GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD DE LAS TIC

(CCN-STIC-869)

IMPLEMENTACIÓN DE APPLOCKER EN EL ESQUEMA NACIONAL DE SEGURIDAD

ens
Esquema Nacional de Seguridad

OCTUBRE 2015

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
CRIPTOLOGICO NACIONAL, c=ES
2016.11.24 16:32:25 +01'00'

NIPO: 002-15-029-1

Fecha de Edición: octubre de 2015

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.

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).

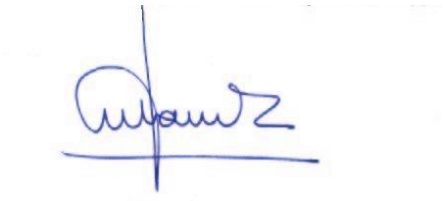
Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información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

Octubre 2015



Félix Sanz Roldán

Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

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 los principios de mínima funcionalidad siguiendo las condiciones de seguridad aplicables a través de medidas que se referencian en el RD 3/2010. La aplicación de la seguridad definida en esta guía se ha diseñado de manera incremental, de tal forma que puede ser aplicada bajo diferentes condicionantes. Aunque es factible que se referencien otras guías, especialmente de la serie CCN-STIC-500 referida a productos y entornos Microsoft, no será un requisito indispensable partir de ninguna de ellas, 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 comprenderá proporcionar los procedimientos para la implementación, establecer la configuración y realizar tareas de administración, maximizando las condiciones de seguridad en servidores Microsoft Windows Server 2008 R2 y Windows Server 2012 R2 así como en clientes Windows 7, como miembros de una infraestructura de dominio, mediante el bloqueo de aplicaciones no controladas por parte de la organización. También se detallarán los procedimientos para realizar la implementación de AppLocker en sistemas independientes a un dominio.
4. La definición, así como la implementación de las plantillas de seguridad, tiene 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. Debido a esto, 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 su adaptación a las necesidades operativas.

3. ALCANCE

6. La guía se ha elaborado con el fin de proporcionar información específica para realizar una implementación de la característica del control de aplicaciones AppLocker, en una configuración de seguridad, siguiendo los preceptos de mínima funcionalidad y con el objeto de prevenir frente a ejecuciones no deseadas, especialmente de código dañino. Se incluyen, además, operaciones básicas de configuraciones adicionales y desactivación del componente, entre otros aspectos, además de aquellas acciones que deben ser llevadas a cabo para el adecuado mantenimiento del servicio.

7. Este documento incluye:

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

   – **Riesgos de la ejecución de aplicaciones**. Se tratará la problemática actual debida a la ejecución de aplicaciones que presentan comportamiento de APT o código dañino, haciendo especial hincapié en el hecho de ejecutar aplicaciones desde el propio perfil del usuario.

   – **Característica de AppLocker**. Se detallará la funcionalidad existente con AppLocker y cómo ayuda a proteger contra la ejecución de código dañino o aplicaciones no controladas por la organización. Se detallarán los mecanismos de su implementación así como las características de uso.

   – **Directivas de AppLocker**. Se establecerán los mecanismos que presenta AppLocker para el control de ejecución de aplicaciones. Aunque la base fundamental de la guía consiste en el control por ruta de ejecución, se establecerán las pautas para que una organización pueda implementar otros controles ante comportamientos de ataques que se hayan podido identificar.

   – **Guía paso a paso en infraestructuras de dominio**. Permitirá la implantación y establecimiento de las configuraciones de seguridad de AppLocker en un dominio para servidores Windows Server 2008 R2, servidores Windows Server 2012 R2 y clientes Windows 7.

   – **Guía de mantenimiento**. Permitirá la realización de tareas de administración de AppLocker y el mantenimiento de las directivas de AppLocker.

   – **Procedimientos de aplicación de AppLocker en clientes y servidores independientes**. Se marcarán los procedimientos y mecanismos para hacer una implementación de AppLocker en los sistemas independientes a un dominio. Debido a las distintas implementaciones que se hayan podido realizar en sistemas independientes a un dominio no se expone un paso a paso concreto, sino unos procedimientos para realizar la implementación que requiera de forma específica cada tipo de sistema.

   – **Lista de comprobación.** Permitirá la verificación del grado de cumplimiento de un servidor o puesto de trabajo con respecto a las condiciones de seguridad que se establecen en esta guía.

4. DESCRIPCIÓN DEL USO DE ESTA GUÍA

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

   – Antes de comenzar a aplicar la guía, además de los requisitos para la instalación de AppLocker, será necesario cumplir los requisitos definidos para Windows Server 2008 R2, Windows Server 2012 R2 y Windows 7, según proceda.

   – Deberán tenerse en consideración las diferentes guías asociadas a los sistemas operativos definidas en la serie 800.

   – A continuación, se deberá instalar y configurar la característica de AppLocker tal y como se describe en la presente guía.

4.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

9. Los contenidos de esta guía son de aplicación para servidores con Sistemas Operativos Microsoft Windows Server 2008 R2, Microsoft Windows Server 2012 R2 y Microsoft Windows 7.
10. La guía ha sido probada y verificada con la versión de Windows Server 2008 R2 Enterprise SP1 de 64 bits, Windows Server 2012 R2 Standard de 64 bits y Windows 7 Enterprise de 64 bits, con los parámetros por defecto de instalación y sus guías correspondientes para su configuración. No se ha verificado en otros tipos de instalaciones como pudieran ser las de tipo OEM.
11. Esta guía ha sido diseñada para reducir la superficie de exposición de los equipos en la ejecución de aplicaciones.
12. Para la elaboración de la guía de seguridad, se ha utilizado un laboratorio basado en una plataforma de virtualización tipo Hyper-V de Windows Server 2012 R2 con las siguientes características técnicas:
    - Servidor Dell PowerEdge™ T320
        - Intel Pentium Xeon Quad Core.
        - HDD 80 GB.
        - 32 GB de RAM.
        - Interfaz de Red 1 GB.
13. Esta guía de seguridad no funcionará con hardware que no cumpla con los requisitos de seguridad mínimos para cada tipo de sistema operativo definido en la siguiente guía. La característica de AppLocker es nativa a los sistemas operativos indicados en la presente guía y no requiere de elementos de hardware adicionales.
14. La guía ha sido desarrollada con el objetivo de dotar a la infraestructura de la seguridad máxima. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesaria la aplicación de acciones adicionales para habilitar servicios o características deseadas en MS Windows Server 2008 R2, MS Windows Server 2012 R2 y MS Windows 7.
15. Para garantizar la seguridad de los servidores y puestos de trabajo, deberán instalarse las actualizaciones, recomendadas por el fabricante, disponibles a través del servicio de Windows Update. Las actualizaciones, por lo general, se liberan los segundos martes de cada mes, no obstante hay que tener presente que determinadas actualizaciones pueden ser liberadas en cualquier momento debido a su criticidad.
16. 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.
17. Antes de aplicar esta guía en producción, deberá asegurarse de haber probado en un entorno aislado y controlado donde se hayan aplicado los test y cambios que se ajustan a los criterios específicos de cada organización.
18. El espíritu de estas guías no está dirigido a reemplazar políticas consolidadas y probadas de las organizaciones sino a 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

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

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

20. 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. Ésta se debía hacer extensible tanto al mantenimiento y gestión de la información como a los procesos de comunicación.

21. 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.

22. 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.

23. 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.

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

25. 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.

26. 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 los sistemas en un correcto y continuo estado de funcionalidad y garantizar la protección de los mismos.

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

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

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

28. 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 y 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

29. 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.

30. 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.

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

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

- Proteger los activos a su cargo. El planteamiento de un servicio tiene como premisa el facultar el acceso, o proporcionar datos a los ciudadanos, en función de sus necesidades y 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 mismo se deberá tener en consideración todo el perjuicio que, sobre las personas a las que pertenecen dichos datos, pudiera recaer debido a una mala práctica.

32. Atendiendo a la capacidad de la Administración Pública para establecer mecanismos y controles sobre sus sistemas y servicios, se definió la figura de las dimensiones de seguridad; éstas diferencian y determinan el impacto que una amenaza podrá realizar sobre los activos de una organización en base a una serie de condiciones. Los términos de dimensiones de seguridad son ampliamente recogidos en todos los aspectos de seguridad de la Tecnología de la Información (TI) y recogen conceptos fundamentales para el tratamiento de sistemas, servicios e información. Las dimensiones de seguridad recogidas en el ENS son cinco:
    - Disponibilidad (D).
    - Autenticidad (A).
    - Integridad (I).
    - Confidencialidad (C).
    - Trazabilidad (T).
33. Conocidas bien por su nombre o bien por sus iniciales, cada una de las dimensiones requerirá de la aplicación de una serie de medidas que podrán ser de índole técnica, organizativa o procedimental. No todas las medidas deberán ser aplicadas en la misma forma. Atendiendo a la criticidad del servicio prestado o la información manejada, deberán aplicarse unas u otras medidas.
34. La consideración de la criticidad se basará en una serie de preceptos que serán descritos a posteriori. A continuación, se detallan las características de las dimensiones de seguridad y los objetivos fundamentales de cada una de ellas.

5.1.1 DISPONIBILIDAD

35. 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 cuyo objetivo es garantizar las metas estipuladas 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.

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

37. 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.

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

5.1.2 AUTENTICIDAD

39. Dentro del planteamiento de la seguridad en el acceso a los sistemas de la información, uno de los primeros elementos a los que se enfrenta cualquier usuario es la autenticación. "¿Quién eres?" es la pregunta más habitual para el acceso a cualquier servicio. No debería acceder a un sistema quien no hubiera sido autorizado para ello y esto cobra más sentido con 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 otra de las máximas de la seguridad, tal y como recoge el ENS.

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

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

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

43. Los sistemas de autenticación, que pueden emplear las organizaciones para llevar a efecto los procedimientos descritos en el ENS, pueden ser de múltiples índoles y tipologías. 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.

44. 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 la 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

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

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

5.1.4 CONFIDENCIALIDAD

47. 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.

48. 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.

49. 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 implementación de protocolos que emplean cifrado, tales como HTTPS. Éstos son la alternativa a protocolos inseguros por el envío en claro, como el protocolo HTTP.

50. 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.

51. La guía CCN-STIC-807 sobre "Criptología de empleo en el Esquema Nacional de Seguridad" detalla la información de qué algoritmos deben 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

52. A menudo, cuando se ha producido una incidencia, lo que resta es poder determinar qué ha pasado, con objeto de aplicar así las medidas correctoras adecuadas. Para que el análisis pueda ser llevado a cabo, será necesario disponer de información. La dimensión de seguridad de "Trazabilidad", definida en el Esquema Nacional 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.

53. 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.

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

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

5.2 NIVELES DE DIMENSIONES DE SEGURIDAD

56. El conjunto de los servicios que presta una Administración Pública lo configuran una serie de 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.

57. 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).

58. 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.

59. 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

60. 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, se deberá diferenciar siempre la información del servicio. Ambos son de aplicación pero se deben valorar de forma independiente.

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

62. 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.

63. 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.

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

65. 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.

66. 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 la que se trate. Habitualmente los servicios establecen requisitos relevantes en términos de disponibilidad. También es habitual que los demás requisitos de seguridad sobre los servicios deriven de los de la información que se maneja.

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

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

- El nivel de seguridad requerido en el aspecto de AUTENTICIDAD se establecerá en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas; o sea, por personas que no son quienes se cree que son.
- El nivel de seguridad requerido en el aspecto de TRAZABILIDAD se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio.

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

- Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad, que afecte a alguna de las dimensiones de seguridad, supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Se entenderá por perjuicio limitado:
  - La reducción, de forma apreciable, de la capacidad de la organización para atender eficazmente a 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, 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 éstas sigan desempeñándose.
  - El sufrimiento de un daño significativo por parte de 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, 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 parte de 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.

68. 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 sistema".

6. LAS MEDIDAS DE SEGURIDAD EN EL ENS ASOCIADAS A APPLOCKER

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

70. La funcionalidad de AppLocker permite garantizar el cumplimiento de algunas de las medidas definidas en el Esquema Nacional de Seguridad. Debe tomarse en consideración que AppLocker es una funcionalidad adicional que, tal y como se describirá posteriormente, permite un mayor control de lo que sucede en puesto de trabajo y servidores. Así, la implementación de AppLocker cubre tres elementos fundamentales.

   – Configuración de seguridad [op.exp.2].
   – Gestión de la configuración [op.exp.3].
   – Protección frente a código dañino [op.exp.6].

71. La "configuración de seguridad [op.exp.2]", aplicable a todos los niveles, establece entre los criterios que el sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad. 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 al fin que se persigue. Se aplicará la regla de «seguridad por defecto», donde las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo. Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.

72. AppLocker limitará ejecuciones de código indebidas impidiendo que, desde determinadas rutas, se puedan lanzar aplicaciones; esto redunda en el hecho de mínima funcionalidad a la vez que evita que acciones de usuarios no conscientes puedan perjudicar la seguridad del sistema manejado.

73. La "Gestión de la configuración [op.exp.3]", aplicable en nivel medio y alto, define que se gestionará de forma continua la configuración de los componentes del sistema de modo que: a) Se mantenga en todo momento la regla de «funcionalidad mínima» ([op.exp.2]). b) Se mantenga en todo momento la regla de «seguridad por defecto» ([op.exp.2]). c) El sistema se adapte a las nuevas necesidades previamente autorizadas ([op. acc.4]). d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]). e) El sistema reaccione a incidencias (ver [op.exp.7]).

74. Por lo tanto, AppLocker constituye un mecanismo ideal para reforzar la seguridad, establecida por la organización, para puestos de trabajo y servidores.

7. APLICACIONES NO CONTROLADAS: RIESGOS DE EJECUCIÓN

75. Uno de los grandes problemas a los que se han enfrentado tradicionalmente las organizaciones corresponde al del código dañino. Independientemente de su tipología, mecanismo de infección, objetivos, etc., todos los códigos dañinos tienen un elemento común: se ejecutan sin que el usuario sea consciente de dicho hecho. Sistemas como el de Control de Cuentas de Usuario (UAC) han supuesto un gran avance en la lucha contra las aplicaciones maliciosas, pero estos sistemas no son suficiente, máxime cuando a día de hoy los virus, troyanos, gusanos, etc., pueden llegar a ejecutarse en el contexto de usuarios no administradores o aprovechar vulnerabilidades de un sistema para perpetrar la acción maliciosa.

76. Adicionalmente, otro reto crítico que tienen las organizaciones corresponde al hecho de que muchas aplicaciones, a día de hoy, no necesitan de su instalación para ser empleadas. El número de aplicaciones portables ha ido creciendo significativamente e incluso navegadores o aplicaciones de tipo "hacking tool" podrían ser empleadas sin el requisito, tradicional en entornos Microsoft, de ser instaladas con una cuenta privilegiada. Así, un usuario estándar podría llegar a ejecutar una aplicación sin que haya sido instalada, bien sea esta acción realizada de forma consciente o bien de forma totalmente inconsciente.

77. La violación de las normas de uso de aplicaciones en las organizaciones, o bien de la propiedad intelectual, son un problema derivado de ejecuciones no controlables por dichas organizaciones.

78. Así, rutas tales como el escritorio o los archivos temporales de navegación, constituyen un lugar idóneo para la ejecución de aplicaciones fuera de las rutas tradicionales: Archivos de Programa, Windows o las definidas por la propia organización.

79. Hechos tales como descargar un ejecutable a través del navegador o depositar un ejecutable en una ubicación donde el usuario pueda escribir, convierten la ubicación en la que se almacenan dichos ejecutables en un lugar proclive para ejecutar aplicaciones no controlables por la organización.

80. Realmente y para ejecutar el control se necesitan una serie de factores: saber qué se ejecuta y realizarlo con el menor privilegio posible. Por lo tanto y para obtener un mayor control sobre su entorno de escritorio, a través de una serie de planes de bloqueo, es necesario que se incluyan restricciones en el uso de las credenciales de administrador. Se recomienda el uso de usuarios estándar, sin privilegios administrativos, ya que ayuda a limitar los cambios en la configuración que se pueden realizar en el entorno de escritorio; no obstante, el uso de usuarios estándar no impide la instalación o ejecución de software desconocido o no deseado en la organización.

81. Las guías CCN-STIC de la serie 800 siguen esa inspiración, limitando en la medida de lo posible el uso de privilegios de administrador para acciones convencionales como el uso de aplicaciones ofimáticas o la navegación a través de un navegador a sitios internos definidos por la organización. AppLocker lleva aún más allá el control al limitar las ubicaciones desde donde se pueden iniciar los ejecutables.

82. AppLocker ofrece un nivel adicional y, por lo tanto, las organizaciones deberían tomarlo en consideración para agregar un control mayor sobre la ejecución de software en sus sistemas, independientemente de si estos son servidores o puestos de trabajo.

83. AppLocker ofrece, tal y como se verá más adelante, mecanismos altamente controlables por la organización, de tal forma que podrían servir perfectamente para luchar contra un proceso de infección de código dañino toda vez que éste haya sido identificado y, por el contrario, la solución de antivirus no tenga la capacidad de detenerlo. Así, si se identifica un ejecutable con contenido malicioso, podría llegar a bloquearse su ejecución por la firma identificable del mismo e independientemente del lugar desde donde se estuviera ejecutando. Si se conoce el problema puede llegar a bloquearse.

84. La ejecución de aplicaciones es habitual en todos los escenarios donde intervienen las tecnologías de la información, pero es especialmente crítica en aquellos escenarios donde los privilegios concedidos a los usuarios son mayores y éstos tienen alta capacidad para la navegación a través de Internet. A los administradores de los sistemas se les plantean retos críticos donde las funcionalidades operacionales que aporta AppLocker permiten un mayor control de la ejecución de aplicaciones.

85. Dentro de las funcionalidades operativas de AppLocker, cabe destacar las siguientes funcionalidades aplicables por los administradores:

    – Evitar que se ejecute software sin licencia en el entorno de escritorio si dicho software no se encuentra en la lista de aplicaciones permitidas.

    – Evitar que aplicaciones vulnerables y no autorizadas, incluido el malware, se ejecuten en el entorno de escritorio.

    – Impedir que los usuarios ejecuten aplicaciones que consumen innecesariamente ancho de banda de la red o que afectan de otro modo al entorno informático de la empresa.

    – Evitar que los usuarios ejecuten aplicaciones que desestabilizan su entorno de escritorio y que aumentan los costos de soporte técnico.

    – Proporcionar más opciones para una administración eficaz de la configuración del escritorio.

    – Permitir a los usuarios ejecutar aplicaciones y actualizaciones de software aprobadas basadas en directivas, y mantener a su vez el requisito de que solo los usuarios con credenciales administrativas puedan instalar o ejecutar aplicaciones y actualizaciones de software.

    – Ayudar a garantizar que el entorno de escritorio cumple las directivas empresariales y la normativa del sector.

86. Los escenarios fundamentales donde AppLocker es de aplicación, son:

    – Inventario de aplicaciones. AppLocker tiene la capacidad de aplicar su directiva en un modo de solo auditoría, donde toda la actividad de acceso a aplicaciones se recopila en registros de eventos para su posterior análisis. También hay disponibles cmdlets de Windows PowerShell para ayudar a entender el uso y el acceso a las aplicaciones.

- Protección frente a software no deseado. AppLocker tiene la capacidad de denegar la ejecución de aplicaciones con solo excluirlas de la lista de aplicaciones permitidas por grupo de negocios o usuario. Si una aplicación no se identifica específicamente por su publicador, ruta de instalación o hash de archivo, se producirá un error al intentar ejecutarla.
- Cumplimiento de licencias. AppLocker puede proporcionar un inventario de uso del software dentro de la organización, de forma que pueda identificar los programas y aplicaciones correspondientes a sus contratos de licencia de software y restringir el uso de elementos de software basándose en dichos contratos.
- Estandarización de software. Se pueden configurar las directivas de AppLocker para permitir la ejecución solo de aplicaciones admitidas o aprobadas en los equipos de un grupo de negocios. Esto permite una implementación de aplicaciones más uniforme.
- Mejora de la capacidad de administración. Las directivas de AppLocker se pueden modificar e implementar a través de la infraestructura de directiva de grupo existente y pueden funcionar junto con configuraciones creadas mediante directivas de restricción de software. A medida que administra el cambio continuado en el soporte técnico de las aplicaciones de un grupo de negocios, puede modificar directivas y utilizar cmdlets para AppLocker con el fin de probar si las directivas producen los resultados esperados. También puede diseñar directivas de control de aplicaciones para aquellas situaciones en las que los usuarios comparten equipos.

8. APPLOCKER

87. El control de aplicaciones, a través de directivas de seguridad, tiene el inicio con las directivas de restricción de software que, implementadas en Windows 2003, ofrecían mecanismos para evitar la ejecución de aplicaciones en función de reglas. La poca flexibilidad y alcance implicó limitaciones en su uso por parte de algunas organizaciones. No obstante y puesto que el germen de la idea resultaba positivo, Microsoft desarrolló AppLocker como mecanismo más modular, fácil de implementar y con una mayor capacidad de gestión. Las diferencias existentes entre ambos componentes, puede localizarlas en la siguiente dirección de URL:

    https://technet.microsoft.com/es-es/library/ee424367(v=ws.10).aspx

88. La implementación de AppLocker, en escenarios de implementación de guías CCN-STIC de la serie 800, requiere de versiones cliente de tipo empresa Windows 7 Enterprise o Windows 7 Ultimate. AppLocker no se encuentra soportado para Windows 7 Professional ni para ninguna de sus versiones domésticas. También se puede implementar en cualquier versión de servidor a partir de Windows Server 2008 R2, incluyendo Windows Server 2012 R2.

89. La versión Professional de Windows 7 puede emplearse para la creación y gestión de reglas de AppLocker pero no pueden ser aplicadas a sistemas que ejecuten Windows 7 Professional.

90. Toda la gestión de las reglas y características de AppLocker puede realizarse a través de la consola de administración de directivas de grupo (GPMC.msc) o la herramienta de administración local de directivas (GPedit.msc).

91. Microsoft no proporciona una manera de desarrollar extensiones AppLocker. Las interfaces no son públicas. Un usuario con credenciales de administrador puede automatizar algunos procesos de AppLocker mediante cmdlets de Windows PowerShell. Para obtener información acerca de los cmdlets de Windows PowerShell para AppLocker, puede consultar la referencia de comandos de PowerShell para AppLocker.

    https://technet.microsoft.com/es-es/library/ee424349(v=ws.10).aspx

92. AppLocker se ejecuta en el contexto de administrador o LocalSystem, esto debe ser tomado en consideración ya que se proporciona el conjunto de privilegios más alto. Si un usuario con credenciales administrativas realiza cambios en una directiva de AppLocker, en un equipo local unido a un dominio, los cambios se podrían sobrescribir en función de la política GPO que contiene la regla de AppLocker para el mismo archivo (o ruta de acceso) que se hubiera cambiado en el equipo local. Sin embargo y debido a que las reglas de AppLocker son aditivas, todavía se evaluará una directiva local que no está en un GPO para ese equipo. Si el equipo local no está unido a un dominio y, por lo tanto, no es administrado directivas de grupo, cualquier persona con credenciales administrativas podría modificar la directiva de AppLocker.

93. AppLocker establece controles para evitar la ejecución de archivos en un directorio aplicando reglas condicionales. No obstante debe tener en consideración, como buena práctica, la restricción del acceso a archivos estableciendo las listas de control de acceso (ACL) según la directiva de seguridad. Por lo tanto, no se deben eliminar, bajo ningún concepto, los permisos que aplican las diferentes guías CCN-STIC aunque se realice la implementación de AppLocker.

94. AppLocker no protege contra la ejecución de archivos binarios de DOS de 16 bits en una máquina de DOS Virtual (NTVDM) de tecnología NT. Esta tecnología permite ejecutar aplicaciones DOS heredadas y programas de Windows de 16 bits en equipos que usan procesadores Intel 80386 o superior cuando ya hay otro sistema operativo ejecutando y controlando el hardware. El resultado es que los binarios de 16 bits todavía pueden ejecutarse en Windows Server 2008 R2, Windows Server 2012 R2 y Windows 7 cuando AppLocker está configurado para bloquear los binarios y bibliotecas. Si el impedir que aplicaciones de 16 bits se ejecuten es un requisito, se debe configurar la regla de denegación de la colección de reglas de ejecutable para NTVDM.exe. Tampoco se puede utilizar AppLocker para evitar la ejecución de código fuera del subsistema Win32. Por ejemplo, aplicaciones ejecutadas a través de la Máquina Virtual de Java.

95. Adicionalmente a ejecutables y ficheros msi, AppLocker puede controlar VBScript, JScript, .bat, .cmd y secuencias de comandos de Windows PowerShell. No obstante, no puede controlar todo el código interpretado que se ejecuta dentro de un proceso de host, por ejemplo, secuencias de comandos Perl y macros. Para controlar el código interpretado con AppLocker, el proceso de host debe llamar a AppLocker antes de ejecutar dicho código y, a continuación, aplicar la acción devuelta por AppLocker. No todos los procesos de host llaman a AppLocker y, por lo tanto, éste no puede controlar cada tipo de código interpretado como son por ejemplo la macros de Microsoft Office.

96. Las reglas de AppLocker permiten o impiden el inicio de una aplicación. AppLocker no controla el comportamiento de las aplicaciones después de que éstas se han ejecutado. En la práctica, una aplicación que está permitida por AppLocker podría utilizar indicadores para pasar por alto las reglas definidas a través de él e iniciar procesos secundarios. Para entornos altamente críticos, se debería realizar un análisis de las aplicaciones investigándolas de forma minuciosa antes de permitir que se ejecuten mediante reglas de AppLocker.

97. AppLocker es dependiente del servicio de identidad de aplicación y utiliza este servicio para comprobar los atributos de un archivo. Por lo tanto, debe configurarse para iniciarse automáticamente. Con este fin y en la presenta guía, se configurará al menos un objeto de directiva de grupo (GPO) que se aplica en las reglas de AppLocker.

8.1 MÉTODO DE CUMPLIMIENTO Y FUNCIONALIDAD DE APPLOCKER

98. Aunque el modo de funcionalidad convencional para el empleo de AppLocker corresponde a evitar la ejecución de aplicaciones mediante la aplicación del valor “exigir reglas”, AppLocker puede emplearse también en modo auditoría, tal y como se define en la presente guía, para el nivel Bajo de aplicación del ENS.

99. El modo de sólo auditoría, permite que una organización adquiera el conocimiento de la funcionalidad de sus aplicaciones para entender como activar el sistema de AppLocker en modo bloqueo.

100. Aunque AppLocker es bastante versátil, para un equipo concreto no pueden estar habilitados ambos modos. Así, la política habilitada con mayor precedencia para un equipo establecerá que el equipo funciona en modo auditoría o en modo bloqueo.

101. Así, si un equipo se encuentra en una unidad organizativa donde se ha creado una política que fuerza el modo de AppLocker en tipo auditoría, independientemente de las otras políticas que pudieran llegar a afectarle, para este equipo el modo de funcionalidad será auditoría.

102. Una vez habilitado AppLocker, éste funciona en modo restrictivo. Es decir, lo que no se permita de forma explícita quedará bloqueado de forma predeterminada.

103. La configuración de directivas de AppLocker funciona de un modo acumulativo, de tal forma que ésta se irá sumando en función de una serie de reglas de funcionalidad que se definen a continuación.

- En primera instancia, se aplicarán las reglas explícitas para denegar una aplicación, firma de fichero o publicador.
- A continuación, se aplicarán las reglas explícitas para permitir ejecutar una aplicación, firma de fichero o publicación.
- Por último, se aplica la regla implícita de denegar todo lo no permitido expresamente.

104. En el marco de un dominio y cuando se establezcan diferentes políticas de grupo, se sumarán las reglas de configuración de AppLocker de todas ellas, dando como resultado la aplicación de las diferentes reglas definidas en todos los objetos de política de grupo (GPO) que se apliquen sobre el equipo.

105. En el caso de equipos independientes, no vinculados a un dominio, la única política hábil será la local (LGPO), por lo tanto, solo serán de aplicación las reglas definidas a través de dicha directiva.

106. El planteamiento y el diseño de objetos de GPO que ofrece AppLocker permite una gran versatilidad para la implementación de reglas de permisividad y bloqueo. A todos los efectos y para la presente guía, se establece como diseño la creación de una política con las reglas generales y políticas específicas a equipos o grupos de ellos con las excepciones, a las condiciones habituales de seguridad, para los equipos de la organización. Estas excepciones serán aplicaciones en rutas no convencionales o necesidades en ubicaciones concretas y dicho diseño será implementado en las correspondientes guías de paso a paso.

8.2 MECANISMOS BASE PARA EL CONTROL DE APPLOCKER

107. El modo de trabajo convencional de AppLocker consiste en definir rutas de carpetas o ficheros concretos para auditar, permitir o denegar su ejecución. Sin embargo, la configuración de AppLocker permite una mayor versatilidad a la hora de establecer esos controles. Así, AppLocker permitirá:

- Establecer controles por ruta de fichero o carpeta.
- Establecer controles por firma de ficheros.
- Establecer controles por publicador.

108. El modo basado en ruta es el modo convencional y el que menor esfuerzo ofrece a un administrador de infraestructuras. Basa su modo de trabajo en permitir o bloquear rutas específicas de ficheros o bien carpetas, siendo de aplicación a todo su contenido.

109. En el caso del sistema basado en firmas este hace uso de la función hash criptográfica SHA-256. Así y para un fichero concreto, se obtiene su firma y será establecido por GPO el permiso o bloqueo de su ejecución. Cuando el fichero sea ejecutado, se obtendrá su hash y se verificará, en función de las reglas, si éste se encuentra permitido o denegado.

110. El uso del control basado en firma permite un mayor afinamiento a la hora de administrar la ejecución de un fichero concreto, pudiendo impedir que un ejecutable sea renombrado como alguno de los de tipos permitidos y pueda saltarse los mecanismos protegidos. Bajo esta circunstancia y salvo que la firma sea la esperada, la aplicación no se ejecutará.

111. Este método, aunque bastante positivo, requiere una mayor carga de administración. Así y ante actualizaciones de software o nuevas versiones, implicaría el tener que generar nuevas reglas de control. Se deberá hacer uso de este sistema para cuestiones muy concretas donde la aplicación a controlar sea una muy específica que no vaya a cambiar.

112. También, este mecanismo puede ser empleado convenientemente, para el hecho de habiendo detectado un código dañino, crear una regla que bloquee, en toda la infraestructura, la firma del fichero correspondiente.

113. El último de los controles de reglas, se establece para bloquear o permitir aplicaciones en función del editor de la aplicación. Esto se basa en el hecho de que el publicador de un fichero (o aplicación) haya firmado el mismo, a su nombre. La información sería tratada a través de los atributos extendidos que se encuentran en los binarios de la aplicación.

114. Aunque, inicialmente, el uso de controles basados en firma del publicador debería ser uno de los métodos más adecuados para la ejecución de aplicación de fabricantes específicos,

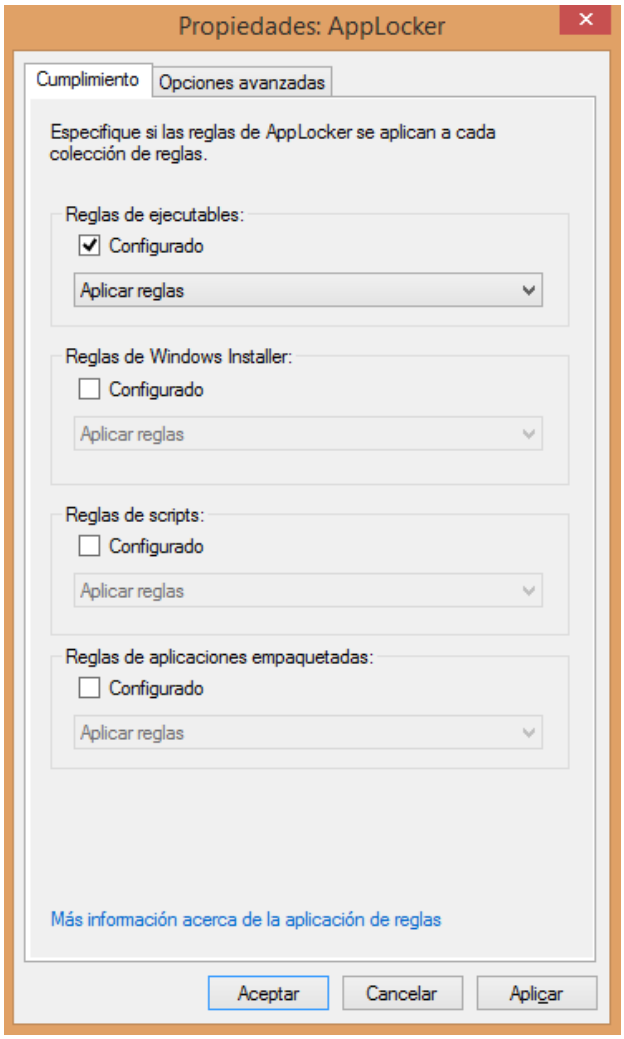
debe tomarse en consideración que no todos los fabricantes firman las aplicaciones o, en ocasiones y como en el caso de Microsoft, solo lo hacen para algunas determinadas.

115. La presente guía establece la metodología base de uso en rutas de ficheros o carpetas. No obstante, se establecerán las condiciones y mecanismos para que el operador pueda generar reglas basadas en firmas para el bloqueo de binarios específicos como aquellos que podrían corresponder a código dañino detectado en la infraestructura.

8.3 TIPOS DE CONTENIDO PARA EL CONTROL DE APPLOCKER

116. Aunque a AppLocker se le conoce fundamentalmente para el control de aplicaciones y lleva a pensar en ficheros de tipo ejecutable con extensión .exe pero existen otros tipos de contenidos que podrían llegar a controlarse mediante AppLocker. Las reglas que permiten administrar los diferentes tipos de ficheros son:

- Reglas de ejecutables.
- Reglas de Windows Installer.
- Reglas de scripts.
- Reglas de aplicaciones empaquetadas.



117. A través de las reglas de ejecutables, se realiza control sobre ficheros con extensión .exe y .com.

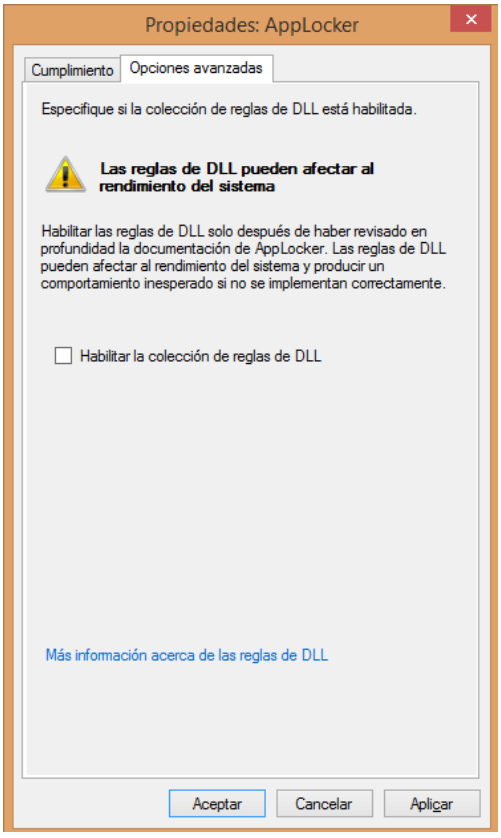
118. A través de las reglas de Windows Installer, se realiza control sobre ficheros con extensiones .msi, .mst y .msp.

119. A través de las reglas de scripts, se realiza control sobre ficheros con las extensiones .ps1, .bat, .cmd, .vbs, .js.

120. El modo de sólo auditoría permite que una organización adquiera el conocimiento de la funcionalidad de sus aplicaciones para, de este modo, entender como activar el sistema de AppLocker en modo bloqueo.

121. Las reglas de aplicaciones empaquetadas basan el control en aplicaciones de tipo .appx concretas e instaladas en un sistema o bien publicadas para una aplicación de este tipo. Este tipo de aplicación es propia de Windows 8, Windows 8.1 y Windows 10. Podría crearse una regla de denegación para el bloqueo de estas aplicaciones. Este tipo de control no tiene consecuencias sobre Windows 7 y sistemas operativos servidor.

122. Adicionalmente, los controles sobre ficheros podrían llegar a extenderse a librerías de vínculos dinámicas del sistema (.dll). No obstante, este tipo de acción no se realiza de forma predeterminada debido a la ralentización que podría llegar a producirse y a la complejidad en el mantenimiento de las reglas. El control a través de las librerías, en caso querer llevarse a cabo, requeriría de habilitar su uso a través de las características avanzadas de AppLocker.



123. La presente guía basa su funcionalidad en el control de ejecutables convencionales. Si fuera necesario, sería posible aplicar mecanismos para el control de otros tipos de ficheros. Como se ha mencionado en el párrafo anterior, se desaconseja emplear AppLocker para el control de archivos DLL.

9. IMPLEMENTACIÓN DE APPLOCKER CON LA GUÍA

124. El objetivo fundamental que se persigue con la implementación de AppLocker, a través de esta guía, es establecer controles para limitar la funcionalidad de código dañino y aplicaciones tipo APT, a la vez que impide al usuario acciones negativas de forma inconsciente, tal y como estipula las medidas definidas en el ENS. Para ello, se van a establecer bloqueos para impedir, fundamentalmente, la ejecución de aplicaciones desde el perfil de los usuarios así como de otras rutas que pudieran ser potencialmente peligrosas.

125. El criterio establecido a través de la presente guía consiste en definir, para el nivel Bajo de implementación en las organizaciones, los controles de AppLocker en modalidad de auditoría. De esta forma, las organizaciones tendrían la capacidad para conocer que estaría sucediendo en sus infraestructuras y los posibles riesgos a los que se enfrentarían.

126. En los casos de niveles Medio y Alto, la guía establece las reglas en modo bloqueo para impedir la ejecución de aplicaciones desde rutas no autorizadas. De esta forma, se establecerán los controles respectivos con el nivel de configuración más seguro que permite AppLocker.

127. Aunque los controles establecidos para AppLocker, a través de la presente guía y para organizaciones con el nivel básico, se implementen en modo de auditoría, se debería evaluar la posibilidad de establecer los controles en modo de aplicación de las reglas y no en este modo.

128. Debe tomarse en consideración, a través de este hecho, que la limitación de ejecución de aplicaciones existentes en el perfil de usuario no debería limitar el uso de las aplicaciones legítimamente instaladas en el equipo. Así, tanto los ejecutables propios del sistema operativo como las aplicaciones existentes en las carpetas de “Archivos de programa” o “Archivos de programa (x86)”, deberían funcionar adecuadamente.

129. Aplicaciones dañinas existentes en archivos temporales de Internet, en ubicaciones temporales o aplicaciones portables existentes en el escritorio del usuario fallarán al no superar los controles específicamente establecidos.

130. La característica de AppLocker proporcionan numerosos mecanismos de control y, por lo tanto, en función de cada organización podrán aplicarse unos u otros. La guía de implementación presente basa la funcionalidad partiendo de una premisa de configuración estándar. Las características de las aplicaciones empleadas por la organización o las funcionalidades operacionales para los equipos podrían requerir configuraciones adicionales a las definidas en la presente guía.

131. La guía ofrece un anexo en modalidad de paso a paso para crear excepciones específicas a las condiciones generales definidas en la presente guía. Debe tenerse en consideración dicho anexo para crear condiciones diferenciales a las establecidas en la presente guía. Si la infraestructura presenta aplicaciones instaladas fuera de las rutas convencionales de archivos de programa, se deberán crear excepciones a las mismas.

132. El objeto fundamental de aplicación del control de AppLocker se realiza sobre los puestos de trabajo, esto es debido a que el riesgo es mayor en los mismos al ser el objeto fundamental de instalación de aplicaciones y navegación a sitios web. No obstante y debido a su consideración, se han creado reglas y condiciones de funcionalidad para los servidores controladores de dominio.

