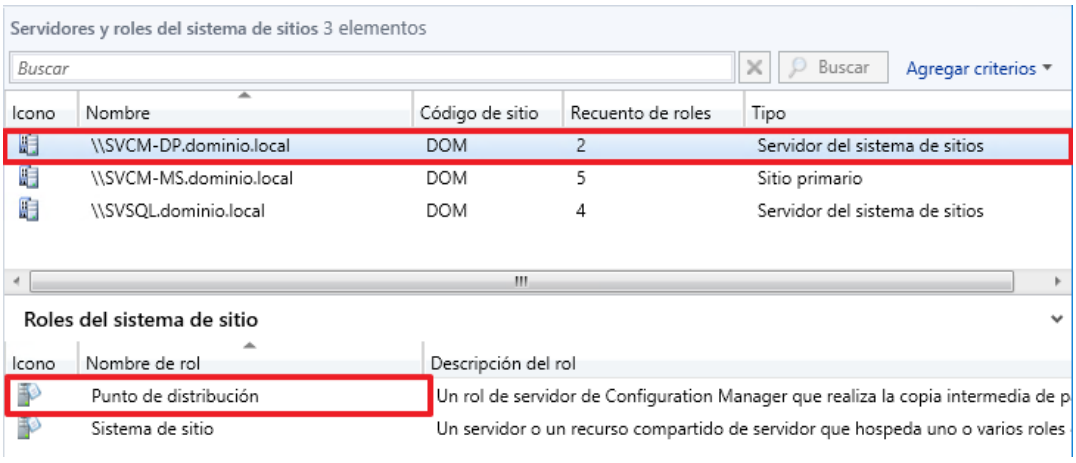
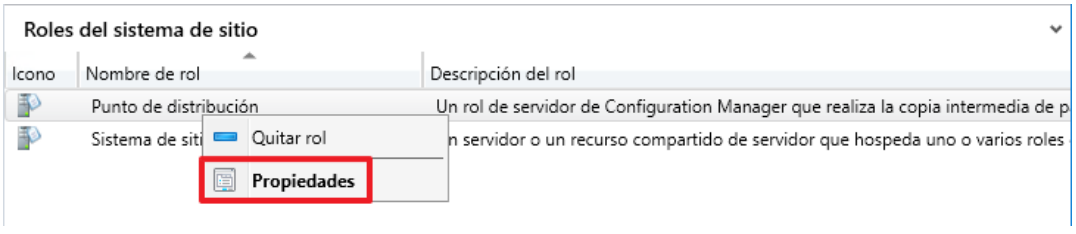
Paso	Descripción
291.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
292.	Pulse sobre el menú inicio. 
293.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
294.	Busque el icono “Consola de Configuration Manager” y marque sobre el para abrir la consola de administración de MS SCCM 2012 R2. 
295.	Seleccione el apartado “Administración”. 

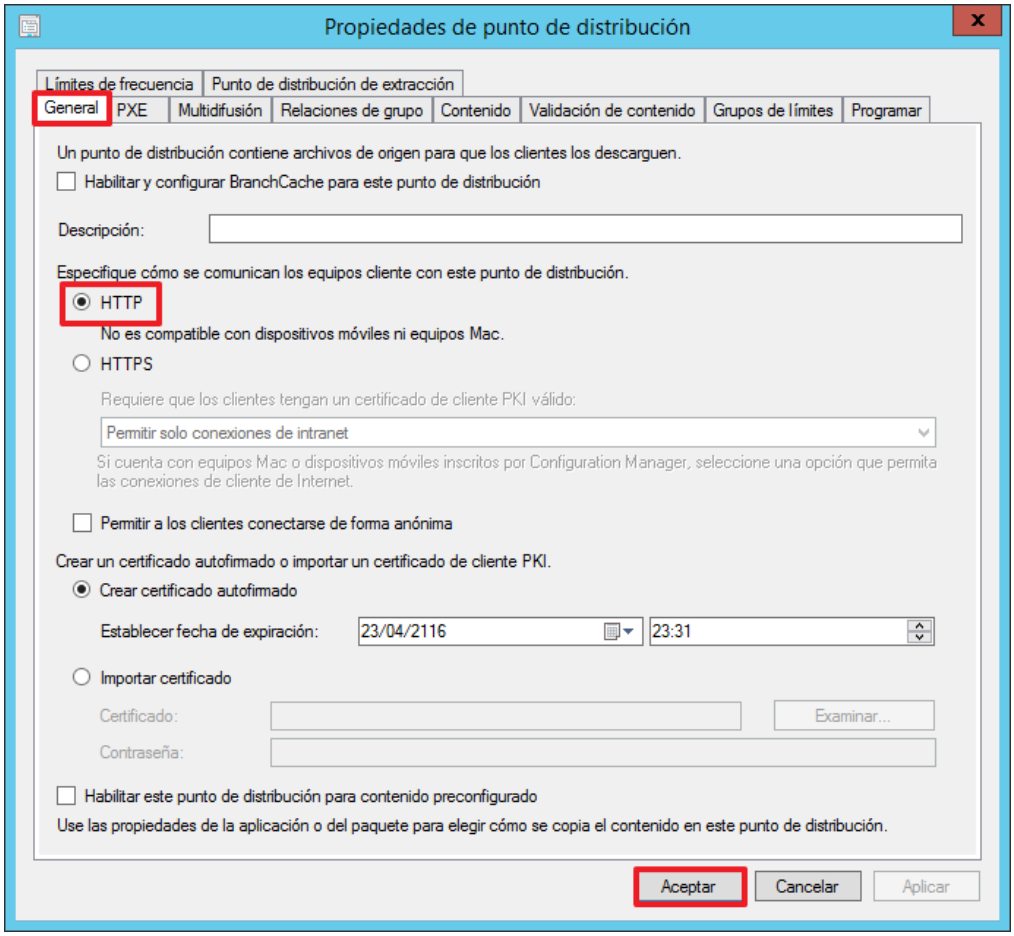
Paso	Descripción
296.	Despliegue “**Configuración del sitio > Sitios**”. 
297.	Seleccione el sitio que desea configurar y pulse sobre el botón “Propiedades” ubicado en la barra superior. 

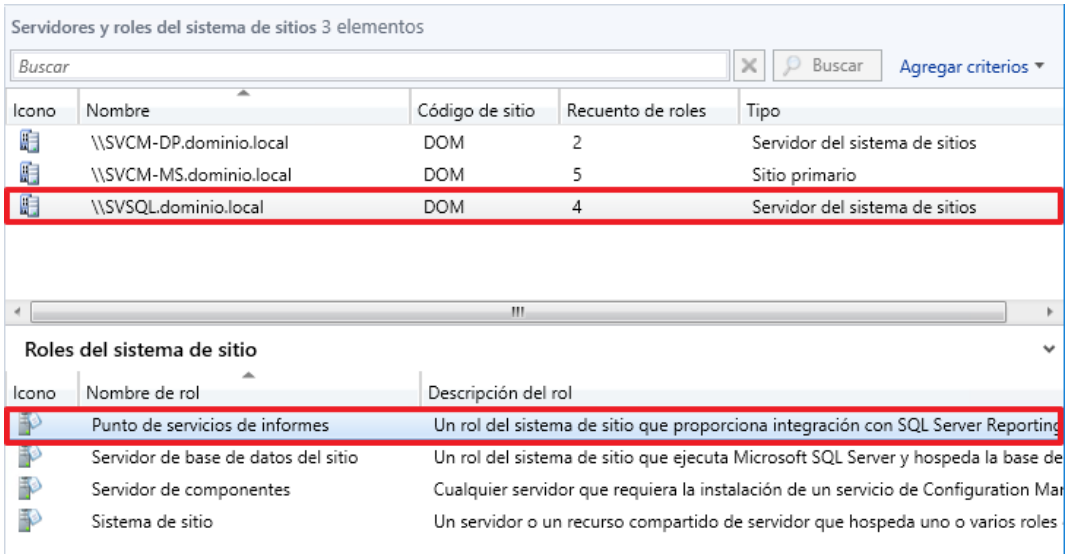
Paso	Descripción
298.	Seleccione la pestaña “Comunicación de equipo cliente” y marque la opción “HTTPS o HTTP”, y la opción “Usar un certificado de cliente PKI (capacidad de autenticación de cliente) cuando esté disponible”. Además, deberá establecer una entidad raíz de confianza previamente configurada en su entorno. 
299.	Sitúese en la pestaña “Firma y cifrado”, marque las siguientes opciones disponibles y pulse “Aceptar” para finalizar la configuración. 

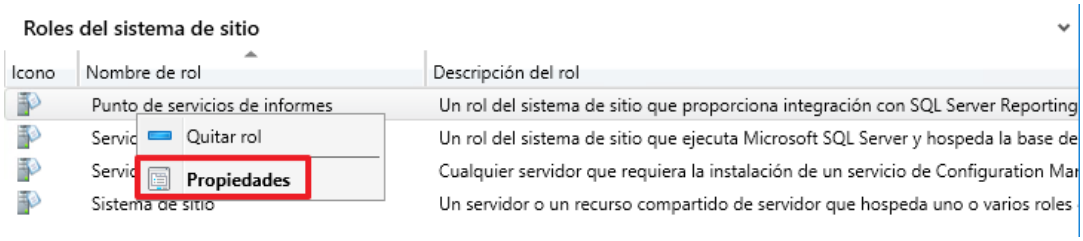
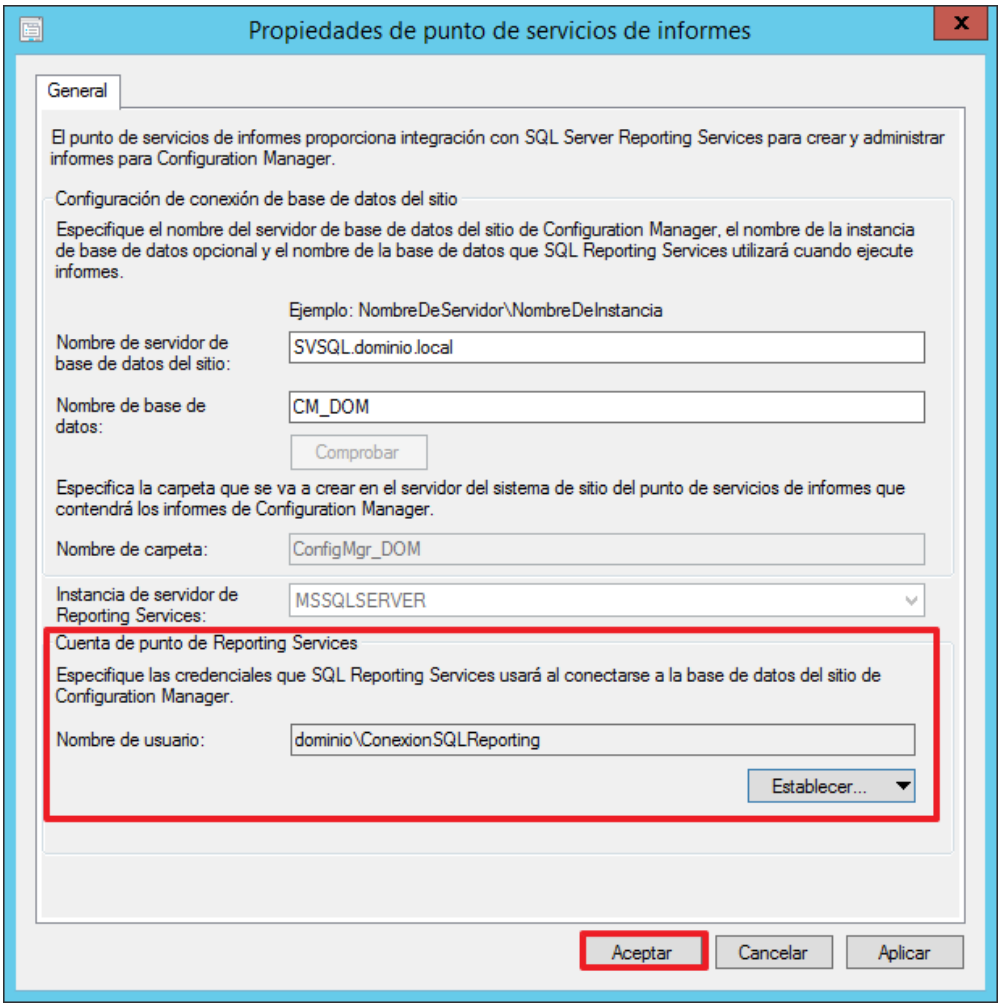
Paso	Descripción
300.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 
301.	Seleccione el servidor que contiene el rol de “Punto de administración”. 
302.	Localice el rol de “Punto de administración” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 

Paso	Descripción
303.	En la pestaña “General”, seleccione en “Conexiones de cliente:” la opción “HTTP” y pulse “Aceptar” para validar los cambios. 
304.	Seleccione el servidor que contiene el rol de “Punto de distribución”. 
305.	Localice el rol de “Punto de distribución” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 

Paso	Descripción
306.	Seleccione en “General:” la opción “HTTP” y pulse “Aceptar” para validar los cambios.
307.	Seleccione el servidor que contiene el rol de “Punto de punto de servicios de informes”.



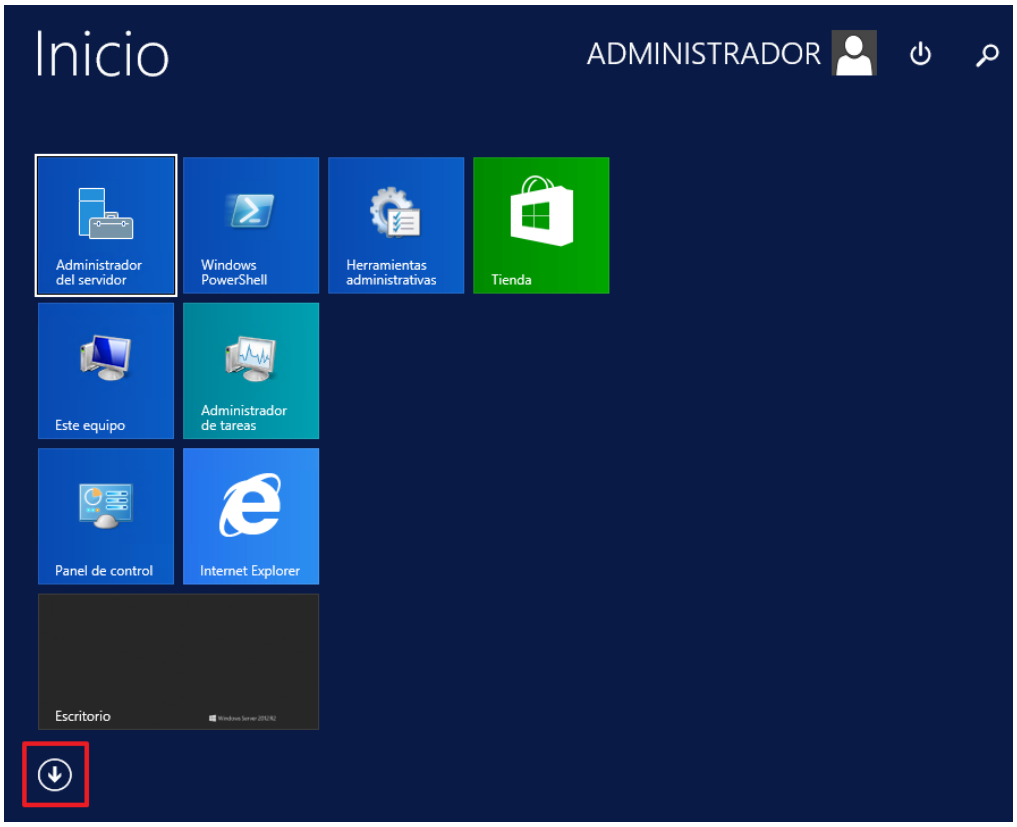


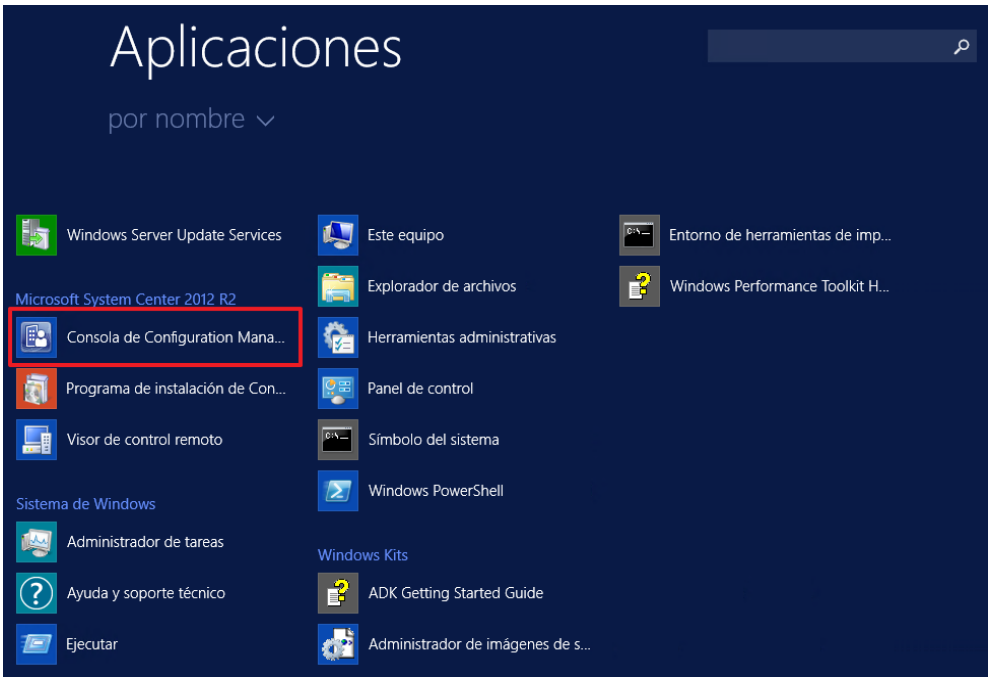
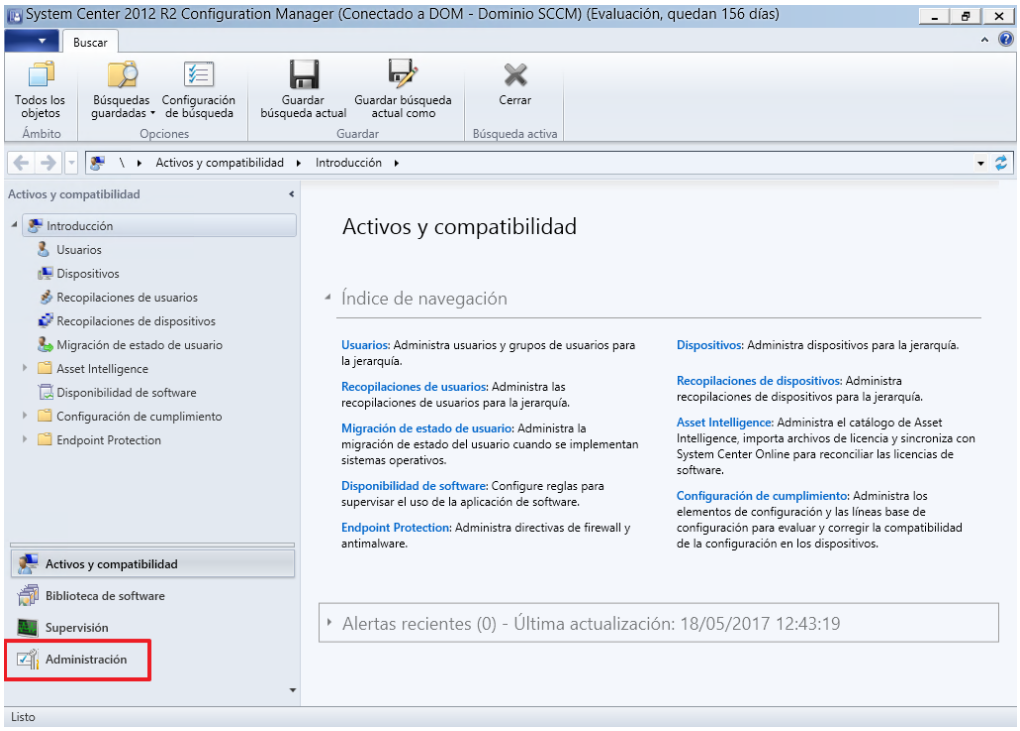
Paso	Descripción
308.	Localice el rol de “Punto de servicios de informes” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 
309.	En la pestaña “General:” especifique una cuenta única de conexión del punto de servicios de informes, y pulse “Aceptar” para validar los cambios.  **Nota:** Deberá adaptar estos pasos a su organización y seleccionar un usuario con las credenciales necesarias para que efectué correctamente la conexión del punto de administración y la base de datos de SQL Server.

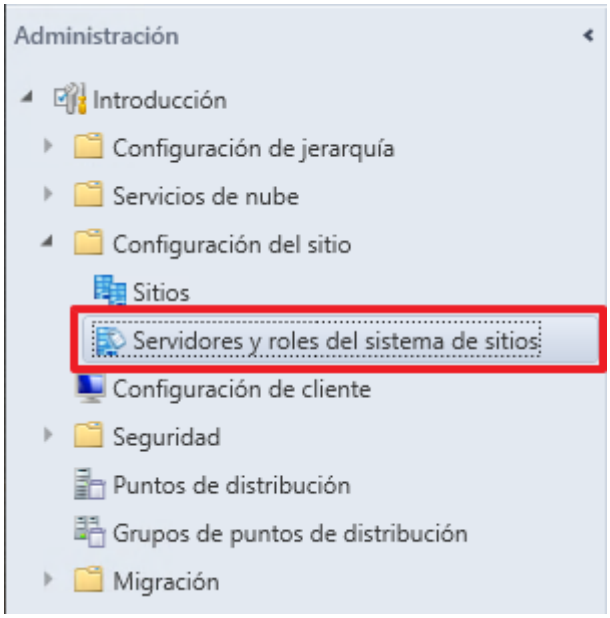
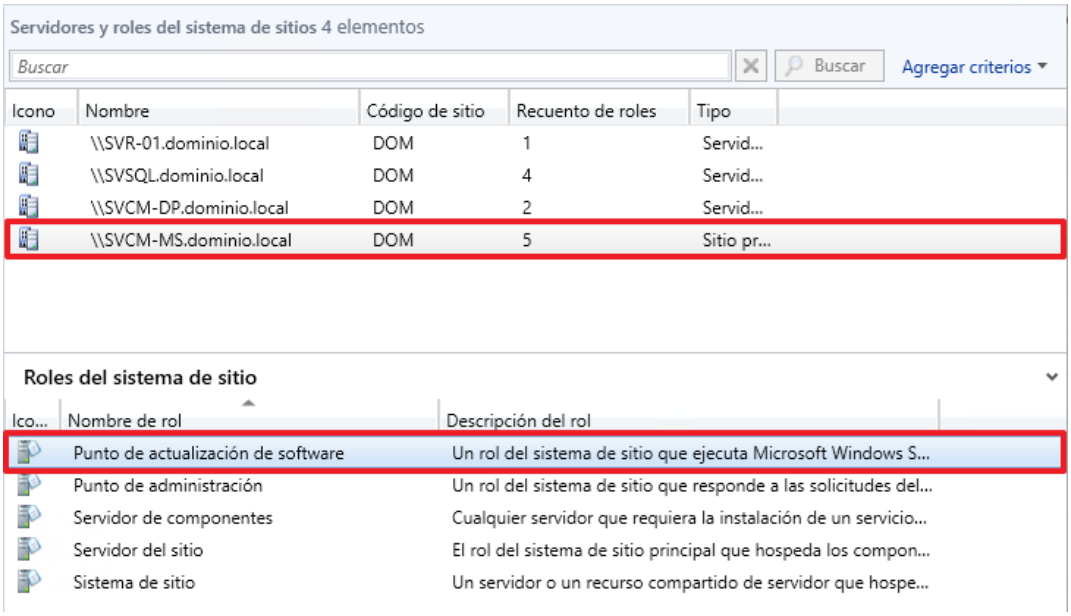
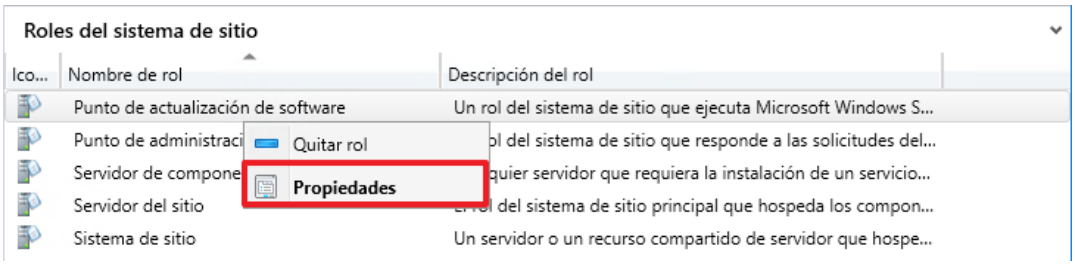
7.5. MANTENIMIENTO ACTUALIZACIONES DE SEGURIDAD

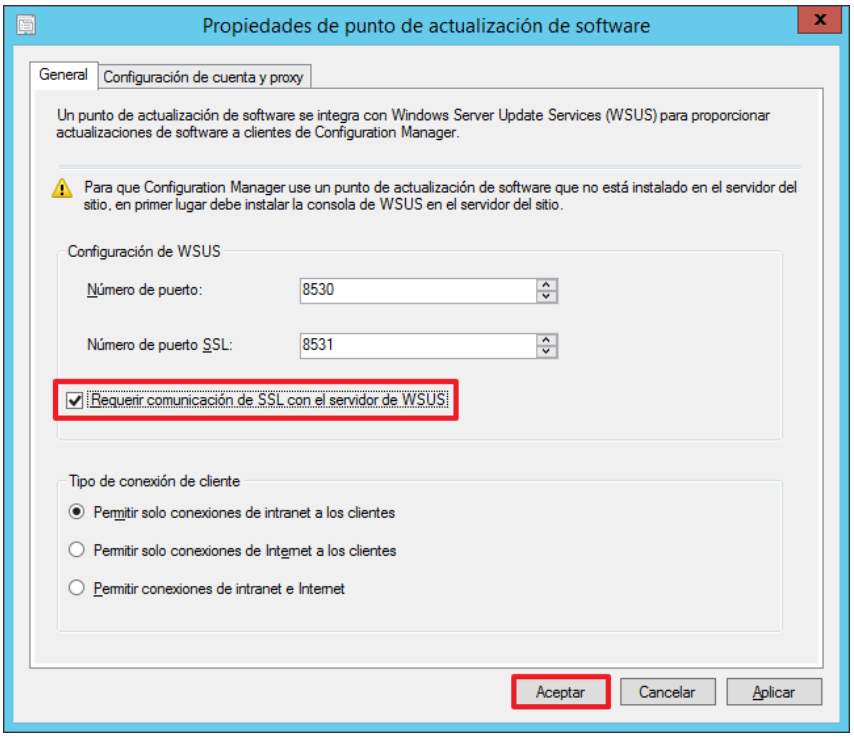
Microsoft SCCM 2012 R2 permite el administrar las actualizaciones de seguridad de clientes mediante el rol de "**Punto de actualización de software**", estableciendo y desplegando las actualizaciones publicadas por el fabricante.

A continuación, se describe un paso a paso para configurar la comunicación con el servidor que contiene el rol de WSUS es cual es necesario para el correcto funcionamiento del rol de "**Punto de actualización de software**".

Paso	Descripción
310.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
311.	Pulse sobre el menú inicio. 
312.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
313.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
314.	Seleccione el apartado “Administración”. 

Paso	Descripción
315.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 
316.	Seleccione el servidor que contiene el rol de “Punto de actualización de software”. 
317.	Localice el rol de “Punto de actualización de software” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 

Paso	Descripción
318.	Seleccione en la pestaña “General” la opción “Requerir comunicación SSL con el servidor de WSUS” y pulse “Aceptar” para validar los cambios. 

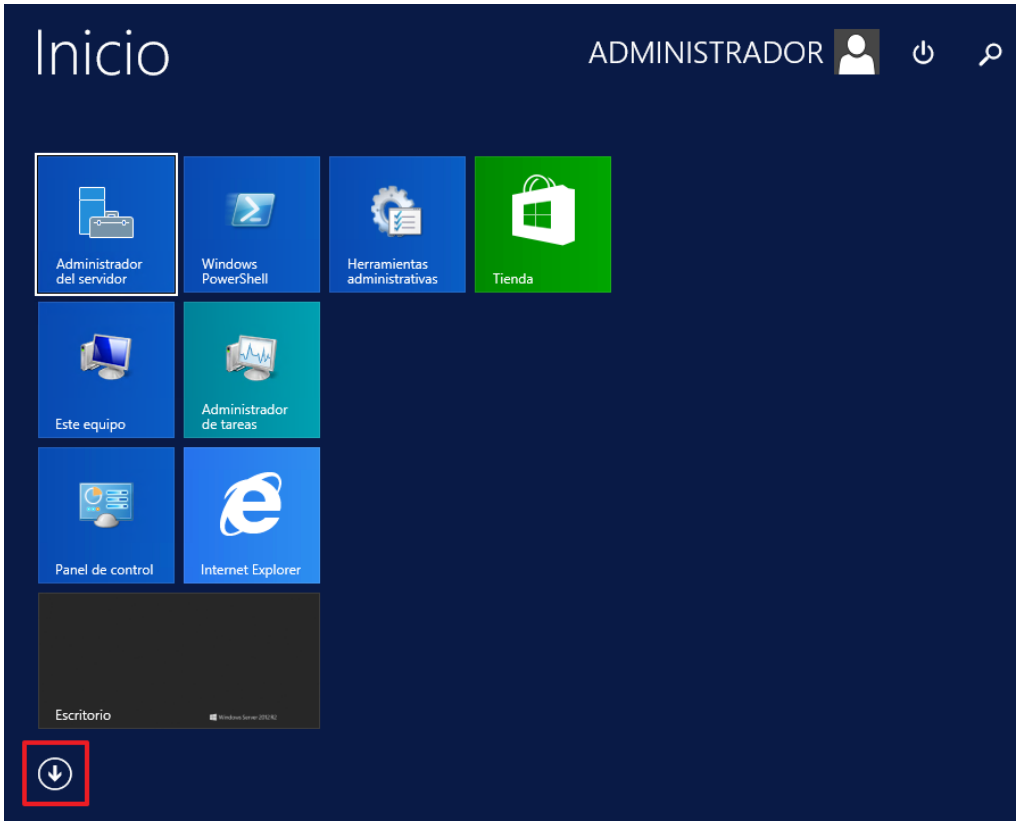
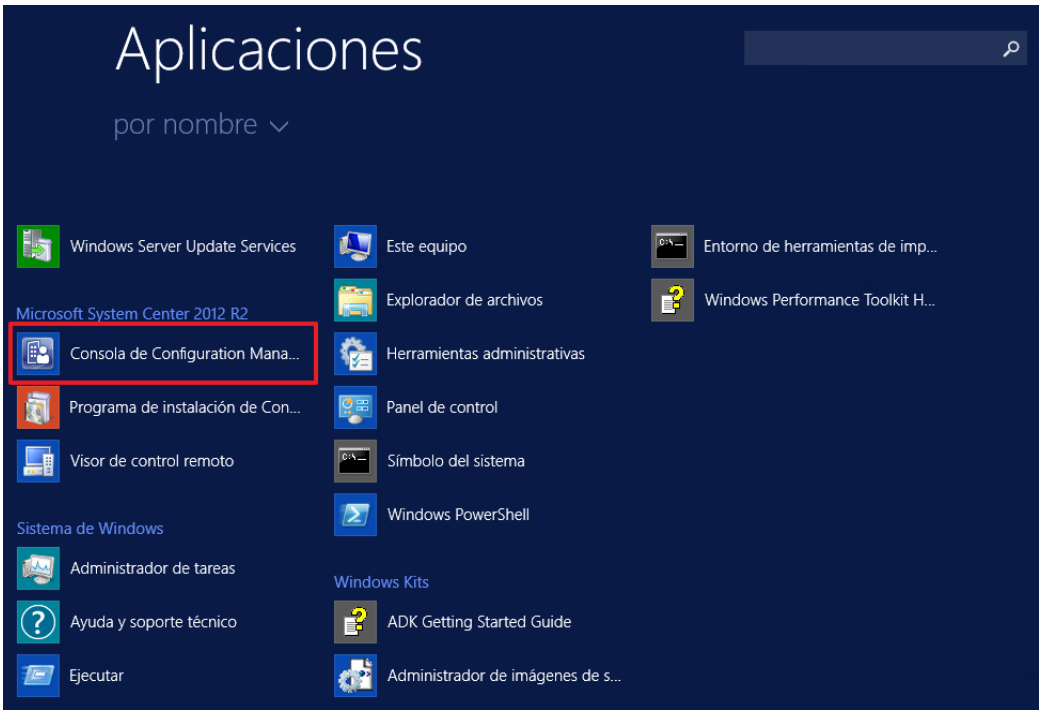
7.6. CONFIGURACIÓN HERRAMIENTAS REMOTAS

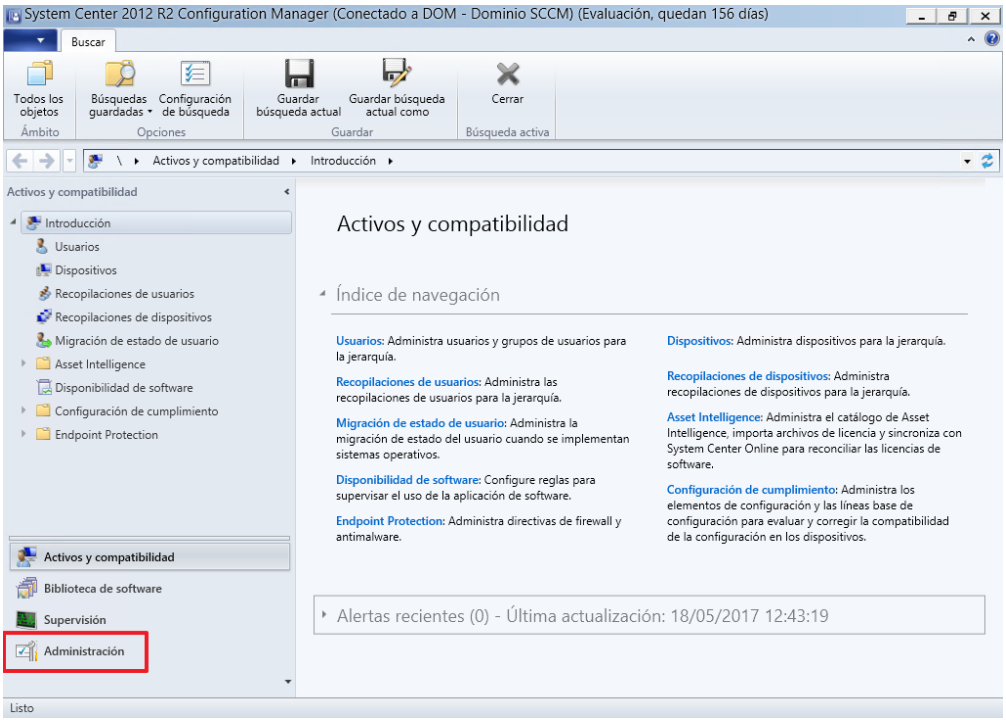
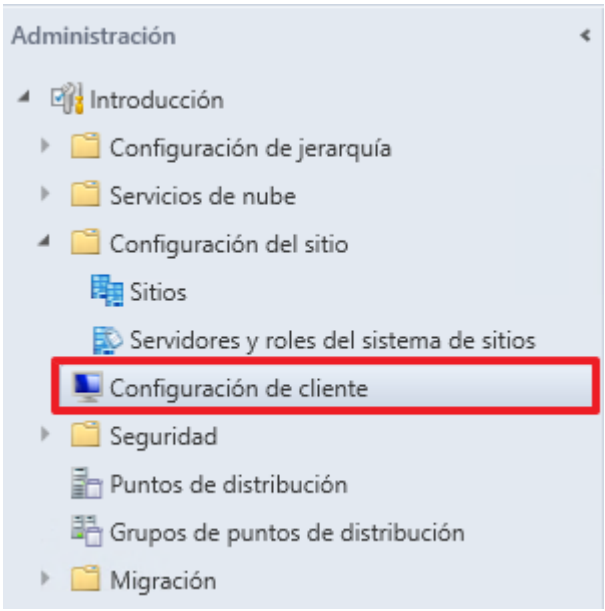
Microsoft SCCM 2012 R2 permite establecer la configuración de control remoto en equipos clientes que se aplica a todos los clientes de la jerarquía.

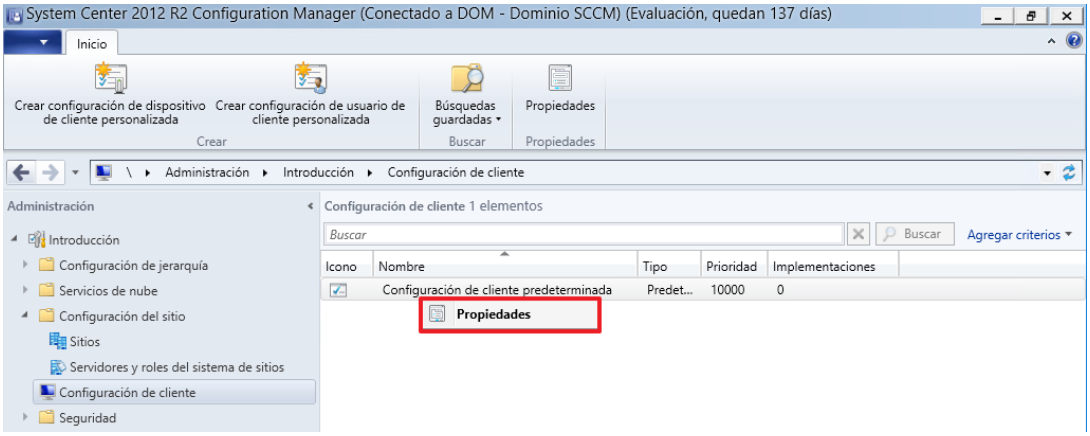
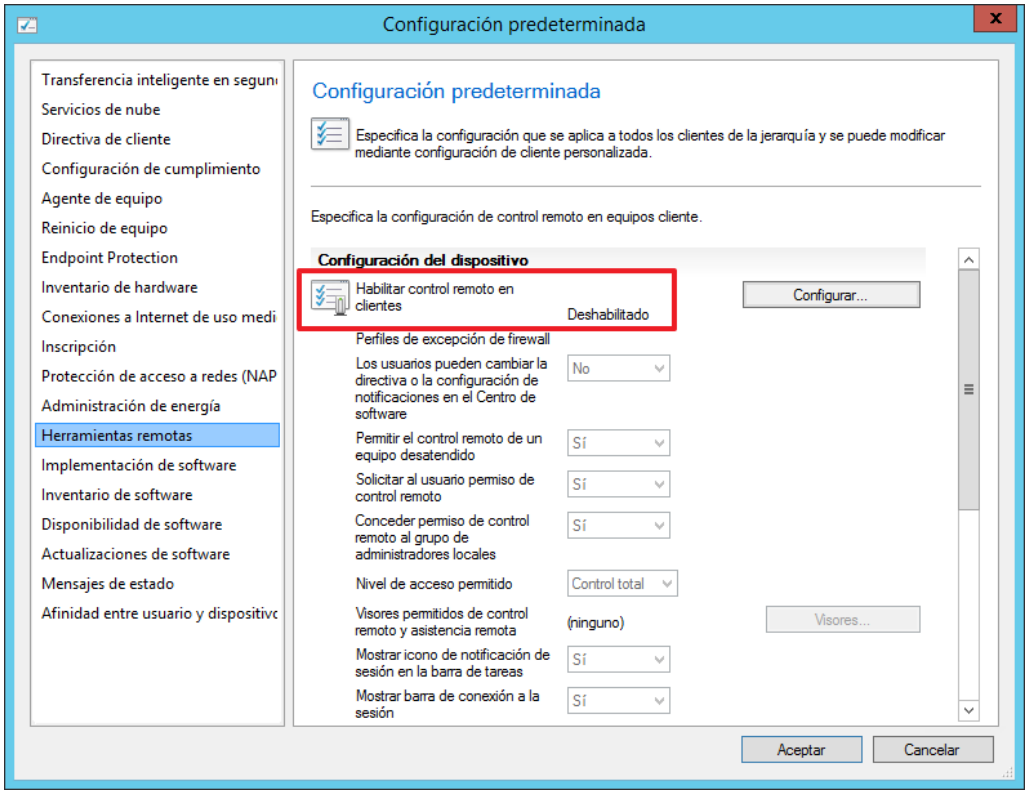
Se recomienda que esta herramienta, siempre que no sea un requisito de la organización, este en estado deshabilitado y en caso de estar habilitada, asegurarse que está configurada correctamente para que únicamente los usuarios con privilegios tengan acceso a esta característica de control remoto de equipos cliente.

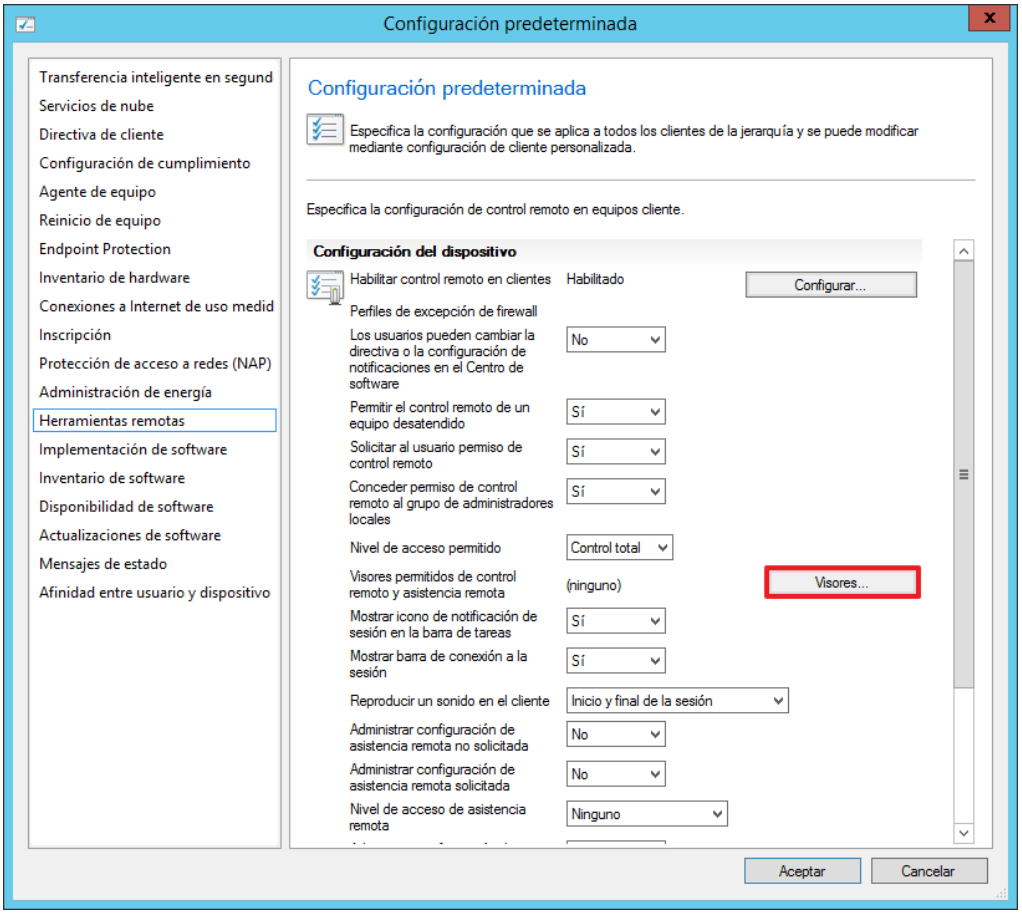
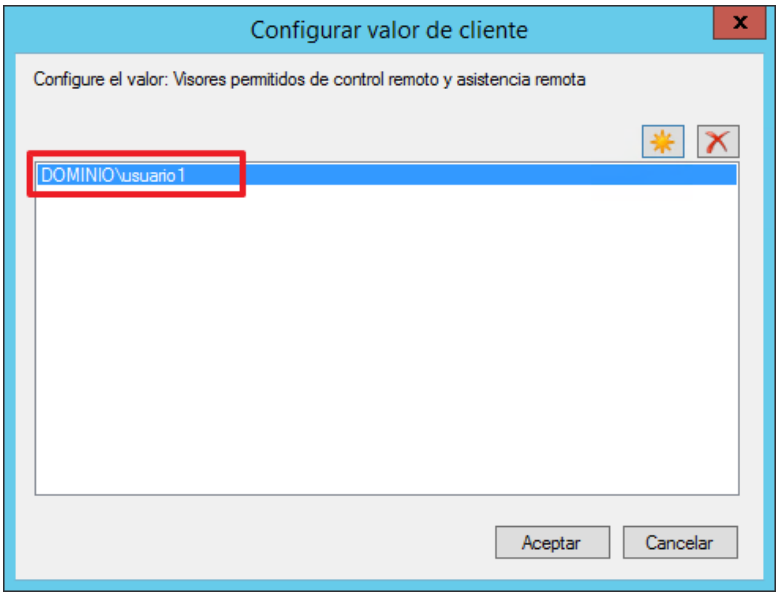
A continuación, se describe como establecer la configuración de control remoto en equipos clientes.

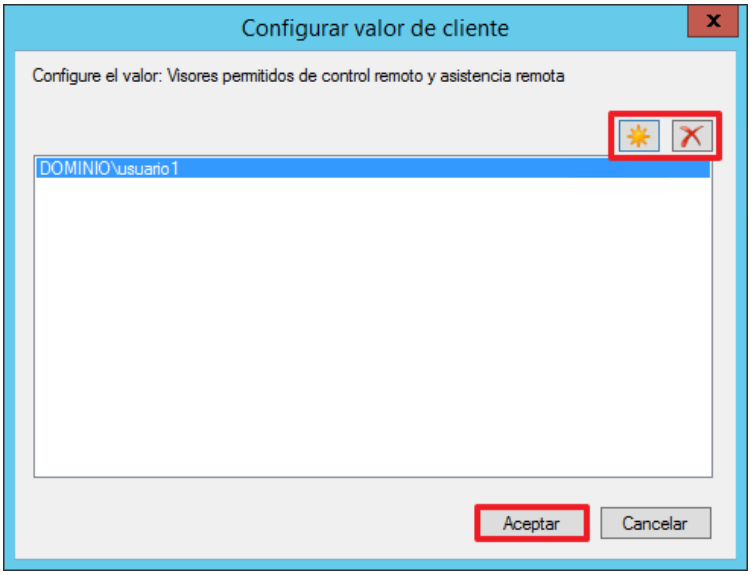
Paso	Descripción
319.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
320.	Pulse sobre el menú inicio. 

Paso	Descripción
321.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
322.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
323.	Seleccione el apartado “Administración”. 
324.	Despliegue “**Configuración del sitio > Configuración de cliente**”. 

Paso	Descripción
325.	Seleccione “Configuración de cliente predeterminada”, pulse con el botón derecho, y seleccione la opción “Propiedades” del menú contextual.  **Nota:** Deberá adaptar los pasos a su organización y seleccionar la configuración de cliente que se esté aplicado a sus equipos cliente.
326.	Localice la pestaña “Herramientas remotas” en la ventana de Configuración predeterminada y a continuación, verifique que la opción “Habilitar control remoto en clientes” esta deshabilitado.  **Nota:** En caso que en su organización se esté haciendo uso de esta característica, y aparezca “habilitado”, deberá verificar los usuarios que tienen permisos para utilizarla

Paso	Descripción
327.	Para comprobar los usuarios que tienen permiso de acceso remoto, pulse el botón “Visores…”. 
328.	Compruebe en el listado los usuarios que tienen permisos de control remoto. 

Paso	Descripción
329.	En caso de requerir añadir o eliminar algún usuario o grupos de usuarios seleccione los dos botones situados en la parte derecha de la imagen en función de la acción que desee realizar. Pulse “Aceptar” una vez haya finalizado la configuración. 

7.7. REGISTRO DE LA ACTIVIDAD

Según el ENS se registrará toda aquella evidencia que pueda, respaldar una demanda judicial, o hacer frente a ella, cuando el suceso pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

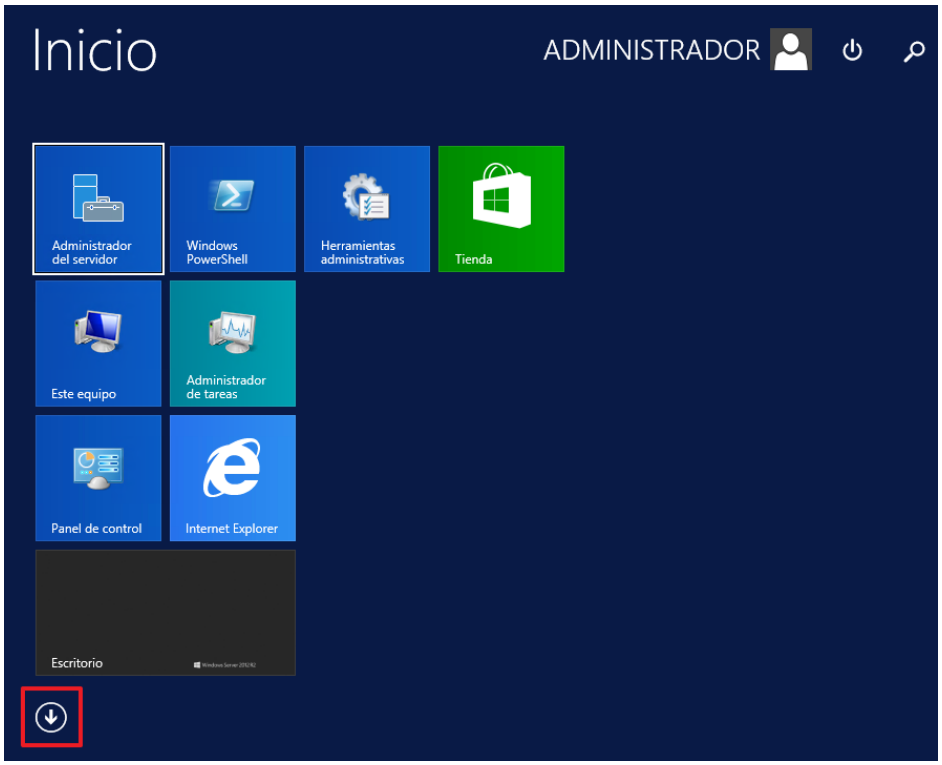
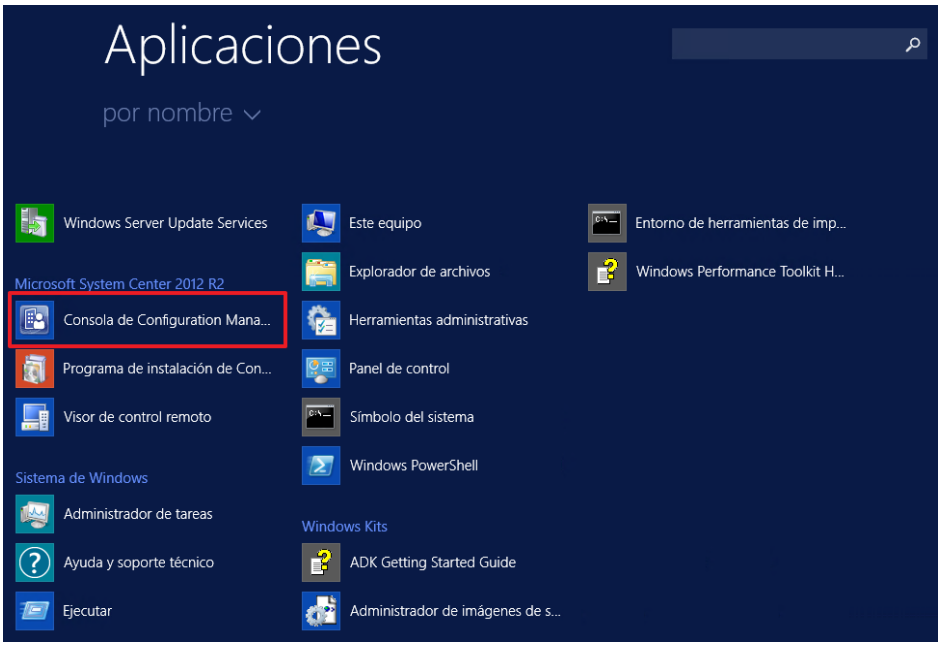
Además, se incluirá la actividad de los usuarios y, con especial atención, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

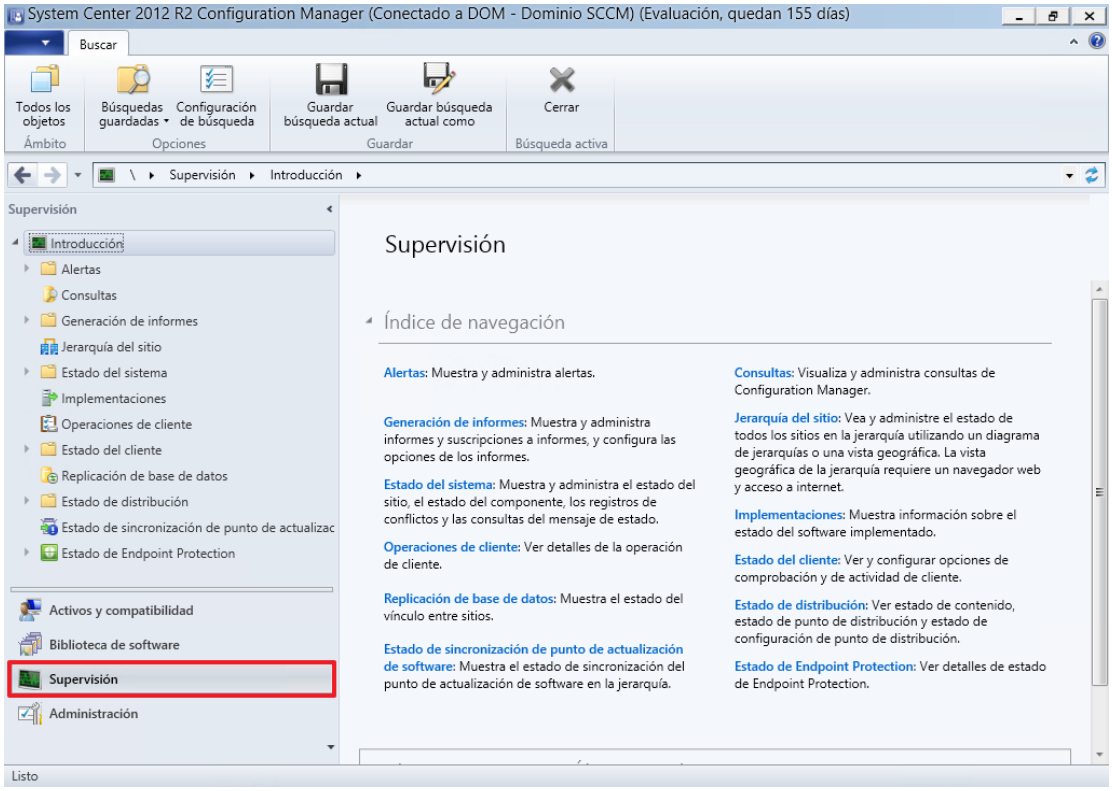
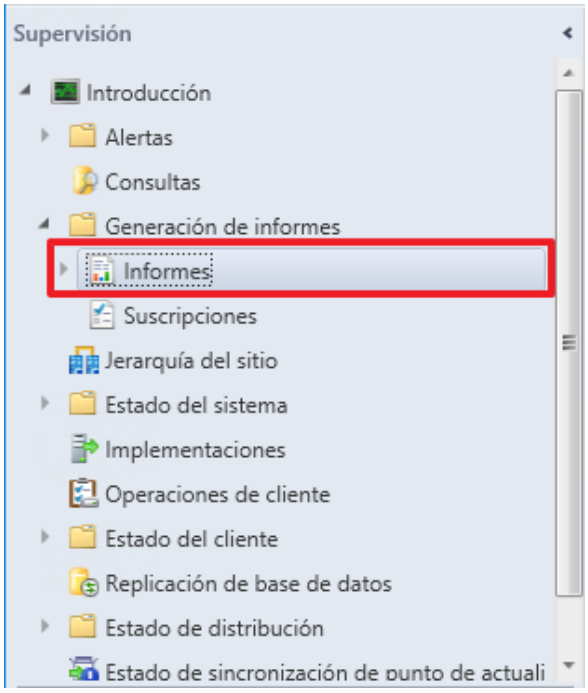
Se ha de tener en consideración que la primera medida para reforzar la seguridad es el mantenimiento y aplicación correcta de la segregación de roles y funciones descrito en el punto 7.2 de la presente guía, limitando con ello el campo de acción de los usuarios administrativos.

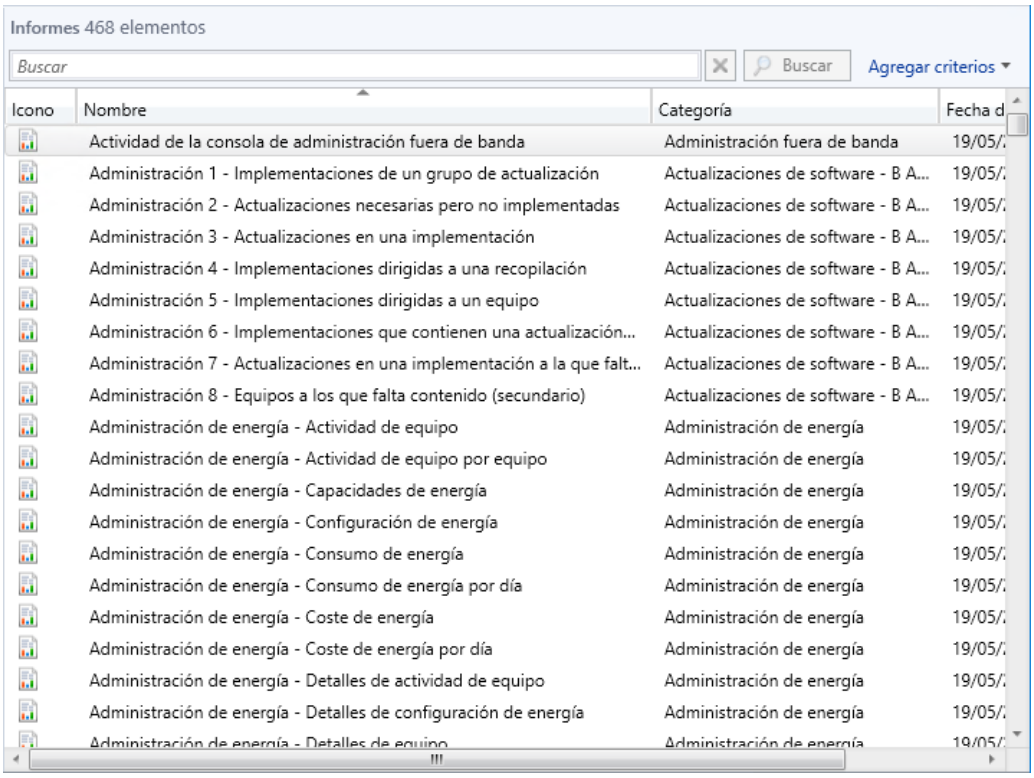
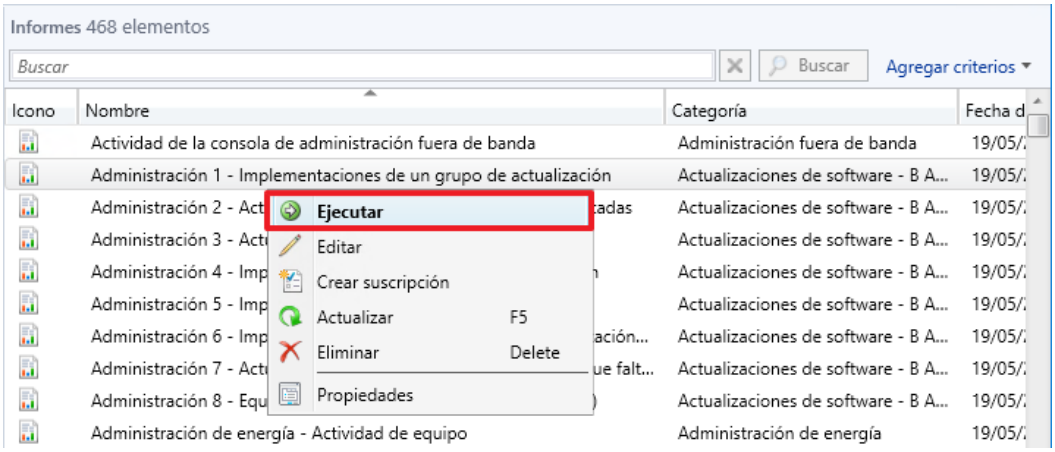
Además del registro de sucesos y evidencias es imprescindible reforzar la seguridad en el acceso a esa información registrada, evitando con ello, acciones ilícitas que puedan poner en riesgo la integridad de la información almacenada.

A continuación, se muestra un paso a paso para ver los informes de actividad de MS SCCM 2012 R2.

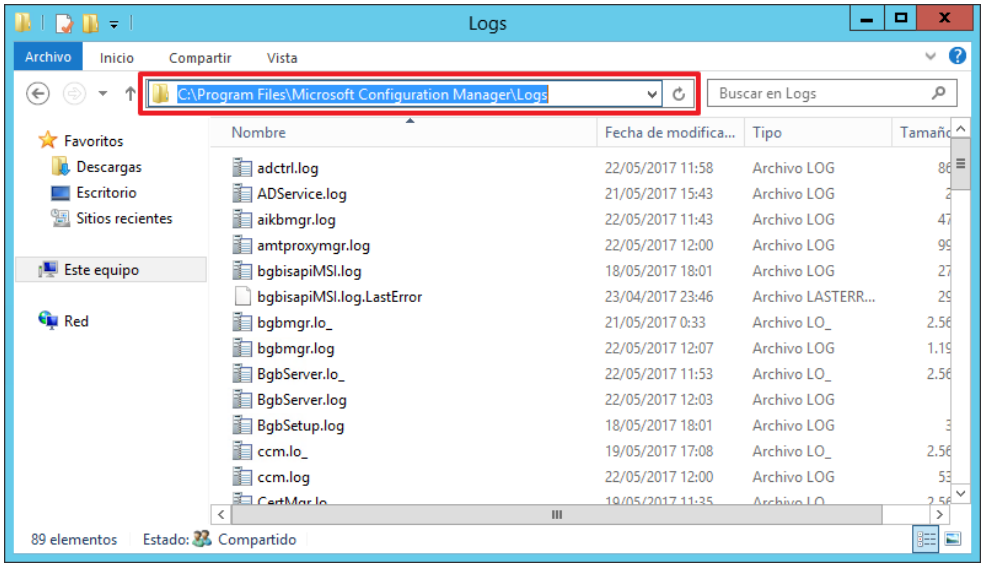
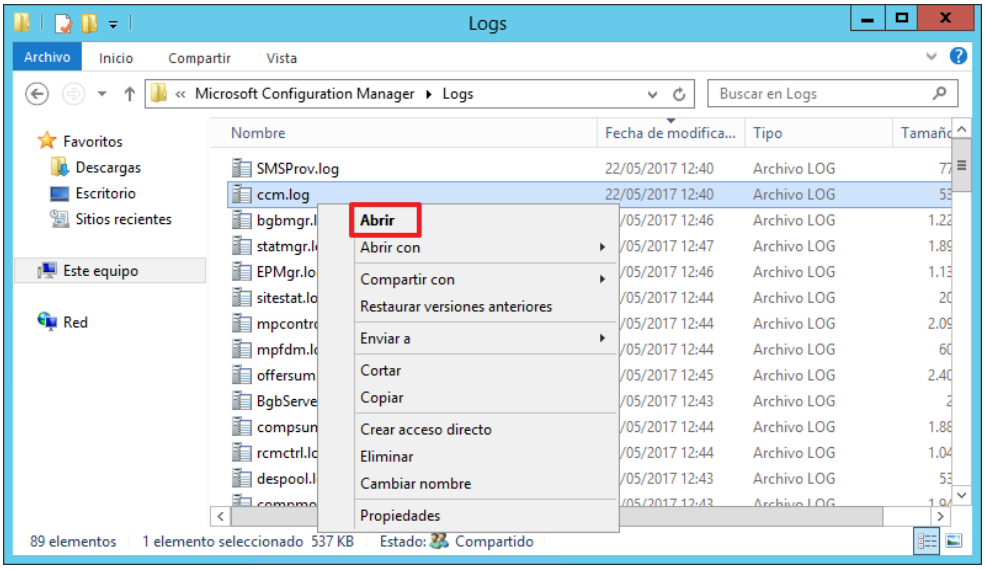
Paso	Descripción
330.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.

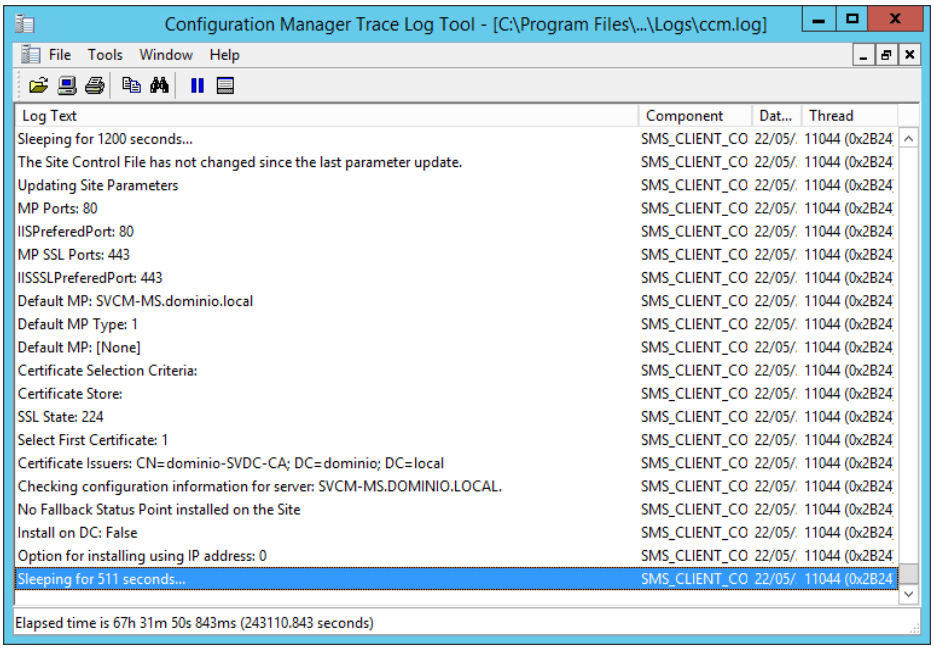
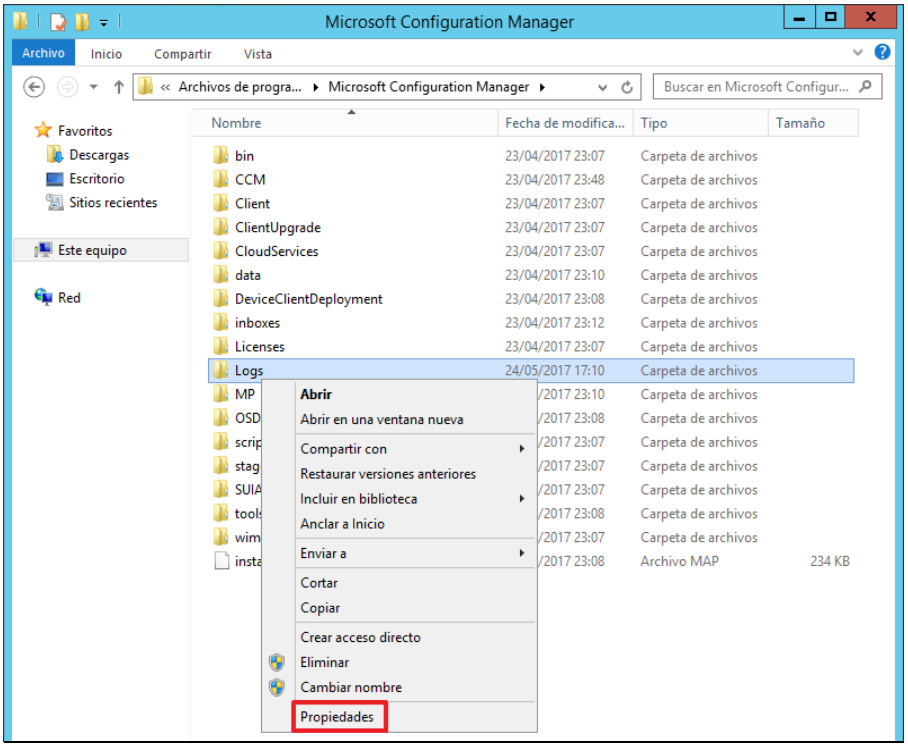
Paso	Descripción
331.	Pulse sobre el menú inicio. 
332.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
333.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

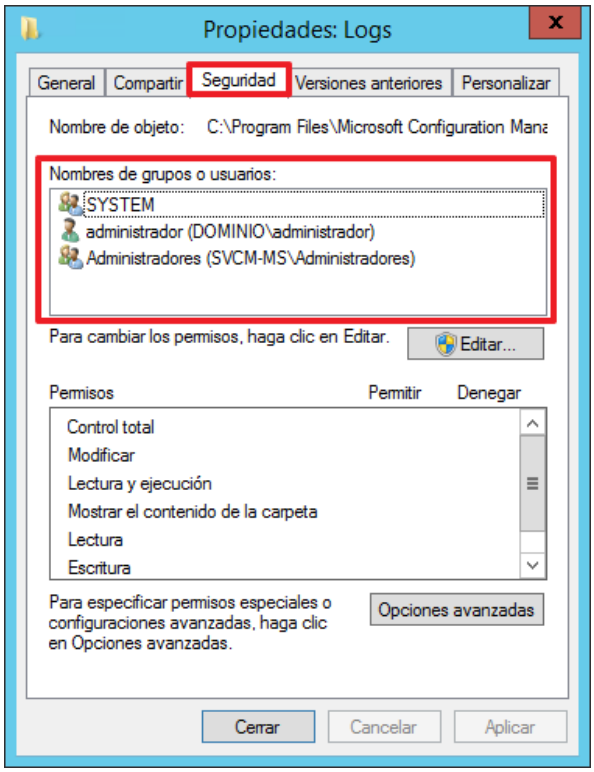
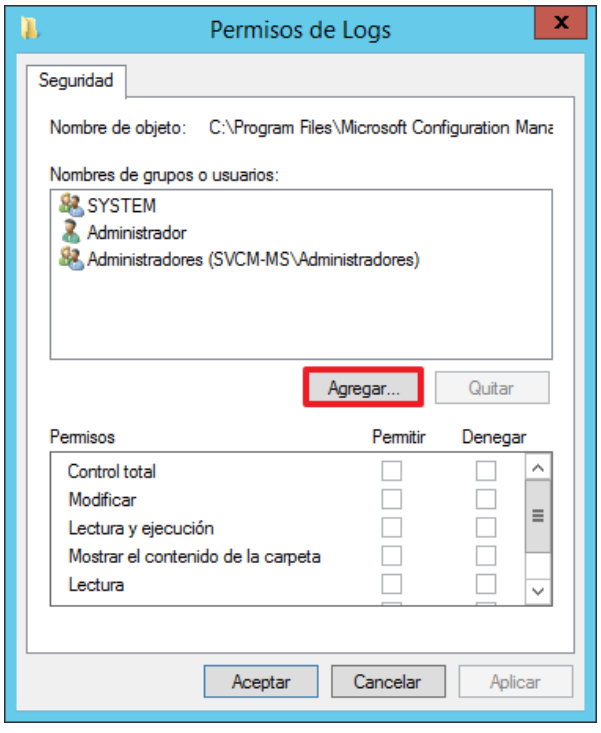
Paso	Descripción
334.	Seleccione el apartado “Supervisión”. 
335.	Despliegue “**Generación de informes > Informes**”. 

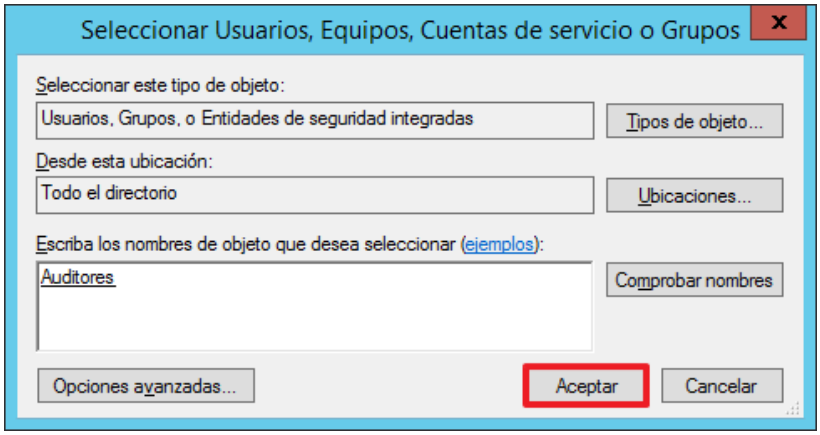
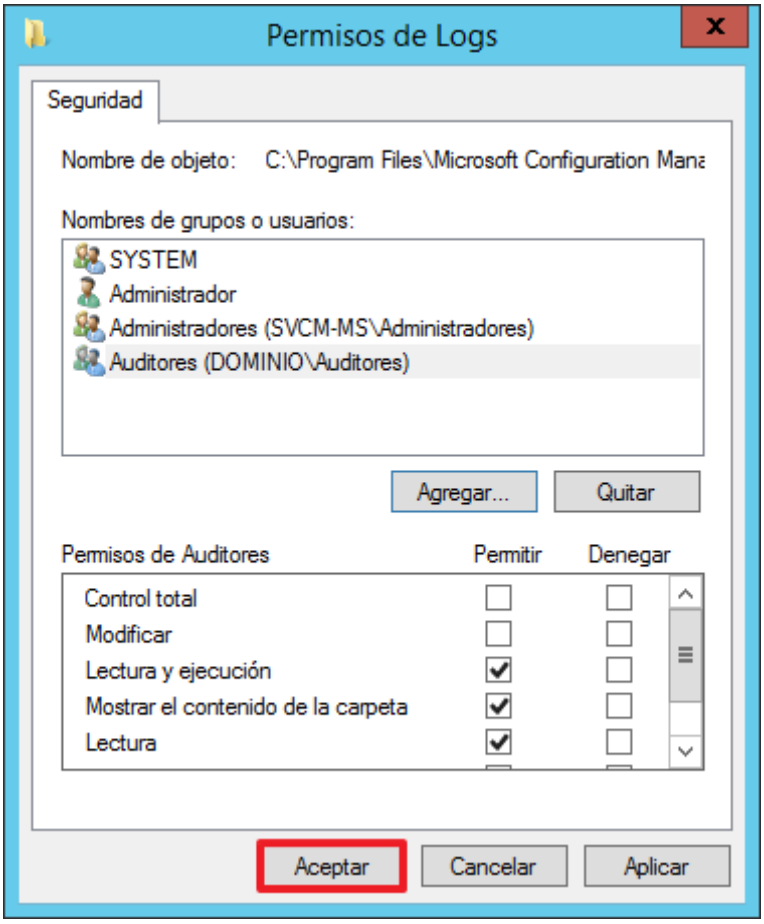
Paso	Descripción
336.	Seleccione de entre todos los informes disponibles el que más se adecue a sus necesidades. 
337.	Una vez localizado, pulse con el botón derecho y seleccione la opción “Ejecutar” del menú contextual para visualizar los datos del informe seleccionado.  **Nota:** En este ejemplo se selecciona el informe “Administración 1 – Implementaciones de un grupo de actualización” por lo que deberá adaptar los pasos a las necesidades de su organización.

Además de los informes presentados en MS SCCM 2012 R2 es posible consultar la actividad del servicio a través de los registros los cuales ofrecen una información más detallada de lo que puede estar sucediendo o buscar evidencias de acciones realizadas.

Paso	Descripción
338.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
339.	Pulse sobre el menú inicio y seleccione el icono “Explorador de archivos”. 
340.	Localice la ruta “C:\Program Files\Microsoft Configuration Manager\Logs”.  **Nota:** La ruta que contiene los registros puede variar en función de la ubicación de la instalación del producto MS SCCM 2012 R2.
341.	Seleccione el archivo.log que más se adecue a sus necesidades y haga clic botón derecho, y seleccione la opción “Abrir” del menú contextual. 

Paso	Descripción
342.	En la siguiente imagen, se muestra un ejemplo del fichero “ccm.log”.  **Nota:** En la imagen se visualiza el log mediante la herramienta propia de Configuration Manager Trace log tool, siendo posible utilizar cualquier editor de textos para su lectura.
343.	Seguidamente, se va a proceder a reforzar la seguridad de la carpeta que contiene los registros para ello, deberá ubicarse en la dirección “C:\Program Files\Microsoft Configuration Manager”. Marque la carpeta “Logs”, pulse con el botón derecho y seleccione la opción “Propiedades” del menú contextual. 

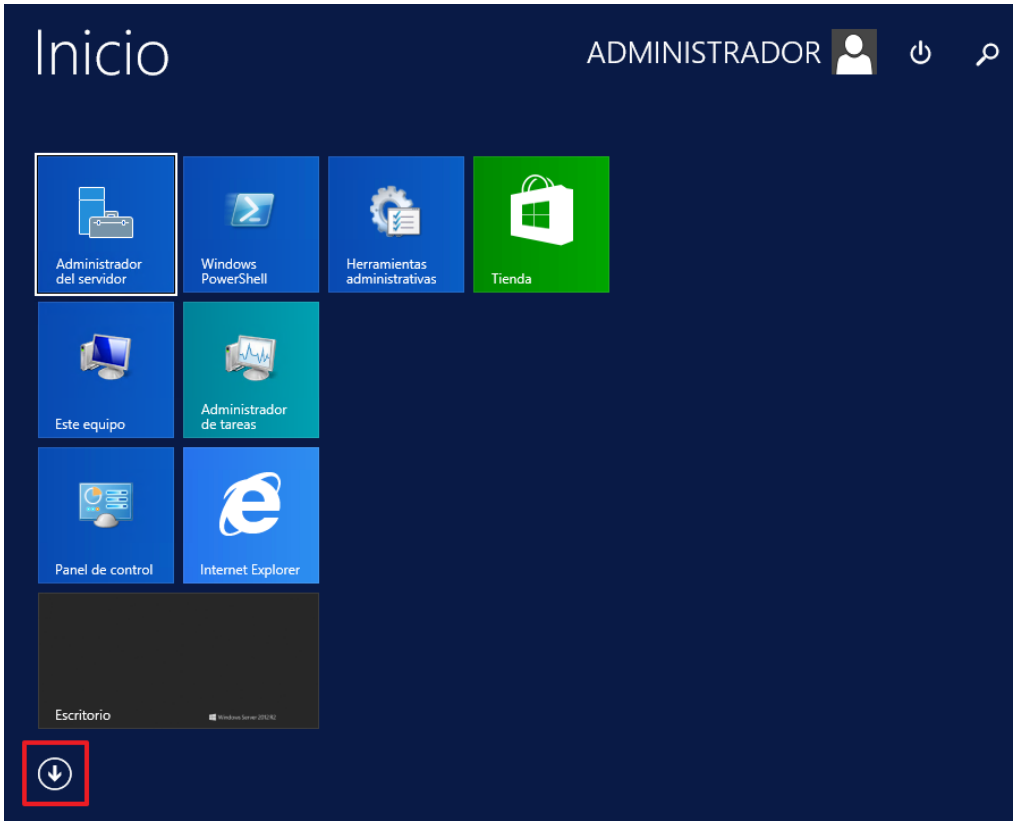
Paso	Descripción
344.	Seleccione la pestaña “Seguridad” y compruebe que únicamente los usuarios imprescindibles tienen acceso a la carpeta y su contenido. 
345.	A modo de ejemplo se va a proceder a agregar un grupo de usuarios los cuales se les concederá permisos de lectura sobre la carpeta “Logs”. Deberá adaptar los próximos pasos adecuándolos a los requerimientos de su organización. Pulse sobre el botón “Agregar”. 

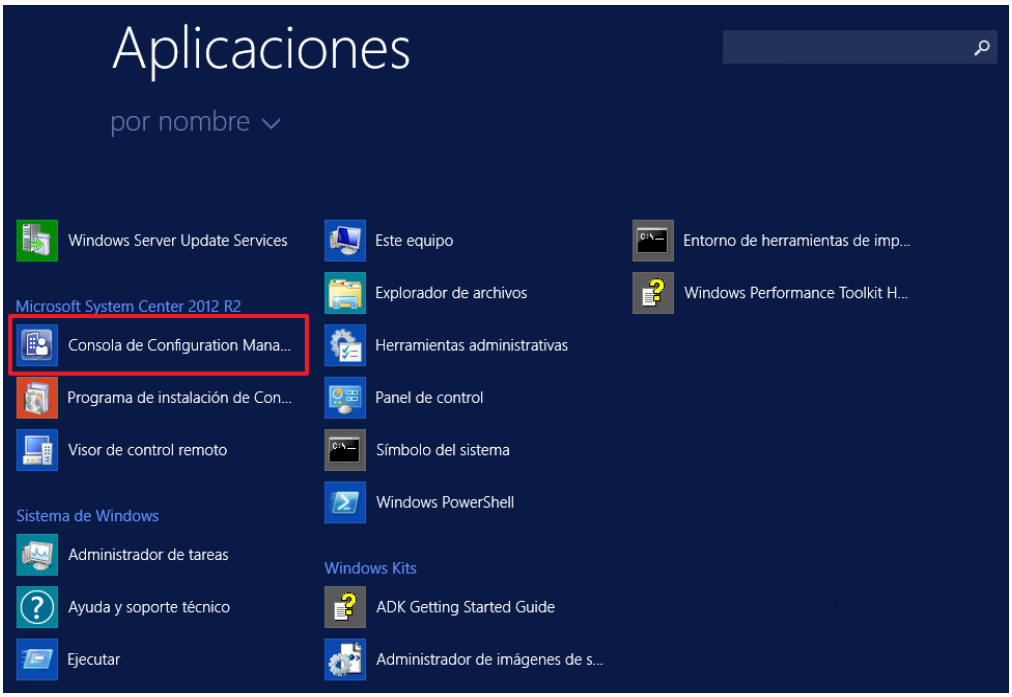
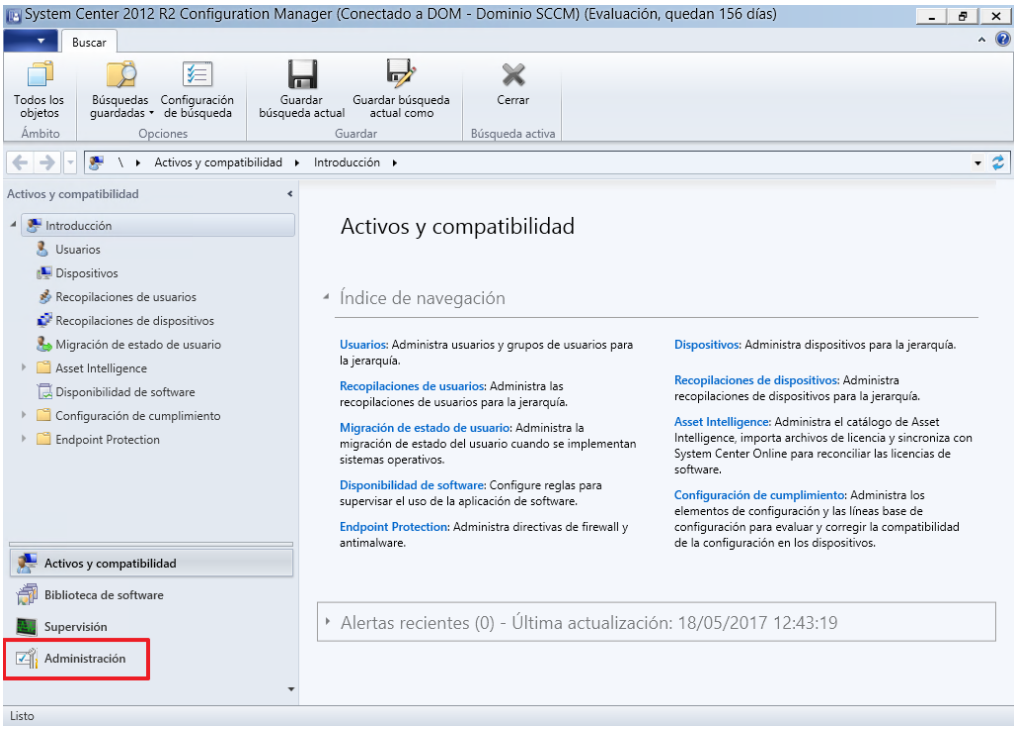
Paso	Descripción
346.	Agregue los usuarios o grupos de usuarios a los que desee conceder acceso y pulse “Aceptar”.  **Nota:** En el presente ejemplo se agrega el grupo de seguridad “Auditores”, deberá adaptar estos pasos a su organización y únicamente agregar los usuarios que necesiten acceso a la carpeta.
347.	Compruebe que el usuario o grupo de usuarios tiene únicamente permisos de lectura y pulse “Aceptar” para finalizar la configuración. 

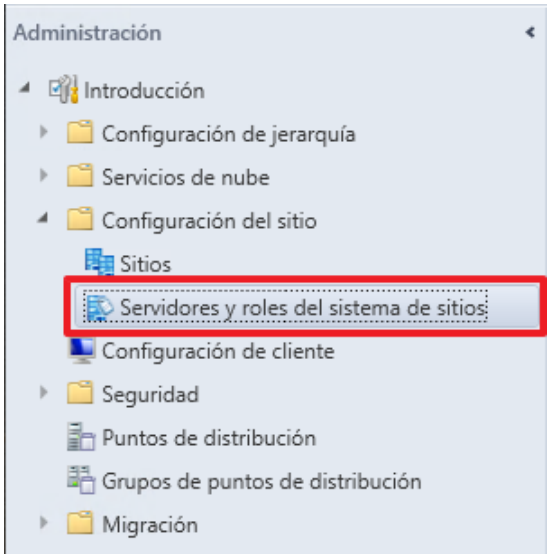
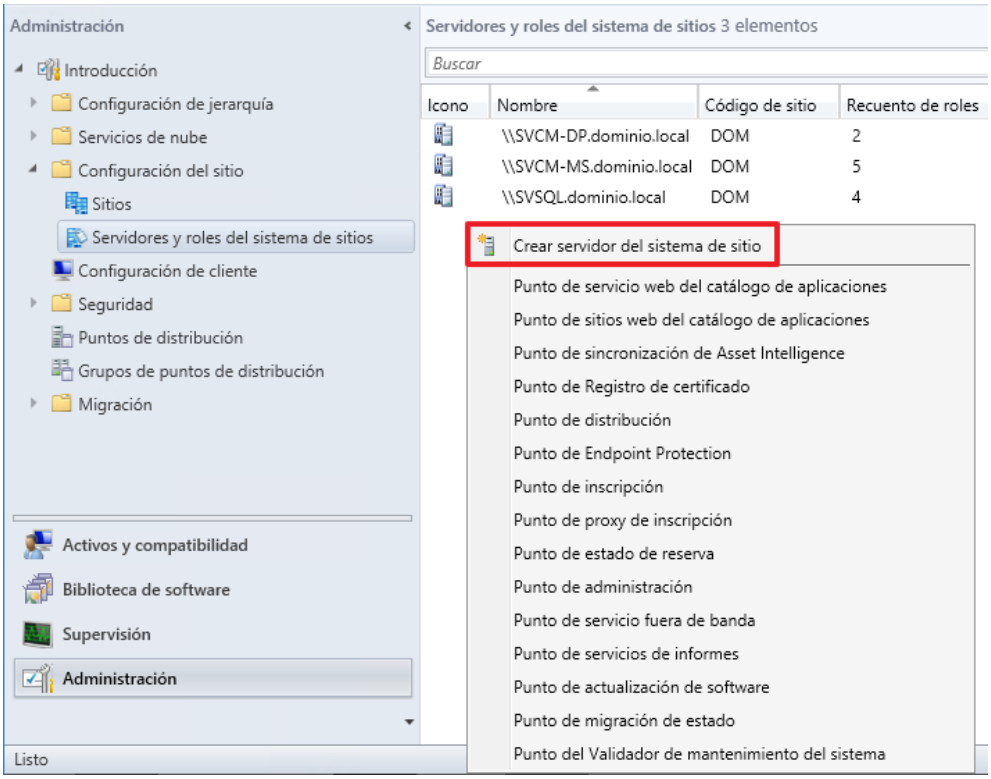
7.8. IMPLEMENTACIÓN DE SERVIDORES Y ROLES DEL SISTEMA DE SITIO

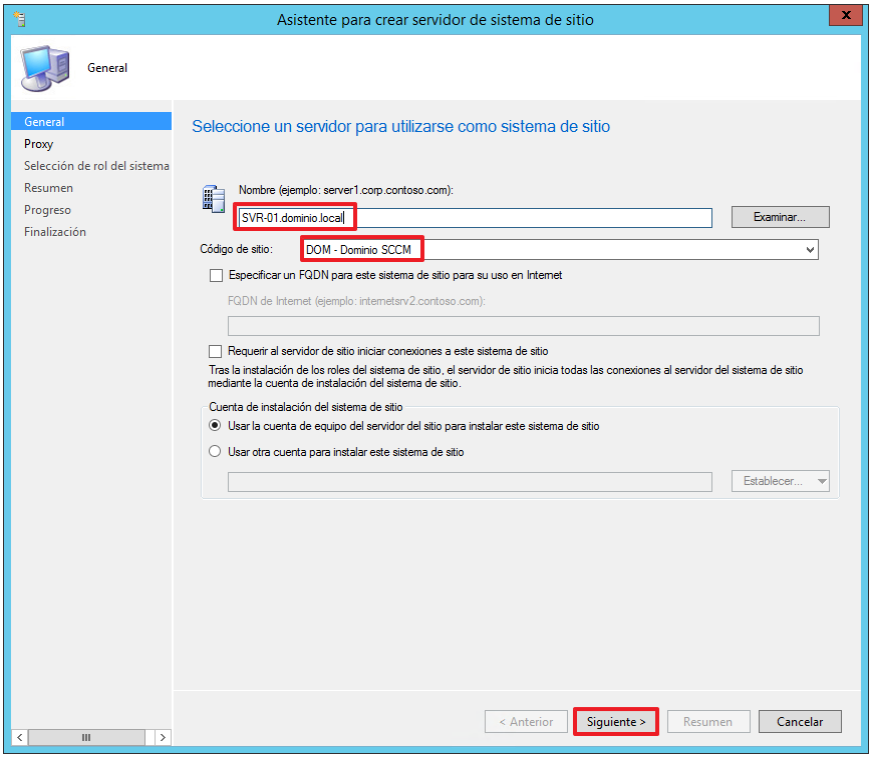
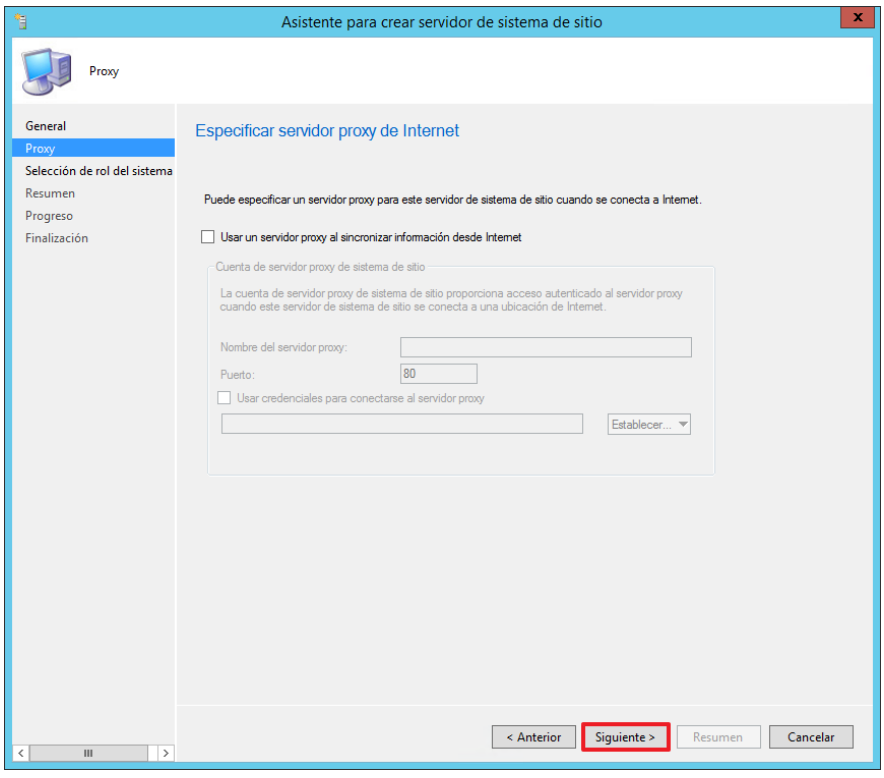
En MS SCCM 2012 R2 es posible agregar múltiples servidores que contengan varios roles para garantizar un servicio de alta disponibilidad, para en caso de que fallen los medios habituales de comunicación existan alternativas que garanticen el servicio, por lo que un mismo rol del sistema de sitio como por ejemplo el rol de punto de distribución es posible implementarlo en varios servidores, disponiendo con ello del mismo servicio en distintos servidores.

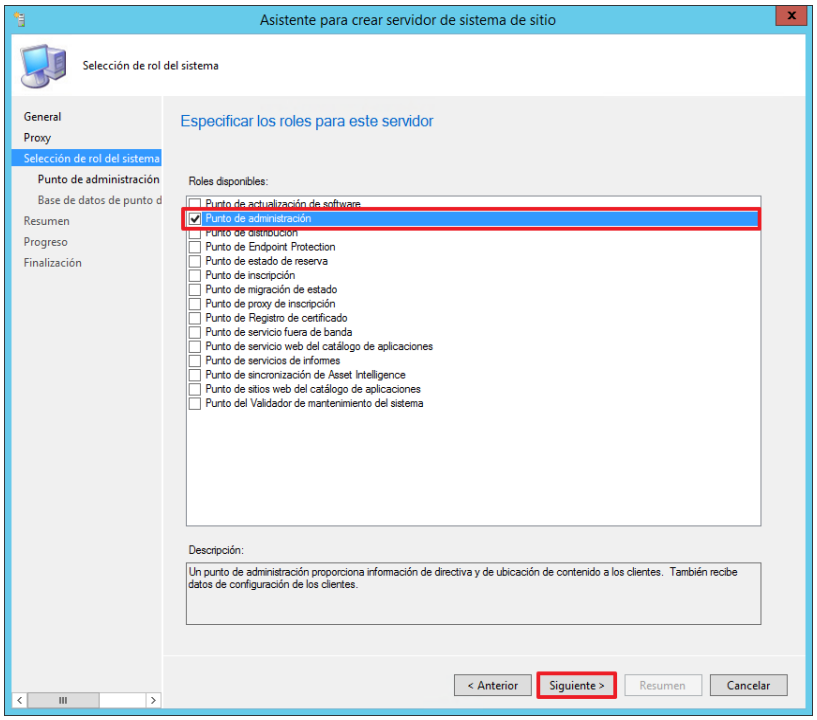
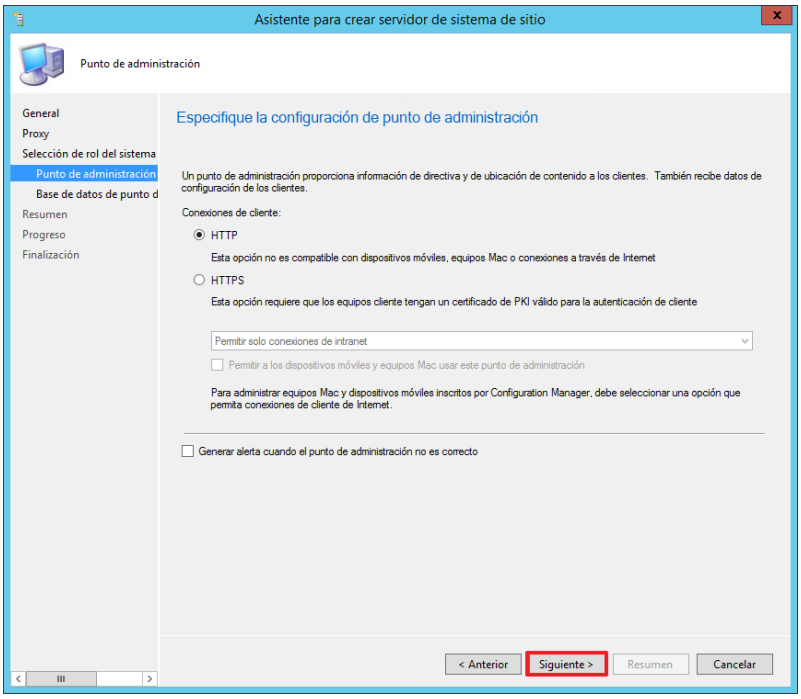
A continuación, se muestra un paso a paso en el que se detalla como agregar un servidor y a su vez como agregar un rol de sitio de MS SCCM 2012 R2.

