



GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-871)

IMPLEMENTACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD EN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2



FEBRERO 2017

Edita:



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
CRYPTOLOGICO NACIONAL, c=ES
2017.02.24 12:25:59 +01'00'

© Centro Criptológico Nacional, 2017

NIPO: 785-17-010-0

Fecha de Edición: febrero de 2017

El Ministerio de Hacienda y Administraciones Públicas ha financiado el desarrollo del presente documento y sus anexos.

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

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, 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 en su artículo 9.2.f).

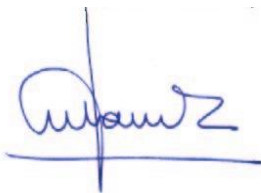
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 crea el Esquema Nacional de Seguridad (ENS), que establece las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

El Real Decreto 3/2010 de 8 de Enero desarrolla el Esquema Nacional de Seguridad y fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración. En su artículo 29 se autoriza que a través de las series CCN-STIC el CCN desarrolle lo establecido en el mismo.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función y a lo reflejado en el ENS, 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.

Febrero 2017



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN	3
2. OBJETO	3
3. ALCANCE	3
4. DESCRIPCIÓN DEL USO DE ESTA GUÍA	4
4.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA	4
5. INTRODUCCIÓN AL ESQUEMA NACIONAL DE SEGURIDAD	6
5.1 DIMENSIONES DE SEGURIDAD.....	8
5.1.1 DISPONIBILIDAD.....	9
5.1.2 AUTENTICIDAD	10
5.1.3 INTEGRIDAD	10
5.1.4 CONFIDENCIALIDAD.....	11
5.1.5 TRAZABILIDAD	11
5.2 NIVELES DE DIMENSIONES DE SEGURIDAD	12
6. MEDIDAS DE SEGURIDAD.....	15
6.1 MARCO ORGANIZATIVO	16
6.2 MARCO OPERACIONAL	17
6.3 MEDIDAS DE PROTECCIÓN.....	18
6.4 RELACIÓN ENTRE LAS DIMENSIONES DE SEGURIDAD, LA NATURALEZA DE LAS MEDIDAS Y LOS NIVELES	20
7. ARQUITECTURA Y SEGURIDAD DEL SERVIDOR DE IMPRESIÓN.....	21
7.1 COMPONENTES Y ENTIDADES DE LOS SERVICIOS DE IMPRESIÓN	24
7.2 AISLAMIENTO DE CONTROLADORES DE IMPRESIÓN	26
7.3 CONFIGURACIÓN DE LA SEGURIDAD DEL SERVIDOR DE IMPRESIÓN	28
7.4 DIRECTIVA DE GRUPO PARA MODIFICAR LA CONFIGURACIÓN DE SEGURIDAD DEL CONTROLADOR DE IMPRESORA.....	37
7.5 REGISTRO DE TRABAJOS DE IMPRESIÓN	39
7.6 DESPLIEGUE DE IMPRESORAS CON DIRECTIVAS DE GRUPO.....	40
8. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN UN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2.....	41
8.1 MARCO OPERACIONAL	41
8.1.1 CONTROL DE ACCESO	41
8.1.2 EXPLOTACIÓN.....	43
8.2 MEDIDAS DE SEGURIDAD.....	45
8.2.1 PROTECCIÓN DE LAS COMUNICACIONES.....	45
8.2.2 PROTECCIÓN DE LA INFORMACIÓN	45
9. RESUMEN Y APLICACIÓN DE MEDIDAS EN SERVIDOR DE IMPRESIÓN.....	46

ANEXOS

ANEXO A. PLANTILLA DE SEGURIDAD APLICABLE AL SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2 DE NIVEL BAJO.....	47
ANEXO B. PLANTILLA DE SEGURIDAD APLICABLE AL SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2 DE NIVEL MEDIO.....	51
ANEXO C. PLANTILLA DE SEGURIDAD APLICABLE AL SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2 DE NIVEL ALTO	54
ANEXO D. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE IMPRESIÓN QUE LES SEAN DE APLICACIÓN EL NIVEL BAJO DEL ENS.....	58
1. INSTALACIÓN DEL ROL SERVIDOR DE IMPRESIÓN	58
2. PREPARACIÓN DEL DOMINIO	61
3. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN.....	72
3.1 PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN.....	72
3.2 GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN.....	77
3.3 GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN ..	82
ANEXO E. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE IMPRESIÓN QUE LES SEAN DE APLICACIÓN EL NIVEL MEDIO DEL ENS.....	86
1. INSTALACIÓN DEL ROL SERVIDOR DE IMPRESIÓN	86
2. PREPARACIÓN DEL DOMINIO	89
3. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN.....	100
3.1 PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN.....	100
3.2 GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN.....	105
3.3 GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN	110
3.4 GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN.....	113
4. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA	119
4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO	119
4.2 INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS	126
4.3 DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS.....	131
4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO	135
ANEXO F. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE IMPRESIÓN QUE LES SEAN DE APLICACIÓN EL NIVEL ALTO DEL ENS	139
1. INSTALACIÓN DEL ROL SERVIDOR DE IMPRESIÓN	139
2. PREPARACIÓN DEL DOMINIO	142
3. CONSIDERACIONES Y CONFIGURACIONES ESPECÍFICAS DE LA ORGANIZACIÓN.....	154
3.1 PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN.....	154
3.2 GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN.....	159
3.3 GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN	163
3.4 GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN.....	167
4. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA	173
4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO	173
4.2 INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS	180
4.3 DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS.....	184
4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO	188
ANEXO G. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE NIVEL BAJO DEL ENS PARA SERVIDOR DE IMPRESIÓN.....	192
ANEXO H. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE NIVEL MEDIO DEL ENS PARA SERVIDOR DE IMPRESIÓN.....	200
ANEXO I. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE NIVEL ALTO DEL ENS PARA SERVIDOR DE IMPRESIÓN	208

1. INTRODUCCIÓN

1. 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 para la protección de los servicios prestados a los ciudadanos y entre las diferentes administraciones.
2. Esta guía tiene en consideración la aplicación de plantillas y condiciones de seguridad para la implementación del servidor de impresión de Microsoft 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 pueden ser aplicadas bajo diferentes condicionantes. Aunque es factible que se referencien otras guías, especialmente de la serie CCN-STIC-500, referidas a productos y entornos Microsoft, no será un requisito indispensable partir de ninguna de ella, ni será una necesidad la implementación de otras, salvo que las exigencias de seguridad para la organización o el entorno, así lo demandaran.

2. OBJETO

3. El propósito de este documento consiste en proporcionar plantillas de seguridad para la aplicación de medidas de seguridad en un escenario de implementación del Esquema Nacional de Seguridad, en el servidor de impresión de Microsoft sobre Windows Server 2012 R2 bajo un entorno de servidor miembro de un dominio.
4. La definición, así como la implementación de las plantillas de seguridad, tienen en cuenta las características de seguridad definidas a través del Real Decreto 3/2010 por el que 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.
5. 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. Por lo tanto, 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

6. La guía se ha elaborado para proporcionar información específica con objeto de realizar una implementación del ENS en el servidor de impresión de Microsoft 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.

7. El escenario en el cual está basada la presente guía tiene las siguientes características técnicas:
 - Implementación del ENS en un servidor de impresión sobre un escenario de dominio de Directorio Activo Microsoft con Microsoft Windows Server 2012 R2 según las directrices de la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2.
 - Implementación de plantillas de seguridad en función de los niveles de seguridad para servidores Microsoft Windows Server 2012 R2 miembros de un dominio de Directorio Activo Microsoft.
8. Este documento incluye:
 - **Descripción del ENS.** Se definirán las condiciones de aplicación del ENS, así como los requisitos de seguridad.
 - **Descripción de la naturaleza de las medidas.** Se referenciarán los marcos de actuación, las dimensiones de seguridad y la aplicación de medidas.
 - **Descripción de las plantillas de seguridad.** Se definirán las diferentes plantillas de seguridad aplicadas según los niveles que establece el ENS.
 - **Mecanismos para la aplicación de configuraciones.** Se incorporan mecanismos para la implementación de forma automática de las configuraciones de seguridad susceptibles de ello.
 - **Guía paso a paso.** Va a permitir implementar y establecer las configuraciones de seguridad en el servidor de impresión en cada uno de sus niveles de seguridad.
 - **Lista de comprobación.** Permitirá verificar el grado de cumplimiento de un cliente con respecto a las condiciones de seguridad que se establecen en esta guía.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

9. Para entender esta guía de seguridad es conveniente explicar el proceso de refuerzo de la seguridad que describe, así como los recursos que proporciona. Esta guía define los procesos que le ayudarán a realizar la instalación de un servidor de impresión sobre Microsoft Windows Server 2012 R2. La guía tiene en consideración que ha realizado la implementación de los mismos y sí le ayudará a implementar la seguridad de los mismos teniendo en consideración lo dispuesto en el ENS.

4.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

10. Los contenidos de esta guía son de aplicación para servidores con Sistemas Operativos Microsoft Windows Server 2012 R2.
11. Debido a la importancia, se reitera que se asume que la instalación del servidor de impresión se realiza sobre un servidor miembro preparado en base a las indicaciones de la guía CCN-STIC-870A Implementación del ENS en Microsoft Windows Server 2012 R2.
12. La guía ha sido desarrollada y probada en entorno de uso de servicios Microsoft y aplicaciones de puesto de trabajo convencionales, 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.

13. Esta guía se ha diseñado para reducir la superficie de exposición de los servidores de impresión y siguiendo las pautas establecidas en el Esquema Nacional de Seguridad.
14. La guía de seguridad ha sido elaborada utilizando un laboratorio basado en una plataforma de virtualización tipo Hyper-V con las siguientes características técnicas:
 - Servidor Dell PowerEdge™ T320:
 - Intel Pentium Xeon CPU ES 2430 2.20GHz.
 - HDD 1TB.
 - 64 GB de RAM.
 - Interfaz de Red 1 Gbits/s.
15. 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. Tenga en cuenta que estos requerimientos son adicionales a los que se establecen para la instalación de sistema operativo sin servidor de impresión. No están soportados los procesadores Itanium de 64 bits.
16. 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, características o funcionalidad de aplicaciones a ejecutar en Microsoft Windows Server 2012 R2.
17. Para garantizar la seguridad de los puestos de trabajo, deberán instalarse las actualizaciones recomendadas por el fabricante, disponibles a través del servicio de Microsoft Update. Las actualizaciones por lo general se liberan los segundos martes de cada mes, no obstante, hay que tener presente que determinadas actualizaciones por su criticidad pueden ser liberadas en cualquier momento. Se deberá tener en cuenta la implementación de las actualizaciones tanto para el sistema operativo como para los diferentes servicios instalados.
18. 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 en ocasiones se realizan para las distintas actualizaciones de seguridad.
19. Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado, donde se habrán aplicado los test y cambios en la configuración que se ajustan a los criterios específicos de cada organización.
20. El espíritu de estas guías no está dirigido a remplazar políticas consolidadas y probadas de las organizaciones, sino servir como la línea base de seguridad que deberá ser adaptada a las necesidades propias de cada organización.

5. INTRODUCCIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

21. 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.
22. 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 constituidos por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información”.
23. Las mejoras introducidas en la Ley 11/2007 sobre la relación entre la Administración Pública con los ciudadanos y entre las diferentes Administraciones Públicas, haciendo uso de la tecnología, requería de la implementación de unos mecanismos que no solo garantizaran la usabilidad de los servicios sino su seguridad. Esta se debía hacer extensible tanto al mantenimiento y gestión de la información como a los procesos de comunicación.
24. 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.
25. Debe tomarse en consideración adicionalmente que en el año 2015 se hace público el Real Decreto 951/2015 sobre la modificación del Real Decreto 3/201 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad. Dicho Real Decreto, modifica entre otras consideraciones algunas medidas de índole técnicas que han sido contempladas en la presente guía de seguridad.
26. 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 técnicas para aplicar las condiciones de seguridad necesarias.
27. 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.
28. 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 implementadas 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.

29. Para lograr este cumplimiento, se exigen una serie de requisitos mínimos que deberán quedar definidos en la política de seguridad:
- Organización e implantación del proceso de seguridad:
 - Análisis y gestión de riesgos.
 - Gestión de personal.
 - Autorización y control de los accesos.
 - Protección de las instalaciones.
 - Adquisición de productos.
 - Seguridad por defecto.
 - Integridad y condiciones para mantener los sistemas y servicios actualizados.
 - Confidencialidad de la información almacenada.
 - Registro de actividad.
 - Incidentes de seguridad.
 - Continuidad de la actividad.
 - Mejora continua del proceso de seguridad.
30. 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 cuenta para mantener siempre los sistemas en un correcto estado de funcionalidad y garantizando la protección de los mismos.
31. 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 medidas de índole organizativas y técnicas 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.
32. 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

33. 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 para los mismos.
34. 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.
35. 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 el 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 a 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 como tener en consideración todo el perjuicio que sobre esas personas pudiera recaer por una mala práctica.
36. Atendiendo a la capacidad de la administración pública para establecer mecanismos y controles sobre sus sistemas y servicios, se definieron 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 y la información. Las dimensiones de seguridad recogidas en el ENS son cinco:

- Disponibilidad (D)
 - Autenticidad (A)
 - Integridad (I)
 - Confidencialidad (C)
 - Trazabilidad (T)
37. Conocidos 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 técnico, organizativo 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.
38. 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 para cada una de ellas.

5.1.1 DISPONIBILIDAD

39. La disponibilidad establece la necesidad para 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 para 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.
40. La implementación de mecanismos para garantizar la disponibilidad, no solo tiene sentido en la aplicación de medidas de índole tecnológicas, 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 haber definido y escrito un mecanismo para recuperar la misma en sistemas alternativos ante la posibilidad de que por un problema severo, como pudiera ser un terremoto, anulara los sistemas originales donde se prestaban los servicios.
41. Dentro de las necesidades para el cumplimiento efectivo de la disponibilidad, el ENS, requiere el establecimiento de medidas que podrían afectar a diferentes condicionantes.
- Dimensionamiento de los servicios.
 - Usos de sistemas, medios, instalaciones y personal alternativos.
 - Copias de seguridad.
 - Condiciones de mantenimiento del suministro eléctrico.
 - Protección frente a incendios o inundaciones.
42. 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 técnicas 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

43. Dentro del planteamiento de la seguridad en el acceso a los sistemas de la información, uno de los primeros a los que se enfrenta cualquier usuario es el de 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 en 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.
44. Los procesos de autenticación, deben verse siempre como una garantía para la protección de la información y no en sí mismo como una incomodidad.
45. No obstante, aunque el proceso de autenticación es uno de los más evidentes, debe entender la dimensión de “Autenticidad” como un elemento mayor, donde evidentemente el proceso de autenticación y todo lo que conlleva, presenta 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.
46. El proceso de autenticidad además se encuentra 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 responsabilidades necesarias.
47. 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.
48. Dentro de los factores para la autenticidad, pueden encontrarse los relativos a:
 - Identificación de ciudadanos o usuarios frente a los servicios.
 - Procesos de registros de acceso.
 - Mecanismos que garanticen la segregación de funciones.
 - Establecimiento de mecanismos de autenticación.
 - Implementación de mecanismos de accesos locales o remotos.
 - 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

49. Un 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.

50. 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 lo corresponde la implementación de medidas enfocadas a firmar digitalmente documentos administrativos.

5.1.4 CONFIDENCIALIDAD

51. 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.
52. 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.
53. 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 cifrado, tales como HTTPS. Estos son la alternativa a protocolos inseguros por el envío en claro como el propio protocolo HTTP.
54. 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.
55. 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

56. A menudo cuando se ha producido una incidencia, lo que resta es poder determinar que ha pasado, con objeto de aplicar así las medidas correctoras adecuadas. Para que el análisis pueda ser llevado a cabo será necesario disponer información. La dimensión de seguridad de trazabilidad definida en el Esquema Nacional de 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.
57. 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:
- Procesos de identificación y control de acceso.
 - Segregación y cumplimiento de funciones.
 - Mecanismos de autenticación.
 - Accesos locales y remotos.

- Registros de la actividad de los usuarios.
 - Empleo de marcas de tiempo.
58. Es importante establecer que no basta con garantizar que se produzcan los registros y que estos se encuentren disponibles, sino también la integridad de los mismos dando validez a los mismos 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.
59. 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, deberán además encontrarse asegurados por medidas de confidencialidad e integridad.

5.2 NIVELES DE DIMENSIONES DE SEGURIDAD

60. El conjunto de los servicios que presta un 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.
61. 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).
62. 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.
63. 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
64. A efectos de valoración para determinar cuáles son los niveles de seguridad, tal y como se describe en la propia guía de seguridad “CCN-STIC-803 Esquema Nacional de Seguridad valoración de los sistemas, se deberá diferenciar siempre la información del servicio. Ambos son de aplicación, pero se deben valorar de forma independiente.

65. La información según establece el ENS es cualquier dato que es relevante para el proceso administrativo y pueden ser tratados 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.
66. La valoración de la información la determina el responsable de la misma, teniendo en cuenta la naturaleza de la información y la normativa que pudiera serle de aplicación. Esta valoración requiere de un conocimiento legal sobre la materia tratada.
67. 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.
68. Se entiende por servicio cada actividad llevada a cabo por la Administración o, bajo un cierto control y regulación de esta, a través organización especializada o no, y destinada a satisfacer necesidades de la colectividad.
69. 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 empleen 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.

70. La valoración de un servicio la determina el responsable del mismo teniendo en cuenta 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; es decir, 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.
71. A modo resumen se describe 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:
 - La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
 - El sufrimiento de un daño menor por los activos de la organización.
 - El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
 - Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.
 - 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:
 - La reducción significativa de la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
 - El sufrimiento de un daño significativo por los activos de la organización.

- El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
 - Causar un perjuicio significativo a algún individuo, de difícil reparación.
 - 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:
- La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
 - El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
 - El incumplimiento grave de alguna ley o regulación.
 - Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
 - Otros de naturaleza análoga.
72. 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. MEDIDAS DE SEGURIDAD

73. Teniendo en consideración la implementación de seguridad en función de la naturaleza y los criterios de categorización aplicables en función de niveles, se hace necesario por lo tanto establecer qué medidas deberán ser aplicada y qué modo. Uno de los apartados más extensos del RD 3/2010 radica precisamente en este punto, quedando todos recogidos en el Anexo II.
74. 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”.
75. La guía de seguridad “CCN-STIC-804 Esquema Nacional de Seguridad guía de implantación” 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 empleen recursos propios o recurran a proveedores y productos externos.

76. 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.
77. En la guía, para cada medida se proporciona:
- Una descripción más amplia que la proporcionada en el ENS.
 - Referencias externas que ayuden a su comprensión y realización.
 - Relación con medidas o controles en otros esquemas de seguridad.
 - Relación con los principios básicos recogidos en el ENS.
 - Indicaciones de lo que se considerará evidencia suficiente de cara a una evaluación de la seguridad.
78. 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:
- Marco organizativo.
 - Marco operacional.
 - Medidas de protección.

6.1 MARCO ORGANIZATIVO

79. 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 técnicos y facultan a la organización para adquirir la capacidad para organizarse y asegurar así el cumplimiento de sus objetivos.
80. Debe 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 aprende de la experiencia, se corrigen defectos o debilidades y se busca 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.
81. 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.
82. Las subcategorías en las que se divide el marco organizativo son cuatro:
- Política de seguridad.
 - Normativa de seguridad.
 - Procedimientos de seguridad.
 - Proceso de autorización.

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

83. 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 LOPD. Por ello deberá tenerse en cuenta 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.
84. 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 organizativas.
85. Puesto que la presente guía se encuadra dentro de la implementación de medidas enfocadas a la protección de servidores Microsoft Windows Server 2012 R2 y el alcance de las medidas aplicables dentro del marco organizativo no son específicamente técnicas, la implementación de este marco no se abordará en esta guía.

6.2 MARCO OPERACIONAL

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

- Planificación.
- Control de acceso.
- Explotación.
- Servicios externos.
- Continuidad del servicio.
- Monitorización del sistema.

				op	Marco operacional
				op.pl	Planificación
categoria	n.a.	+	++	op.pl.1	Análisis de riesgos
categoria	aplica	=	=	op.pl.2	Arquitectura de seguridad
categoria	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoria	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 login)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (remote login)
				op.exp	Explotación
categoria	aplica	=	=	op.exp.1	Inventario de activos
categoria	aplica	=	=	op.exp.2	Configuración de seguridad
categoria	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoria	aplica	=	=	op.exp.4	Mantenimiento
categoria	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoria	aplica	=	=	op.exp.6	Protección frente a código dañino
categoria	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
categoria	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
categoria	aplica	=	+	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoria	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoria	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
categoria	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoria	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

87. Algunas de las medidas de seguridad aplicables a través de la presente guía en un entorno de Microsoft Windows Server 2012 R2, vienen definidas por la aplicación de condiciones a través del marco operacional. En páginas posteriores se tratarán y definirán como realizar su aplicación a través de la aplicación de plantillas y consideraciones que deberán ser tenidas en cuenta.

6.3 MEDIDAS DE PROTECCIÓN

88. Las medidas de protección constituyen el grueso de aplicación de las medidas de índole técnico. 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.

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

- Protección de las instalaciones e infraestructuras.
- Gestión de personal.

- Protección de los equipos.
- Protección de las comunicaciones.
- Protección de los soportes de comunicación.
- Protección de las aplicaciones informáticas.
- Protección de la información.
- Protección de los servicios.

				mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoria	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoria	aplica	=	=	mp.if.2	Identificación de las personas
categoria	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
categoria	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
categoria	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoria	aplica	=	=	mp.per.2	Deberes y obligaciones
categoria	aplica	=	=	mp.per.3	Concienciación
categoria	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoria	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoria	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos
				mp.com	Protección de las comunicaciones
categoria	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
categoria	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
categoria	aplica	=	=	mp.si.3	Custodia
categoria	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoria	n.a.	aplica	=	mp.sw.1	Desarrollo
categoria	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoria	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
categoria	aplica	=	=	mp.s.1	Protección del correo electrónico
categoria	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

90. Algunas de las medidas de seguridad aplicables a través de la presente guía, en una implantación de Servidor de impresión sobre Microsoft 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.

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

91. 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:
- Dimensiones de seguridad.
 - Niveles de seguridad.
 - Naturaleza de las medidas.
92. 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.
93. Para tener en consideración la descripción de la tabla, tómese 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
------	--------	---	----	----------	----------------------------

94. 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.
95. 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 a 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”, indica 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.
96. 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.
97. 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.

98. La última de las columnas refiere 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.
99. El siguiente punto de la presente guía establecerá las diferentes medidas a aplicar sobre un Servidor de impresión sobre Microsoft Windows Server 2012 R2. Dichas medidas tendrán en consideración tanto lo dispuesto en el propio RD 3/2010, el RD 951/2015, así como las diferentes guías ya publicadas de la serie CCN-STIC-800 en materia de ENS.

7. ARQUITECTURA Y SEGURIDAD DEL SERVIDOR DE IMPRESIÓN

100. Los servicios de impresión de Microsoft Windows Server 2012 R2 permiten compartir impresoras en una red y centralizar las tareas de administración del servidor de impresión y las impresoras de red mediante el complemento de administración de impresión, que ayuda a supervisar las colas de impresión y a recibir notificaciones cuando dichas colas interrumpen el procesamiento de los trabajos de impresión.
101. Además, permite migrar los servidores de impresión e implementar conexiones de impresora con directivas de grupo.
102. En Microsoft Windows Server 2012 R2 se mantienen algunas de las mejoras que ya se incorporaron en Microsoft Windows Server 2008 R2, las cuales se describen a continuación:
 - Capacidad integrada para la implementación de impresoras con la directiva de grupo. Puede usar la consola de administración de impresión con directivas de grupo para implementar automáticamente conexiones de impresora para usuarios o equipos e instalar los controladores de impresoras apropiados. Esta función apareció por primera vez en Microsoft Windows Server 2003 R2, pero requería el uso de la herramienta “PushPrinterConnections.exe” en un script de inicio (en conexiones por equipo) o en un script de inicio de sesión (en conexiones por usuario). Ahora esta funcionalidad está incluida en los equipos cliente que ejecutan Microsoft Windows 7 y Microsoft Windows Server 2012 y superior. Asimismo, estos sistemas operativos ahora pueden recibir conexiones de impresora por usuario durante las operaciones de actualización de la directiva de grupo en segundo plano.
 - Capacidad de importación y exportación de las colas de impresión. Puede usar el asistente para migración de impresoras o la herramienta de línea de comandos “Printbrm.exe” para exportar colas de impresión, configuraciones de impresora, puertos de impresora y monitores de idioma y, después, importarlos en otro servidor de impresión que ejecute un sistema operativo Microsoft Windows Server 2012 R2. Este procedimiento es una forma eficaz de consolidar varios servidores de impresión o reemplazar un servidor de impresión antiguo. El Asistente para migración de impresoras y la herramienta de línea de comandos “Printbrm.exe” sustituyen a “Print Migrator 3.1”.

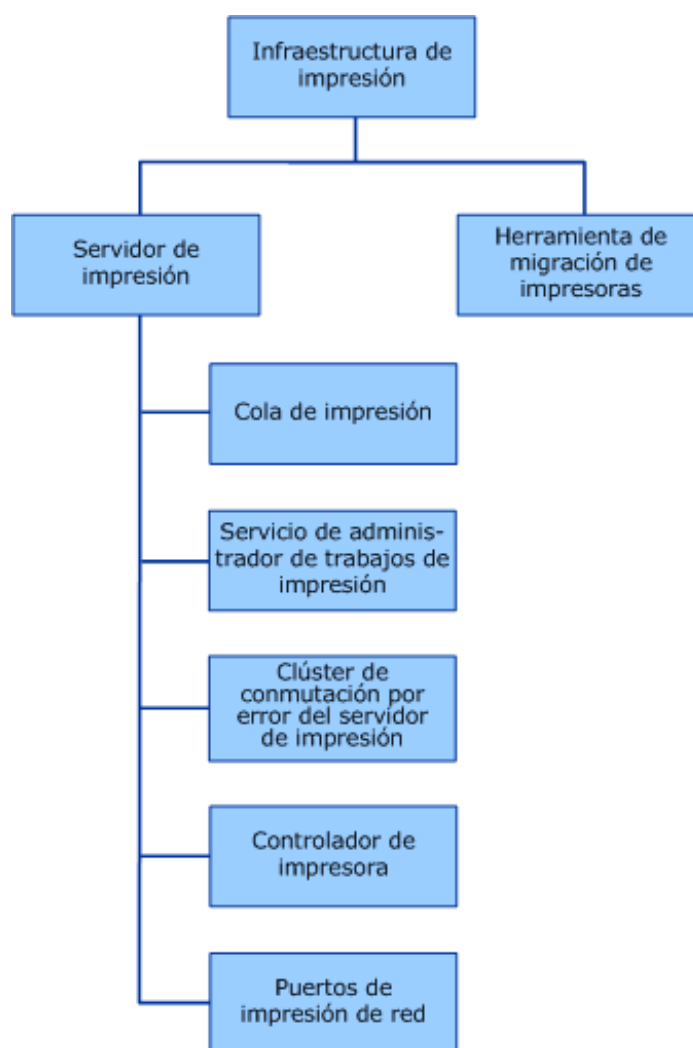
- Mejora de las descripciones de los eventos del Visor de eventos y de la información de la resolución. Se han redactado de nuevo todas las descripciones de los eventos relacionados con la impresión que aparecen en el visor de eventos con objeto de aumentar su utilidad para la comprensión y la solución de problemas de impresión. Además, si se hace clic en el vínculo “ayuda en línea” del registro de eventos mientras se está viendo un evento, aparece en un explorador web información detallada del evento referente a cómo diagnosticar un problema y resolverlo, y también acerca de cómo comprobar si el problema se corrigió correctamente.
- Mejoras de la seguridad en la instalación de controladores de impresora. La configuración de seguridad predeterminada de Microsoft Windows Server 2012 R2 permite a los usuarios que no sean miembros del grupo local Administradores instalar solamente controladores de impresora de confianza, como los que se incluyen en Windows o en paquetes de controladores de impresoras firmados digitalmente. Esto ayuda a garantizar que los usuarios no puedan instalar controladores de impresora no probados o no confiables, o en los que se haya incorporado código dañino.
- No obstante, este aumento de seguridad implica que algunos usuarios no podrán instalar el controlador apropiado para una impresora compartida, incluso si el controlador ha sido probado y aprobado en su entorno. Para permitir que usuarios que no sean miembros del grupo local Administradores puedan conectarse a un servidor de impresión e instalar controladores de impresora hospedadas en el servidor, puede usar uno de estos métodos:
 - Instalar paquetes de controladores de impresoras en el servidor de impresión.
 - Usar la directiva de grupo para implementar conexiones de impresora en usuarios o equipos.
 - Usar la directiva de grupo para modificar la configuración de seguridad del controlador de impresora.
- Mejoras de los filtros de impresora en Administración de impresión. En la consola de administración de impresión, los filtros permiten mostrar solamente aquellas impresoras que cumplan un conjunto concreto de criterios. Por ejemplo, puede resultar conveniente filtrar las impresoras que cumplan determinadas condiciones de error o las impresoras de un grupo de edificios, con independencia del servidor de impresión que usen. Los filtros se almacenan en la carpeta “Filtros personalizados” de impresora del árbol de “Administración de impresión” y son dinámicos, por lo que los datos siempre están actualizados.
- Los filtros se han mejorado en Microsoft Windows Server 2012 R2 en dos sentidos:
 - Filtro personalizado Todos los controladores. Un filtro predeterminado nuevo que presenta todos los controladores instalados en el servidor seleccionado, así como sus versiones.
 - Aumento del número de criterios de filtrado a seis. Al aumentar el número de criterios de filtrado desde el límite anterior de tres, ahora es posible crear filtros más específicos.

- Integración del “Administrador del servidor”. En Microsoft Windows Server 2012 R2, se puede usar el administrador del servidor para instalar la función del servidor “Servicios de impresión”, servicios de funciones opcionales y otras características. El administrador del servidor también muestra eventos relacionados con la impresión desde el visor de eventos e incluye una instancia del complemento administración de impresión que solamente puede administrar el servidor local.
- Los servicios de impresión se implementan en Microsoft Windows Server 2012 R2 como una función de servidor del administrador del servidor con los siguientes servicios de función secundarios:
 - Servidor de impresión.
 - Servicio Line Printer Daemon (LPD).
 - Impresión en Internet.
- A partir de Microsoft Windows Server 2012 R2 se desusa el protocolo Line Printer Daemon (LPR/LPD). Con el tiempo se quitará esta característica, los clientes que imprimen en un servidor que usa este protocolo, como los clientes de UNIX, no podrán conectarse ni imprimir. En su lugar, los clientes de UNIX deberían usar el IPP. Los clientes de Windows se pueden conectar con impresoras UNIX compartidas mediante el Monitor de puerto estándar de Windows.
- Aislamiento de controladores de impresora. Antes de Microsoft Windows 7 y Microsoft Windows Server 2008 R2, el error de los componentes de controladores de impresora era un problema principal en la compatibilidad con servidores de impresión. El error de un controlador de impresora cargado en un proceso de administrador de trabajos de impresión producía un error en el proceso, lo que llevaba a una interrupción de todo el sistema de impresión. El impacto de un error en el administrador de trabajos de impresión en un servidor de impresión es particularmente significativo por el gran número de usuarios e impresoras a los que afecta.
- En Microsoft Windows 7 y Microsoft Windows Server 2012 R2, ahora se pueden configurar los componentes de controlador de impresora para que se ejecuten en un proceso aislado independiente del proceso del administrador de trabajos de impresión. Al aislar el controlador de impresora se evita que un controlador de impresora defectuoso detenga todas las operaciones de impresión en un servidor de impresión, lo que resulta en una mayor confiabilidad del servidor.
- Además del beneficio de mejorar toda la estabilidad del sistema de impresión, esta nueva característica ofrece un medio para aislar nuevos controladores de prueba y de depuración, así como para identificar los controladores de impresora que están causando problemas en el administrador de trabajos de impresión.
- Impresión con reconocimiento de ubicación de red. En Microsoft Windows 7, el valor Impresora predeterminada reconoce la ubicación de red. Un usuario de portátil o teléfono móvil puede establecer una impresora predeterminada diferente para cada red a la que se conecte. Es posible tener una impresora predeterminada para el hogar y otra impresora predeterminada para la oficina. Su portátil puede seleccionar automáticamente la impresora predeterminada correcta, según la ubicación actual del usuario.

103. Para usar la consola de “Administración de impresión” en Microsoft Windows Server 2012 R2, se debe instalar la función servidor de impresión en el equipo donde desea usar la administración de impresión.
104. Para implementar conexiones de impresora con la directiva de grupo, el entorno debe cumplir los siguientes requisitos:
 - El esquema de servicios de dominio de Directorio Activo (AD DS) debe usar una versión de esquema de Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012 o Microsoft Windows Server 2012 R2.
105. Requisitos de seguridad:
 - Para administrar un servidor de impresión remoto, debe ser miembro de los grupos “Ops. de impresión” u “Ops. de servidores”, o del grupo local “Administradores” en el servidor de impresión remoto. Estas credenciales no son necesarias para supervisar los servidores de impresión remotos, aunque algunas funciones estarán deshabilitadas.
 - Para usar la consola de administración de impresión (Printmanagement.msc) con la directiva de grupo, debe ser miembro del grupo local Administradores y tener acceso de escritura a los objetos de directiva de grupo (GPO) en el dominio de AD DS o la unidad organizativa donde desea implementar las conexiones de impresora.
 - Se recomienda a los administradores que usen una cuenta con permisos restrictivos para realizar tareas rutinarias no administrativas, y usar una cuenta con más permisos sólo cuando realicen tareas administrativas específicas.

7.1 COMPONENTES Y ENTIDADES DE LOS SERVICIOS DE IMPRESIÓN

106. La infraestructura de impresión de un servidor permite que usuarios locales y remotos ejecuten trabajos de impresión en el propio servidor, así como administrar las impresoras y todos sus aspectos relacionados con la impresión.
107. A continuación, se muestra una estructura jerárquica de las entidades administradas en los servicios de impresión de Microsoft Windows Server 2012 R2.

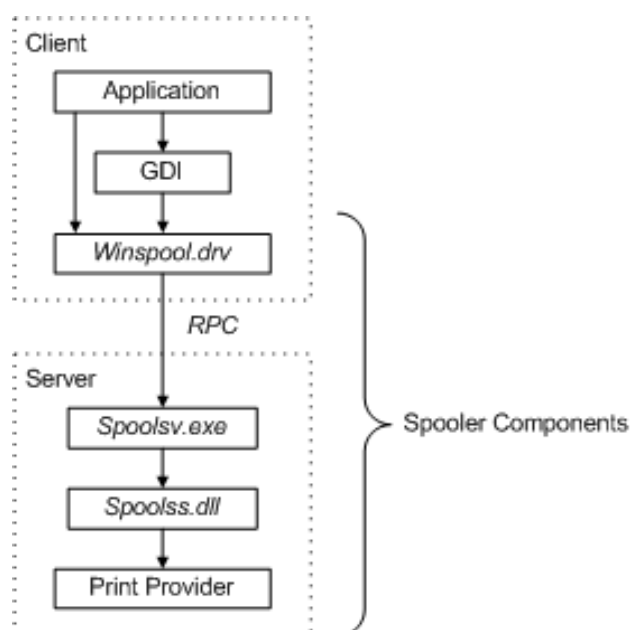


108. A continuación, se detallan algunos elementos de la estructura jerárquica de las entidades administradas en los servicios de impresión de Microsoft Windows Server 2012 R2.

- Cola de impresión (Print Queue). Una cola de impresión es una representación de un dispositivo de impresión o impresora física en Microsoft Windows. Cuando se abre la cola de impresión se muestran todos los trabajos activos y su estado.
- Servicio de cola de impresión (Print Spooler Service). Cada servidor de impresión dispone de un único servicio de cola de impresión, el cual gestiona todos los trabajos de impresión y las colas que están configuradas en dicho servidor.
- Clúster de conmutación por error de servicios de impresión (Print Server Failover Clúster). Un clúster es un grupo de servidores independientes que funcionan en conjunto para incrementar la disponibilidad del servicio de impresión u otros servicios. Si uno de los servidores falla, otro de los miembros del clúster asume la responsabilidad del servicio. En esta guía no se contempla la instalación de un clúster de conmutación por error para los servicios de impresión.
- Controlador de impresora (Printer Driver). El controlador de impresora es el software del fabricante que permite que Microsoft Windows Server 2012 R2 interactúe con el hardware de impresión. Cada impresora que se instale requiere de un controlador de impresora asociado al fabricante, modelo y versión de dicha impresora.

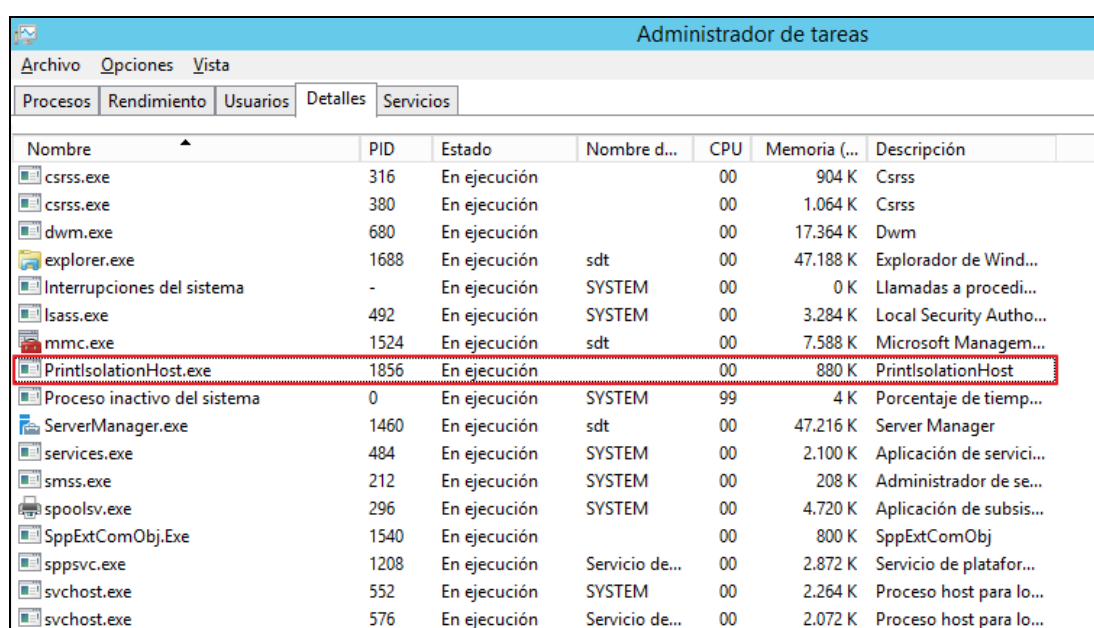
7.2 AISLAMIENTO DE CONTROLADORES DE IMPRESIÓN

109. Como su nombre indica, el aislamiento de controladores de impresión en Microsoft Windows Server 2012 R2 permite que algunos de los componentes del controlador se ejecuten en un proceso o procesos separados de la cola de impresión.
110. De esta forma, cualquier problema o error asociado con controladores defectuosos se aíslan del servicio de cola de impresión y no afecta al resto de los procesos.
111. En Windows Server, el servicio de impresión se compone de dos elementos básicos, la cola de impresión y los controladores de impresoras.
112. La cola de impresión es el componente principal y se ejecuta en el proceso “spoolsvc.exe”, el cual se inicia junto con el sistema y continúa en ejecución hasta que el sistema se apaga.
113. A continuación, se muestra un diagrama de los dos componentes mencionados.



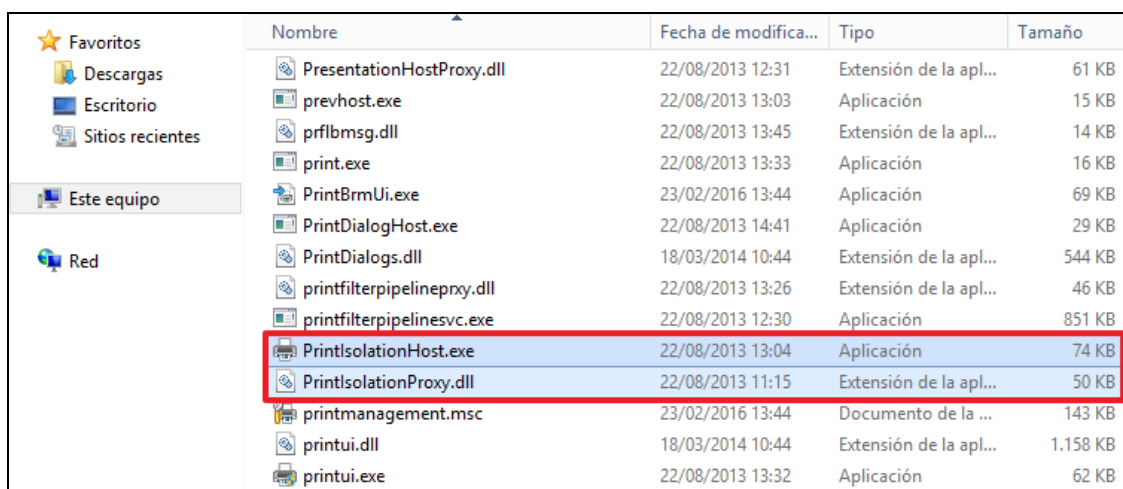
114. Con respecto al aislamiento de controladores, existen tres modos básicos de aislamiento que se pueden configurar para controladores individuales:
 - Ninguno. En este modo, los componentes del controlador de impresión se cargan en el proceso de cola de impresión. Este modo es el que se encontraba en versiones anteriores de Windows Server.
 - Compartido. En este modo, múltiples controladores se configuran para el aislamiento y se cargan en el mismo proceso compartido, el cual está a su vez separado del proceso de cola de impresión. Aunque esta arquitectura protege el proceso de cola de impresión, los controladores compartidos pueden verse afectados unos con otros.
 - Aislado. En este modo, cada controlador se carga de forma completamente aislada en su propio espacio de ejecución. Esta arquitectura protege tanto al proceso de cola de impresión como a los controladores de impresión entre sí.
115. Los modos de aislamiento se deben configurar por cada uno de los controladores de forma individual, no a nivel de todo el sistema.

116. Así mismo, es posible que ciertos controladores de impresión no puedan ejecutarse en modo de aislamiento debido a que hacen llamadas directamente a la cola de impresión o a otros módulos de configuración de la impresora.
117. Cuando se utiliza el modo de aislamiento, cada vez que se realiza una impresión se lanza un proceso denominado “PrintIsolationHost.exe”. De esta forma, el proceso de cola de impresión únicamente se limita a actuar de proxy para las llamadas del procesador de impresión y otros componentes del controlador.
118. Dentro de los procesos “spoolsv.exe” y “PrintIsolationHost.exe” se carga una librería denominada “PrintIsolationProxy.dll” que redirige las llamadas a impresoras específicas entre los procesos.
119. A continuación, se muestra un ejemplo de la ejecución en modo de aislamiento de los controladores de impresión.



Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Descripción
csrss.exe	316	En ejecución		00	904 K	Csrss
csrss.exe	380	En ejecución		00	1.064 K	Csrss
dwm.exe	680	En ejecución		00	17.364 K	Dwm
explorer.exe	1688	En ejecución	sdt	00	47.188 K	Explorador de Wind...
Interrupciones del sistema	-	En ejecución	SYSTEM	00	0 K	Llamadas a procedi...
lsass.exe	492	En ejecución	SYSTEM	00	3.284 K	Local Security Autho...
mmc.exe	1524	En ejecución	sdt	00	7.588 K	Microsoft Managem...
PrintIsolationHost.exe	1856	En ejecución		00	880 K	PrintIsolationHost
Proceso inactivo del sistema	0	En ejecución	SYSTEM	99	4 K	Porcentaje de tiemp...
ServerManager.exe	1460	En ejecución	sdt	00	47.216 K	Server Manager
services.exe	484	En ejecución	SYSTEM	00	2.100 K	Aplicación de servi...
smss.exe	212	En ejecución	SYSTEM	00	208 K	Administrador de se...
spoolsv.exe	296	En ejecución	SYSTEM	00	4.720 K	Aplicación de subsis...
SppExtComObj.Exe	1540	En ejecución		00	800 K	SppExtComObj
sppsvc.exe	1208	En ejecución	Servicio de...	00	2.872 K	Servicio de platafor...
svchost.exe	552	En ejecución	SYSTEM	00	2.264 K	Proceso host para lo...
svchost.exe	576	En ejecución	Servicio de...	00	2.072 K	Proceso host para lo...

120. Como se puede observar, por cada proceso de impresión se carga la librería de redirección de llamadas “PrintIsolationProxy.dll”.



Nombre	Fecha de modifica...	Tipo	Tamaño
PresentationHostProxy.dll	22/08/2013 12:31	Extensión de la apl...	61 KB
prevhost.exe	22/08/2013 13:03	Aplicación	15 KB
prflbmsg.dll	22/08/2013 13:45	Extensión de la apl...	14 KB
print.exe	22/08/2013 13:33	Aplicación	16 KB
PrintBrmUi.exe	23/02/2016 13:44	Aplicación	69 KB
PrintDialogHost.exe	22/08/2013 14:41	Aplicación	29 KB
PrintDialogs.dll	18/03/2014 10:44	Extensión de la apl...	544 KB
printfilterpipelineprxy.dll	22/08/2013 13:26	Extensión de la apl...	46 KB
printfilterpipelinesvc.exe	22/08/2013 12:30	Aplicación	851 KB
PrintIsolationHost.exe	22/08/2013 13:04	Aplicación	74 KB
PrintIsolationProxy.dll	22/08/2013 11:15	Extensión de la apl...	50 KB
printmanagement.msc	23/02/2016 13:44	Documento de la ...	143 KB
printui.dll	18/03/2014 10:44	Extensión de la apl...	1.158 KB
printui.exe	22/08/2013 13:32	Aplicación	62 KB

121. La configuración del aislamiento de controladores de impresión se puede realizar mediante el registro de Windows directamente o mediante directivas de grupo (GPO), encontrándose éstas en la ruta “Configuración de equipo > Directivas > Plantillas administrativas > Impresoras”. A continuación, se indican las directivas relacionadas:
- Ejecutar controladores de impresión en procesos aislados. Esta configuración de directiva determina si el administrador de trabajos de impresión ejecutará controladores de impresión en un proceso aislado o separado. Cuando se carguen controladores de impresión en un proceso aislado (o procesos aislados), un error de controlador de impresión no provocará un error del servicio del administrador de trabajos de impresión. Si se habilita o no establece esta configuración de directiva, de forma predeterminada el administrador de trabajos de impresión ejecutará controladores de impresión en un proceso aislado. Si se deshabilita esta configuración de directiva, el administrador de trabajos de impresión ejecutará controladores de impresión en el proceso del administrador de trabajos de impresión.
 - Invalidar la configuración de compatibilidad de ejecución de controlador de impresión notificada por el controlador de impresión. Esta configuración de directiva determina si el administrador de trabajos de impresión invalidará la compatibilidad del aislamiento del controlador notificada por el controlador de impresión. Esto permite ejecutar controladores de impresión en un proceso aislado, aunque el controlador no notifique una incompatibilidad. Si habilita esta configuración de directiva, el administrador de trabajos de impresión aislará todos los controladores de impresión que no renuncien a participar explícitamente en el aislamiento de controladores. Si deshabilita o no establece esta configuración de directiva, el administrador de trabajos de impresión usará el valor de la marca de compatibilidad del aislamiento de controladores notificado por el controlador de impresión.
122. Los valores de estas directivas se reflejan en los siguientes valores del registro:
- HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PrintDriverIsolationExecutionPolicy
 - HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PrintDriverIsolationOverrideCompat
123. Además de los valores indicados, se pueden controlar otros aspectos relacionados con el comportamiento del aislamiento desde los siguientes valores del registro de Windows:
- HKLM\SYSTEM\CurrentControlSet\Control\Print\PrintDriverIsolationIdleTimeout
 - HKLM\SYSTEM\CurrentControlSet\Control\Print\PrintDriverIsolationTimeBeforeRecycle
 - HKLM\SYSTEM\CurrentControlSet\Control\Print\PrintDriverIsolationMaxobjsBeforeRecycle

7.3 CONFIGURACIÓN DE LA SEGURIDAD DEL SERVIDOR DE IMPRESIÓN

124. Planear la seguridad de los servidores de impresión y determinar cómo restringir el acceso a ellos es una parte importante de la administración de los servidores de impresión.
125. En Microsoft Windows Server 2012 R2, puede delegar tareas de administración de impresión directamente a usuarios que no son administradores del sistema.

126. También puede definir la configuración de seguridad predeterminada de la impresora que se hereda al agregar nuevas impresoras al servidor de impresión.
127. Estos cambios hacen posibles las siguientes mejoras en la administración de impresoras y servidores de impresión:
- Puede controlar el acceso a recursos y equilibrar cargas de trabajo delegando determinadas tareas administrativas de impresión a usuarios sin agregarlos al grupo de seguridad Administradores.
 - Puede administrar la configuración de permisos mediante la interfaz de usuario mejorada de la pestaña seguridad en el cuadro de diálogo “Propiedades del servidor de impresión”.
 - Puede administrar la infraestructura de impresoras configurando las opciones de seguridad de impresora predeterminadas que las nuevas impresoras heredan automáticamente al agregarlas. Puede configurar las opciones por servidor para que no tenga que configurar las impresoras individualmente.
128. Los permisos del servidor de impresión controlan los niveles de acceso para los usuarios de un servidor de impresión determinado. Los permisos de impresora controlan qué tareas de impresión pueden realizar los usuarios en las impresoras agregadas recientemente que están administradas por el servidor de impresión.
129. Los administradores deben asignar estos permisos cuando sea necesario a los usuarios que no sean administradores del sistema.
130. Una vez que un administrador personaliza la configuración de seguridad para el servidor de impresión, todas las impresoras recién agregadas a este servidor de impresión heredan esta configuración de seguridad automáticamente, es decir, no se modifica la configuración de seguridad para las impresoras existentes en el servidor.
131. Los dos niveles de permisos del servidor de impresión son:
- Ver servidor. El permiso “Ver servidor” asigna la capacidad de ver el servidor de impresión. Sin este permiso, los usuarios no pueden ver las impresoras administradas por el servidor. De forma predeterminada este permiso se concede a los miembros del grupo “Todos”.
 - Administrar servidor. El permiso “Administrar servidor” asigna la capacidad para crear y eliminar colas de impresión (con controladores ya instalados), agregar o eliminar puertos y agregar o eliminar formularios. Un usuario estándar con este permiso se denomina “administrador de impresión delegado”.
132. Los tres niveles de permisos de impresora son los siguientes:
- Imprimir. El permiso “Imprimir” asigna a los usuarios la posibilidad de conectarse a impresoras e imprimir, pausar, reanudar, iniciar y cancelar sus propios documentos. De forma predeterminada, este permiso se concede a los miembros del grupo “Todos” cuando se crea una cola de impresión.
 - Administrar documentos. El permiso “Administrar documentos” asigna la posibilidad de controlar la configuración del trabajo para todos los documentos, así como pausar, reiniciar y eliminar todos los documentos.

- Administrar impresoras. El permiso “Administrar impresora” asigna la posibilidad de pausar y reiniciar la impresora, cambiar la configuración del administrador de trabajos en cola, compartir una impresora, ajustar los permisos de la impresora y cambiar las propiedades de la impresora.

133. En Microsoft Windows Server 2012 R2, la configuración de seguridad predeterminada para el servidor de impresión y la impresora es la siguiente.

Nivel de permisos	Todos	Propietario de creadores	Administradores
Imprimir	Permitir		Permitir
Administrar documentos		Permitir	Permitir
Administrar impresoras			Permitir
Ver servidor	Permitir		Permitir
Administrar servidor			Permitir

134. Los miembros del grupo “Administradores” pueden crear un administrador de impresión delegado completo asignando el permiso “Administrar servidor” a un usuario.

135. Cuando se asigna el permiso “Administrar servidor”, también se asigna automáticamente el permiso “Ver servidor”.

136. También puede delegar un subconjunto de estos permisos para crear un administrador de impresión delegado parcial.

Nota: Antes de agregar cualquier impresora al servidor, debe crear un grupo de usuarios que pueden realizar tareas de impresión delegadas y, a continuación, configurar los permisos apropiados. Si lo hace, todas las impresoras recién agregadas heredan automáticamente esta configuración y no tiene que configurar individualmente las impresoras existentes para el servidor de impresión.

137. En la tabla siguiente se enumeran las tareas de impresión que un usuario puede realizar cuando tiene asignados los permisos correspondientes en la pestaña “Seguridad” de las “Propiedades” del servidor de impresión.

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Ver la cola de impresión (en el servidor local)				Sí	
Imprimir documentos propios en la cola	Sí				

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Ver, pausar, reiniciar y cancelar todos los trabajos de impresión de una cola			Sí		
Actualizar controladores instalados o incluidos, y controladores disponibles en Windows Update, en una cola existente.		Sí			
Nota: Esto no se aplica a los entornos de impresión en clúster.					
Agregar o eliminar un formulario en una cola		Sí			
Ver las propiedades de impresora				Sí	
Ver las propiedades del servidor de impresión				Sí	
Configurar los permisos de seguridad de impresora en una cola de impresión		Sí			
Administrar el descriptor de seguridad marca setServerSecurit y Descriptor del servidor de impresión					
Agregar una cola de impresión a un servidor de impresión					Sí, cuando los controladores ya están instalados.

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Eliminar una cola de impresión de un servidor de impresión		Sí, pero solo la cola para la que tiene permisos.			
Agregar un controlador de impresión a un servidor de impresión					Sí, pero solo localmente. El usuario debe ser miembro del grupo "Administradores" para poder agregar controladores (incluso de forma remota) al servidor de impresión.
Eliminar un controlador de impresión de un servidor de impresión					Sí, pero solo para los controladores (no los paquetes de controladores)
Agregar, eliminar y configurar puertos en un servidor de impresión					Sí

Nivel de permisos	Imprimir	Administrar impresoras	Administrar documentos	Ver servidor	Administrar servidor
Agregar y eliminar un formulario en un servidor de impresión		Un usuario que tiene asignados los permisos Administrar impresoras, pero no Administrar servidor, puede agregar un formulario cuando AllowUserManageForms está establecido en el Registro de Windows en un valor distinto de cero. Un usuario puede agregar formularios hasta el valor especificado para AllowUserManageForms. Un usuario solo puede agregar y eliminar formularios de usuario. Sin embargo, un usuario con el permiso SERVER_ACCESS_ADMINISTER puede agregar y eliminar formularios de impresora y de usuario sin ninguna limitación.			Sí
Compartir la impresora		Sí, si tiene los permisos Administrar impresora en el servidor de impresión y se han habilitado las excepciones Compartir impresoras y archivos en Firewall de Windows con seguridad avanzada			Sí, si tiene los permisos Administrar impresora en el servidor de impresión y se han habilitado las excepciones Compartir impresoras y archivos en Firewall de Windows con seguridad avanzada

138. A continuación, se muestra una lista de grupos de seguridad de impresión sugeridos y en la siguiente tabla sus permisos asociados:

- Grupo “Administradores del sistema”. Consta de los miembros del grupo de seguridad Administradores.
- Grupo “Administradores de impresión”. Consta de los miembros del grupo Administradores del sistema y los usuarios a los que se ha asignado algún conjunto de derechos de administrador de impresión delegado. Dependiendo de los derechos que asigne, los miembros de este grupo se pueden considerar administradores delegados completos o administradores delegados parciales.

139. En la tabla siguiente se muestra qué acciones se pueden realizar dependiendo de los permisos asignados:

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Ver la cola de impresión en el servidor local	Sí	Sí	Sí	Sí	Sí
Imprimir en la cola	Sí	Sí	Sí	Sí	Sí
Ver, pausar, reiniciar o cancelar trabajos de impresión que sean propiedad del usuario en una cola	Sí	Sí	Sí	Sí	Sí
Modificar todos los trabajos de impresión de una cola			Sí	Sí	Sí

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Actualizar un controlador instalado o incluido en una cola existente			Sí	Sí	Sí
Agregar o eliminar un formulario en la cola			Sí	Sí	Sí
Ver las propiedades de impresora	Sí	Sí	Sí	Sí	Sí
Ver las propiedades del servidor de impresión	Sí	Sí	Sí	Sí	Sí
Administrar el permiso de seguridad en la cola de impresión			Sí	Sí	Sí
Administrar el descriptor de seguridad <i>marca setServerSecurityDescriptor</i> del servidor de impresión					Sí

	Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
Agregar y eliminar la cola de impresión en un servidor		Sí, pero puede agregar una impresora usando solo un controlador preinstalado.	Sí, pero solo puede eliminar la cola de impresión con el permiso Administrar impresora.	Sí, pero puede agregar una impresora usando solo un controlador preinstalado.	Sí
Agregar y eliminar un controlador de impresión en un servidor		Sí, pero solo localmente. El usuario debe ser miembro del grupo Administradores para poder agregar controladores no incluidos o para agregar controladores al servidor de impresión de forma remota.		Sí, pero solo localmente. El usuario debe ser miembro del grupo Administradores para poder agregar controladores no incluidos o para agregar controladores al servidor de impresión de forma remota.	Sí
Agregar, eliminar y configurar puertos en un servidor de impresión		Sí		Sí	Sí
Agregar y eliminar un formulario en un servidor de impresión		Sí		Sí	Sí

Usuarios estándar: pueden conectarse a impresoras e imprimir sus documentos (Permisos: Imprimir, Ver servidor)	Administradores delegados parciales: pueden agregar impresoras (Permisos: Imprimir, Ver servidor, Administrar servidor)	Administradores delegados parciales: pueden administrar colas existentes (Permisos: Imprimir, Ver servidor, Administrar impresoras, Administrar documentos)	Administradores delegados completos: pueden realizar todas las tareas de impresión administrativas (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)	Administradores del sistema: pueden administrar el sistema totalmente (Permisos: Imprimir, Administrar documentos, Administrar impresoras, Ver servidor, Administrar servidor)
		Sí, si tiene los permisos Administrar impresora en el servidor de impresión y se han habilitado las excepciones Compartir impresoras y archivos* en Firewall de Windows con seguridad avanzada.	Sí, si se han habilitado las excepciones Compartir impresoras y archivos* en Firewall de Windows con seguridad avanzada.	Sí

Nota: Se recomienda que solo un miembro del grupo Administradores del sistema instale controladores. Si un administrador de impresión delegado piensa agregar o administrar colas de forma remota, el Administrador del sistema debe instalar el controlador en el siguiente directorio mediante scripts o manualmente: \\Windows\\System32\\spool\\drivers\\x64\\3

140. Más adelante en esta guía se indicarán los procedimientos para crear administradores delegados y gestionar adecuadamente los permisos de impresión en cada una de las impresoras instaladas en un servidor de impresión basado en Microsoft Windows Server 2012 R2.

7.4 DIRECTIVA DE GRUPO PARA MODIFICAR LA CONFIGURACIÓN DE SEGURIDAD DEL CONTROLADOR DE IMPRESORA

141. Tal y como se ha indicado anteriormente, la configuración de seguridad predeterminada de Microsoft Windows 7 y Microsoft Windows Server 2012 R2 permite que usuarios que no sean miembros del grupo local “Administradores” solo puedan instalar controladores de impresoras de confianza, como las ofrecidas con Windows o en paquetes de controladores de impresoras firmados digitalmente.
142. Puede usar la configuración de la directiva de grupo “Restricciones de apuntar e imprimir” para controlar la forma en que los usuarios instalan controladores de impresoras desde los servidores de impresión.

143. Esta configuración se puede usar para permitir a los usuarios conectarse únicamente a determinados servidores de impresión que sean de confianza. Puesto que este valor evita que los usuarios se conecten a otros servidores de impresión que pueden hospedar potencialmente controladores de impresión, no probados o dañinos, puede desactivar los mensajes de advertencia de instalación de controladores de impresión sin poner en riesgo la seguridad.
144. Se recomienda evaluar cuidadosamente las necesidades de impresión de los usuarios antes de establecer los servidores de impresión a los que podrán conectarse. Si los usuarios necesitan conectarse de forma ocasional a impresoras compartidas de una sucursal u otro departamento, asegúrese de que se incluyen estos servidores de impresión en la lista (si cree que los controladores de impresión instalados en los servidores son de confianza).
145. Además, puede usar la opción “Restricciones de punto y de impresión” para desactivar completamente los indicadores de advertencia, aunque este valor deshabilitará la seguridad mejorada en la instalación de controladores de impresoras de Microsoft Windows 7 y Microsoft Windows Server 2012 R2 para los usuarios.
146. Para permitir que los usuarios se conecten únicamente a determinados servidores de impresión en los que confía, la directiva “Restricciones de apuntar e imprimir” se debe habilitar y activar la casilla “Los usuarios solo pueden apuntar e imprimir en los siguientes servidores”. A continuación, se pueden escribir los nombres completos de los servidores a los cuales desea que los usuarios puedan conectarse. Separe cada nombre con un punto y coma.
147. Además, se pueden ocultar las advertencias de seguridad, para ello, en el cuadro “Al instalar los controladores para una nueva conexión” se debe seleccionar la opción “No mostrar advertencia ni indicador de elevación” y en el cuadro “Al actualizar los controladores de una conexión existente”, escoja la opción “Mostrar solo advertencia”.

Restricciones de apuntar e imprimir

Restricciones de apuntar e imprimir Valor anterior Valor siguiente

☐ No configurada Comentario:

☒ **Habilitada**

☐ Deshabilitada

Compatible con: Al menos Windows Vista

Opciones:

☒ Los usuarios solo pueden apuntar e imprimir en los siguientes servidores:

Escriba los nombres completos de los servidores separados por punto y coma

SRV01

☐ Los usuarios solo pueden apuntar e imprimir en equipos de su bosque

Indicadores de seguridad:

Al instalar los controladores para una nueva conexión: No mostrar advertencia ni indicador de elevación

Al actualizar los controladores de una conexión existente: Mostrar solo advertencia

Esta opción solo se aplica a: Windows Vista y posterior

Ayuda:

Esta configuración de directiva controla el comportamiento de Apuntar e imprimir del cliente, incluidos los avisos de seguridad para equipos con Windows Vista. La configuración de directiva solo se aplica a clientes que no sean administradores de impresión y a equipos miembros de un dominio.

Si habilita esta configuración de directiva:

- Los clientes con Windows XP y versiones posteriores solo podrán descargar componentes de controlador de impresión de una lista de servidores designados explícitamente. Si hay disponible un controlador de impresión compatible en el cliente, se establecerá una conexión a la impresora. Si no hay disponible un controlador de impresión compatible en el cliente, no se establecerá ninguna conexión.
- Los clientes con Windows Vista se pueden configurar para no mostrar las advertencias de seguridad ni los símbolos del sistema con privilegios elevados cuando los usuarios apunten e imprimen o cuando los controladores de las conexiones de impresoras necesitan actualizarse.

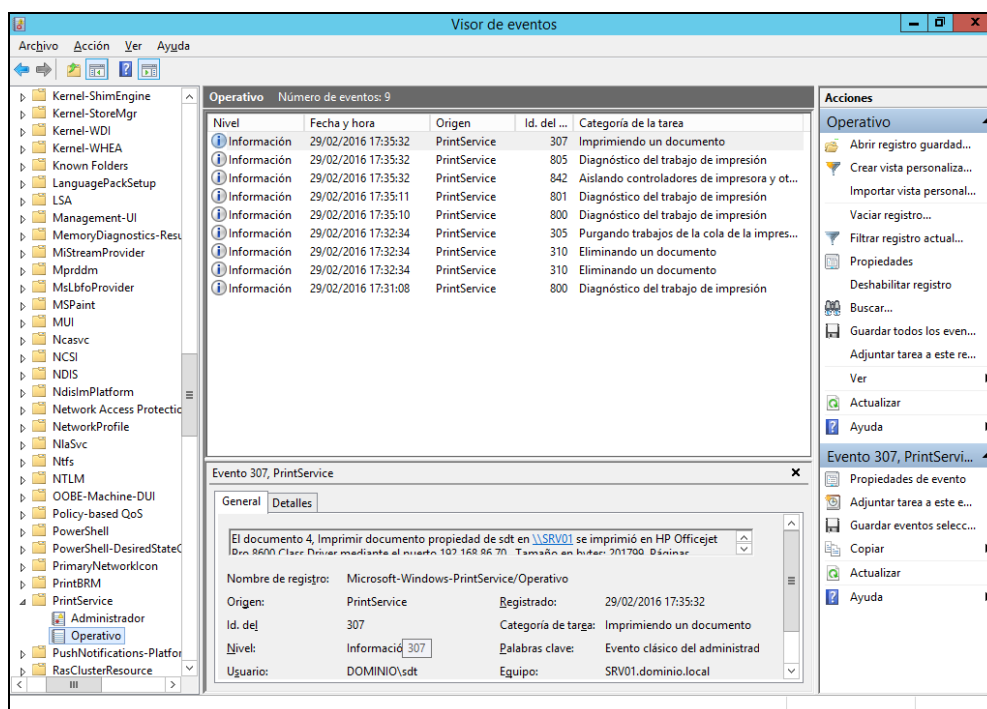
Si no establece esta configuración de directiva:

- Los equipos cliente con Windows Vista pueden apuntar e imprimir en cualquier servidor.
- Los equipos con Windows Vista mostrarán una advertencia y un símbolo del sistema con privilegios elevados cuando los usuarios creen una conexión de impresora a cualquier servidor mediante Apuntar e imprimir.

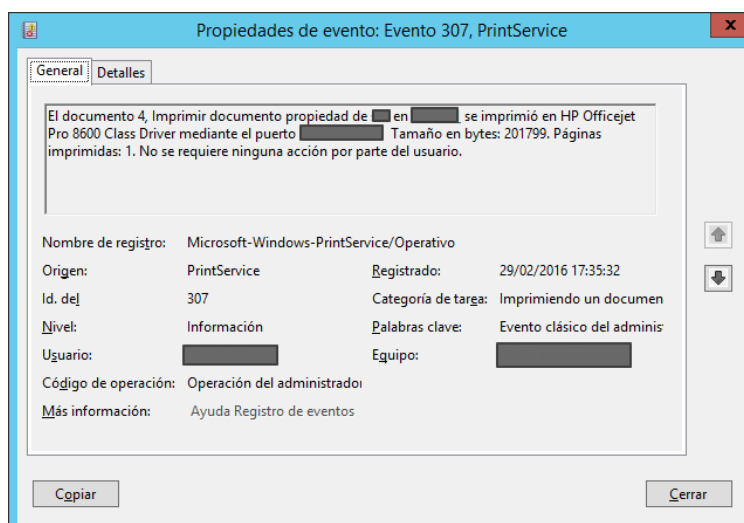
Aceptar Cancelar Aplicar

7.5 REGISTRO DE TRABAJOS DE IMPRESIÓN

148. Debido al cumplimiento de normativas o legislación, se requiere en muchos casos dejar registrado, ¿Quién ha ejecutado un trabajo de impresión con todos sus detalles?
149. Para ello, Microsoft Windows Server 2012 R2 permite habilitar el registro de operaciones con un alto nivel de detalle de los diferentes trabajos de impresión que se están ejecutando en dicho servidor.
150. Sin embargo, este registro de operaciones de impresión, por defecto no está habilitado.
151. El registro de operaciones se localiza en la consola administrativa del visor de eventos en la ruta “Inicio > Herramientas administrativas > Visor de eventos”, una vez dentro, localice “Visor de eventos (local) > Registros de aplicaciones y servicios > Microsoft > Windows > PrintService > Operativo”.



152. El evento con identificador 307 es el que indica la operación de impresión, así como el dueño del documento y la impresora en donde ha sido ejecutado.



7.6 DESPLIEGUE DE IMPRESORAS CON DIRECTIVAS DE GRUPO

153. Se puede utilizar el complemento “Administración de impresión con directiva de grupo” para implementar automáticamente conexiones de impresora para usuarios o equipos e instalar los controladores de impresora apropiados.
154. Este método de instalación de una impresora resulta útil en lugares como laboratorios, clases u oficinas sucursales, donde la mayoría de los equipos o usuarios necesitan obtener acceso a las mismas impresoras.
155. También es un método útil para la implementación de controladores de impresoras para usuarios que no son miembros del grupo local “Administradores” y ejecutan Microsoft Windows 7.
156. Para implementar conexiones de impresora con directivas de grupo, el entorno debe cumplir el siguiente requisito:
 - El esquema de servicios de dominio de Directorio Activo (AD DS) debe usar una versión de esquema Microsoft Windows Server 2012 o Microsoft Windows Server 2012 R2.
157. En las conexiones por equipo, Windows agrega las conexiones de impresora cuando el usuario inicia sesión (o cuando el equipo se reinicia si se usa la utilidad “PushPrinterConnections.exe”).
158. En las conexiones por usuario, Windows agrega las conexiones de impresora durante la actualización de la directiva en segundo plano (o cuando el usuario inicia sesión si se usa la utilidad “PushPrinterConnections.exe”).
159. Si se quita la configuración de conexión de impresora desde la GPO, Windows quita las impresoras correspondientes del equipo cliente durante la siguiente actualización de directiva en segundo plano o en el inicio de sesión del usuario (o en el siguiente reinicio o inicio de sesión si se usa la utilidad “PushPrinterConnections.exe”).
160. La utilidad “PushPrinterConnections.exe” lee la configuración de la conexión de impresora de la directiva de grupo y agrega las conexiones de impresora adecuadas al equipo o a la cuenta de usuario (o actualiza las conexiones existentes).
161. El archivo “PushPrinterConnections.exe” detecta el sistema operativo y finaliza automáticamente en los equipos que ejecutan Microsoft Windows 7 o Microsoft Windows Server 2012 R2. Estos equipos tienen compatibilidad integrada para las conexiones de impresora que se implementan con directivas de grupo, de modo que puede implementar correctamente este archivo en todos los equipos cliente de su organización.
162. En esta guía se indica cómo proceder para realizar un despliegue de impresoras mediante directivas de grupo para clientes basados en Microsoft Windows 7.

8. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN UN SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2

163. Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de un servidor de impresión y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de plantillas de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande. En este último caso, por ejemplo, para la segregación de roles, se detallarán procedimientos y condiciones que deberá aplicar un operador de una organización para hacerlas efectivas.
164. Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta Microsoft para el servidor de impresión, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de objetos de políticas de grupo (GPO) o las innatas a la gestión del sistema.
165. Para un mejor entendimiento de las medidas éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a los niveles que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de los diferentes niveles de seguridad.

8.1 MARCO OPERACIONAL

8.1.1 CONTROL DE ACCESO

166. El control de acceso cubre todo el conjunto de acciones que bien preparatorias o ejecutivas orientadas a determinar qué o quién puede o no acceder a un recurso del sistema, mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará que nadie accederá a recursos sin la debida autorización. Adicionalmente se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.
167. Toda medida de control de acceso busca el equilibrio entre la usabilidad y la protección del sistema. De tal forma que la seguridad se irá incrementando en base al nivel exigido. Por lo tanto, se requiere una menor exigencia de seguridad para el nivel bajo mientras que en el nivel medio y alto se requiere una mayor exigencia.

8.1.1.1 OP. ACC. 2. REQUISITOS DE ACCESO

168. Los requisitos de acceso se aplican desde el nivel bajo y atenderán a la necesidad que los recursos del sistema queden protegidos con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de los derechos de acceso suficientes.
169. Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad para la organización, a través de la persona responsable de dicha determinación y haciendo uso de las tecnologías necesarias.

170. Desde el punto de vista tecnológico, esta medida abarca un gran número de actividades, de tal forma que los puntos de control para restringir o conceder un acceso son abundantes. Realizar administración del Directorio Activo, acceder a un fichero o una carpeta o imprimir en un recurso, son acciones que pueden ser controladas y determinar para ello los permisos asignados.
171. La plantilla de seguridad, recoge una serie de permisos que serán asignados con objeto de limitar las acciones por parte de usuarios y administradores. De esta forma y controlando los requisitos de acceso, se reducirán todos aquellos riesgos del uso habitual de administración de un puesto de trabajo.
172. Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Microsoft para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia
173. Se deberá tener en consideración debido a dicha norma que los permisos otorgados a los usuarios serán los mínimos requeridos no siendo necesario que estos posean permisos adicionales para la tarea que van a realizar. Por ejemplo, si un usuario tiene permiso de impresión en un dispositivo, no por ello implica que sea necesario que posea el permiso de “Control total”. Con la concesión de este permiso se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de imprimir se debe considerar como la opción más óptima desde el punto de vista del ENS.

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

174. Aplicable a partir del nivel medio, se considera un requerimiento importante para una organización la segregación de funciones en base a la actividad. De esta forma se establece cadenas de autorización y control enfocadas a evitar la existencia de una única persona autorizada y que ésta pueda abusar de sus derechos para cometer alguna acción ilícita.
175. Desde el punto de vista formal la segregación de funciones deberá realizarse al menos para las siguientes tareas:
 - Desarrollo de operación.
 - Configuración y mantenimiento del sistema de operación.
 - Auditoría o supervisión de otra función.
176. Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura y puesta en marcha de la guía “CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2”.

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

177. Estas medidas requieren consolidación de los derechos de acceso, de tal forma que:
 - Exista la aplicación del mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para poder cumplir las obligaciones.

- Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
 - 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.
178. De esta forma el principio de mínima exposición y menor privilegio se puede materializar de forma extensiva a los propios administradores de los servidores y servicios que gestiona la organización.
179. Se deberán establecer así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda imprimir contenido por un dispositivo de impresión no autorizado. Se establece por lo tanto a nivel de dispositivos de impresión el aplicar mecanismos de ACL para permitir la impresión de contenido a los usuarios que los requieran exclusivamente

8.1.2 EXPLOTACIÓN

180. Se incluyen en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define a través de ellas una serie de procesos tanto para el control, como para la gestión que deberán llevarse a cabo por parte de las entidades.
181. Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

8.1.2.1 OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

182. Los dispositivos de impresión antes de su entrada en producción, deberán configurarse de tal forma que:
- Se retiren cuentas y contraseñas estándar.
 - Se aplicará la regla de mínima funcionalidad.
 - Se deshabilitarán protocolos adicionales innecesarios para el correcto funcionamiento del dispositivo de impresión, tales como, SMTP, Telnet, etc.
183. Se considera indispensable que el dispositivo de impresión no deberá proporcionar funcionalidades gratuitas. Solamente las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello se eliminarán o desactivarán mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias e incluso aquellas que sean inadecuadas para el fin que se persigue.
184. Para el cumplimiento de este sentido las diferentes plantillas de seguridad, se dotarán de las funcionalidades necesarias para deshabilitar y configurar todos aquellos servicios que, no siendo necesarios para ningún entorno operativo, pudieran constituir un riesgo de seguridad. Adicionalmente se protegerán los más importantes de tal forma que quedarán configurados a través de las políticas de grupo que correspondieran por niveles. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

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

8.1.2.2 OP. EXP. 5. GESTIÓN DE CAMBIOS

186. En el nivel bajo del ENS se recomienda mantener un control de los cambios realizados en el sistema, y en los niveles medio y alto de seguridad se deberá mantener un control continuo de los cambios realizados en el sistema, por lo que, todos los cambios anunciados por el proveedor o fabricante de los controladores de los dispositivos de impresión, deberán ser analizados previamente para establecer su conveniencia en la incorporación al sistema o no.
187. Previamente a la puesta en producción de una modificación, se ha de comprobar su correcta funcionalidad en el sistema en un entorno que no esté en producción, este entorno debe ser un fiel reflejo del entorno de producción.
188. Todos los cambios realizados deben ser planificados con anterioridad para minimizar en la medida de lo posible el impacto sobre la prestación de los servicios afectados.
189. Se ha de tener en consideración mediante un análisis de riesgos si los cambios a realizar son de mayor o menor relevancia para la seguridad del sistema, por ello, aquellos cambios que impliquen una situación de riesgo de nivel alto deberán ser aprobados explícitamente de forma previa a su implantación.

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

190. Aplicable en los niveles medio y alto de seguridad establecidos en el ENS, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:
- Quién realiza la actividad, cuándo la realiza y sobre qué.
 - 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.
 - Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.
 - La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.
 - El nivel alto requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.
191. El servidor de impresión, implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que de forma predeterminada los datos son almacenados localmente. Existen no obstante mecanismos nativos para la suscripción y recolección de evento. La guía “CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2” permitirá establecer los procedimientos para la recogida y análisis de los registros de auditoría, desde múltiples sistemas, permitiendo establecer mecanismos de correlación.

8.2 MEDIDAS DE SEGURIDAD

192. Este conjunto de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que se incluye una gran variedad de las mismas que son aplicables desde las más puramente procedimentales, a las puramente físicas o de aplicación técnica.
193. Solo estas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado son de aplicación sobre las funcionalidades del propio rol de servidor de impresión.
194. Se considera en este sentido que la organización ha dispuestos todos aquellos mecanismos de control físico necesarios, con objeto evitar el acceso a los equipos de escritorio existentes por parte de personal no autorizado.

8.2.1 PROTECCIÓN DE LAS COMUNICACIONES

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

8.2.1.1 MP. COM. 2. PROTECCIÓN DE LA CONFIDENCIALIDAD

196. Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberá prevenirse ataques activos, garantizando que los mismos serán al menos detectados, permitiendo activarse los procedimientos que se hubieran previsto en el tratamiento frente a incidentes.
197. En aquellas organizaciones que les sea de aplicación cualquier nivel del ENS deberán tener en consideración la implementación en los dispositivos de impresión, de un sistema de seguridad de impresión mediante código o tarjeta identificativa, con el propósito de mantener la confidencialidad de los documentos impresos.
198. Se deberá asegurar el borrado de los documentos almacenados en el dispositivo de impresión así como establecer mecanismos de cifrado en los datos almacenados, en caso que el dispositivo de impresión lo permitiese. Para ello se deberá tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

8.2.2 PROTECCIÓN DE LA INFORMACIÓN

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

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

200. Se debe asegurar la integridad de la información con un nivel alto de confidencialidad durante su almacenamiento, transmisión o impresión.
201. Solo será visible en claro dicha información cuando se esté realizando uso de ella.
202. Se deberá asegurar la implementación de seguridad en los dispositivos de impresión, mediante código o tarjeta identificativa, con el propósito de mantener la confidencialidad de los documentos impresos.