133. En el caso de servidores miembros e independientes, se darán pautas para la creación de reglas de funcionalidad de AppLocker. No obstante, deberá tener en consideración las características de cada uno de los servicios existentes, para que estos servidores presenten una mayor seguridad pero, no por ello, quede mermada su funcionalidad.

134. La implementación de las políticas de AppLocker para el dominio, tanto para controladores de dominio como para puestos de trabajo, muestra la siguiente estructura:

    – Una GPO general con las dos reglas básicas marcadas como forzadas para permitir ejecutables desde la ruta WINDIR y PROGRAMFILES. Adicionalmente, esta política general se encargará de iniciar de forma securizada el servicio "Servicio de identidad de la aplicación (AppIDSvc)" necesario para el funcionamiento de AppLocker. También en esta política, se han establecido reglas para evitar la ejecución de aplicaciones de rutas que, perteneciendo a la carpeta Windows, un usuario estándar podría llegar a escribir. Un ejemplo de este sería el caso de la carpeta "c:\windows\temp", ubicación dentro de la carpeta Windows donde los usuarios del dominio podrían llegar a escribir. Se ha identificado la existencia de código dañino que se copia en dicha ubicación para saltarse los bloqueos, aprovechando la necesidad de permitir la ejecución de ficheros existentes en la carpeta Windows.

    – Una GPO de excepciones con una regla básica predefinida para permitir al grupo "Administradores" ejecutar binarios desde el CD-ROM. Esta política de grupo con excepciones será la que se deberá modificar con el fin de aplicar condiciones de seguridad excepcionales para los sistemas.

En el caso de los sistemas independientes y debido a la imposibilidad de aplicación de políticas de seguridad incrementales se ha definido un mecanismo de implementación específico de AppLocker para el despliegue de las configuraciones de seguridad. Deberá remitirse a los anexos F y G para hacer uso de AppLocker en un puesto de trabajo o servidor independiente.

ANEXO A. PLANTILLAS DE SEGURIDAD PARA LOS CONTROLADORES DE DOMINIO WINDOWS SERVER 2008 R2 Y WINDOWS SERVER 2012 R2

Para la aplicación de la presente guía, se han generado varias plantillas de seguridad para cada uno de los niveles definidos, del Esquema Nacional de Seguridad, que deberán ser aplicadas en la unidad organizativa "Domain Controllers", con el fin de que apliquen a los controladores de domino o, en su defecto, en la unidad organizativa que contenga los controladores de dominio de su organización.

1. PLANTILLAS DE SEGURIDAD PARA EL NIVEL BAJO DEL ENS

En este apartado se indican las plantillas de seguridad correspondientes al nivel bajo de aplicación en el ENS para controladores de dominio.

1.1 CONTROLADOR DE DOMINIO

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS AppLocker Raiz DC - bajo:

CCN-STIC-869 ENS AppLocker Raiz DC - bajo

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Identidad de aplicación (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	NT AUTHORITY\SYSTEM	Leer
Permitir	NT AUTHORITY\SYSTEM	Iniciar, Detener, Poner en pausa y continuar
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	BUILTIN\Opers. de servidores	Control total
Permitir	NT AUTHORITY\SERVICIO	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de control de aplicaciones

Reglas Dll

No se definieron reglas del tipo 'Reglas Dll'.

Reglas ejecutables

Directiva	Configuración

Aplicar reglas de este tipo	Falso

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	%WINDIR%*	Ruta de acceso	No
Permitir	Todos	%PROGRAMFILES%*	Ruta de acceso	No
Denegar	Todos	%WINDIR%\Temp*	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

1.2 EXCEPCIONES PARA CONTROLADOR DE DOMINIO

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS AppLocker Excepciones DC - bajo:

CCN-STIC-869 ENS AppLocker Excepciones DC - bajo
Configuración del equipo (habilitada)
Directivas
Configuración de Windows
Configuración de seguridad
Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	D:\ntds*	Ruta de acceso	No
Permitir	BUILTIN\Administradores	Permitir ejecucion desde CD, DVD solo para Administradores	Ruta de acceso	No
Permitir	Todos	D:\sysvol*	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

2. PLANTILLAS DE SEGURIDAD PARA LOS NIVELES MEDIO Y ALTO DEL ENS

En este apartado se indican las plantillas de seguridad correspondientes a los niveles medio y alto de aplicación en el ENS para controladores de dominio.

2.1 CONTROLADOR DE DOMINIO

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS AppLocker Raiz DC – medio alto:

CCN-STIC-869 ENS AppLocker Raiz DC - medio alto
Configuración del equipo (habilitada)
Directivas

Configuración de Windows
Configuración de seguridad
Servicios del sistema
Identidad de aplicación (Modo de inicio: Automático)
Permisos

Tipo	Nombre	Permiso
Permitir	NT AUTHORITY\SYSTEM	Leer
Permitir	NT AUTHORITY\SYSTEM	Iniciar, Detener, Poner en pausa y continuar
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	BUILTIN\Opers. de servidores	Control total
Permitir	NT AUTHORITY\SERVICIO	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Directiva	Configuración
Aplicar reglas de este tipo	Verdadero

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	%WINDIR%*	Ruta de acceso	No
Permitir	Todos	%PROGRAMFILES%*	Ruta de acceso	No
Denegar	Todos	%WINDIR%\Temp*	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

2.2 EXCEPCIONES PARA CONTROLADOR DE DOMINIO

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto:

CCN-STIC-869 ENS AppLocker Excepciones DC - medio alto

Configuración del equipo (habilitada)
Directivas
Configuración de Windows
Configuración de seguridad
Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	D:\ntds*	Ruta de acceso	No
Permitir	BUILTIN\Administradores	Permitir ejecucion desde CD, DVD solo para Administradores	Ruta de acceso	No
Permitir	Todos	D:\sysvol*	Ruta de acceso	No

Reglas de Windows Installer

No se definieron reglas del tipo 'Reglas de Windows Installer'.

Reglas de scripts

No se definieron reglas del tipo 'Reglas de scripts'.

Configuración del usuario (habilitada)

Configuración no definida.

ANEXO B. PLANTILLAS DE SEGURIDAD PARA LOS CLIENTES WINDOWS 7 ENTERPRISE Y ULTIMATE MIEMBROS DE DOMINIO

Para la aplicación de la presente guía, se han generado varias plantillas de seguridad para cada uno de los niveles definidos, del Esquema Nacional de Seguridad, que deberán ser aplicadas en las unidades organizativas que contengan los equipos Windows 7 a los que sean de aplicación las configuraciones de seguridad definidas por el ENS y la presente guía. Puede hacer uso del filtrado de seguridad para aplicar las siguientes plantillas únicamente a los equipos o grupos de equipos deseados.

1. PLANTILLAS DE SEGURIDAD PARA EL NIVEL BAJO DEL ENS

En este apartado se indican las plantillas de seguridad correspondientes al nivel bajo de aplicación en el ENS para clientes Windows 7 miembros de dominio.

1.1 CLIENTE WINDOWS 7

A continuación se presenta una tabla con la plantilla CCN-STIC- 869 ENS Applocker Raiz W7 Miembro - bajo:

CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Identidad de aplicación (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	NT AUTHORITY\SYSTEM	Leer
Permitir	NT AUTHORITY\SYSTEM	Iniciar, Detener, Poner en pausa y continuar
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SERVICIO	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de control de aplicaciones

Reglas Dll

No se definieron reglas del tipo 'Reglas Dll'.

Reglas ejecutables

Directiva	Configuración

Aplicar reglas de este tipo	Falso

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	%WINDIR%*	Ruta de acceso	No
Permitir	Todos	%PROGRAMFILES%*	Ruta de acceso	No
Denegar	Todos	%WINDIR%\Temp*	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

1.2 EXCEPCIONES PARA EQUIPOS CLIENTE WINDOWS 7

A continuación se presenta una tabla con la plantilla CCN-STIC- 869 ENS Applocker Excepciones W7 Miembro - bajo:

CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo
Configuración del equipo (habilitada)
Directivas
Configuración de Windows
Configuración de seguridad
Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	BUILTIN\Administradores	Permitir ejecucion desde CD, DVD solo para Administradores	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

2. PLANTILLAS DE SEGURIDAD PARA LOS NIVELES MEDIO Y ALTO DEL ENS

En este apartado se indican las plantillas de seguridad correspondientes a los niveles medio y alto de aplicación en el ENS para clientes Windows 7 miembros de dominio.

2.1 CLIENTE WINDOWS 7

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS Applocker Raiz W7 Miembro – medio alto:

CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - medio alto
Configuración del equipo (habilitada)
Directivas
Configuración de Windows
Configuración de seguridad
Servicios del sistema
Identidad de aplicación (Modo de inicio: Automático)
Permisos

Tipo	Nombre	Permiso
Permitir	NT AUTHORITY\SYSTEM	Leer
Permitir	NT AUTHORITY\SYSTEM	Iniciar, Detener, Poner en pausa y continuar
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	NT AUTHORITY\SERVICIO	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Directiva	Configuración
Aplicar reglas de este tipo	Verdadero

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	%WINDIR%*	Ruta de acceso	No
Permitir	Todos	%PROGRAMFILES%*	Ruta de acceso	No
Denegar	Todos	%WINDIR%\Temp*	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

2.2 EXCEPCIONES PARA EQUIPOS CLIENTE WINDOWS 7

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS Applocker Excepciones W7 Miembro – medio alto:

CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - medio alto

Configuración del equipo (habilitada)
Directivas
Configuración de Windows
Configuración de seguridad
Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	BUILTIN\Administradores	Permitir ejecucion desde CD, DVD solo para Administradores	Ruta de acceso	No

Reglas de Windows Installer

No se definieron reglas del tipo 'Reglas de Windows Installer'.

Reglas de scripts

No se definieron reglas del tipo 'Reglas de scripts'.

Configuración del usuario (habilitada)

Configuración no definida.

ANEXO C. PLANTILLAS DE SEGURIDAD PARA LOS SERVIDORES WINDOWS SERVER 2008 R2 Y WINDOWS SERVER 2012 R2 MIEMBROS DE DOMINIO

Para la aplicación de la presente guía se han generado varias plantillas de seguridad para cada uno de los niveles del Esquema Nacional de Seguridad definidos, que deberán ser aplicadas en las unidades organizativas que contengan los equipos servidores Windows Server 2008 R2 y Windows Server 2012 R2 a los que sean de aplicación las configuraciones de seguridad definidas por el ENS y la presente guía. Puede hacer uso del filtrado de seguridad para aplicar las siguientes plantillas únicamente a los servidores o grupos de servidores deseados.

1. PLANTILLAS DE SEGURIDAD PARA EL NIVEL BAJO DEL ENS

En este apartado se indican las plantillas de seguridad correspondientes al nivel bajo de aplicación en el ENS para servidores Windows Server 2008 R2 y Windows Server 2012 R2 miembros de dominio.

1.1 SERVIDORES WINDOWS 2008 R2 Y WINDOWS 2012 R2

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo:

CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Identidad de aplicación (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	NT AUTHORITY\SYSTEM	Leer
Permitir	NT AUTHORITY\SYSTEM	Iniciar, Detener, Poner en pausa y continuar
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	BUILTIN\Opers. de servidores	Control total
Permitir	NT AUTHORITY\SERVICIO	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de control de aplicaciones

Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Directiva	Configuración
Aplicar reglas de este tipo	Falso

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	%WINDIR%*	Ruta de acceso	No
Permitir	Todos	%PROGRAMFILES%*	Ruta de acceso	No
Denegar	Todos	%WINDIR%\Temp*	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

1.2 EXCEPCIONES PARA SERVIDORES WINDOWS 2008 R2 Y WINDOWS 2012 R2

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - bajo:

CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - bajo
Configuración del equipo (habilitada)
Directivas
Configuración de Windows
Configuración de seguridad
Directivas de control de aplicaciones
Reglas Dll
No se definieron reglas del tipo 'Reglas Dll'.
Reglas ejecutables

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	BUILTIN\Administradores	Permitir ejecucion desde CD, DVD solo para Administradores	Ruta de acceso	No

Reglas de Windows Installer
No se definieron reglas del tipo 'Reglas de Windows Installer'.
Reglas de scripts
No se definieron reglas del tipo 'Reglas de scripts'.
Configuración del usuario (habilitada)
Configuración no definida.

2. PLANTILLAS DE SEGURIDAD PARA LOS NIVELES MEDIO Y ALTO DEL ENS

En este apartado se indican las plantillas de seguridad correspondientes a los niveles medio y alto de aplicación en el ENS para servidores Windows 2008 R2 y Windows 2012 R2 miembros de dominio.

2.1 SERVIDORES WINDOWS 2008 R2 Y WINDOWS 2012 R2

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - medio alto:

CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - medio alto

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Servicios del sistema

Identidad de aplicación (Modo de inicio: Automático)

Permisos

Tipo	Nombre	Permiso
Permitir	NT AUTHORITY\SYSTEM	Leer
Permitir	NT AUTHORITY\SYSTEM	Iniciar, Detener, Poner en pausa y continuar
Permitir	BUILTIN\Administradores	Control total
Permitir	NT AUTHORITY\INTERACTIVE	Leer
Permitir	BUILTIN\Opers. de servidores	Control total
Permitir	NT AUTHORITY\SERVICIO	Leer

Auditoría

Tipo	Nombre	Acceso
Errores	Todos	Control total

Directivas de control de aplicaciones

Reglas Dll

No se definieron reglas del tipo 'Reglas Dll'.

Reglas ejecutables

Directiva	Configuración
Aplicar reglas de este tipo	Verdadero

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	Todos	%WINDIR%*	Ruta de acceso	No
Permitir	Todos	%PROGRAMFILES%*	Ruta de acceso	No
Denegar	Todos	%WINDIR%\Temp*	Ruta de acceso	No

Reglas de Windows Installer

No se definieron reglas del tipo 'Reglas de Windows Installer'.

Reglas de scripts

No se definieron reglas del tipo 'Reglas de scripts'.

Configuración del usuario (habilitada)

Configuración no definida.

2.2 EXCEPCIONES PARA SERVIDORES WINDOWS 2008 R2 Y WINDOWS 2012 R2

A continuación se presenta una tabla con la plantilla CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - medio alto:

CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - medio alto

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas de control de aplicaciones

Reglas Dll

No se definieron reglas del tipo 'Reglas Dll'.

Reglas ejecutables

Acción	Usuario	Nombre	Tipo de regla	Excepciones
Permitir	BUILTIN\Administradores	Permitir ejecucion desde CD, DVD solo para Administradores	Ruta de acceso	No

Reglas de Windows Installer

No se definieron reglas del tipo 'Reglas de Windows Installer'.

Reglas de scripts

No se definieron reglas del tipo 'Reglas de scripts'.

Configuración del usuario (habilitada)

Configuración no definida.

ANEXO D. GUÍA PASO A PASO PARA LA CONFIGURACIÓN DE APPLOCKER EN CONTROLADORES DE DOMINIO, SERVIDORES Y CLIENTES QUE LES SEA DE APLICACIÓN EL NIVEL BAJO DEL ENS

El presente anexo, ha sido diseñado para ayudar a los operadores de sistemas a realizar la implantación del servicio AppLocker en una red de dominio y con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad. El presente anexo aplica tanto a controladores de dominio como a servidores Microsoft Windows Server 2008 R2 o 2012 R2 y clientes Windows 7 Ultimate o Enterprise. 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.

La activación, configuración y creación de reglas de AppLocker sobre los clientes y servidores se llevará a cabo mediante GPOs vinculados a las diversas unidades organizativas. No se hará uso de políticas locales en los clientes o servidores para evitar posibles problemas en la aplicación de las mismas. Se definirán dos GPOs, uno que contenga reglas y configuraciones globales y otro destinado a las excepciones y nuevas reglas que puedan surgir con posterioridad a la aplicación de esta guía. Dependiendo de su entorno, es posible que necesite crear nuevas excepciones. Para ello, consulte el anexo H. Las capturas de pantalla de los pasos realizados en el controlador de dominio, corresponden con un entorno Windows Server 2008 R2. No obstante, la aplicación y los pasos descritos en el presente anexo son igualmente válidos para un controlador de dominio basado en Windows Server 2012 R2.

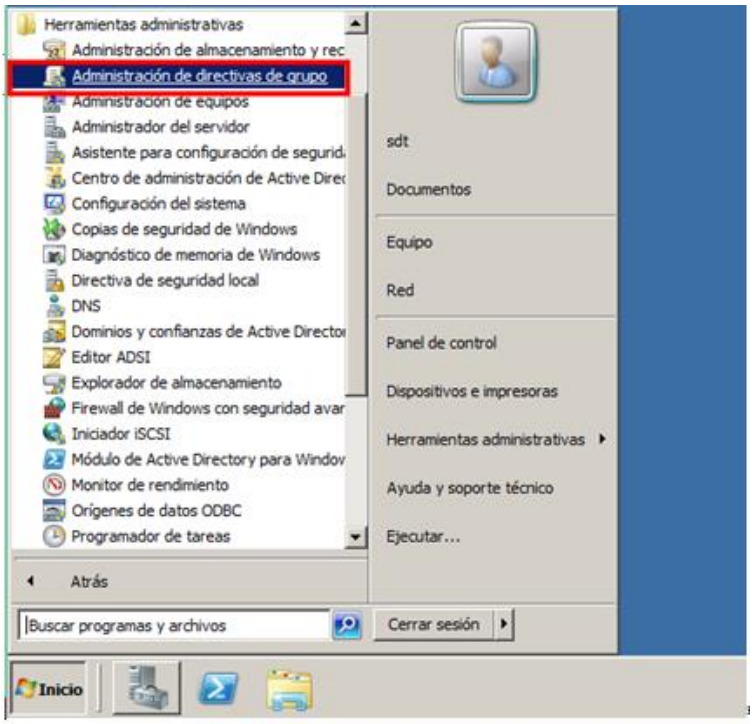
Para la implantación en nivel bajo, según criterios del Esquema Nacional de Seguridad, las reglas de AppLocker se implementarán en modo auditoría. De este modo, no se restringirá la ejecución de ningún binario pero se guardarán eventos de auditoría con información sobre el procesado de las reglas para cada ejecución de software, de tal manera que se aprovecha AppLocker como elemento de auditoría de ejecución de software.

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

1. CONFIGURACIÓN DE APPLOCKER EN CONTROLADOR DE DOMINIO WINDOWS SERVER 2008 R2 O WINDOWS SERVER 2012 R2

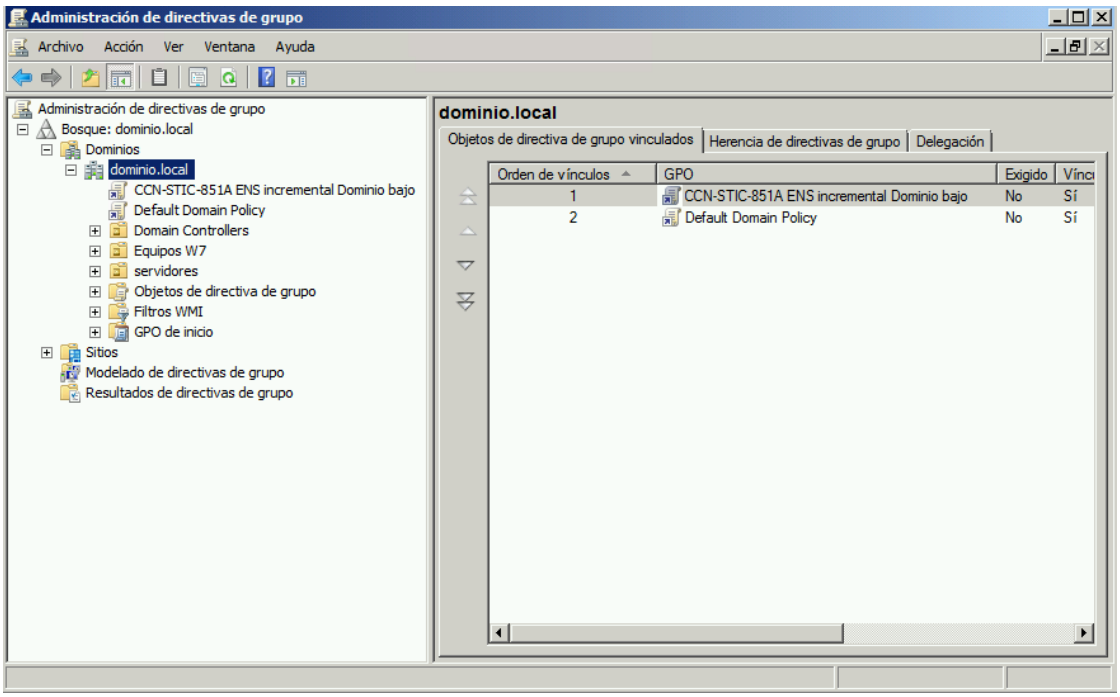
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

Nota: Esta guía asume que a los servidores controladores del dominio, se les ha aplicado la configuración descrita en la guía CCN-STIC-851A para nivel bajo según Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio a securizar con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\scripts" del controlador de dominio.
4.	Asegúrese de que al menos los siguientes directorios hayan sido copiados al directorio “C:\scripts” del controlador de dominio: – CCN-STIC-869 AppLocker Raiz DC – bajo – CCN-STIC-869 AppLocker Excepciones DC - bajo
5.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo.** 
6.	Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos. 

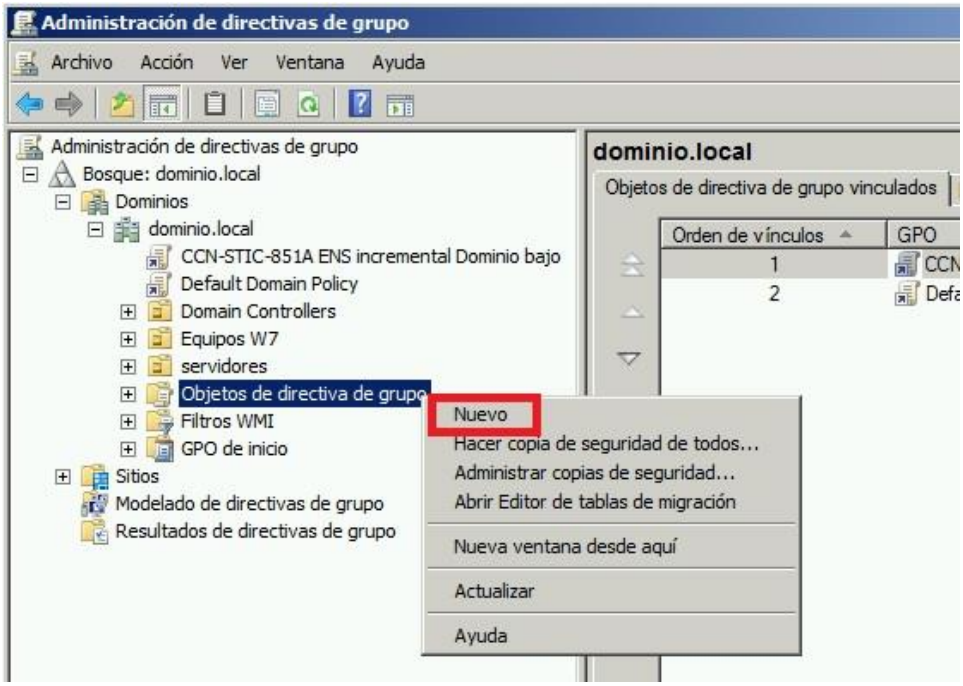
Paso	Descripción

7. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio>,** como se muestra en la siguiente imagen.

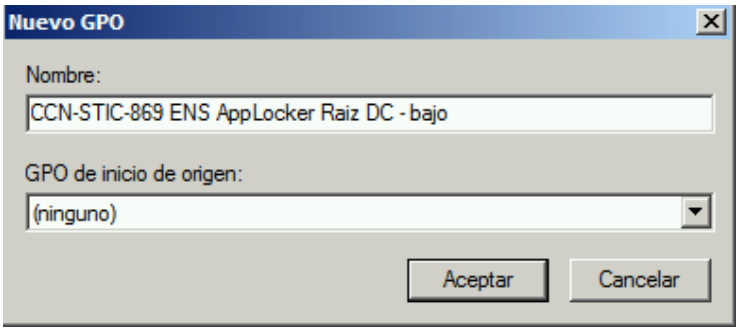


A continuación se procederá a la creación de las GPOs necesarias.

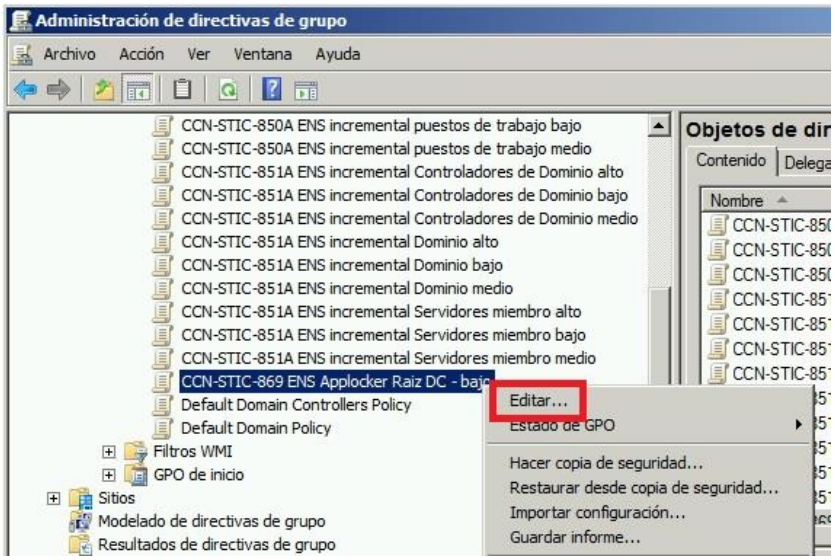
8. Expanda y seleccione el contenedor "**Objetos de directiva de grupo**", y marcando con el botón derecho sobre dicho elemento, elija la opción "Nuevo" del menú contextual que aparecerá.



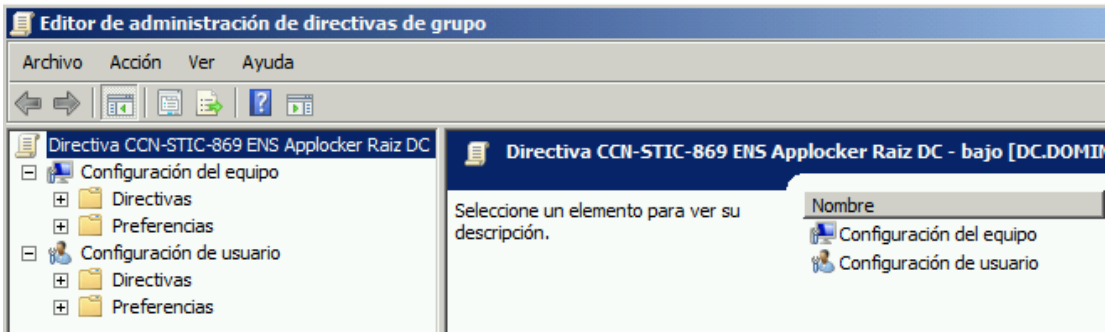
Paso	Descripción
9.	Asigne el siguiente nombre al nuevo GPO: “CCN-STIC-869 ENS AppLocker Raiz DC - bajo” y pulse “Aceptar” para cerrar la ventana.



10.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Raiz DC - bajo**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



11.	Con ello se lanzará el “Editor de administración de directivas de grupo”.



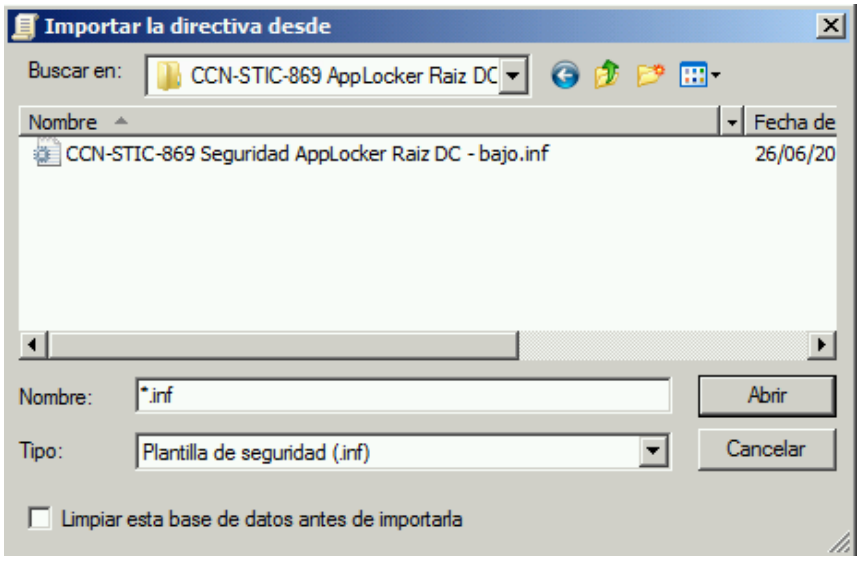
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando primero la configuración de la plantilla de seguridad que acompaña a esta guía, e importando posteriormente la configuración de reglas de AppLocker que aplicarán a los controladores de dominio.

Paso	Descripción

12. En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción “Importar directiva…”

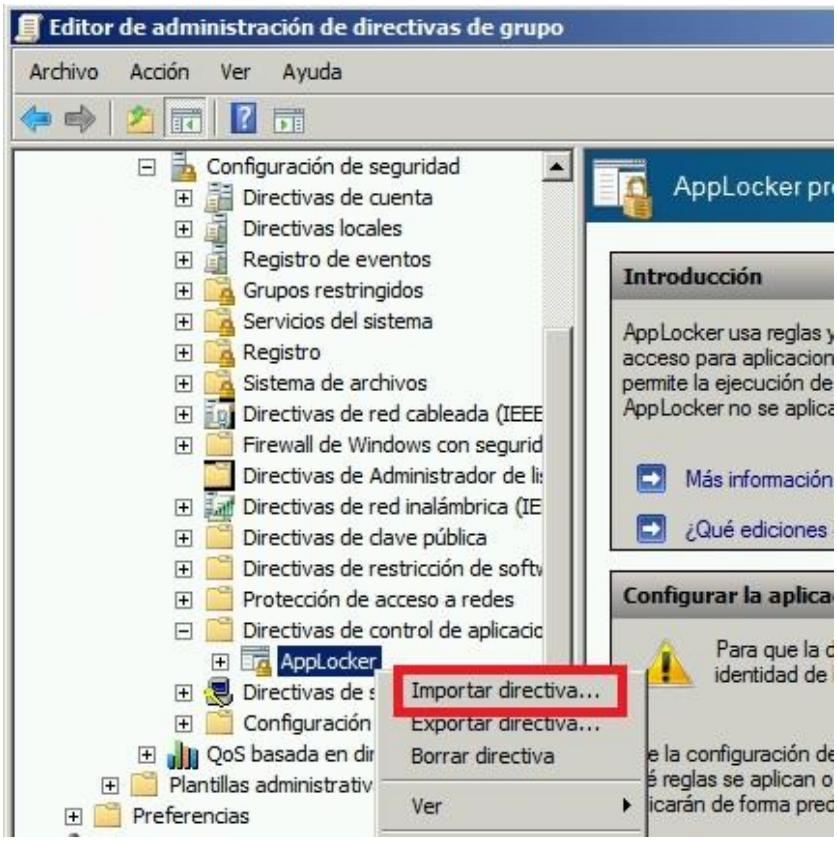
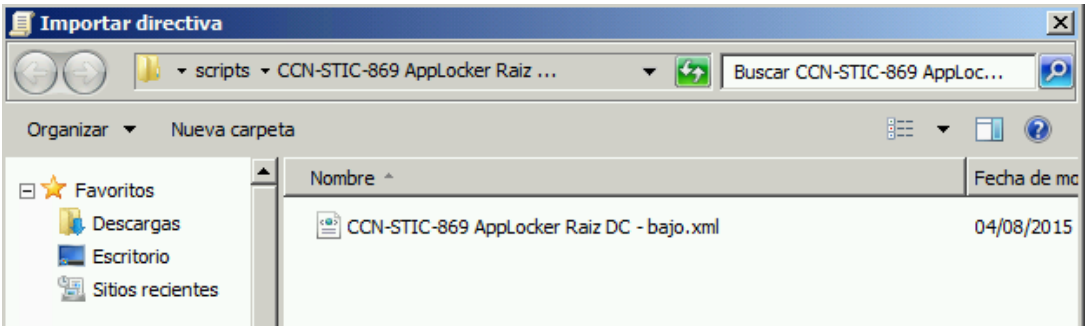
Directiva CCN-STIC-869 ENS AppLocker Raiz DC - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad.

13. En el cuadro de dialogo abierto navegue hasta el directorio “c:\scripts\CCN-STIC-869 AppLocker Raiz DC - bajo” y seleccione el fichero “**CCN-STIC-869 Seguridad AppLocker Raiz DC – bajo.inf**” haciendo doble clic sobre él o pulsando sobre el botón “Abrir”.

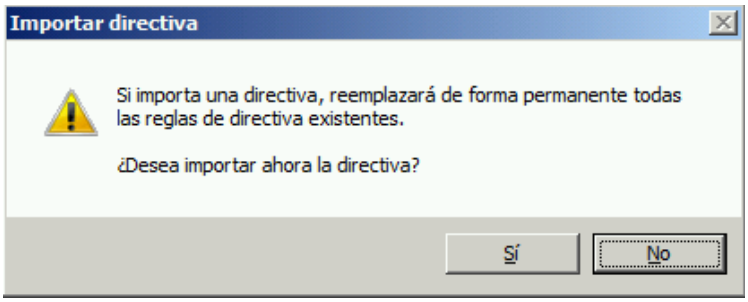


Con ello habrá quedado importada la plantilla de seguridad en este GPO.

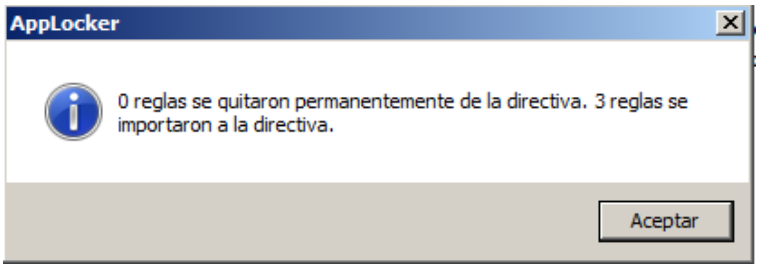
Nota: No cierre todavía el “Editor de administración de directivas de grupo”, y continúe con el siguiente paso.

Paso	Descripción
14.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-ENS 869 AppLocker Raiz DC - bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
15.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\scripts\CCN-STIC-869 AppLocker Raiz DC - bajo” y seleccione el fichero “**CCN-STIC-869 AppLocker Raiz DC – bajo.xml**” mediante doble clic sobre el fichero o pulsando “Abrir”. 

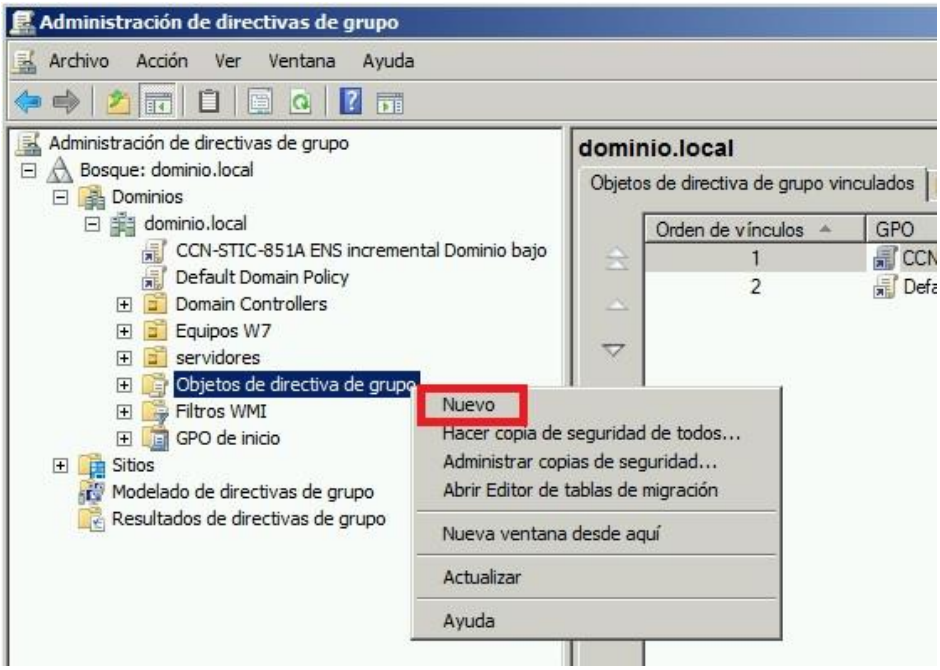
Paso	Descripción
16.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Si”.



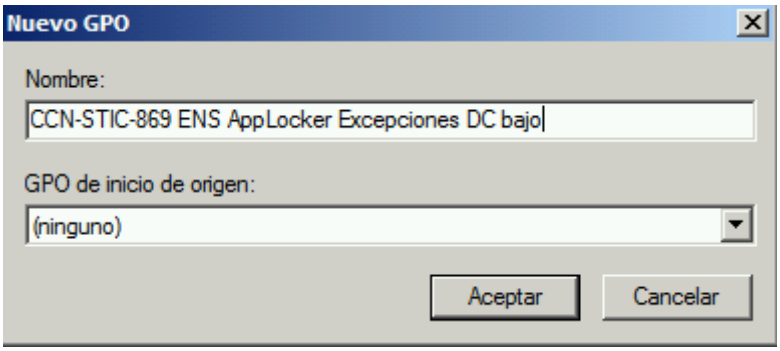
17.	Aparecerá un nuevo mensaje informativo indicando que se importaron tres reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.



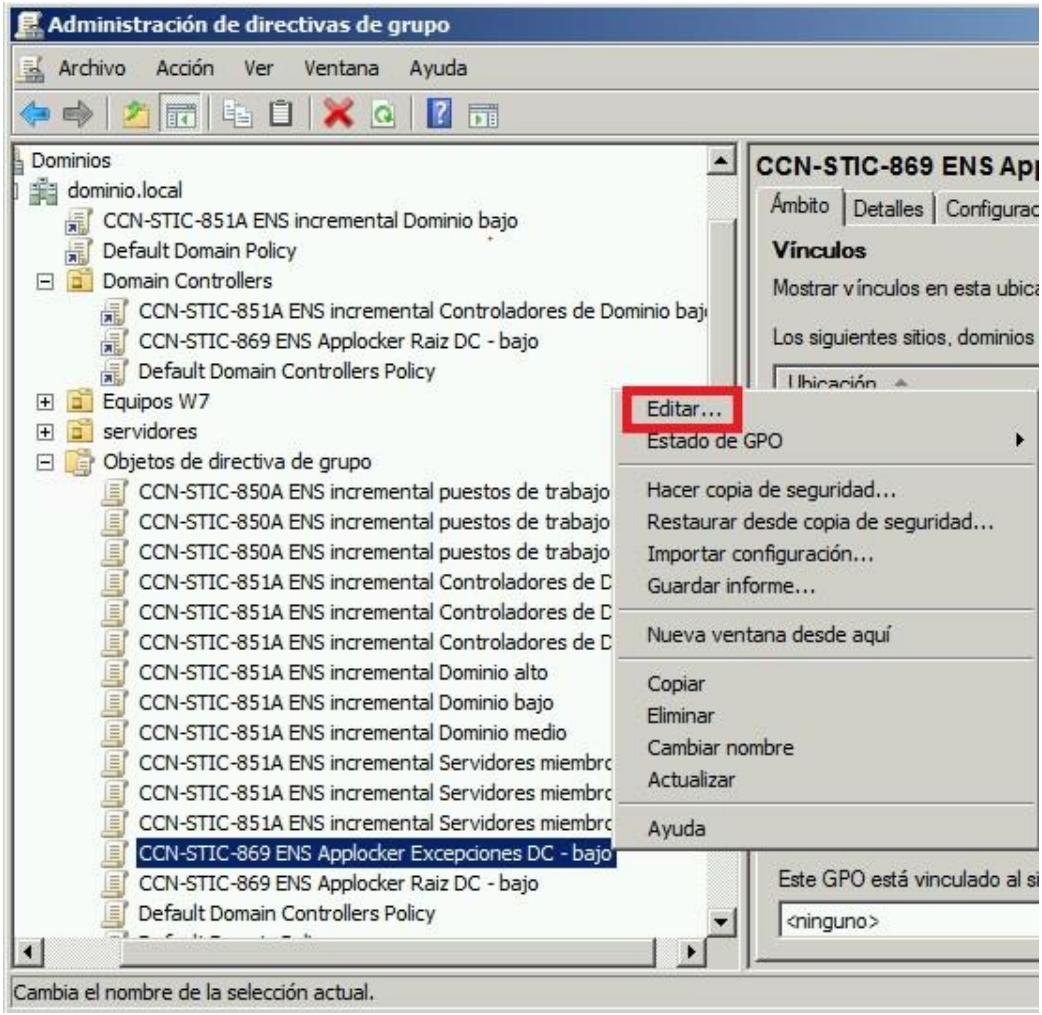
18.	El GPO "CCN-STIC-869 ENS AppLocker Raiz DC - bajo" está creado y configurado. Cierre la ventana del “Editor de administración de directivas de grupo”.
19.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Objetos de directiva de grupo”**, y marcando con el botón derecho sobre dicho elemento, elija la opción “Nuevo” del menú contextual que aparecerá.