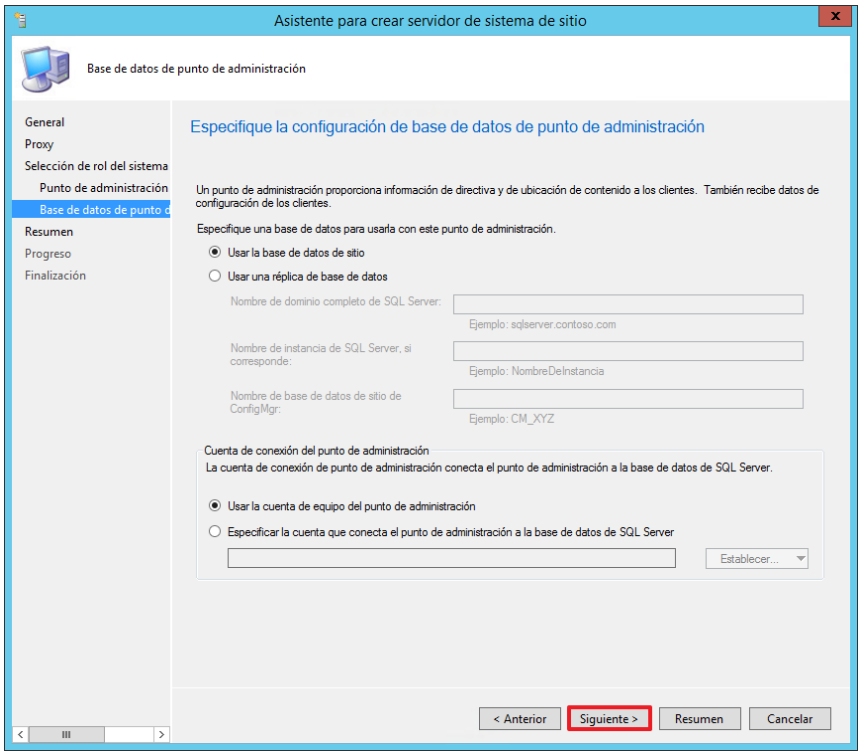
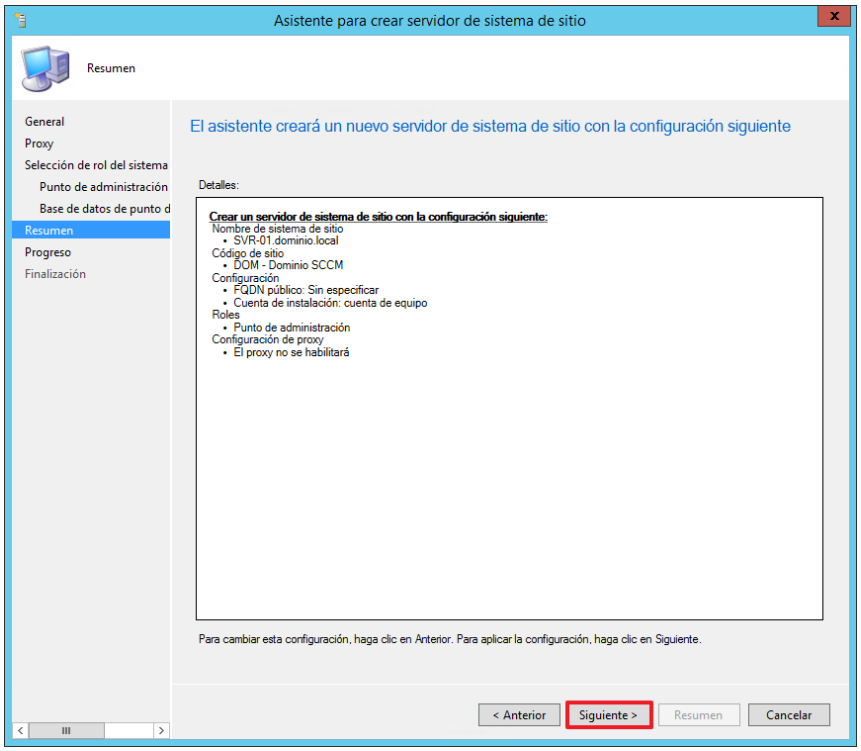
Paso	Descripción
348.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
349.	Pulse sobre el menú inicio. 
350.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

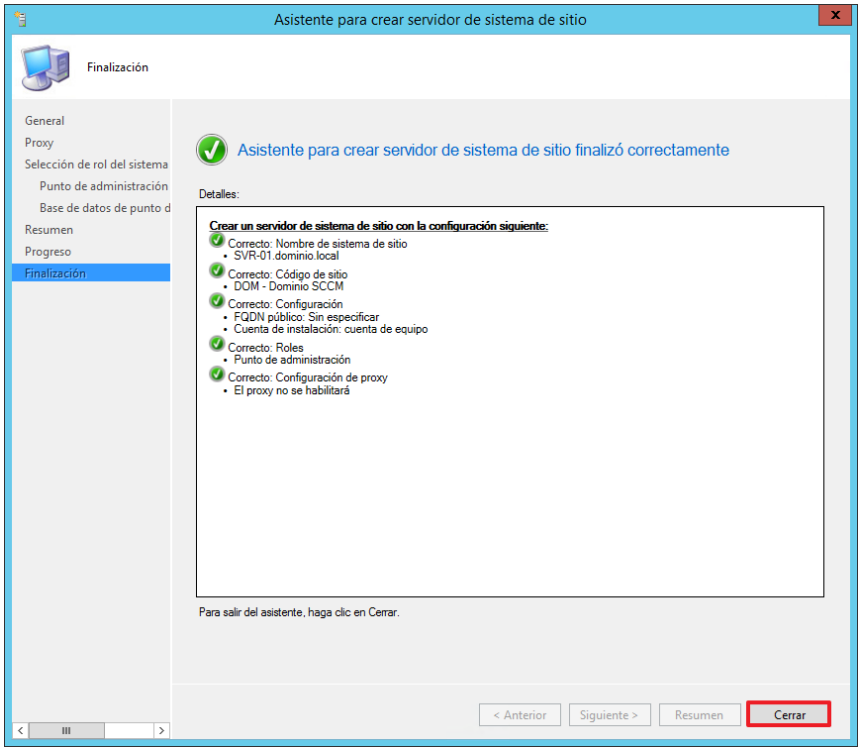
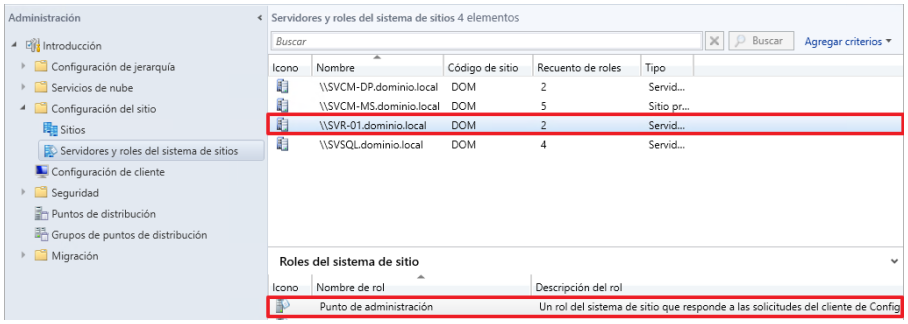
Paso	Descripción
351.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
352.	Seleccione el apartado “Administración”. 

Paso	Descripción
353.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 
354.	Pulse con el botón derecho sobre un espacio en blanco y seleccione la opción “crear servidor del sistema de sitio” para agregar un nuevo servidor al sitio ya creado.  **Nota:** Este paso contempla que usted ya tiene un sitio creado anteriormente y un servidor preparado para ser unido al sitio de Configuration Manager.

Paso	Descripción
355.	Seleccione el nombre del servidor que desea añadir y el sitio y pulse “Siguiente >”  **Nota:** Tanto el nombre del servidor como el del sitio han sido creados para elaborar la presente guía por lo que deberá adaptar estos pasos a su organización.
356.	En caso de que su servidor se conecte a internet a través de un proxy deberá configurar la presente pantalla, y pulsar “Siguiente >” para continuar. 

Paso	Descripción
357.	A continuación, seleccione el rol del sistema de sitio que quiere implementar en dicho servidor y pulse “Siguiente >”.  **Nota:** En el presente ejemplo se implementa el rol de “Punto de administración”, deberá adaptar estos pasos a los requerimientos de su organización.
358.	En los siguientes pasos, se va a establecer una configuración específica para el rol de “Punto de administración”, en caso de haber seleccionado otro rol del sistema de sitio deberá adaptar estos pasos a su organización. Pulse “Siguiente >” para continuar. 

Paso	Descripción
359.	Para avanzar con la configuración del rol del sistema de sitio. Pulse “Siguiente >” para continuar. 
360.	Pulse “Siguiente >” para continuar con la implementación. 

Paso	Descripción
361.	Compruebe que se ha creado el servidor de sitio correctamente y pulse “Cerrar” para finalizar el asistente. 
362.	Una vez realizada la implementación del servidor y del rol del sistema de sitio, verifique que el proceso ha sido correcto. 

7.9. BORRADO Y DESTRUCCIÓN

Las medidas de borrado y destrucción de información se aplicarán a todo tipo de equipos susceptibles de almacenar información.

MS SCCM 2012 R2 no permite eliminar una base de datos directamente por lo que será necesario iniciar sesión en el servidor que aloje la base de datos de sitio. Se debe tener en consideración que el usuario que realiza la acción debe tener los permisos adecuados y una vez desvinculado se deberá eliminar físicamente la carpeta contenedora de la información, y si desea eliminar el soporte de dicha información deberá proceder siguiendo el procedimiento marcado en el borrado y destrucción de soportes físicos que establece el ENS.

Nota: Si desea obtener más información sobre el borrado de bases de datos de Microsoft SQL Server puede visitar el sitio web: https://technet.microsoft.com/es-es/library/ms177419(v=sql.110).aspx

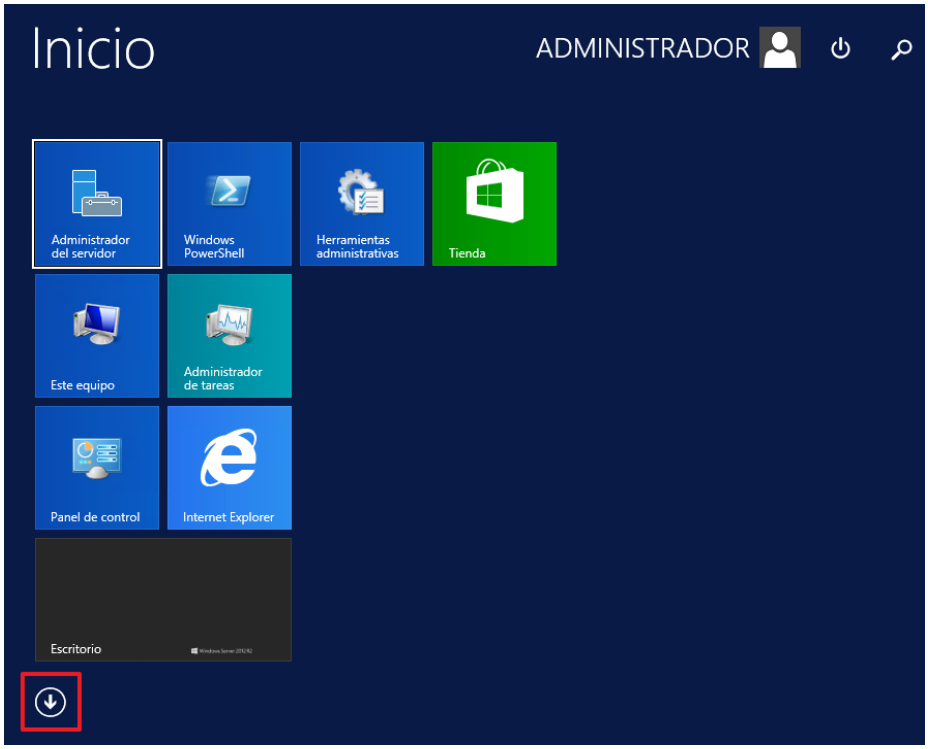
7.10.COPIAS DE SEGURIDAD

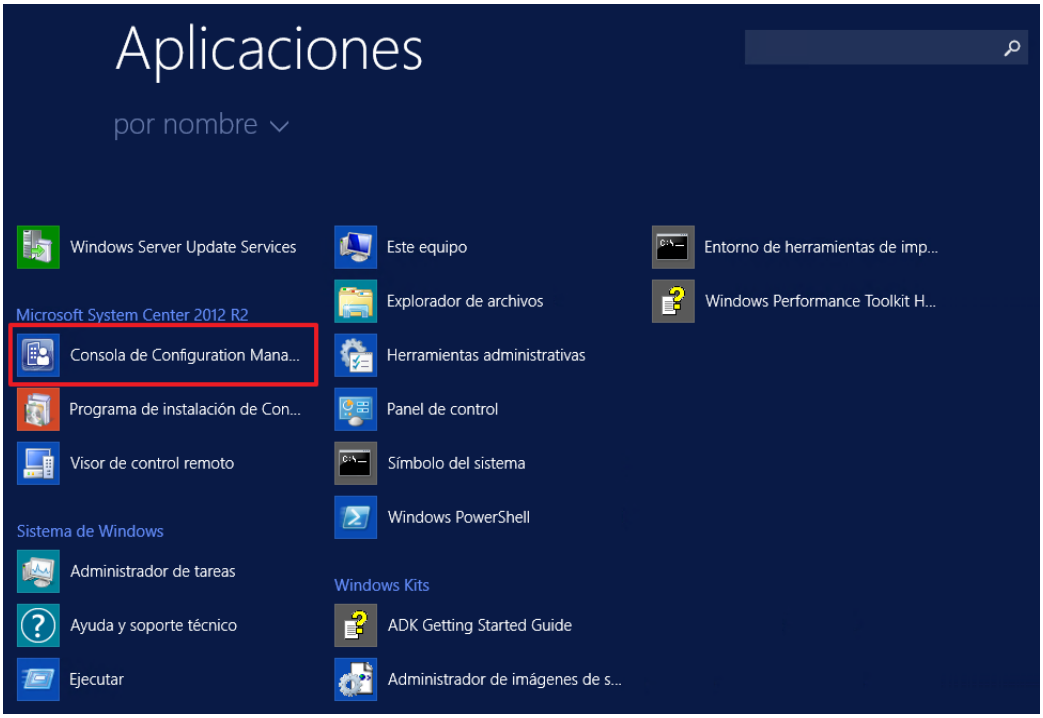
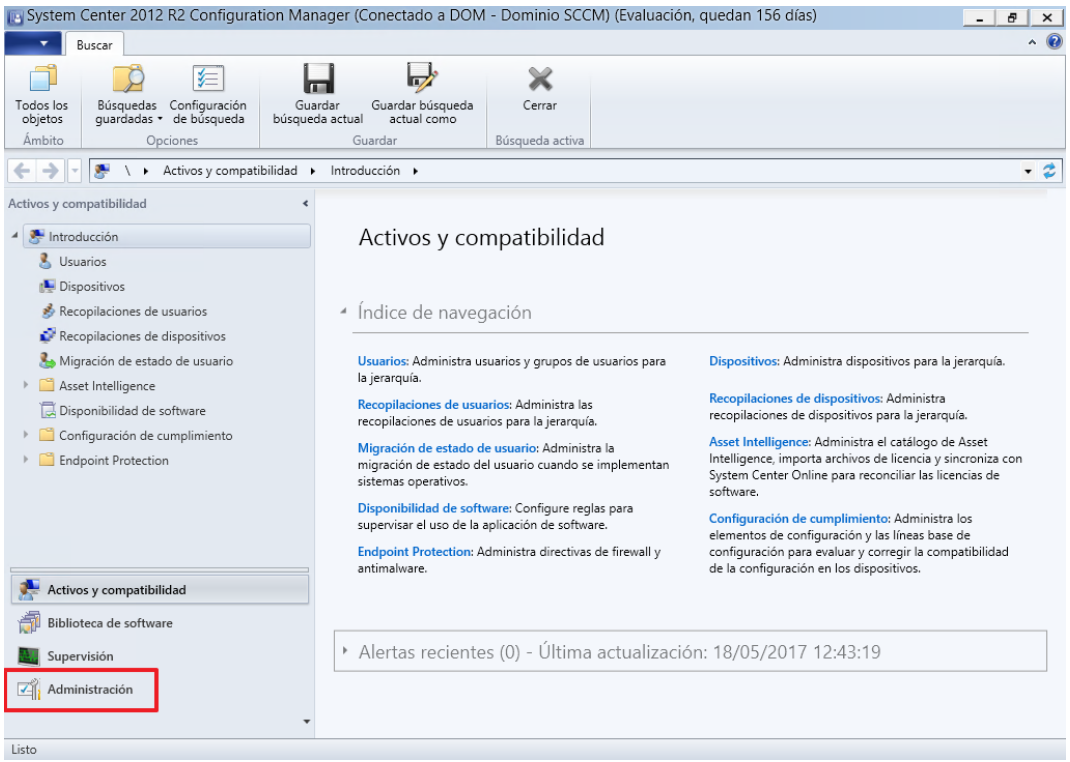
MS SCCM 2012 R2 permite realizar copias de seguridad de los sitios, así como de las bases de datos de los sitios, para en caso de desastre, tener la posibilidad de restaurar el sistema en el menor tiempo posible y minimizar al máximo una posible pérdida de información.

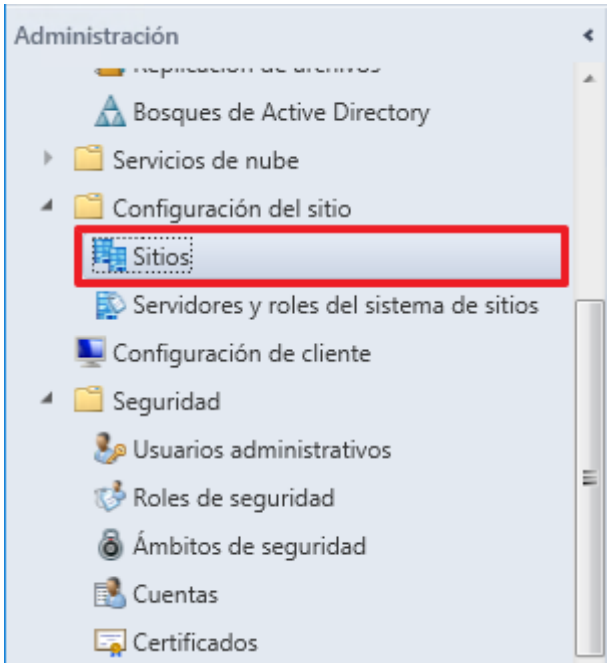
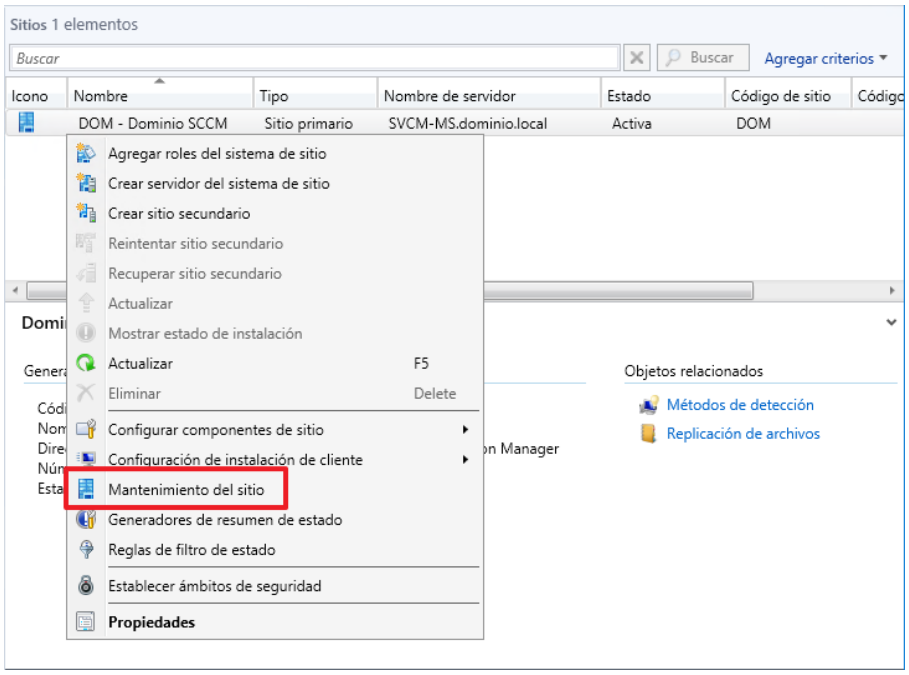
Tal y como se establece en el ENS las copias de seguridad conservarán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.

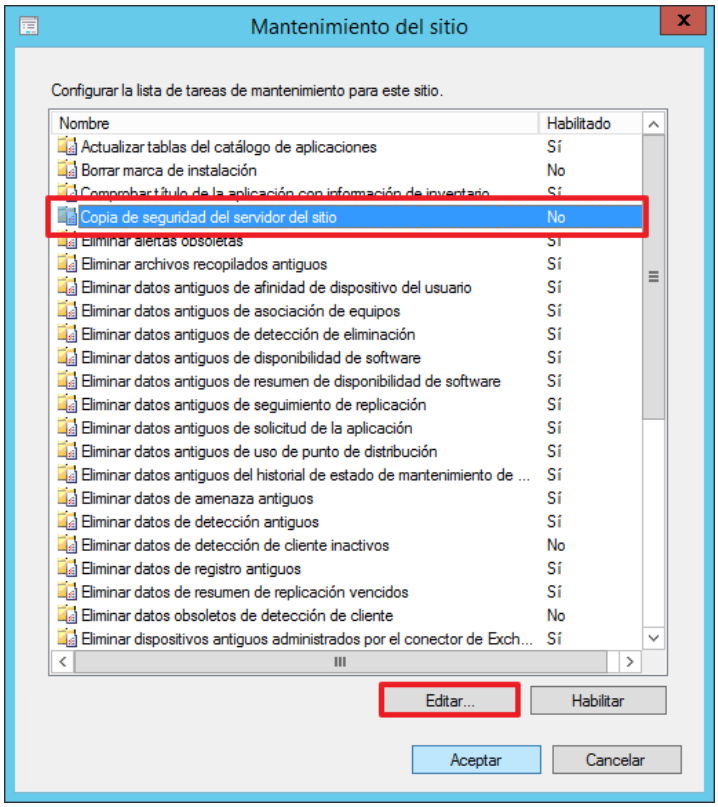
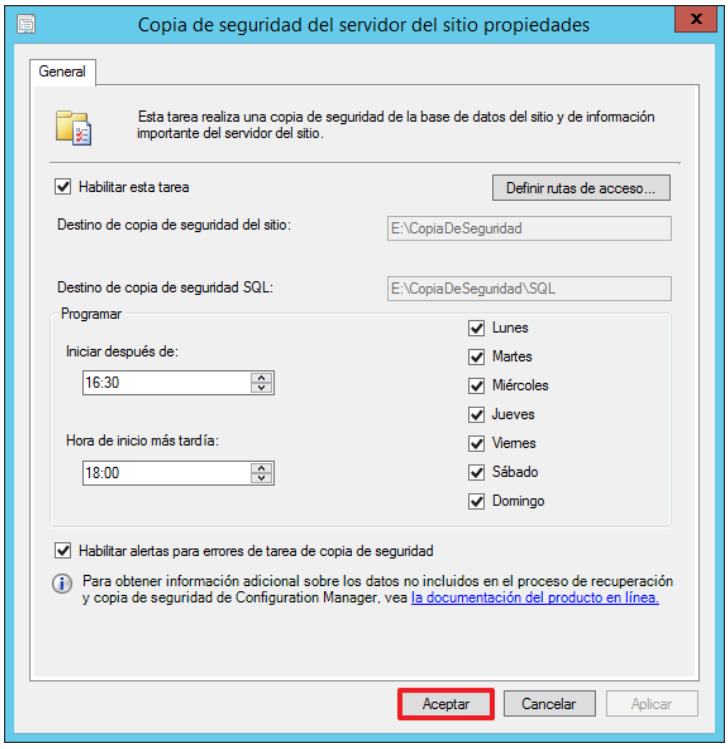
Para los niveles medio y alto de seguridad según lo establecido en el ENS se recomienda que el acceso a la ubicación de las copias de seguridad sea limitado exclusivamente al personal autorizado con el fin de evitar poner en riesgo la una posible manipulación malintencionada de los datos almacenados.

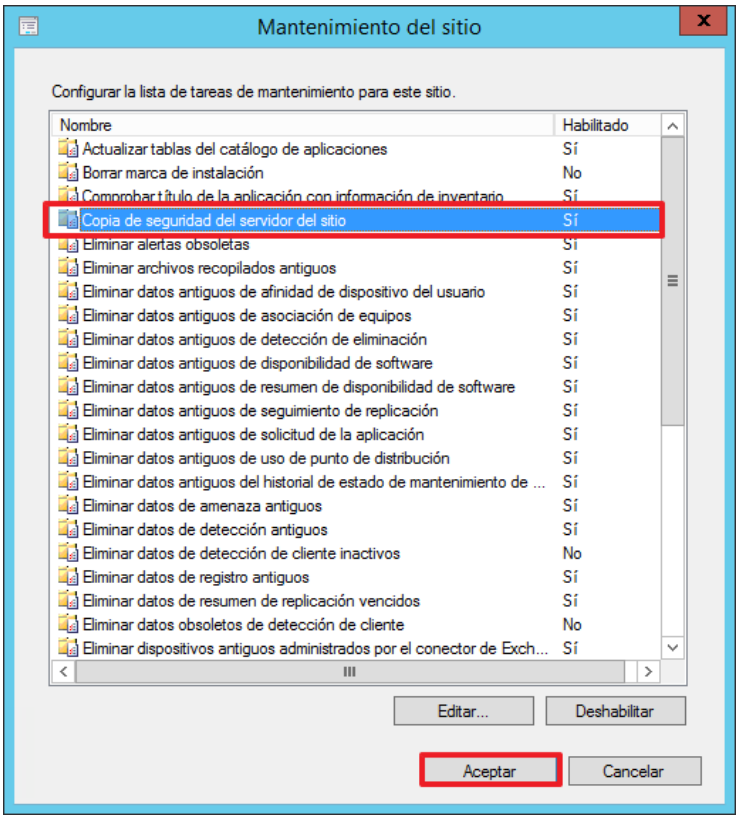
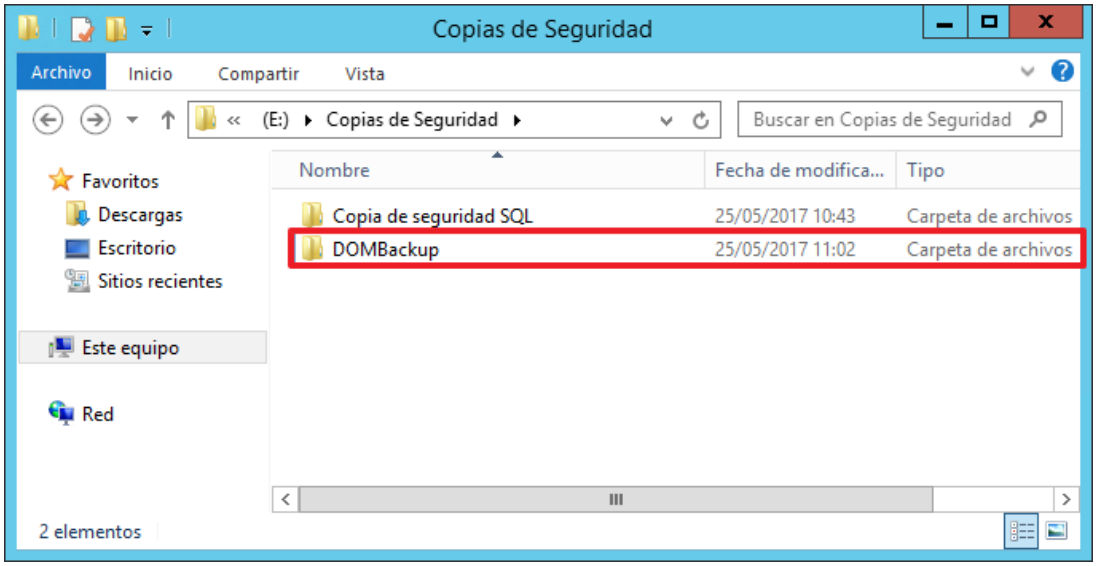
A continuación, se muestra un paso a paso de como habilitar las copias de seguridad de un sitio.

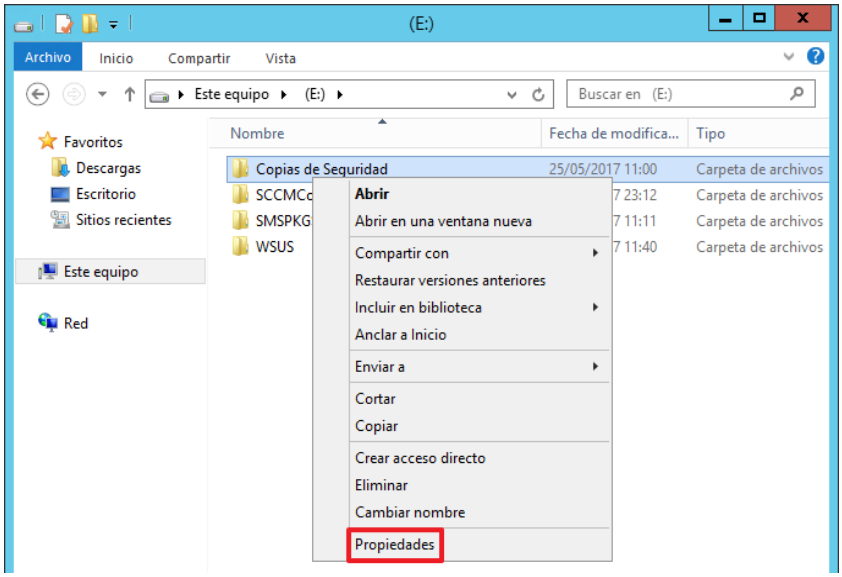
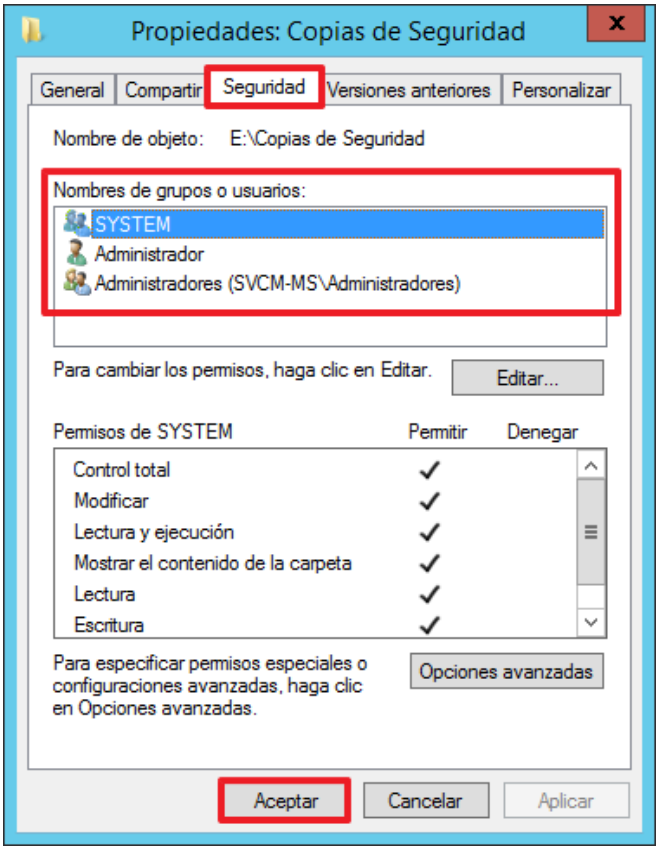
Paso	Descripción
363.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
364.	Pulse sobre el menú inicio. 
365.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
366.	Marque con el botón Izquierdo sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
367.	Seleccione el apartado “Administración”. 

Paso	Descripción
368.	Despliegue “**Configuración del sitio > Sitios**”. 
369.	Localice el sitio sobre el que desea habilitar las copias de seguridad, pulse con el botón derecho sobre el sitio y seleccione la opción “Mantenimiento del sitio” del menú contextual. 

Paso	Descripción
370.	Localice la opción “Copia de seguridad del servidor del sitio” y pulse sobre el botón “Editar”. 
371.	Configure los parámetros adecuándolos a su organización y pulse “Aceptar” para guardar la configuración. 

Paso	Descripción
372.	Confirme que la opción “Copia de seguridad del servidor del sitio” está habilitada y pulse “Aceptar” para cerrar las opciones de mantenimiento del sitio. 
373.	Una vez realizada la copia de seguridad, diríjase a la ruta en la que se almacenan las copias de seguridad y compruebe que se están realizando correctamente. 

Paso	Descripción
374.	En el directorio raíz donde tiene ubicadas las copias de seguridad, seleccione la carpeta y pulse la opción “Propiedades” del menú contextual. 
375.	Seleccione la pestaña “Seguridad” y compruebe que los grupos y usuarios que aparecen tienen los permisos adecuados de acceso a los datos de las copias de seguridad. Pulse “Aceptar” cuando haya verificado que los datos son los correctos.  **Nota:** Deberá dar permisos de acceso a la carpeta “Copias de seguridad” únicamente al personal autorizado de gestionar los datos de copias de seguridad del sitio.

ANEXO B.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL MEDIO DEL ENS

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores MS SCCM 2012 R2 sobre Microsoft Windows Server 2012 R2 con implementación de seguridad de nivel medio del ENS.

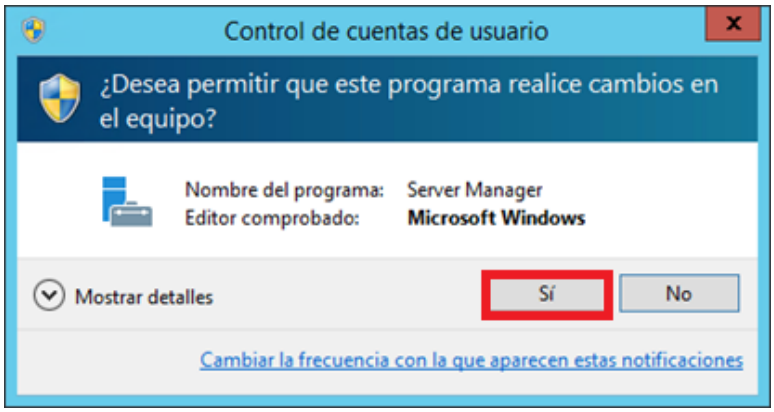
Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

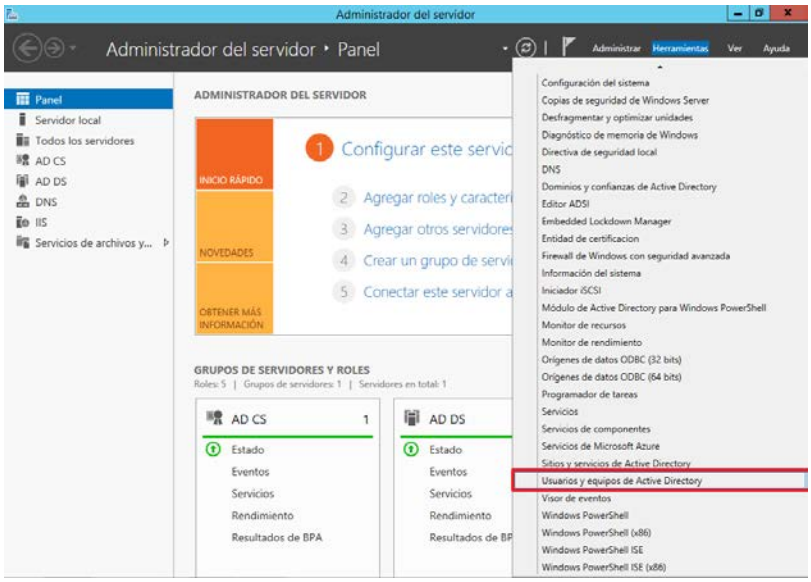
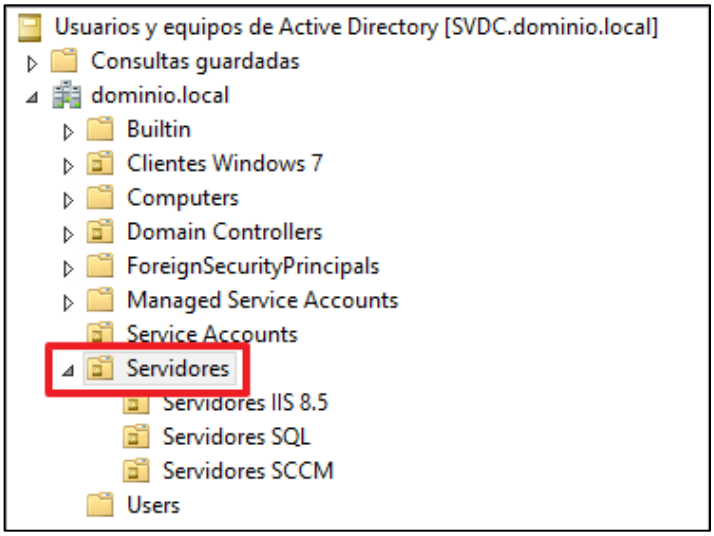
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

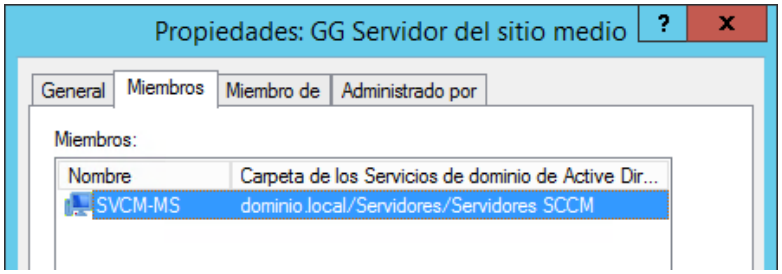
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

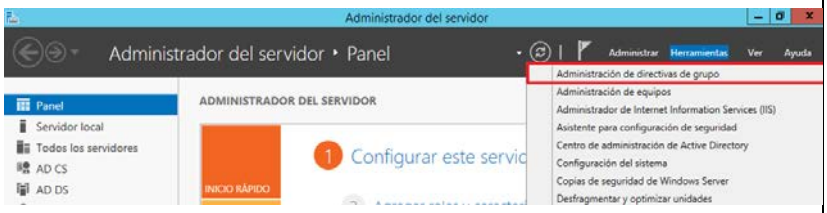
a) Administrador de directivas de grupo (gpmc.msc)

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

Comprobación	OK/NOK	Como hacerlo
1. Inicie sesión en un controlador de dominio		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Pulse "Sí" en la ventana que se muestra a continuación. 

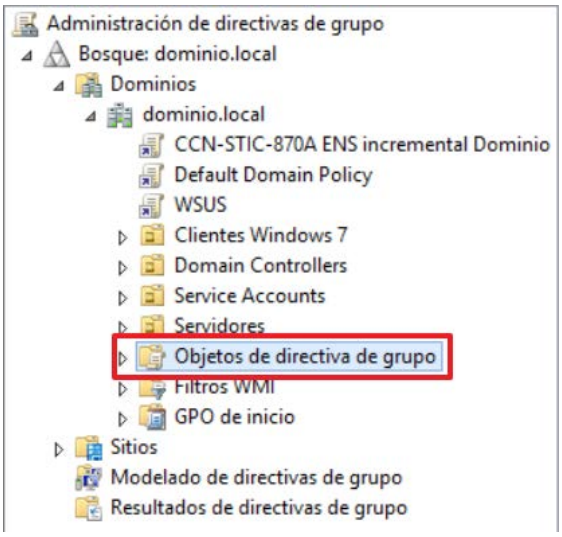
Comprobación	OK/NOK	Como hacerlo
2. Verifique que están creados los grupos de seguridad global.		Ejecute la herramienta "Usuarios y equipos de Active Directory". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio. Seleccione el contenedor "Servidores SCCM" y "Servidores SQL", situados en la siguiente ruta: "**Usuarios y equipos de Active Directory → [Su dominio] → Servidores**". Verifique que están creados los grupos de seguridad en función de los roles de sistema de sitio que ha reforzado la seguridad. 

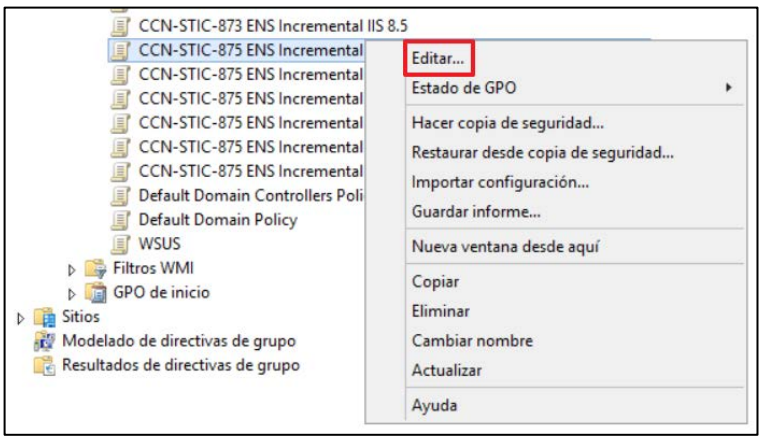
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="2">Como hacerlo</th></tr>
<tr><td></td><td colspan="2">Grupo de seguridad</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">GG Servidor Base de datos del sitio medio</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de servicios de informes medio</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor del sitio medio</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de administración medio</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de distribución medio</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de actualización de software medio</td><td></td></tr>
<tr><td>3. Verifique que los servidores que han sido catalogados correctamente</td><td></td><td colspan="2">Pulse doble clic sobre cada grupo de seguridad y seleccione la pestaña “Miembros” para verificar que los servidores que corresponden a este grupo de seguridad aparecen en el listado.
 

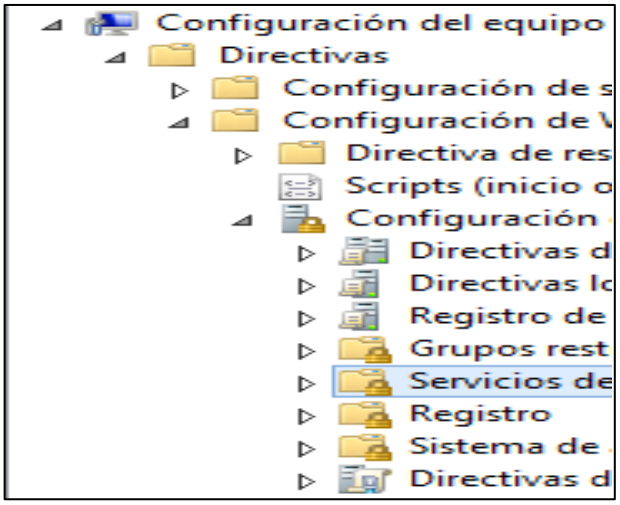
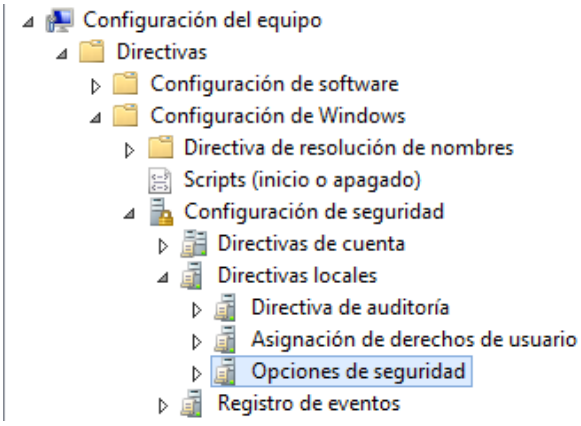
Nota: La imagen mostrada anteriormente corresponde a un ejemplo de los miembros del grupo de seguridad “GG Servidor del sitio medio”, deberá realizar esta comprobación en todos los grupos de seguridad correspondientes y verificar que aparecen los servidores que pertenecen a cada grupo.</td></tr>
<tr><td>4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.</td><td></td><td colspan="2">Ejecute la herramienta “Administrador de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: “Herramientas → Administración de directivas de grupo”.
 

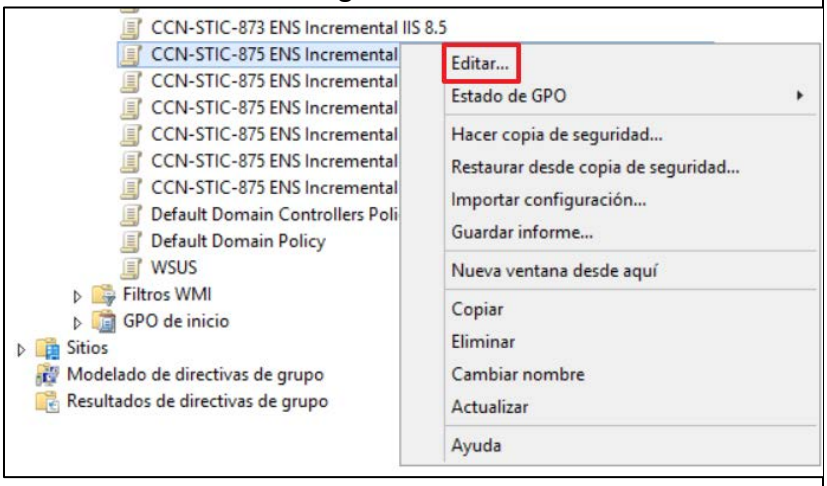
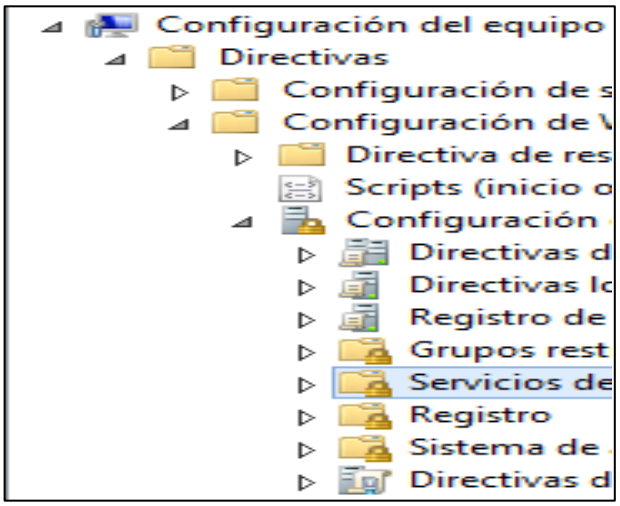
Nota: Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio.

Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”.
Verifique que están creados los objetos de directiva de grupo en función de los roles de sistema de sitio que ha reforzado la seguridad y que en la columna “Estado de GPO” figuran como habilitadas.</td></tr>
</table>

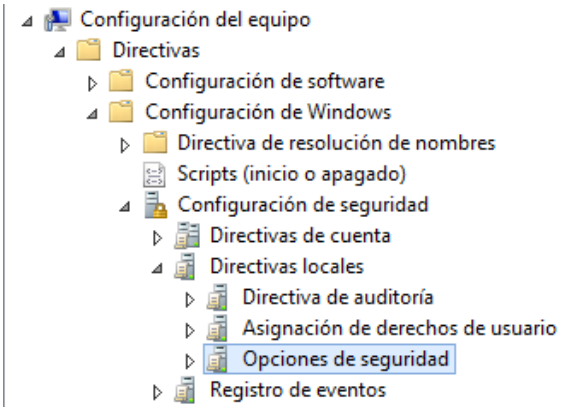
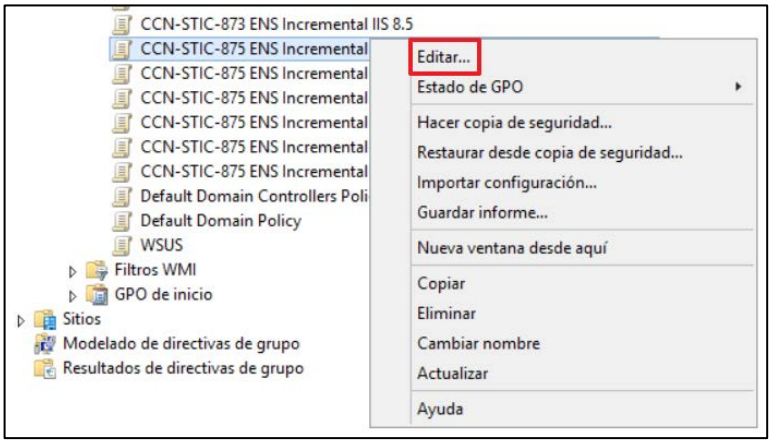
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td> 

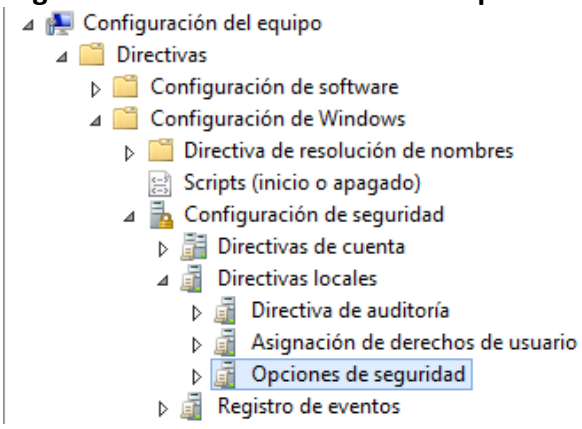
<table>
<tr><th>Grupo de seguridad</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de actualización de software medio</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de administración medio</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de distribución medio</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de servicios de informes medio</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Servidor del sitio medio</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de -SQL medio</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
<tr><td>5. Verifique la configuración de la directiva</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de actualización de software medio” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

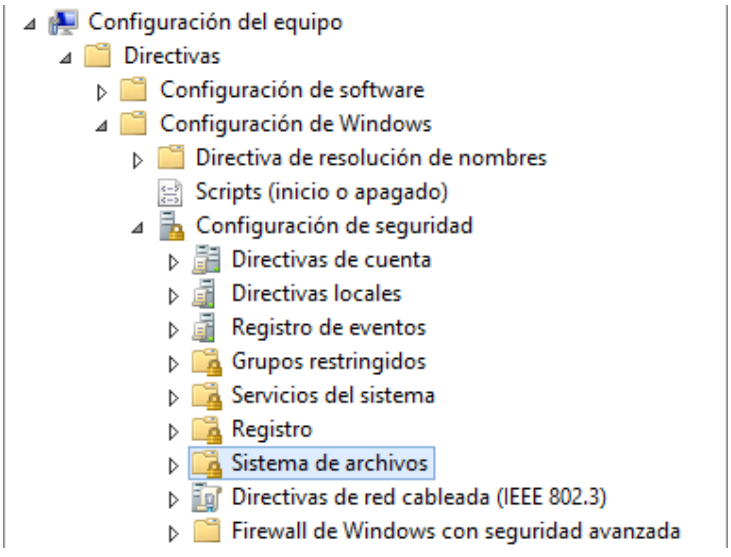
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>6. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”.
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>Administración remota de Windows (WS-Management)</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>Servicio de transferencia inteligente en segundo plano (BITS)</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>Servidor</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>WSusCertServer</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>WsusService</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
<tr><td>7. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Como 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>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>8. Verifique la configuración de la directiva</td><td></td><td colspan="3">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de administración medio” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>9. Verifique los servicios del sistema.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

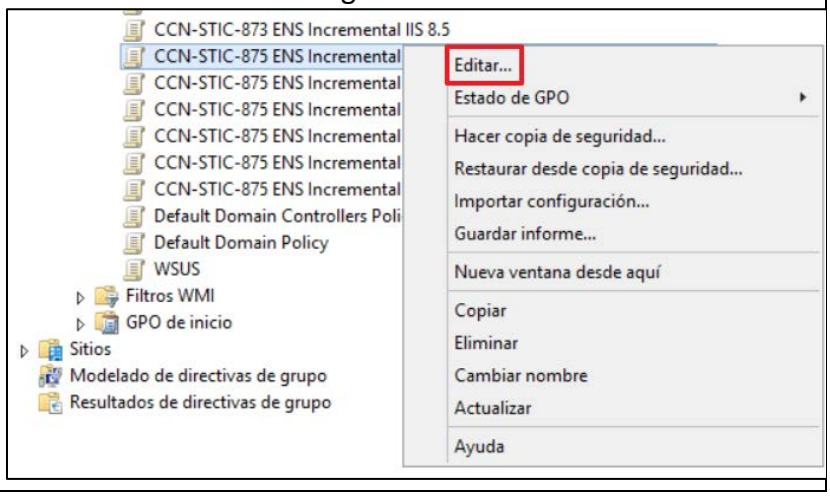
<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
</table>

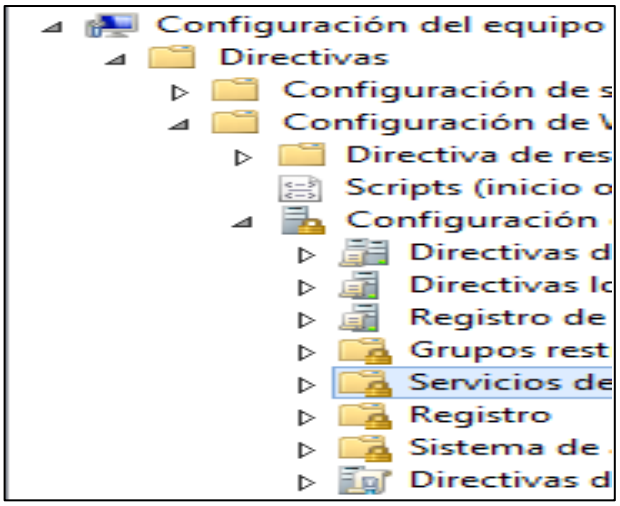
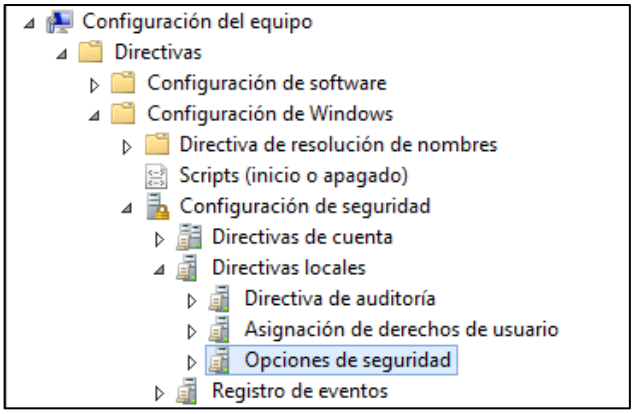
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td rowspan="4">10. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td colspan="2">Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td colspan="2">Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
<tr><td>11. Verifique la configuración de la directiva</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución medio” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

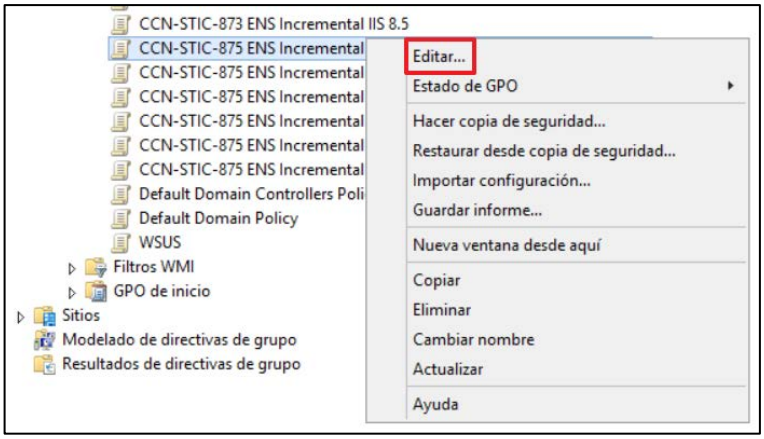
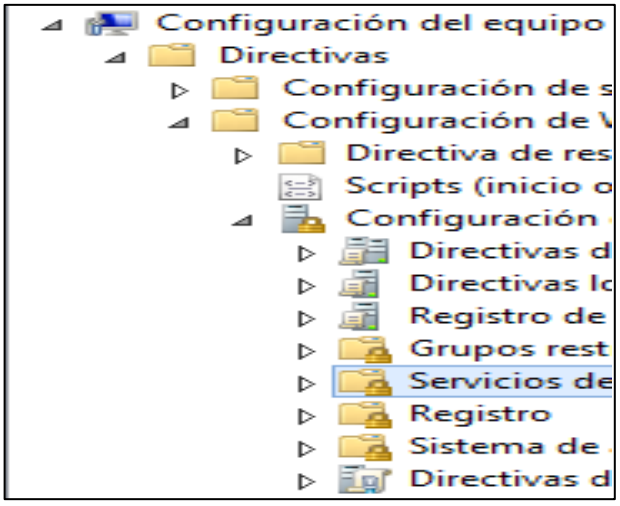
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>12. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>13. Verifique la configuración del Sistema de archivos</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos”.
 

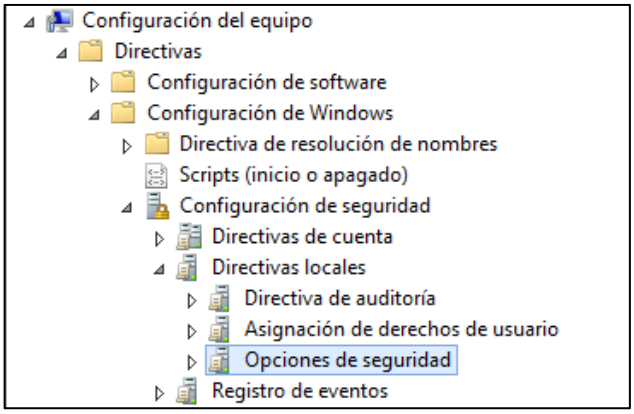
Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades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

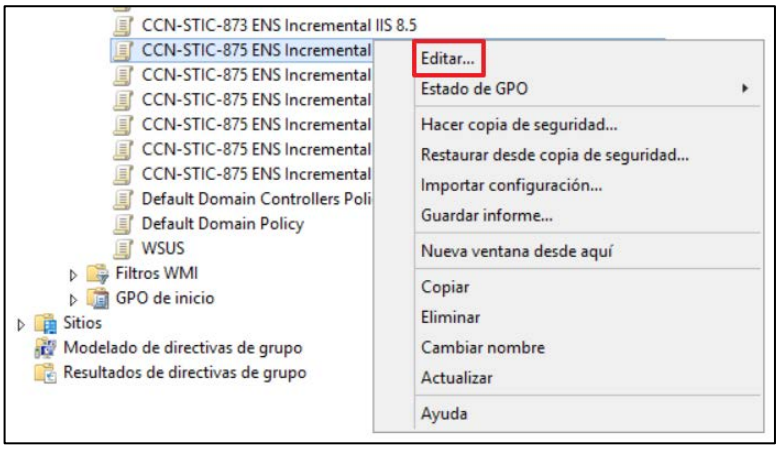
Comprobación	OK/NOK	Como hacerlo			
		Archivo	Usuario	Permiso	OK/NOK
		E:\SCCMContentLib	Administradores	Control total	
			SYSTEM	Control total	
			Usuarios	Leer	
		E:\SMS_DP$	SYSTEM	Control total	
			Administradores	Control total	
			Administrador	Control total	
		E:\SMSPKGE$	Administradores	Control total	
			Usuarios	Leer y ejecutar	
		E:\SMSSIG	IUSR	Escribir (Denegar)	
			SYSTEM	Control total	
			Administradores	Control total	
			Usuarios	Leer	
14. Verifique la configuración de la directiva		Seleccione el objeto de directiva de grupo "**CCN-STIC-875 ENS Incremental Punto de servicios de informes medio**" y pulse la opción "Editar…". Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones. 			

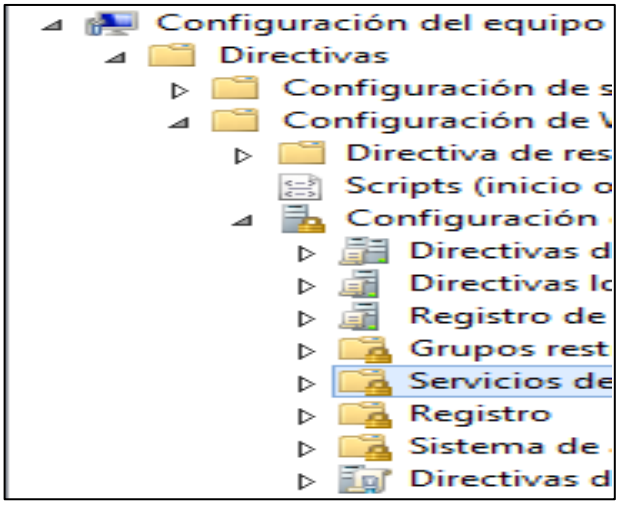
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>15. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
<tr><td>16. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
</table>

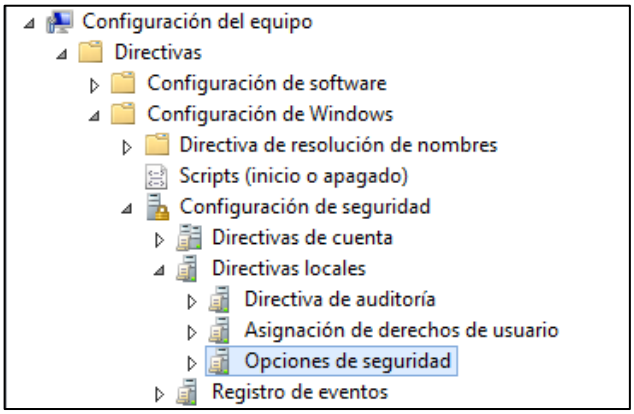
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>17. Verifique la configuración de la directiva</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental servidor del sitio medio” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>18. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

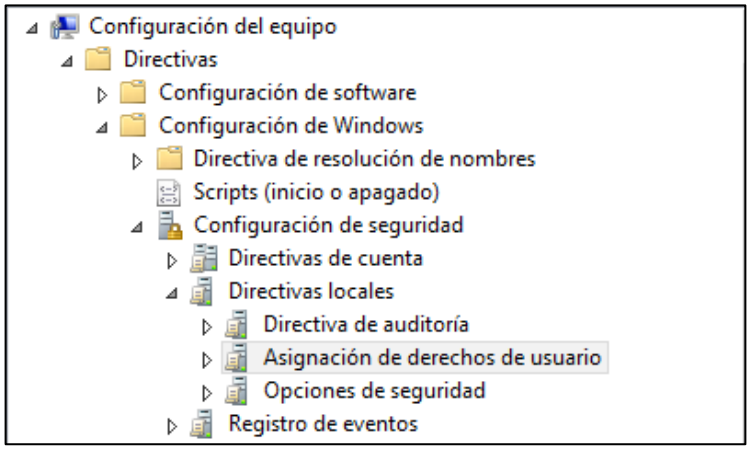
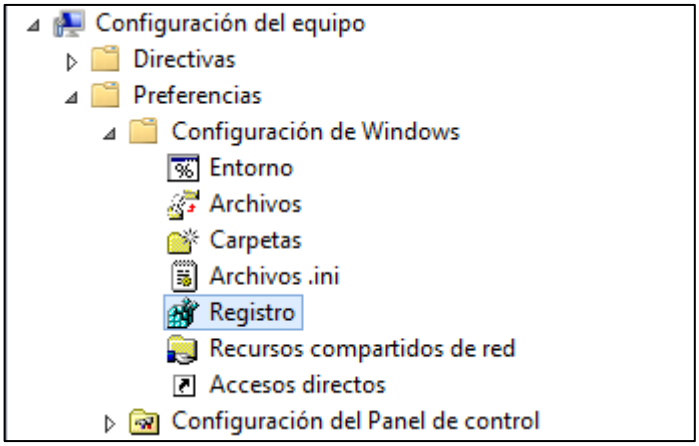
<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_SITE_VSS_WRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_COMPONENT_MANAGER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>CcmExec</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_NOTIFICATION_SERVER</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_BACKUP</td><td>Manual</td><td>Configurado</td><td></td></tr>
</table></td></tr>
</table>

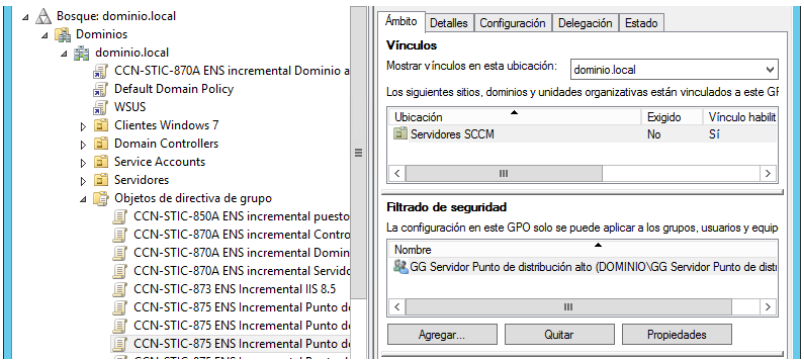
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>19. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>20. Verifique la configuración de la directiva</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental SQL medio” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>21. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>MSSQLSERVER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLSERVERAGENT</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLWRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table>
Nota: Deberá adaptar el servicio SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL, por el servicio configurado con el nombre de dominio de su organización.</td></tr>
<tr><td>22. Verifique las opciones de seguridad</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Como hacerlo</th></tr>
<tr><td></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td></td><td colspan="2">Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
<tr><td>23. Verifique la asignación de derechos de usuario</td><td></td><td colspan="3">Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos usuario”.
 
</td></tr>
<tr><td></td><td colspan="2">Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">Inicio de sesión como servicio</td><td>DOMINIO\SQLServiceAccount</td><td></td></tr>
<tr><td></td><td colspan="4">Nota: Deberá adaptar estos pasos a su organización y comprobar que el usuario con permisos de inicio de sesión como servicio es el adecuado.</td></tr>
<tr><td>24. Verifique las preferencias de registro</td><td></td><td colspan="3">Seleccione el siguiente nodo. “Configuración del Equipo → Preferencias → Configuración de Windows → Registro.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Como hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Parametro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>DisabledByDefault</td><td>Acción: Actualización
subárbol: HKEY_LOCAL_MACHINE
Clave: SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Client
Tipo: REG_DWORD
Valor: 00000000</td><td></td></tr>
<tr><td>Enabled</td><td>Acción: Actualización
subárbol: HKEY_LOCAL_MACHINE
Clave: SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Server
Tipo: REG_DWORD
Valor: 00000001</td><td></td></tr>
</table></td></tr>
<tr><td>25. Verifique que cada objeto de directiva de tiene definido el filtro de seguridad correspondiente</td><td></td><td colspan="3">En el árbol de la izquierda, pulse doble clic sobre el objeto de directiva de grupo: “Bosques [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo”
Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo seguridad correspondiente a cada objeto de directiva de grupo.
 

Nota: La imagen mostrada anteriormente corresponde a un ejemplo del filtro de seguridad del objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución medio” al que corresponde el filtro de seguridad “GG Servidor punto de distribución medio”, deberá realizar esta comprobación en todos los objetos de directivas de grupo correspondientes y verificar que están vinculados los grupos de seguridad que pertenecen a cada directiva.</td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo		
		Directiva	Grupo de seguridad	OK/NOK
		CCN-STIC-875 ENS Incremental Punto de actualización de software medio	GG Servidor Punto de actualización de software medio	
		CCN-STIC-875 ENS Incremental Punto de administración medio	GG Servidor Punto de administración medio	
		CCN-STIC-875 ENS Incremental Punto de distribución medio	GG Servidor Punto de distribución medio	
		CCN-STIC-875 ENS Incremental Punto de servicios de informes medio	GG Servidor Punto de servicios de informes medio	
		CCN-STIC-875 ENS Incremental Servidor del sitio medio	GG Servidor del sitio medio	
		CCN-STIC-875 ENS Incremental Punto de SQL medio	GG Servidor Base de datos del sitio medio	

2. COMPROBACIONES EN SERVIDOR MIEMBRO

Para realizar las comprobaciones pertinentes en los servidores miembros, se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

a) Administrador del Servidor

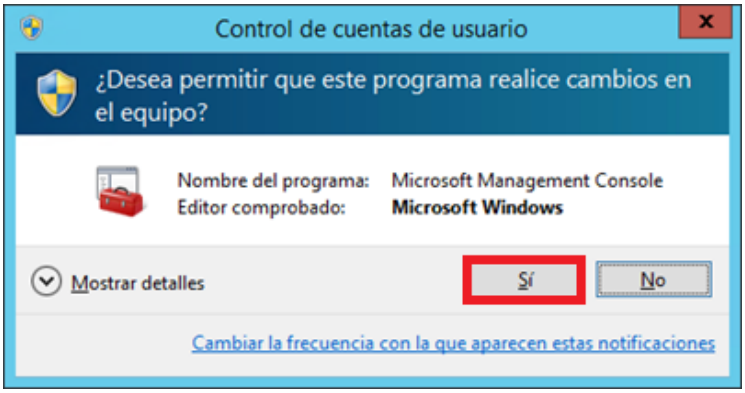
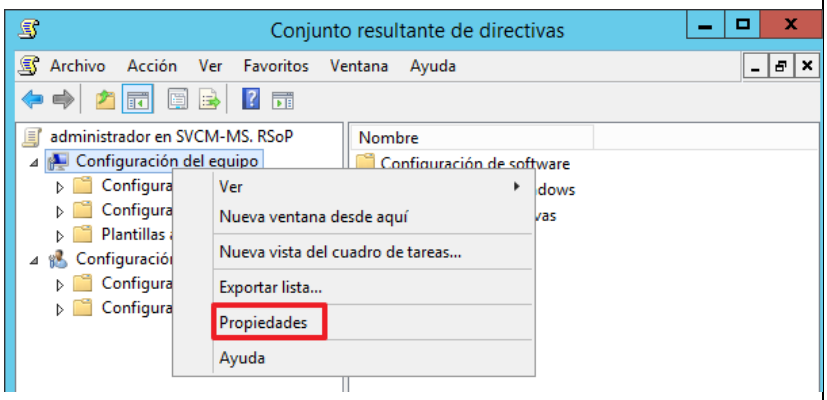
b) Conjunto resultante de directivas (rsop.msc)

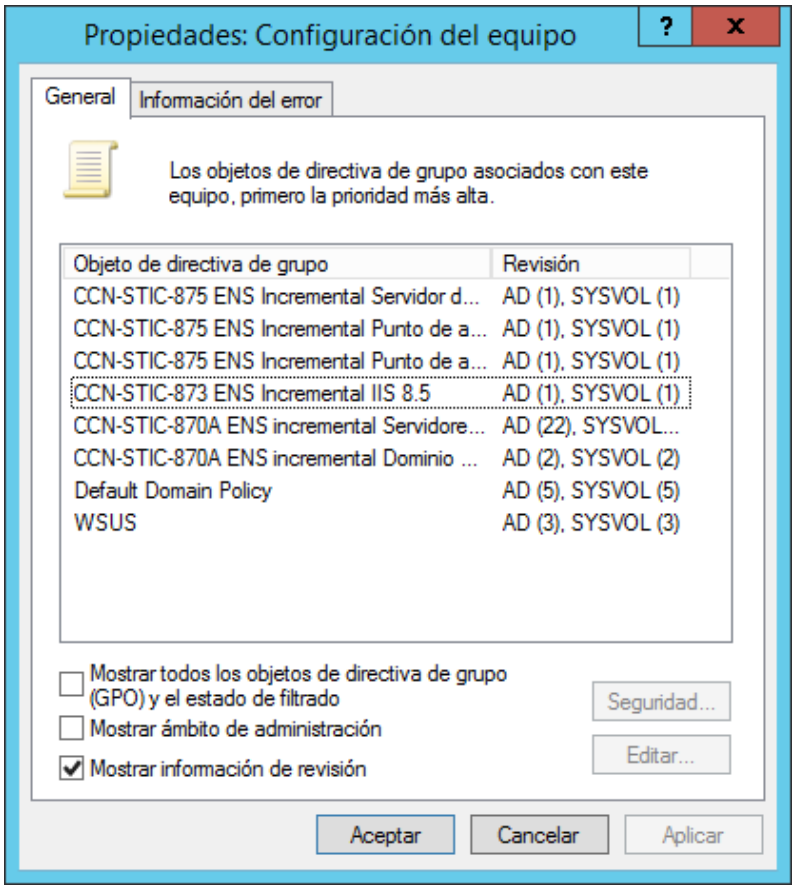
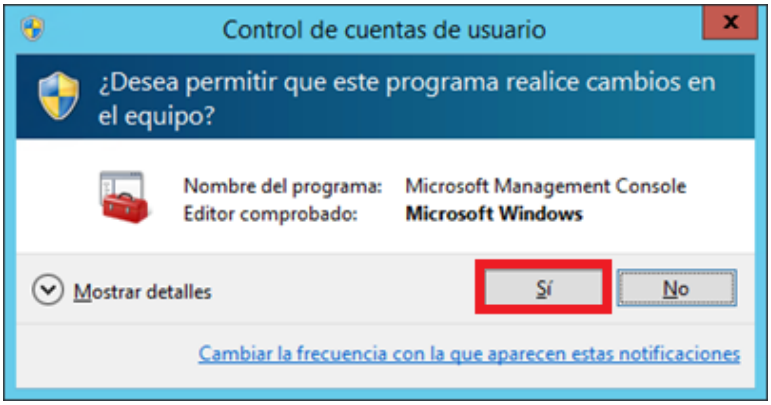
c) Consola de servicios (services.msc)

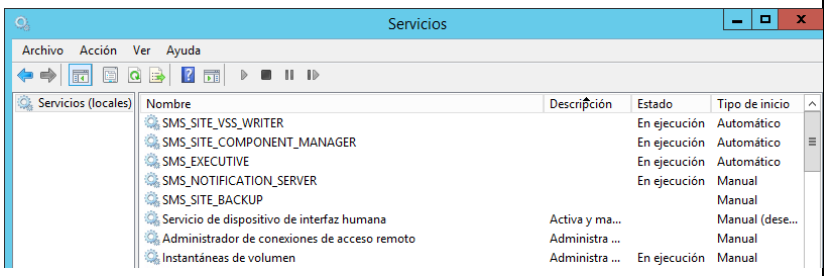
d) Editor de registro (regedit.exe)

e) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Como hacerlo
26. Inicie sesión en un servidor miembro del dominio		En uno de los servidores miembro del dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

Comprobación	OK/NOK	Como hacerlo
27. Verifique que el equipo ha recibido la directiva de grupo correspondiente con el rol de sistema de sitio que esta implementado.		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación.  Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura:  En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo". Verifique que en dicha sección aparecen listados, los objetos de directiva de grupo correspondientes con el servidor miembro que está comprobando.

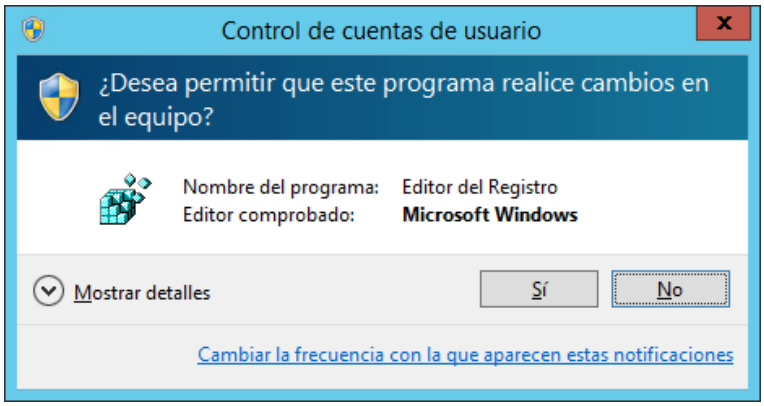
Comprobación	OK/NOK	Como hacerlo
		 **Nota:** Se debe tener en consideración que el listado de objetos de directivas de grupo variara en función del servidor miembro que este comprobando y de los roles de sistema de sitio que dicho servidor tenga implementado.
28. Verifique que los servicios del sistema están correctamente configurados		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Pulse "Sí" en la ventana que se muestra a continuación. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td>Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:
 

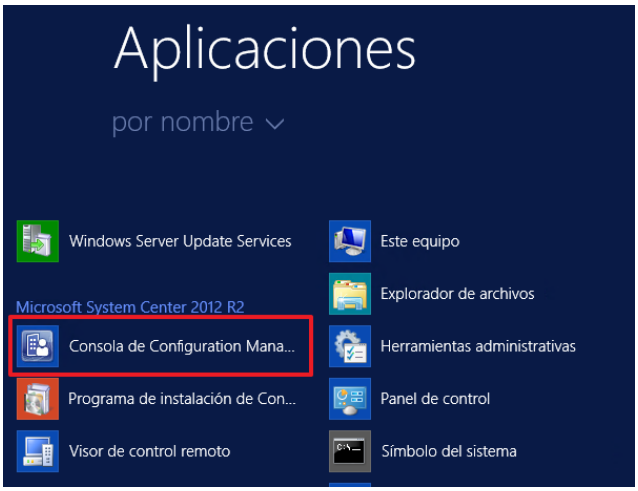
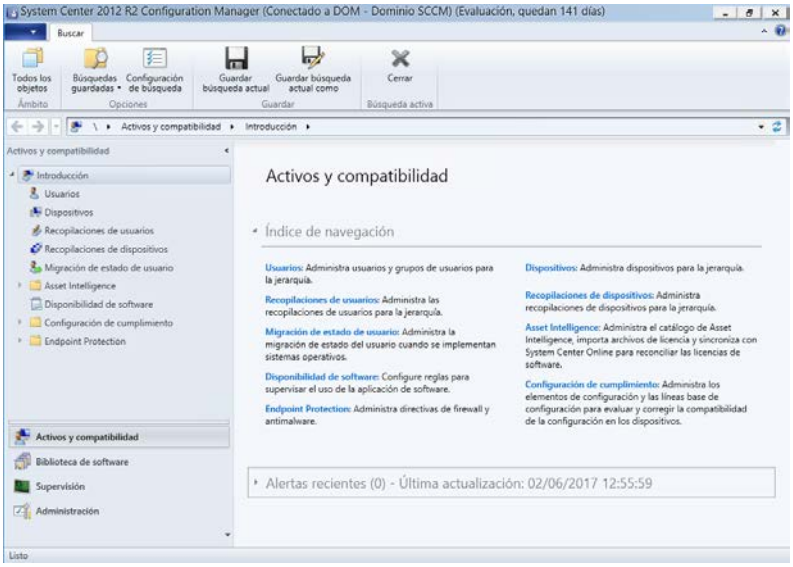
Nota: Dependiendo del servidor miembro que este comprobando y del rol del sistema de sitio implementado, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.</td></tr>
</table>

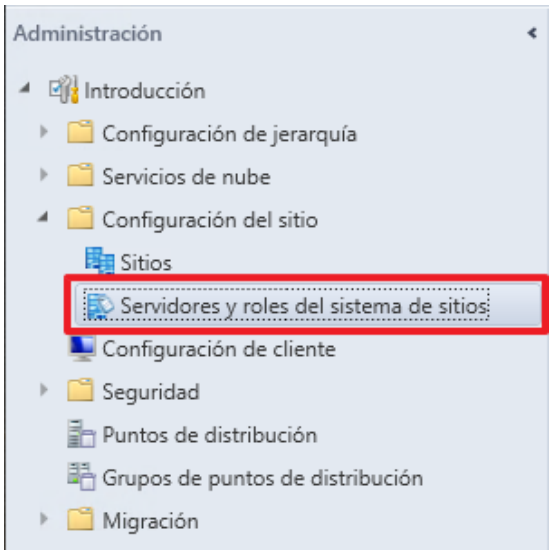
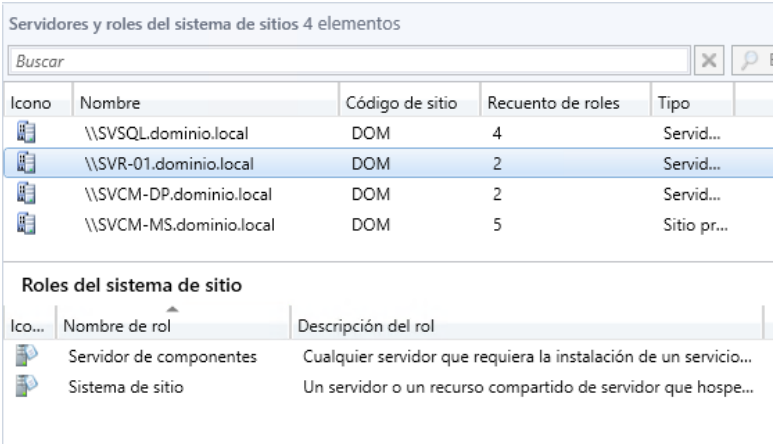
Directiva	Servicio	Iniciado	Permiso	OK/NOK
CCN-STIC-875 ENS Incremental Punto de actualización de software medio	Administración remota de Windows (WS-Management)	Automático	Configurado	
	Servicio de transferencia inteligente en segundo plano (BITS)	Automático	Configurado	
	Servidor	Automático	Configurado	
	WSusCertServer	Automático	Configurado	
	WsusService	Automático	Configurado	
CCN-STIC-875 ENS Incremental Punto de administración medio	SMS_EXECUTIVE	Automático	Configurado	
CCN-STIC-875 ENS Incremental Punto de servicios de informes medio	SMS_EXECUTIVE	Automático	Configurado	

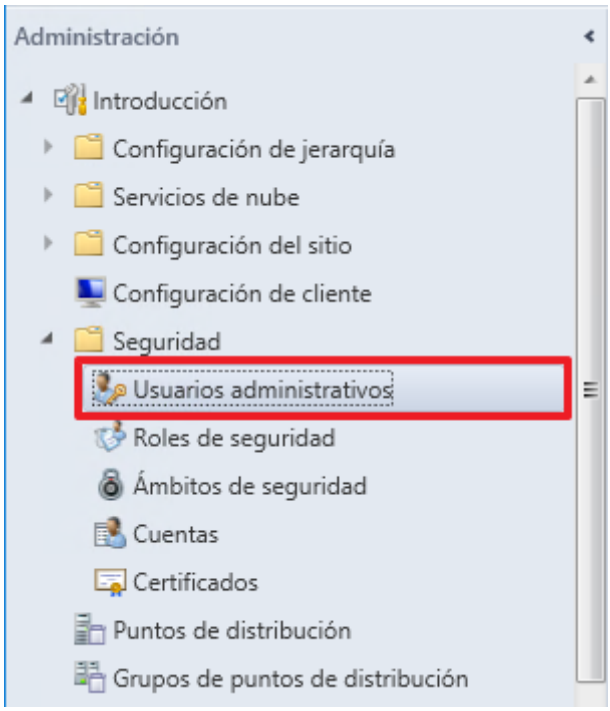
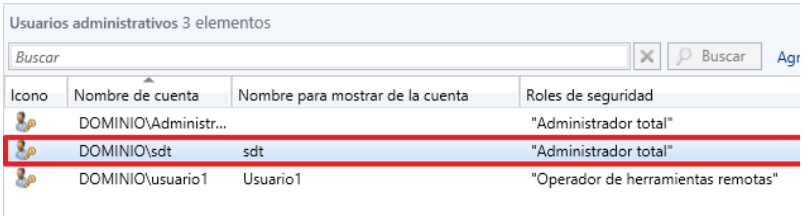
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="5">Como hacerlo</th></tr>
<tr><td rowspan="11"></td><td rowspan="11"></td><td>Directiva</td><td>Servicio</td><td>Iniciado</td><td>Permiso</td><td>OK/NOK</td></tr>
<tr><td rowspan="5">CCN-STIC-875 ENS Incremental servidor del sitio medio</td><td>SMS_SITE_VSS_WRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_COMPONENT_MANAGER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>CcmExec</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_NOTIFICATION_SERVER</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_BACKUP</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td rowspan="4">CCN-STIC-875 ENS Incremental SQL medio</td><td>MSSQLSERVER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLSERVERAGENT</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLWRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td colspan="5">Nota: Deberá adaptar el servicio SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL, por el servicio configurado con el nombre de dominio de su organización.</td></tr>
<tr><td>29. Verifique que se han asignado los permisos correctos en el sistema de archivos.</td><td></td><td colspan="5">En los servidores miembro donde tenga implementado el rol de sistema de sitio de Punto de distribución y se le esté aplicando la directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución medio”. Verifique los permisos asignados utilizando el Explorador de Windows: “Windows+R → Explorer”.
En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada.
Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña “Seguridad”. En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados</td></tr>
</table>

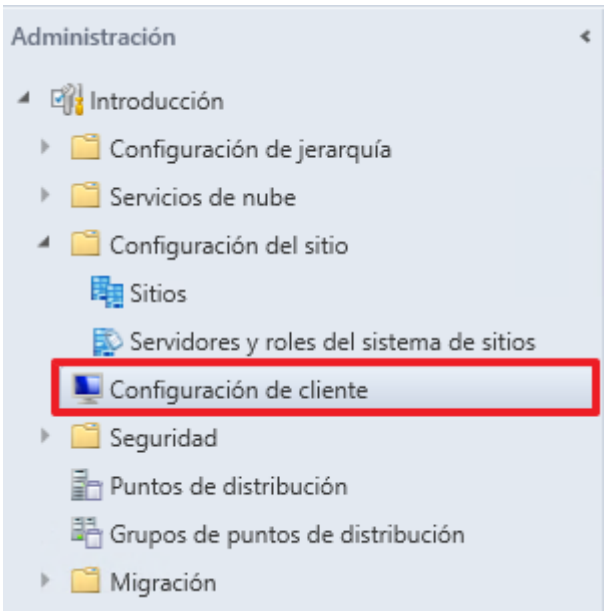
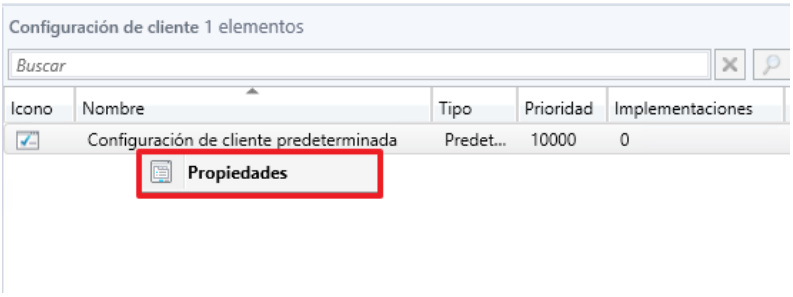
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="4">Como hacerlo</th></tr>
<tr><td rowspan="11"></td><td colspan="2">Archivo</td><td>Usuario</td><td>Permiso</td><td>OK/NOK</td></tr>
<tr><td colspan="2" rowspan="3">E:\SCCMContentLib</td><td>Administradores</td><td>Control total</td><td></td></tr>
<tr><td>SYSTEM</td><td>Control total</td><td></td></tr>
<tr><td>Usuarios</td><td>Leer</td><td></td></tr>
<tr><td colspan="2" rowspan="3">E:\SMS_DP$</td><td>SYSTEM</td><td>Control total</td><td></td></tr>
<tr><td>Administradores</td><td>Control total</td><td></td></tr>
<tr><td>Administrador</td><td>Control total</td><td></td></tr>
<tr><td colspan="2" rowspan="2">E:\SMSPKGE$</td><td>Administradores</td><td>Control total</td><td></td></tr>
<tr><td>Usuarios</td><td>Leer y ejecutar</td><td></td></tr>
<tr><td colspan="2" rowspan="4">E:\SMSSIG</td><td>IUSR</td><td>Escribir (Denegar)</td><td></td></tr>
<tr><td>SYSTEM</td><td>Control total</td><td></td></tr>
<tr><td>Administradores</td><td>Control total</td><td></td></tr>
<tr><td>Usuarios</td><td>Leer</td><td></td></tr>
<tr><td>30. Verifique los valores del registro.</td><td colspan="5">En los servidores miembro donde tenga implementado el rol de servidor de base de datos del sitio y se le esté aplicando la directiva de grupo “CCN-STIC-875 ENS Incremental SQL medio”.
Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como medio siguiendo los criterios del ENS, mediante el uso del “Editor del Registro”.
“Windows+R → Regedit”
El Control de cuentas de usuario solicitará elevación de privilegios. Pulse “Sí” en la ventana que se muestra a continuación.
 

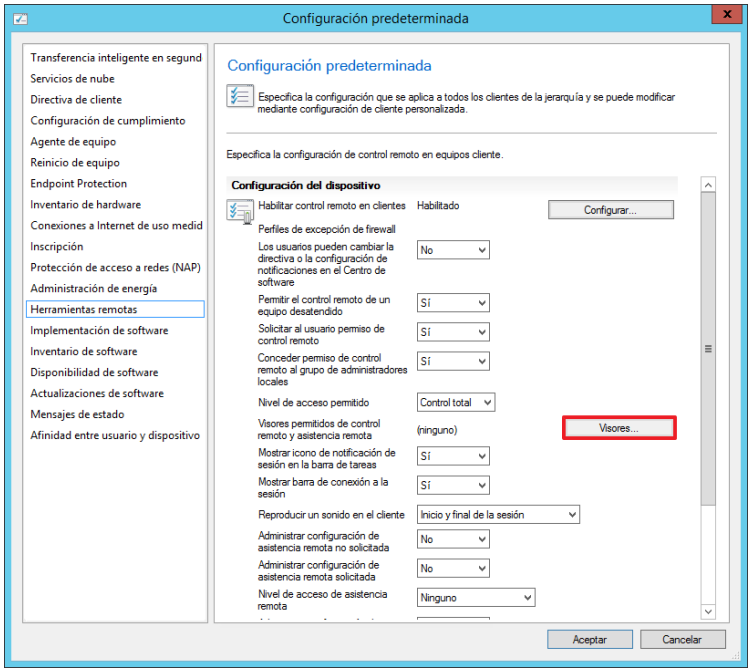
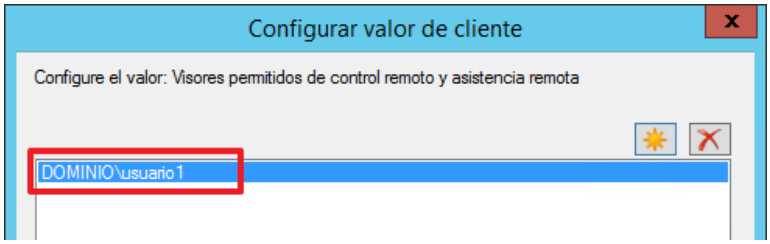
<table>
<tr><th>Valor del registro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Client \DisabledByDefault</td><td>00000000</td><td></td></tr>
<tr><td>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Server \Enabled</td><td>00000001</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo
31. Inicie sesión en el servidor miembro donde tiene instalada la consola de administración de MS SCCM 2012 R2, verifique que accede correctamente		Inicie sesión en la consola de administración de Configuration Manager desde el menú “Inicio > Todas las aplicaciones > Microsoft System Center 2012 R2 > Consola de Configuration Manager”. 
32. Verifique que tiene acceso a la Consola de Configuración		Compruebe que accede correctamente a la consola de configuración de MS SCCM 2012 R2. 

Comprobación	OK/NOK	Como hacerlo
33. Verifique que los roles de sistema de sitio están implementados en los servidores correspondientes		Despliegue "**Configuración del sitio > Servidores y roles del sistema de sitios**".  Verifique seleccionando cada servidor, que tiene implementados los roles de sistema de sitio correspondientes.  **Nota:** Tanto los nombres de los servidores como el del sitio han sido creados para elaborar la presente guía por lo que deberá adaptar estos pasos a su organización.

Comprobación	OK/NOK	Como hacerlo
34. Verifique los permisos asignados a los usuarios administrativos.		Despliegue "**Introducción > Seguridad > Usuarios administrativos**".  Compruebe que los usuarios tienen asignados los roles de seguridad correctamente.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización.

Comprobación	OK/NOK	Como hacerlo
35. Verifique los permisos asignados a los usuarios con permisos de control remoto.		Despliegue "**Introducción > Configuración del sitio > Configuración de cliente**".  Compruebe que los usuarios tienen asignados los permisos correctamente. Para ello pulse con el botón derecho sobre "Configuración de cliente predeterminada" y pulse botón derecho, y seleccione la opción "Propiedades" del menú contextual. 

Comprobación	OK/NOK	Como hacerlo
36. Verifique los usuarios que tienen permisos.		Pulse sobre el botón “Visores…”.  Compruebe en el listado los usuarios que tienen permisos de control remoto.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización.

ANEXO C. CONFIGURACION SEGURA DE MS SCCM 2012 R2 EN EL ENS PARA EL NIVEL ALTO

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de System Center Configuration Manager 2012 R2 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.

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para System Center Configuration Manager 2012 R2, 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.

ANEXO C.1. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL ALTO DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas, a realizar una implementación de seguridad en escenarios donde se tenga que reforzar la seguridad de Microsoft SCCM 2012 R2 sobre MS Windows Server 2012 R2, con una categorización de seguridad alto 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 al nivel alto, 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, se deberán realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

MS SCCM 2012 R2 requiere de otros servicios adicionales para su instalación y correcto funcionamiento, por lo que es necesario realizar una preparación previa del entorno antes de instalar MS SCCM 2012 R2, en caso de necesitar información sobre los requisitos previos de instalación de MS SCCM 2012 R2, visite el siguiente sitio web: https://docs.microsoft.com/es-es/sccm/core/plan-design/configs/site-and-site-system-prerequisites

En la presente guía se van a reforzar la seguridad de los principales roles de sitio de MS SCCM 2012 R2.

a) Sistema de sitio
b) Servidor del sitio
c) Punto de distribución
d) Punto de administración

e) Punto de actualización de software

f) Punto de servicios de informes

g) Servidor base de datos del sitio

Nota: Si instala MS SCCM 2012 R2 por primera vez con la guía 870A aplicada previamente debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell, la cual se encuentra deshabilitada por GPO.

Para la implementación de la presente guía se han generado unas plantillas de seguridad que deberán ser aplicada en las unidades organizativas correspondientes donde se encuentren alojados los servidores que vayan a formar parte de MS System Center Configuration Manager 2012 R2.

Hay que tener en consideración que el objetivo de implementación de estos tipos de servidores puede ser para un uso de múltiples roles, por ejemplo, como punto de distribución, punto de actualización de software o punto de servicios de informes., por lo que no existirá una ubicación específica dentro del directorio activo, aunque en la presente guía se intentan agrupar en las unidades organizativas “Servidores SCCM” y “Servidores SQL” para una mejor gestión.