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

9. RESUMEN Y APLICACIÓN DE MEDIDAS EN SERVIDOR DE IMPRESIÓN

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

Control	Medida	Mecanismo de aplicación
OP. ACC.2	Requisitos de acceso	Revisión e implementación de guía CCN-STIC-871, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-871, adaptándolos a la organización.
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-871, adaptándolos a la organización.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Implementación de GPO a través de plantillas facilitadas en la presente guía.
OP. EXP. 8	Registro de la actividad de los usuarios	Revisión e implementación de guía CCN-STIC-871, adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde el nivel bajo. Revisión e implementación guía CCN-STIC-859 de recolección y consolidación de eventos con Windows 2008 R2.

ANEXO A. PLANTILLA DE SEGURIDAD APLICABLE AL SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2 DE NIVEL BAJO

Para que los clientes Windows puedan hacer uso de los servicios del servidor de impresión es necesario aplicar la plantilla de seguridad incremental para clientes Windows que se incluye junto con esta guía. Esta plantilla únicamente habilita el servicio “Cola de impresión” y configura las conexiones USB.

CCN-STIC-871 ENS Incremental servidor de impresion bajo

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas locales/Directiva de auditoría

Directiva	Configuración
Auditar el acceso a objetos	Aciertos, errores
Directivas locales/Opciones de seguridad	
Cliente de redes de Microsoft	

Directiva	Configuración
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Dispositivos

Directiva	Configuración
Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitado

Servidor de red Microsoft

Directiva	Configuración
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Servicios del sistema

Servidor (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total

Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Cola de impresión (Modo de inicio: Automático)**Permisos**

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Sistema de archivos**%SystemRoot%\infusbport.inf**

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario**Permisos**

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

%SystemRoot%\infusbstor.PNF

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario
Permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

%SystemRoot%\System32\drivers\USBSTOR.SYS

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario
Permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario		Habilitado	

se propaguen a este objeto y a todos los objetos secundarios

Configuración del usuario (habilitada)
Configuración no definida.

ANEXO B. PLANTILLA DE SEGURIDAD APLICABLE AL SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2 DE NIVEL MEDIO

Para que los clientes Windows puedan hacer uso de los servicios del servidor de impresión es necesario aplicar la plantilla de seguridad incremental para clientes Windows que se incluye junto con esta guía. Esta plantilla únicamente habilita el servicio “Cola de impresión” y configura las conexiones USB.

CCN-STIC-871 ENS Incremental servidor de impresion medio

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas locales/Directiva de auditoría

Directiva	Configuración
Auditar el acceso a objetos	Aciertos, errores
Directivas locales/Opciones de seguridad	
Cliente de redes de Microsoft	

Directiva	Configuración
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Dispositivos

Directiva	Configuración
Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitado

Servidor de red Microsoft

Directiva	Configuración
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Servicios del sistema

Servidor (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\SYSTEM	Control total

Permitir	NT AUTHORITY\INTERACTIVE	Leer
----------	--------------------------	------

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Cola de impresión (Modo de inicio: Automático)**Permisos**

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Sistema de archivos**%SystemRoot%\infusbport.inf**

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario**Permisos**

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

%SystemRoot%\infusbstor.PNF

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario

Permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

%SystemRoot%\System32\drivers\USBSTOR.SYS

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario**Permisos**

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

Configuración del usuario (habilitada)

Configuración no definida.

ANEXO C. PLANTILLA DE SEGURIDAD APLICABLE AL SERVIDOR DE IMPRESIÓN SOBRE MICROSOFT WINDOWS SERVER 2012 R2 DE NIVEL ALTO

Para que los clientes Windows puedan hacer uso de los servicios del servidor de impresión es necesario aplicar la plantilla de seguridad incremental para clientes Windows que se incluye junto con esta guía. Esta plantilla únicamente habilita el servicio “Cola de impresión” y configura las conexiones USB.

CCN-STIC-871 ENS Incremental servidor de impresion alto

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas locales/Directiva de auditoría

Directiva	Configuración
Auditar el acceso a objetos	Aciertos, errores
Directivas locales/Opciones de seguridad	
Cliente de redes de Microsoft	

Directiva	Configuración
Cliente de redes de Microsoft: enviar contraseña sin cifrar a servidores SMB de terceros	Deshabilitado
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (si el servidor lo permite)	Habilitado
Cliente de redes de Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Dispositivos

Directiva	Configuración
Dispositivos: impedir que los usuarios instalen controladores de impresora	Habilitado

Servidor de red Microsoft

Directiva	Configuración
Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente lo permite)	Habilitado
Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)	Habilitado

Servicios del sistema

Servidor (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total

Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Cola de impresión (Modo de inicio: Automático)**Permisos**

Tipo	Nombre	Permiso
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\SYSTEM	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Sistema de archivos**%SystemRoot%\infusbpport.inf**

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario**Permisos**

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

%SystemRoot%\infusbstor.PNF

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario
Permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Habilitado	

%SystemRoot%\System32\drivers\USBSTOR.SYS

Configurar este archivo o carpeta: propagar los permisos heredables a todas las subcarpetas y archivos

Propietario
Permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	BUILTIN\Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	NT AUTHORITY\SYSTEM	Control total	Esta carpeta, subcarpetas y archivos
Permitir	BUILTIN\Usuarios	Leer y ejecutar	Esta carpeta, subcarpetas y archivos
Permitir que los permisos heredables del primario se propaguen a este objeto y a todos los objetos secundarios		Deshabilitado	

Auditoría

Tipo	Nombre	Acceso	Aplicar a
Todos	NT AUTHORITY\Usuarios autenticados	Control total	Esta carpeta, subcarpetas y archivos
Permitir que las entradas de auditoría heredables del primario		Habilitado	

se propaguen a este objeto y a todos los objetos secundarios

Configuración del usuario (habilitada)
Configuración no definida.

ANEXO D. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE IMPRESIÓN QUE LES SEAN 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 empleen servidores de impresión con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran 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, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

Nota: Si instala el Servidor de impresión por primera vez con la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2 aplicada debe habilitar la instalación remota de roles, características y servicios de rol a través de Shell la cual se encuentra deshabilitada por GPO.

1. INSTALACIÓN DEL ROL SERVIDOR DE IMPRESIÓN

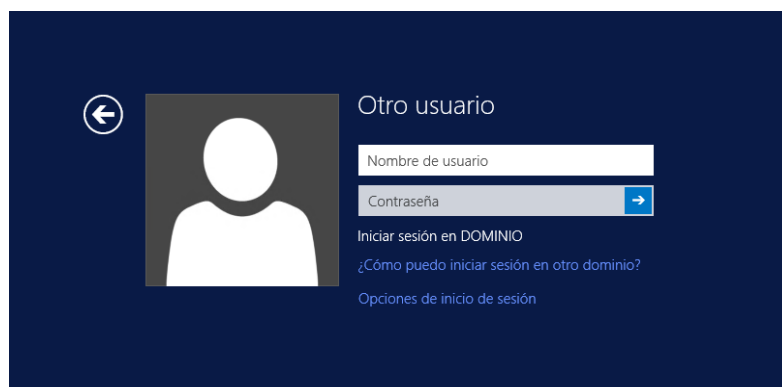
Este procedimiento está diseñado para ayudar a los operarios a realizar una instalación básica del rol “Servidor de impresión”.

Tenga en consideración que si desea añadir más características o roles al Servidor de impresión deberá modificar el script y adaptarlo a las necesidades de su organización.

Nota: El procedimiento descrito a continuación, indica como instalar el rol “Servidor de impresión”. Si desea realizar este procedimiento continúe con el siguiente punto. En caso de tener ya instalado el rol “Servidor de impresión” vaya al punto “2 PREPARACIÓN DEL DOMINIO”.

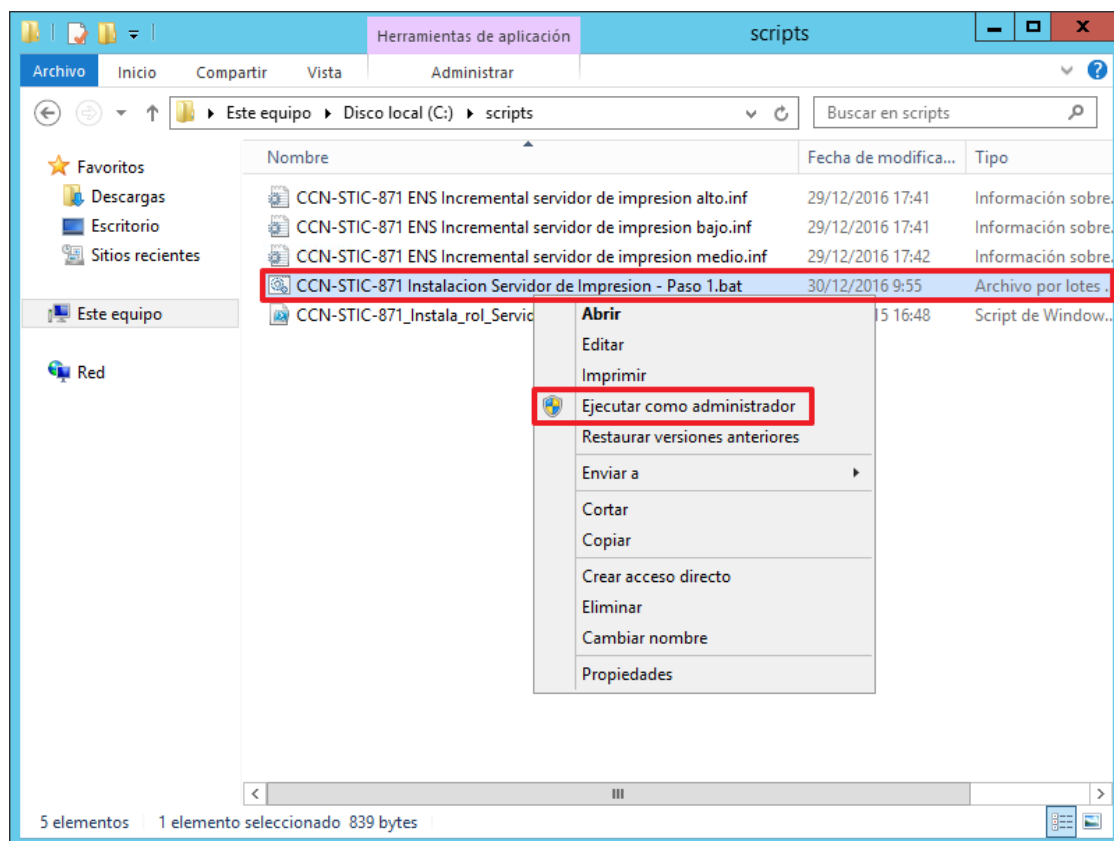
Paso	Descripción
------	-------------

1. Inicie sesión en el servidor miembro donde vaya a instalar el rol “Servidor de impresión”.

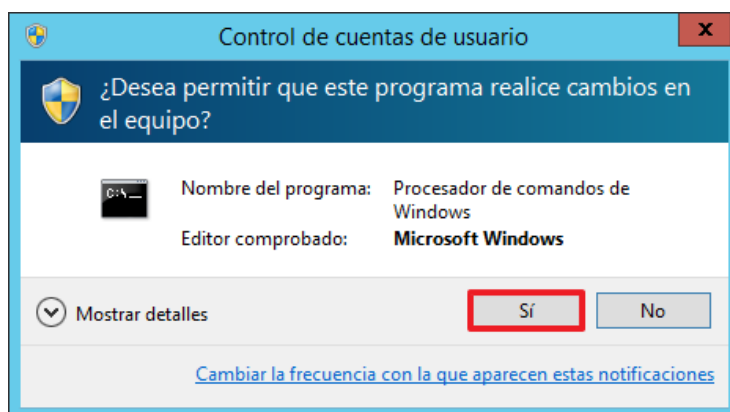


Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	En el directorio “C:\Scripts” localice el fichero “CCN-STIC-871 Instalacion Servidor de Impresion – Paso 1.bat”. Seleccione con el botón derecho del ratón y pulse sobre la opción del menú contextual “Ejecutar como administrador”.



5. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse “Sí” para continuar.



Paso	Descripción
------	-------------

6. Se lanzará el script. Pulse cualquier tecla para comenzar la instalación.

```

C:\Windows\System32\cmd.exe

CCN-STIC-871 Servidor de Impresion - Paso 1

Este script instala el rol Servidor de impresion.

Antes de ejecutar este script asegurese que los ficheros y
scripts de esta guia se encuentran en el directorio C:\Scripts.

Si desea instalar características adicionales cierre esta ventana
y modifique el presente script.

Presione una tecla para continuar . . . _

```

7. La instalación comenzará. Espere a que finalice.

```

Administrador: Windows PowerShell

Recopilando datos...
10 %
[]

Si desea instalar características adicionales cierre esta ventana
y modifique el presente script.

Presione una tecla para continuar . . .

C:\Scripts>powershell.exe -executionpolicy RemoteSigned -File CCN-STIC-871_Instala_rol_ServidorImpresion.ps1

```

8. Cuando haya finalizado la instalación pulse una tecla para cerrar la ventana.

```

Administrador: Windows PowerShell

CCN-STIC-871 Servidor de Impresion - Paso 1

Este script instala el rol Servidor de impresion.

Antes de ejecutar este script asegurese que los ficheros y
scripts de esta guia se encuentran en el directorio C:\Scripts.

Si desea instalar características adicionales cierre esta ventana
y modifique el presente script.

Presione una tecla para continuar . . .

C:\Scripts>powershell.exe -executionpolicy RemoteSigned -File CCN-STIC-871_Instala_rol_ServidorImpresion.ps1

Success Restart Needed Exit Code      Feature Result
-----
True     No           Success      {Servidor de impresión, Servicios de i...

ADVERTENCIA: La actualización automática de Windows no está habilitada. Para
asegurarse de que la característica o el rol recién instalados se actualicen
automáticamente, active Windows Update en el Panel de control.

CCN-STIC-871 Servidor de Impresion - Paso 1 : EJECUCION FINALIZADA

Presione una tecla para continuar . . .

```

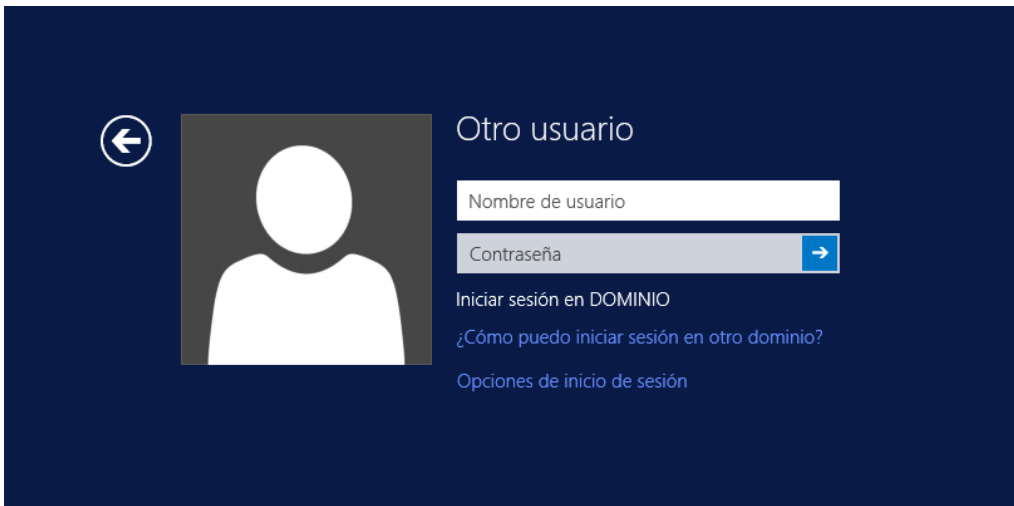
Nota: Ignore la advertencia sobre las actualizaciones automáticas de Windows.

9. Elimine la carpeta "C:\Scripts".

2. PREPARACIÓN DEL DOMINIO

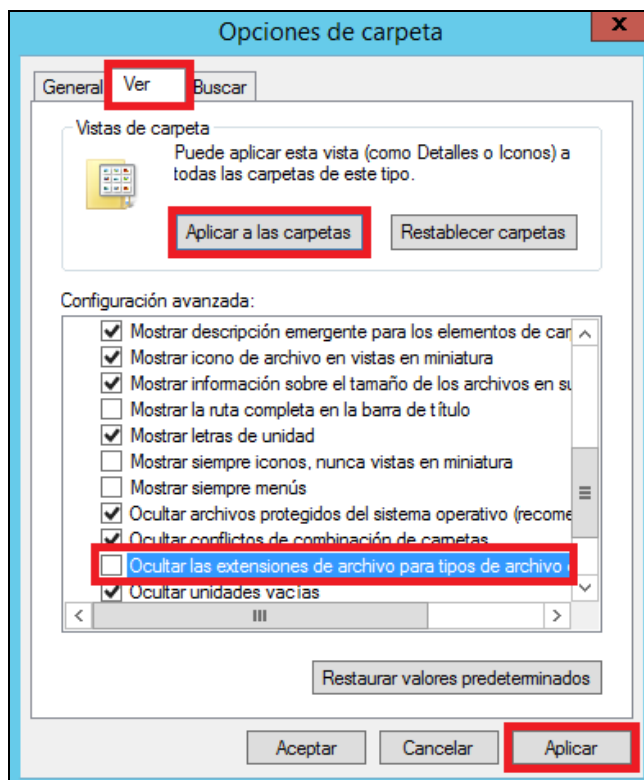
Los pasos que se describen a continuación deberá realizarlos en un Controlador de Dominio del dominio al que pertenece el equipo que está asegurando. Estos pasos sólo se realizarán cuando se incluya el primer servidor de impresión miembro del dominio. Durante este procedimiento se crea la unidad organizativa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

Nota: Esta guía asume que los servidores Controladores del Dominio al que pertenece el equipo servidor de impresión que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-870A Implementación del ENS en Microsoft Windows Server 2012 R2. Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

Paso	Descripción
10.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios del ENS. 
	Nota: Inicie sesión con una cuenta que sea Administrador del Dominio.
11.	Cree el directorio “Scripts” en la unidad “C:\”. Nota: Los scripts asumen que su ubicación en el sistema será bajo “C:\scripts”. Si los colocara en otra ubicación, tendrá que editar los scripts para reflejar la nueva ubicación.
12.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
13.	Configure el “Explorador de Windows” para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que “Explorador de Windows” muestra las extensiones de los archivos.

Paso	Descripción
------	-------------

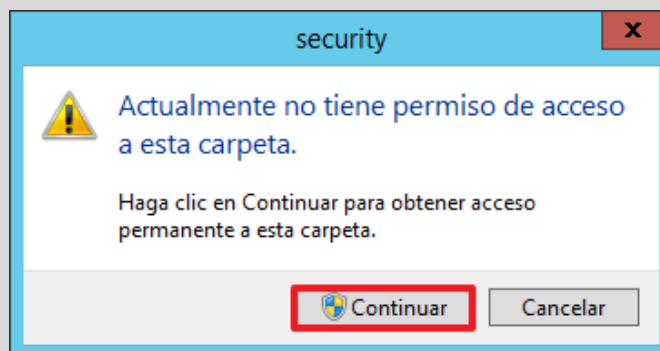
14. Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, “Opciones”. En la venta emergente, seleccione la pestaña “Ver” y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”, como se muestra en la imagen.



Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación "¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?", y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

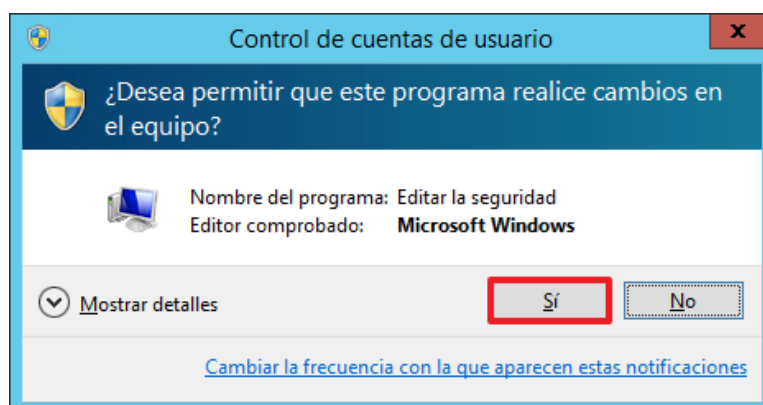
15. Adicionalmente acceda al directorio “C:\Windows\security\templates”.

Nota: Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón “Continuar” ante la ventana emergente.

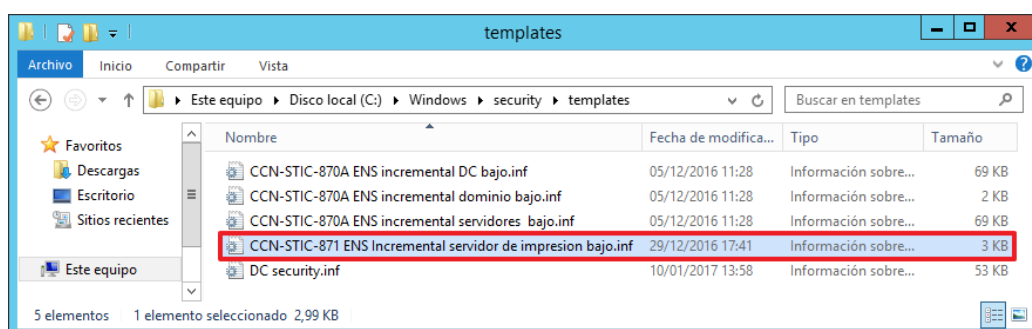


Paso	Descripción
------	-------------

16. El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.



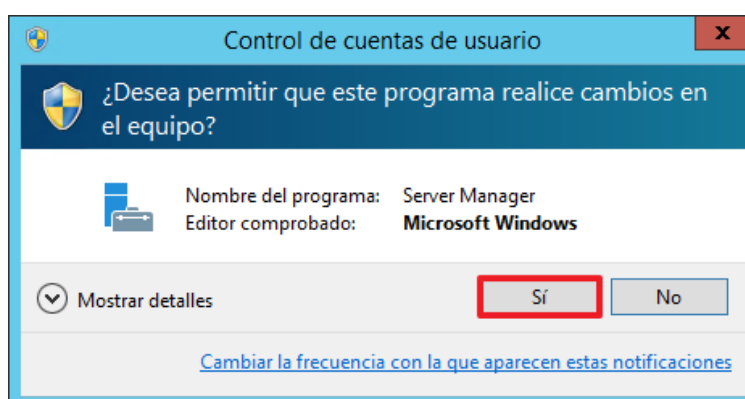
17. Copie el fichero “CCN-STIC-871 ENS Incremental servidor de impresion bajo.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\security\templates”.



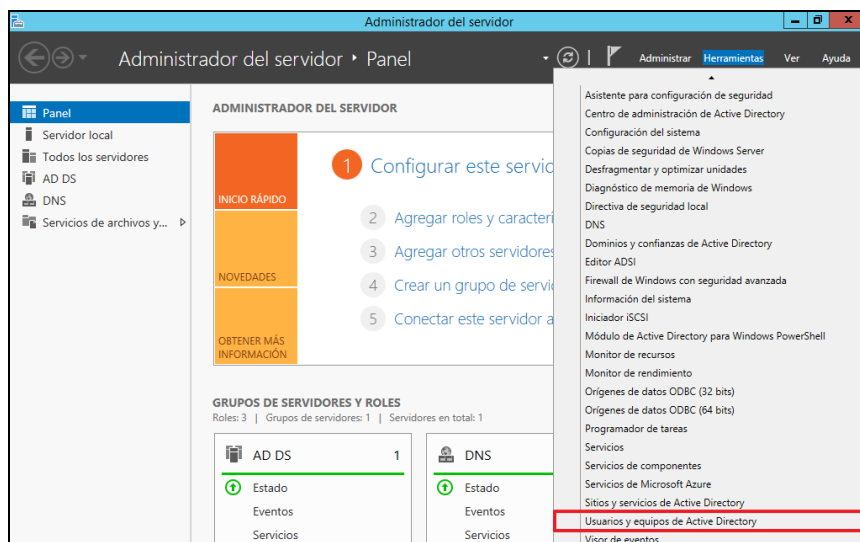
18. A continuación, deberá crear la unidad organizativa "Servidores de Impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.



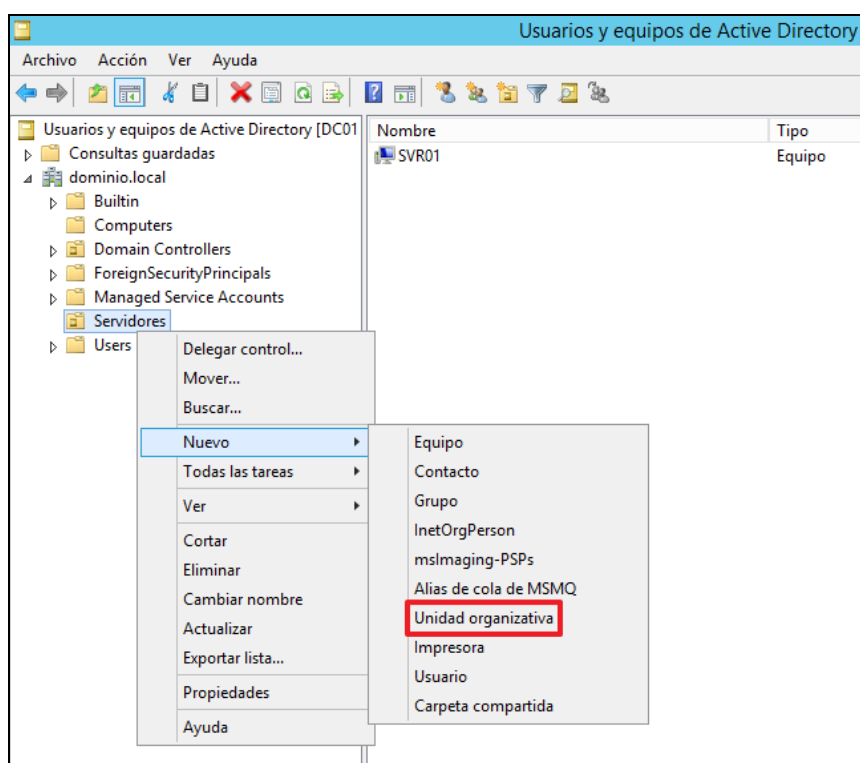
19. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



Paso	Descripción
20.	Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione: “Herramientas → Usuarios y equipos de Active Directory”



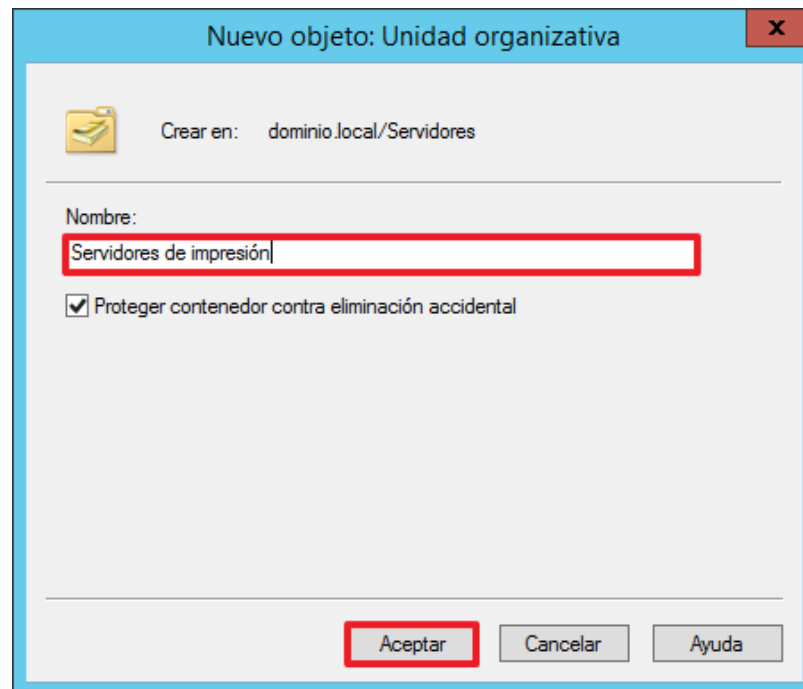
21. En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2. Para ello, seleccione el nodo “<<dominio>> / <<unidad organizativa>>”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo > Unidad organizativa”.



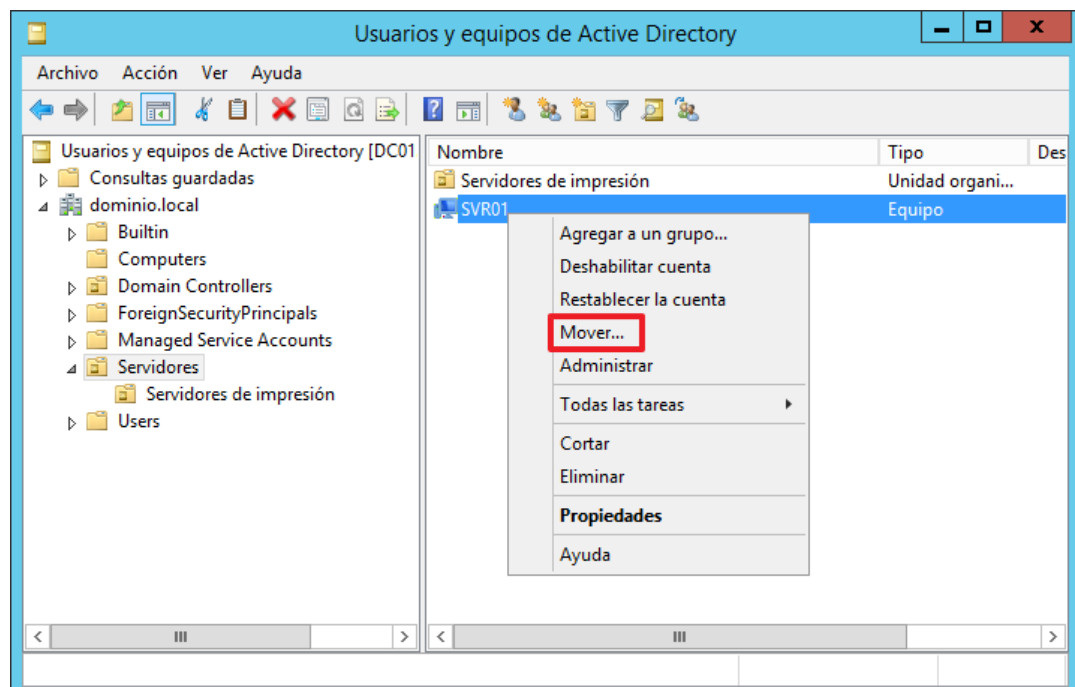
Nota: En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local/Servidores”.

Paso	Descripción
------	-------------

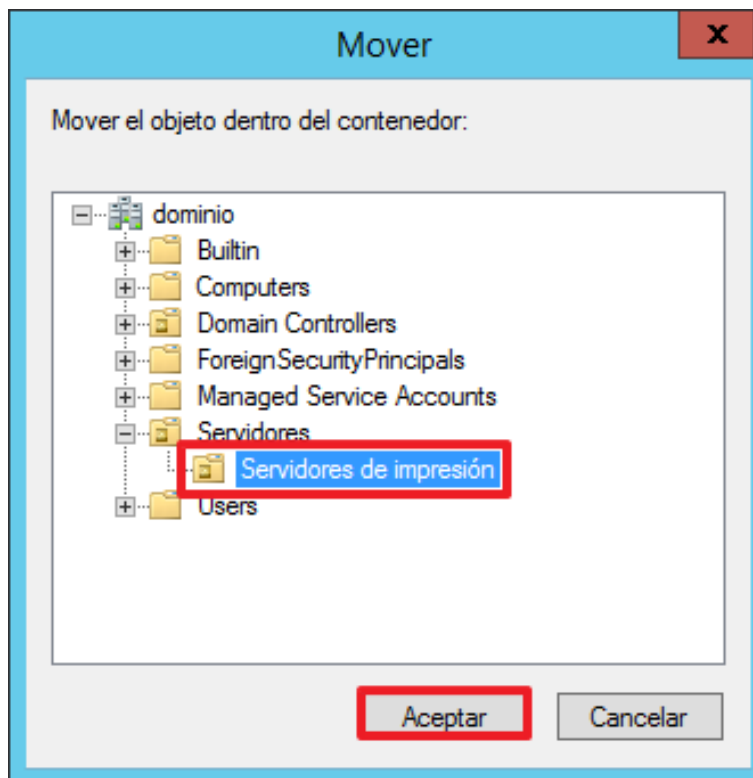
22. Introduzca el nombre “Servidores de impresión” tal y como se muestra en la imagen y pulse sobre “Aceptar”.



23. Una vez creada la nueva Unidad organizativa, deberá mover los servidores de impresión a la unidad organizativa “Servidores de impresión”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”.



Paso	Descripción
24.	A continuación, seleccione la unidad organizativa “Servidores de impresión” y pulse “Aceptar”.

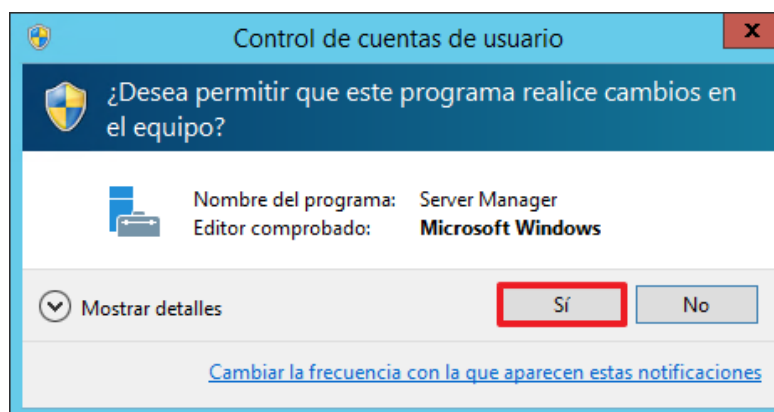


25. Cierre la herramienta “Usuarios y equipos de Active Directory”.

26. A continuación, deberá crear la GPO "CCN-STIC-871 ENS Incremental servidor de impresion bajo". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.

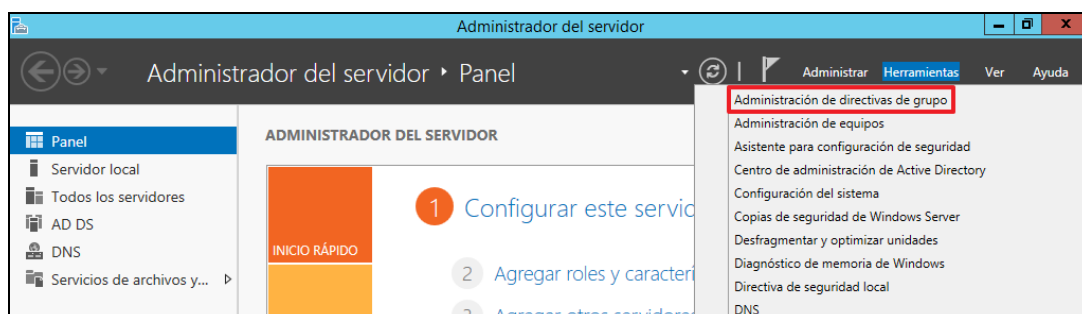


27. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



Paso	Descripción
------	-------------

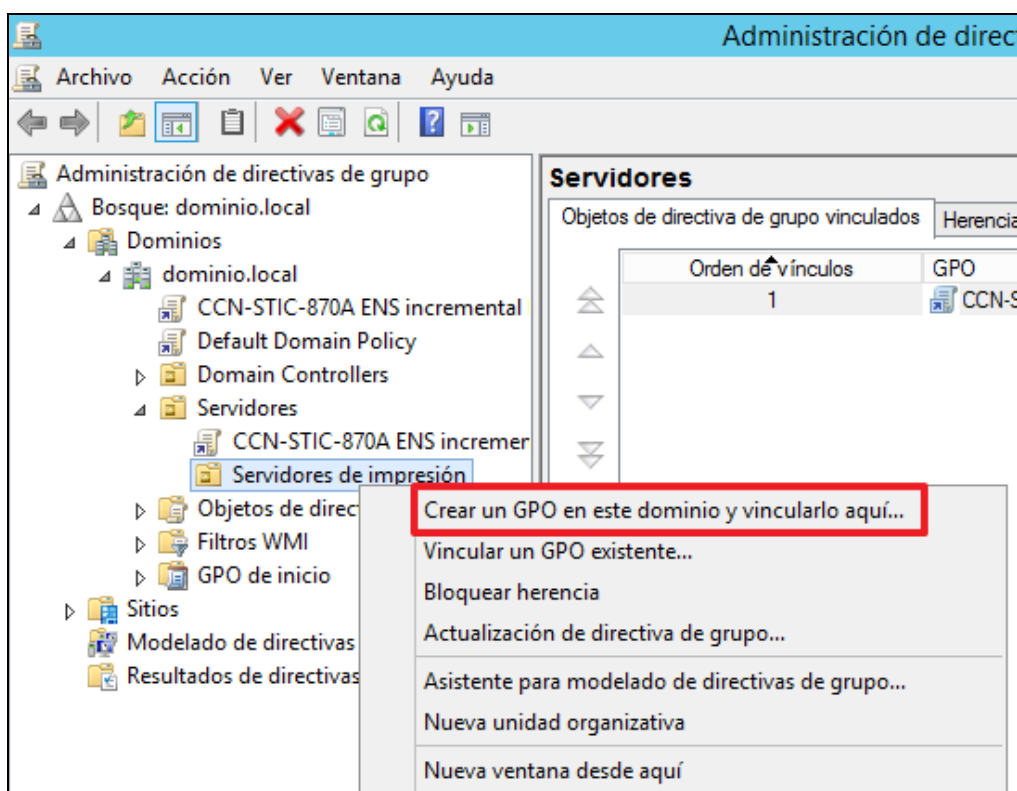
28. Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”.



29. A continuación, despliegue el nodo “Bosque: <<nombre de bosque>> / Dominios / <<nombre de dominio>> / Servidores / Servidores de impresión”.

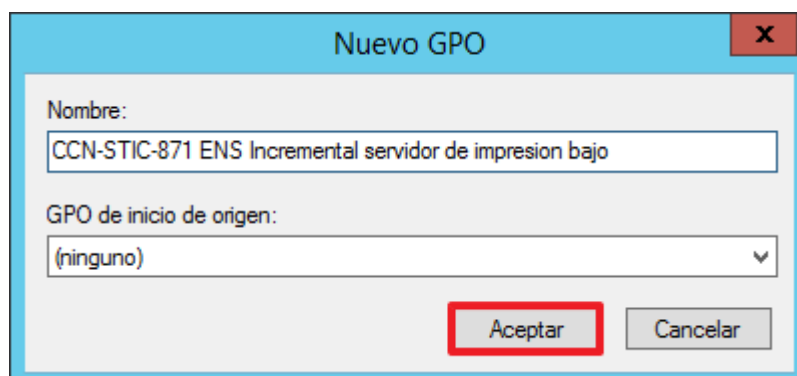
Nota: En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de impresión”.

30. Pulse con el botón derecho sobre la unidad organizativa “Servidores de impresión” y seleccione “Crear un GPO en este dominio y vincularlo aquí...”.

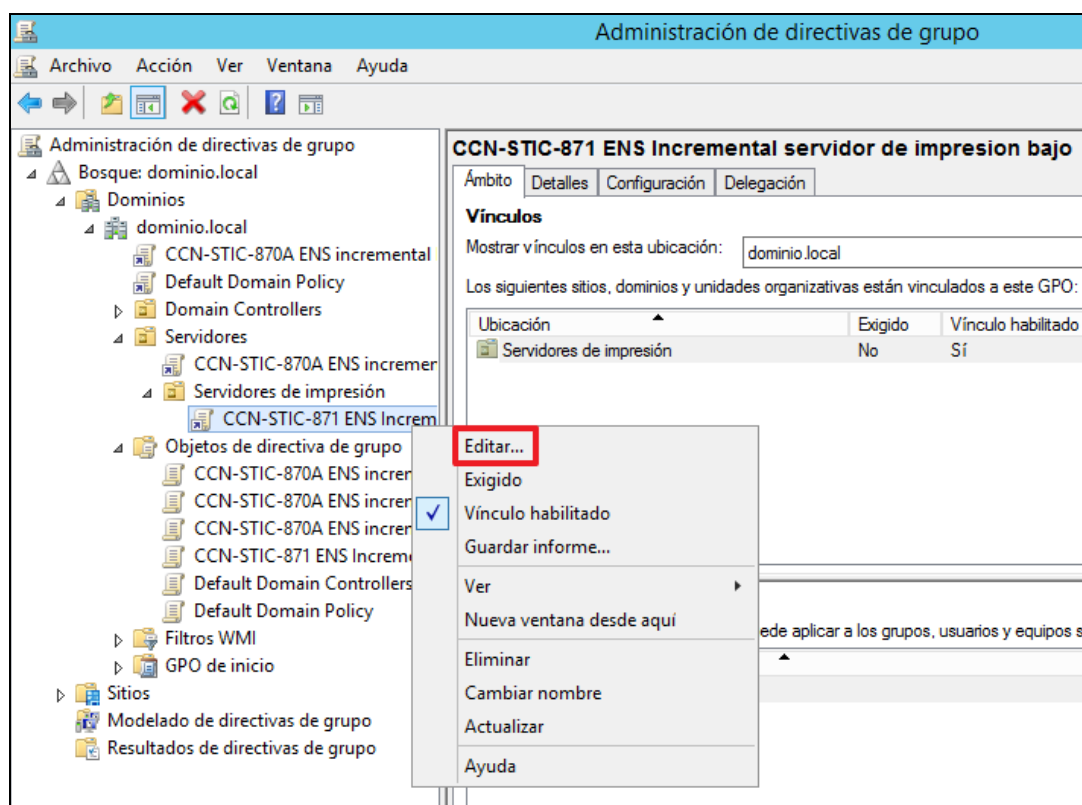


Paso	Descripción
------	-------------

31. Escriba el nombre de la GPO "CCN-STIC-871 ENS Incremental servidor de impresion bajo" y haga clic en el botón "Aceptar".



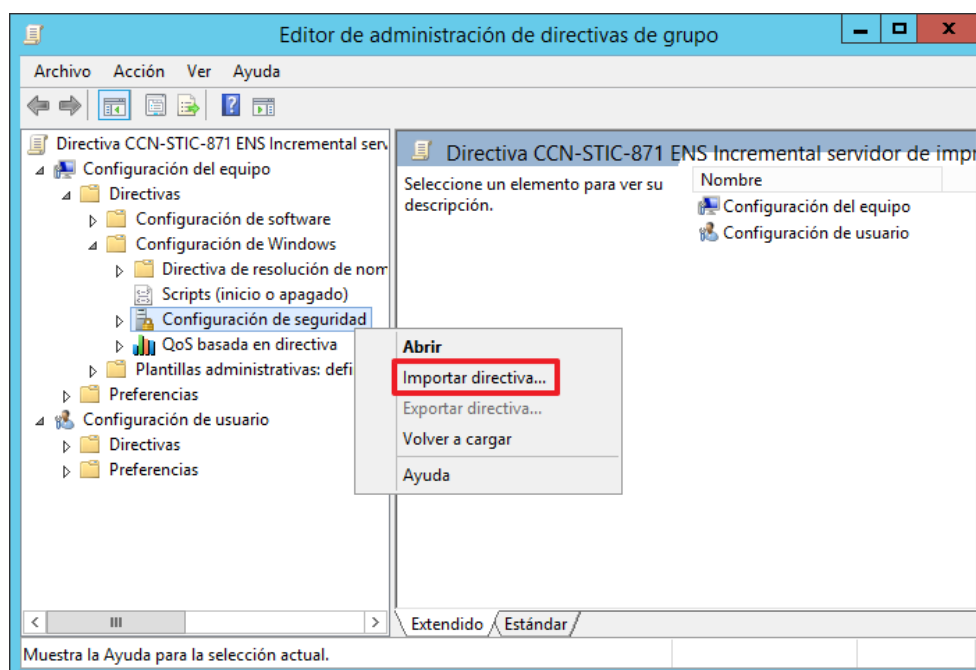
32. Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción "Editar".



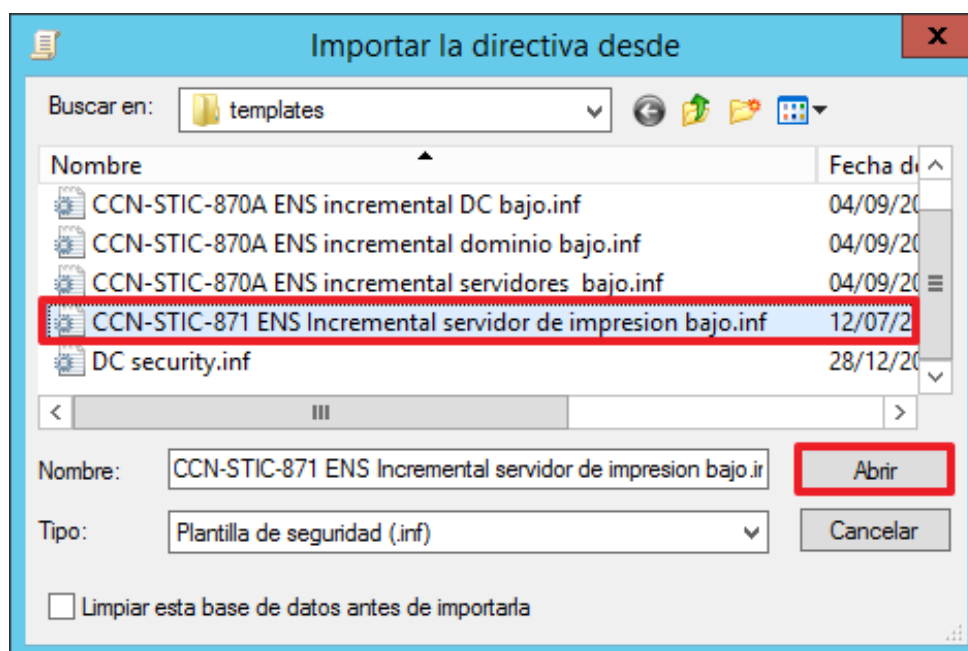
33. Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta:
"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"

Paso	Descripción
------	-------------

34. Pulse con el botón derecho sobre “Configuración de seguridad” y seleccione la opción “Importar directiva...”.



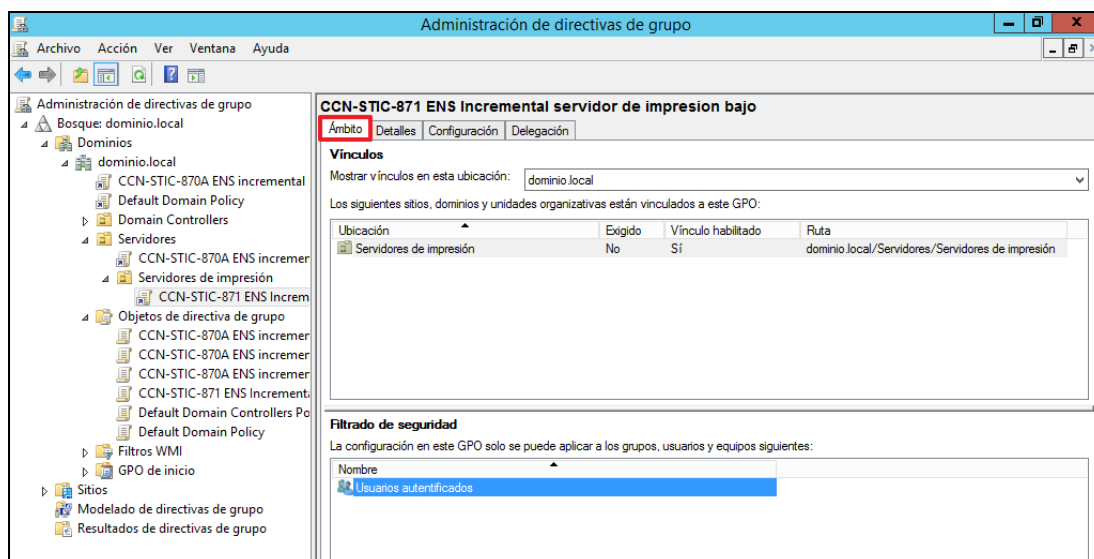
35. Seleccione de la ruta “C:\Windows\security\templates” el fichero “CCN-STIC-871 ENS Incremental servidor de impresion bajo.inf” y pulse el botón “Abrir”.



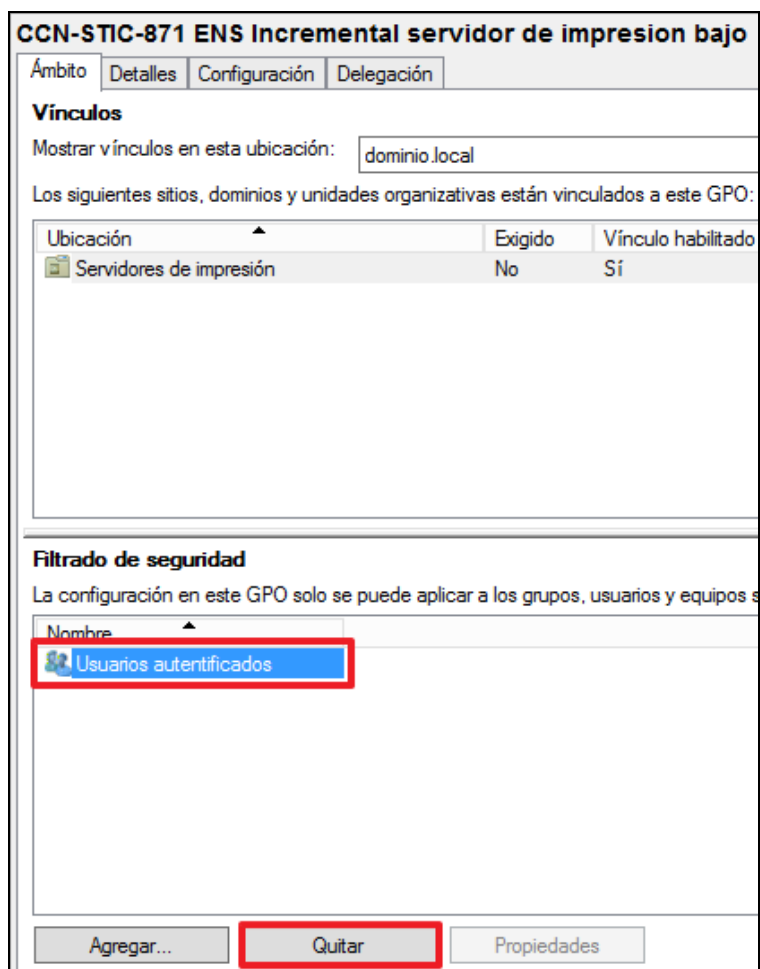
36. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

Paso	Descripción
------	-------------

- | | |
|-----|--|
| 37. | Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. |
|-----|--|

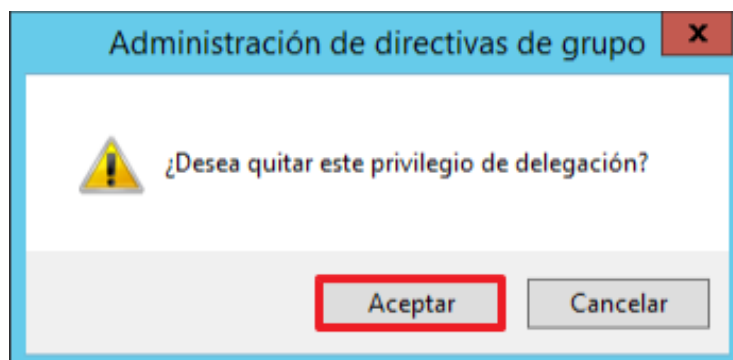


- | | |
|-----|---|
| 38. | En la opción de filtrado de seguridad, seleccione “Usuarios autenticados” y pulse la opción “Quitar”. |
|-----|---|



Paso	Descripción
------	-------------

- | | |
|-----|---|
| 39. | Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”. |
|-----|---|



- | | |
|-----|--|
| 40. | A continuación, pulse el botón “Agregar...”. |
|-----|--|

CCN-STIC-871 ENS Incremental servidor de impresion bajo

Ámbito Detalles Configuración Delegación

Vínculos

Mostrar vínculos en esta ubicación: dominio.local

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado
📁 Servidores de impresión	No	Sí

Filtrado de seguridad

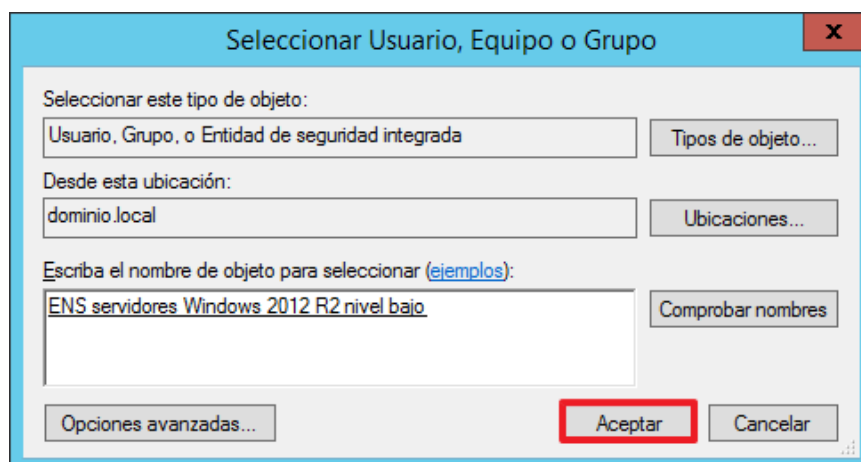
La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos sig

Nombre

Agregar... Quitar Propiedades

Paso	Descripción
------	-------------

41. Introduzca como nombre “ENS servidores Windows 2012 R2 nivel bajo”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2. A continuación, pulse el botón “Aceptar”.



Nota: En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a las necesidades de su organización.

3. 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.

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

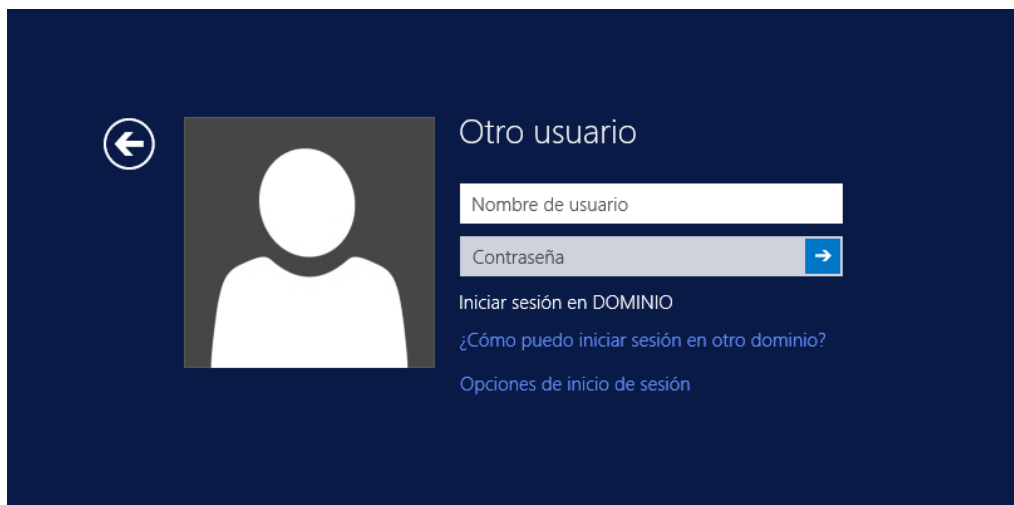
3.1 PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

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 ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

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

Paso	Descripción
------	-------------

42. Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de impresión.

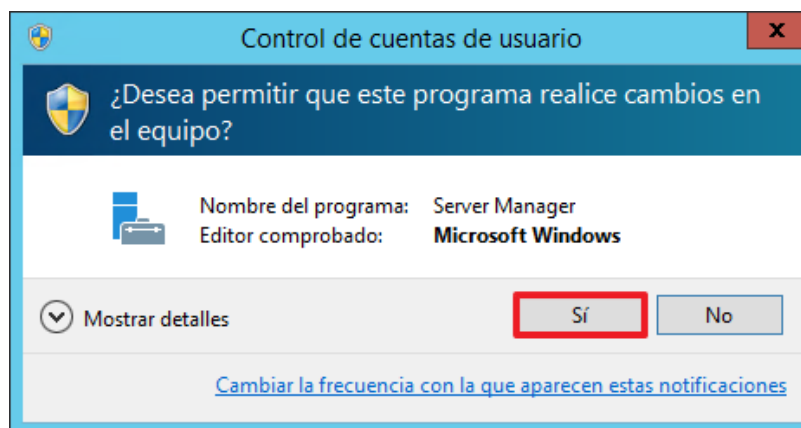


Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

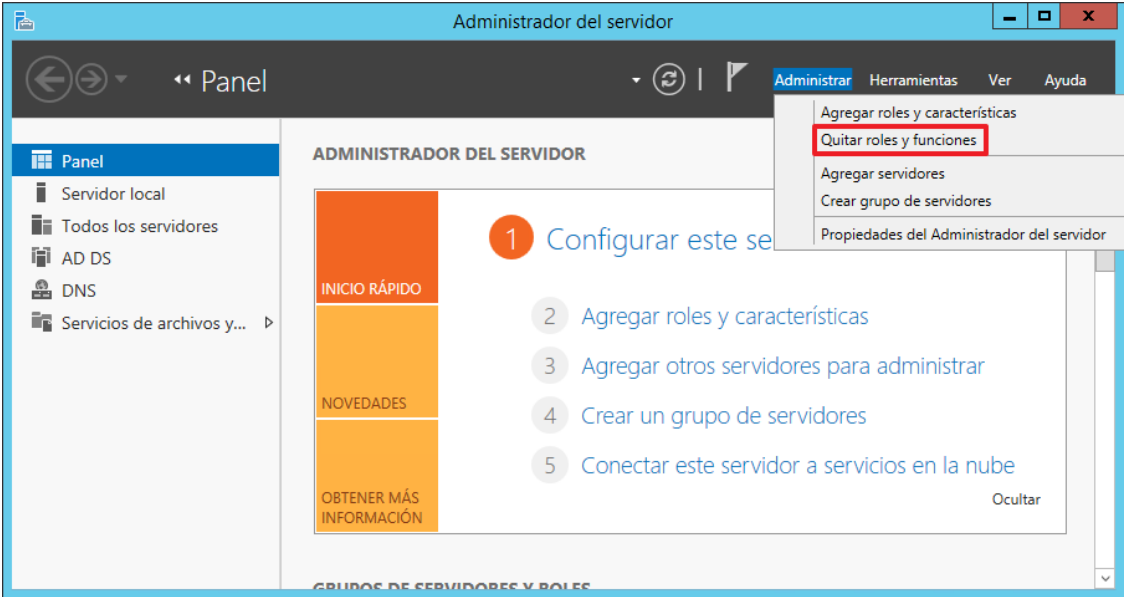
43. Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas.



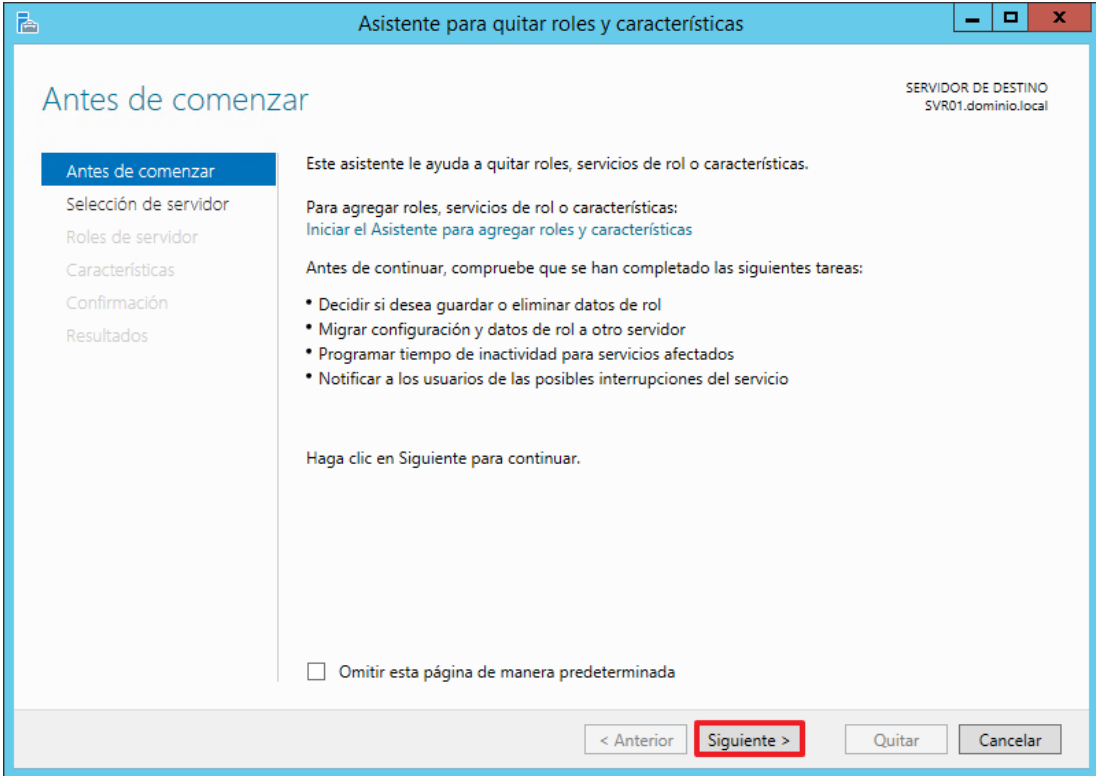
44. El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.



Paso	Descripción
45.	A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.



46. Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar.



Asistente para quitar roles y características

Antes de comenzar

SERVIDOR DE DESTINO
SVR01.dominio.local

Este asistente le ayuda a quitar roles, servicios de rol o características.

Para agregar roles, servicios de rol o características:
[Iniciar el Asistente para agregar roles y características](#)

Antes de continuar, compruebe que se han completado las siguientes tareas:

- Decidir si desea guardar o eliminar datos de rol
- Migrar configuración y datos de rol a otro servidor
- Programar tiempo de inactividad para servicios afectados
- Notificar a los usuarios de las posibles interrupciones del servicio

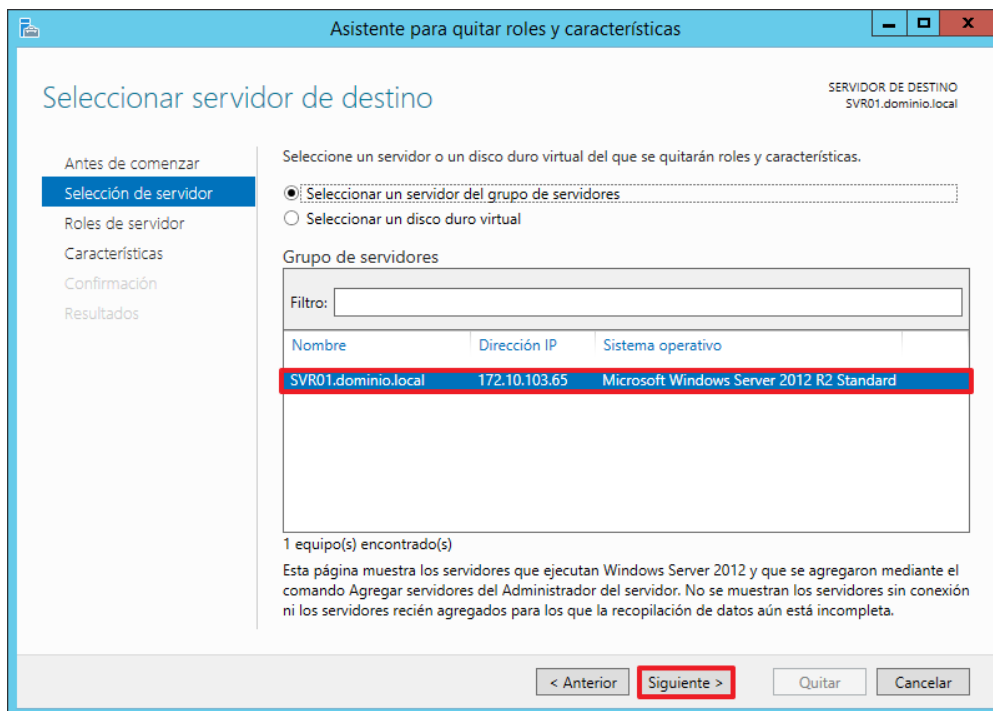
Haga clic en Siguiente para continuar.

☐ Omitir esta página de manera predeterminada

< Anterior **Siguiente >** Quitar Cancelar

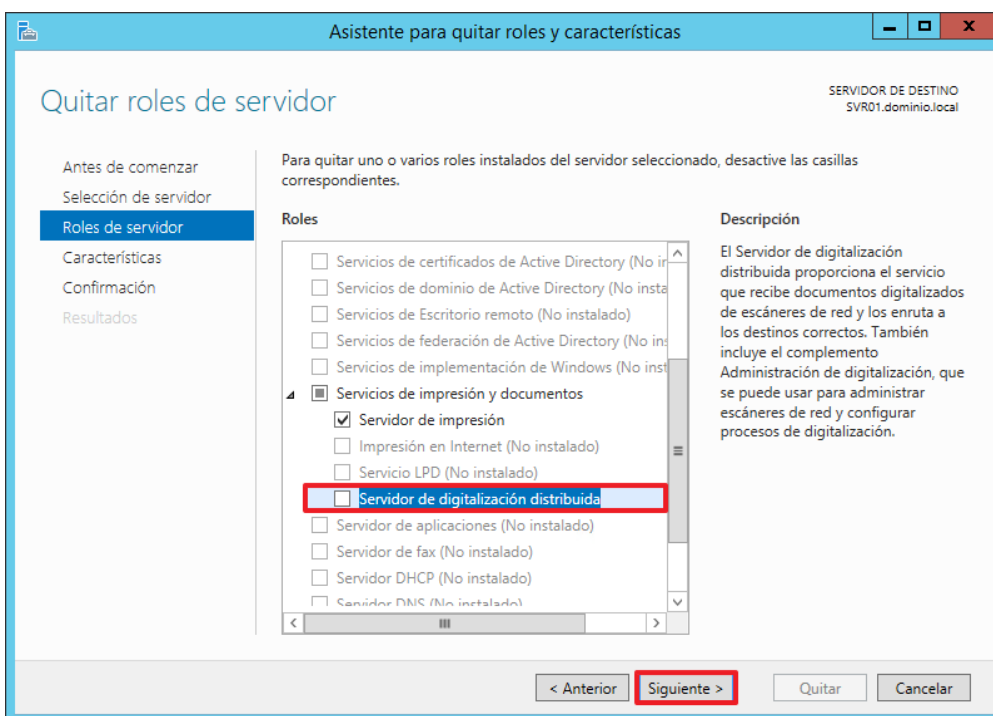
Paso	Descripción
------	-------------

47. Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.



Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

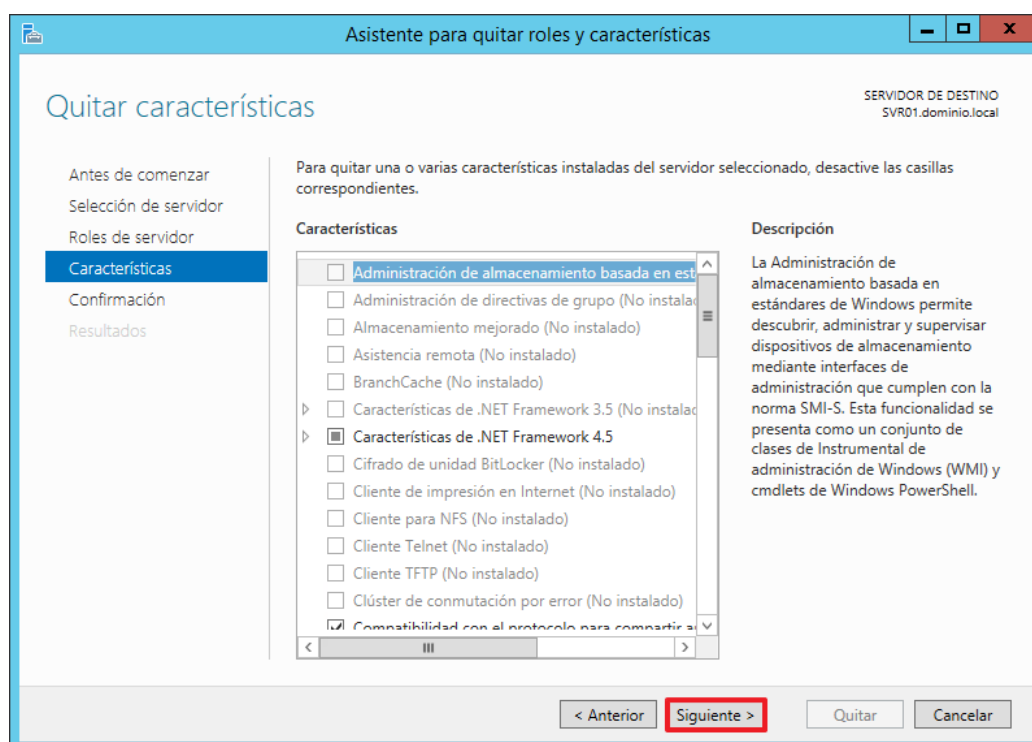
48. En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”.



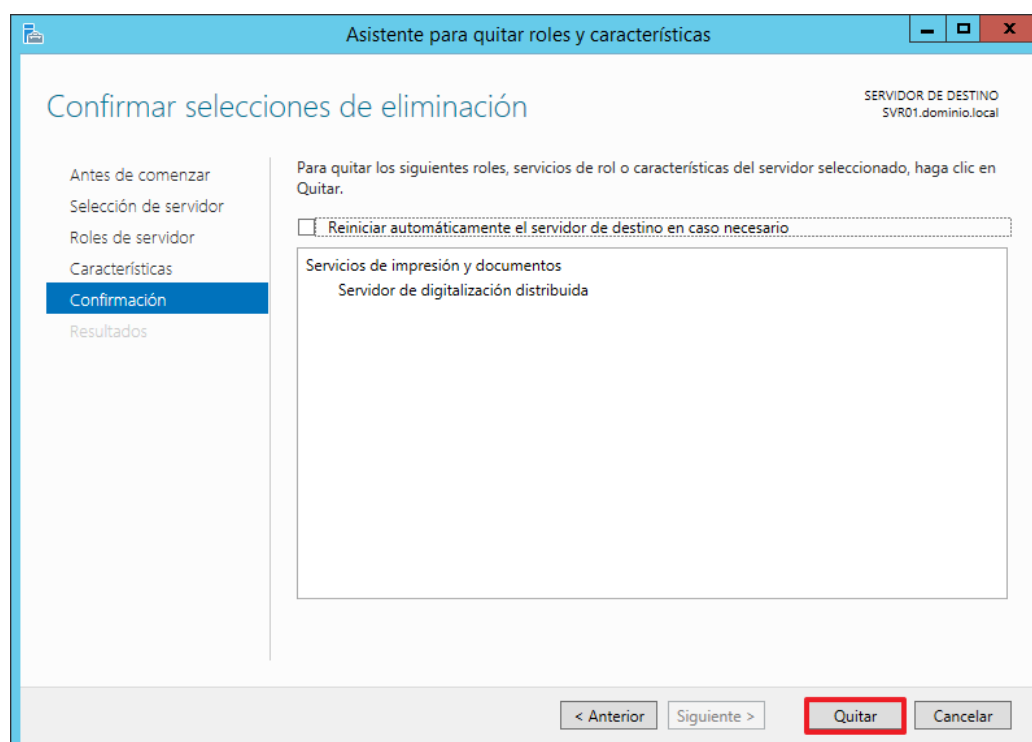
Nota: En este ejemplo se desinstala el rol “servidor de digitalización distribuida”.

Paso	Descripción
------	-------------

49. En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional.

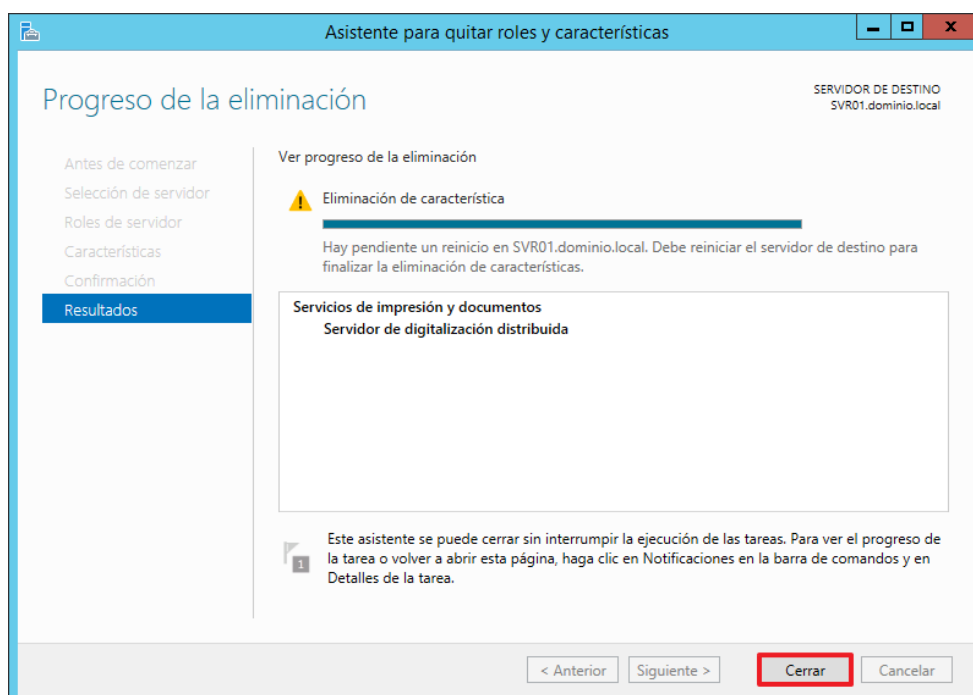


50. En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.



Paso	Descripción
------	-------------

51. El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación.



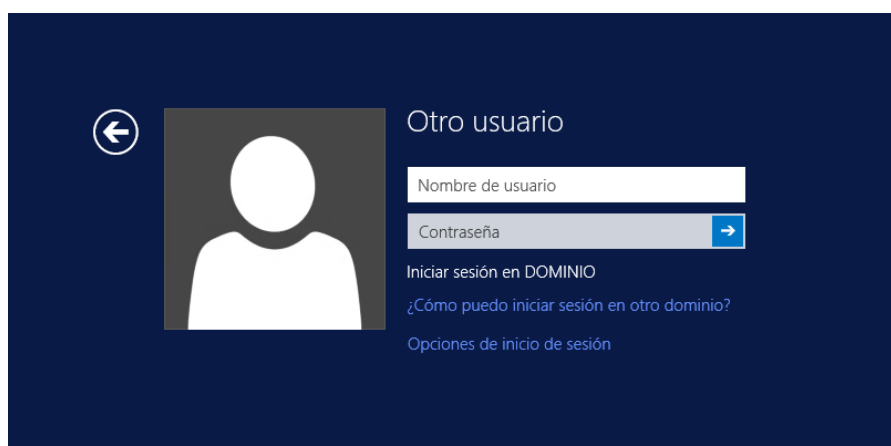
52. En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración.

3.2 GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN

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

Paso	Descripción
------	-------------

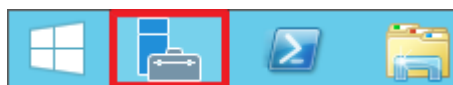
53. Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.



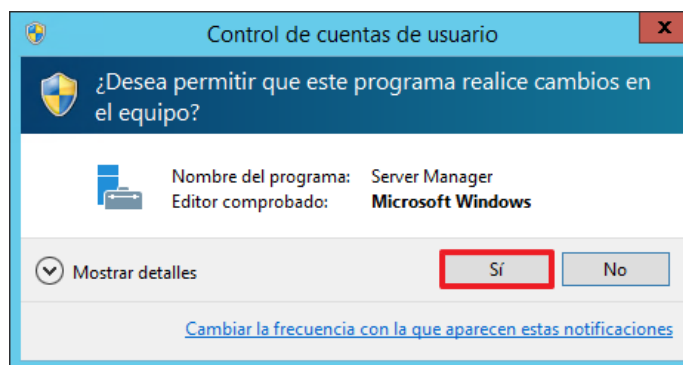
Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

Paso	Descripción
------	-------------

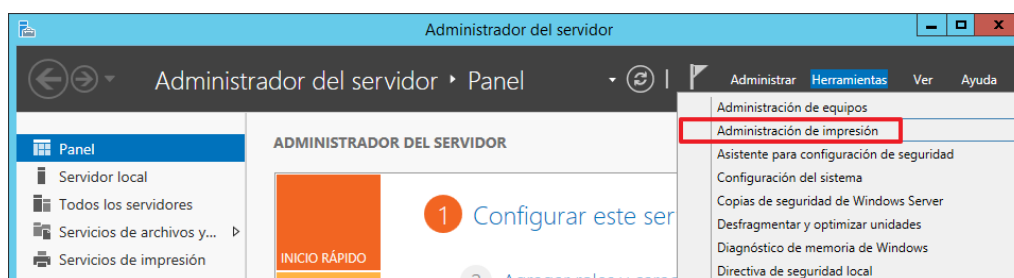
54. A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta “Administrador del servidor” mediante el icono correspondiente.