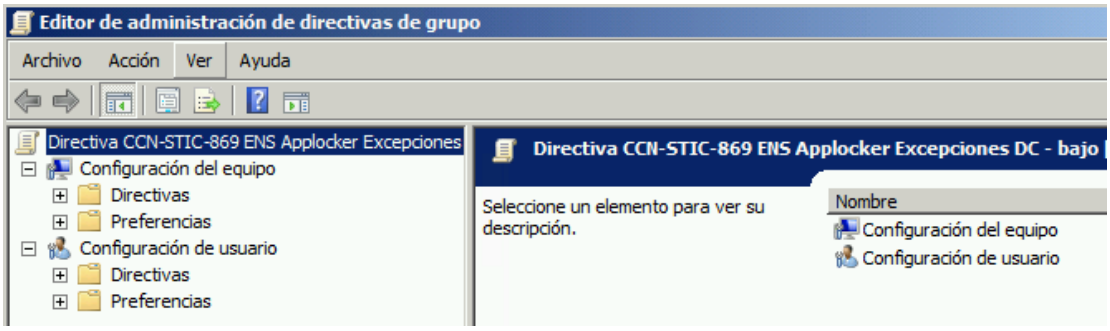
Paso	Descripción
20.	Asigne el siguiente nombre al GPO: “CCN-STIC-869 ENS AppLocker Excepciones DC - bajo” y pulse sobre “Aceptar” para cerrar la ventana.



21.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Excepciones DC - bajo**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



Paso	Descripción
22.	Con ello se lanzará el “Editor de administración de directivas de grupo”.

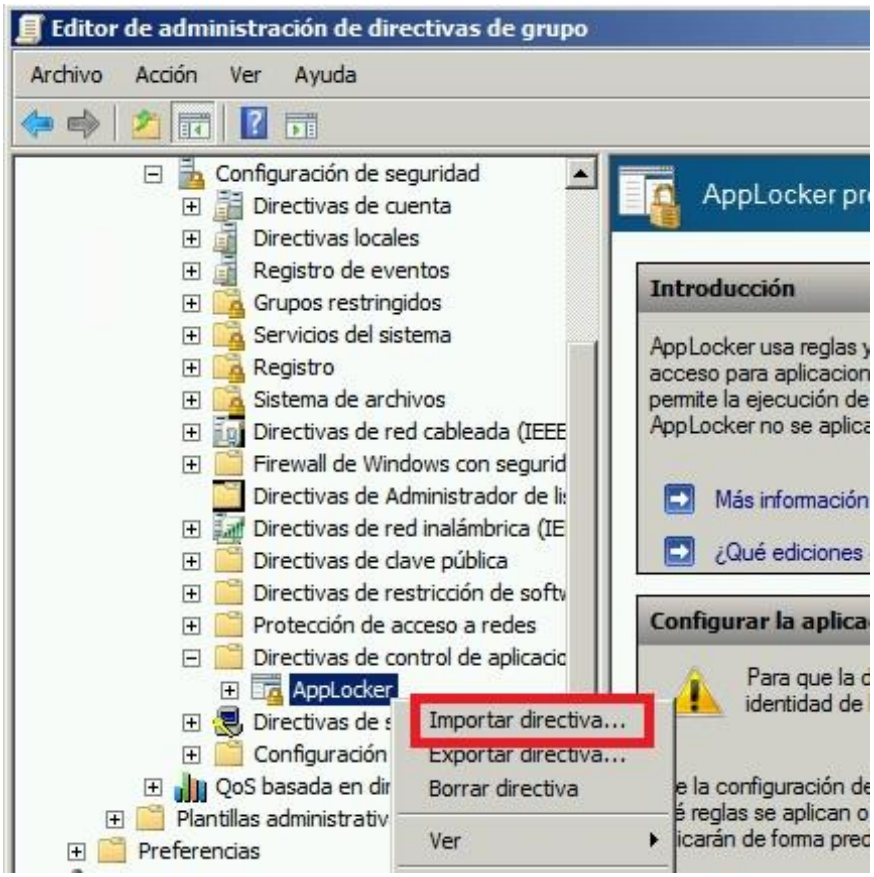


En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando la configuración de las reglas de AppLocker.

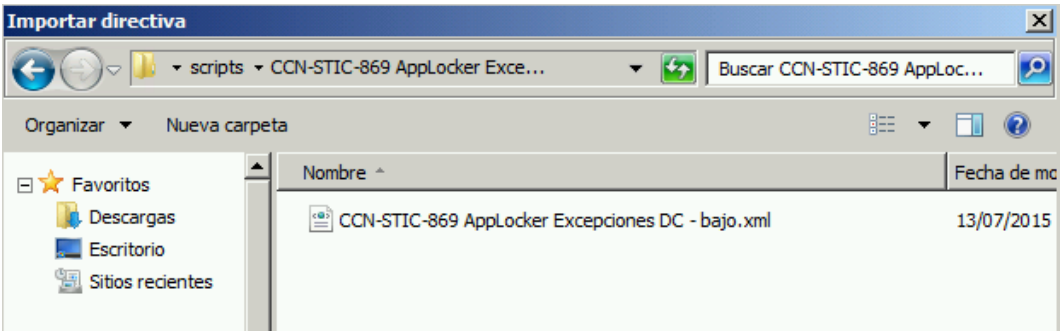
23. En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación:

Directiva CCN-STIC-869 ENS AppLocker Excepciones DC - bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

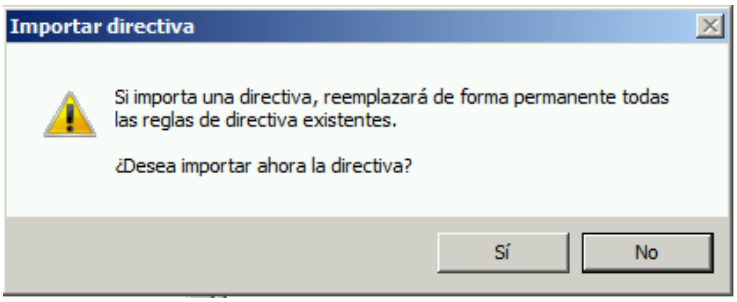
Elija la opción importar directiva del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.



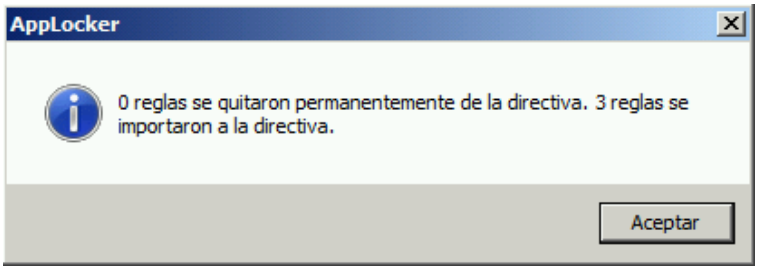
Paso	Descripción
24.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Excepciones DC -bajo”, seleccione el fichero “**CCN-STIC-869 AppLocker Excepciones DC - bajo.xml**” mediante doble clic sobre él o pulsando “Abrir”.



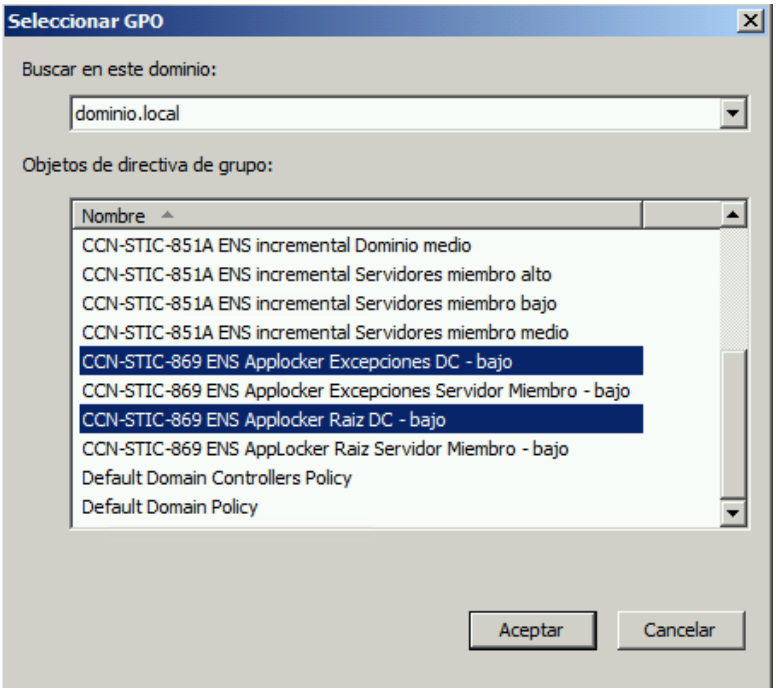
25.	Se le solicitará confirmación ya que la importación de directivas de AppLocker sobrescribe la configuración actual. Seleccione “Sí”.



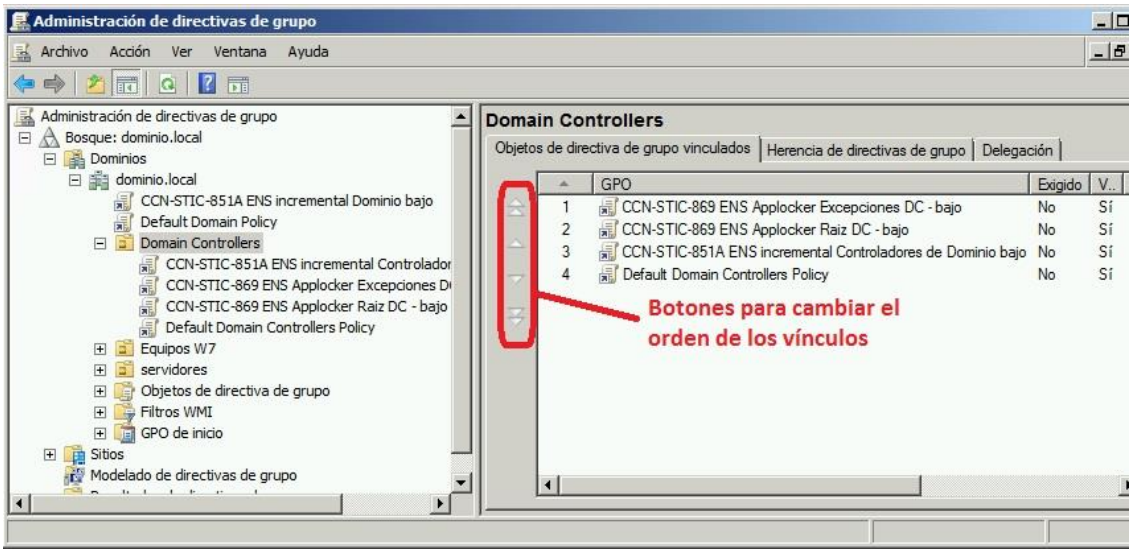
26.	Aparecerá un nuevo mensaje informativo indicando que se importaron 3 reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.



27.	Las reglas recién importadas asumen que el controlador de dominio tiene los ficheros de configuración del directorio activo en la unidad “D:\” (D:\ntds y D:\SYSVOL). Si su caso no es así, puede editar la política de AppLocker en este momento para adaptarla a sus necesidades. **Nota:** En el anexo H, puede encontrar más información sobre los pasos a seguir para la creación, edición, o eliminación de reglas de AppLocker. Tenga en consideración que, en este caso, no será necesario realizar el procedimiento desde una máquina de referencia ya que el GPO no se encuentra vinculado a ninguna Unidad Organizativa.
28.	Cuando termine de adaptar la política a sus necesidades cierre la ventana del “Editor de administración de directivas de grupo” y proceda a la vinculación de los GPO “CCN-STIC-869 ENS AppLocker Raiz DC - bajo" y “CCN-STIC-869 ENS AppLocker Excepciones DC – bajo” a la unidad organizativa donde residan sus controladores de dominio. Sigua los pasos tal y como se detallan a continuación.

Paso	Descripción
29.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Domain Controllers**". Pulse botón derecho sobre la OU y elija la opción "Vincular un GPO existente…" del menú contextual.  **Nota:** Si sus controladores de dominio se encontraran en otra ubicación, vincule la siguiente GPO en dicha OU.
30.	En el nuevo cuadro de diálogo desplegado, seleccione los GPO (haciendo uso de la tecla "CTRL"): "CCN-STIC-869 ENS AppLocker Raiz DC - bajo" y "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo" pulse "Aceptar". 

Paso	Descripción
31.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Domain Controllers**", y observe el orden de los vínculos en la parte central de la ventana.



El orden de los vínculos ha de ser el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones DC – bajo.
2) CCN-STIC-869 ENS AppLocker Raiz DC – bajo.
3) CCN-STIC-851A ENS incremental Controladores de Dominio bajo.
4) Resto de GPOs.

Si el orden mostrado fuera otro, seleccione los GPOs por turnos y utilice los botones indicados en la figura para cambiar el orden de los vínculos de forma que coincida con el indicado.

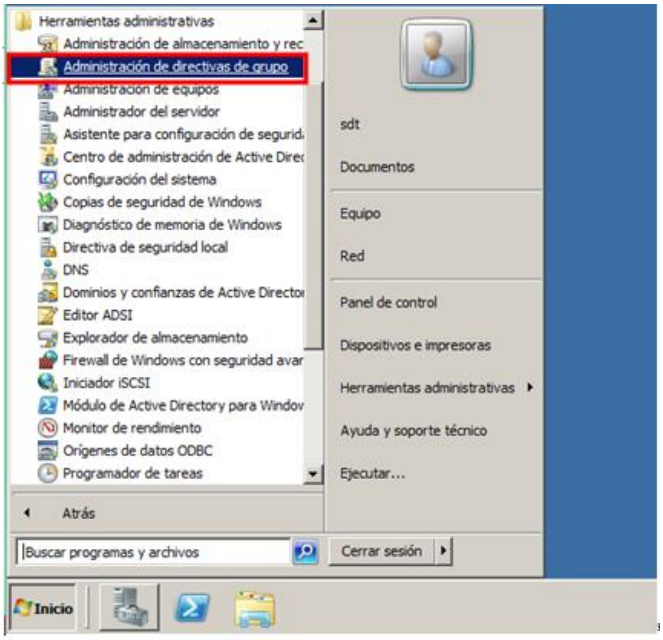
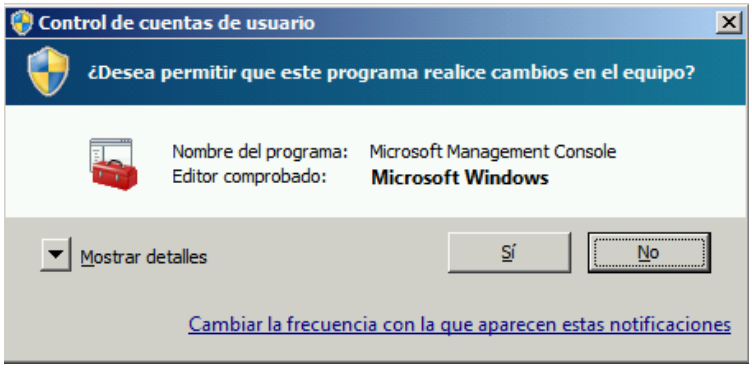
32.	Cierre la ventana del “Administración de directivas de grupo”.
33.	Elimine la carpeta c:\scripts.

2. CONFIGURACIÓN DE APPLOCKER EN SERVIDOR MIEMBRO WINDOWS SERVER 2008 R2 O WINDOWS SERVER 2012 R2

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

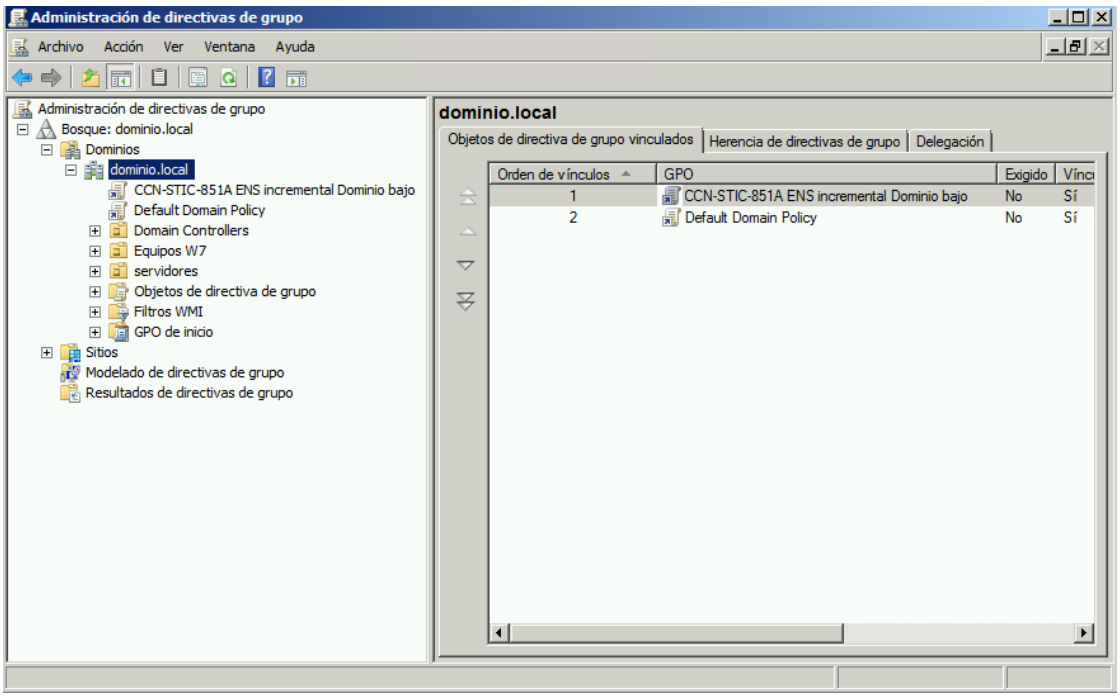
Nota: Esta guía asume que a los servidores controladores del dominio y servidor miembro se les ha aplicado la configuración descrita en la guía CCN-STIC-851A para nivel bajo según Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio.

Paso	Descripción
4.	Asegúrese de que al menos los siguientes directorios hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-869 AppLocker Raiz Servidor Miembro – bajo – CCN-STIC-869 AppLocker Excepciones Servidor Miembro - bajo
5.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo.** 
6.	Pulse “Sí” en la ventana “Control de cuentas de usuario” para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos. 

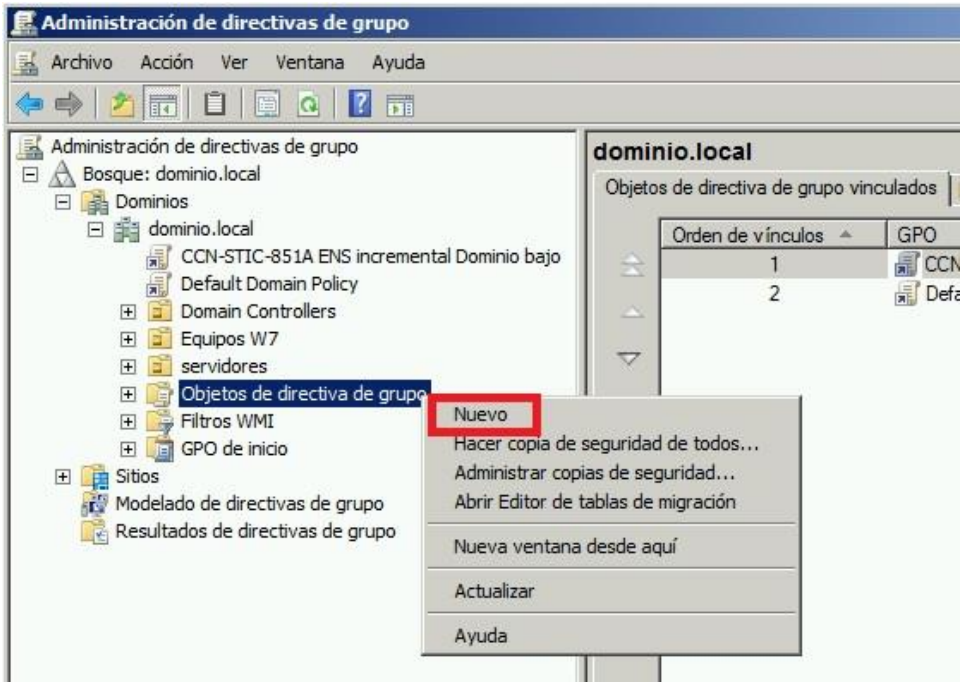
Paso	Descripción

7. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio>,** como se muestra en la siguiente imagen.

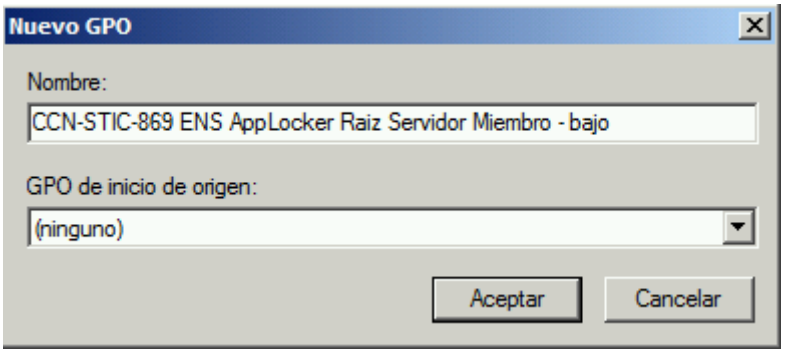


A continuación se procederá a la creación de las GPOs necesarias.

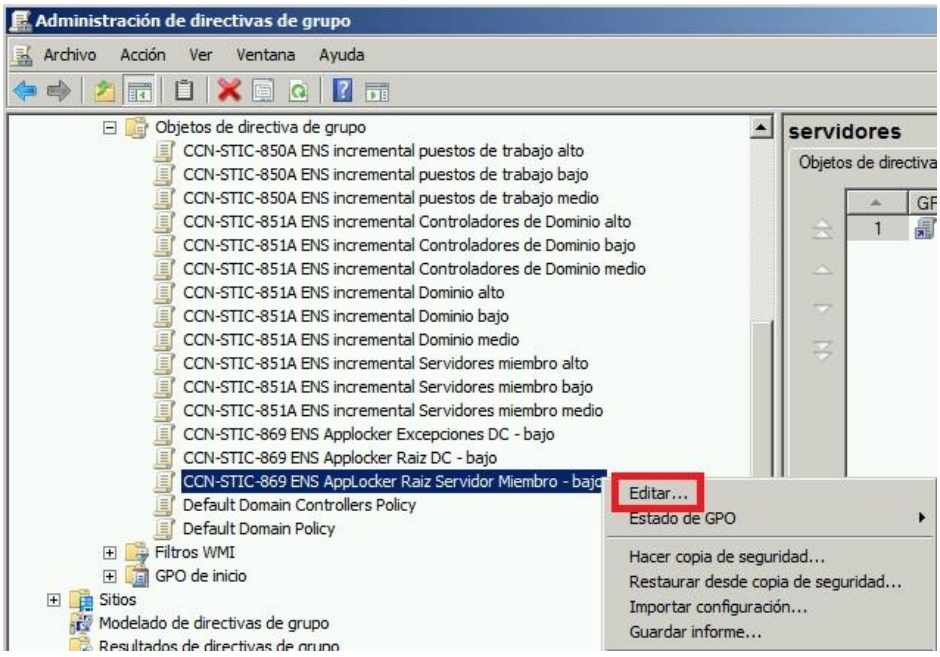
8. Expanda y seleccione el contenedor "**Objetos de directiva de grupo**", y marcando con el botón derecho sobre dicho elemento, elija la opción "Nuevo" del menú contextual que aparecerá.



Paso	Descripción
9.	Asigne el siguiente nombre al nuevo GPO: “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo” y pulse “Aceptar” para cerrar la ventana.

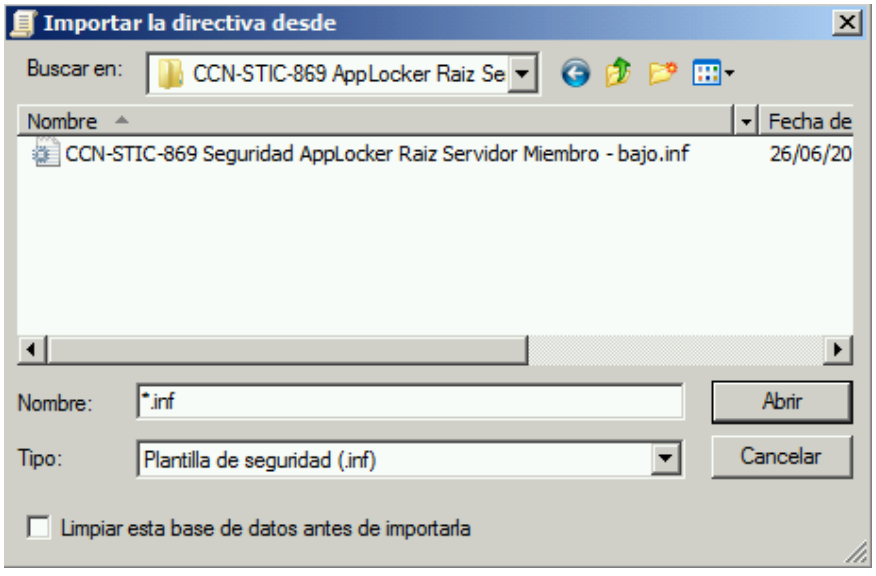


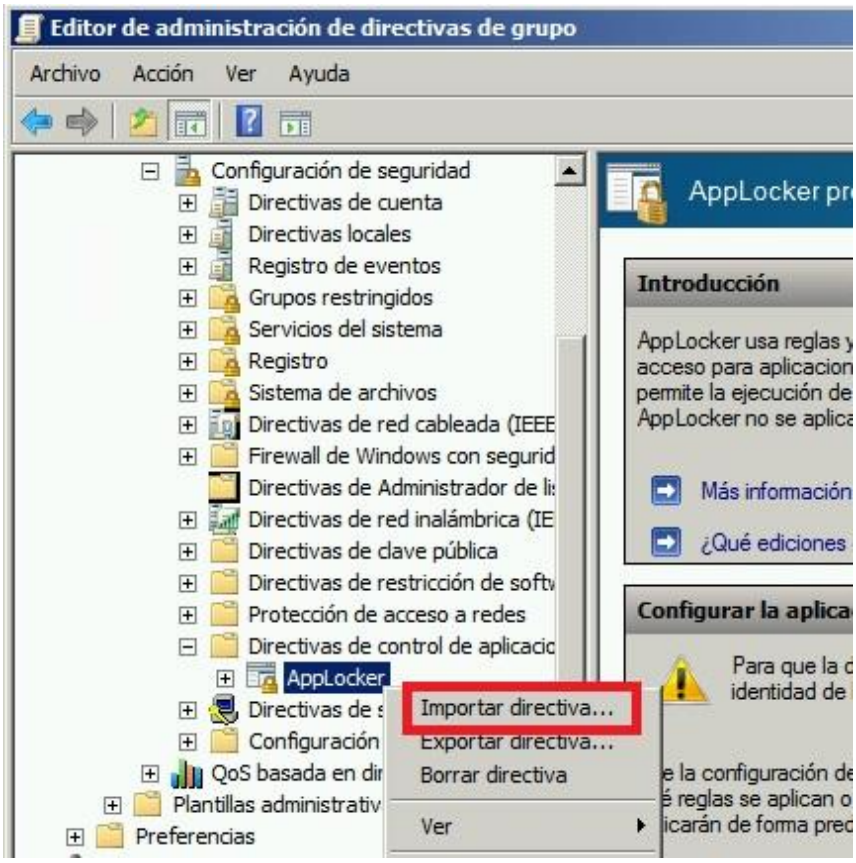
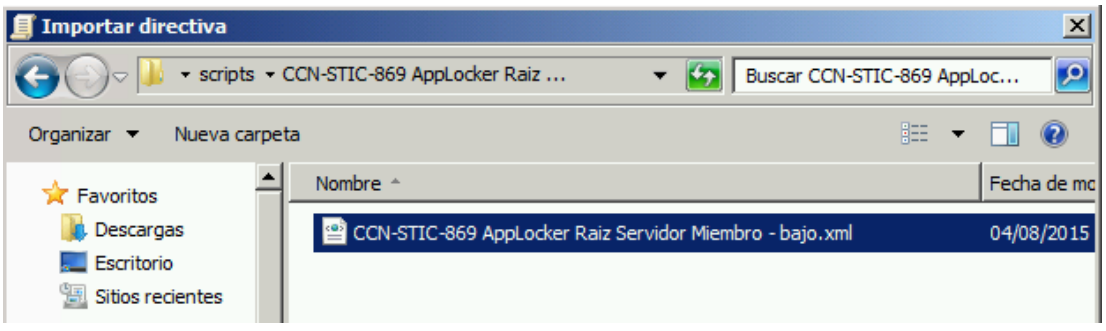
10.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



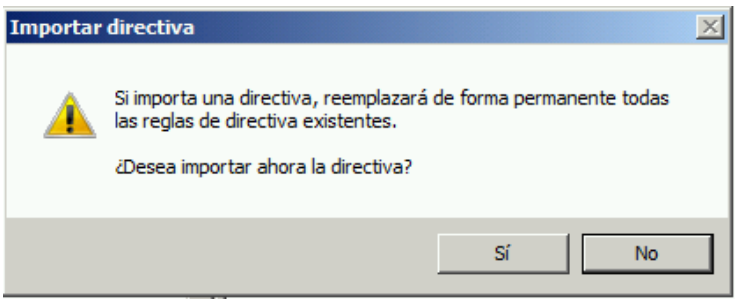
11.	Con ello se lanzará el “Editor de administración de directivas de grupo”.

En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando primero la configuración de la plantilla de seguridad que acompaña a esta guía e importando posteriormente la configuración de reglas de AppLocker que aplicarán a los Servidores Miembros.

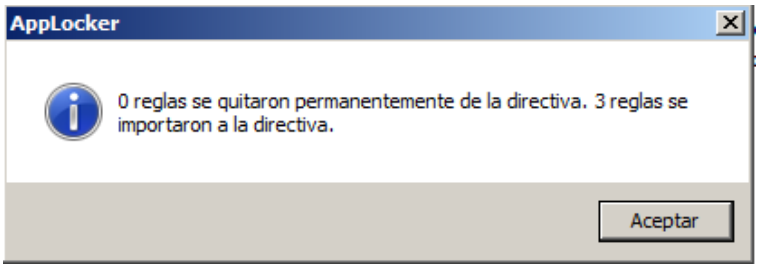
Paso	Descripción
12.	En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción “Importar directiva…” **Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad.** 
13.	En el cuadro de dialogo abierto navegue hasta el directorio “c:\scripts\CCN-STIC-869 AppLocker Raiz Servidor Miembro - bajo” y seleccione el fichero “**CCN-STIC-869 Seguridad AppLocker Raiz Servidor Miembro – bajo.inf**”. Pulse doble clic sobre el fichero o sobre el botón “Abrir” para importar la plantilla.  Con ello habrá quedado importada la plantilla de seguridad en este GPO. **Nota:** No cierre todavía el “Editor de administración de directivas de grupo”, y continúe con el siguiente paso.

Paso	Descripción
14.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-ENS 869 AppLocker Raiz Servidor Miembro - bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
15.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\scripts\CCN-STIC-869 AppLocker Raiz Servidor Miembro - bajo” y seleccione el fichero “**CCN-STIC-869 AppLocker Raiz Servidor Miembro – bajo.xml**” mediante doble clic sobre el fichero o pulsando “Abrir”. 

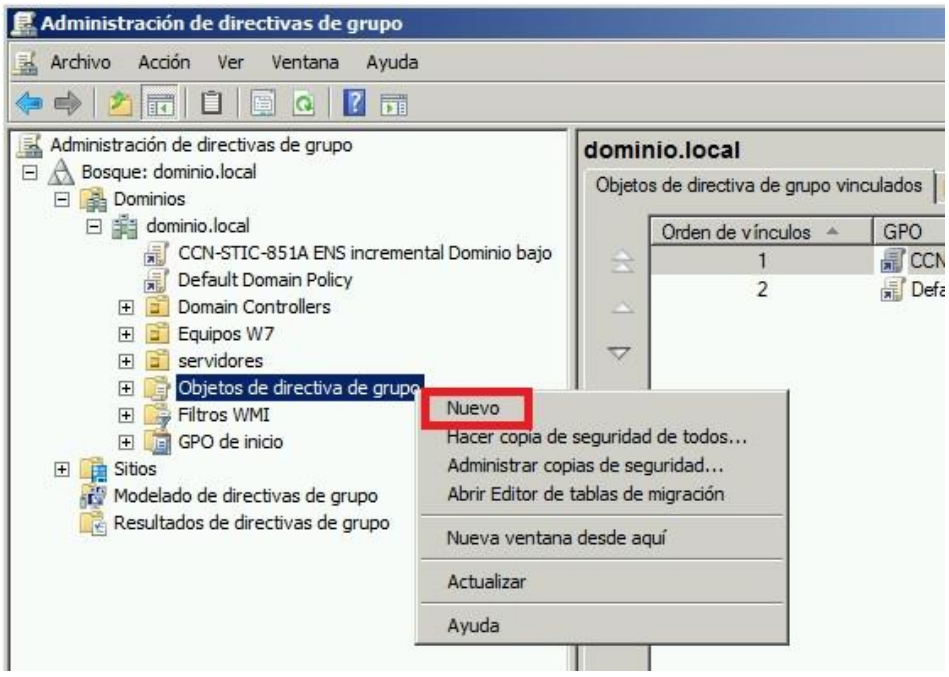
Paso	Descripción
16.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Si”.



17.	Aparecerá un nuevo mensaje informativo indicando que se importaron tres reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.

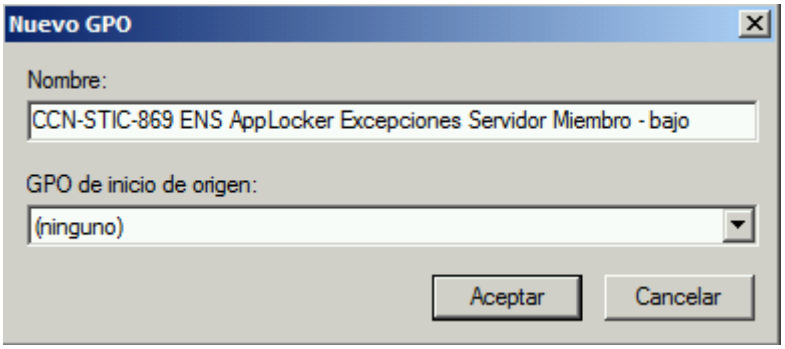


18.	El GPO "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo" está creado y configurado. Cierre la ventana del “Editor de administración de directivas de grupo”.
19.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Objetos de directiva de grupo”**, y marcando con el botón derecho sobre dicho elemento, elija la opción “Nuevo” del menú contextual que aparecerá.

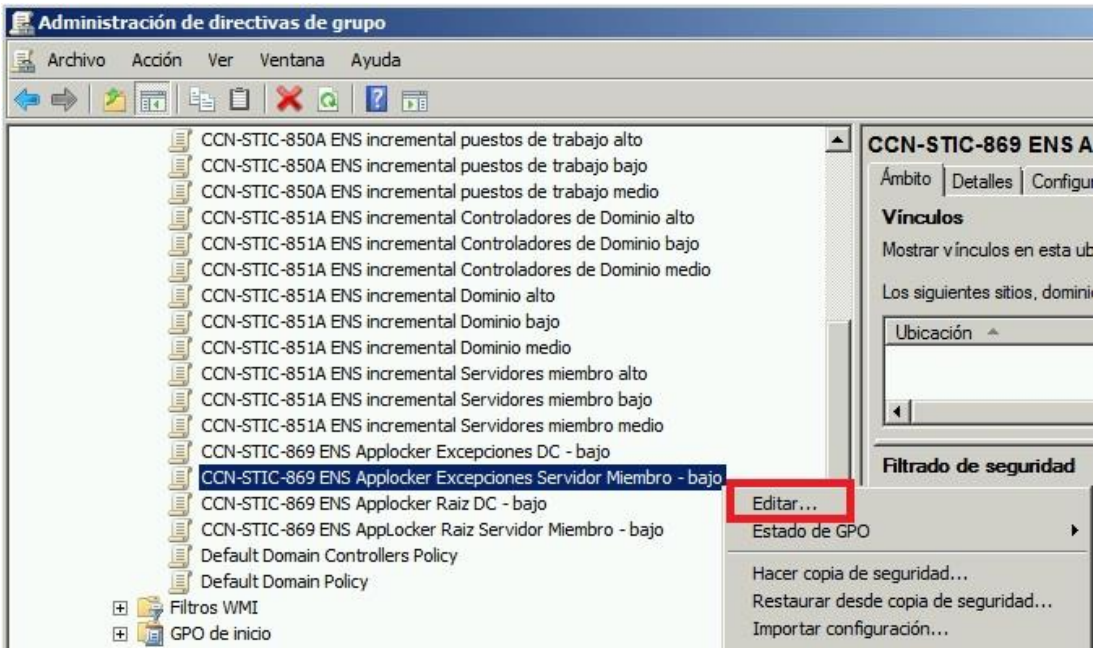


Paso	Descripción

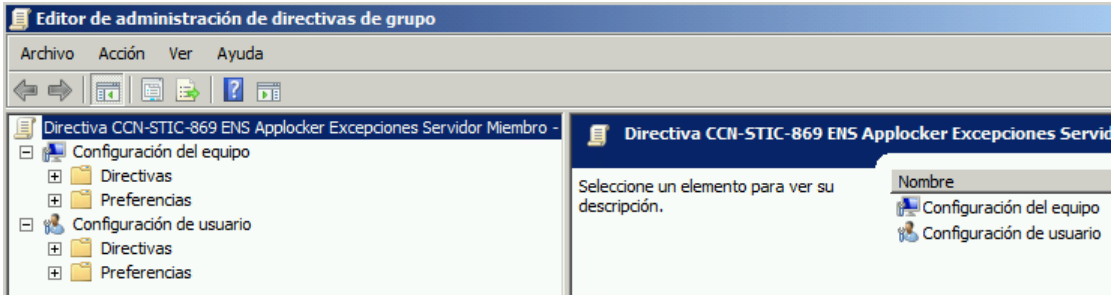
20. Asigne el siguiente nombre al GPO: “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro - bajo”. Pulse “Aceptar” para cerrar la ventana.



21. Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro - bajo**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



22. Con ello se lanzará el “Editor de administración de directivas de grupo”.



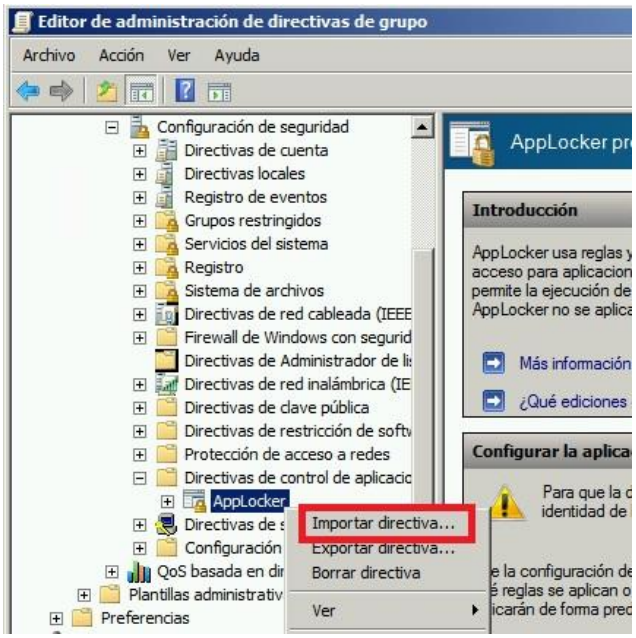
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando la configuración de las reglas de AppLocker.

Paso	Descripción

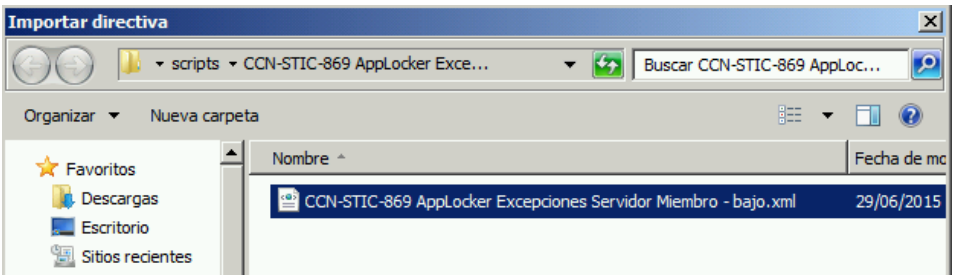
23. En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación:

    Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro - bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

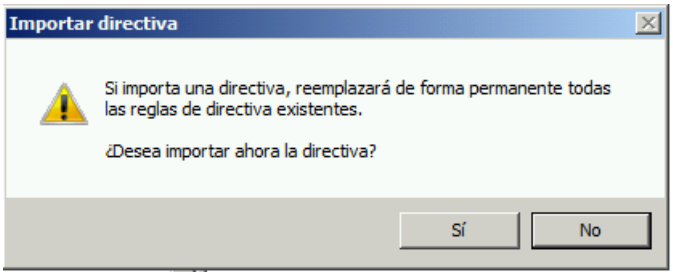
    Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.

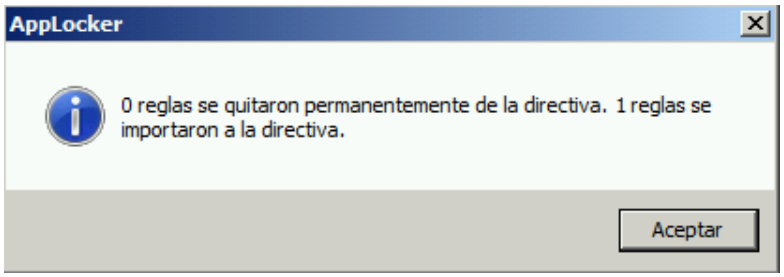


24. En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Excepciones Servidor Miembro -bajo”, seleccione el fichero “**CCN-STIC-869 AppLocker Excepciones Servidor miembro - bajo.xml**” haciendo doble clic sobre él o pulsando “Abrir”.



25. Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



Paso	Descripción
26.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje. 
27.	Antes de vincular los GPO a las unidades organizativas donde residan los servidores miembros ha de evaluar si se hace necesario establecer nuevas reglas de AppLocker para permitir software instalado en rutas no estándar. Si es así no cierre el “Editor de administración de directivas de grupo” y continúe en el paso siguiente. Si por el contrario no desea crear nuevas reglas cierre el “Editor de administración de directivas de grupo” y continúe en el paso 38. **Nota:** La definición de GPO con configuraciones de AppLocker para nivel bajo del Esquema Nacional de Seguridad no activa la aplicación de las reglas de AppLocker. Éstas se encuentran en modo auditoría de tal manera que sólo se guardarán eventos en el fichero de log de AppLocker donde podrá consultar qué ejecuciones habrían sido bloqueadas si la aplicación de las reglas se hubiera encontrado activada. Para más información sobre la creación, edición de reglas de AppLocker consulte el anexo H

Los dos GPO creados en los pasos anteriores (CCN-STIC-869 ENS Applocker Raiz Servidor Miembro - bajo y CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - bajo) no se vincularán a la Unidad Organizativa donde resida el servidor hasta que no se hayan creado las excepciones necesarias para el correcto funcionamiento de los aplicativos del servidor. Se hace necesario evaluar qué rutas extra o nuevos ejecutables se han de permitir antes de la vinculación de los GPO.

Con el objeto de ayudar al administrador a definir dichas rutas, a continuación se enumeran las reglas que por defecto incluyen las dos políticas creadas:

- CCN-STIC-869 ENS Applocker Raiz Servidor Miembro - bajo:
  - Permitir ejecución para todos los usuarios desde %WINDIR%
  - Permitir ejecución para todos los usuarios desde %PROGRAMFILES%
  - Bloquear ejecución para todos los usuarios desde %WINDIR\Temp%
- CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - bajo:
  - Permitir ejecución desde CD y DVD para usuarios Administradores.

La creación de nuevas reglas a modo de excepción se ha de realizar mediante la edición del GPO CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - bajo. El GPO CCN-STIC-869 Applocker Raiz Servidor Miembro - bajo no se debe modificar.

Los siguientes pasos describen la operativa, a modo de ejemplo, para permitir la ejecución de una aplicación instalada en “C:\<aplicación>.

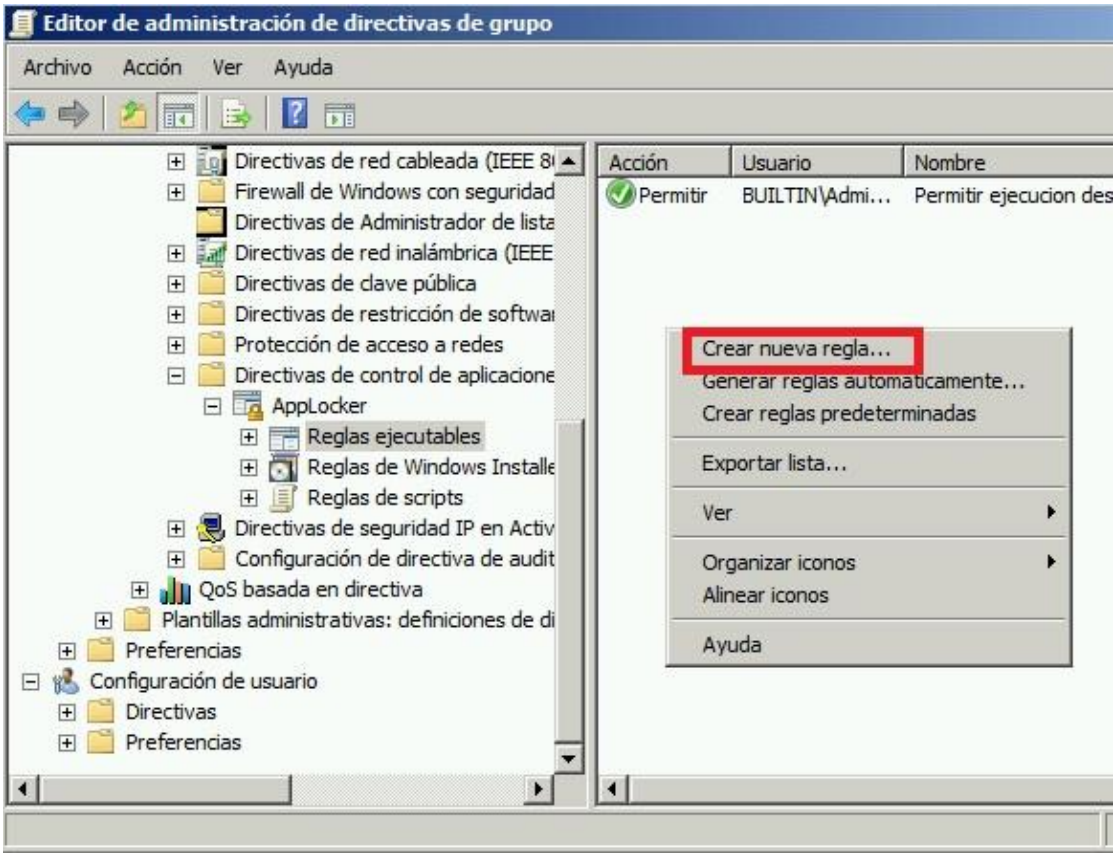
Nota: Para más información sobre la creación y edición de reglas de AppLocker consulte el anexo H.

Paso	Descripción
28.	Haciendo uso del mismo “Editor de administración de directivas de grupo” del paso anterior podrá crear o modificar las reglas que considere.

Nota: Las nuevas reglas para servidores miembros siempre se han de crear sobre la directiva “CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro – bajo”.

Para crear una nueva regla, navegue hasta la ubicación indicada y elija la opción “Crear nueva regla…” del menú contextual que aparece tras pulsar botón derecho en el panel derecho o sobre el objeto “Reglas Ejecutables” del menú situado en el panel de la izquierda.

Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro –bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables

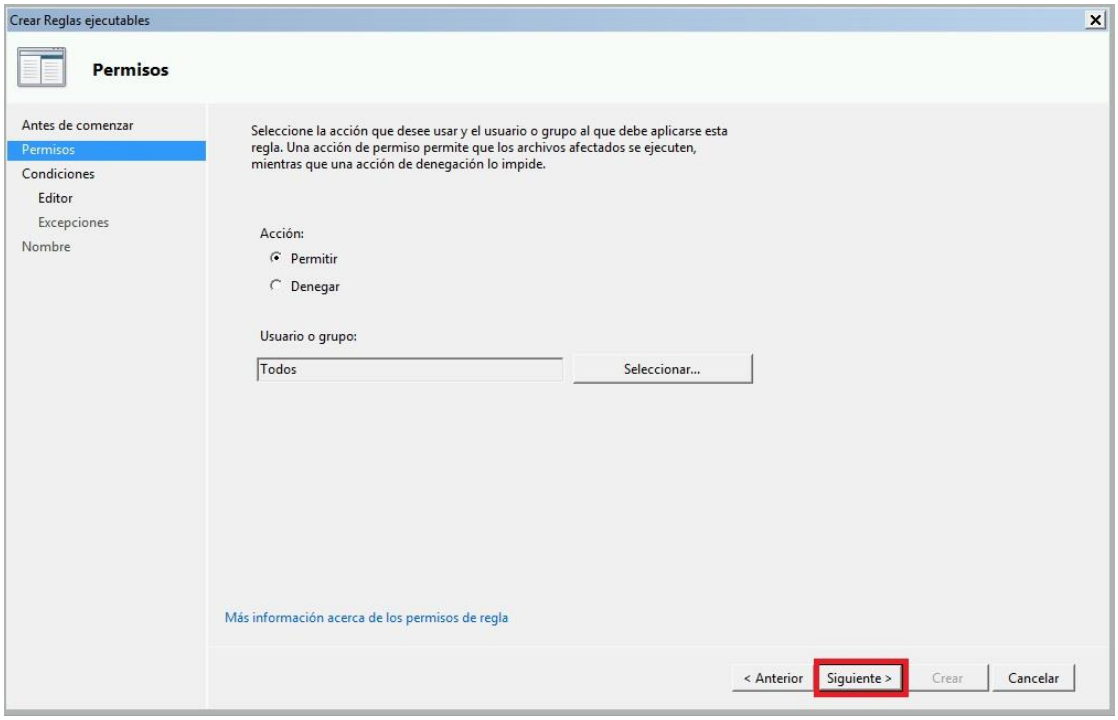


Nota: No es necesario editar la directiva de AppLocker en una máquina de referencia tal y como se describe en el anexo H ya que los nuevos GPO todavía no se encuentran vinculados a ninguna Unidad Organizativa.

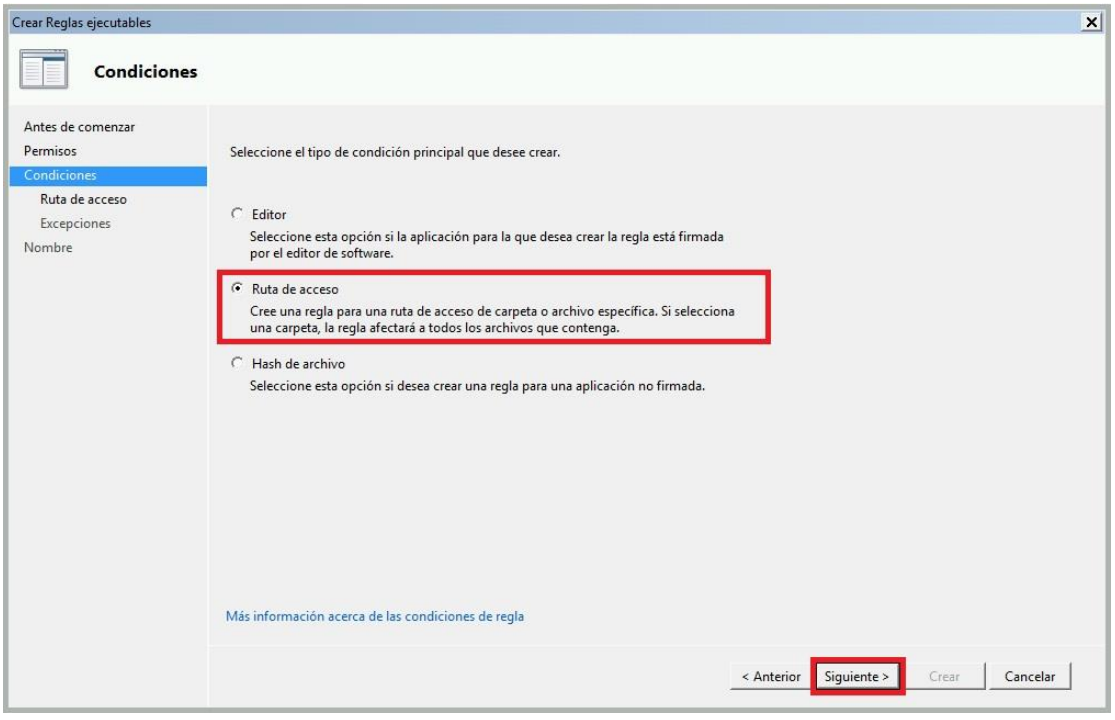
29.	En la primera ventana del asistente pulse “Siguiente >”.

Paso	Descripción

30. En permisos mantenga la configuración existente y pulse el botón “Siguiente >”.

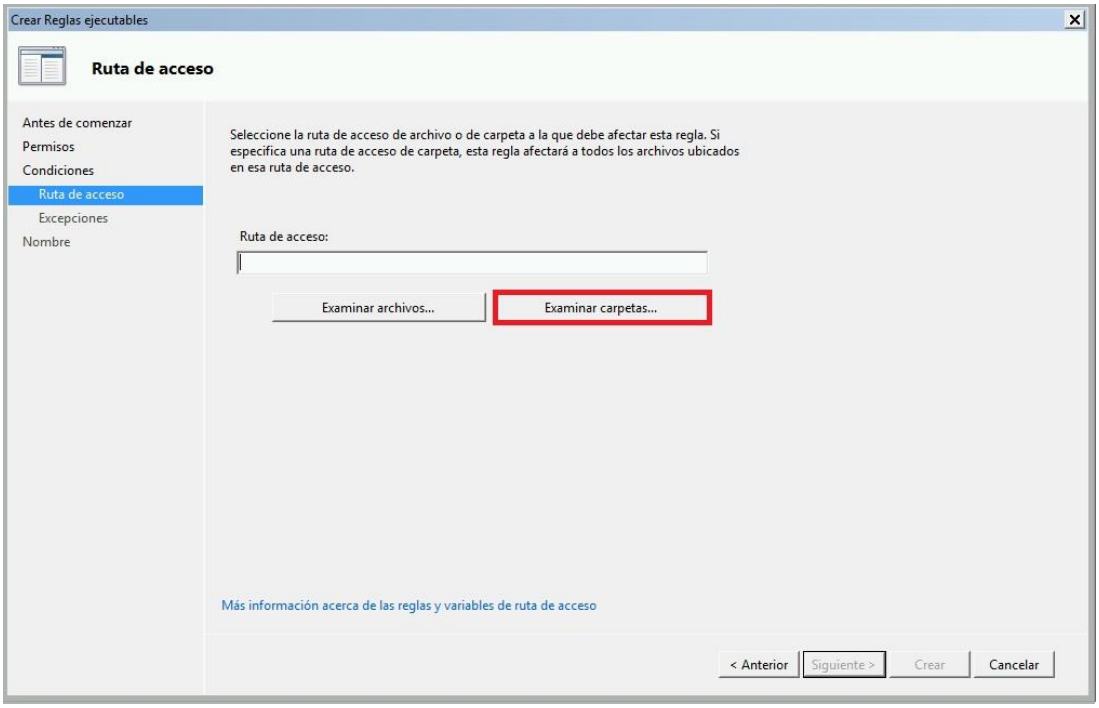


31. En la pantalla de condiciones, seleccione la opción “Ruta de acceso” y pulse “Siguiente >”.



Paso	Descripción

32. En la pantalla “Ruta de acceso” pulse el botón “Examinar carpetas…”.

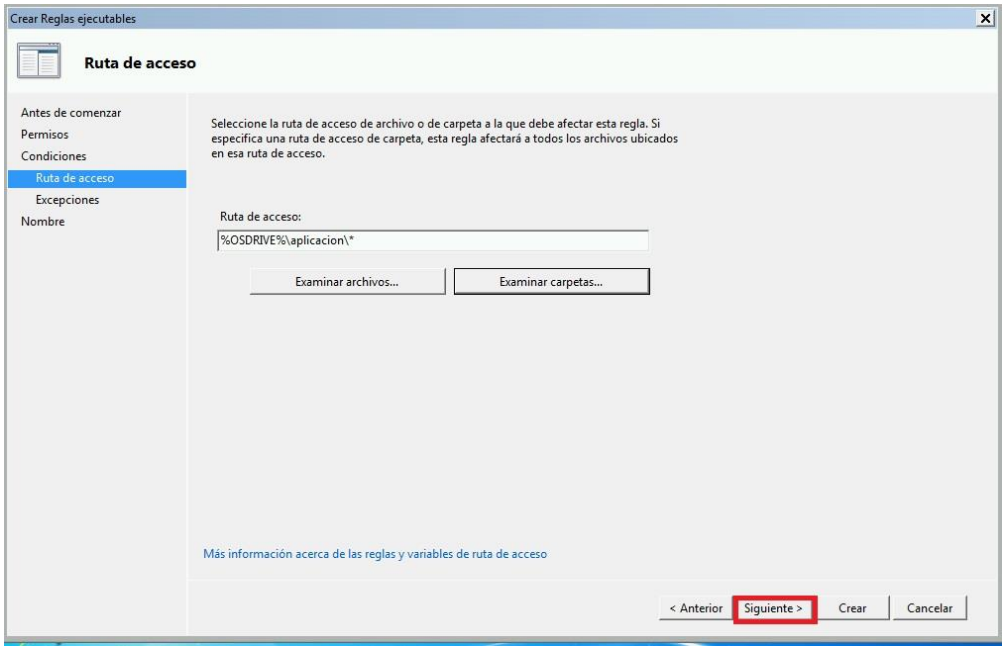


Nota: El ejemplo mostrado simula que se va a permitir ejecutar contenido de una carpeta. Si solo fuera a ejecutar un único archivo .exe de dicha carpeta se debería emplear la opción “Examinar archivos…” y seleccionar el único fichero ejecutable. Debe tener en consideración que las aplicaciones actuales son altamente complejas y puede que la carga de la aplicación se realice a través de un fichero .exe, pero este luego llame o dependa de otros ejecutables. Si tiene claro que la aplicación solo va a necesitar llamar a un fichero ejecutable, puede seleccionar la opción examinar archivos, de lo contrario deberá emplear el mecanismo de examinar carpetas para permitir la ejecución de todo el contenido de dicha carpeta.

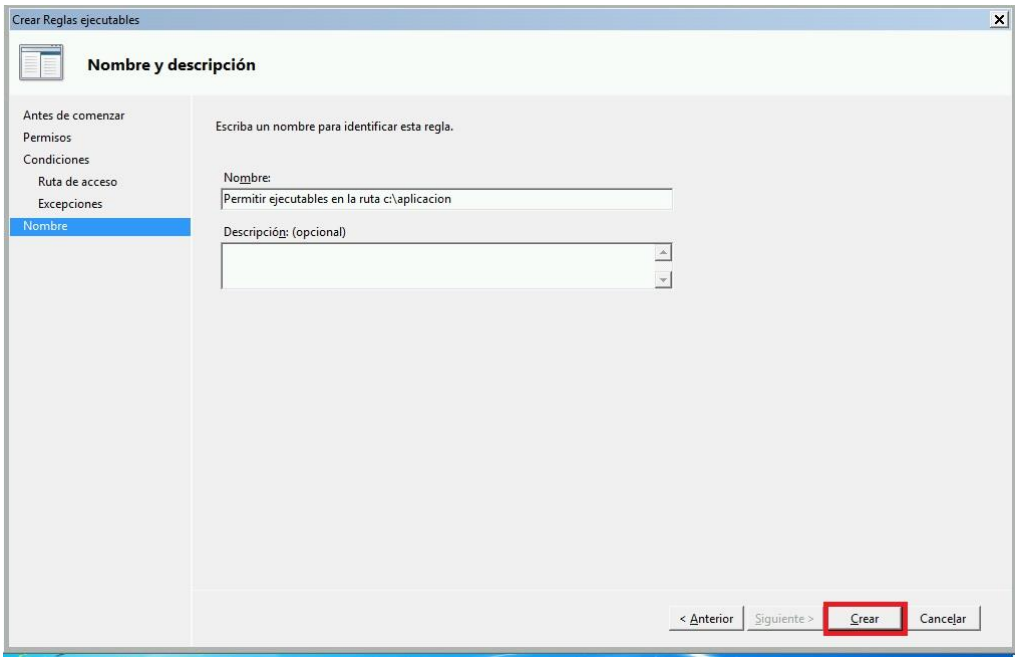
33. Seleccione la carpeta de la que desee crear la excepción. En el ejemplo se establece que el contenido ejecutable se encuentra en la carpeta “C:\aplicacion”.

Nota: Si no existiese la ruta de la aplicación del servidor en el controlador de domino, cree toda la estructura de carpetas necesaria para poder seleccionarla.

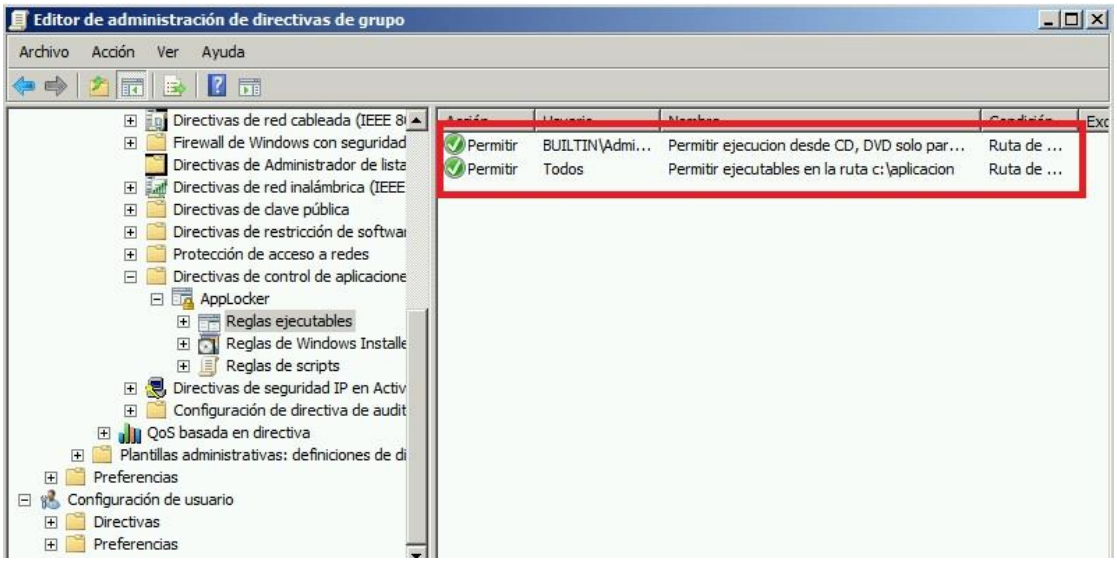
Paso	Descripción
34.	Una vez agregada la carpeta, pulse el botón “Siguiente >”.



35.	Si desea que algún contenido específico en dicha carpeta no sea ejecutado podrá agregar una excepción en la pantalla de “Excepciones”. Bien cuando haya agregado las excepciones o si no desea realizar ninguna excepción, pulse el botón “Siguiente >”.
36.	Para finalizar, deberá asignar un nombre identificativo a la regla. En el ejemplo, se asignará el nombre “Permitir ejecutables en la ruta c:\aplicacion”. Pulse el botón “Crear” cuando haya asignado un nombre.



Paso	Descripción
37.	Compruebe la creación de la regla en el panel derecho del “Editor de administración de directivas de grupo”.



38.	Cierre el “Editor de Administración de directivas de grupo”.

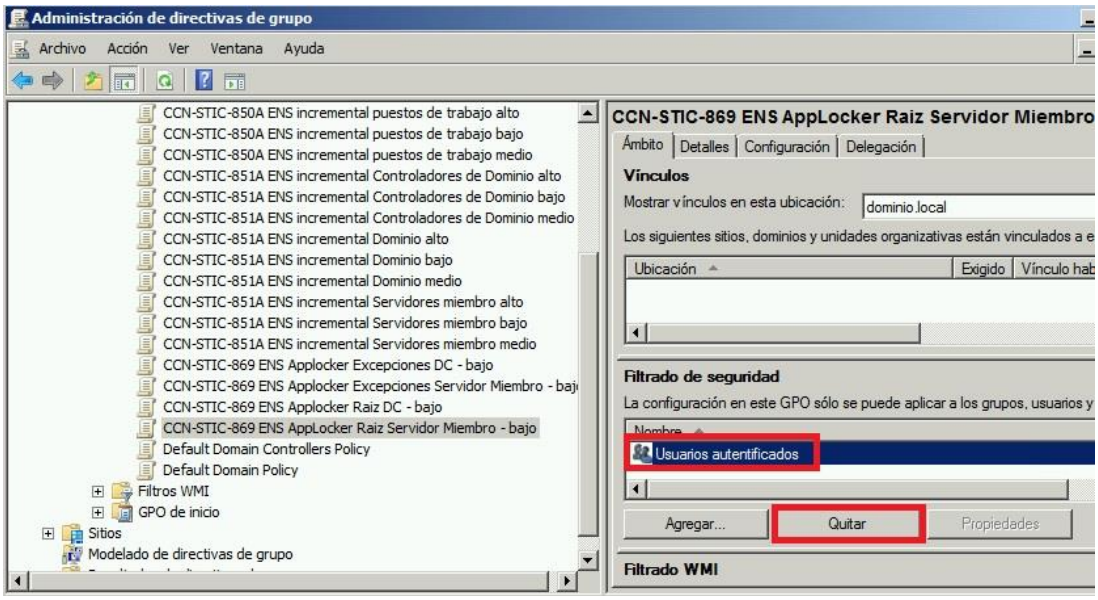
Una vez creadas todas las reglas necesarias para la ejecución del software del servidor, se puede proceder a la vinculación de las directivas a la unidad organizativa a la que pertenezca el servidor a securizar. Si dicha unidad contiene otros servidores que no han de recibir las reglas de AppLocker será necesario filtrar la aplicación de las dos directivas haciendo uso del filtrado de seguridad.

En los siguientes pasos se describe cómo vincular dichas políticas a la unidad organizativa donde resida el servidor o servidores a securizar y cómo usar el filtrado de seguridad para que sólo apliquen al servidor o servidores requeridos.

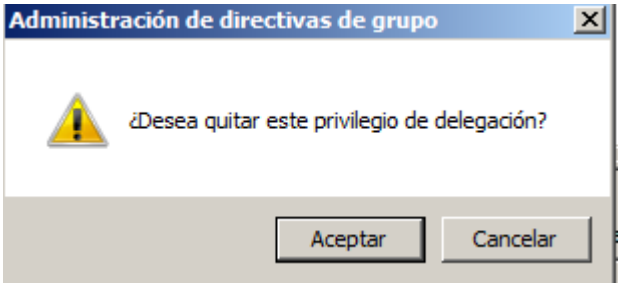
En este ejemplo, se securiza un único servidor llamado “SVR1” que reside en la unidad organizativa “Servidores”.

Paso	Descripción
39.	**Nota:** Si en su caso no precisa definir filtrado de seguridad (porque puede aplicar la política a todos los servidores de la Unidad Organizativa seleccionada) continúe directamente en el paso 46.

Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el objeto **"Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ CCN-STIC-869 ENS Applocker Raiz Servidor Miembro - bajo" **, y elimine el grupo "Usuarios autentificados" del submenú "Filtrado de seguridad" situado en el panel derecho. Para ello, seleccione el objeto "Usuarios autentificados" y pulse sobre el botón "Quitar".

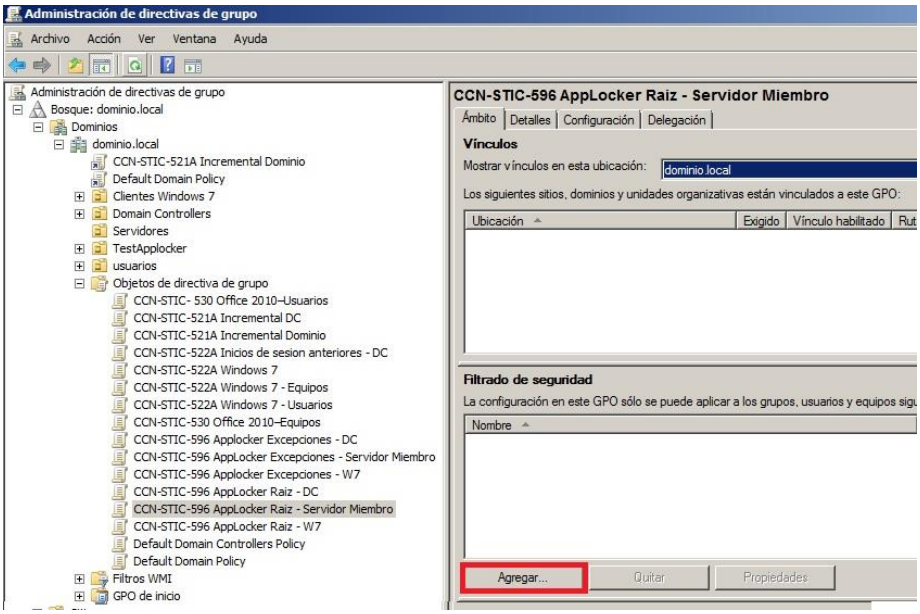


40. Pulse "Aceptar" en la ventana de confirmación.

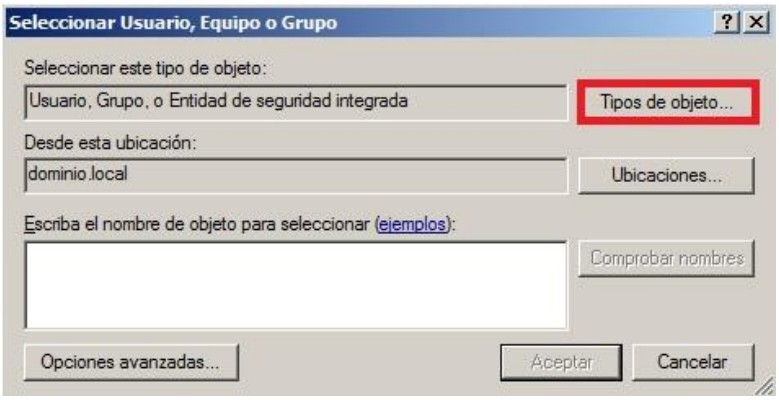


Paso	Descripción

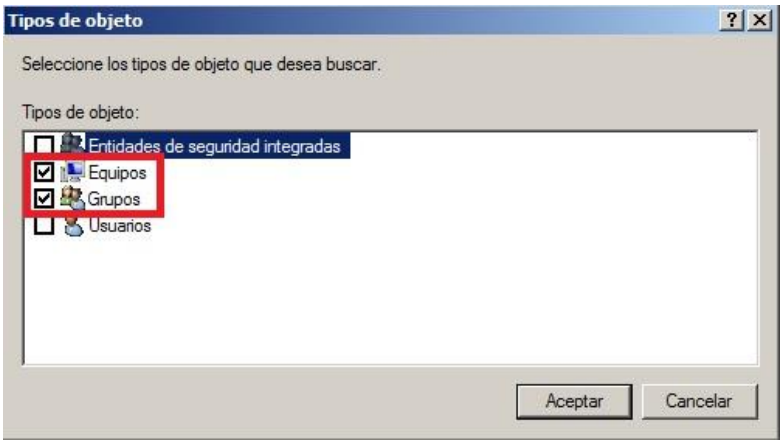
41. Agregue el servidor o grupo de servidores a los que se les vaya a aplicar las reglas de AppLocker. Para ello pulse “Agregar…” en el submenú de “Filtrado de Seguridad”.



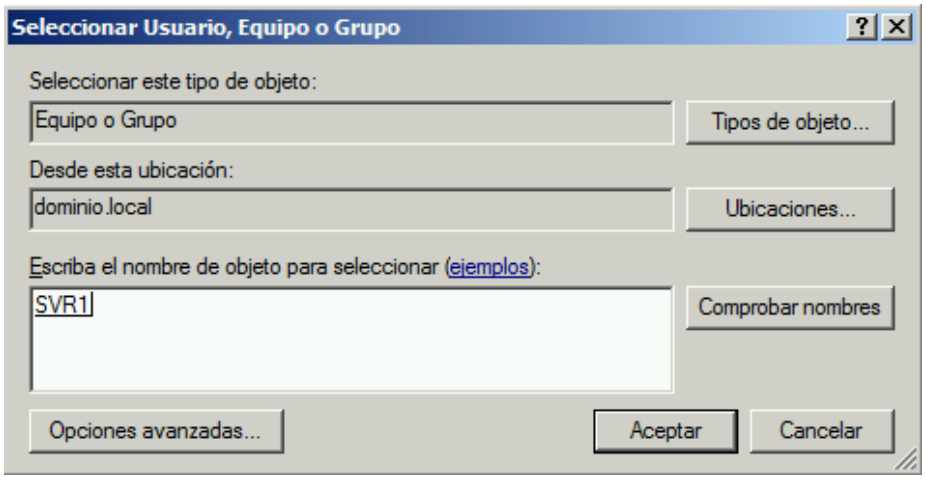
42. En la siguiente ventana, pulse “Tipos de objeto…”.



43. Seleccione “Equipos” y “Grupos” para posteriormente poder buscar por la cuenta de equipo o grupos de equipos. Pulse “Aceptar”.

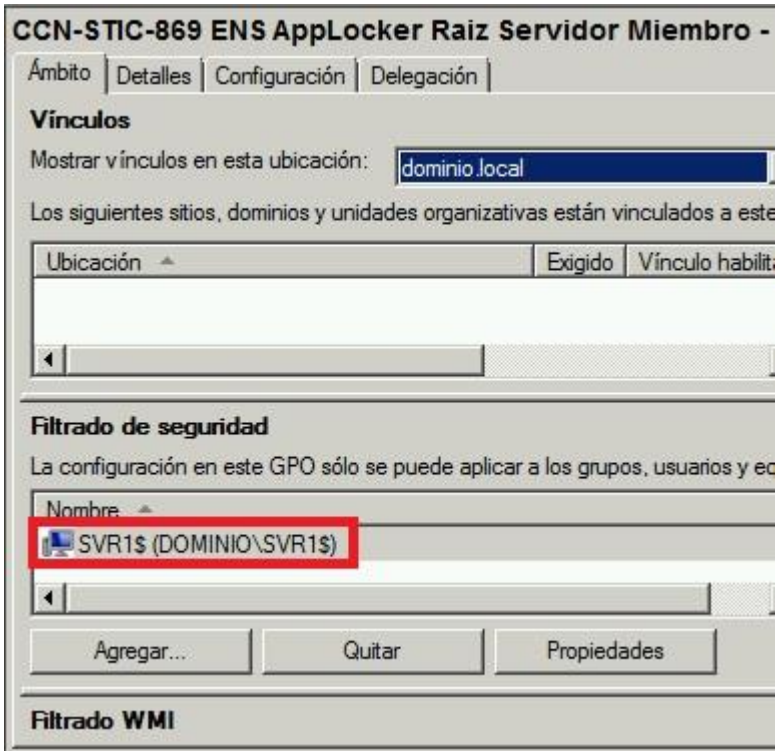


Paso	Descripción
44.	De nuevo, en la ventana de “Seleccionar Usuario”, escriba el equipo, equipos o grupos de equipos (separados por comas) a los que desee aplicar la política y pulse “Aceptar”.