Los detalles de las siguientes plantillas se encuentran exportados en sus ficheros correspondientes con formato HTML en la carpeta “Scripts\Nivel Alto” que se acompaña junto a este documento.

a) CCN-STIC-875 ENS Incremental Servidor Punto de actualización de software alto

b) CCN-STIC-875 ENS Incremental Servidor Punto de administración alto

c) CCN-STIC-875 ENS Incremental Servidor Punto de distribución alto

d) CCN-STIC-875 ENS Incremental Servidor Punto de servicios de informes alto

e) CCN-STIC-875 ENS Incremental Servidor del sitio alto

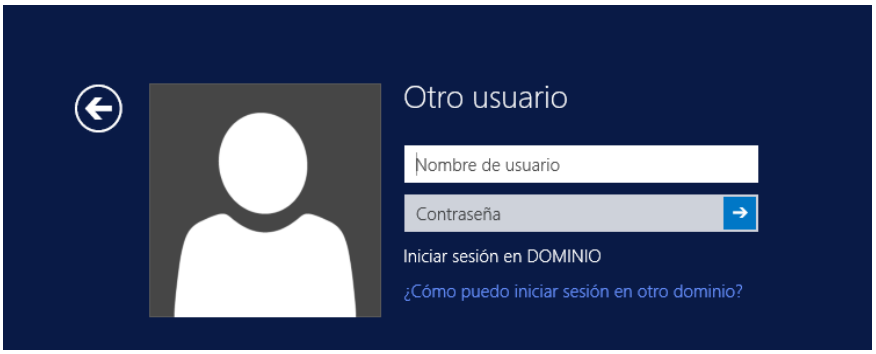
f) CCN-STIC-875 ENS Incremental SQL alto

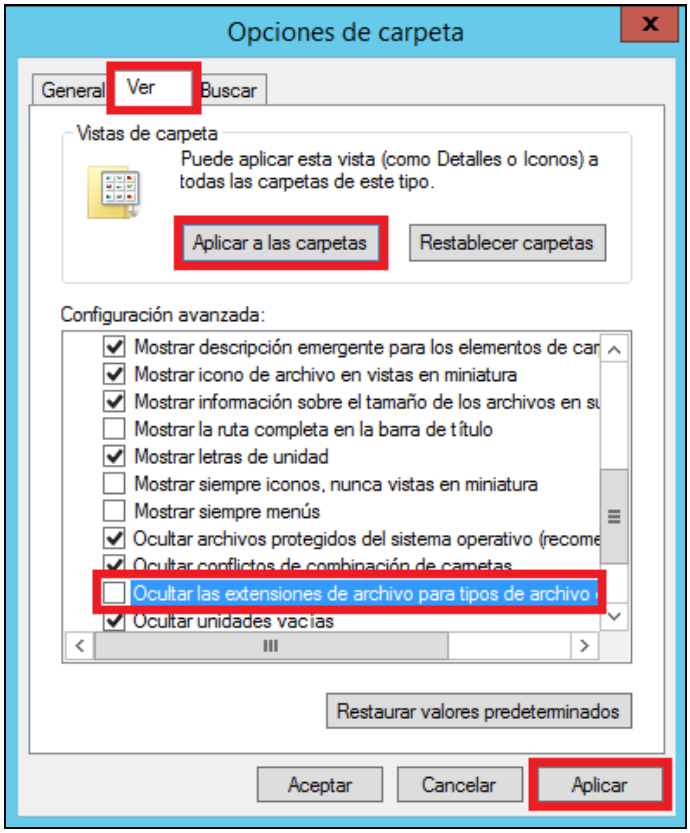
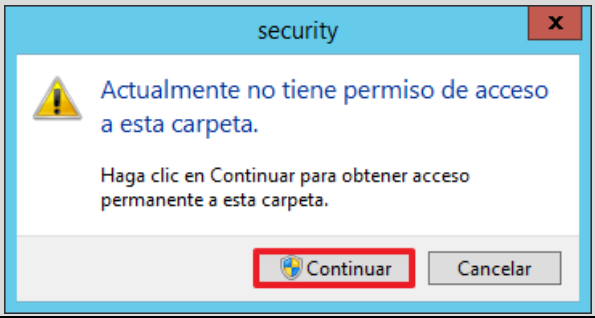
1. REFUERZO DE SEGURIDAD DEL SERVIDOR SQL Y ROL DE SERVIDOR BASE DE DATOS DEL SITIO

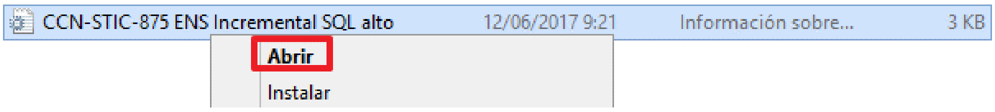
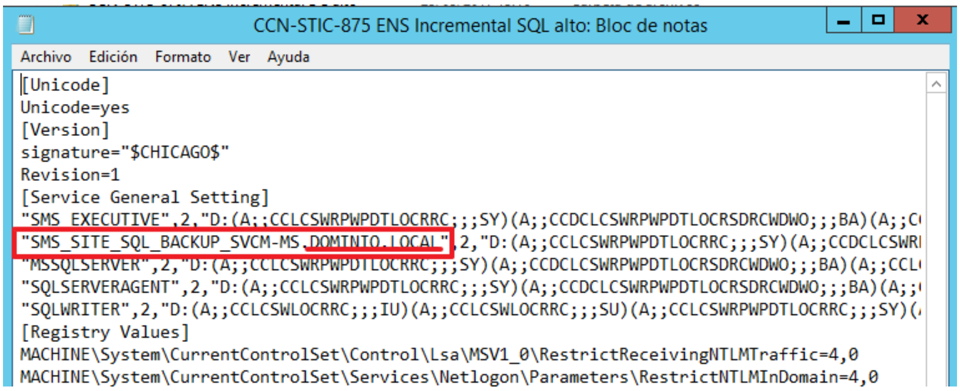
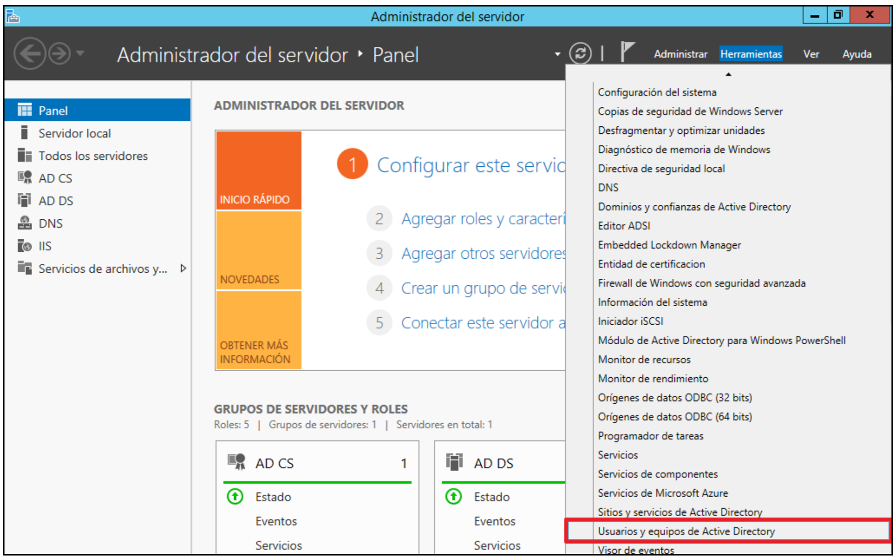
Es necesario dar permisos de inicio de sesión como servicio a los usuarios necesarios para iniciar los servicios de SQL requeridos para el correcto funcionamiento del producto MS SQL server y MS SCCM 2012 R2.

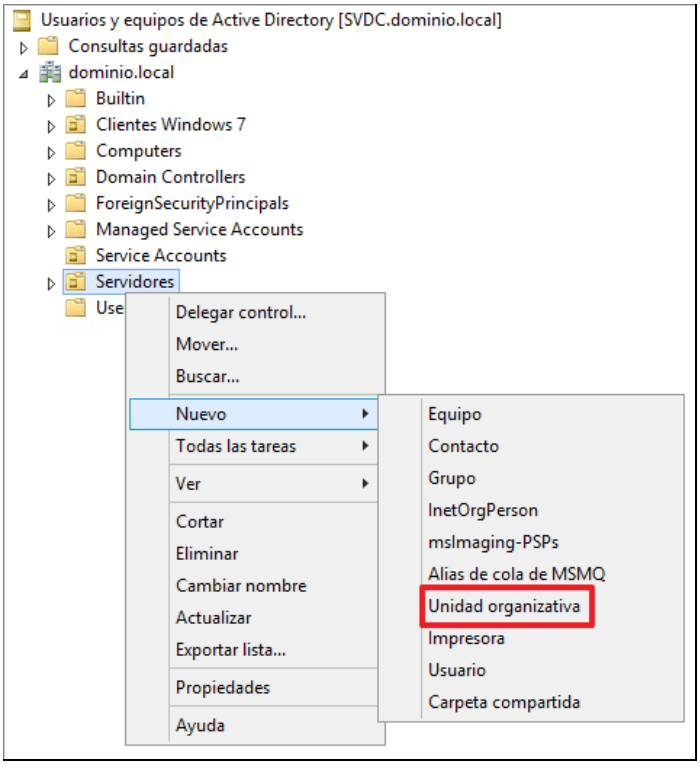
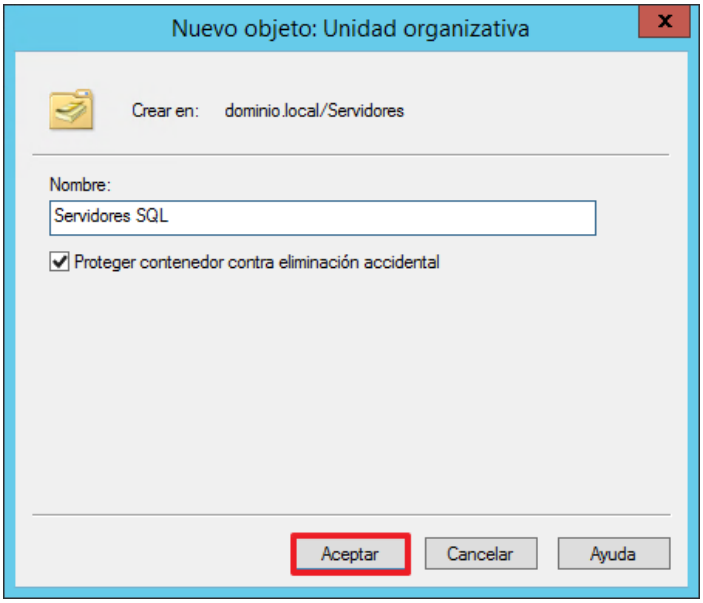
Se ha de tener en consideración que el servidor que aloja el producto de MS SQL Server también contiene Internet Information Services 8.5 para el rol de servicios de informes de SCCM por lo que será necesario aplicar previamente la guía de seguridad “CCN-STIC-873 ENS Incremental IIS 8.5”.

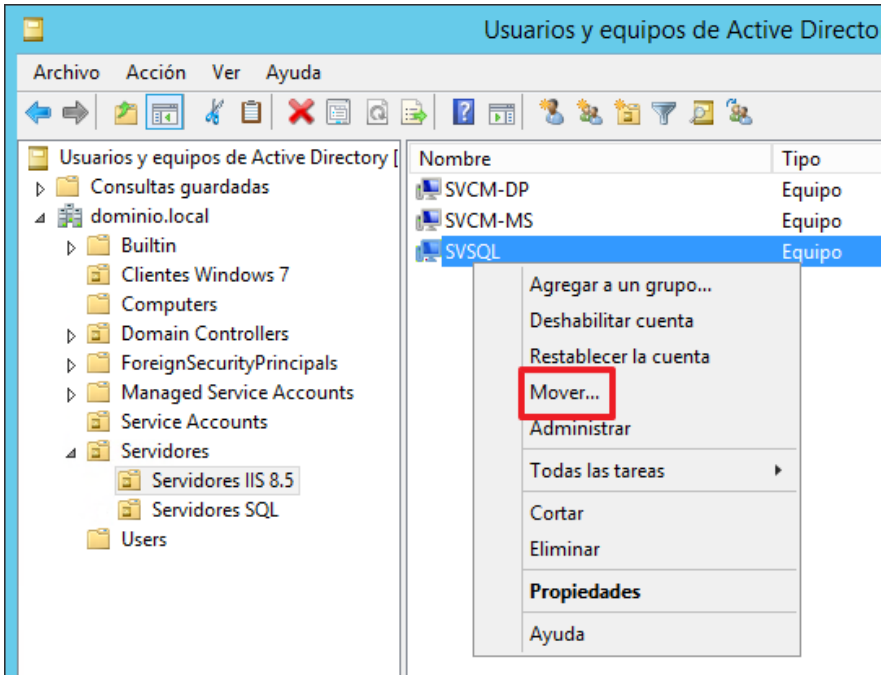
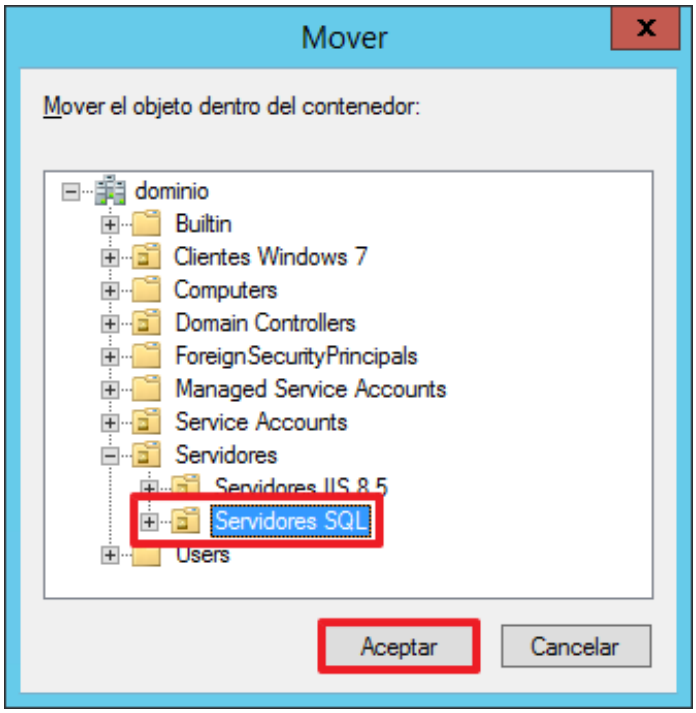
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

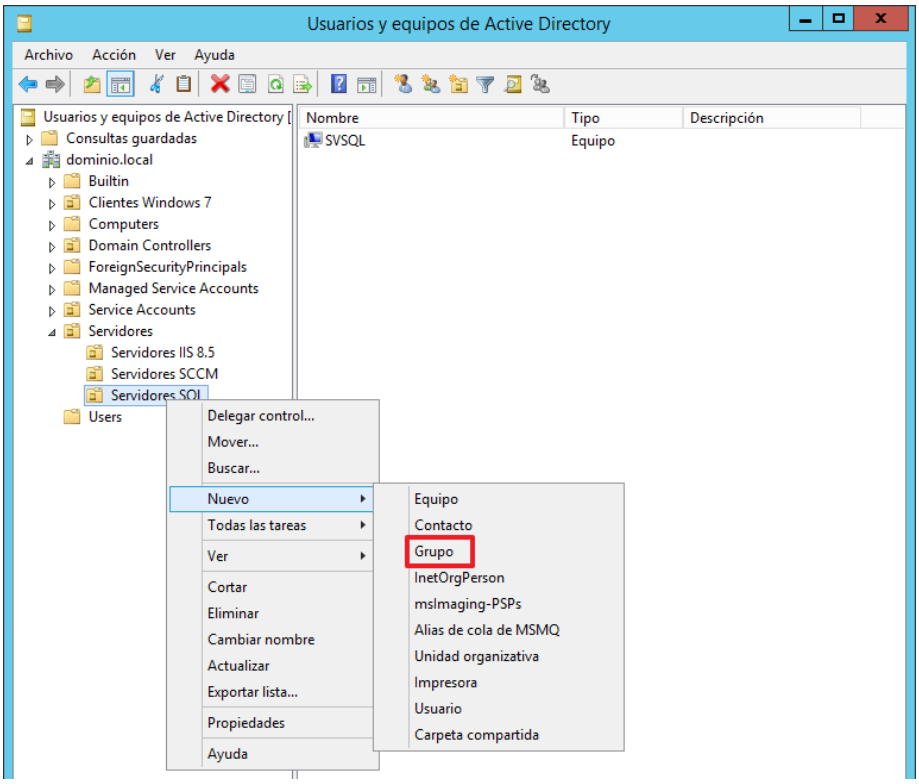
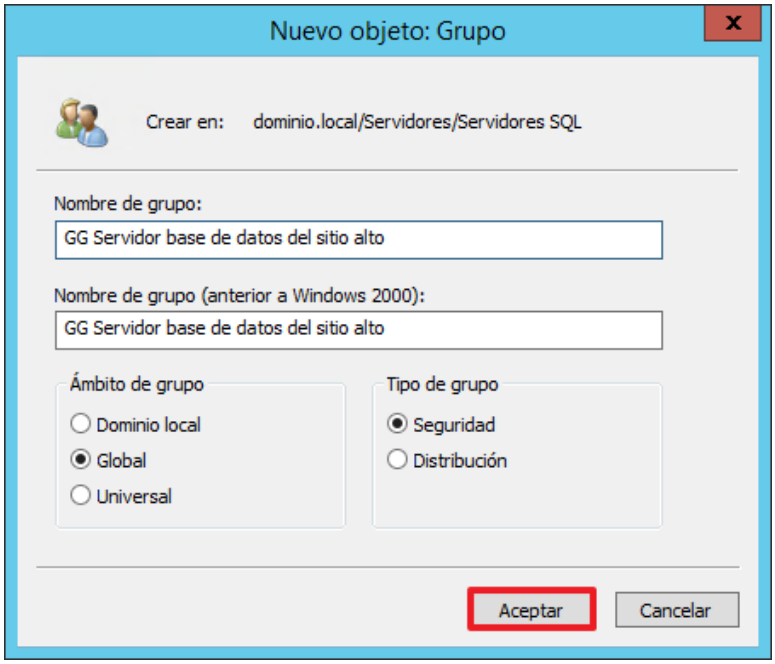
Paso	Descripción
1.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
3.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
4.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.

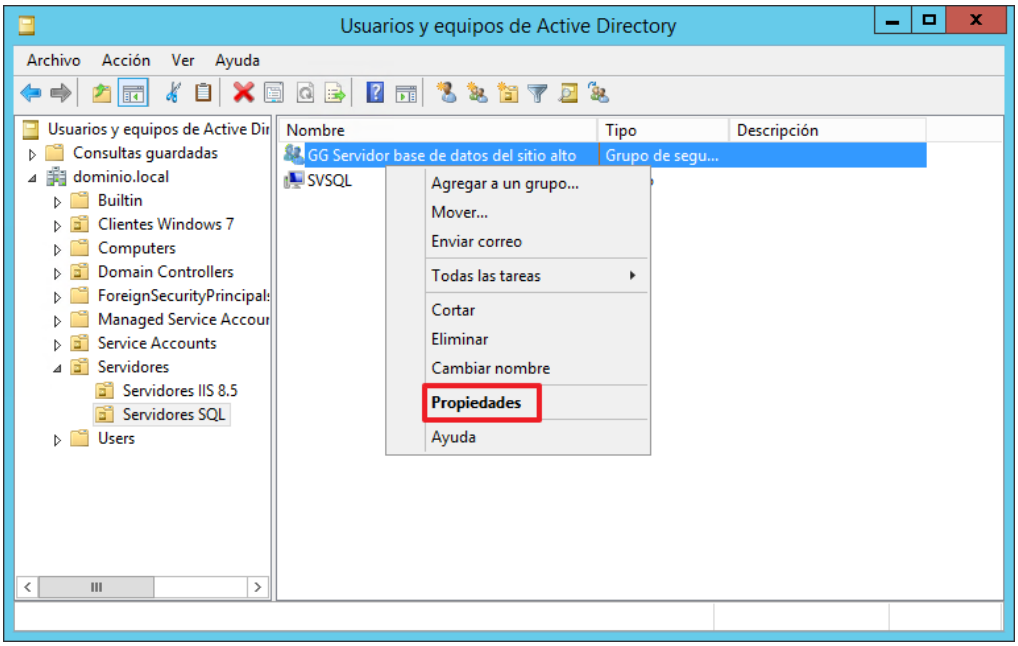
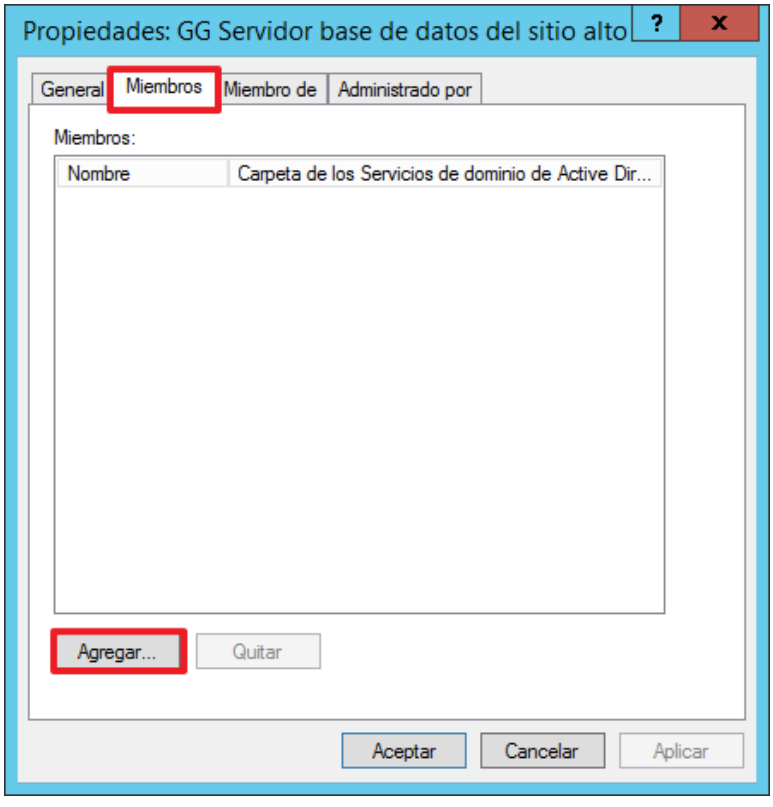
Paso	Descripción
5.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".
6.	Copie el fichero “CCN-STIC-875 ENS Incremental SQL alto.inf” que se encuentra en la ruta “C:\Scripts\Nivel alto” al directorio “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 

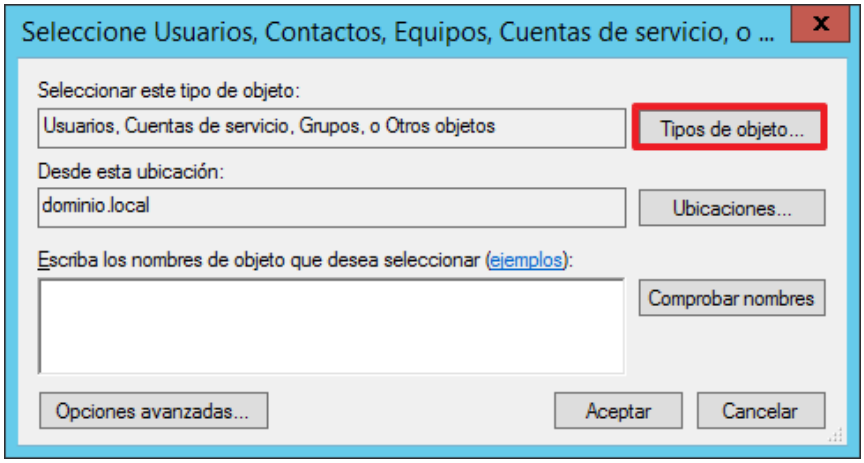
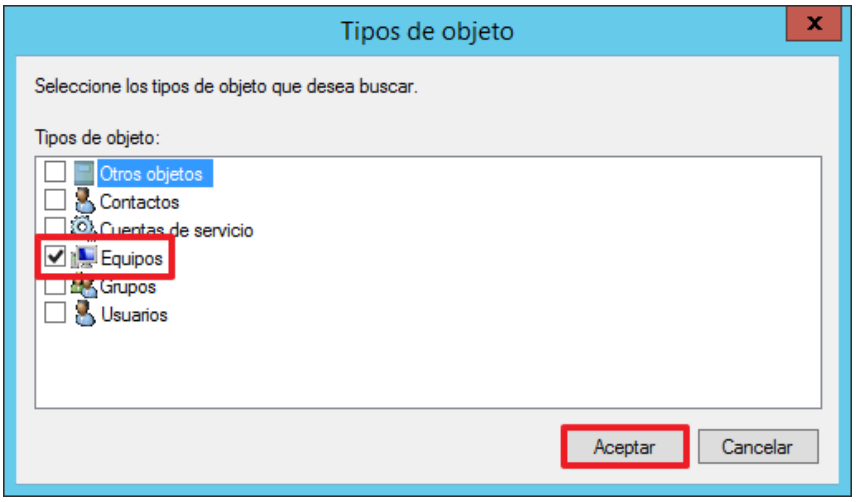
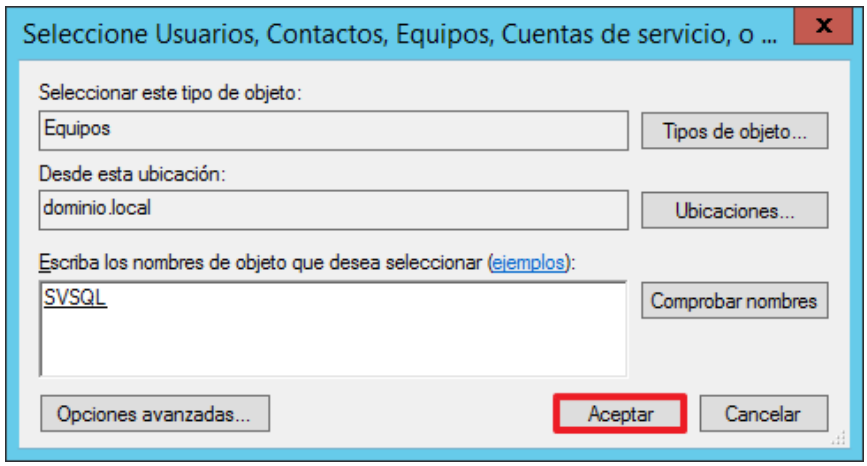
Paso	Descripción
7.	Pulse con el botón derecho sobre el fichero y seleccione la opción “Abrir” del menú contextual. 
8.	Deberá modificar el fichero para adaptarlo a su organización, para ello, localice el servicio “SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL” y modifique el nombre del servicio cambiando el texto “DOMINIO.LOCAL” por el nombre de dominio de su organización.  **Nota:** Si no modifica este fichero el servicio “SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL”, no se reforzará la seguridad según los parámetros establecidos en el documento.
9.	Guarde los cambios realizados y cierre el documento.
10.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

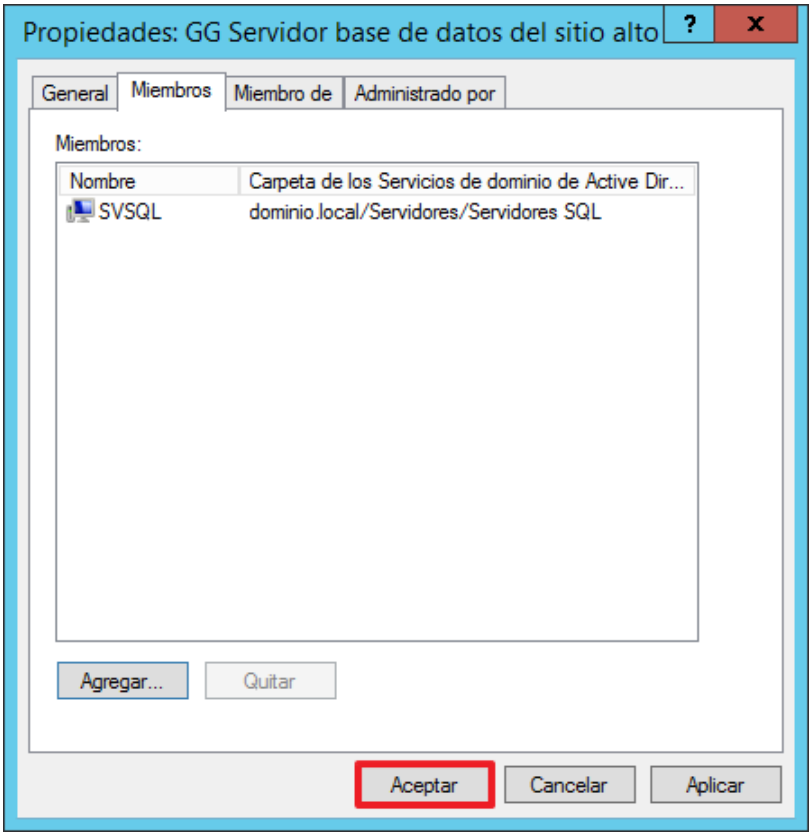
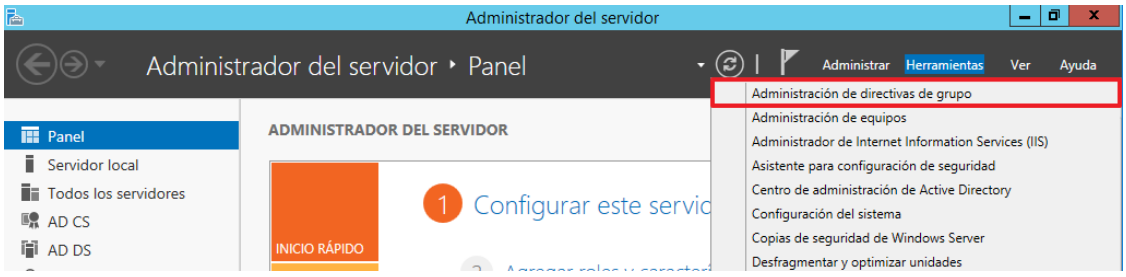
Paso	Descripción
11.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
12.	En la consola, cree una unidad organizativa denominada “Servidores SQL” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar”. 

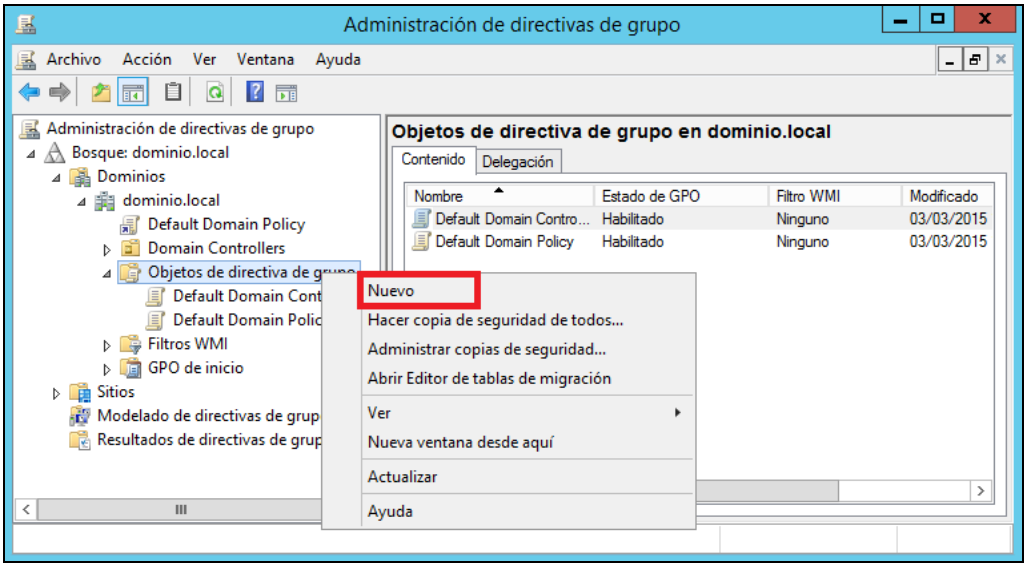
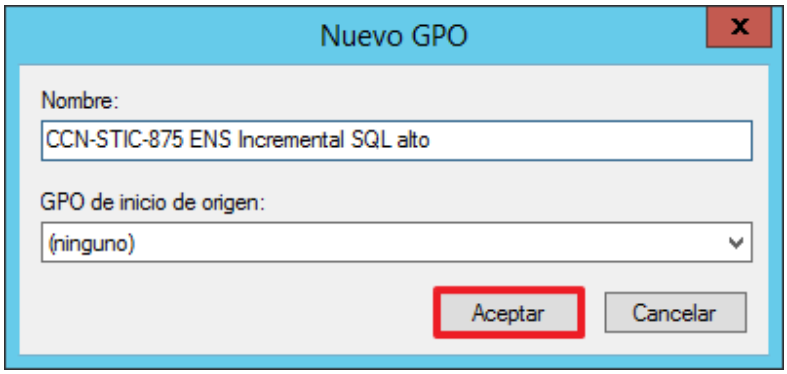
Paso	Descripción
13.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores SQL a la unidad organizativa “Servidores SQL”. Para ello, localice los servidores y haga clic con el botón derecho sobre “mover” en el servidor que desee ubicar en la nueva unidad organizativa. 
14.	En el árbol de contenedores, seleccione la unidad organizativa “Servidores SQL” y “Aceptar”. 

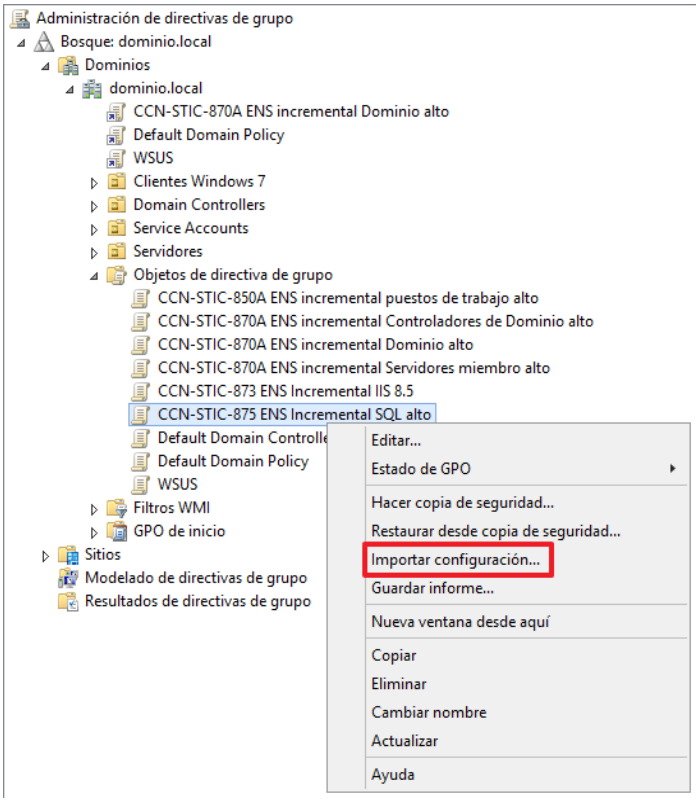
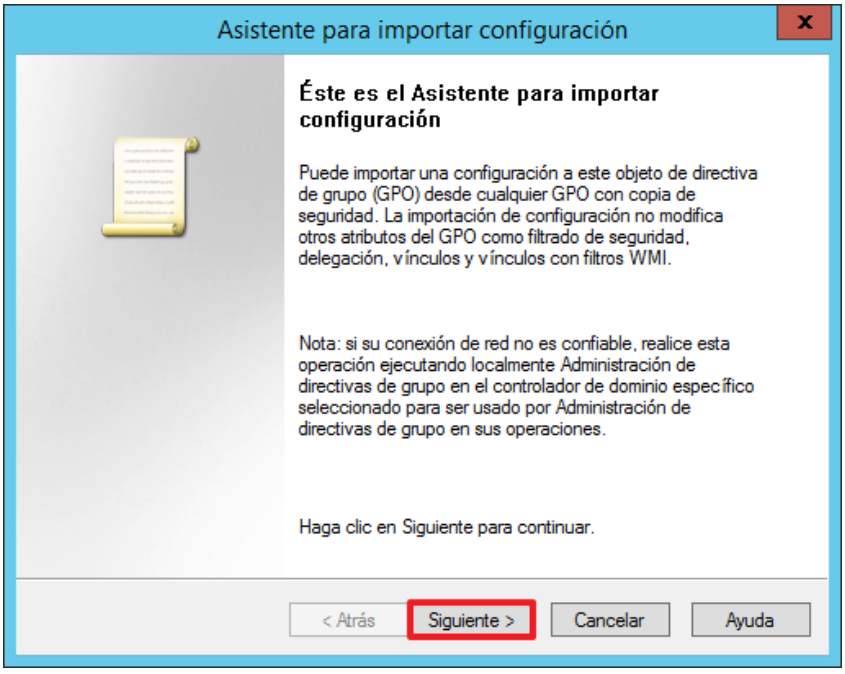
Paso	Descripción
15.	Para el siguiente paso, seleccione la unidad organizativa “Servidores SQL”, pulse con el botón derecho y marque la opción “Nuevo > Grupo” del menú contextual. 
16.	Escriba el nombre “GG Servidor base de datos del sitio alto” y pulse “Aceptar”. 

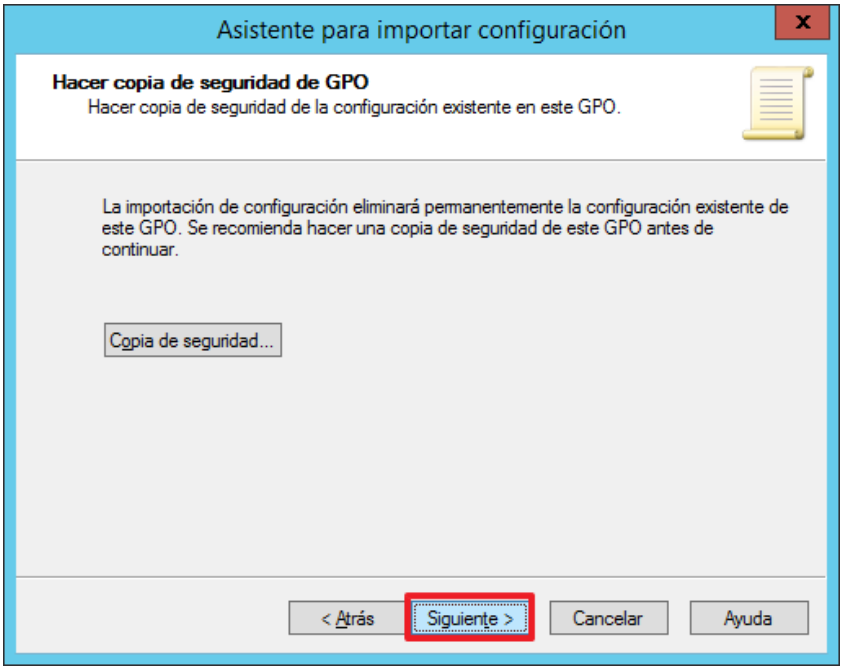
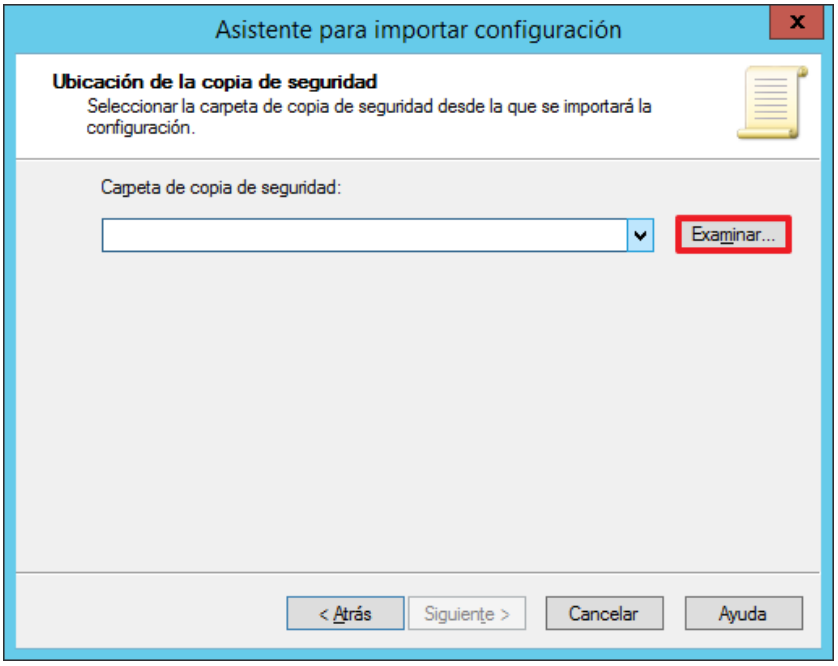
Paso	Descripción
17.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
18.	Seleccione la pestaña “Miembros” y pulse “Agregar…” para añadir los equipos que contengan MS SQL Server al grupo. 

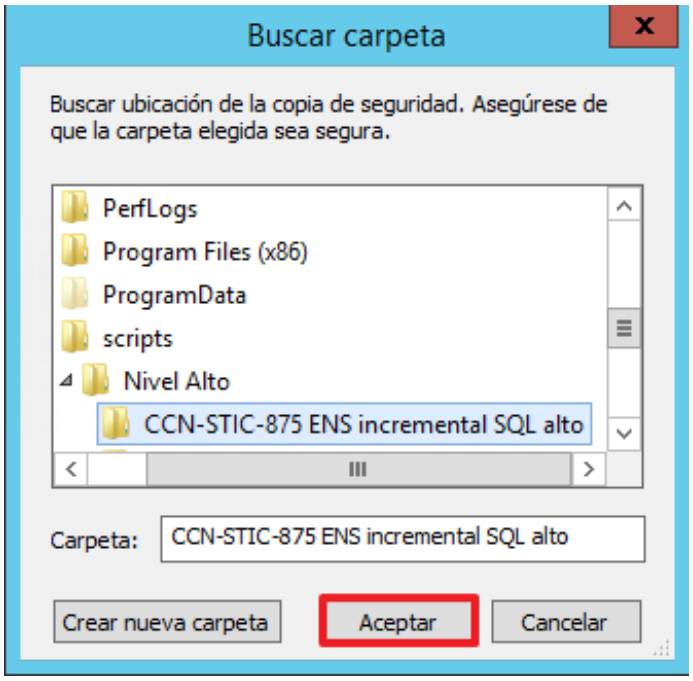
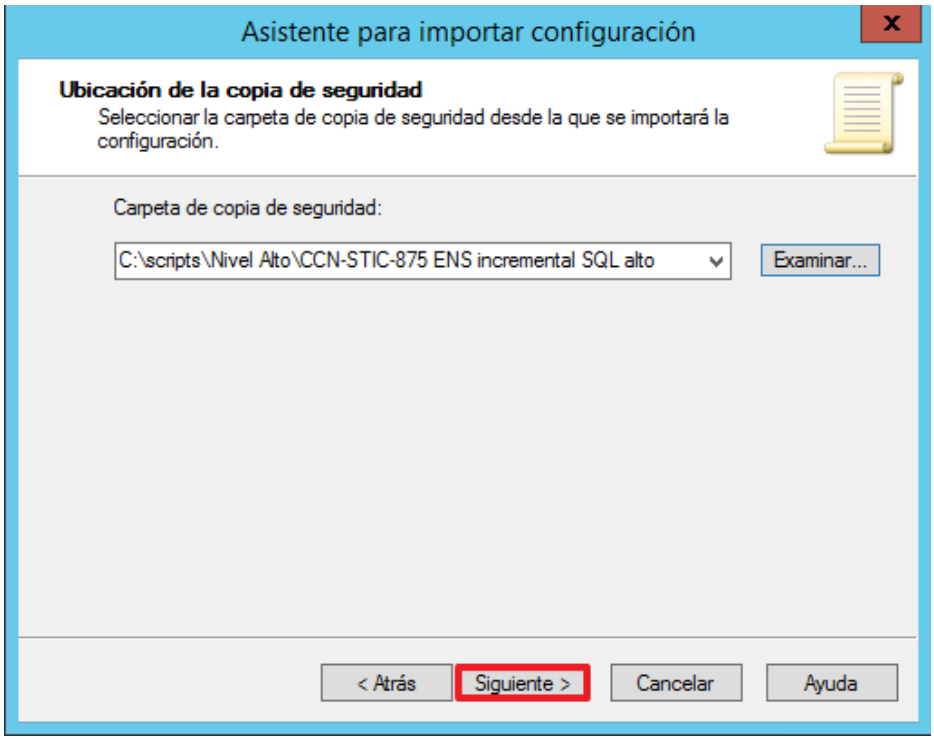
Paso	Descripción
19.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
20.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
21.	Agregue los equipos y pulse sobre “Aceptar”. 

Paso	Descripción
22.	Marque de nuevo en “Aceptar” para cerrar las propiedades del grupo. 
23.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
24.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
25.	Despliegue los contenedores y sitúese sobre la carpeta “Objetos de directiva de grupo”.

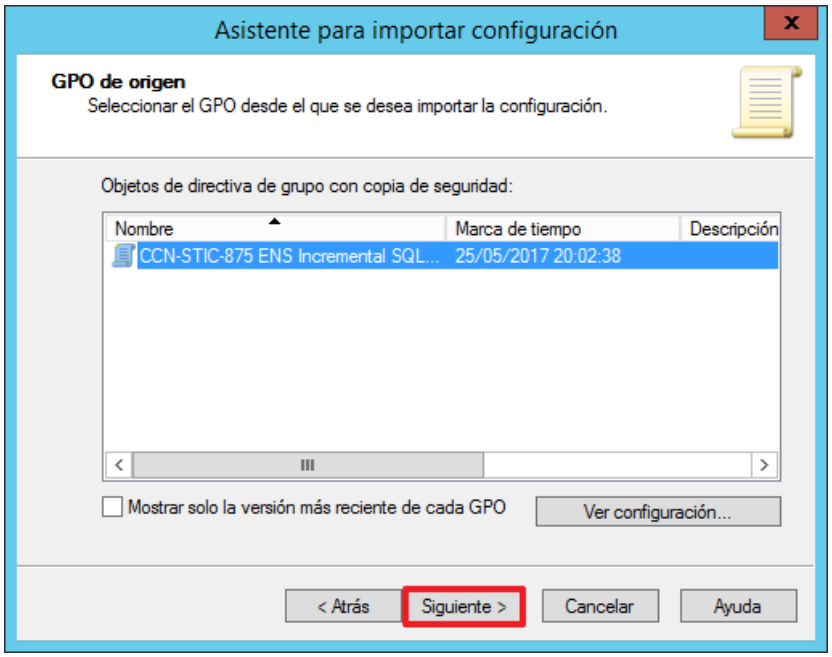
Paso	Descripción
26.	Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”. 
27.	Introduzca como nombre “CCN-STIC-875 ENS Incremental SQL alto” y pulse el botón “Aceptar”.  **Nota:** Se debe tener en consideración que en esta directiva de seguridad se va a habilitar el protocolo SSL 3.0 para el correcto funcionamiento del servicio de SQL, en caso de que exista algún inconveniente deberá adaptar estos pasos a su organización.

Paso	Descripción
28.	La nueva política requiere una configuración de plantillas administrativas. Para ello y seleccionando la política, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración…”. 
29.	En el asistente de importación de configuración, pulse el botón “Siguiente >”. 

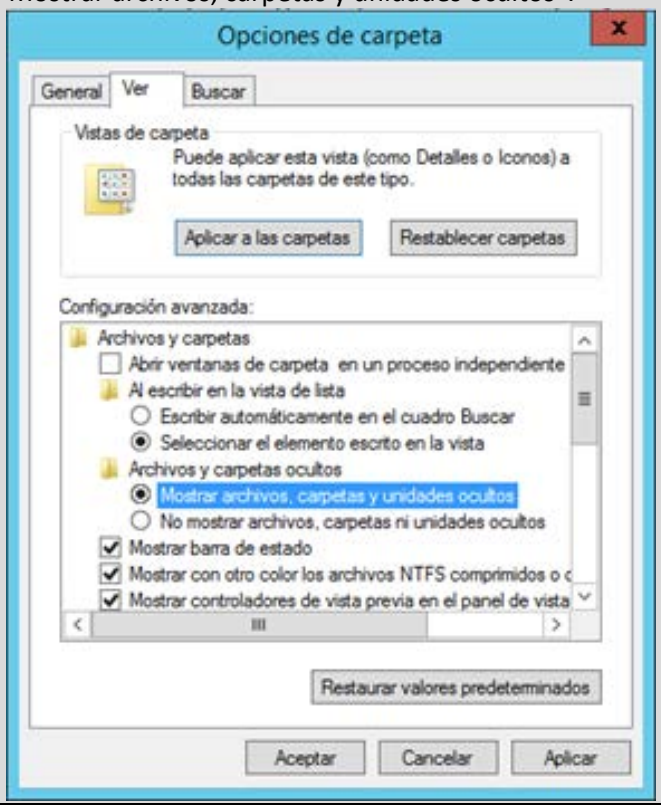
Paso	Descripción
30.	En la selección de copia de seguridad pulse el botón “Siguiente >”.  **Nota:** No es necesaria la realización de ninguna copia de seguridad, puesto que la política se encuentra vacía.
31.	En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”. 

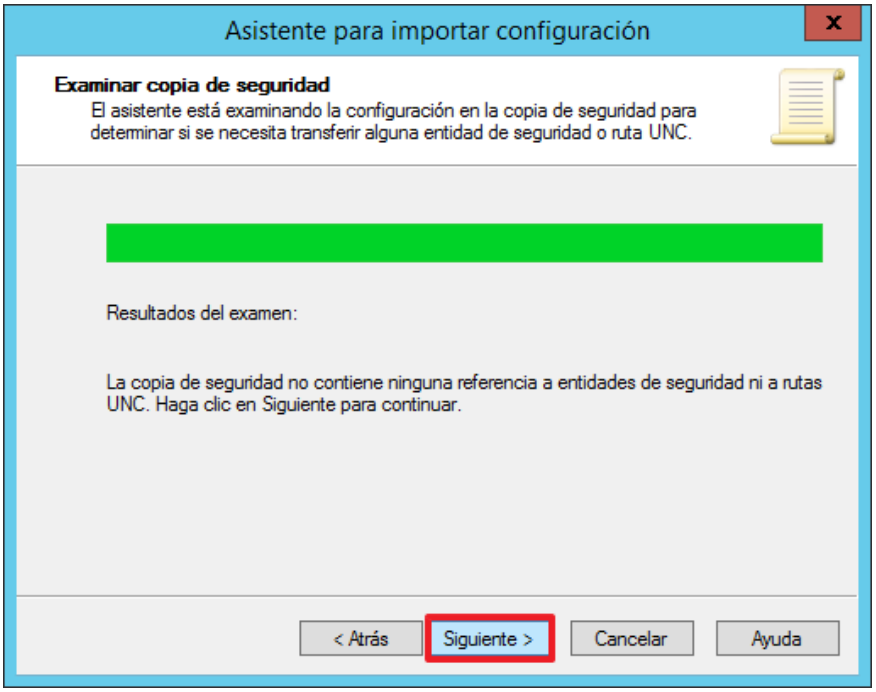
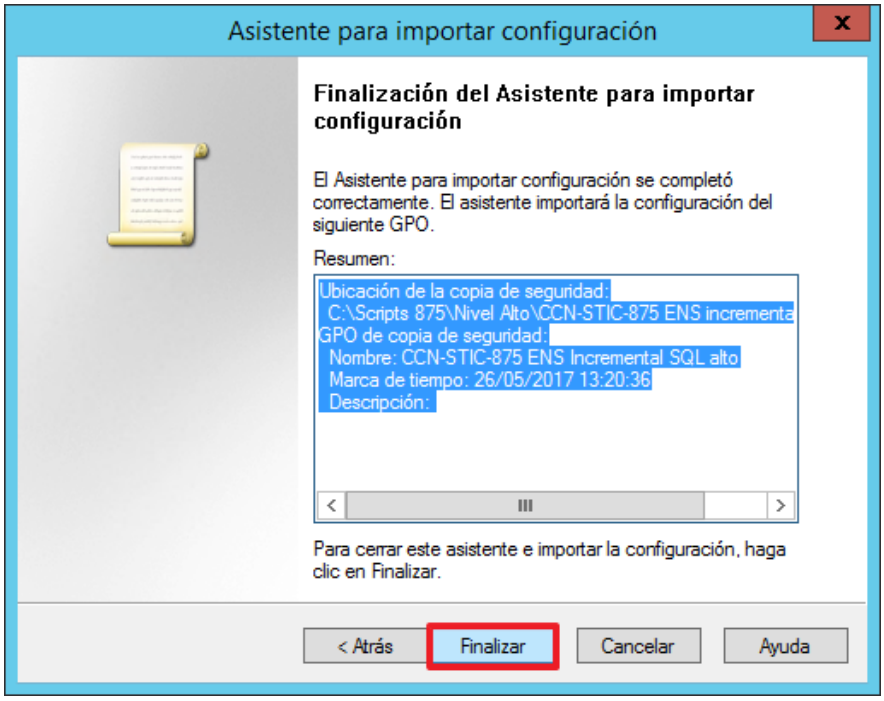
Paso	Descripción
32.	Seleccione la carpeta “CCN-STIC-875 ENS Incremental SQL alto” que encontrará en la carpeta “C:\Scripts\Nivel alto” y pulse el botón “Aceptar”. 
33.	Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada. 

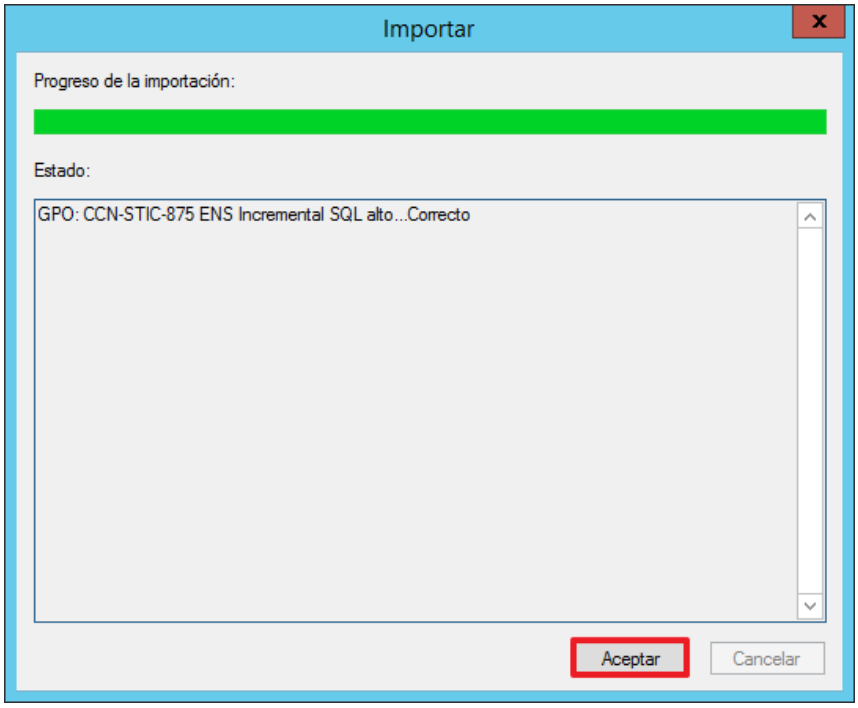
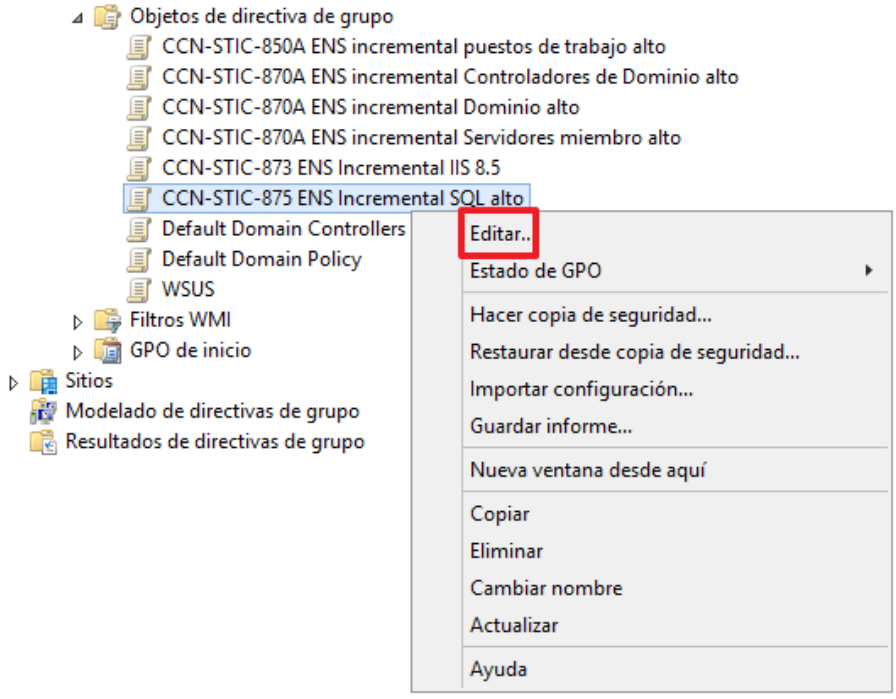
Paso	Descripción
34.	En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-875 Incremental SQL alto” y pulse el botón “Siguiente >”.

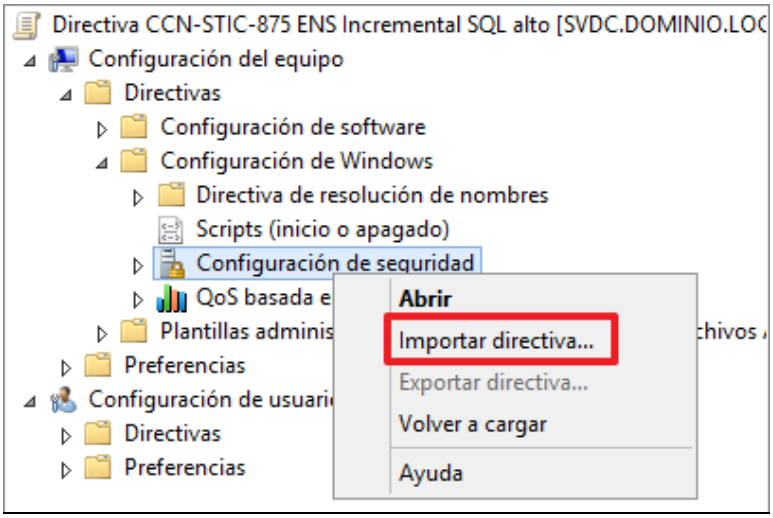
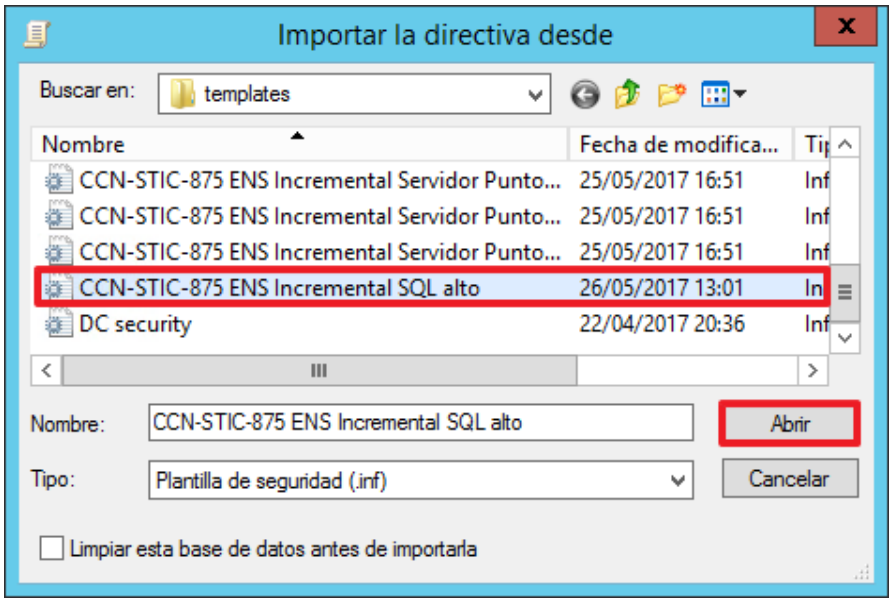


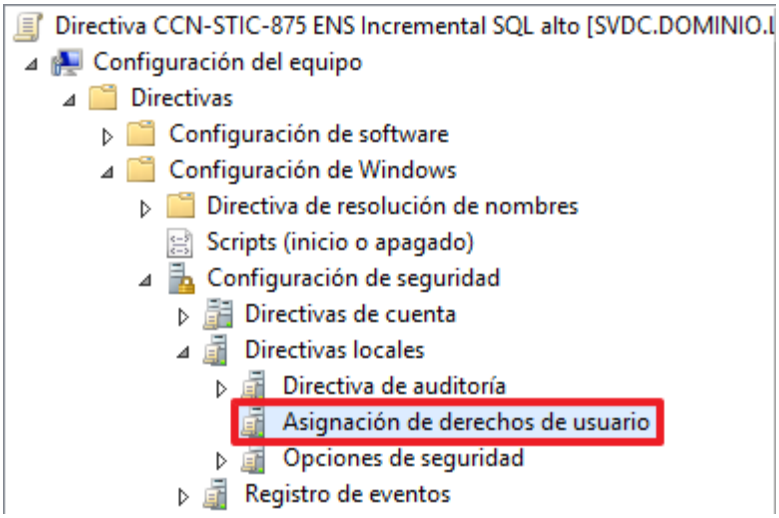
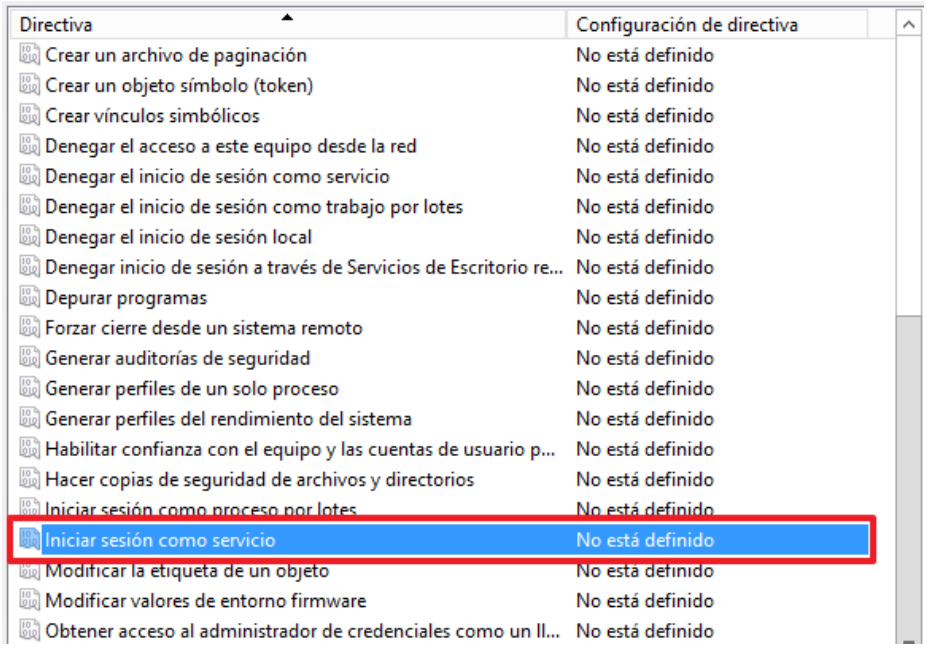
Nota: Si no apareciera una política es debido a que no se han copiado los ficheros correspondientes. Compruebe que en la carpeta seleccionada se encuentra el fichero “manifest.xml”. Este es un fichero oculto y, por lo tanto, debe activar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”.

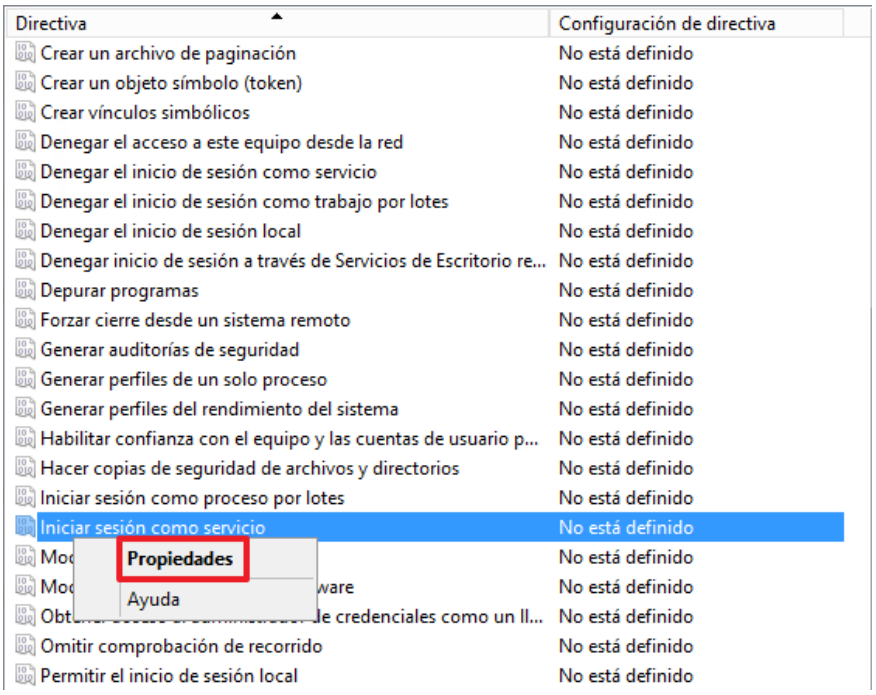
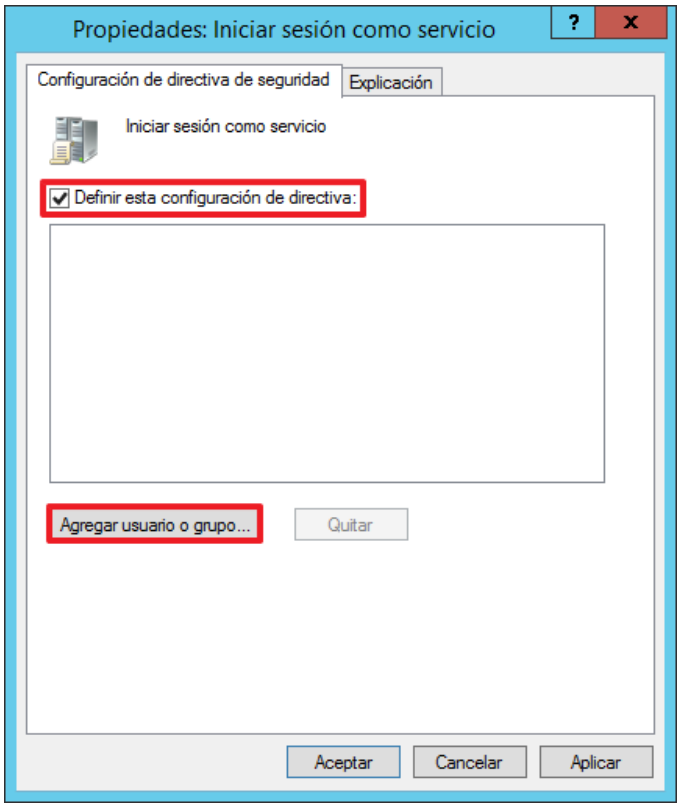


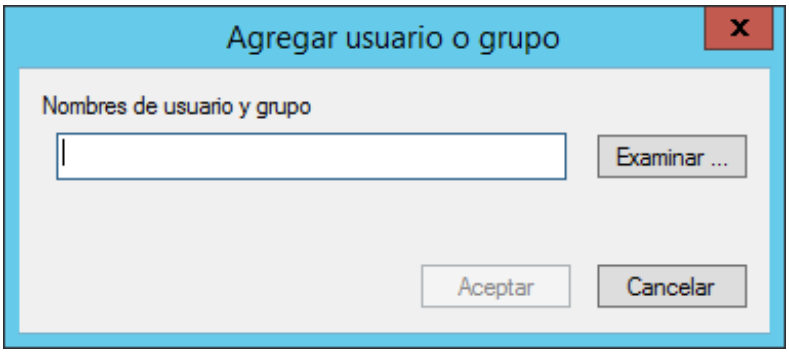
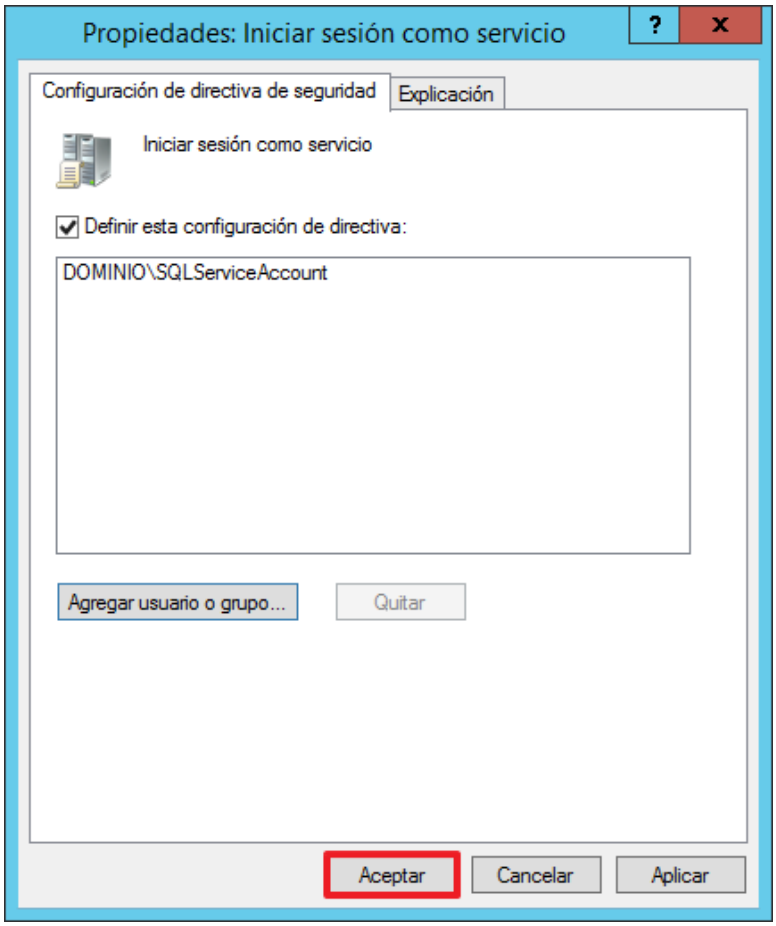
Paso	Descripción
35.	En la pantalla de examen, pulse el botón “Siguiente >”. 
36.	Si apareciera la ventana “Migrar referencias”, mantenga las opciones y pulse el botón “Siguiente >”.
37.	Para terminar de importar la configuración pulse el botón “Finalizar”. 

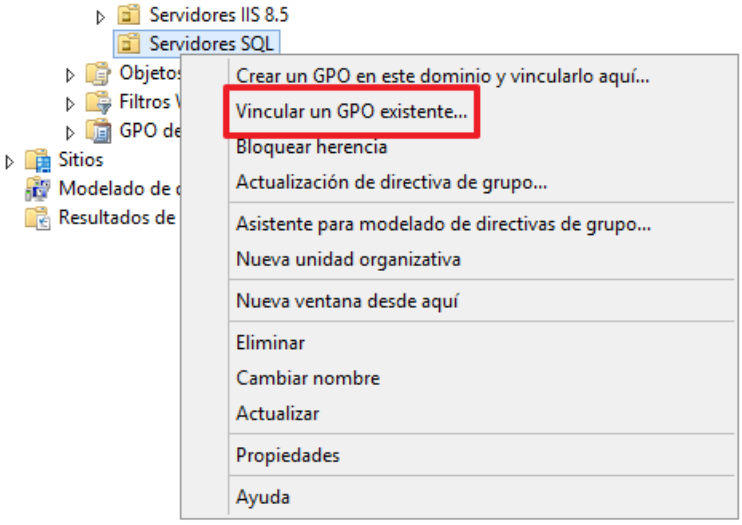
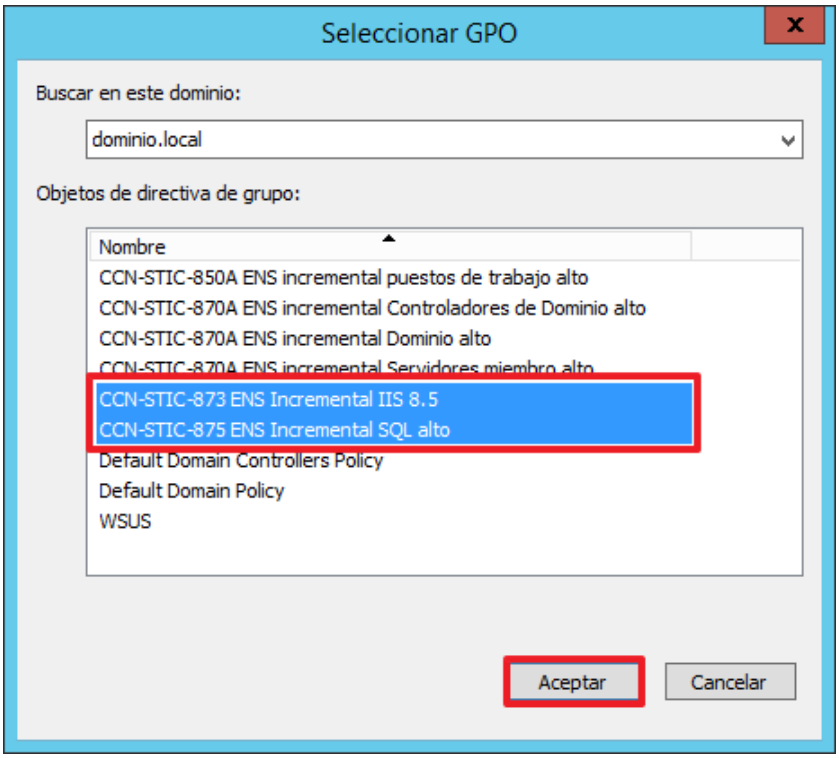
Paso	Descripción
38.	En la siguiente ventana, para cerrar el asistente pulse el botón “Aceptar”. 
39.	Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Editar”. 

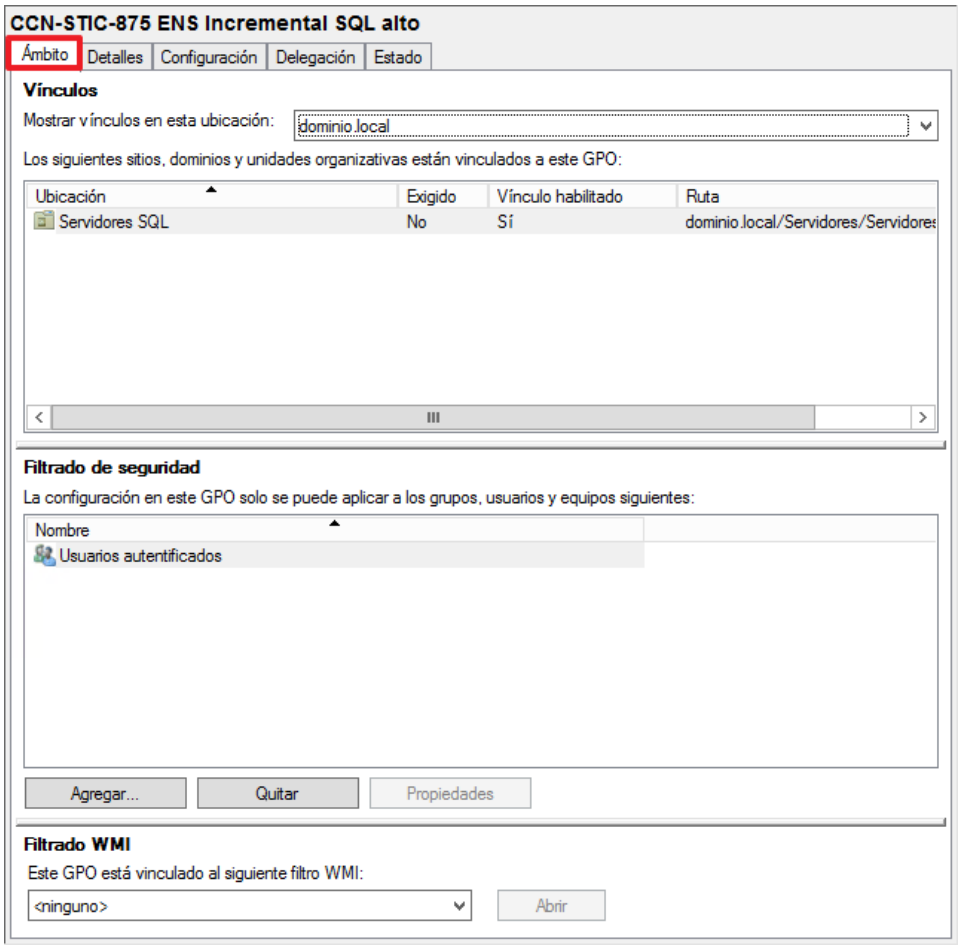
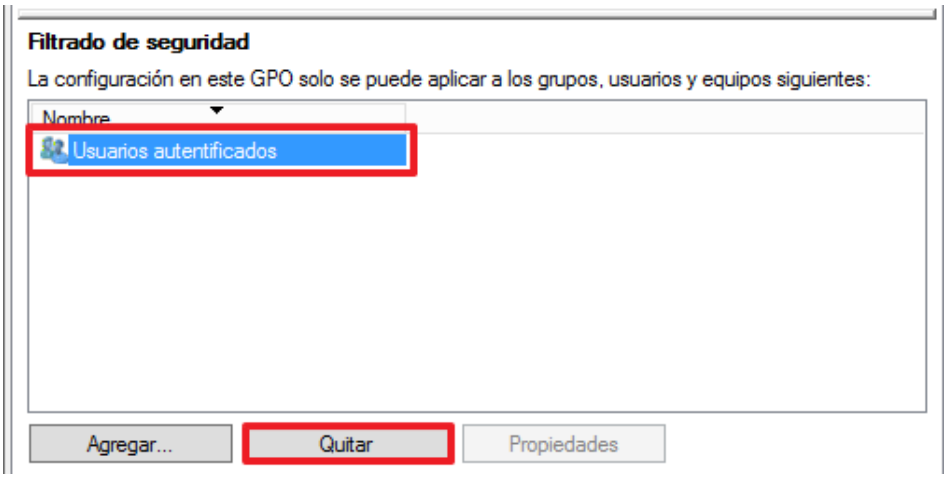
Paso	Descripción
40.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". Y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 
41.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental SQL alto.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en el botón "Abrir". 

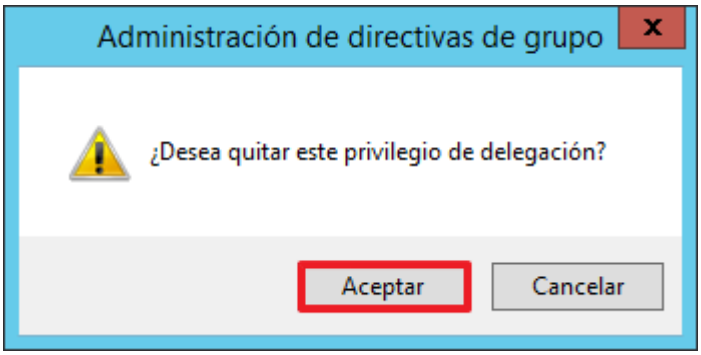
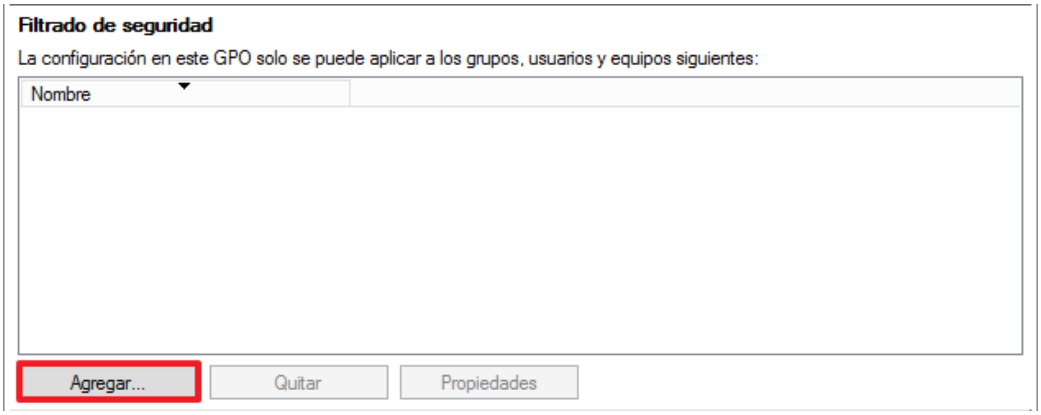
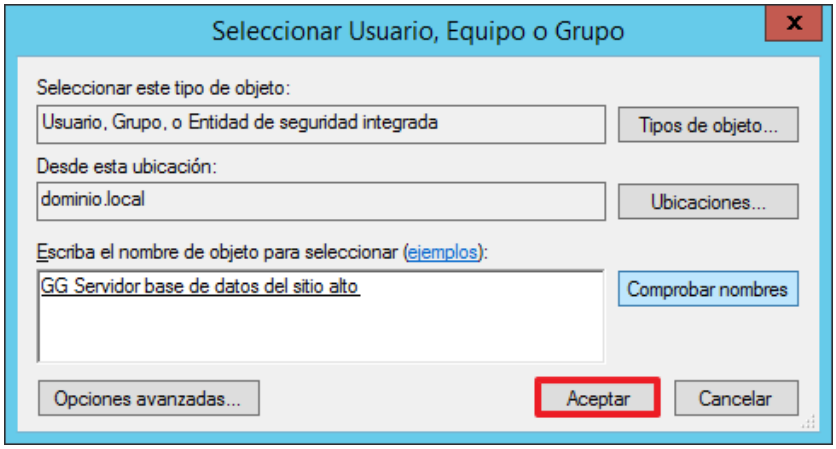
Paso	Descripción
42.	A continuación, despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta: **"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos de usuario".** 
43.	A continuación, seleccione la directiva "Iniciar sesión como servicio". 

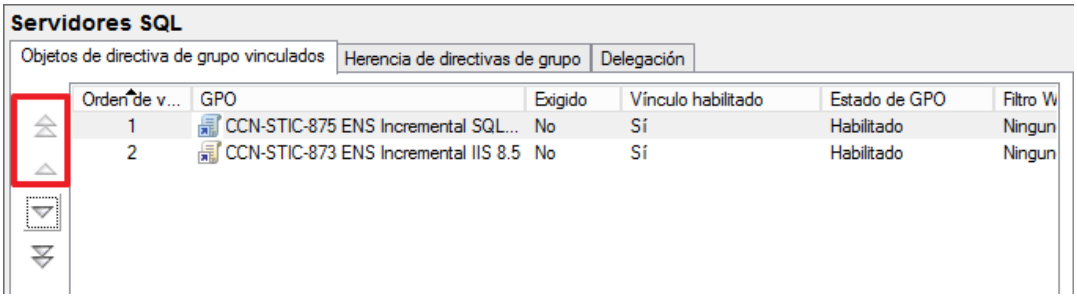
Paso	Descripción
44.	Pulse con el botón derecho sobre la directiva y seleccione la opción “Propiedades” del menú contextual. 
45.	A continuación, active la casilla “Definir esta configuración de directiva” y pulse sobre “Agregar usuario o grupo...”. 

Paso	Descripción
46.	Agregue los usuarios necesarios para iniciar los servicios de SQL requeridos para un correcto funcionamiento del servicio. 
47.	Una vez añadidos los usuarios necesarios pulse “Aceptar”.  **Nota:** Deberá adaptar estos pasos a su organización y añadir únicamente los usuarios necesarios para un correcto funcionamiento de los servicios utilizados para el correcto funcionamiento de la base de datos.
48.	Cierre el editor de administración de directivas de grupo para finalizar la configuración.

Paso	Descripción
49.	A continuación, seleccione la unidad organizativa “Servidores SQL” y pulse botón derecho, “Vincular un GPO existente…”. 
50.	Seleccione los objetos de directiva de grupo con nombre, “CCN-STIC-875 ENS Incremental SQL alto” y “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse “Aceptar”. 

Paso	Descripción
51.	Seleccione la directiva de grupo “CCN-STIC-875 ENS Incremental SQL alto” y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 
52.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 

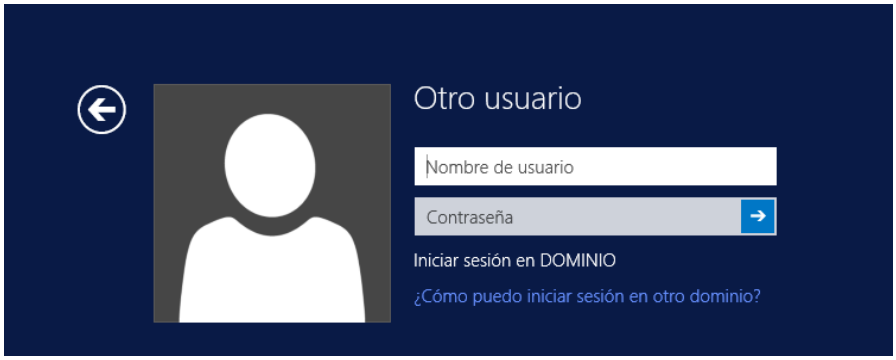
Paso	Descripción
53.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
54.	Una vez quitado, pulse el botón “Agregar…”. 
55.	Introduzca como nombre “GG Servidor base de datos del sitio alto” y pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.

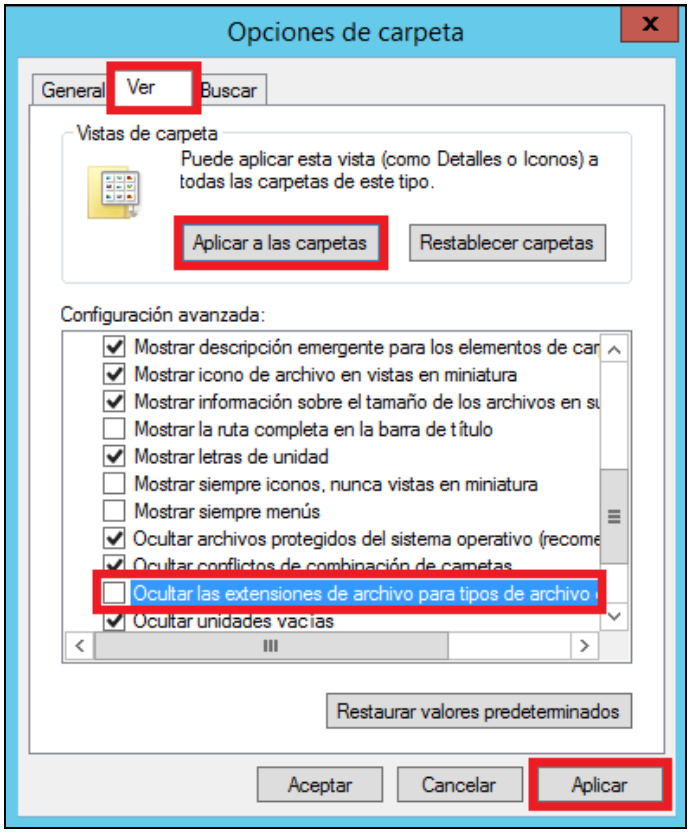
Paso	Descripción
56.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva “CCN-STIC-875 ENS Incremental SQL alto” aparezca en primer lugar. Para ello seleccione, la unidad organizativa “Servidores SQL” y a continuación, haga clic sobre la fecha doble hacia arriba para que se sitúe con el número 1 de orden vínculos, tal y como se muestra en la imagen. 
57.	Cierre el administrador de directivas de grupo para finalizar con la configuración.

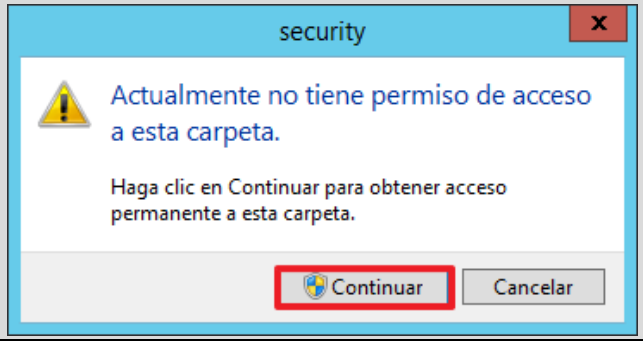
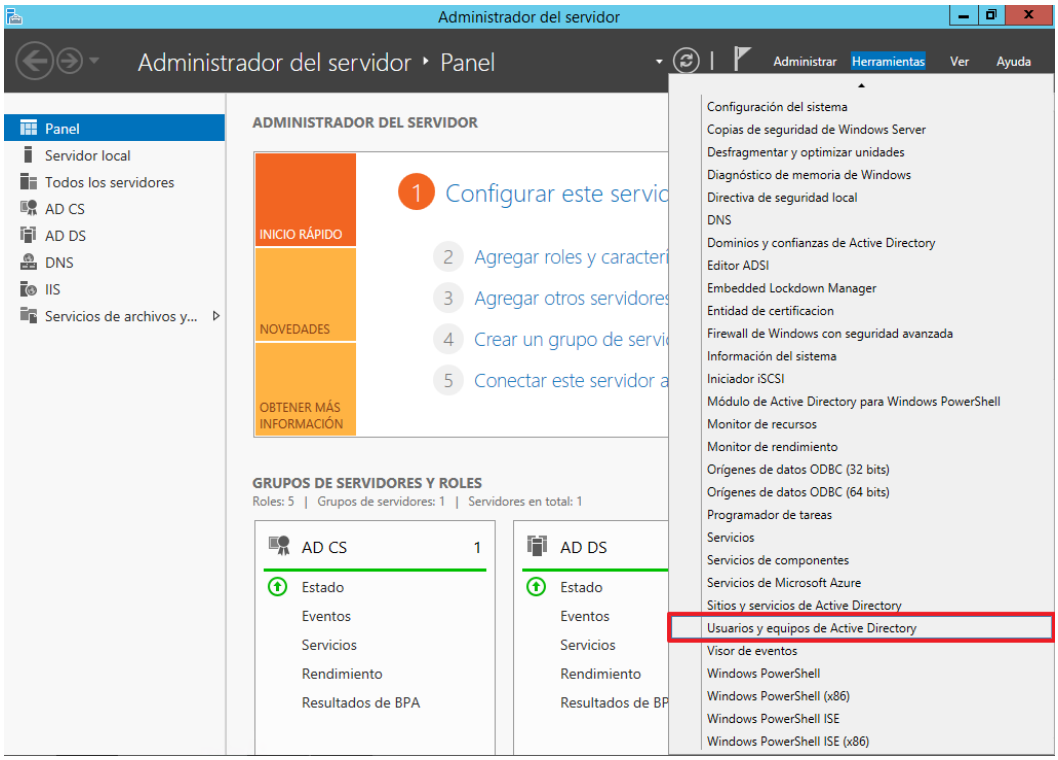
2. REFUERZO DE SEGURIDAD DEL SERVIDOR DEL SITIO

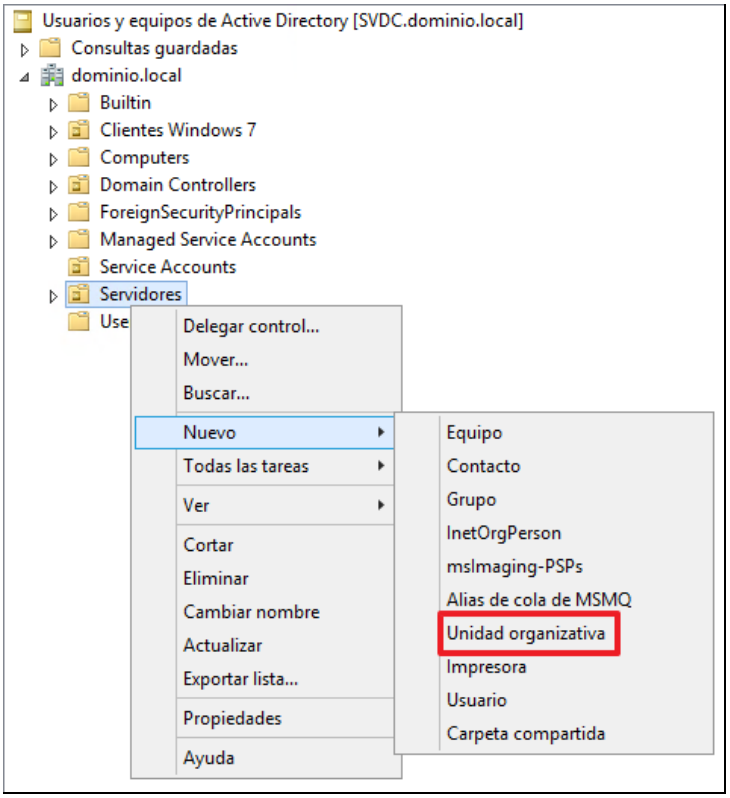
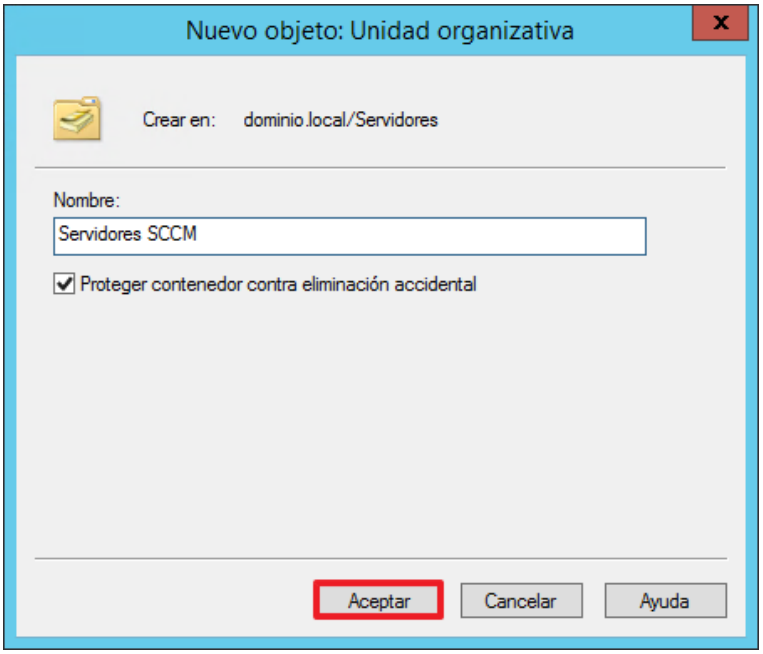
En el apartado siguiente, se describen las tareas para reforzar la seguridad de un servidor con el rol de servidor de sitio, el cual también incluye el rol de Sistema de sitio y servidor de componentes.