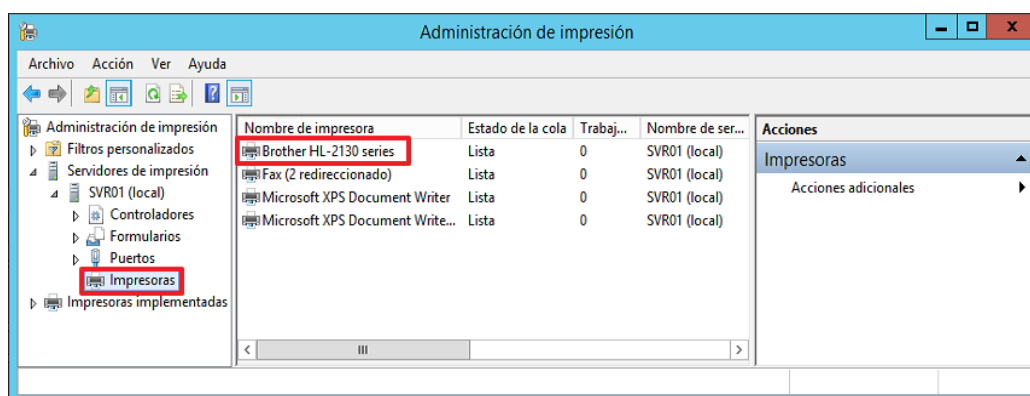
55. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



56. Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de impresión”.



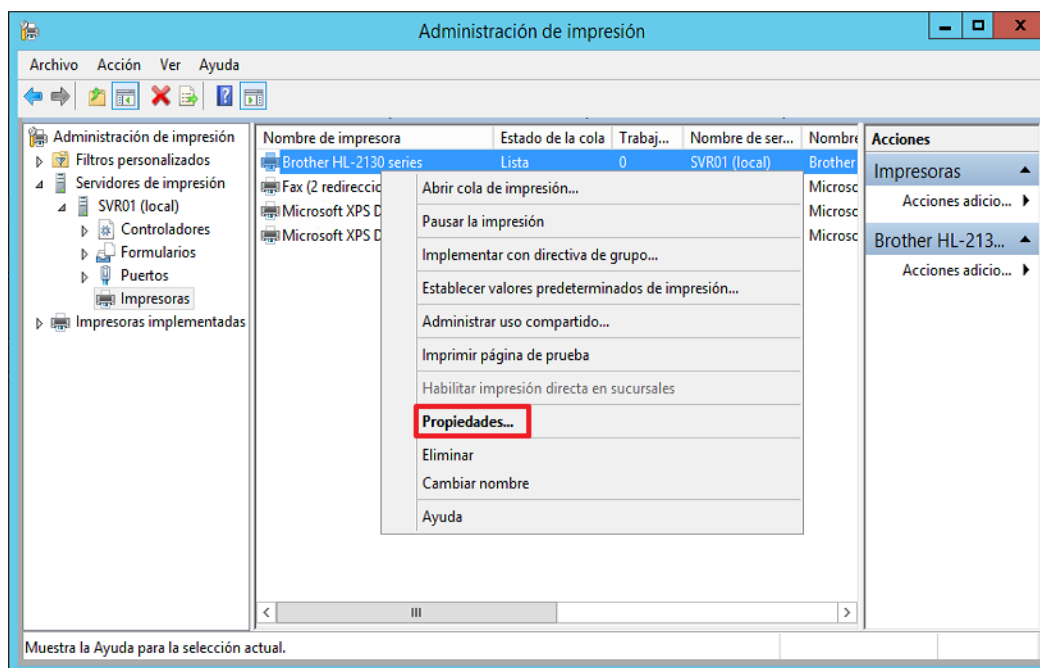
57. Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo “Servidores de impresión / <<nombre del servidor>> / Impresora”.



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

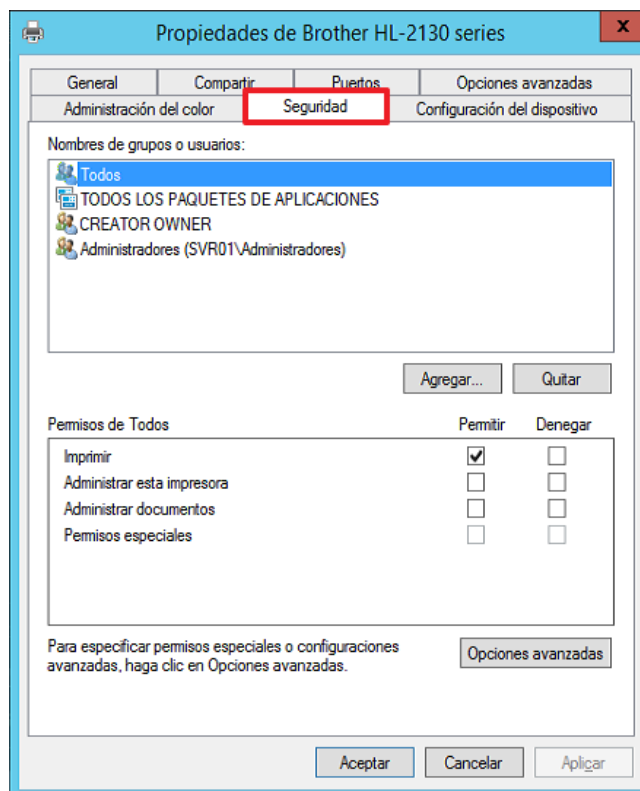
Paso	Descripción
------	-------------

- | | |
|-----|---|
| 58. | Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades...”. |
|-----|---|



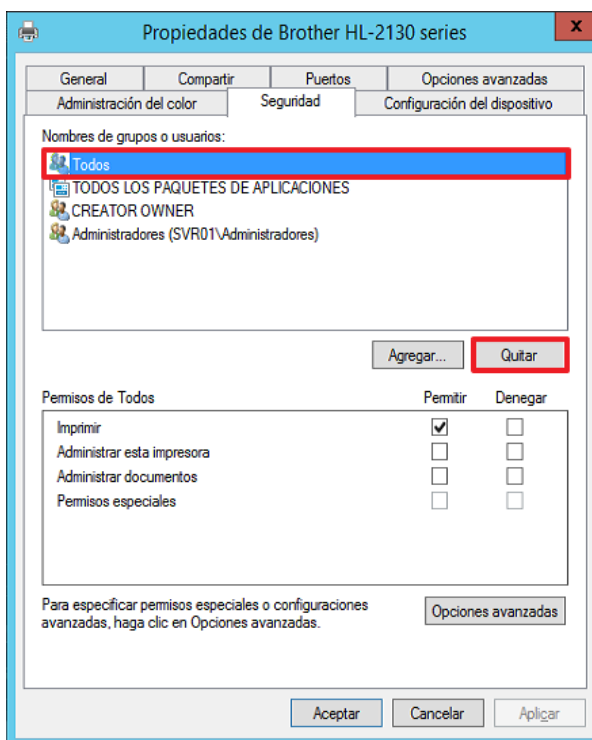
Nota: En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.

59. A continuación, seleccione la pestaña “Seguridad”.



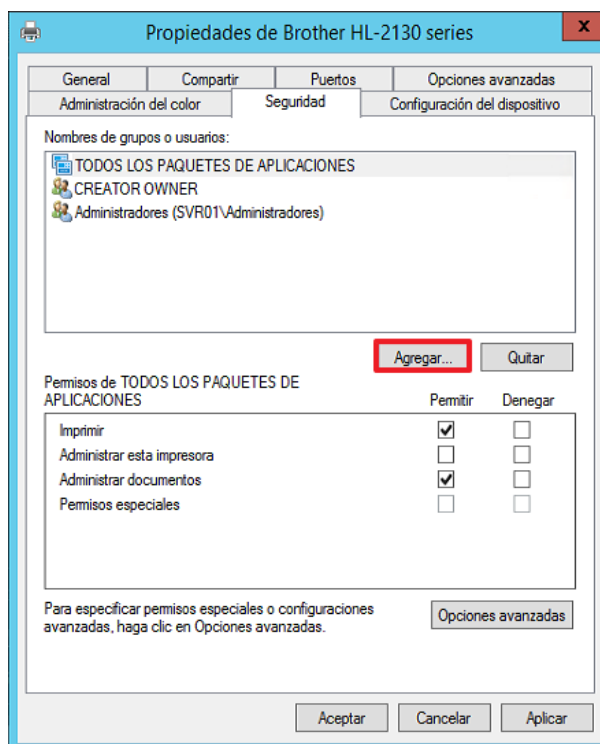
Paso	Descripción
------	-------------

60. Seleccione el grupo de usuarios “Todos” y a continuación pulse en la opción “Quitar”.



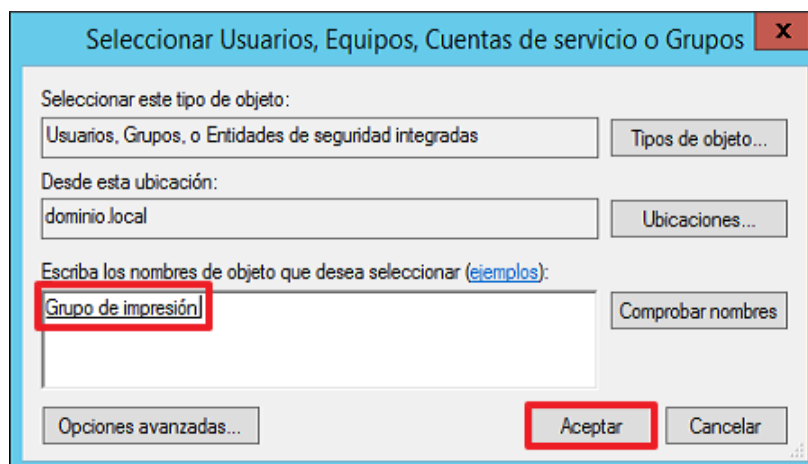
Nota: Debera adaptar este paso a los requisitos de su organización eliminando los usuarios o grupos de usuarios que no requieran de permisos sobre el dispositivo de impresión.

61. A continuación, pulse sobre el botón “Agregar” para añadir el grupo de usuarios que tendrá permiso para poder imprimir por el dispositivo de impresión seleccionado.



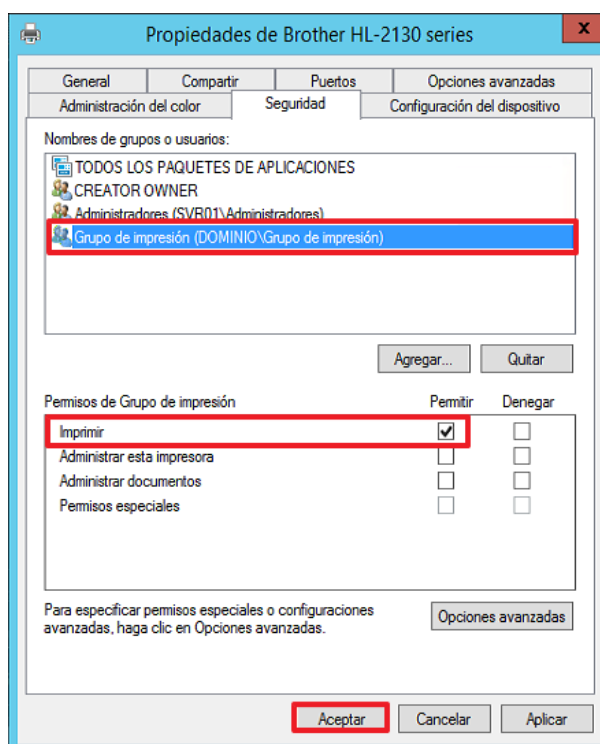
Paso	Descripción
------	-------------

62. Localice el grupo que quiere añadir para que obtenga permisos para imprimir, y pulse sobre “Aceptar”.



Nota: En esta guía se selecciona el grupo de seguridad “Grupo de impresión” al cual pertenecen los usuarios que van a obtener permiso para poder imprimir a través de los dispositivos de impresión seleccionados. Deberá adaptar este paso a los requisitos de su organización.

63. Una vez añadido el grupo de seguridad, localice el grupo y seleccione en los permisos únicamente la opción de “Imprimir”. Pulse “Aceptar” para cerrar la ventana.



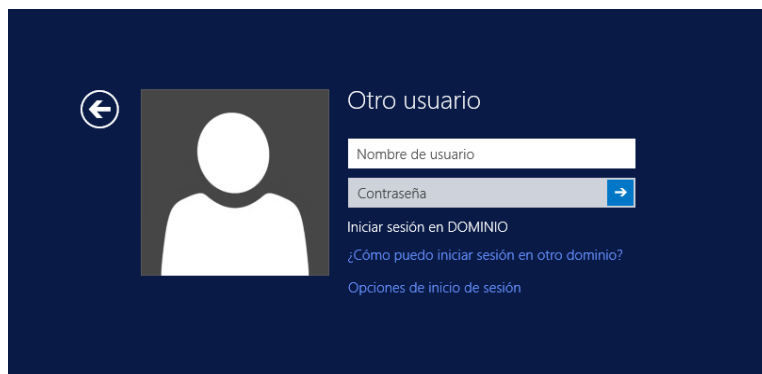
Nota: En este ejemplo se utiliza el grupo denominado “Grupo de impresión”.

64. Debera repetir estos pasos para asignar permisos de impresión sobre todos los dispositivos de impresión que este securizando.

3.3 GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN

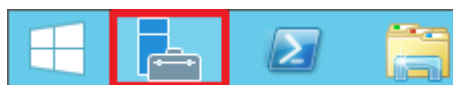
En este apartado se tendrá en consideración la gestión de permisos de administración sobre los dispositivos de impresión según lo establecido por el ENS, para con ello limitar y controlar el acceso a los dispositivos de impresión.

Paso	Descripción
65.	Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.

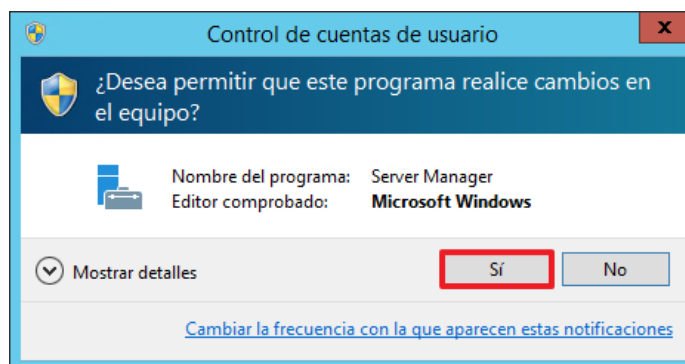


Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

66. A continuación, deberá iniciar la herramienta "Administración de impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.

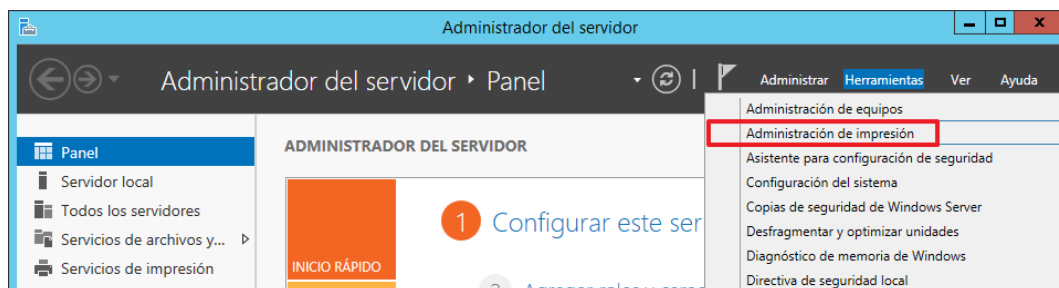


67. El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.

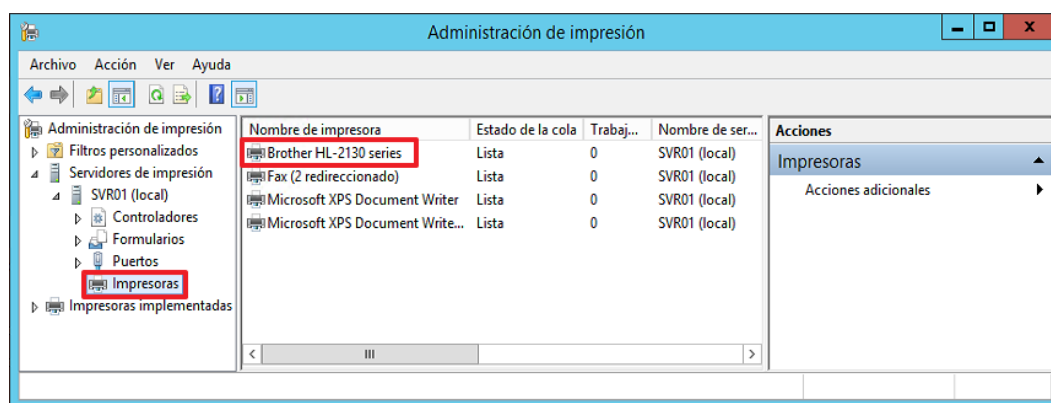


Paso	Descripción
------	-------------

- | | |
|-----|--|
| 68. | <p>Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:</p> <p>“Herramientas → Administración de impresión”.</p> |
|-----|--|

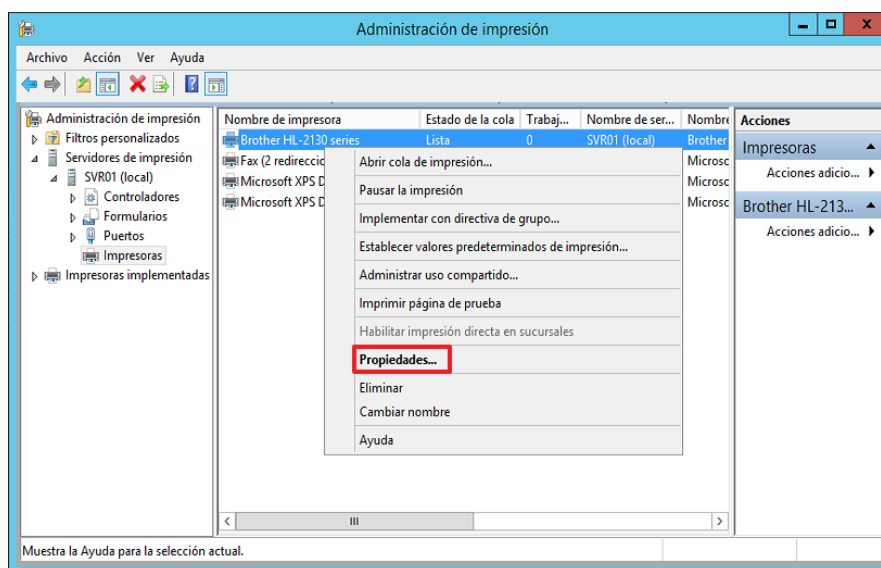


- | | |
|-----|---|
| 69. | <p>Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. Para ello despliegue el nodo “Servidores de impresión / <<nombre del servidor>> / Impresoras”.</p> |
|-----|---|



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

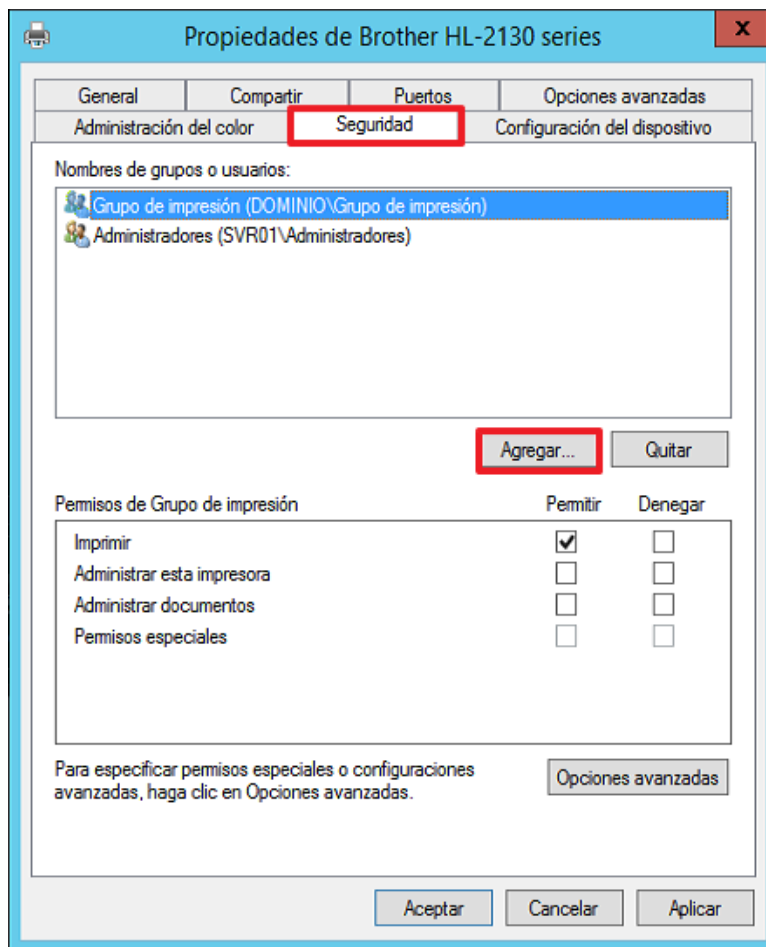
- | | |
|-----|--|
| 70. | <p>Pulse con el botón derecho sobre el dispositivo de impresión y seleccione la opción “Propiedades...”.</p> |
|-----|--|



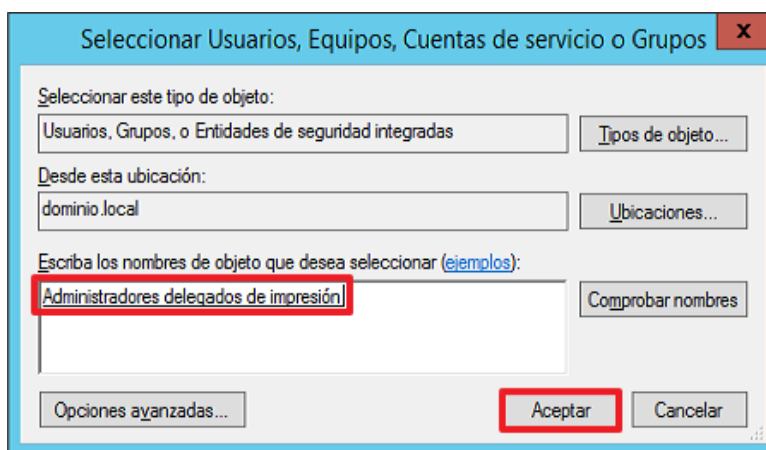
Nota: Para este ejemplo se utiliza el dispositivo denominado “Brother HL-2130 series”.

Paso	Descripción
------	-------------

71. A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Agregar...”.



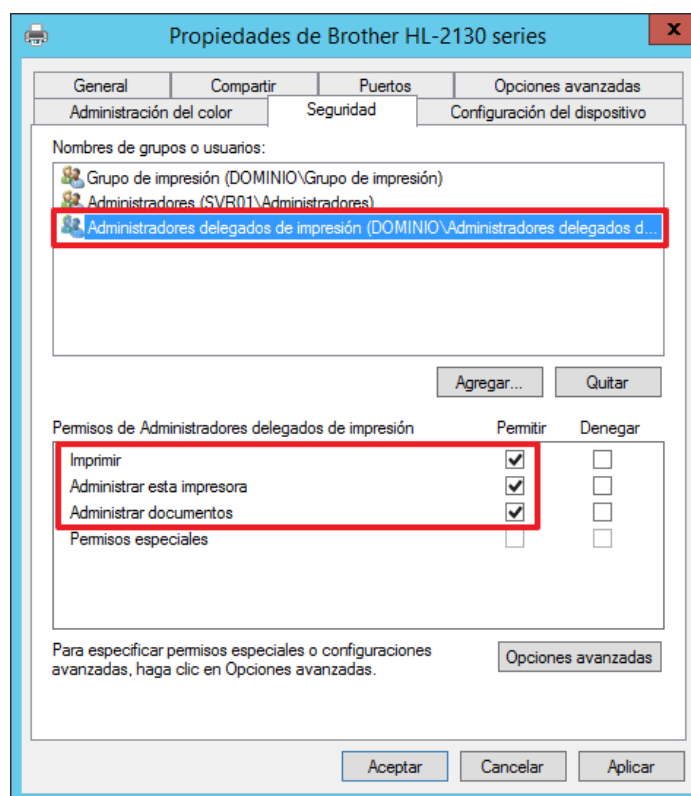
72. Localice el grupo que quiere añadir para que obtenga permisos para poder administrar el dispositivo de impresión seleccionado, y pulse sobre el “Aceptar”.



Nota: En esta guía se selecciona el grupo de seguridad “Administradores delegados de impresión” al cual pertenecen los usuarios que van a obtener permisos administrativos sobre los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.

Paso	Descripción
------	-------------

73. Una vez añadido el grupo de seguridad “Administradores delegados de impresión”, localice el grupo y seleccione los siguientes permisos:
- Imprimir.
 - Administrar esta impresora.
 - Administrar documentos.



74. Una vez establecidos los permisos, pulse “Aceptar” para confirmar los cambios y cerrar la ventana de propiedades del dispositivo de impresión.

ANEXO E. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE IMPRESIÓN QUE LES SEAN 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 empleen servidores de impresión con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran 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, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

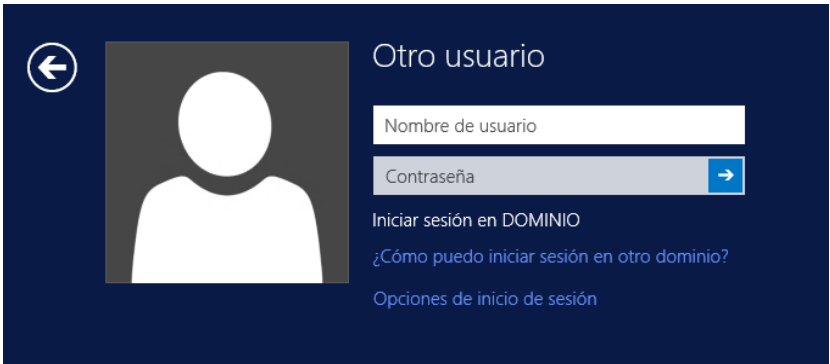
Nota: Si instala el Servidor de impresión por primera vez con la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2 aplicada debe habilitar la instalación remota de roles. Para ello consulte el punto 4 GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA.

1. INSTALACIÓN DEL ROL SERVIDOR DE IMPRESIÓN

Este procedimiento está diseñado para ayudar a los operarios a realizar una instalación básica del rol “Servidor de impresión”.

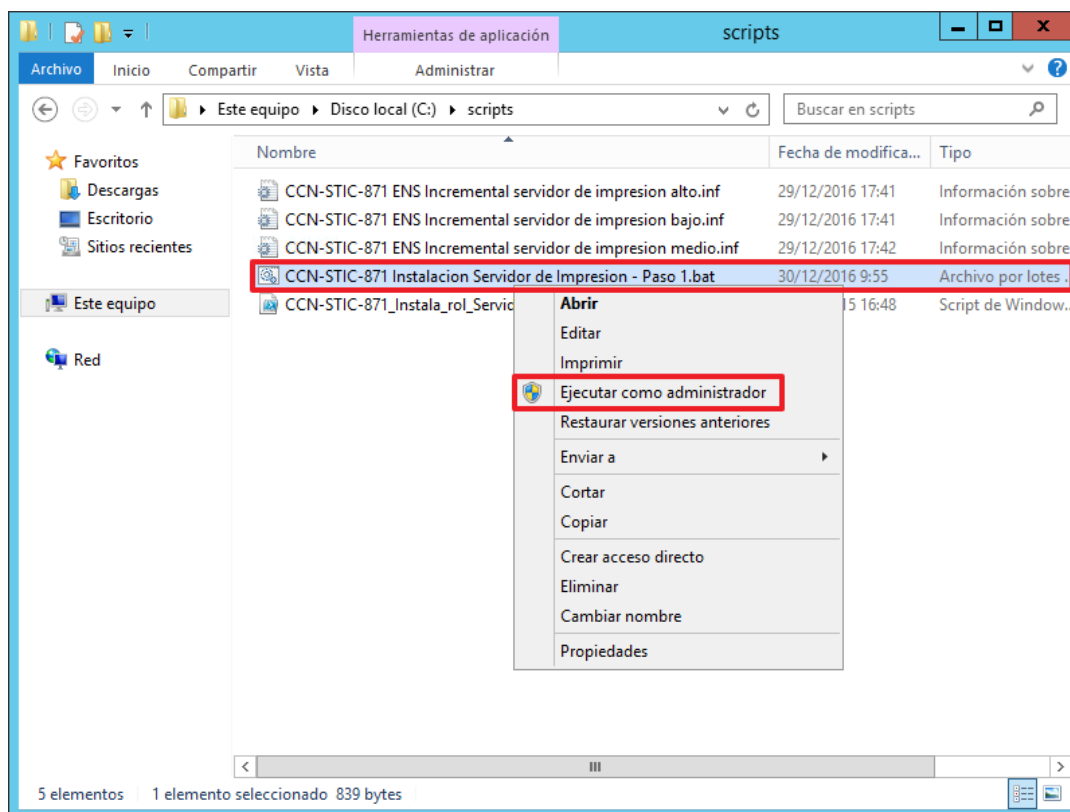
Tenga en consideración que si desea añadir más características o roles al Servidor de impresión deberá modificar el script y adaptarlo a las necesidades de su organización.

Nota: El procedimiento descrito a continuación, indica como instalar el rol “Servidor de impresión”. Si desea realizar este procedimiento continúe con el siguiente punto. En caso de tener ya instalado el rol “Servidor de impresión” vaya al punto “2 PREPARACIÓN DEL DOMINIO”.

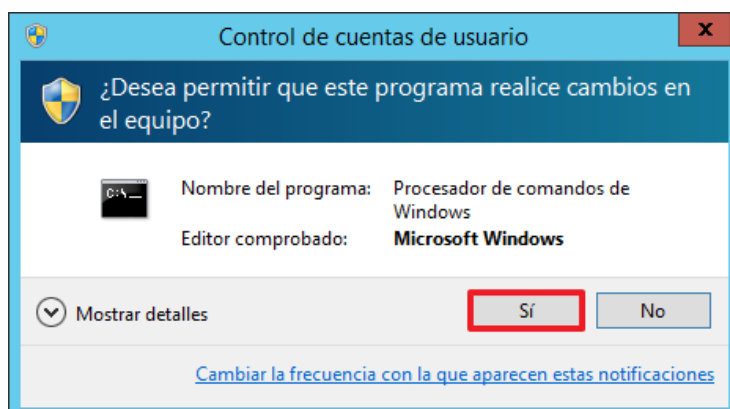
Paso	Descripción
1.	Inicie sesión en el servidor miembro donde vaya a instalar el rol Servidor de impresión. 

Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	En el directorio “C:\Scripts” localice el fichero “CCN-STIC-871 Instalacion Servidor de Impresion – Paso 1.bat”. Seleccione con el botón derecho del ratón y pulse sobre la opción del menú contextual “Ejecutar como administrador”.



5. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse “Sí” para continuar.



Paso	Descripción
------	-------------

6. Se lanzará el script. Pulse cualquier tecla para comenzar la instalación.

```

C:\Windows\System32\cmd.exe

CCN-STIC-871 Servidor de Impresion - Paso 1

Este script instala el rol Servidor de impresion.

Antes de ejecutar este script asegurese que los ficheros y
scripts de esta guia se encuentran en el directorio C:\Scripts.

Si desea instalar características adicionales cierre esta ventana
y modifique el presente script.

Presione una tecla para continuar . . . _

```

7. La instalación comenzará. Espere a que finalice.

```

Administrador: Windows PowerShell

Recopilando datos...
10 %
[ooooooooo]

Si desea instalar características adicionales cierre esta ventana
y modifique el presente script.

Presione una tecla para continuar . . .

C:\Scripts>powershell.exe -executionpolicy RemoteSigned -File CCN-STIC-871_Instala_rol_ServidorImpresion.ps1

```

8. Cuando haya finalizado la instalación pulse una tecla para cerrar la ventana.

```

Administrador: Windows PowerShell

CCN-STIC-871 Servidor de Impresion - Paso 1

Este script instala el rol Servidor de impresion.

Antes de ejecutar este script asegurese que los ficheros y
scripts de esta guia se encuentran en el directorio C:\Scripts.

Si desea instalar características adicionales cierre esta ventana
y modifique el presente script.

Presione una tecla para continuar . . .

C:\Scripts>powershell.exe -executionpolicy RemoteSigned -File CCN-STIC-871_Instala_rol_ServidorImpresion.ps1

Success Restart Needed Exit Code      Feature Result
-----
True     No          Success      {Servidor de impresión, Servicios de i...

ADVERTENCIA: La actualización automática de Windows no está habilitada. Para
asegurarse de que la característica o el rol recién instalados se actualicen
automáticamente, active Windows Update en el Panel de control.

CCN-STIC-871 Servidor de Impresion - Paso 1 : EJECUCION FINALIZADA

Presione una tecla para continuar . . .

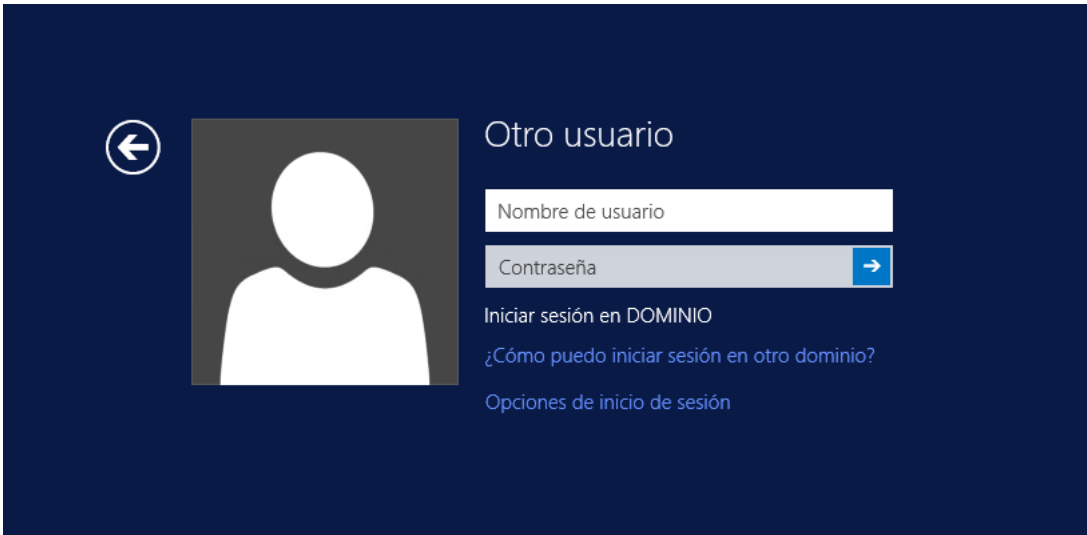
```

Nota: Ignore la advertencia sobre las actualizaciones automáticas de Windows.

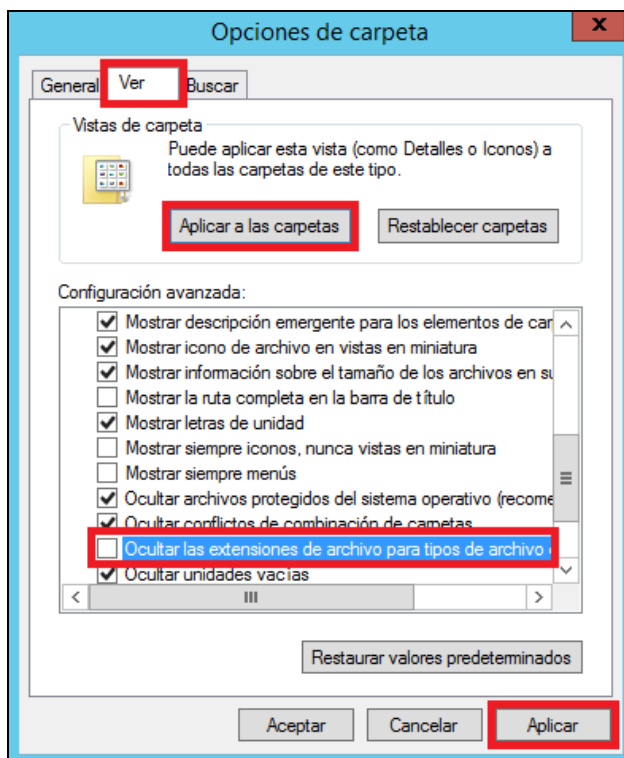
2. PREPARACIÓN DEL DOMINIO

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

Nota: Esta guía asume que a los servidores Controladores del Dominio al que pertenece el equipo servidor de impresión que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-870A Implementación del ENS en Windows Server 2012 R2. Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

Paso	Descripción
9.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios de ENS. 
	Nota: Inicie sesión con una cuenta que sea Administrador del Dominio.
10.	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.
11.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
12.	Configure el "Explorador de Windows" para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que "Explorador de Windows" muestra las extensiones de los archivos.

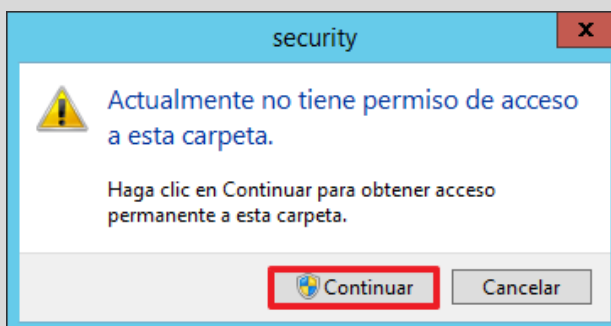
Paso	Descripción
13.	Para configurar el “Explorador de Windows” y que éste muestre las extensiones de todos los archivos, abra una ventana del “Explorador de Windows”, seleccione el menú “Vista” y dentro de dicho menú, “Opciones”. En la venta emergente, seleccione la pestaña “Ver” y desmarque la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”, como se muestra en la imagen.



Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación "¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?", y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

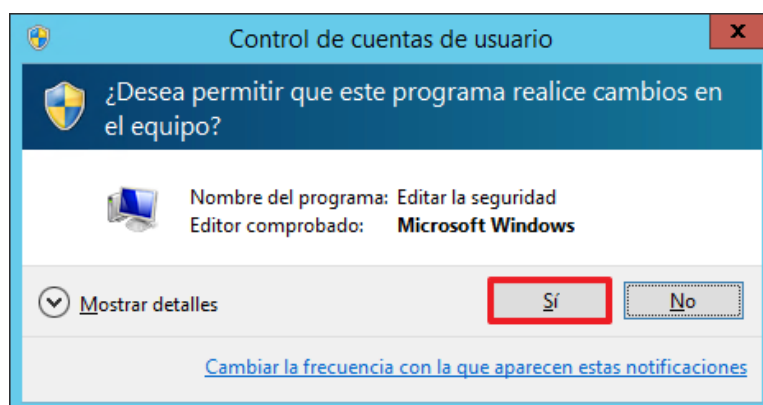
14. Adicionalmente acceda al directorio "C:\Windows\security\templates".

Nota: Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón "Continuar" ante la ventana emergente.

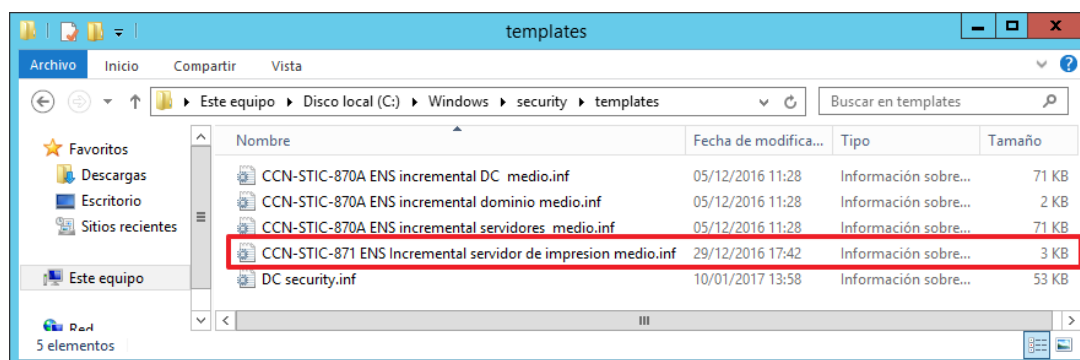


Paso	Descripción
------	-------------

15. El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Pulse “Sí” para continuar.



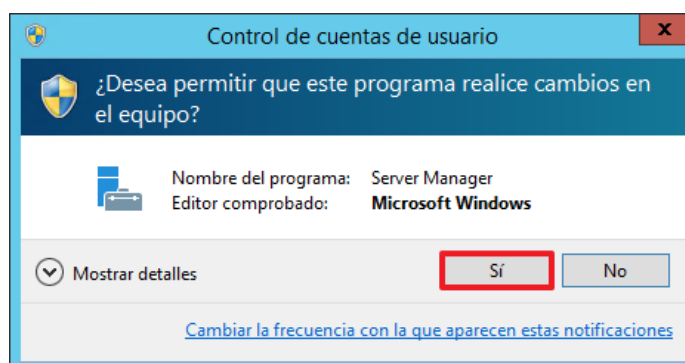
16. Copie el fichero “CCN-STIC-871 ENS Incremental servidor de impresion medio.inf” ubicado en “C:\Scripts” en el directorio “C:\Windows\security\templates”.



17. A continuación, deberá crear la unidad organizativa "Servidores de Impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.

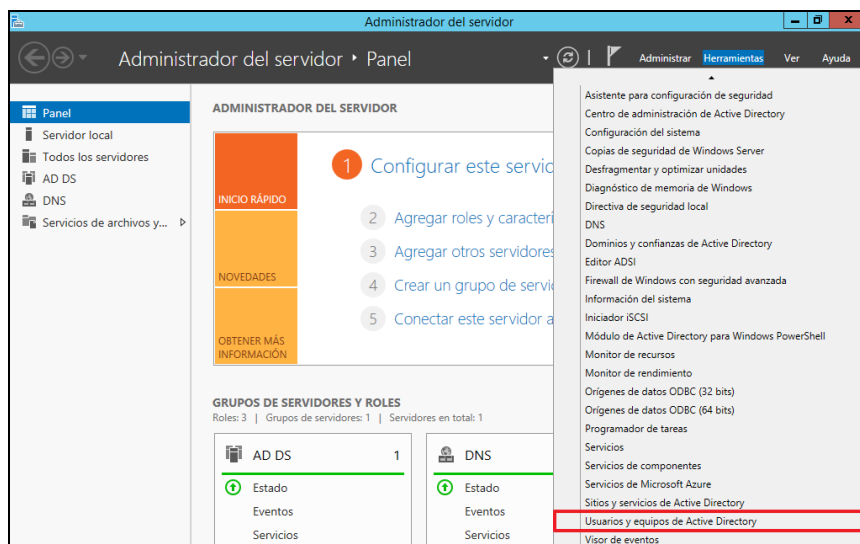


18. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.

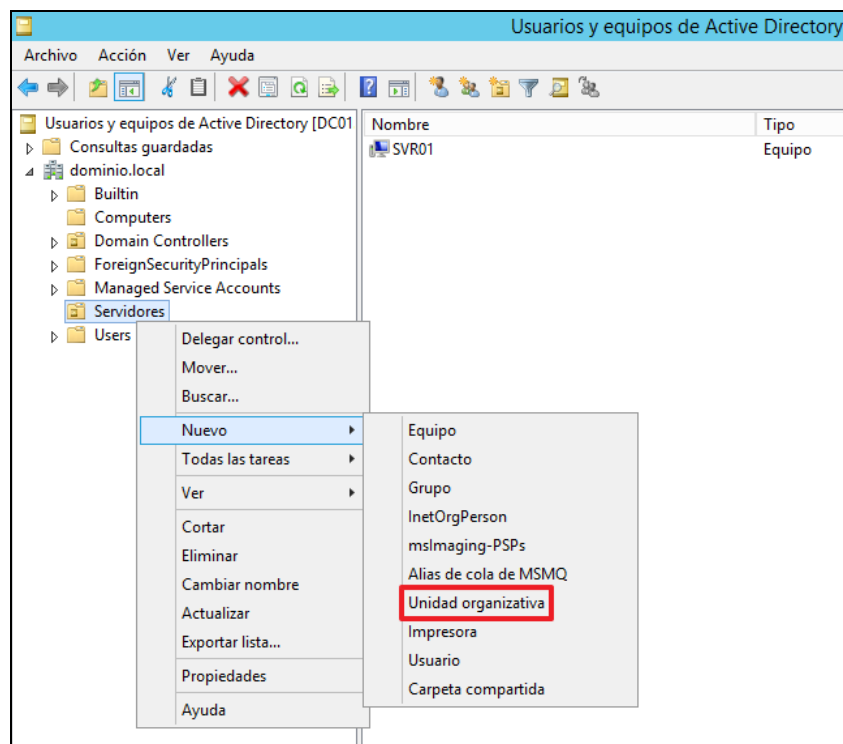


Paso	Descripción
------	-------------

19. Inicie la herramienta “Usuarios y equipos de Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Usuarios y equipos de Active Directory”



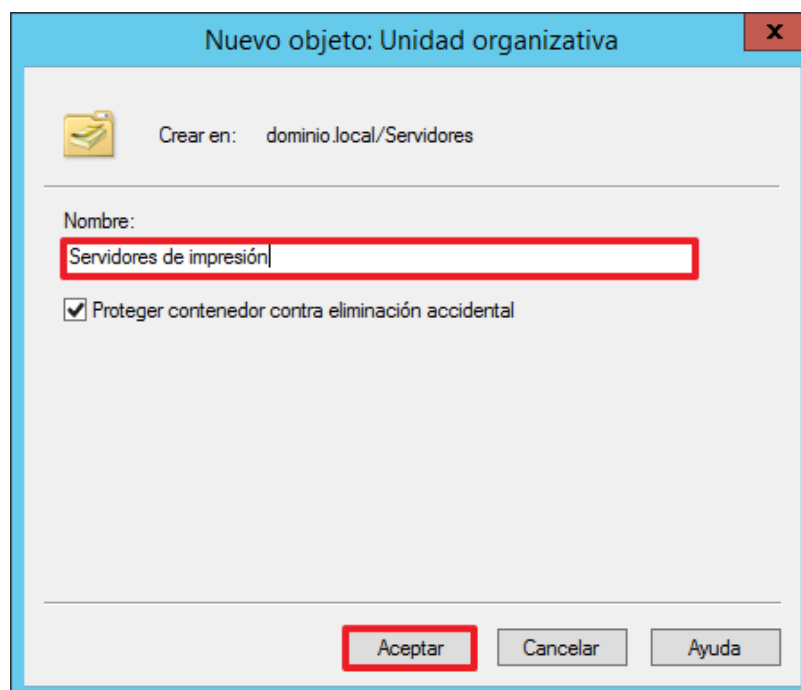
20. En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2. Para ello, seleccione el nodo “<<dominio>> / <<unidad organizativa>>”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo > Unidad organizativa”.



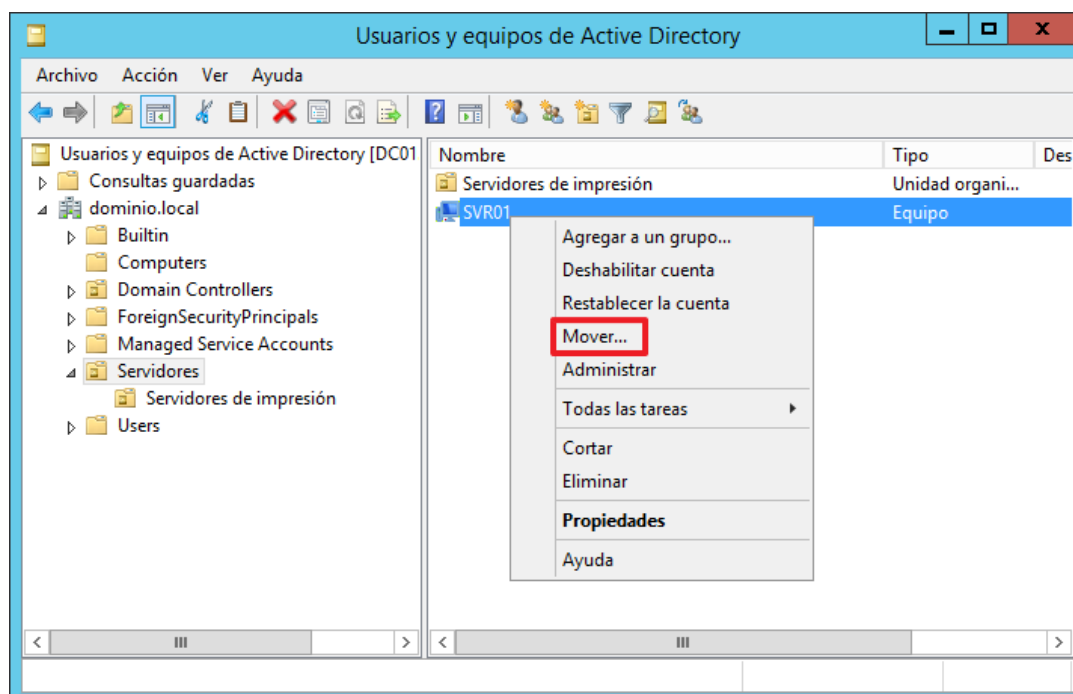
Nota: En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local/servidores”.

Paso	Descripción
------	-------------

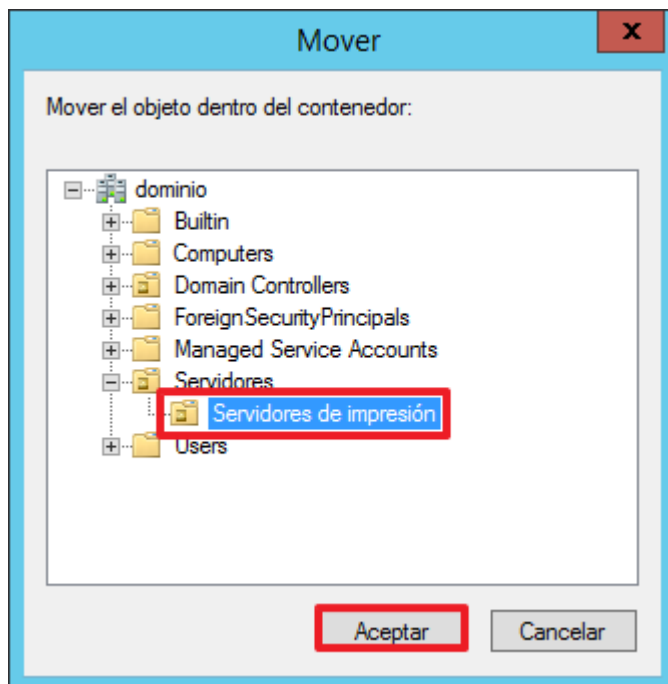
21. Introduzca el nombre “Servidores de impresión” tal y como se muestra en la imagen y pulse sobre “Aceptar”.



22. Una vez creada la nueva Unidad organizativa, deberá mover los servidores de impresión a la unidad organizativa “Servidores de impresión”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”.



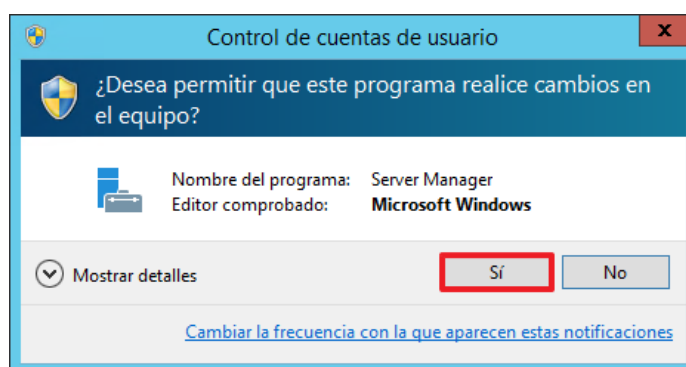
Paso	Descripción
23.	A continuación, seleccione la unidad organizativa “Servidores de impresión” y pulse “Aceptar”.



24. Cierre la herramienta “Usuarios y equipos de Active Directory”.
25. A continuación, deberá crear la GPO "CCN-STIC-871 ENS Incremental servidor de impresion medio". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.

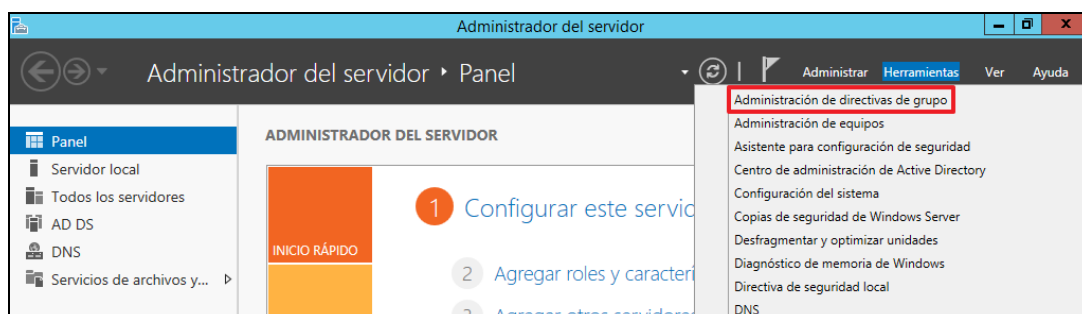


26. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



Paso	Descripción
------	-------------

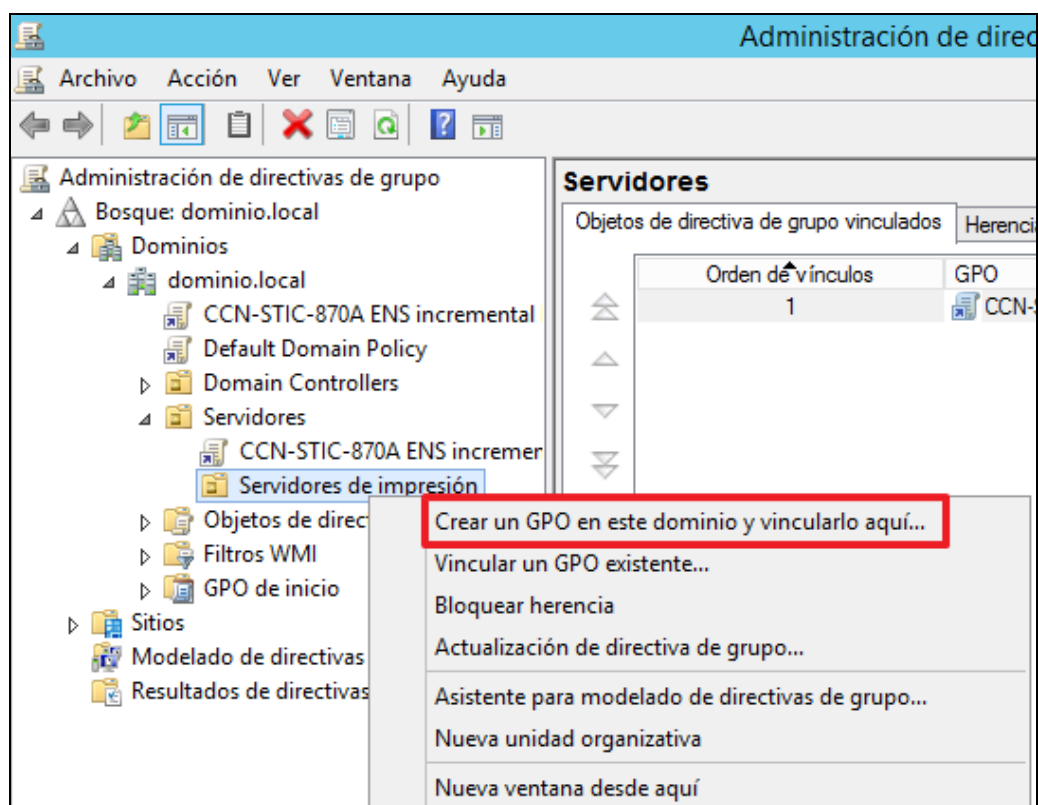
27. Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”.



28. A continuación, despliegue el nodo “Bosque: <<nombre de bosque>> / Dominios / <<nombre de dominio>> / Servidores / Servidores de impresión”.

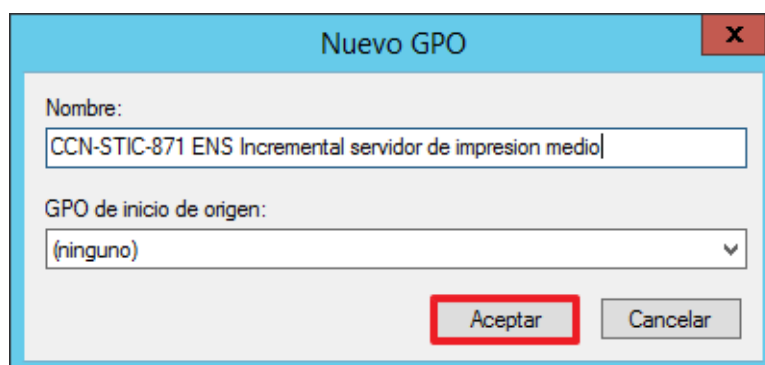
Nota: En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es “Servidores de impresión”.

29. Pulse con el botón derecho sobre la unidad organizativa “Servidores de impresión” y seleccione “Crear un GPO en este dominio y vincularlo aquí...”.

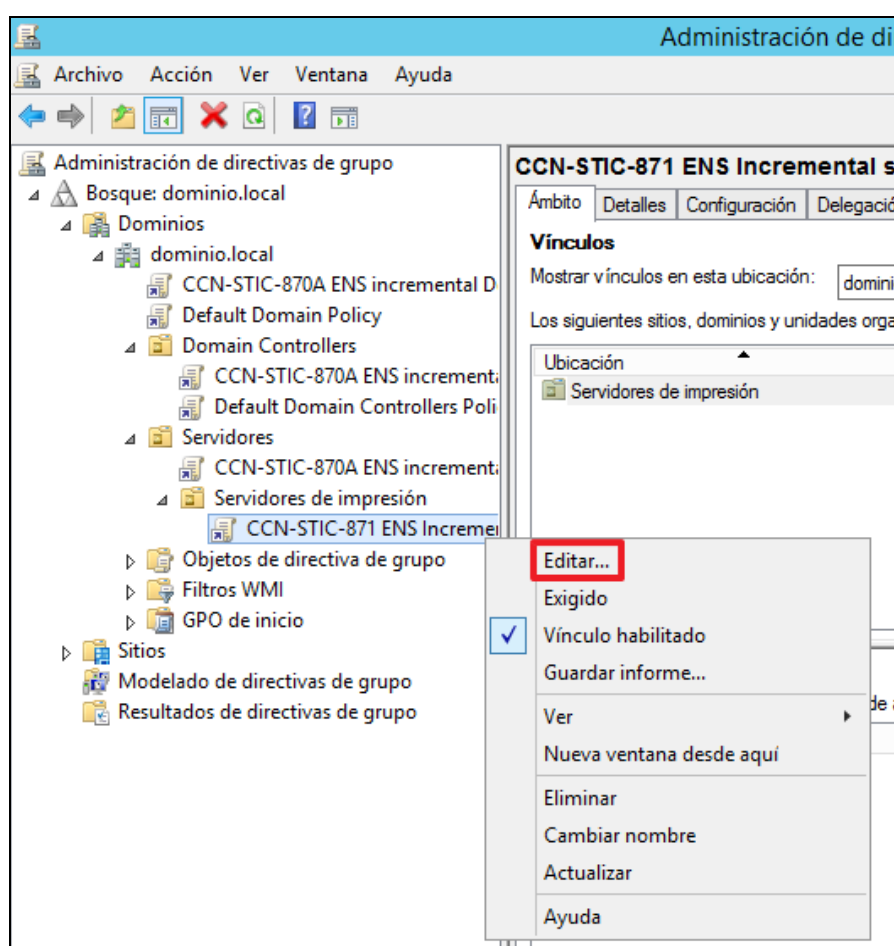


Paso	Descripción
------	-------------

30. Escriba el nombre de la GPO "CCN-STIC-871 ENS Incremental servidor de impresion medio" y haga clic en el botón "Aceptar".



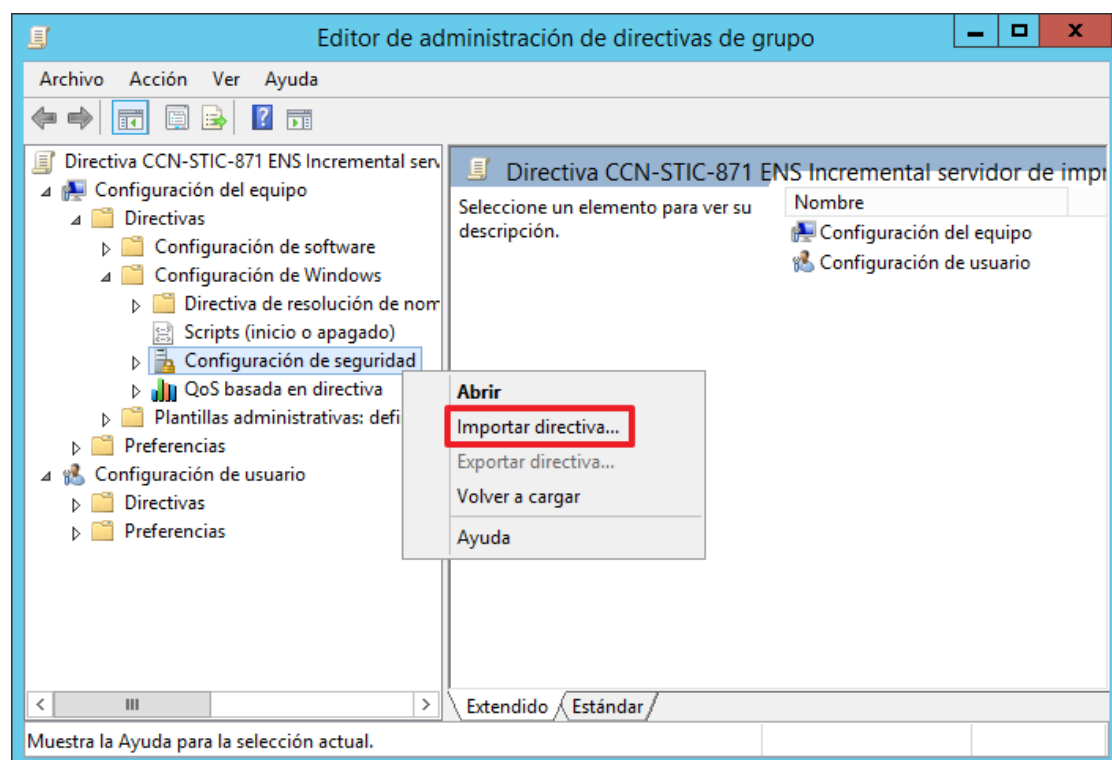
31. Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción "Editar".



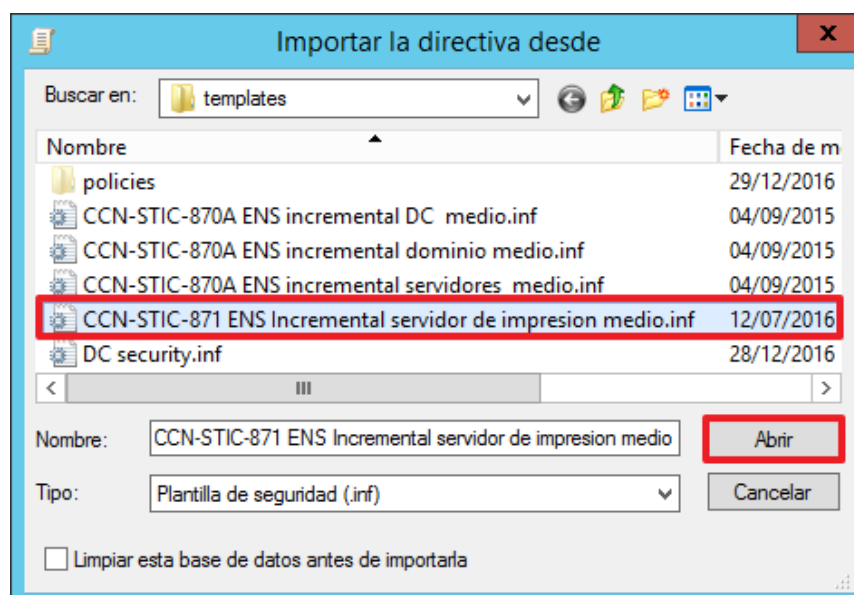
32. Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta:
"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad"

Paso	Descripción
------	-------------

33. Pulse con el botón derecho sobre configuración de seguridad y seleccione la opción “Importar directiva...”.



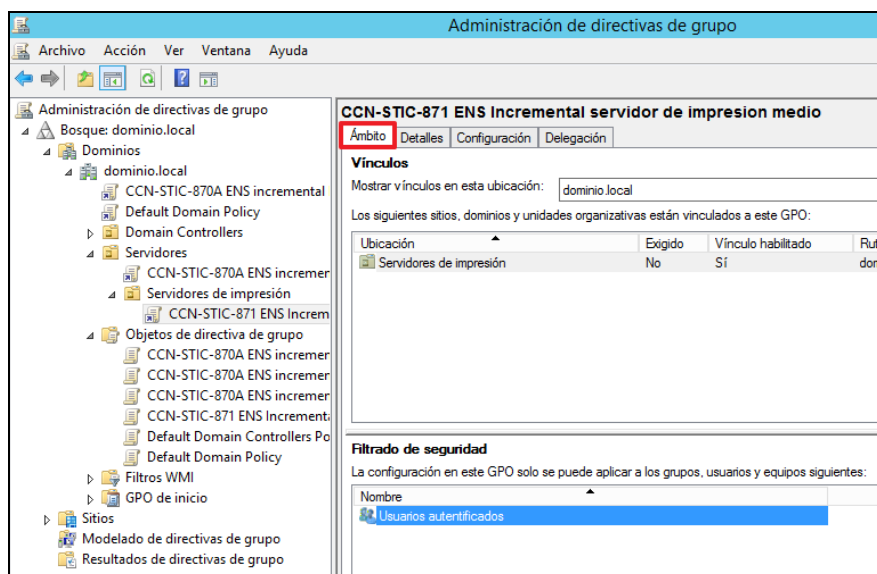
34. Seleccione de la ruta “C:\Windows\security\templates” el fichero “CCN-STIC-871 ENS Incremental servidor de impresion medio.inf” y pulse el botón “Abrir”.



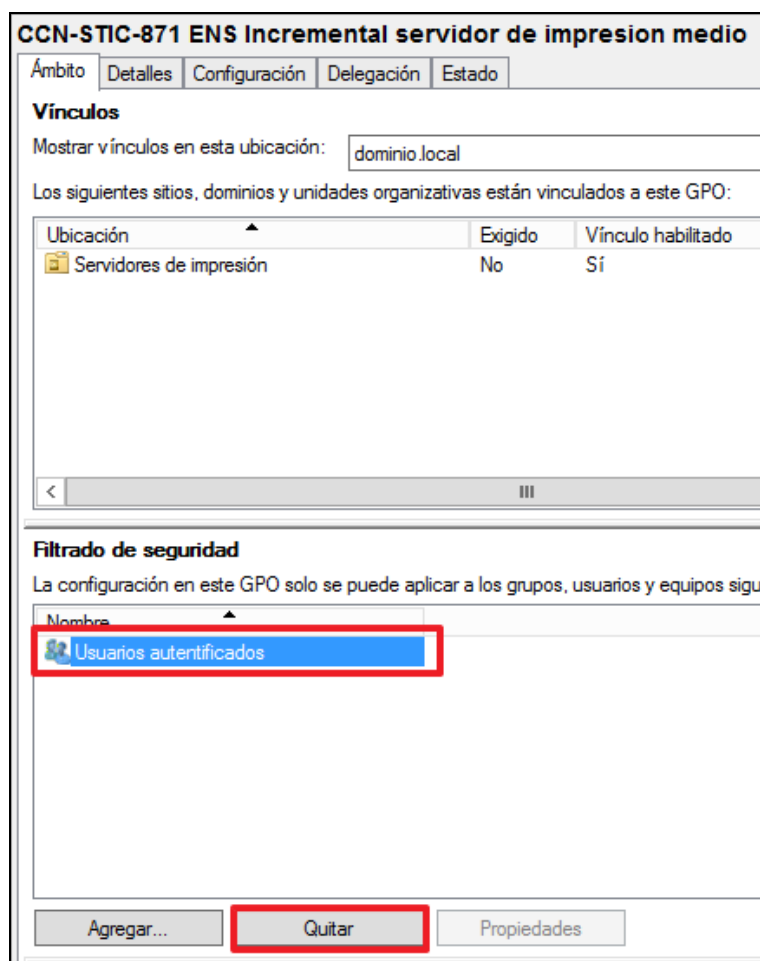
35. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.

Paso	Descripción
------	-------------

- | | |
|-----|--|
| 36. | Seleccione la nueva política de grupo configurada y vaya a la pestaña “Ámbito” que se encuentra en el panel derecho. |
|-----|--|

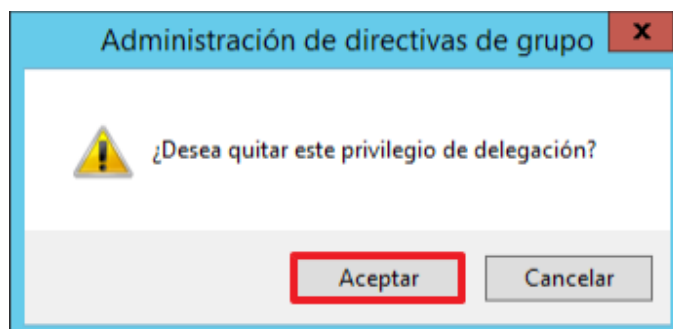


- | | |
|-----|---|
| 37. | En la opción de filtrado de seguridad, seleccione “Usuarios autenticados” y pulse la opción “Quitar”. |
|-----|---|

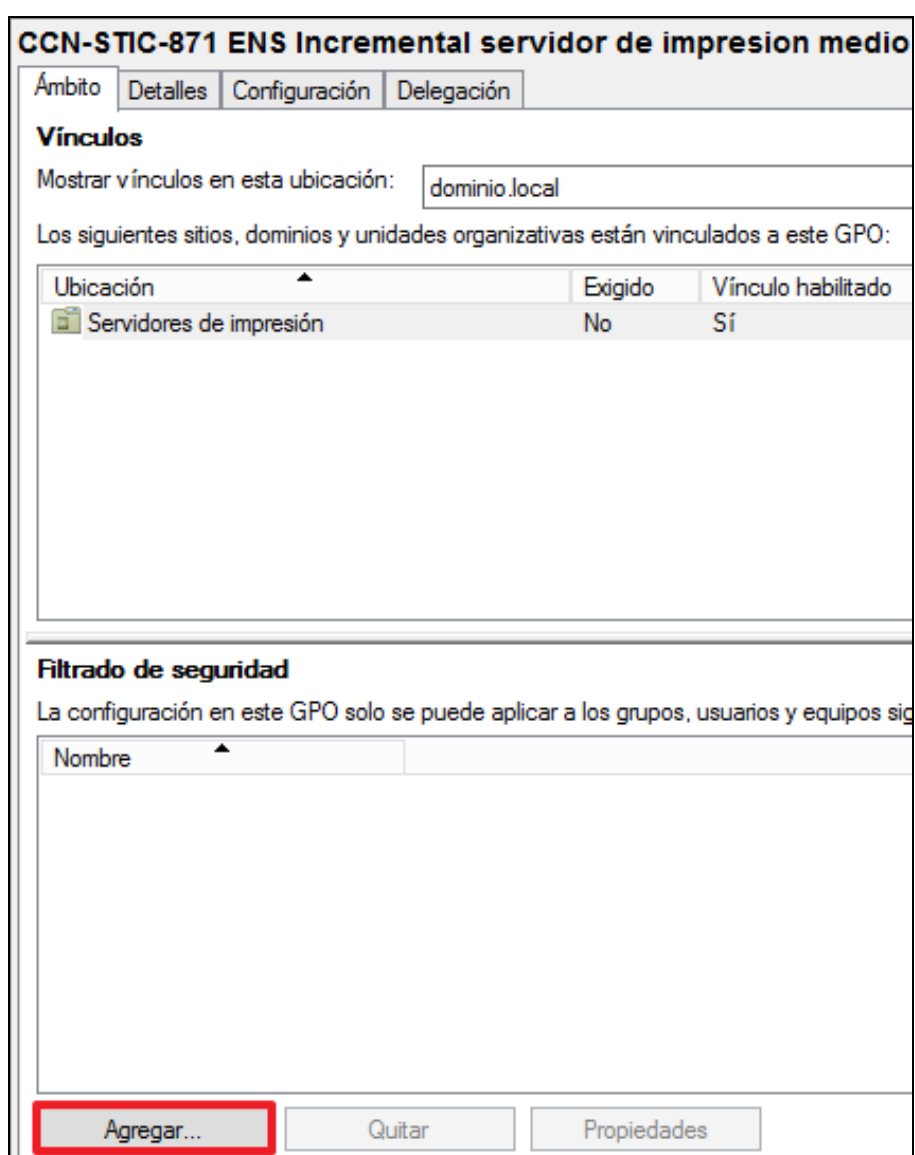


Paso	Descripción
------	-------------

- | | |
|-----|---|
| 38. | Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”. |
|-----|---|



- | | |
|-----|--|
| 39. | A continuación, pulse el botón “Agregar...”. |
|-----|--|



Paso	Descripción
------	-------------

40. Introduzca como nombre “ENS servidores Windows 2012 R2 nivel medio”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2. A continuación, pulse el botón “Aceptar”.

Nota: En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a las necesidades de su organización.

3. 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.