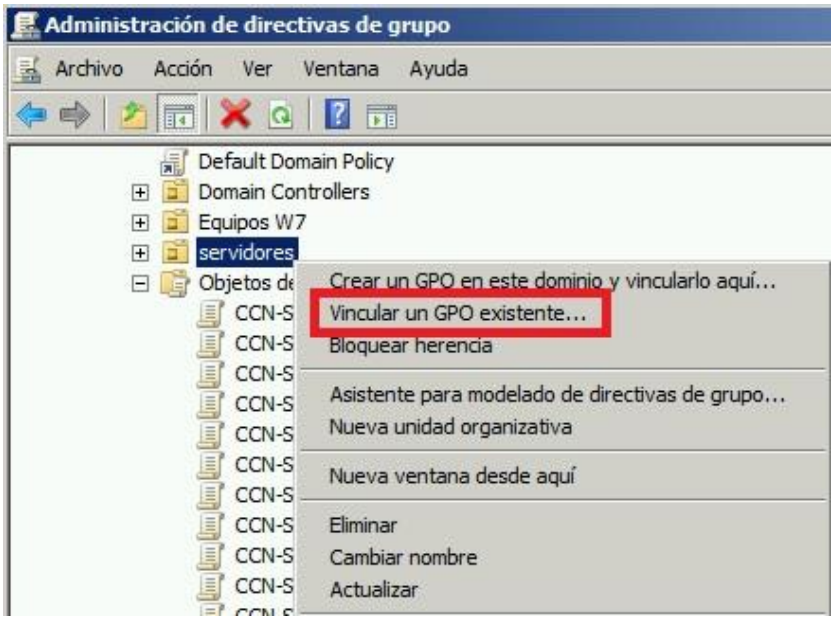
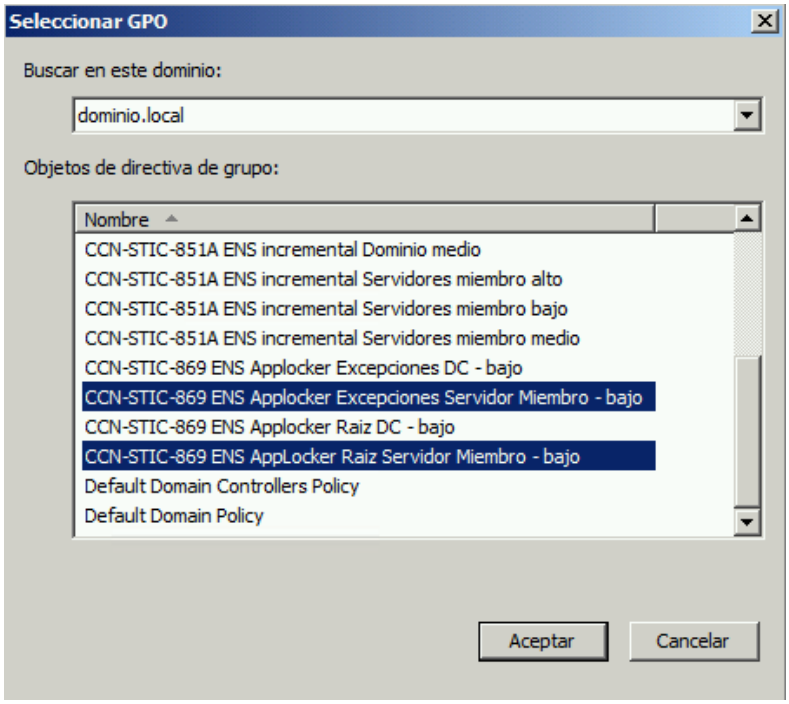


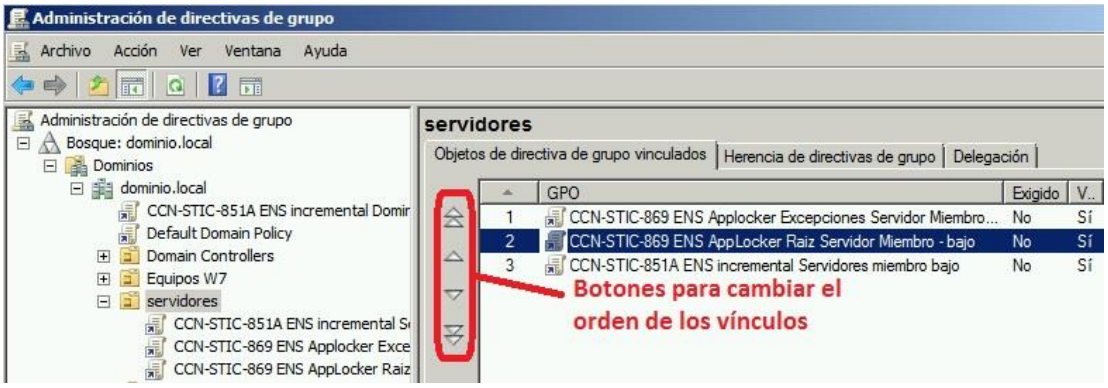
Nota: En este ejemplo únicamente se va a aplicar la política a un servidor: “SVR1”.

45.	Compruebe que el listado de servidores y/o grupos se ha actualizado en el submenú “Filtrado de Seguridad” de la consola de “Administración de directivas de grupo”.



46.	Repita los pasos del 38 al 44 para la directiva **CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro - bajo**.
47.	Proceda a la vinculación de los dos GPO a la unidad organizativa que contenga al servidor tal y como se le indica en los siguientes pasos. En este ejemplo la OU se llama: “Servidores”.

Paso	Descripción
48.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ <OU que contenga al servidor miembro>**". Pulse botón derecho sobre la OU que contenga al servidor miembro y elija la opción "Vincular un GPO existente…" del menú contextual. En este ejemplo el nombre de la OU es "Servidores". 
49.	En el nuevo cuadro de diálogo desplegado, seleccione los GPO (haciendo uso de la tecla "CTRL"): "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo" y "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro - bajo". Pulse "Aceptar". 

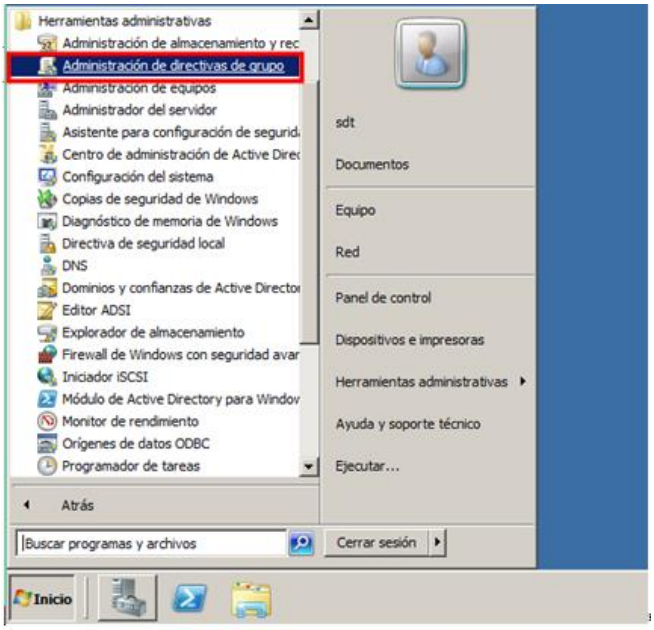
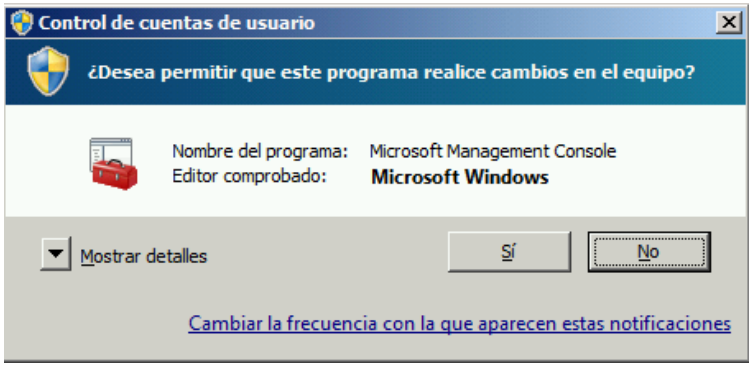
Paso	Descripción
50.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Servidores**", y observe el orden de los vínculos en la parte central de la ventana.  El orden de los vínculos ha de ser el siguiente: 1) CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro - bajo 2) CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro - bajo 3) CCN-STIC-869 ENS incremental Servidores miembro bajo 4) Resto de GPOs Si el orden mostrado fuera otro, seleccione los GPOs por turnos y utilice los botones indicados en la figura para cambiar el orden de los vínculos de forma que coincida con el indicado aquí.
51.	Ya puede cerrar la consola de “Administración de directivas de grupo”.
52.	Borre la carpeta “C:\scripts” del controlador de dominio.

3. CONFIGURACIÓN DE APPLOCKER EN CLIENTE WINDOWS 7 MIEMBRO DE DOMINIO

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

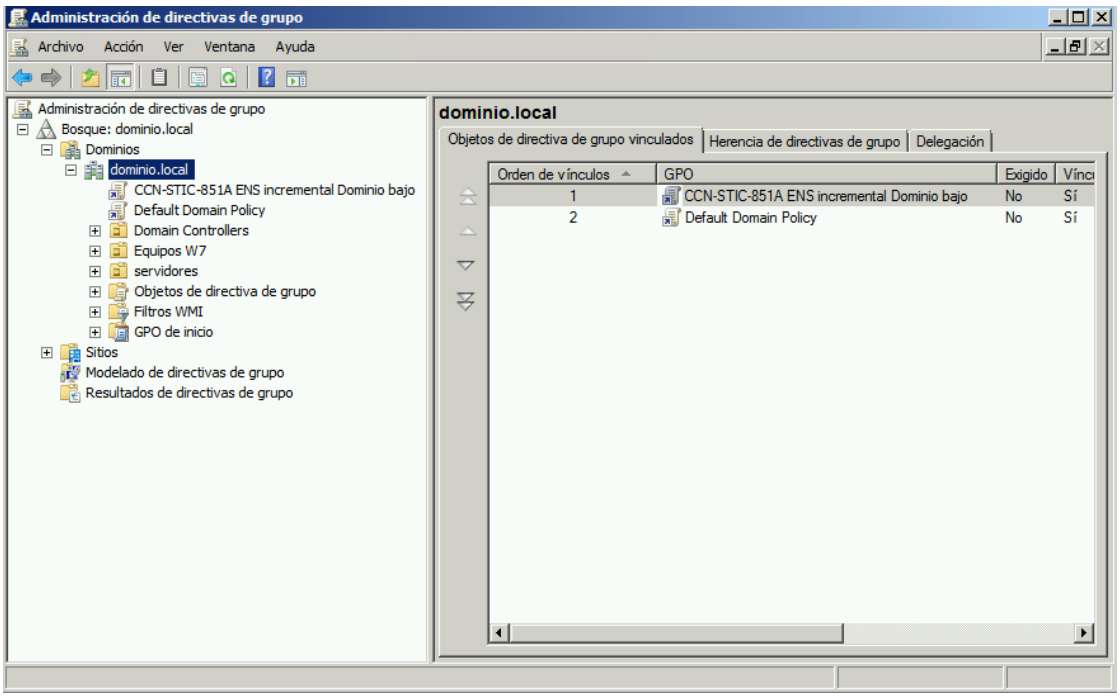
Nota: Esta guía asume que a los servidores controladores del dominio, a los que va a pertenecer el equipo cliente, se les ha aplicado la configuración descrita en la guía CCN-STIC-851A para nivel bajo según el Esquema nacional de Seguridad. También se asume que los clientes y controladores de dominio tienen aplicadas las configuraciones descritas en la guía CCN-STIC-850A.

Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\scripts" del controlador de dominio.

Paso	Descripción
4.	Asegúrese de que al menos los siguientes directorios hayan sido copiados al directorio "C:\scripts" del controlador de dominio: – CCN-STIC-869 AppLocker Raiz W7 miembro – bajo – CCN-STIC-869 AppLocker Excepciones W7 miembro - bajo
5.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo.** 
6.	Pulse "Sí" en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos. 

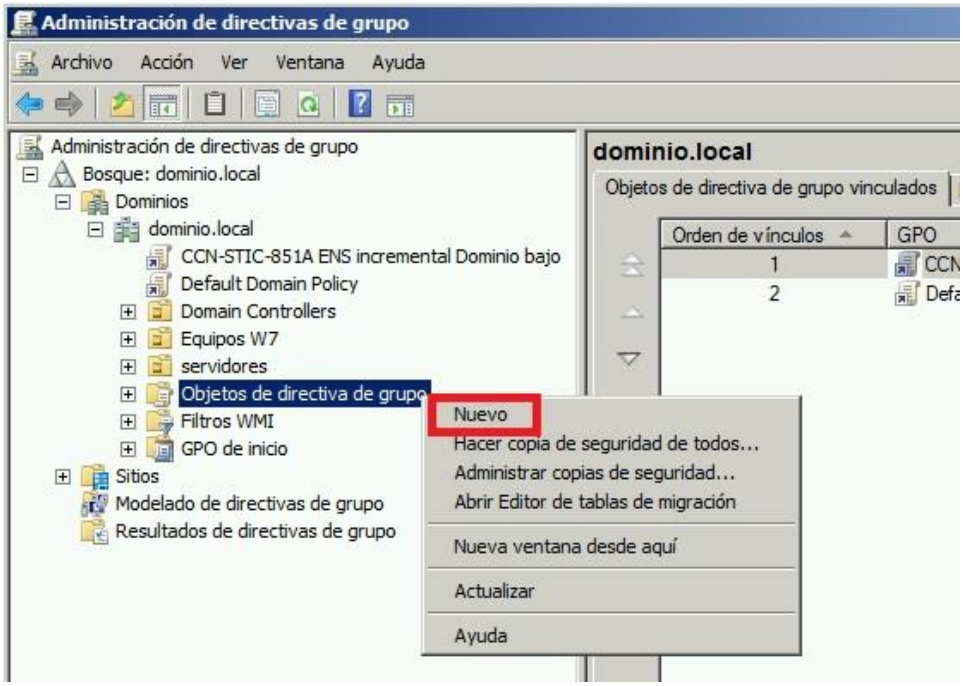
Paso	Descripción

7. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio>,** como se muestra en la siguiente imagen.



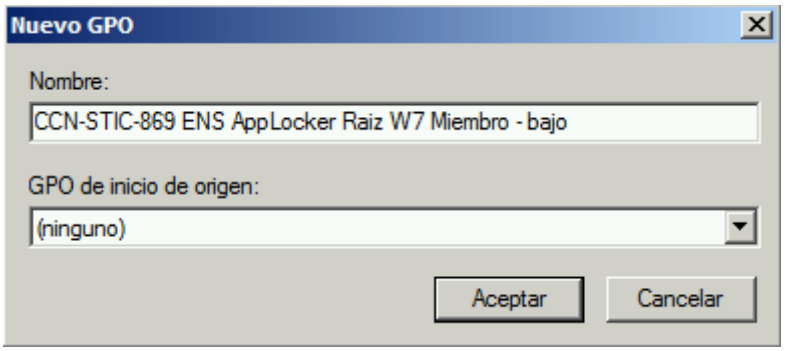
A continuación se procederá a la creación de las GPOs necesarias.

8. Expanda y seleccione el contenedor "**Objetos de directiva de grupo**", y marcando con el botón derecho sobre dicho elemento, elija la opción "Nuevo" del menú contextual que aparecerá.

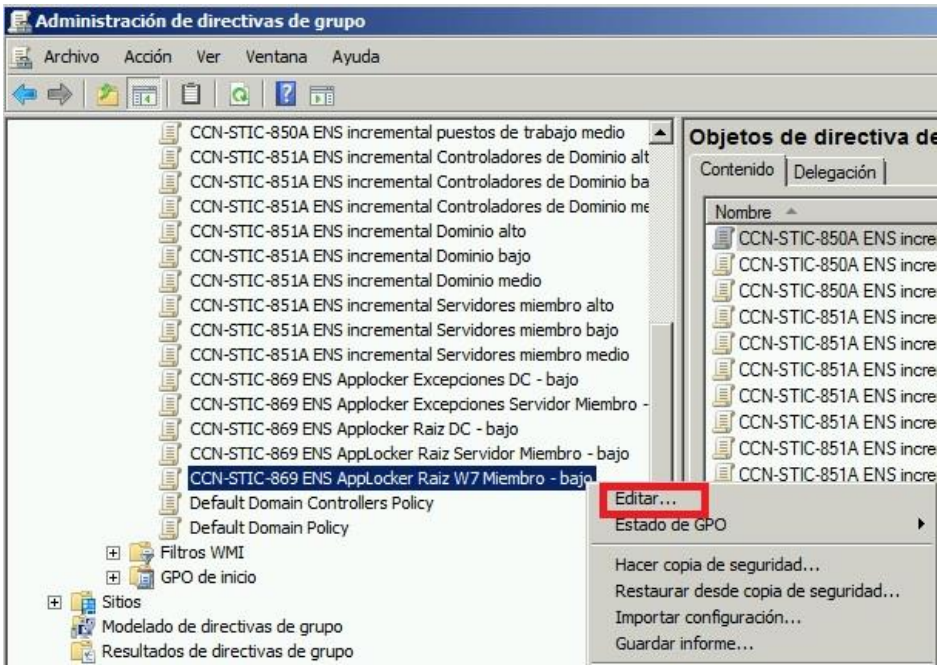


Paso	Descripción

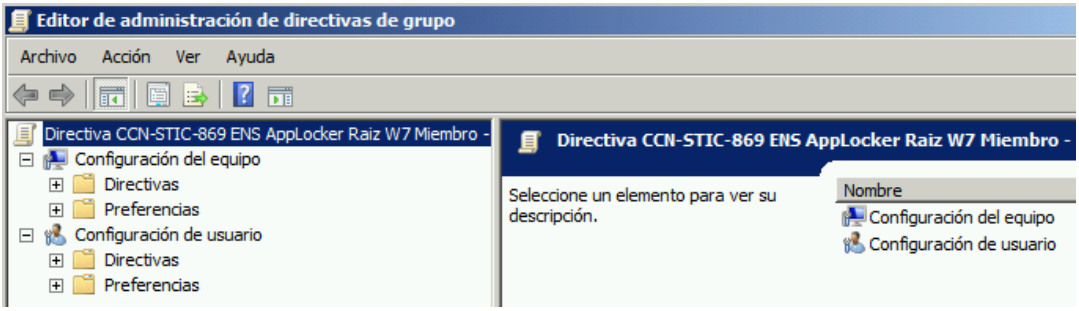
9. Asigne el siguiente nombre al nuevo GPO: “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo”. Pulse “Aceptar” para cerrar la ventana.



10. Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo**", y marcando con el botón derecho sobre él, elija la opción "Editar…" del menú contextual que aparecerá.



11. Con ello se lanzará el “Editor de administración de directivas de grupo”.



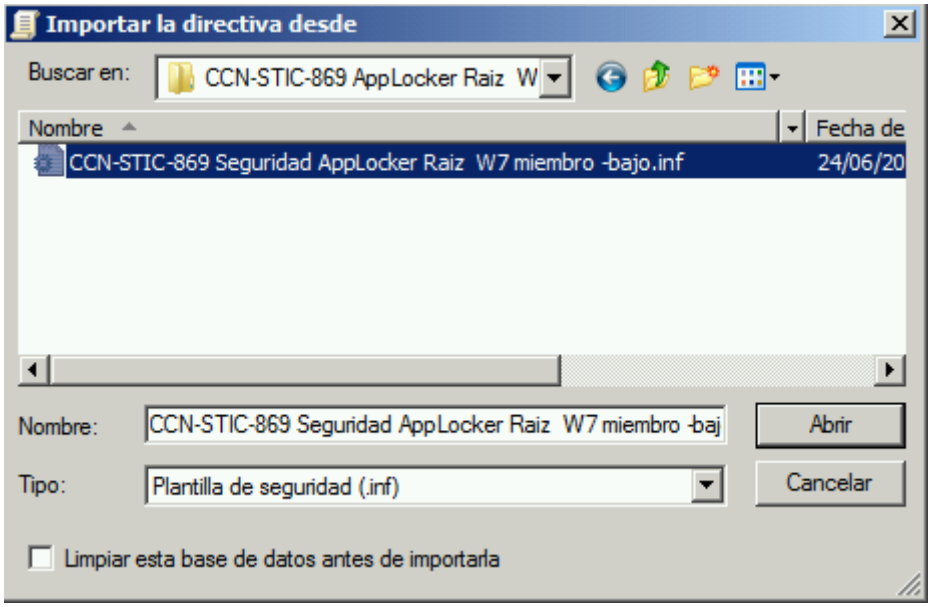
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando primero la configuración de la plantilla de seguridad que acompaña a esta guía, e importando posteriormente la configuración de reglas de AppLocker que aplicarán a los clientes Windows 7.

Paso	Descripción

12. En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción “Importar directiva…”

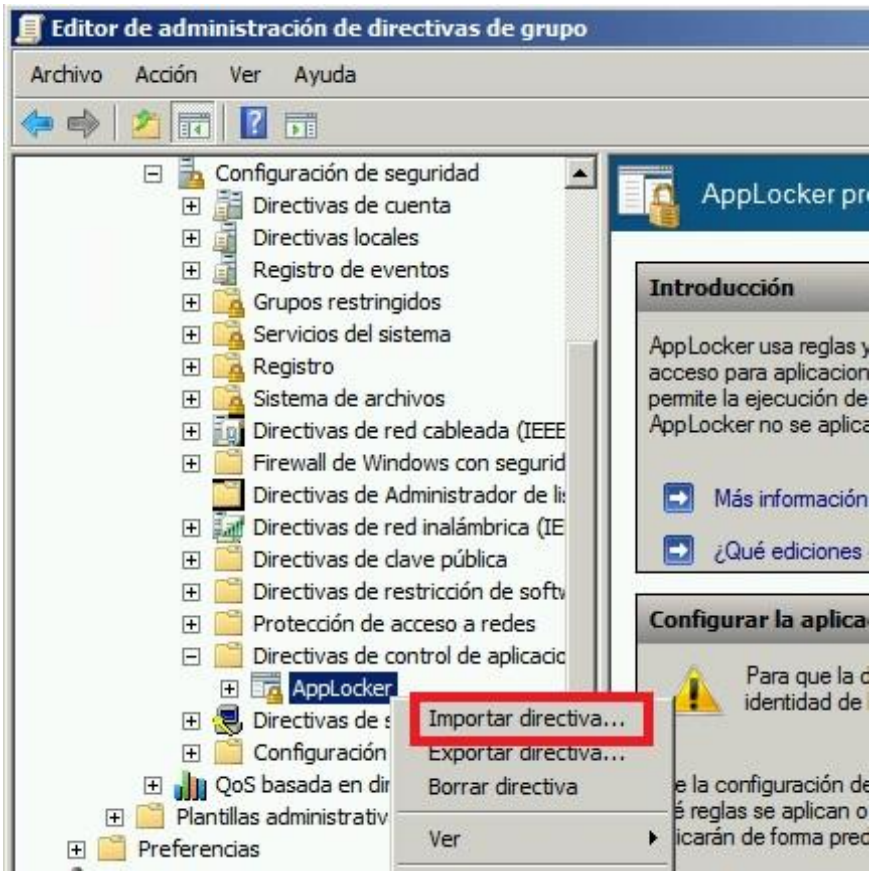
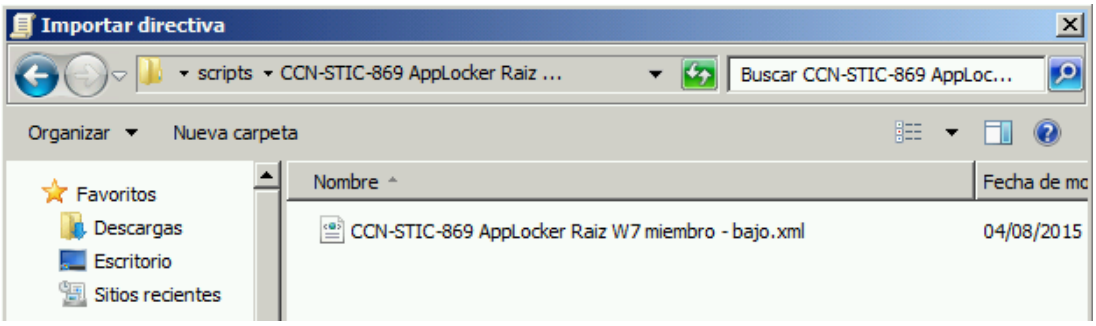
Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad.

13. En el cuadro de dialogo abierto, navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz W7 - bajo” y seleccione el fichero “**CCN-STIC-869 Seguridad AppLocker Raiz W7 Miembro – bajo.inf**” pulsando doble clic sobre el fichero o sobre el botón “Abrir”.

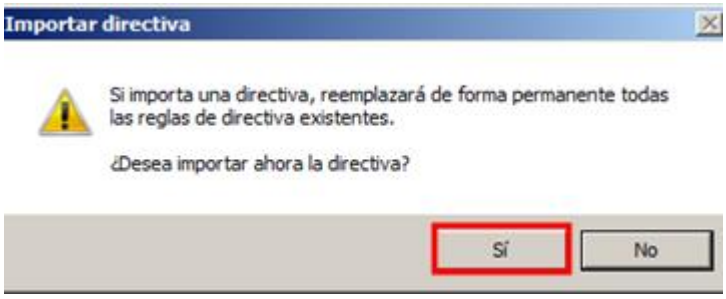


Con ello habrá quedado importada la plantilla de seguridad en este GPO.

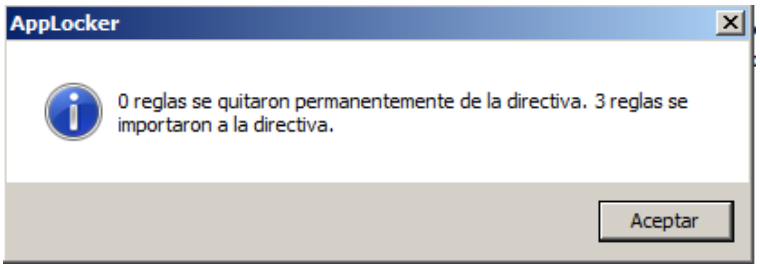
Nota: No cierre todavía el “Editor de administración de directivas de grupo”, y continúe con el siguiente paso.

Paso	Descripción
14.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-ENS 869 AppLocker Raiz W7 Miembro - bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
15.	En el cuadro de dialogo abierto, navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz W7 - bajo” y seleccione el fichero “**CCN-STIC-869 AppLocker Raiz W7 Miembro– bajo.xml**” mediante doble clic sobre él o pulsando “Abrir”. 

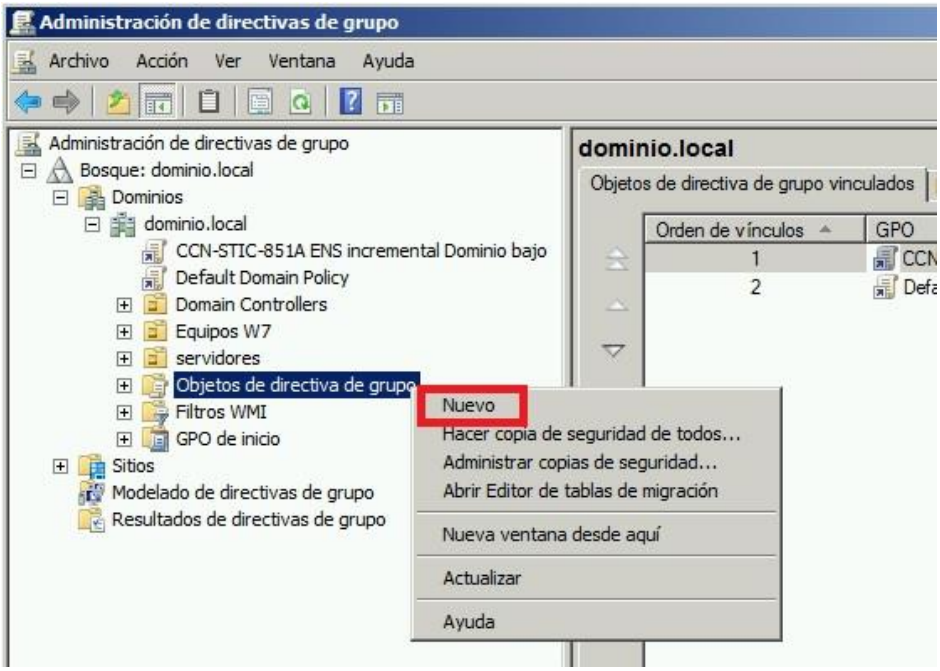
Paso	Descripción
16.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Si”.



17.	Aparecerá un nuevo mensaje informativo indicando que se importaron tres reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.

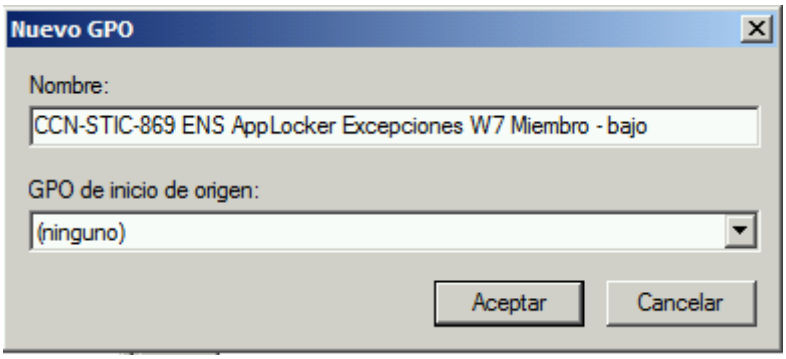


18.	El GPO "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo" está creado y configurado. Cierre la ventana del “Editor de administración de directivas de grupo”.
19.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Objetos de directiva de grupo”**, y marcando con el botón derecho sobre dicho elemento, elija la opción “Nuevo” del menú contextual que aparecerá.

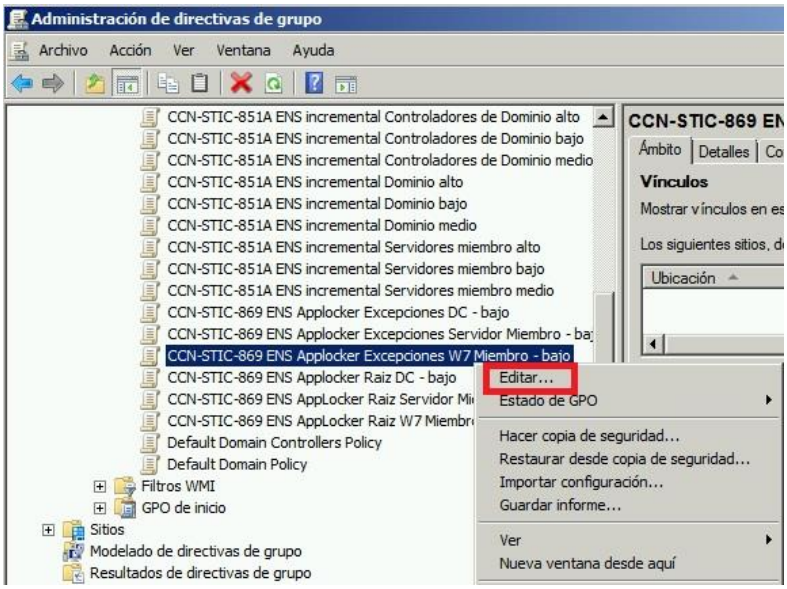


Paso	Descripción

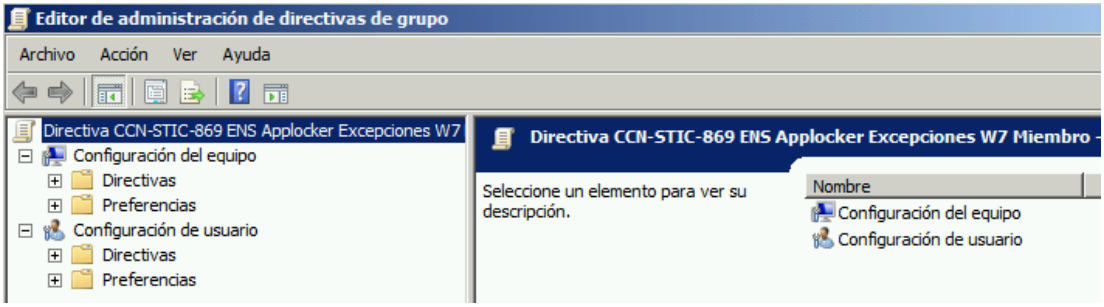
20. Asigne el siguiente nombre al GPO: “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”. Pulse “Aceptar” para cerrar la ventana.



21. Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



22. Con ello se lanzará el “Editor de administración de directivas de grupo”.



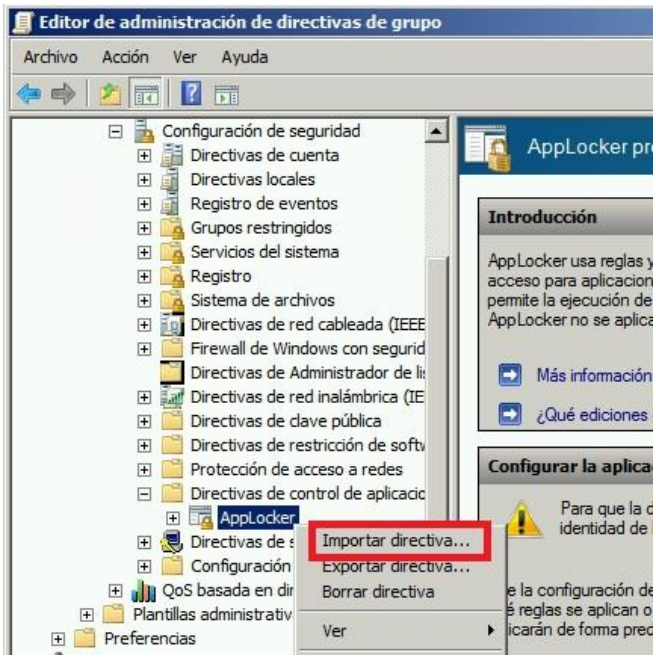
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando la configuración de las reglas de AppLocker.

Paso	Descripción

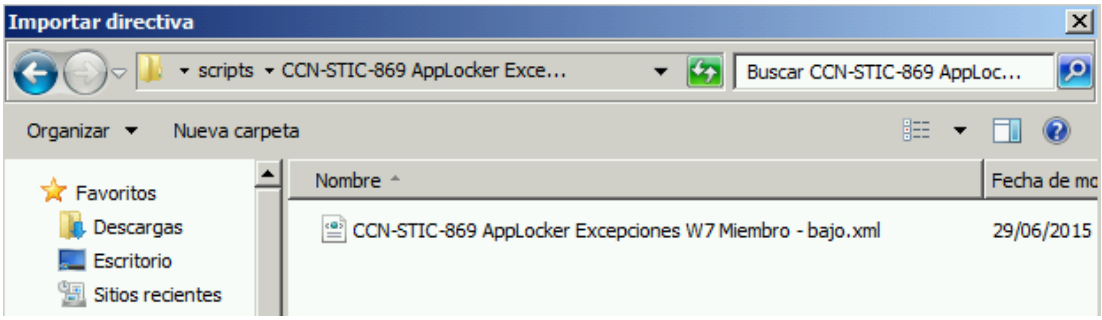
23. En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación:

    Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

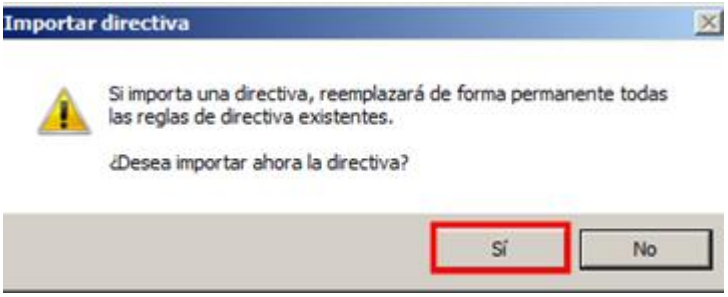
    Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.

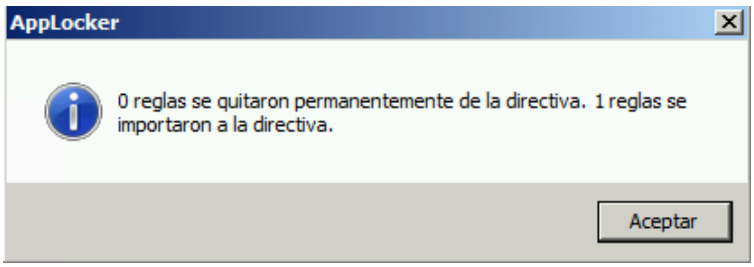


24. En el cuadro de dialogo abierto, navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Excepciones W7 Miembro -bajo”, seleccione el fichero “**CCN-STIC-869 AppLocker Excepciones W7 Miembro - bajo.xml**” mediante doble clic sobre él o pulsando “Abrir”.



25. Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.

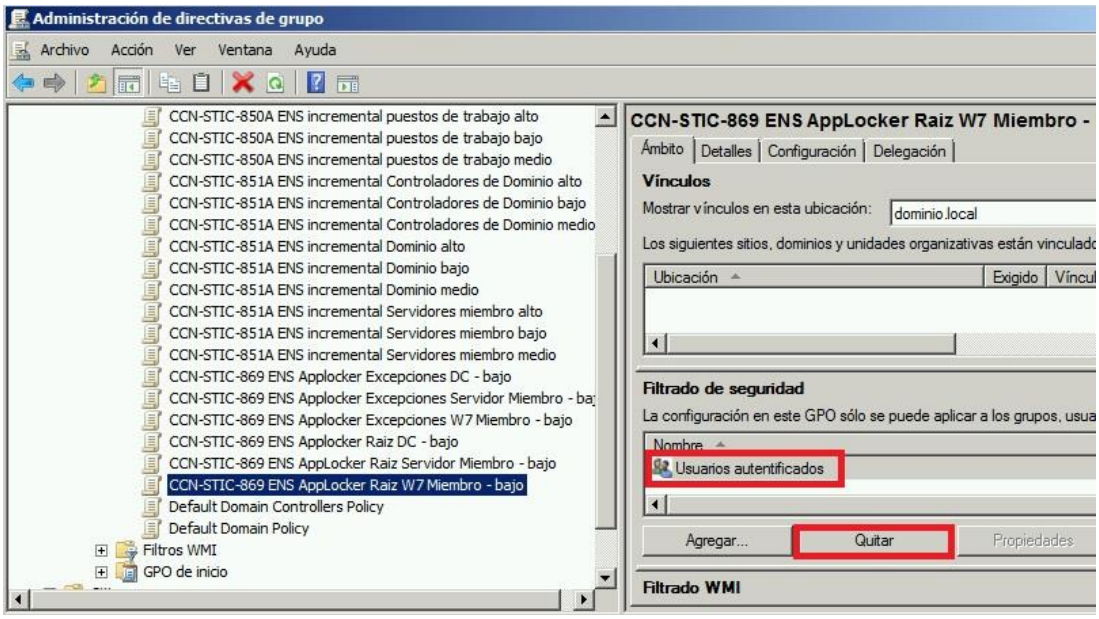
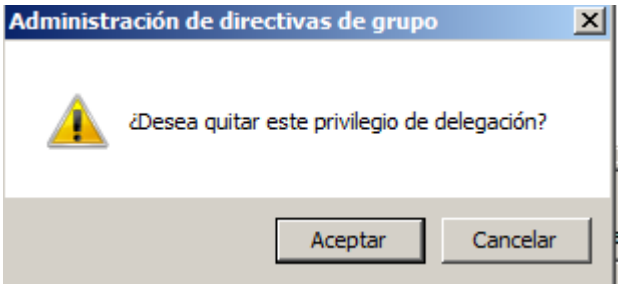


Paso	Descripción
26.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. 
27.	El GPO recién importado contiene una única regla para permitir ejecución de binarios desde unidades de CD o DVD. Antes de proceder a la vinculación de los GPO a las unidades organizativas donde se encuentren los clientes Windows 7, puede proceder a la edición del GPO para añadir más reglas que se ajusten al software que tengan instalados sus clientes. El GPO "CCN-STIC-869 ENS Applocker Excepciones W7 Miembro - bajo" está diseñado para recibir las nuevas reglas que se ajusten a su organización. Edite dicho GPO **Nota:** Las reglas de AppLocker definidas en los dos GPO recién creados se encuentran en modo auditoría, de tal manera que no se prohibirá la ejecución de ningún software. Sólo se guardarán eventos descriptivos en el fichero de log de eventos de AppLocker. Para más información sobre la auditoría de logs en AppLocker consulte el apartado 4 del presente anexo. Para más información sobre los pasos a seguir en la creación, edición y eliminación de reglas de AppLocker, consulte el anexo H. Tenga en consideración que, en este caso, no será necesario realizar el procedimiento desde una máquina de referencia ya que el GPO no se encuentra vinculado a ninguna unidad organizativa.
28.	Cuando termine de adaptar la política a sus necesidades, cierre la ventana del "Editor de administración de directivas de grupo"

Una vez creadas todas las reglas necesarias para la ejecución del software en los clientes Windows 7, se puede proceder a la vinculación de las directivas a la unidad organizativa a la que pertenezcan los clientes a securizar. Si dicha unidad contiene clientes que no han de recibir las reglas de AppLocker, será necesario filtrar la aplicación de las dos directivas haciendo uso del filtrado de seguridad de tal manera que la política sólo aplicará al equipo o conjunto de equipos deseados.