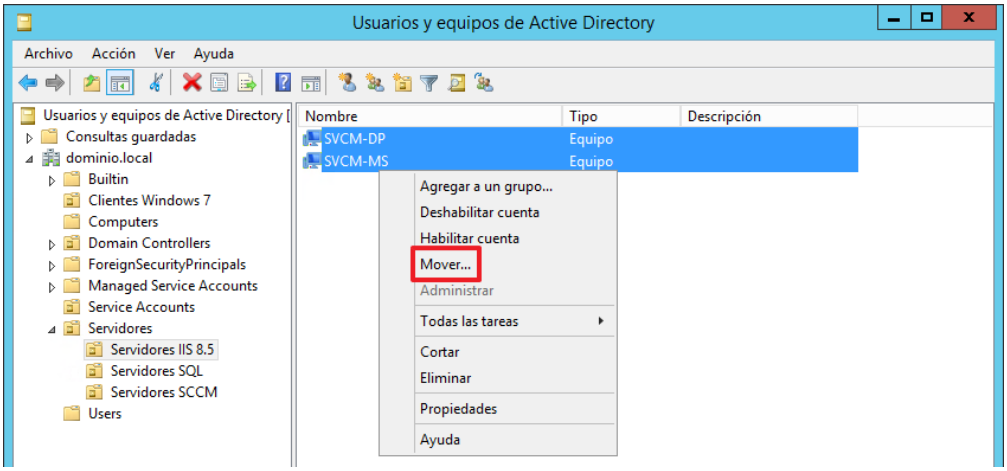
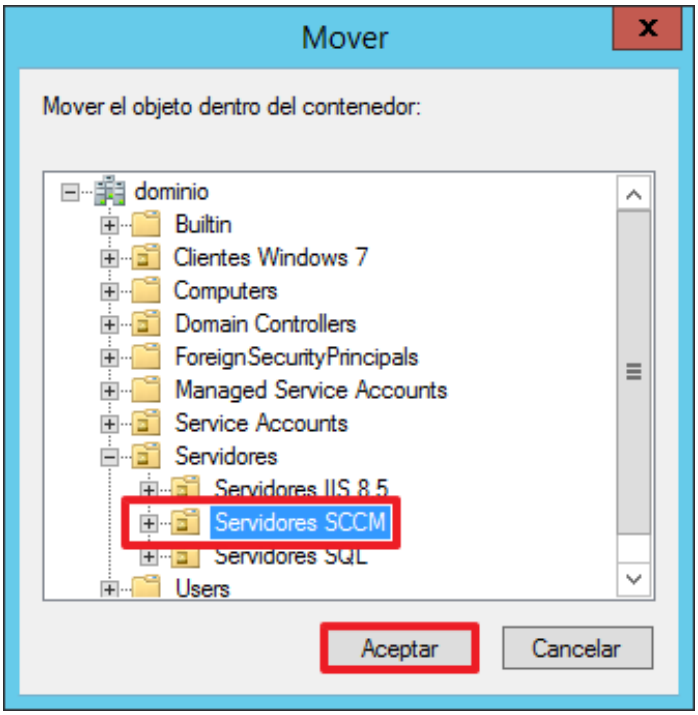
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

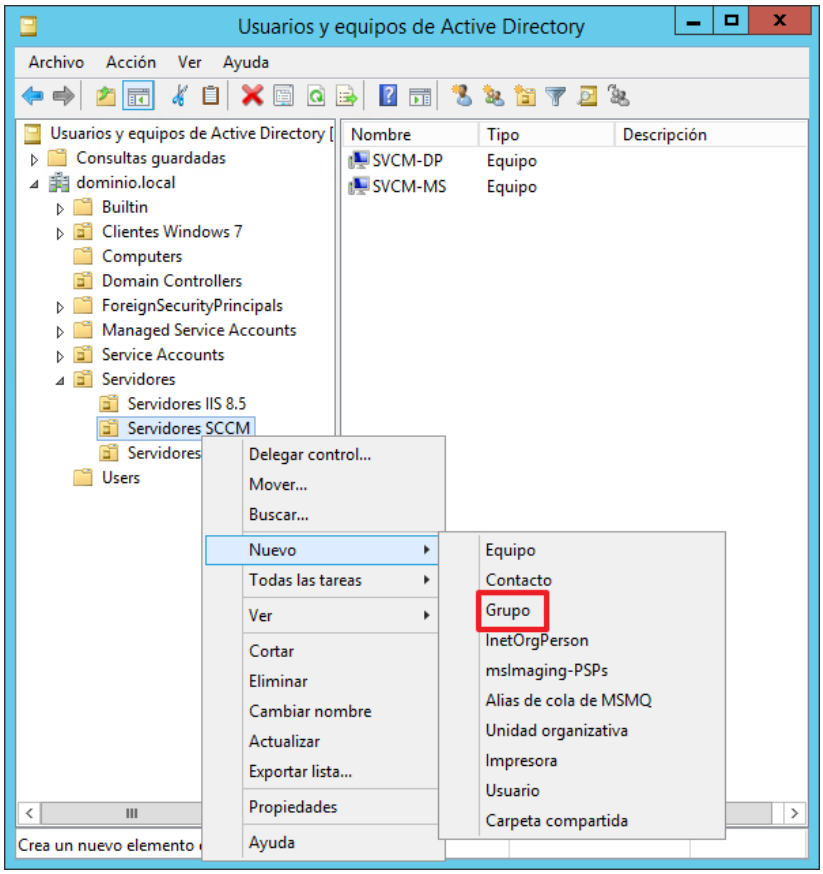
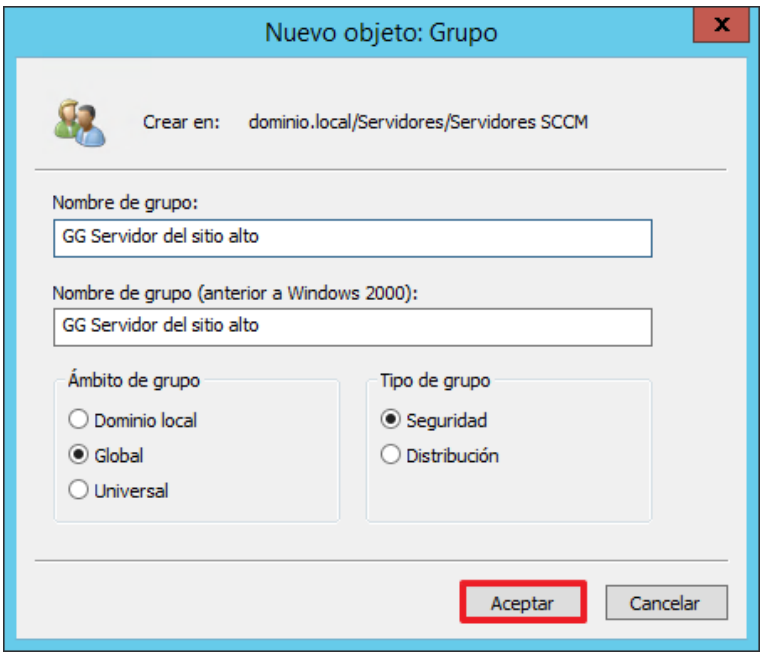
Paso	Descripción
58.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
59.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.
60.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.

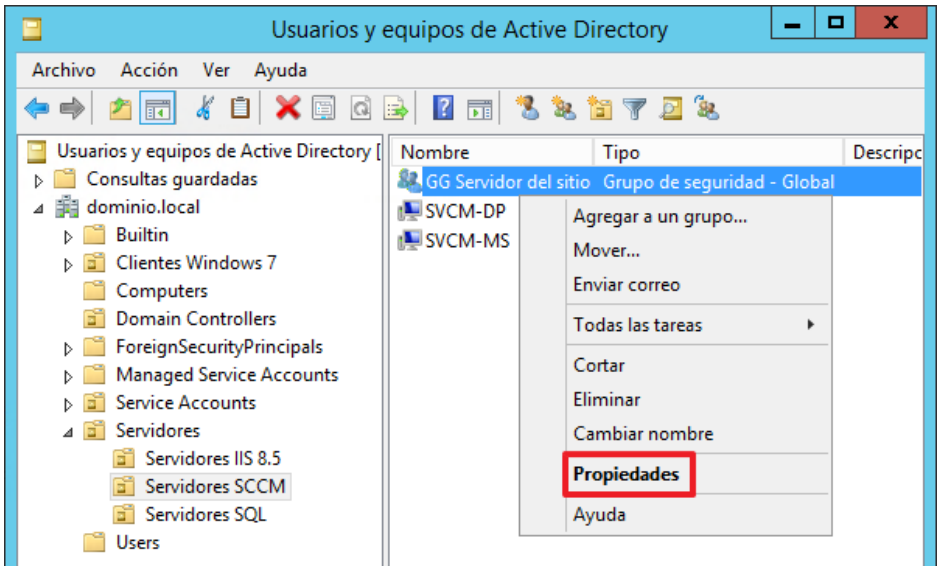
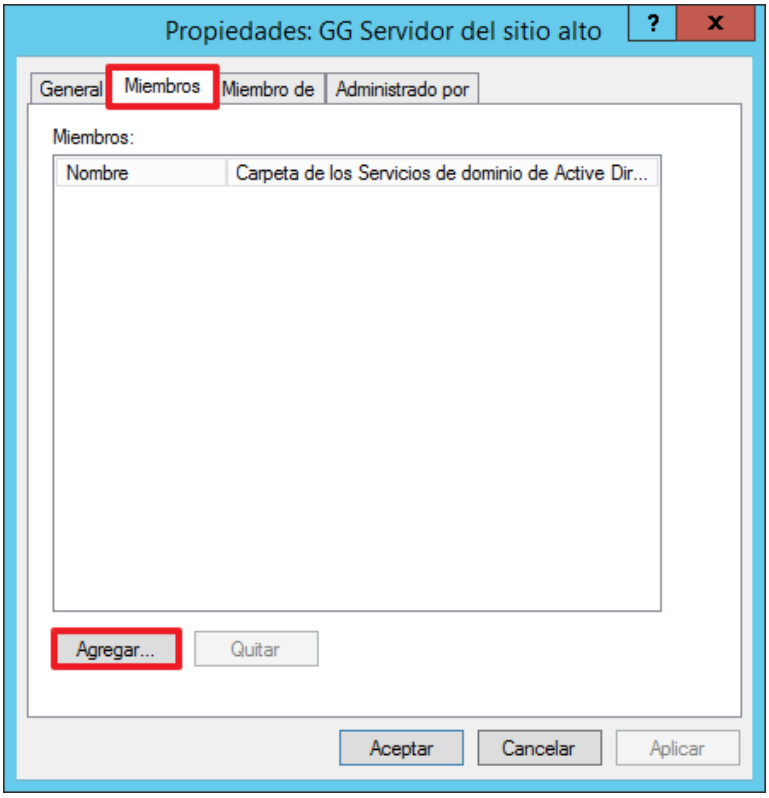
Paso	Descripción
61.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
62.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

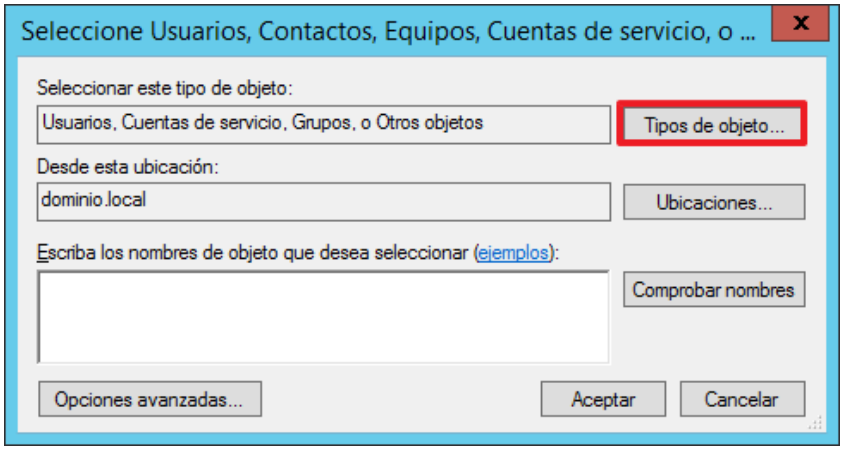
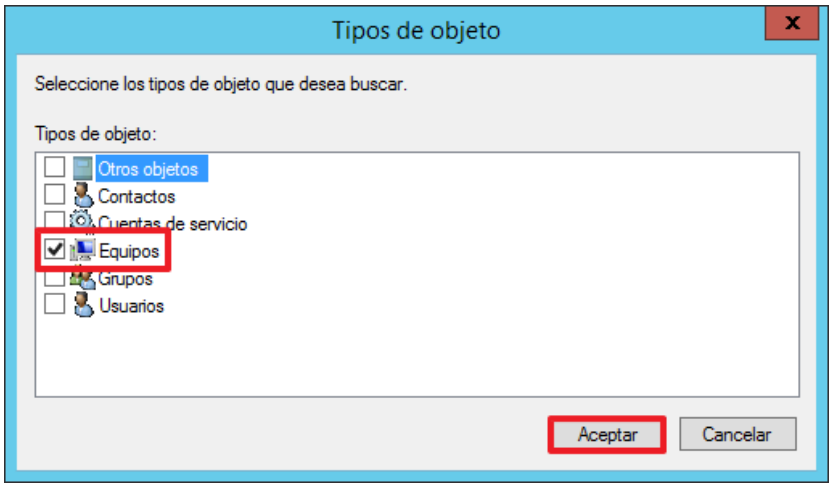
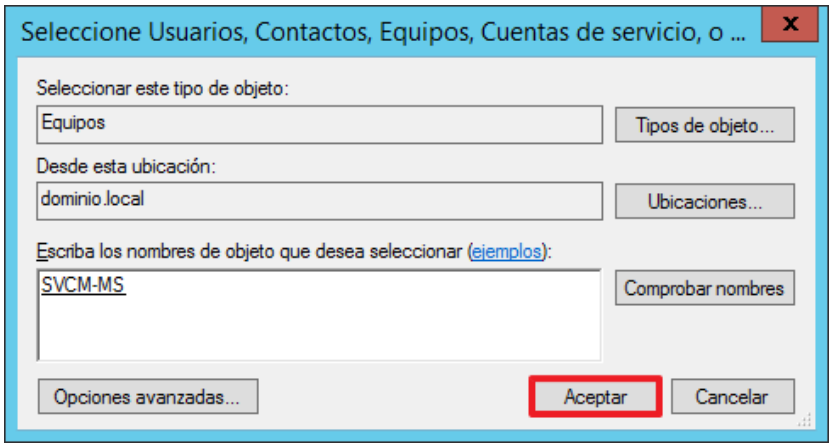
Paso	Descripción
63.	Copie los ficheros “CCN-STIC-875 ENS Incremental Servidor del sitio alto.inf” que se encuentra en la ruta “C:\Scripts\Nivel alto” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
64.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

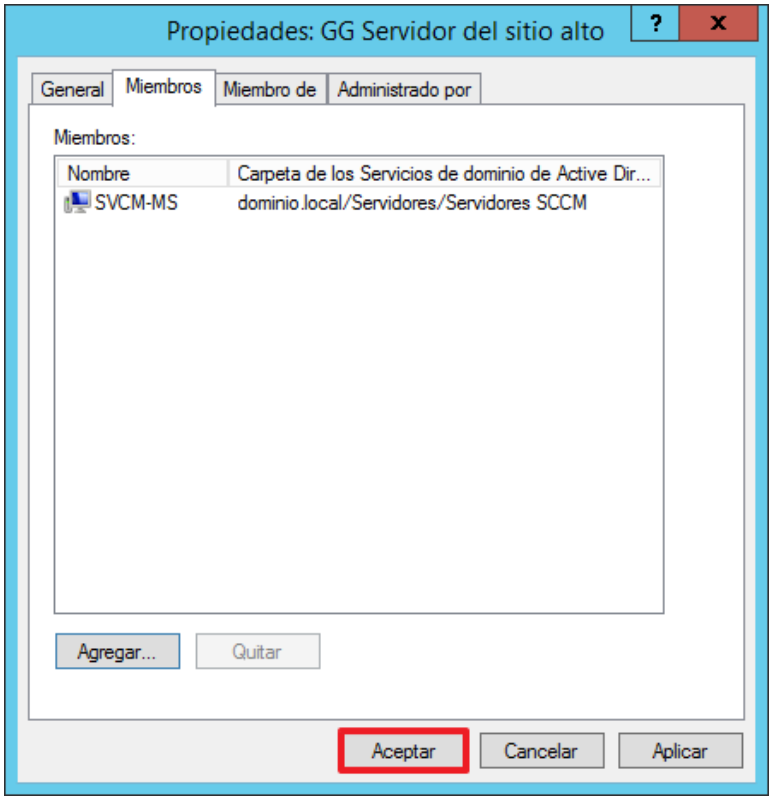
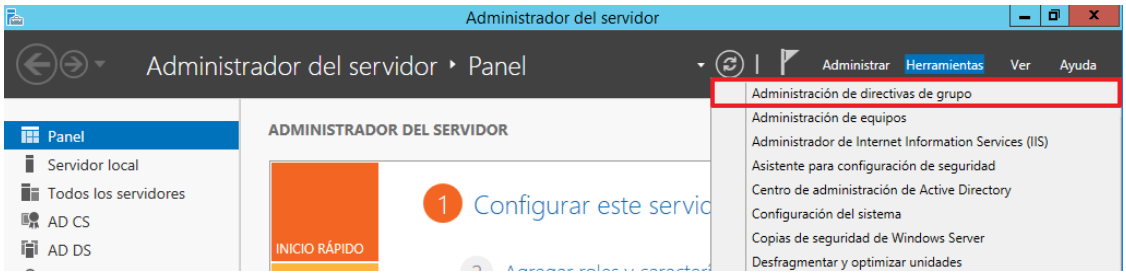
Paso	Descripción
65.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
66.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar” 

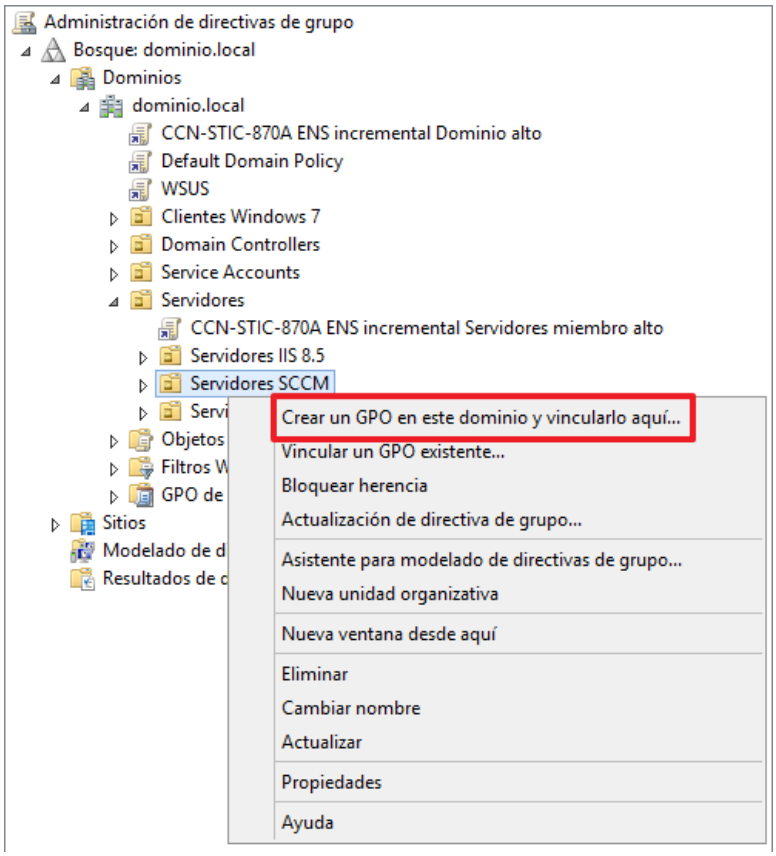
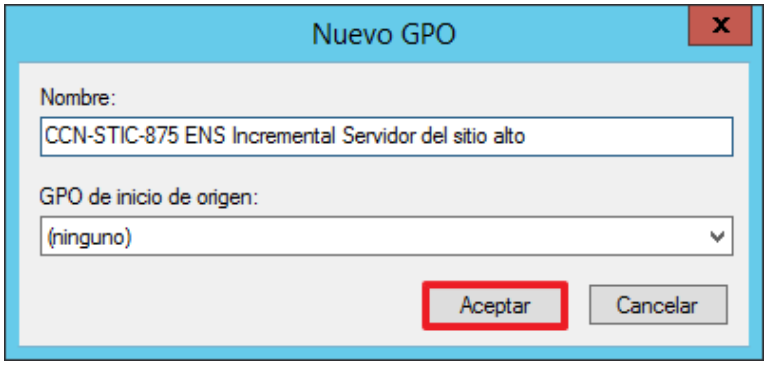
Paso	Descripción
67.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
68.	En el árbol de contenedores, seleccione la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

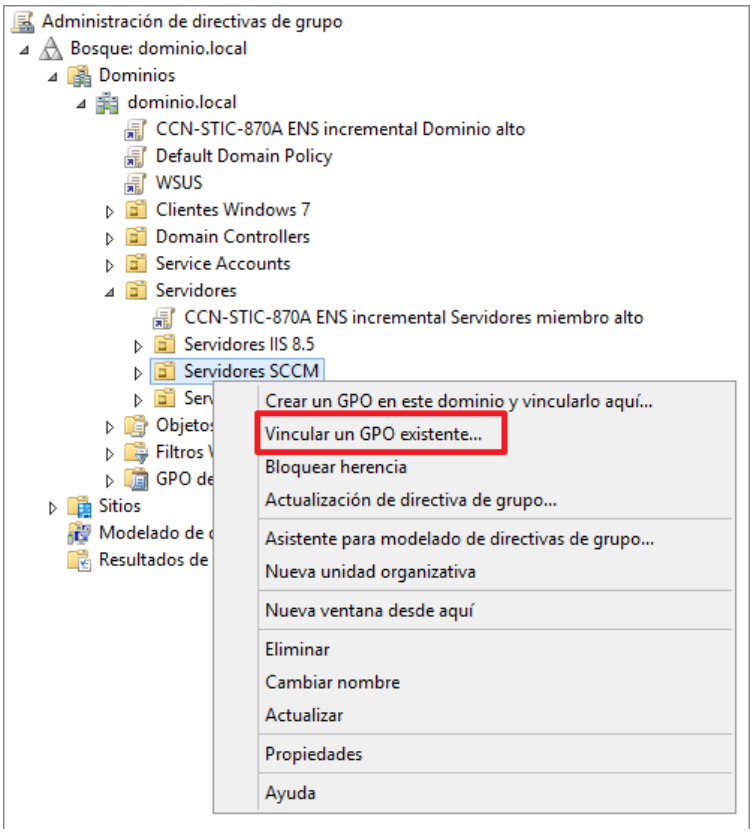
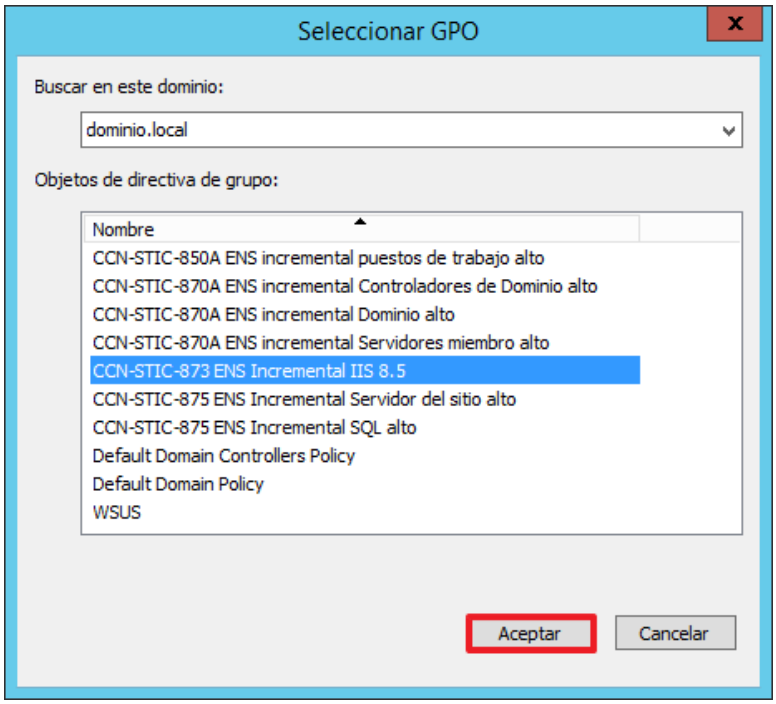
Paso	Descripción
69.	Para el siguiente paso, seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
70.	Escriba el nombre “GG Servidor del sitio alto” y pulse “Aceptar”. 

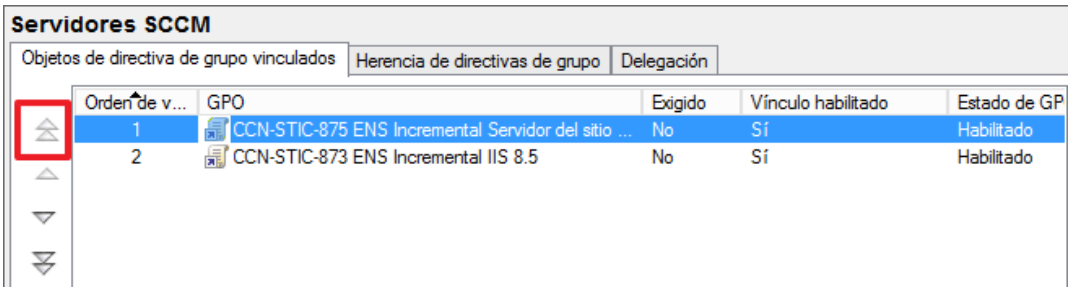
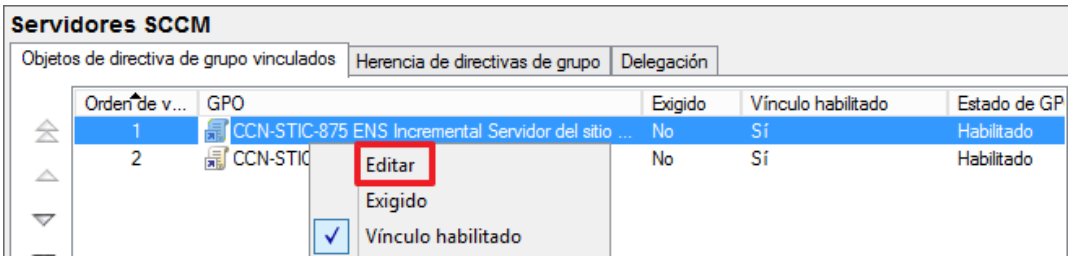
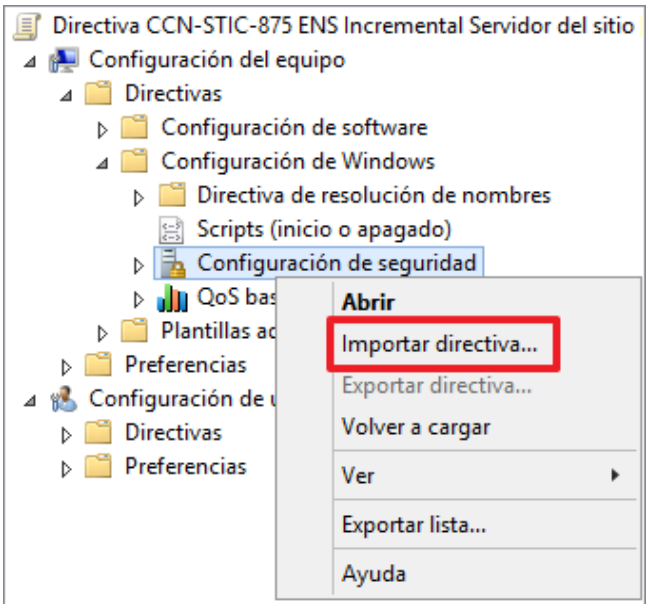
Paso	Descripción
71.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
72.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “servidor de sitio” al grupo. 

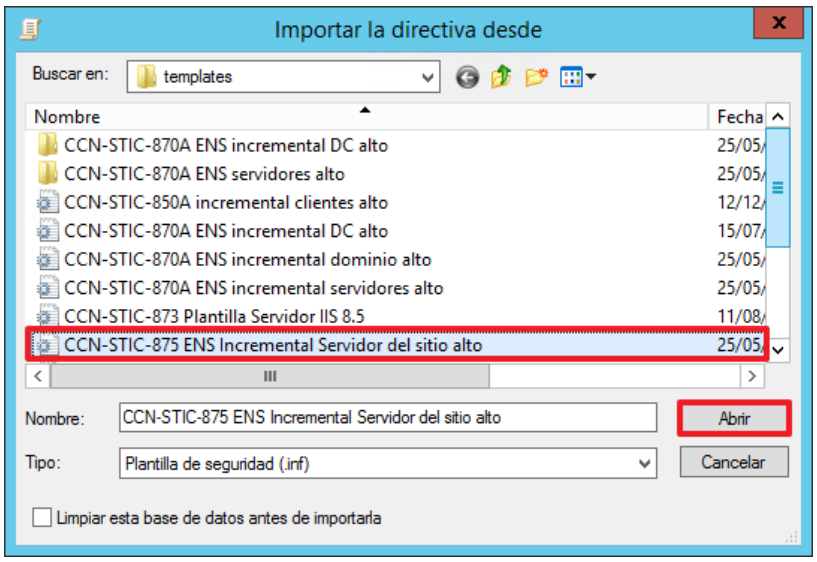
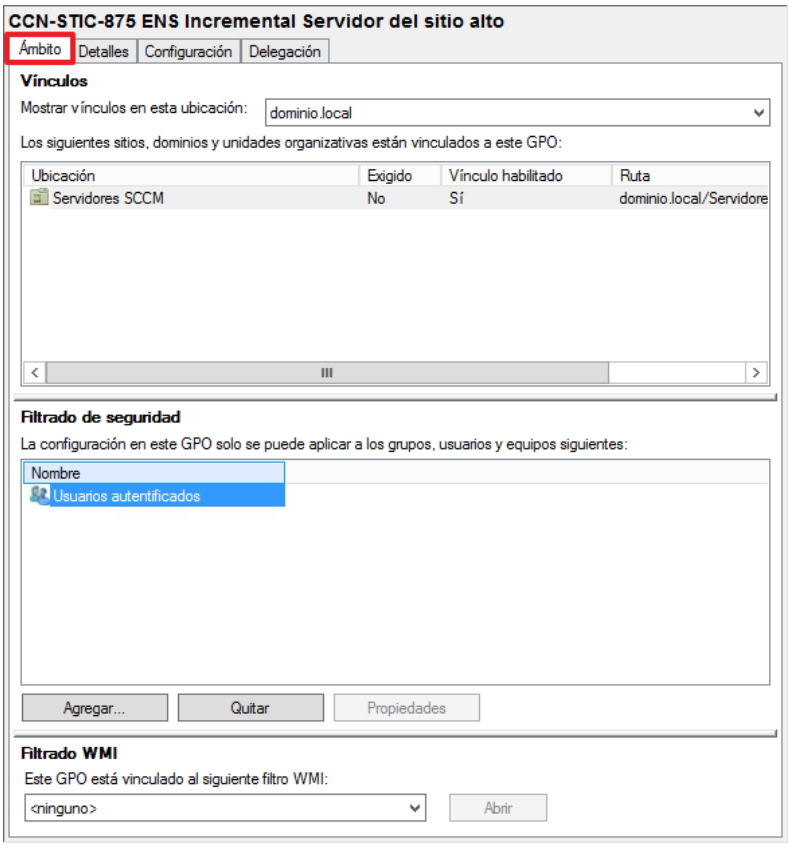
Paso	Descripción
73.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
74.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
75.	Agregue los equipos y pulse sobre “Aceptar”. 

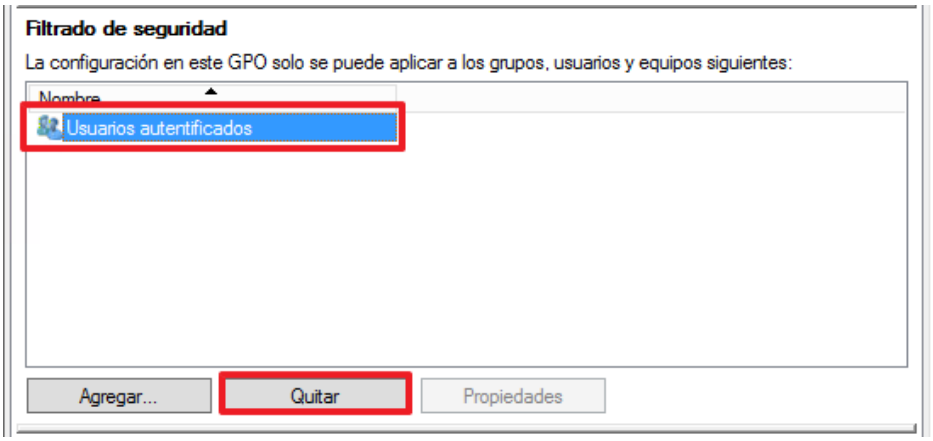
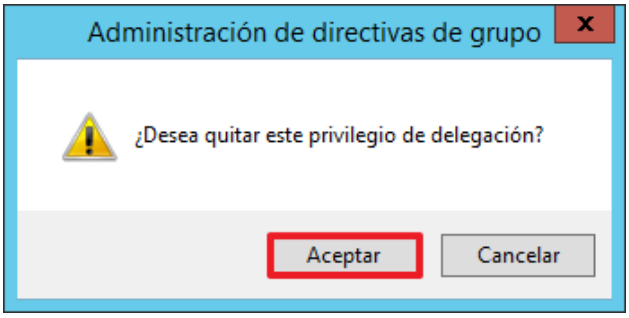
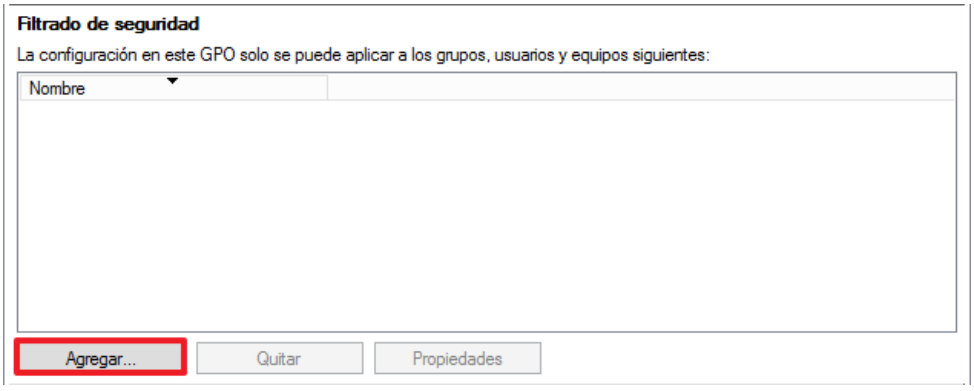
Paso	Descripción
76.	Marque de nuevo en “Aceptar” para cerrar las propiedades del grupo. 
77.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
78.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

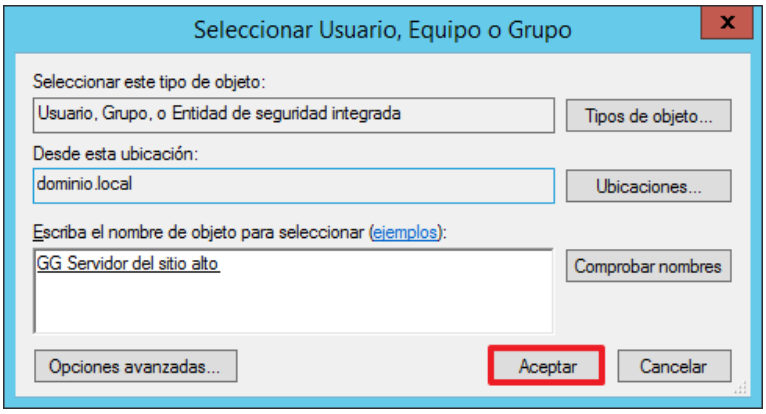
Paso	Descripción
79.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
80.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Servidor del sitio alto” y haga clic en el botón “Aceptar”. 
81.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.

Paso	Descripción
82.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
83.	A continuación, seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre “Aceptar”. 

Paso	Descripción
84.	Para que la aplicación de las directivas se realice en el orden correcto, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Servidor del sitio alto" aparezca en primer lugar. Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Servidor del sitio alto" y a continuación, haga clic sobre la fecha doble hacia arriba para que se sitúe con el número 1 de orden vínculos, tal y como se muestra en la imagen. 
85.	A continuación, edite la GPO: "CCN-STIC-875 ENS Incremental Servidores del sitio alto" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
86.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**" y haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
87.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Servidor del sitio alto.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
88.	Cierre el “editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
89.	Seleccione el nuevo objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Servidor del sitio alto” y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

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

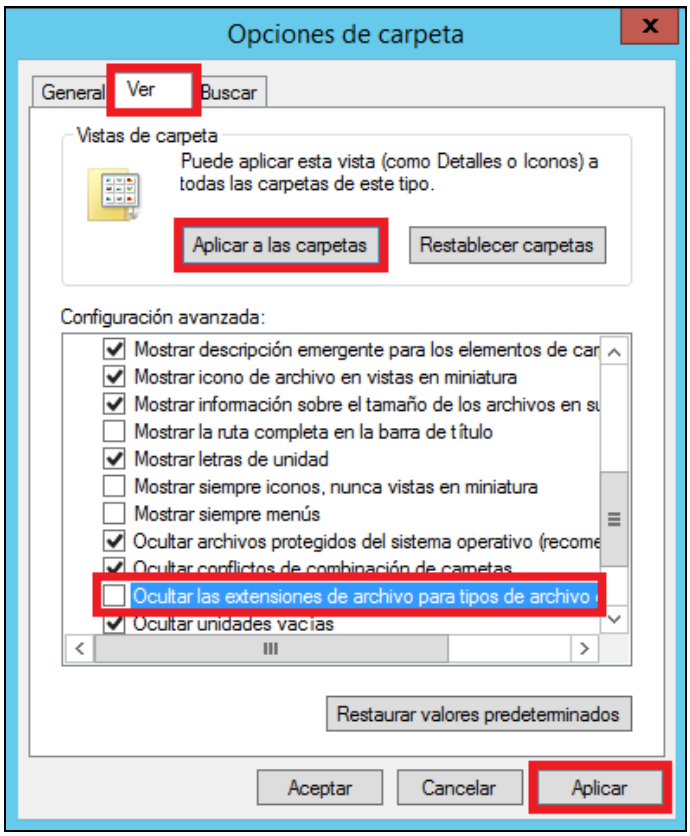
Paso	Descripción
93.	Introduzca como nombre “GG Servidor del sitio alto” <y pulse sobre el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
94.	Cierre el administrador de directivas de grupo para finalizar con la configuración.

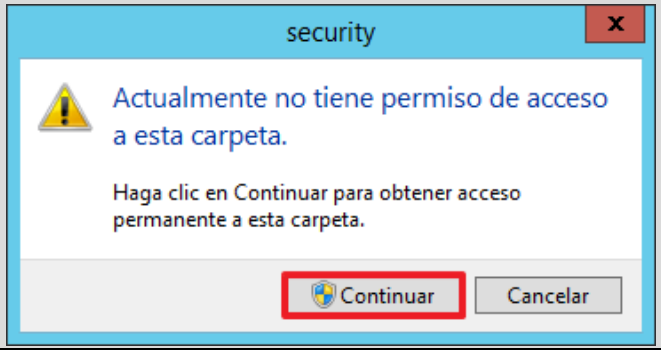
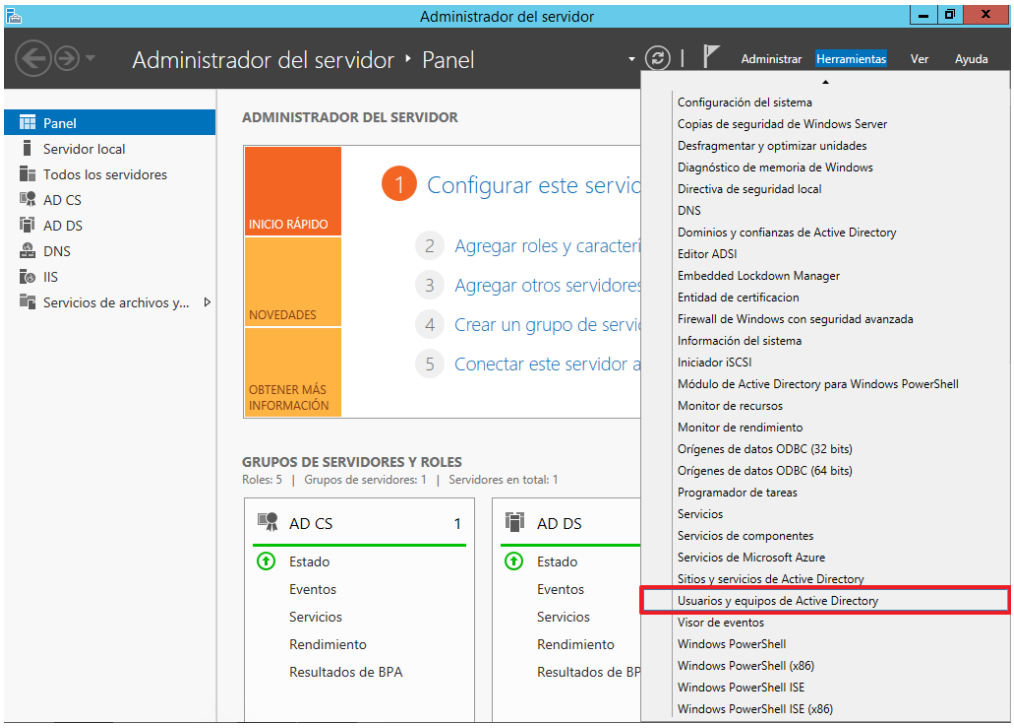
3. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE ADMINISTRACIÓN

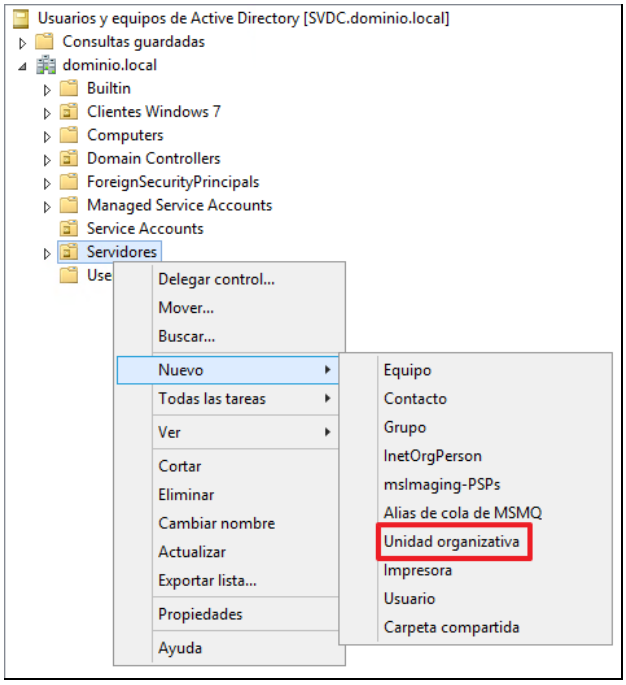
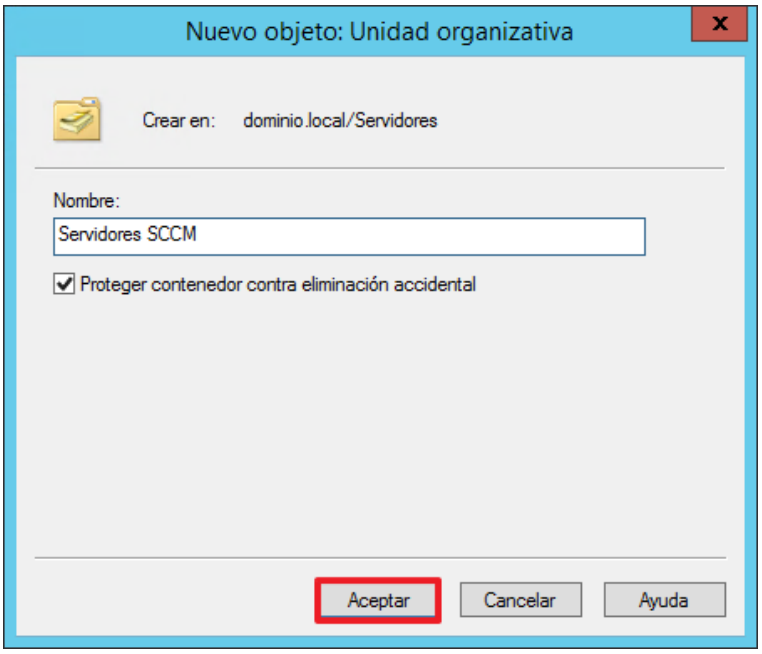
En el apartado siguiente, se describen las tareas para reforzar la seguridad de los servidores que disponen del rol de punto de administración implementado en el equipo.

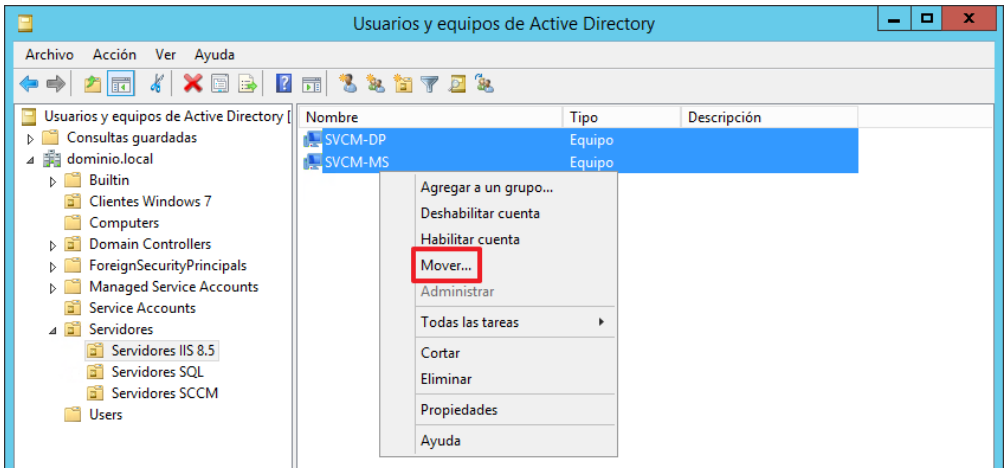
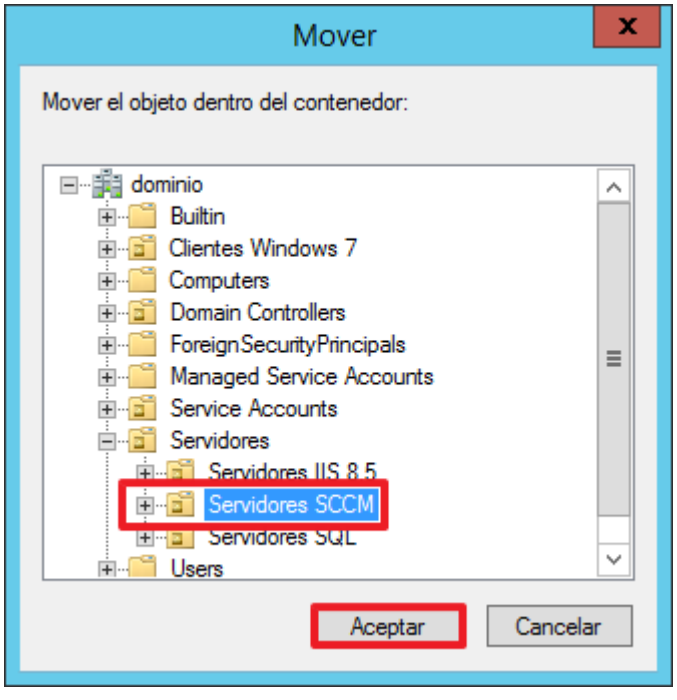
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

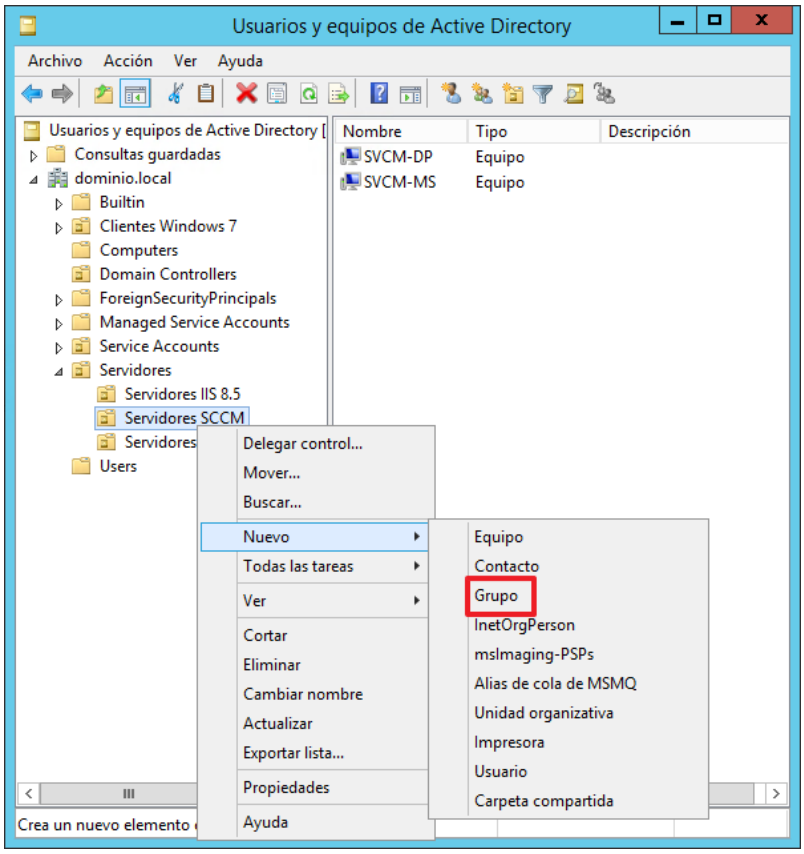
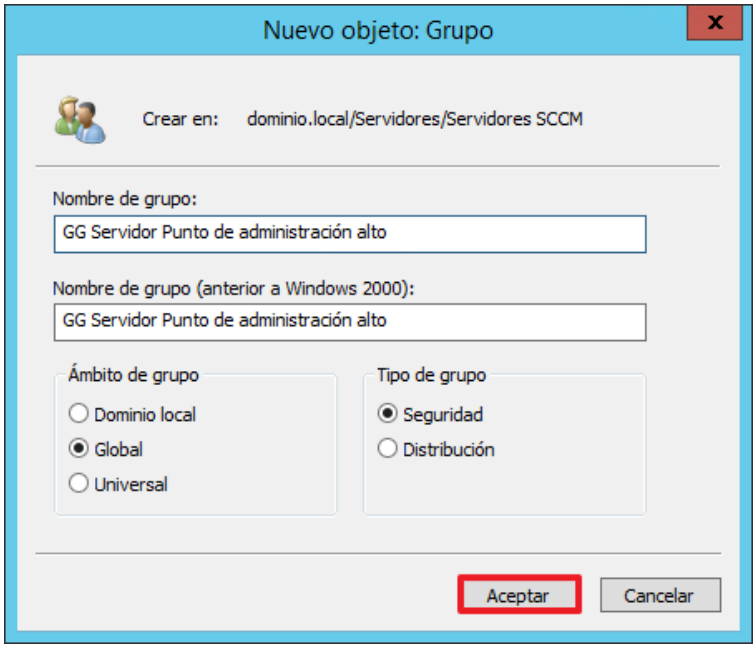
Paso	Descripción
95.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
96.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

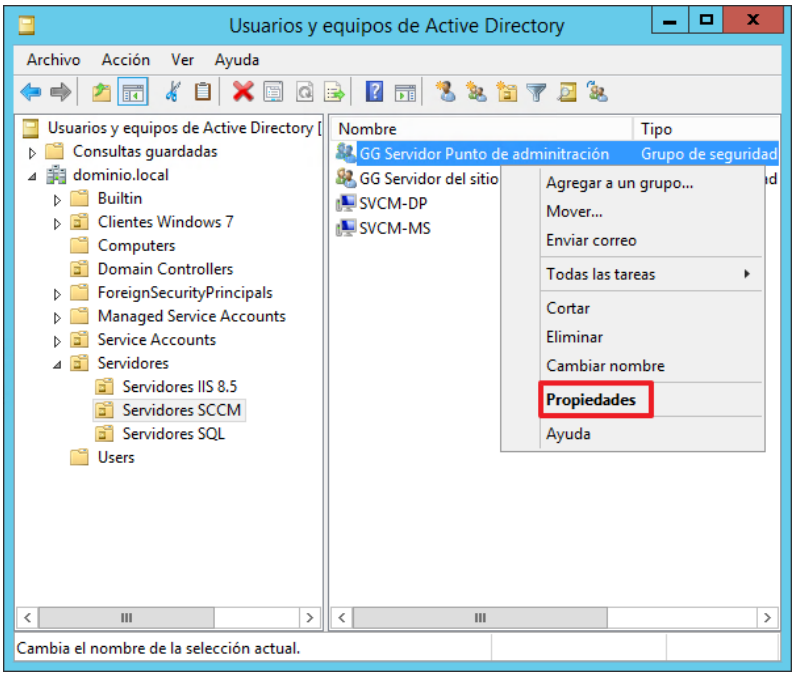
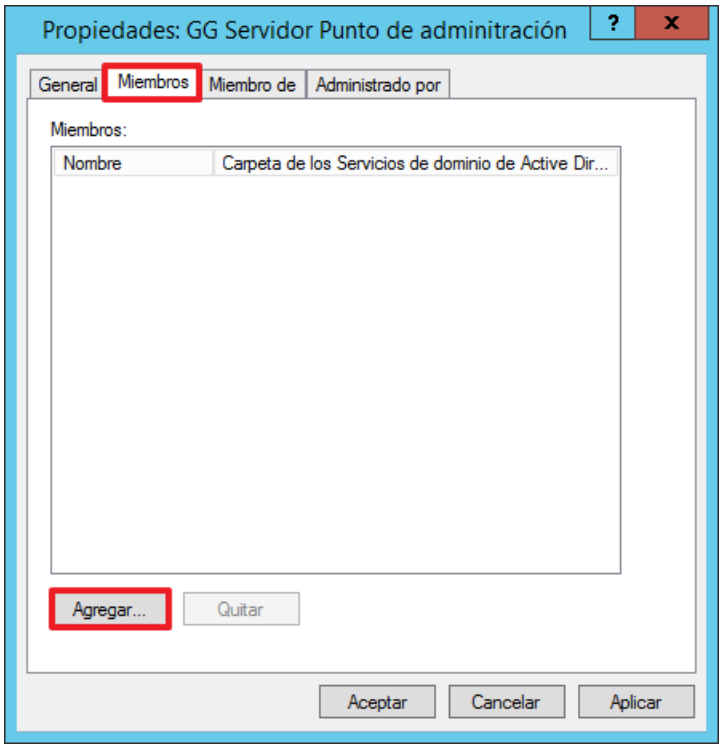
Paso	Descripción
97.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
98.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
99.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

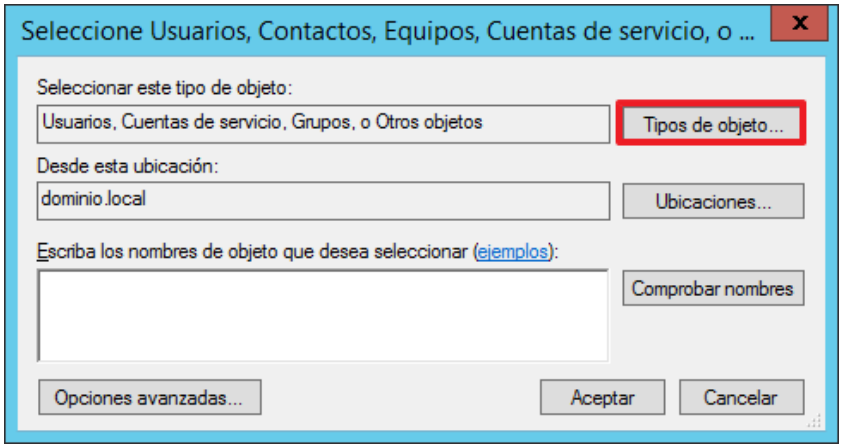
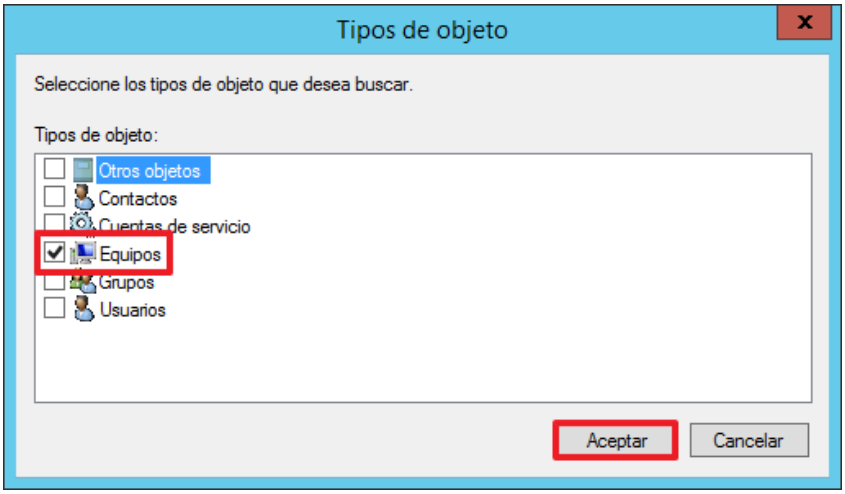
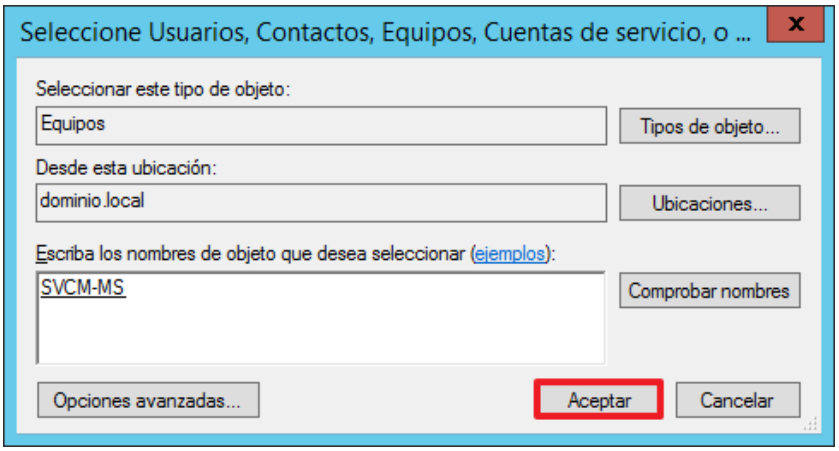
Paso	Descripción
100.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de administración alto.inf” que se encuentra en la ruta “C:\Scripts\Nivel alto” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
101.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
102.	A continuación, se va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 105. En caso contrario continúe con el paso a paso.

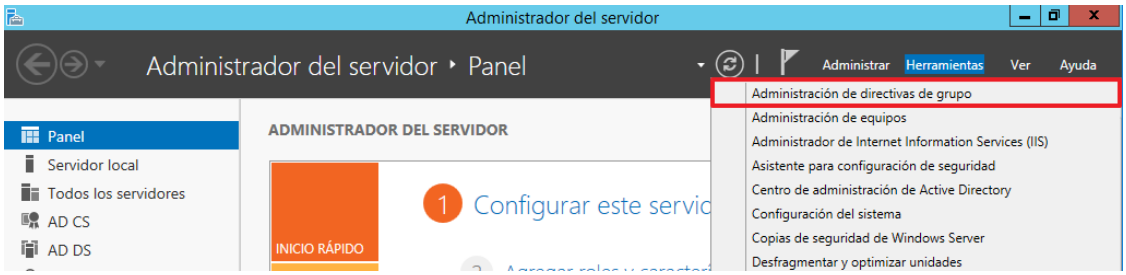
Paso	Descripción
103.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
104.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar”. 

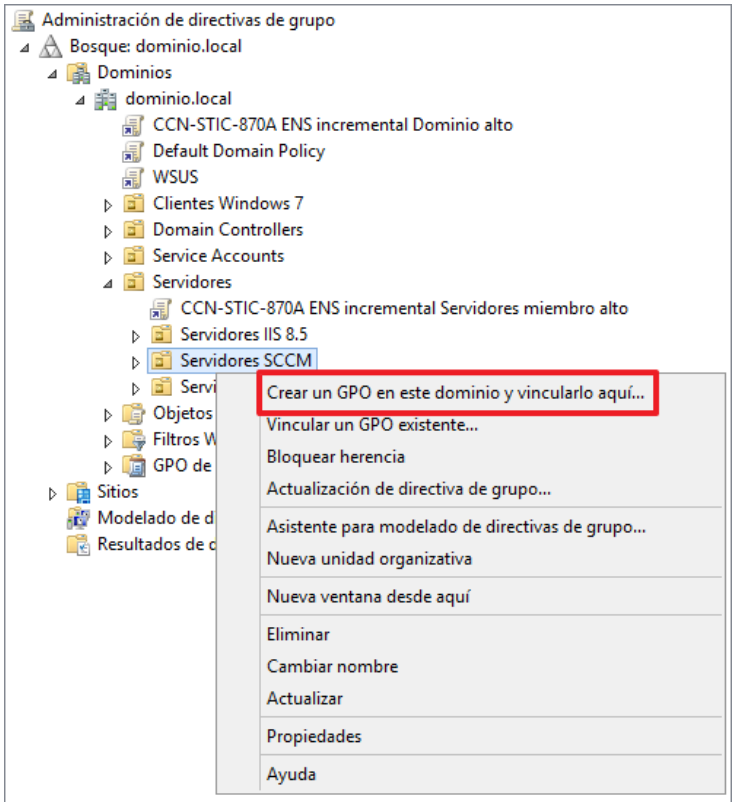
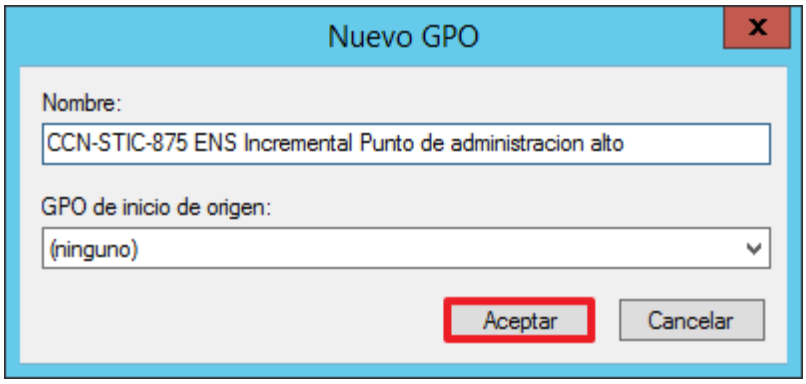
Paso	Descripción
105.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
106.	A continuación, seleccione la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

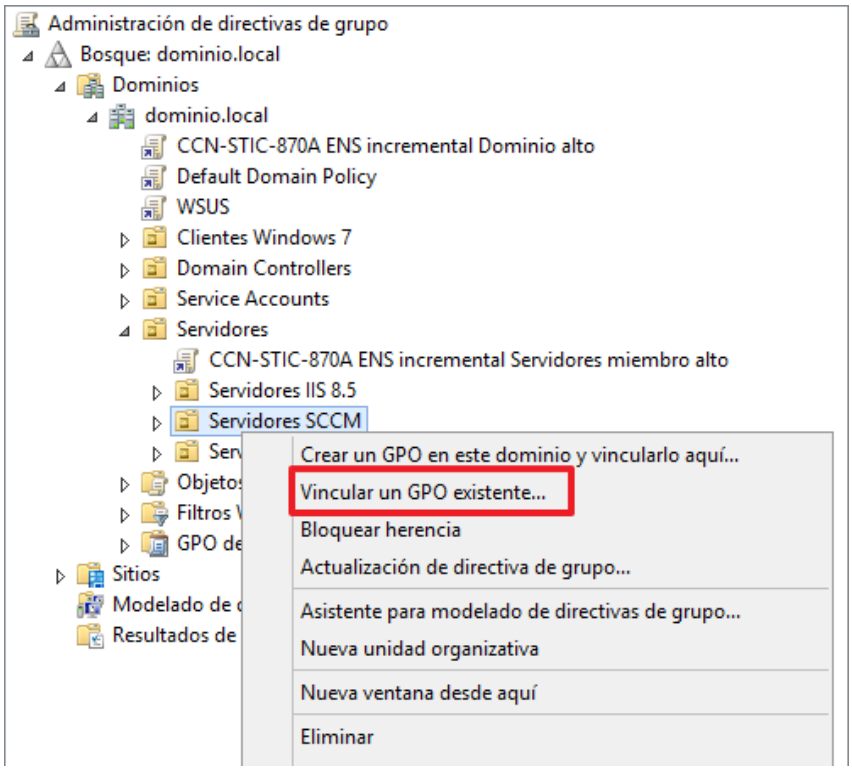
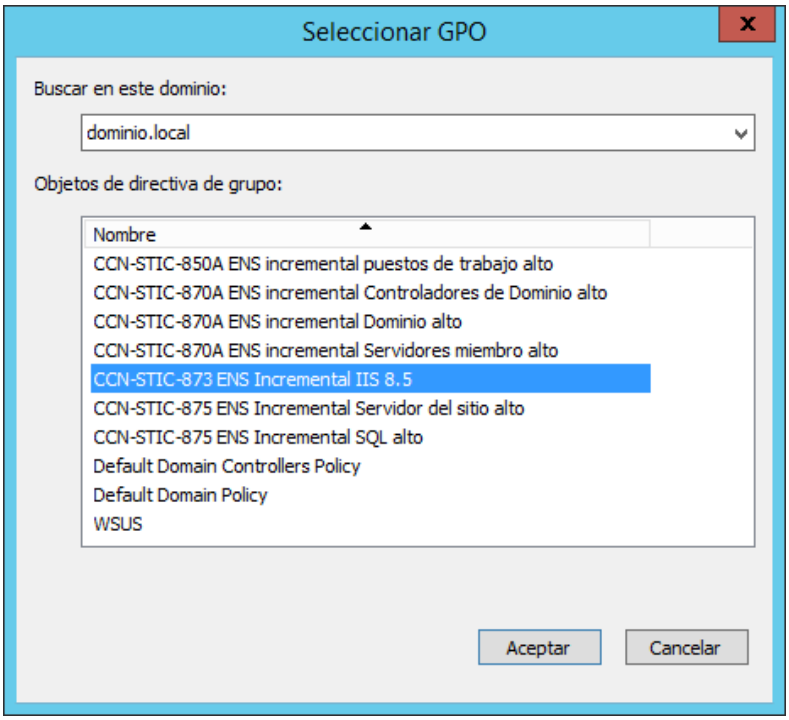
Paso	Descripción
107.	Para el siguiente paso, seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
108.	Escriba el nombre “GG Servidor Punto de administración alto” y pulse “Aceptar”. 

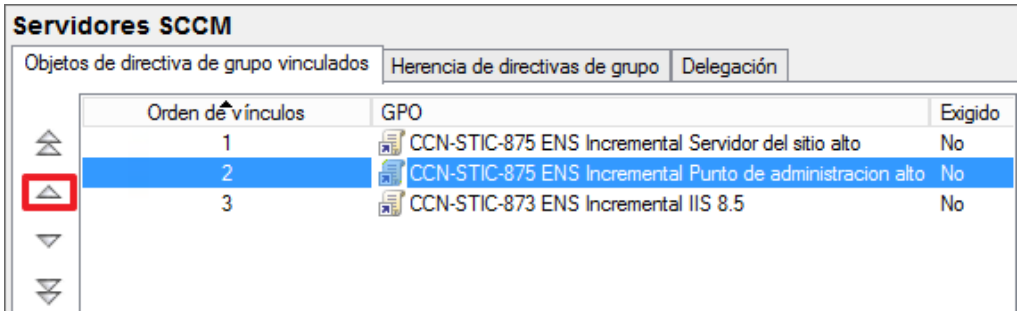
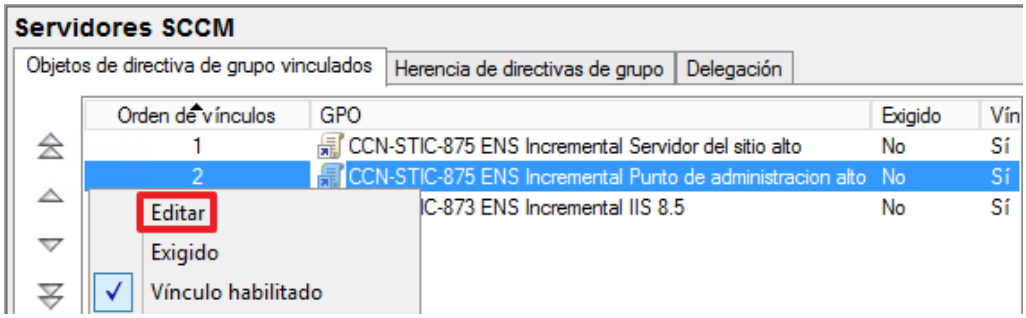
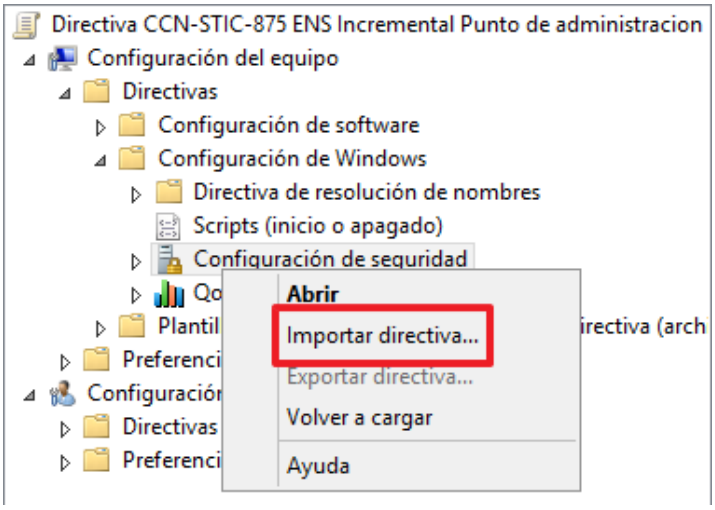
Paso	Descripción
109.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
110.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de administración” al grupo. 

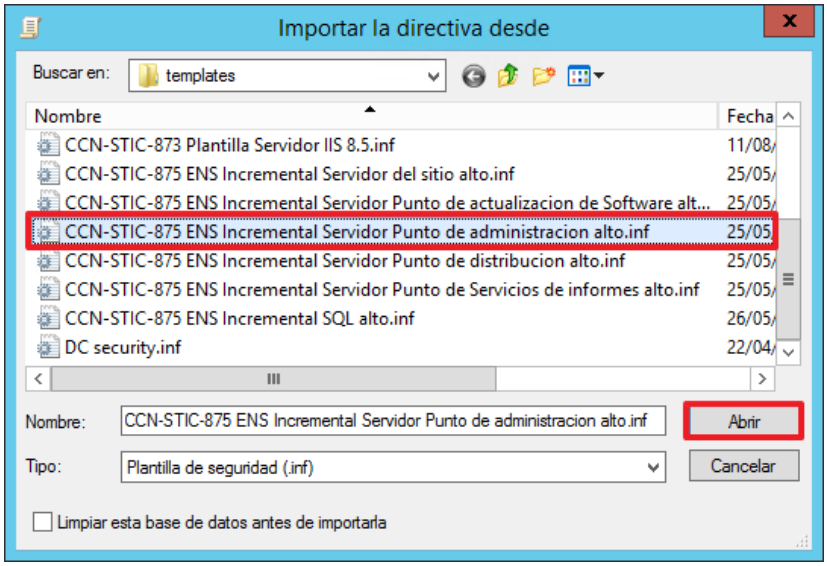
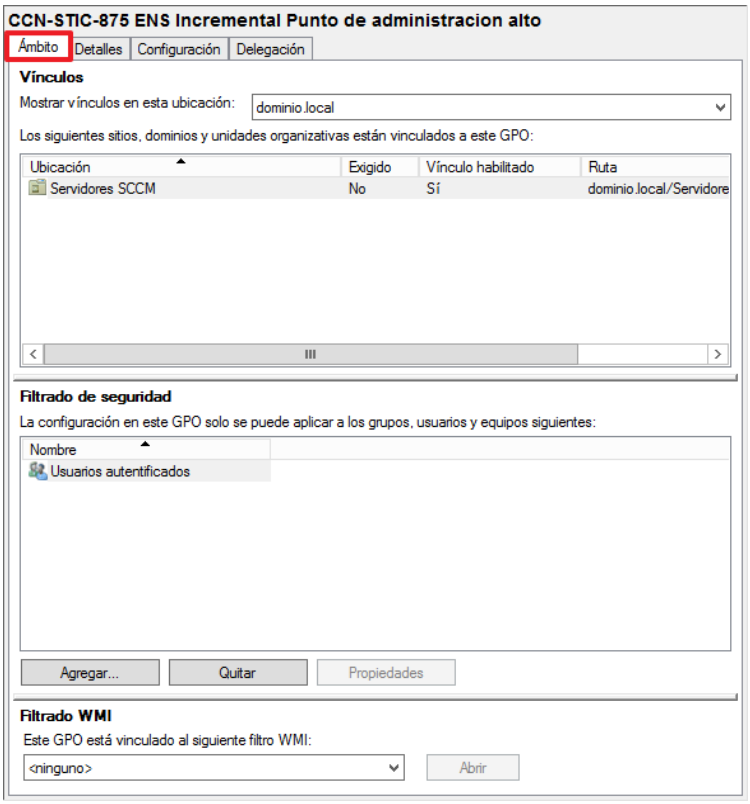
Paso	Descripción
111.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
112.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
113.	Agregue los equipos y pulse sobre “Aceptar”. 

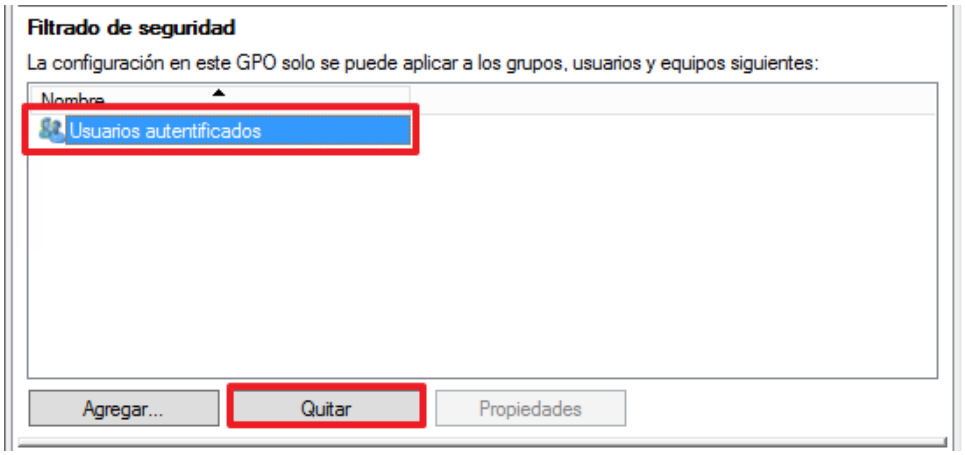
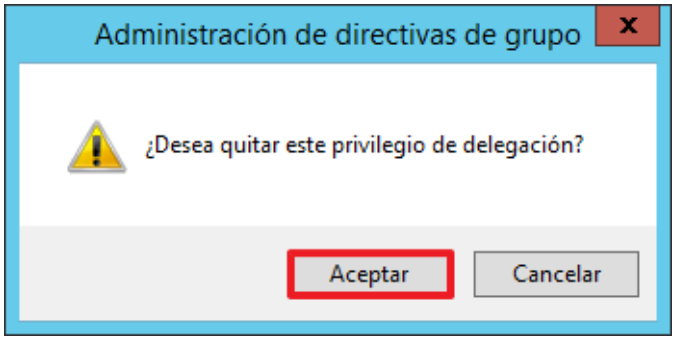
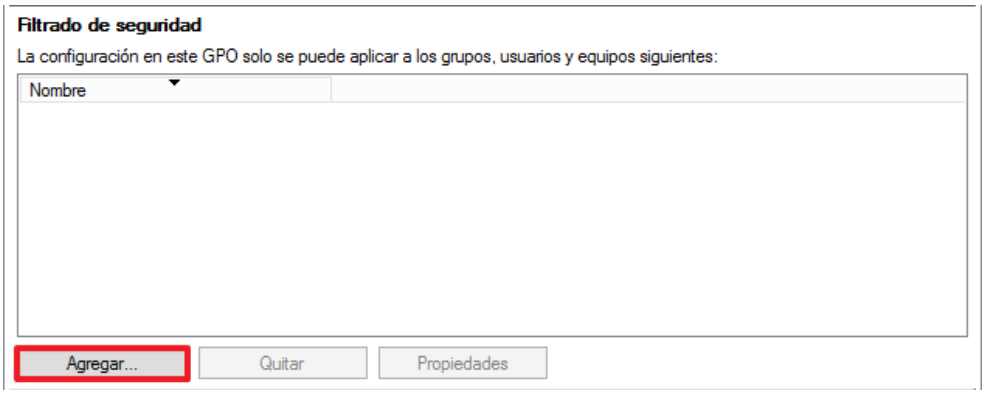
Paso	Descripción
114.	Marque de nuevo en “Aceptar” para cerrar las propiedades del grupo. 
115.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
116.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

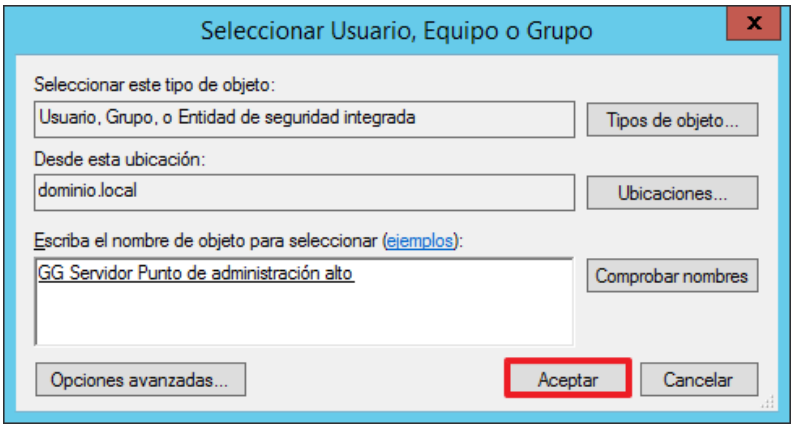
Paso	Descripción
117.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
118.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de administración alto” y haga clic en el botón “Aceptar”. 
119.	En los siguientes pasos, se va a asociar la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” en la unidad organizativa “Servidores SCCM”, en caso de que ya haya vinculado la directiva en algún paso anterior, continúe con el paso 124, en caso contrario continúe con el siguiente paso.
120.	A continuación, se vinculará la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.

Paso	Descripción
121.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
122.	A continuación, seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
123.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva “CCN-STIC-875 ENS Incremental Punto de administración alto” aparezca posicionada por encima de la directiva “CCN-STIC-873 ENS Incremental IIS 8.5”. Para ello seleccione, dentro de la unidad organizativa “Servidores SCCM”, la directiva “CCN-STIC-875 ENS Incremental Punto de administración alto” y a continuación, haga clic sobre la flecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
124.	A continuación, edite la GPO: “CCN-STIC-875 ENS Incremental Punto de administración alto” creada anteriormente haciendo clic con el botón derecho y seleccionando la opción “Editar” del menú contextual. 
125.	Expanda el nodo “**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**”. A continuación, haga clic con el botón derecho sobre “Configuración de seguridad” y seleccione en el menú contextual la opción “Importar directiva…”. 

Paso	Descripción
126.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de administración alto.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
127.	Cierre el "editor de administración de directivas de grupo" una vez que se haya realizado la importación de la configuración de seguridad.
128.	Seleccione el nuevo objeto de directiva de grupo "CCN-STIC-875 ENS Incremental Punto de administración alto.inf" y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

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

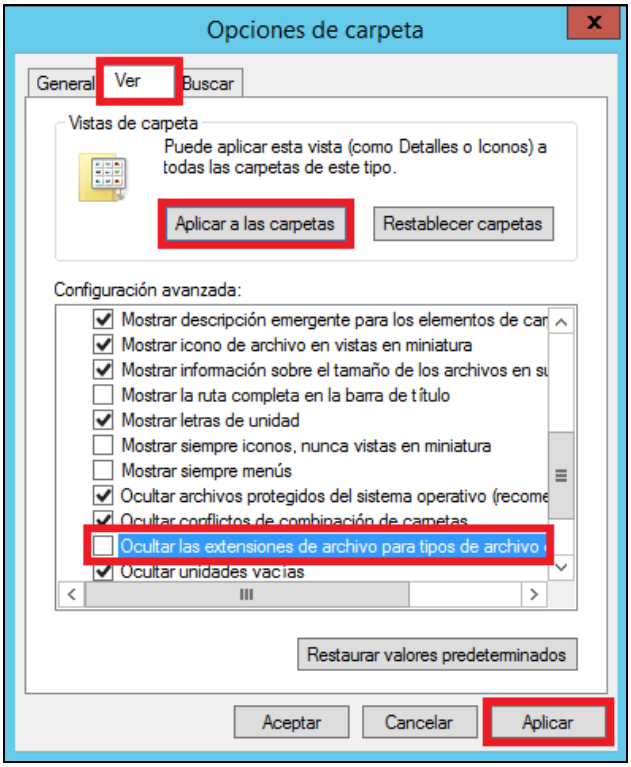
Paso	Descripción
132.	Introduzca como nombre “GG Servidor Punto de administración alto”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.

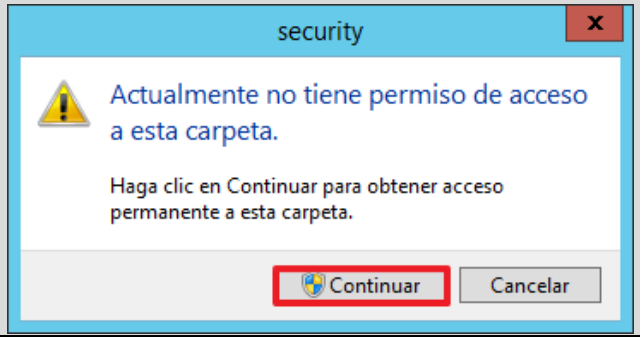
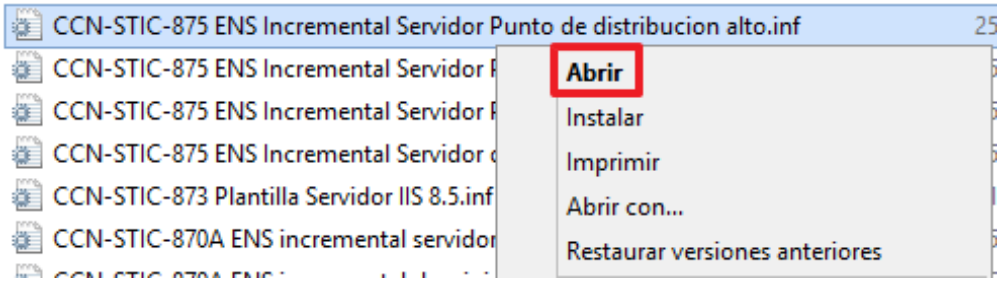
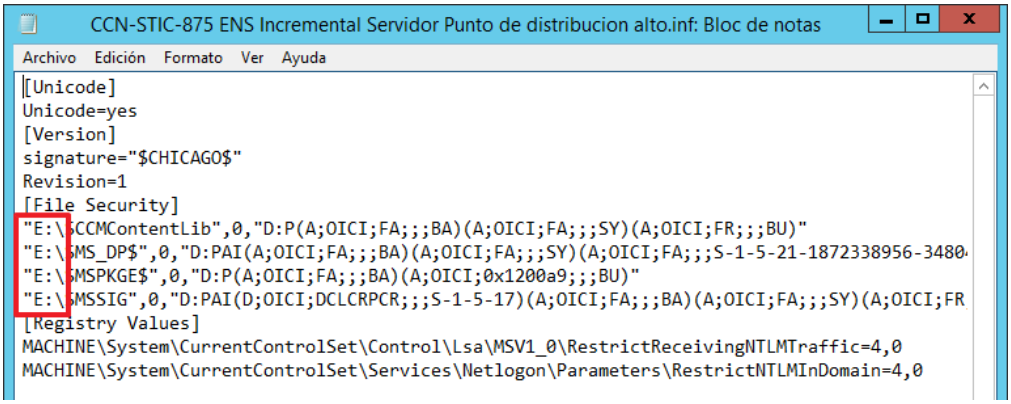
4. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE DISTRIBUCIÓN

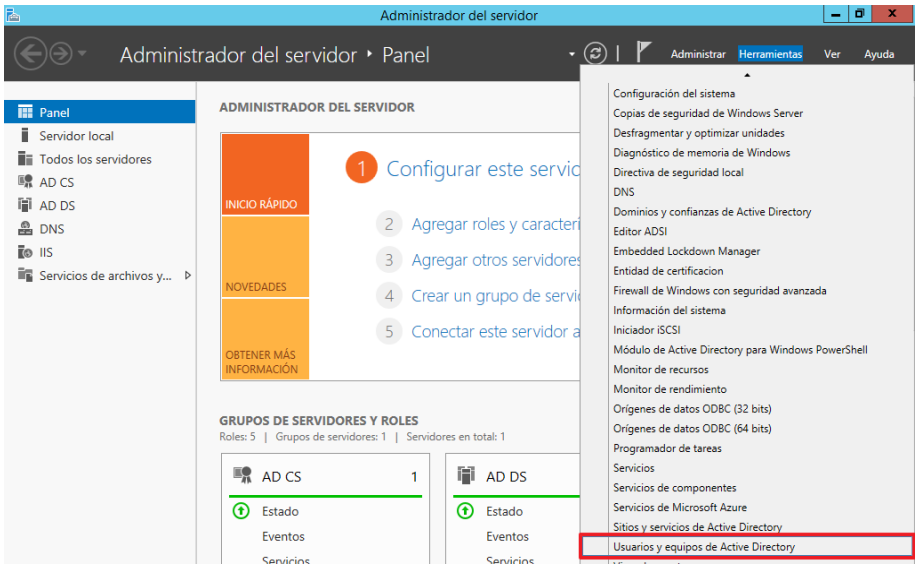
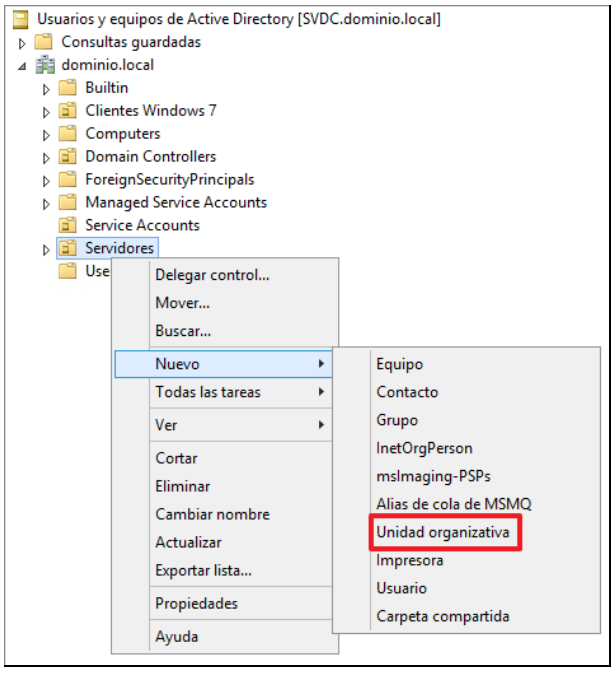
En el apartado siguiente, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de distribución implementado en el equipo.

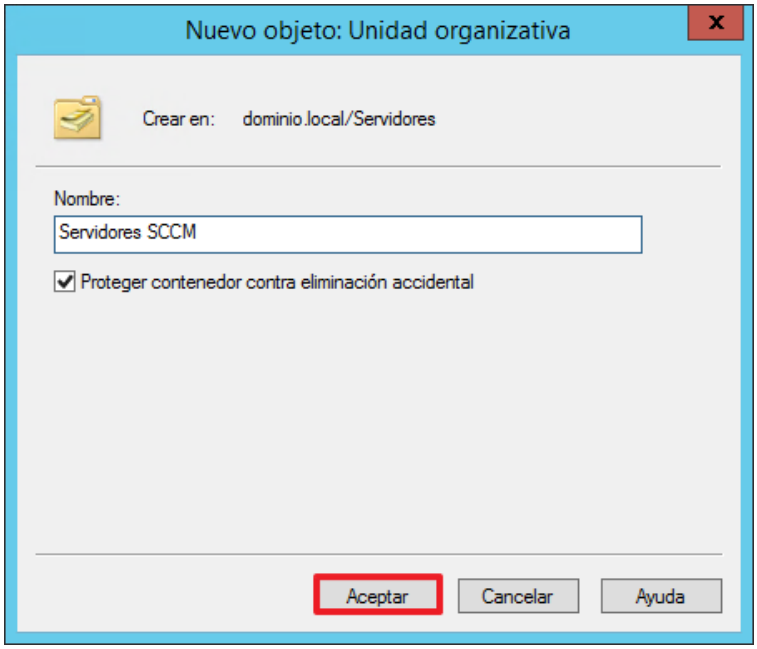
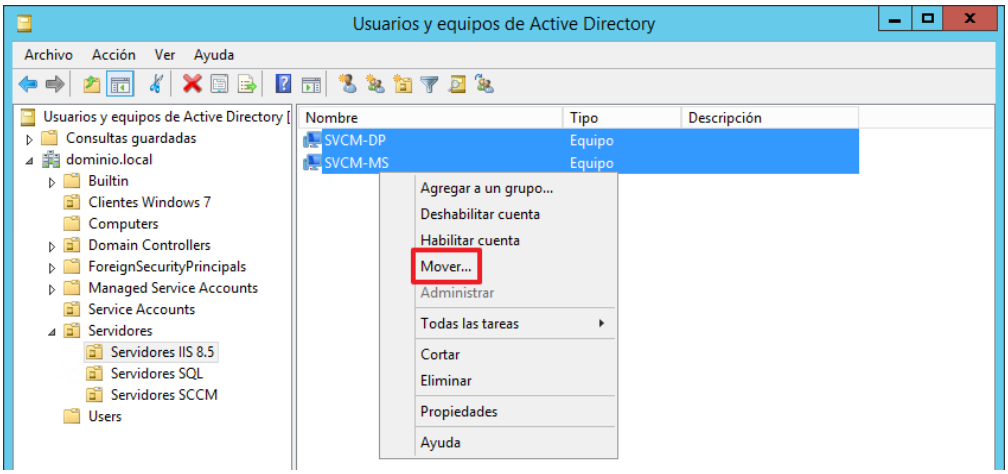
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

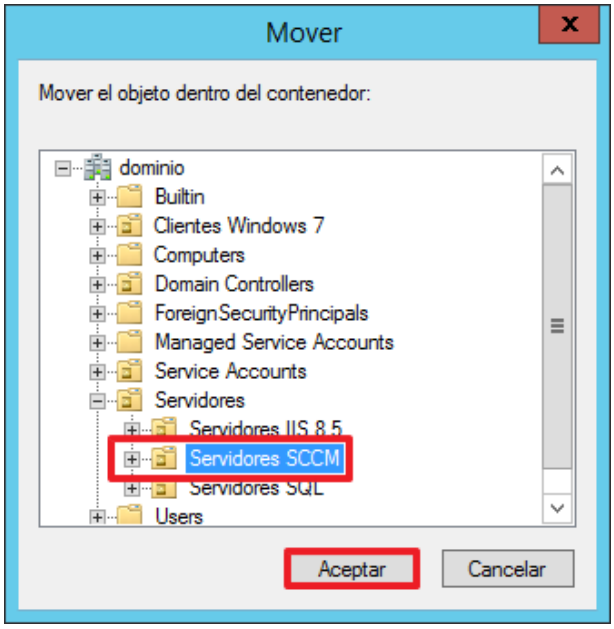
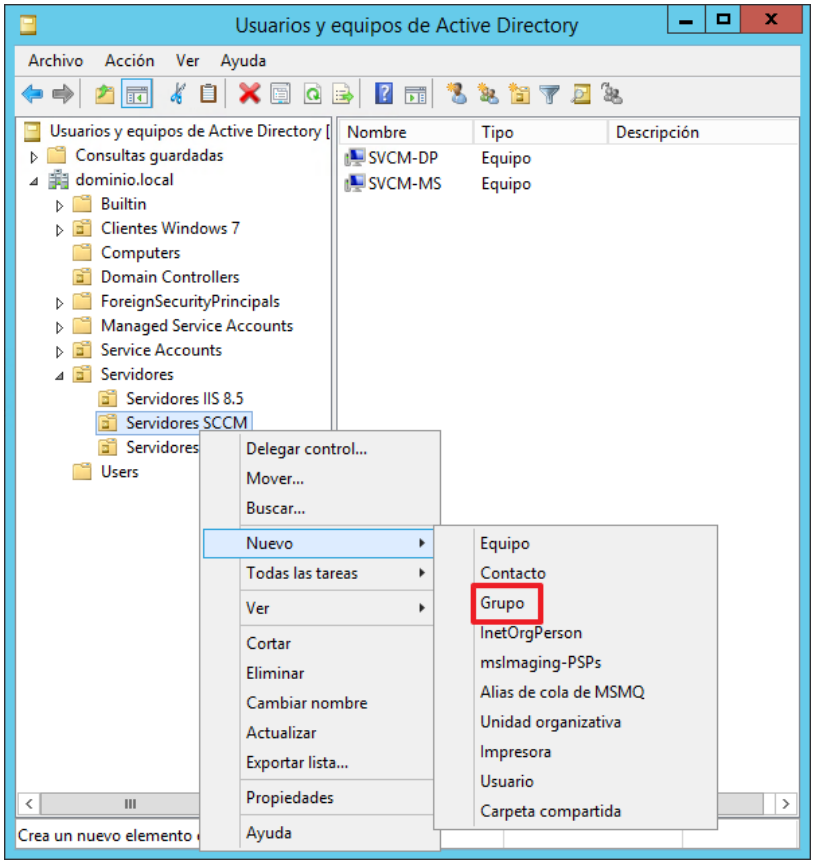
Paso	Descripción
133.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
134.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

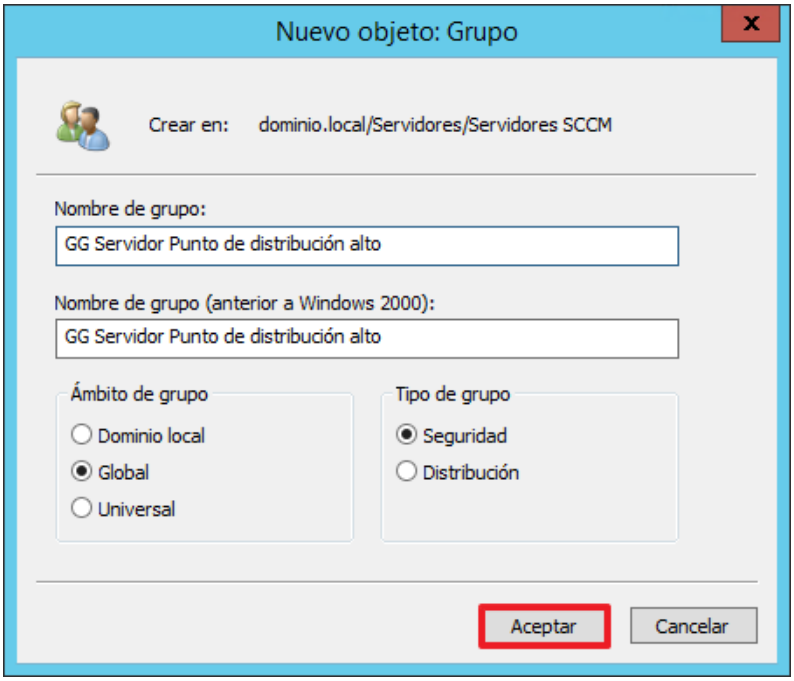
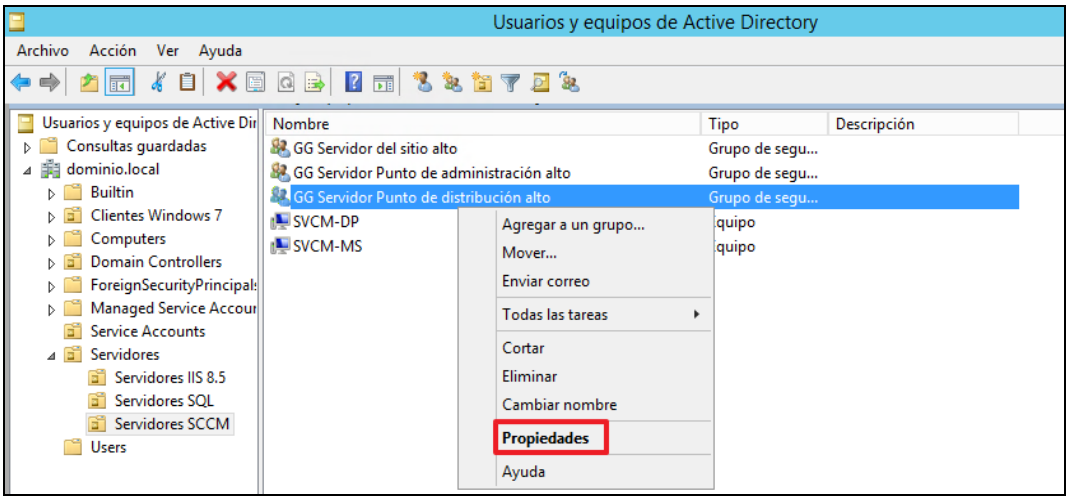
Paso	Descripción
135.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
136.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
137.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

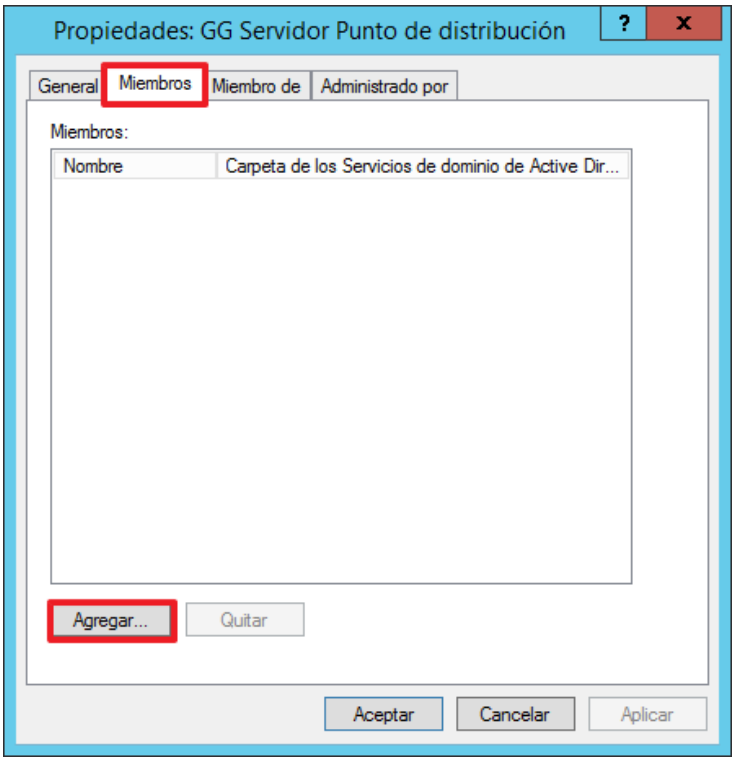
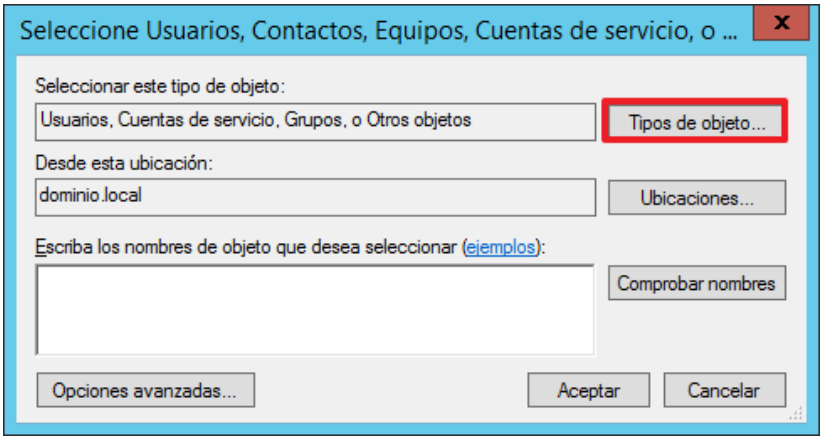
Paso	Descripción
138.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de distribución alto.inf” que se encuentra en la ruta “C:\Scripts\Nivel alto” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
139.	Pulse con el botón derecho sobre el fichero y seleccione la opción “Abrir” del menú contextual. 
140.	Deberá modificar la ruta del fichero para adaptarlo a su organización, para ello localice la ruta de las carpetas sobre las que desea aplicar seguridad y modifíquela en función de la ruta de directorios de su organización.  **Nota:** Si no modifica este fichero los permisos establecidos en la presente guía no se aplicarán correctamente sobre las carpetas que se quiere reforzar la seguridad.
141.	Guarde los cambios realizados y cierre el documento.