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

3.1 PRINCIPIO DE MÍNIMA FUNCIONALIDAD Y MÍNIMA EXPOSICIÓN

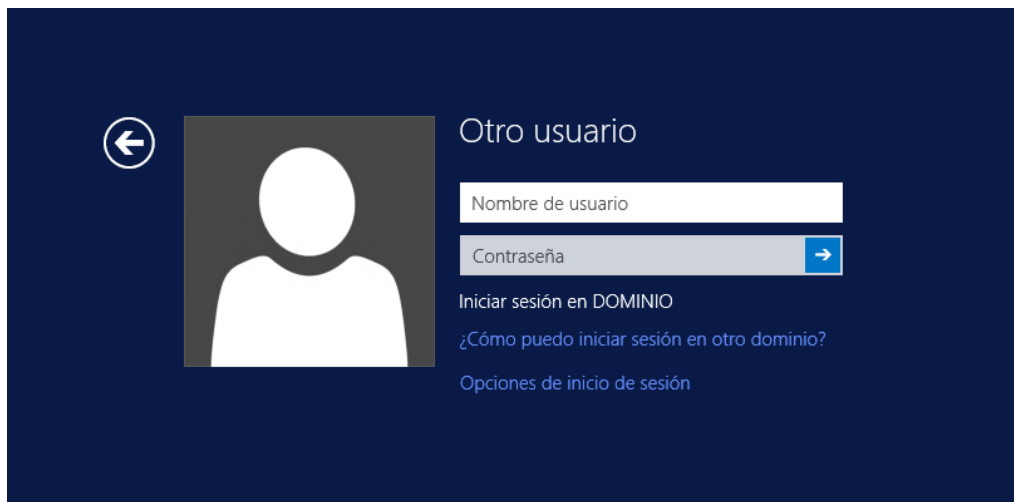
Uno de los aspectos que marca el ENS, desde su requisito de nivel bajo en el Marco Operacional es la mínima funcionalidad y mínima exposición evitando con ello posibles ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar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

Para realizar el siguiente paso a paso deberá realizar previamente el paso “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” y una vez finalizado deberá realizar el paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

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

Paso	Descripción
------	-------------

- | | |
|-----|--|
| 41. | Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de impresión. |
|-----|--|

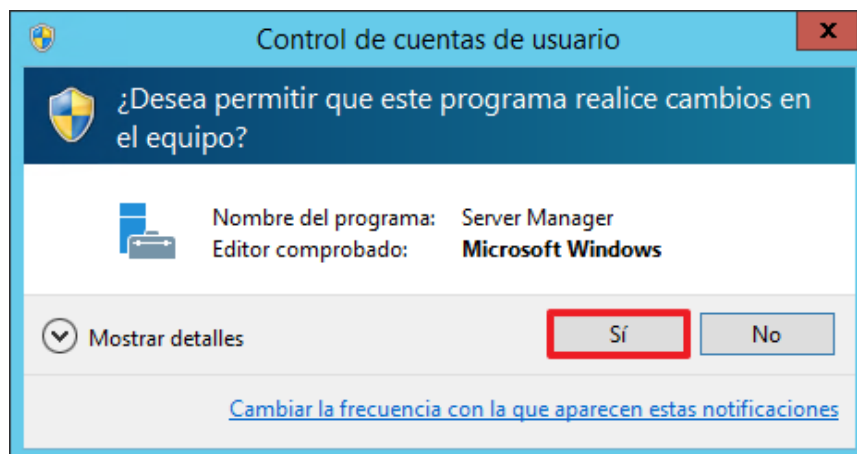


Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

- | | |
|-----|---|
| 42. | Abra el "Administrador del servidor". Para ello pulse sobre el botón correspondiente en la barra de tareas. |
|-----|---|

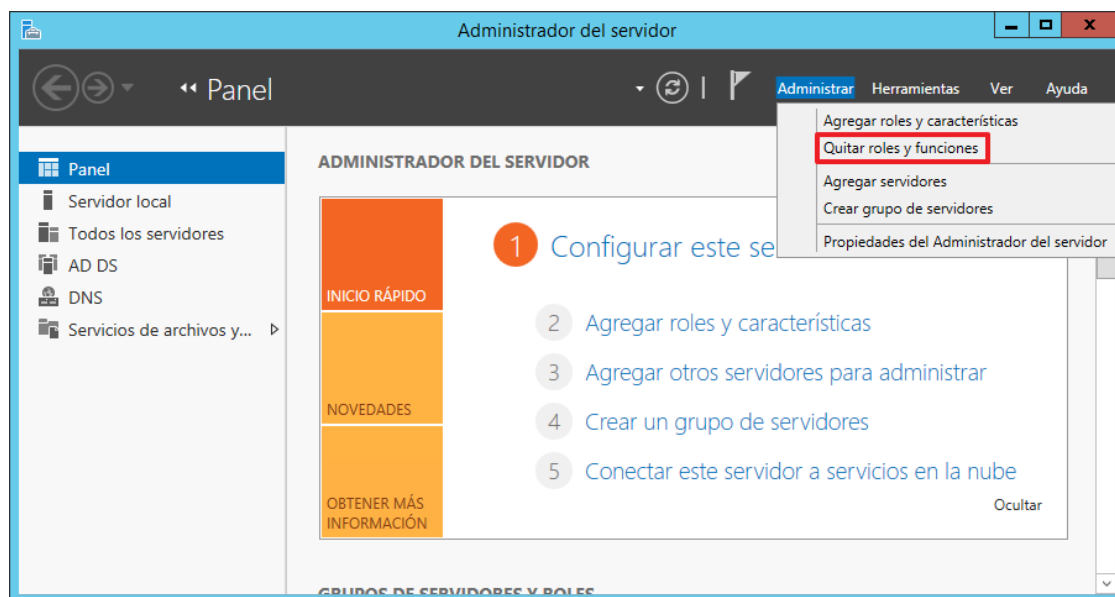


- | | |
|-----|--|
| 43. | El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar. |
|-----|--|

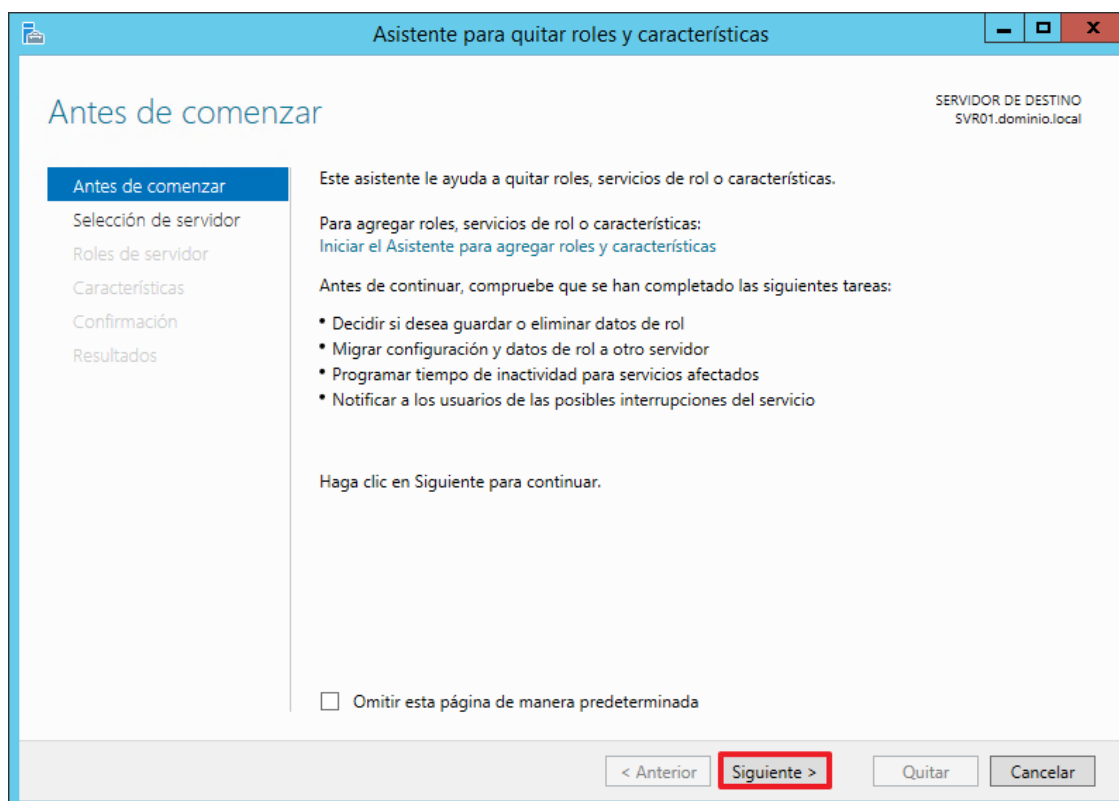


Paso	Descripción
------	-------------

44. A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.

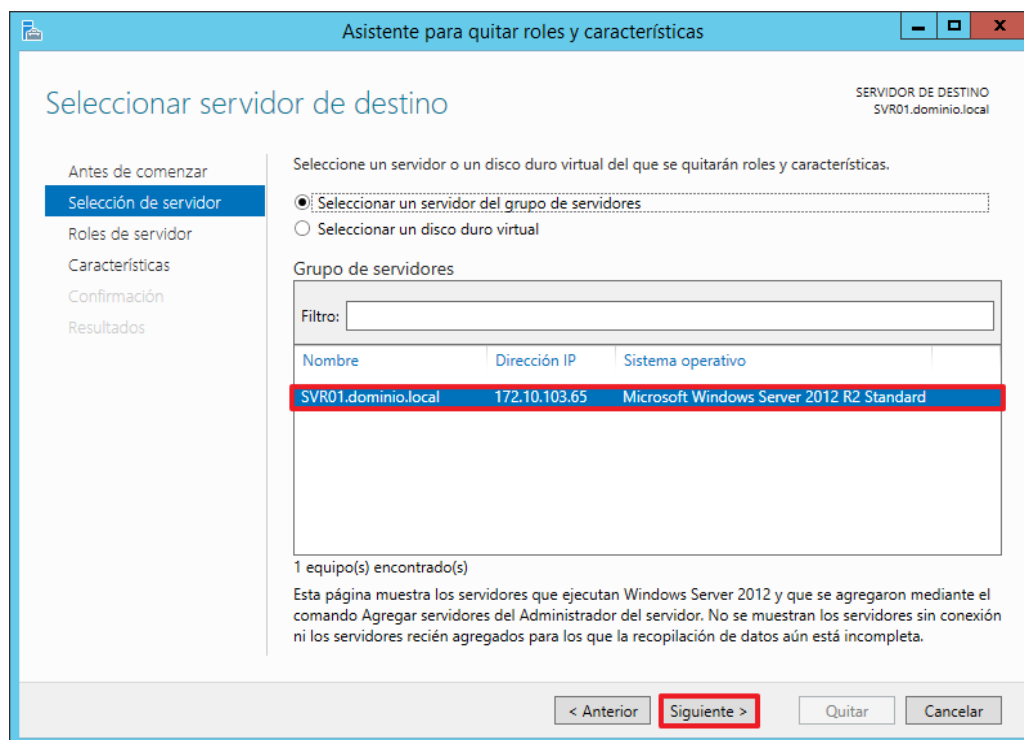


45. Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar.



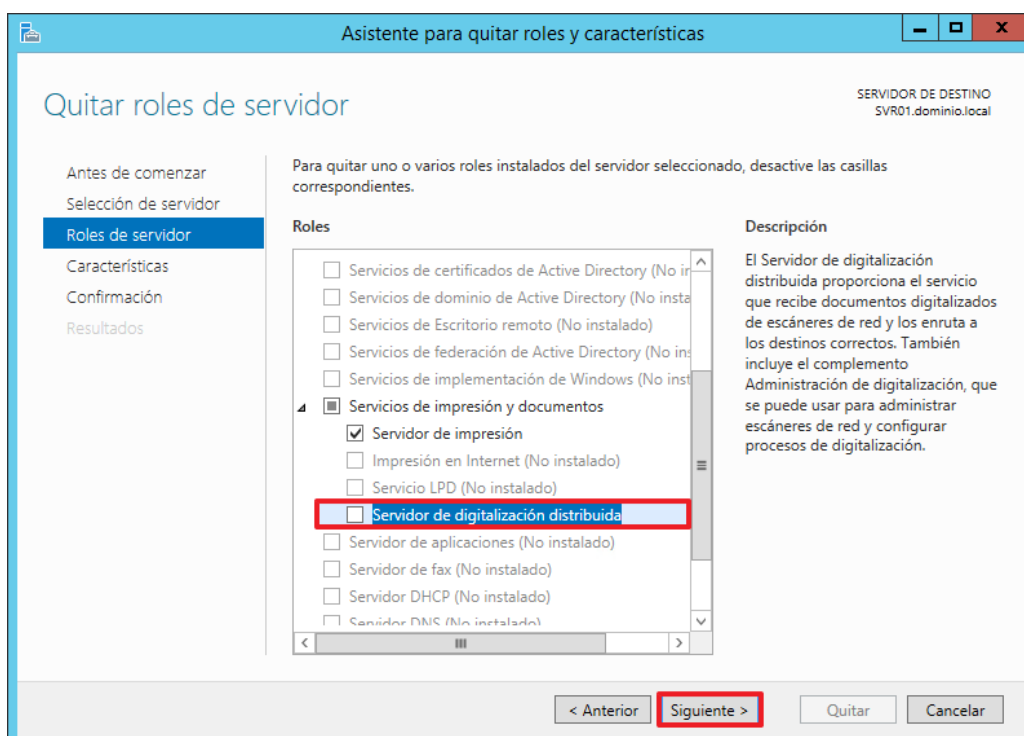
Paso	Descripción
------	-------------

- | | |
|-----|--|
| 46. | Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”. |
|-----|--|



Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

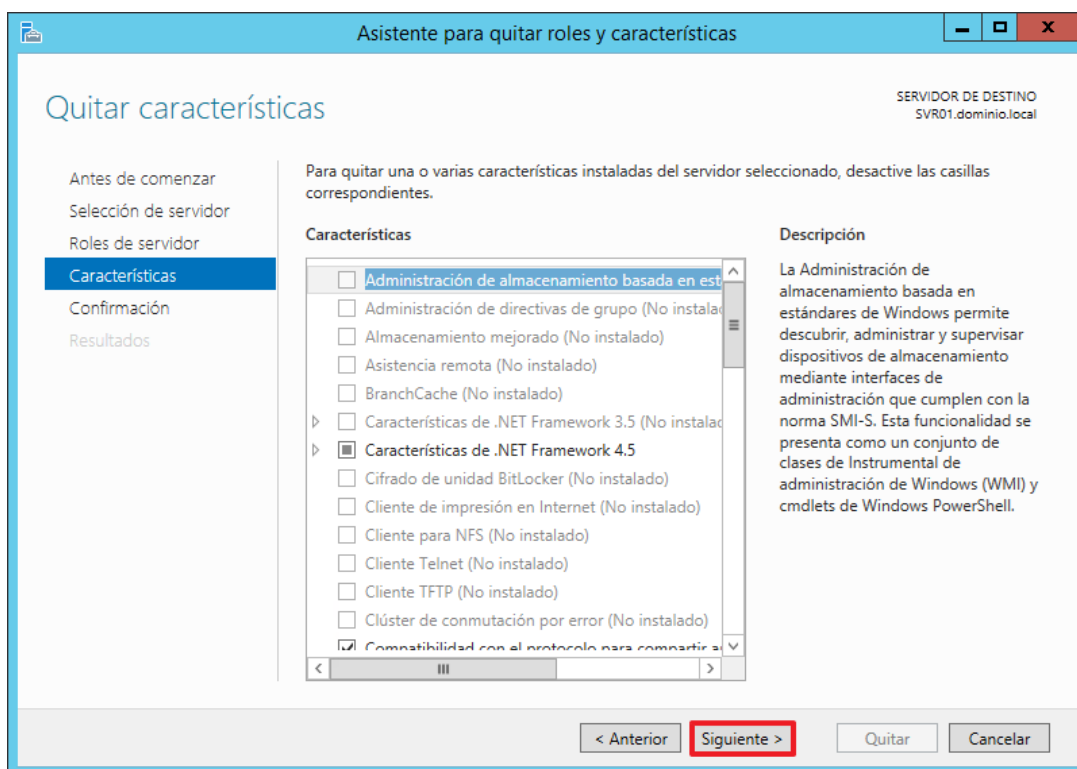
- | | |
|-----|--|
| 47. | En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”. |
|-----|--|



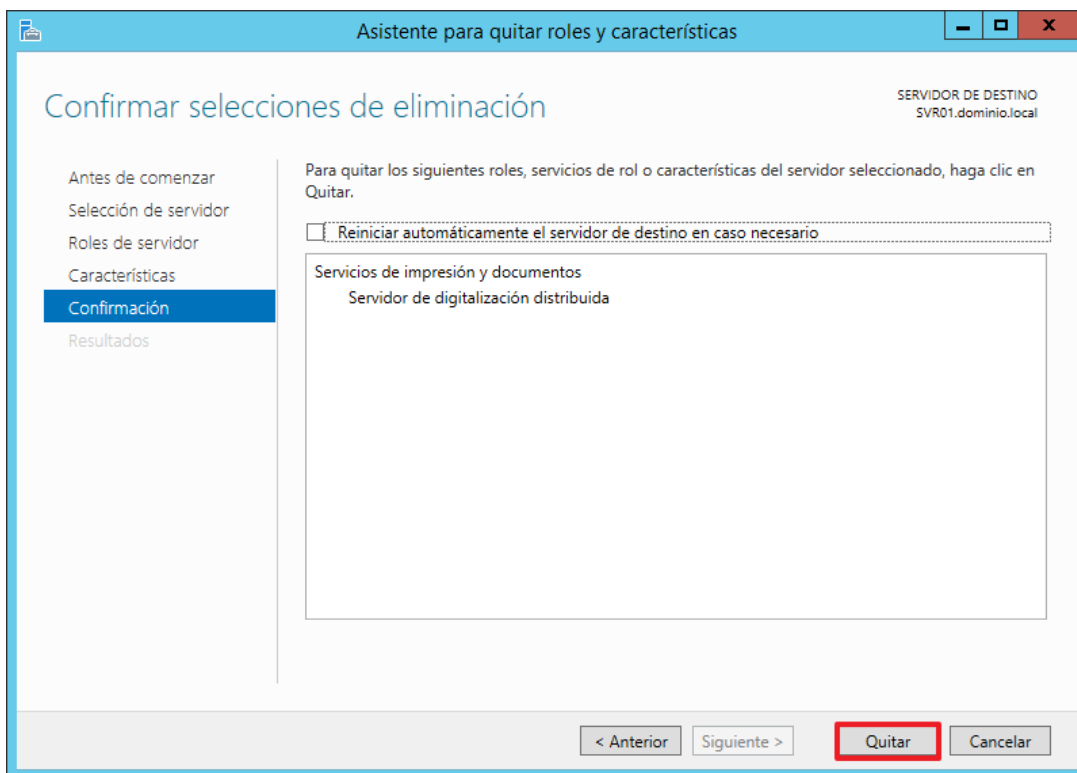
Nota: En este ejemplo se desinstala el rol “servidor de digitalización distribuida”.

Paso	Descripción
------	-------------

- | | |
|-----|---|
| 48. | En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. |
|-----|---|

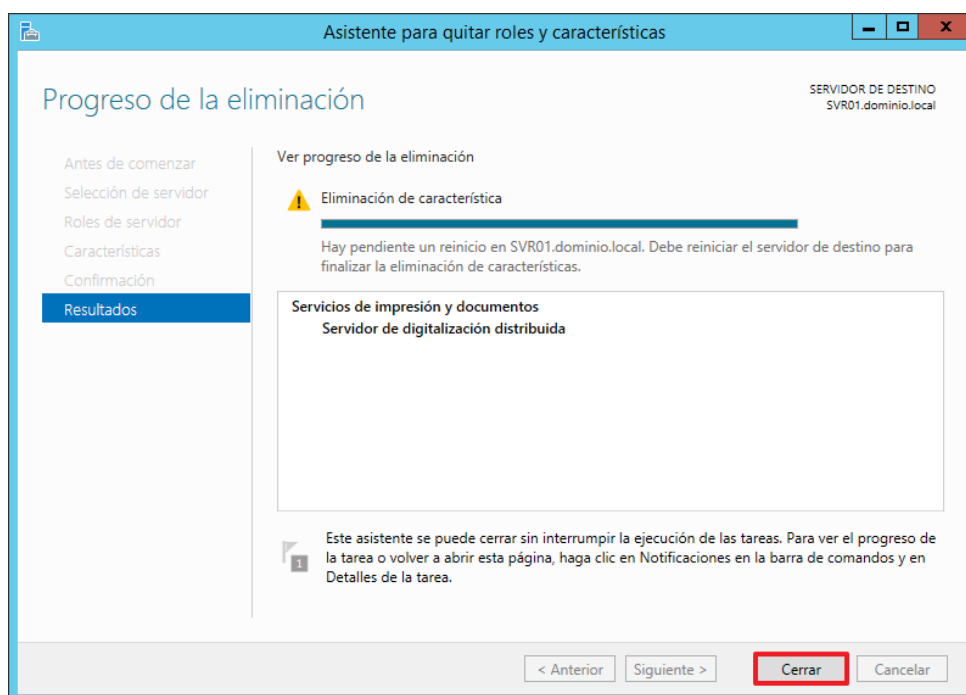


- | | |
|-----|--|
| 49. | En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso. |
|-----|--|



Paso	Descripción
------	-------------

50. El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación.



51. En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración.

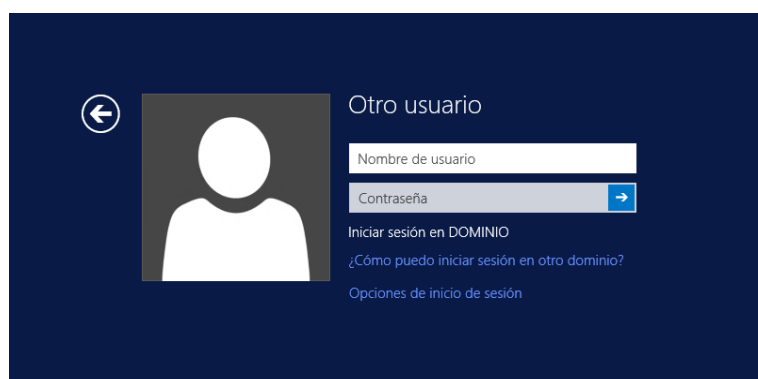
52. A continuación, deberá desvincular la GPO creada anteriormente para eliminar un rol, para ello realice el punto “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

3.2 GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN

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

Paso	Descripción
------	-------------

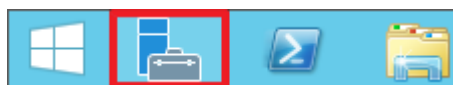
53. Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.



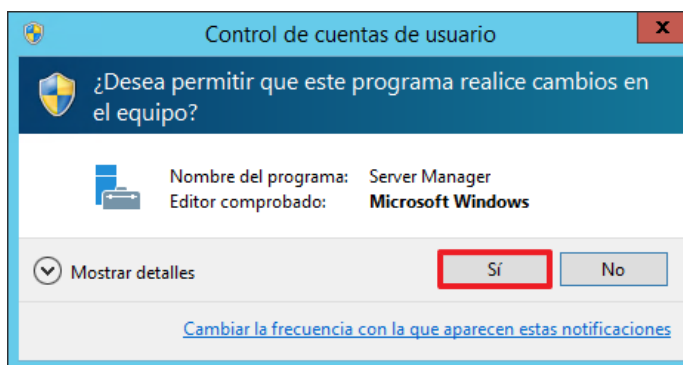
Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

Paso	Descripción
------	-------------

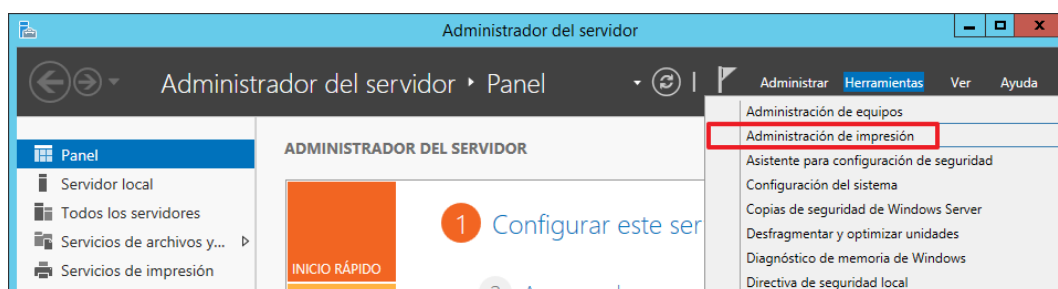
54. A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta “Administrador del servidor” mediante el icono correspondiente.



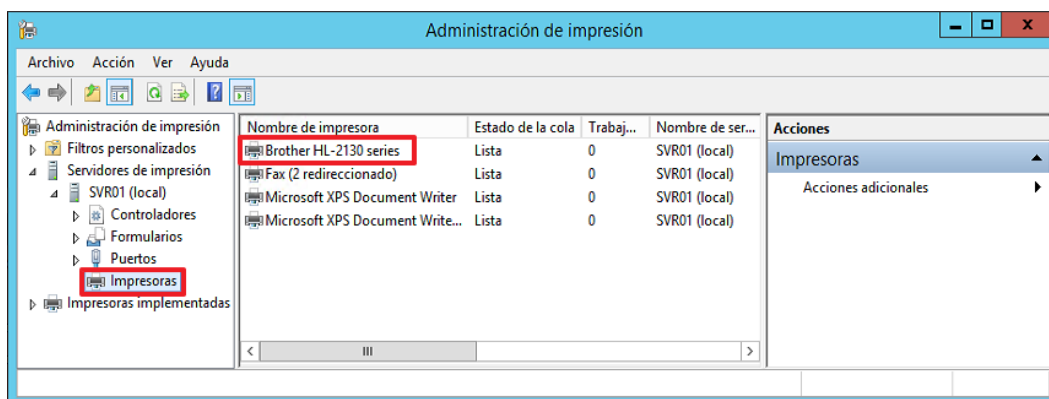
55. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



56. Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de impresión”.



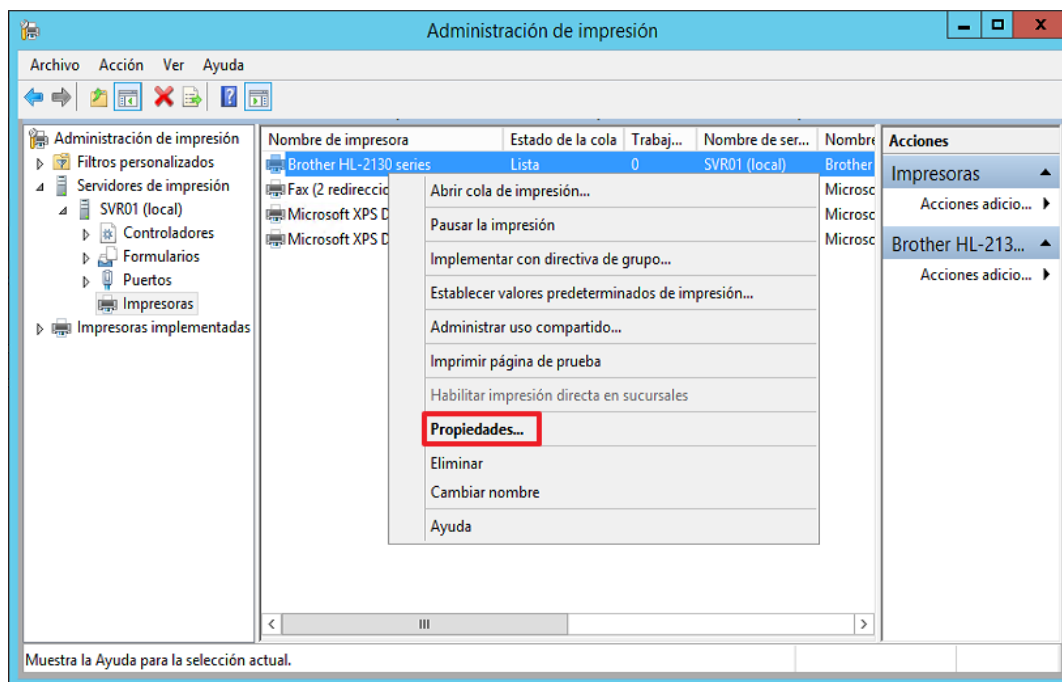
57. Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo “Servidores de impresión / <<nombre del servidor>> / Impresora”.



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

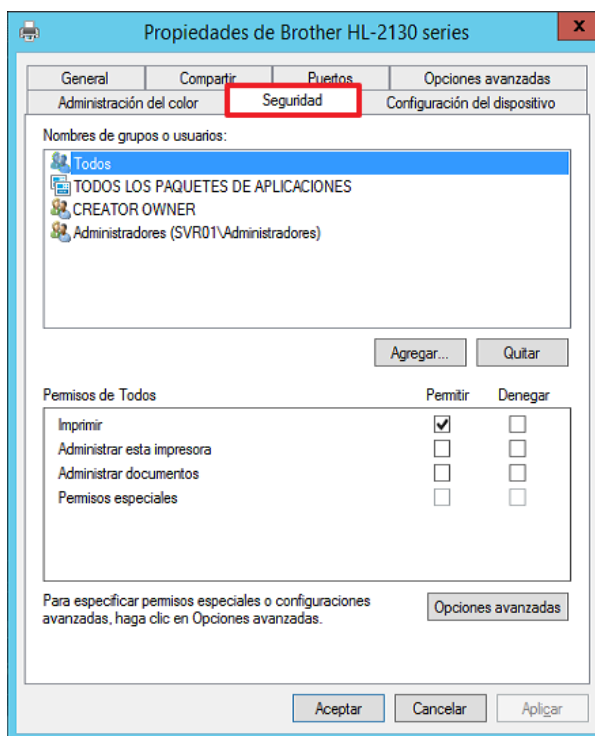
Paso	Descripción
------	-------------

- | | |
|-----|---|
| 58. | Pulse con el botón derecho sobre el dispositivo de impresión al que desea aplicar permisos y seleccione la opción “Propiedades...”. |
|-----|---|



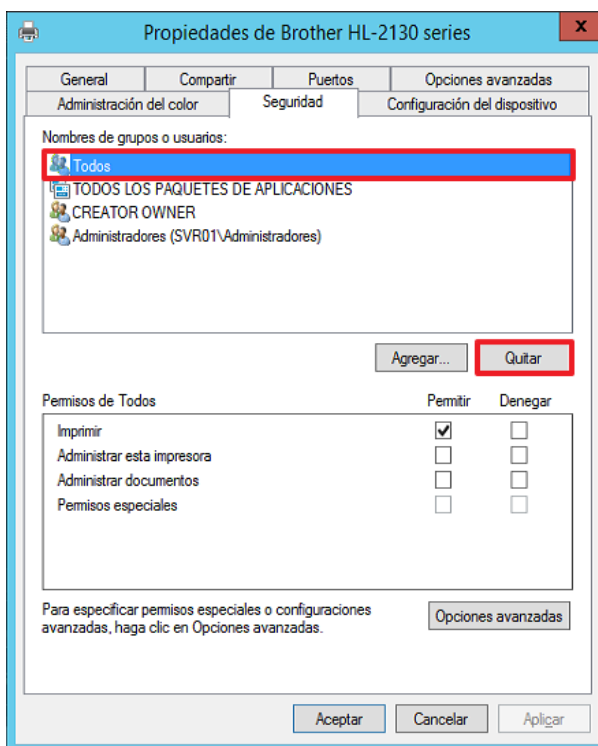
Nota: En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.

59. A continuación, seleccione la pestaña “Seguridad”.



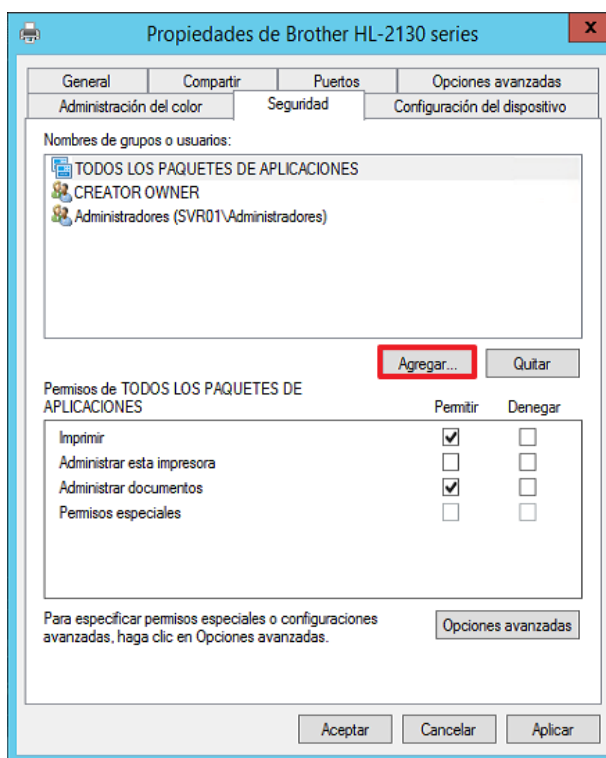
Paso	Descripción
------	-------------

60. Seleccione el grupo de usuarios “Todos” y a continuación pulse en la opción “Quitar”.



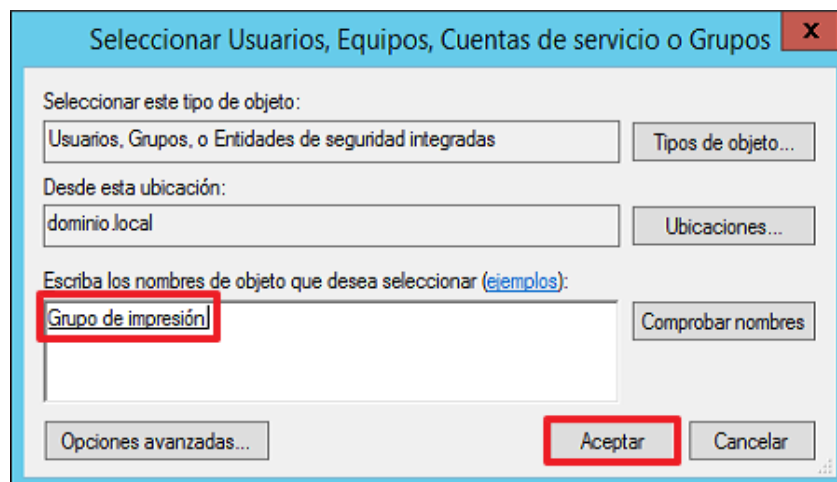
Nota: Debera adaptar este paso a los requisitos de su organización eliminando los usuarios o grupos de usuarios que no requieran de permisos sobre el dispositivo de impresión.

61. A continuación, pulse sobre el botón “Agregar” para añadir el grupo de usuarios que tendrá permiso para poder imprimir por este dispositivo de impresión.



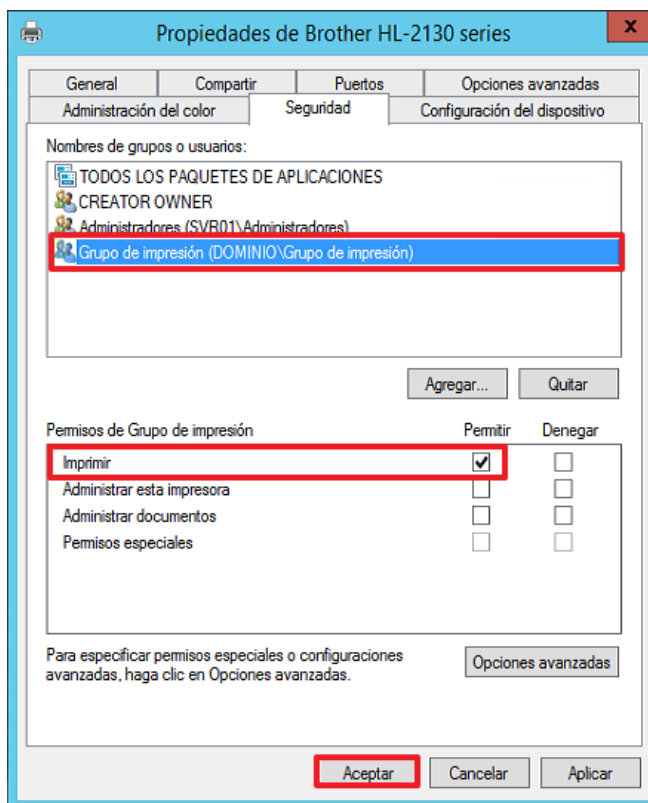
Paso	Descripción
------	-------------

62. Localice el grupo que quiere añadir para que obtenga permisos para imprimir, y pulse sobre “Aceptar”.



Nota: En esta guía se selecciona el grupo de seguridad “Grupo de impresión” al cual pertenecen los usuarios que van a obtener permiso para poder imprimir a través de los dispositivos de impresión seleccionados. Deberá adaptar este paso a los requisitos de su organización.

63. Una vez añadido el grupo de seguridad, localice el grupo y seleccione en los permisos únicamente la opción de “Imprimir”. Pulse “Aceptar” para cerrar la ventana.



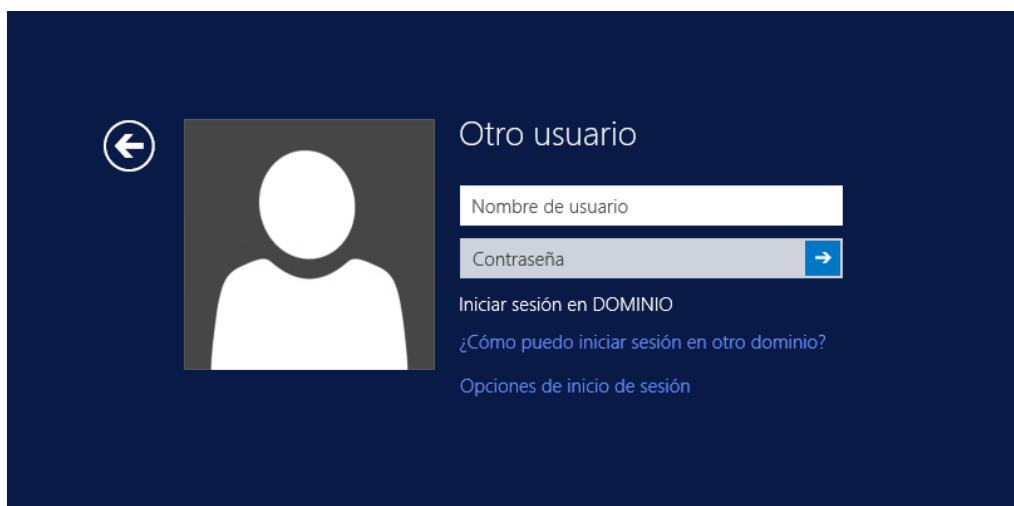
Nota: En este ejemplo se utiliza el grupo denominado “Grupo de impresión”.

64. Debera repetir estos pasos para asignar permisos de impresión sobre todos los dispositivos de impresión que este securizando.

3.3 GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN

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

Paso	Descripción
65.	Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.

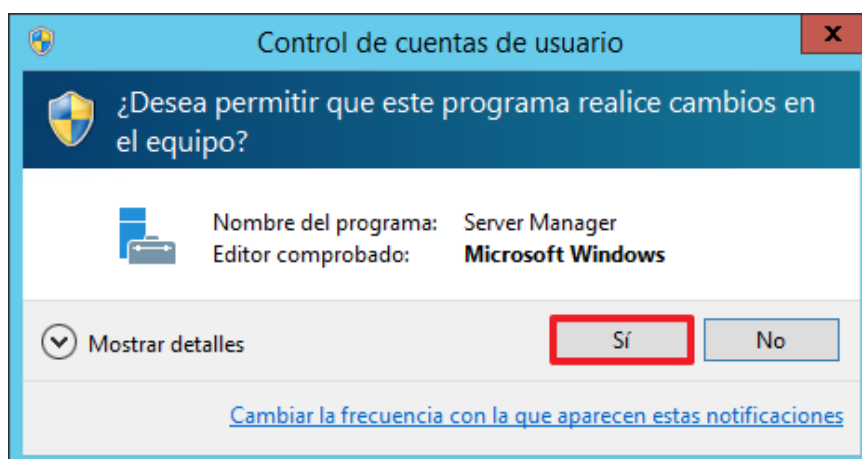


Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

66. A continuación, deberá iniciar la herramienta "Administración de impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.

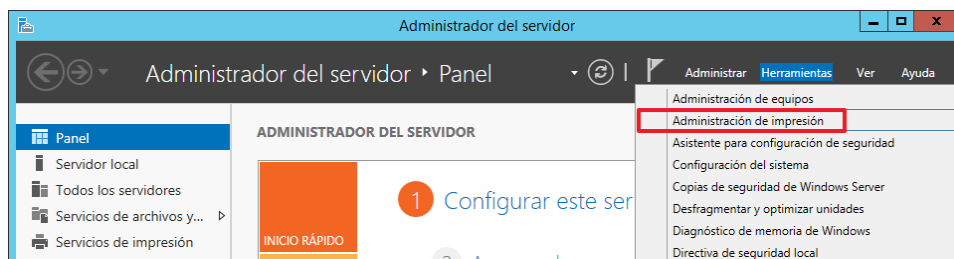


67. El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.

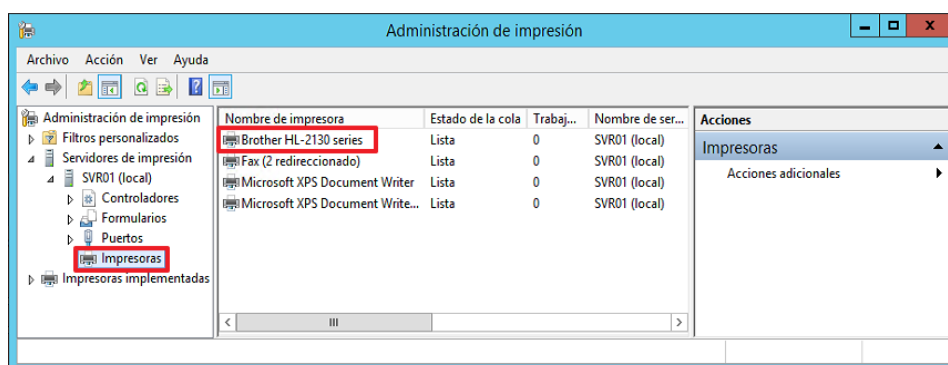


Paso	Descripción
------	-------------

- | | |
|-----|---|
| 68. | <p>Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:</p> <p>“Herramientas → Administración de impresión”</p> |
|-----|---|

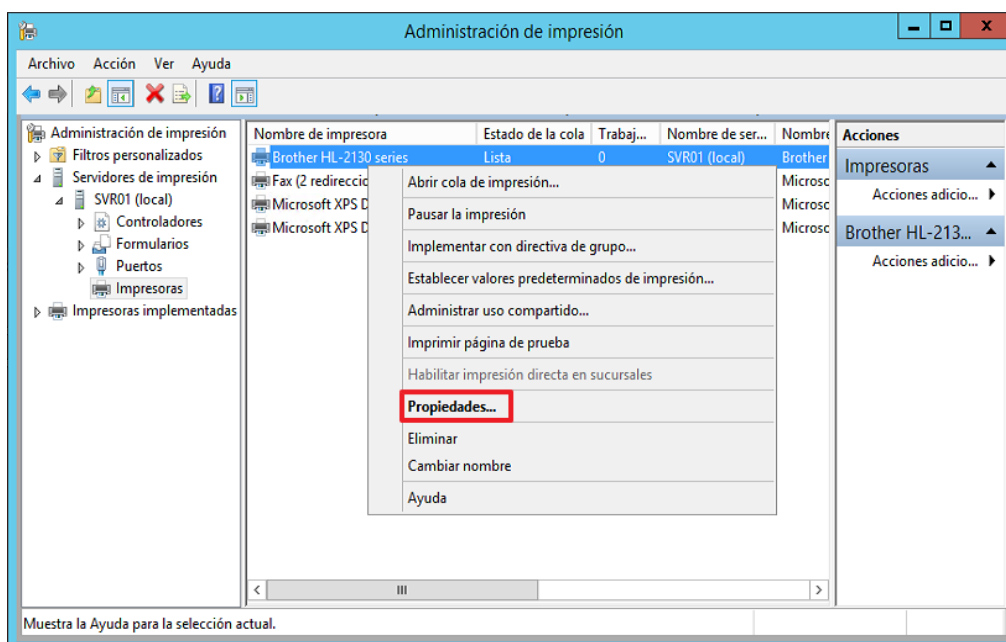


- | | |
|-----|---|
| 69. | <p>Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. Para ello despliegue el nodo “Servidores de impresión / <<nombre del servidor>> / Impresoras”.</p> |
|-----|---|



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

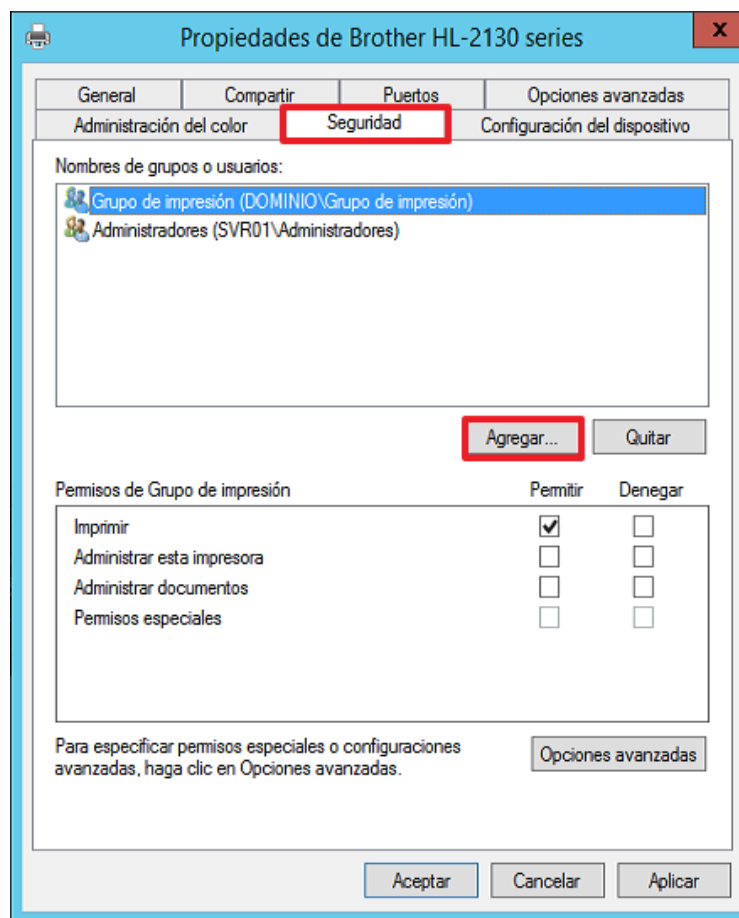
- | | |
|-----|--|
| 70. | <p>Pulse con el botón derecho sobre el dispositivo de impresión y seleccione la opción “Propiedades...”.</p> |
|-----|--|



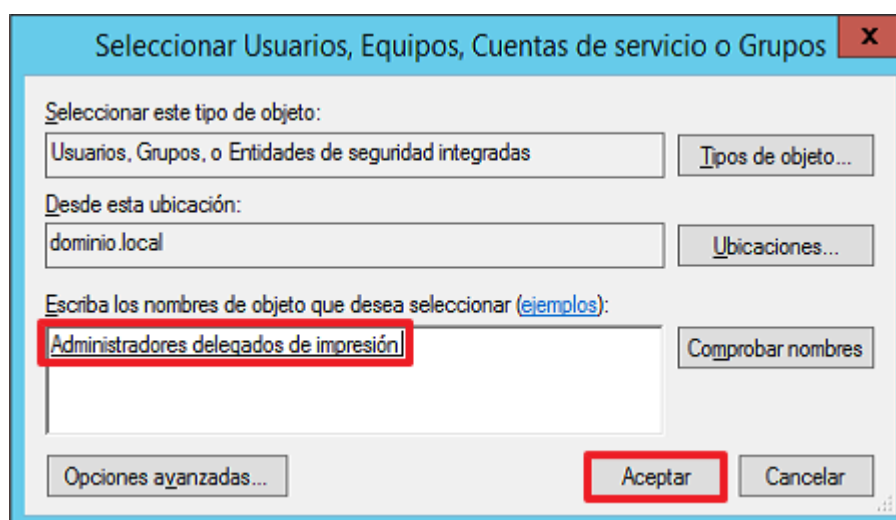
Nota: Para este ejemplo se utiliza el dispositivo denominado “Brother HL-2130 series”.

Paso	Descripción
------	-------------

71. A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Agregar...”.

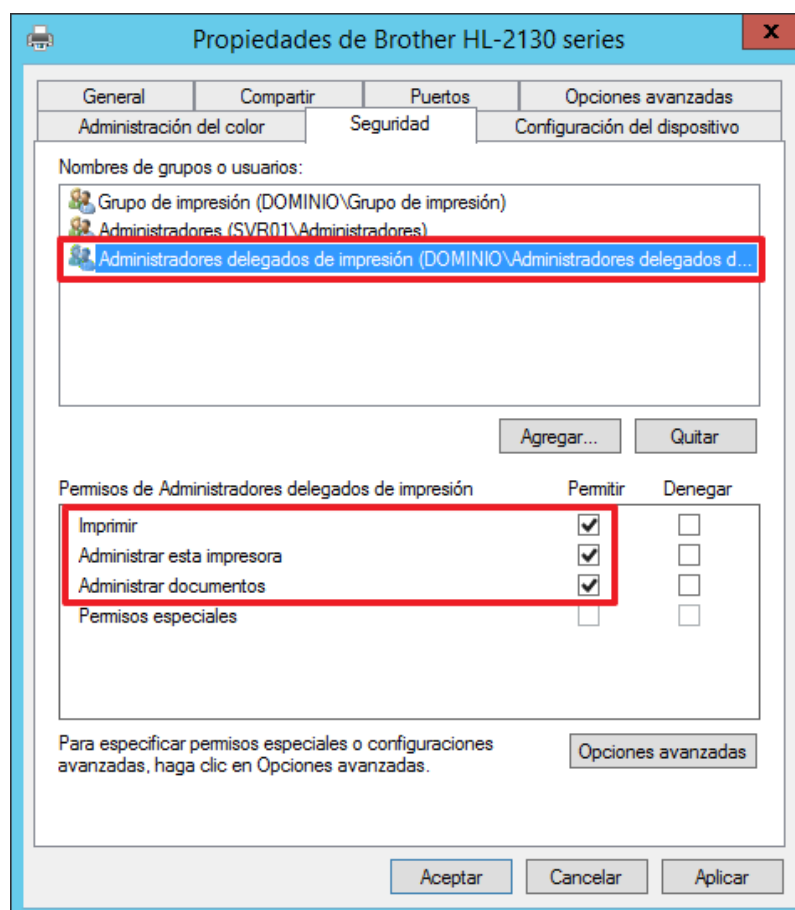


72. Localice el grupo que quiere añadir para que obtenga permisos para poder administrar el dispositivo de impresión seleccionado, y pulse sobre el “Aceptar”.



Nota: En esta guía se selecciona el grupo de seguridad “Administradores delegados de impresión” al cual pertenecen los usuarios que van a obtener permisos administrativos sobre los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.

Paso	Descripción
73.	Una vez añadido el grupo de seguridad “Administradores delegados de impresión”, localice el grupo y seleccione los siguientes permisos: – Imprimir. – Administrar esta impresora. – Administrar documentos.



74. Una vez establecidos los permisos, pulse “Aceptar” para confirmar los cambios y cerrar la ventana de propiedades del dispositivo de impresión.

3.4 GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN

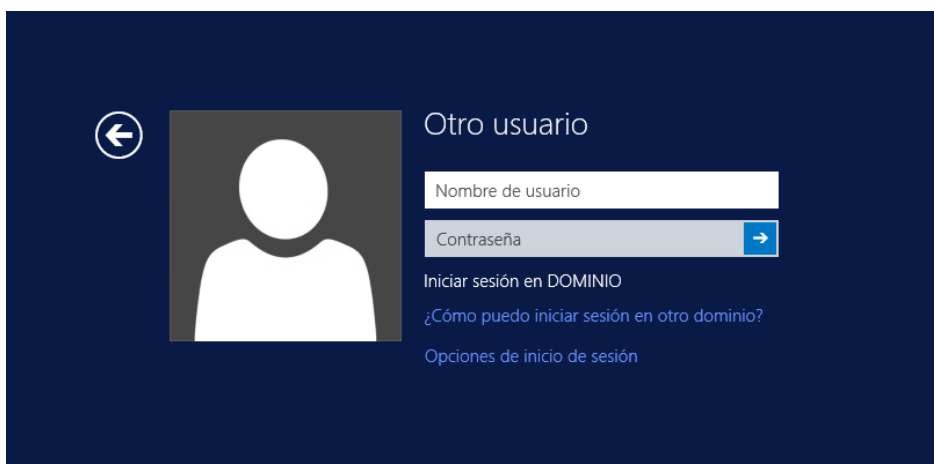
En este apartado se tendrá en consideración la habilitación de la auditoría en los dispositivos de impresión tal y como se especifica para los niveles medio y alto que establece el ENS.

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

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

Paso	Descripción
------	-------------

75. Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.

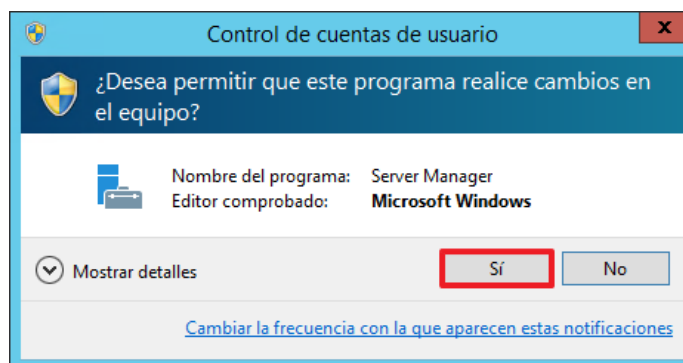


Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

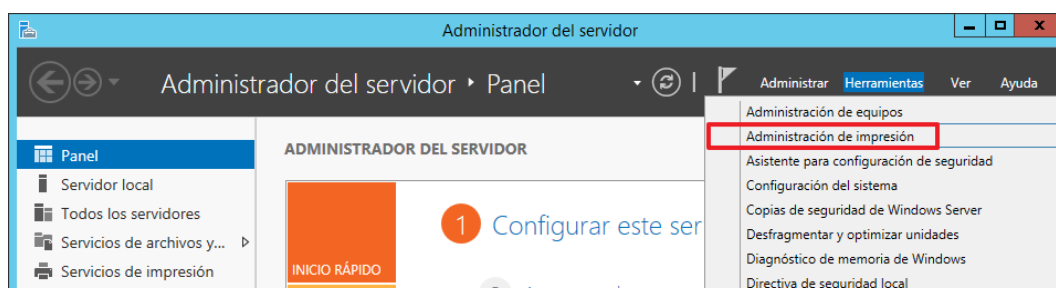
76. A continuación, deberá iniciar la herramienta "Administración de impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.



77. El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.

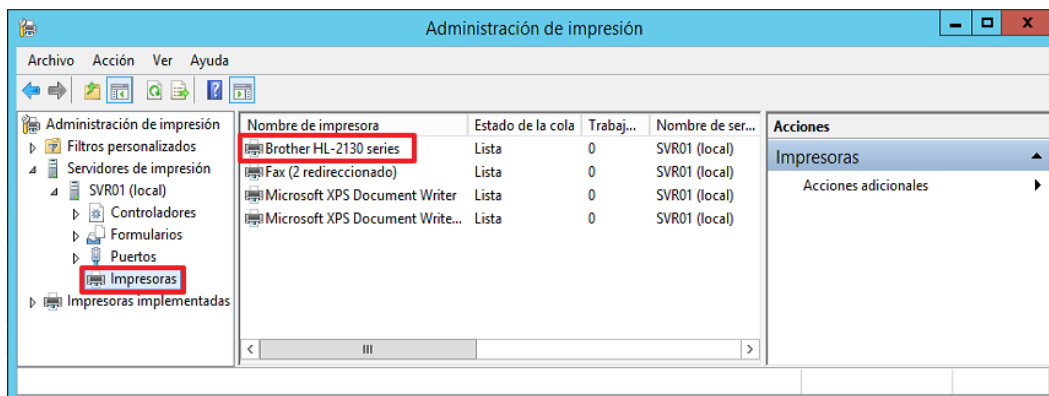


78. Inicie la herramienta "Administración de impresión". Para ello, sobre el menú superior derecho de la herramienta "Administrador del servidor" seleccione:
"Herramientas → Administración de impresión".



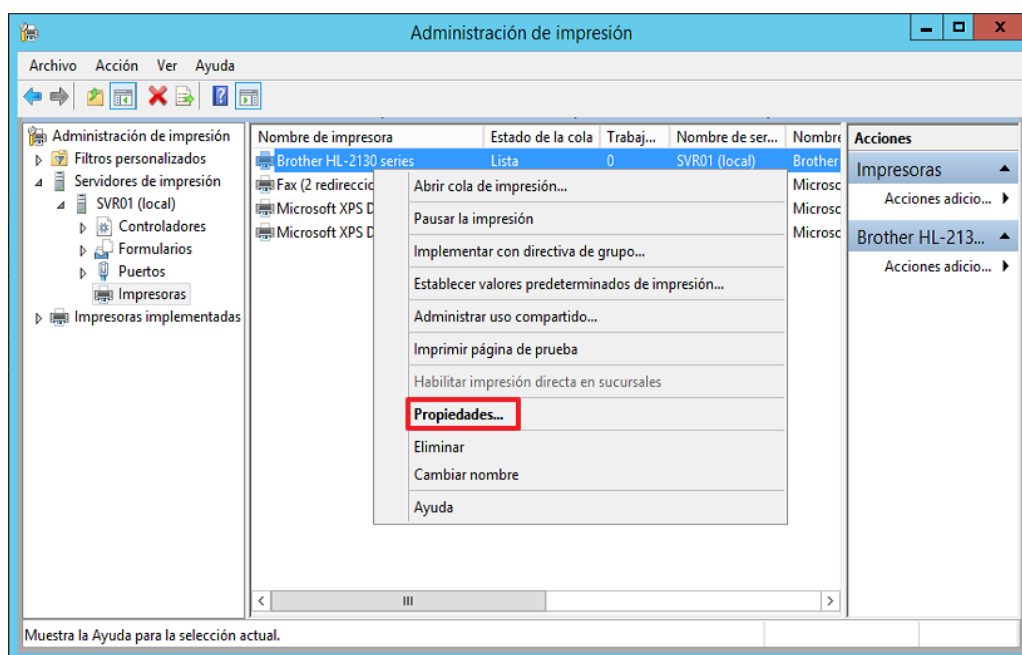
Paso	Descripción
------	-------------

- | | |
|-----|---|
| 79. | Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. |
|-----|---|



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”. Deberá adaptar los pasos a las necesidades de su organización.

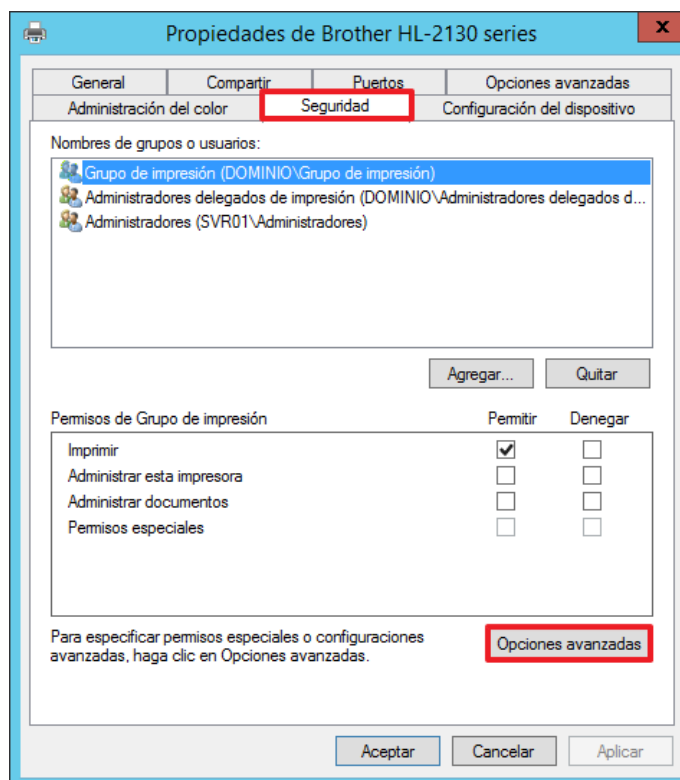
- | | |
|-----|---|
| 80. | Pulse con el botón derecho sobre el dispositivo de impresión y seleccione la opción “Propiedades...”. |
|-----|---|



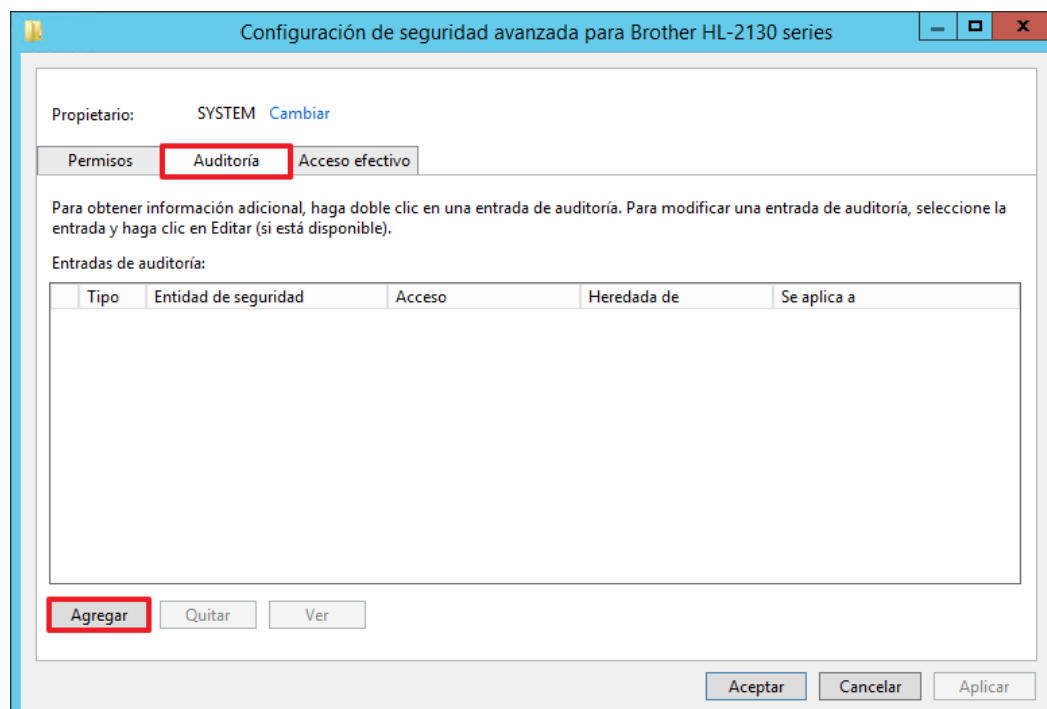
Nota: En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.

Paso	Descripción
------	-------------

81. A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Opciones avanzadas”.

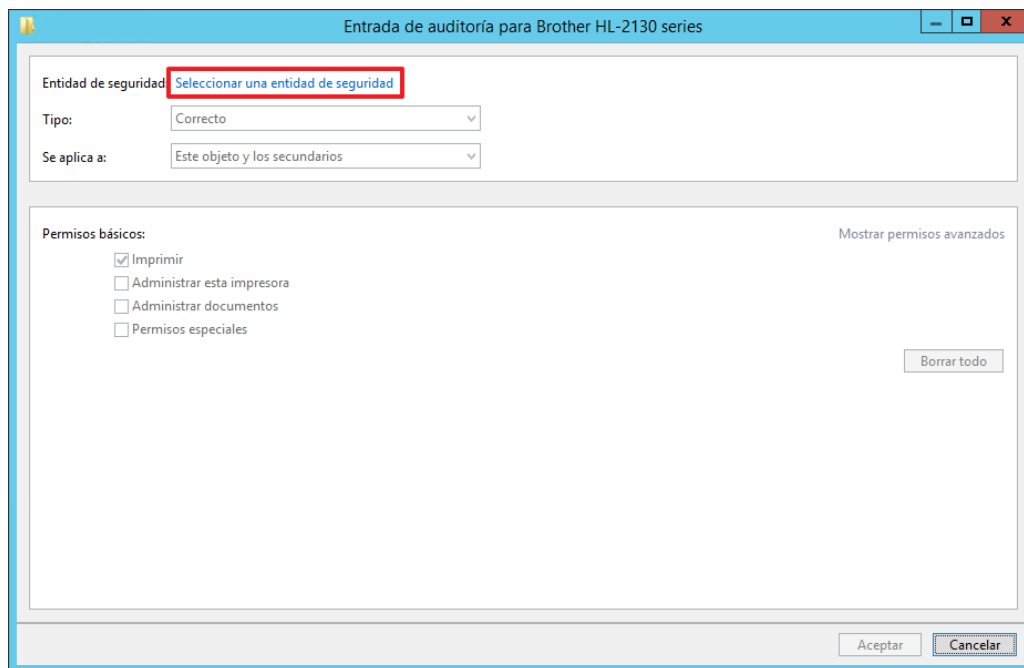


82. Sitúese en la pestaña “Auditoría” y a continuación pulse sobre “Agregar”.

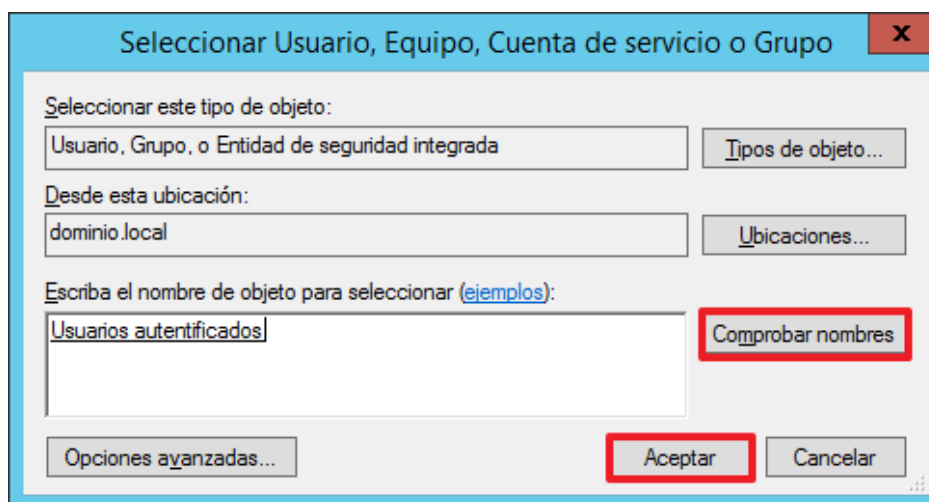


Paso	Descripción
------	-------------

83. Pulse sobre “Seleccionar una entidad de seguridad”.

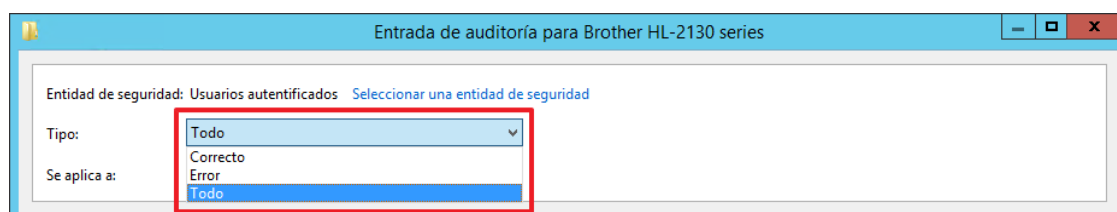


84. Añada los grupos sobre los que desee realizar la auditoría, pulse sobre el botón “Comprobar nombres” y pulse sobre “Aceptar”.



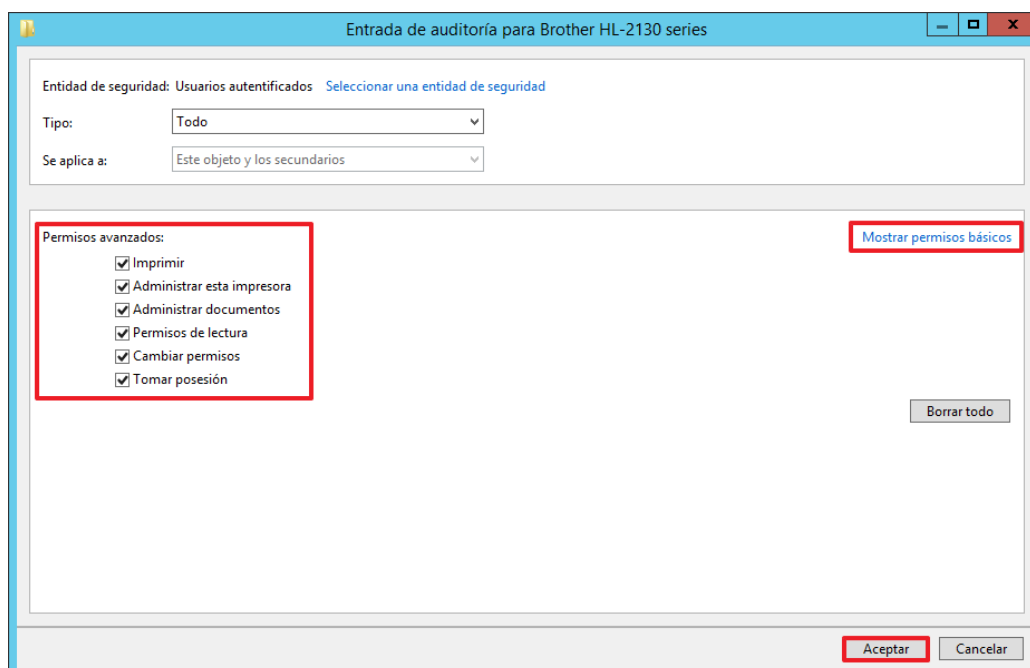
Nota: En este ejemplo se utiliza el grupo “Usuarios autenticados”.

85. En la ventana desplegable “Tipo”, seleccione “Todo”, para que se visualicen tanto los eventos erróneos como los eventos correctos.

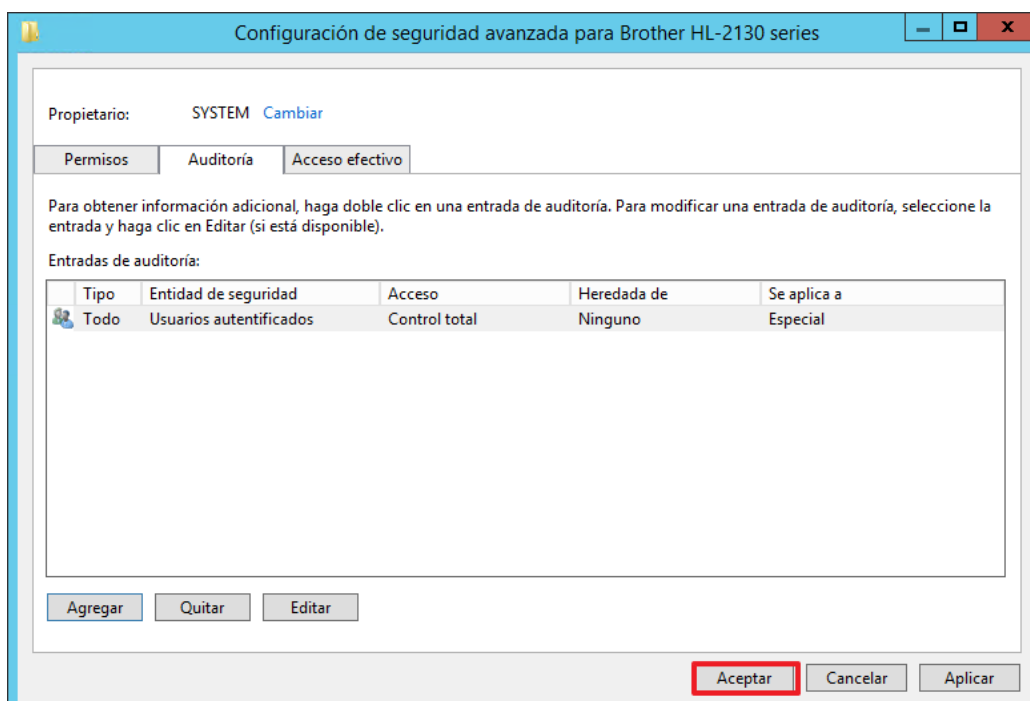


Paso	Descripción
------	-------------

- | | |
|-----|---|
| 86. | En la parte derecha de la ventana, pulse sobre “Mostrar permisos avanzados” y seleccione todas las casillas de eventos auditable, tal y como se muestra en la imagen. Pulse sobre el botón “Aceptar”. |
|-----|---|



- | | |
|-----|---|
| 87. | Pulse de nuevo sobre el botón “Aceptar” para cerrar la configuración de seguridad avanzada de la impresora. |
|-----|---|



- | | |
|-----|--|
| 88. | Finalmente pulse “Aceptar” para cerrar la ventana de “Propiedades” de la impresora. |
| 89. | Repita estos mismos pasos para cada uno de los dispositivos de impresión que deben ser auditados en su organización. |

4. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA

Estos paso a paso se deberán aplicar para instalar o desinstalar roles y/o características implementadas en un servidor miembro del dominio, que le sea de aplicación la guía de securización “CCN-STIC-870A - Implementación del ENS en Windows Server 2012 R2” en su nivel medio o nivel alto del ENS.

Si no desea gestionar los roles y/o características del sistema, no continúe con el paso a paso definido en las siguientes subsecciones.

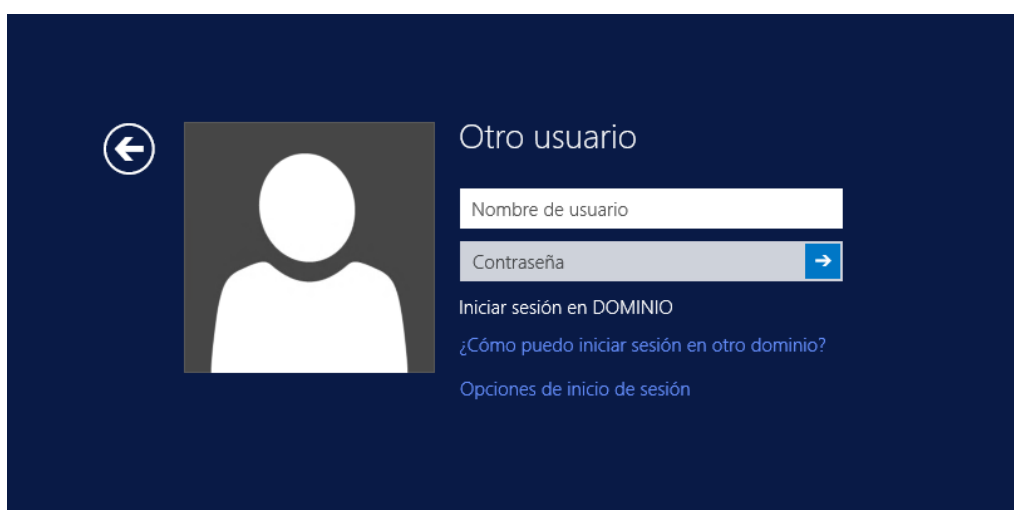
4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO

Para instalar o eliminar un rol y/o característica será necesario la creación de una política de seguridad temporal para tal efecto.

Los pasos que se describen a continuación se realizarán en un Controlador de Dominio del directorio activo al que va a pertenecer el servidor miembro que se está securizando.

Nota: Recuerde que una vez instalados o eliminados los roles y/o características necesarias deberá aplicar el paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

Paso	Descripción
90.	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.

91. 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.

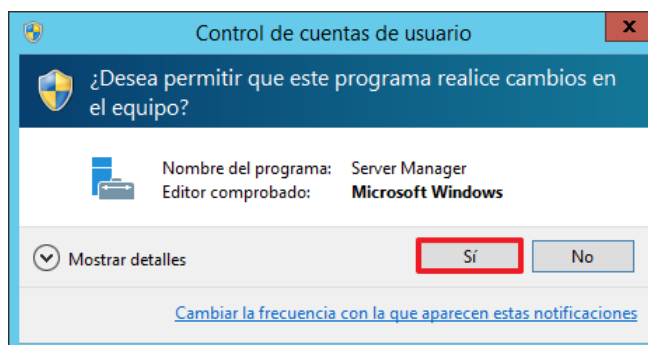
92. Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

93. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



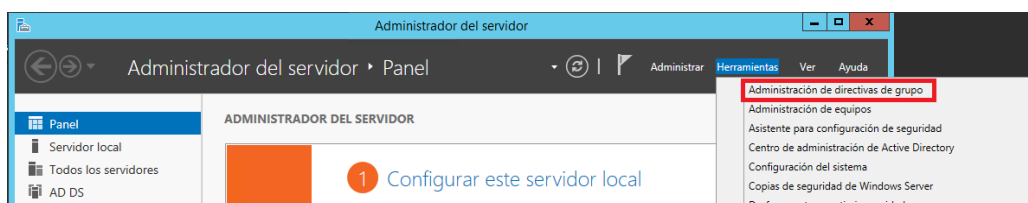
Paso	Descripción
------	-------------

94. El "Control de cuentas de usuario" le solicitará la elevación de privilegios. Pulse "Sí" para continuar.

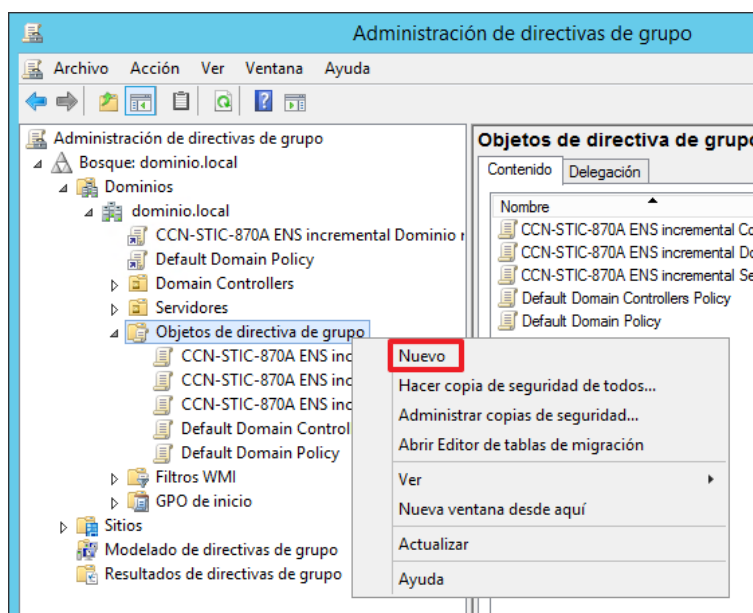


Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios podrá solicitar credenciales para continuar.

95. Inicie la herramienta "Administración 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"

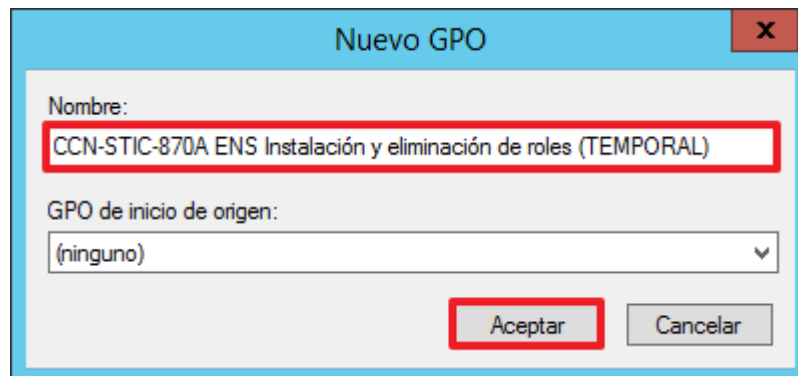


96. Ubíquese sobre el nodo "Objetos de directiva de grupo" ubicado en "Bosque:<su dominio> / Dominios / <su dominio> / Objetos de directiva de grupo".
97. Si ya estuviese creada la directiva de grupo "CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)" deberá continuar a partir del paso 108.
98. Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción "Nuevo".