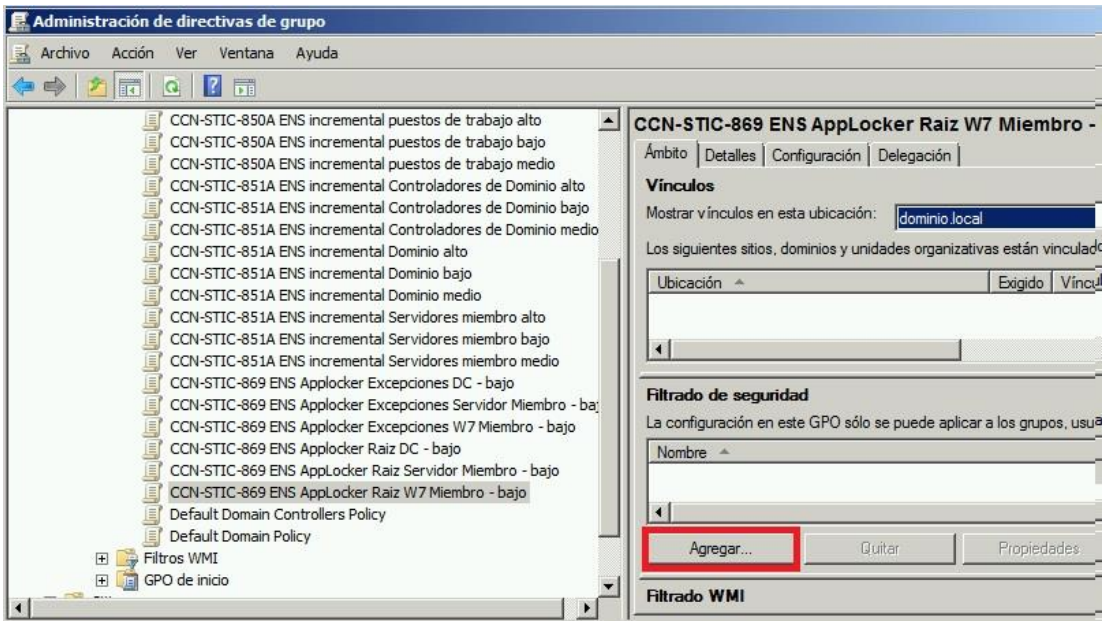
En los siguientes pasos se describe cómo vincular dichas políticas a la unidad organizativa donde residan los clientes Windows 7 y cómo usar el filtrado de seguridad para que sólo apliquen a los clientes requeridos.

En este ejemplo se securizará un cliente llamado "CLN1" que reside en la unidad organizativa "Equipos W7"

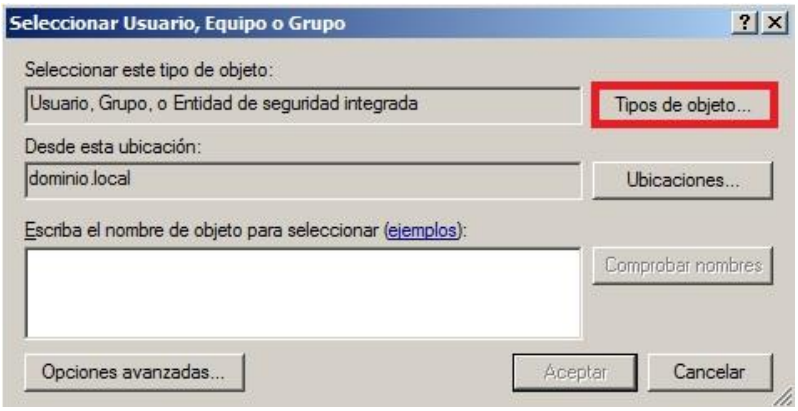
Paso	Descripción
29.	**Nota:** Si en su caso no precisa definir filtrado de seguridad (porque puede aplicar la política a todos los equipos de la Unidad Organizativa seleccionada) continúe directamente en el paso 37. Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el objeto **"Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ CCN-STIC-869 ENS Applocker Raiz W7 Miembro - bajo" **, y elimine el grupo "Usuarios autentificados" del submenú "Filtrado de seguridad" situado en el panel derecho. Para ello, seleccione el objeto "Usuarios autentificados" y pulse sobre el botón "Quitar". 
30.	Pulse "Aceptar" en la ventana de confirmación. 

Paso	Descripción

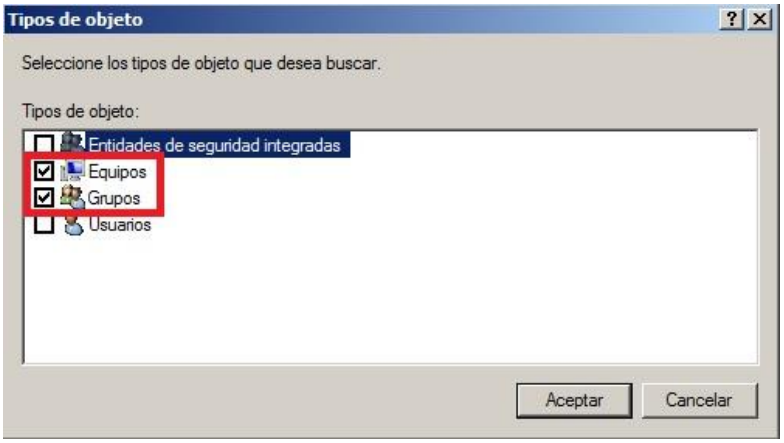
31. Agregue al equipo o grupo de equipos a los que se les vaya a aplicar las reglas de AppLocker. Para ello pulse “Agregar…” en el submenú de “Filtrado de Seguridad”.



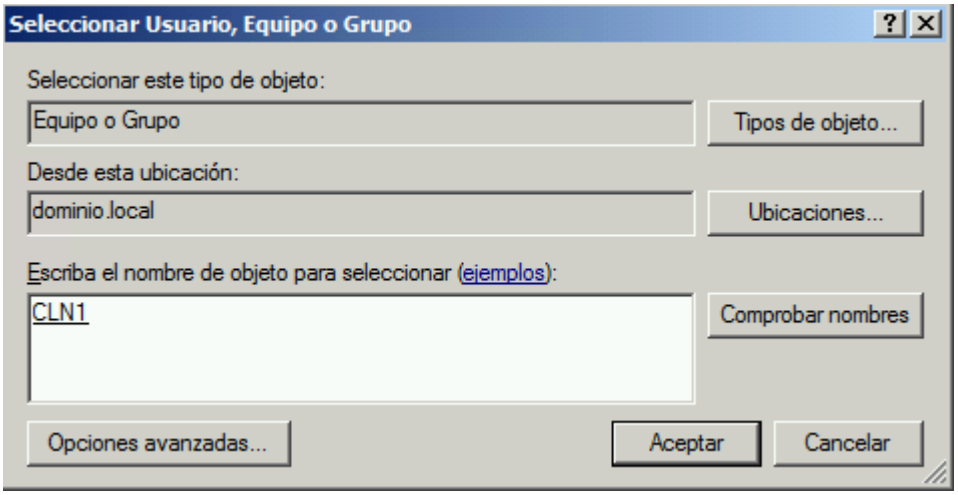
32. En la siguiente ventana, pulse “Tipos de objeto…”.



33. Seleccione “Equipos” y “Grupos” para posteriormente poder buscar por la cuenta de equipo o grupos de equipos. Pulse “Aceptar”.

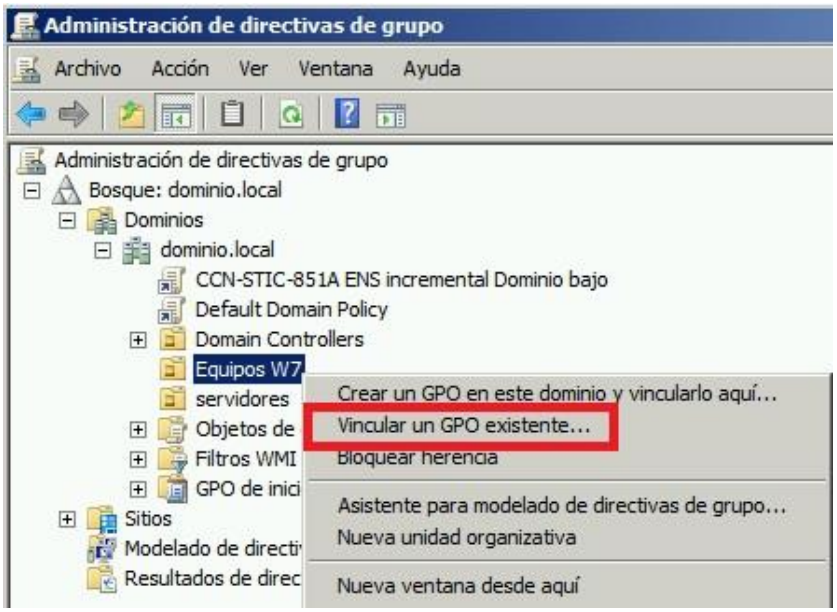
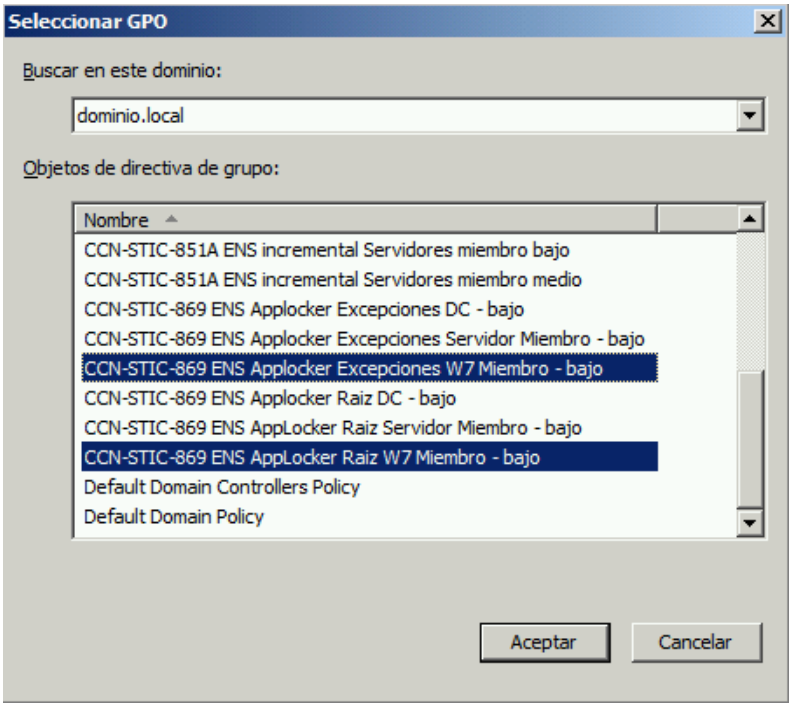


Paso	Descripción
34.	De nuevo en la ventana de “Seleccionar Usuario”, escriba el equipo, equipos, o grupos de equipos (separados por comas) a los que desee aplicar la política y pulse “Aceptar”. En este ejemplo únicamente se va a aplicar la política a un puesto de trabajo: “CLN1”.

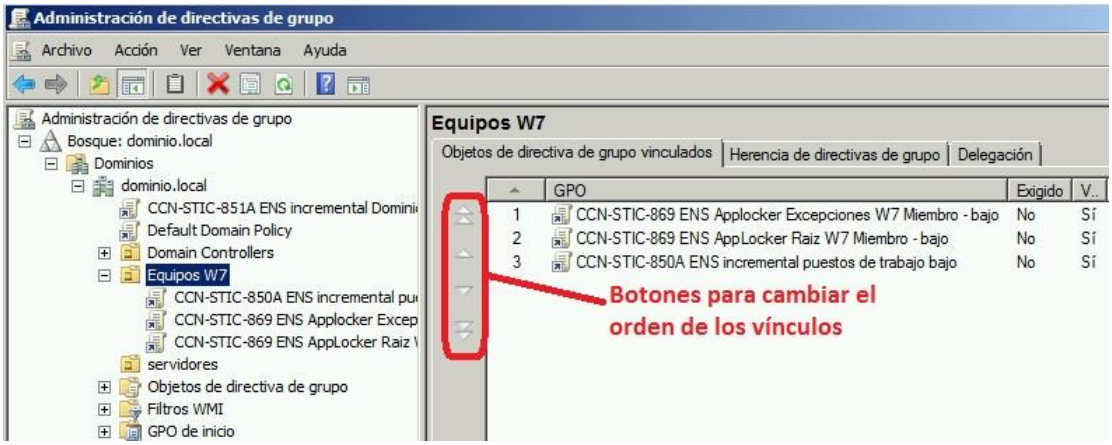


35.	Compruebe que el listado de servidores y/o grupos se ha actualizado en el submenú “Filtrado de Seguridad” de la consola de “Administración de directivas de grupo”.

36.	Repita los pasos del 29 al 35 para la directiva **CCN-STIC-869 ENS Applocker Excepciones W7 Miembro - bajo**.
37.	Proceda a la vinculación de los dos GPO a la unidad organizativa que contenga al servidor tal y como se le indica en los siguientes pasos. En este ejemplo la OU se llama: “Equipos W7”.

Paso	Descripción
38.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ <OU que contenga al cliente miembro>**". Pulse botón derecho sobre la OU que contenga al equipo miembro y elija la opción "Vincular un GPO existente…" del menú contextual.  **Nota:** En este ejemplo el nombre de la OU es "Equipos W7".
39.	En el nuevo cuadro de diálogo desplegado, seleccione los GPO (haciendo uso de la tecla "CTRL"): "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo" y "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" pulse "Aceptar". 

Paso	Descripción
40.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Equipos W7**", y observe el orden de los vínculos en la parte central de la ventana.



El orden de los vínculos ha de ser el siguiente:

5) CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo
6) CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo
7) CCN-STIC-869 ENS incremental puestos de trabajo bajo
8) Resto de GPOs

Si el orden mostrado fuera otro, seleccione los GPOs por turnos y utilice los botones indicados en la figura para cambiar el orden de los vínculos de forma que coincida con el indicado aquí.

41.	Ya puede cerrar la consola de “Administración de directivas de grupo”.
42.	Borre la carpeta “C:\Scripts” del controlador de dominio.

4. AUDITORÍA DE EVENTOS DE APPLOCKER

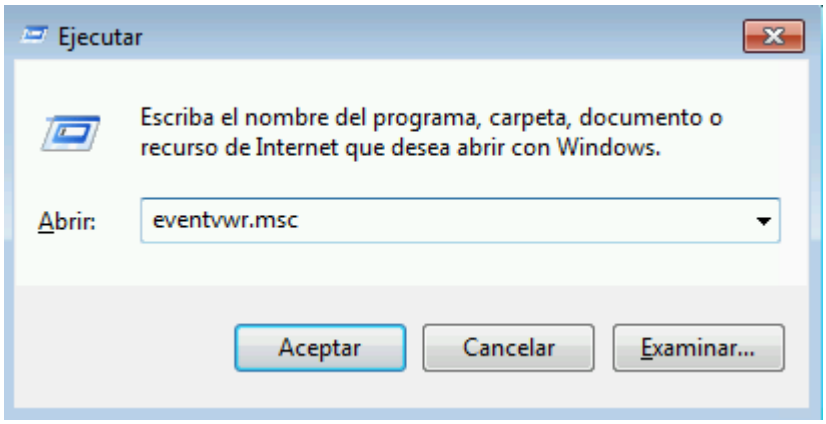
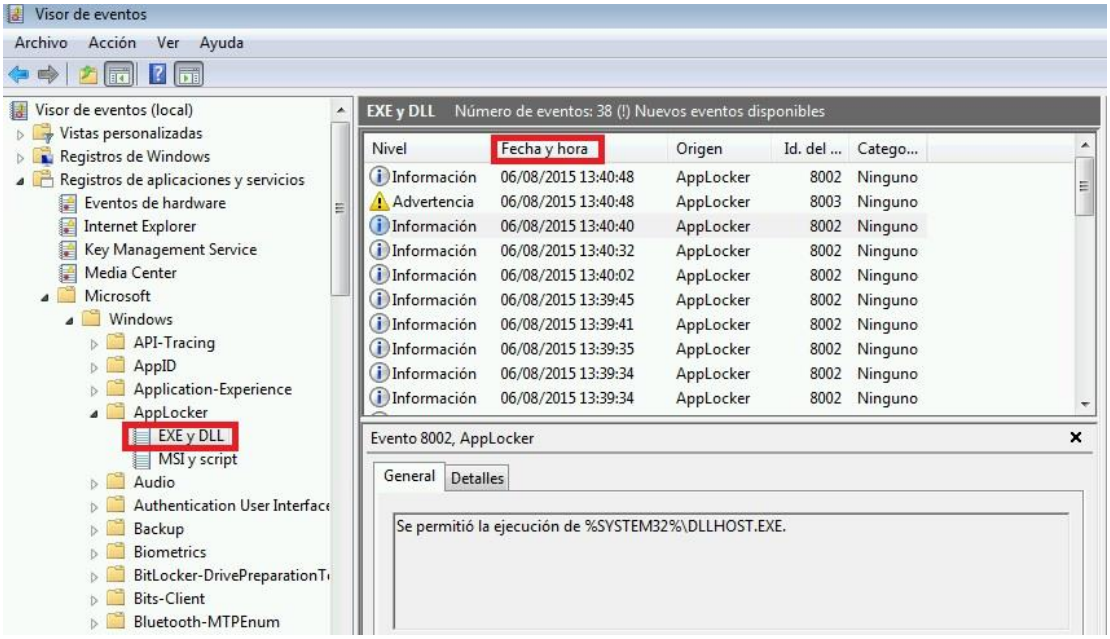
Las políticas definidas en este anexo contienen reglas de AppLocker configuradas exclusivamente en modo auditoría. No se aplican las reglas en modo forzado, por tanto se podrá ejecutar cualquier binario sin restricción en las máquinas donde se hayan aplicado las políticas. La configuración de AppLocker se encargará de almacenar los logs de eventos de permiso y restricción de ejecución con el objetivo de auditar qué software se ha ejecutado en la máquina.

El presente apartado tiene como objetivo asistir, a los administradores u operadores de sistemas o soporte, en la revisión de los eventos específicos de AppLocker.

Los siguientes pasos deberán realizarse en la máquina o máquinas a revisar (pueden ser servidores o estaciones de trabajo).

El siguiente ejemplo está tomado de un cliente Windows 7 con un usuario simple (que por defecto tiene permisos de lectura sobre los eventos del equipo).

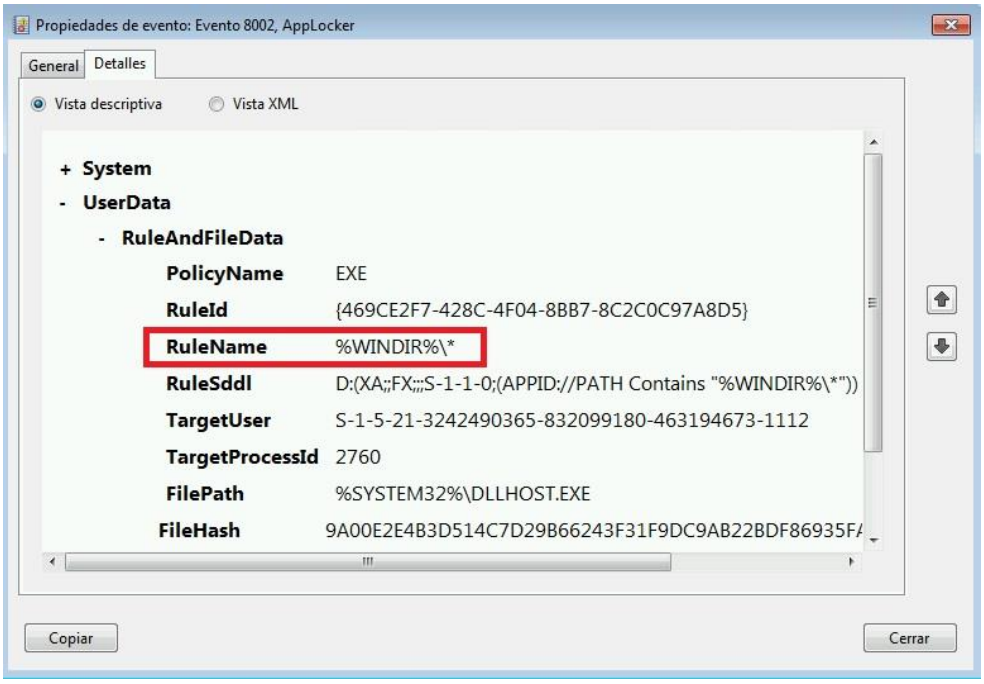
Paso	Descripción
1.	Inicie sesión en la máquina objeto del análisis de eventos. Puede iniciar sesión con un usuario sin especiales privilegios.

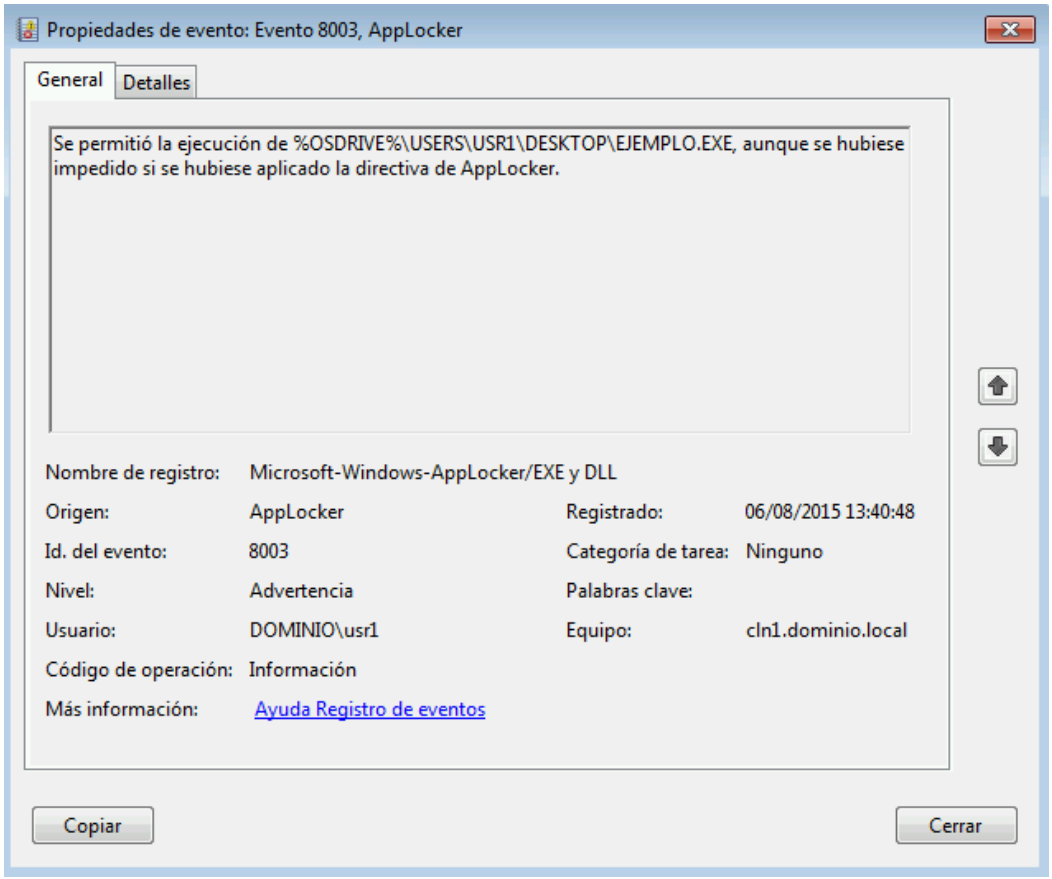
Paso	Descripción
2.	Copie un fichero ejecutable (por ejemplo %WINDIR%\system32\cmd.exe) al escritorio del usuario iniciado.
3.	Ejecute el binario desde el escritorio. No tendrá problemas en ejecutar, sin embargo al estar situado en una ruta no permitida por las reglas de AppLocker definidas en éste anexo, se producirá un evento con ID 8003 que informará de que se ha ejecutado una aplicación desde una ubicación no permitida por las reglas definidas. Para comprobar dichos eventos se hará uso del visor de eventos de Microsoft.
4.	Despliegue el menú “Ejecutar” haciendo uso de la combinación de teclas “Windows + R”.
5.	En el menú “Ejecutar” escriba “eventvwr.msc” y pulse “Aceptar”. 
6.	En el “Visor de Eventos” navegue hasta la siguiente ubicación: **Visor de eventos (local) / Registros de aplicaciones y servicios / Microsoft / Windows / AppLocker / EXE y DLL** En el menú central podrá ver los eventos que se han registrado organizados por tiempo. 

Paso	Descripción

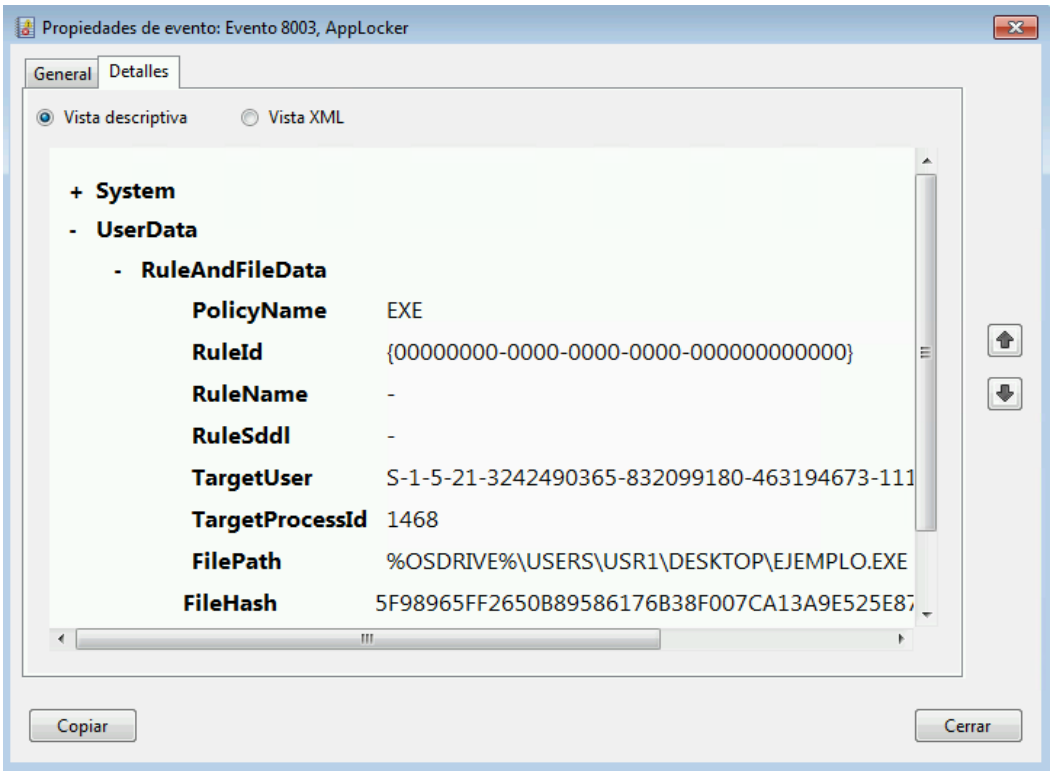
7. Los eventos 8002 indican permisividad. Haciendo doble clic sobre un evento con ID 8002 podrá ver más información sobre el mismo. Los campos reseñables son:
   - Usuario: usuario que lanzó el ejecutable.
   - Registrado: fecha y hora de ejecución.
   - Id. Del evento: número identificativo del evento.
   - En el cuadro de texto principal se indica el nombre y ruta del ejecutable permitido.

8. En la pestaña “detalles” encontramos el nombre de la regla que ha permitido la ejecución del binario además de otros campos informativos.



Paso	Descripción
9.	Los eventos 8003 indican ejecuciones de software que hubieran sido bloqueadas por alguna de las reglas de AppLocker, en el caso de que hubiesen estado forzadas. Haciendo doble clic sobre el evento con ID 8003 generado en el paso 3 de éste apartado podrá ver más información sobre el mismo. Los campos reseñables son: – Usuario: usuario que lanzó el ejecutable. – Registrado: fecha y hora de ejecución. – Id. Del evento: número identificativo del evento. – En el cuadro de texto principal se indica el ejecutable que se ha permitido. También se indica que dicha ejecución se habría bloqueado si las reglas de AppLocker se encontraran activas en lugar de en modo auditoría. 

Paso	Descripción
10.	En la pestaña “Detalles” se encontraría el nombre de la regla que haya bloqueado la ejecución del binario.



Nota: En este caso no se aprecia el nombre de la regla pero sí su identificador ({00000000-0000-0000-0000-000000000000}) que corresponde con la regla de negación por defecto. Si no hay una regla de permisividad para la ruta indicada, AppLocker bloquea por defecto la ejecución del binario.

ANEXO E. GUÍA PASO A PASO PARA LA CONFIGURACIÓN DE APPLOCKER EN CONTROLADORES DE DOMINIOS, SERVIDORES Y CLIENTES QUE LES SEAN DE APLICACIÓN EL NIVEL MEDIO O ALTO DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar la implantación del servicio AppLocker en una red de dominio con una categorización de seguridad media o alta según los criterios del Esquema Nacional de Seguridad. El presente anexo aplica tanto a controladores de dominio y servidores Microsoft Windows Server 2008 R2 o 2012 R2 como a clientes Windows 7 Ultimate o Enterprise. 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 y la información manejada por la organización correspondieran al nivel medio o alto, deberá realizar las implementaciones según se referencian en el presente anexo.

La activación, configuración y creación de reglas de AppLocker sobre los clientes y servidores se llevará a cabo mediante GPOs vinculados a las diversas unidades organizativas. No se hará uso de políticas locales en los clientes o servidores para evitar posibles problemas en la aplicación de las mismas. Se definirán dos GPOs, una que contenga reglas y configuraciones globales y otra destinada a las excepciones y nuevas reglas que puedan surgir con posterioridad a la aplicación de esta guía. Dependiendo de su entorno es posible que necesite crear nuevas excepciones, para ello consulte el anexo H. Las capturas de pantalla de los pasos realizados en el controlador de dominio corresponden con un entorno Windows Server 2008 R2. No obstante, la aplicación y los pasos descritos en el presente anexo son igualmente válidos para un controlador de dominio basado en Windows Server 2012 R2.

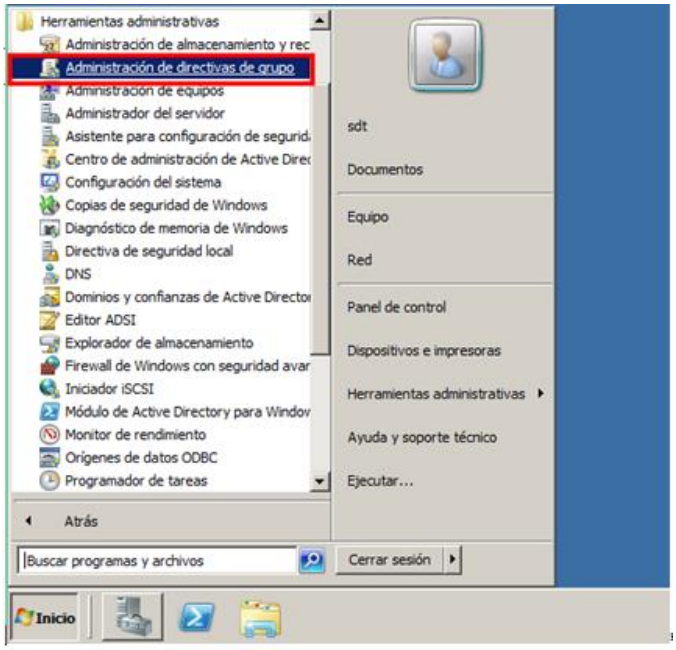
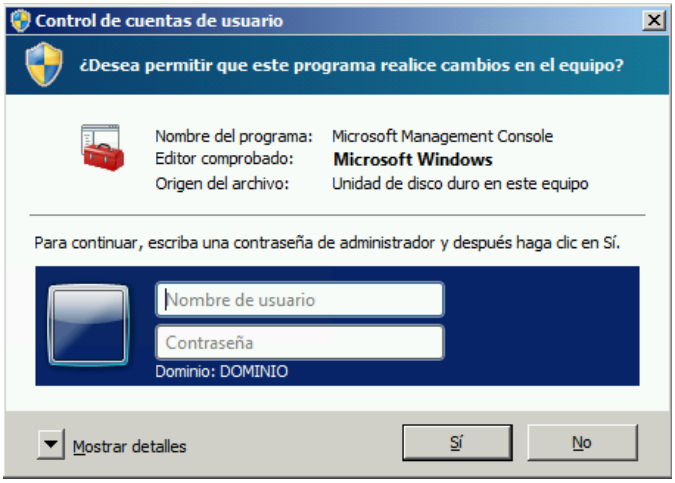
Para la implantación en nivel medio o alto según criterios del Esquema Nacional de Seguridad, las reglas de AppLocker se implementarán en modo forzado de tal manera que se restringirá la ejecución de binarios ubicados en rutas de instalación no estándar.

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

1. CONFIGURACIÓN DE APPLOCKER EN CONTROLADOR DE DOMINIO WINDOWS SERVER 2008 R2 O WINDOWS SERVER 2012 R2

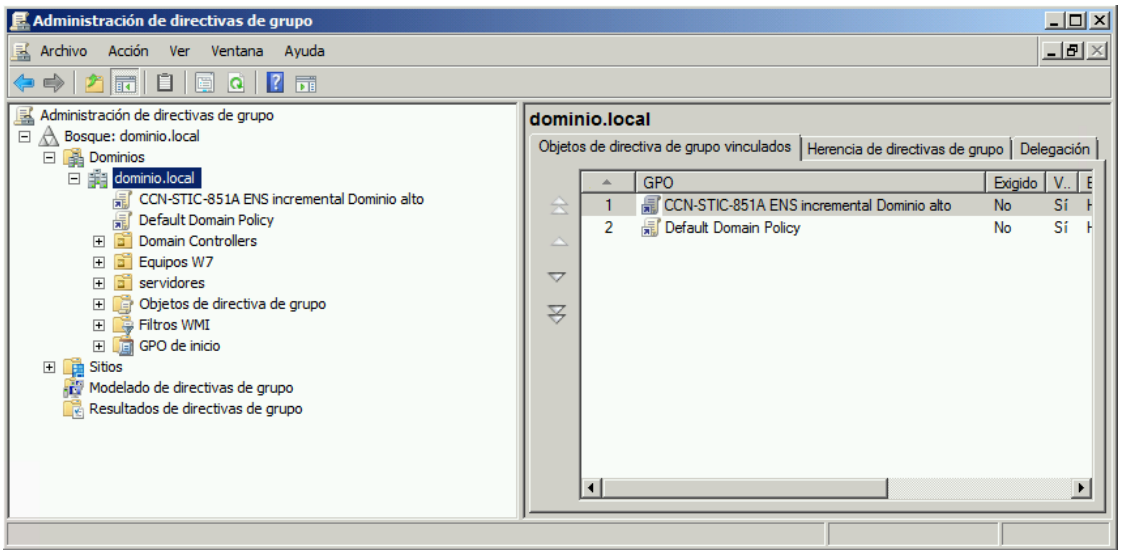
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán los GPO necesarios.

Nota: Esta guía asume que a los servidores controladores del dominio se les ha aplicado la configuración descrita en la guía CCN-STIC-851A para nivel medio o alto según Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio a securizar con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\Scripts" del controlador de dominio.
4.	Asegúrese de que al menos los siguientes directorios hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-869 AppLocker Raiz DC – medio alto – CCN-STIC-869 AppLocker Excepciones DC – medio alto
5.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo.** 
6.	El control de cuentas de usuario le solicitará usuario y contraseña con permisos de administración. Introduzca las credenciales con privilegios de administrador del dominio y pulse “Sí”. 

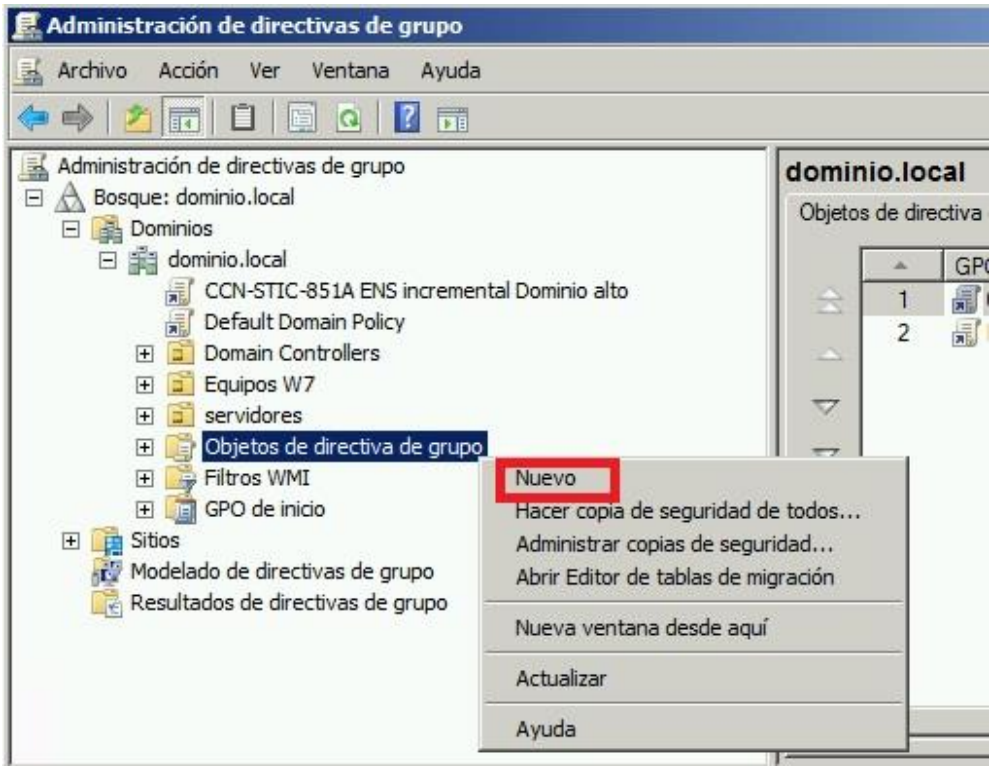
Paso	Descripción

7. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio>,** como se muestra en la siguiente imagen.

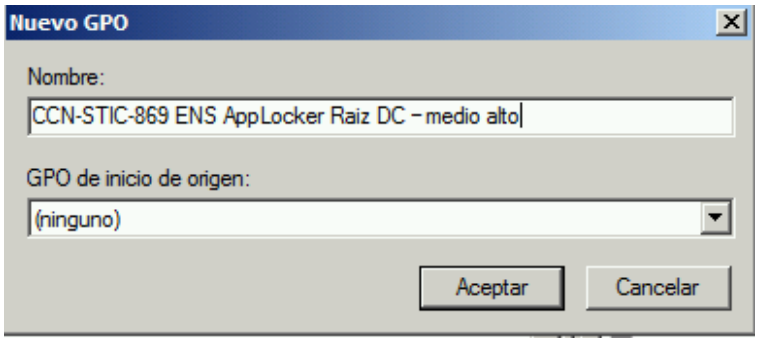


A continuación se procederá a la creación de las GPOs necesarias.