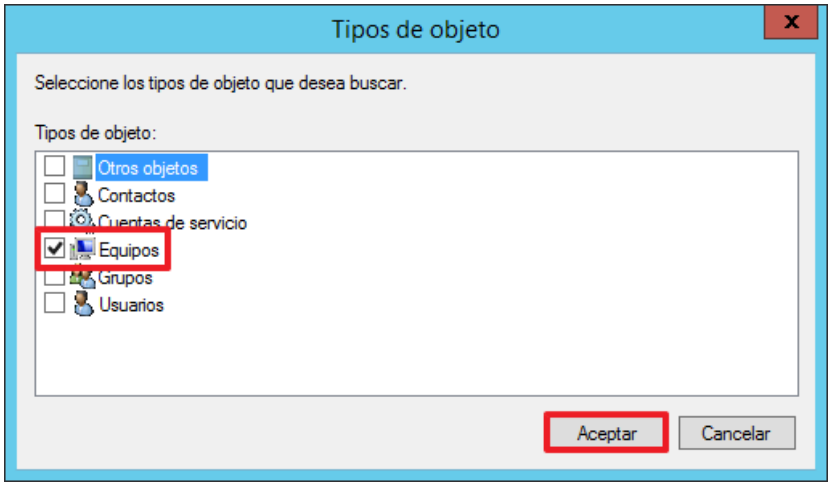
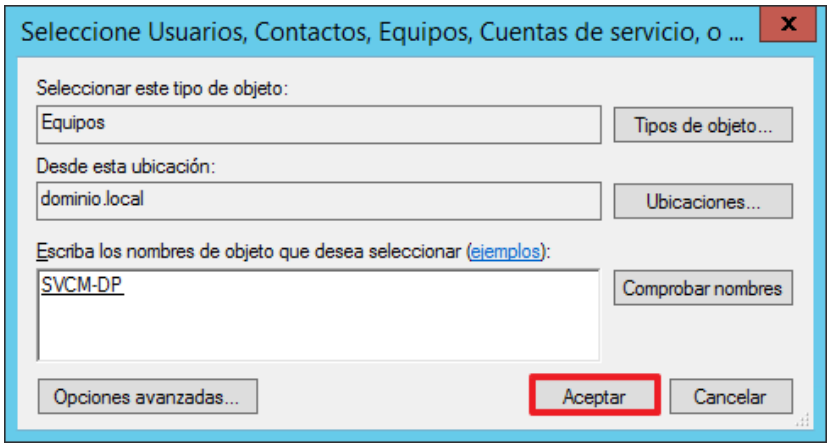
Paso	Descripción
142.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .
143.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 148. En caso contrario continúe con el paso a paso.
144.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 

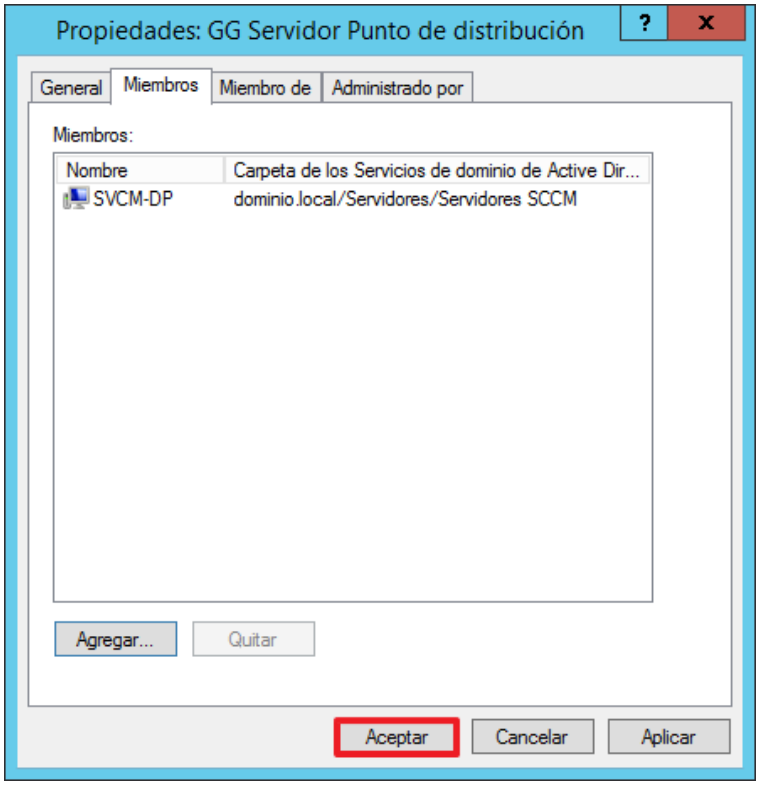
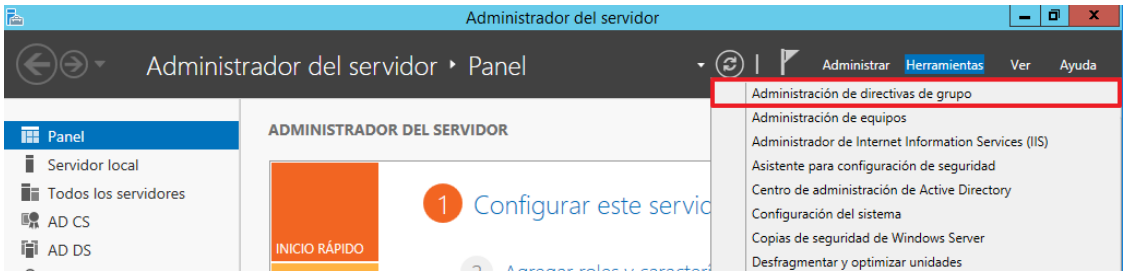
Paso	Descripción
145.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen. 
146.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.

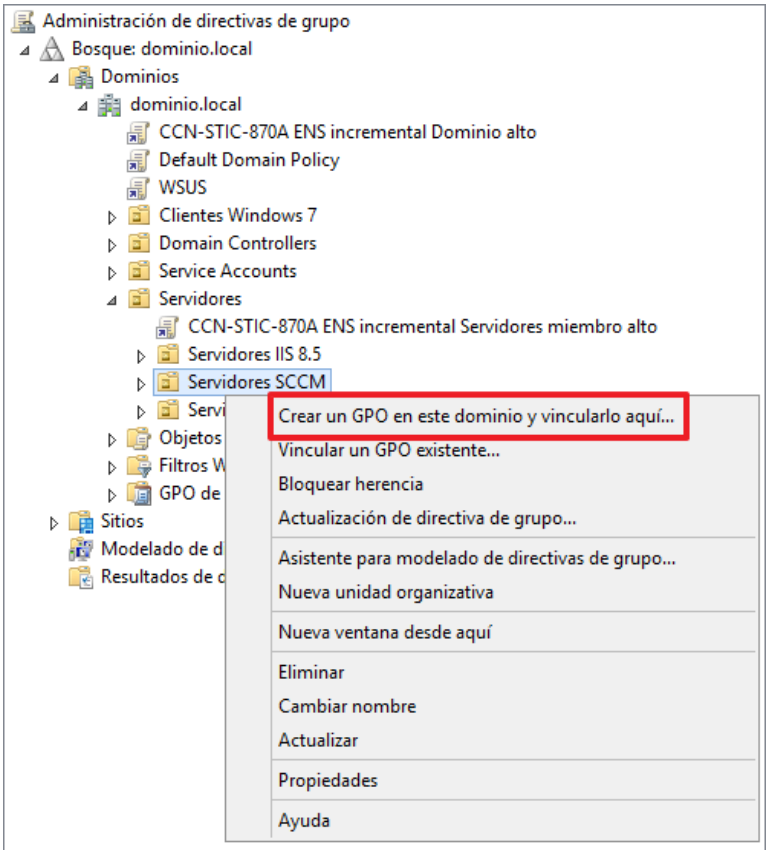
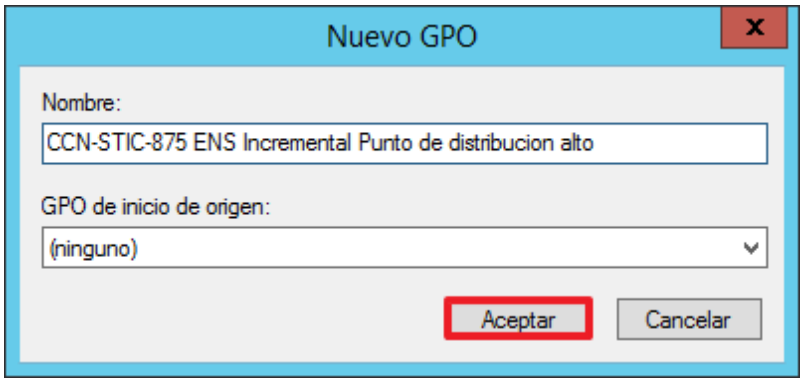
Paso	Descripción
147.	A continuación, seleccione la unidad organizativa “Servidores SCCM”. 
148.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 

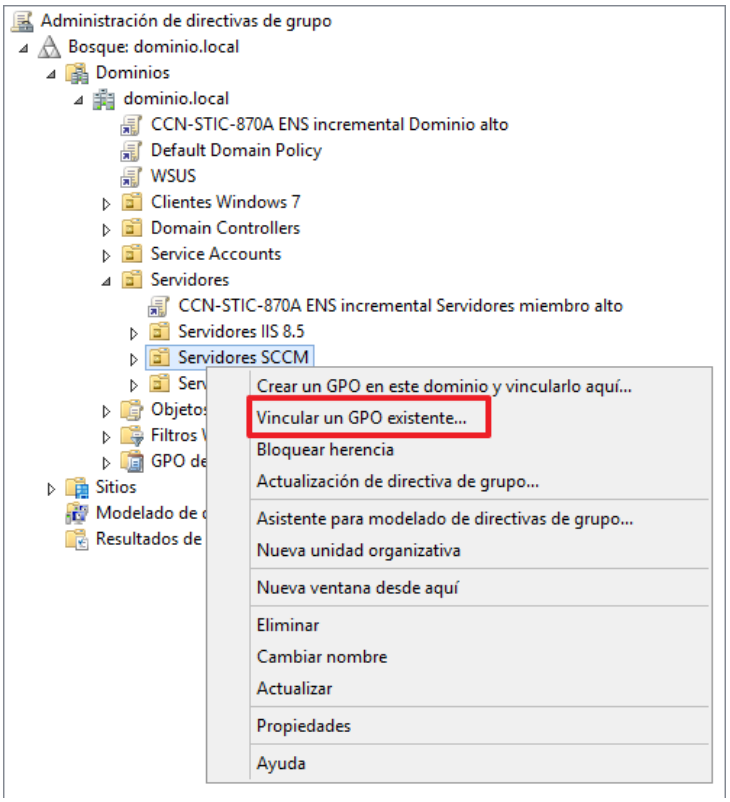
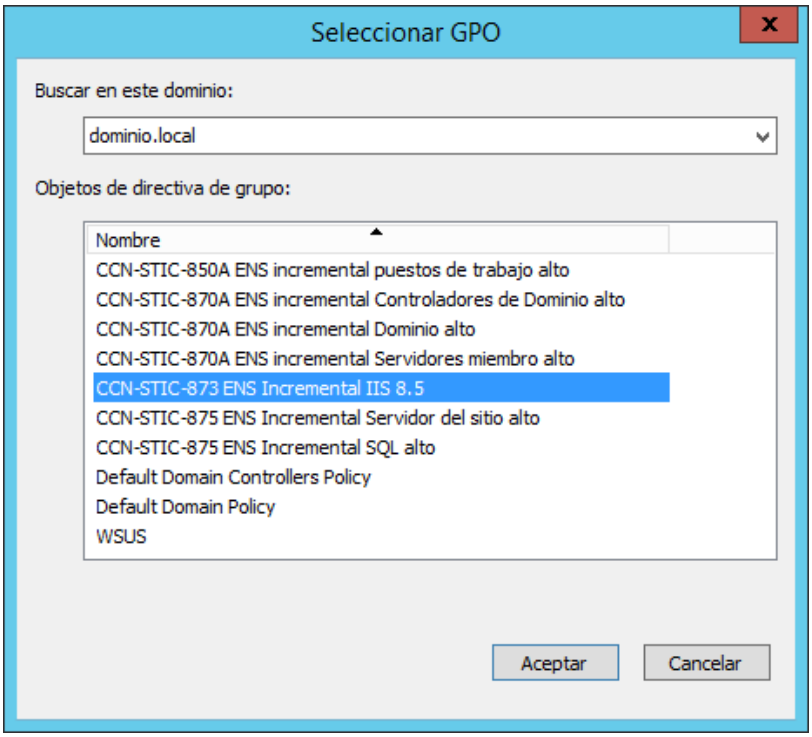
Paso	Descripción
149.	Escriba el nombre “GG Servidor Punto de distribución alto” y pulse “Aceptar”. 
150.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 

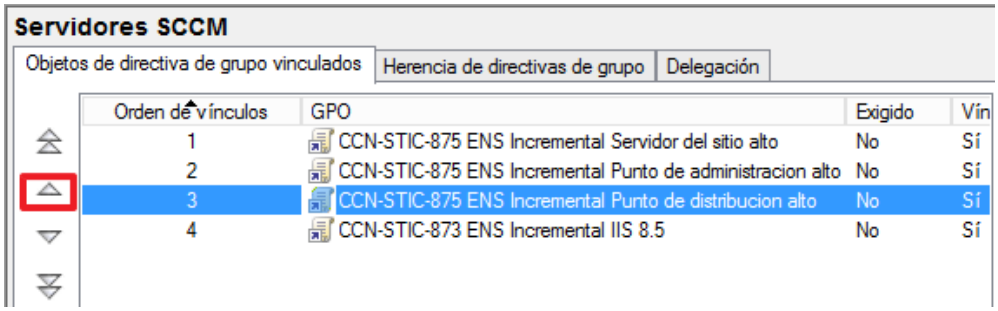
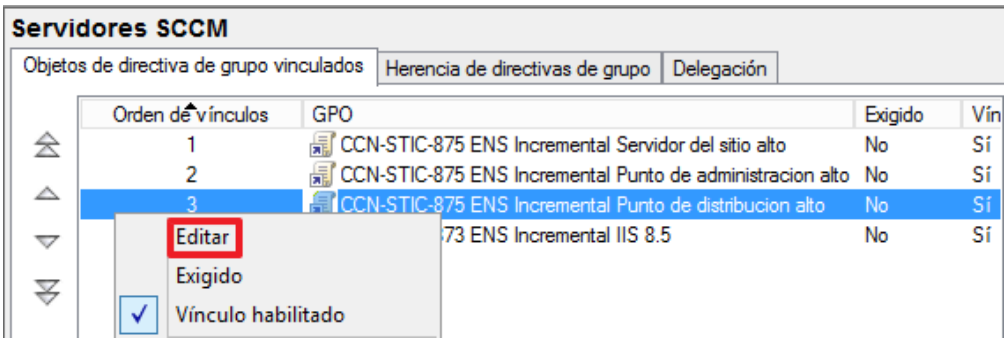
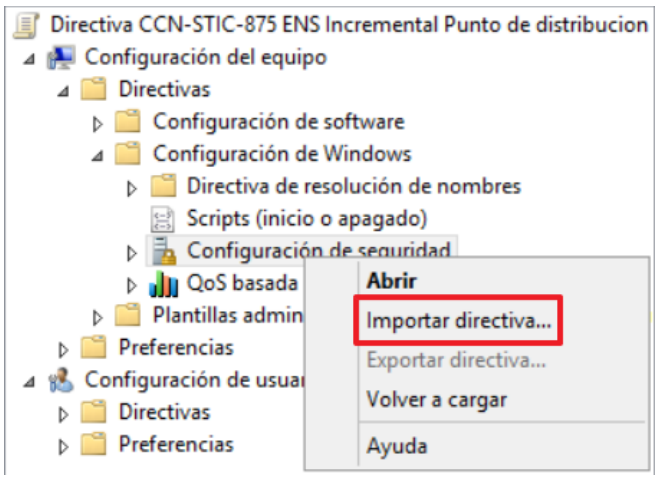
Paso	Descripción
151.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de distribución” al grupo. 
152.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 

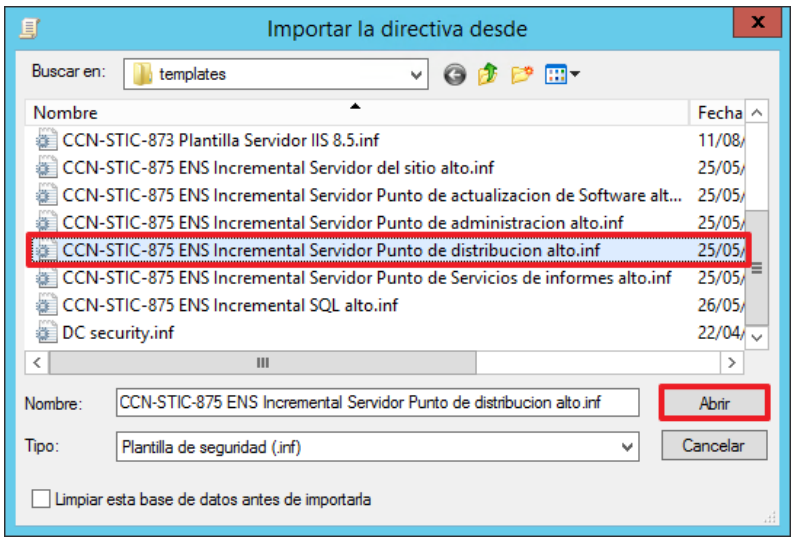
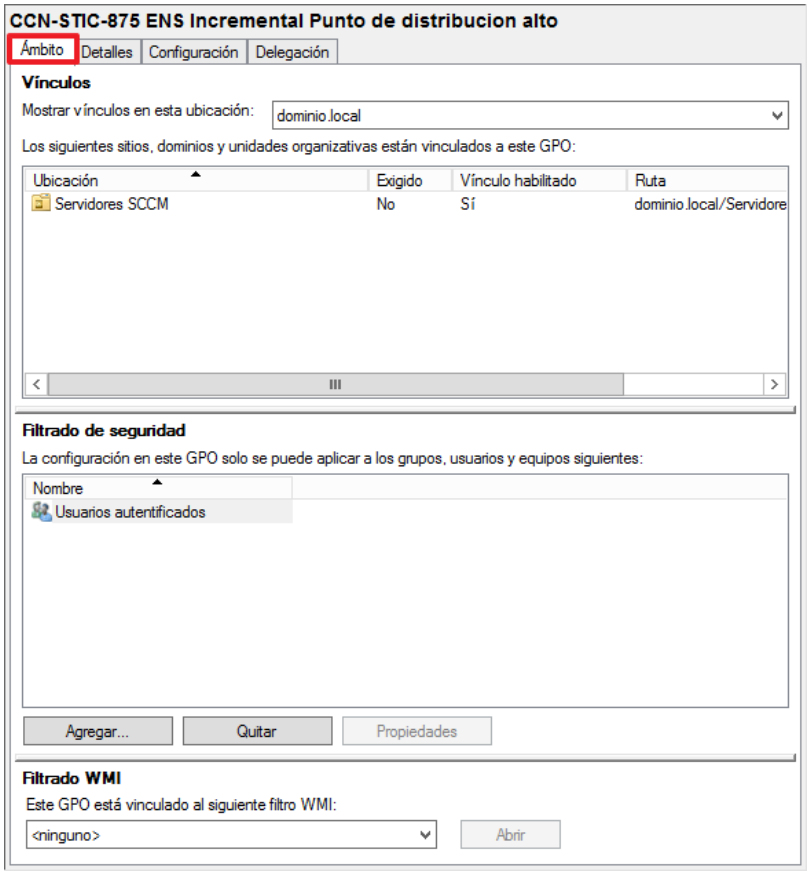
Paso	Descripción
153.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
154.	Agregue los equipos y pulse sobre “Aceptar”. 

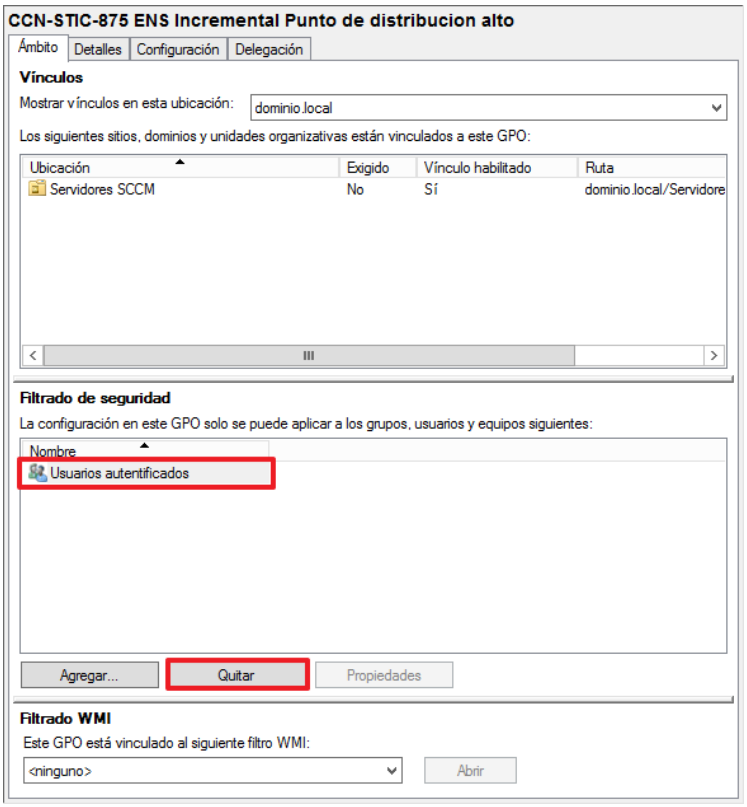
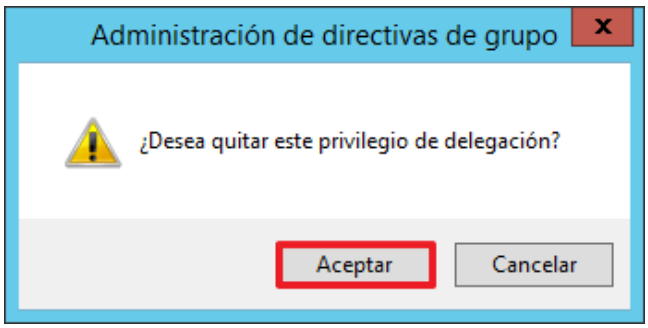
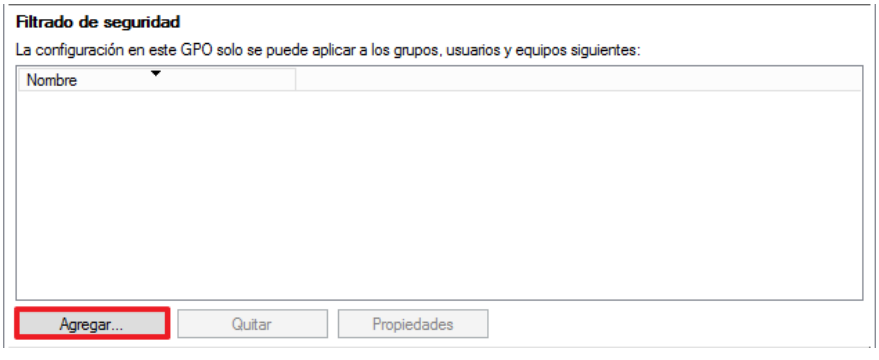
Paso	Descripción
155.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
156.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
157.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  .

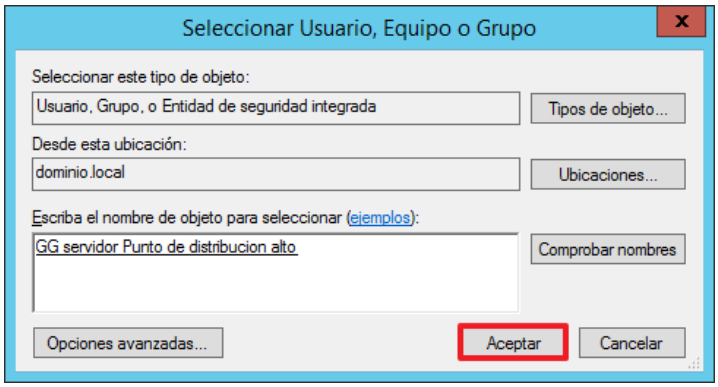
Paso	Descripción
158.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
159.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de distribución alto” y haga clic en el botón “Aceptar”. 
160.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”, En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 165, en caso contrario continúe con el paso a paso.
161.	A continuación, se va a asociar la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.

Paso	Descripción
162.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
163.	A continuación, seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
164.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de distribución alto" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de distribución alto" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
165.	Para modificar la GPO: "CCN-STIC-875 ENS Incremental Punto de distribución alto" creada anteriormente haga clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
166.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
167.	Importe la plantilla de seguridad "CCN-STIC-875 ENS Incremental Punto de distribución alto.inf" que previamente debe haberse copiado en la ruta "%SYSTEMROOT%\Security\Templates" y haga clic en botón "Abrir". 
168.	Cierre el "Editor de administración de directivas de grupo" una vez que se haya realizado la importación de la plantilla de seguridad.
169.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña "Ámbito" que se encuentra en el panel derecho. 

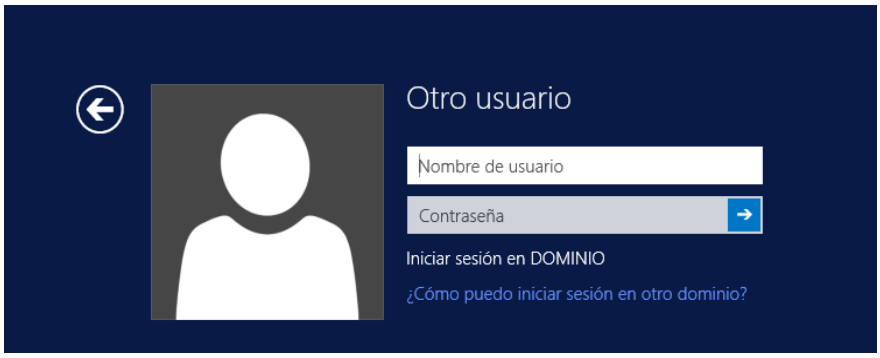
Paso	Descripción
170.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
171.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
172.	Una vez quitado, pulse el botón “Agregar…”. 

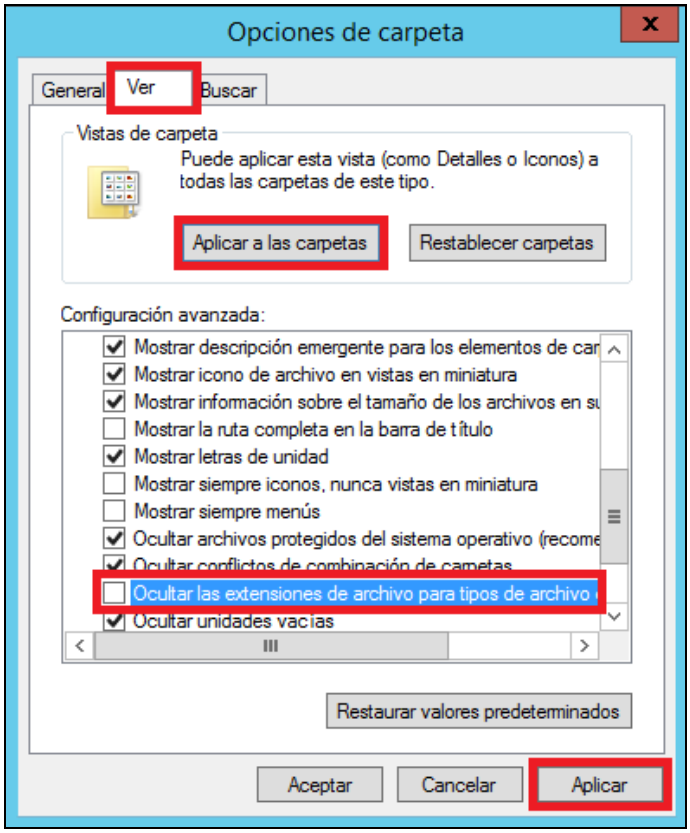
Paso	Descripción
173.	Introduzca como nombre “GG Servidor Punto de distribución alto”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.

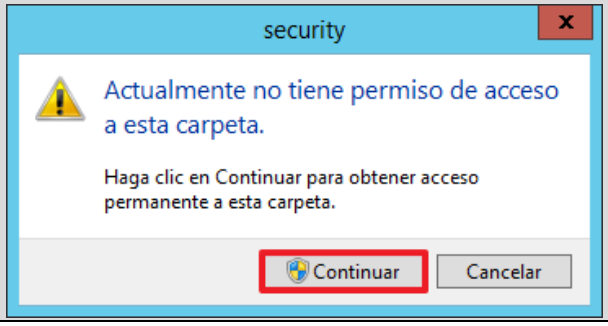
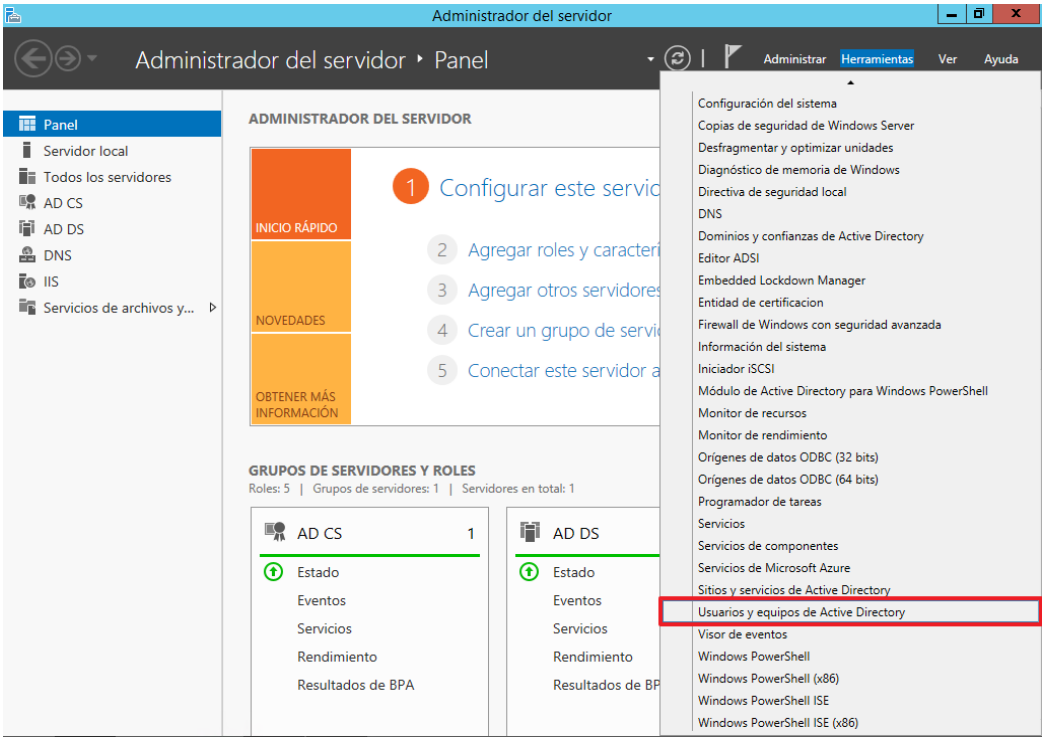
5. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE ACTUALIZACIÓN DE SOFTWARE

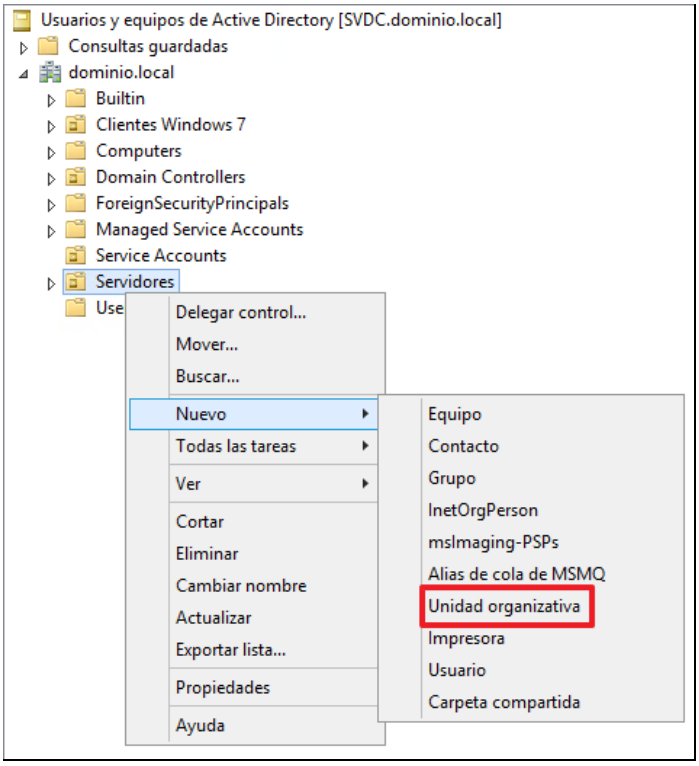
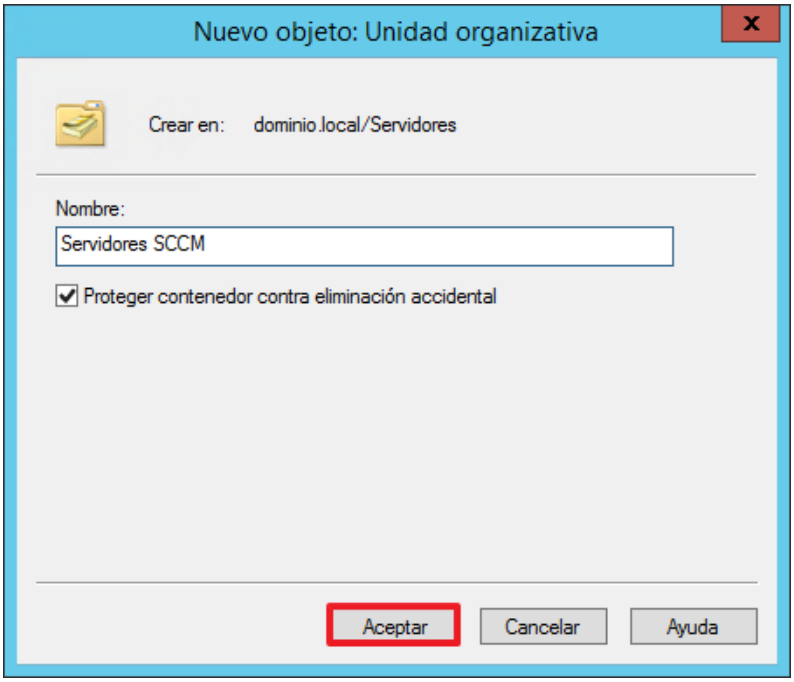
En el apartado siguiente, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de actualización de software implementado en el equipo.

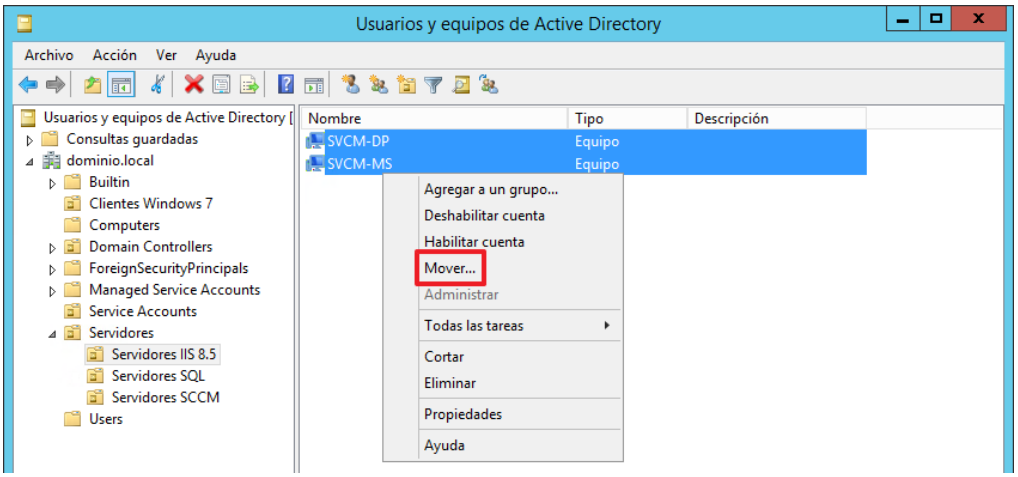
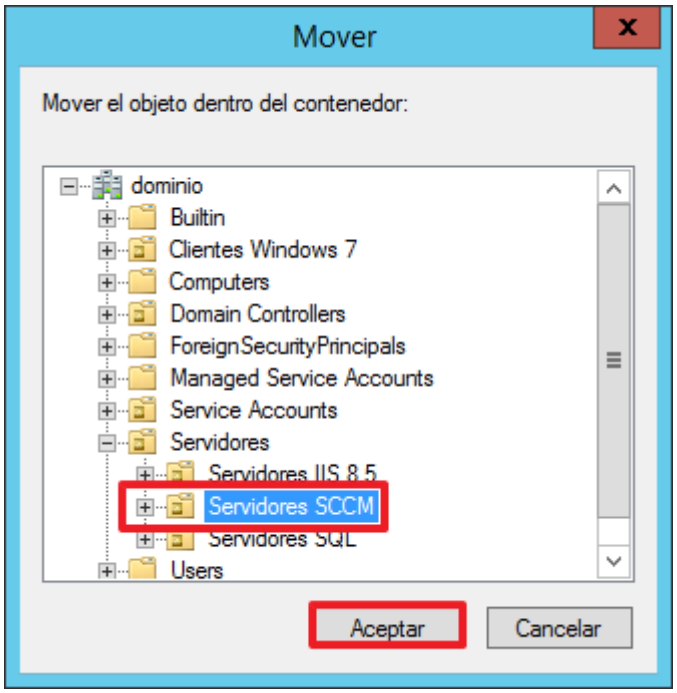
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2.

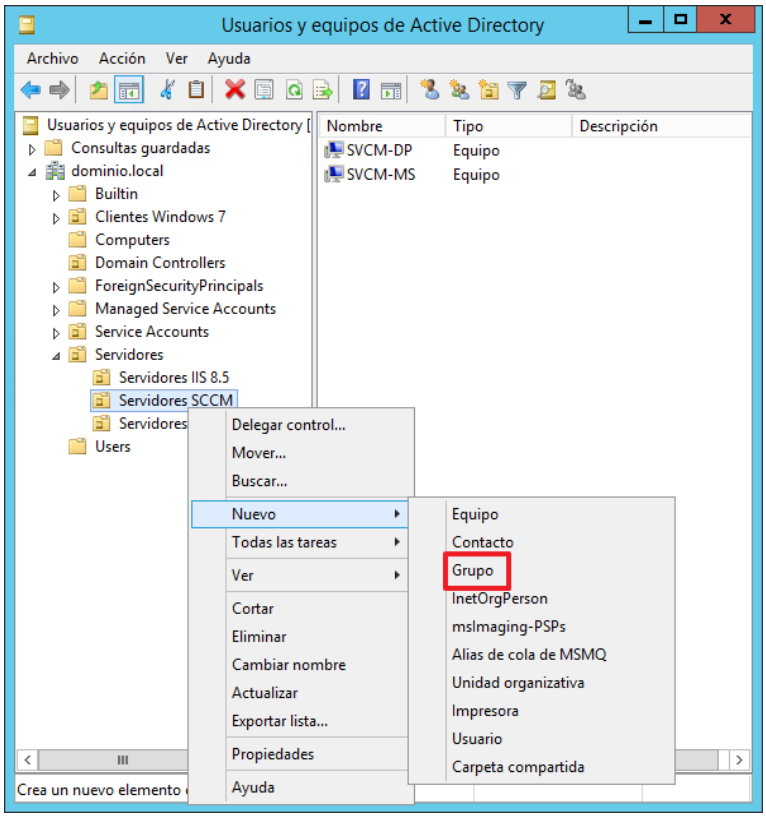
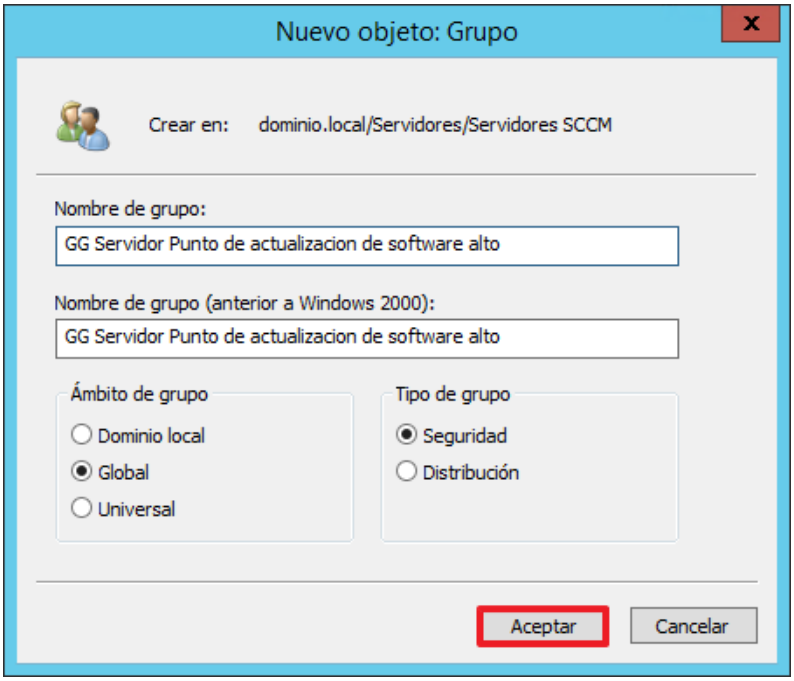
Paso	Descripción
174.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
175.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

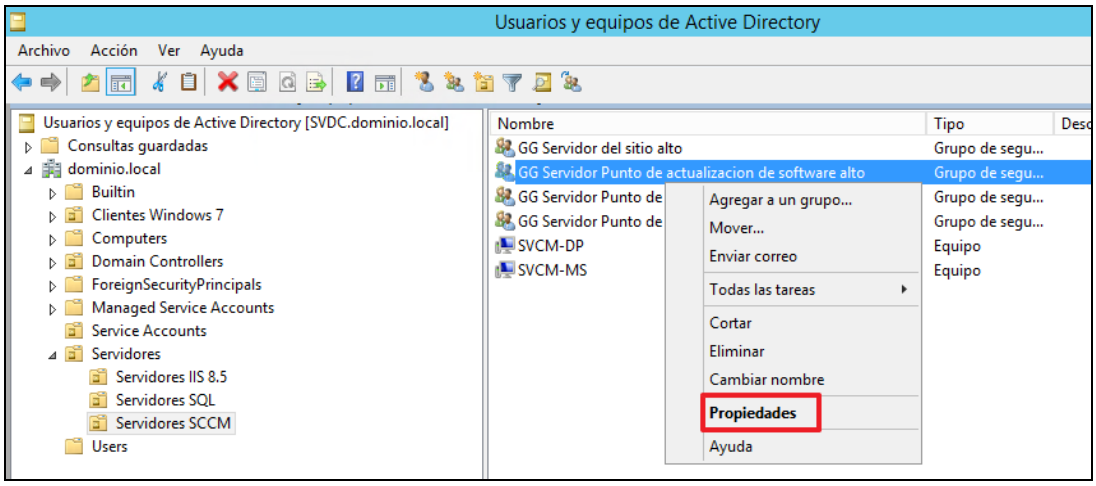
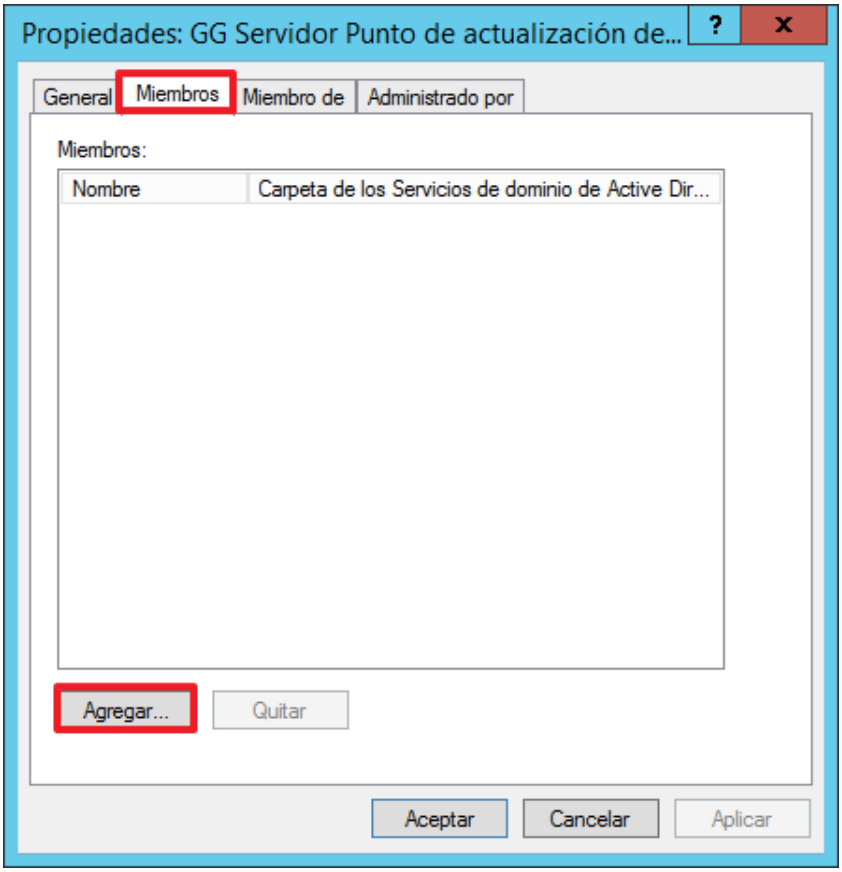
Paso	Descripción
176.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
177.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”. De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

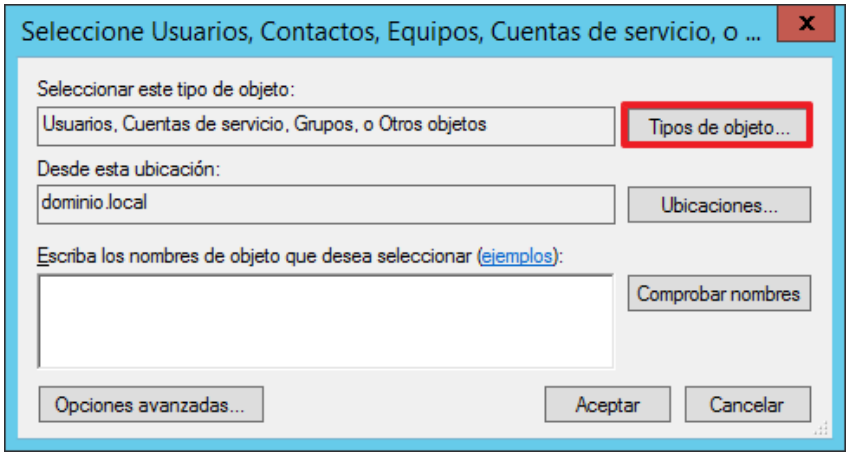
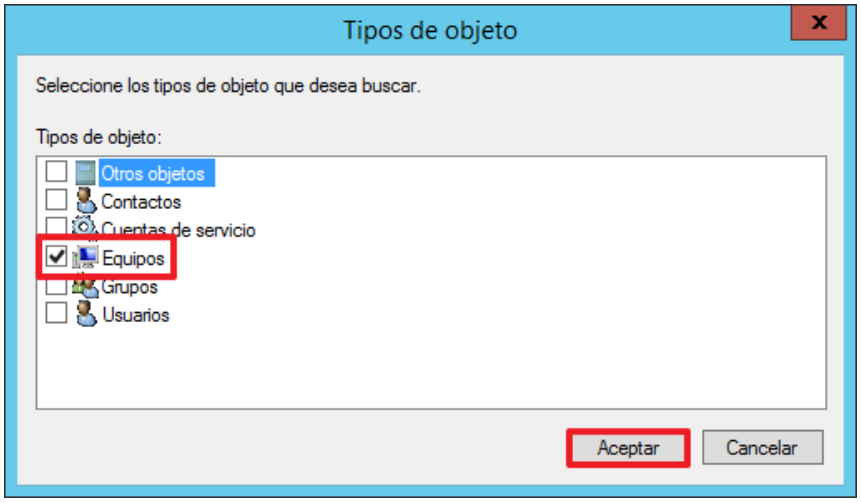
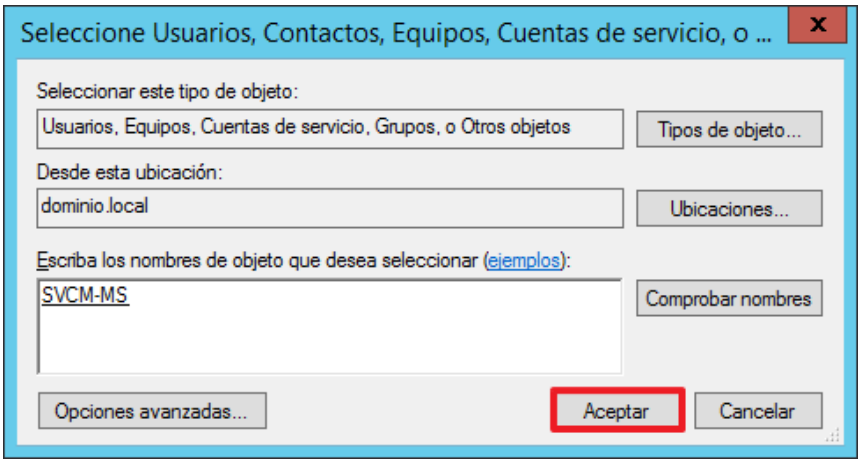
Paso	Descripción
178.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de actualización de software alto.inf” que se encuentra en la ruta “C:\Scripts\Nivel alto” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
179.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
180.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SCCM si ya ha realizado esta tarea, vaya directamente al paso 185. En caso contrario continúe con el paso a paso.

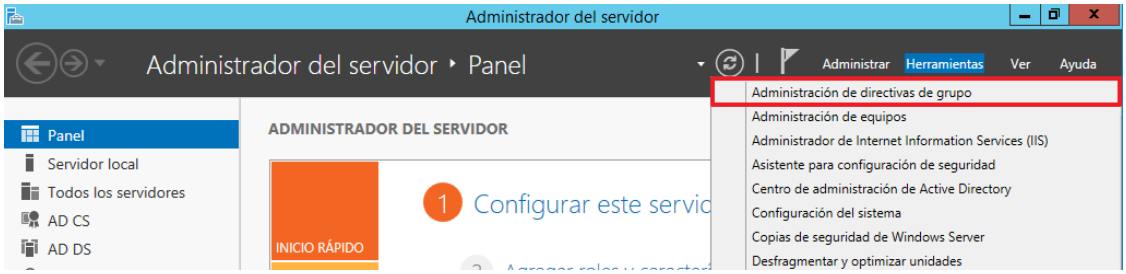
Paso	Descripción
181.	Para la creación de una nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
182.	En la consola, cree una unidad organizativa denominada “Servidores SCCM” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse “Aceptar”. 

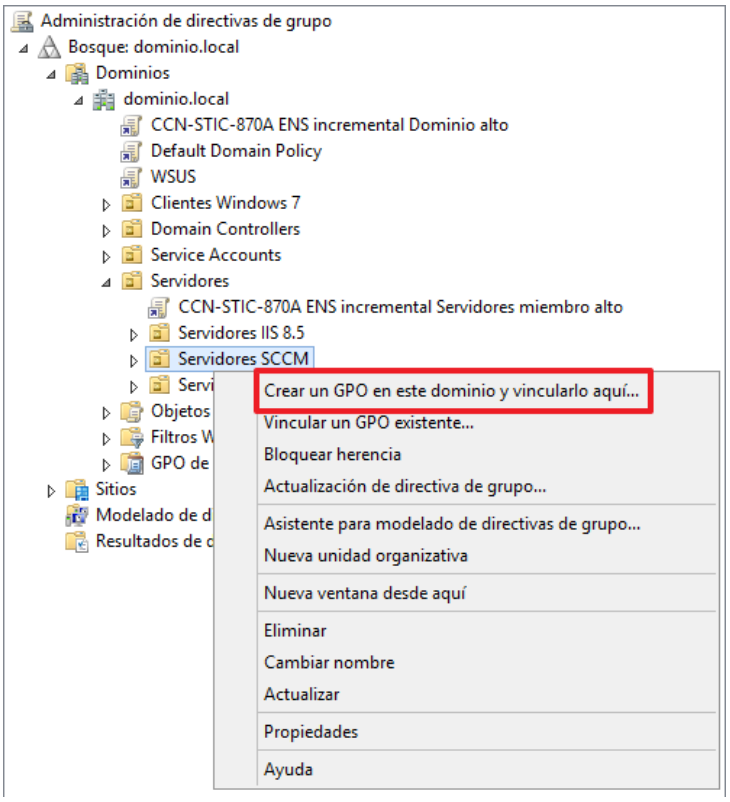
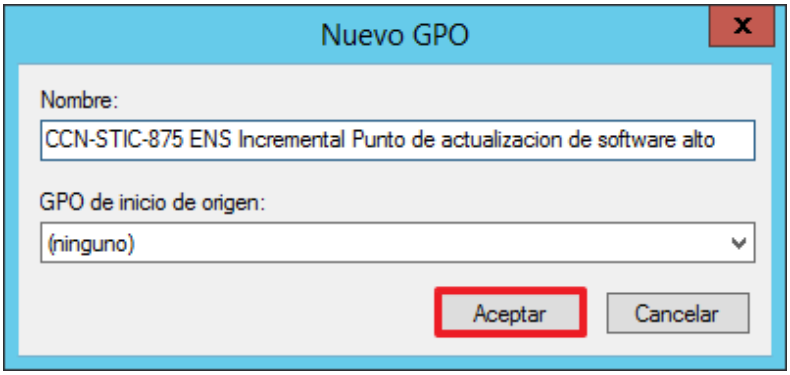
Paso	Descripción
183.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores que contengan SCCM a la unidad organizativa “Servidores SCCM”. Para ello, deberá hacer clic con el botón derecho sobre “Mover” en los servidores que desee ubicar en la nueva unidad organizativa.  **Nota:** Deberá localizar los servidores que desea reforzar la seguridad y adaptar estos pasos a su organización.
184.	Marque sobre la unidad organizativa “Servidores SCCM” y pulse “Aceptar”. 

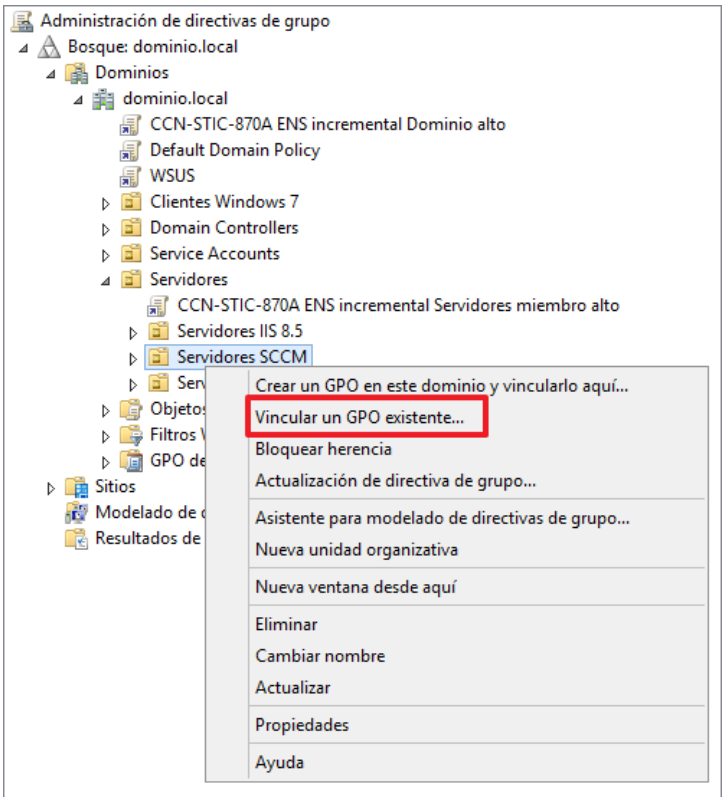
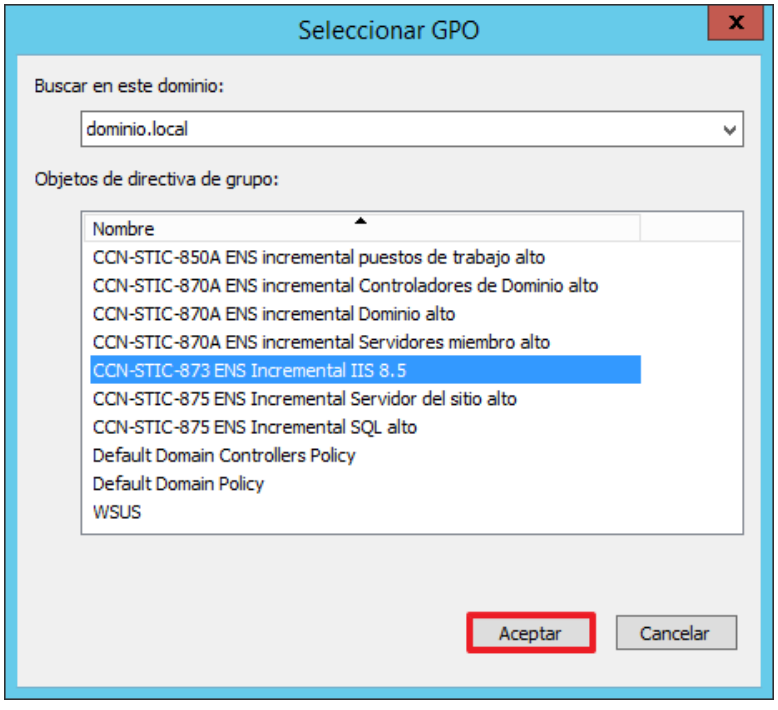
Paso	Descripción
185.	Seleccione la unidad organizativa “Servidores SCCM”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
186.	Escriba el nombre “GG Servidor Punto de actualización de software alto” y pulse “Aceptar”. 

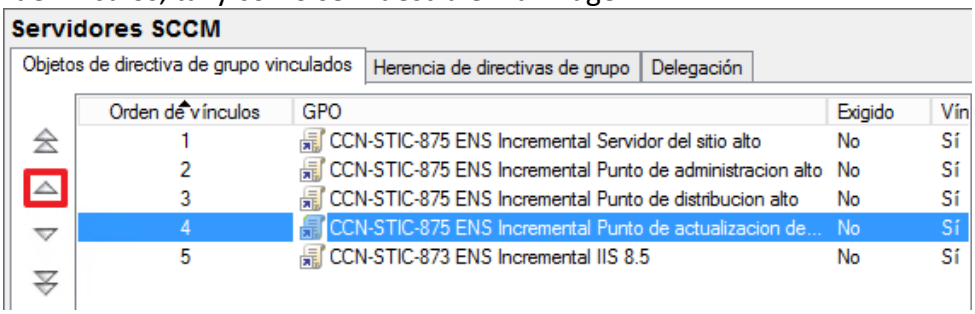
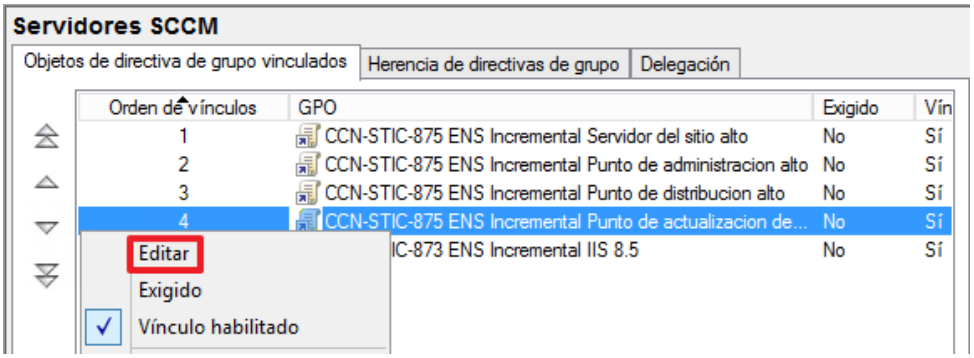
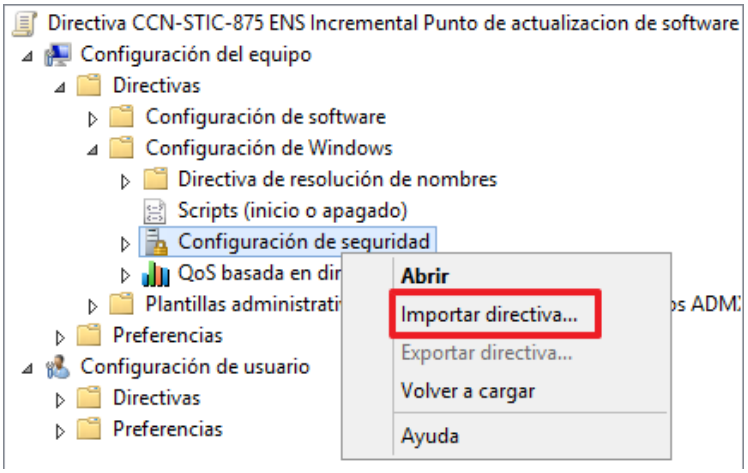
Paso	Descripción
187.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
188.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de actualización de software” al grupo. 

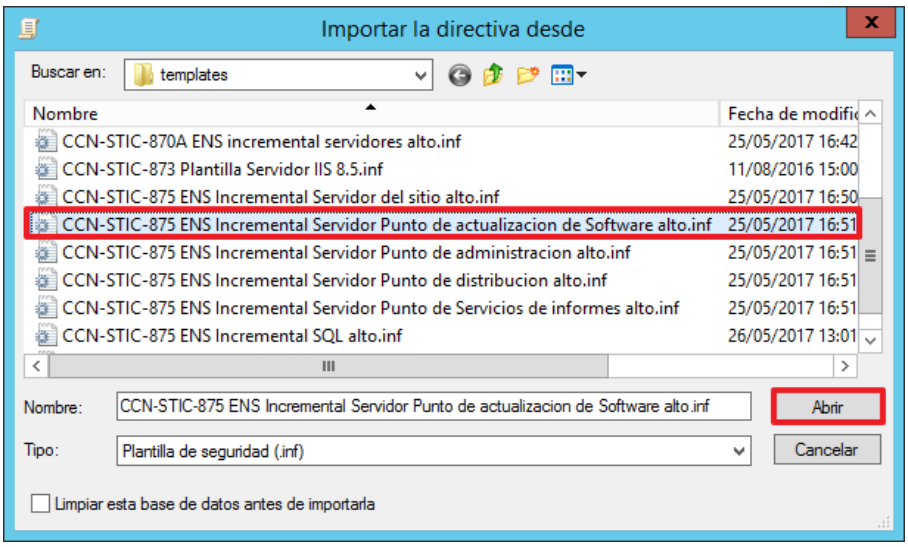
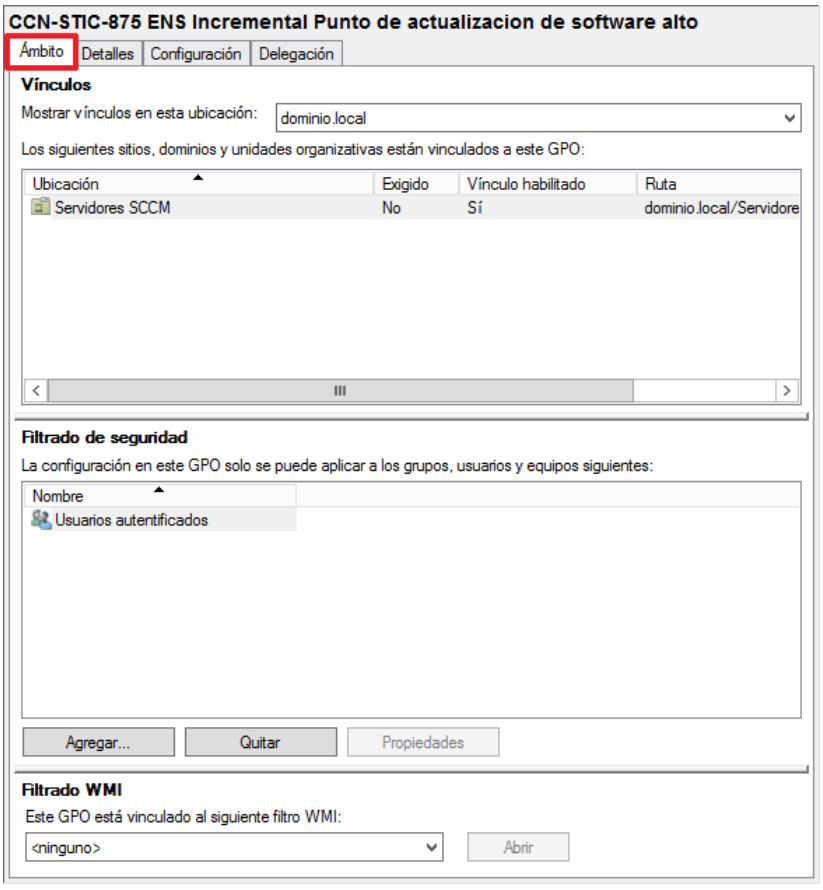
Paso	Descripción
189.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
190.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
191.	Agregue los equipos y pulse sobre “Aceptar”. 

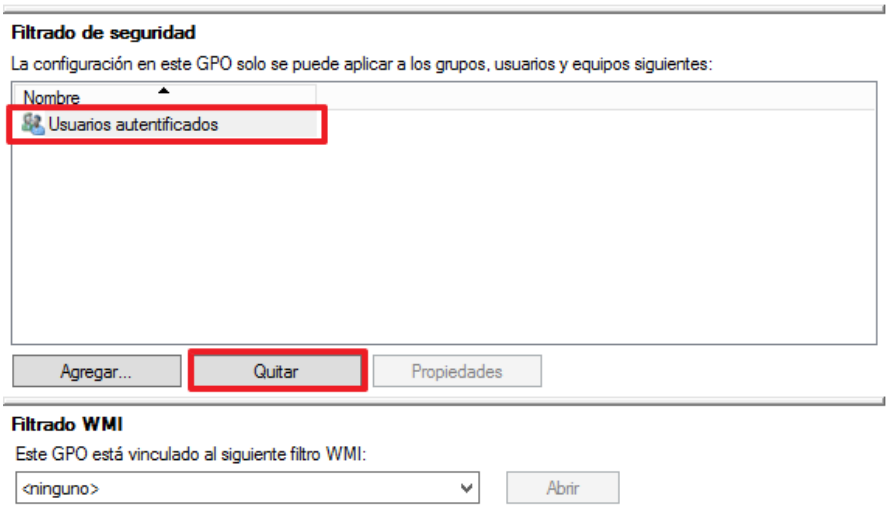
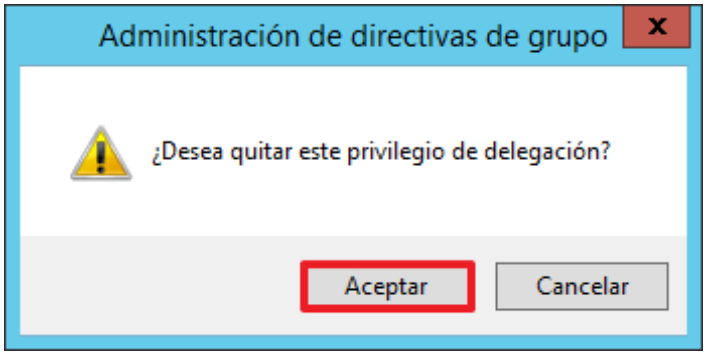
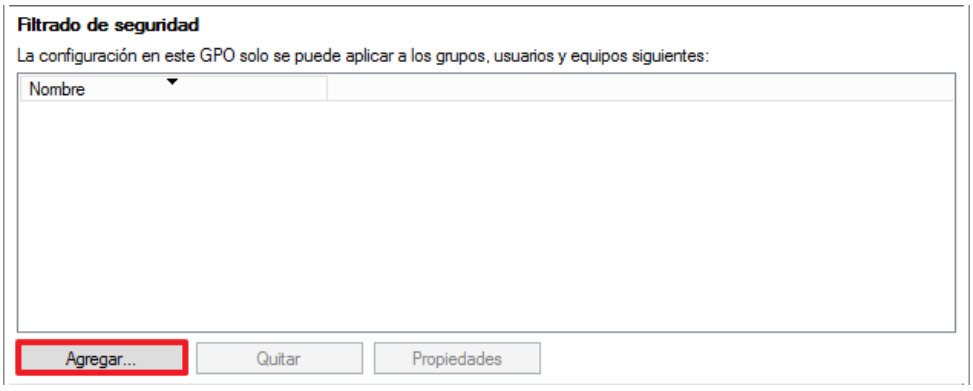
Paso	Descripción
192.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
193.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
194.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

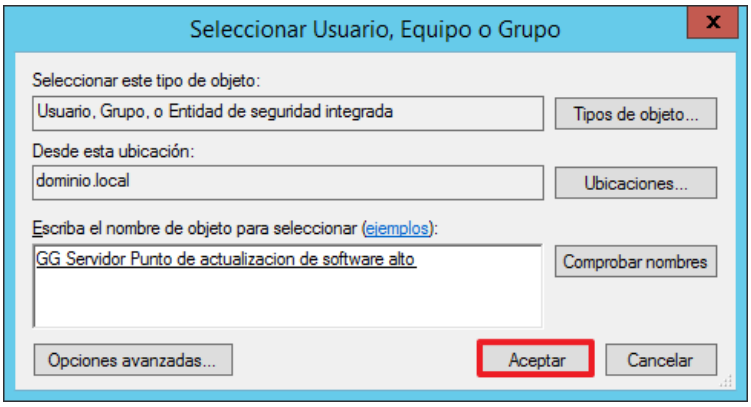
Paso	Descripción
195.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SCCM”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”. 
196.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de actualización de software alto” y haga clic en el botón “Aceptar”. 
197.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”, En el caso de que ya haya realizado este proceso anteriormente, prosiga con el paso 202, en caso contrario continúe con el paso a paso.
198.	A continuación, se asociará la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SCCM”.

Paso	Descripción
199.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SCCM” y haga clic sobre “Vincular un GPO existente…” 
200.	Seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre “Aceptar”. 

Paso	Descripción
201.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de actualización de software alto" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SCCM", la directiva "CCN-STIC-875 ENS Incremental Punto de actualización de software alto" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
202.	Para editar la GPO: "CCN-STIC-875 ENS Incremental Punto de actualización de software alto" creada anteriormente, haga clic con el botón derecho y seleccione la opción "Editar" del menú contextual. 
203.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
204.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Punto de actualización de software alto.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
205.	Cierre el “Editor de administración de directivas de grupo” una vez que se haya realizado la importación de la plantilla de seguridad.
206.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

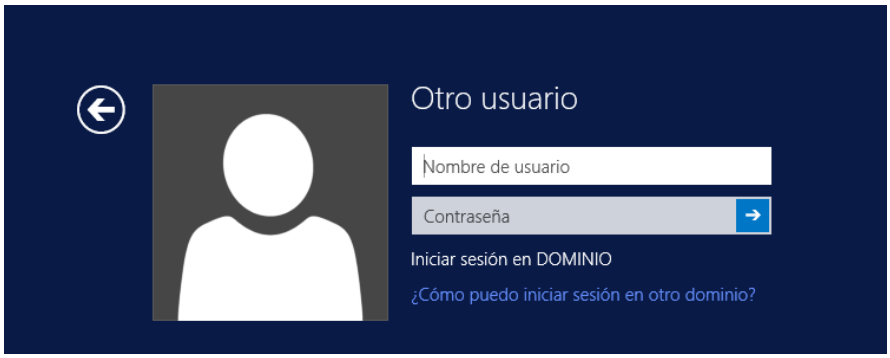
Paso	Descripción
207.	En la opción de filtrado de seguridad, seleccione “Usuarios autentificados” y pulse la opción “Quitar”. 
208.	Pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación. 
209.	Una vez quitado, pulse el botón “Agregar…”. 

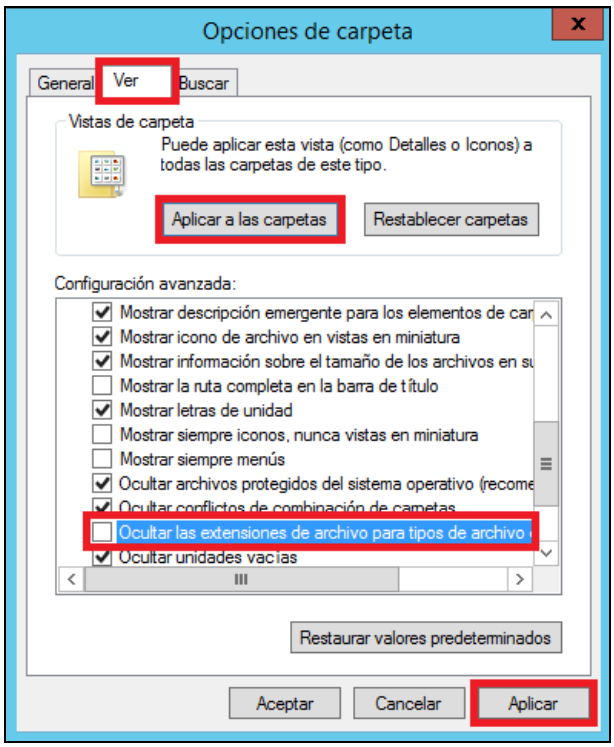
Paso	Descripción
210.	Introduzca como nombre “GG Servidor Punto de actualización de software alto”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
211.	Cierre el “Editor de administración de directivas de grupo”.

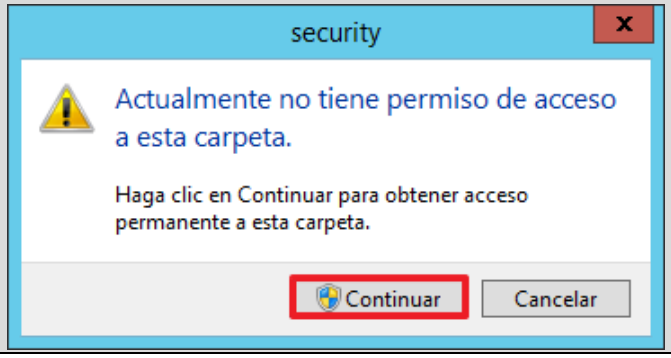
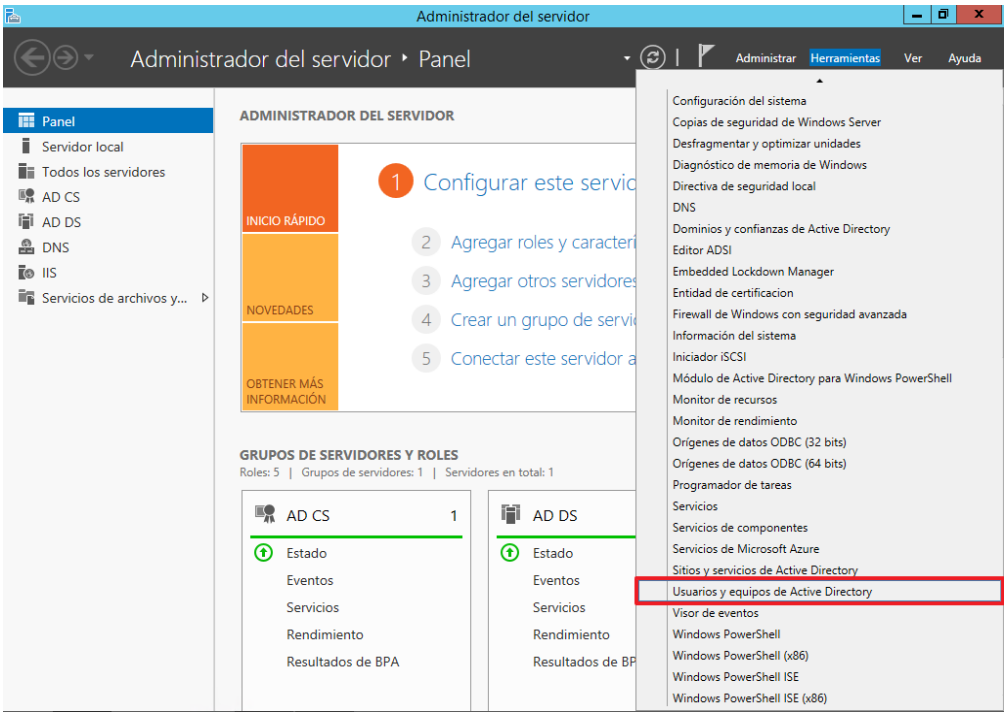
6. REFUERZO DE SEGURIDAD DEL ROL DE PUNTO DE SERVICIOS DE INFORME

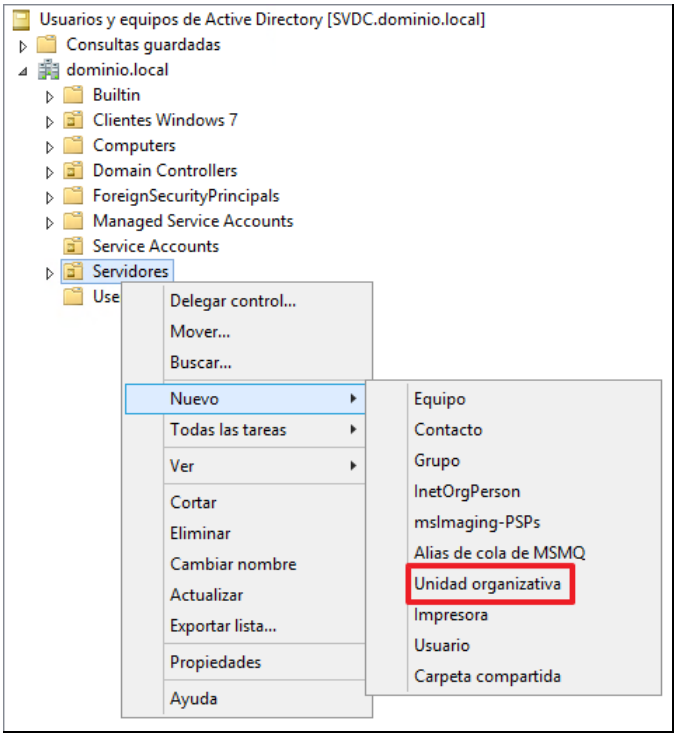
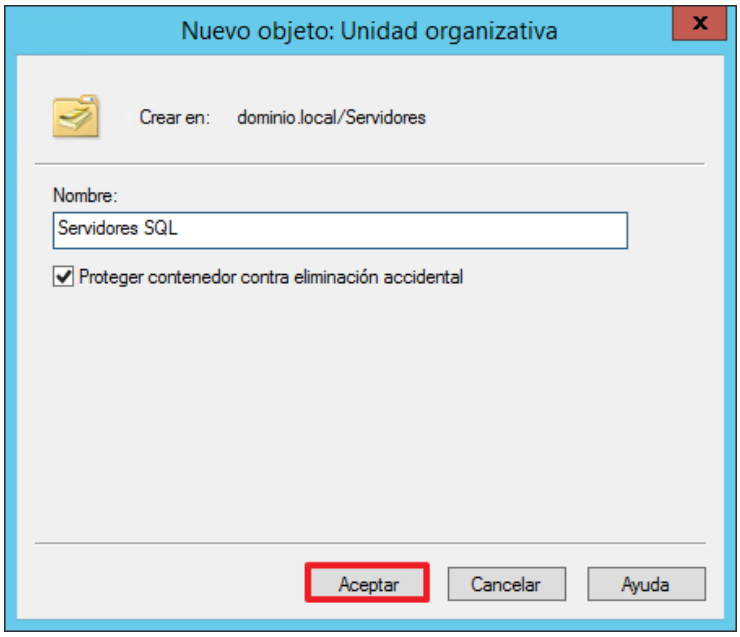
A continuación, se describen los pasos para reforzar la seguridad de los servidores que disponen del rol de punto de servicios de informes implementado en el equipo.

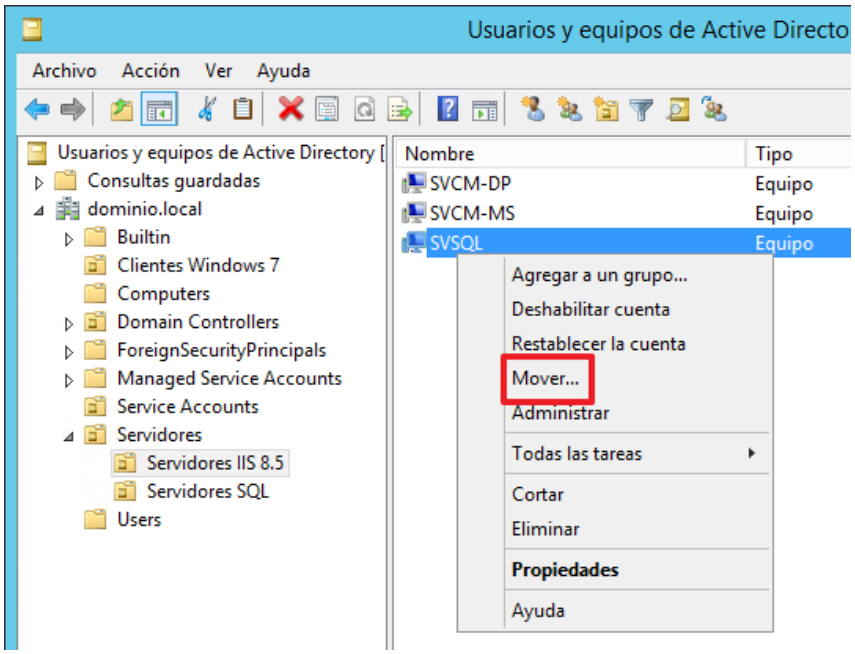
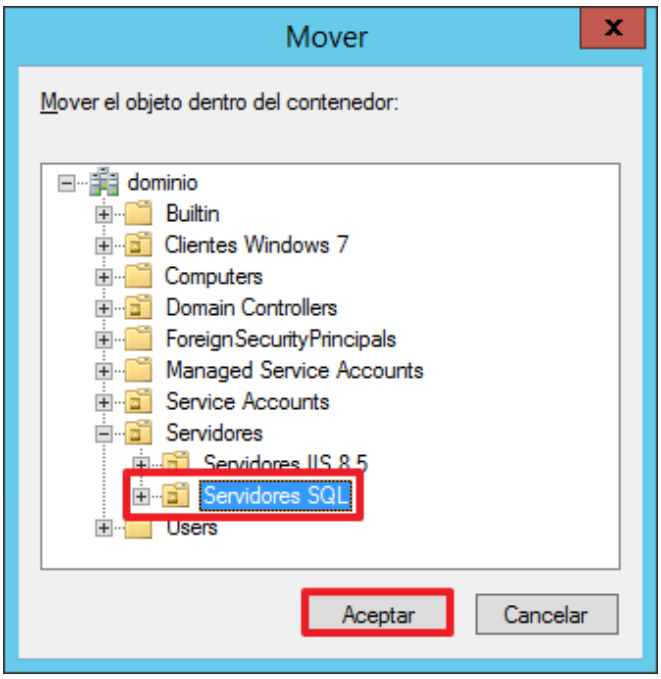
El proceso de refuerzo de seguridad se realizará en el controlador de dominio del domino al que pertenece el servidor miembro que forma parte de la implementación de MS SCCM 2012 R2

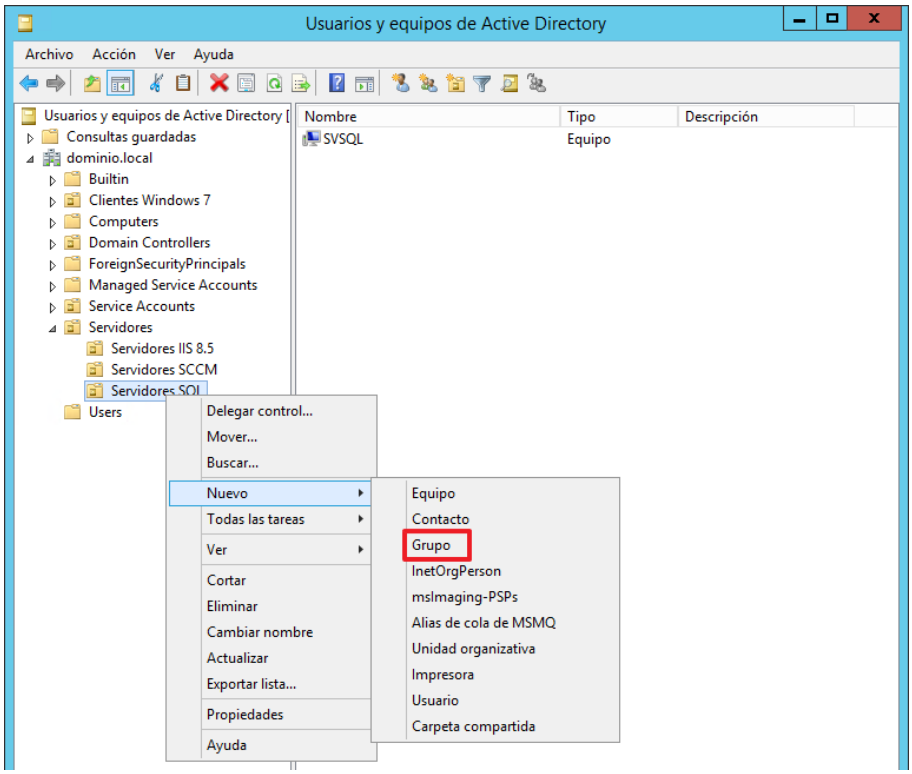
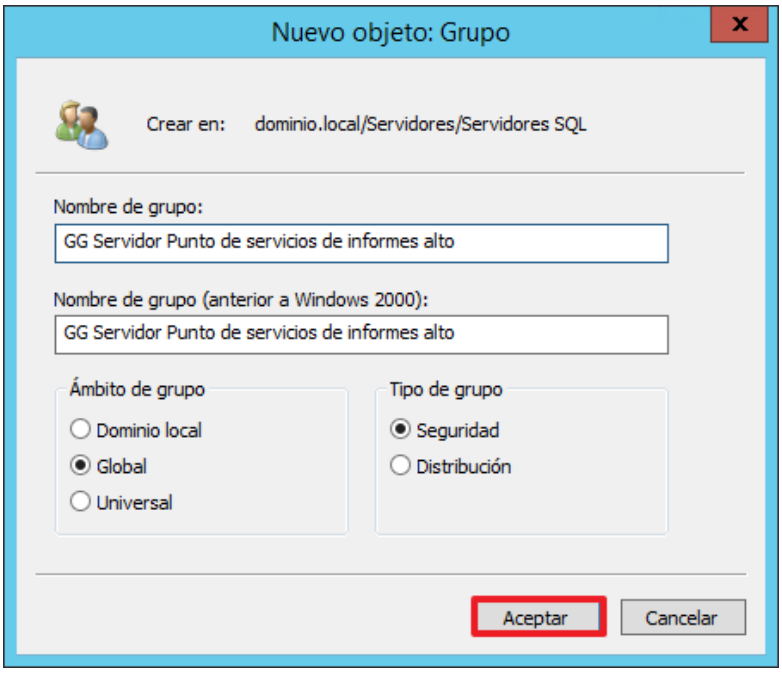
Paso	Descripción
212.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.  **Nota:** Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
213.	Cree el directorio “Scripts” en la unidad “C:\”. **Nota:** Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendría que editar los scripts para reflejar la nueva ubicación.