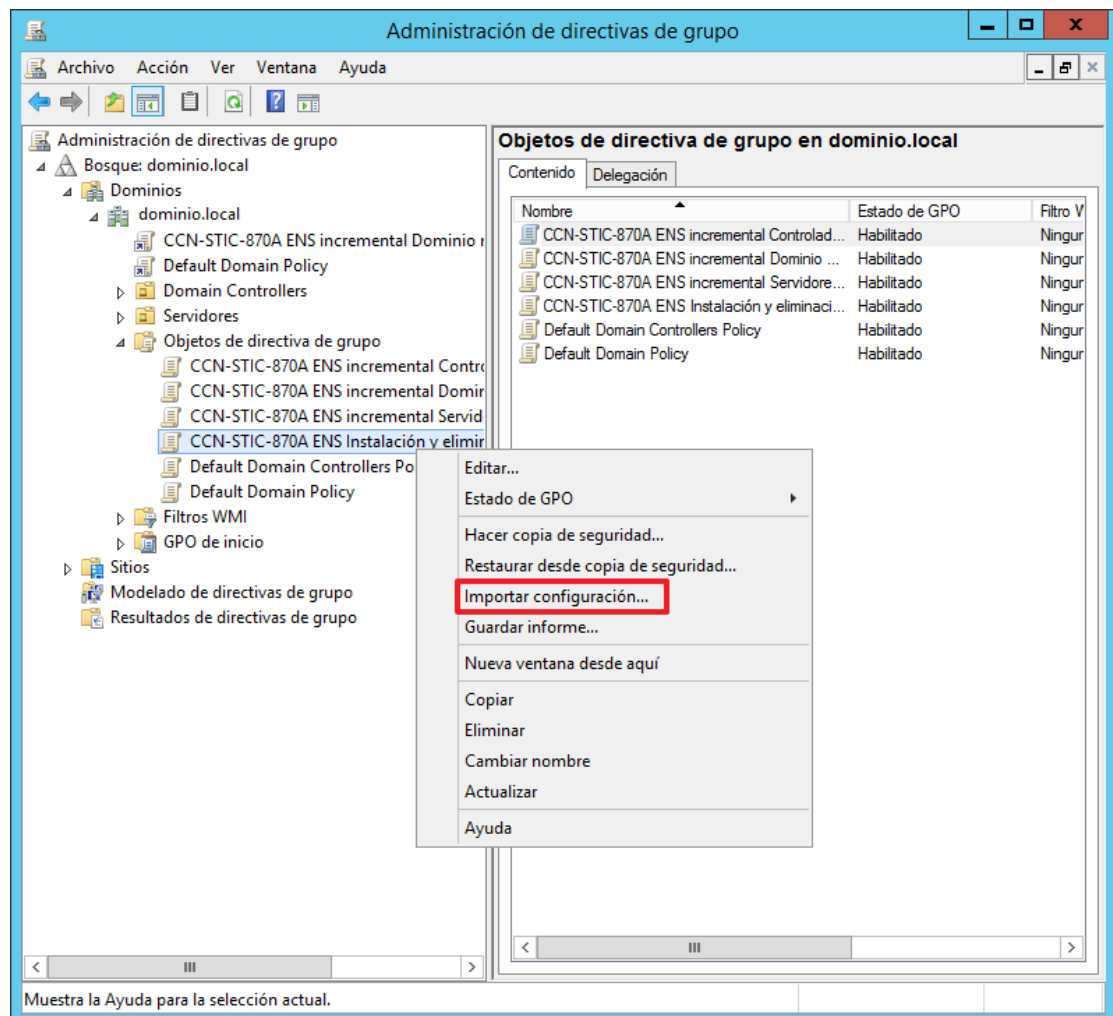


Paso	Descripción
------	-------------

99. Introduzca como nombre “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Aceptar”.



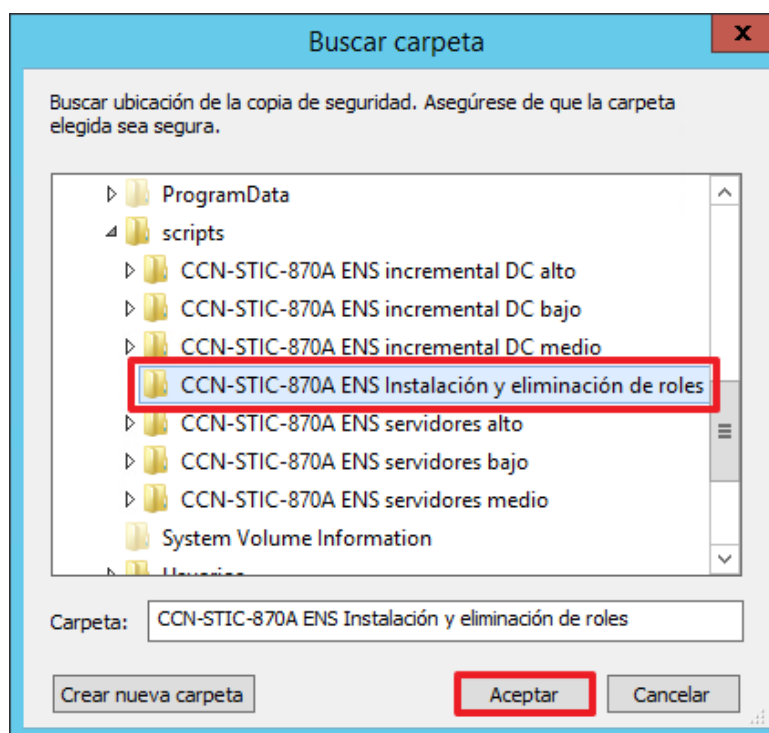
100. Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración...”.



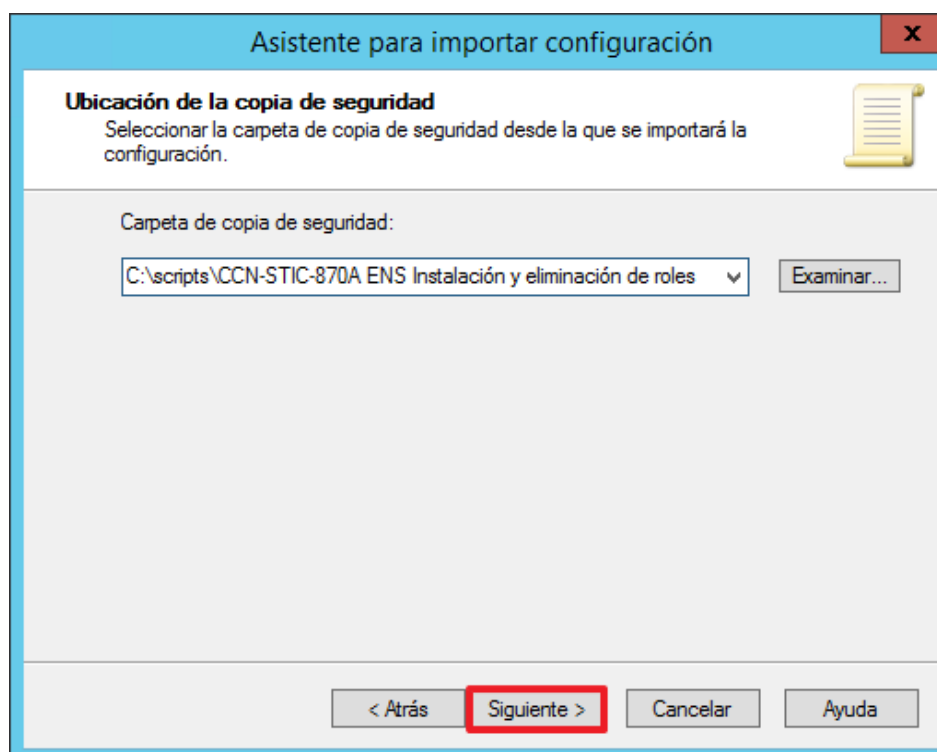
101. En el asistente de importación de configuración, pulse el botón “Siguiente >”.

102. En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.

Paso	Descripción
103.	Seleccione la carpeta "CCN-STIC-870A ENS Instalación y eliminación de roles" que encontrará en la carpeta "C:\Scripts" y pulse el botón "Aceptar".

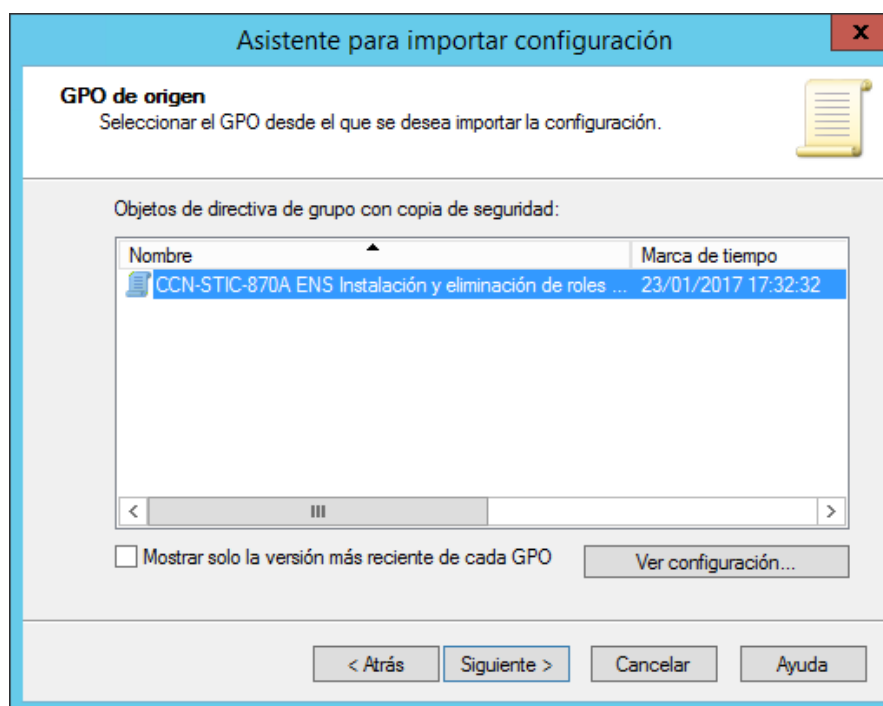


104. Pulse el botón "Siguiente >" una vez seleccionada la carpeta adecuada.

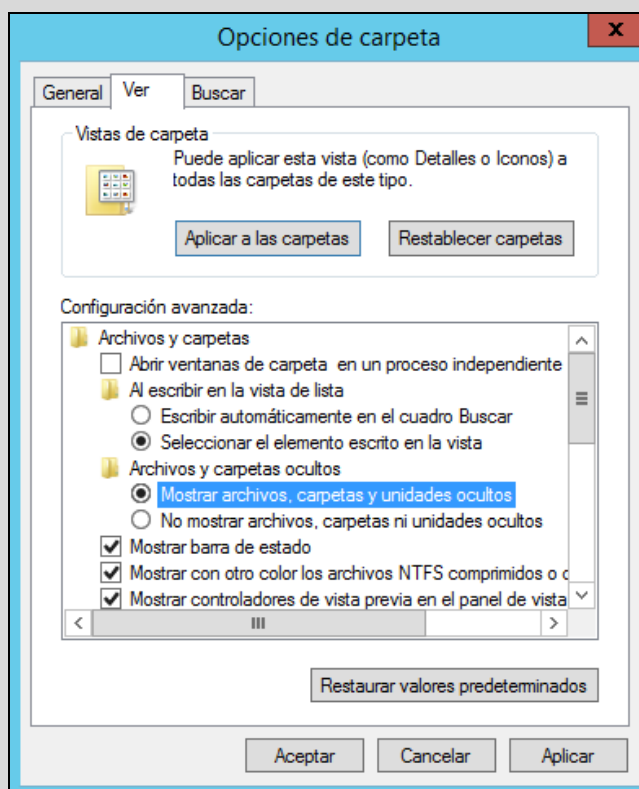


Paso	Descripción
------	-------------

105. En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” 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 mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”.



Paso	Descripción
106.	En la pantalla de examen, pulse el botón “Siguiente >”.
107.	Para completar el asistente pulse el botón “Finalizar”.
108.	A continuación, seleccione la nueva política de grupo configurada y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho.

CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)

Ámbito Detalles Configuración Delegación Estado

Vinculos

Mostrar vínculos en esta ubicación: dominio2.local

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado	Ruta

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
Usuarios autenticados

Agregar... Quitar Propiedades

Filtrado WMI

Este GPO está vinculado al siguiente filtro WMI:

<ninguno> Abrir

109. En la opción de filtrado de seguridad, seleccione “Usuarios autenticados” y pulse la opción “Quitar”.

Filtrado de seguridad

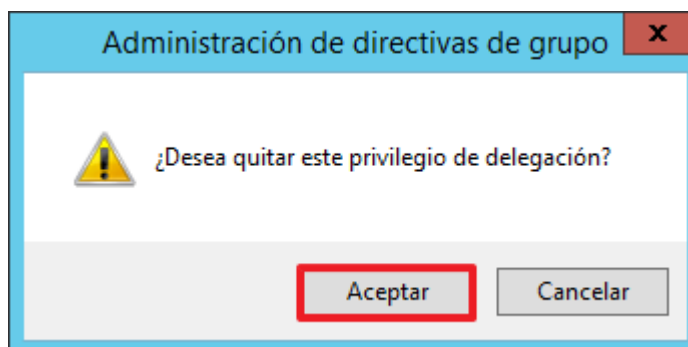
La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
Usuarios autenticados

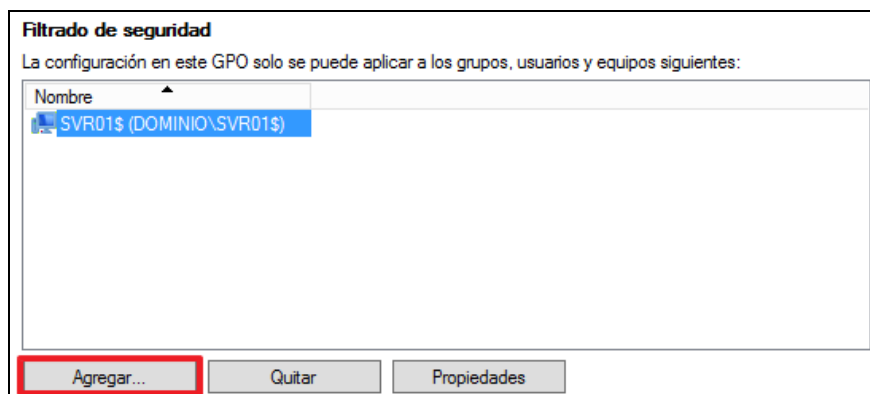
Agregar... Quitar Propiedades

Paso	Descripción
------	-------------

110. A continuación, pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.

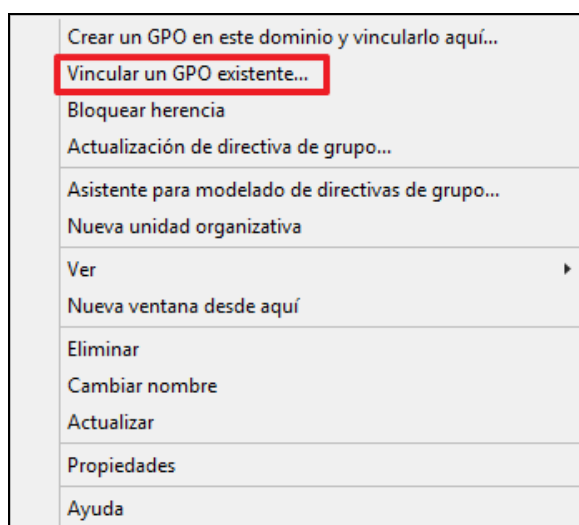


111. Una vez quitado, pulse el botón “Agregar...” y seleccione únicamente los equipos o grupos sobre los que desea aplicar la política de seguridad.



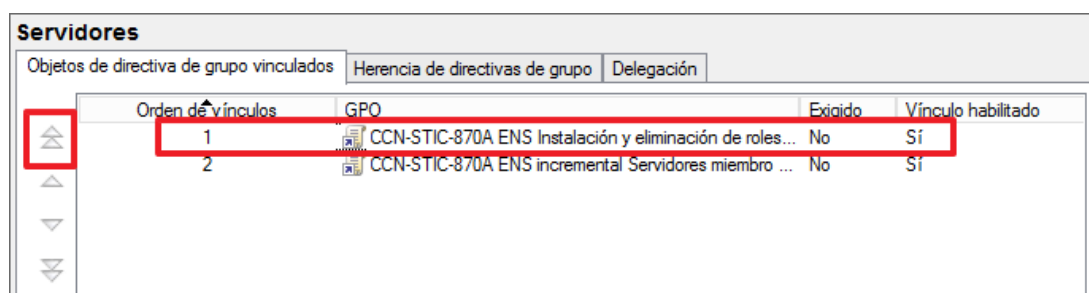
Nota: En este ejemplo se agrega el equipo “SVR01”.

112. A continuación, identifique las unidades organizativas en la que desea instalar o eliminar algún rol y/o característica. Pulse con el botón derecho sobre la unidad organizativa deseada y seleccione la opción del menú contextual “Vincular un GPO existente...”.



Nota: En este ejemplo se selecciona la unidad organizativa “Servidores”.

Paso	Descripción
113.	Una vez vinculado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 870A ENS Instalación y eliminación de roles”
114.	Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 870A ENS Instalación y eliminación de roles” en primer lugar dentro del orden de vinculación.

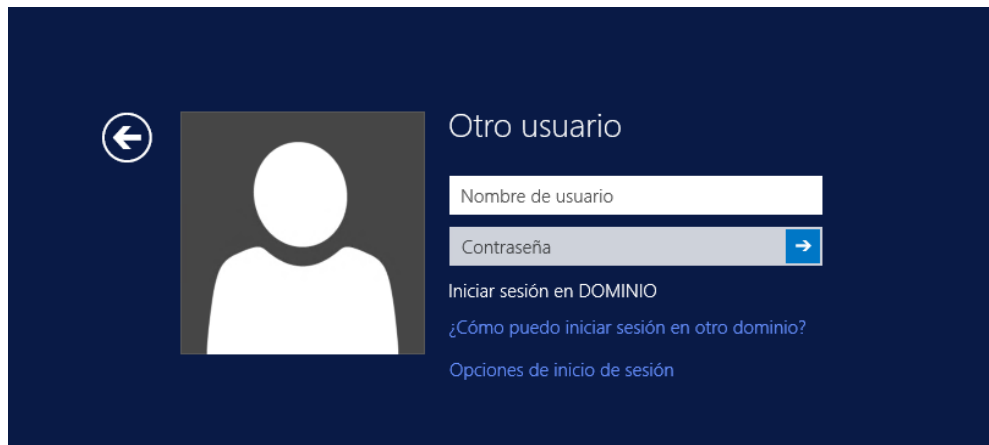


4.2 INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO”.

Paso	Descripción
115.	Inicie sesión en el servidor miembro donde vaya a instalar un rol y/o característica.



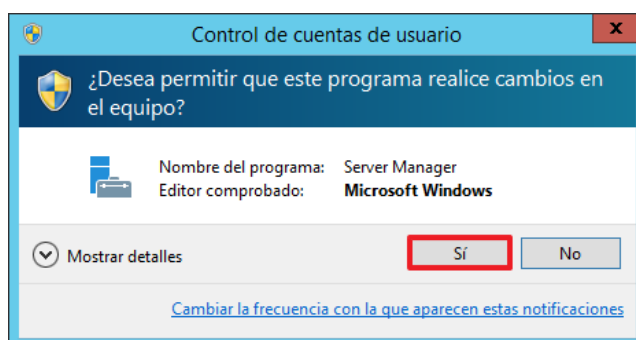
Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

116. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



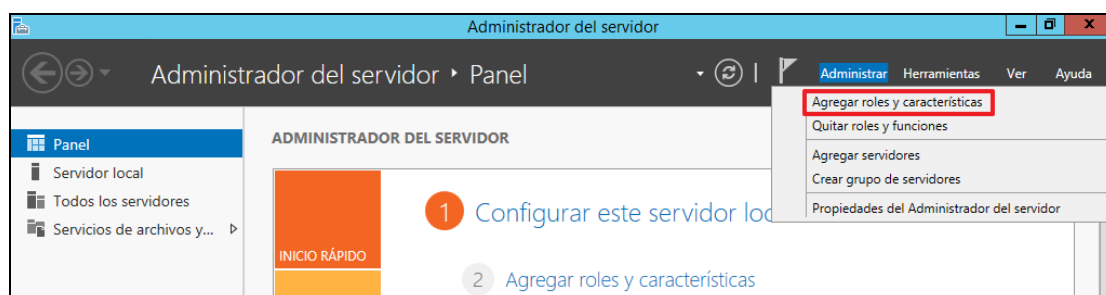
Paso	Descripción
------	-------------

117. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.

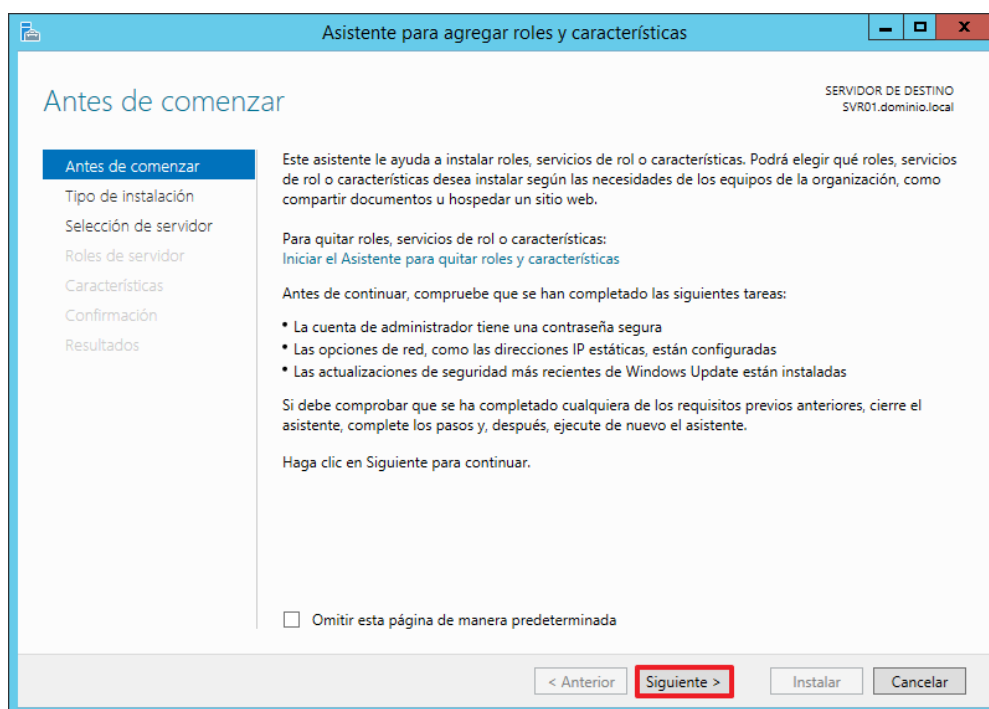


Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios podrá solicitar credenciales para continuar.

118. A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Agregar roles y características”.

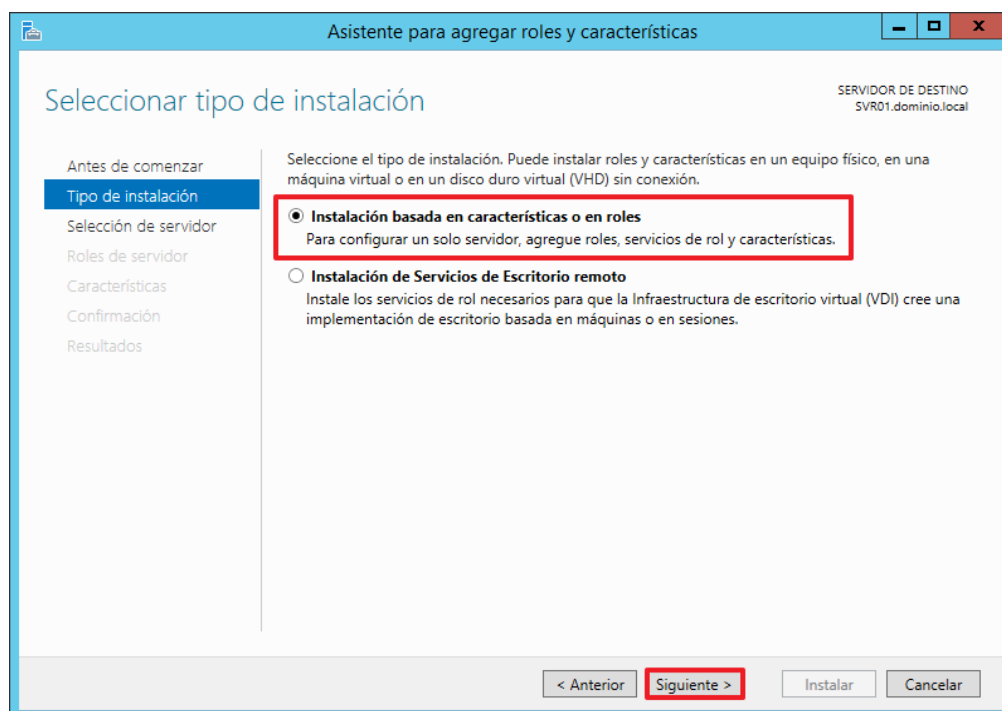


119. Comenzará el asistente para agregar roles y características. Pulse sobre el botón “Siguiente >” para continuar.

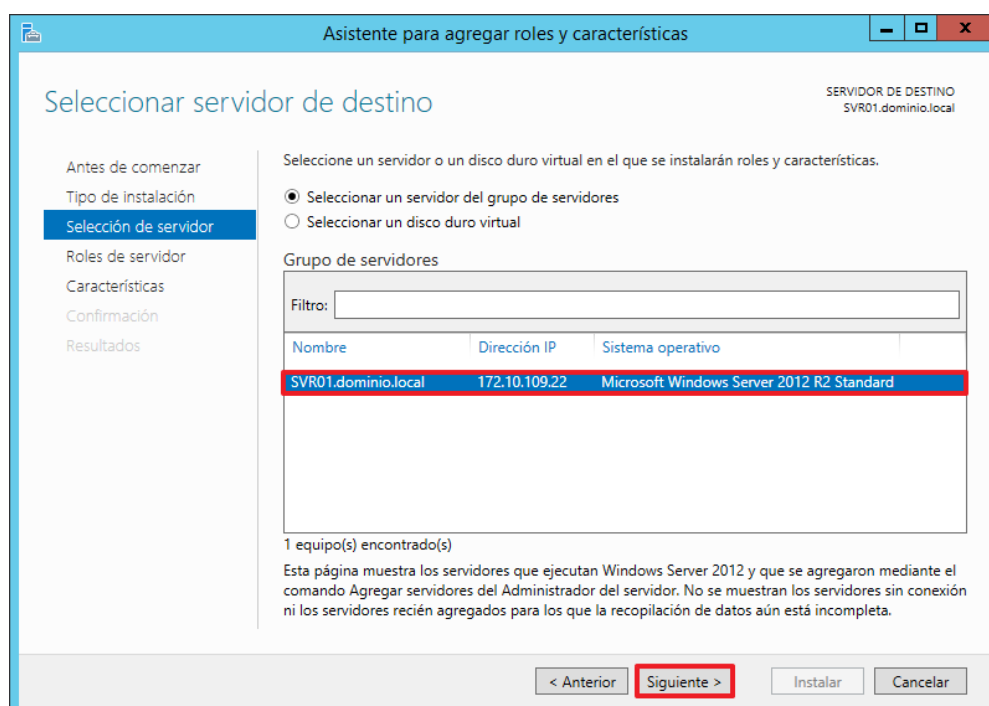


Paso Descripción

120. Seleccione el tipo de instalación, “Instalación basada en características o roles” y pulse “Siguiente ->” para continuar.



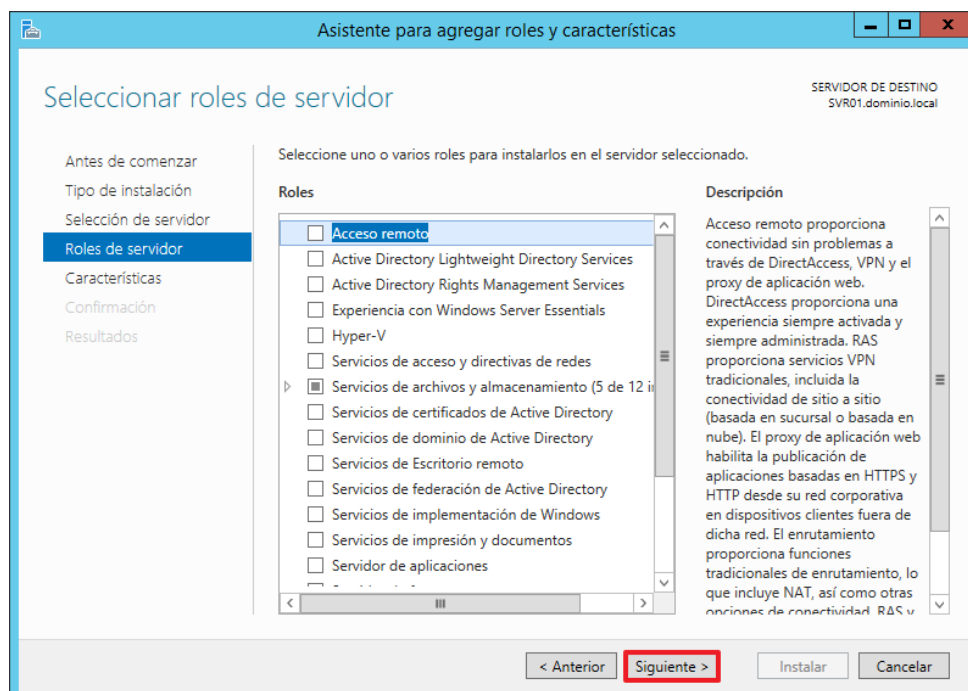
121. Seleccione el servidor sobre el cual desea instalar un rol o una característica, y pulse “Siguiente >”.



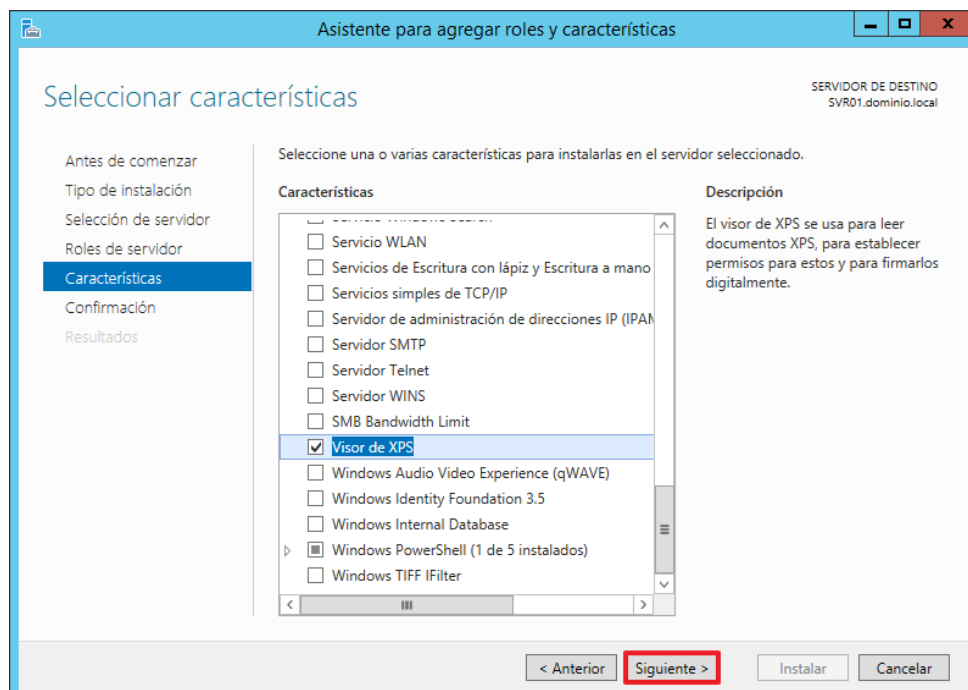
Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

Paso	Descripción
------	-------------

- | | |
|------|---|
| 122. | En la siguiente ventana, seleccione los roles que desee instalar en el sistema y pulse “Siguiente >”. |
|------|---|



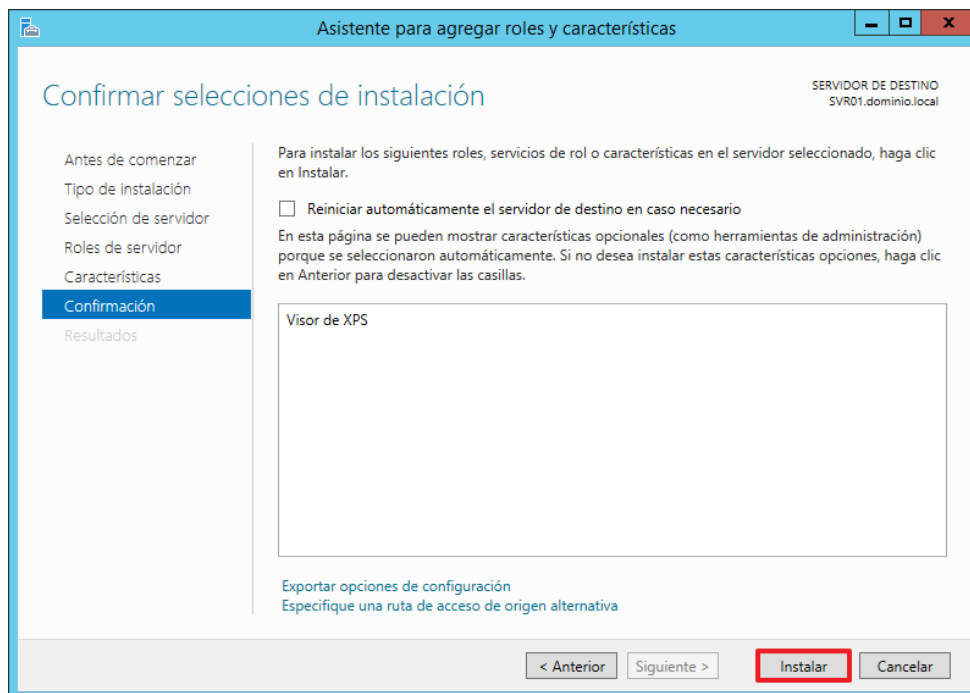
- | | |
|------|--|
| 123. | A continuación, en la siguiente ventana podrá seleccionar las características que desee instalar en el sistema. Seleccione aquellas que desee instalar y pulse “Siguiente ->”. |
|------|--|



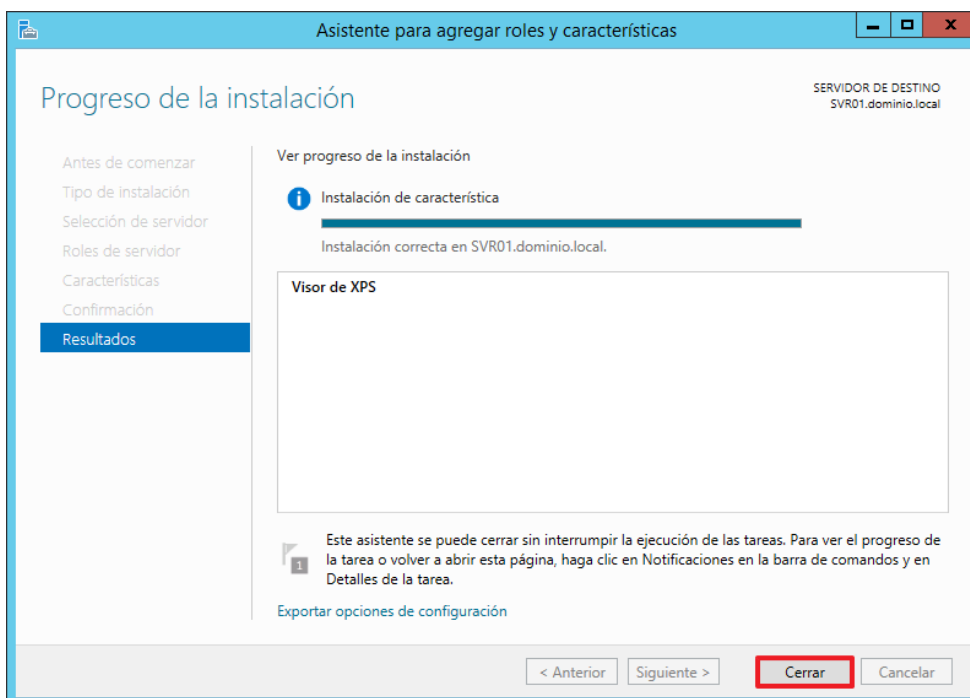
Nota: En este ejemplo se instala la característica “Visor de XPS”, deberá adaptar este paso a los requerimientos de su organización.

Paso	Descripción
------	-------------

124. En la ventana “Confirmación” pulse “Instalar” para iniciar el proceso.



125. Una vez finalizado el proceso de instalación, pulse sobre “Cerrar” para finalizar la instalación.



Nota: En caso de ser necesario, el servidor requerirá un reinicio para finalizar la instalación de roles y características.

126. Una vez finalizada la instalación de roles y/o características, deberá aplicar el siguiente paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

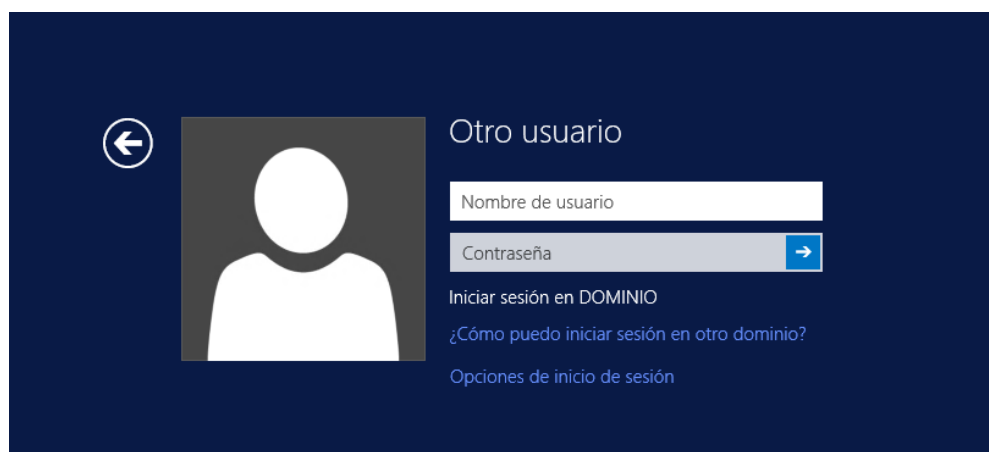
4.3 DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO”.

Paso	Descripción
------	-------------

127. Inicie sesión en el servidor miembro donde vaya a eliminar un rol y/o característica.

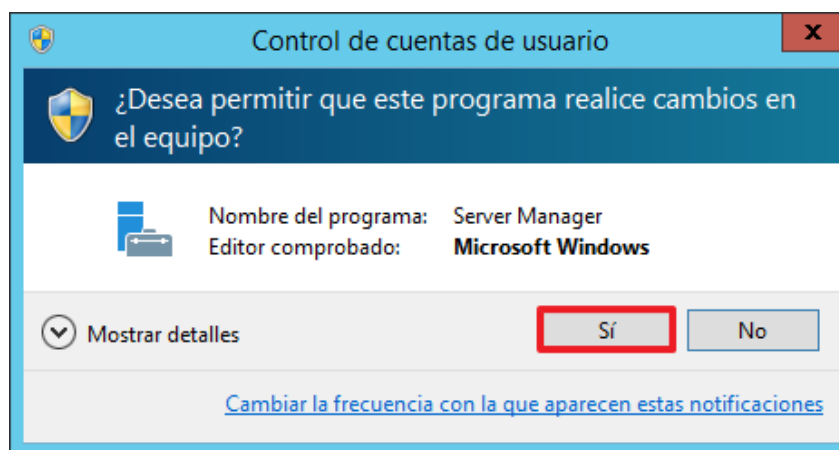


Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

128. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



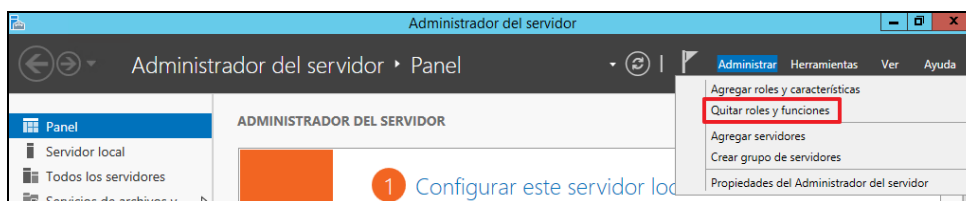
129. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



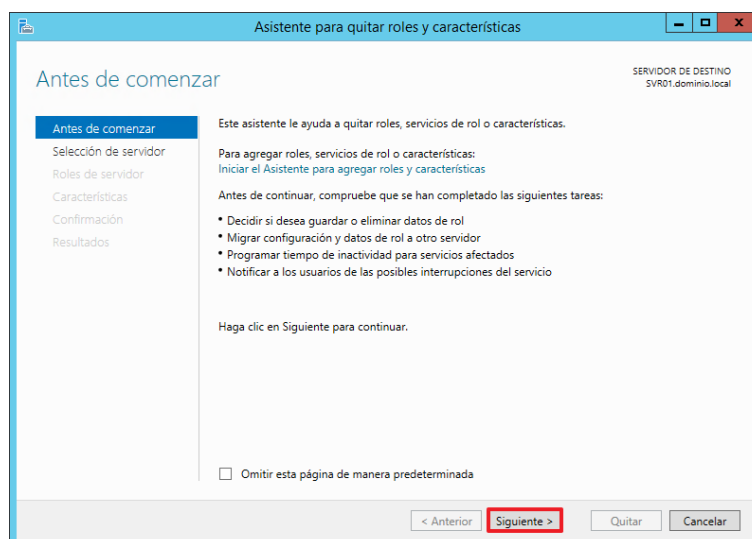
Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios le podrá solicitar credenciales para continuar.

Paso	Descripción
------	-------------

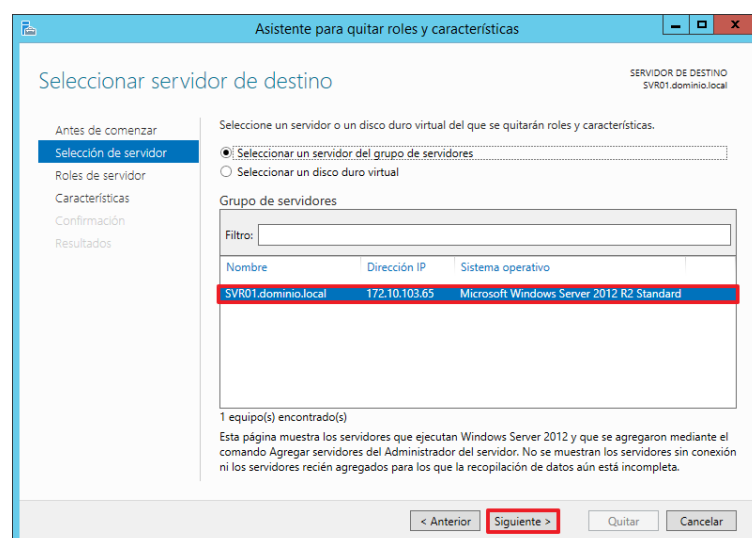
130. A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.



131. Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar.



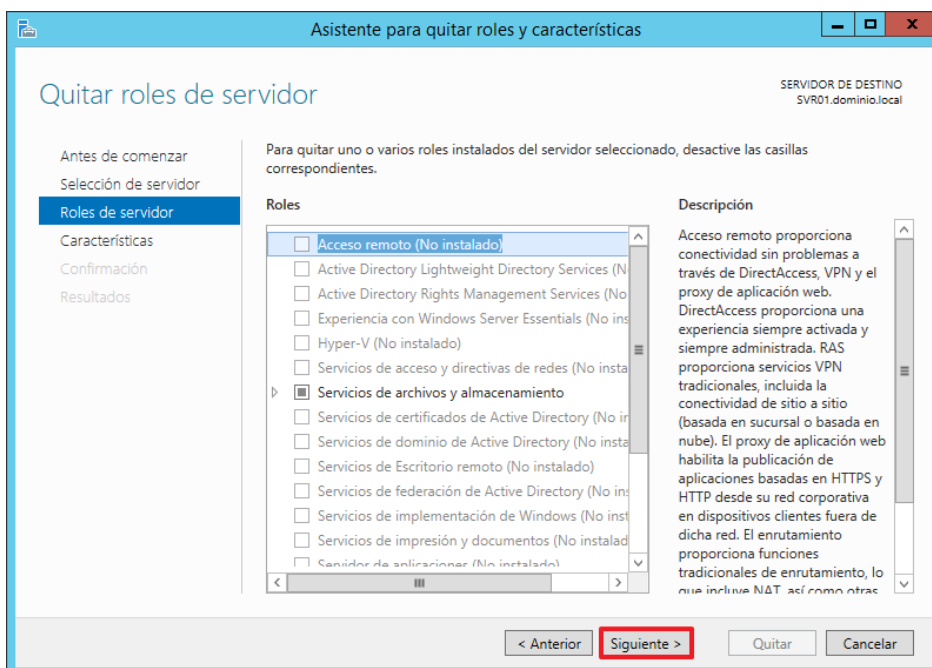
132. Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”.



Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

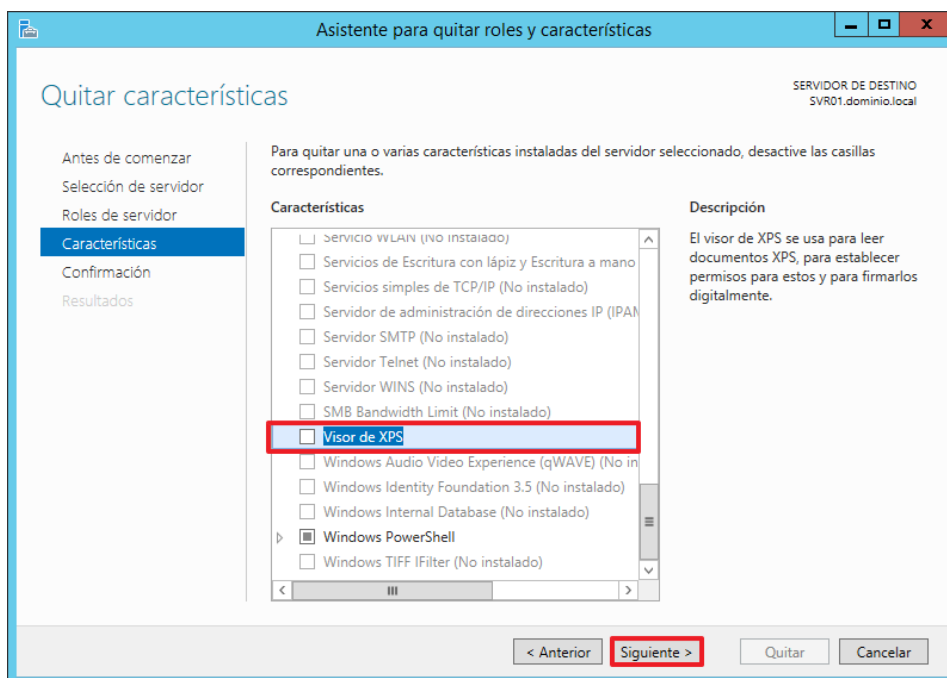
Paso	Descripción
------	-------------

- | | |
|------|--|
| 133. | En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”. |
|------|--|



Nota: En este ejemplo no se desinstala ningún rol, deberá adaptar este paso a los requerimientos de su organización.

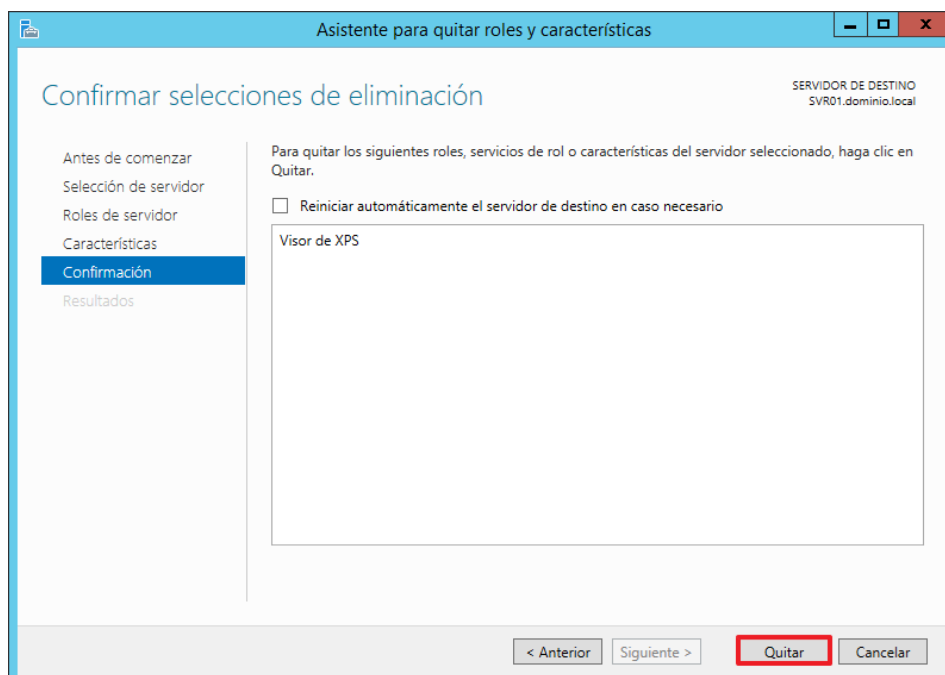
- | | |
|------|---|
| 134. | A continuación, en la siguiente ventana podrá seleccionar las características que desee desinstalar del sistema. Desmarque aquellas que desee desinstalar y pulse “Siguiente ->”. |
|------|---|



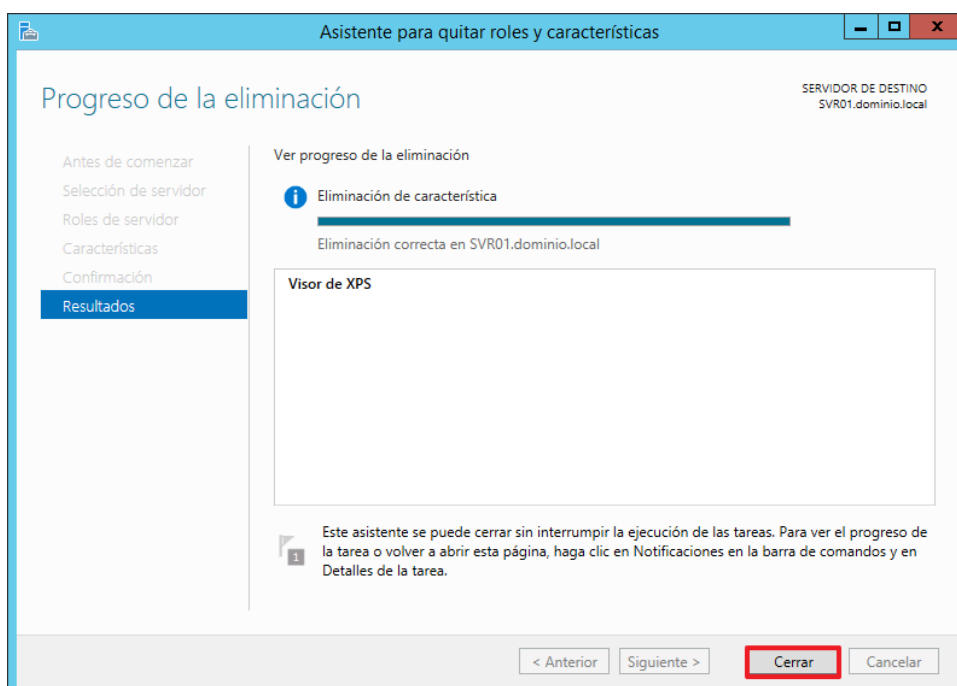
Nota: En este ejemplo se desinstala la característica “Visor de XPS”, deberá adaptar este paso a los requerimientos de su organización.

Paso	Descripción
------	-------------

135. En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.



136. Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar la desinstalación.



Nota: En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.

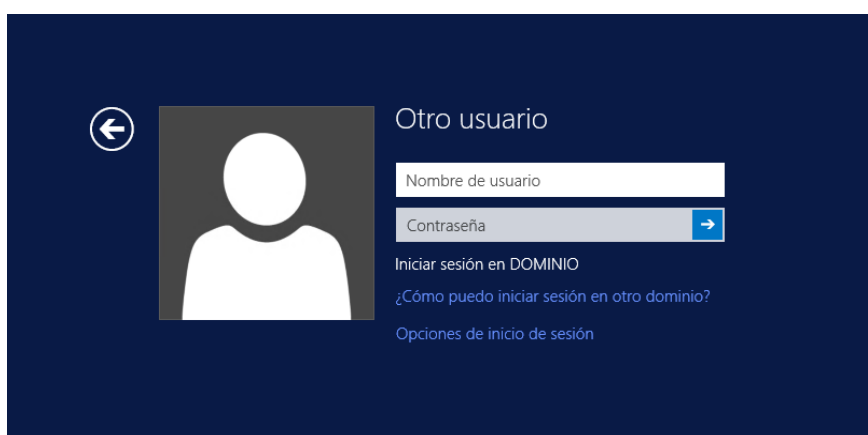
137. Una vez finalizada la desinstalación de roles y/o características, deberá aplicar el siguiente paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO

Para desvincular o eliminar la GPO “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” creada en el paso “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” deberá implementar el siguiente paso a paso.

Los pasos que se describen a continuación se realizarán en un Controlador de Dominio del dominio al que va a pertenecer el servidor miembro que se está securizando.

Paso	Descripción
138.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.

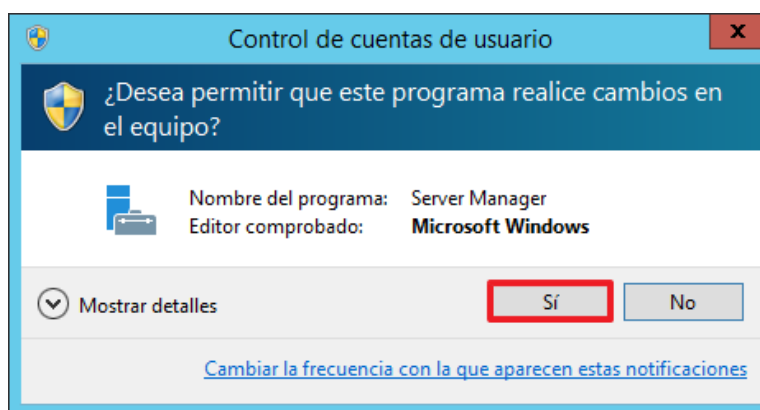


Nota: Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.

139. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



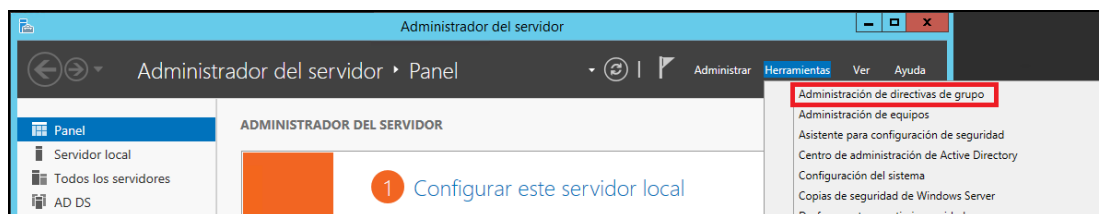
140. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



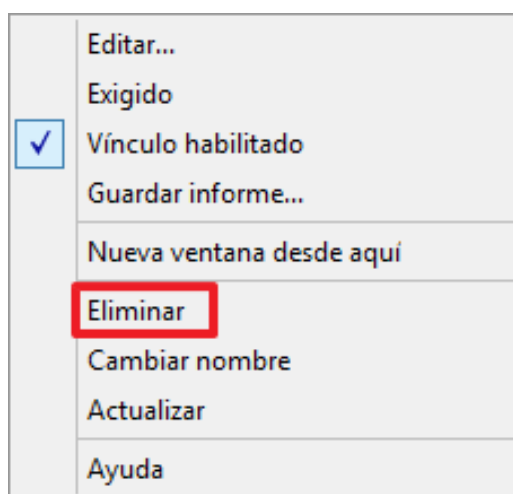
Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios podrá solicitar credenciales para continuar.

Paso	Descripción
------	-------------

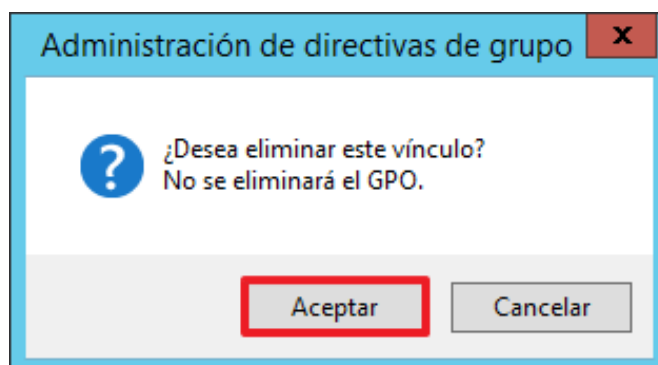
141. Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de directivas de grupo”



142. Localice la unidad organizativa donde se está aplicando la GPO “CCN-STIC-870A ENS Instalación o eliminación de roles (TEMPORAL)”.
143. Pulse botón derecho sobre la GPO y seleccione la opción del menú contextual “Eliminar”.



144. Pulse “Aceptar” ante el mensaje emergente “¿Desea eliminar este vínculo? No se eliminará el GPO.”



Paso	Descripción
------	-------------

145. A continuación, seleccione la política de grupo “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” ubicada en el contenedor “Objetos de directiva de grupo” y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho.

CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)

Ámbito Detalles Configuración Delegación Estado

Vínculos

Mostrar vínculos en esta ubicación: dominio.local

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado	Ruta
III			

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
SVR01\$ (DOMINIO\SVR01\$)

Agregar... Quitar Propiedades

Filtrado WMI

Este GPO está vinculado al siguiente filtro WMI:

<ninguno> Abrir

146. En la opción “Filtrado de seguridad”, Seleccione los equipos o grupos sobre los que se está aplicando la política de seguridad y pulse sobre el botón “Quitar”.

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos siguientes:

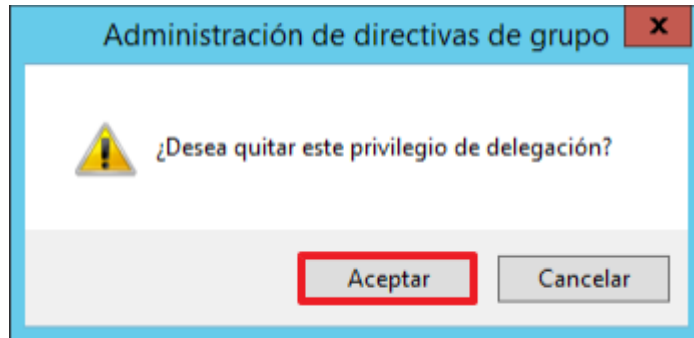
Nombre
SVR01\$ (DOMINIO\SVR01\$)

Agregar... **Quitar** Propiedades

Nota: En este ejemplo se elimina el equipo “SVR01”

Paso	Descripción
------	-------------

147. Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.



ANEXO F. IMPLEMENTACIÓN DE SEGURIDAD PASO A PASO PARA SERVIDORES DE IMPRESIÓN QUE LES SEAN 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 empleen servidores de impresión con una categorización de seguridad alta 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, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

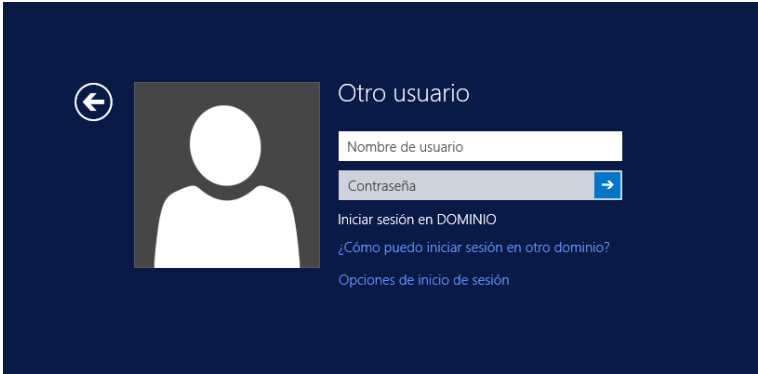
Nota: Si instala el Servidor de impresión por primera vez con la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2 aplicada debe habilitar la instalación remota de roles. Para ello consulte el punto 4 GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA.

1. INSTALACIÓN DEL ROL SERVIDOR DE IMPRESIÓN

Este procedimiento está diseñado para ayudar a los operarios a realizar una instalación básica del rol Servidor de impresión.

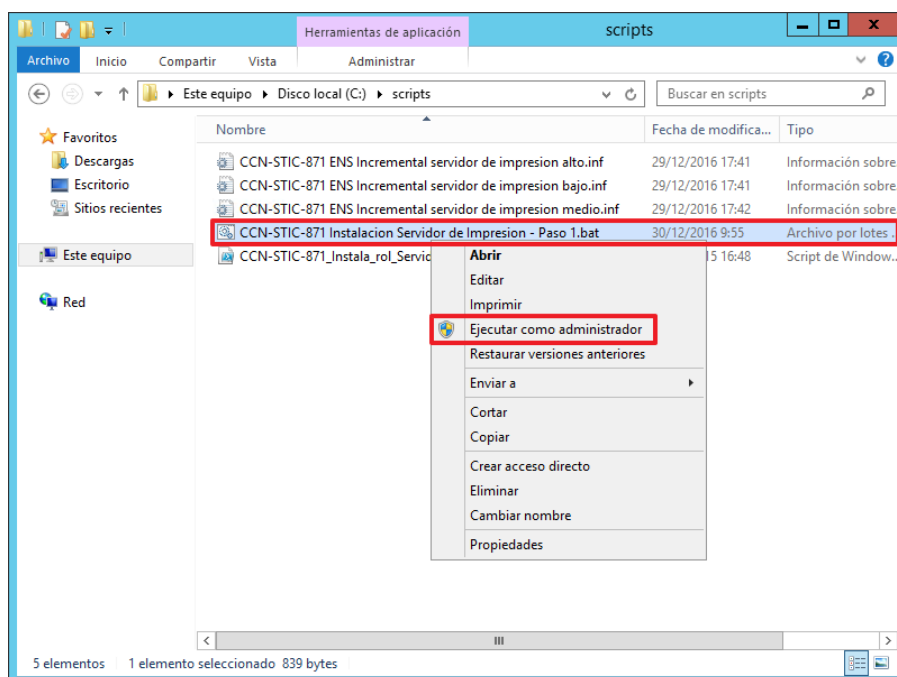
Tenga en consideración que si desea añadir más características o roles al Servidor de impresión deberá modificar el script y adaptarlo a las necesidades de su organización.

Nota: El procedimiento descrito a continuación, indica como instalar el rol “Servidor de impresión”. Si desea realizar este procedimiento continúe con el siguiente punto. En caso de tener ya instalado el rol “Servidor de impresión” vaya al punto “2 PREPARACIÓN DEL DOMINIO”.

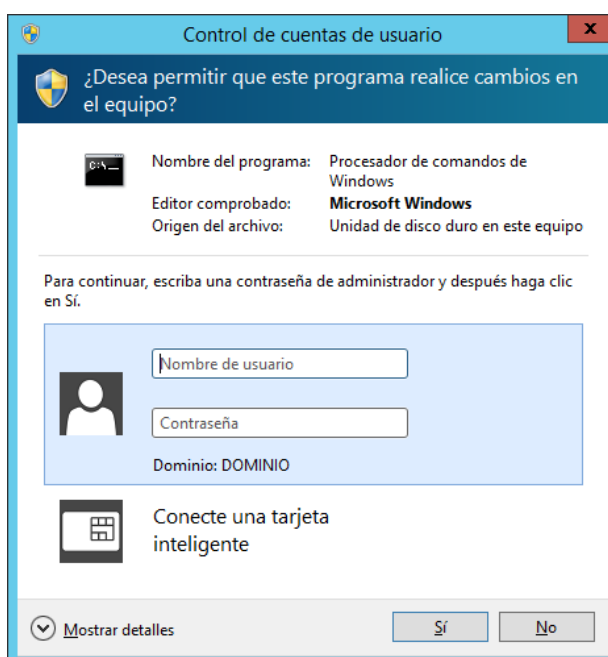
Paso	Descripción
1.	Inicie sesión en el servidor miembro donde vaya a instalar el rol Servidor de impresión. 

Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.
4.	En el directorio “C:\Scripts” localice el fichero “CCN-STIC-871 Instalacion Servidor de Impresion – Paso 1.bat”. Seleccione con el botón derecho del ratón y pulse sobre la opción del menú contextual “Ejecutar como administrador”.



5. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse “Sí” para continuar.



Paso	Descripción
------	-------------

6. Se lanzará el script. Pulse cualquier tecla para comenzar la instalación.

7. La instalación comenzará. Espere a que finalice.

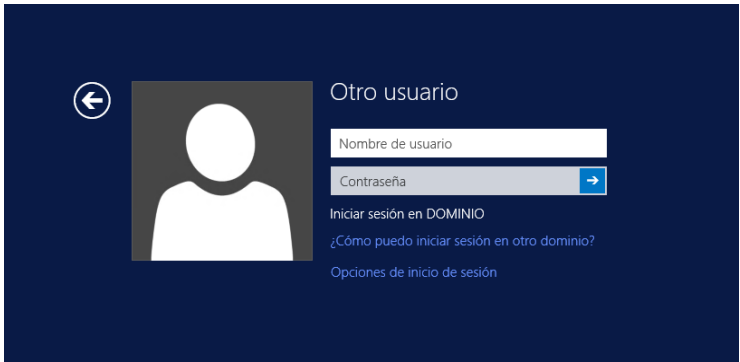
8. Cuando haya finalizado la instalación pulse una tecla para cerrar la ventana.

Nota: Ignore la advertencia sobre las actualizaciones automáticas de Windows.

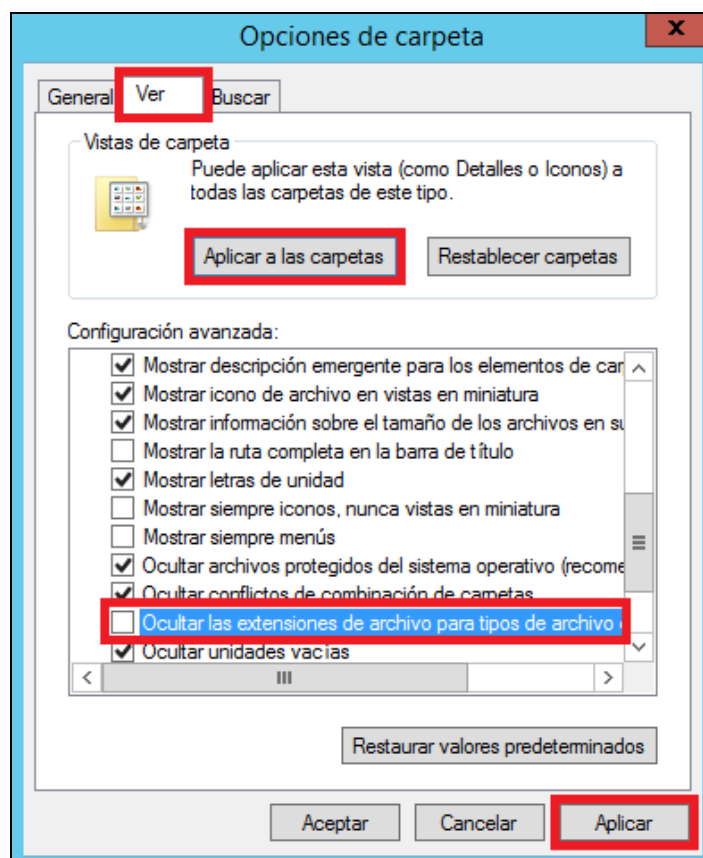
2. PREPARACIÓN DEL DOMINIO

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

Nota: Esta guía asume que a los servidores Controladores del Dominio al a pertenece el equipo servidor de impresión que está asegurando, se les ha aplicado la configuración descrita en la guía CCN-STIC-870A Implementación del ENS en Windows Server 2012 R2. Si no es así, aplique la guía correspondiente al Controlador de Dominio, antes de continuar con la aplicación de ésta.

Paso	Descripción
9.	Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad para el Servidor de impresión según criterios de ENS. 
	Nota: Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.
10.	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.
11.	Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio "C:\Scripts".
12.	Configure el "Explorador de Windows" para que muestre las extensiones de los archivos. Por defecto, el Explorador de Windows oculta las extensiones conocidas de los archivos y ello dificulta la identificación de los mismos. En el resto de pasos se asumirá que "Explorador de Windows" muestra las extensiones de los archivos.

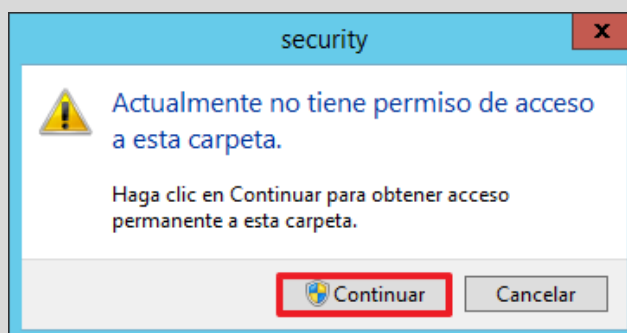
Paso	Descripción
13.	Para configurar "Explorador de Windows" para mostrar las extensiones de todos los archivos, abra una ventana de "Explorador de Windows", seleccione el menú "Vista" y dentro de dicho menú, "Opciones". De la ventana que aparecerá, seleccione la pestaña "Ver" y desmarque la opción "Ocultar las extensiones de archivo para tipos de archivo conocidos", como se muestra en la siguiente figura:



Pulse entonces, en este orden, "Aplicar" (botón en la esquina inferior derecha), "Aplicar a las carpetas" (botón en la parte superior), responda pulsando "Sí" a la pregunta de confirmación "¿Desea que la configuración de vista en todas las carpetas de este tipo coincida con la configuración de vista de esta carpeta?", y finalmente pulse "Aceptar" para cerrar la ventana "Opciones de carpeta".

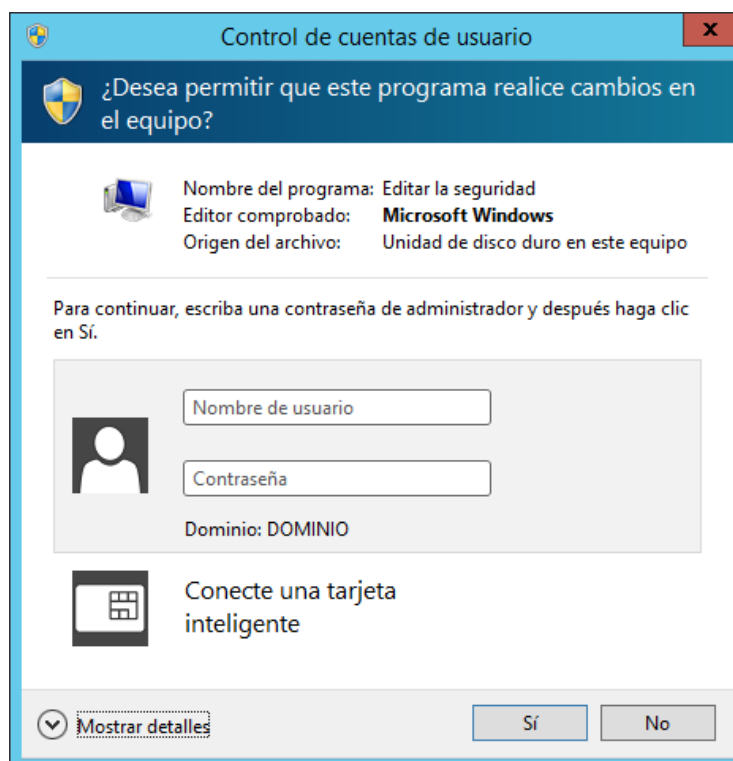
14. Adicionalmente acceda al directorio "C:\Windows\security\templates".

Nota: Para acceder a directorios protegidos por el sistema deberá obtener los permisos correspondientes para ello. Pulse sobre el botón "Continuar" ante la ventana emergente.

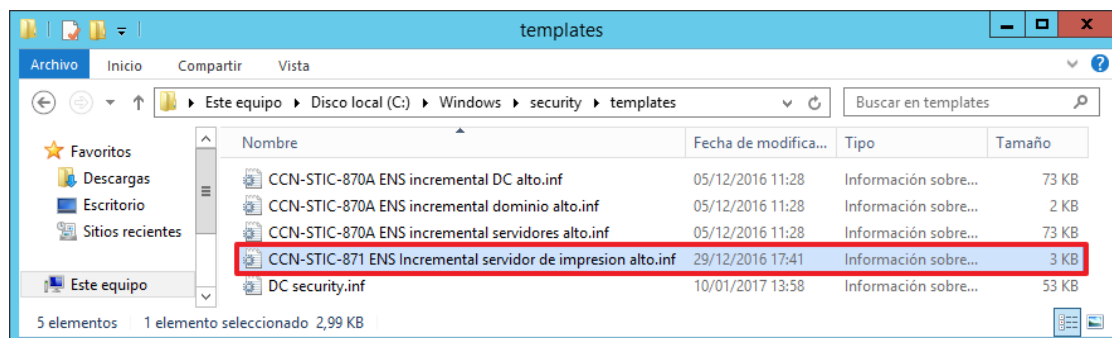


Paso	Descripción
------	-------------

- | | |
|-----|--|
| 15. | El Control de cuentas de usuario le solicitará la elevación de privilegios para poder acceder al directorio especificado. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse "Sí" para continuar. |
|-----|--|



- | | |
|-----|--|
| 16. | Copie el fichero "CCN-STIC-871 ENS Incremental servidor de impresion alto.inf" ubicado en "C:\Scripts" en el directorio "C:\Windows\security\templates". |
|-----|--|

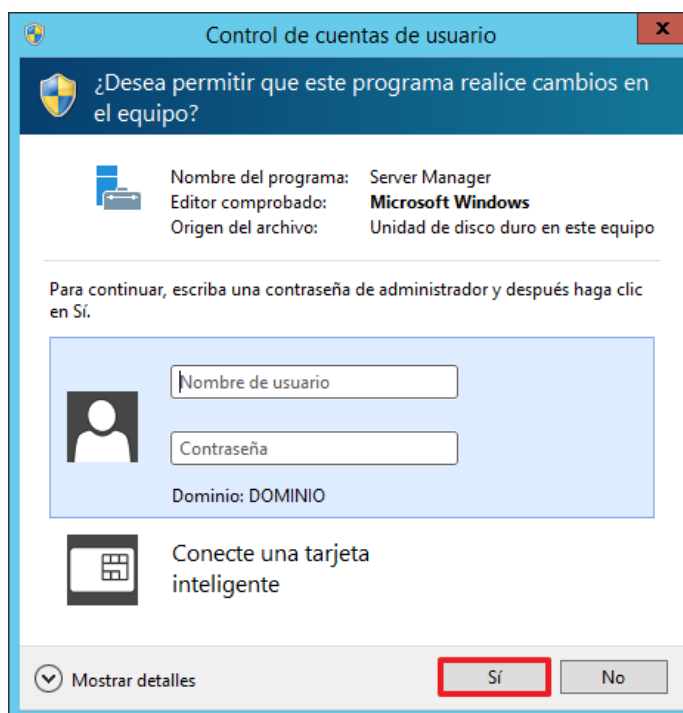


- | | |
|-----|--|
| 17. | A continuación, deberá crear la unidad organizativa "Servidores de Impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente. |
|-----|--|

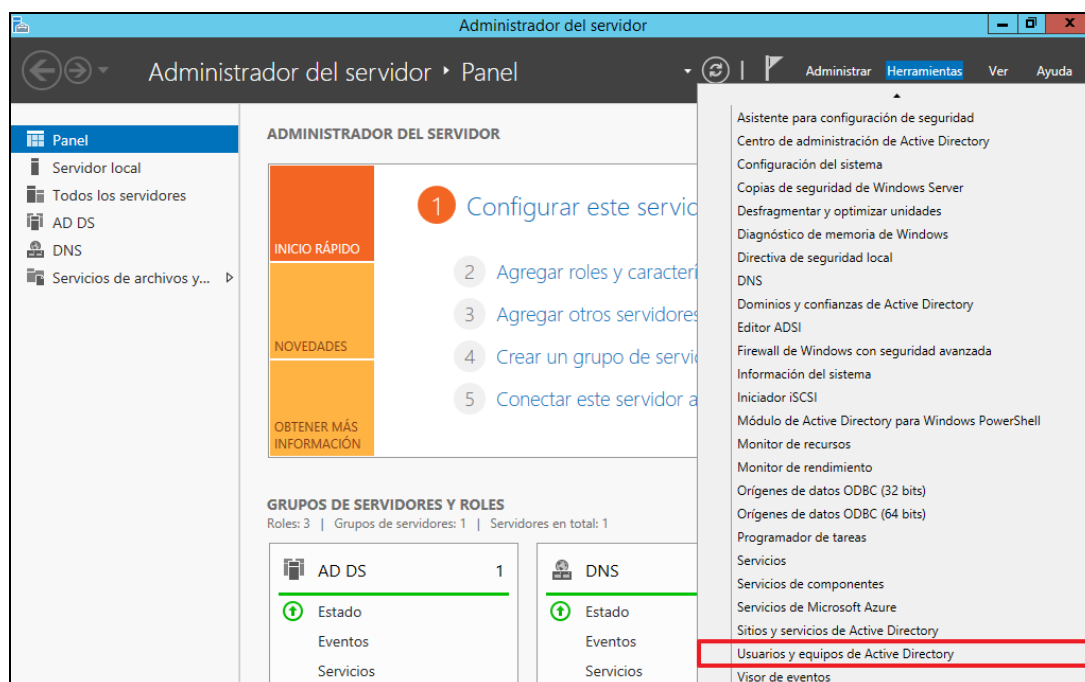


Paso	Descripción
------	-------------

18. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse “Sí” para continuar.

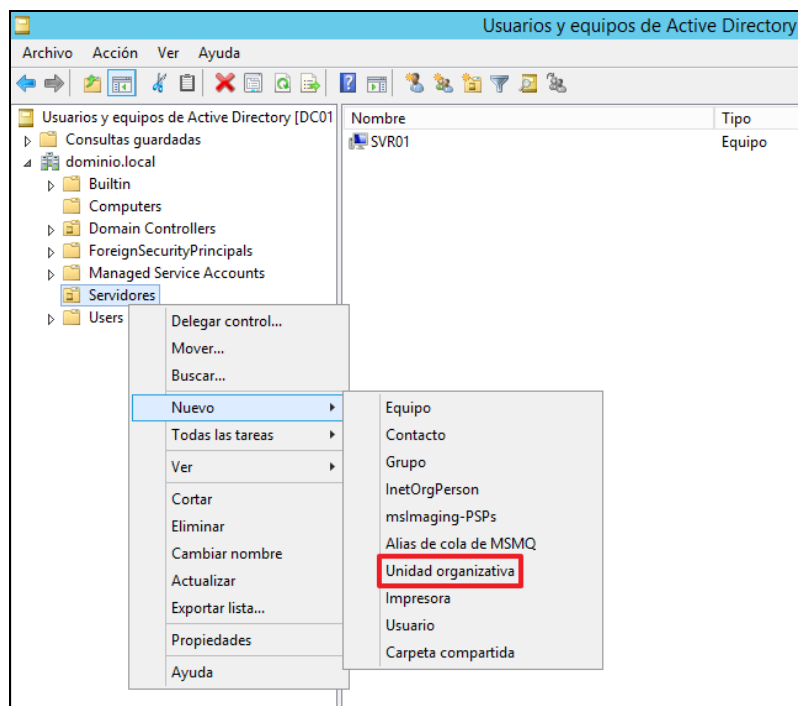


19. Inicie la herramienta “Usuarios y equipos Active Directory”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Usuarios y equipos de Active Directory”.