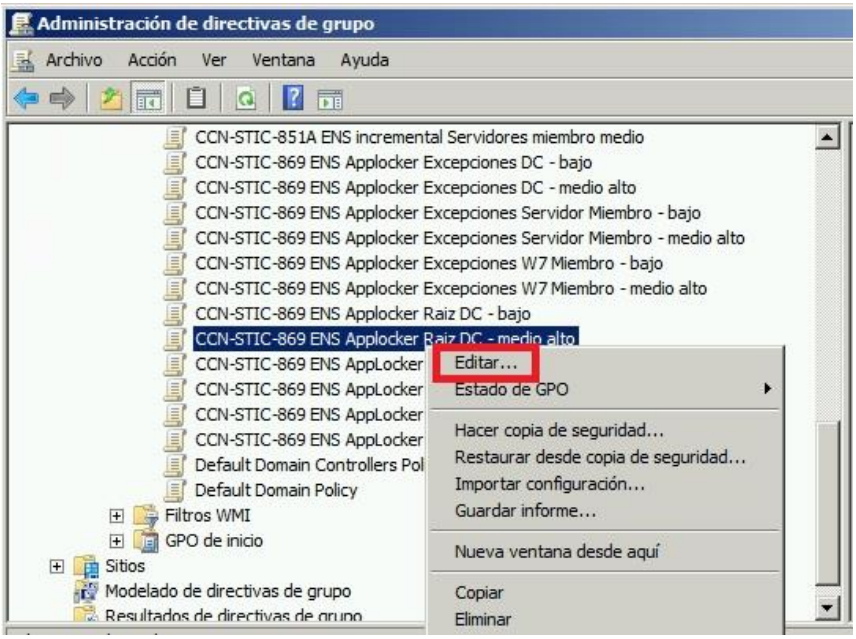
8. Expanda y seleccione el contenedor "**Objetos de directiva de grupo**" y, marcando con el botón derecho sobre dicho elemento, elija la opción "Nuevo" del menú contextual que aparecerá.



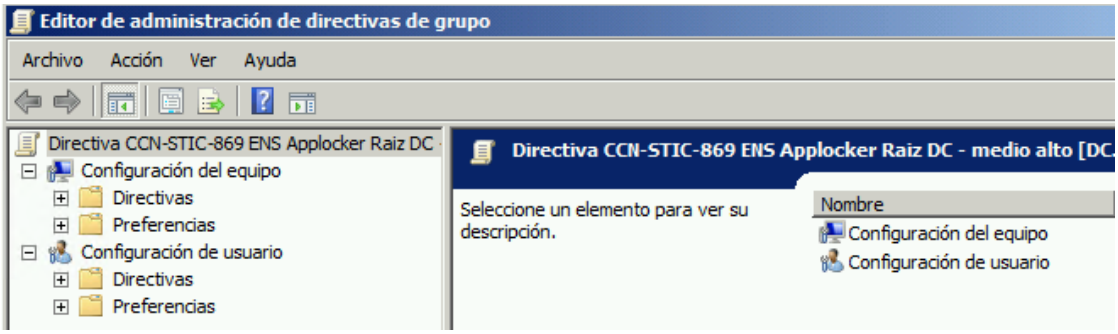
Paso	Descripción
9.	Asigne el siguiente nombre al nuevo GPO: “CCN-STIC-869 ENS AppLocker Raiz DC – medio alto”. Pulse “Aceptar” para cerrar la ventana.



10.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Raiz DC – medio alto**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



11.	Con ello se lanzará el “Editor de administración de directivas de grupo”.



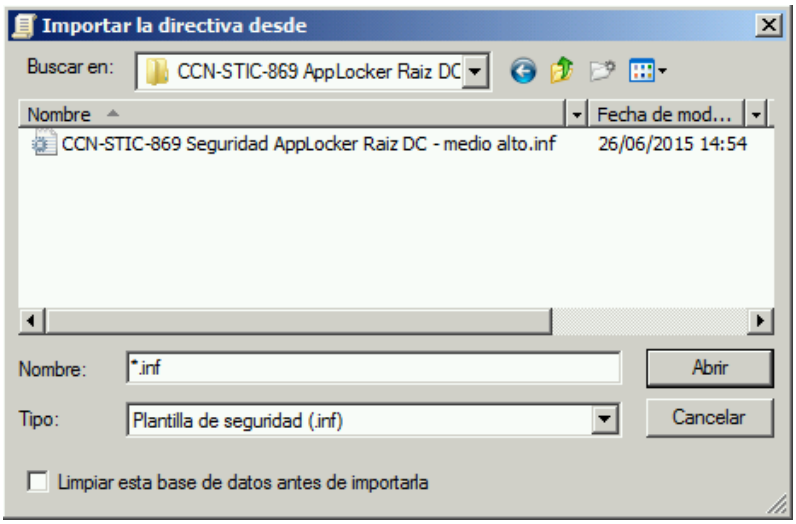
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando primero la configuración de la plantilla de seguridad que acompaña a esta guía e importando posteriormente la configuración de reglas de AppLocker que aplicarán a los controladores de dominio.

Paso	Descripción

12. En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho sobre ella, elija la opción “Importar directiva…”.

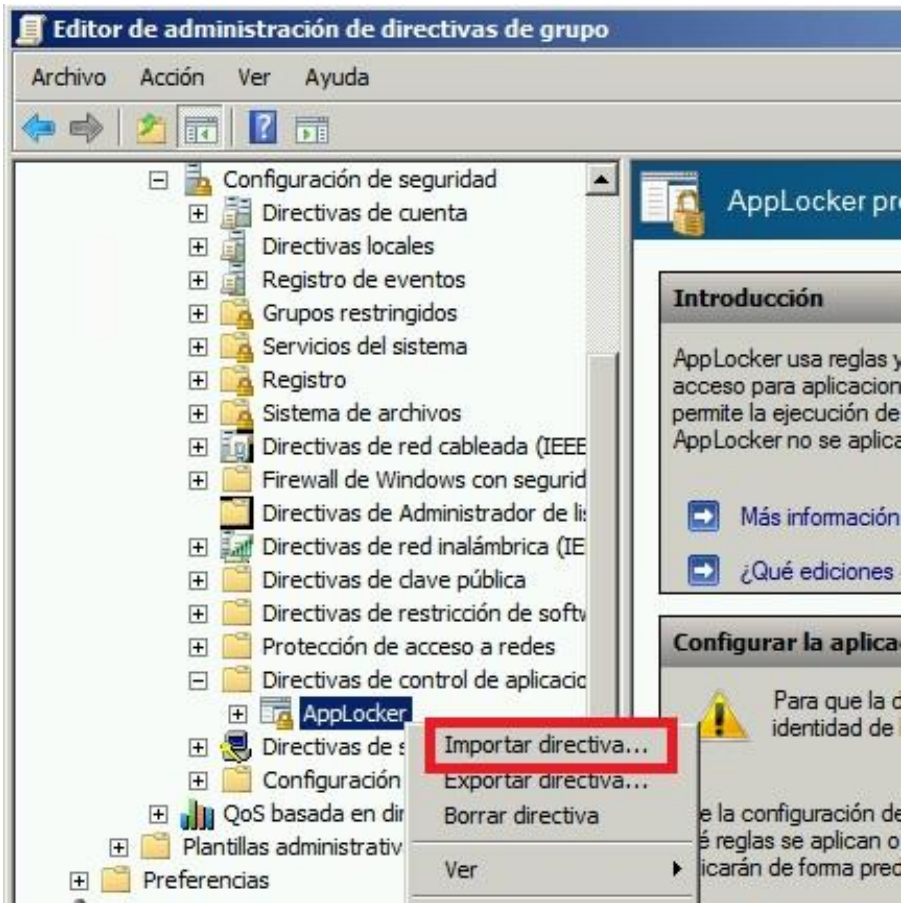
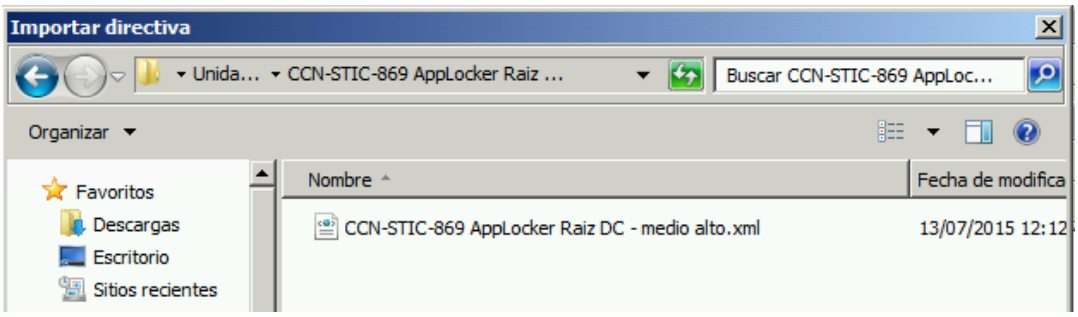
Directiva CCN-STIC-869 ENS AppLocker Raiz DC – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad.

13. En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz DC – medio alto” y seleccione el fichero “**CCN-STIC-869 Seguridad AppLocker Raiz DC – medio alto.inf**” mediante doble clic sobre él o pulsando el botón “Abrir”.

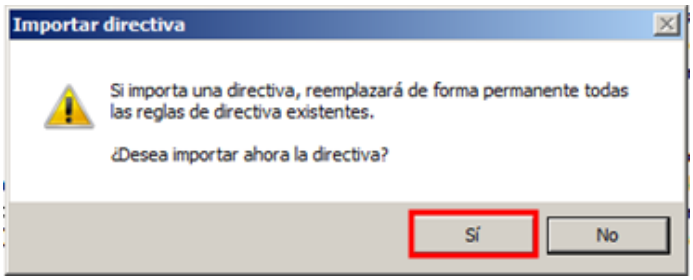


Con esto, habrá quedado importada la plantilla de seguridad en este GPO.

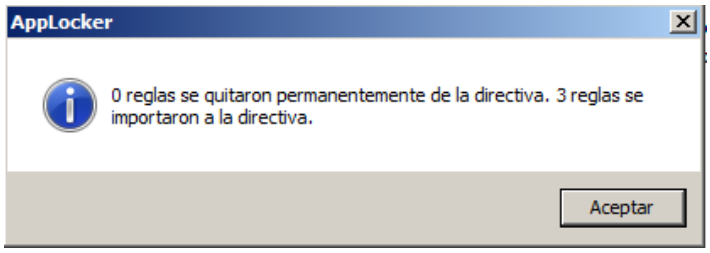
Nota: No cierre todavía el “Editor de administración de directivas de grupo”, y continúe con el siguiente paso.

Paso	Descripción
14.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-ENS 869 AppLocker Raiz DC – medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
15.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz DC – medio alto” y seleccione el fichero “**CCN-STIC-869 AppLocker Raiz DC – medio alto.xml**” mediante doble clic sobre él o pulsando el botón “Abrir”. 

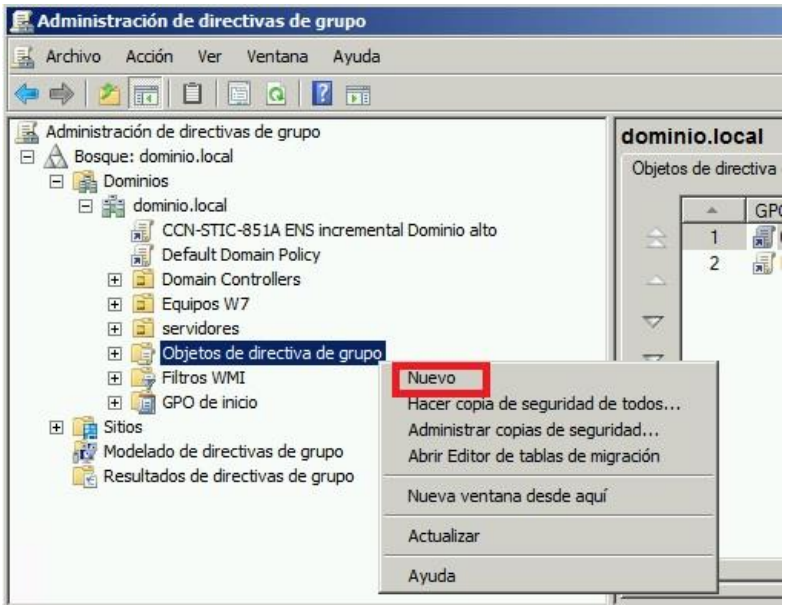
Paso	Descripción
16.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Si”.



17.	Aparecerá un nuevo mensaje informativo indicando que se importaron tres reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.

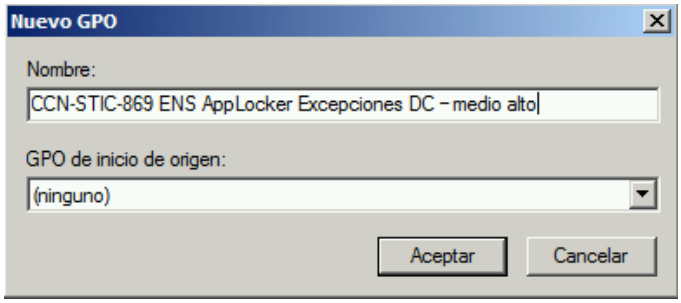


18.	El GPO "CCN-STIC-869 ENS AppLocker Raiz DC – medio alto" está creado y configurado. Cierre la ventana del “Editor de administración de directivas de grupo”.
19.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Objetos de directiva de grupo”**, y marcando con el botón derecho sobre dicho elemento, elija la opción “Nuevo” del menú contextual que aparecerá.

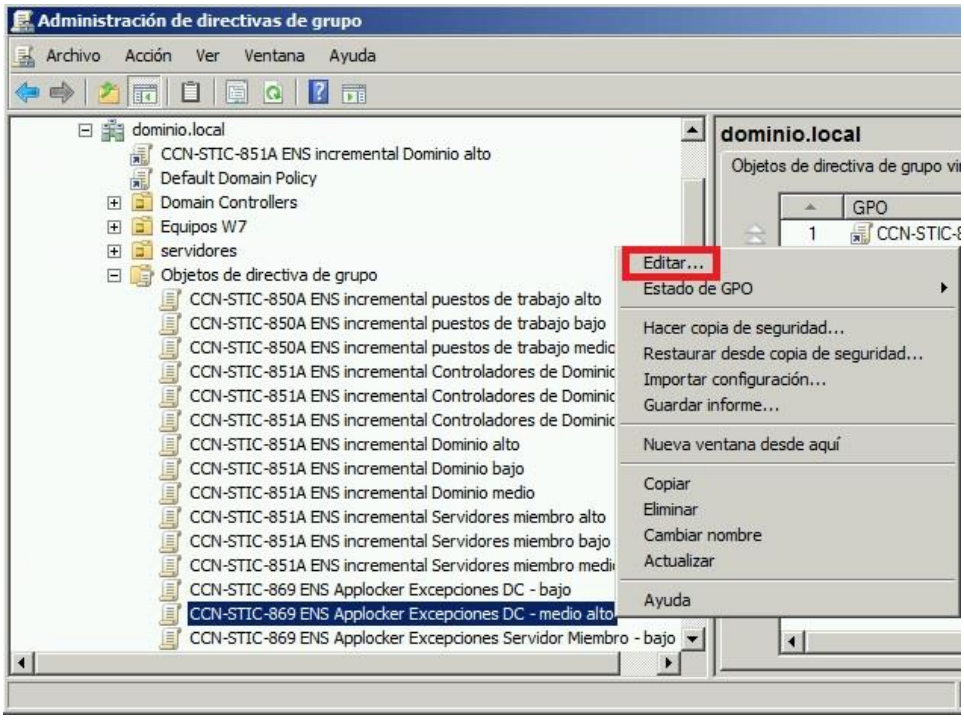


Paso	Descripción

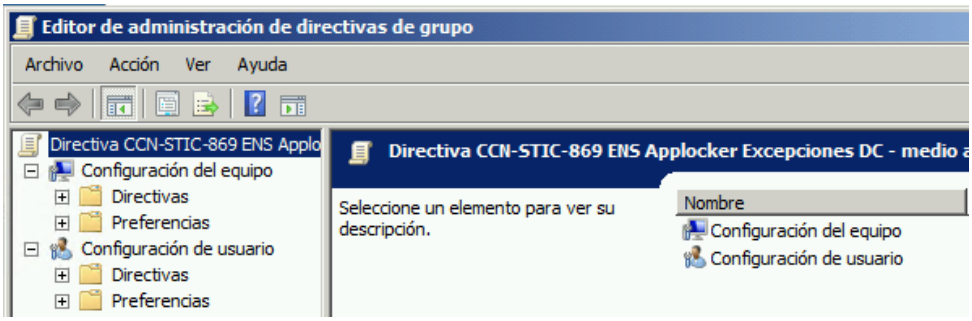
20. Asigne el siguiente nombre al GPO: “CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto”. Pulse “Aceptar” para cerrar la ventana.



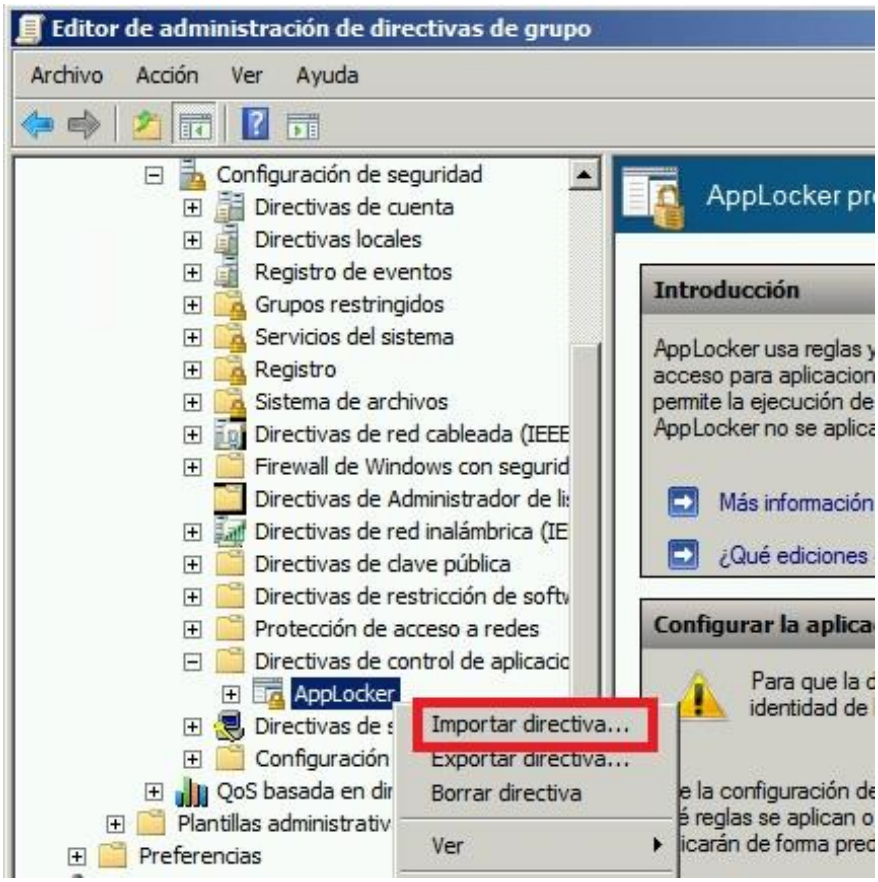
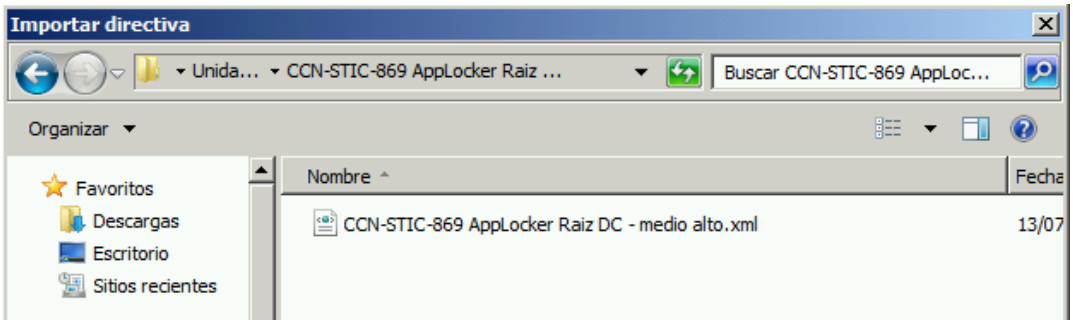
21. Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.

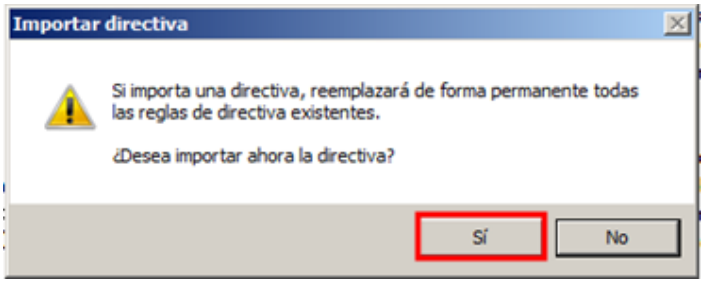
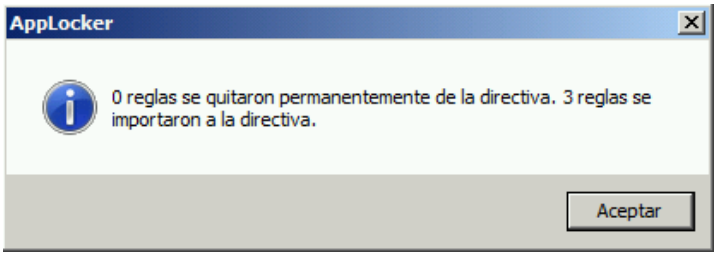


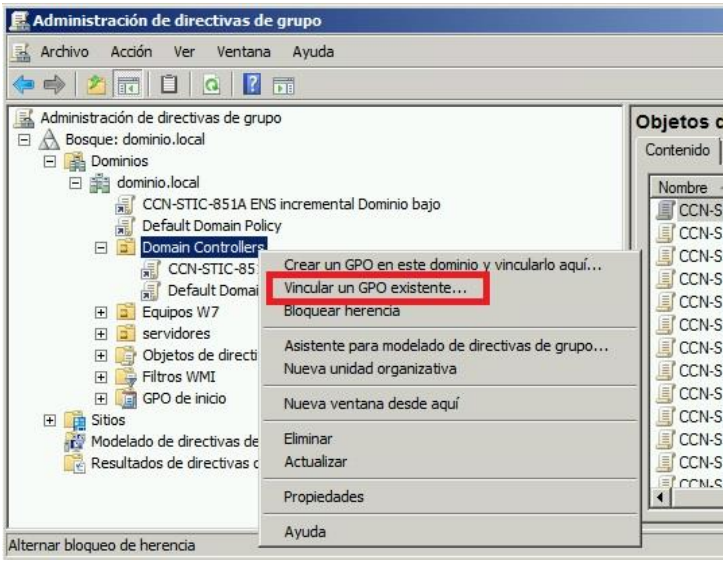
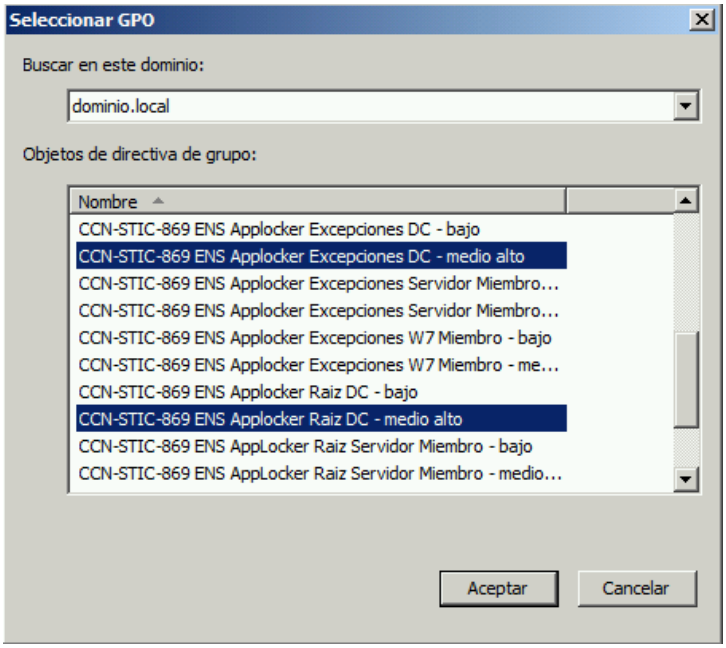
22. Con ello se lanzará el “Editor de administración de directivas de grupo”.



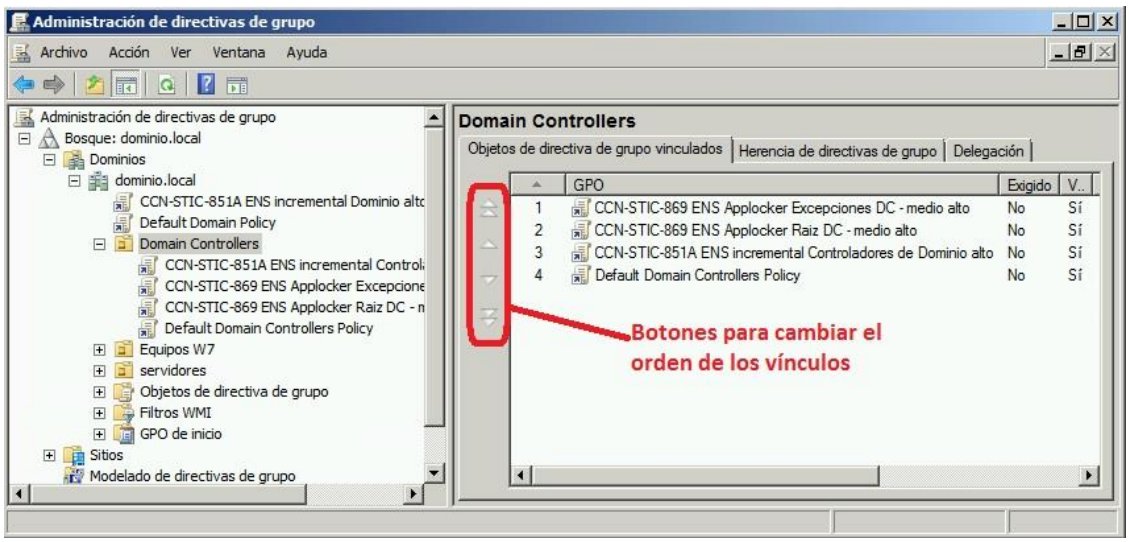
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando la configuración de las reglas de AppLocker.

Paso	Descripción
23.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
24.	En el cuadro de dialogo abierto navegue hasta el directorio “c:\scripts\CCN-STIC-869 AppLocker Excepciones DC – medio alto”, seleccione el fichero “**CCN-STIC-869 AppLocker Excepciones DC – medio alto.xml**” mediante doble clic sobre él o pulsando “Abrir”. 

Paso	Descripción
25.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”. 
26.	Aparecerá un nuevo mensaje informativo indicando que se importaron 3 reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje. 
27.	Las reglas recién importadas asumen que el controlador de dominio tiene los ficheros de configuración del directorio activo en la unidad “D:\” (D:\ntds y D:\SYSVOL). Si su caso no es así, puede editar la política de AppLocker en este momento para adaptarla a sus necesidades. **Nota:** En el anexo H puede encontrar más información sobre los pasos a seguir para la creación, edición, o eliminación de reglas de AppLocker. Tenga en consideración que en este caso no será necesario realizar el procedimiento desde una máquina de referencia ya que el GPO no se encuentra vinculado a ninguna Unidad Organizativa.
28.	Cuando termine de adaptar la política a sus necesidades, cierre la ventana del “Editor de administración de directivas de grupo” y proceda a la vinculación de los GPO “CCN-STIC-869 ENS AppLocker Raiz DC – medio alto" y “CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto” a la unidad organizativa donde residan sus controladores de dominio. Siga los pasos tal y como se detallan a continuación.

Paso	Descripción
29.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Domain Controllers**". Pulse botón derecho sobre la OU y elija la opción “Vincular un GPO existente…” del menú contextual.  **Nota:** Si sus controladores de dominio se encontraran en otra ubicación vincule la siguiente GPO en dicha OU.
30.	En el nuevo cuadro de diálogo desplegado, seleccione los GPO (haciendo uso de la tecla “CTRL”): “CCN-STIC-869 ENS AppLocker Raiz DC – medio alto” y “CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto”. Pulse “Aceptar”. 

Paso	Descripción
31.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Domain Controllers**", y observe el orden de los vínculos en la parte central de la ventana.



El orden de los vínculos ha de ser el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto.
2) CCN-STIC-869 ENS AppLocker Raiz DC – medio alto.
3) Resto de GPOs.

Si el orden mostrado fuera otro, seleccione los GPOs por turnos y utilice los botones indicados en la figura para cambiar el orden de los vínculos de forma que coincida con el indicado aquí.

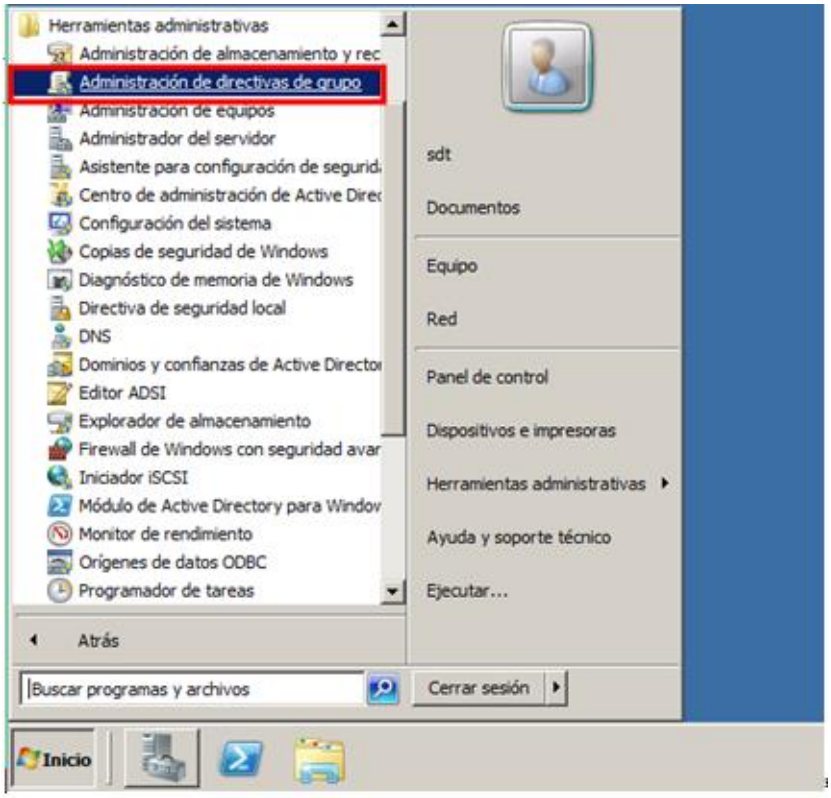
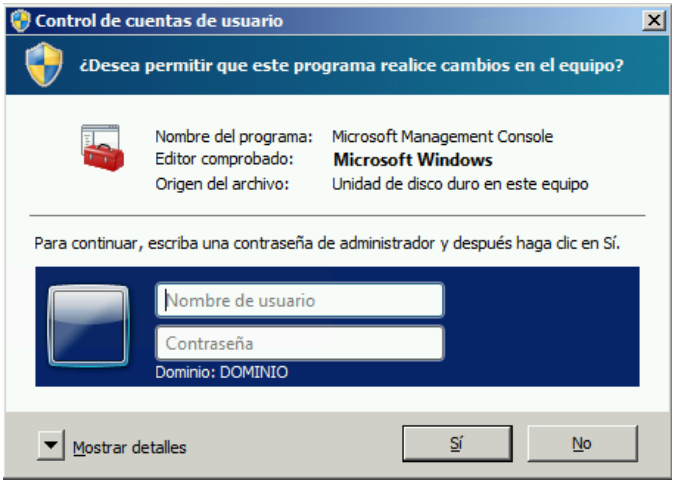
32.	Cierre la ventana del “Administración de directivas de grupo”.
33.	Elimine la carpeta “C:\Scripts”.

2. CONFIGURACIÓN DE APPLOCKER EN SERVIDOR MIEMBRO WINDOWS SERVER 2008 R2 O WINDOWS SERVER 2012 R2

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

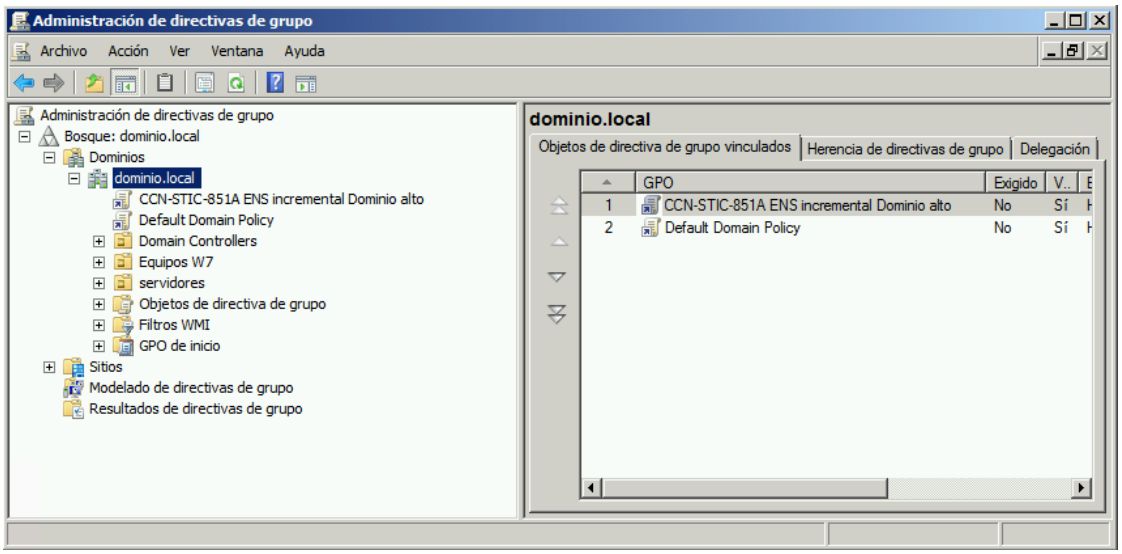
Nota: Esta guía asume que a los servidores controladores del dominio y servidor miembro, se les ha aplicado la configuración descrita en la guía CCN-STIC-851A para nivel medio o alto según el Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\scripts" del controlador de dominio.

Paso	Descripción
4.	Asegúrese de que al menos los siguientes directorios hayan sido copiados al directorio "C:\Scripts" del controlador de dominio: – CCN-STIC-869 AppLocker Raiz Servidor Miembro – medio alto – CCN-STIC-869 AppLocker Excepciones Servidor Miembro – medio alto
5.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo.** 
6.	El control de cuentas de usuario le solicitará usuario y contraseña con permisos de administración. Introduzca las credenciales con privilegios de administrador del dominio y pulse "Sí". 

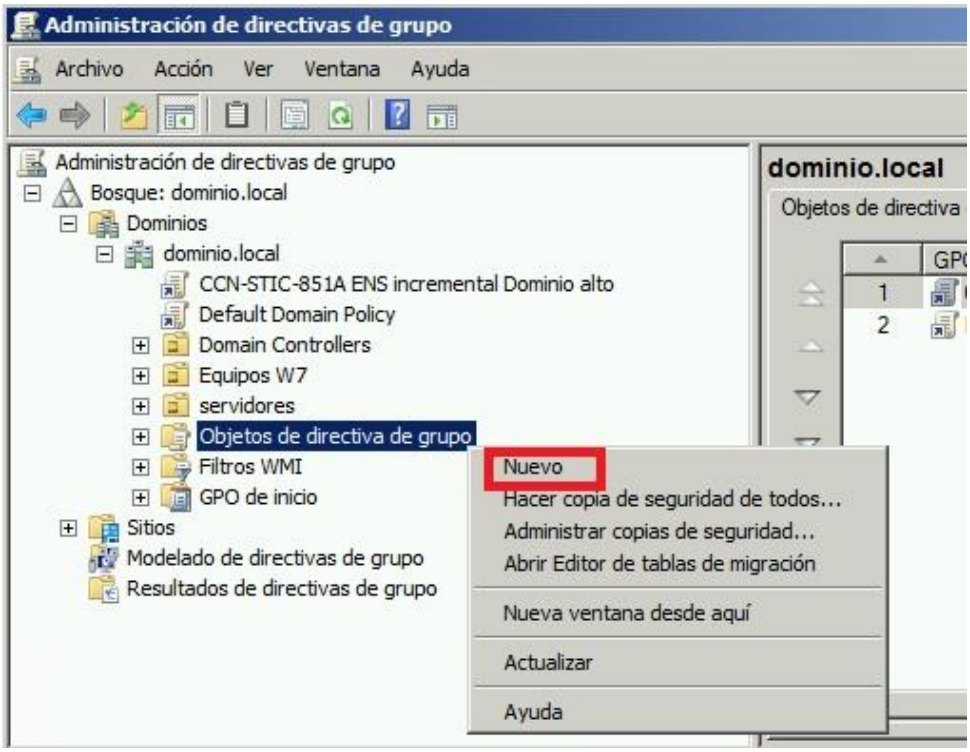
Paso	Descripción

7. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio>,** como se muestra en la siguiente imagen.

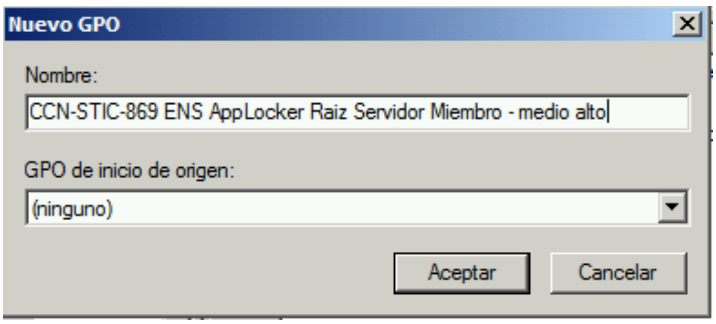


A continuación se procederá a la creación de los GPOs necesarios.

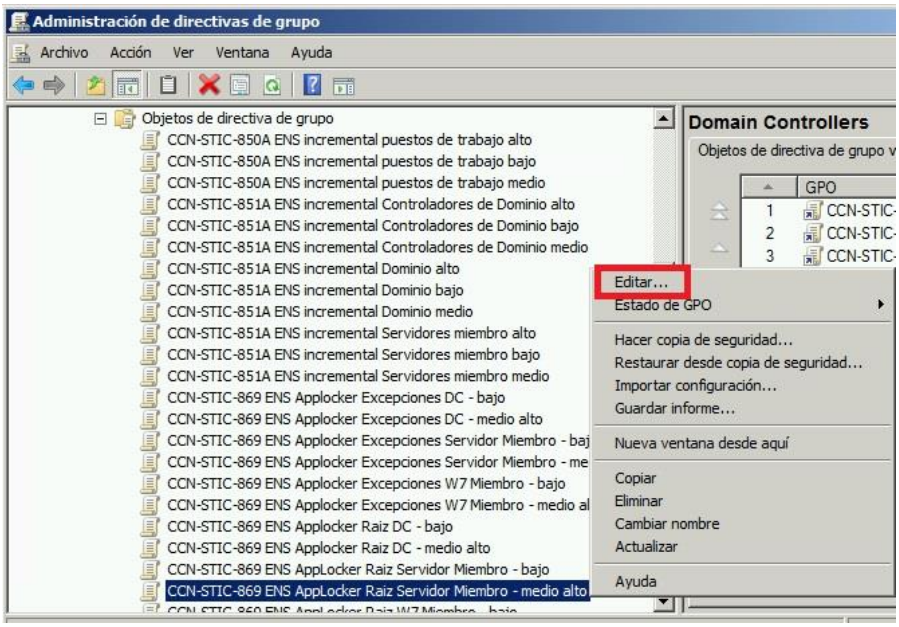
8. Expanda y seleccione el contenedor "**Objetos de directiva de grupo**" y, marcando con el botón derecho sobre dicho elemento, elija la opción "Nuevo" del menú contextual que aparecerá.



Paso	Descripción
9.	Asigne el siguiente nombre al nuevo GPO: “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto”. Pulse “Aceptar” para cerrar la ventana.



10.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.