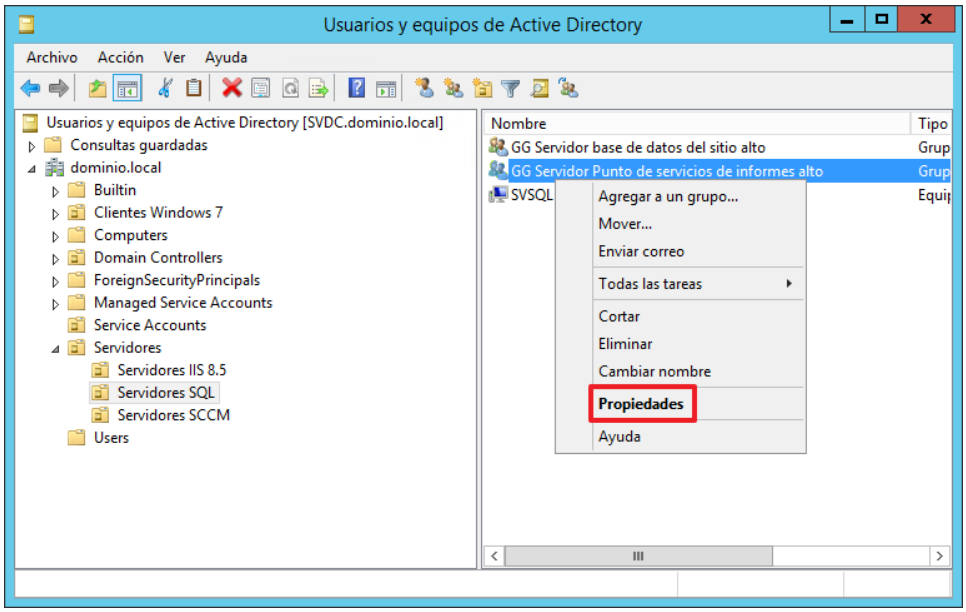
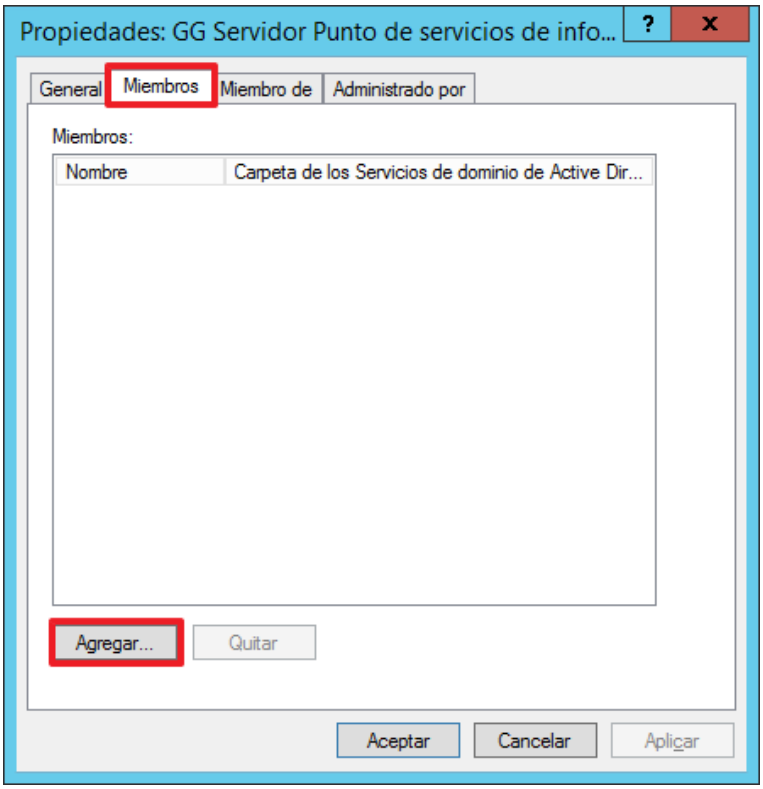
Paso	Descripción
214.	Copie los archivos asociados a esta guía en el directorio “C:\Scripts”.
215.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos. Para configurar el “Explorador de Windows” para mostrar las extensiones de todos los archivos, abra una ventana de “Explorador de Windows”, seleccione en el menú superior, “Vista” y dentro de dicho menú, "Opciones”.
216.	De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura.  Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación que aparecerá (¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?), y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

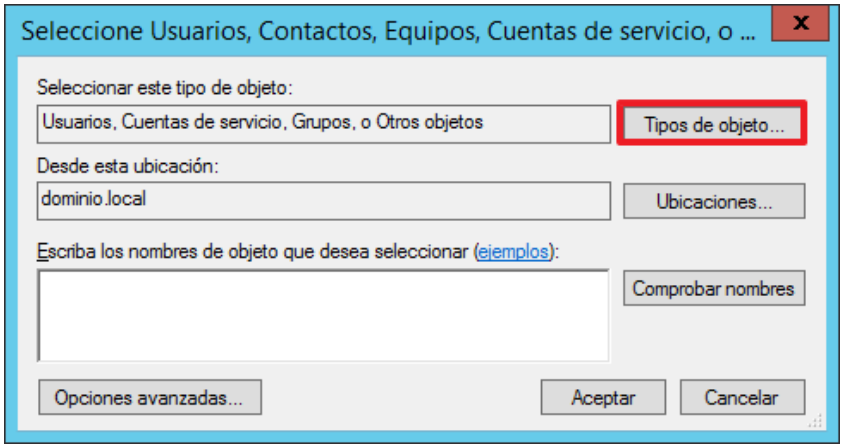
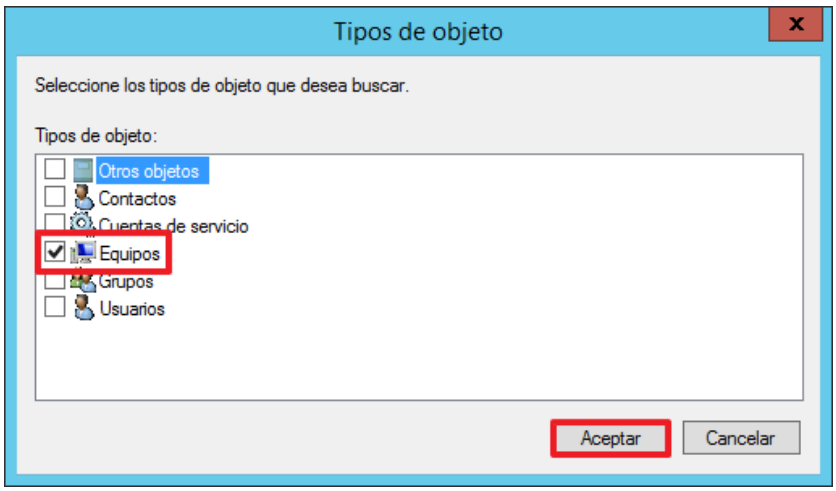
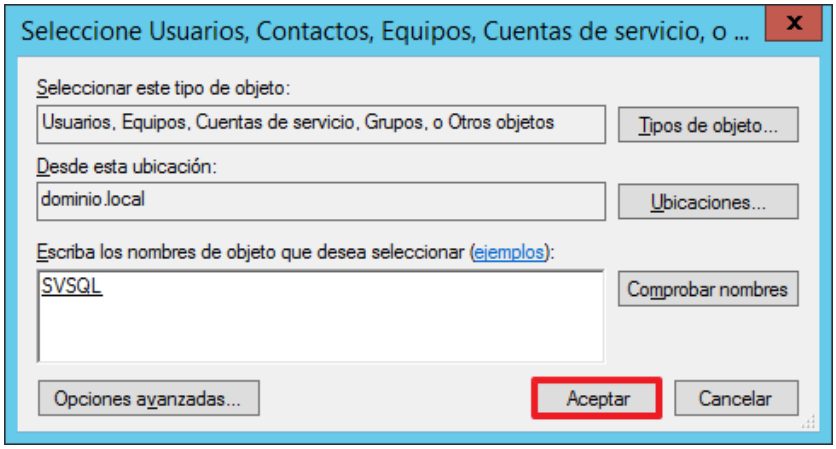
Paso	Descripción
217.	Copie el fichero “CCN-STIC-875 ENS Incremental Punto de servicios de informes alto.inf” que se encuentra en la ruta “C:\Scripts\Nivel alto” al directorio de destino “%SYSTEMROOT%\Security\Templates” del Controlador de Dominio. **Nota:** Para copiar ficheros en carpetas protegidas por el sistema, el sistema le solicitará una elevación de privilegios. Haga clic en el botón “Continuar” e introduzca las credenciales de la cuenta con que ha iniciado sesión, la cual debe ser al menos administrador de dominio. 
218.	Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Usuarios y equipos de Active Directory”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .
219.	En los siguientes pasos, se va a crear la unidad organizativa que aloje los servidores de SQL si ya ha realizado esta tarea, vaya directamente al paso 224.En caso contrario continúe con el paso a paso.

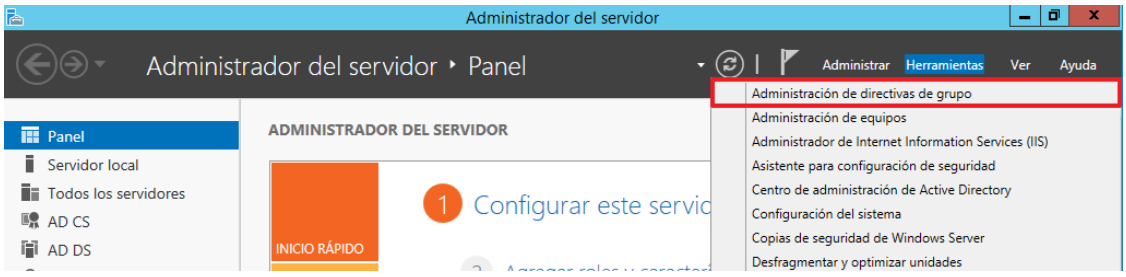
Paso	Descripción
220.	Para la creación de la nueva unidad organizativa utilizando el menú contextual, pulse con el botón derecho sobre la unidad organizativa “Servidores” y despliegue “Nuevo” > “Unidad organizativa”. 
221.	En la consola, cree una unidad organizativa denominada “Servidores SQL” dependiendo de la unidad organizativa “Servidores”, tal y como se muestra en la imagen y pulse en “Aceptar”. 

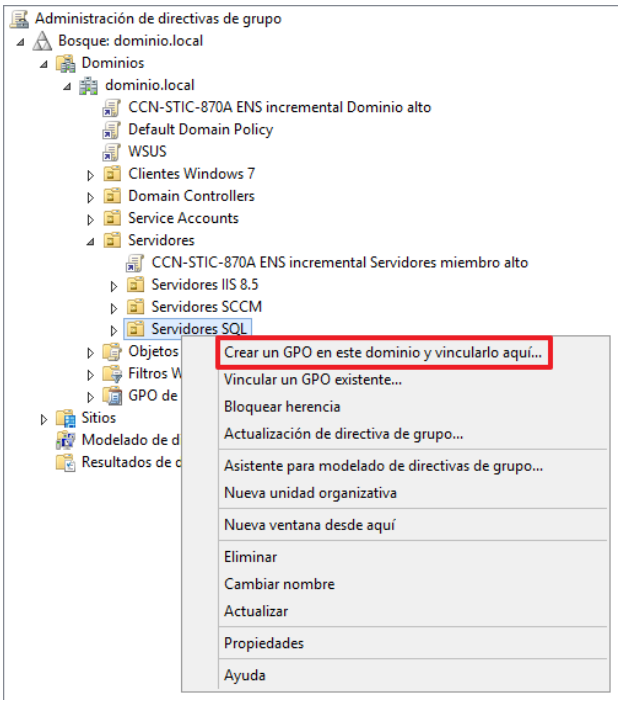
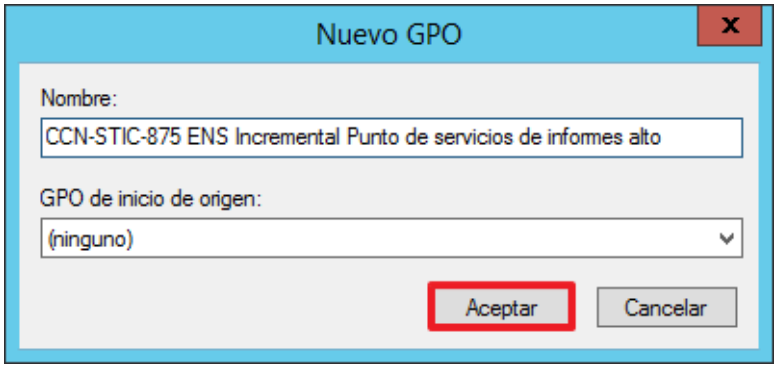
Paso	Descripción
222.	Una vez creada la nueva Unidad organizativa, deberá mover los servidores SQL a la unidad organizativa "Servidores SQL". Para ello, deberá localizar los servidores y hacer clic con el botón derecho sobre "mover" en el servidor que desee ubicar en la nueva unidad organizativa. 
223.	Seleccione la unidad organizativa "Servidores SQL" y pulse "Aceptar". 

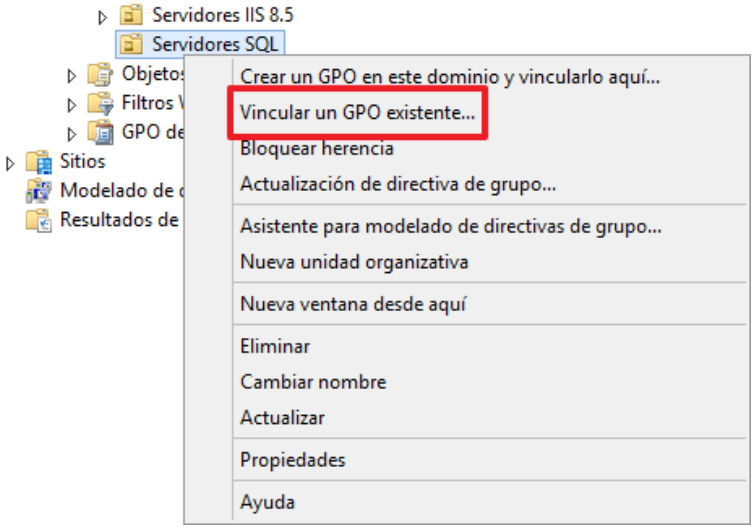
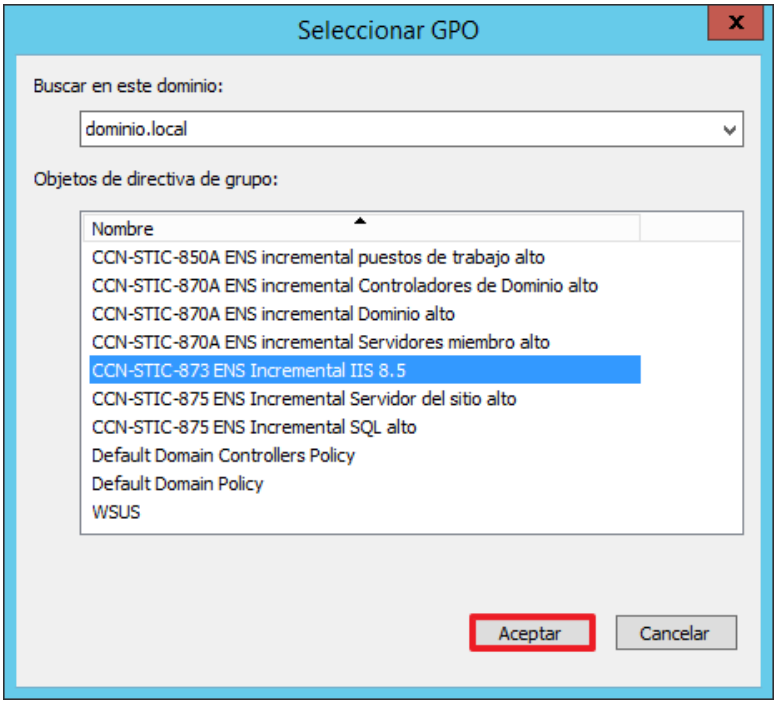
Paso	Descripción
224.	En el siguiente paso, seleccione la unidad organizativa “Servidores SQL”, pulse con el botón derecho y seleccione la opción “Nuevo > Grupo” del menú contextual. 
225.	Escriba el nombre “GG Servidor Punto de servicios de informes alto” y pulse “Aceptar”. 

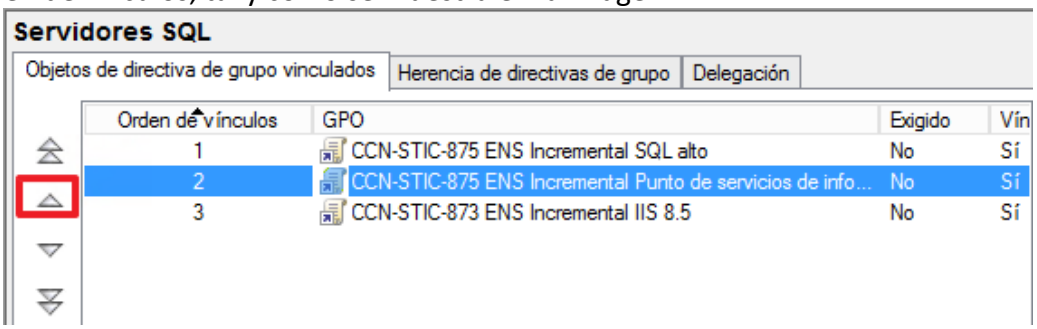
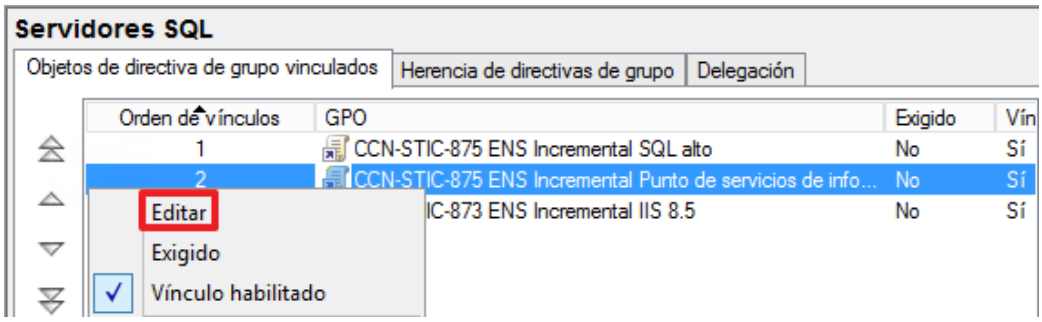
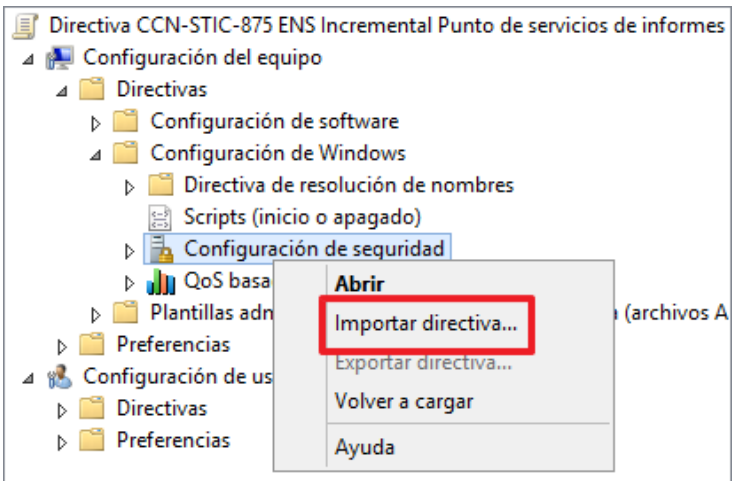
Paso	Descripción
226.	Pulse con el botón derecho sobre el grupo recién creado, y seleccione la opción “Propiedades” del menú contextual. 
227.	Seleccione la pestaña “Miembros” y pulse “Agregar” para añadir los equipos que contengan el rol de “Punto de Servicios de informes” al grupo. 

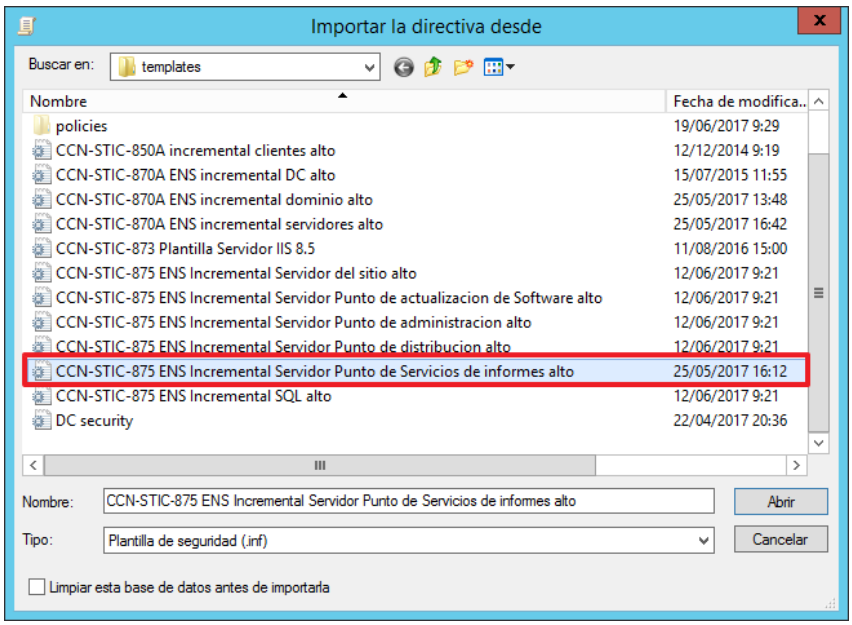
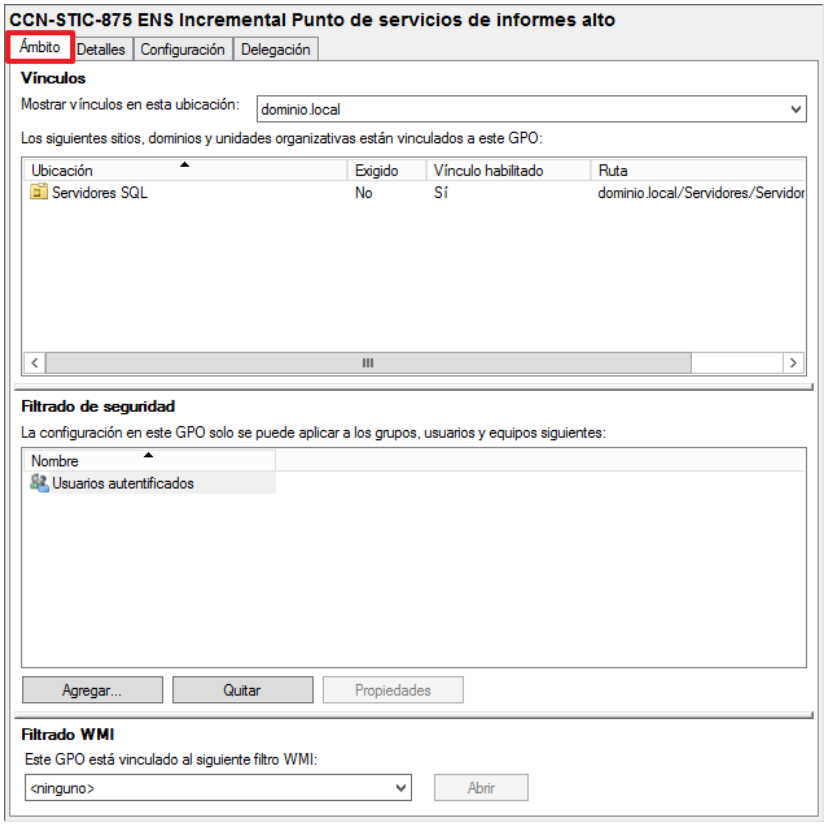
Paso	Descripción
228.	Pulse sobre “Tipos de objeto…” para modificar el tipo de objeto que va a seleccionar. 
229.	Deje marcado únicamente el tipo de objeto “Equipo” y pulse “Aceptar”. 
230.	Agregue los equipos y pulse sobre “Aceptar”. 

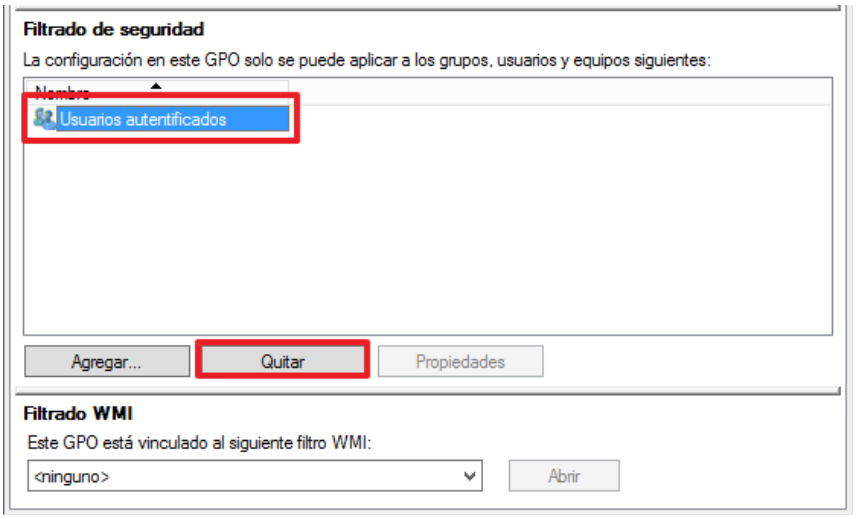
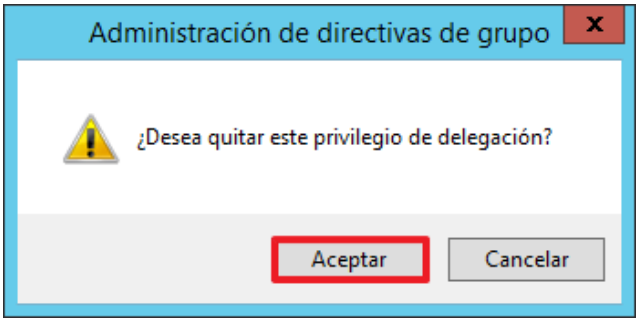
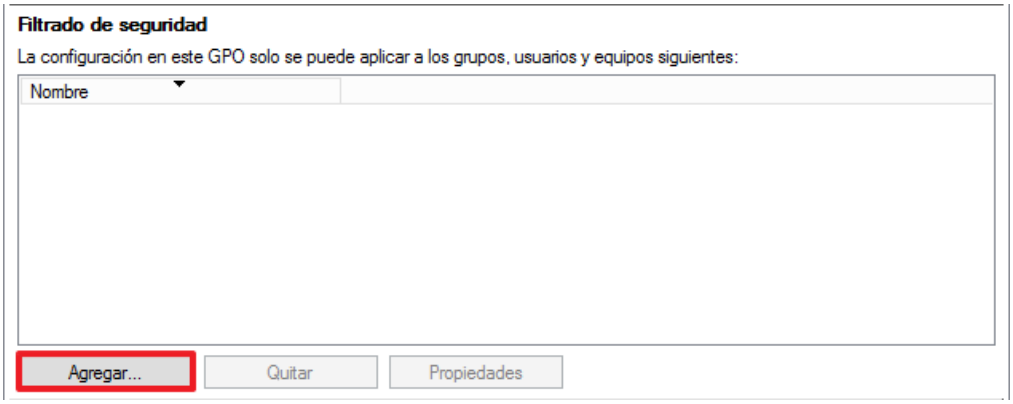
Paso	Descripción
231.	Pulse “Aceptar” para cerrar las propiedades del grupo. 
232.	Cierre la herramienta de “Usuarios y equipos de Active Directory”
233.	Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: **“Herramientas → Administración de directivas de grupo”**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

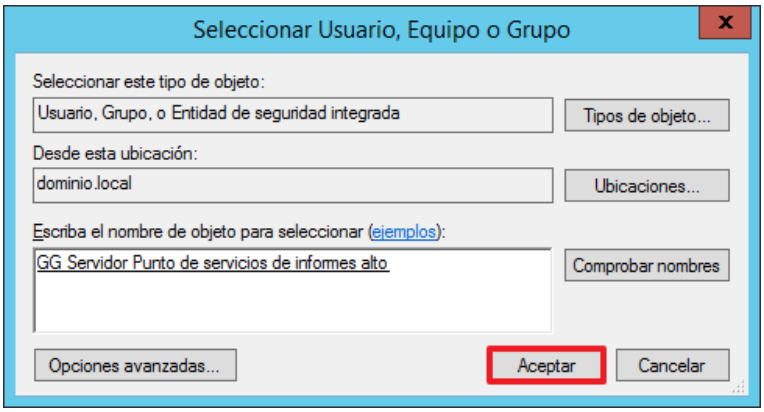
Paso	Descripción
234.	Desde la consola de administración de directivas de grupo, cree un nuevo objeto de directiva de grupo en la unidad organizativa recién creada “Servidores SQL”, haciendo clic con el botón derecho en el menú “Crear un GPO en este dominio y vincularlo aquí…”.  **Nota:** Deberá adaptar estos pasos a su organización seleccionando la Unidad Organizativa que aloje los roles en los que está reforzando la seguridad.
235.	Escriba el nombre de la GPO “CCN-STIC-875 ENS Incremental Punto de Servicios de Informes alto” y haga clic en el botón “Aceptar”. 
236.	En los siguientes pasos, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5”, en caso de que ya haya vinculado la directiva en algún paso anterior, continúe con el paso 241, en caso contrario continúe con el siguiente paso.
237.	A continuación, se va a vincular la directiva de grupo “CCN-STIC-873 ENS Incremental IIS 8.5” creada en la guía “CCN-STIC-873 Implementación del ENS en IIS 8.5 sobre Windows Server 2012 R2”, en la unidad organizativa “Servidores SQL.

Paso	Descripción
238.	Pulse con el botón derecho sobre la unidad organizativa “Servidores SQL” y haga clic sobre “Vincular un GPO existente…” 
239.	A continuación, seleccione el objeto de directiva de grupo: “CCN-STIC-873 ENS Incremental IIS 8.5” y pulse sobre aceptar. 

Paso	Descripción
240.	Para que la aplicación de las directivas se realice correctamente, asegúrese de que la directiva "CCN-STIC-875 ENS Incremental Punto de Servicios de informes alto" aparezca posicionada por encima de la directiva "CCN-STIC-873 ENS Incremental IIS 8.5". Para ello seleccione, dentro de la unidad organizativa "Servidores SQL", la directiva "CCN-STIC-875 ENS Incremental Punto de Servicios de informes alto" y a continuación, haga clic sobre la fecha hacia arriba para que se sitúe por encima en el orden de vínculos, tal y como se muestra en la imagen. 
241.	A continuación, edite la GPO: "CCN-STIC-875 ENS Incremental Punto de servicios de informes alto" creada anteriormente haciendo clic con el botón derecho y seleccionando la opción "Editar" del menú contextual. 
242.	Expanda el nodo "**Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad**". A continuación, haga clic con el botón derecho sobre "Configuración de seguridad" y seleccione en el menú contextual la opción "Importar directiva…". 

Paso	Descripción
243.	Importe la plantilla de seguridad “CCN-STIC-875 ENS Incremental Punto de servicios de informes alto.inf” que previamente debe haberse copiado en la ruta “%SYSTEMROOT%\Security\Templates” y haga clic en botón “Abrir”. 
244.	Cierre el “Editor de administración de directivas de grupo” una vez que se haya realizado la importación de la configuración de seguridad.
245.	Seleccione el nuevo objeto de directiva de grupo configurado y localice la pestaña “Ámbito” que se encuentra en el panel derecho. 

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

Paso	Descripción
249.	Introduzca como nombre “GG Servidor Punto de servicios de informes alto”. A continuación, pulse el botón “Aceptar”.  **Nota:** En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a su organización, para que la directiva de grupo creada anteriormente se aplique únicamente sobre los equipos correspondientes.
250.	Cierre el “Administrador de directivas de grupo”.

7. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN

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

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

En la presente guía la conexión con el servidor que tiene implementado SCCM se efectúa a través de escritorio remoto, debido a la aplicación de los refuerzos de seguridad que se van a realizar, en caso que los usuarios administrativos solo requieran de acceso para administrar SCCM se recomienda que la conexión se realice a través de la consola de administración de SCCM desde su puesto de trabajo y no mediante escritorio remoto, evitando con ello otorgar más permisos de los estrictamente necesarios.

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

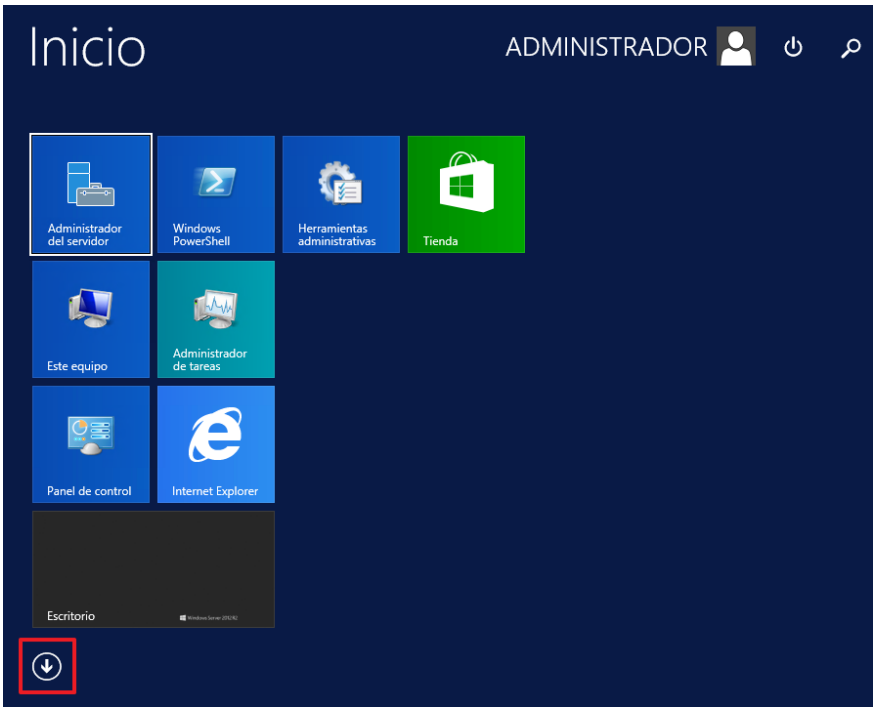
Nota: Todas las recomendaciones de seguridad indicadas en la presente guía deben ser adaptadas al entorno de su organización. Se aconseja realizar las pruebas pertinentes en un entorno de preproducción antes de ser incluidas en su entorno de producción.

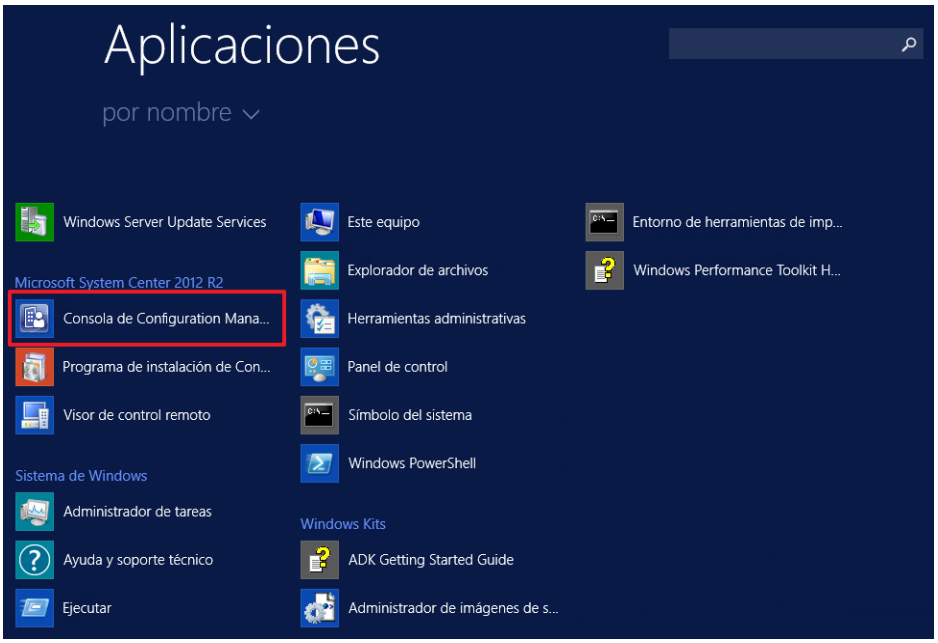
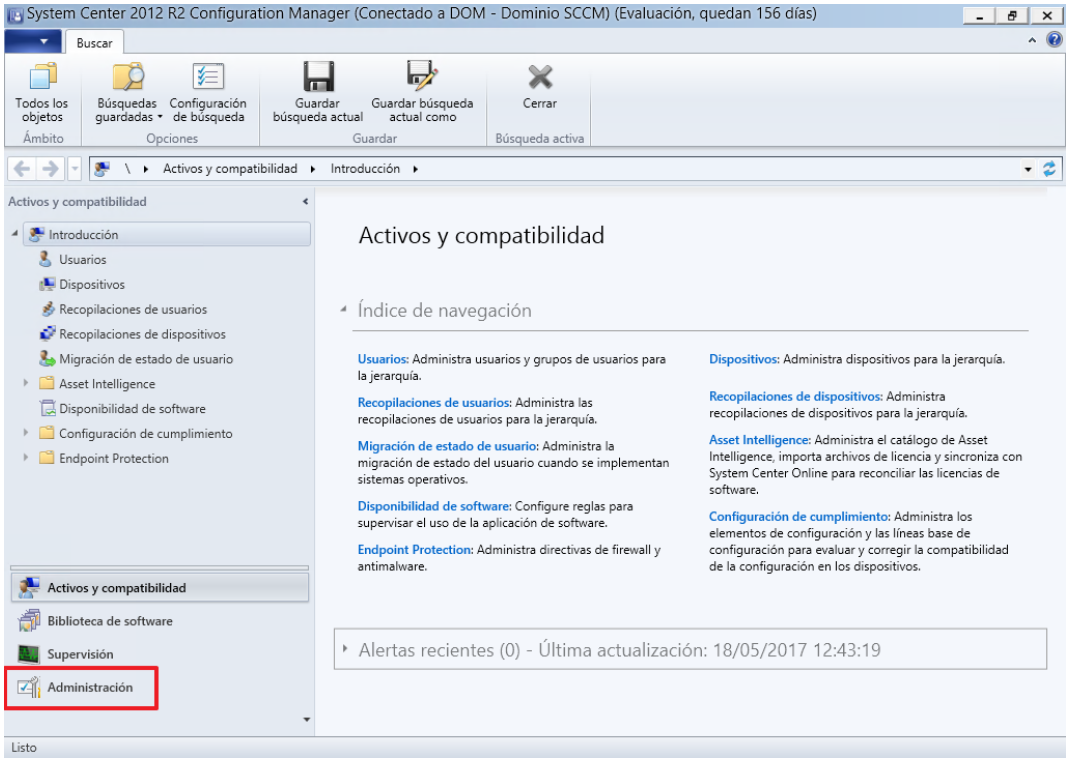
7.1. PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

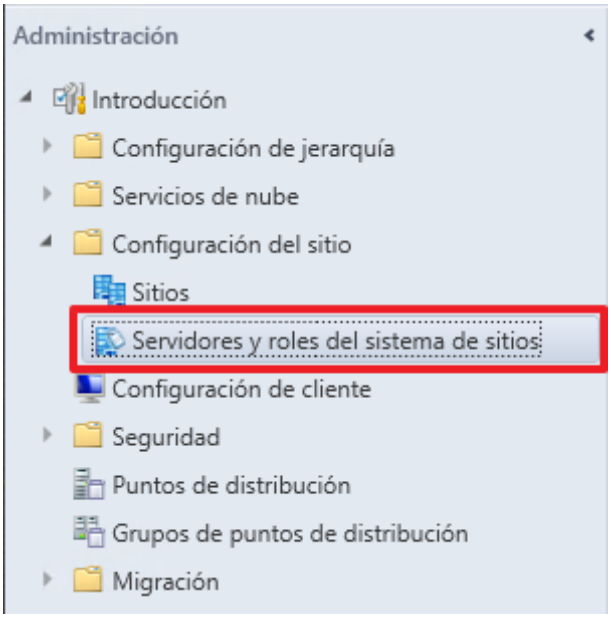
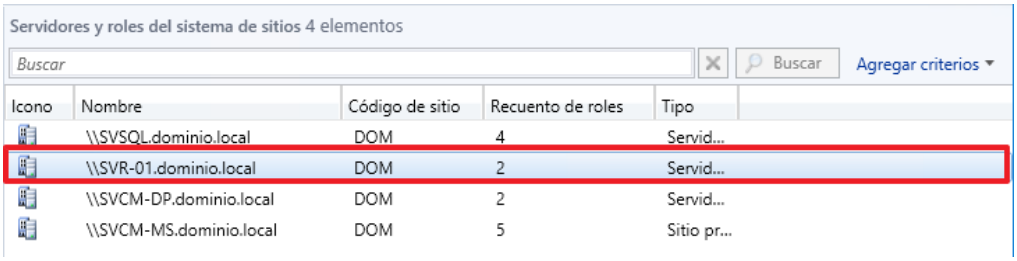
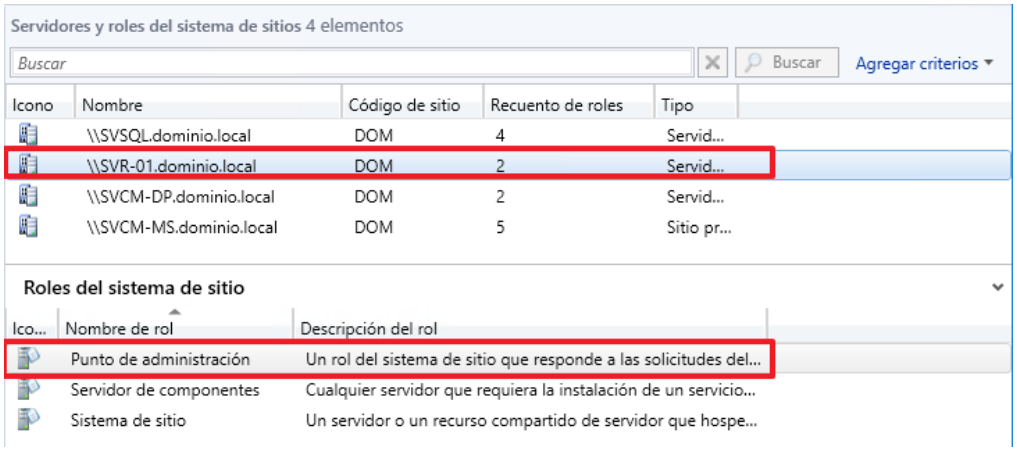
Uno de los aspectos que marca el ENS, desde su requisito de nivel bajo en el Marco Operacional, es la mínima funcionalidad y mínima exposición evitando con ello posibles vulnerabilidades minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario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

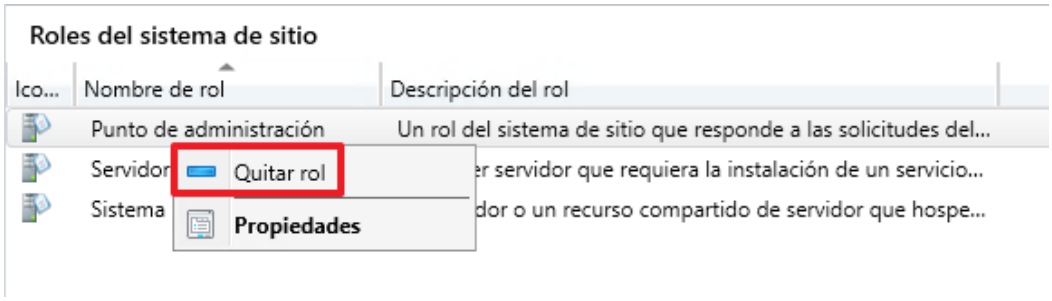
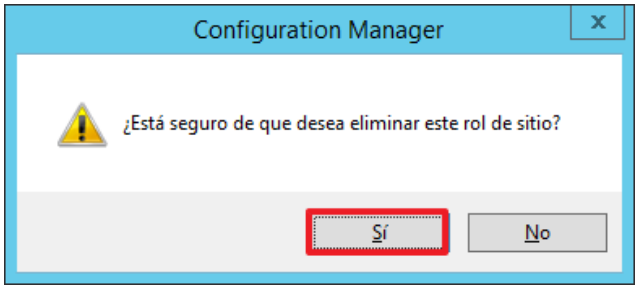
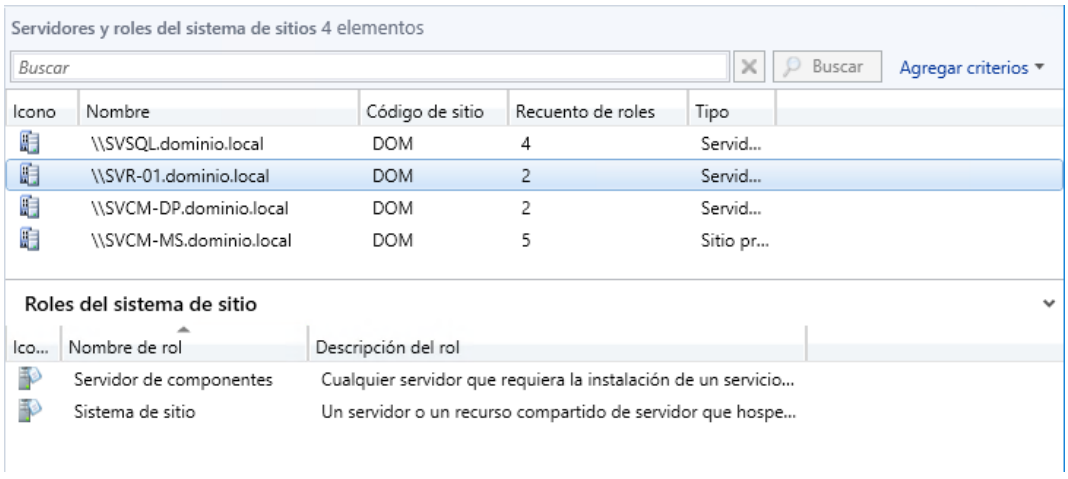
Microsoft SCCM 2012 R2 permite el añadir o quitar roles en los servidores función de la tarea a desempeñar por el servidor, por ejemplo, un servidor destinado únicamente a la distribución de paquetes, el cual tiene instalado el rol de punto de distribución, no es necesario que tenga otro rol para el cual el servidor no está destinado.

Seguidamente, se muestra un ejemplo de cómo desinstalar un rol específico implementado en un servidor. El siguiente paso a paso da por hecho que ya instalado previamente un rol y que por necesidades de la organización dicho rol se ha de desinstalar del servidor, aplicando con ello el principio de mínima funcionalidad quitando características que ya no son necesarias de un servidor de su organización.

Paso	Descripción
251.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
252.	Pulse sobre el menú inicio. 
253.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
254.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
255.	Selección el apartado “Administración”. 

Paso	Descripción
256.	Despliegue "**Configuración del sitio > Servidores y roles del sistema de sitios**". 
257.	A continuación, seleccione en el menú derecho el servidor del que quiere quitar un rol de sistema de sitios.  **Nota:** Deberá adaptar estos pasos a su organización seleccionando el servidor que contenga implementado el rol que desea quitar.
258.	En este ejemplo se va a quitar el rol de "Punto de administración" el cual ha sido implementado previamente. Asegúrese que selecciona el servidor correcto y en la parte inferior seleccione el rol que desea desinstalar. 

Paso	Descripción
259.	A continuación, una vez seleccionado el rol que desea quitar, pulse con el botón derecho y seleccione la opción “Quitar rol” del menú contextual. 
260.	Pulse “Sí” sobre la advertencia que aparece cuando está intentando quitar el rol. 
261.	A continuación, compruebe que ha quitado el rol correctamente. 

7.2. SEGREGACIÓN DE ROLES Y FUNCIONES

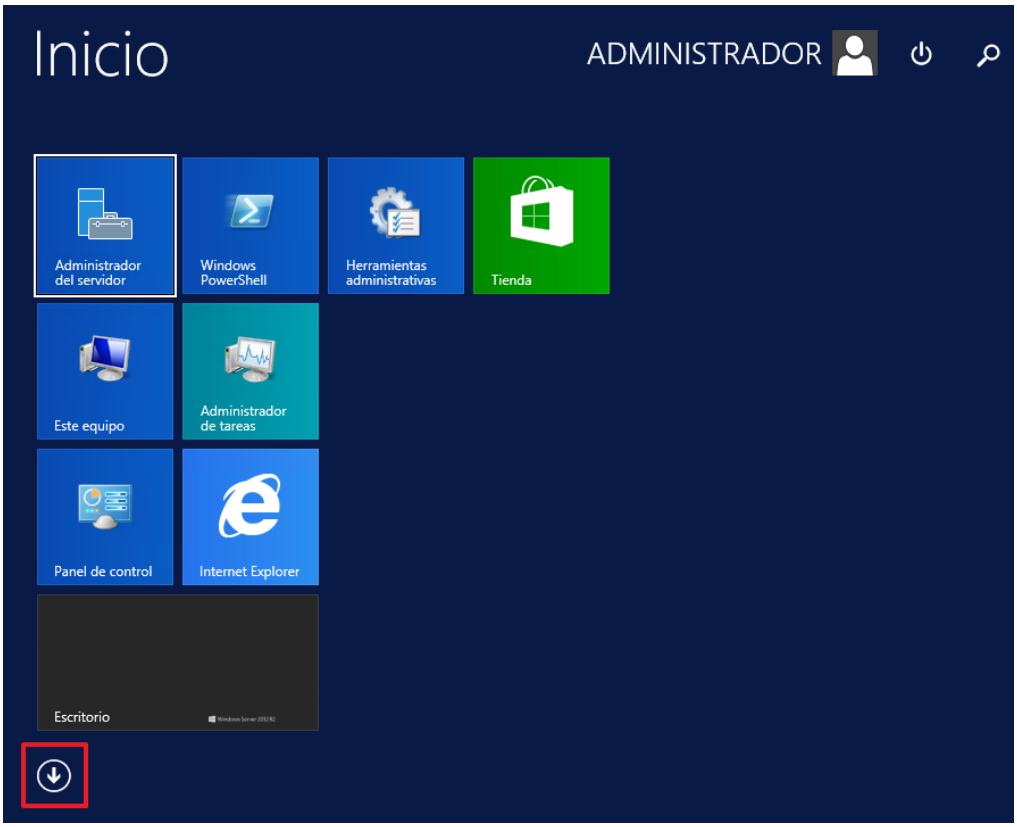
Antes de poder aplicar diferentes mecanismos de auditoría y conformidad, debe tener presente que determinadas funcionalidades requieren de la obtención de permisos específicos para la realización de las operaciones. La asignación de dichos permisos se basa en el modelo RBAC (Role Based Access Control). Dicho modelo tiene su base fundamental en la pertenencia a grupos y a la aplicación de directivas sobre dichos grupos.

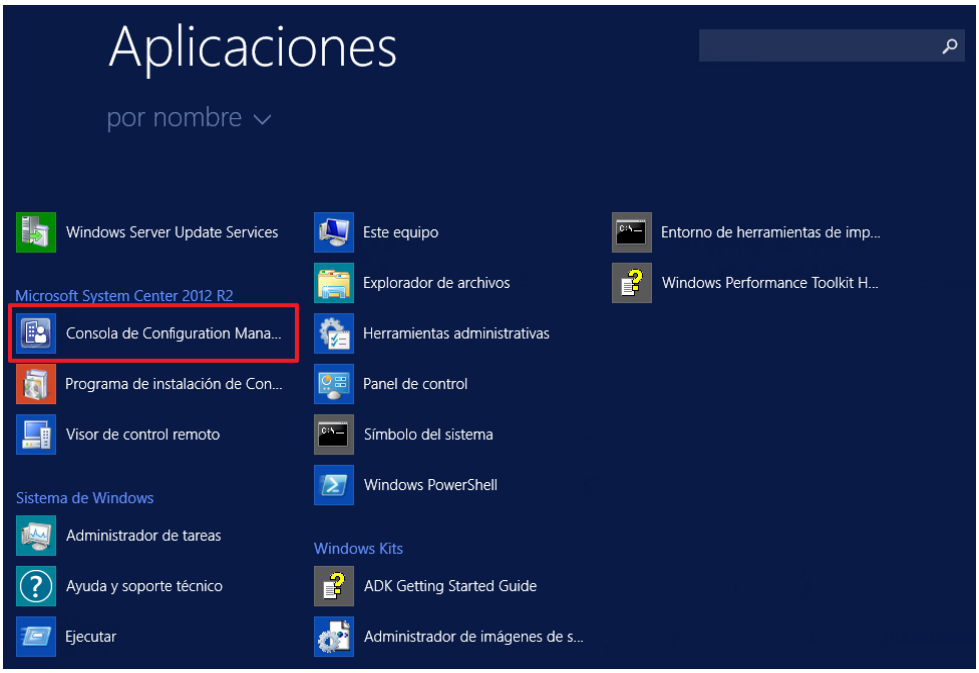
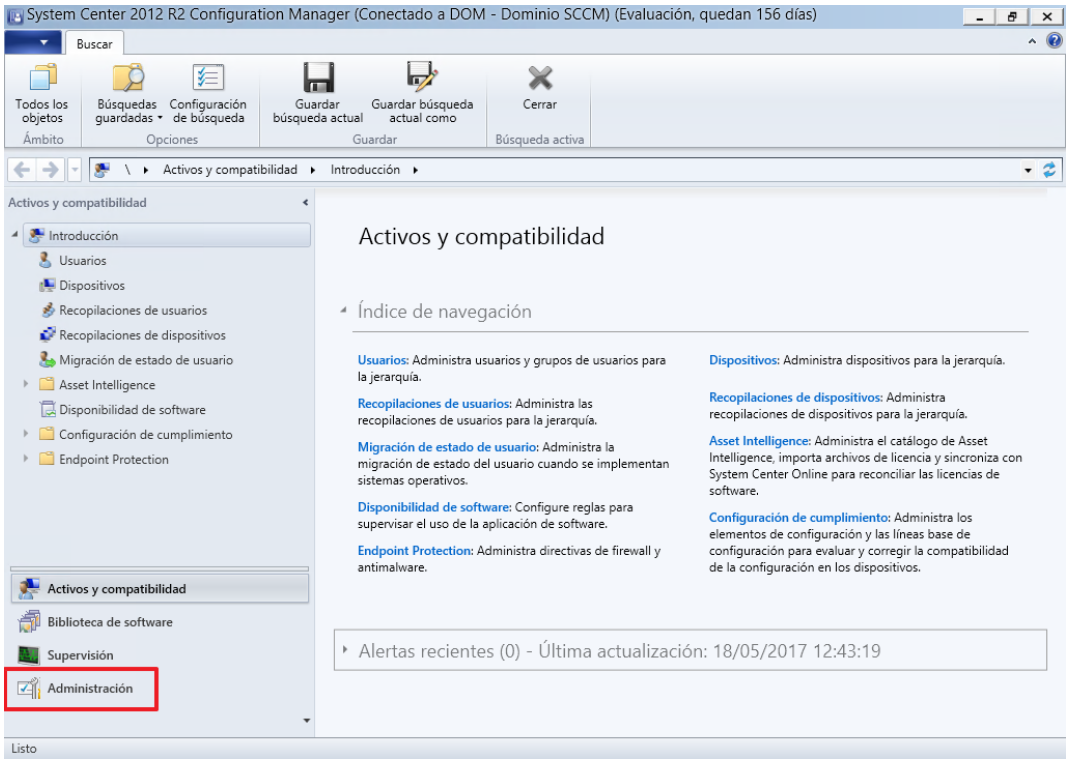
Así mismo, este modelo permite establecer una jerarquía de roles segregados, de tal forma que algunos usuarios de la organización pueden realizar tareas de administración, a la vez que otros pueden asumir la funcionalidad de auditores.

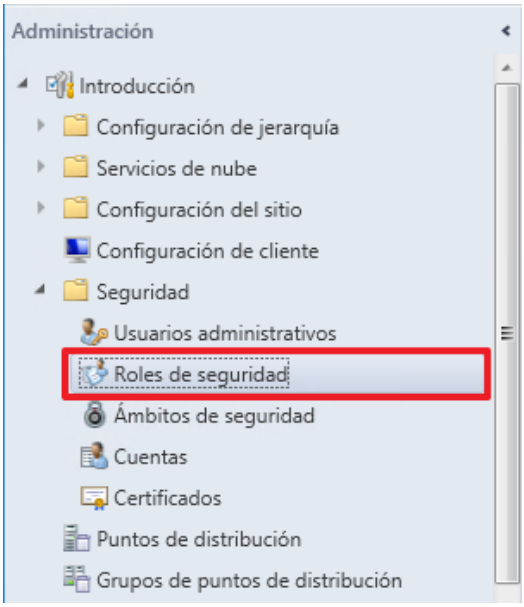
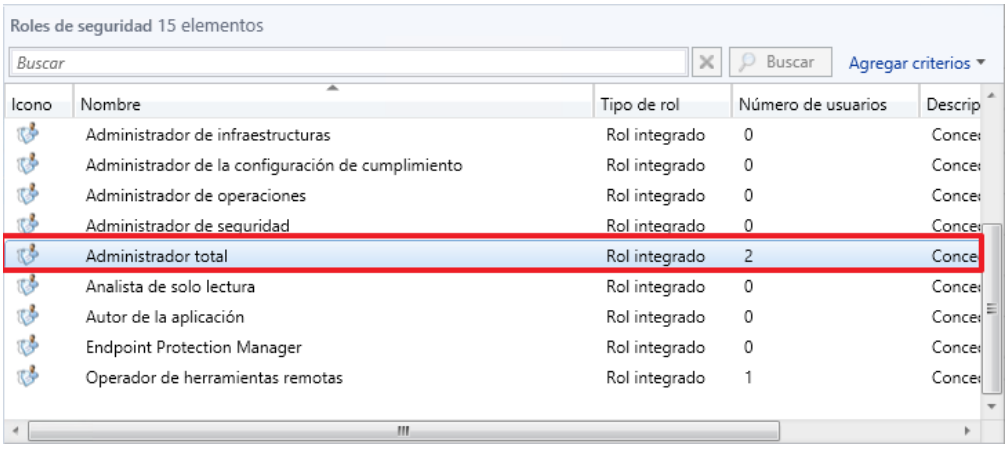
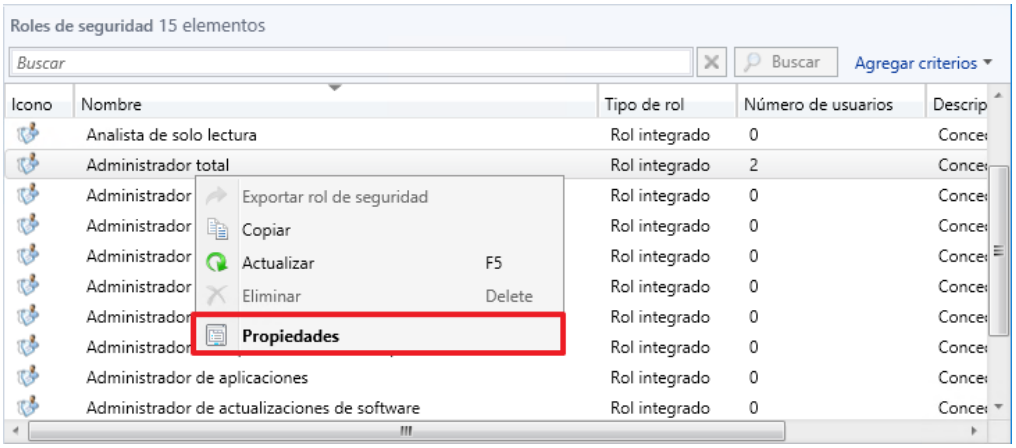
La administración de roles de seguridad y permisos se puede realizar a través de la consola principal de Configuration Manager o bien a través de cmdlets de PowerShell.

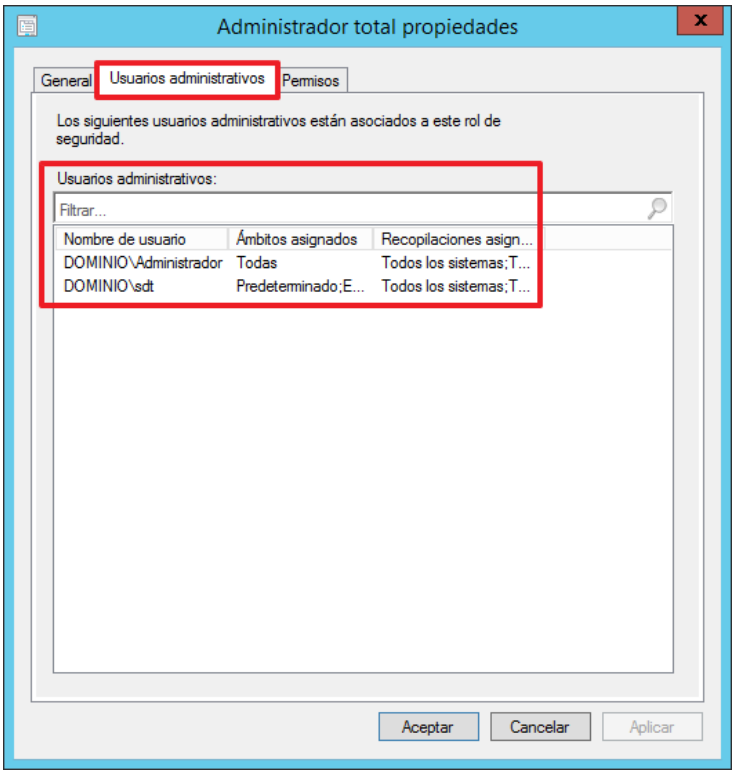
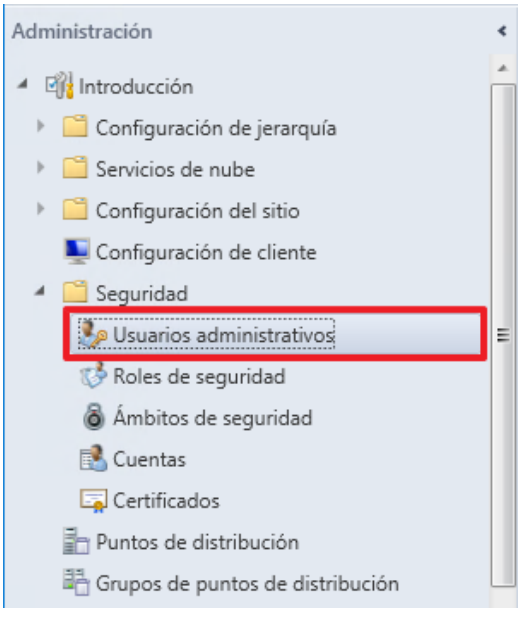
A continuación, se muestra un ejemplo de cómo comprobar los roles de seguridad que tiene asignado un usuario al igual que el procedimiento para asignar un rol de seguridad concreto a un usuario determinado.

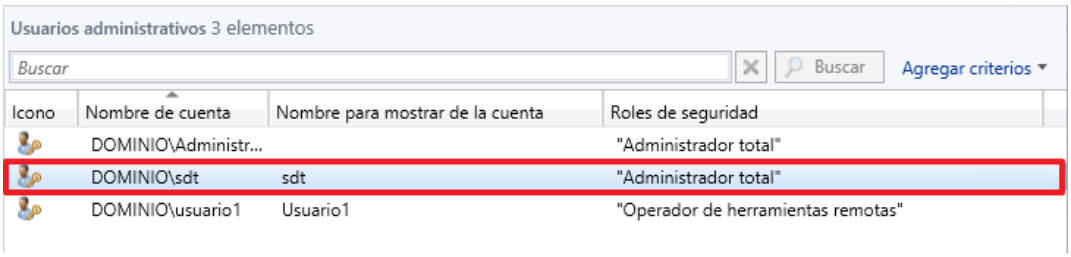
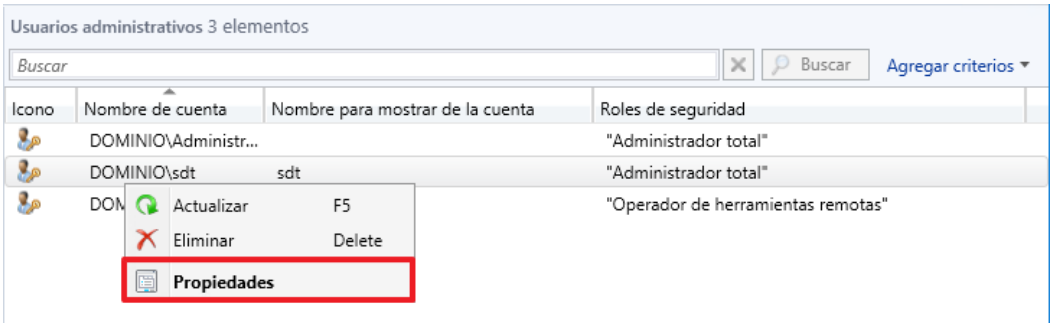
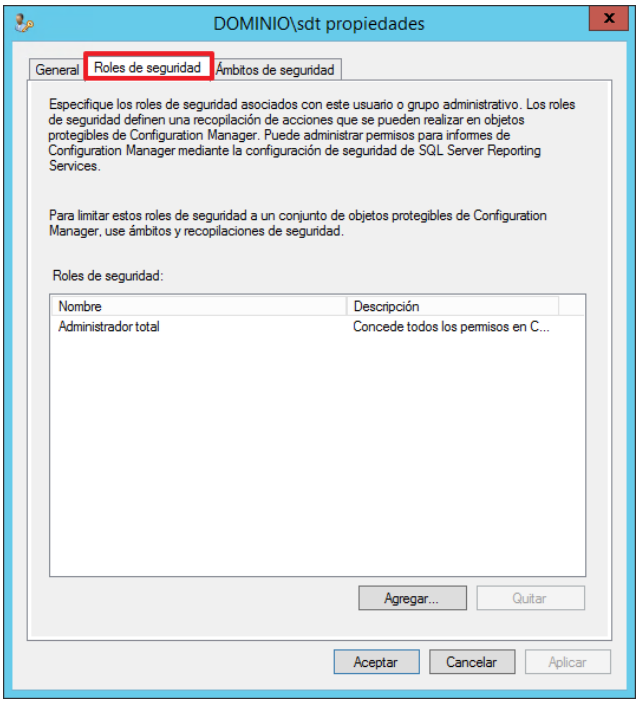
Nota: Si desea crear más información sobre la administración de roles y permisos visite la siguiente web: https://technet.microsoft.com/en-us/library/gg682106.aspx

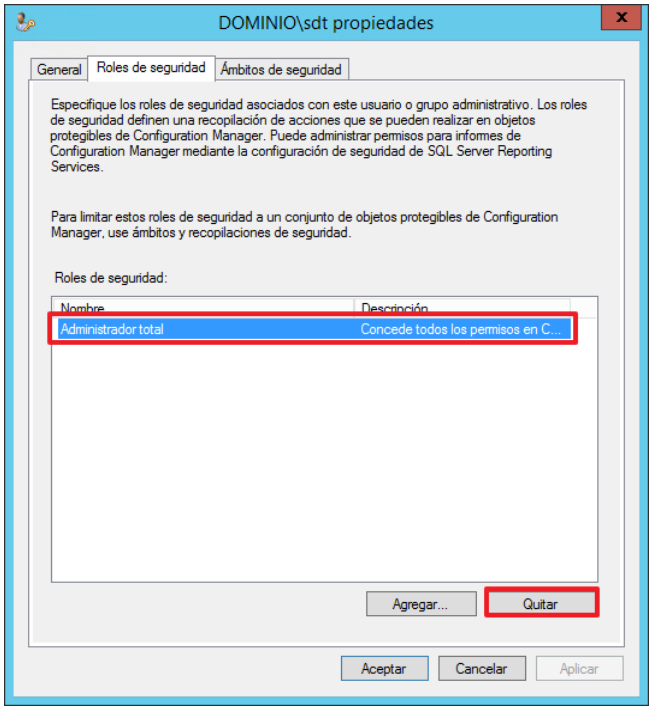
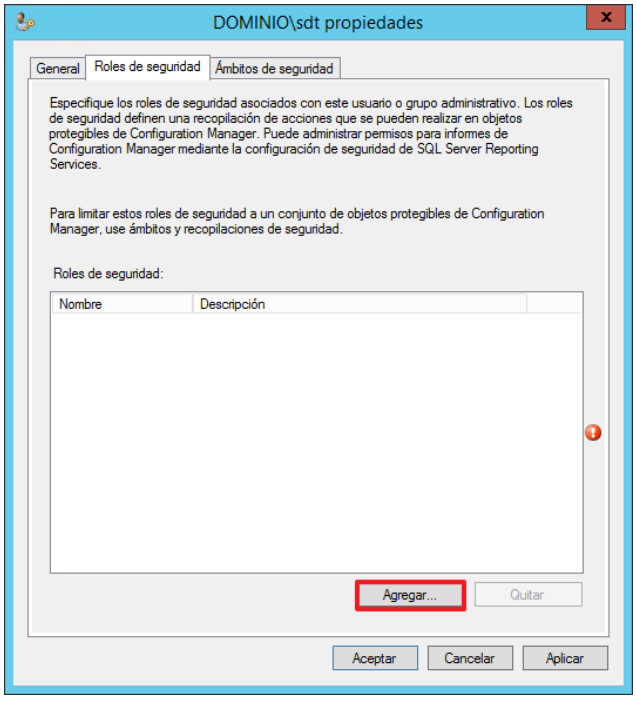
Paso	Descripción
262.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
263.	Pulse sobre el menú inicio. 
264.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

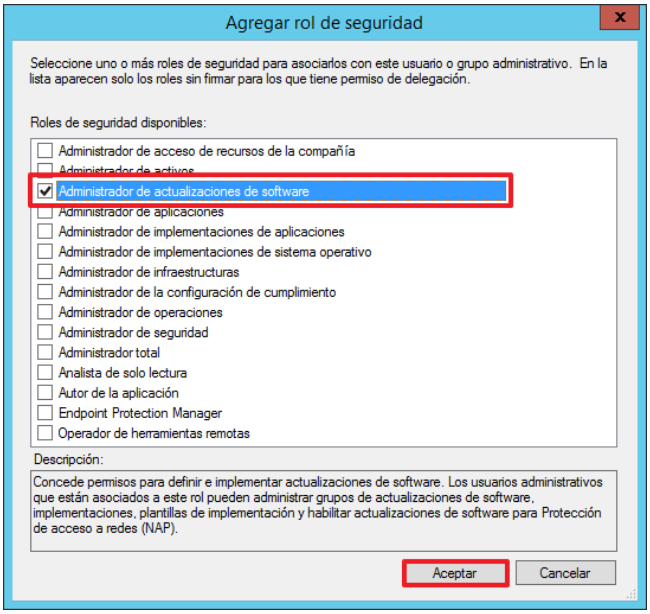
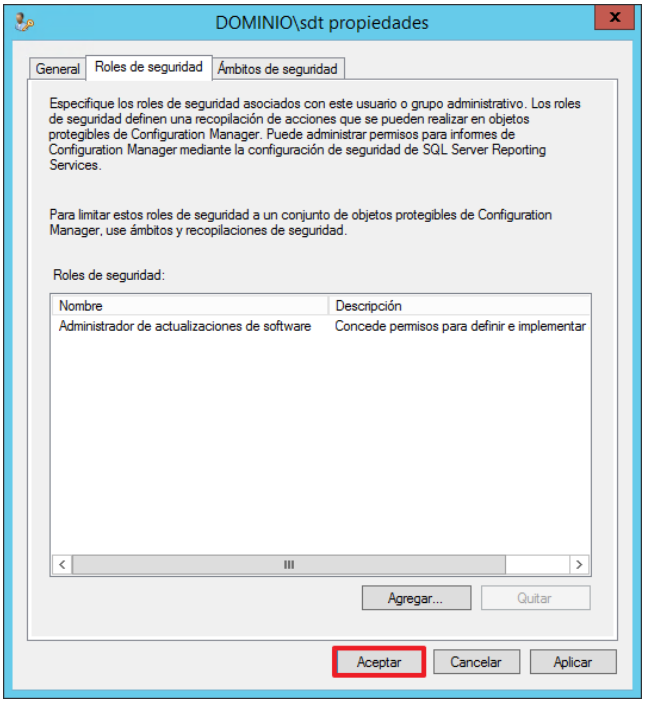
Paso	Descripción
265.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
266.	Seleccione el apartado “Administración”. 

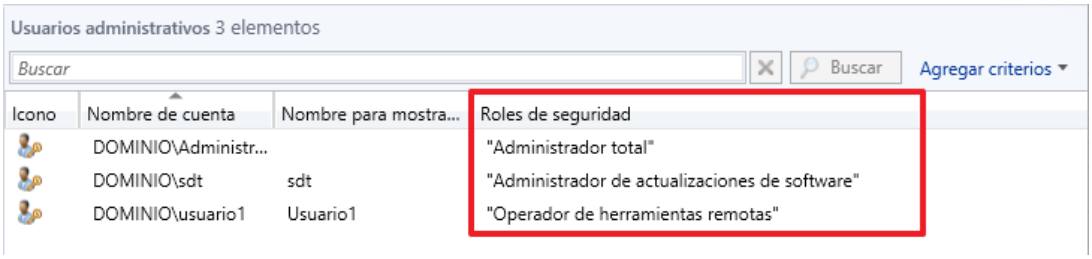
Paso	Descripción
267.	Despliegue “**Seguridad > Roles de seguridad**”. 
268.	Localice el rol de seguridad “Administrador total”. 
269.	Una vez seleccionado el rol de seguridad “Administrador total”, pulse con el botón derecho y marque la opción “Propiedades” del menú contextual. 

Paso	Descripción
270.	Seleccione la pestaña “Usuarios administrativos” y compruebe que los usuarios administrativos que aparecen son correctos ya que el rol de “Administrador total” concede todos los permisos en Configuration Manager. Una vez finalizada la comprobación pulse “Aceptar” para cerrar la ventana. 
271.	En el caso que requiera quitar el rol de seguridad “Administrador total” de un usuario y agregarle otro rol de seguridad deberá seleccionar la pestaña “Usuarios administrativos”. 

Paso	Descripción
272.	Localice el usuario administrativo que desea cambiar la configuración de roles de seguridad.  **Nota:** Los usuarios mostrados en la imagen son usuarios ficticios creados para elaborar la presente guía, por lo que deberá adaptar estos pasos a su organización. La presente guía no detalla como añadir usuarios administrativos a la consola de Configuration Manager.
273.	A continuación, una vez seleccionado el usuario al cual quiere modificar los roles de seguridad, pulse con el botón derecho y marque la opción “Propiedades” del menú contextual. 
274.	Seleccione la pestaña “Roles de seguridad”. 

Paso	Descripción
275.	Seleccione el rol que desea quitar y pulse sobre el botón “Quitar”. 
276.	Seleccione “Agregar” para añadir el rol de seguridad que desee aplicar sobre el usuario seleccionado anteriormente. 

Paso	Descripción
277.	Seleccione el rol que desea asignar y pulse “Aceptar”.  **Nota:** En este ejemplo se agrega el rol de seguridad “Administrador de actualizaciones de software”, deberá adaptar estos pasos a sus requerimientos.
278.	Pulse sobre “Aceptar” para confirmar la configuración y cerrar la ventana de propiedades del usuario. 

Paso	Descripción
279.	Es posible comprobar el rol asignado a un usuario desde la propia ventana de "usuarios administrativos.  **Nota:** Es posible que un usuario tenga varios roles de seguridad, pero en la presente guía no se contempla esta casuística.

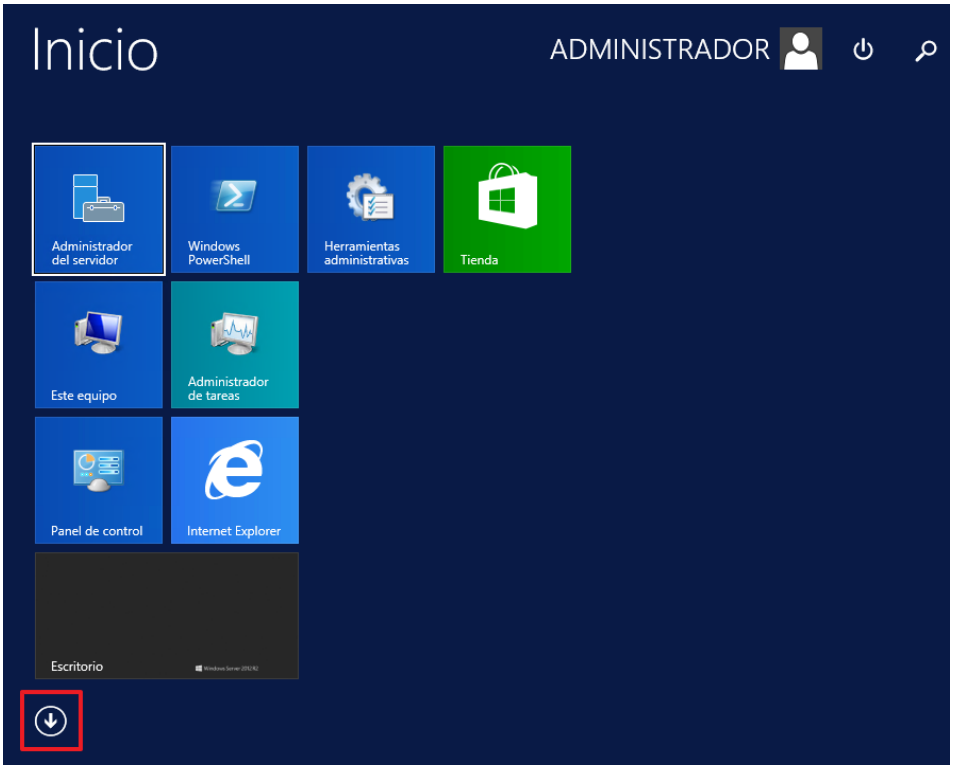
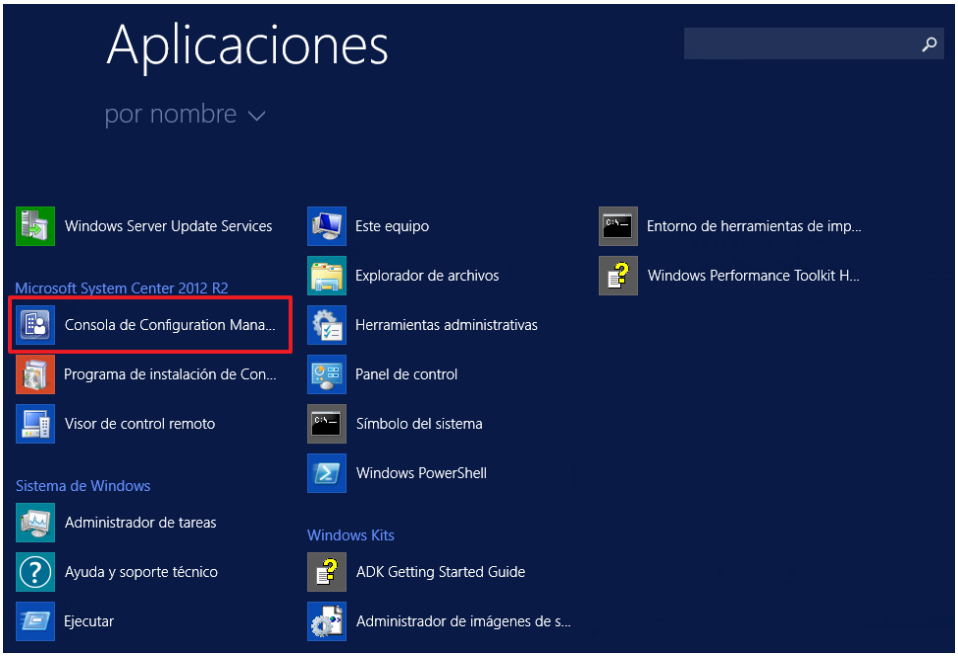
7.3. GESTIÓN DE DERECHOS DE ACCESO

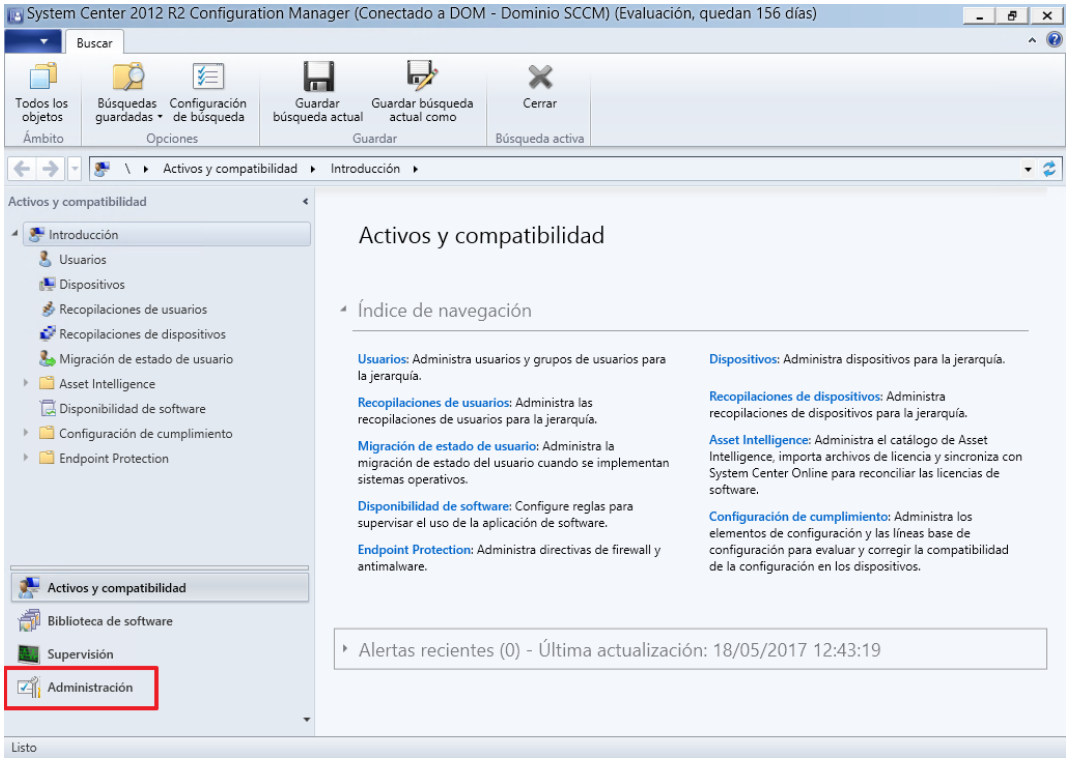
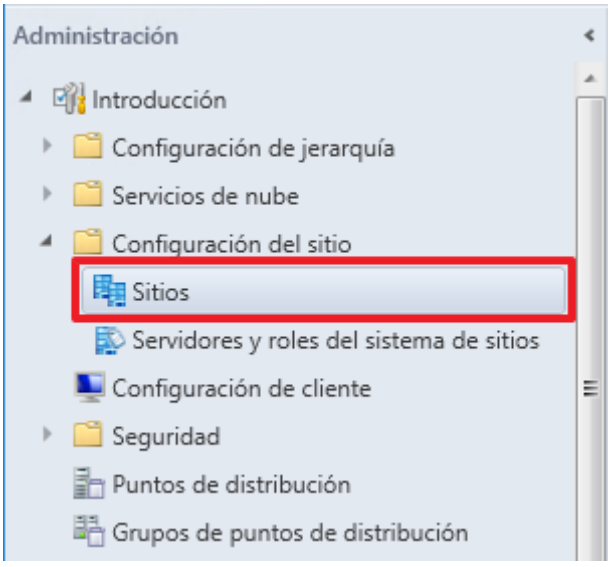
Microsoft SCCM 2012 R2 permite el establecer el método de aprobación de los clientes evitando con ello que equipos cliente no autorizados conecten con SCCM.

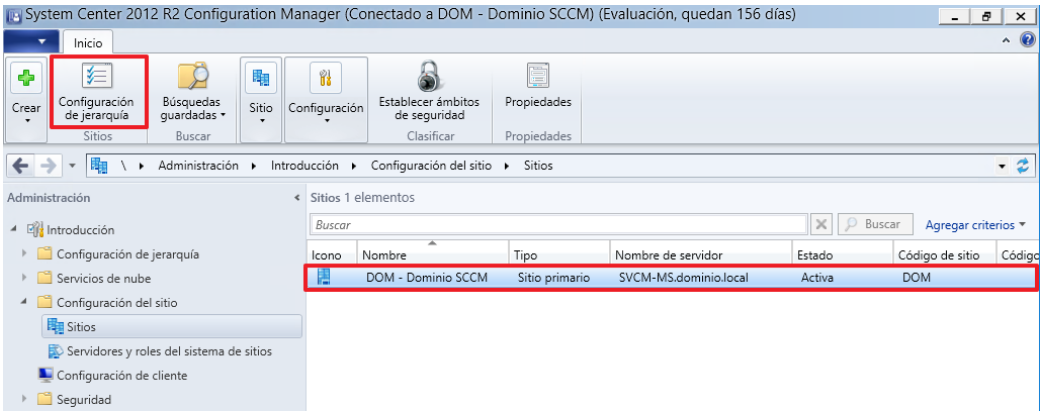
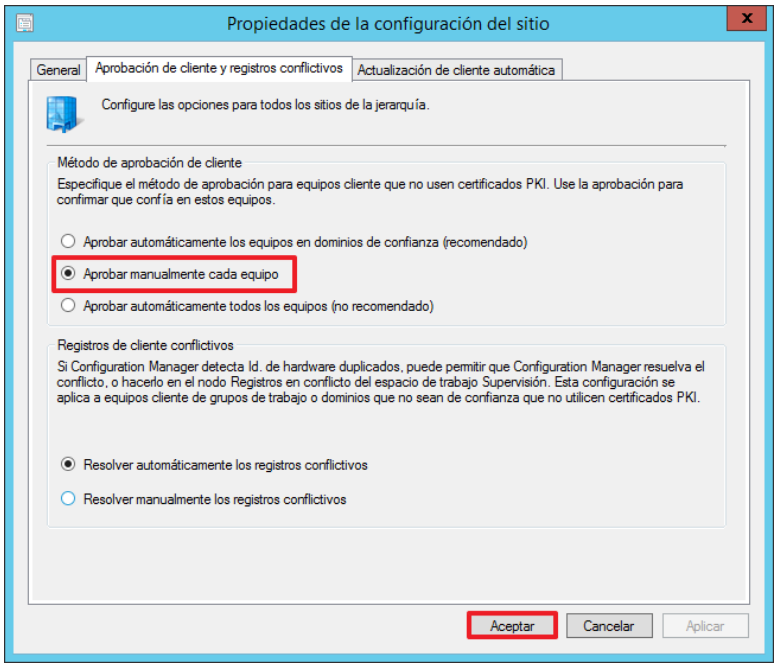
Para los niveles de seguridad medio y alto del ENS se recomienda que el derecho de acceso de los equipos cliente de MS SCCM 2012 R2 no se realice de forma automatizada si no que se requiera de la intervención de personal autorizado que permita la conexión del equipo cliente con MS SCCM 2012 R2.

En el proceso siguiente, se describe como establecer la aprobación de clientes en SCCM.

Paso	Descripción
280.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
281.	Pulse sobre el menú inicio. 

Paso	Descripción
282.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
283.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
284.	Seleccione el apartado “Administración”. 
285.	Despliegue “**Configuración del sitio > Sitios**”. 

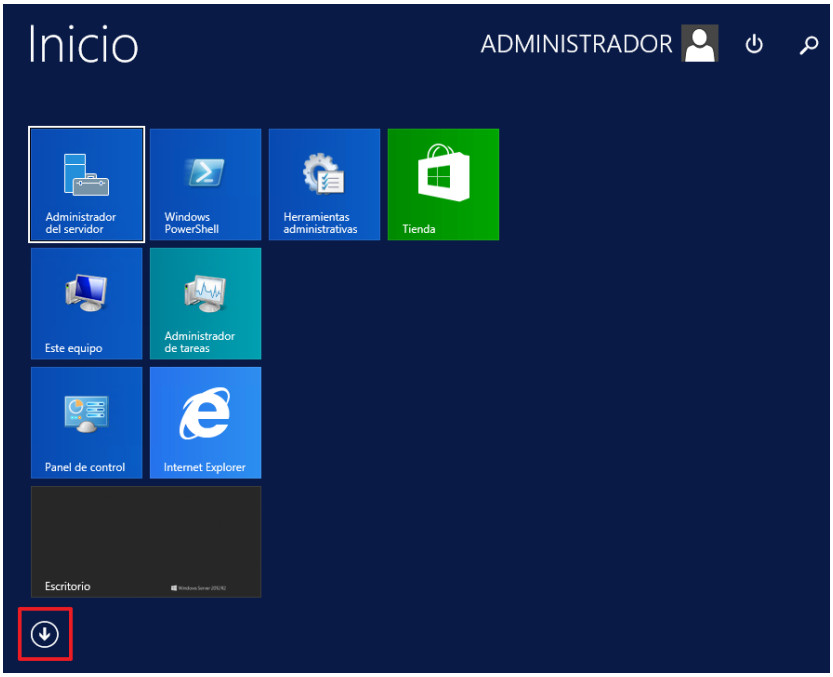
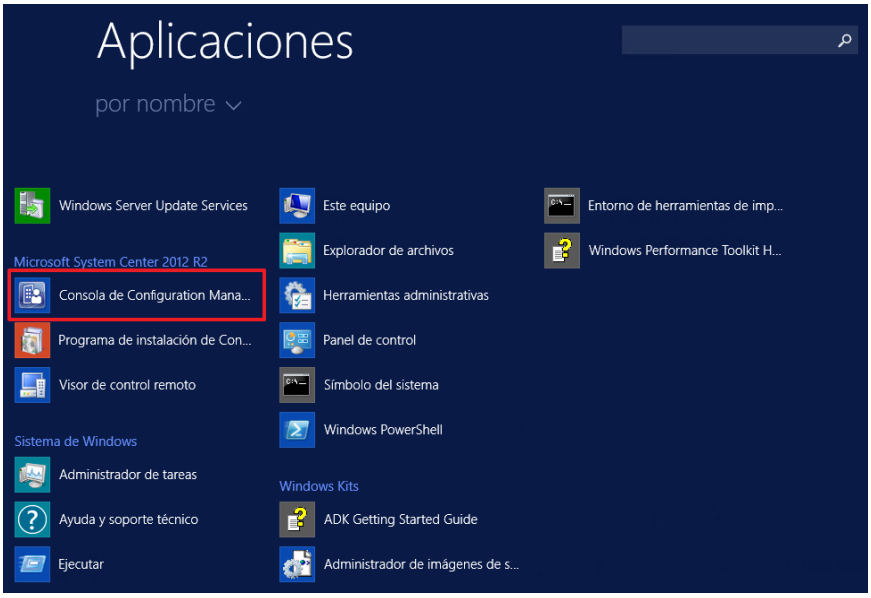
Paso	Descripción
286.	Seleccione el sitio que desea configurar y pulse sobre la opción “Configuración de jerarquía”. 
287.	Localice la pestaña “Aprobación de cliente y registros conflictivos”, marque la opción “**Aprobar manualmente cada equipo**” y pulse “**Aceptar**” para validar la configuración. 

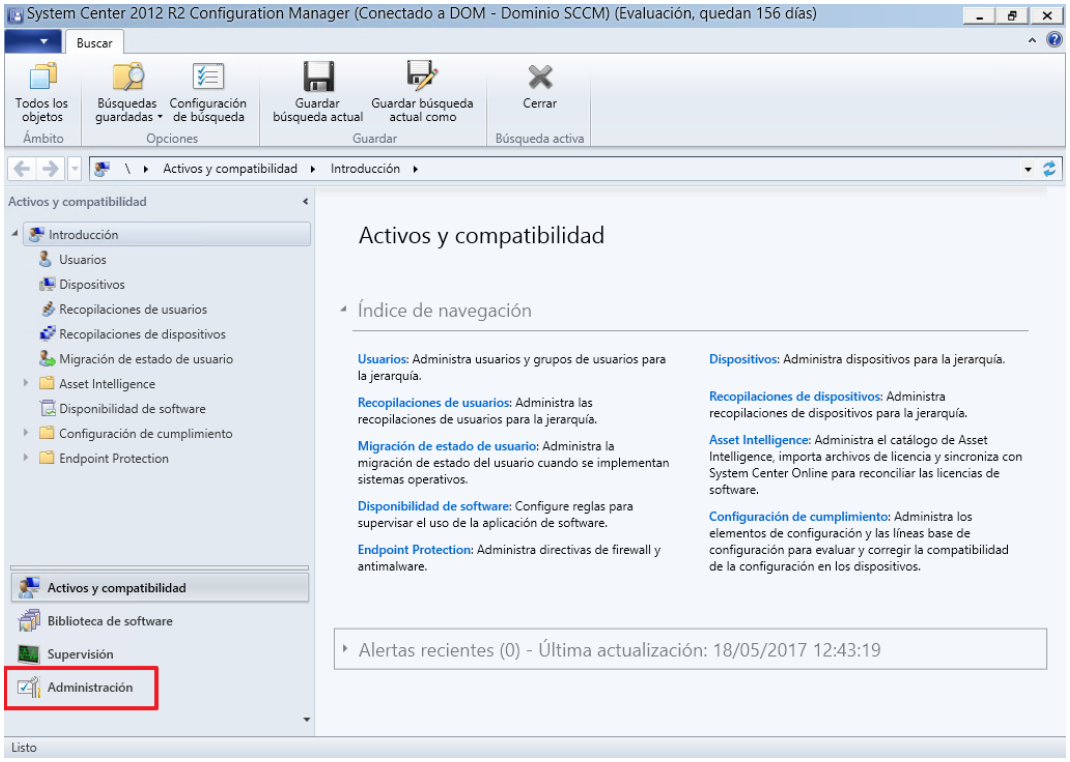
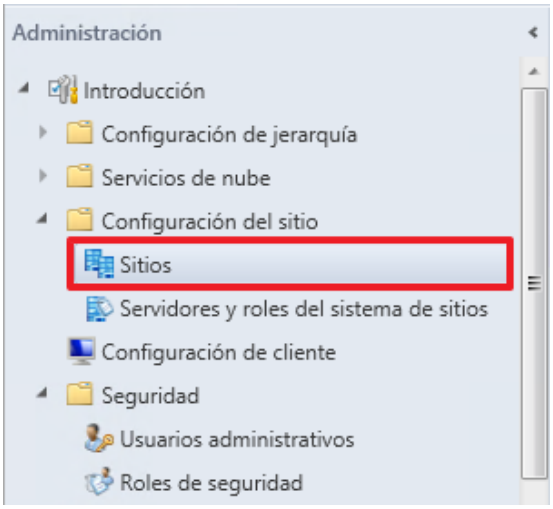
7.4. COMUNICACIÓN CON MS SCCM 2012 R2

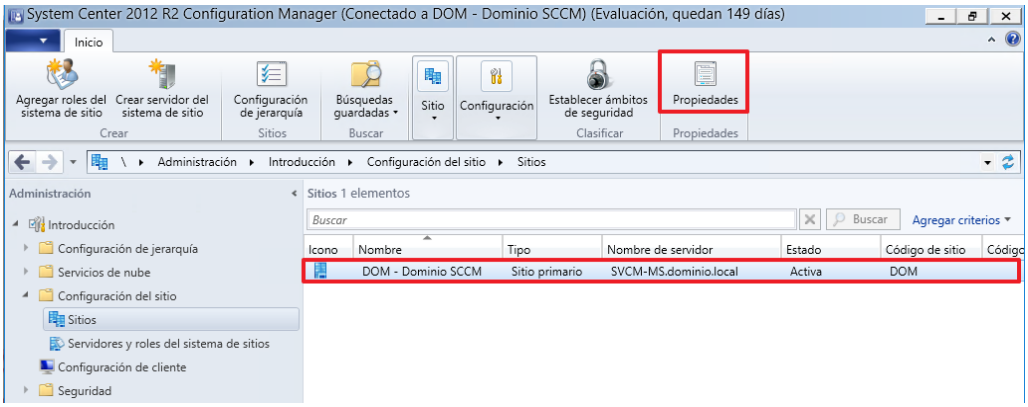
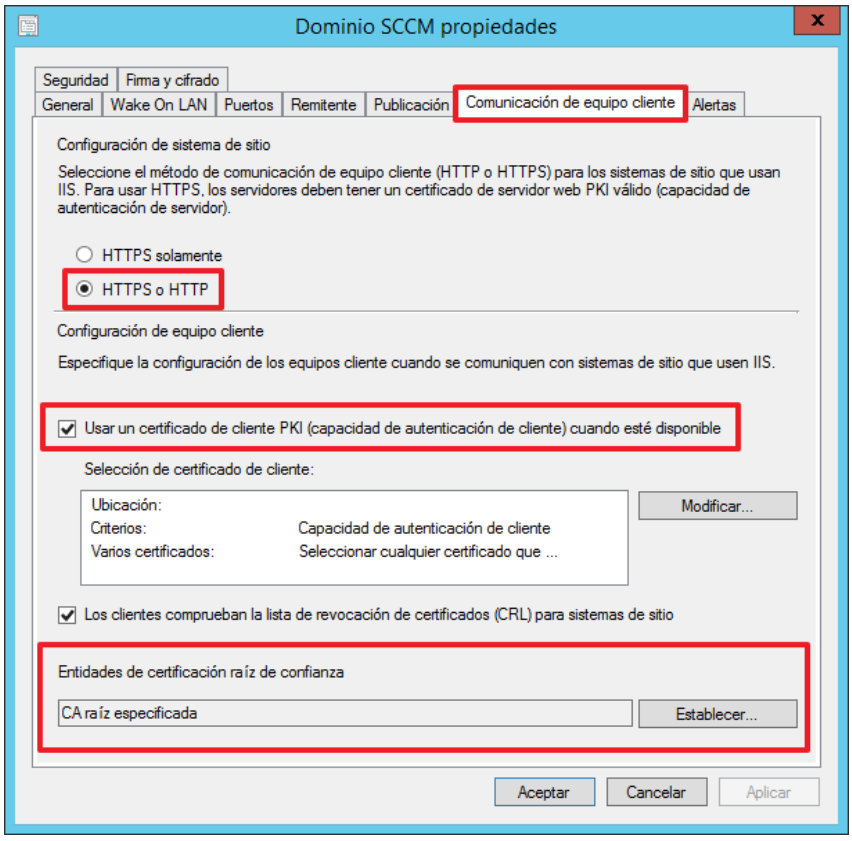
Microsoft SCCM 2012 R2 permite el establecer el método de comunicación de los equipos cliente estableciéndose en función del nivel de seguridad que se establezca en el ENS.