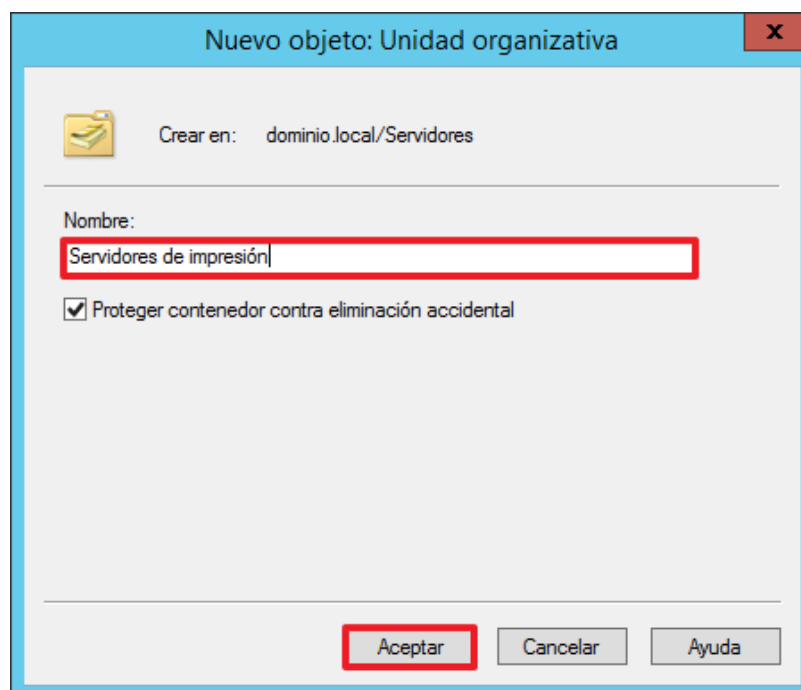
Paso	Descripción
------	-------------

20. En la consola, cree una nueva unidad organizativa dentro de la unidad organizativa donde se encuentren los servidores de su organización y sobre la que se aplica la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2. Para ello, seleccione el nodo “<<dominio>> / <<unidad organizativa>>”, y desplegando el menú contextual con el botón derecho, seleccione la opción “Nuevo > Unidad organizativa”.



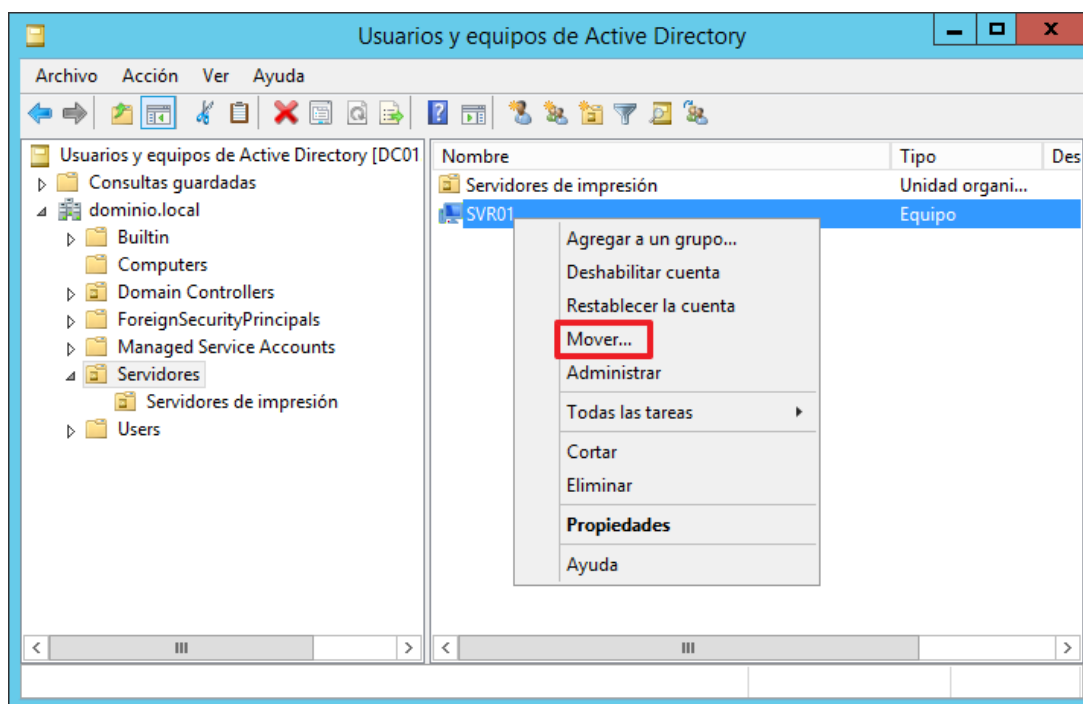
Nota: En este ejemplo, la unidad organizativa de servidores se encuentra en “dominio.local/Servidores”.

21. Introduzca el nombre “Servidores de impresión” tal y como se muestra en la imagen y pulse sobre “Aceptar”.

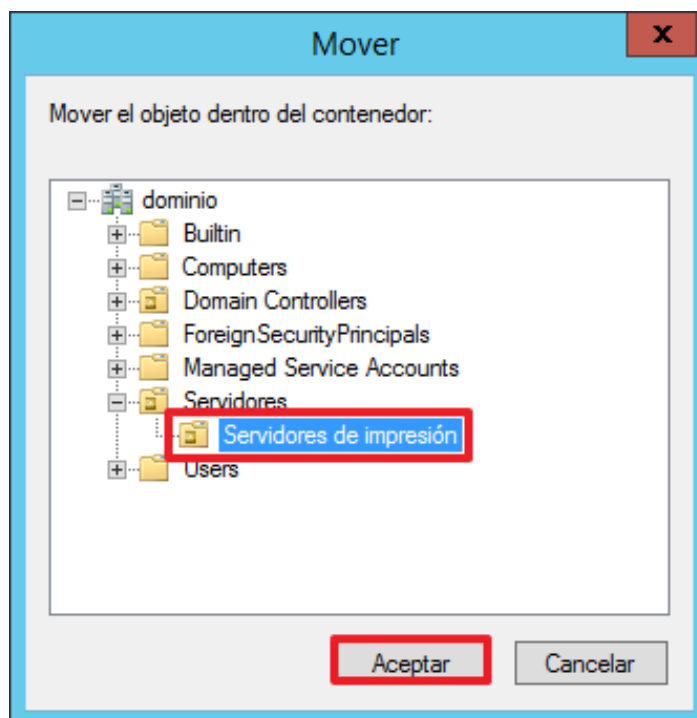


Paso	Descripción
------	-------------

22. Una vez creada la nueva Unidad organizativa, deberá mover los servidores de impresión a la unidad organizativa “Servidores de impresión”. Para ello, haga clic con el botón derecho sobre el equipo que desee reubicar y seleccione la opción del menú contextual “Mover...”.



23. A continuación, seleccione la unidad organizativa “Servidores de impresión” y pulse “Aceptar”.



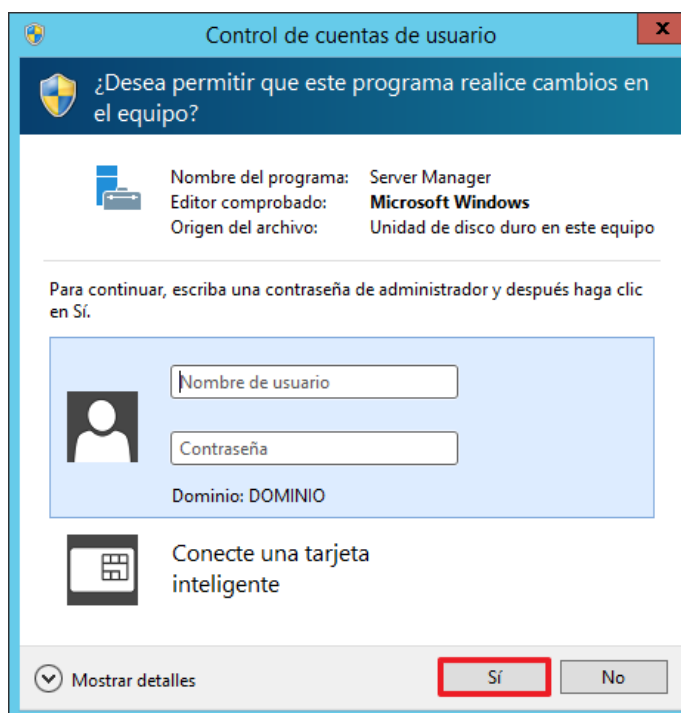
24. Cierre la herramienta de “Usuarios y equipos de Active Directory”.

Paso	Descripción
------	-------------

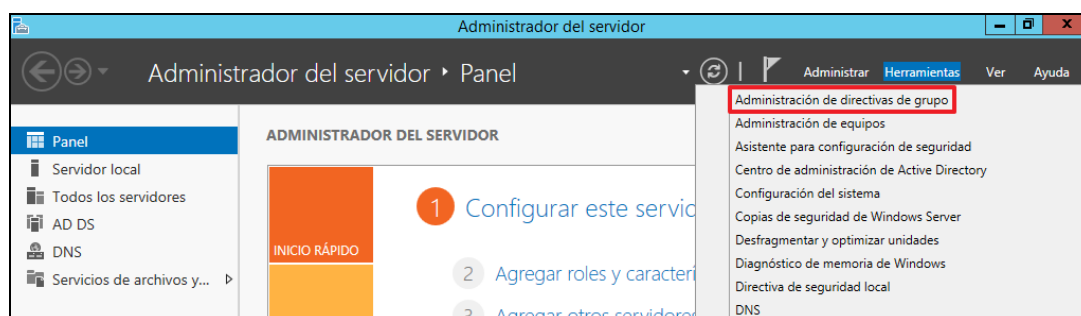
25. A continuación, deberá crear la GPO "CCN-STIC-871 ENS Incremental servidor de impresion alto". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.



26. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse "Sí" para continuar.



27. 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".

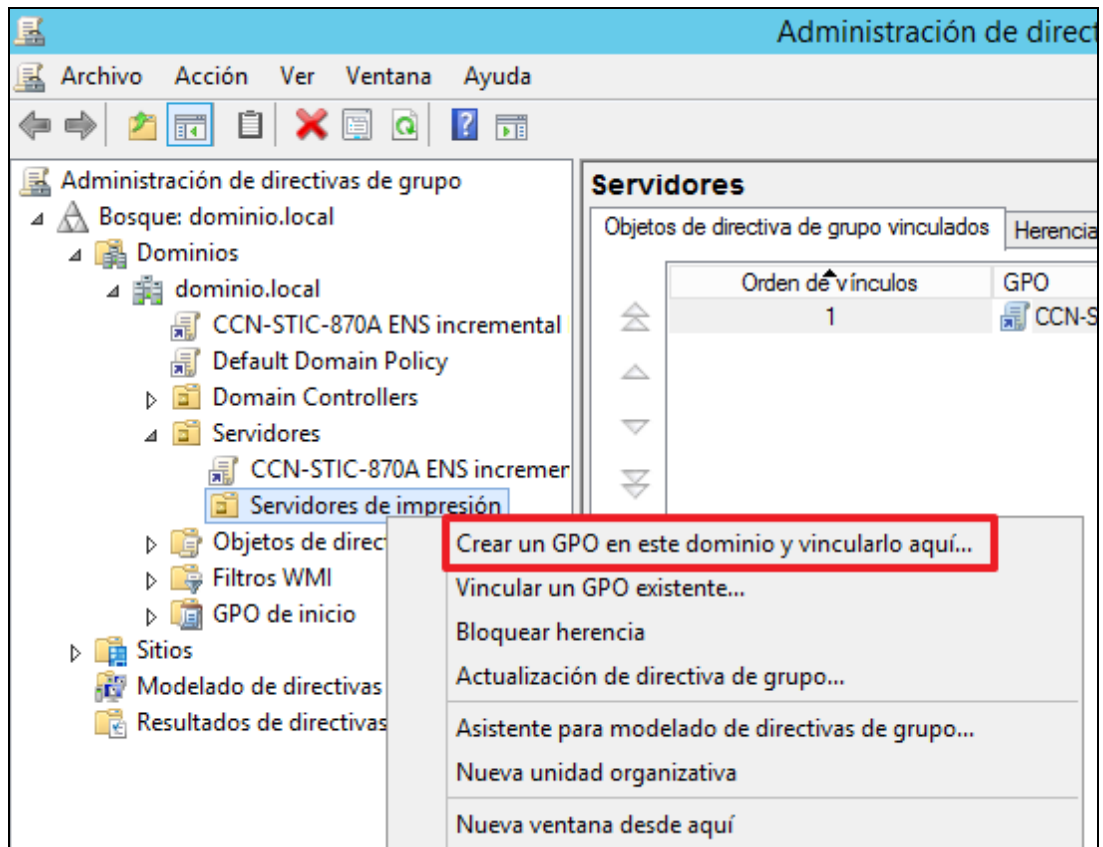


28. A continuación, despliegue el nodo "Bosque: <<nombre de bosque>> / Dominios / <<nombre de dominio>> / Servidores / Servidores de impresión".

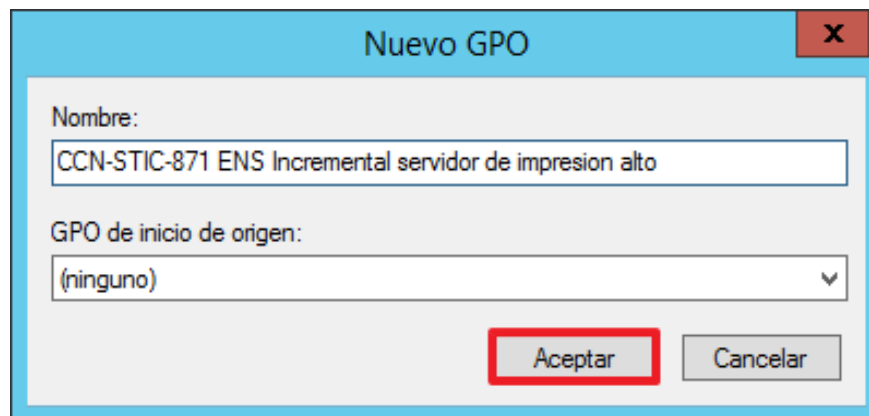
Nota: En este ejemplo el nombre de la unidad organizativa donde se encuentran los servidores es "Servidores de impresión".

Paso	Descripción
------	-------------

29. Pulse con el botón derecho sobre la unidad organizativa “Servidores de impresión” y seleccione “Crear un GPO en este dominio y vincularlo aquí...”.

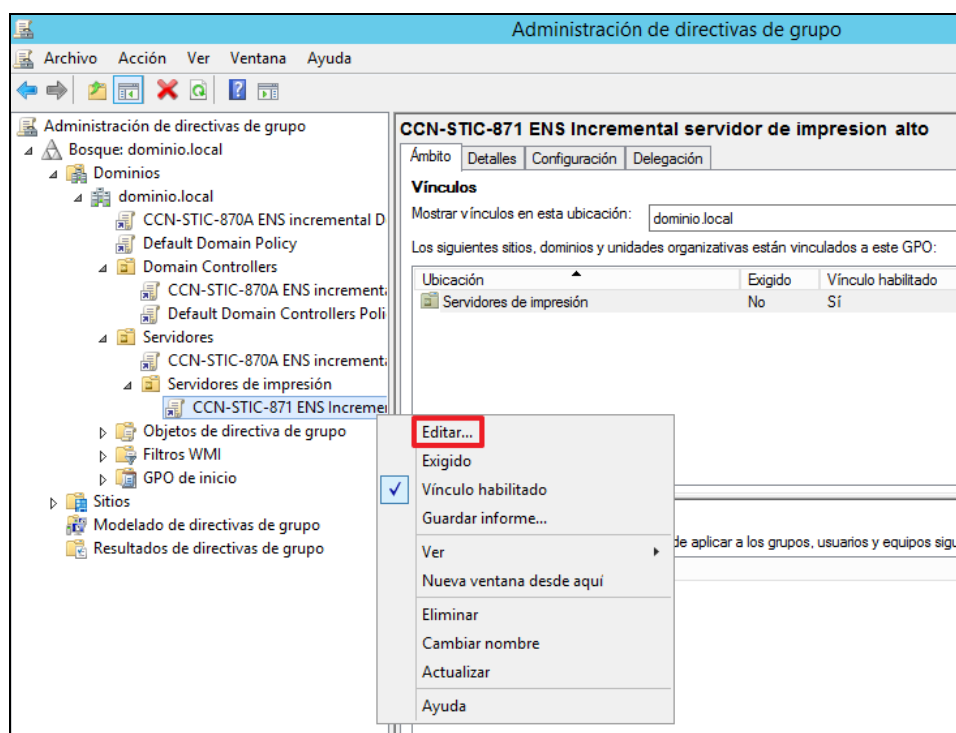


30. Escriba el nombre de la GPO “CCN-STIC-871 ENS Incremental servidor de impresion alto” y haga clic en el botón “Aceptar”.



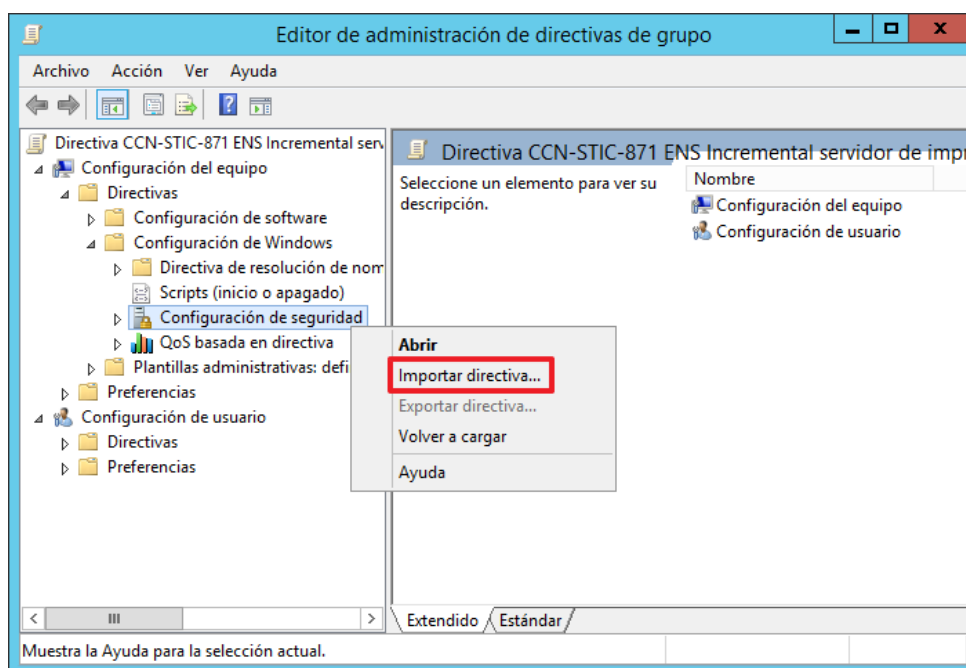
Paso	Descripción
------	-------------

- | | |
|-----|--|
| 31. | Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción "Editar". |
|-----|--|



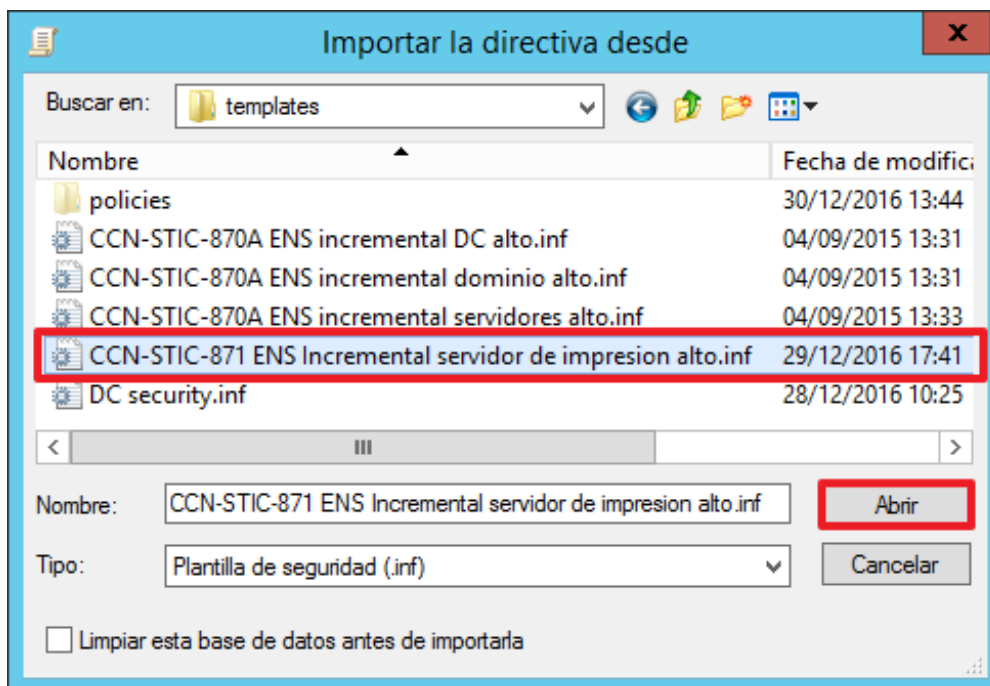
- | | |
|-----|---|
| 32. | Despliegue el objeto de directiva de grupo y sitúese en la siguiente ruta:
"Configuración de equipo → Directivas → Configuración de Windows → Configuración de seguridad" |
|-----|---|

- | | |
|-----|---|
| 33. | Pulse con el botón derecho sobre configuración de seguridad y seleccione la opción "Importar directiva...". |
|-----|---|

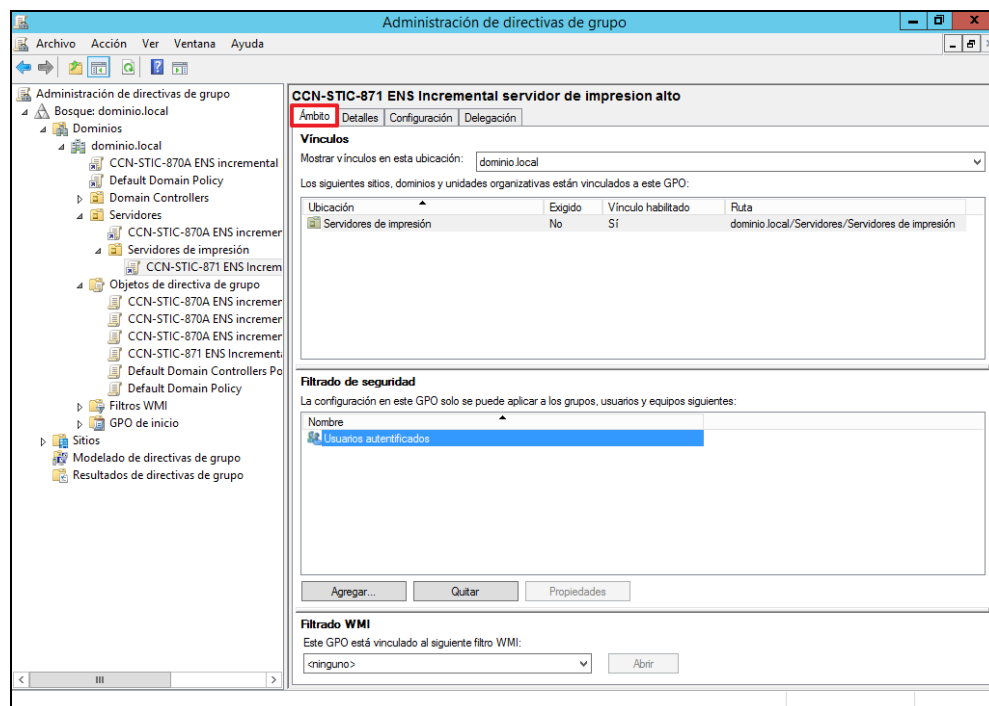


Paso	Descripción
------	-------------

34. Seleccione de la ruta "C:\Windows\security\templates" el fichero "CCN-STIC-871 ENS Incremental servidor de impresion alto.inf" y pulse el botón "Abrir".

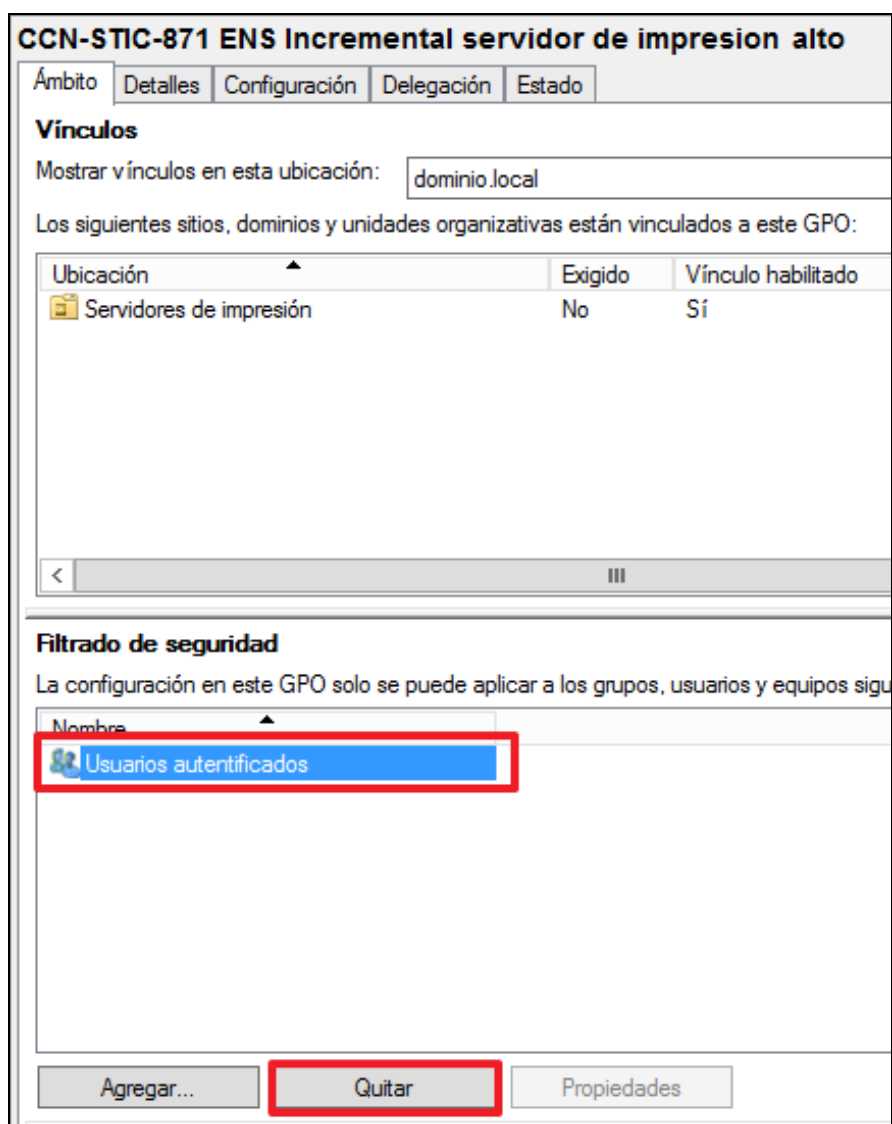


35. Cierre la política una vez que se haya realizado la importación de la configuración de seguridad.
36. Seleccione la nueva política de grupo configurada y vaya a la pestaña "Ámbito" que se encuentra en el panel derecho.

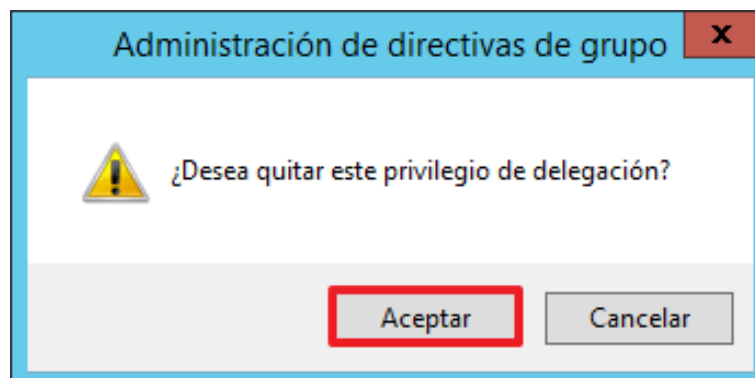


Paso	Descripción
------	-------------

37. En la opción de filtrado de seguridad, seleccione “Usuarios autenticados” y pulse la opción “Quitar”.



38. Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.



Paso	Descripción
------	-------------

39. A continuación, pulse el botón “Agregar...”.

CCN-STIC-871 ENS Incremental servidor de impresion alto

Ámbito Detalles Configuración Delegación

Vínculos

Mostrar vínculos en esta ubicación: dominio.local

Los siguientes sitios, dominios y unidades organizativas están vinculados a este GPO:

Ubicación	Exigido	Vínculo habilitado
📁 Servidores de impresión	No	Sí

Filtrado de seguridad

La configuración en este GPO solo se puede aplicar a los grupos, usuarios y equipos sig

Nombre

Agregar... Quitar Propiedades

40. Introduzca como nombre “ENS servidores Windows 2012 R2 nivel alto”. Este grupo corresponde con el generado en la aplicación de la guía CCN-STIC-870A – Implementación del ENS en Windows Server 2012 R2.
- A continuación, pulse el botón “Aceptar”.

Seleccionar Usuario, Equipo o Grupo

Seleccionar este tipo de objeto:

Usuario, Grupo, o Entidad de seguridad integrada Tipos de objeto...

Desde esta ubicación:

dominio.local Ubicaciones...

Escriba el nombre de objeto para seleccionar (ejemplos):

ENS servidores Windows 2012 R2 nivel alto Comprobar nombres

Opciones avanzadas... Aceptar Cancelar

Nota: En caso de no disponer del grupo mostrado en la guía, deberá adaptar estos pasos a las necesidades de su organización.

3. 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.

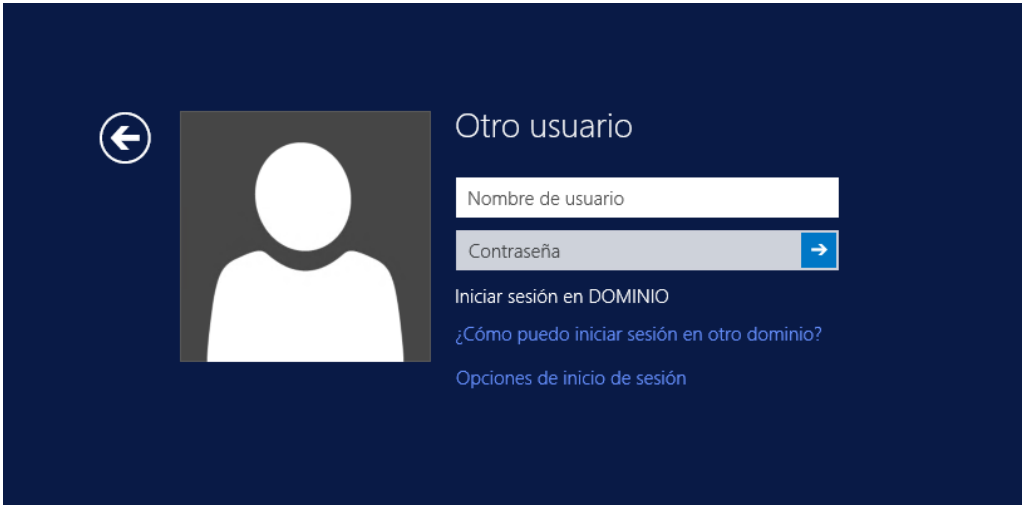
Este punto recoge estas consideraciones, así como una serie de aspectos posteriores de configuración que deberán aplicarse.

3.1 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 ataques, minimizando en la medida de lo posible la exposición del entorno, por lo que para cumplir con esta medida es necesario quitar todas aquellas características las cuales puedan ser vulnerables frente a ataques o no se esté haciendo uso de ellas en la organización.

Para realizar el siguiente paso a paso deberá realizar previamente el paso “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” y una vez finalizado deberá realizar el paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

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

Paso	Descripción
41.	Inicie sesión en el servidor miembro donde tenga instalado el rol Servidor de impresión. 

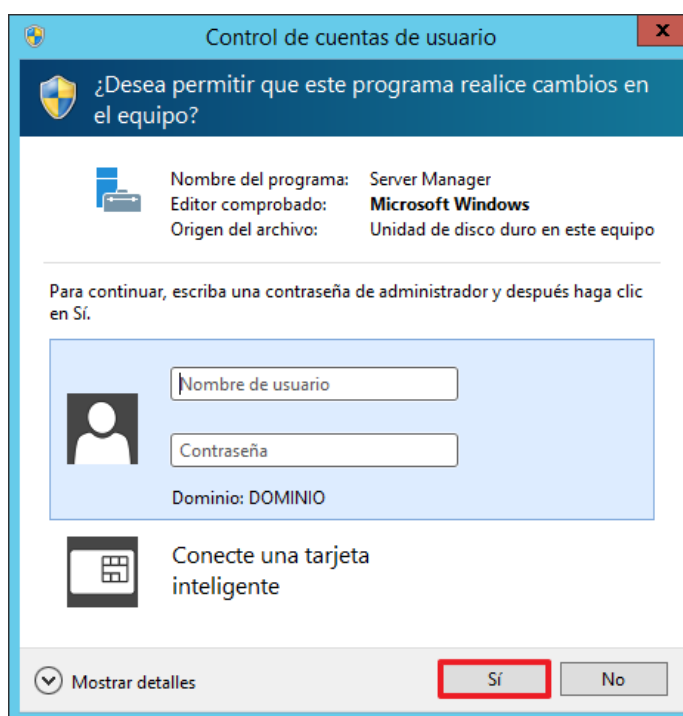
Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
------	-------------

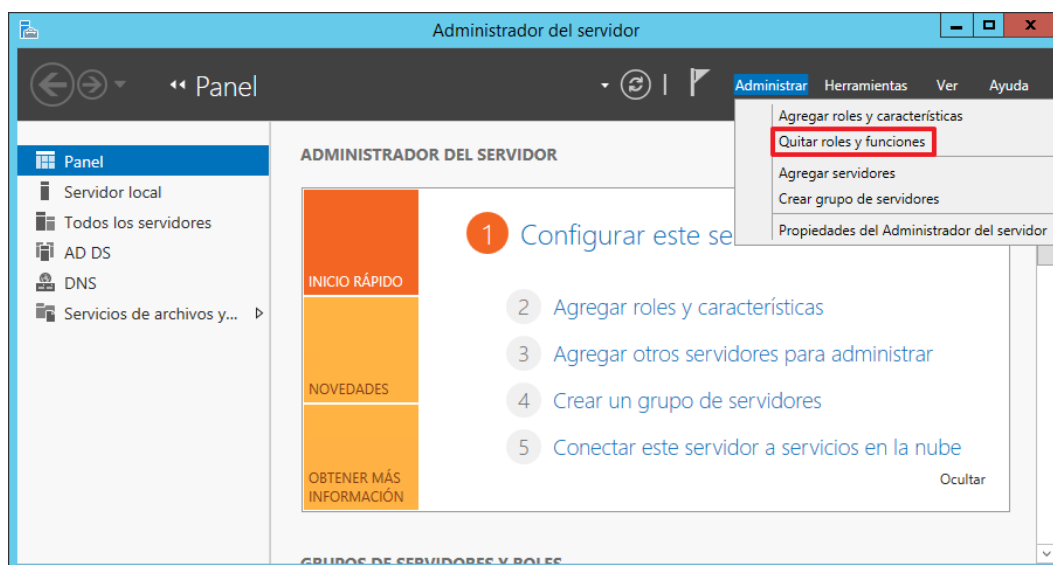
42. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



43. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.

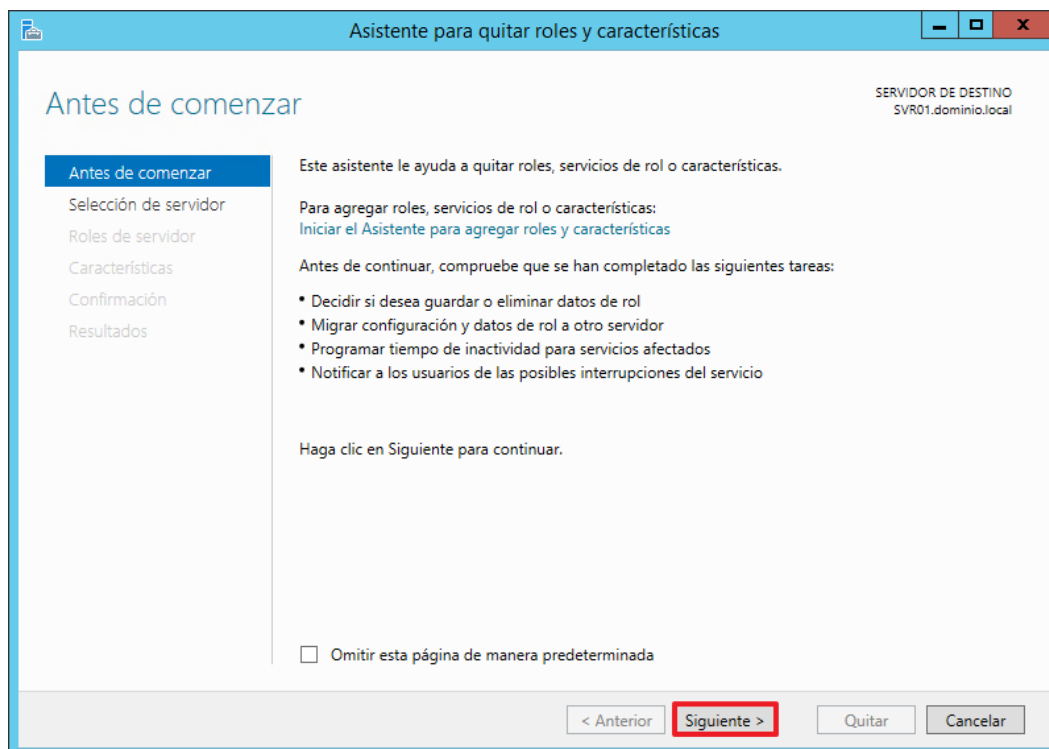


44. A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.

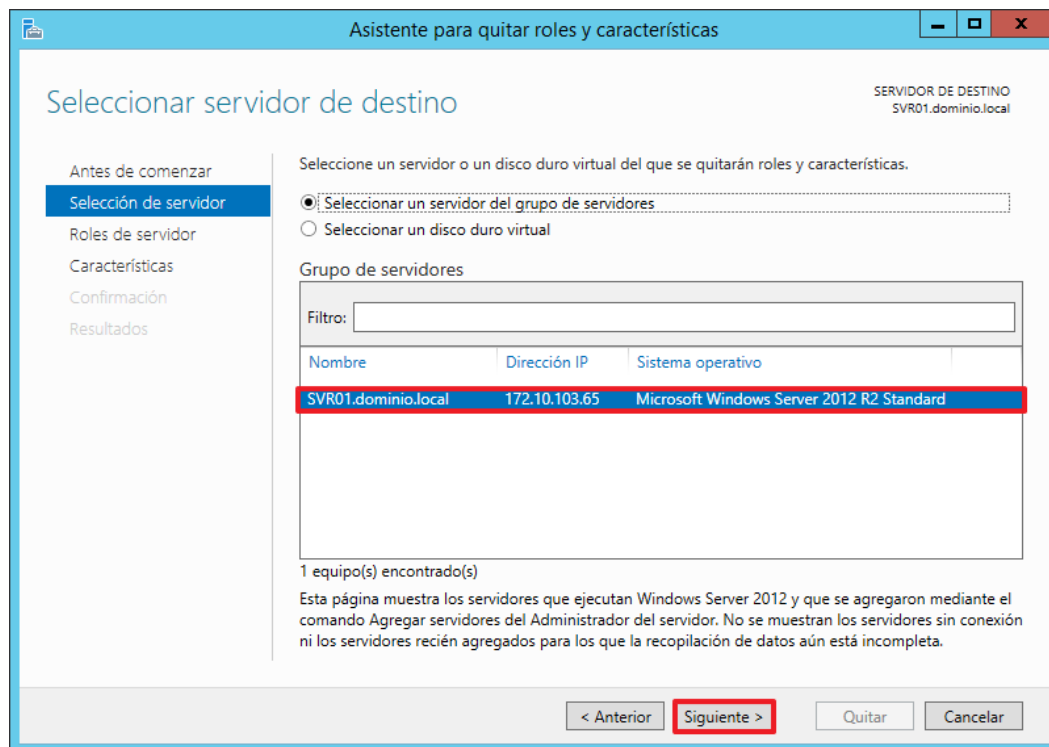


Paso	Descripción
------	-------------

45. Se lanzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar.



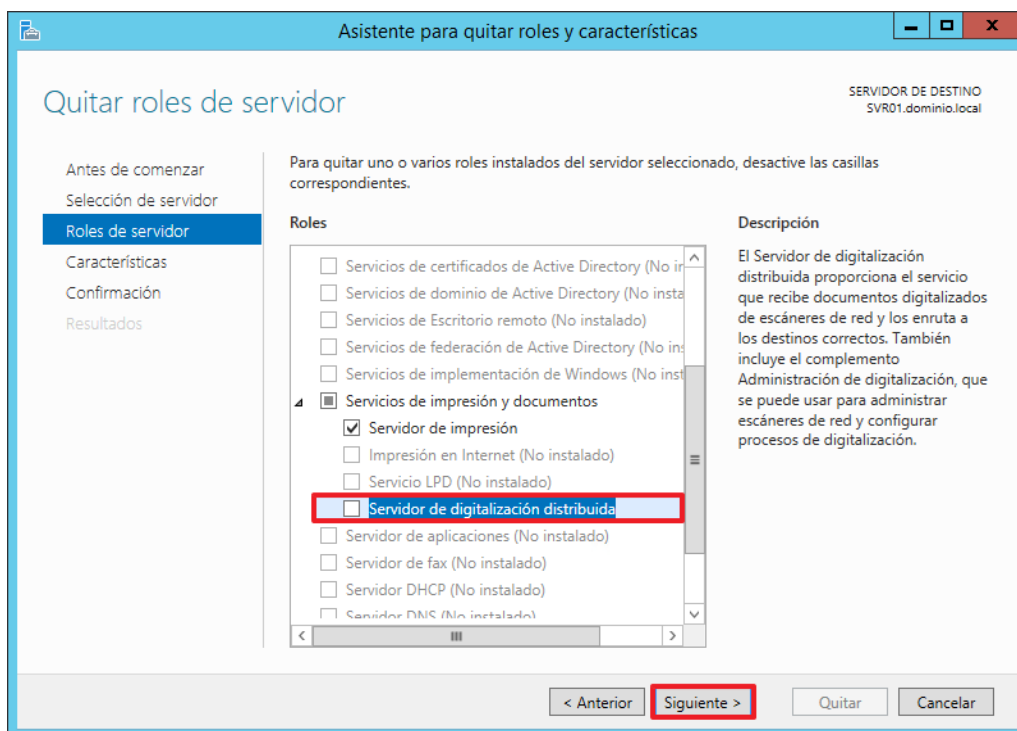
46. Seleccione el servidor sobre el cual desea eliminar un rol o característica y pulse “Siguiente >”.



Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

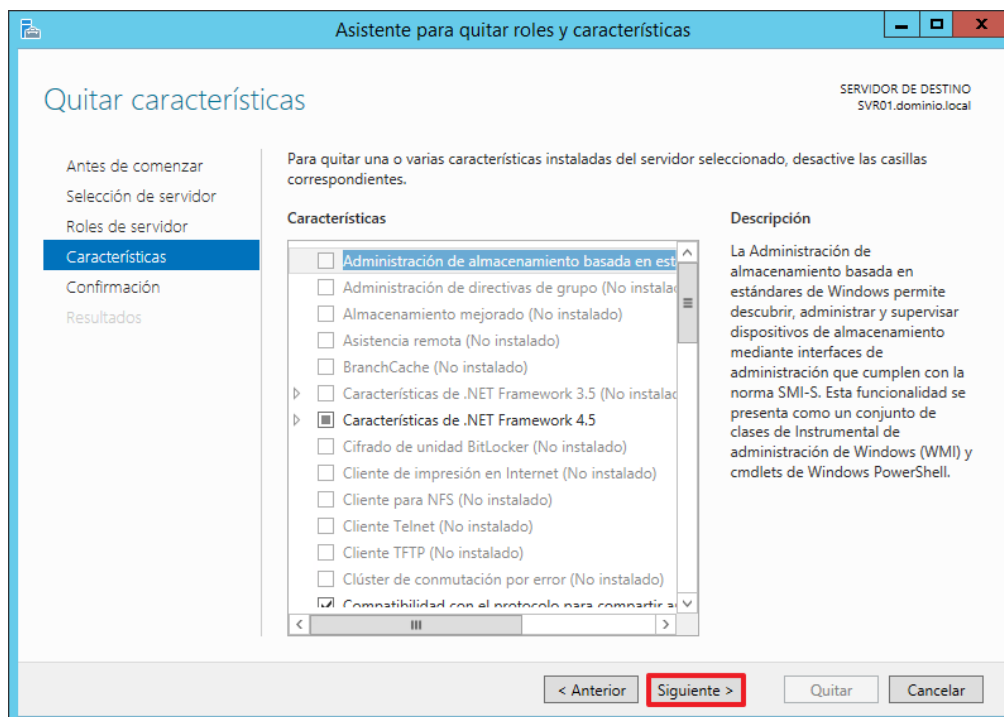
Paso	Descripción
------	-------------

- | | |
|-----|--|
| 47. | En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”. |
|-----|--|



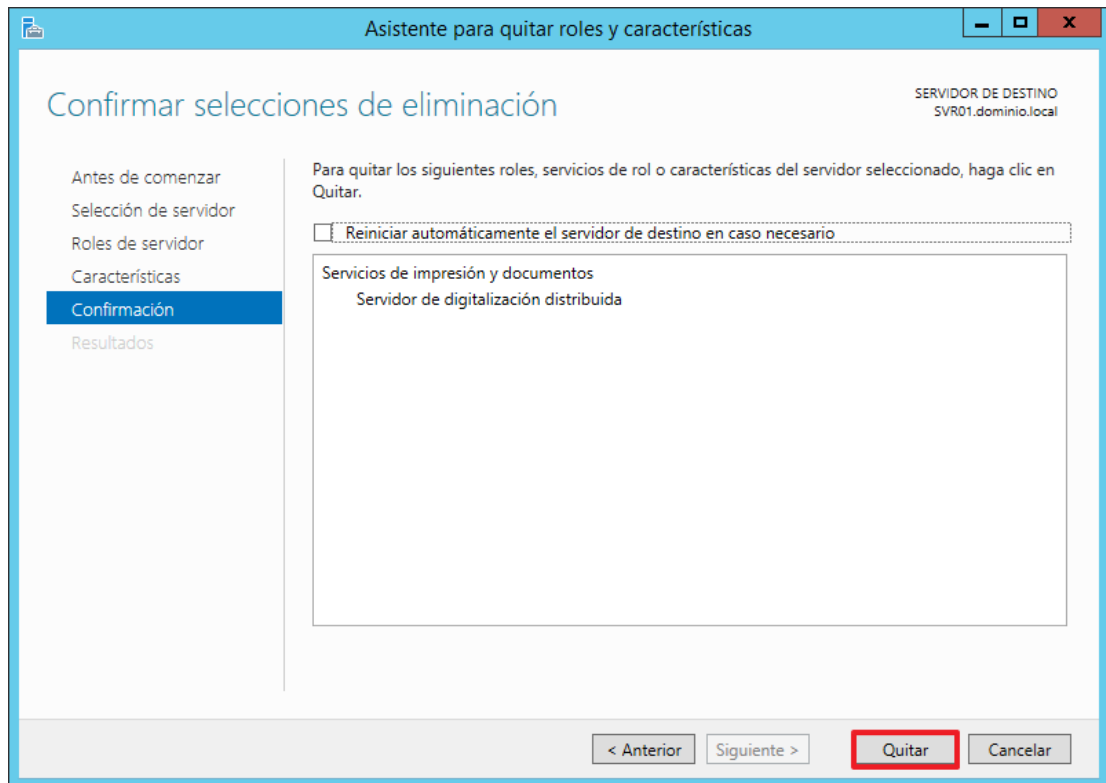
Nota: En este ejemplo se desinstala el rol “servidor de digitalización distribuida”.

- | | |
|-----|---|
| 48. | En la ventana de características pulse el botón “Siguiente >”. En este ejemplo no se desinstala ninguna característica adicional. |
|-----|---|

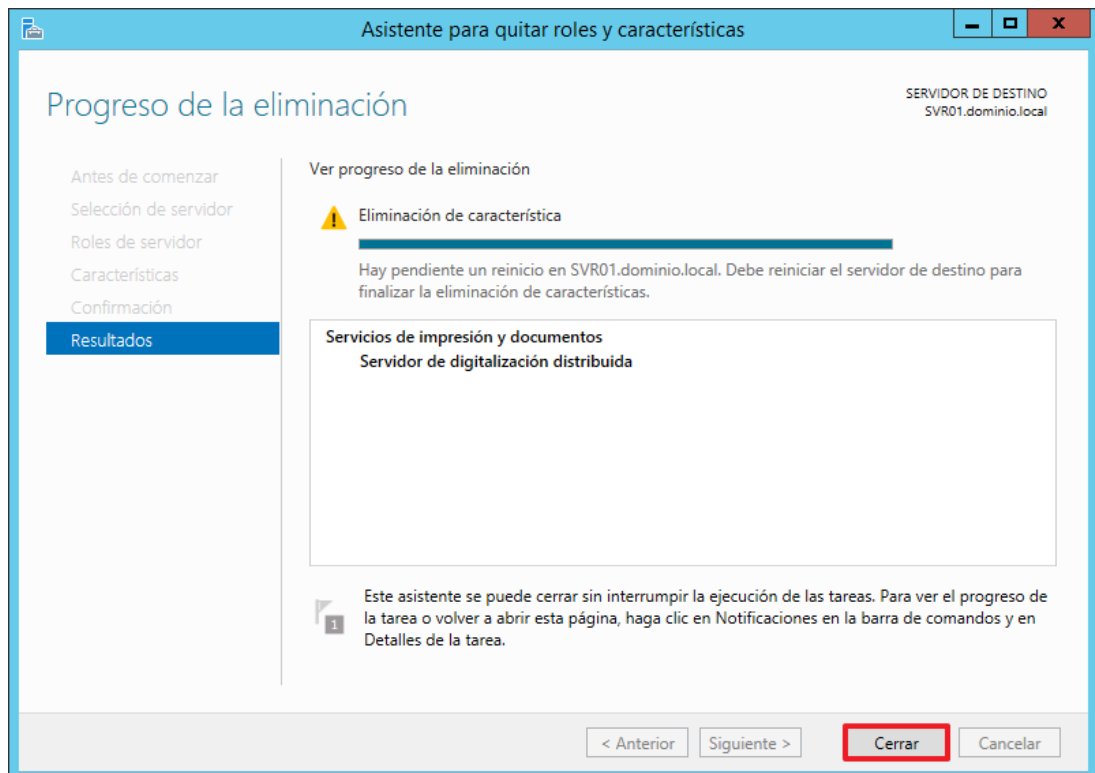


Paso Descripción

49. En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.



50. El proceso comenzará y una vez finalizado, y si todo ha ido bien bastará con pulsar sobre “Cerrar” para finalizar la desinstalación.

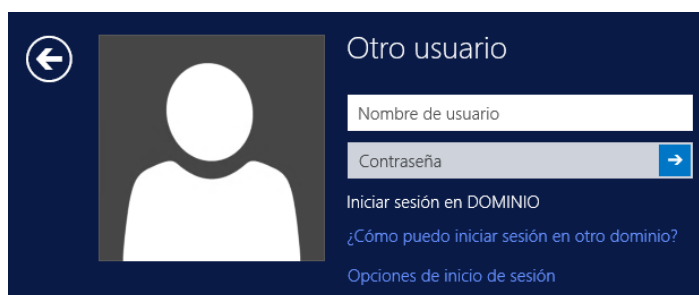


Paso	Descripción
51.	En caso de ser necesario el servidor requerirá un reinicio para finalizar la configuración.
52.	A continuación, deberá desvincular la GPO creada anteriormente para eliminar un rol, para ello realice el punto “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

3.2 GESTIÓN DE PERMISOS SOBRE DISPOSITIVOS DE IMPRESIÓN

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

Paso	Descripción
53.	Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.

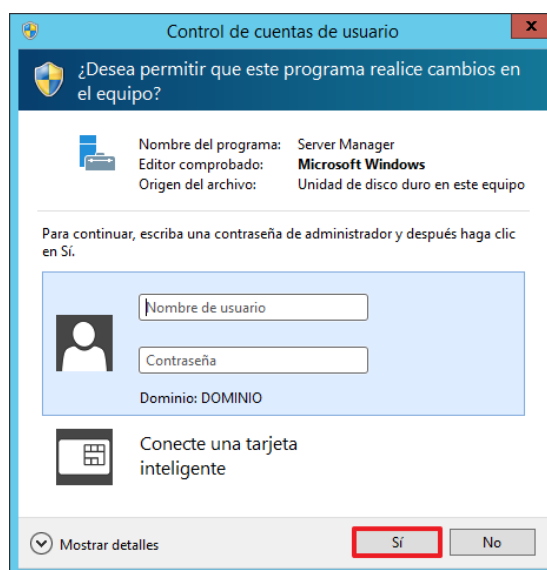


Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

54. A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta “Administrador del servidor” mediante el icono correspondiente.

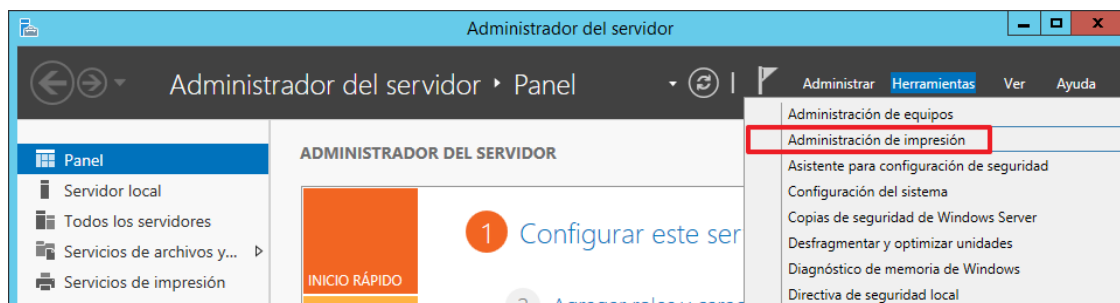


55. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse “Sí” para continuar.

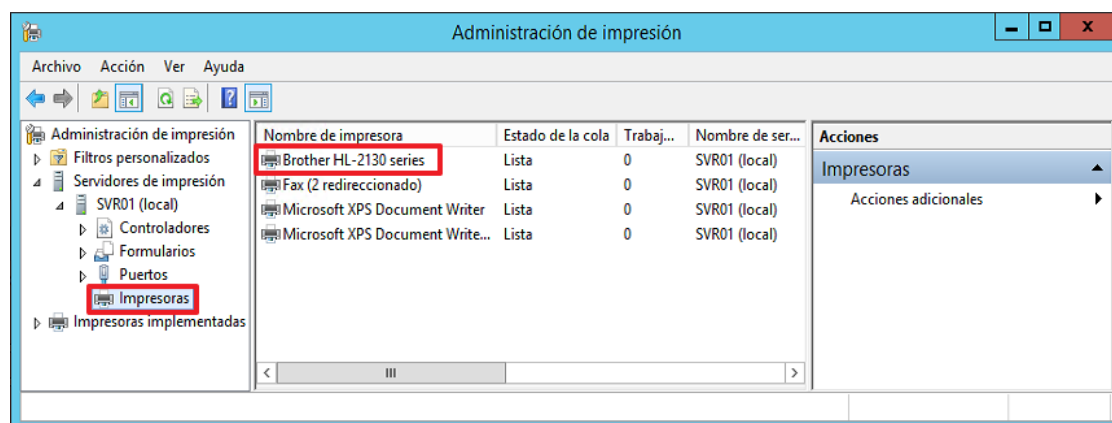


Paso	Descripción
------	-------------

56. Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de impresión”.

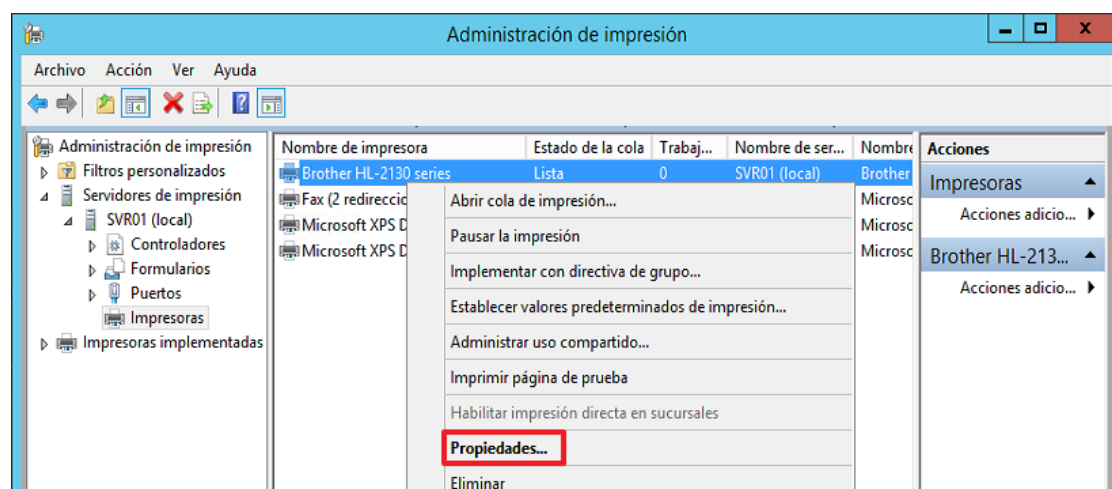


57. Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de impresión. Para ello despliegue el nodo “Servidores de impresión / <<nombre del servidor>> / Impresora”.



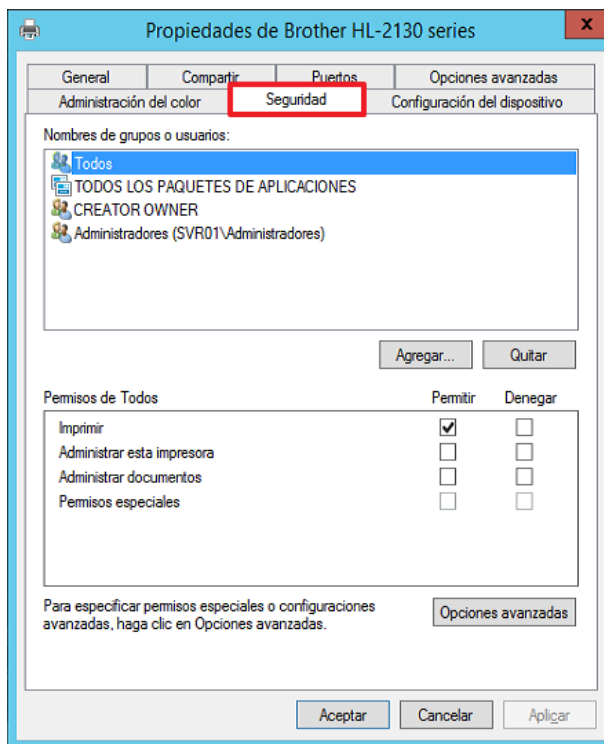
Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

58. Pulse con el botón derecho sobre el dispositivo de impresión “Brother HL-2130 series” y seleccione la opción “Propiedades...”.

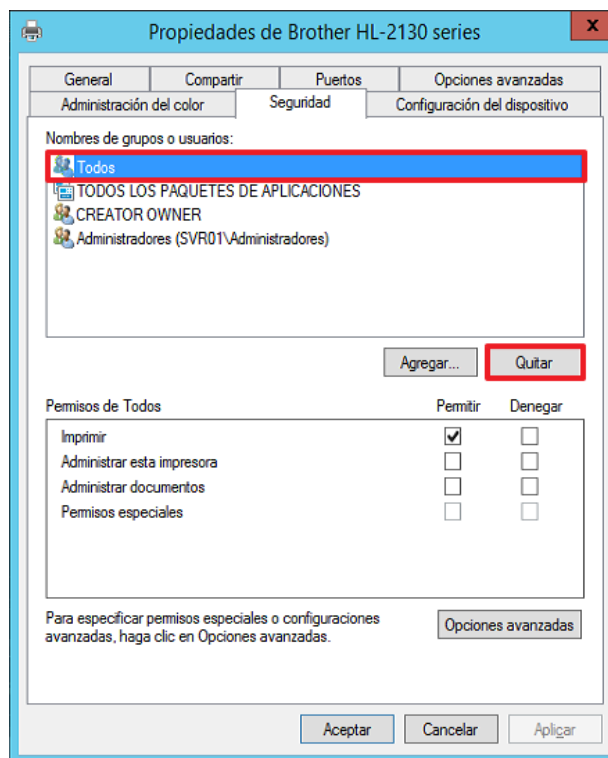


Paso	Descripción
------	-------------

59. A continuación, seleccione la pestaña “Seguridad”.



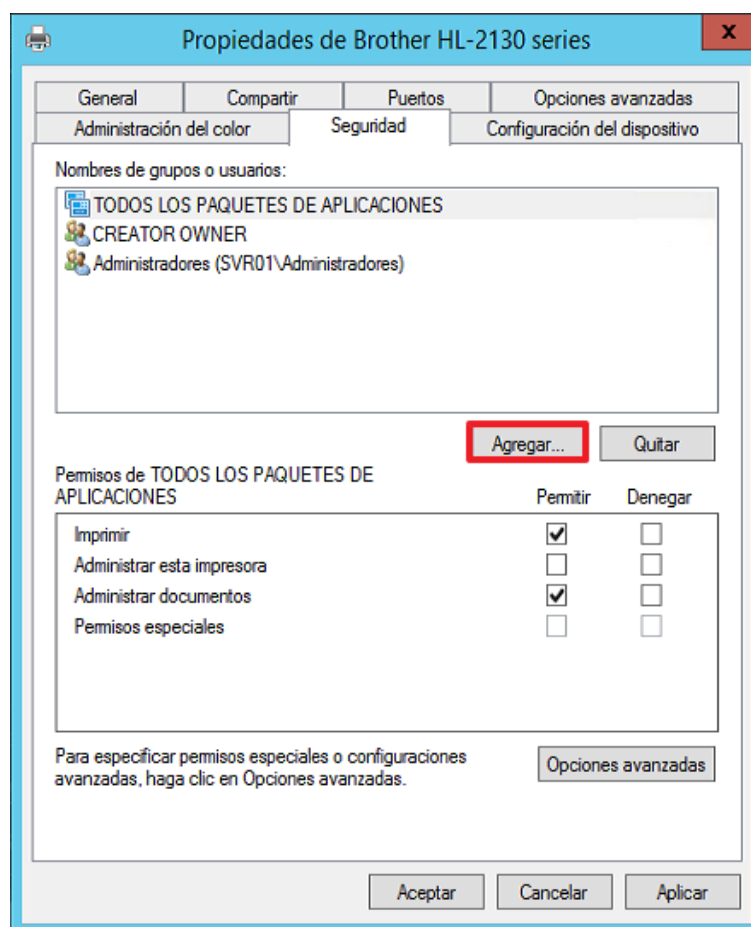
60. Seleccione el grupo de usuarios “Todos” y a continuación pulse en la opción “Quitar”.



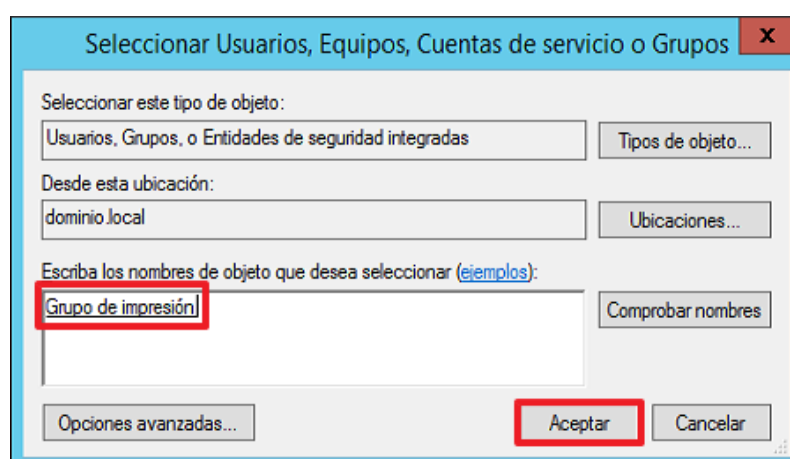
Nota: Debera adaptar este paso a los requisitos de su organización eliminando los usuarios o grupos de usuarios que no requieran de permisos sobre el dispositivo de impresión.

Paso	Descripción
------	-------------

- | | |
|-----|--|
| 61. | A continuación, pulse sobre el botón “Agregar” para añadir el grupo de usuarios que tendrá permiso para poder imprimir por el dispositivo de impresión seleccionado. |
|-----|--|



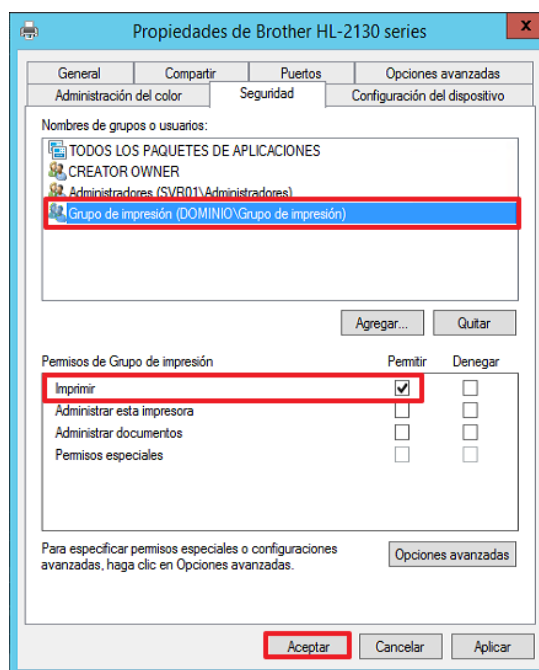
- | | |
|-----|---|
| 62. | Localice el grupo que quiere añadir para que obtenga permisos para imprimir, y pulse sobre “Aceptar”. |
|-----|---|



Nota: En esta guía se selecciona el grupo de seguridad “Grupo de impresión” al cual pertenecen los usuarios que van a obtener permiso para poder imprimir a través de los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.

Paso	Descripción
------	-------------

63. Una vez añadido el grupo de seguridad, localice el grupo y seleccione en los permisos únicamente la opción de “Imprimir”. Pulse “Aceptar” para cerrar la ventana.



Nota: En este ejemplo se utiliza el grupo denominado “Grupo de impresión”.

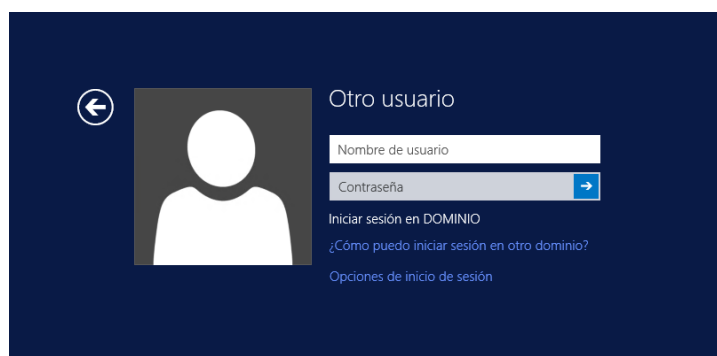
64. Debera repetir estos pasos para asignar permisos de impresión sobre todos los dispositivos de impresión que este securizando.

3.3 GESTIÓN DE PERMISOS DE ADMINISTRACIÓN DE DISPOSITIVOS DE IMPRESIÓN

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

Paso	Descripción
------	-------------

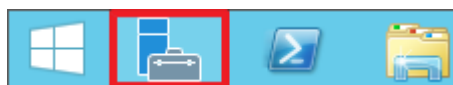
65. Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.



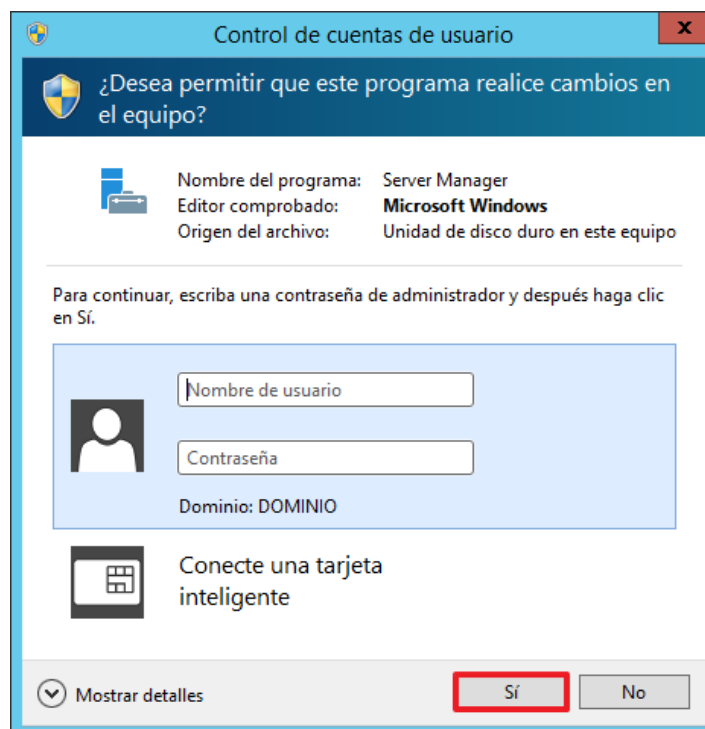
Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

Paso	Descripción
------	-------------

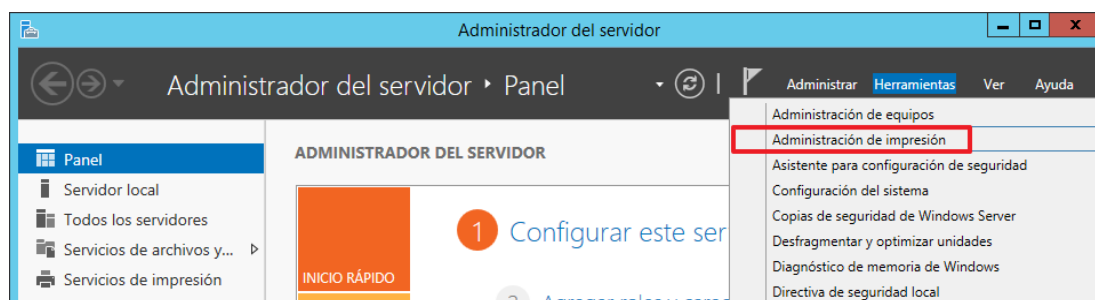
66. A continuación, deberá iniciar la herramienta “Administración de impresión”. Para ello, utilice la herramienta “Administrador del servidor” mediante el icono correspondiente.



67. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse “Sí” para continuar.

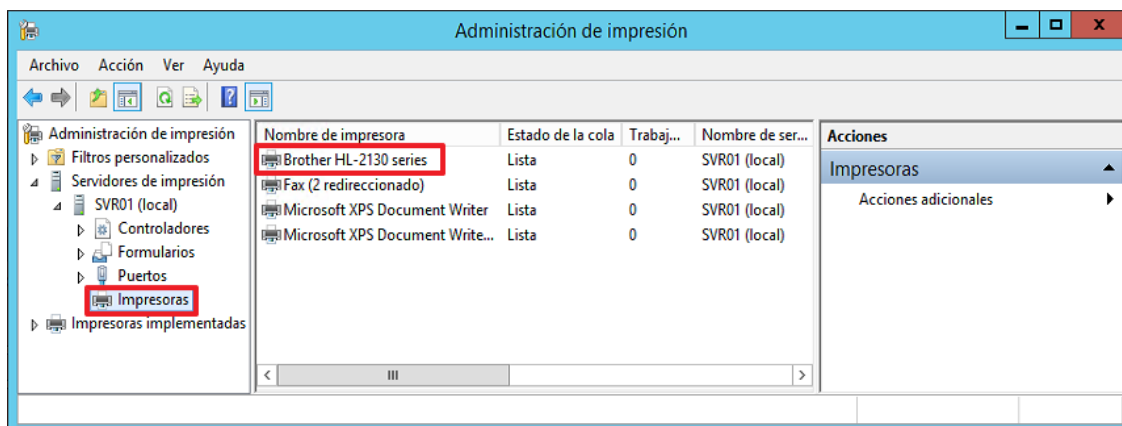


68. Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de impresión”



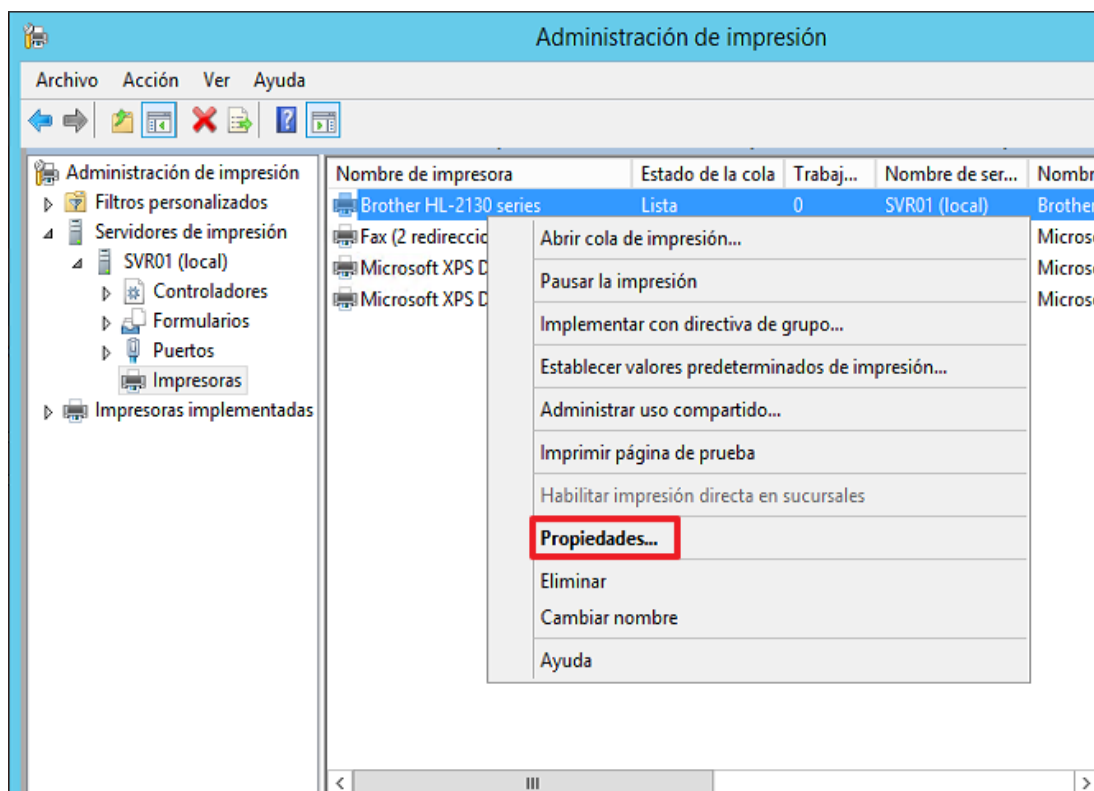
Paso	Descripción
------	-------------

- | | |
|-----|--|
| 69. | Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión. Para ello despliegue el nodo “Servidores de impresión / <<nombre del servidor>> / Impresoras”. |
|-----|--|



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades su organización.

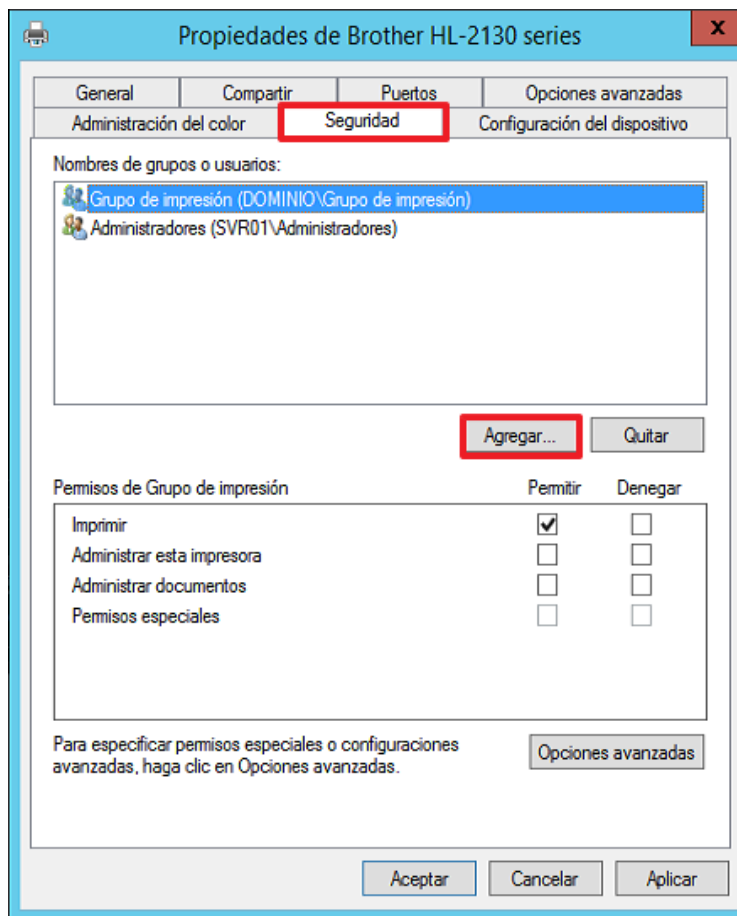
- | | |
|-----|---|
| 70. | Pulse con el botón derecho sobre el dispositivo de impresión y seleccione la opción “Propiedades...”. |
|-----|---|



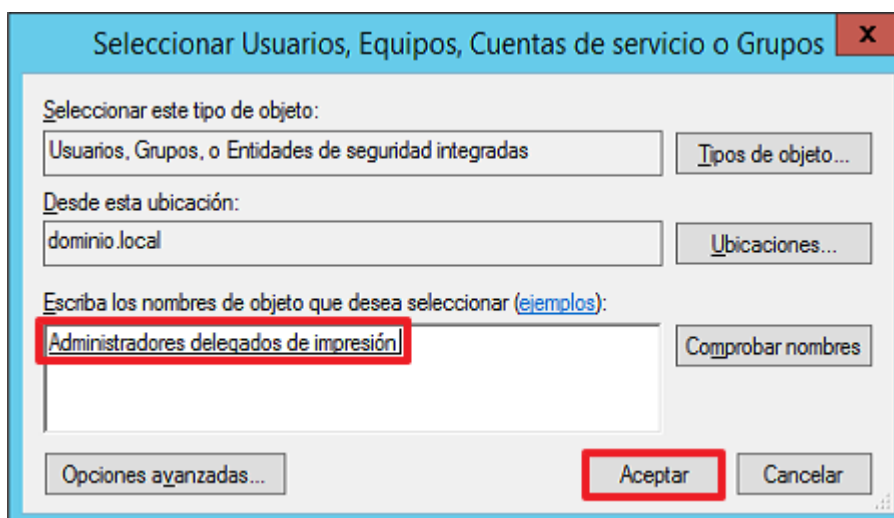
Nota: Para este ejemplo se utiliza el dispositivo denominado “Brother HL-2130 series”.

Paso	Descripción
------	-------------

71. A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Agregar...”.

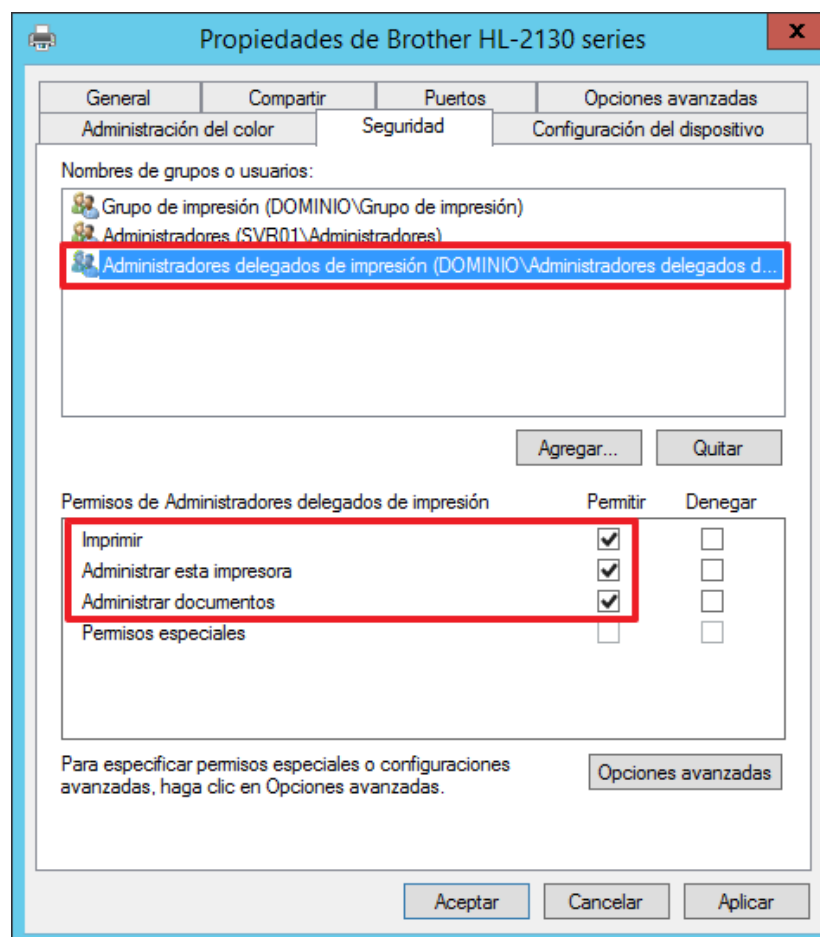


72. Localice el grupo que quiere añadir para que obtenga permisos para poder administrar el dispositivo de impresión seleccionado, y pulse sobre el “Aceptar”.



Nota: En esta guía se selecciona el grupo de seguridad “Administradores delegados de impresión” al cual pertenecen los usuarios que van a obtener permisos administrativos sobre los dispositivos de impresión seleccionados, deberá adaptar este paso a los requisitos de su organización.

Paso	Descripción
73.	Una vez añadido el grupo de seguridad “Administradores delegados de impresión”, localice el grupo y seleccione los siguientes permisos: – Imprimir. – Administrar esta impresora. – Administrar documentos.



74. Una vez establecidos los permisos, pulse “Aceptar” para confirmar los cambios y cerrar la ventana de propiedades del dispositivo de impresión.

3.4 GESTIÓN DE AUDITORIA SOBRE LOS DISPOSITIVOS DE IMPRESIÓN

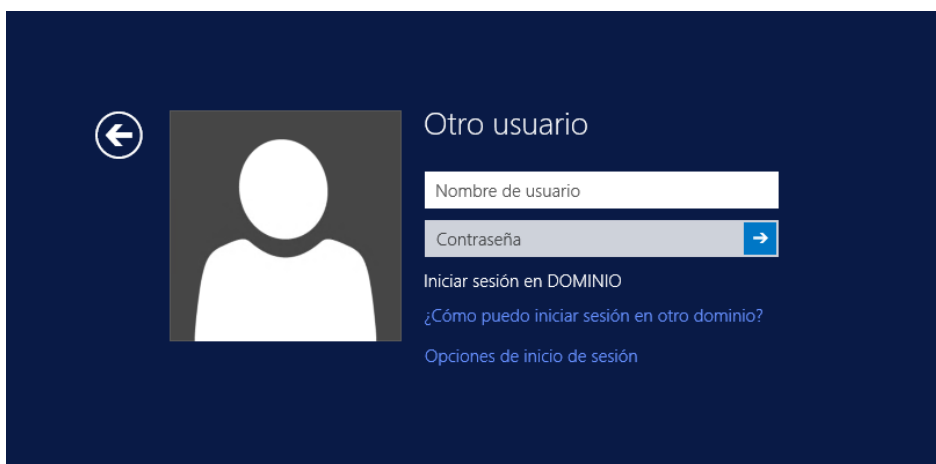
En este apartado se tendrá en consideración la habilitación de la auditoría en los dispositivos de impresión tal y como se especifica para los niveles medio y alto que establece el ENS.

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

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

Paso	Descripción
------	-------------

75. Inicie sesión en el servidor de impresión donde tiene instalados los dispositivos de impresión sobre los cuales se va a aplicar la seguridad según criterios de ENS.

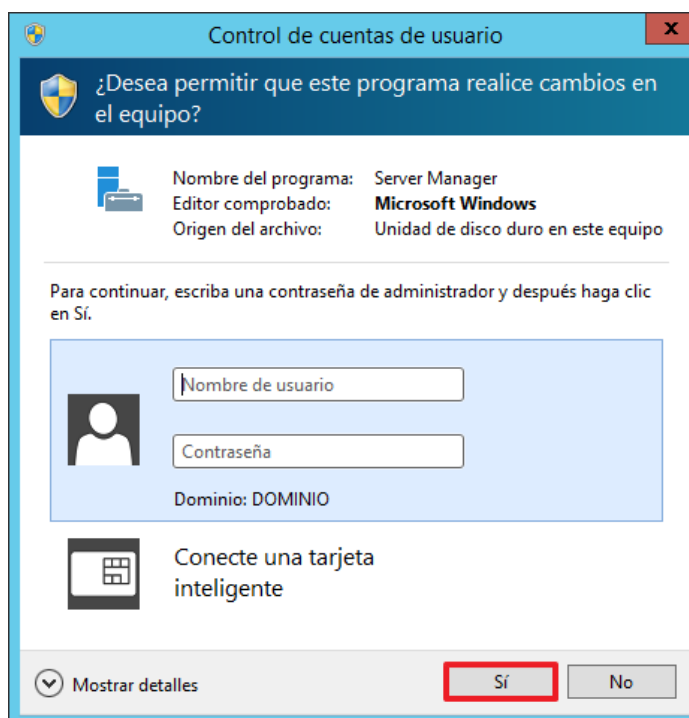


Nota: Inicie sesión con una cuenta con privilegios de Administrador del Dominio.

76. A continuación, deberá iniciar la herramienta "Administración de impresión". Para ello, utilice la herramienta "Administrador del servidor" mediante el icono correspondiente.

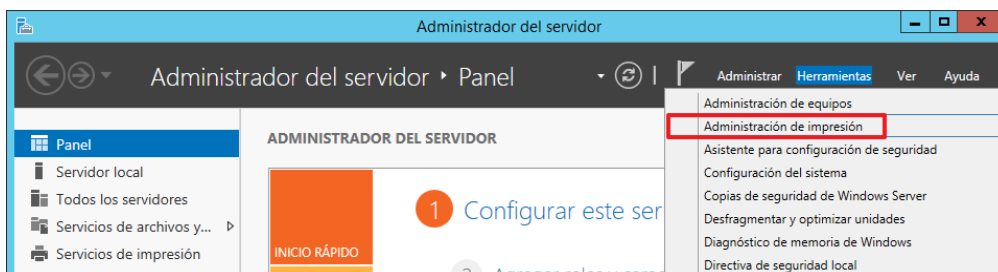


77. El Control de cuentas de usuario le solicitará la elevación de privilegios. Introduzca las credenciales de un usuario con permisos de administrador del dominio y pulse "Sí" para continuar.

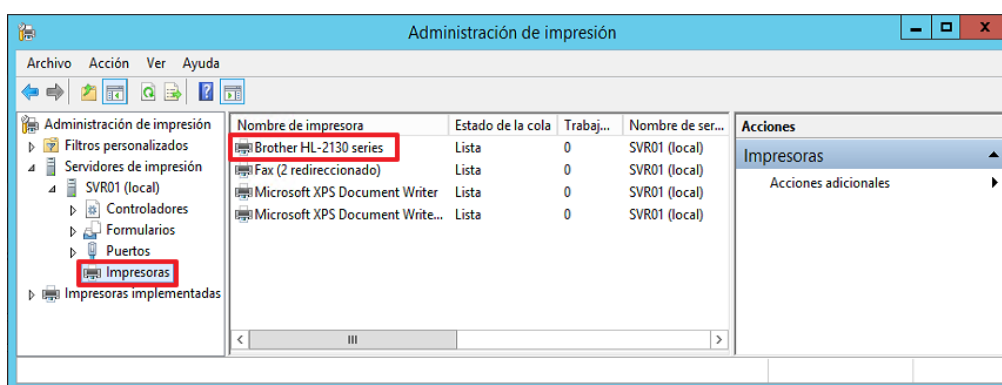


Paso	Descripción
------	-------------

78. Inicie la herramienta “Administración de impresión”. Para ello, sobre el menú superior derecho de la herramienta “Administrador del servidor” seleccione:
“Herramientas → Administración de impresión”

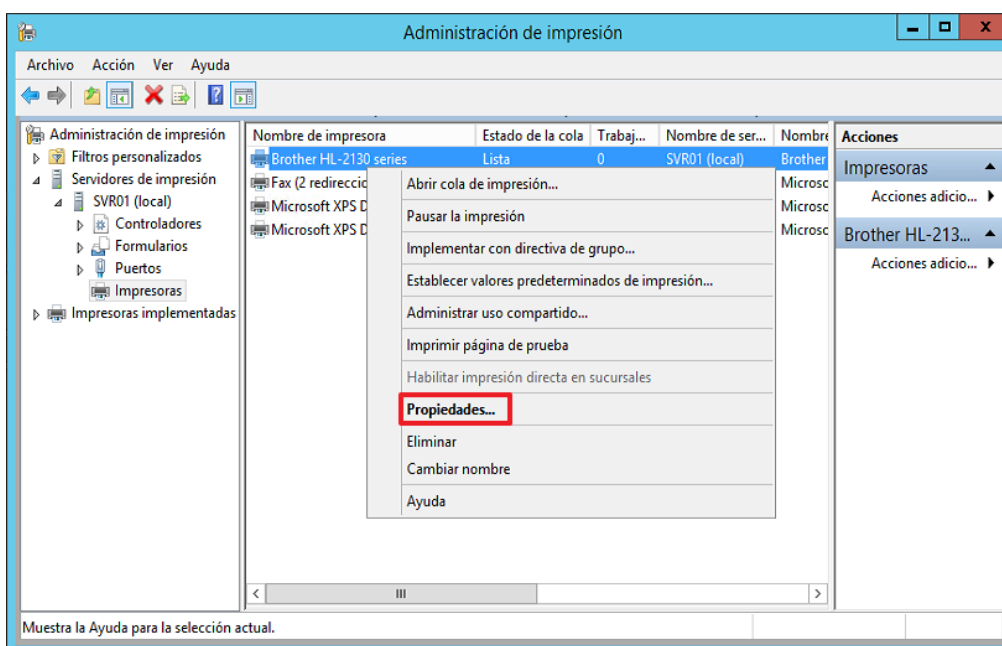


79. Localice el dispositivo de impresión sobre el que se van a aplicar los permisos de gestión.



Nota: En este ejemplo se selecciona el dispositivo de impresión “Brother HL-2130 series”, deberá adaptar los pasos a las necesidades de su organización.

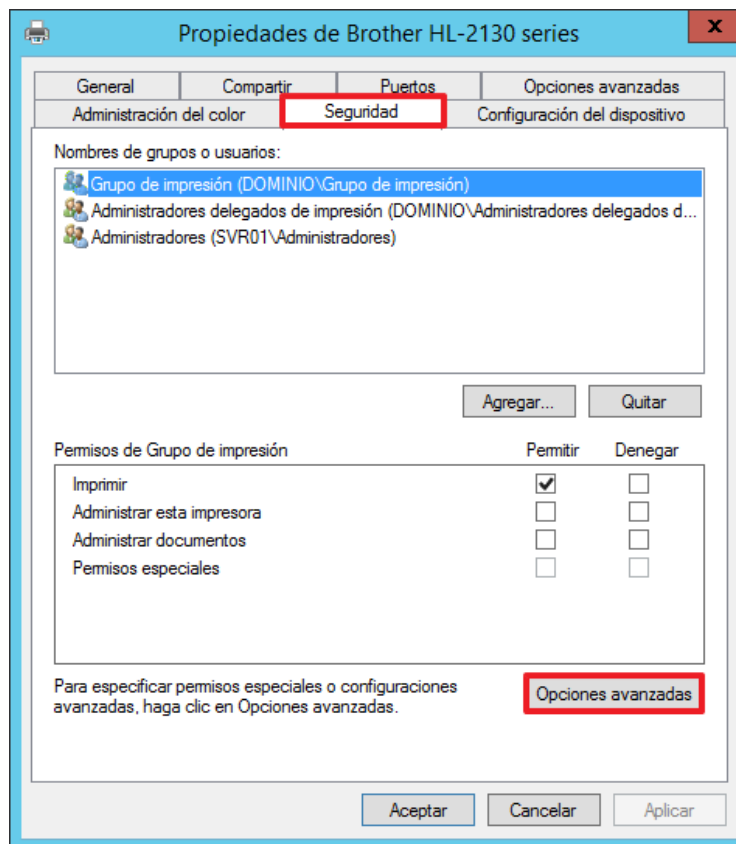
80. Pulse con el botón derecho sobre el dispositivo de impresión y seleccione la opción “Propiedades...”.



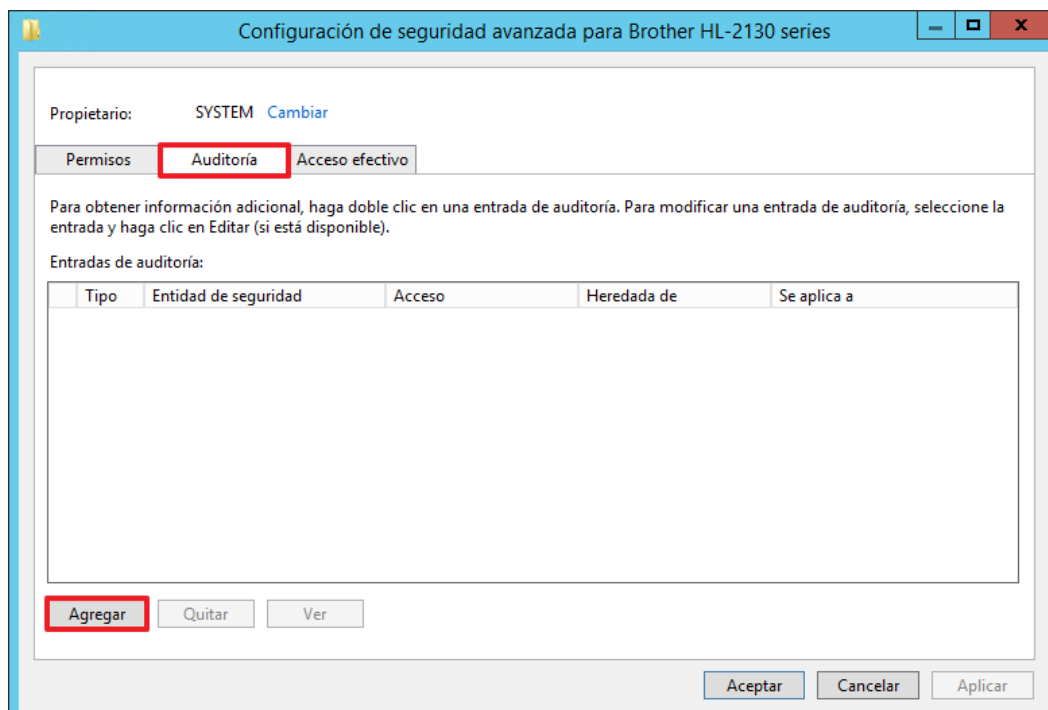
Nota: En este ejemplo se utiliza el dispositivo de impresión denominado “Brother HL-2130 series”.

Paso	Descripción
------	-------------

81. A continuación, seleccione la pestaña “Seguridad” y pulse sobre “Opciones avanzadas”.

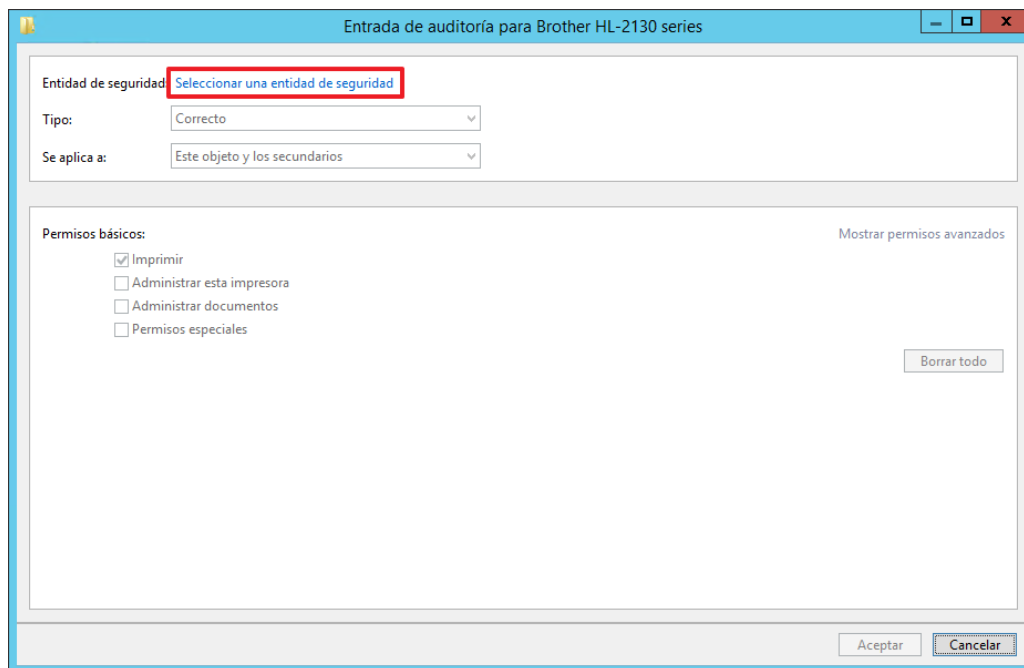


82. Sitúese en la pestaña “Auditoría” y a continuación pulse sobre “Agregar”.

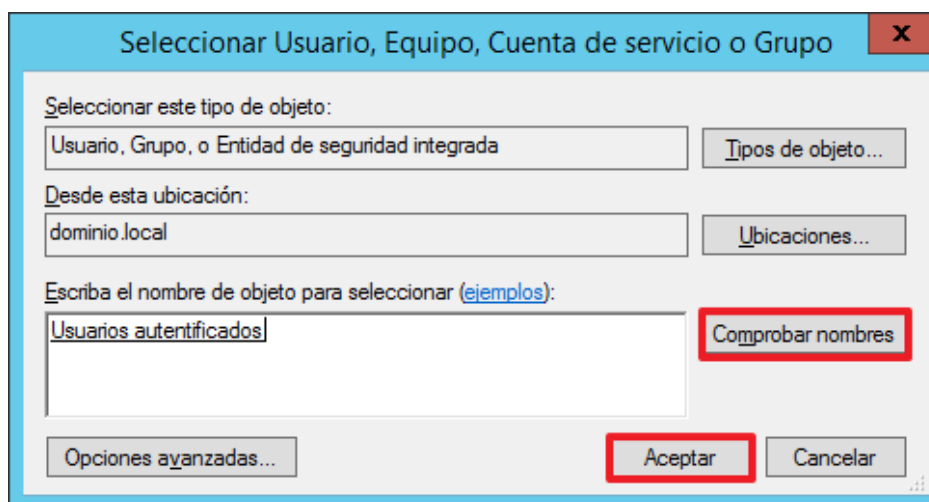


Paso	Descripción
------	-------------

83. Pulse sobre “Seleccionar una entidad de seguridad”.

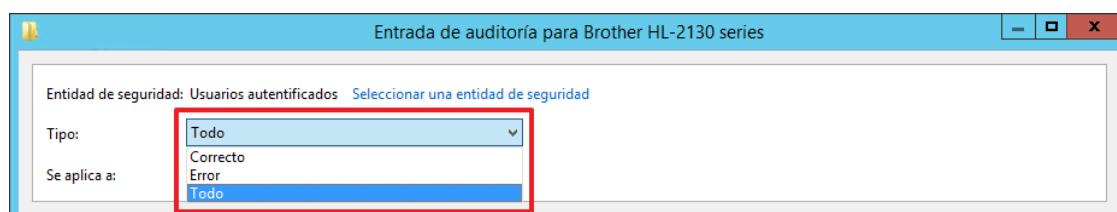


84. Añada los grupos sobre los que desee realizar la auditoría, pulse sobre el botón “Comprobar nombres” y pulse sobre “Aceptar”.



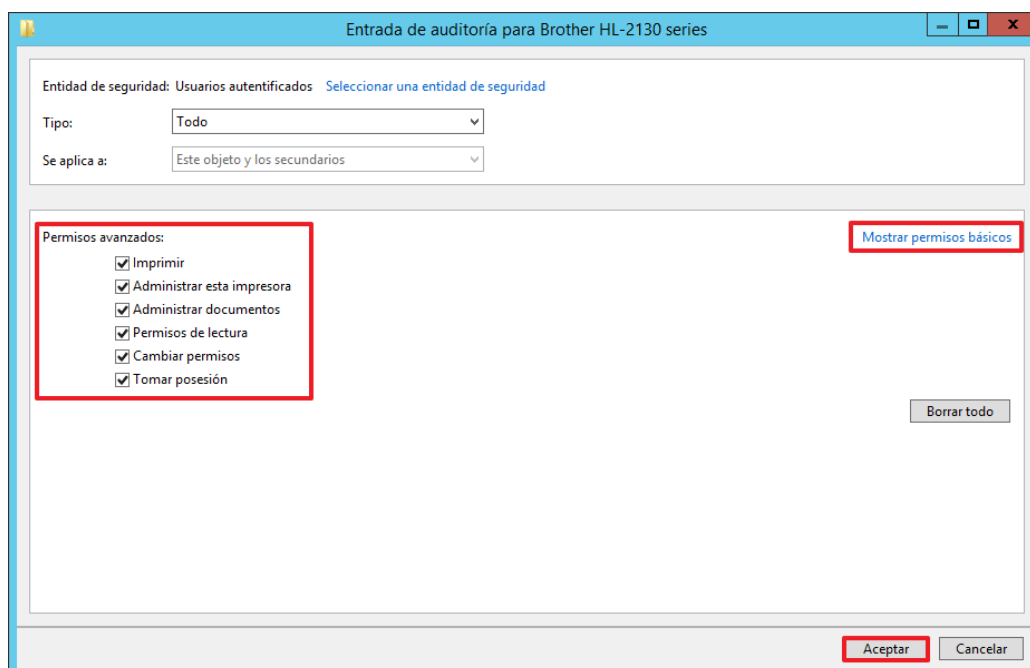
Nota: En este ejemplo se utiliza el grupo “Usuarios autenticados”.

85. En la ventana desplegable “Tipo”, seleccione “Todo”, para que se visualicen tanto los eventos erróneos como los eventos correctos.

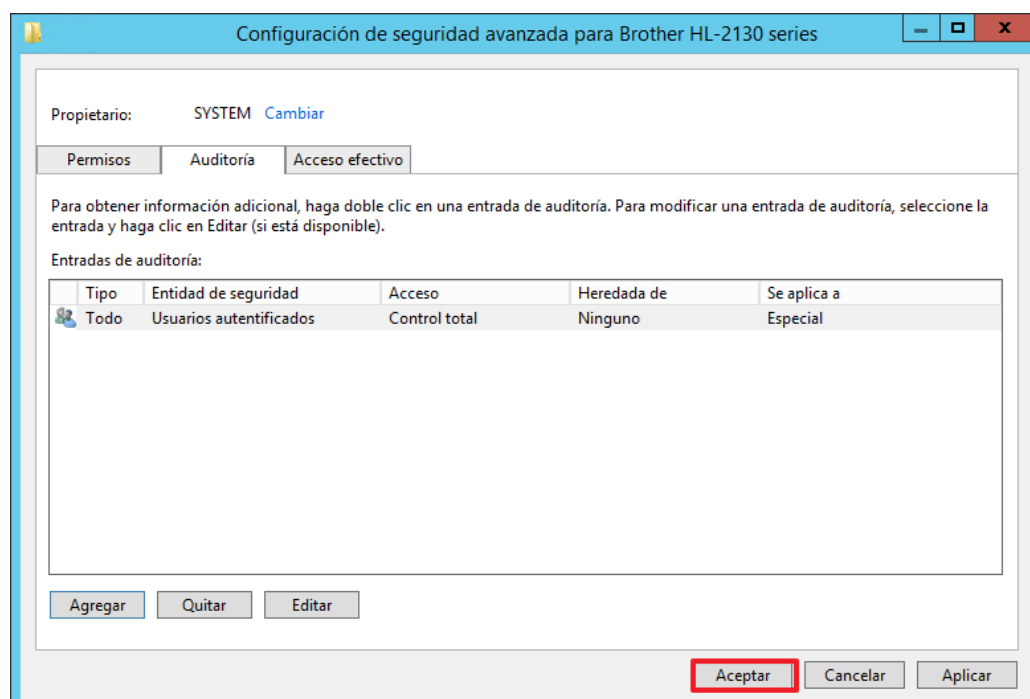


Paso	Descripción
------	-------------

- | | |
|-----|---|
| 86. | En la parte derecha de la ventana, pulse sobre “Mostrar permisos avanzados” y seleccione todas las casillas de eventos auditable, tal y como se muestra en la imagen. Pulse sobre el botón “Aceptar”. |
|-----|---|



- | | |
|-----|---|
| 87. | Pulse de nuevo sobre el botón “Aceptar” para cerrar la configuración de seguridad avanzada de la impresora. |
|-----|---|



- | | |
|-----|--|
| 88. | Pulse, finalmente, “Aceptar” para cerrar la ventana de “Propiedades” de la impresora. |
| 89. | Repita estos mismos pasos para cada uno de los dispositivos de impresión que deben ser auditados en su organización. |

4. GESTIÓN DE ROLES Y/O CARACTERÍSTICAS DEL SISTEMA

Estos paso a paso se deberán aplicar para instalar o desinstalar roles y/o características implementadas en un servidor miembro del dominio, que le sea de aplicación la guía de securización “CCN-STIC-870A - Implementación del ENS en Microsoft Windows Server 2012 R2” en su nivel medio o nivel alto del ENS.

Si no desea gestionar los roles y/o características del sistema, no continúe con el paso a paso definido en las siguientes subsecciones.

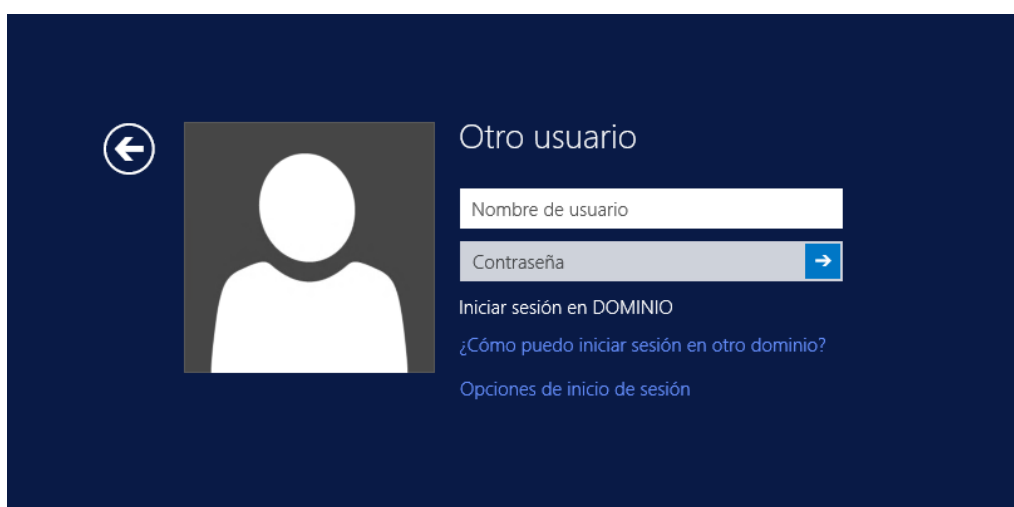
4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO

Para instalar o eliminar un rol y/o característica será necesario la creación de una política de seguridad temporal para tal efecto.

Los pasos que se describen a continuación se realizarán en un Controlador de Dominio del directorio activo al que va a pertenecer el servidor miembro que se está securizando.

Nota: Recuerde que una vez instalados o eliminados los roles y/o características necesarias deberá aplicar el paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

Paso	Descripción
90.	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.

91. 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.

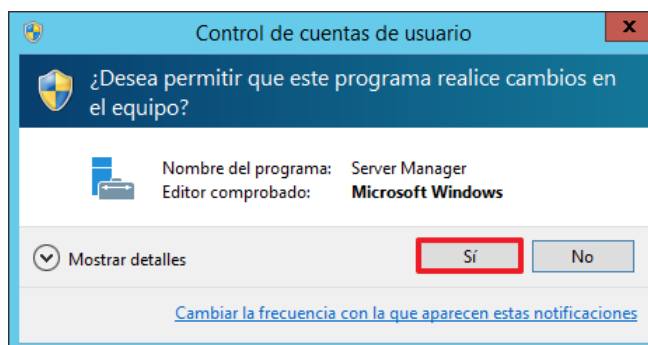
92. Copie los scripts y plantillas de seguridad asociadas a esta guía en el directorio “C:\Scripts”.

93. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



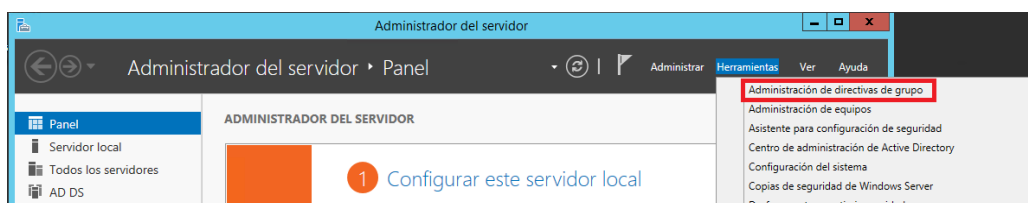
Paso	Descripción
------	-------------

94. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.

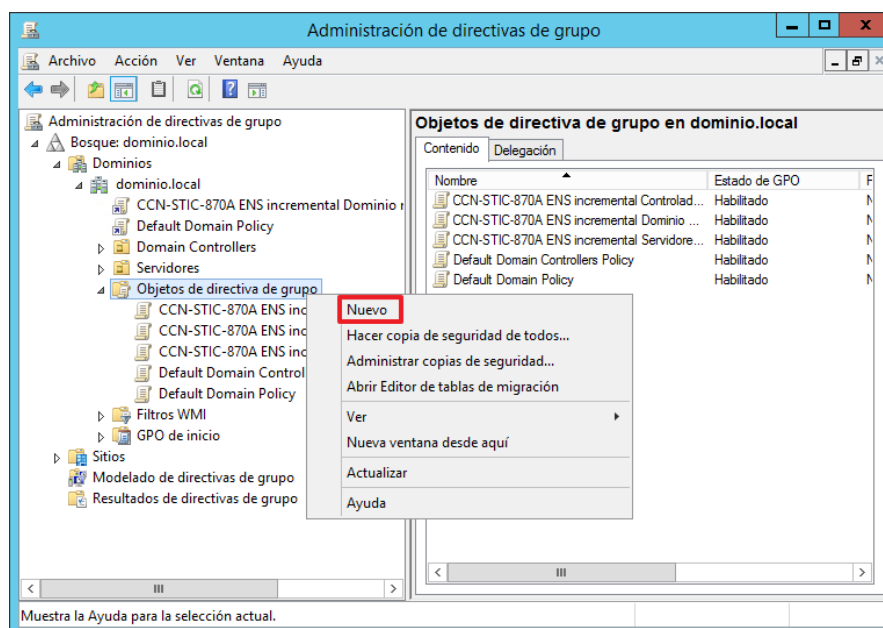


Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios podrá solicitar credenciales para continuar.

95. Inicie la herramienta “Administración 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”

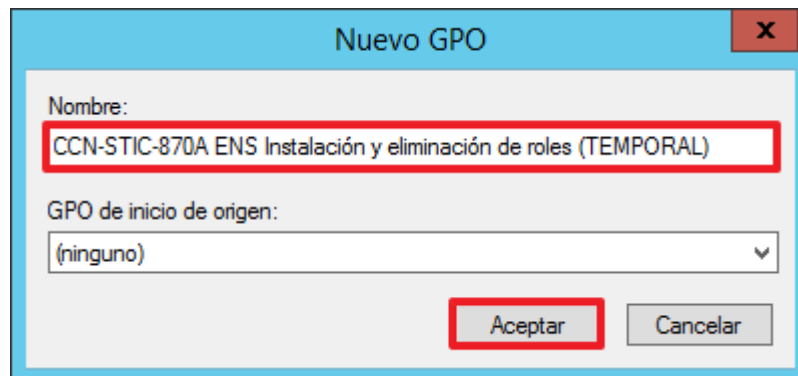


96. Ubíquese sobre el nodo “Objetos de directiva de grupo” ubicado en “Bosque:<su dominio> / Dominios / <su dominio> / Objetos de directiva de grupo”.
97. Si ya estuviese creada la directiva de grupo “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” deberá continuar a partir del paso 108.
98. Pulse con el botón derecho, sobre dicha carpeta y seleccione la opción “Nuevo”.

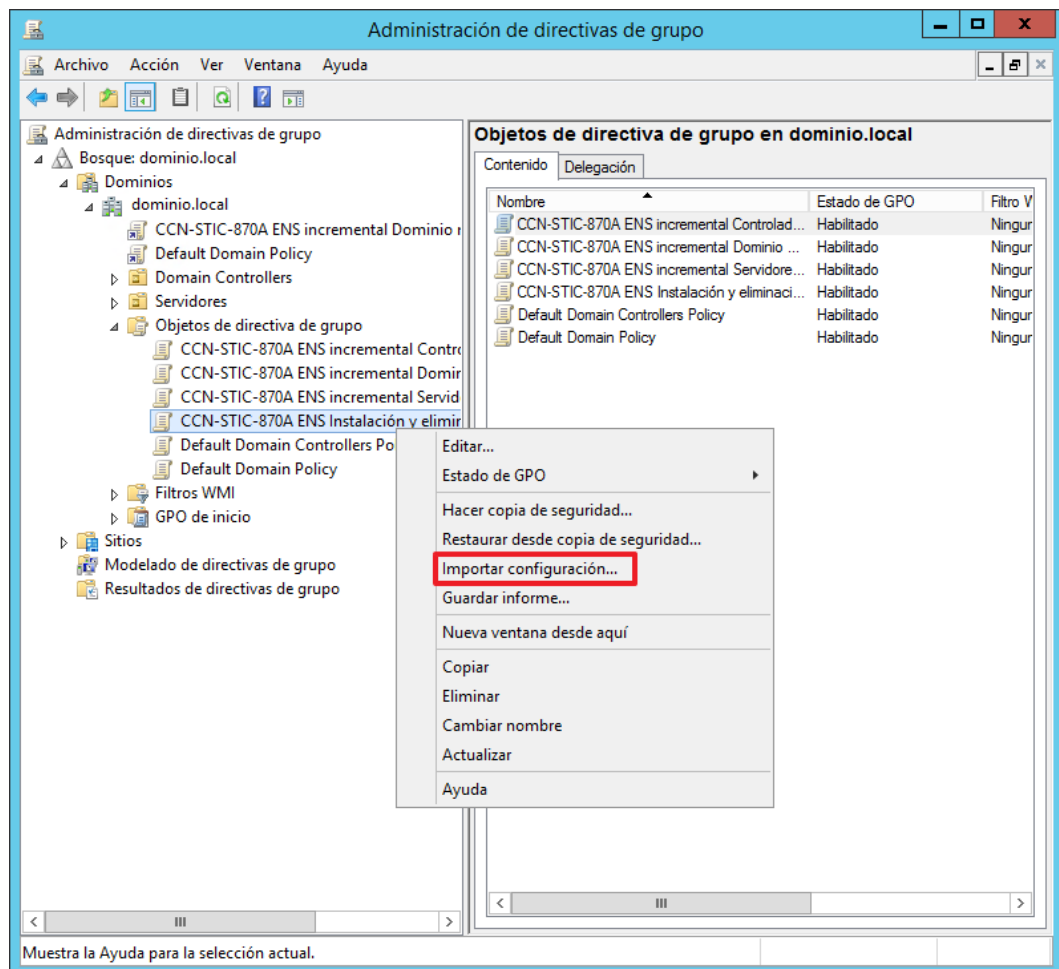


Paso	Descripción
------	-------------

99. Introduzca como nombre “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” y pulse el botón “Aceptar”.



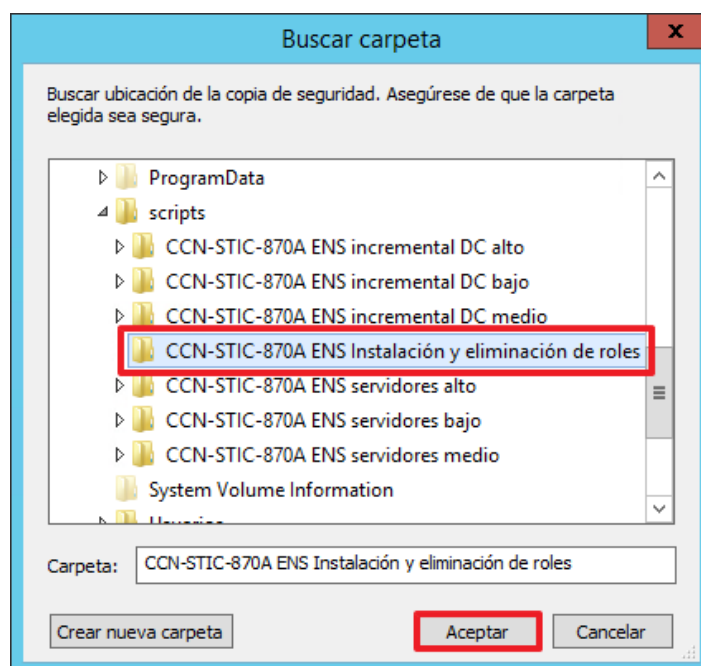
100. Seleccione la política recién creada, pulse con el botón derecho sobre la misma y seleccione la opción “Importar configuración...”.



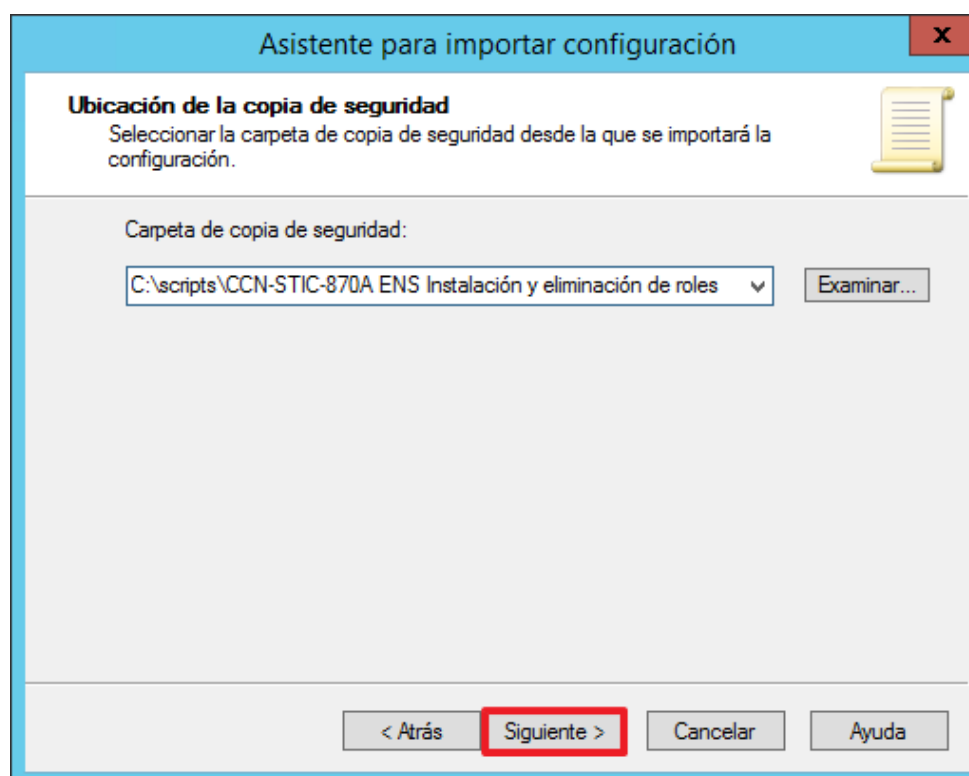
101. En el asistente de importación de configuración, pulse el botón “Siguiente >”.

102. En “Carpeta de copia de seguridad”, pulse el botón “Examinar...”.

Paso	Descripción
103.	Seleccione la carpeta “CCN-STIC-870A ENS Instalación y eliminación de roles” que encontrará en la carpeta “C:\Scripts” y pulse el botón “Aceptar”.

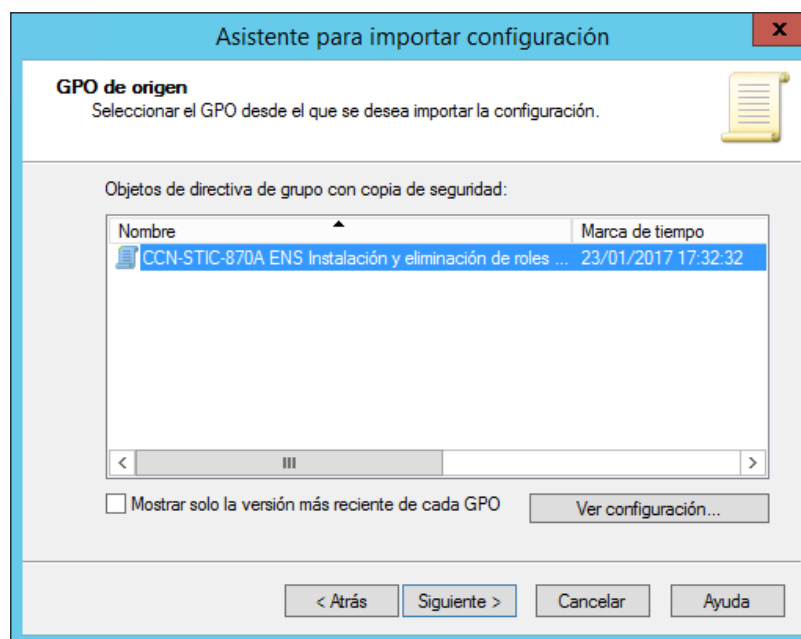


104. Pulse el botón “Siguiente >” una vez seleccionada la carpeta adecuada.

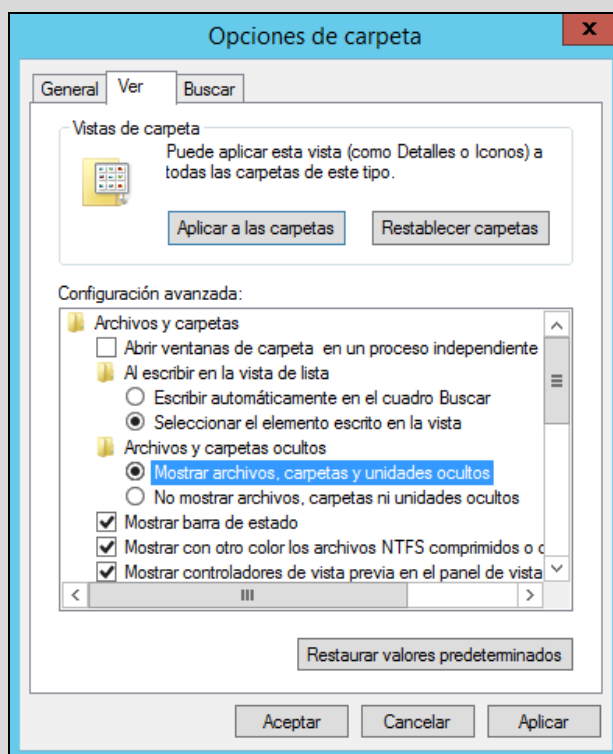


Paso	Descripción
------	-------------

105. En la pantalla siguiente compruebe que aparece la política de seguridad “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” 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 mostrar en “opciones de carpeta” la opción “Mostrar archivos, carpetas y unidades ocultos”.

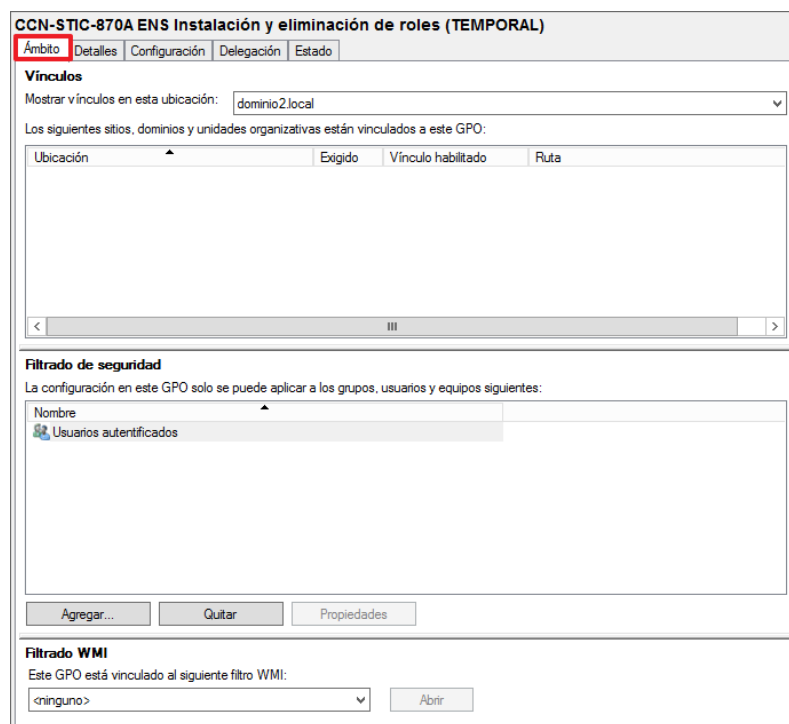


106. En la pantalla de examen, pulse el botón “Siguiente >”.

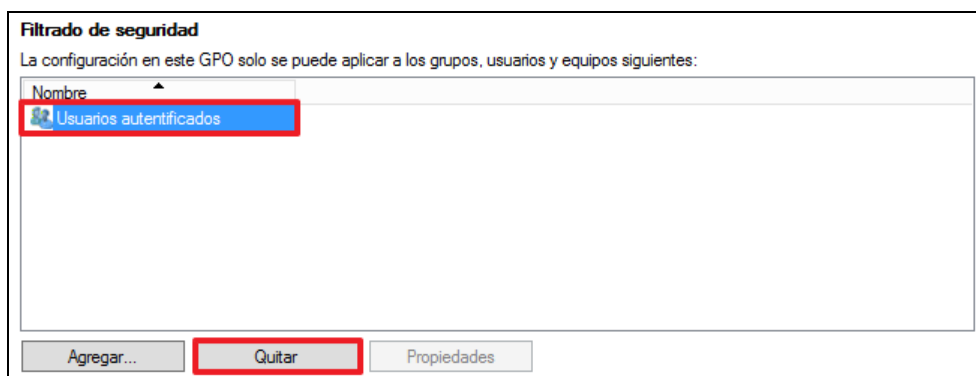
107. Para completar el asistente pulse el botón “Finalizar”.

Paso	Descripción
------	-------------

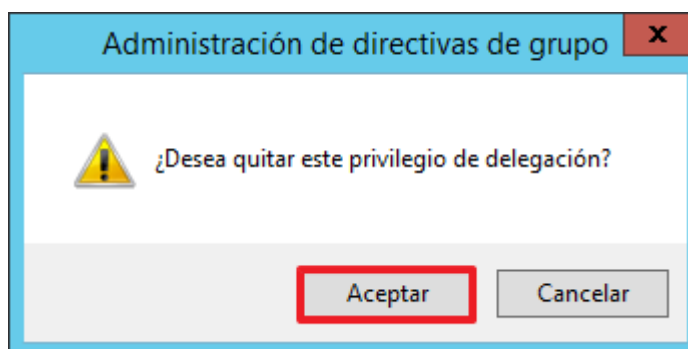
108. A continuación, seleccione la nueva política de grupo configurada y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho.



109. En la opción de filtrado de seguridad, seleccione “Usuarios autenticados” y pulse la opción “Quitar”.

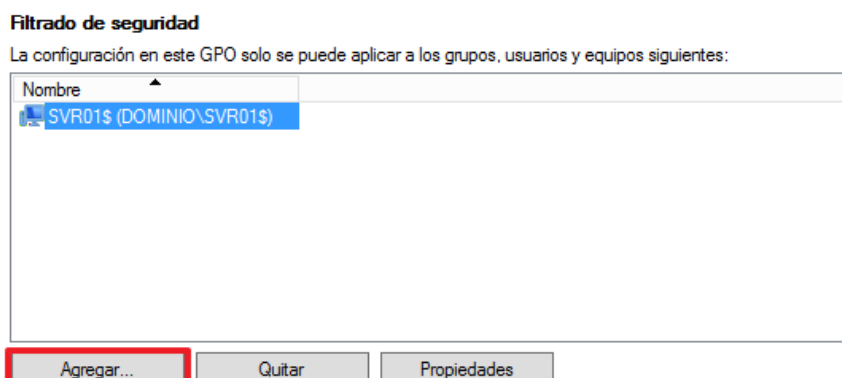


110. A continuación, pulse el botón “Aceptar” cuando le pregunte si desea quitar este privilegio de delegación.



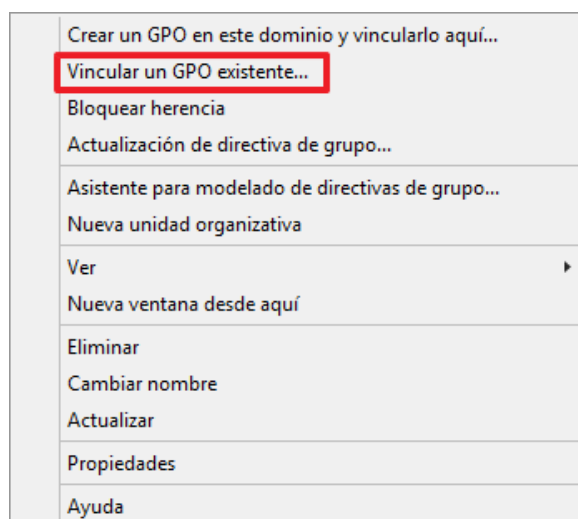
Paso	Descripción
------	-------------

111. Una vez quitado, pulse el botón “Agregar...” y seleccione únicamente los equipos o grupos sobre los que desea aplicar la política de seguridad.



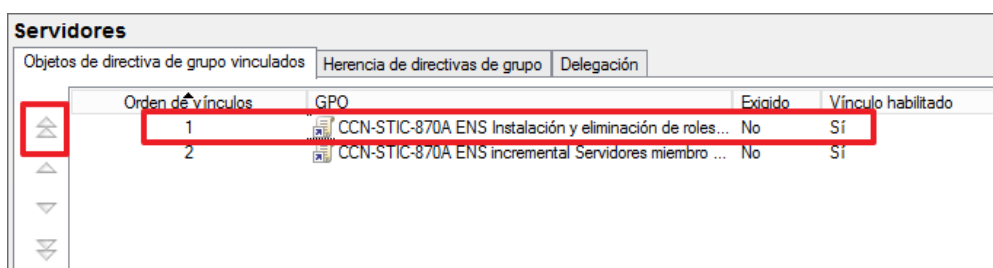
Nota: En este ejemplo se agrega el equipo “SVR01”.

112. A continuación, identifique las unidades organizativas en la que desea instalar o eliminar algún rol y/o característica. Pulse con el botón derecho sobre la unidad organizativa deseada y seleccione la opción del menú contextual “Vincular un GPO existente...”.



Nota: En este ejemplo se selecciona la unidad organizativa “Servidores”.

113. Una vez vinculado, en el panel derecho seleccione la pestaña “Objetos de directiva de grupo vinculados” y seleccione la política “CCN-STIC 870A ENS Instalación y eliminación de roles”
114. Pulse el botón con la flecha que apunta hacia arriba hasta situar la política “CCN-STIC 870A ENS Instalación y eliminación de roles” en primer lugar dentro del orden de vinculación.



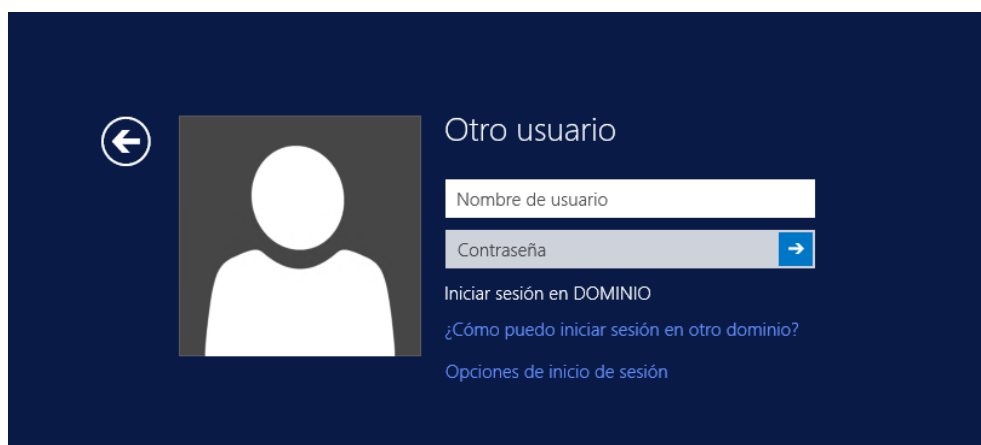
4.2 INSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO”.

Paso	Descripción
------	-------------

115. Inicie sesión en el servidor miembro donde vaya a instalar un rol y/o característica.

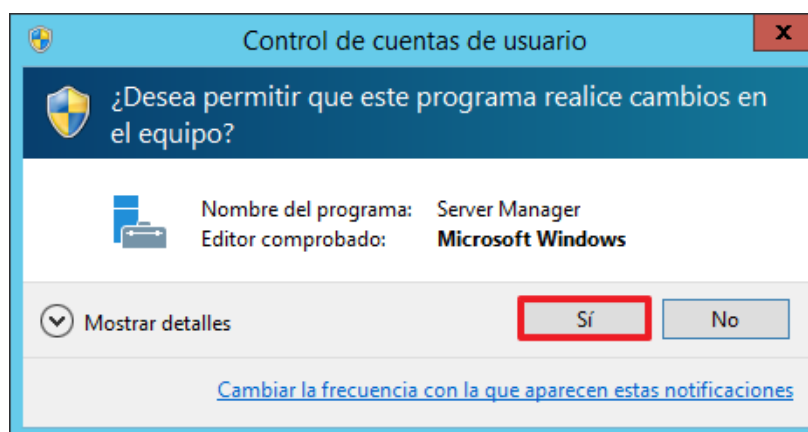


Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

116. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



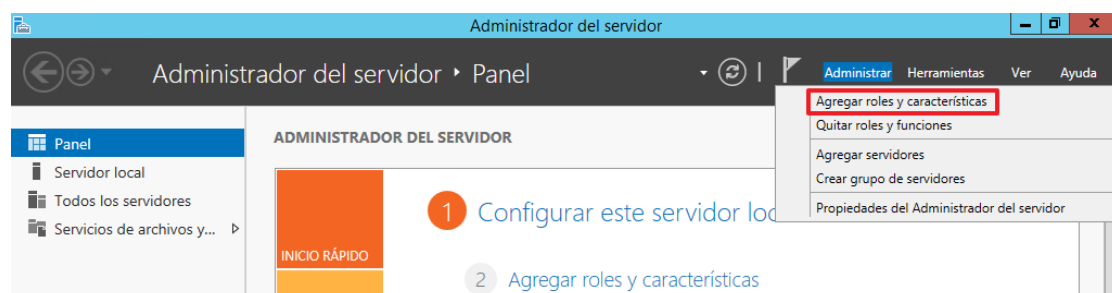
117. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



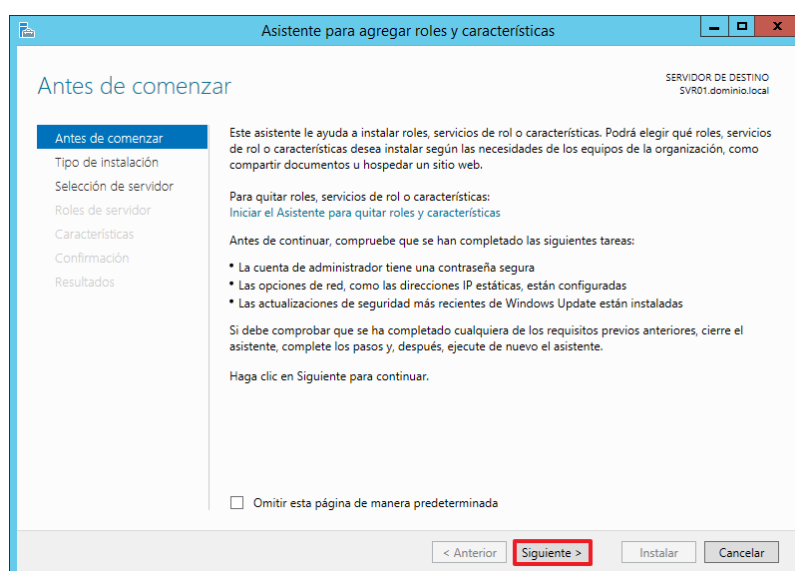
Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios podrá solicitar credenciales para continuar.

Paso	Descripción
------	-------------

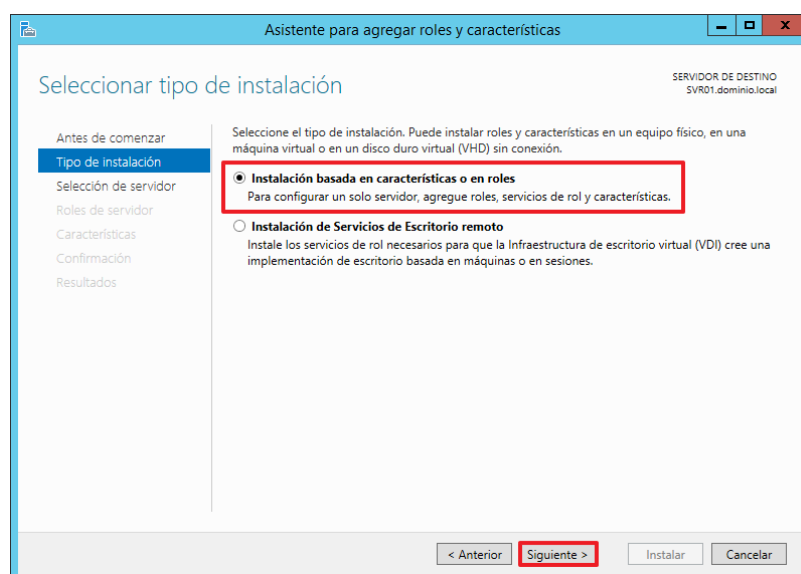
118. A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Agregar roles y características”.



119. Comenzará el asistente para agregar roles y características. Pulse sobre el botón “Siguiente >” para continuar.

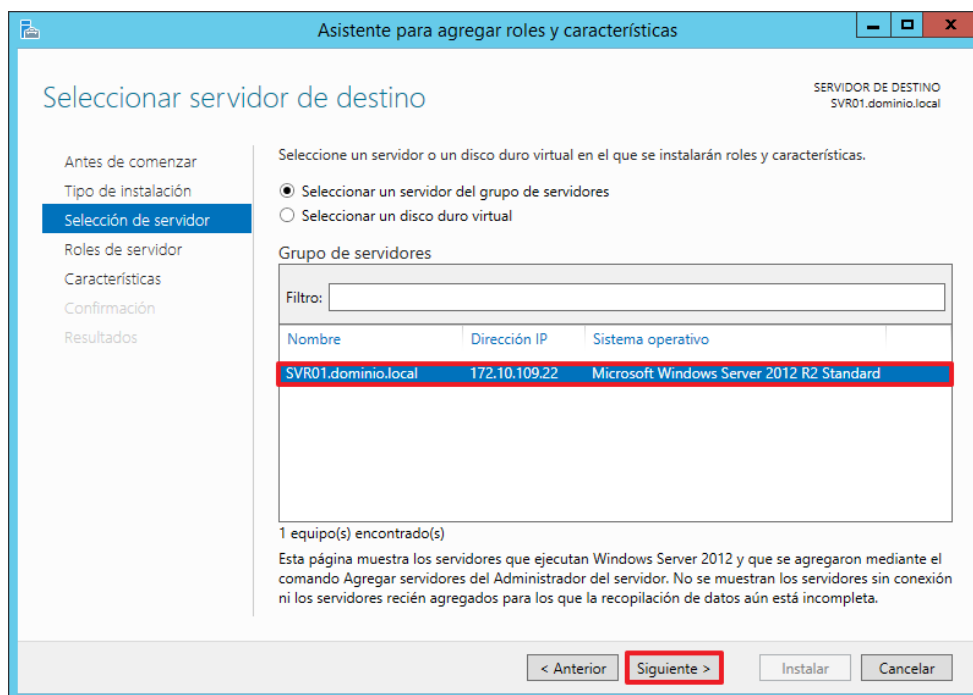


120. Seleccione el tipo de instalación, “Instalación basada en características o roles” y pulse “Siguiente ->” para continuar.



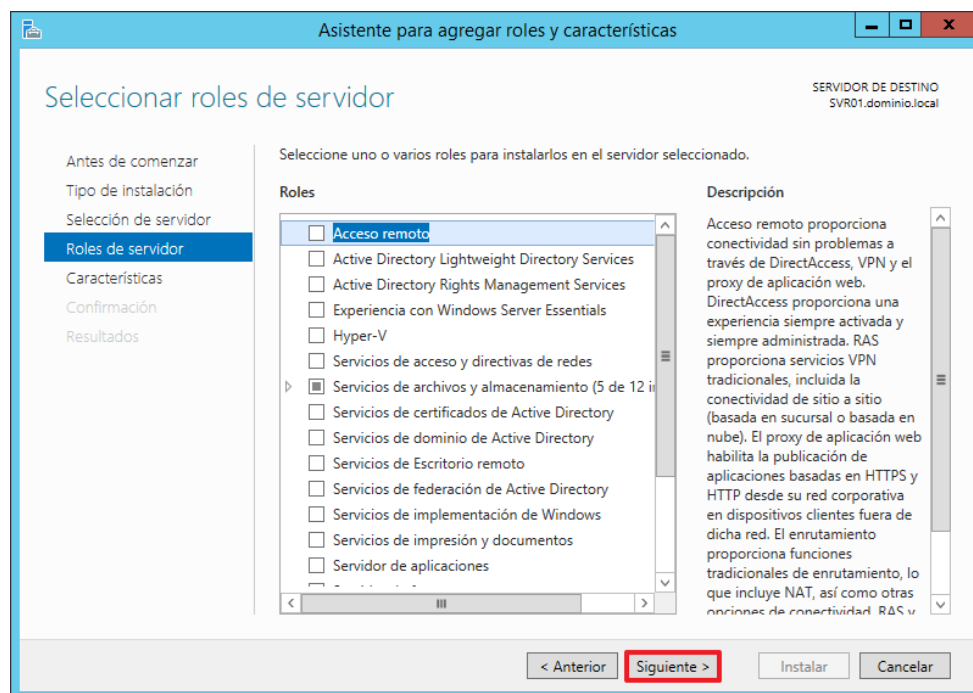
Paso	Descripción
------	-------------

- | | |
|------|---|
| 121. | Seleccione el servidor sobre el cual desea instalar un rol o una característica, y pulse “Siguiente >”. |
|------|---|



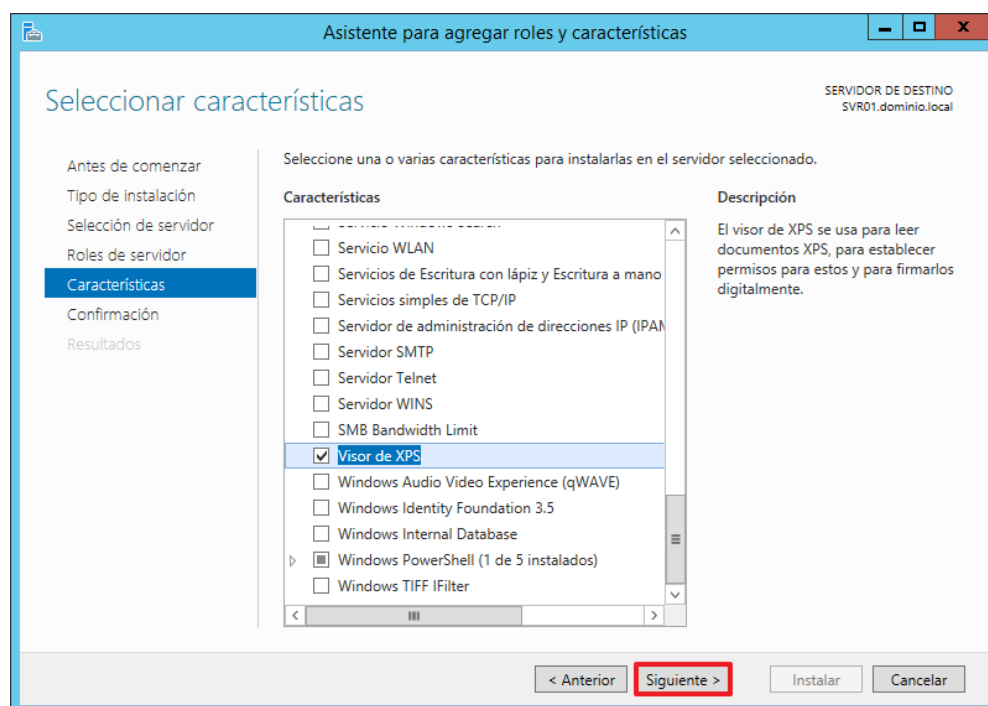
Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

- | | |
|------|---|
| 122. | En la siguiente ventana, seleccione los roles que desee instalar en el sistema y pulse “Siguiente >”. |
|------|---|



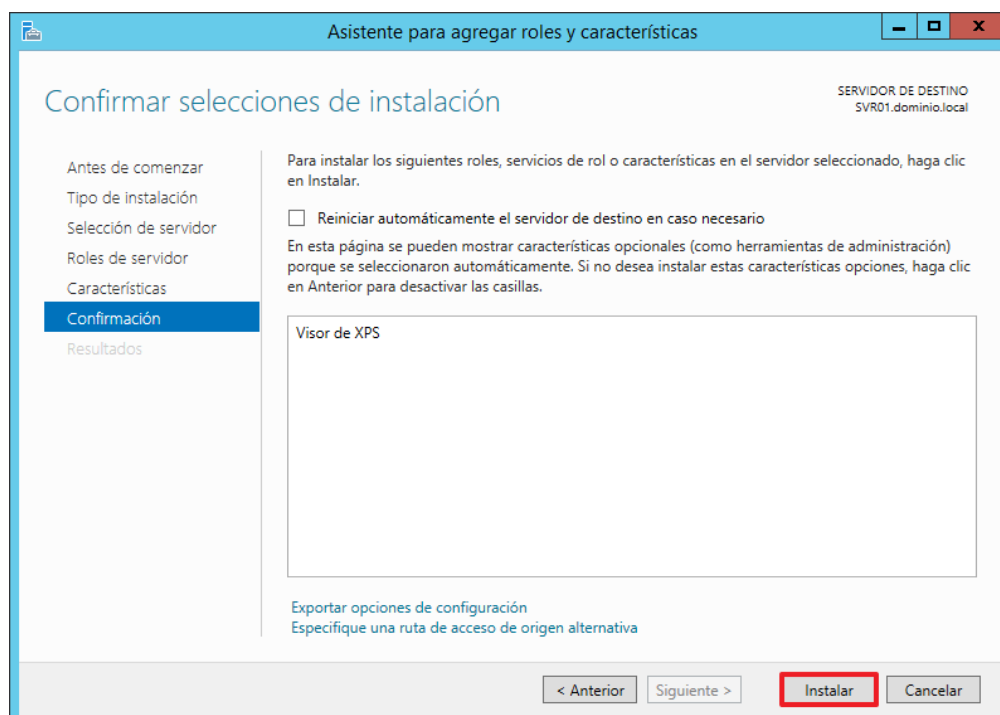
Paso	Descripción
------	-------------

- | | |
|------|--|
| 123. | A continuación, en la siguiente ventana podrá seleccionar las características que desee instalar en el sistema. Seleccione aquellas que desee instalar y pulse “Siguiente ->”. |
|------|--|

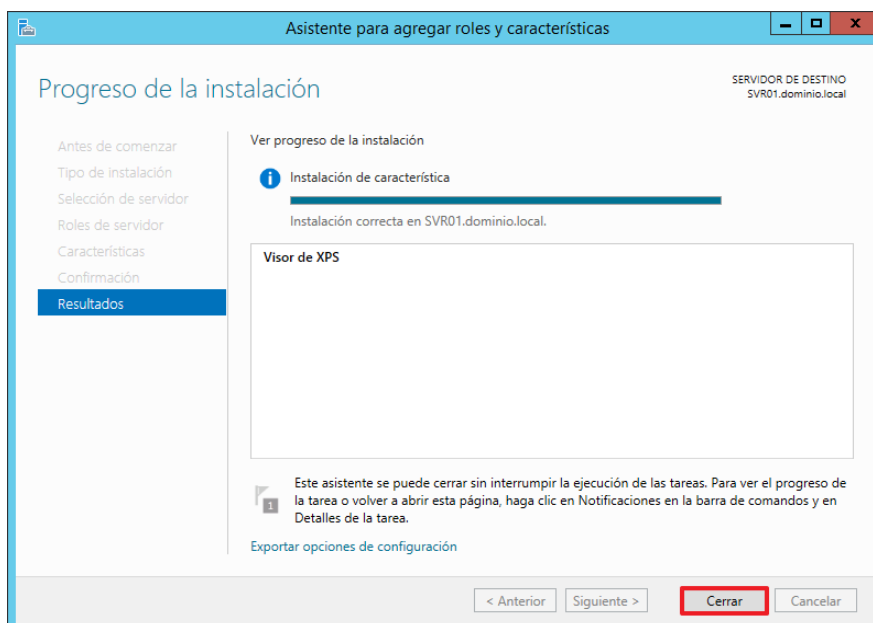


Nota: En este ejemplo se instala la característica “Visor de XPS”, deberá adaptar este paso a los requerimientos de su organización.

- | | |
|------|--|
| 124. | En la ventana “Confirmación” pulse “Instalar” para iniciar el proceso. |
|------|--|



Paso	Descripción
125.	Una vez finalizado el proceso de instalación, pulse sobre “Cerrar” para finalizar la instalación.



Nota: En caso de ser necesario, el servidor requerirá un reinicio para finalizar la instalación de roles y características.

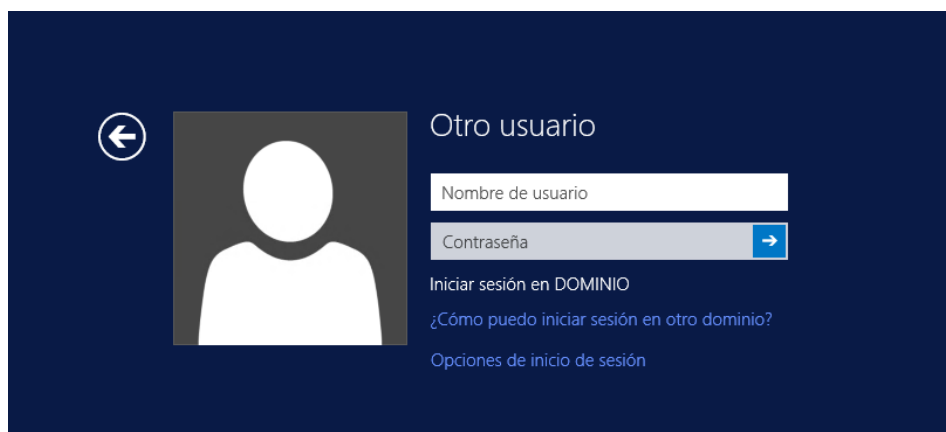
126. Una vez finalizada la instalación de roles y/o características, deberá aplicar el siguiente paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

4.3 DESINSTALACIÓN DE ROLES Y/O CARACTERÍSTICAS

Los pasos que se describen a continuación se realizarán en el servidor miembro del dominio que se está securizando.

Nota: Para continuar este paso a paso debe haber aplicado previamente el punto “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO”.

Paso	Descripción
127.	Inicie sesión en el servidor miembro donde vaya a eliminar un rol y/o característica.



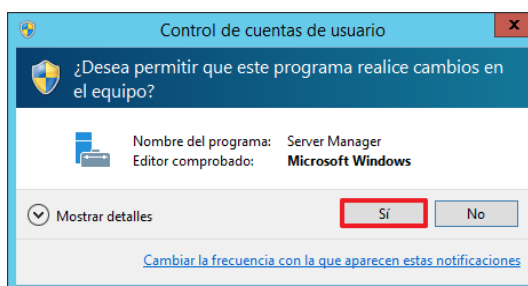
Nota: Inicie sesión con una cuenta que sea Administrador del Dominio o Administrador local del equipo.

Paso	Descripción
------	-------------

128. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.

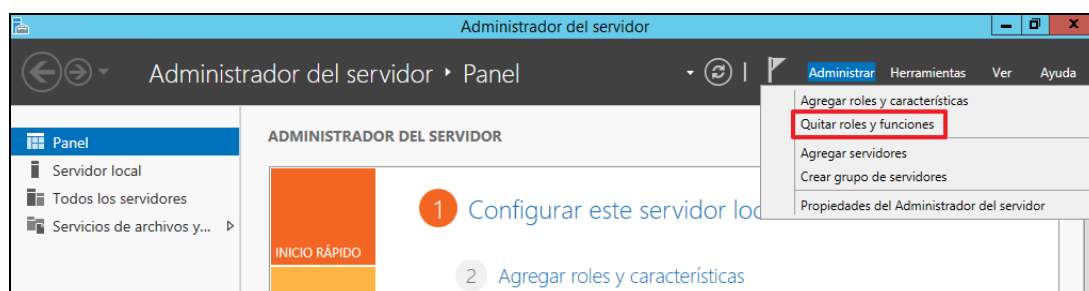


129. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.