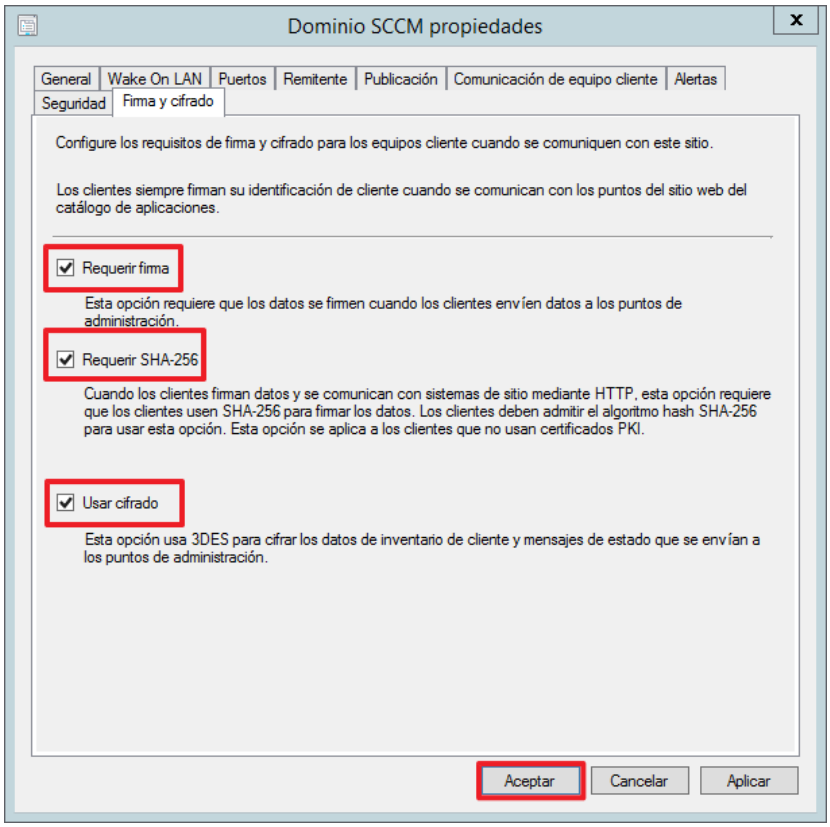
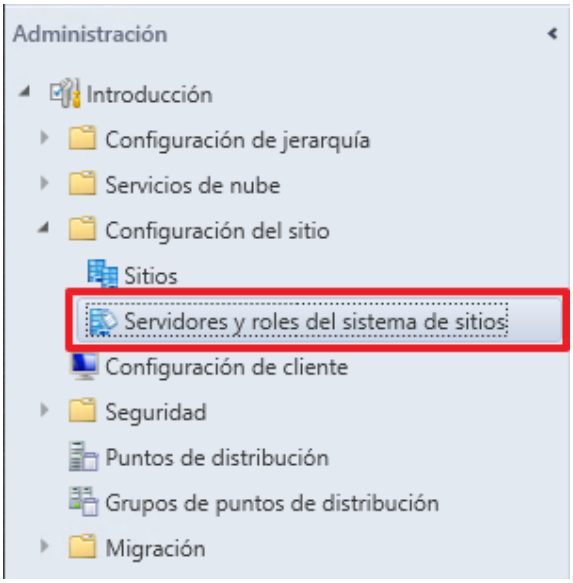
Para el nivel alto de seguridad del ENS se recomienda que el establecimiento de la comunicación entre MS SCCM 2012 R2 y los equipos clientes, se realice mediante certificado, y para la comunicación con el sitio se recomienda tener habilitado únicamente HTTPS.

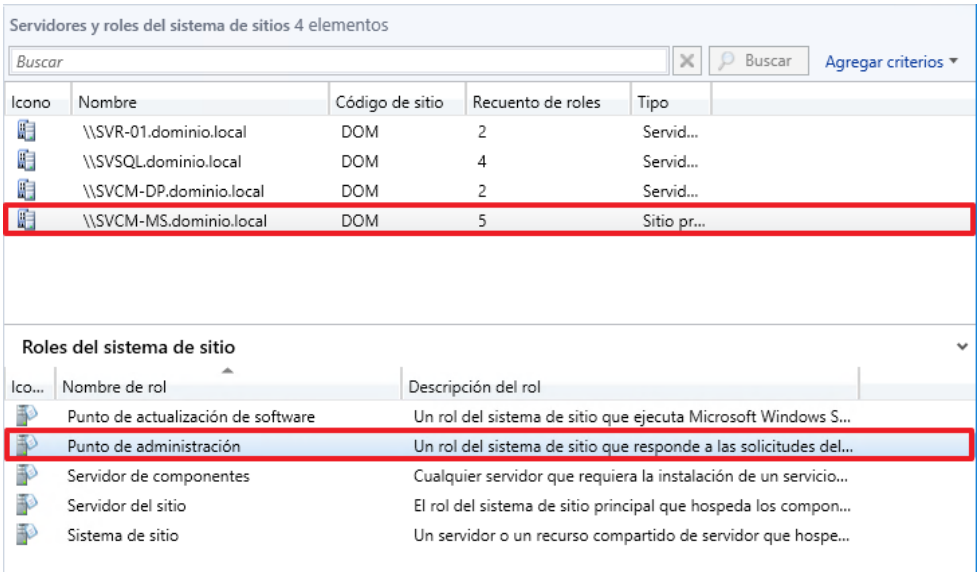
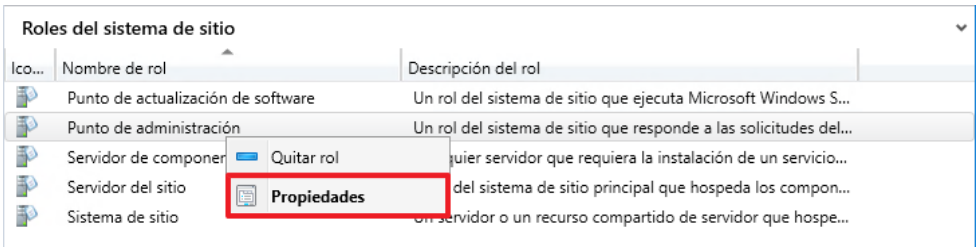
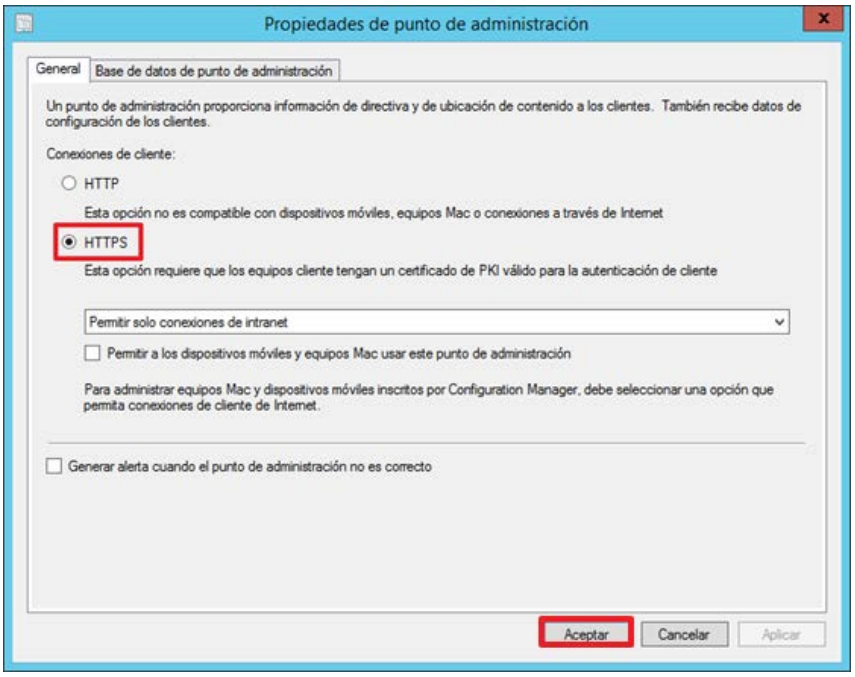
A continuación, se describe un paso a paso para reforzar la seguridad de las comunicaciones de MS SCCM 2012 R2.

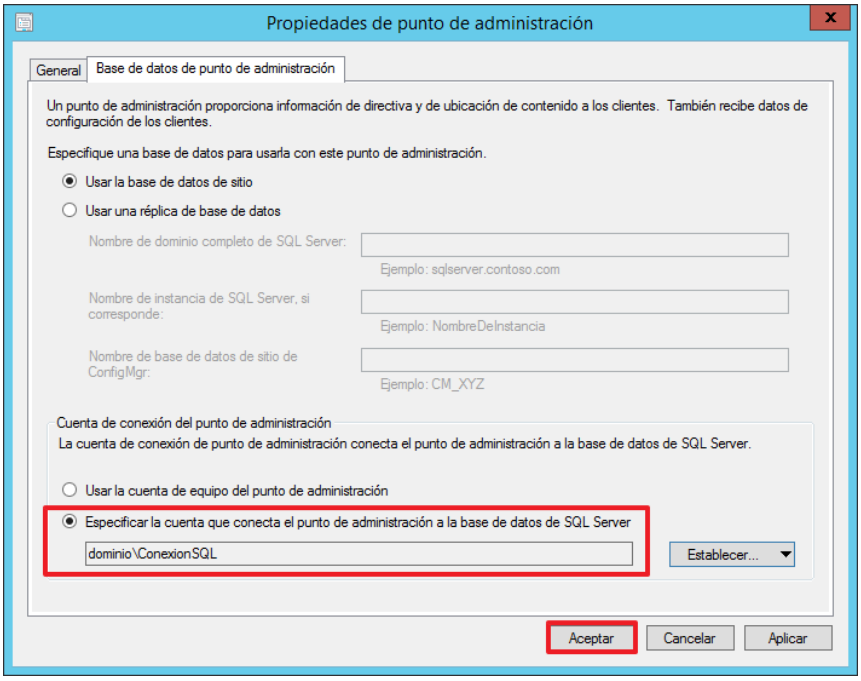
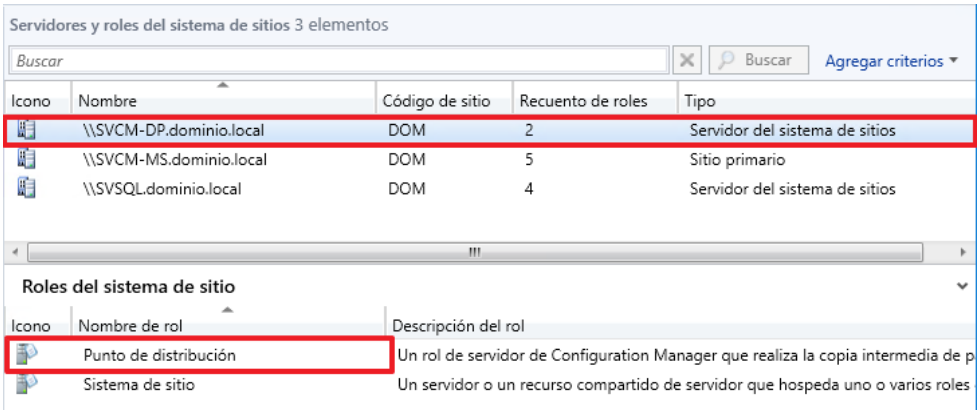
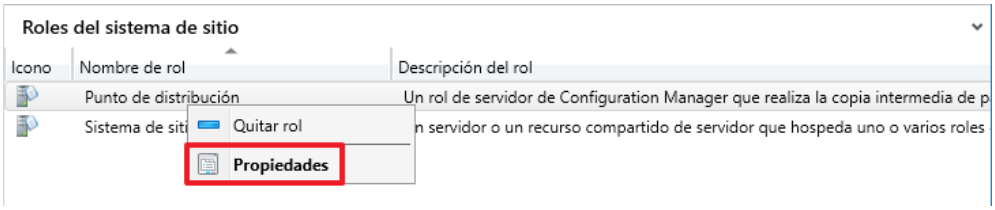
Paso	Descripción
288.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
289.	Pulse sobre el menú inicio. 
290.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
291.	Busque el icono “Consola de Configuration Manager” y marque sobre el para abrir la consola de administración de MS SCCM 2012 R2. 

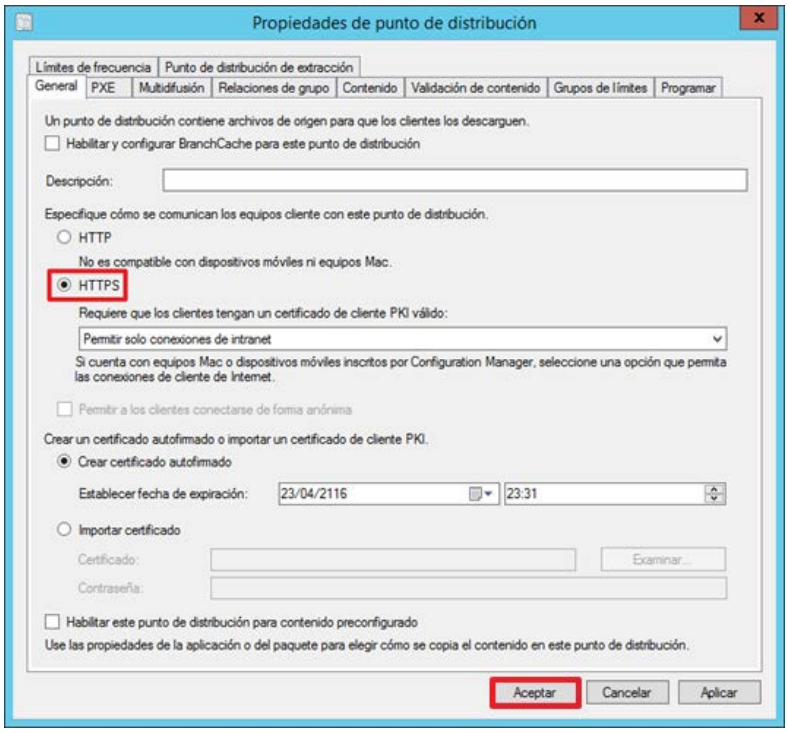
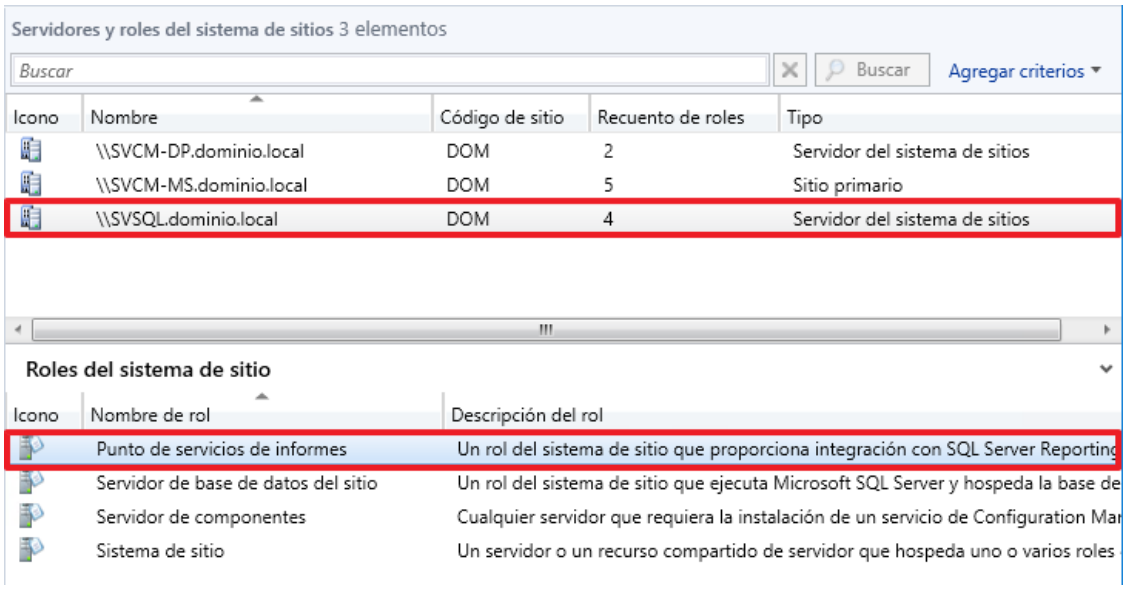
Paso	Descripción
292.	Seleccione el apartado “Administración”. 
293.	Despliegue “**Configuración del sitio > Sitios**”. 

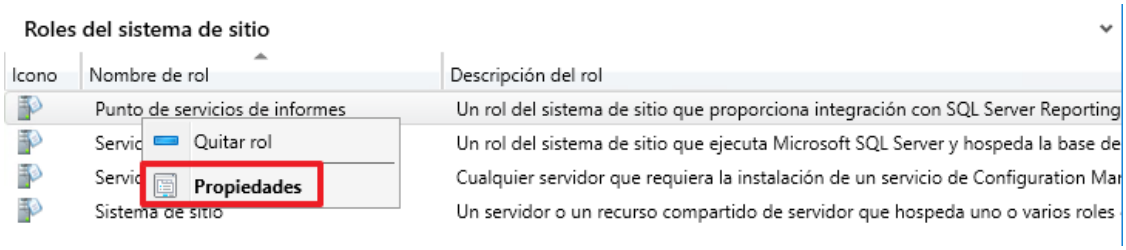
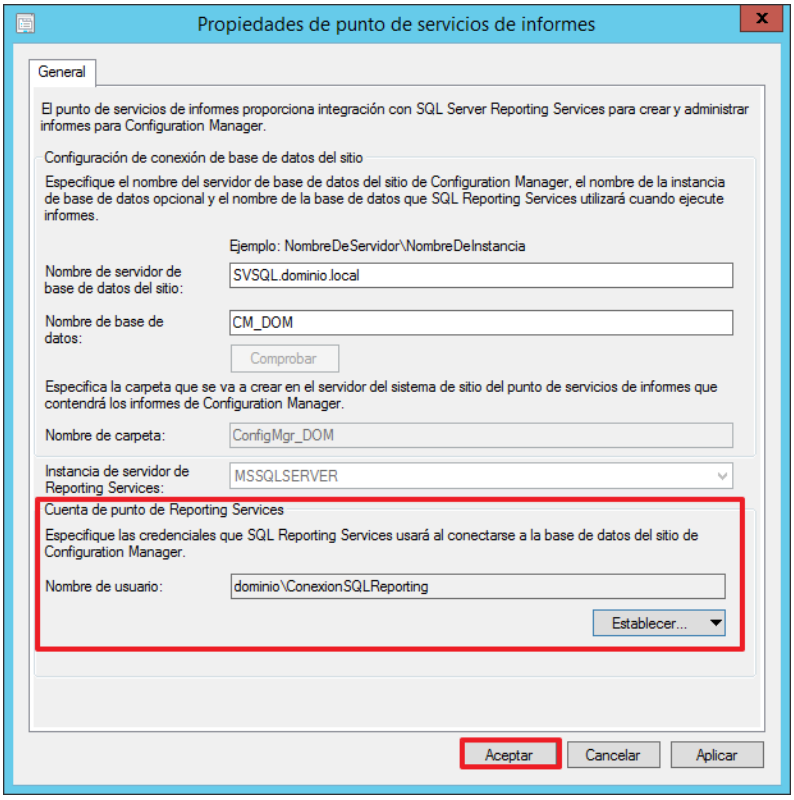
Paso	Descripción
294.	Seleccione el sitio que desea configurar y pulse sobre el botón “Propiedades” ubicado en la barra superior. 
295.	Seleccione la pestaña “Comunicación de equipo cliente” y marque la opción “HTTPS o HTTP”, y la opción “Usar un certificado de cliente PKI (capacidad de autenticación de cliente) cuando esté disponible”. Además, deberá establecer una entidad raíz de confianza previamente configurada en su entorno. 

Paso	Descripción
296.	Sitúese en la pestaña “Firma y cifrado”, marque las siguientes opciones disponibles y pulse “Aceptar” para finalizar la configuración. 
297.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 

Paso	Descripción
298.	Seleccione el servidor que contiene el rol de “Punto de administración”. 
299.	Localice el rol de “Punto de administración” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 
300.	En la pestaña “General”, seleccione en “Conexiones de cliente:” la opción “HTTPS” y pulse “Aceptar” para validar los cambios. 

Paso	Descripción
301.	Marque en la pestaña “Base de datos de punto de administración” y especifique una cuenta única de conexión del punto de administración a la base de datos SQL, y pulse “Aceptar” para validar los cambios.  **Nota:** Deberá adaptar estos pasos a su organización y seleccionar un usuario con las credenciales necesarias para que efectué correctamente la conexión del punto de administración y la base de datos de SQL Server.
302.	Seleccione el servidor que contiene el rol de “Punto de distribución”. 
303.	Localice el rol de “Punto de distribución” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 

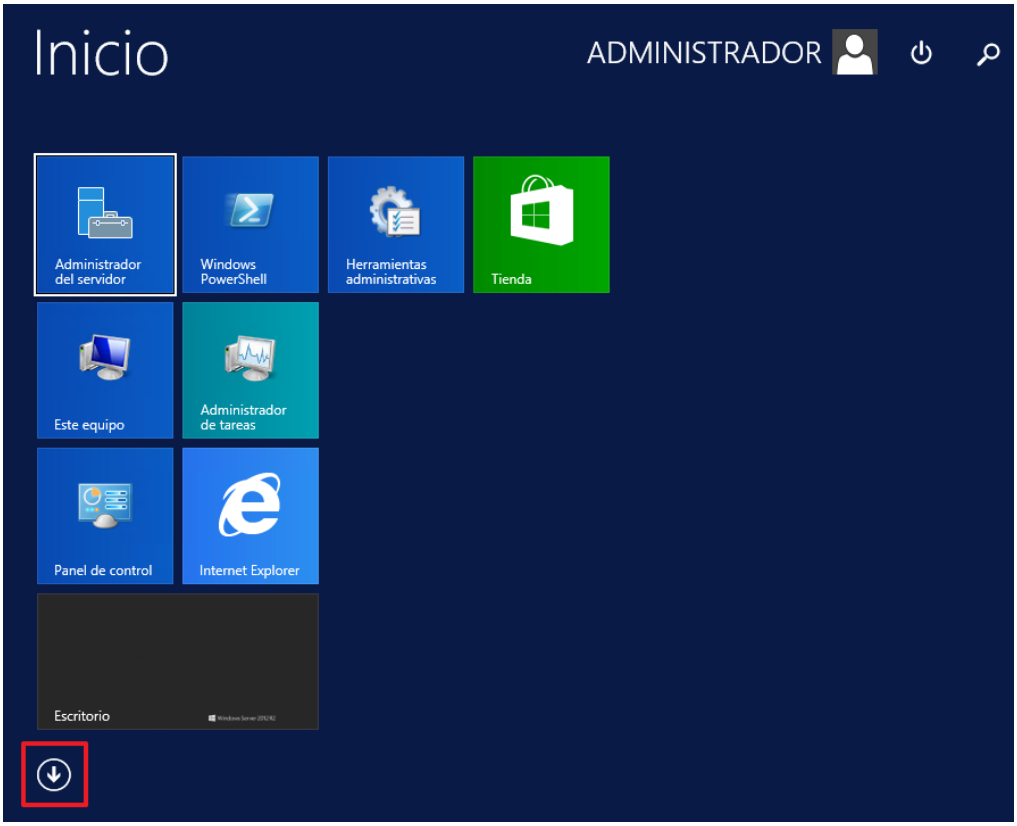
Paso	Descripción
304.	Seleccione en la pestaña “General:” la opción “HTTPS” y pulse “Aceptar” para validar los cambios. 
305.	Seleccione el servidor que contiene el rol de “Punto de punto de servicios de informes”. 

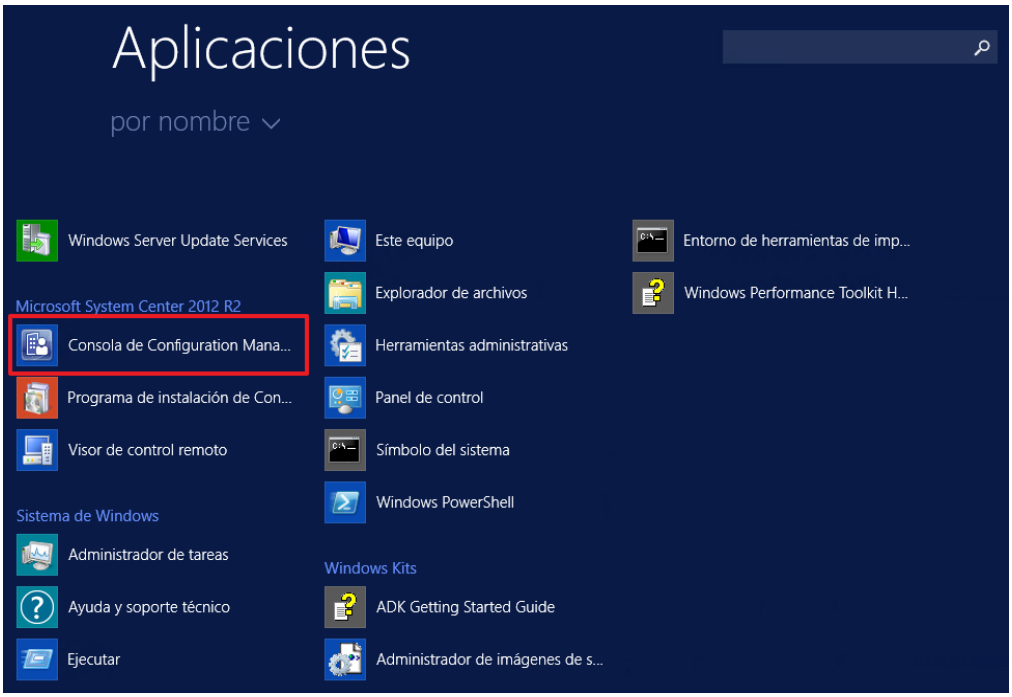
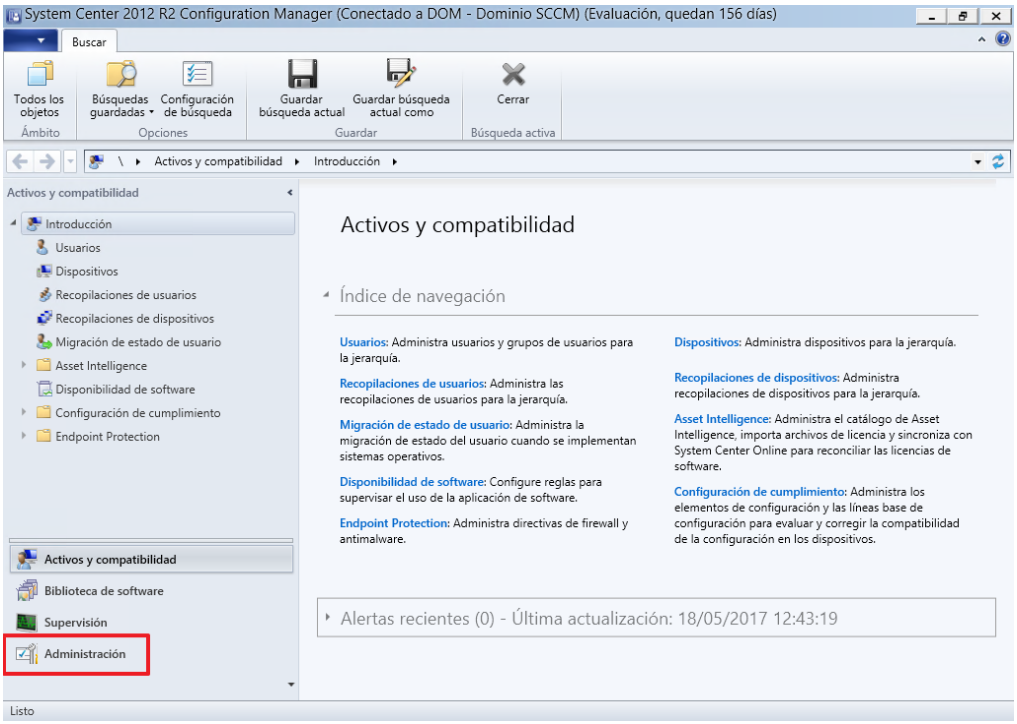
Paso	Descripción
306.	Localice el rol de “Punto de servicios de informes” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 
307.	En “General:” especifique una cuenta única de conexión del punto de servicios de informes, y pulse “Aceptar” para validar los cambios.  **Nota:** Deberá adaptar estos pasos a su organización y seleccionar un usuario con las credenciales necesarias para que efectué correctamente la conexión del punto de administración y la base de datos de SQL Server.

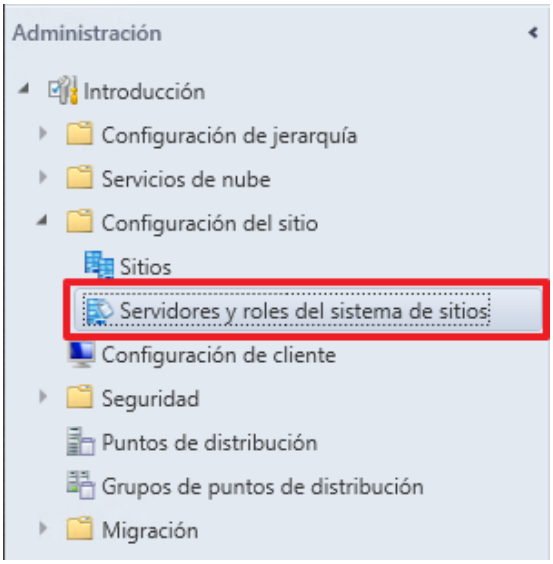
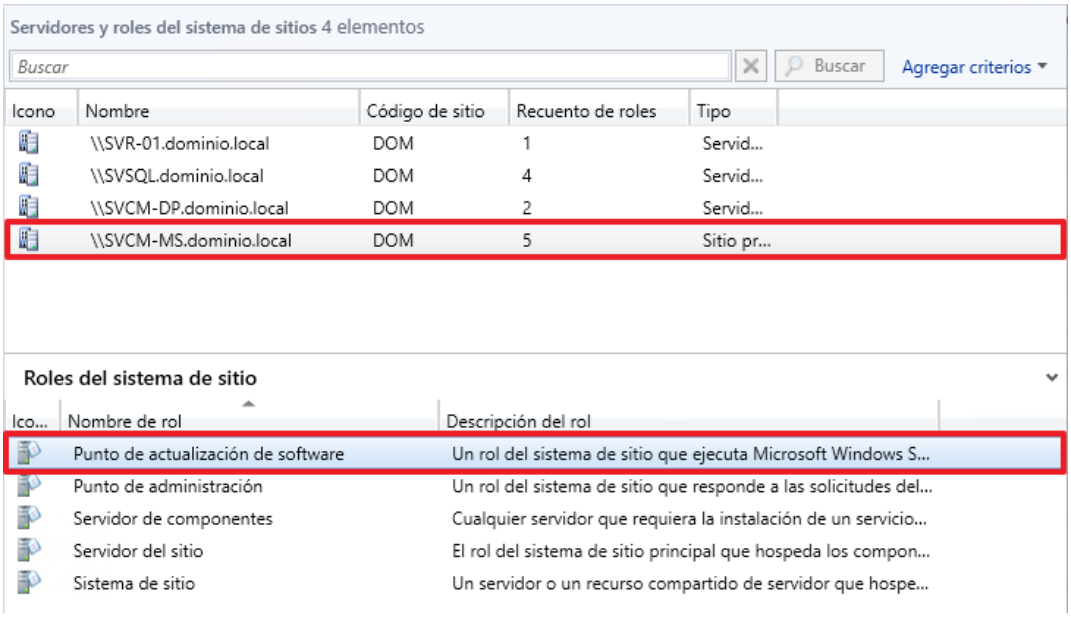
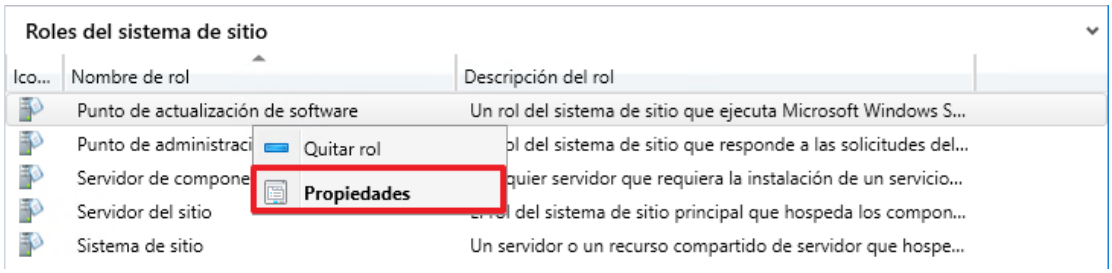
7.5. MANTENIMIENTO ACTUALIZACIONES DE SEGURIDAD

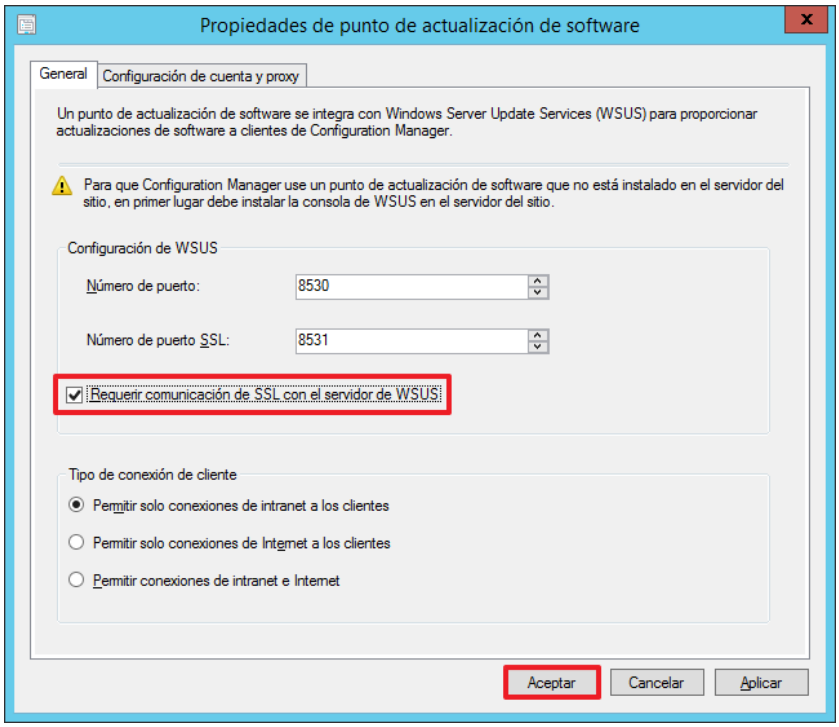
Microsoft SCCM 2012 R2 permite el administrar las actualizaciones de seguridad de clientes mediante el rol de “**Punto de actualización de software**”, estableciendo y desplegando las actualizaciones publicadas por el fabricante.

A continuación, se describe un paso a paso para configurar la comunicación con el servidor que contiene el rol de WSUS es cual es necesario para el correcto funcionamiento del rol de “**Punto de actualización de software**”.

Paso	Descripción
308.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
309.	Pulse sobre el menú inicio. 
310.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

Paso	Descripción
311.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
312.	Seleccione el apartado “Administración”. 

Paso	Descripción
313.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 
314.	Seleccione el servidor que contiene el rol de “Punto de actualización de software”. 
315.	Localice el rol de “Punto de actualización de software” y pulse con el botón derecho sobre la opción “Propiedades” del menú contextual. 

Paso	Descripción
316.	Seleccione en la pestaña “General” la opción “Requerir comunicación SSL con el servidor de WSUS” y pulse “Aceptar” para validar los cambios. 

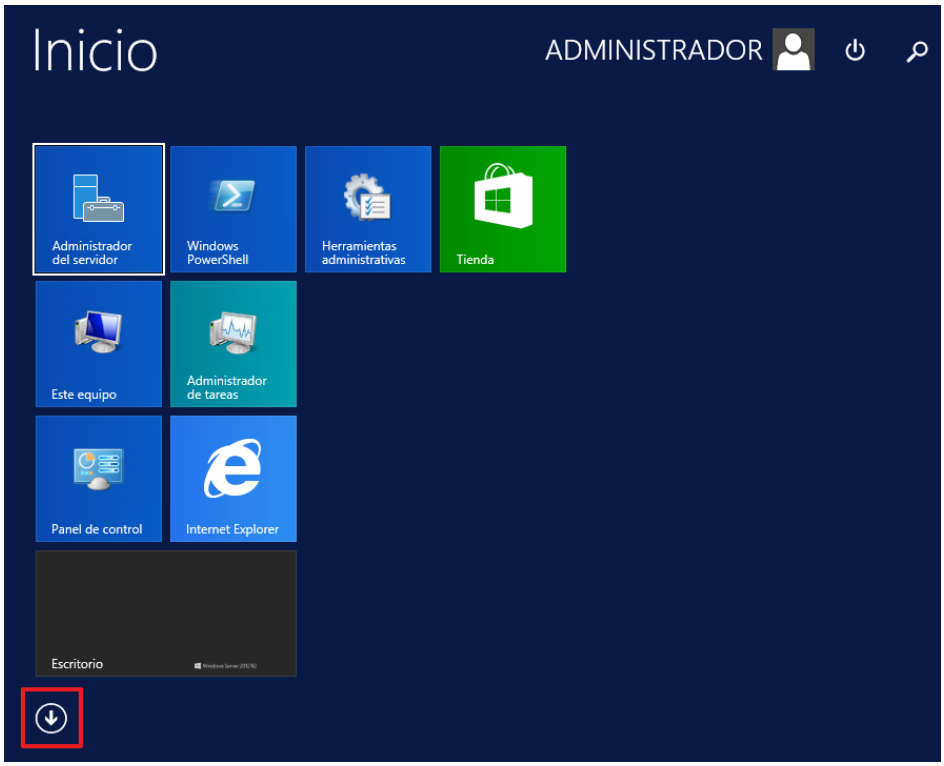
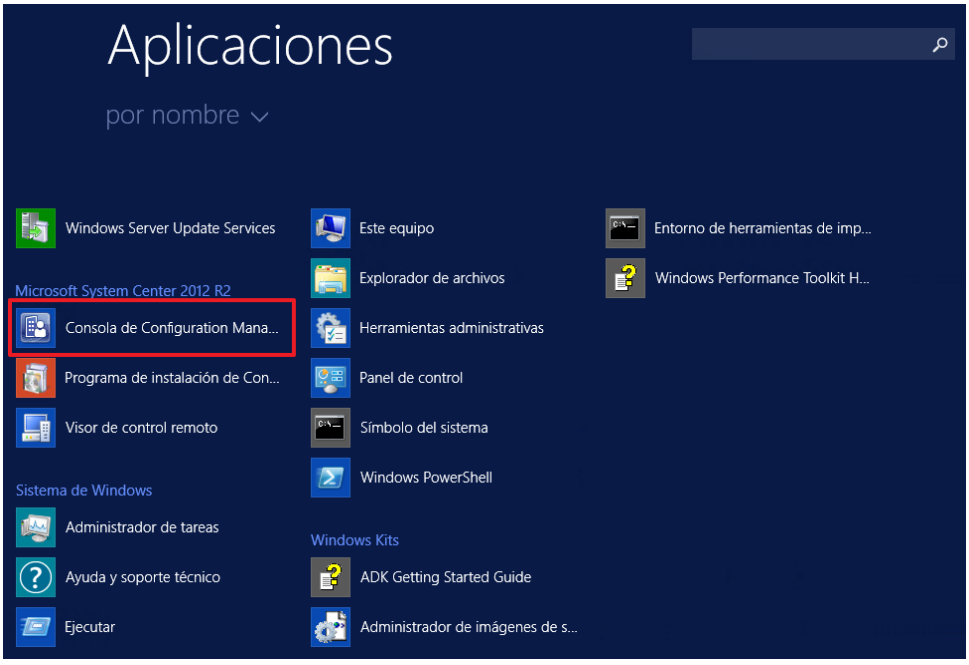
7.6. CONFIGURACIÓN HERRAMIENTAS REMOTAS

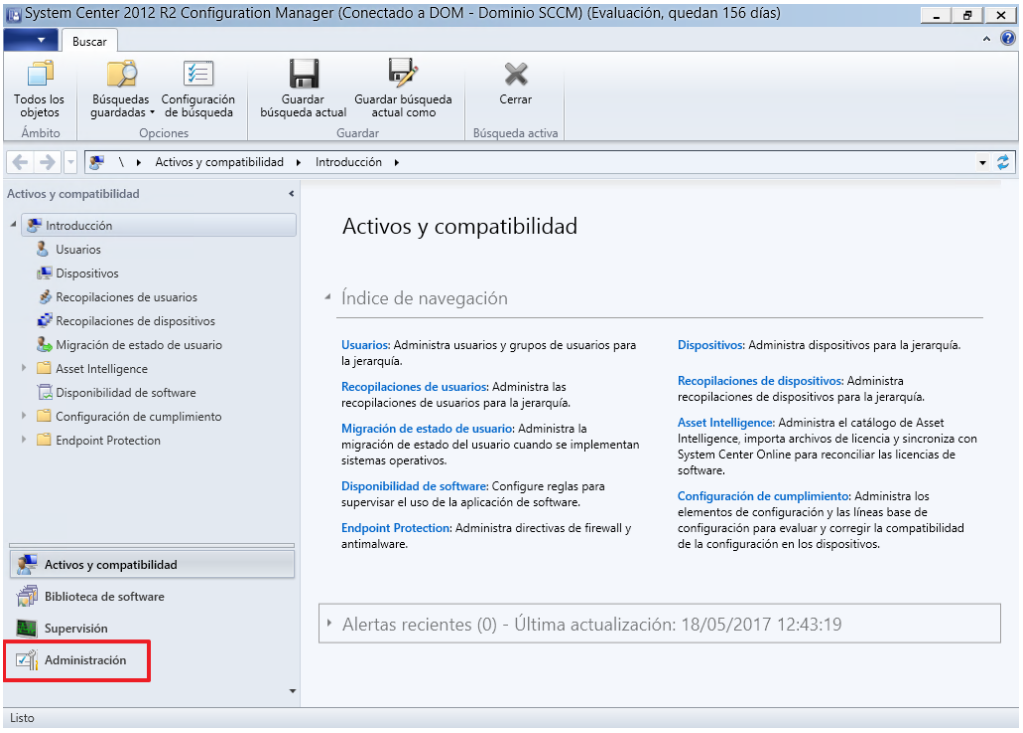
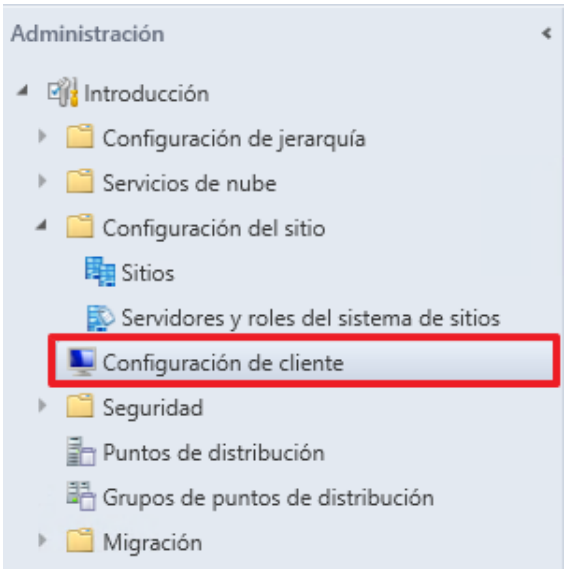
Microsoft SCCM 2012 R2 permite establecer la configuración de control remoto en equipos clientes que se aplica a todos los clientes de la jerarquía.

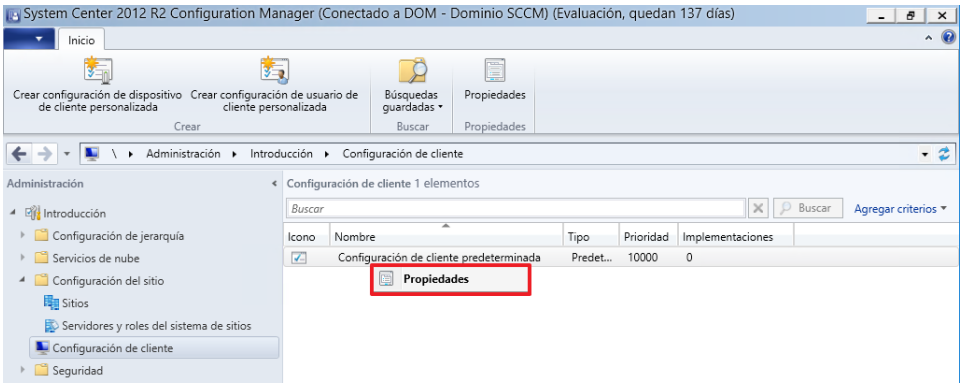
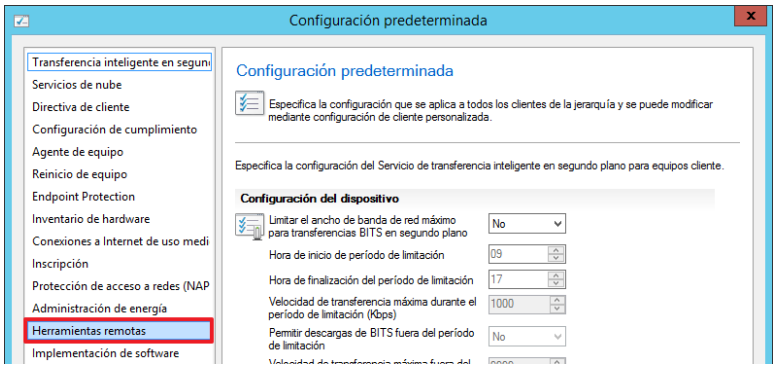
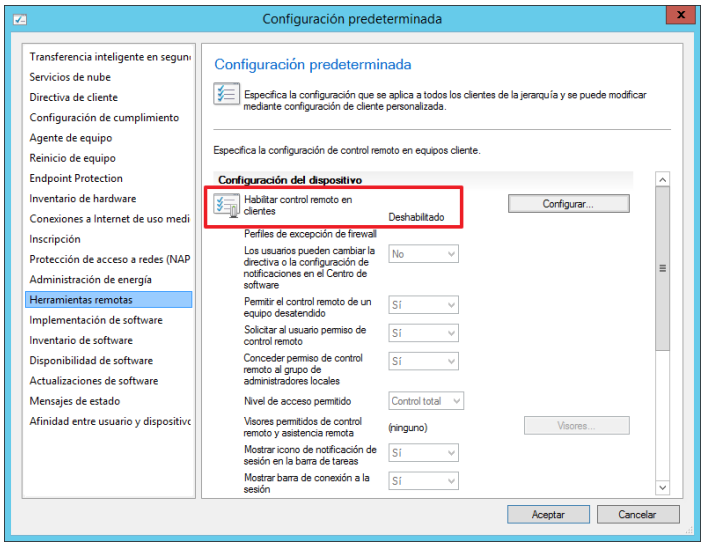
Se recomienda que esta herramienta, siempre que no sea un requisito de la organización, este en estado deshabilitado y en caso de estar habilitada, asegurarse que está configurada correctamente para que únicamente los usuarios con privilegios tengan acceso a esta característica de control remoto de equipos cliente.

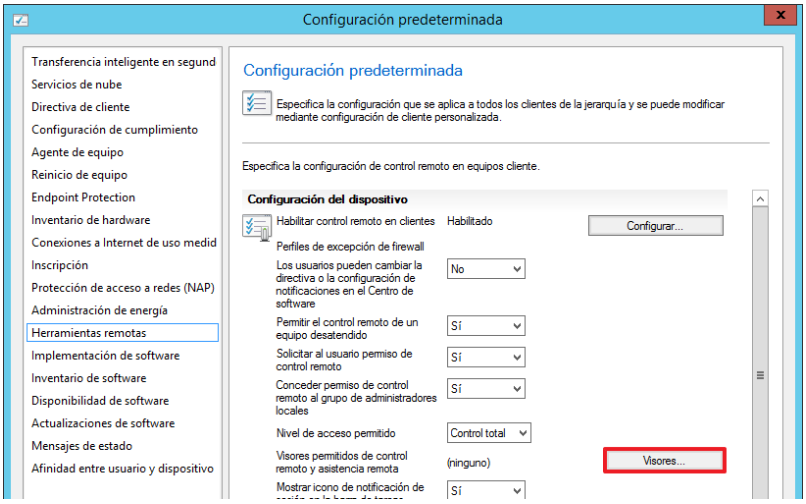
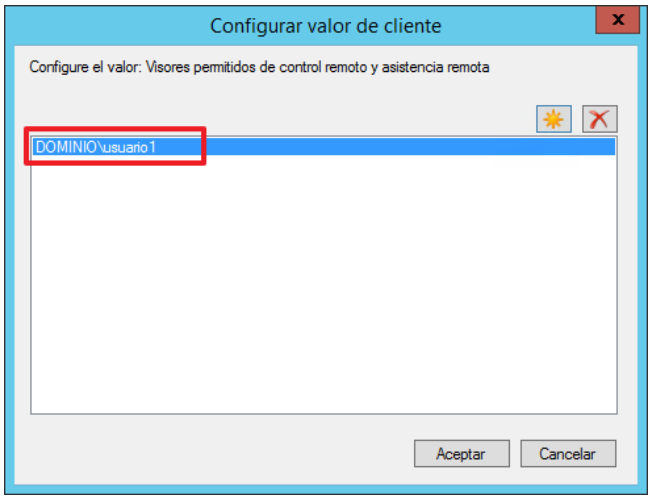
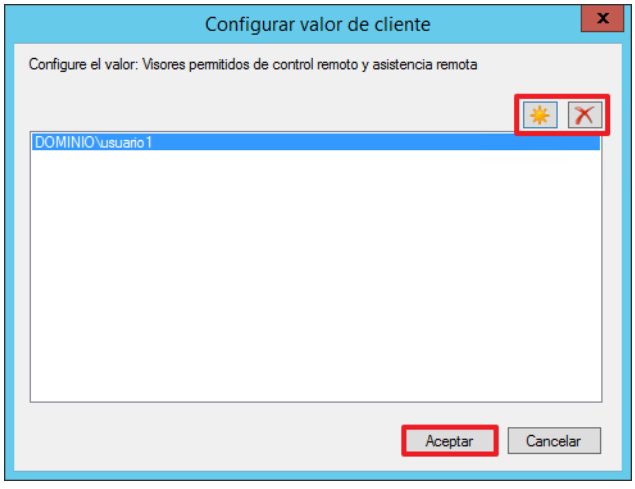
A continuación, se describe como establecer la configuración de control remoto en equipos clientes.

Paso	Descripción
317.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
318.	Pulse sobre el menú inicio. 

Paso	Descripción
319.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
320.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
321.	Seleccione el apartado “Administración”. 
322.	Despliegue “**Configuración del sitio > Configuración de cliente**”. 

Paso	Descripción
323.	Seleccione “Configuración de cliente predeterminada”, pulse con el botón derecho, y seleccione la opción “Propiedades” del menú contextual.  **Nota:** Deberá adaptar los pasos a su organización y seleccionar la configuración de cliente que se esté aplicado a sus equipos cliente.
324.	Localice el apartado “Herramientas remotas” en el menú izquierdo de la ventana de “Configuración predeterminada”. 
325.	A continuación, verifique que la opción “Habilitar control remoto en clientes” esta deshabilitado.  **Nota:** En caso que en su organización se esté haciendo uso de esta característica, y aparezca “habilitado”, deberá verificar los usuarios que tienen permisos para utilizarla.

Paso	Descripción
326.	Para comprobar los usuarios que tienen permiso de acceso remoto, pulse el botón “Visores…”. 
327.	Compruebe en el listado los usuarios que tienen permisos de control remoto. 
328.	En caso de requerir añadir o eliminar algún usuario o grupos de usuarios seleccione los dos botones situados en la parte derecha de la imagen en función de la acción que desee realizar. Pulse “Aceptar” una vez haya finalizado la configuración. 

7.7. REGISTRO DE LA ACTIVIDAD

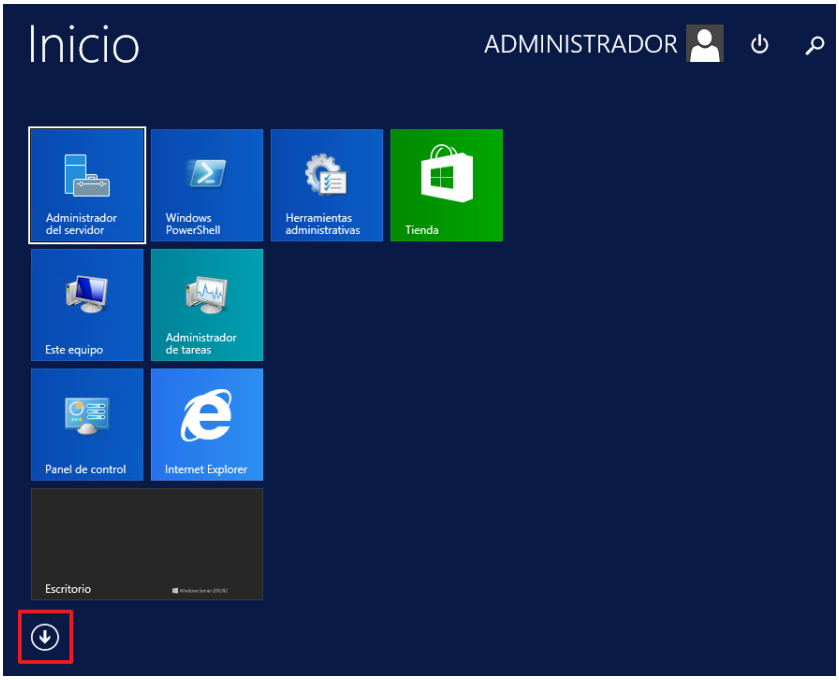
Según el ENS se registrará toda aquella evidencia que pueda, respaldar una demanda judicial, o hacer frente a ella, cuando el suceso pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos.

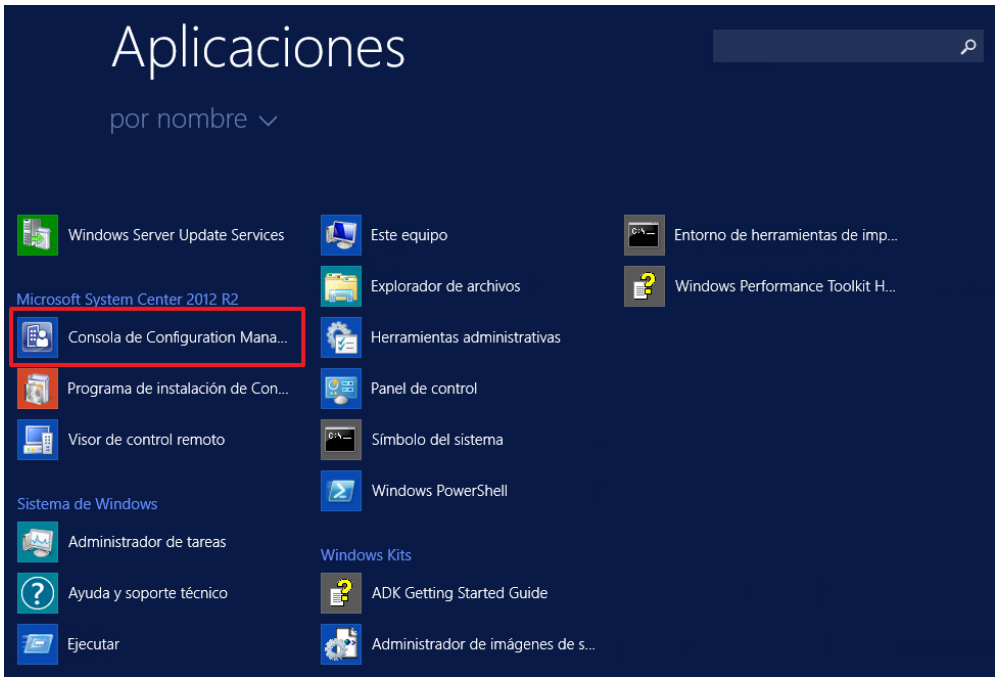
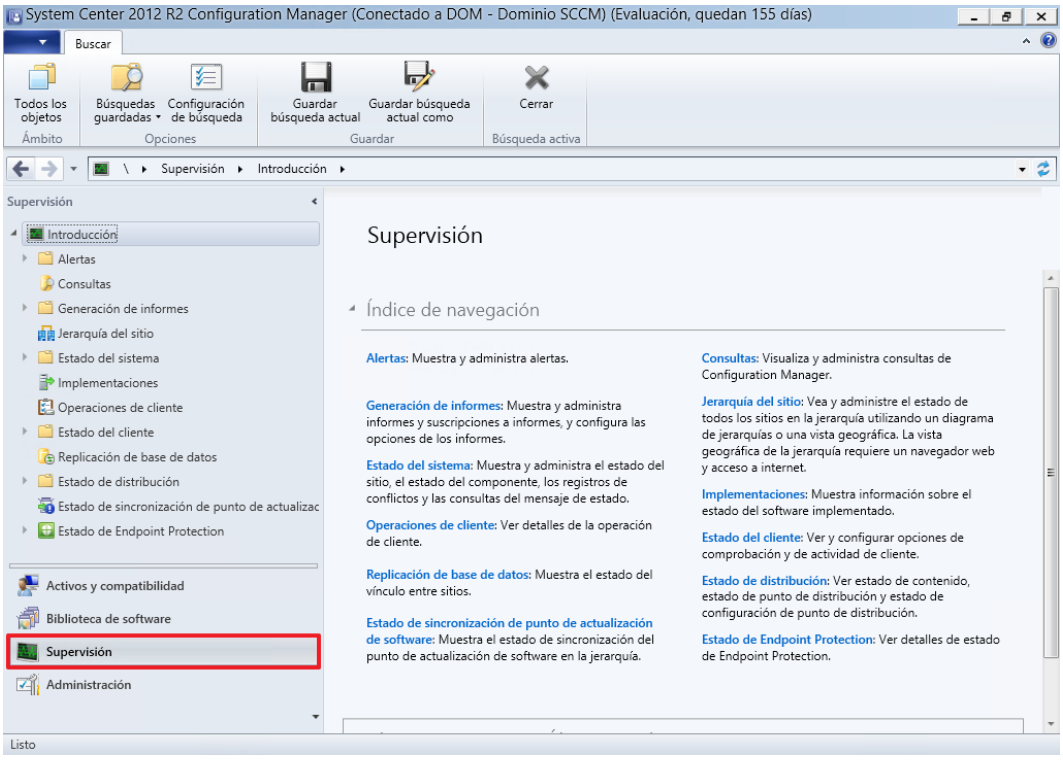
Además, se incluirá la actividad de los usuarios y, con especial atención, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

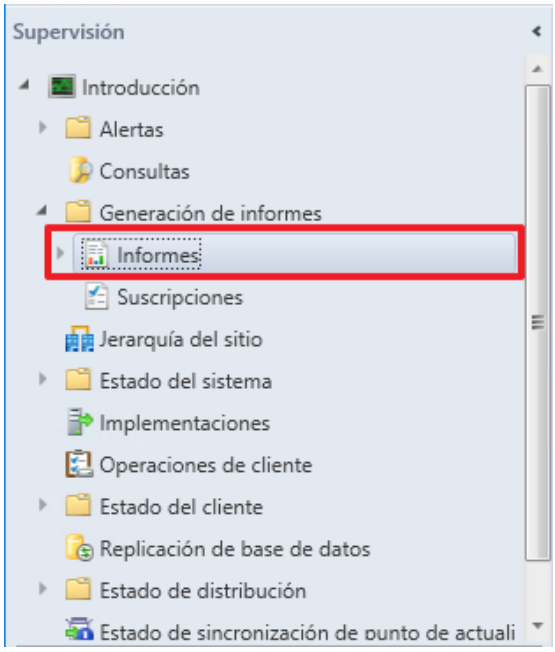
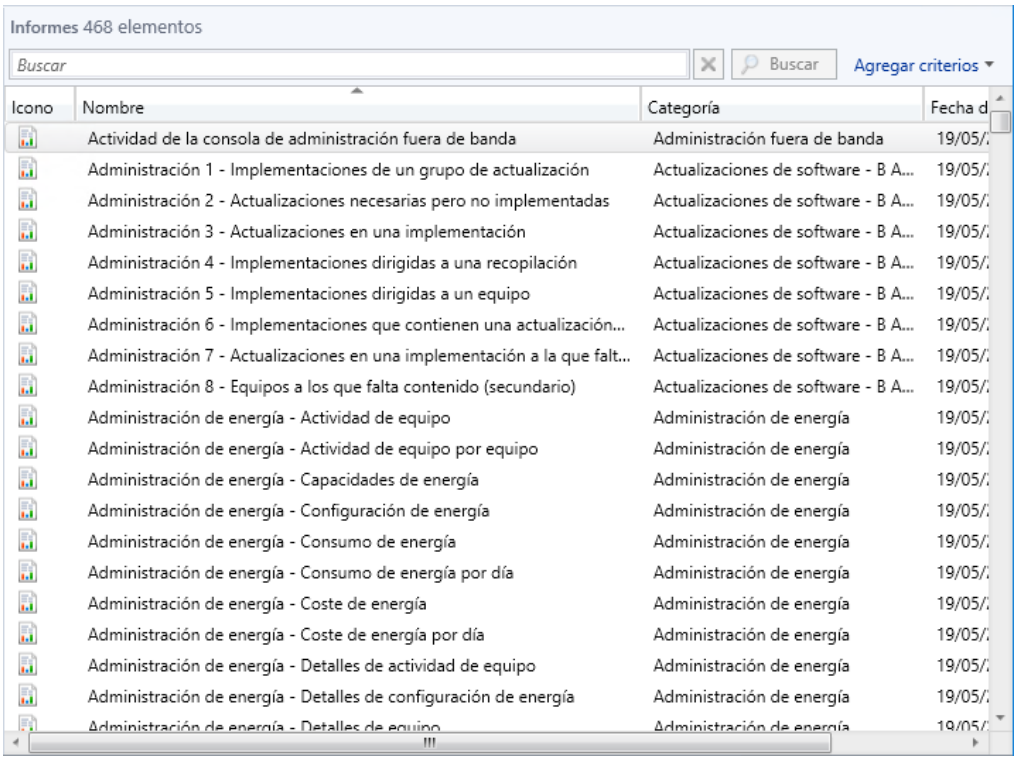
Se ha de tener en consideración que la primera medida para reforzar la seguridad es el mantenimiento y aplicación correcta de la segregación de roles y funciones limitando con ello el campo de acción de los usuarios administrativos.

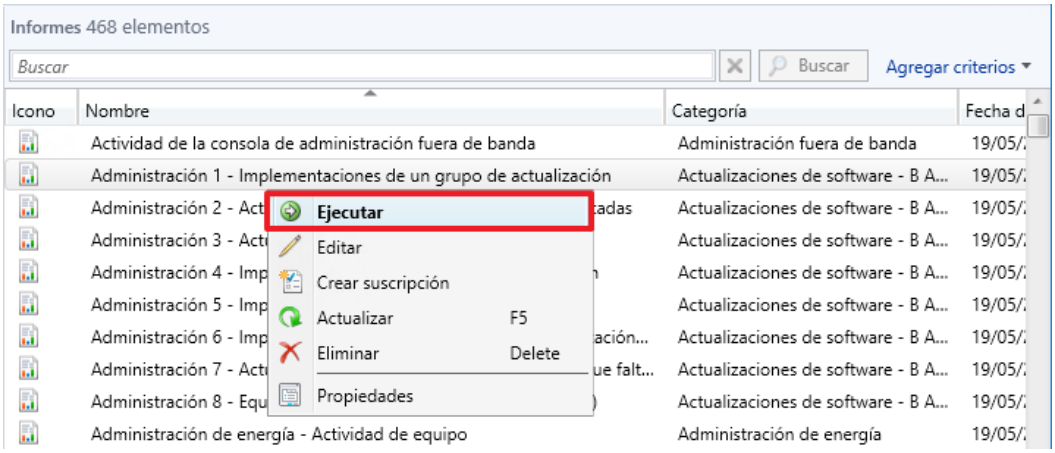
Además del registro de sucesos y evidencias es imprescindible reforzar la seguridad en el acceso a esa información registrada, evitando con ello, acciones ilícitas que puedan poner en riesgo la integridad de la información almacenada.

A continuación, se muestra un paso a paso para ver los informes de actividad de MS SCCM 2012 R2.

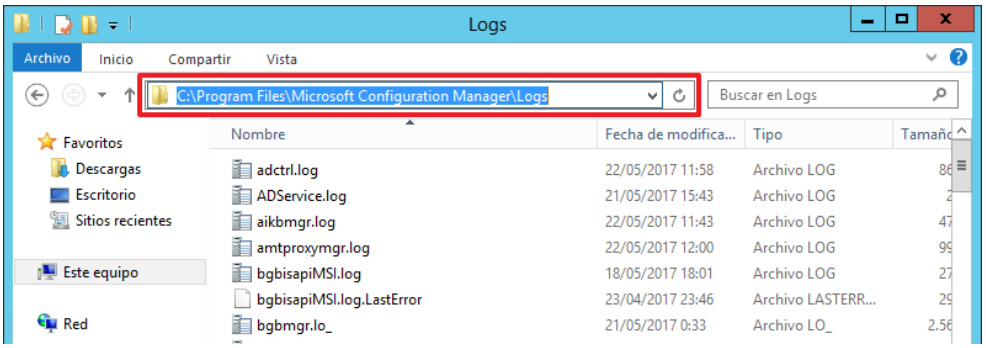
Paso	Descripción
329.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
330.	Pulse sobre el menú inicio. 
331.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 

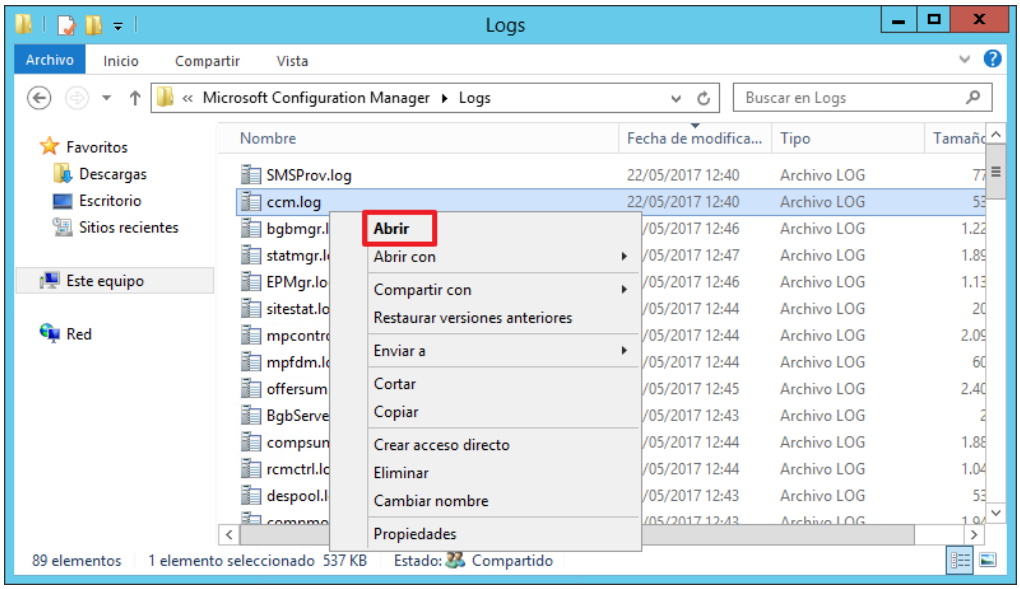
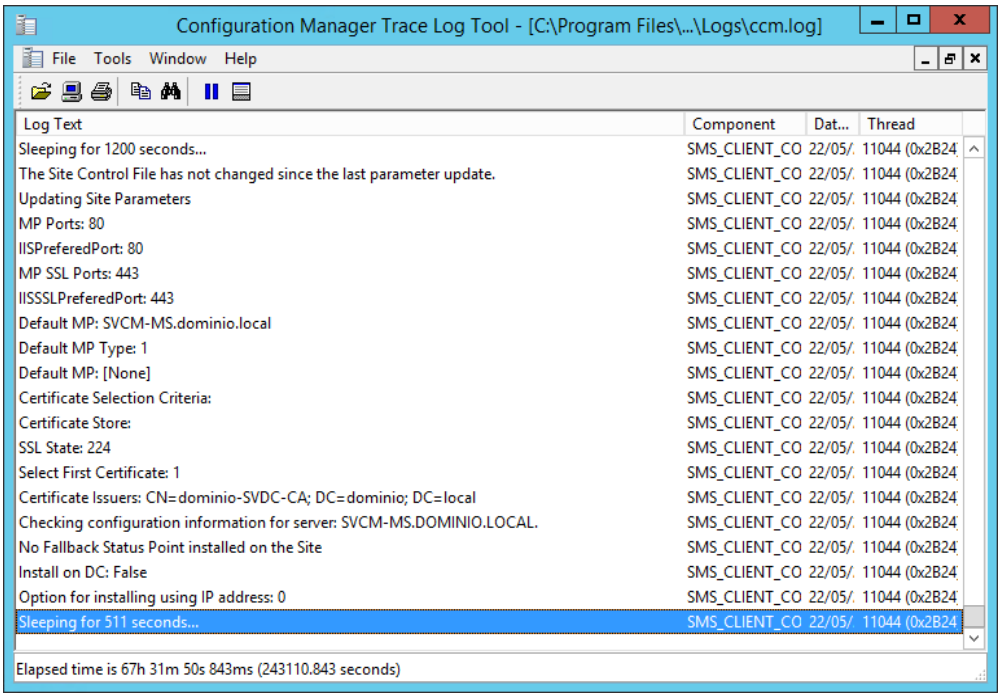
Paso	Descripción
332.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 
333.	A continuación, seleccione el apartado “Supervisión”. 

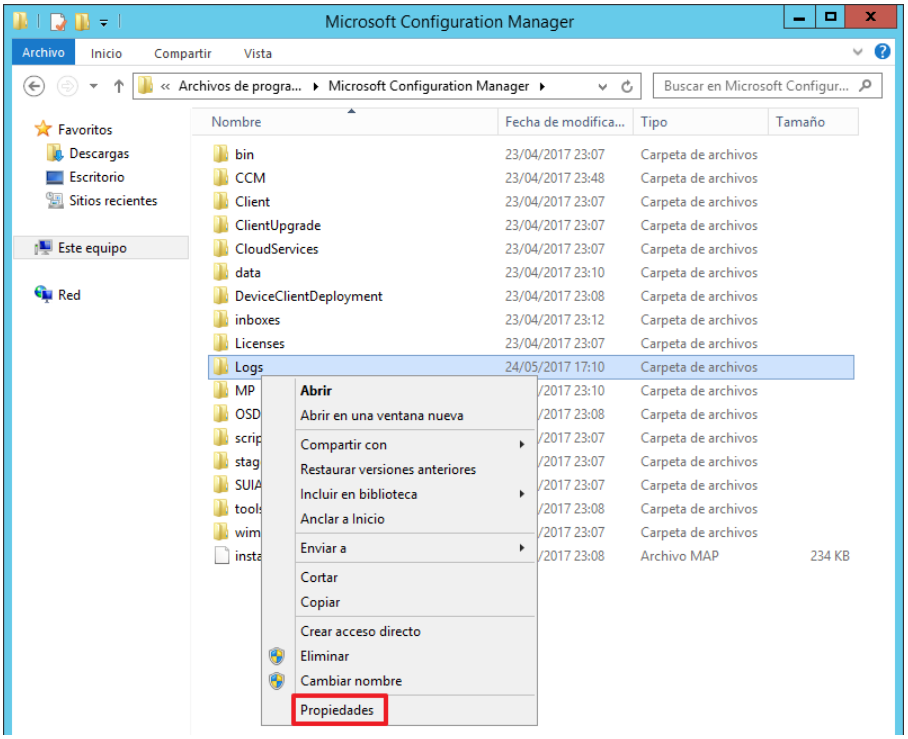
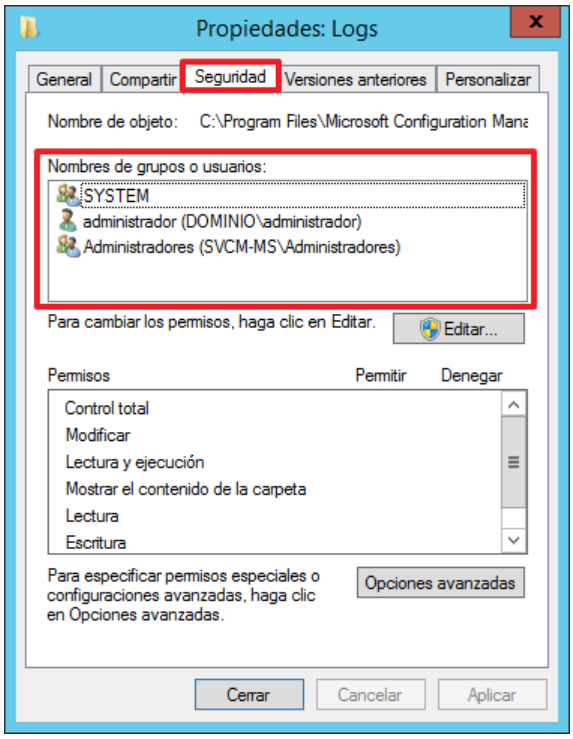
Paso	Descripción
334.	Despliegue "**Generación de informes > Informes**". 
335.	Seleccione de entre todos los informes disponibles el que más se adecue a sus necesidades. 

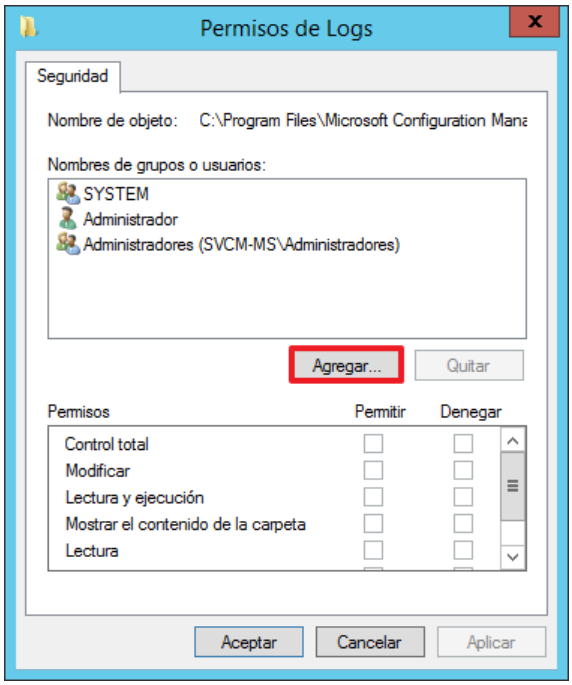
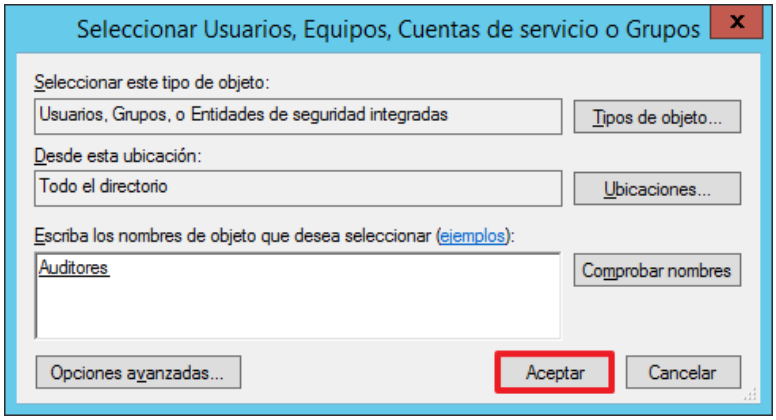
Paso	Descripción
336.	Una vez localizado, pulse con el botón derecho y seleccione la opción “Ejecutar” del menú contextual para visualizar los datos del informe seleccionado.  **Nota:** En este ejemplo se selecciona el informe “Administración 1 – Implementaciones de un grupo de actualización” por lo que deberá adaptar los pasos a las necesidades de su organización.

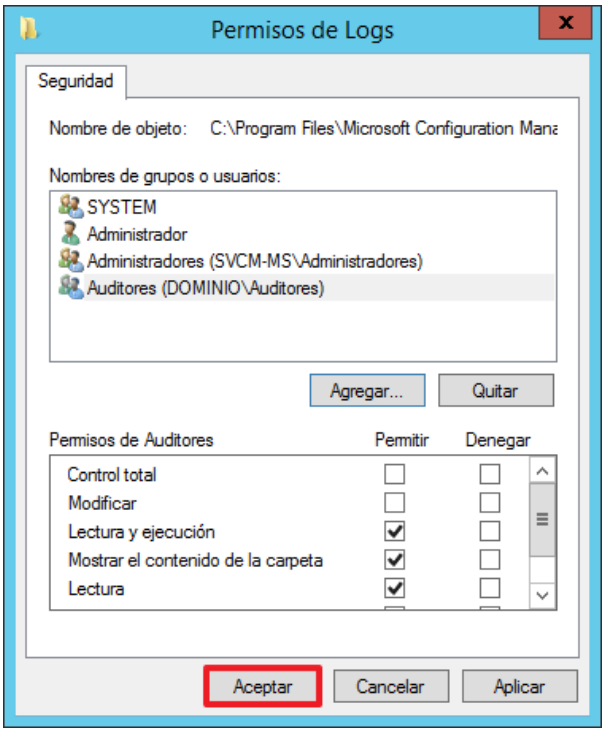
Además de los informes presentados en MS SCCM 2012 R2 es posible consultar la actividad del servicio a través de los registros los cuales ofrecen una información más detallada de lo que puede estar sucediendo o buscar evidencias de acciones realizadas.

Paso	Descripción
337.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
338.	Pulse sobre el menú inicio y seleccione el icono “Explorador de archivos”. 
339.	Localice la ruta “C:\Program Files\Microsoft Configuration Manager\Logs”.  **Nota:** La ruta que contiene los registros puede variar en función de la ubicación de la instalación del producto MS SCCM 2012 R2.

Paso	Descripción
340.	Seleccione el archivo.log que más se adecue a sus necesidades y haga clic botón derecho, y seleccione la opción “Abrir” del menú contextual. 
341.	En la siguiente imagen, se muestra un ejemplo del fichero “ccm.log”.  **Nota:** En la imagen se visualiza el log mediante la herramienta propia de Configuration Manager Trace log tool, siendo posible utilizar cualquier editor de textos para su lectura.

Paso	Descripción
342.	Seguidamente, se va a proceder a reforzar la seguridad de la carpeta que contiene los registros para ello, deberá ubicarse en la dirección "C:\Program Files\Microsoft Configuration Manager". Marque la carpeta "Logs", pulse con el botón derecho y seleccione la opción "Propiedades" del menú contextual. 
343.	Seleccione la pestaña "Seguridad" y compruebe que únicamente los usuarios imprescindibles tienen acceso a la carpeta y su contenido. 

Paso	Descripción
344.	A modo de ejemplo se va a proceder a agregar un grupo de usuarios los cuales se les concederá permisos de lectura sobre la carpeta “Logs”. Deberá adaptar los próximos pasos adecuándolos a los requerimientos de su organización. Pulse sobre el botón “Agregar”. 
345.	Agregue los usuarios o grupos de usuarios a los que desee conceder acceso y pulse “Aceptar”.  **Nota:** En el presente ejemplo se agrega el grupo de seguridad “Auditores”, deberá adaptar estos pasos a su organización y únicamente agregar los usuarios que necesiten acceso a la carpeta.

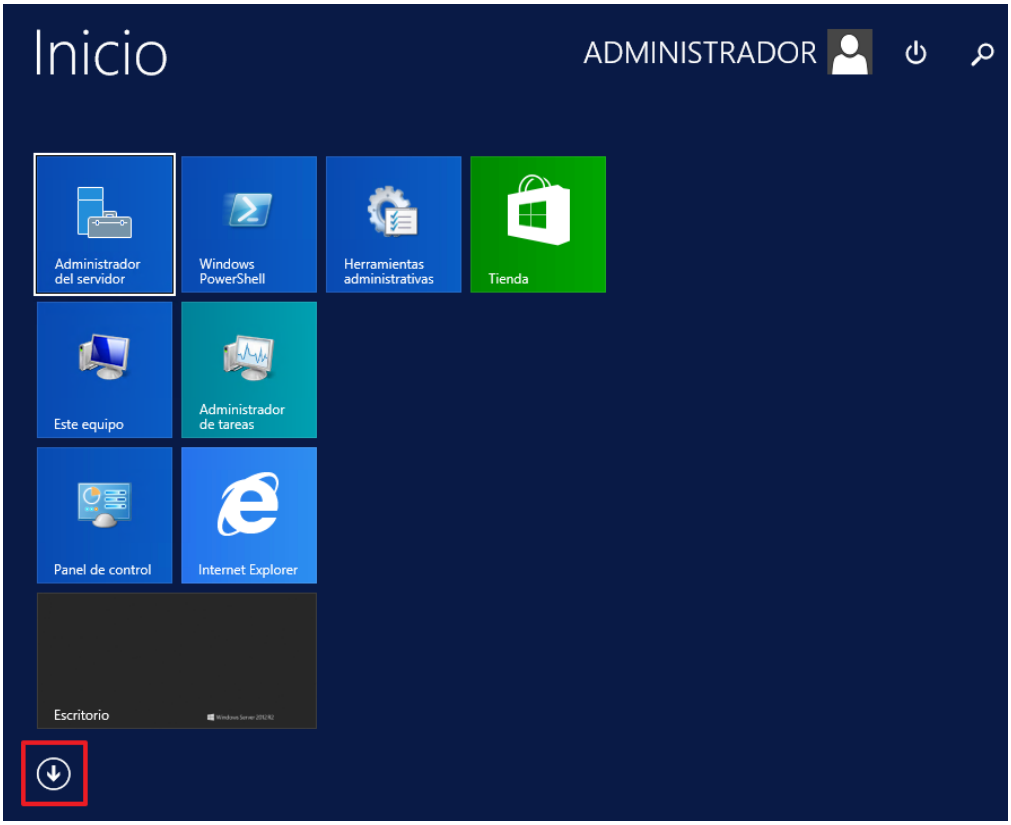
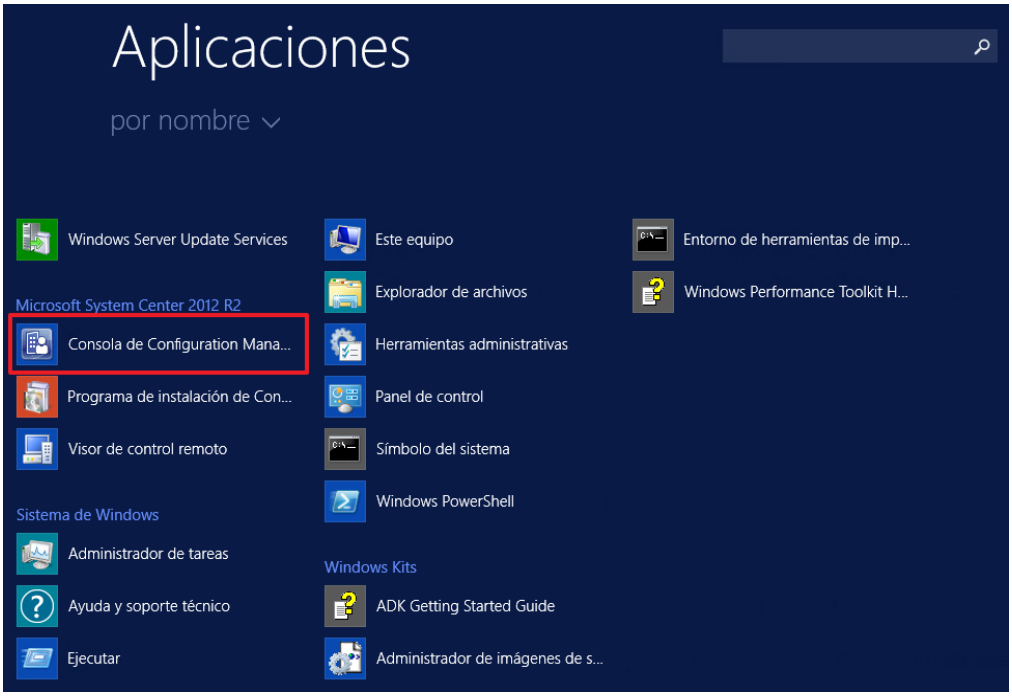
Paso	Descripción
346.	Compruebe que el usuario o grupo de usuarios tiene únicamente permisos de lectura y pulse “Aceptar” para finalizar la configuración. 

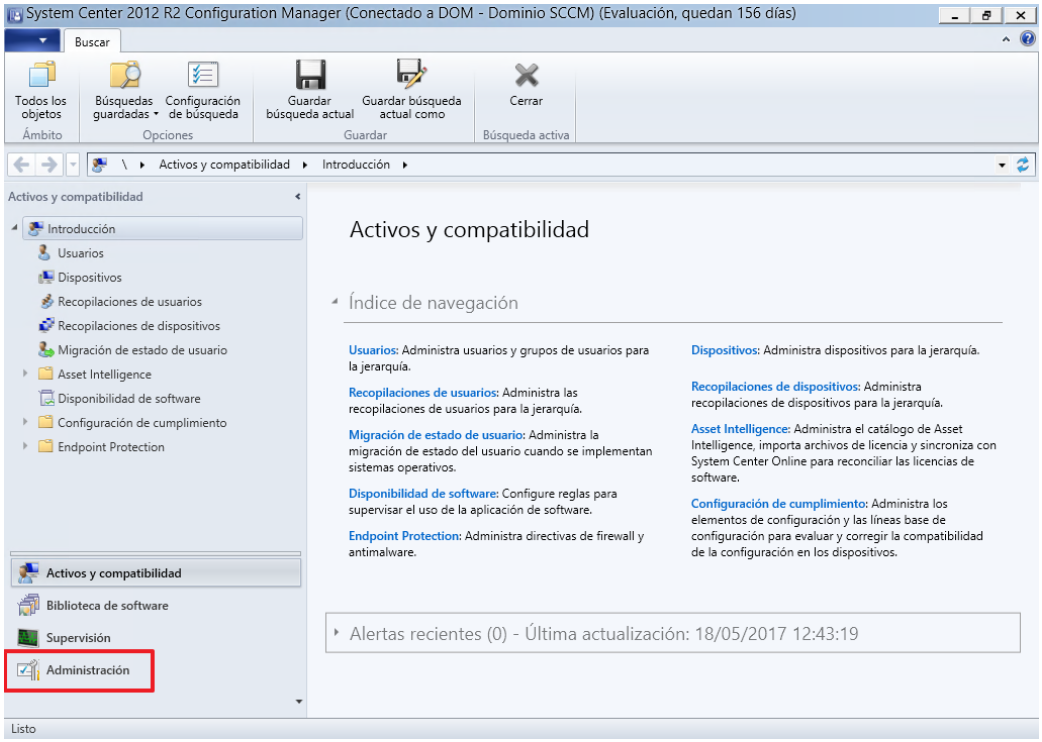
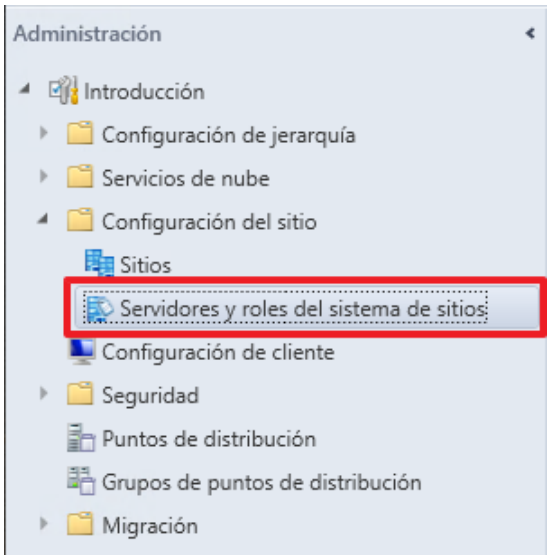
7.8. IMPLEMENTACIÓN DE SERVIDORES Y ROLES DEL SISTEMA DE SITIO

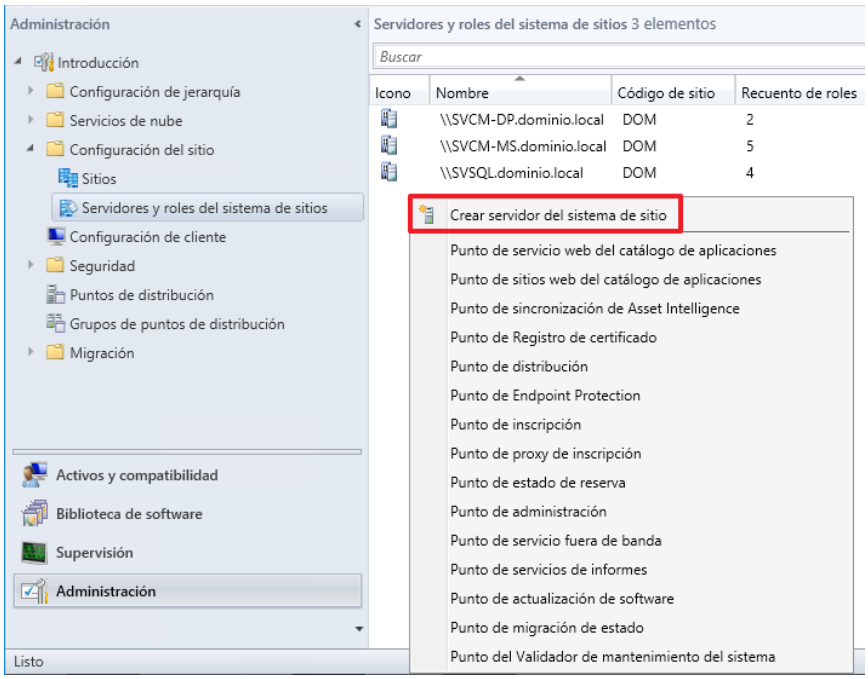
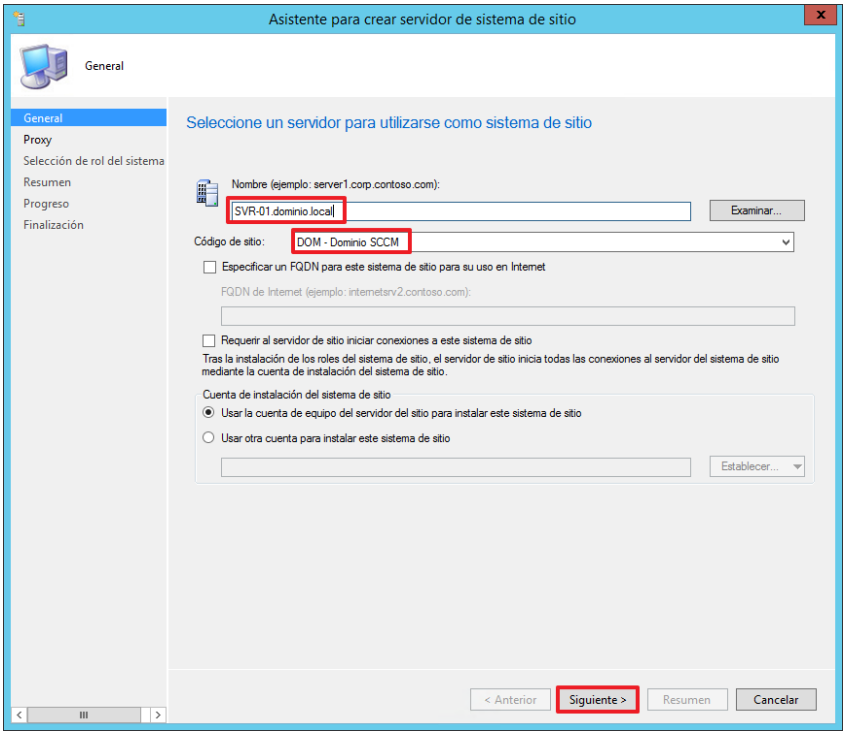
En MS SCCM 2012 R2 es posible agregar múltiples servidores que contengan varios roles para garantizar un servicio de alta disponibilidad, para en caso de que fallen los medios habituales de comunicación existan alternativas que garanticen el servicio, por lo que un mismo rol del sistema de sitio, como por ejemplo el rol de punto de distribución, es posible implementarlo en varios servidores, disponiendo con ello del mismo servicio en distintos servidores.

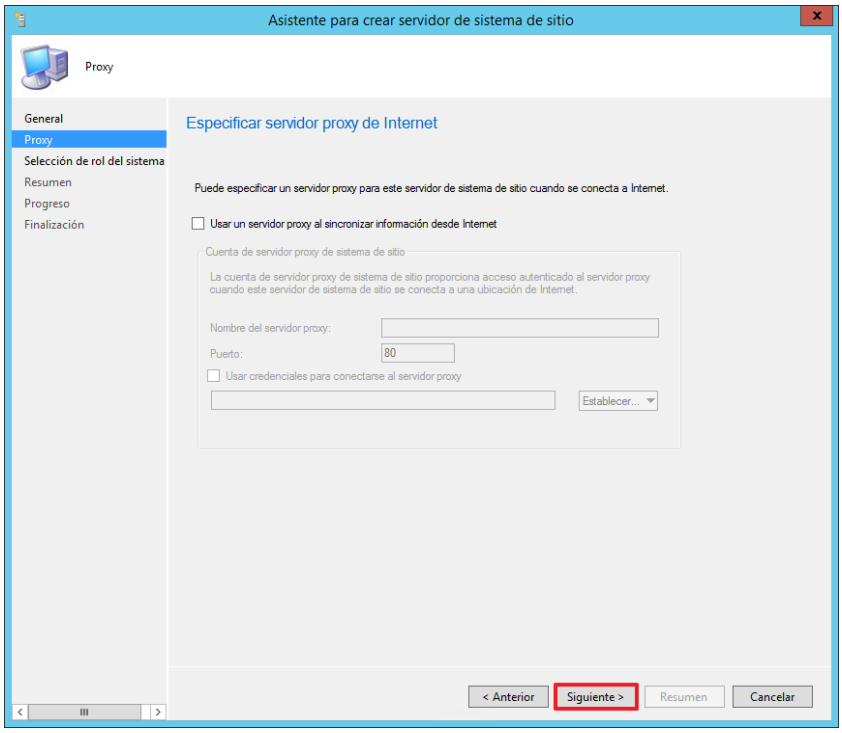
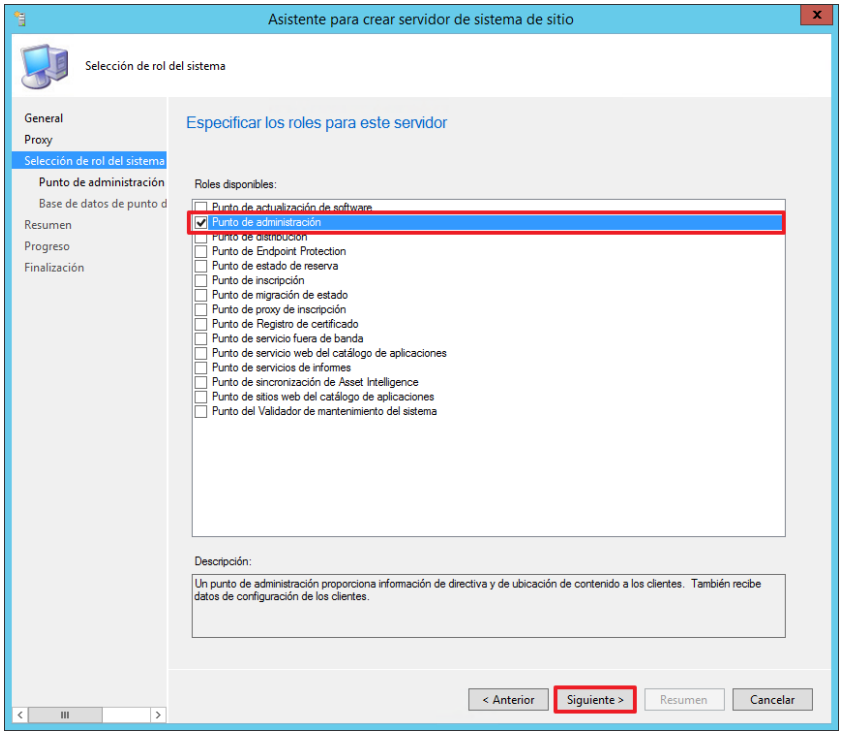
A continuación, se muestra un paso a paso en el que se detalla como agregar un servidor y a su vez como agregar un rol de sitio de MS SCCM 2012 R2.