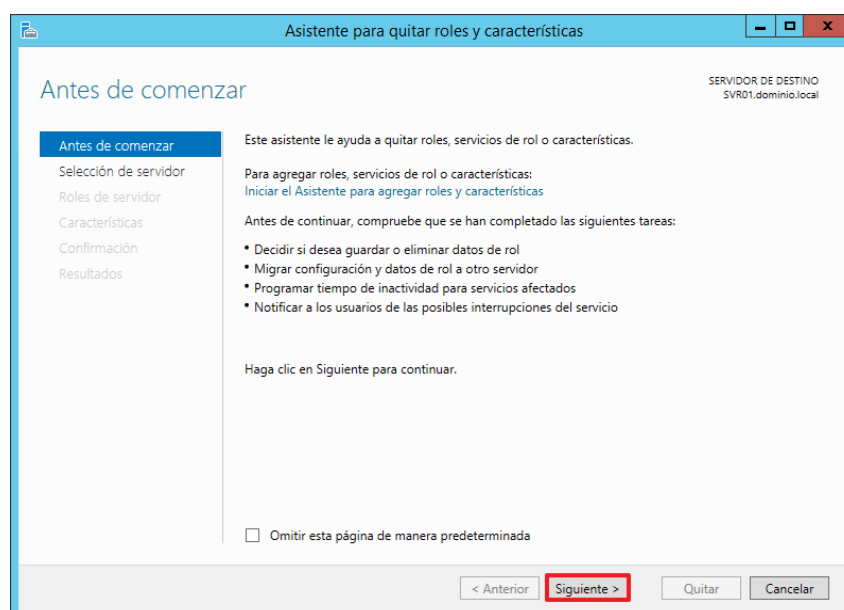


Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios le podrá solicitar credenciales para continuar.

130. A continuación, pulse sobre el botón “Administrar” y seleccione la opción “Quitar roles y funciones”.

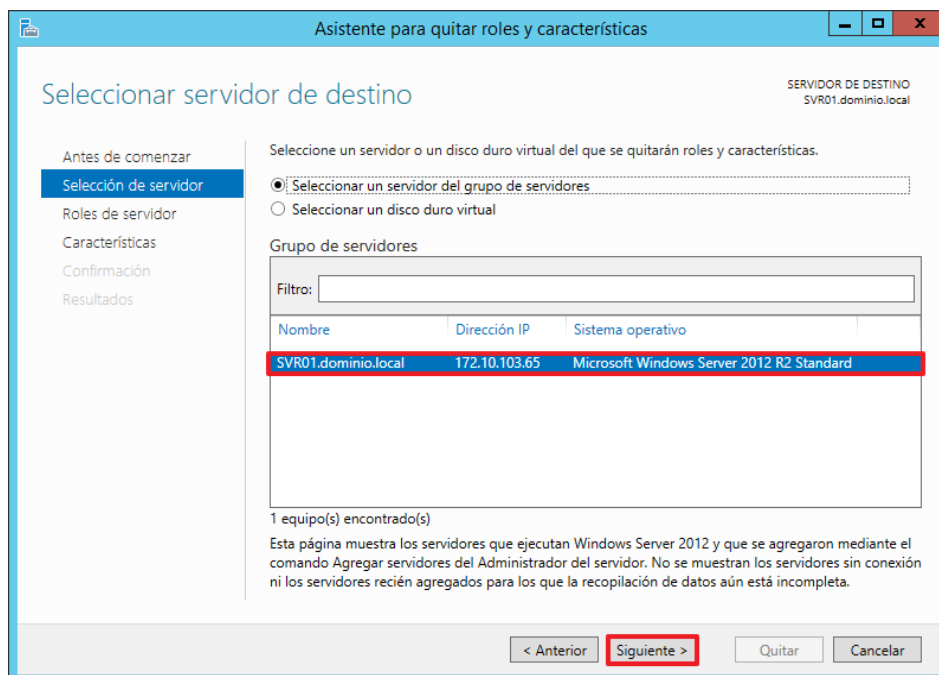


131. Comenzará el asistente para quitar roles y características. Pulse sobre el botón “Siguiente >” para continuar.



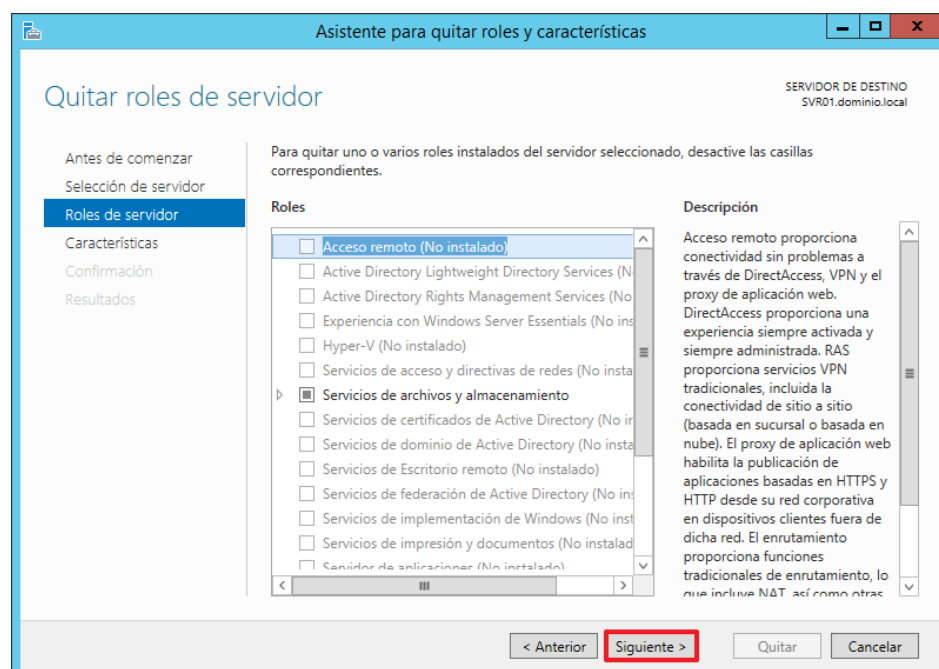
Paso	Descripción
------	-------------

- | | |
|------|--|
| 132. | Seleccione el servidor sobre el cual desea eliminar un rol o una característica y pulse “Siguiente >”. |
|------|--|



Nota: En este ejemplo se utiliza el servidor con el nombre “SVR01”.

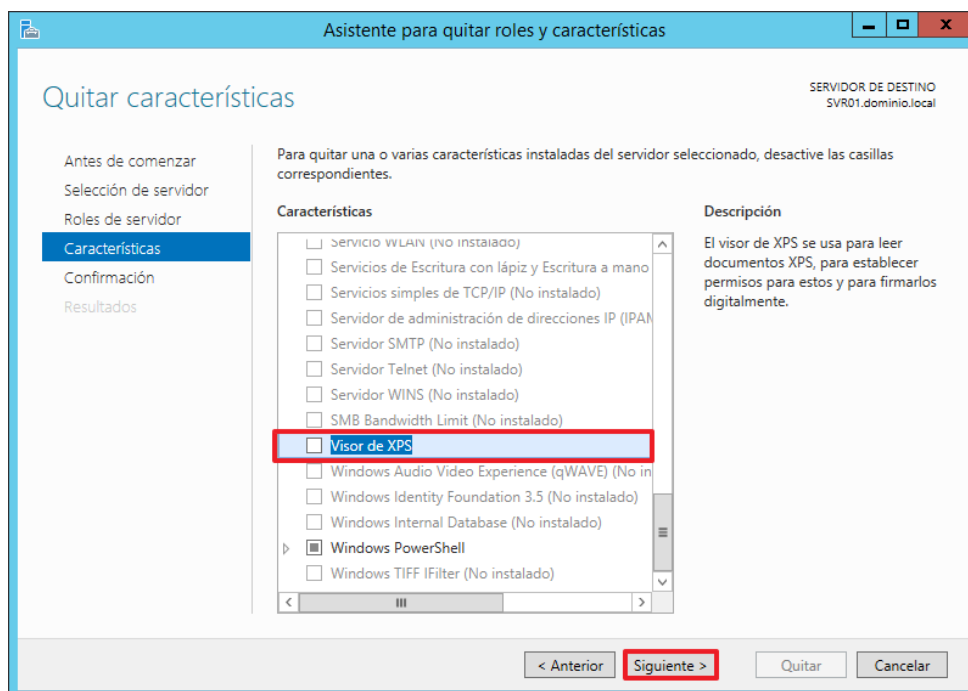
- | | |
|------|--|
| 133. | En la siguiente ventana se podrán eliminar los roles que estén instalados en el sistema. Desmarque aquellos que desee desinstalar y pulse “Siguiente >”. |
|------|--|



Nota: En este ejemplo no se desinstala ningún rol, deberá adaptar este paso a los requerimientos de su organización.

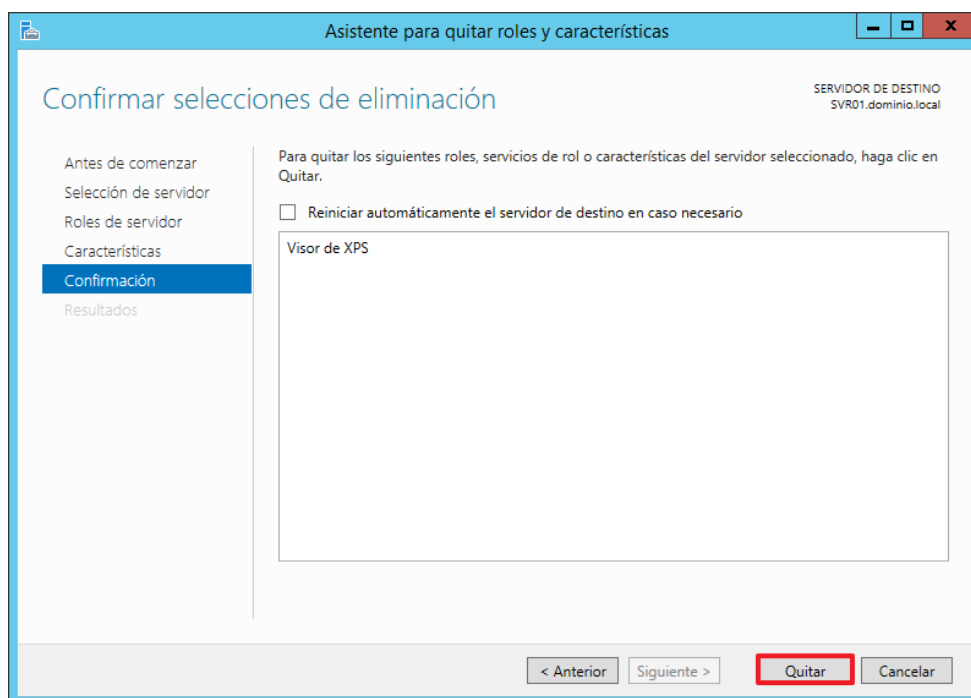
Paso	Descripción
------	-------------

134. A continuación, en la siguiente ventana podrá seleccionar las características que desee desinstalar del sistema. Desmarque aquellas que desee desinstalar y pulse “Siguiente ->”.



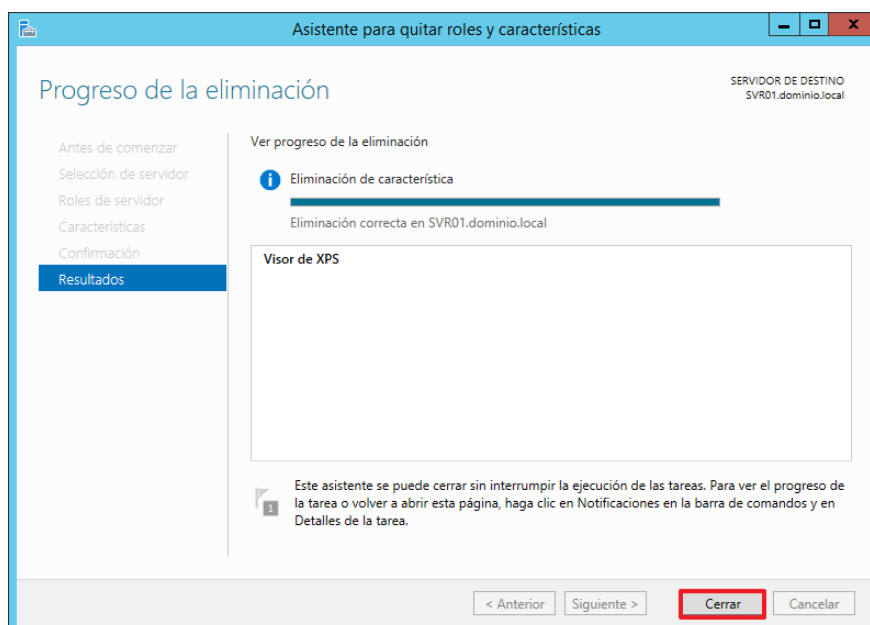
Nota: En este ejemplo se desinstala la característica “Visor de XPS”, deberá adaptar este paso a los requerimientos de su organización.

135. En la ventana “Confirmación” pulse “Quitar” para iniciar el proceso.



Paso	Descripción
------	-------------

136. Una vez finalizado el proceso de desinstalación, pulse sobre “Cerrar” para finalizar la desinstalación.



Nota: En caso de ser necesario el servidor requerirá un reinicio para finalizar la desinstalación de roles y características.

137. Una vez finalizada la desinstalación de roles y/o características, deberá aplicar el siguiente paso “4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO”.

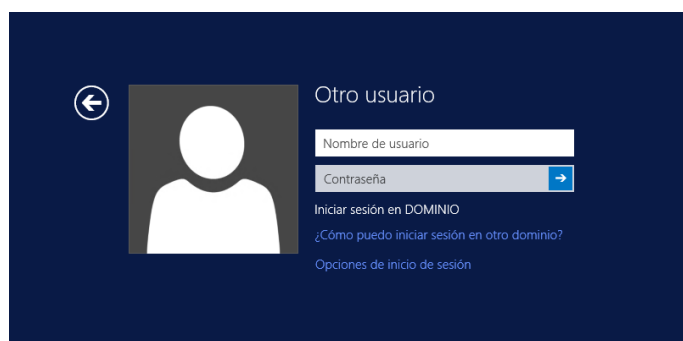
4.4 DESVINCULACIÓN DE UNA POLÍTICA DE GRUPO

Para desvincular o eliminar la GPO “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” creada en el paso “4.1 PREPARACIÓN DEL DIRECTORIO ACTIVO” deberá implementar el siguiente paso a paso.

Los pasos que se describen a continuación se realizarán en un Controlador de Dominio del dominio al que va a pertenecer el servidor miembro que se está securizando.

Paso	Descripción
------	-------------

138. Inicie sesión en un servidor Controlador de Dominio del dominio donde se va aplicar seguridad según criterios de ENS.



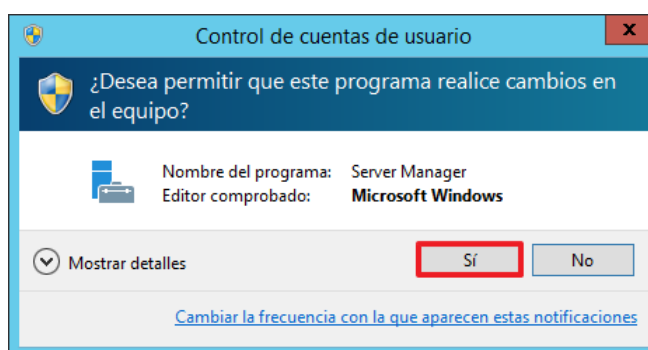
Nota: Deberá iniciar sesión con una cuenta que sea Administrador del Dominio.

Paso	Descripción
------	-------------

139. Abra el “Administrador del servidor”. Para ello pulse sobre el botón correspondiente en la barra de tareas.



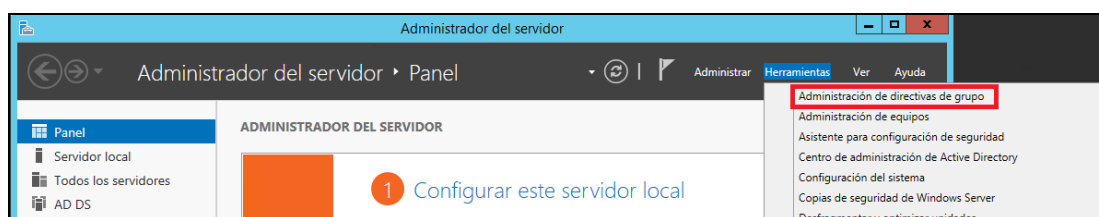
140. El “Control de cuentas de usuario” le solicitará la elevación de privilegios. Pulse “Sí” para continuar.



Nota: Dependiendo del nivel de ENS que se aplique sobre el servidor que se está securizando la elevación de privilegios podrá solicitar credenciales para continuar.

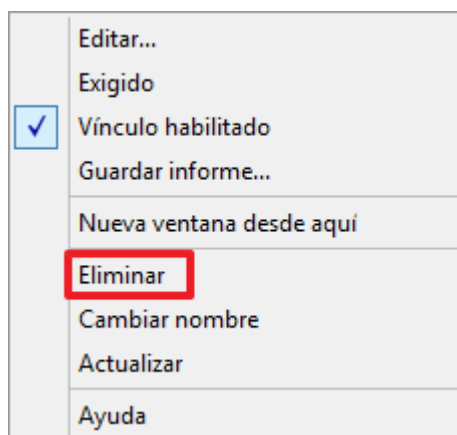
141. Inicie la herramienta “Administración de Directivas de Grupo”. Para ello, sobre el menú superior de la derecha de la herramienta “Administrador del servidor” seleccione:

“Herramientas → Administración de directivas de grupo”



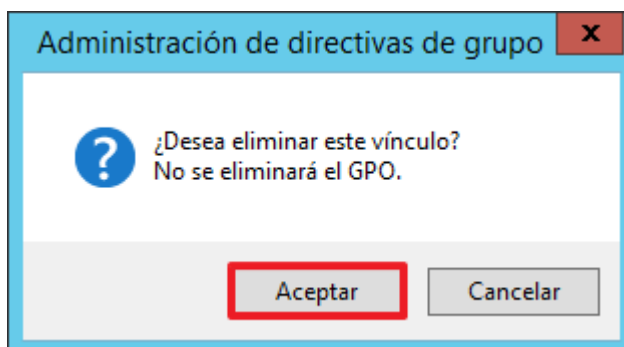
142. Localice la unidad organizativa donde se está aplicando la GPO “CCN-STIC-870A ENS Instalación o eliminación de roles (TEMPORAL)”.

143. Pulse botón derecho sobre la GPO y seleccione la opción del menú contextual “Eliminar”.

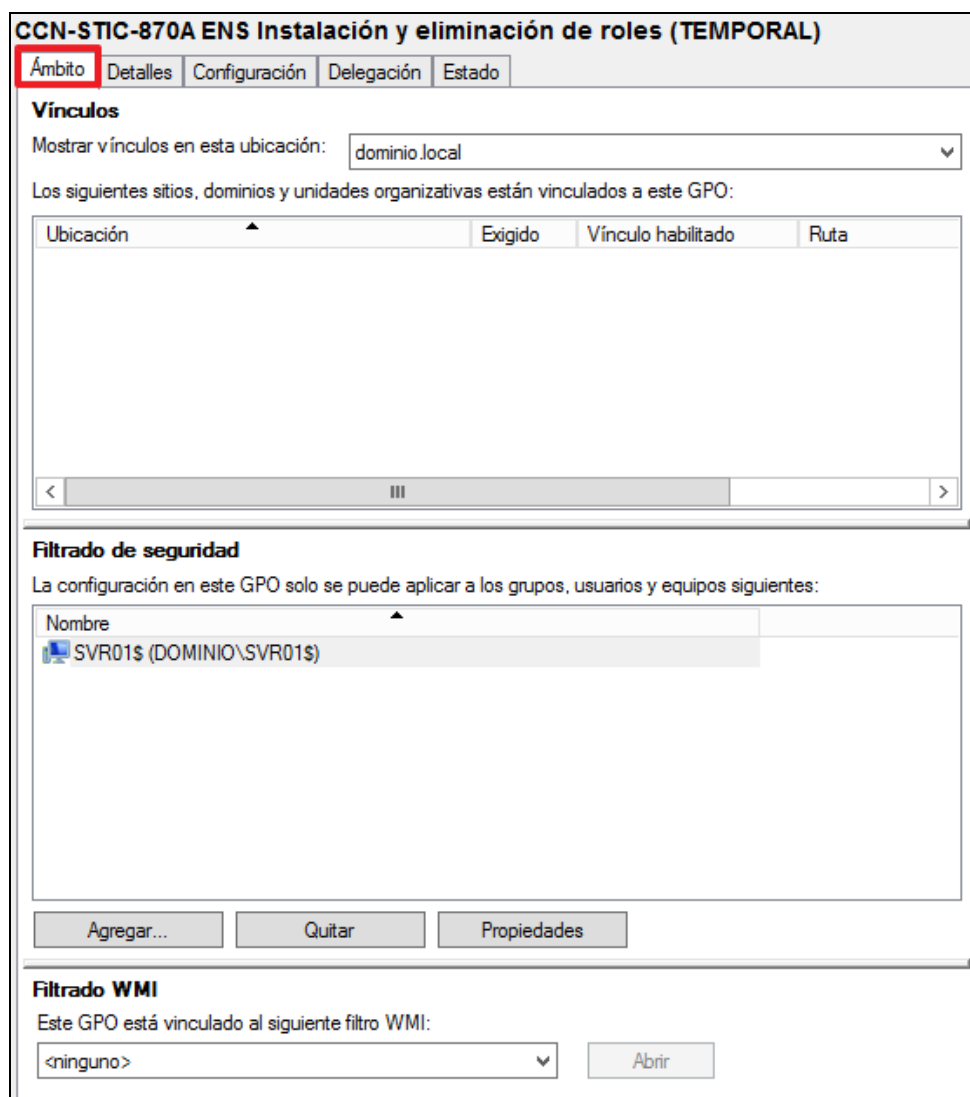


Paso	Descripción
------	-------------

144. Pulse “Aceptar” ante el mensaje emergente “¿Desea eliminar este vínculo? No se eliminará el GPO.”

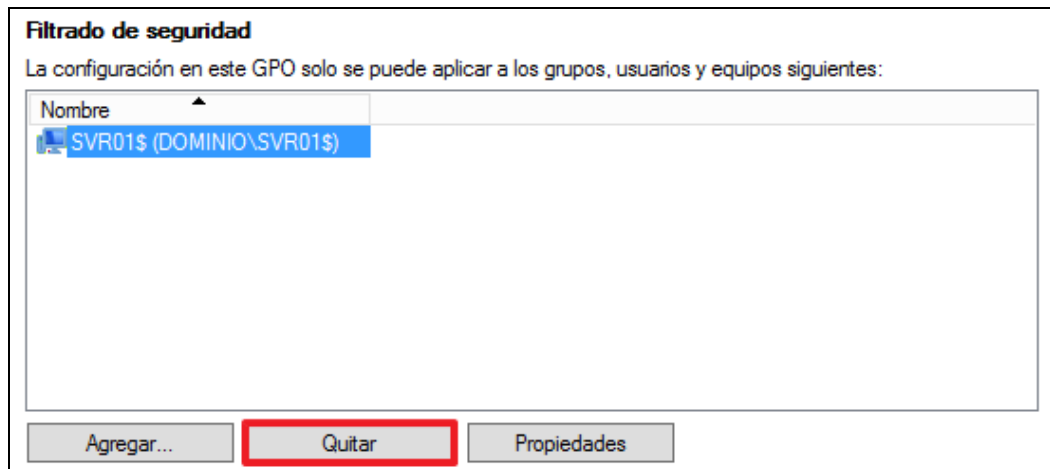


145. A continuación, seleccione la política de grupo “CCN-STIC-870A ENS Instalación y eliminación de roles (TEMPORAL)” ubicada en el contenedor “Objetos de directiva de grupo” y diríjase a la pestaña “Ámbito” que se encuentra en el panel derecho.



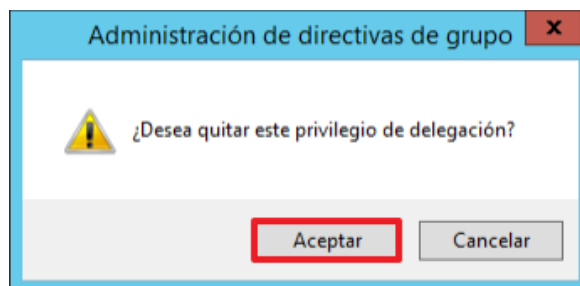
Paso	Descripción
------	-------------

146. En la opción “Filtrado de seguridad”, Seleccione los equipos o grupos sobre los que se está aplicando la política de seguridad y pulse sobre el botón “Quitar”.



Nota: En este ejemplo se elimina el equipo “SVR01”

147. Pulse “Aceptar” ante el mensaje emergente “¿Desea quitar este privilegio de delegación?”.



ANEXO G. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE NIVEL BAJO DEL ENS PARA SERVIDOR DE IMPRESIÓN

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

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

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

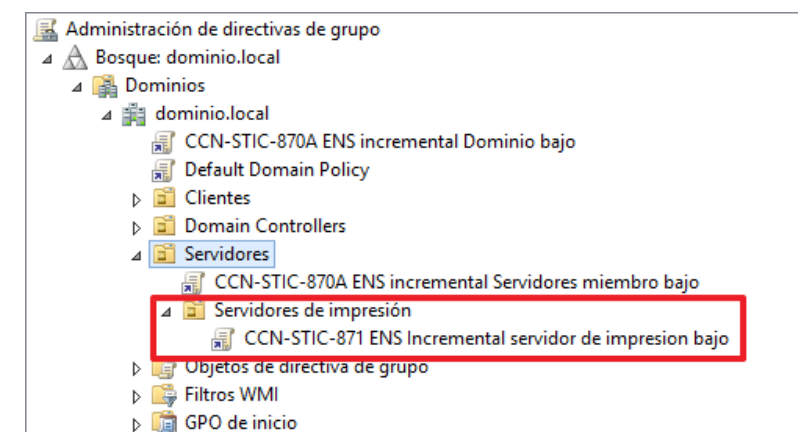
- En el Controlador de Dominio:
 - Usuarios y equipos de Active Directory (dsa.msc).
 - Administrador de directivas de grupo (gpmc.msc).
 - Editor de objetos de directiva de grupo (gpedit.msc).
- En el servidor de impresión:
 - Administrador de Windows (explorer.exe).
 - PowerShell (powershell.exe).
 - Servicios (services.msc).
 - Editor de objetos de directiva de grupo (gpedit.msc).
 - Administrador de impresión (printmanagement.msc).

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

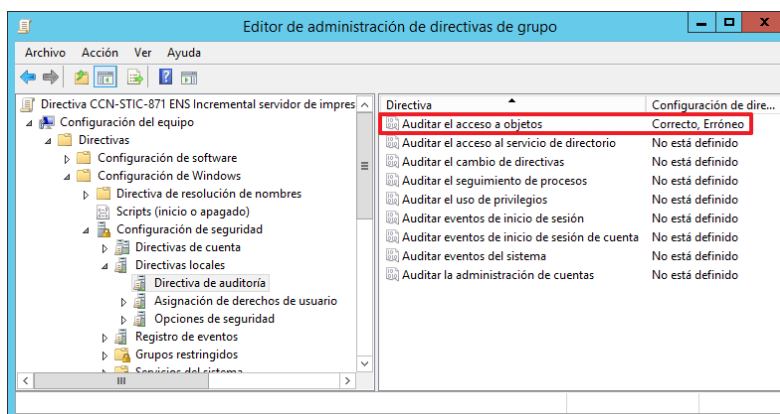
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.

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

- Verifique que está creada la directiva "CCN-STIC-871 ENS Incremental servidor de impresion bajo".

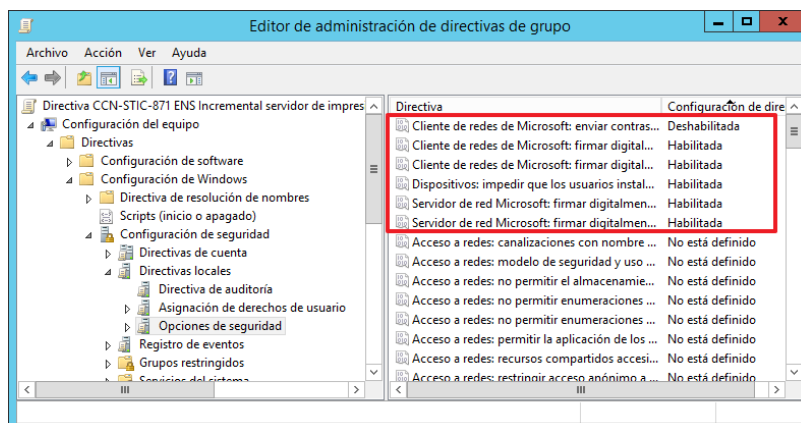


- Verifique los valores de auditoría de la directiva "CCN-STIC-871 ENS Incremental servidor de impresion bajo".
- Utilizando el editor de directiva de grupo, haga clic derecho sobre la directiva "CCN-STIC-871 ENS Incremental servidor de impresion bajo" y seleccione la opción "Editar...". Verifique que la directiva tiene los siguientes valores en las directivas de auditoría dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas locales \ Directiva de auditoría.



Directiva	Valor	OK/NOK
Auditar el acceso a objetos	Correcto, Erróneo	

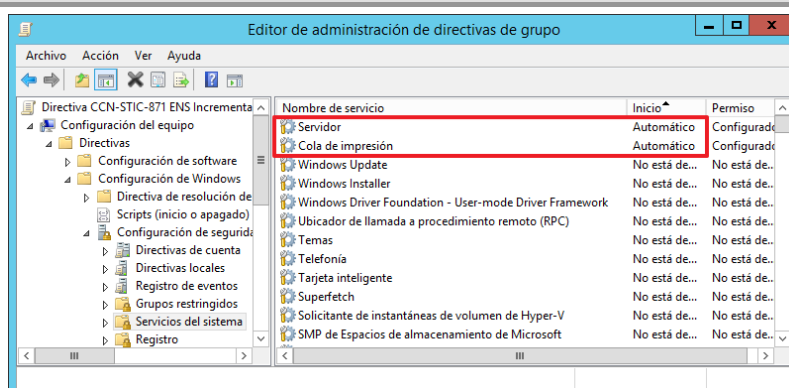
Comprobación	OK/NOK	Cómo hacerlo
4. Verifique las opciones de seguridad de la directiva "CCN-STIC-871 ENS Incremental servidor de impresion bajo".		Utilizando el editor de directiva de grupo, verifique que la directiva "CCN-STIC-871 ENS Incremental servidor de impresion bajo" tiene los siguientes valores en las opciones de seguridad dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas locales \ Opciones de seguridad.



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

5. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-871 ENS Incremental servidor de impresion bajo.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-871 ENS Incremental servidor de Impresion bajo" tiene los siguientes valores de servicios de sistema dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del sistema.
--	--	--

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

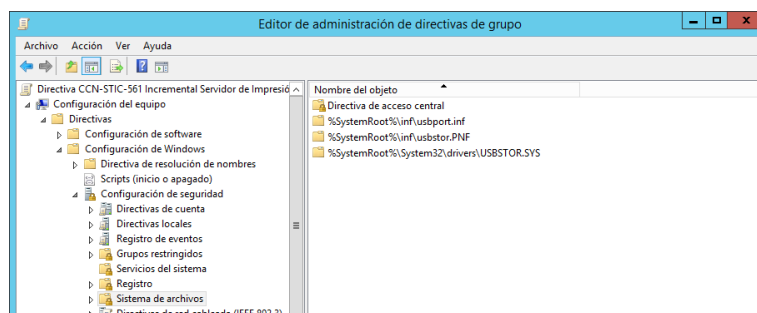


Servicio	Valor	OK/NOK
Cola de impresión	Automático	
Servidor	Automático	

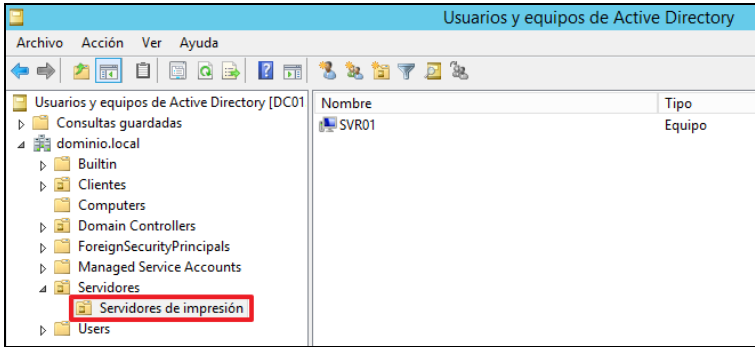
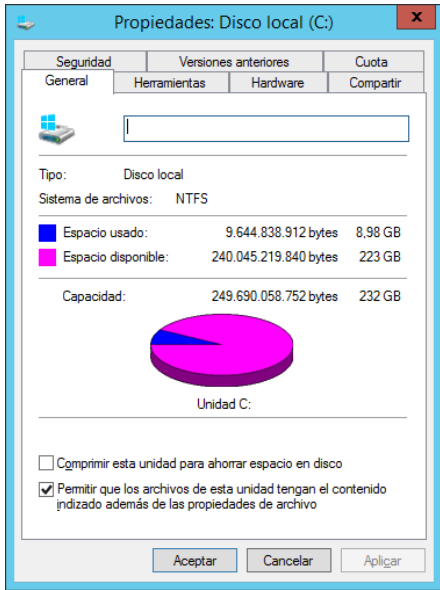
6. Verifique los valores de seguridad del sistema de archivos en la directiva CCN-STIC-871 ENS Incremental servidor de impresion bajo.

Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-871 ENS Incremental servidor de impresion bajo” tiene los siguientes valores de seguridad del sistema de archivos dentro de:

Directiva CCN-STIC-871 ENS Incremental Servidor de Impresion bajo \ Configuración del equipo\ Directivas \ Configuración de Windows \ Configuración de seguridad \ Sistema de archivos.

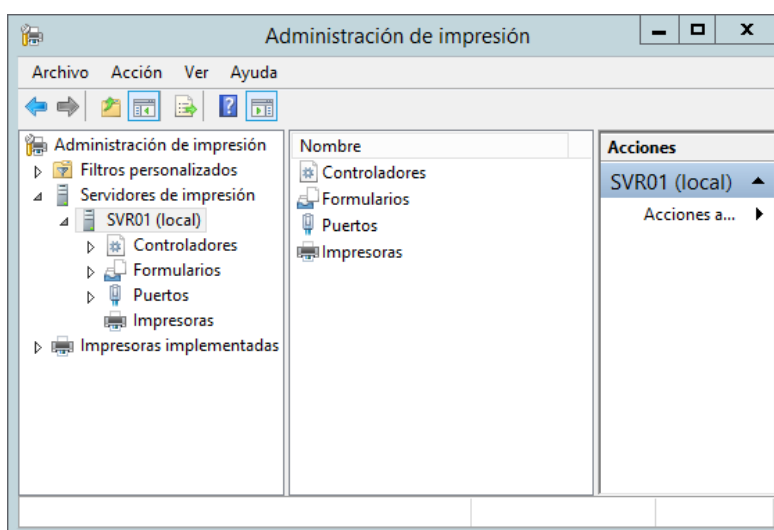


Directiva	Permisos otorgados	OK/NOK
%SystemRoot%\inf\usbport.inf	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	
%SystemRoot%\inf\usbstor.pnf	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	
%SystemRoot%\System32\drivers\USBSTOR.sys	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que el servidor de impresión está dentro de la unidad organizativa "Servidores de impresión".		Utilice la herramienta Usuarios y equipos de Active Directory (Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory) y seleccione la unidad organizativa "Servidores de impresión". Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de impresión que se están asegurando. 
8. Inicie sesión en el servidor de impresión.		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.
9. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL's. 
10. Verifique que están instalados los componentes que se indican.		En el "Administrador del Servidor", pulse sobre la opción "Servidor Local" del menú de la izquierda y diríjase a la parte final de la ventana principal, "Roles y características", por medio del scroll lateral derecho.
Componente		OK/NOK
Servicios de impresión y documentos		
Servidor de impresión		

Comprobación	OK/NOK	Cómo hacerlo
11. Verifique que los servicios del sistema relacionados con el servidor de impresión están configurados correctamente.		Ejecute el complemento Servicios (ejecutando “services.msc” desde, botón derecho sobre Inicio → Ejecuta) y compruebe el tipo de inicio de los servicios.
Servicio	Valor	OK/NOK
Servidor	Automático	
Cola de impresión	Automático	

12. Verifique que la instalación del servidor de impresión se ha realizado correctamente.
- Utilizando la herramienta de administración de impresión (ejecutando “printmanagement.msc” desde, botón derecho sobre Inicio → Ejecutar), verifique que la consola se inicia y presenta el servidor local como un servidor de impresión.



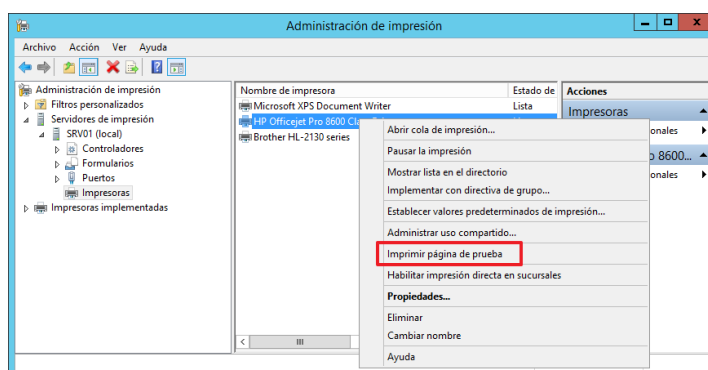
Nota: En esta comprobación, el servidor se denomina “SVR01”. En su organización debe comprobar que aparece el nombre del servidor de impresión que está implementando.

13. Verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.
- Utilizando la herramienta de administración de impresión (ejecutando “printmanagement.msc” desde, botón derecho sobre Inicio → Ejecutar), verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.
- Para ello, seleccione cada una de las impresoras que aparecen en el nodo “Impresoras” con el botón derecho del ratón y pulse sobre la opción “Imprimir página de prueba”.

Comprobación

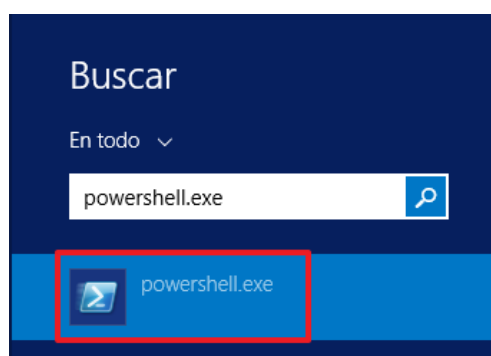
OK/NOK

Cómo hacerlo



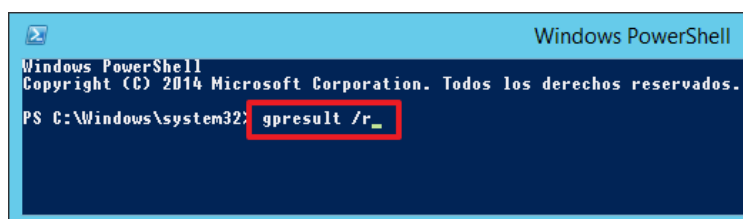
14. Inicie la consola de PowerShell.

Ejecute la consola de PowerShell. Para ello pulse "Inicio", teclee "powershell.exe" y pulse "Enter".



15. Verifique que se están aplicando las GPOs correspondientes.

Verifique que se están aplicando las GPOs correspondientes ejecutando el comando "gpresult /r".



16. Verifique que se están aplicando las GPOs correspondientes.

Verifique que se aplican las siguientes GPOs:

- CCN-STIC-871 ENS Incremental servidor de impresión bajo.
- CCN-STIC-870A ENS incremental servidores miembro bajo.
- CCN-STIC-870A ENS incremental dominio bajo.

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

```

Selecccionar Administrador: Windows PowerShell

PS C:\Users\administrador.DOMINIO> gpresult /r

Herramienta de resultados para la Directiva de grupos del
sistema operativo Microsoft (R) Windows (R) v2.0
© 2013 Microsoft Corporation. Todos los derechos reservados.

Creado el 02/01/2017 a las 13:33:08

RSOP datos para DOMINIO\administrador en SUR01 : modo de inicio de sesión
-----

Configuración del sistema operativo: Servidor miembro
Versión del sistema operativo: 6.3.9600
Nombre de sitio: Default-First-Site-Name
Perfil móvil: n/a
Perfil local: C:\Users\administrador.DOMINIO
¿Conectado a un vínculo de baja velocidad?: No

CONFIGURACIÓN DE EQUIPO
-----
CN=SUR01,OU=Servidores de impresión,OU=Servidores,DC=dominio,DC=local
última vez que se aplicó la Directiva de grupo: 02/01/2017 a las 13:32:49
Directivas de grupo aplicadas desdeDC01.dominio.local
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio: DOMINIO
Tipo de dominio: Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
CCN-STIC-871 ENS Incremental servidor de impresion bajo
CCN-STIC-870A ENS incremental Servidores miembro bajo
CCN-STIC-870A ENS incremental Dominio bajo
Default Domain Policy

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
Filtrar: No aplicado (vacío)

```

ANEXO H. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE NIVEL MEDIO DEL ENS PARA SERVIDOR DE IMPRESIÓN

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

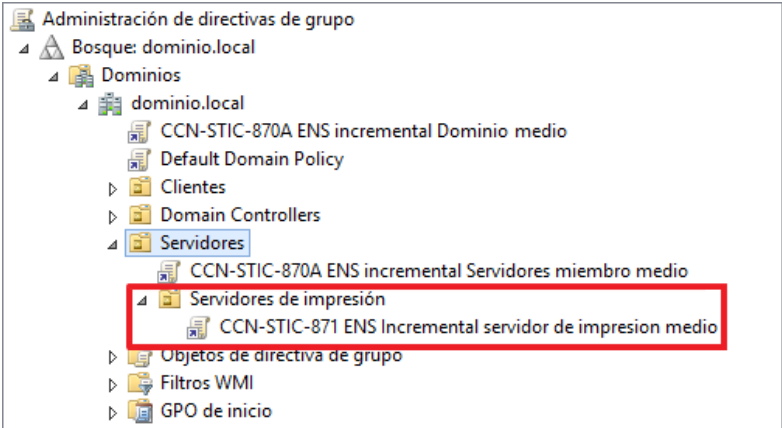
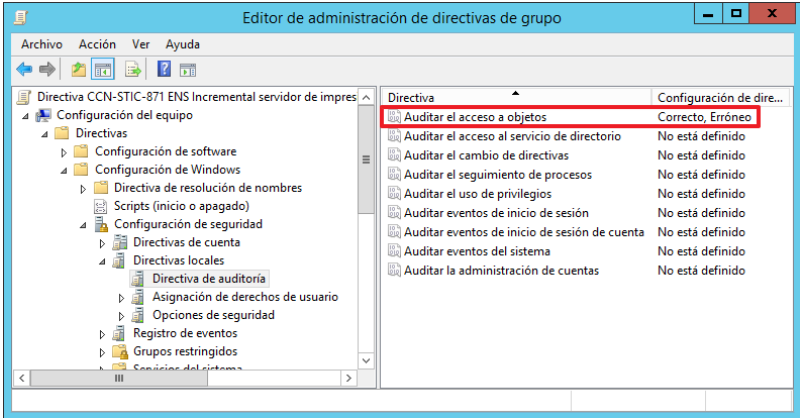
Para realizar esta lista de comprobación, primero se deberá iniciar sesión en un Controlador de Dominio con una cuenta de usuario que tenga privilegios de administración en el dominio. A continuación, se realizarán las comprobaciones comunes a todos los servidores de impresión que son miembros del dominio.

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

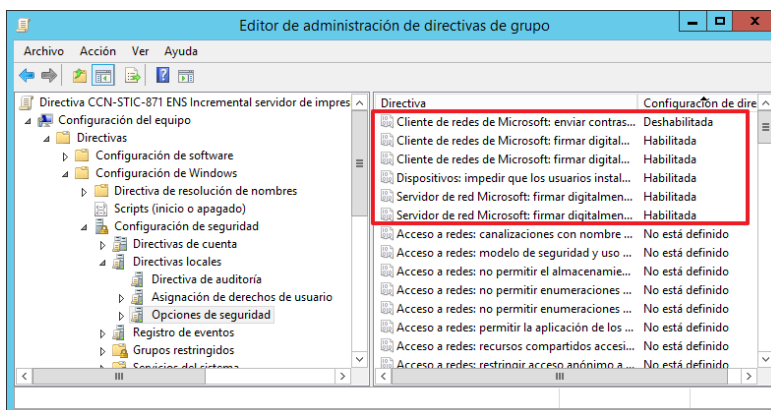
- En el Controlador de Dominio:
 - Usuarios y equipos de Active Directory (dsa.msc).
 - Administrador de directivas de grupo (gpmc.msc).
 - Editor de objetos de directiva de grupo (gpedit.msc).
- En el servidor de impresión:
 - Administrador de Windows (explorer.exe).
 - PowerShell (powershell.exe).
 - Servicios (services.msc).
 - Editor de objetos de directiva de grupo (gpedit.msc).
 - Administrador de impresión (printmanagement.msc).

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

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

Comprobación	OK/NOK	Cómo hacerlo						
2. Verifique que está creada la directiva CCN-STIC-871 ENS Incremental servidor de impresion medio.		Utilice el Administrador de directivas de grupo (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de impresión” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-871 ENS Incremental servidor de impresion medio”. 						
3. Verifique los valores de auditoría de la directiva CCN-STIC-871 ENS Incremental servidor de impresion medio.		Utilizando el editor de directiva de grupo, haga clic derecho sobre la directiva “CCN-STIC-871 ENS Incremental servidor de impresion medio” y seleccione la opción “Editar...”, verifique que la directiva tiene los siguientes valores en las directivas de auditoría dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion medio \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas locales \ Directiva de auditoría. 						
<table> <tr> <th>Directiva</th><th>Valor</th><th>OK/NOK</th></tr> <tr> <td>Auditar el acceso a objetos</td><td>Correcto, Erróneo</td><td></td></tr> </table>			Directiva	Valor	OK/NOK	Auditar el acceso a objetos	Correcto, Erróneo	
Directiva	Valor	OK/NOK						
Auditar el acceso a objetos	Correcto, Erróneo							

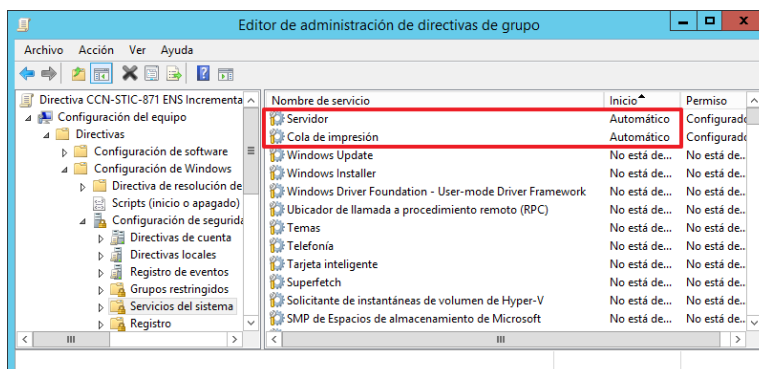
Comprobación	OK/NOK	Cómo hacerlo
4. Verifique las opciones de seguridad de la directiva CCN-STIC-871 ENS Incremental servidor de impresion medio.		Utilizando el editor de directiva de grupo, verifique que la directiva “CCN-STIC-871 ENS Incremental servidor de impresion medio” tiene los siguientes valores en las opciones de seguridad dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion medio \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas locales \ Opciones de seguridad.



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

5. Verifique los valores de los servicios del sistema de la directiva CCN-STIC-871 ENS Incremental servidor de impresion medio.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-871 ENS Incremental servidor de impresion medio” tiene los siguientes valores de servicios de sistema dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion medio \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del sistema.
---	--	---

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

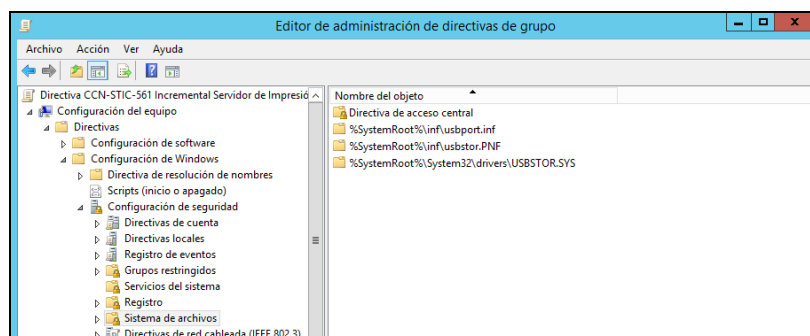


Servicio	Valor	OK/NOK
Cola de impresión	Automático	
Servidor	Automático	

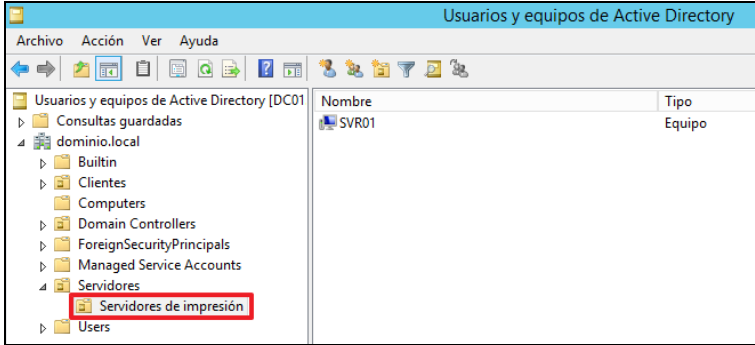
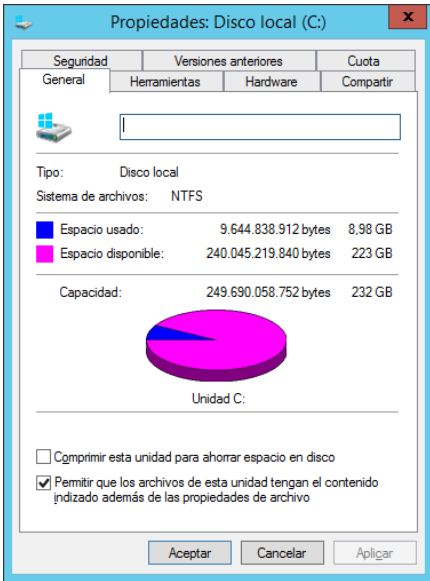
6. Verifique los valores de seguridad del sistema de archivos en la directiva CCN-STIC-871 ENS Incremental servidor de impresion medio.

Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-871 ENS Incremental servidor de impresion medio” tiene los siguientes valores de seguridad del sistema de archivos dentro de:

Directiva CCN-STIC-871 ENS Incremental Servidor de impresion medio \ Configuración del equipo\ Directivas \ Configuración de Windows \ Configuración de seguridad \ Sistema de archivos.

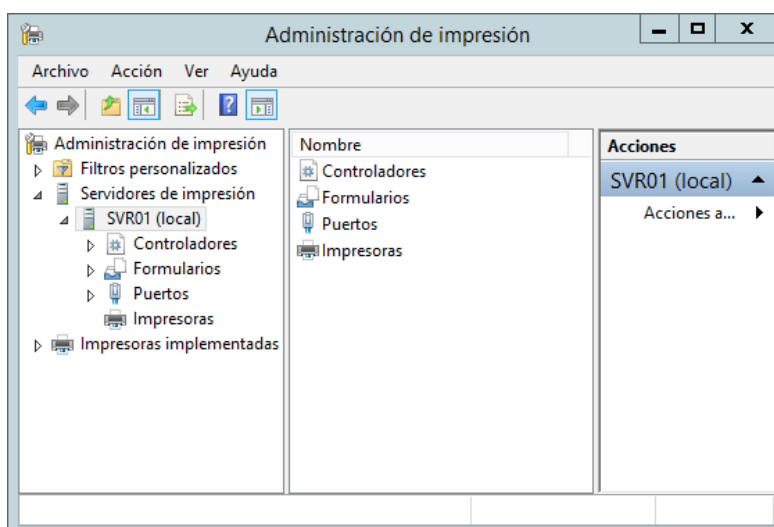


Directiva	Permisos otorgados	OK/NOK
%SystemRoot%\inf\usbport.inf	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	
%SystemRoot%\inf\usbstor.pnf	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	
%SystemRoot%\System32\drivers\USBSTOR.sys	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que el servidor de impresión está dentro de la unidad organizativa "Servidores de impresión".		Utilice la herramienta Usuarios y equipos de Active Directory (Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory) y seleccione la unidad organizativa "Servidores de impresión". Compruebe que existe un objeto de tipo equipo por cada uno de los servidores de impresión que se están asegurando.
		
8. Inicie sesión en el servidor de impresión.		Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.
9. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL's.
		
10. Verifique que están instalados los componentes que se indican.		En el "Administrador del Servidor", pulse sobre la opción "Servidor Local" del menú de la izquierda y diríjase a la parte final de la ventana principal, "Roles y características", por medio del scroll lateral derecho.
Componente		OK/NOK
Servicios de impresión y documentos		
Servidor de impresión		

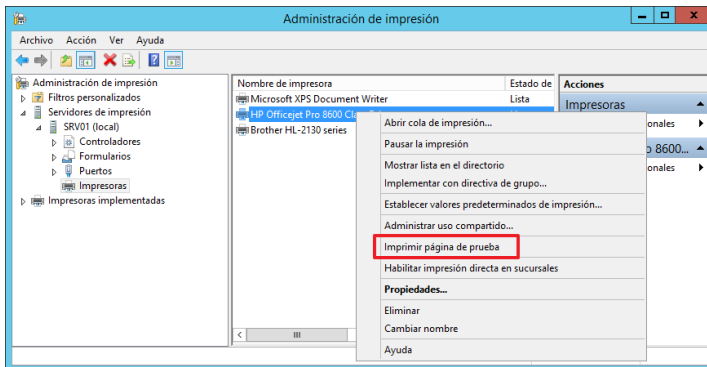
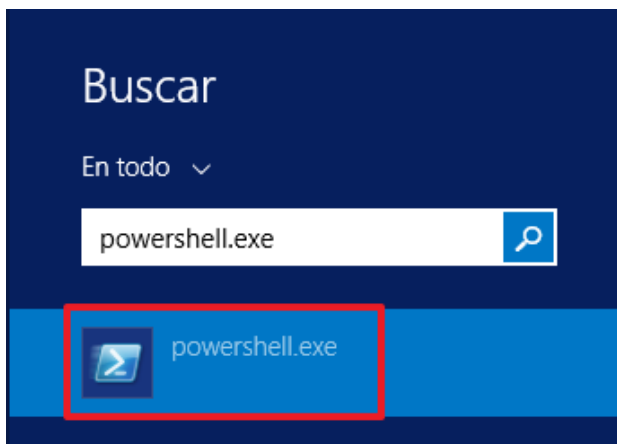
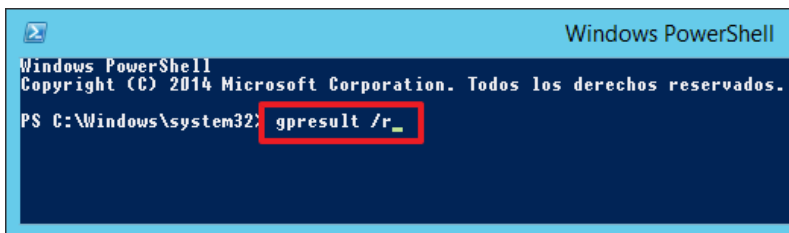
Comprobación	OK/NOK	Cómo hacerlo									
11. Verifique que los servicios del sistema relacionados con el servidor de impresión están configurados correctamente.		Ejecute el complemento Servicios (ejecutando “services.msc” desde, botón derecho sobre Inicio → Ejecutar...) y compruebe el tipo de inicio de los servicios.									
<table> <tr> <th>Servicio</th><th>Valor</th><th>OK/NOK</th></tr> <tr> <td>Servidor</td><td>Automático</td><td></td></tr> <tr> <td>Cola de impresión</td><td>Automático</td><td></td></tr> </table>			Servicio	Valor	OK/NOK	Servidor	Automático		Cola de impresión	Automático	
Servicio	Valor	OK/NOK									
Servidor	Automático										
Cola de impresión	Automático										

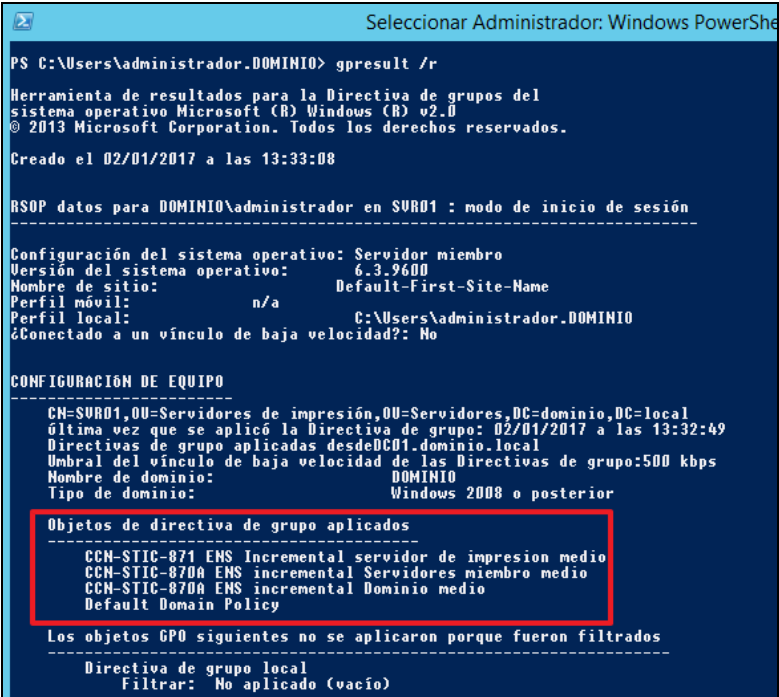
12. Verifique que la instalación del servidor de impresión se ha realizado correctamente.
- Utilizando la herramienta de administración de impresión (ejecutando “printmanagement.msc” desde, botón derecho sobre Inicio → Ejecutar...), verifique que la consola se inicia y presenta el servidor local como un servidor de impresión.



Nota: En esta comprobación, el servidor se denomina “SVR01”. En su organización debe comprobar que aparece el nombre del servidor local de impresión que está implementando.

13. Verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.
- Utilizando la herramienta de administración de impresión (ejecutando “printmanagement.msc” desde, botón derecho sobre Inicio → Ejecutar...), verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.
- Para ello, seleccione cada una de las impresoras que aparecen en el nodo “Impresoras” con el botón derecho del ratón y pulse sobre la opción “Imprimir página de prueba”.

Comprobación	OK/NOK	Cómo hacerlo
		
14. Inicie la consola de PowerShell.		Ejecute la consola de PowerShell. Para ello pulse “Inicio”, teclee “powershell.exe” y pulse “Enter”. 
15. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se están aplicando las GPOs correspondientes ejecutando el comando “gpresult /r”. 
16. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se aplican las siguientes GPOs: – CCN-STIC-871 ENS Incremental servidor de impresión medio. – CCN-STIC-870A ENS incremental servidores miembro medio. – CCN-STIC-870A ENS incremental dominio medio.

Comprobación	OK/NOK	Cómo hacerlo
		 <pre> PS C:\Users\administrador.DOMINIO> gresult /r Herramienta de resultados para la Directiva de grupos del sistema operativo Microsoft (R) Windows (R) v2.0 © 2013 Microsoft Corporation. Todos los derechos reservados. Creado el 02/01/2017 a las 13:33:08 RSOP datos para DOMINIO\administrador en SUR01 : modo de inicio de sesión ----- Configuración del sistema operativo: Servidor miembro Versión del sistema operativo: 6.3.9600 Nombre de sitio: Default-First-Site-Name Perfil móvil: n/a Perfil local: C:\Users\administrador.DOMINIO ¿Conectado a un vínculo de baja velocidad?: No CONFIGURACIÓN DE EQUIPO ----- CN=SUR01,OU=Servidores de impresión,OU=Servidores,DC=dominio,DC=local última vez que se aplicó la Directiva de grupo: 02/01/2017 a las 13:32:49 Directivas de grupo aplicadas desdeDC01.dominio.local Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps Nombre de dominio: DOMINIO Tipo de dominio: Windows 2008 o posterior Objetos de directiva de grupo aplicados ----- CCN-STIC-871 ENS Incremental servidor de impresion medio CCN-STIC-870A ENS incremental Servidores miembro medio CCN-STIC-870A ENS incremental Dominio medio Default Domain Policy Los objetos GPO siguientes no se aplicaron porque fueron filtrados ----- Directiva de grupo local Filtrar: No aplicado (vacío) </pre>

ANEXO I. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE NIVEL ALTO DEL ENS PARA SERVIDOR DE IMPRESIÓN

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

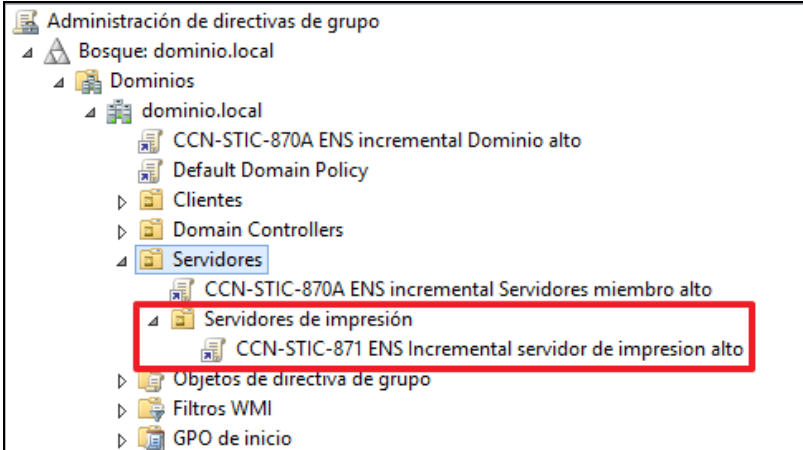
Para realizar esta lista de comprobación, primero se deberá iniciar sesión en un Controlador de Dominio con una cuenta de usuario que tenga privilegios de administración en el dominio. A continuación, se realizarán las comprobaciones comunes a todos los servidores de impresión que son miembros del dominio.

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

- En el Controlador de Dominio:
 - Usuarios y equipos de Active Directory (dsa.msc).
 - Administrador de directivas de grupo (gpmc.msc).
 - Editor de objetos de directiva de grupo (gpedit.msc).
- En el servidor de impresión:
 - Administrador de Windows (explorer.exe).
 - PowerShell (powershell.exe).
 - Servicios (services.msc).
 - Editor de objetos de directiva de grupo (gpedit.msc).
 - Administrador de impresión (printmanagement.msc).

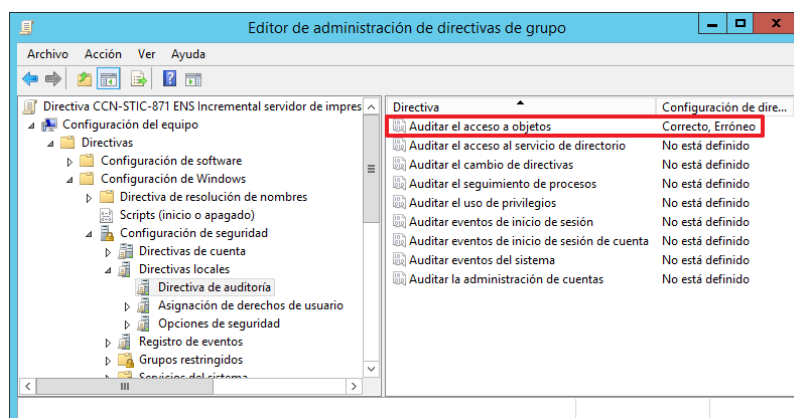
Nota: La lista de comprobación está basada en los nombres de objetos de directivas, unidades organizativas y cuentas de servicios tal y como se ha indicado durante la presente guía. Deberá adaptar los pasos según la configuración de su organización.

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un Controlador de Dominio.		En uno de los controladores de dominio, inicie sesión con una cuenta que tenga privilegios de administración del dominio.
2. Verifique que está creada la directiva CCN-STIC-871 ENS Incremental servidor de impresion alto.		Utilice el Administrador de directivas de grupo (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Servidores de impresión” que se encuentra en la Unidad Organizativa “Servidores”. Verifique que está creada la política “CCN-STIC-871 ENS Incremental servidor de impresion alto”.

Comprobación	OK/NOK	Cómo hacerlo
		

3. Verifique los valores de auditoría de la directiva CCN-STIC-871 ENS Incremental servidor de impresion alto.

Utilizando el editor de directiva de grupo, haga clic derecho sobre la directiva “CCN-STIC-871 ENS Incremental servidor de impresion alto” y seleccione la opción “Editar...”, verifique que la directiva tiene los siguientes valores en las directivas de auditoría dentro de:
Directiva CCN-STIC-871 ENS Incremental Servidor de impresion alto
Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Directiva de auditoría.



Directiva	Valor	OK/NOK
Auditar el acceso a objetos	Correcto, Erróneo	

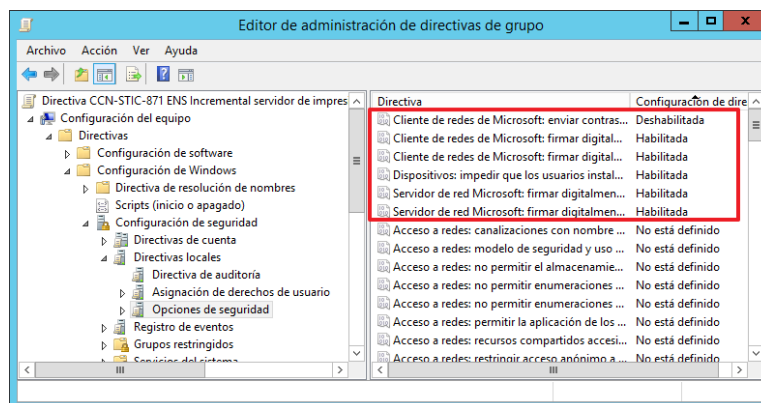
4. Verifique las opciones de seguridad de la directiva CCN-STIC-871 ENS Incremental servidor de impresion alto.

Utilizando el editor de directiva de grupo, verifique que la directiva “CCN-STIC-871 ENS Incremental servidor de impresion alto” tiene los siguientes valores en las opciones de seguridad dentro de:
Directiva CCN-STIC-871 ENS Incremental servidor de impresion alto
Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad.

Comprobación

OK/NOK

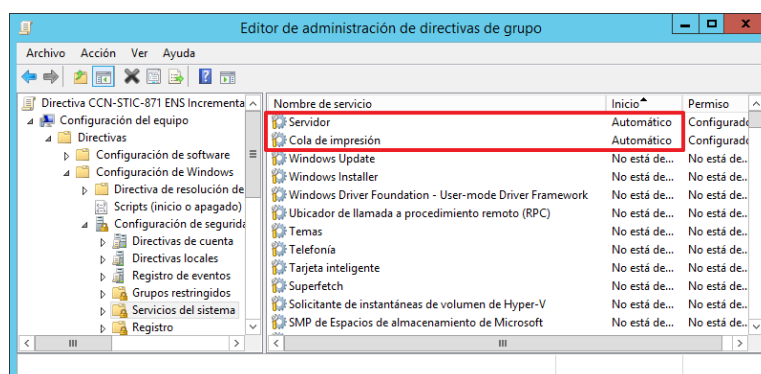
Cómo hacerlo



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

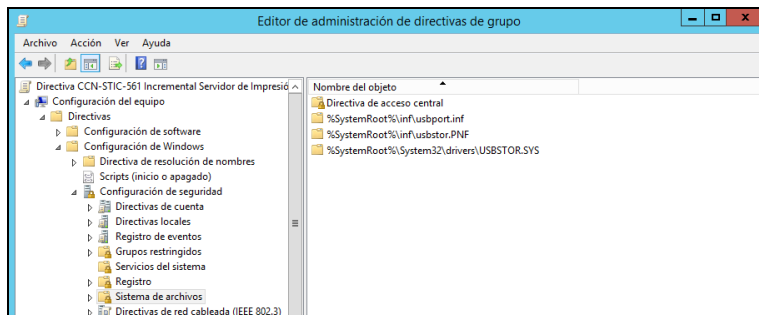
- Verifique los valores de los servicios del sistema de la directiva CCN-STIC-871 ENS Incremental servidor de impresion alto.

Utilizando el editor de objetos de directiva de grupo, verifique que la directiva "CCN-STIC-871 ENS Incremental Servidor de impresion alto" tiene los siguientes valores de servicios de sistema dentro de:
Directiva CCN-STIC-871 ENS Incremental Servidor de impresion alto
Configuración del equipo\ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del sistema.



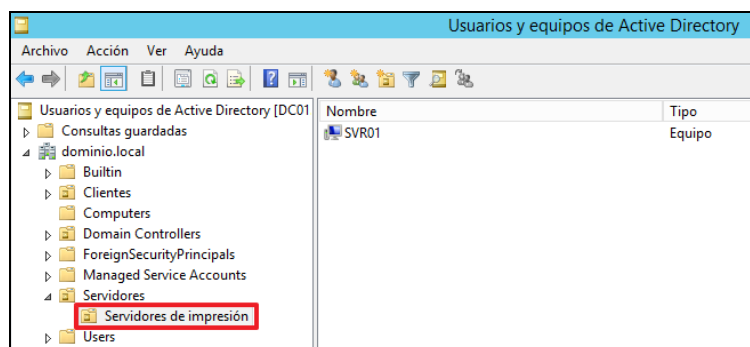
Servicio	Valor	OK/NOK
Cola de impresión	Automático	
Servidor	Automático	

Comprobación	OK/NOK	Cómo hacerlo
6. Verifique los valores de seguridad del sistema de archivos en la directiva CCN-STIC-871 ENS Incremental servidor de impresion alto.		Utilizando el editor de objetos de directiva de grupo, verifique que la directiva “CCN-STIC-871 ENS Incremental servidor de impresion alto” tiene los siguientes valores de seguridad del sistema de archivos dentro de: Directiva CCN-STIC-871 ENS Incremental servidor de impresion alto \ Configuración del equipo\ Directivas \ Configuración de Windows \ Configuración de seguridad \ Sistema de archivos.

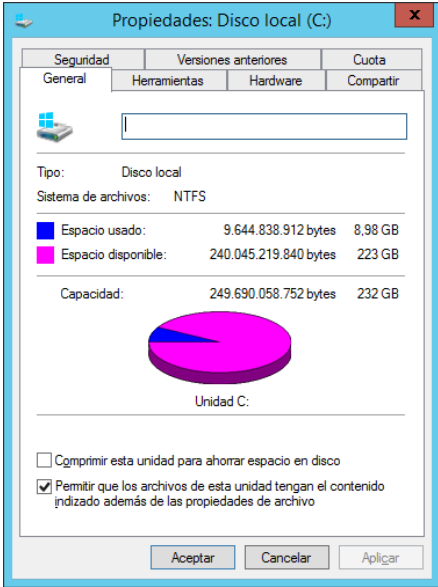


Directiva	Permisos otorgados	OK/NOK
%SystemRoot%\inf\usbport.inf	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	
%SystemRoot%\inf\usbstor.pnf	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	
%SystemRoot%\System32\drivers\USBSTOR.sys	SYSTEM: control total Administradores: control total Usuarios: leer, listar el contenido de la carpeta y ejecutar	

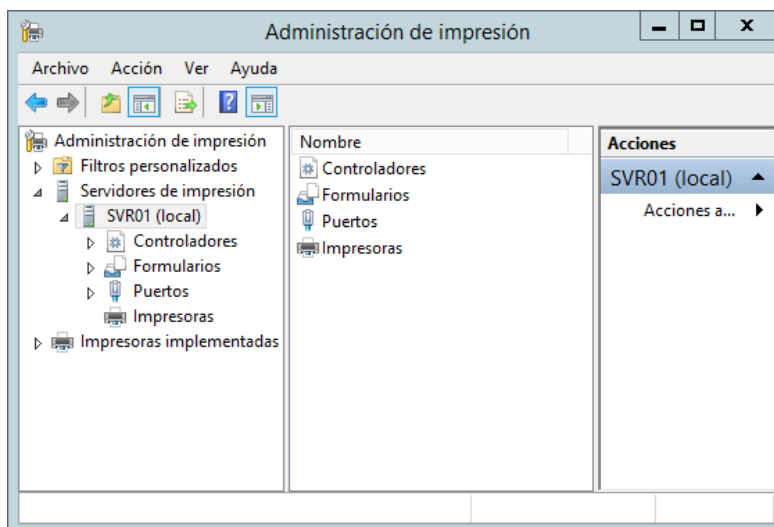
7. Verifique que el servidor de impresión está dentro de la unidad organizativa “Servidores de impresión”.	Utilice la herramienta Usuarios y equipos de Active Directory (Inicio → Herramientas administrativas → Usuarios y equipos de Active Directory) y seleccione la unidad organizativa “Servidores de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



8. Inicie sesión en el servidor de impresión.	Para completar el resto de la lista de verificación deberá iniciar sesión con una cuenta que tenga permisos de administrador local del servidor o administrador del dominio.
---	---

Comprobación	OK/NOK	Cómo hacerlo									
9. Verifique que todos los volúmenes están formateados con NTFS.		Utilizando el explorador de Windows (botón derecho sobre Inicio → Explorador de archivos, botón derecho sobre la unidad C:\), verifique en las propiedades de cada partición el uso del sistema de archivos NTFS o cualquier otro que permita la aplicación de ACL's. 									
10. Verifique que están instalados los componentes que se indican.		En el "Administrador del Servidor", pulse sobre la opción "Servidor Local" del menú de la izquierda y diríjase a la parte final de la ventana principal, "Roles y características", por medio del scroll lateral derecho. <table border="1"> <thead> <tr> <th>Componente</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Servicios de impresión y documentos</td><td></td><td></td></tr> <tr> <td>Servidor de impresión</td><td></td><td></td></tr> </tbody> </table>	Componente	Valor	OK/NOK	Servicios de impresión y documentos			Servidor de impresión		
Componente	Valor	OK/NOK									
Servicios de impresión y documentos											
Servidor de impresión											
11. Verifique que los servicios del sistema relacionados con el servidor de impresión están configurados correctamente.		Ejecute el complemento Servicios (ejecutando "services.msc" desde, botón derecho sobre Inicio → Ejecutar...) y compruebe el tipo de inicio de los servicios. <table border="1"> <thead> <tr> <th>Servicio</th><th>Valor</th><th>OK/NOK</th></tr> </thead> <tbody> <tr> <td>Servidor</td><td>Automático</td><td></td></tr> <tr> <td>Cola de impresión</td><td>Automático</td><td></td></tr> </tbody> </table>	Servicio	Valor	OK/NOK	Servidor	Automático		Cola de impresión	Automático	
Servicio	Valor	OK/NOK									
Servidor	Automático										
Cola de impresión	Automático										
12. Verifique que la instalación del servidor de impresión se ha realizado correctamente.		Utilizando la herramienta de administración de impresión (ejecutando "printmanagement.msc" desde, botón derecho sobre Inicio → Ejecutar...), verifique que la consola se inicia y presenta el servidor local como un servidor de impresión.									

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

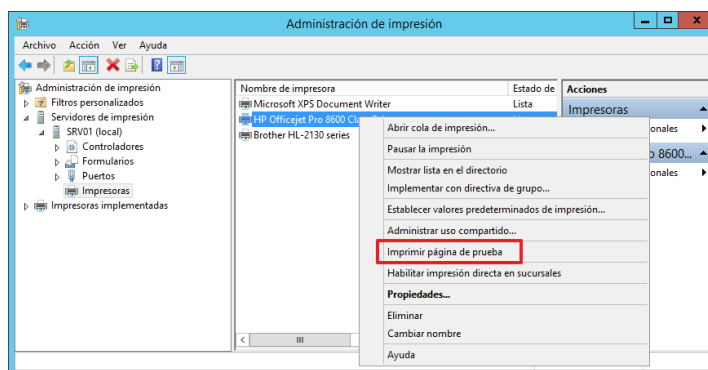


Nota: En esta comprobación, el servidor se denomina “SVR01”. En su organización debe comprobar que aparece el nombre del servidor local de impresión que está implementando.

13. Verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.

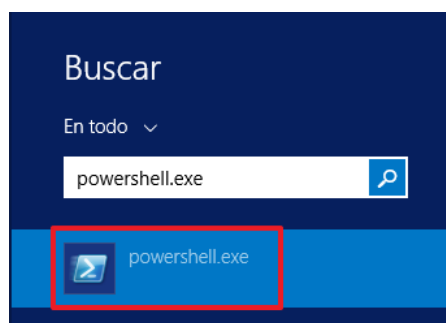
Utilizando la herramienta de administración de impresión (ejecutando “printmanagement.msc” desde, botón derecho sobre Inicio → Ejecutar...), verifique que las impresoras instaladas imprimen correctamente desde el servidor de impresión.

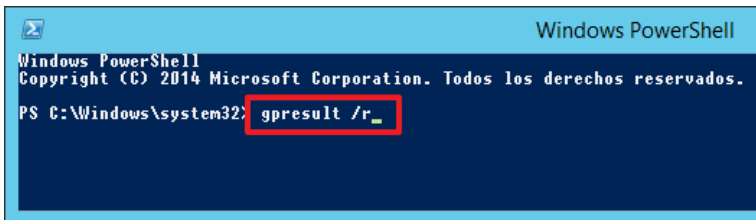
Para ello, seleccione cada una de las impresoras que aparecen en el nodo “Impresoras” y con el botón derecho del ratón y pulse sobre la opción “Imprimir página de prueba”.



14. Inicie la consola de PowerShell.

Ejecute la consola de PowerShell. Para ello pulse “Inicio”, teclee “powershell.exe” y pulse “Enter”.



Comprobación	OK/NOK	Cómo hacerlo
15. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se están aplicando las GPOs correspondientes, ejecutando el comando "gpresult /r". 
16. Verifique que se están aplicando las GPOs correspondientes.		Verifique que se aplican las siguientes GPOs: – CCN-STIC-871 ENS Incremental servidor de impresión alto. – CCN-STIC-870A ENS incremental servidores miembro alto. – CCN-STIC-870A ENS incremental dominio alto. 