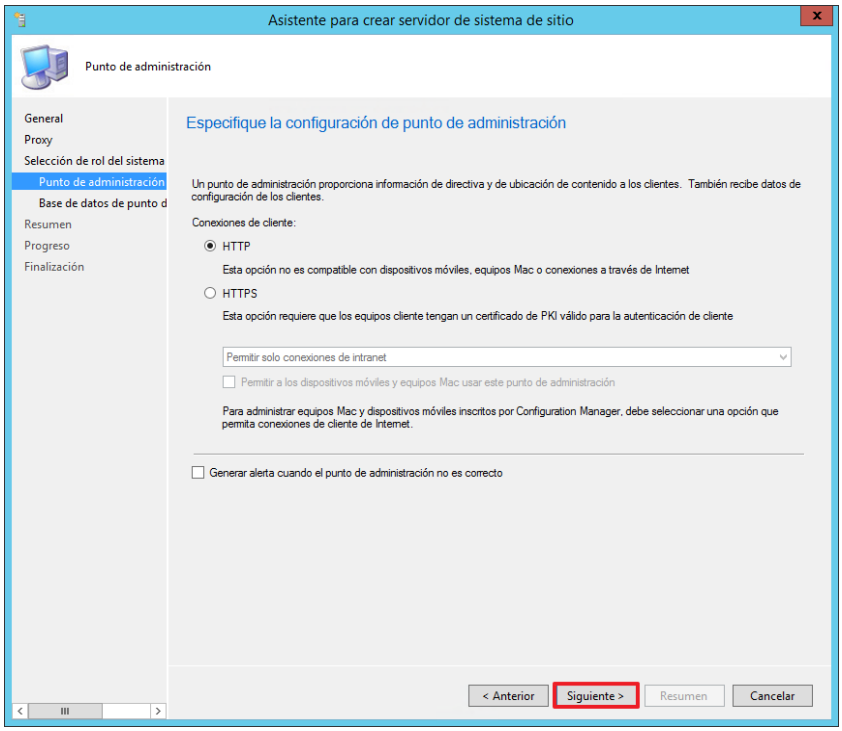
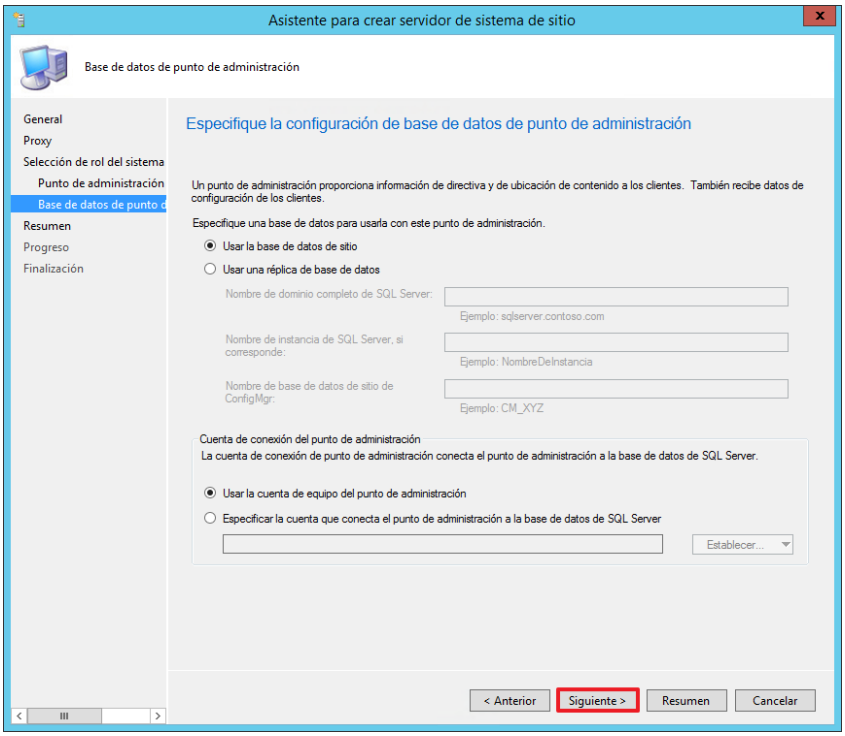
Paso	Descripción
347.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
348.	Pulse sobre el menú inicio. 

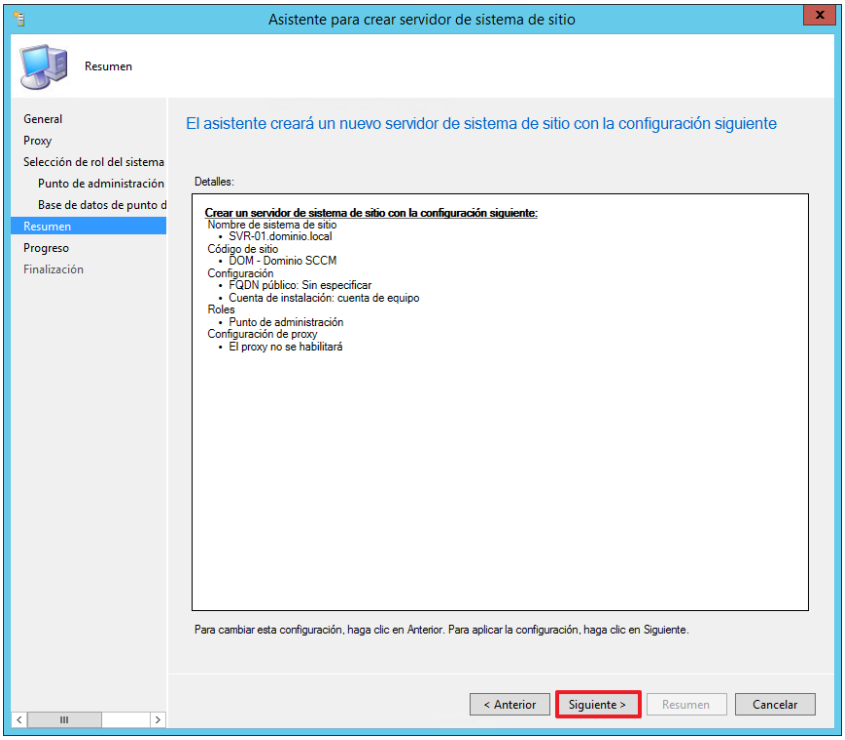
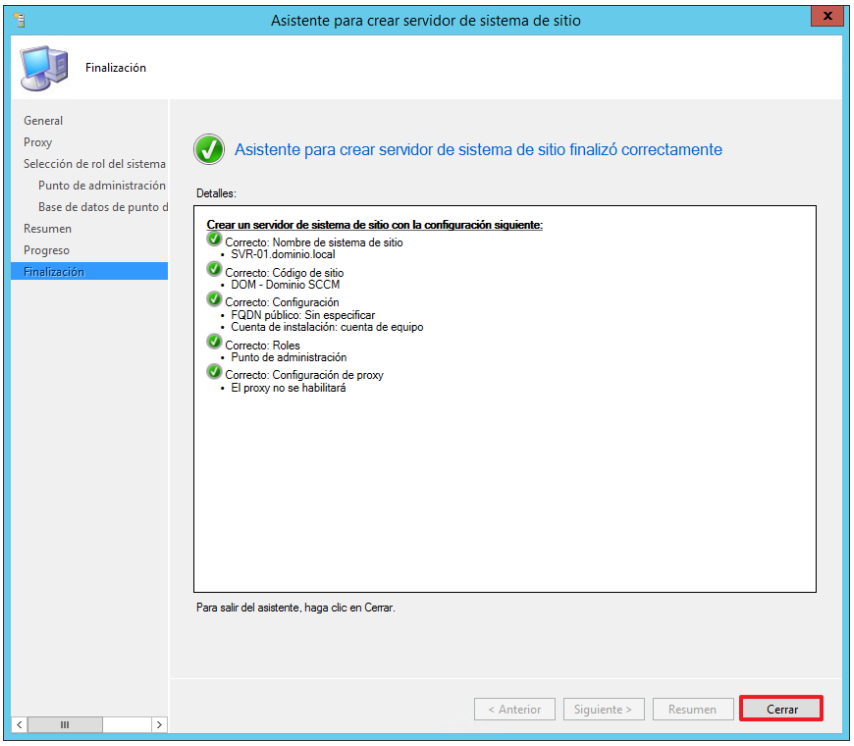
Paso	Descripción
349.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
350.	Haga clic con el ratón sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

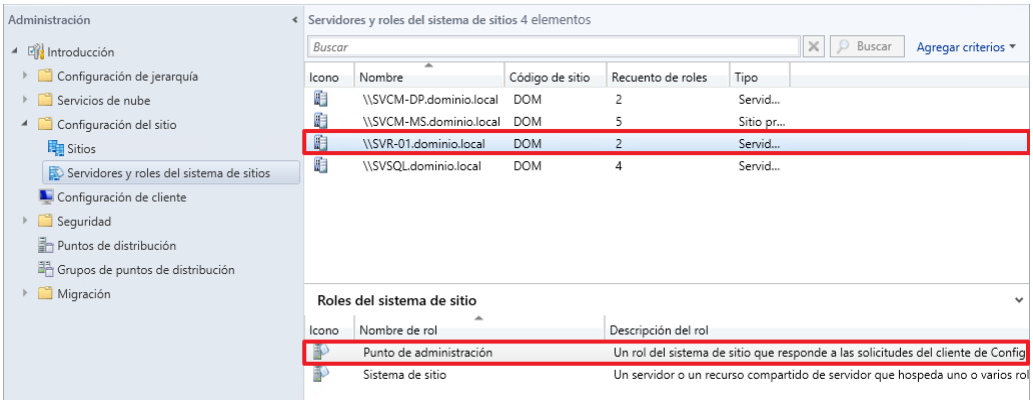
Paso	Descripción
351.	Seleccione el apartado “Administración”. 
352.	Despliegue “**Configuración del sitio > Servidores y roles del sistema de sitios**”. 

Paso	Descripción
353.	Pulse con el botón derecho sobre un espacio en blanco y seleccione la opción “crear servidor del sistema de sitio” para agregar un nuevo servidor al sitio ya creado.  **Nota:** Este paso contempla que usted ya tiene un sitio creado anteriormente y un servidor preparado para ser unido al sitio de Configuration Manager.
354.	Seleccione el nombre del servidor que desea añadir y el sitio y pulse “Siguiente >”  **Nota:** Tanto el nombre del servidor como el del sitio han sido creados para elaborar la presente guía por lo que deberá adaptar estos pasos a su organización.

Paso	Descripción
355.	En caso de que su servidor se conecte a internet a través de un proxy deberá configurar la presente pantalla, y pulsar “Siguiente >” para continuar. 
356.	Seleccione el rol del sistema de sitio que quiere implementar en dicho servidor y pulse “Siguiente >”.  **Nota:** En el presente ejemplo se implementa el rol de “Punto de administración”, deberá adaptar estos pasos a los requerimientos de su organización.

Paso	Descripción
357.	En los siguientes pasos, se va a establecer una configuración específica para el rol de “Punto de administración”, en caso de haber seleccionado otro rol del sistema de sitio deberá adaptar estos pasos a su organización. Pulse “Siguiente >” para continuar. 
358.	Para avanzar con la configuración del rol del sistema de sitio. Pulse “Siguiente >” para continuar. 

Paso	Descripción
359.	Pulse “Siguiente >” para continuar con la implementación. 
360.	Compruebe que se ha creado el servidor de sitio correctamente y pulse “Cerrar” para finalizar el asistente. 

Paso	Descripción
361.	Una vez realizada la implementación del servidor y del rol del sistema de sitio, verifique que el proceso ha sido correcto. 

7.9. BORRADO Y DESTRUCCIÓN

Las medidas de borrado y destrucción de información se aplicarán a todo tipo de equipos susceptibles de almacenar información.

MS SCCM 2012 R2 no permite eliminar una base de datos directamente por lo que será necesario iniciar sesión en el servidor que aloje la base de datos de sitio. Se debe tener en consideración que el usuario que realiza la acción debe tener los permisos adecuados y una vez desvinculado se deberá eliminar físicamente la carpeta contenedora de la información, y si desea eliminar el soporte de dicha información deberá proceder siguiendo el procedimiento marcado en el borrado y destrucción de soportes físicos que establece el ENS.

Nota: Si desea obtener más información sobre el borrado de bases de datos de Microsoft SQL Server puede visitar el sitio web: https://technet.microsoft.com/es-es/library/ms177419(v=sql.110).aspx

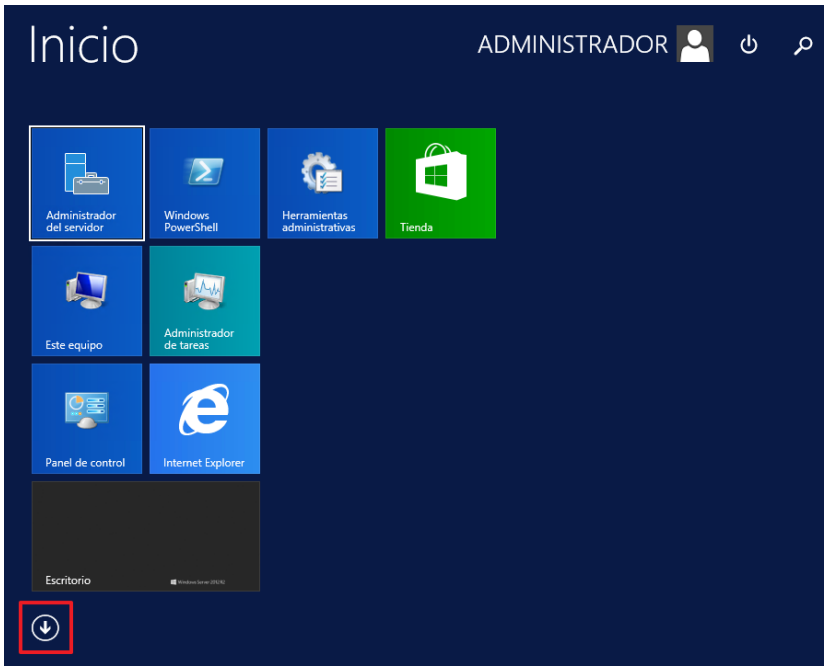
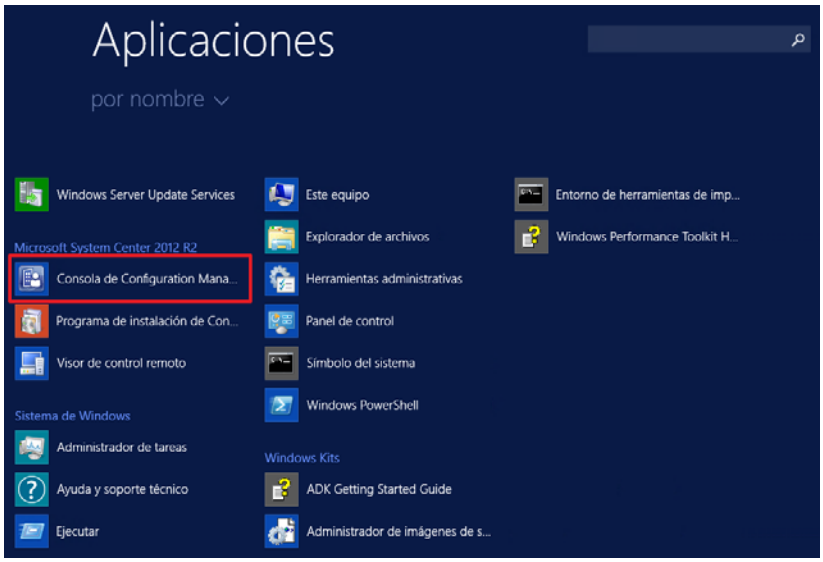
7.10. COPIAS DE SEGURIDAD

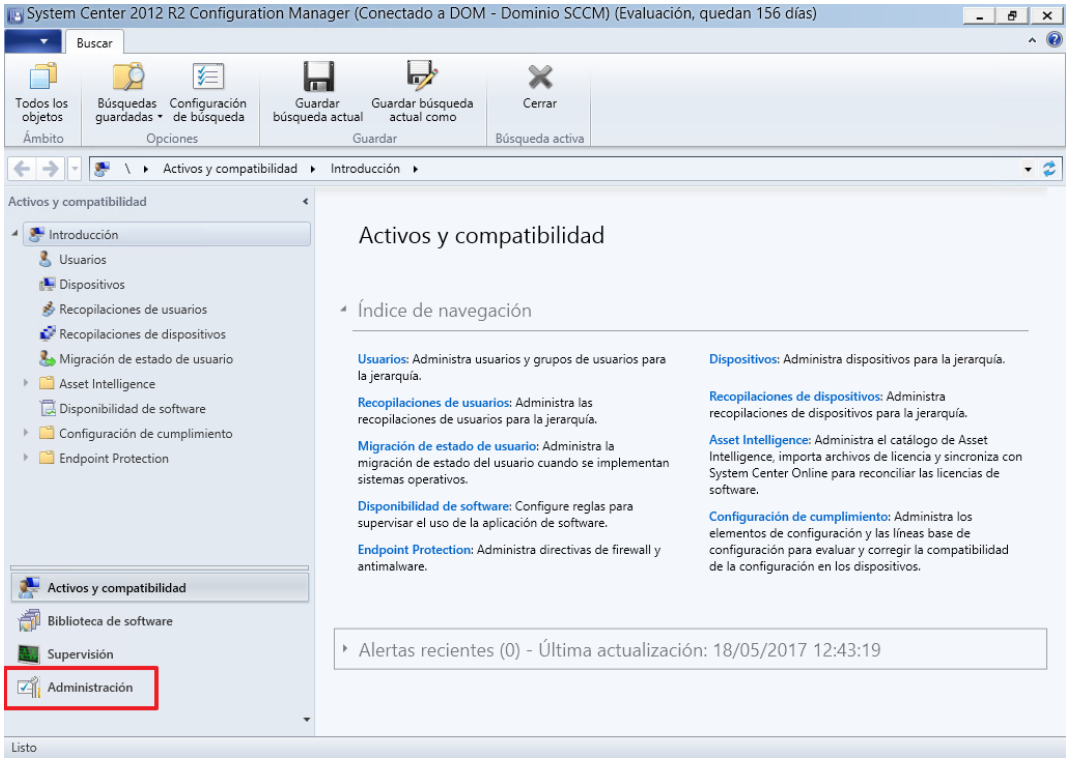
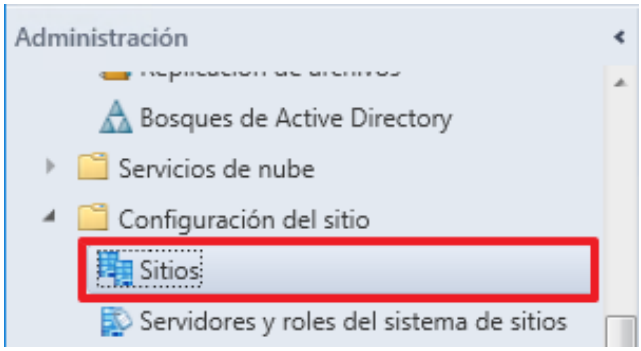
MS SCCM 2012 R2 permite realizar copias de seguridad de los sitios, así como de las bases de datos de los sitios, para en caso de desastre, tener la posibilidad de restaurar el sistema en el menor tiempo posible y minimizar al máximo una posible pérdida de información.

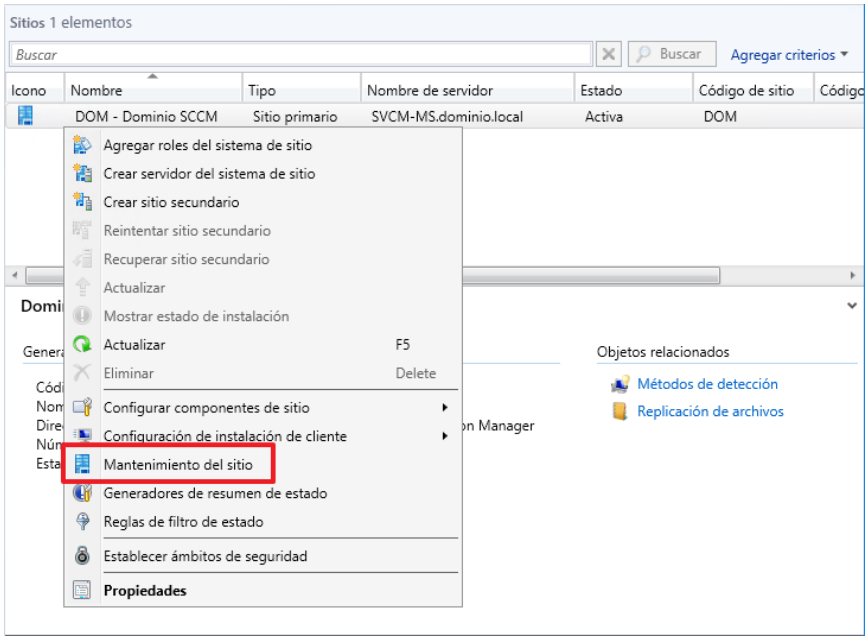
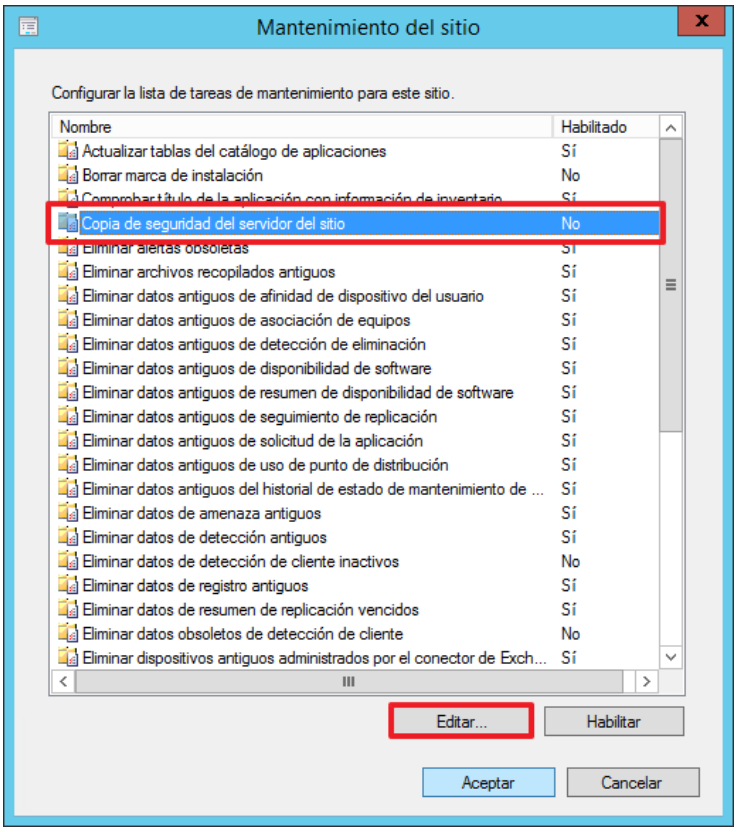
Tal y como se establece en el ENS las copias de seguridad conservarán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad.

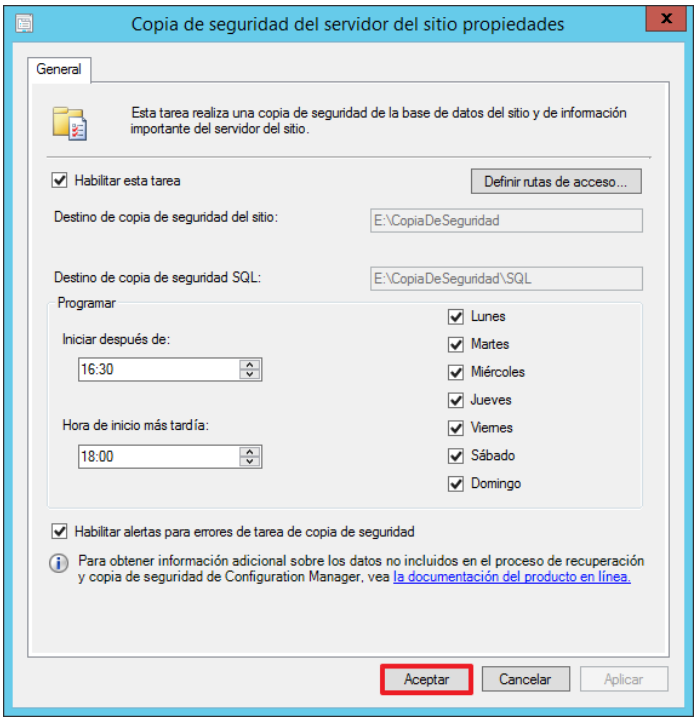
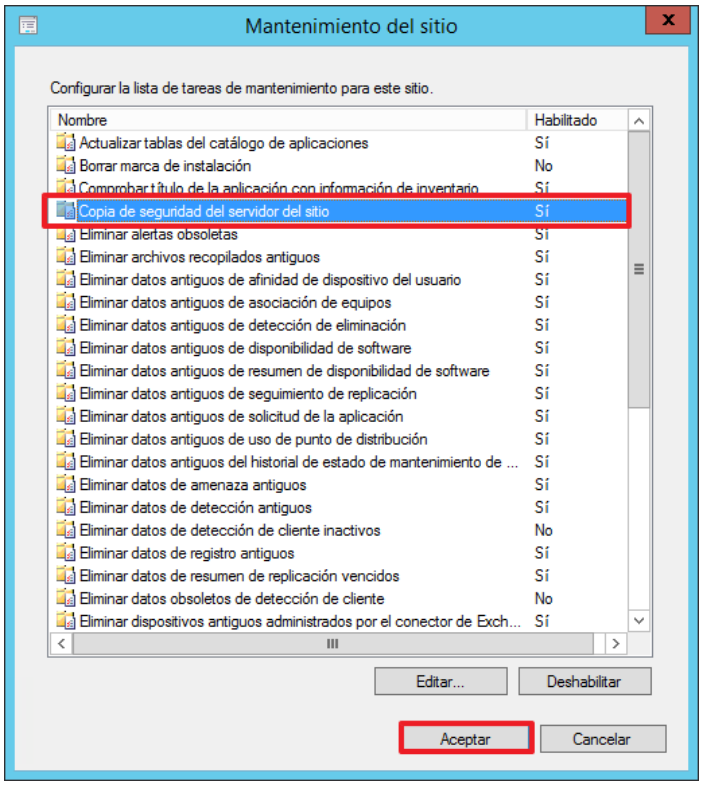
Para los niveles medio y alto de seguridad según lo establecido en el ENS se recomienda que el acceso a la ubicación de las copias de seguridad sea limitado exclusivamente al personal autorizado con el fin de evitar poner en riesgo la una posible manipulación malintencionada de los datos almacenados.

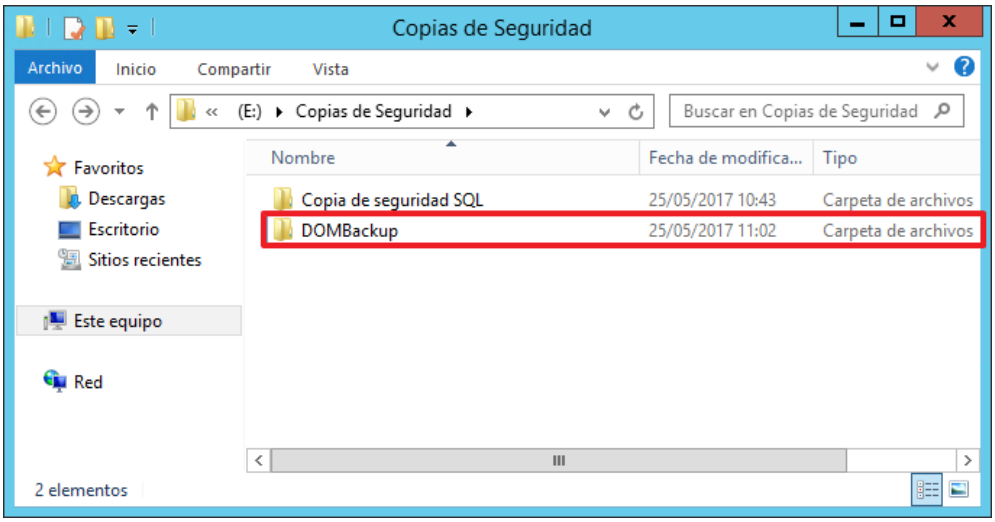
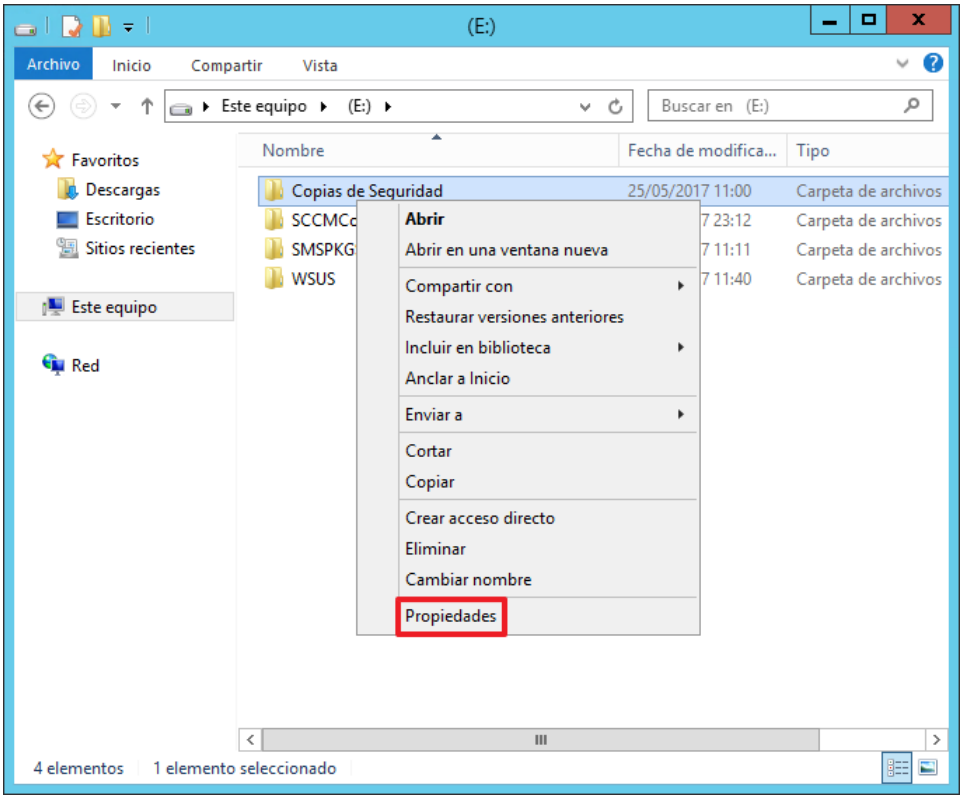
A continuación, se muestra un paso a paso de como habilitar las copias de seguridad de un sitio.

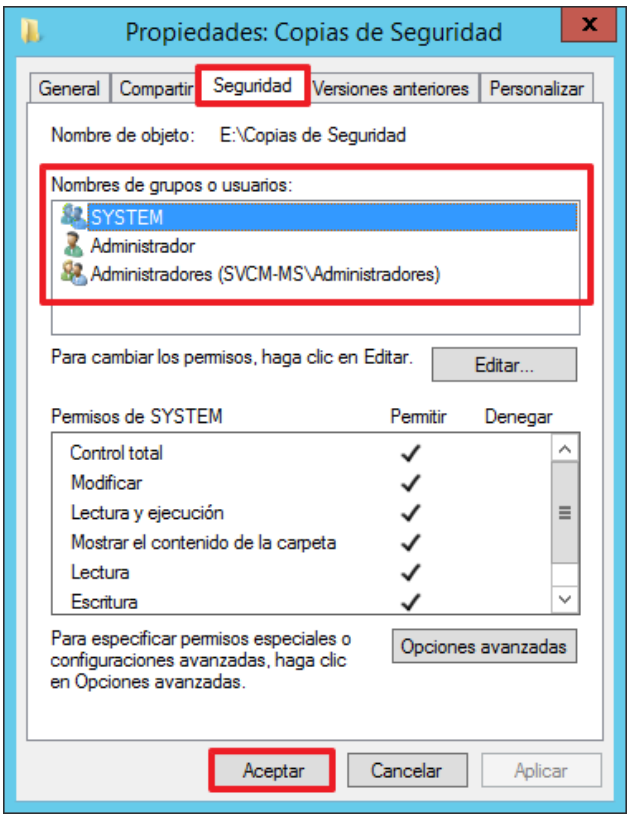
Paso	Descripción
362.	Inicie sesión con una cuenta de administrador de dominio en el servidor miembro donde está implementado MS SCCM 2012 R2. **Nota:** Para este ejemplo se utiliza la cuenta DOMINIO\Administrador.
363.	Pulse sobre el menú inicio. 
364.	Pulse el símbolo recuadrado en la imagen y muestre todas las aplicaciones instaladas. 
365.	Marque con el botón Izquierdo sobre el icono “Consola de Configuration Manager” para abrir la consola de administración de MS SCCM 2012 R2. 

Paso	Descripción
366.	Seleccione el apartado “Administración”. 
367.	Despliegue “**Configuración del sitio > Sitios**”. 

Paso	Descripción
368.	Localice el sitio sobre el que desea habilitar las copias de seguridad, pulse con el botón derecho sobre el sitio y seleccione la opción “Mantenimiento del sitio” del menú contextual. 
369.	Localice la opción “Copia de seguridad del servidor del sitio” y pulse sobre el botón “Editar”. 

Paso	Descripción
370.	Configure los parámetros adecuándolos a su organización y pulse “Aceptar” para guardar la configuración. 
371.	Confirme que la opción “Copia de seguridad del servidor del sitio” está habilitada y pulse “Aceptar” para cerrar las opciones de mantenimiento del sitio. 

Paso	Descripción
372.	Una vez realizada la copia de seguridad, diríjase a la ruta en la que se almacenan las copias de seguridad y compruebe que se están almacenando correctamente. 
373.	En el directorio raíz donde tiene ubicadas las copias de seguridad, seleccione la carpeta y pulse la opción “Propiedades” del menú contextual. 

Paso	Descripción
374.	Seleccione la pestaña “Seguridad” y compruebe que los grupos y usuarios que aparecen tienen los permisos adecuados de acceso a los datos de las copias de seguridad. Pulse “Aceptar” cuando haya verificado que los datos son los correctos.  **Nota:** Deberá dar permisos de acceso a la carpeta “Copias de seguridad” únicamente al personal autorizado de gestionar los datos de copias de seguridad del sitio.

ANEXO C.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES MS SCCM 2012 R2 SOBRE WINDOWS SERVER 2012 R2 QUE LES SEA DE APLICACIÓN EL NIVEL ALTO DEL ENS

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores MS SCCM 2012 R2 sobre Microsoft Windows Server 2012 R2 con implementación de seguridad de nivel alto del ENS.

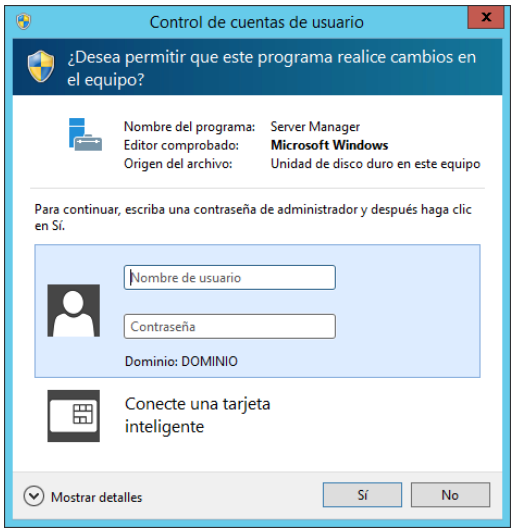
Para realizar esta lista de comprobación primero deberá iniciar sesión en un controlador de dominio con una cuenta de usuario que tenga privilegios de administración en el dominio.

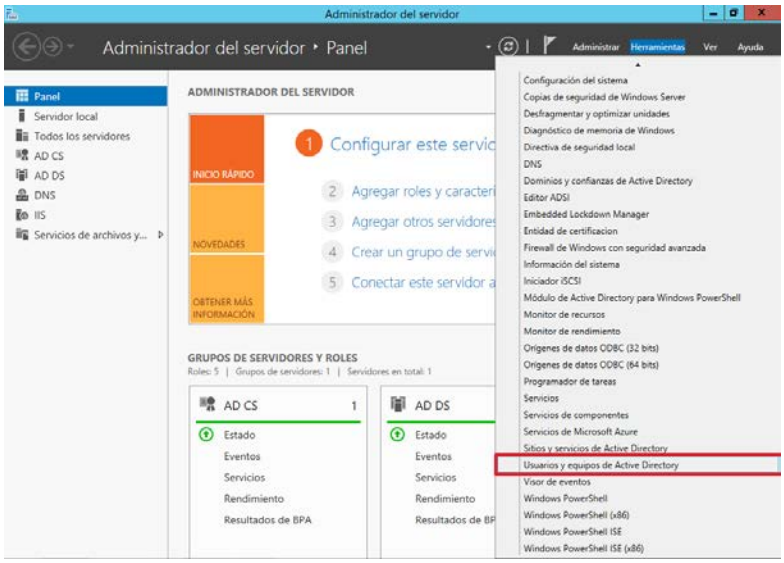
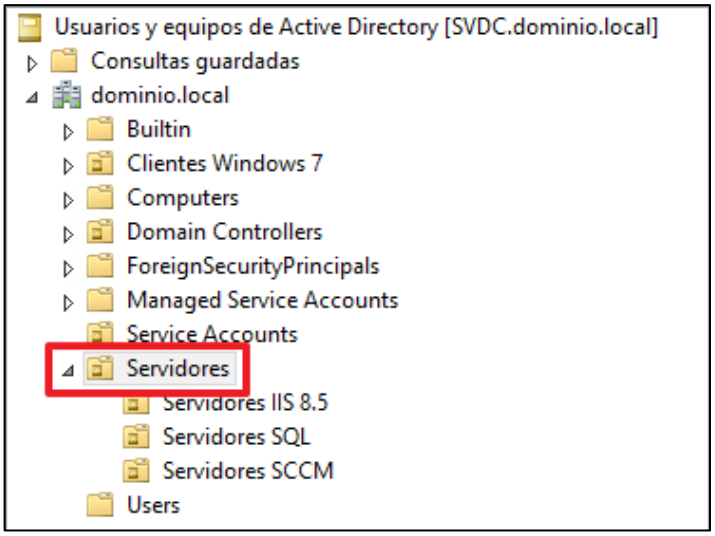
1. COMPROBACIONES EN CONTROLADOR DE DOMINIO

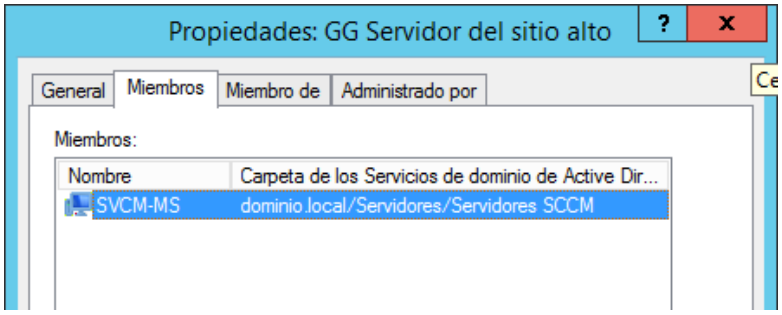
Para realizar las comprobaciones pertinentes en el controlador de dominio se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

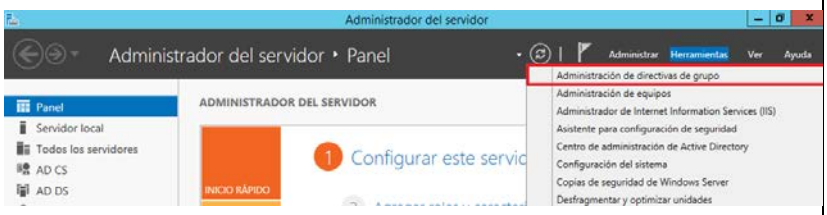
a) Administrador de directivas de grupo (gpmc.msc)

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

Comprobación	OK/NOK	Como hacerlo
1. Inicie sesión en un controlador de dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio. El sistema solicitará elevación de privilegios para poder ejecutar el "Administrador del Servidor". Introduzca credenciales de administrador y pulse "Sí" en la ventana de "Control de cuentas de usuario". 

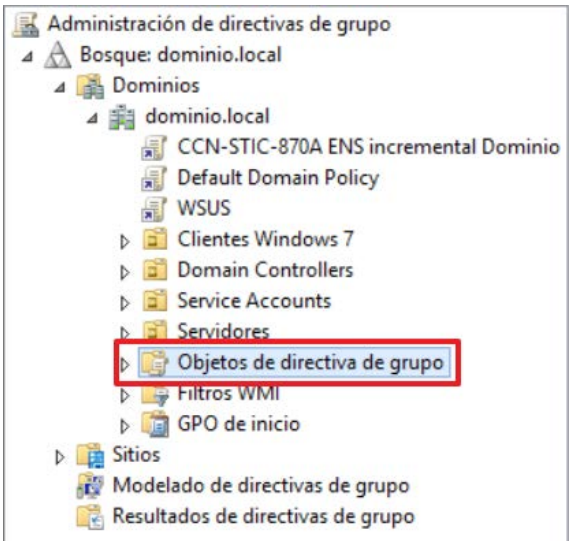
Comprobación	OK/NOK	Como hacerlo
2. Verifique que están creados los grupos de seguridad global.		Ejecute la herramienta "Usuarios y equipos de Active Directory". Para ello, sobre el menú superior de la derecha de la herramienta "Administrador del servidor" seleccione: **"Herramientas → Usuarios y equipos de Active Directory"**  **Nota:** Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio  . Seleccione el contenedor "Servidores SCCM" y "Servidores SQL", situados en la siguiente ruta: "**Usuarios y equipos de Active Directory → [Su dominio] → Servidores**". Verifique que están creados los grupos de seguridad en función de los roles de sistema de sitio que ha reforzado la seguridad. 

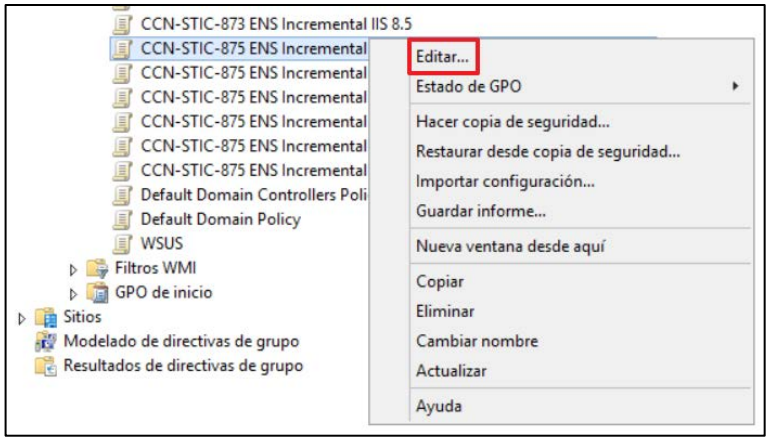
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="2">Como hacerlo</th></tr>
<tr><td></td><td colspan="2">Grupo de seguridad</td><td>OK/NOK</td></tr>
<tr><td></td><td colspan="2">GG Servidor Base de datos del sitio alto</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de servicios de informes alto</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor del sitio alto</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de administración alto</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de distribución alto</td><td></td></tr>
<tr><td></td><td colspan="2">GG Servidor Punto de actualización de software alto</td><td></td></tr>
<tr><td>3. Verifique que los servidores que han sido catalogados correctamente.</td><td></td><td colspan="2">Pulse doble clic sobre cada grupo de seguridad y seleccione la pestaña “Miembros” para verificar que los servidores que corresponden a este grupo de seguridad aparecen en el listado.
 

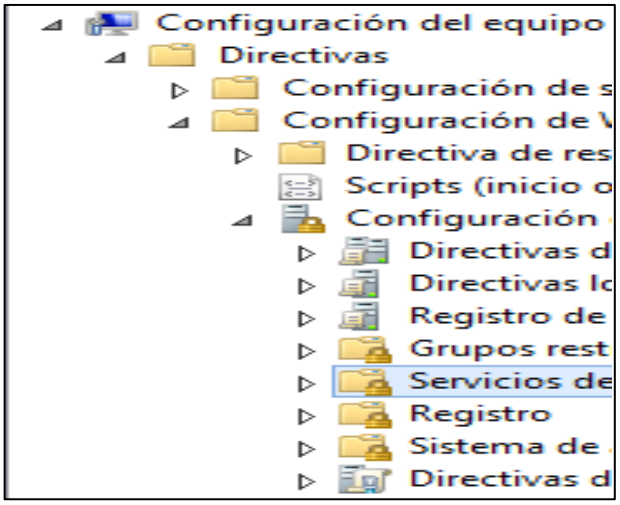
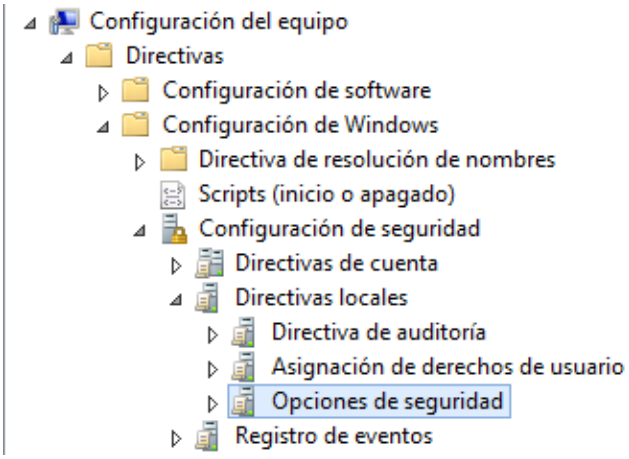
Nota: La imagen mostrada anteriormente corresponde a un ejemplo de los miembros del grupo de seguridad “GG Servidor del sitio alto”, deberá realizar esta comprobación en todos los grupos de seguridad correspondientes y verificar que aparecen los servidores que pertenecen a cada grupo.</td></tr>
<tr><td>4. Verifique que los objetos de directivas de grupo han sido creados y están habilitados.</td><td></td><td colspan="2">Ejecute la herramienta “Administrador de directivas de grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione: “Herramientas → Administración de directivas de grupo”.
 

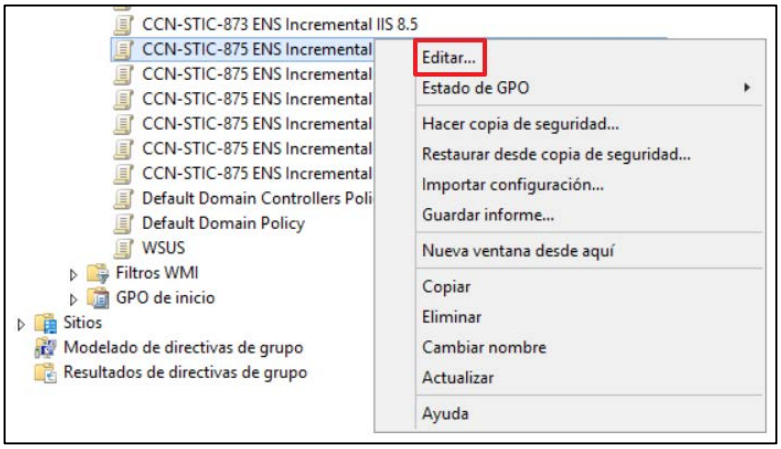
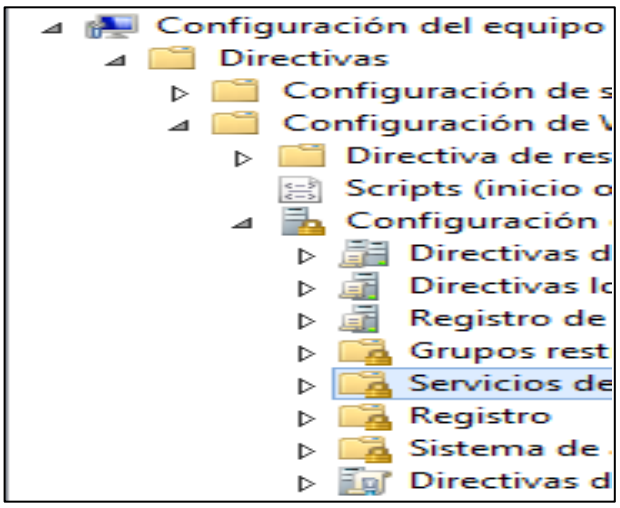
Nota: Si no está iniciado el Administrador del servidor, puede iniciarlo desde el botón situado en la barra de tareas del controlador de dominio .

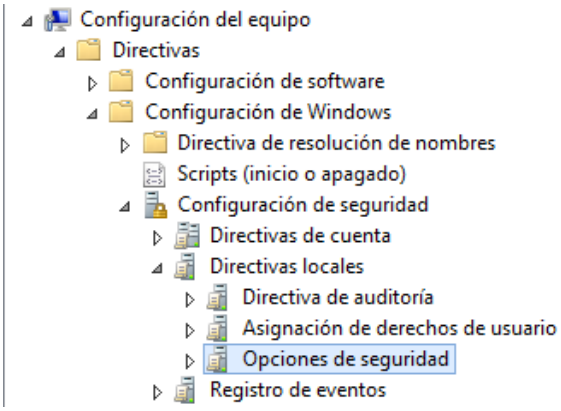
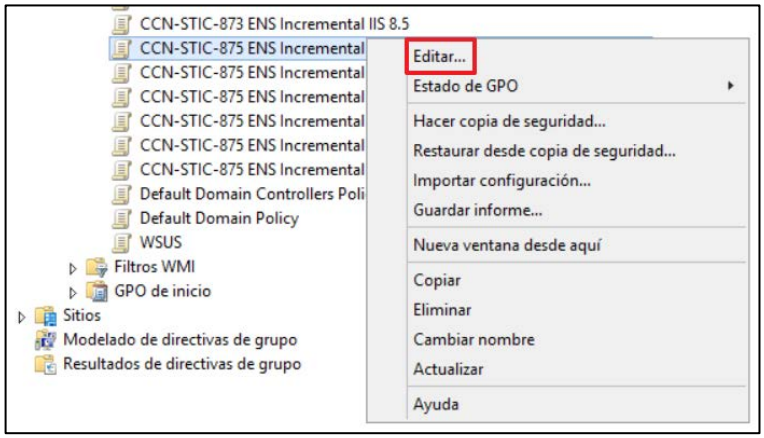
Dentro de la consola diríjase a los “Objetos de directiva de grupo”: “Bosque: [Su Bosque] → Dominios → [Su Dominio] → Objetos de directiva de grupo”.
Verifique que están creados los objetos de directiva de grupo en función de los roles de sistema de sitio que ha reforzado la seguridad y que en la columna “Estado de GPO” figuran como habilitadas.</td></tr>
</table>

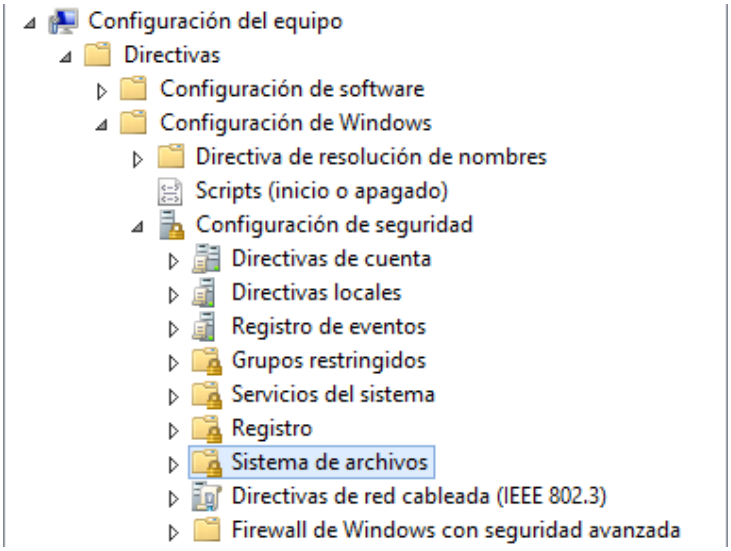
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td> 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de actualización de software alto</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de administración alto</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de distribución alto</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de servicios de informes alto</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Servidor del sitio alto</td><td>Habilitado</td><td></td></tr>
<tr><td>CCN-STIC-875 ENS Incremental Punto de -SQL alto</td><td>Habilitado</td><td></td></tr>
</table></td></tr>
<tr><td>5. Verifique la configuración de la directiva.</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de actualización de software alto” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>6. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”.
 
</td></tr>
<tr><td colspan="2"></td><td>
<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>Administración remota de Windows (WS-Management)</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>Servicio de transferencia inteligente en segundo plano (BITS)</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>Servidor</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>WSusCertServer</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>WsusService</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table>
</td></tr>
<tr><td>7. Verifique las opciones de seguridad.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
</table>

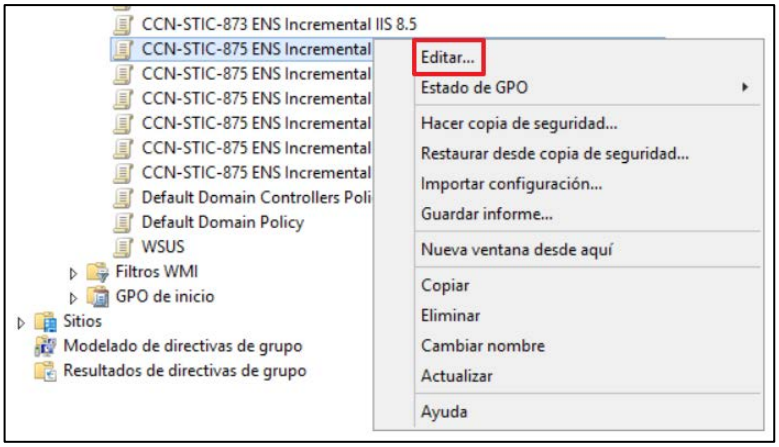
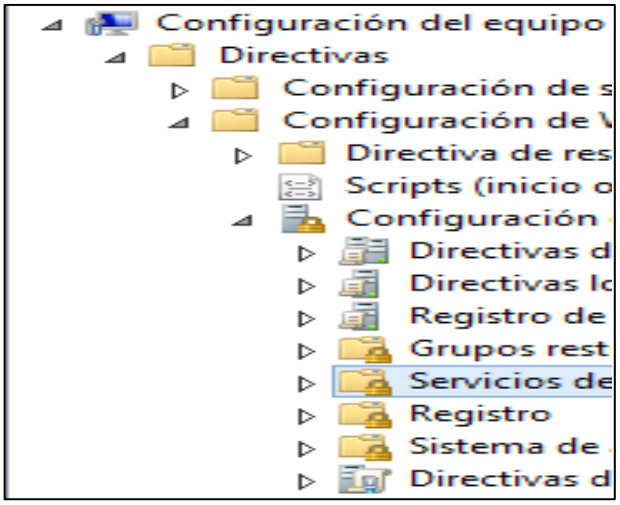
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Como hacerlo</th></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>8. Verifique la configuración de la directiva.</td><td></td><td colspan="3">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de administración alto” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>9. Verifique los servicios del sistema.</td><td></td><td colspan="3">Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 
</td></tr>
<tr><td></td><td></td><td colspan="3"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td rowspan="4">10. Verifique las opciones de seguridad.</td><td></td><td colspan="3">Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td></td><td>Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td></td><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
<tr><td>11. Verifique la configuración de la directiva.</td><td></td><td colspan="3">Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución alto” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td rowspan="4">12. Verifique las opciones de seguridad.</td><td></td><td colspan="3">Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.</td></tr>
<tr><td></td><td>Directiva</td><td>Valor</td><td>OK/NOK</td></tr>
<tr><td></td><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td></td><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table>

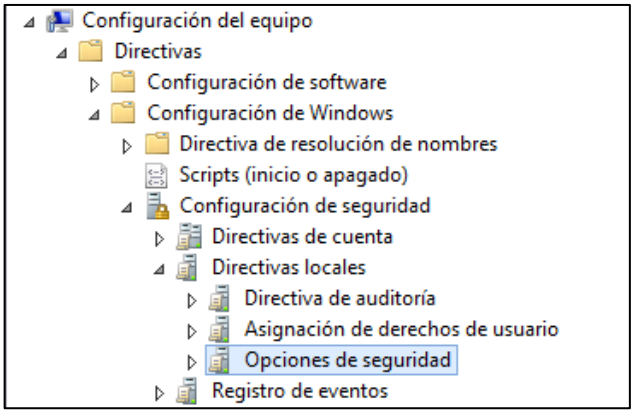
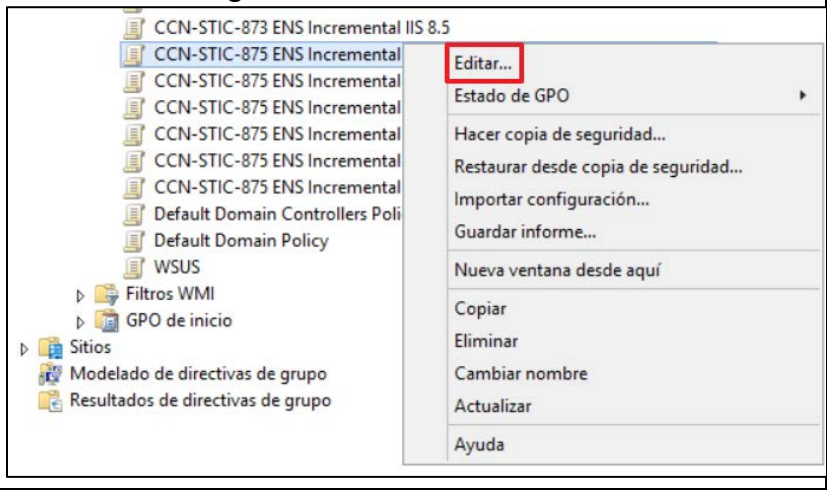
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>13. Verifique las opciones del Sistema de archivos.</td><td></td><td>Compruebe que se ha aplicado correctamente los permisos sobre los siguientes directorios.
Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Sistema de archivos”.
 

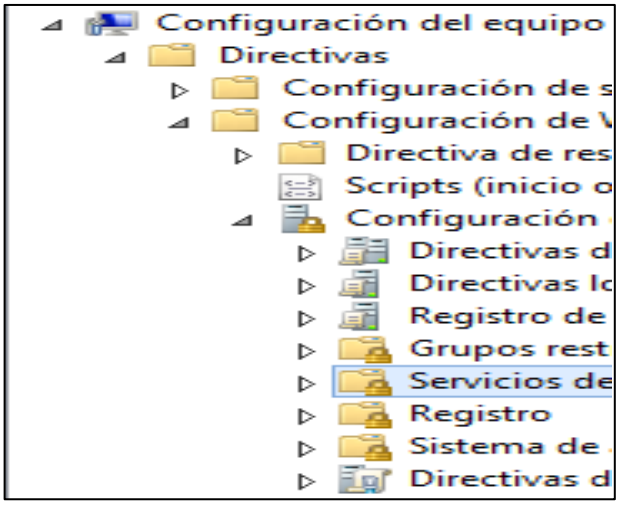
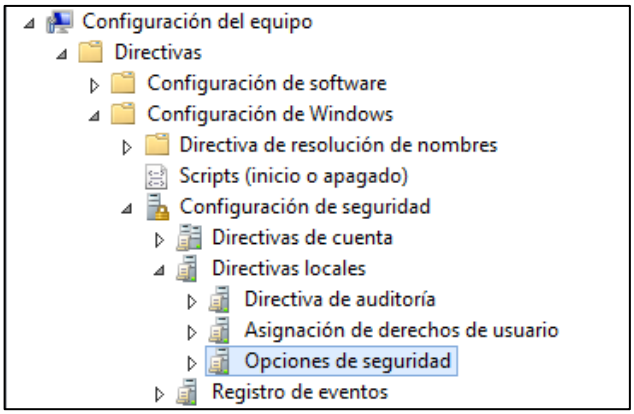
Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, haciendo doble clic sobre él o marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades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

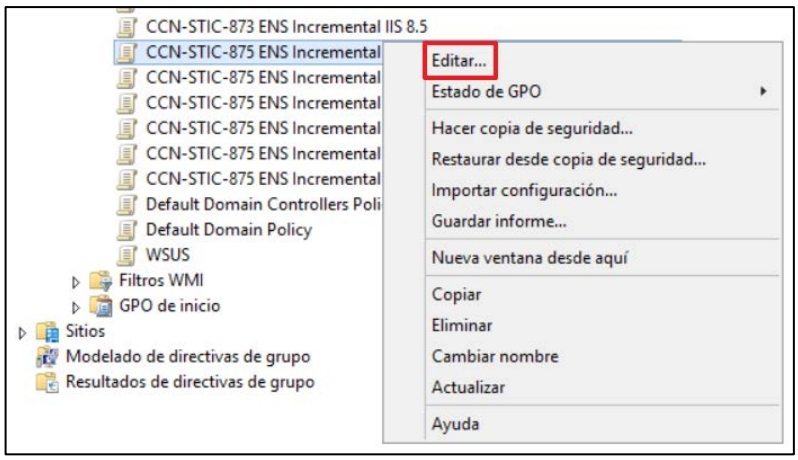
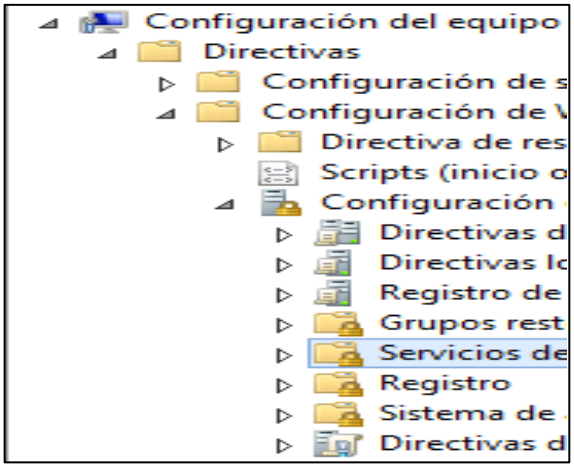
Archivo	Usuario	Permiso	OK/NOK
E:\SCCMContentLib	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer	
E:\SMS_DP$	SYSTEM	Control total	
	Administradores	Control total	
	Administrador	Control total	
E:\SMSPKGE$	Administradores	Control total	
	Usuarios	Leer y ejecutar	
E:\SMSSIG	IUSR	Escribir (Denegar)	
	SYSTEM	Control total	
	Administradores	Control total	
	Usuarios	Leer	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>14. Verifique la configuración de la directiva.</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental Punto de servicios de informes alto” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>15. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo.
“Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

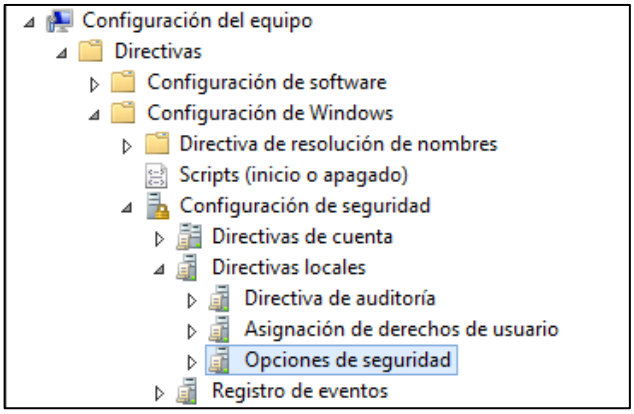
<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table></td></tr>
</table>

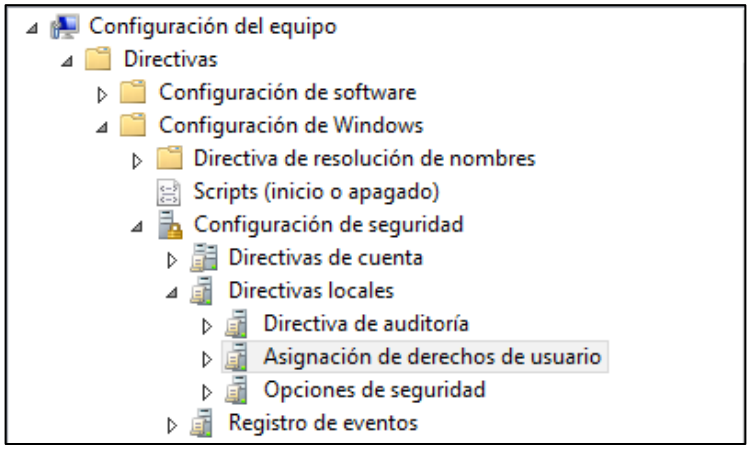
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td rowspan="4">16. Verifique las opciones de seguridad.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td colspan="3"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>17. Verifique la configuración de la directiva.</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental servidor del sitio alto” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>18. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>SMS_SITE_VSS_WRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_COMPONENT_MANAGER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>CcmExec</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_NOTIFICATION_SERVER</td><td>Manual</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_BACKUP</td><td>Manual</td><td>Configurado</td><td></td></tr>
</table></td></tr>
<tr><td>19. Verifique las opciones de seguridad.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 
</td></tr>
<tr><td></td><td colspan="2"><table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
</table>

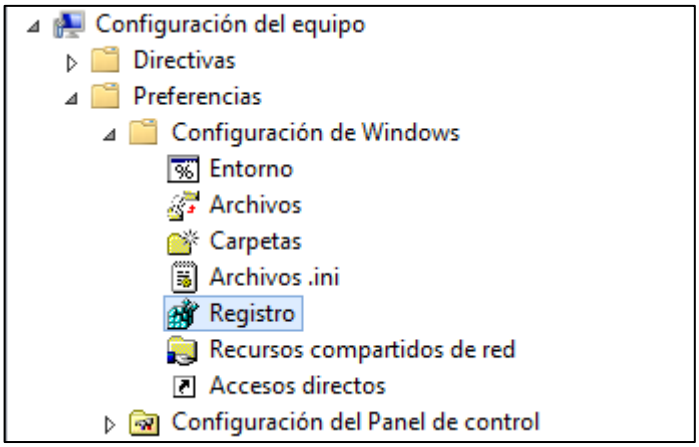
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>20. Verifique la configuración de la directiva.</td><td></td><td>Seleccione el objeto de directiva de grupo “CCN-STIC-875 ENS Incremental SQL Alto” y pulse la opción “Editar…”. Se abrirá el editor de directivas de grupo, deberá navegar sobre los elementos del árbol de nodos para verificar las distintas configuraciones.
 
</td></tr>
<tr><td>21. Verifique los servicios del sistema.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Servicios del sistema”
 

<table>
<tr><th>Servicio</th><th>Iniciado</th><th>Permiso</th><th>OK/NOK</th></tr>
<tr><td>MSSQLSERVER</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_EXECUTIVE</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLSERVERAGENT</td><td>Automático</td><td>Configurado</td><td></td></tr>
<tr><td>SQLWRITER</td><td>Automático</td><td>Configurado</td><td></td></tr>
</table>
Nota: Deberá adaptar el servicio SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL, por el servicio configurado con el nombre de dominio de su organización.</td></tr>
</table>

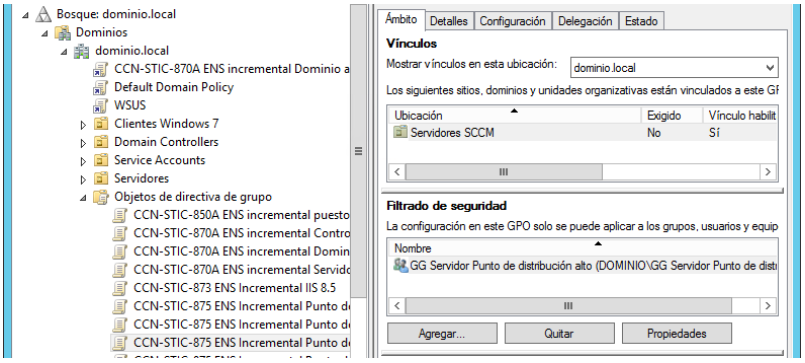
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>22. Verifique las opciones de seguridad.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Opciones de seguridad”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Seguridad de red: Restringir NTLM: autenticación NTLM en este dominio</td><td>Deshabilitado</td><td></td></tr>
<tr><td>Seguridad de red: Restringir NTLM: tráfico NTLM entrante</td><td>Permitir todo</td><td></td></tr>
</table></td></tr>
<tr><td>23. Verifique la asignación de derechos de usuario.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Directivas → Configuración de Windows → Configuración de seguridad → Directivas locales → Asignación de derechos usuario”.
 

<table>
<tr><th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Inicio de sesión como servicio</td><td>DOMINIO\SQLServiceAccount</td><td></td></tr>
</table>
Nota: Deberá adaptar estos pasos a su organización y comprobar que el usuario con permisos de inicio de sesión como servicio es el adecuado.</td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>24. Verifique las entradas del registro.</td><td></td><td>Seleccione el siguiente nodo. “Configuración del Equipo → Preferencias → Configuración de Windows → Registro.
 

<table>
<tr><th>Parametro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>DisabledByDefault</td><td>Acción: Actualización
subárbol: HKEY_LOCAL_MACHINE
Clave: SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Client
Tipo: REG_DWORD
Valor: 00000000</td><td></td></tr>
<tr><td>Enabled</td><td>Acción: Actualización
subárbol: HKEY_LOCAL_MACHINE
Clave: SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Server
Tipo: REG_DWORD
Valor: 00000001</td><td></td></tr>
</table></td></tr>
<tr><td>25. Verifique que cada objeto de directiva de tiene definido el filtro de seguridad que corresponde.</td><td></td><td>En el árbol de la izquierda, pulse doble clic sobre el objeto de directiva de grupo: “Bosques [Su Bosque] → Dominios → [Su Dominio] → Objetos de Directiva de Grupo”
Verifique en la pestaña “Ámbito” que dentro del campo “Filtrado de seguridad” figura el grupo seguridad correspondiente a cada objeto de directiva de grupo.</td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo
		 **Nota:** La imagen mostrada anteriormente corresponde a un ejemplo del filtro de seguridad del objeto de directiva de grupo "CCN-STIC-875 ENS Incremental Punto de distribución alto" al que corresponde el filtro de seguridad "GG Servidor punto de distribución alto", deberá realizar esta comprobación en todos los objetos de directivas de grupo correspondientes y verificar que están vinculados los grupos de seguridad que pertenecen a cada directiva.

Directiva	Grupo de seguridad	OK/NOK
CCN-STIC-875 ENS Incremental Punto de actualización de software alto	GG Servidor Punto de actualización de software alto	
CCN-STIC-875 ENS Incremental Punto de administración alto	GG Servidor Punto de administración alto	
CCN-STIC-875 ENS Incremental Punto de distribución alto	GG Servidor Punto de distribución alto	
CCN-STIC-875 ENS Incremental Punto de servicios de informes alto	GG Servidor Punto de servicios de informes alto	
CCN-STIC-875 ENS Incremental Servidor del sitio alto	GG Servidor del sitio alto	
CCN-STIC-875 ENS Incremental Punto de -SQL alto	GG Servidor Base de datos del sitio alto	

2. COMPROBACIONES EN SERVIDOR MIEMBRO

Para realizar las comprobaciones pertinentes en los servidores miembros, se deberán ejecutar diferentes consolas de administración y herramientas del sistema. Éstas estarán disponibles si se ha iniciado sesión en el servidor con una cuenta de usuario que es administrador local del servidor o administrador del dominio. Las consolas y herramientas que se utilizarán son las siguientes:

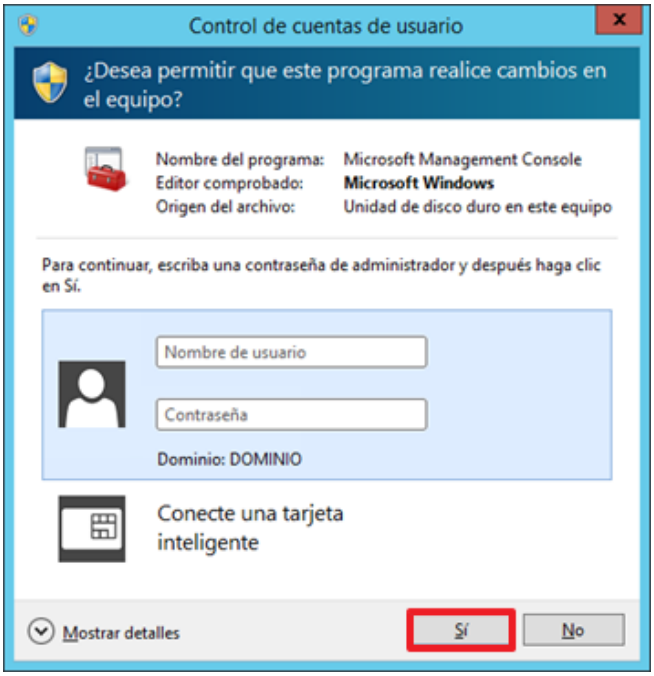
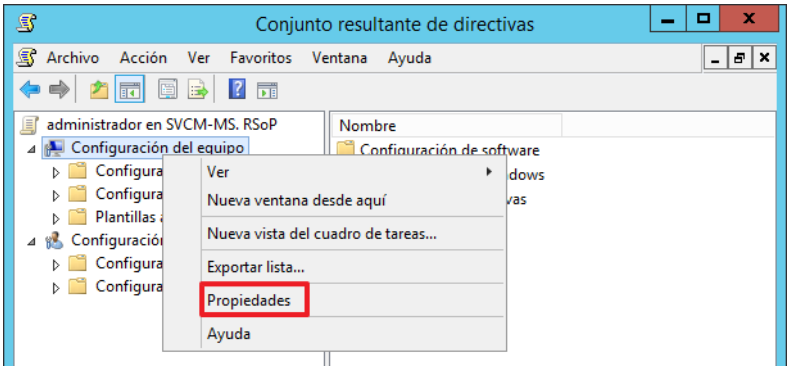
c) Administrador del Servidor

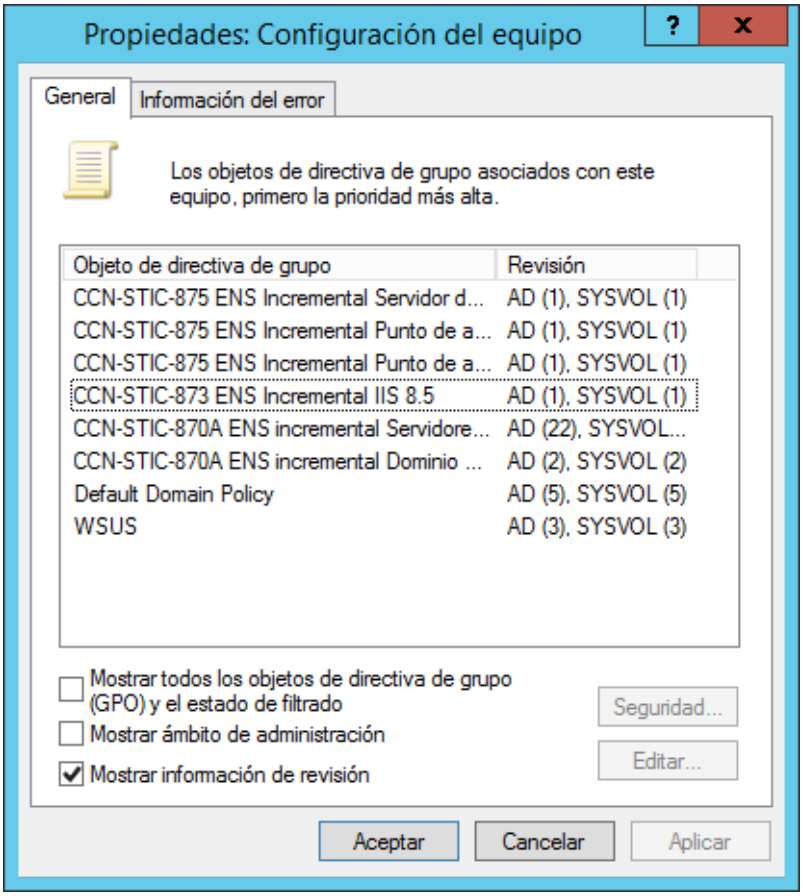
d) Conjunto resultante de directivas (rsop.msc)

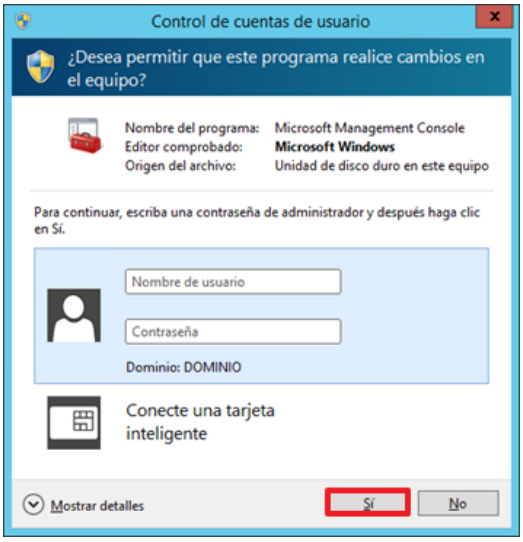
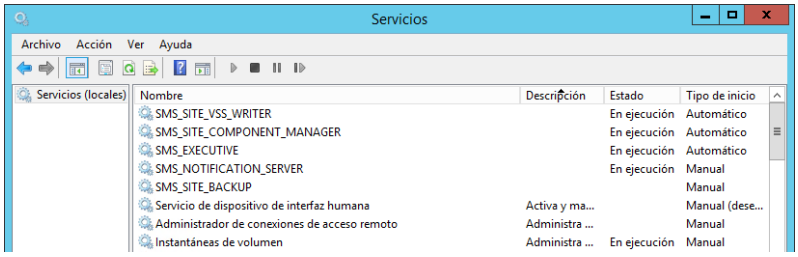
e) Consola de servicios (services.msc)

f) Editor de registro (regedit.exe)

g) Explorador de Archivos (explorer.exe)

Comprobación	OK/NOK	Como hacerlo
26. Inicie sesión en un servidor miembro del dominio		En uno de los servidores miembro del dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
27. Verifique que el equipo ha recibido la directiva de grupo que corresponde con el rol de sistema de sitio que esta implementado.		Ejecute la consola de administración "Conjunto resultante de directivas" (el sistema solicitará elevación de privilegios): **"Tecla Windows+R → rsop.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca credenciales de administrador y pulse "Sí" en la ventana de "Control de cuentas de usuario": 
28. Verifique la configuración asignada.		Seleccione en ella la rama "Configuración del equipo", márquela con el botón derecho del ratón y seleccione la opción "Propiedades" del menú contextual que aparecerá, como se muestra en la figura: 

Comprobación	OK/NOK	Como hacerlo
29. Verifique los objetos de directivas de grupo asociados.		En la ventana de propiedades que aparecerá, seleccione la pestaña "General" y observe la sección "Objeto de directiva de grupo". Verifique que en dicha sección aparecen listados, los objetos de directiva de grupo correspondientes con el servidor miembro que está comprobando.  **Nota:** Se debe tener en consideración que el listado de objetos de directivas de grupo variara en función del servidor miembro que este comprobando y de los roles de sistema de sitio que dicho servidor tenga implementado.

Comprobación	OK/NOK	Como hacerlo
30. Verifique que los servicios del sistema están correctamente configurados.		Usando la consola de servicios (el sistema solicitará elevación de privilegios): **"Windows+R → services.msc"** El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca credenciales de administrador y pulse "Sí" para continuar. 
31. Verifique los servicios de inicio.		Verifique que el tipo de inicio de los servicios que aparecen en el sistema y en la siguiente tabla coinciden:  **Nota:** Dependiendo del servidor miembro que este comprobando y del rol del sistema de sitio implementado, es posible que no aparezcan todos los servicios aquí relacionados o que aparezcan servicios adicionales.

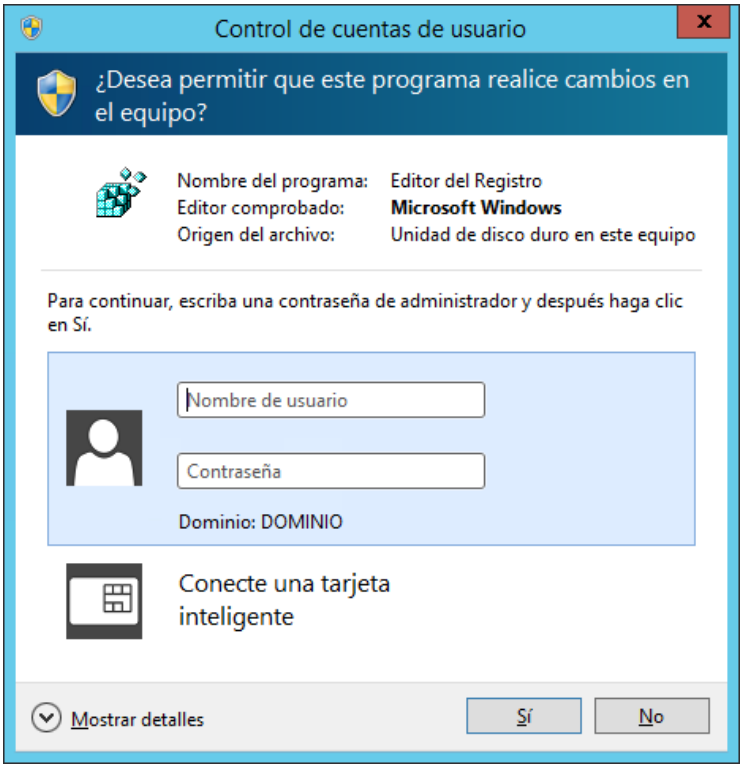
Directiva	Servicio	Iniciado	Permiso	OK/NOK
CCN-STIC-875 ENS Incremental Punto de actualización de software alto	Administración remota de Windows (WS-Management)	Automático	Configurado	
	Servicio de transferencia inteligente en segundo plano (BITS)	Automático	Configurado	
	Servidor	Automático	Configurado	
	WSusCertServer	Automático	Configurado	
	WsusService	Automático	Configurado	

Comprobación	OK/NOK	Como hacerlo			
	Directiva	**Servicio**	**Iniciado**	**Permiso**	**OK/NOK**
	CCN-STIC-875 ENS Incremental Punto de administración alto	SMS_EXECUTIVE	Automático	Configurado	
	CCN-STIC-875 ENS Incremental Punto de servicios de informes alto	SMS_EXECUTIVE	Automático	Configurado	
	CCN-STIC-875 ENS Incremental servidor del sitio alto	SMS_SITE_VSS_WRITER	Automático	Configurado	
		SMS_SITE_COMPONENT_MANAGER	Automático	Configurado	
		CcmExec	Automático	Configurado	
		SMS_NOTIFICATION_SERVER	Manual	Configurado	
		SMS_SITE_BACKUP	Manual	Configurado	
	CCN-STIC-875 ENS Incremental SQL Alto	MSSQLSERVER	Automático	Configurado	
		SMS_EXECUTIVE	Automático	Configurado	
		SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL	Automático	Configurado	
		SQLSERVERAGENT	Automático	Configurado	
		SQLWRITER	Automático	Configurado	
	Nota: Deberá adaptar el servicio SMS_SITE_SQL_BACKUP_SVCM-MS.DOMINIO.LOCAL, por el servicio configurado con el nombre de dominio de su organización.				

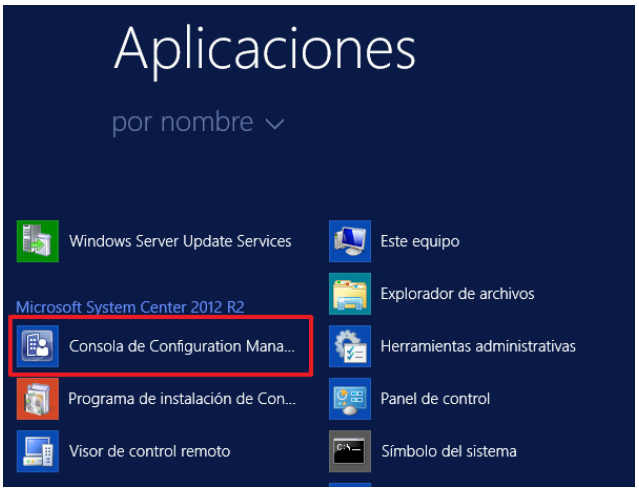
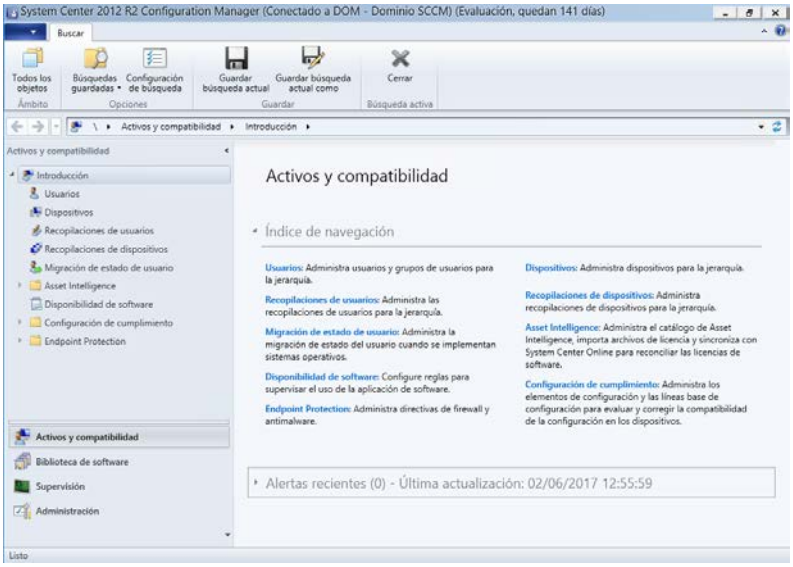
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>32. Verifique que se han asignado los permisos correctos en el sistema de archivos.</td><td></td><td>En los servidores miembro donde tenga implementado el rol de sistema de sitio de Punto de distribución y se le esté aplicando la directiva de grupo “CCN-STIC-875 ENS Incremental Punto de distribución alto”. Verifique los permisos asignados utilizando el Explorador de Windows: “Windows+R → Explorer”.
En caso de no saber dónde apunta cada una de las rutas abreviadas que se especifica, ejecute Explorer <<ruta>> donde <<ruta>> se sustituirá por la ruta abreviada.

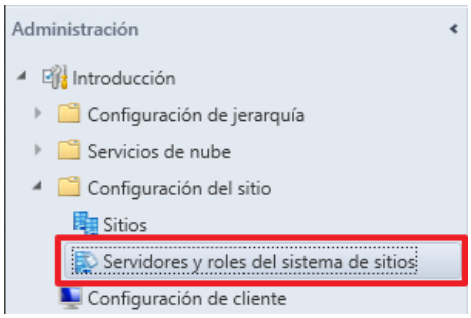
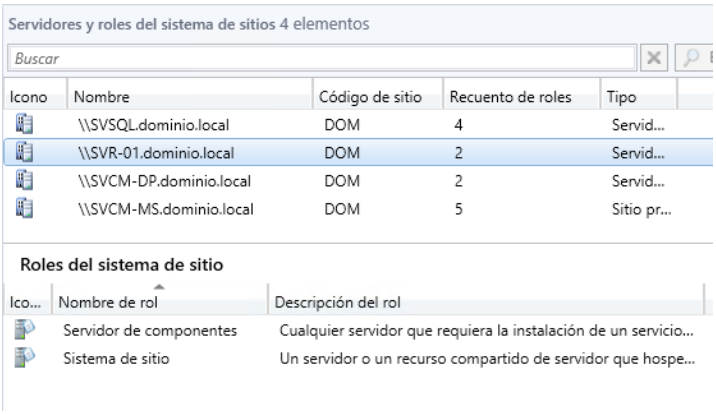
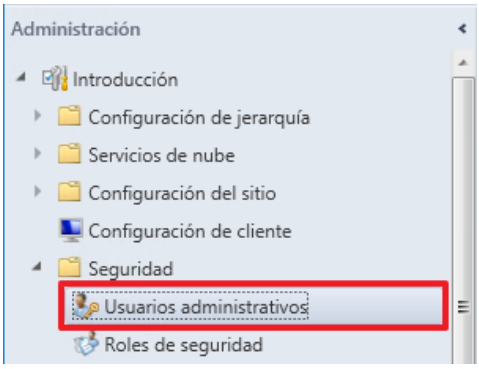
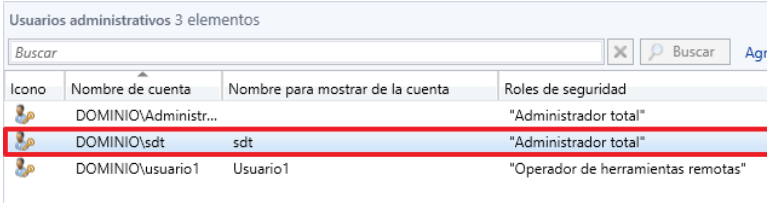
Nota: Para verificar los permisos de cada fichero o carpeta en la directiva de dominio deberá abrir las propiedades del objeto, marcándolo con el botón derecho y eligiendo la opción “Propiedades” del menú contextual que aparecerá; una vez abierta la ventana de propiedades deberá situarse en la pestaña “Seguridad”. En la mayoría de los casos, el Control de cuentas de usuario solicitará elevación de privilegios. Dependiendo del equipo, es posible que no aparezcan todos los archivos o carpetas aquí relacionados, ya que algunos pueden haber sido desinstalados o no instalados</td></tr>
</table>

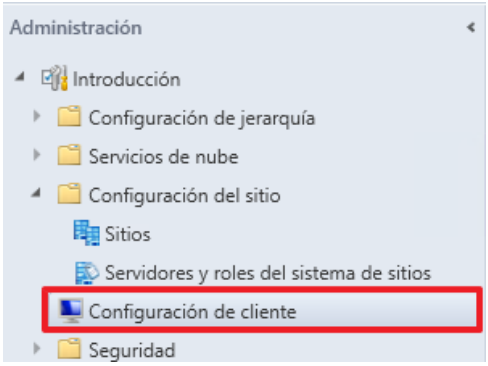
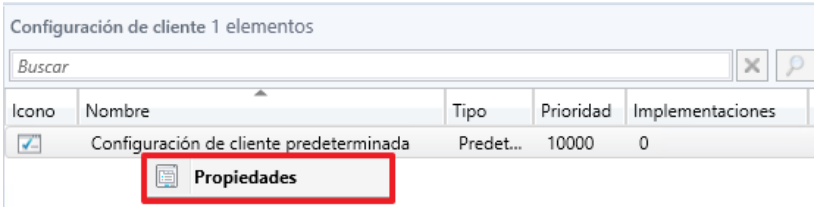
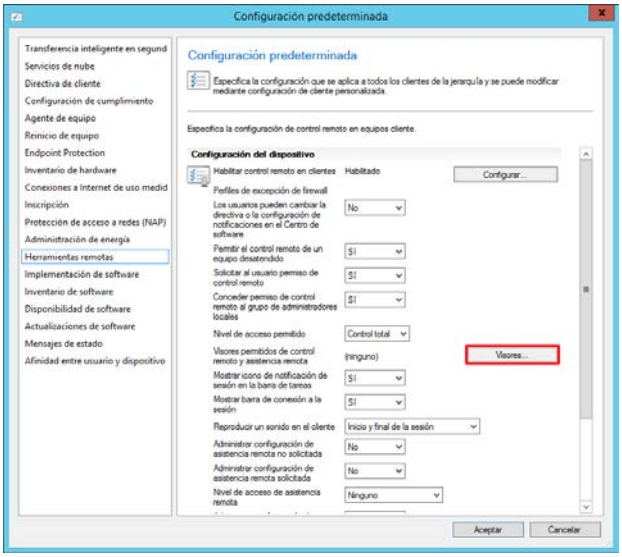
Archivo	Usuario	Permiso	OK/NOK
E:\SCCMContentLib	Administradores	Control total	
	SYSTEM	Control total	
	Usuarios	Leer	
E:\SMS_DP$	SYSTEM	Control total	
	Administradores	Control total	
	Administrador	Control total	
E:\SMSPKGE$	Administradores	Control total	
	Usuarios	Leer y ejecutar	
E:\SMSSIG	IUSR	Escribir (Denegar)	
	SYSTEM	Control total	
	Administradores	Control total	
	Usuarios	Leer	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>33. Verifique los valores del registro.</td><td></td><td>En los servidores miembro donde tenga implementado el rol de servidor de base de datos del sitio y se le esté aplicando la directiva de grupo “CCN-STIC-875 ENS Incremental SQL Alto”. Compruebe los valores del registro definidos en los Controladores de Dominio que pertenezcan al grupo categorizado como alto siguiendo los criterios del ENS, mediante el uso del “Editor del Registro”.
“Windows+R → Regedit”
El Control de cuentas de usuario solicitará elevación de privilegios. Introduzca credenciales de administrador y pulse “Sí” para continuar.
 

<table>
<tr><th>Valor del registro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Client \DisabledByDefault</td><td>00000000</td><td></td></tr>
<tr><td>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\schannel\Protocols\SSL 3.0\Server \Enabled</td><td>00000001</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo
34. Inicie sesión en el servidor miembro donde tiene instalada la consola de administración de MS SCCM 2012 R2, verifique que el acceso es correcto.		Inicie sesión en la consola de administración de Configuration Manager desde el menú “Inicio > Todas las aplicaciones > Microsoft System Center 2012 R2 > Consola de Configuration Manager”. 
35. Verifique que tiene acceso a la Consola de Configuración.		Compruebe que accede correctamente a la consola de configuración de MS SCCM 2012 R2. 

Comprobación	OK/NOK	Como hacerlo
36. Verifique que los roles de sistema de sitios están asociados a los servidores que ha establecido.		Despliegue "**Configuración del sitio > Servidores y roles del sistema de sitios**".  Verifique seleccionando cada servidor, que tiene implementados los roles de sistema de sitios asignados. 
37. Verifique los permisos asignados a los usuarios administrativos.		Despliegue "**Introducción > Seguridad > Usuarios administrativos**".  Compruebe que los usuarios tienen asignados los roles de seguridad correctamente. 

Comprobación	OK/NOK	Como hacerlo
38. Verifique los permisos asignados a los usuarios con permisos de control remoto.		Despliegue "**Introducción > Configuración del sitio > Configuración de cliente**".  Compruebe que los usuarios tienen asignados los permisos correctamente. Para ello, pulse con el botón derecho sobre "Configuración de cliente predeterminada" y seleccione la opción "Propiedades" del menú contextual. 
39. Verifique los usuarios que tienen permisos de control remoto.		Pulse sobre el botón "Visores…".  Compruebe en el listado los usuarios que tienen permisos de control remoto.