11.	Con ello, se lanzará el “Editor de administración de directivas de grupo”.

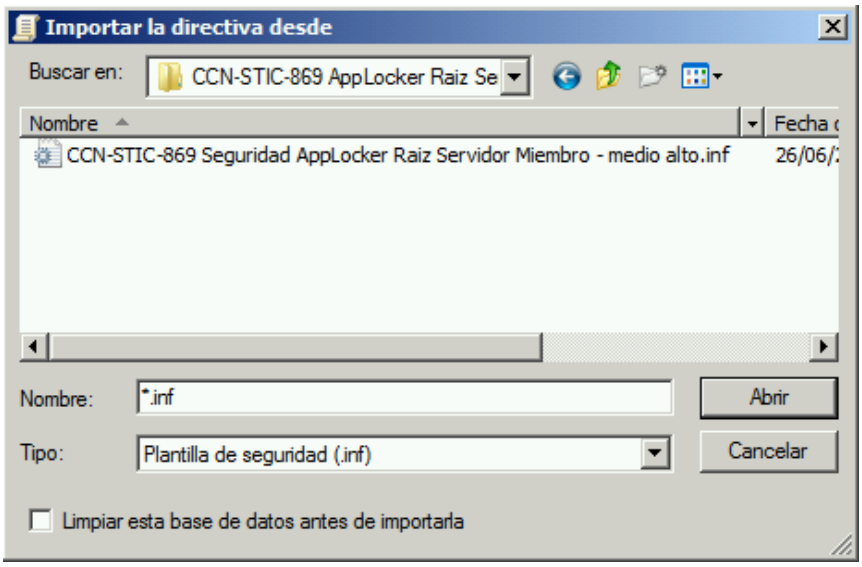
En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando primero la configuración de la plantilla de seguridad que acompaña a esta guía e importando posteriormente la configuración de reglas de AppLocker que aplicarán a los Servidores Miembros.

Paso	Descripción

12. En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción “Importar directiva…”

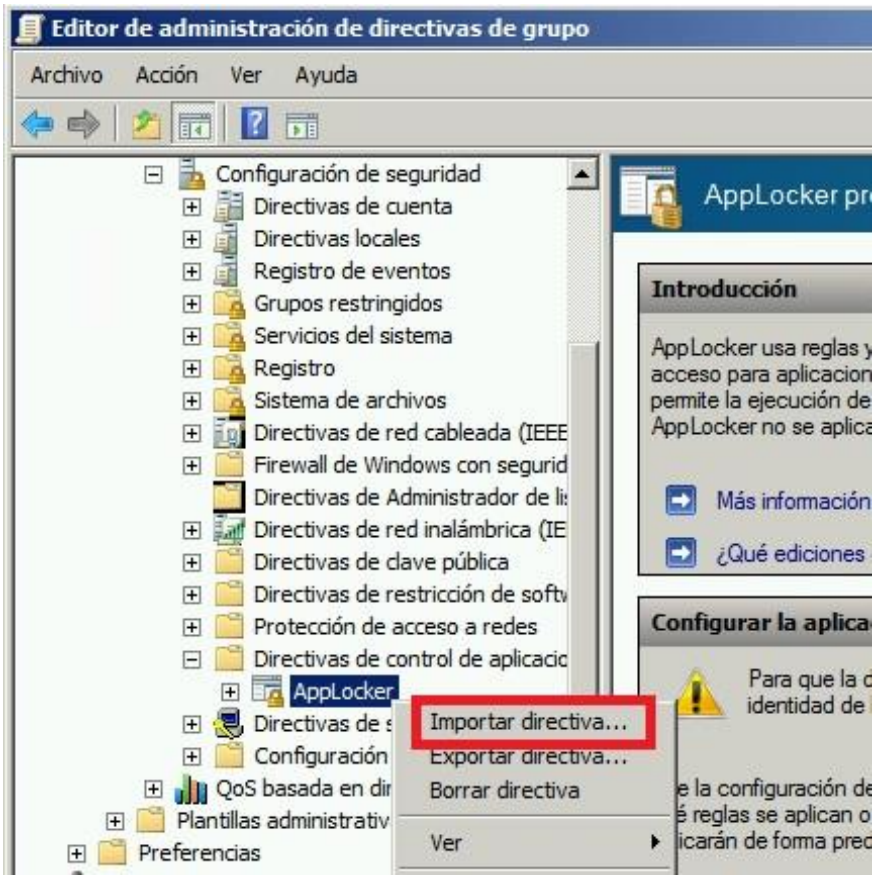
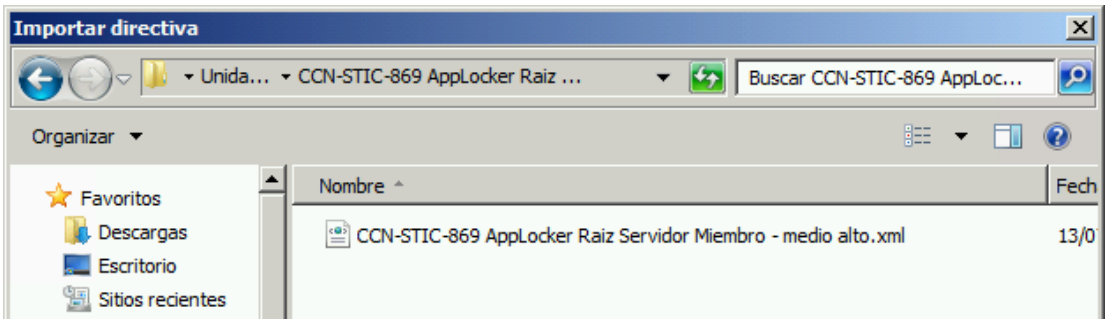
Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad.

13. En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz Servidor Miembro – medio alto” y seleccione el fichero “**CCN-STIC-869 Seguridad AppLocker Raiz Servidor Miembro – medio alto.inf**” mediante doble clic sobre él o pulsando “Abrir”.

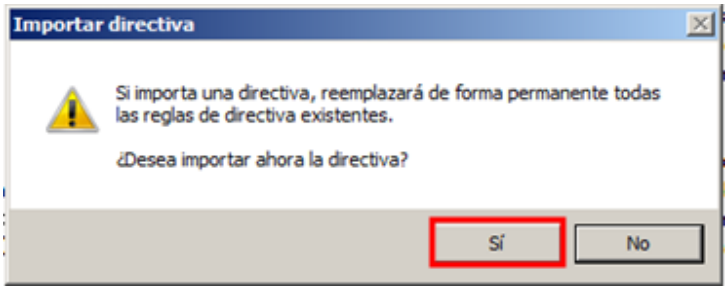


Con esto, habrá quedado importada la plantilla de seguridad en este GPO.

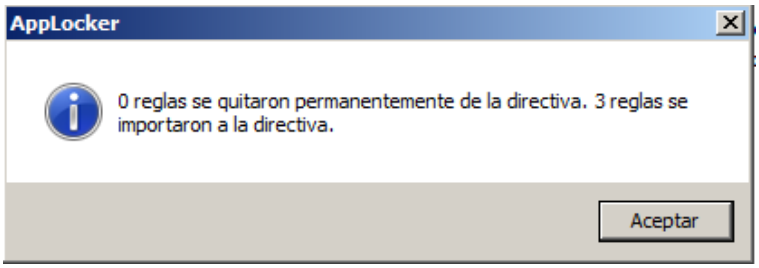
Nota: No cierre todavía el “Editor de administración de directivas de grupo” y continúe con el siguiente paso.

Paso	Descripción
14.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-ENS 869 AppLocker Raiz Servidor Miembro – medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
15.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz Servidor Miembro – medio alto” y seleccione el fichero “**CCN-STIC-869 AppLocker Raiz Servidor Miembro – medio alto.xml**” mediante doble clic sobre él o pulsando el botón “Abrir”. 

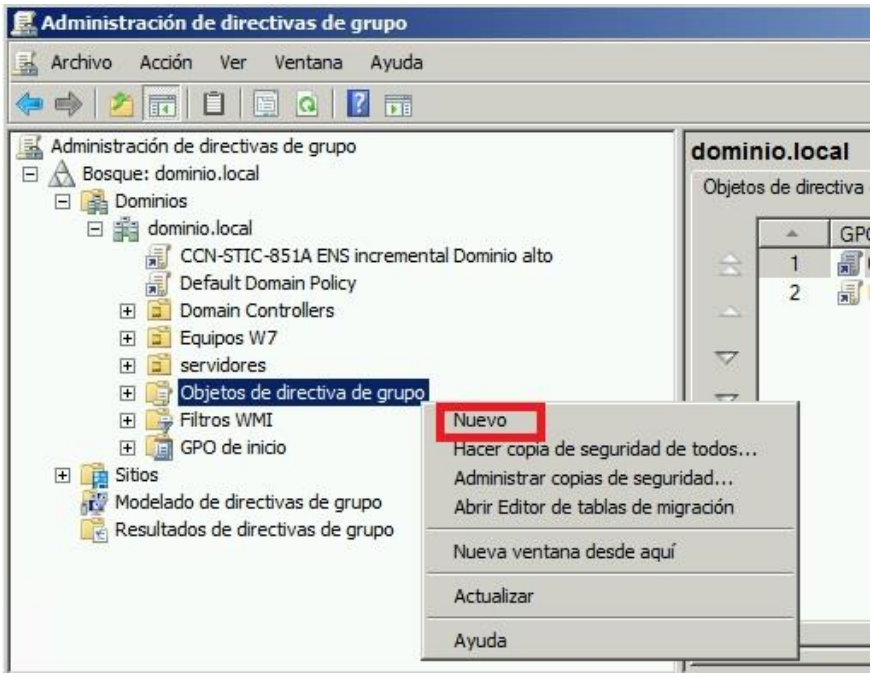
Paso	Descripción
16.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Si”.



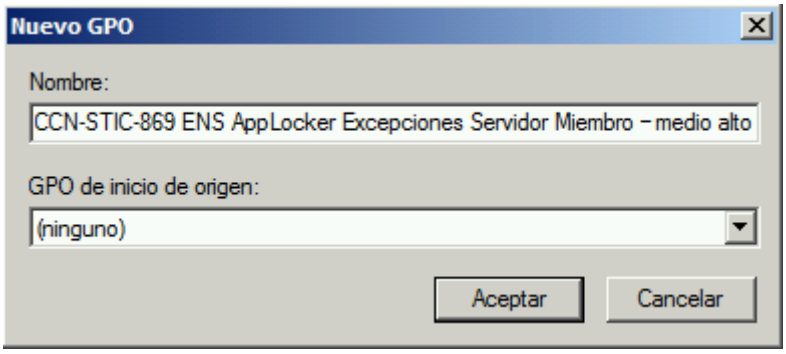
17.	Aparecerá un nuevo mensaje informativo indicando que se importaron tres reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.



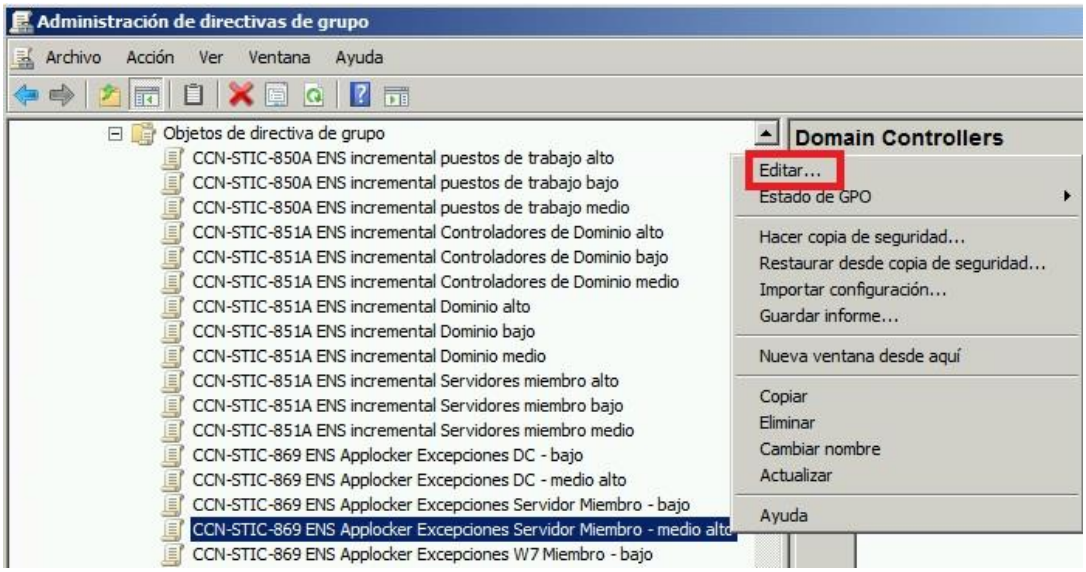
18.	El GPO "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto" está creado y configurado. Cierre la ventana del “Editor de administración de directivas de grupo”.
19.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Objetos de directiva de grupo”**, y marcando con el botón derecho sobre dicho elemento, elija la opción “Nuevo” del menú contextual que aparecerá.



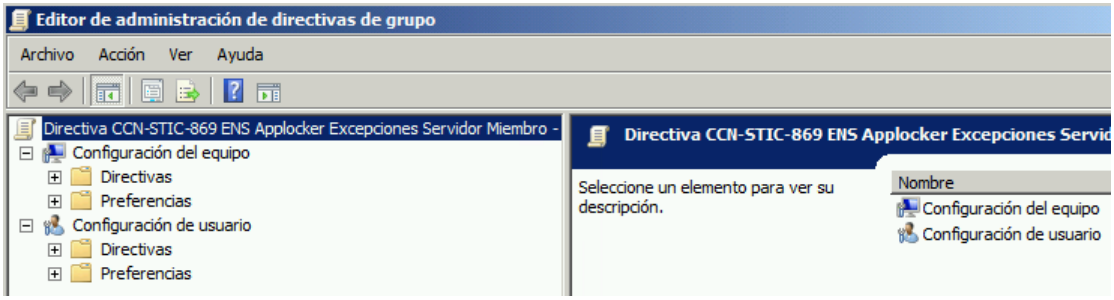
Paso	Descripción
20.	Asigne el siguiente nombre al GPO: “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto”. Pulse “Aceptar” para cerrar la ventana.



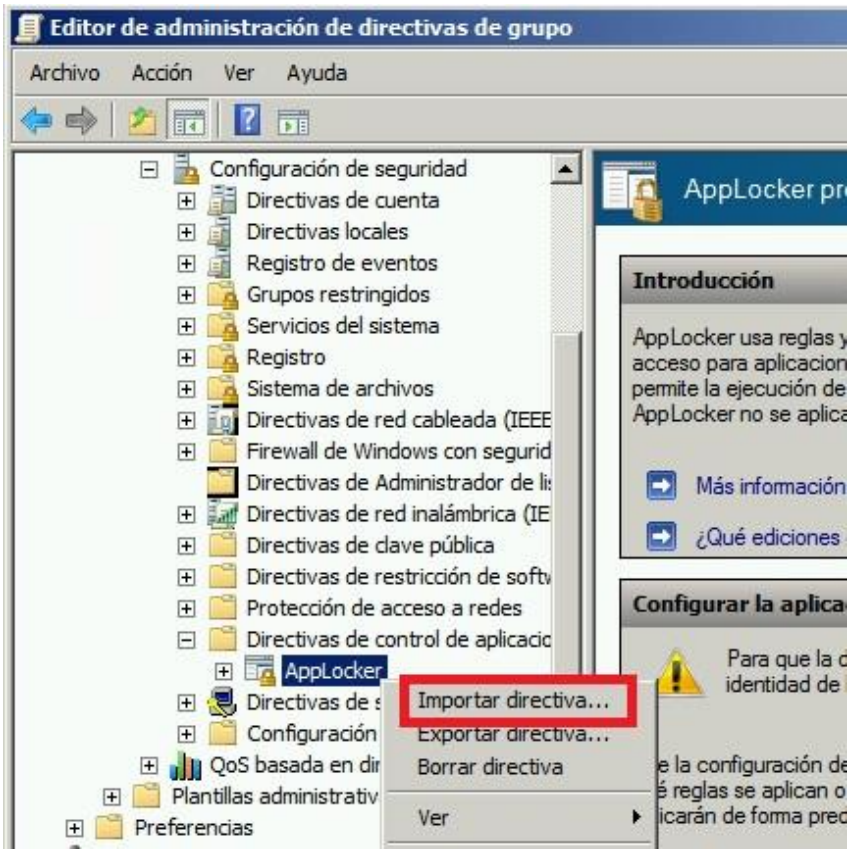
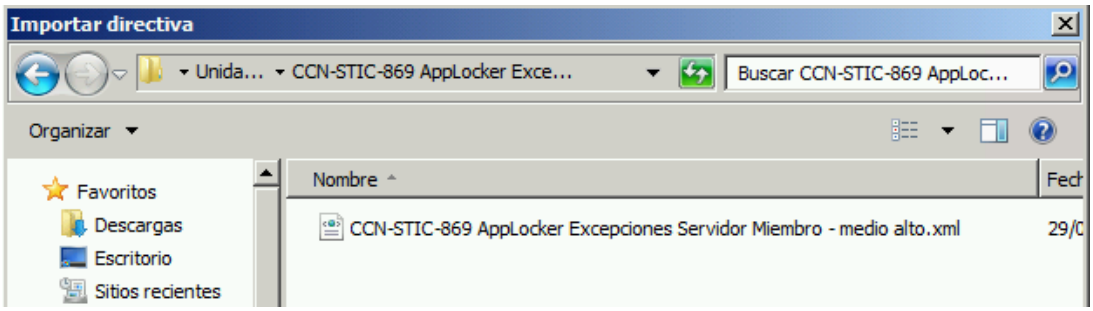
21.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto**" y, marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.

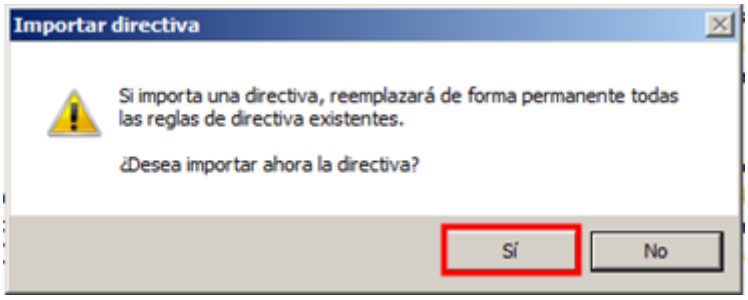
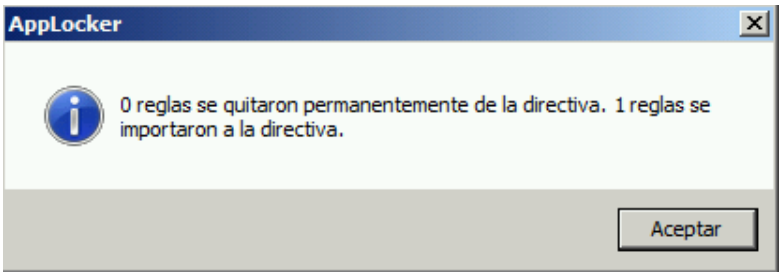


22.	Con ello se lanzará el “Editor de administración de directivas de grupo”.



En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando la configuración de las reglas de AppLocker.

Paso	Descripción
23.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción importar directiva del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
24.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Excepciones Servidor Miembro –medio alto”, seleccione el fichero “**CCN-STIC-869 AppLocker Excepciones Servidor Miembro – medio alto.xml**” y haga doble clic sobre él o pulse “Abrir”. 

Paso	Descripción
25.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”. 
26.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. 
27.	Antes de vincular los GPO a las unidades organizativas donde residan los servidores miembros ha de evaluar si se hace necesario establecer nuevas reglas de AppLocker para permitir software instalado en rutas no estándar. Si es así no cierre el “Editor de administración de directivas de grupo” y continúe en el paso siguiente. Si por el contrario no desea crear nuevas reglas cierre el “Editor de administración de directivas de grupo” y continúe en el paso 38.

Los dos GPO creados en los pasos anteriores (CCN-STIC-869 ENS Applocker Raiz Servidor Miembro – medio alto y CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro – medio alto) no se vincularán a la Unidad Organizativa donde resida el servidor hasta que se hayan creado las excepciones necesarias para el correcto funcionamiento de los aplicativos de dicho servidor. Se hace necesario evaluar qué rutas extra o nuevos ejecutables se han de permitir antes de la vinculación de los GPO.

Con el objeto de ayudar al administrador a definir dichas rutas, a continuación se enumeran las reglas que por defecto incluyen las dos políticas creadas:

- CCN-STIC-869 ENS Applocker Raiz Servidor Miembro – medio alto:
  - Permitir ejecución para todos los usuarios desde %WINDIR%
  - Permitir ejecución para todos los usuarios desde %PROGRAMFILES%
  - Bloquear ejecución para todos los usuarios desde %WINDIR\Temp%
- CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro – medio alto:
  - Permitir ejecución desde CD y DVD para usuarios Administradores.

La creación de nuevas reglas a modo de excepción se ha de realizar mediante la edición del GPO CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro – medio alto. El GPO CCN-STIC-869 Applocker Raiz Servidor Miembro – medio alto no se debe modificar.

Los siguientes pasos describen la operativa, a modo de ejemplo, para permitir la ejecución de una aplicación instalada en "C:\aplicacion".

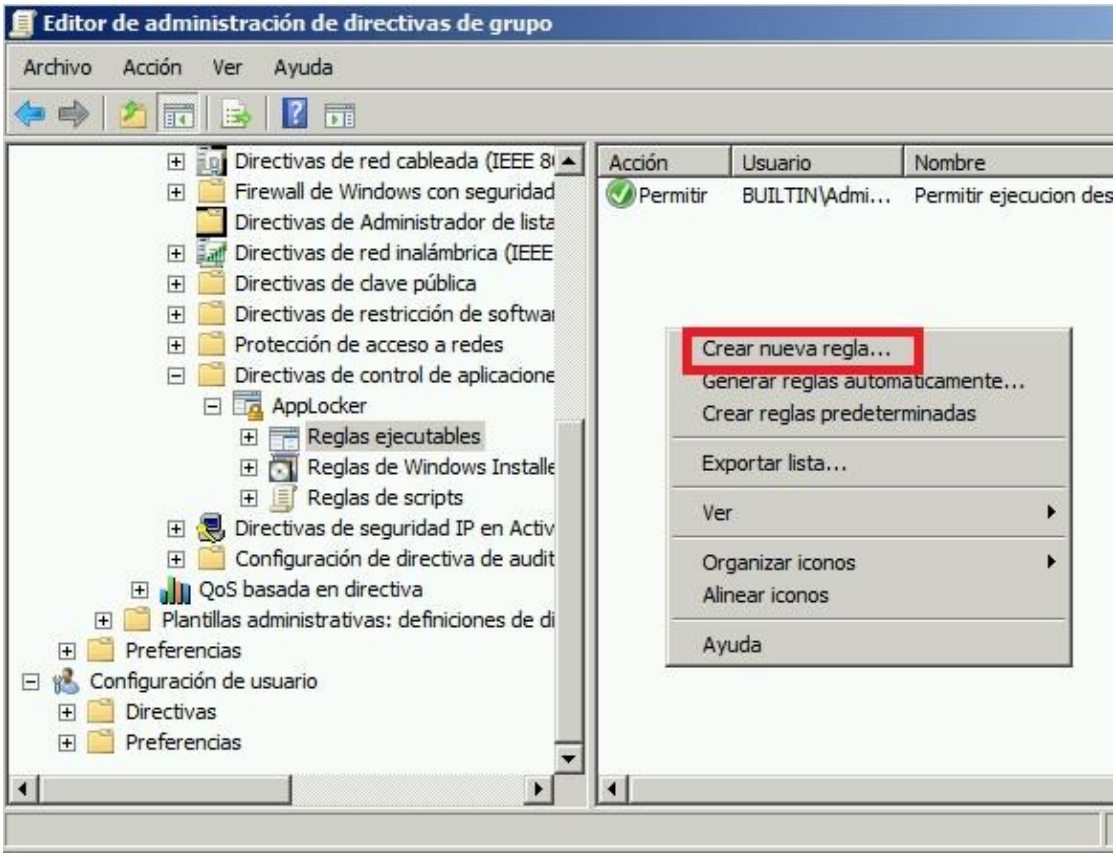
Nota: La carpeta "Aplicación" ha sido creada a modo de ejemplo. Para más información sobre la creación y edición de reglas de AppLocker consulte el anexo H.

Paso	Descripción
28.	Haciendo uso del mismo "Editor de administración de directivas de grupo" del paso anterior podrá crear o modificar las reglas que considere.

Nota: Las nuevas reglas para servidores miembros siempre se han de crear sobre la directiva CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro – medio alto.

Para crear una nueva regla, navegue hasta la ubicación indicada y elija la opción "Crear nueva regla…" del menú contextual que aparece tras pulsar botón derecho en el panel derecho.

Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro –medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables

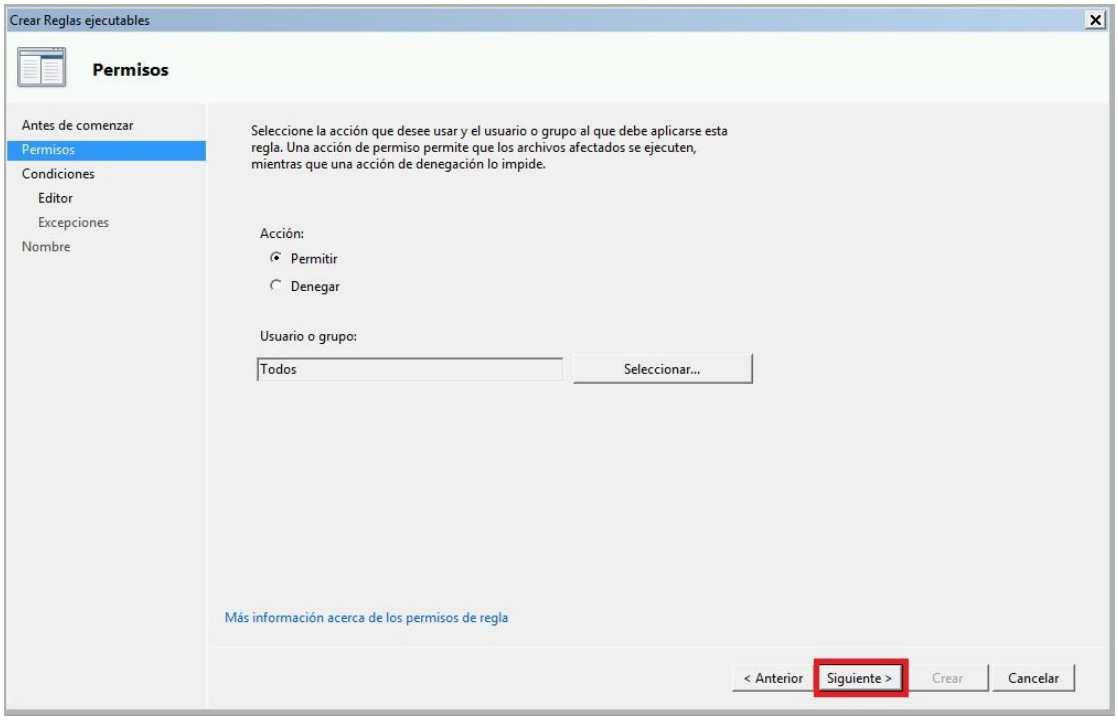


Nota: No es necesario editar la directiva de AppLocker en una máquina de referencia tal y como se describe en el anexo H, ya que los nuevos GPO todavía no se encuentran vinculados a ninguna Unidad Organizativa.

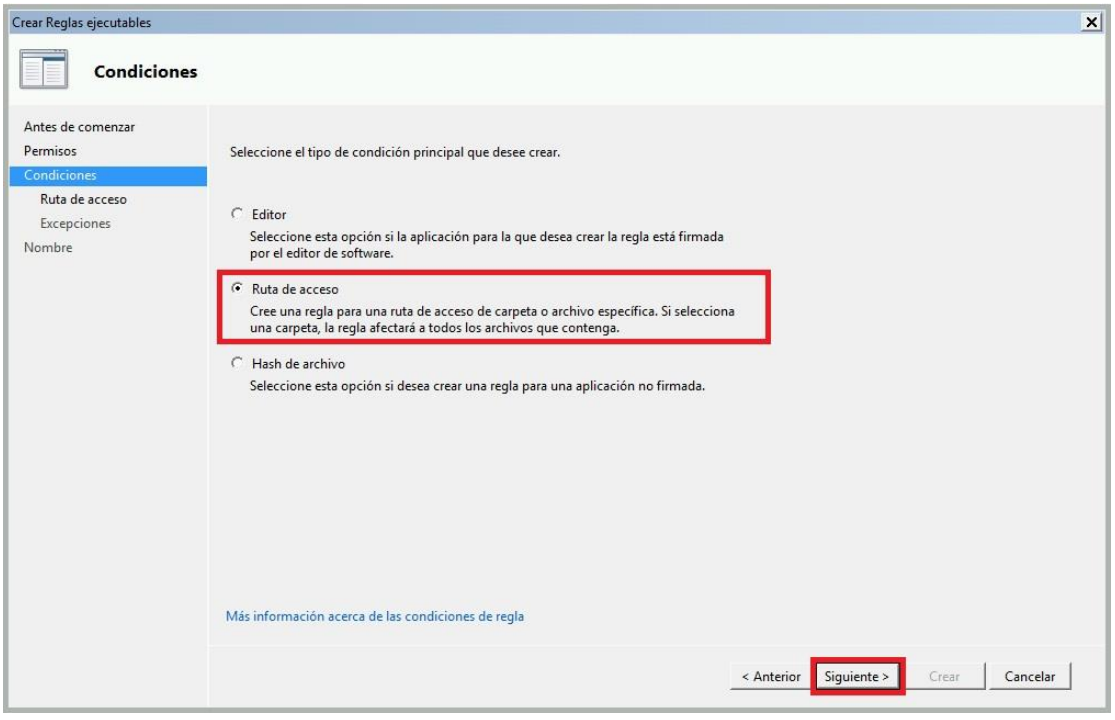
29.	En la primera ventana del asistente pulse "Siguiente >".

Paso	Descripción

30. En permisos mantenga la configuración existente y pulse el botón “Siguiente >”.

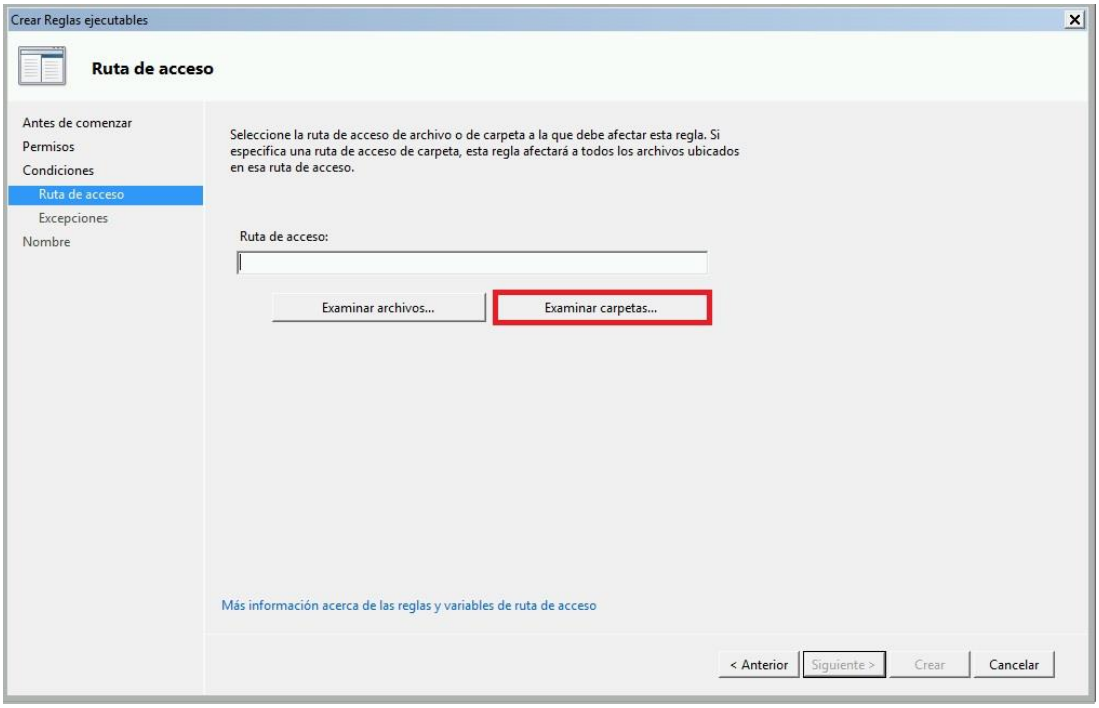


31. En la pantalla de condiciones, seleccione la opción “Ruta de acceso” y pulse “Siguiente >”.



Paso	Descripción

32. En la pantalla “Ruta de acceso” pulse el botón “Examinar carpetas…”.

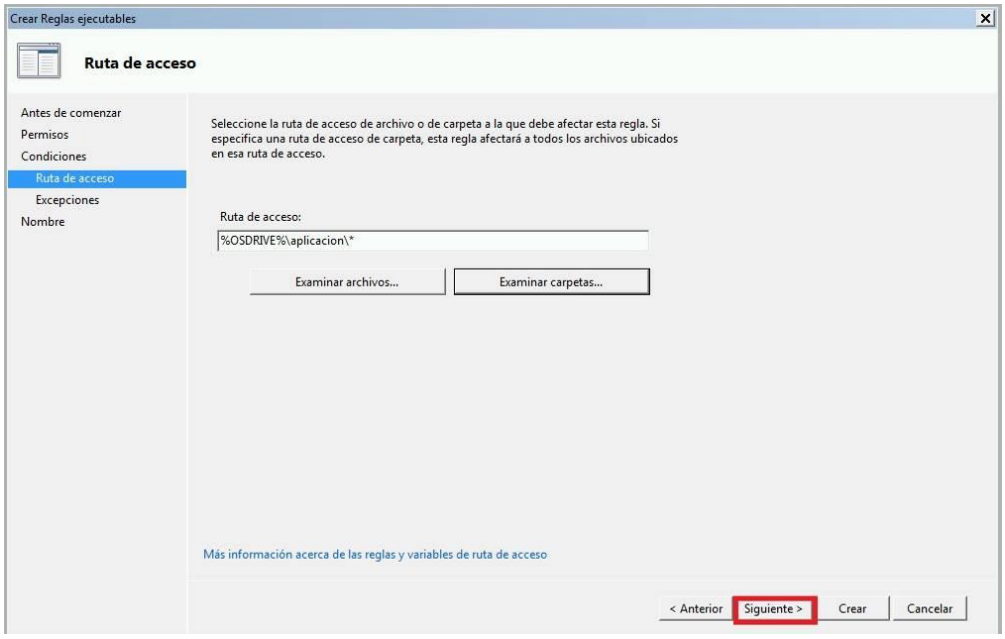


Nota: El ejemplo mostrado simula que se va a permitir ejecutar contenido de una carpeta. Si sólo fuera a ejecutar un único archivo .exe de dicha carpeta, se debería emplear la opción “Examinar archivos…” y seleccionar el único fichero ejecutable. Debe tener en consideración que las aplicaciones actuales son altamente complejas y puede que la carga de la aplicación se realice a través de un fichero .exe, pero este luego llame o dependa de otros ejecutables. Si tiene claro que la aplicación solo va a necesitar llamar a un fichero ejecutable, puede seleccionar la opción examinar archivos, de lo contrario deberá emplear el mecanismo de examinar carpetas para permitir la ejecución de todo el contenido de dicha carpeta.

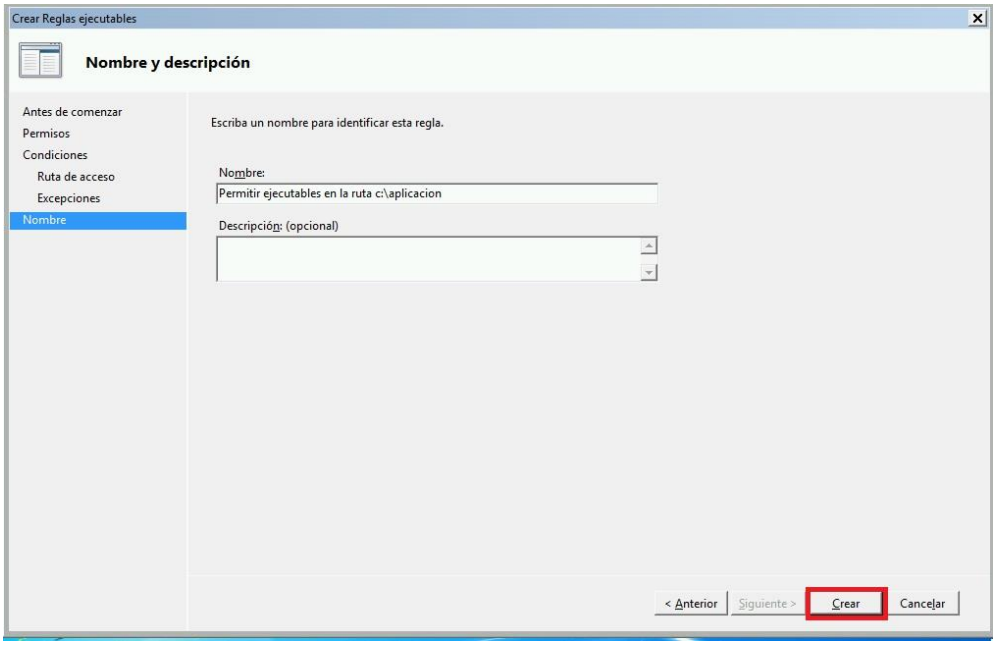
33. Seleccione la carpeta de la que desee crear la excepción. En el ejemplo se establece que el contenido ejecutable se encuentra en la carpeta “C:\aplicacion”.

Nota: Si no existiese la ruta de la aplicación del servidor en el controlador de domino, cree toda la estructura de carpetas necesaria para poder seleccionarla.

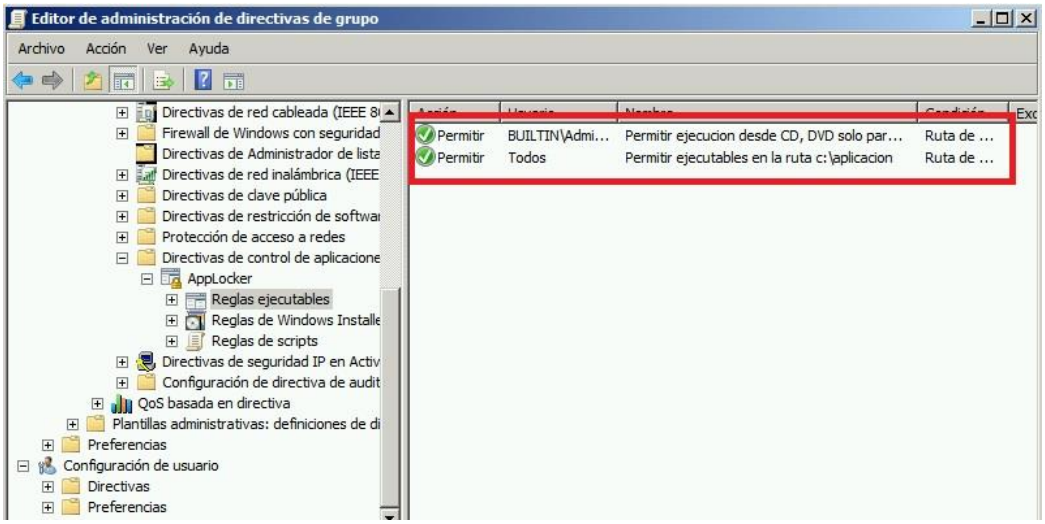
Paso	Descripción
34.	Una vez agregada la carpeta, pulse el botón “Siguiente >”.



35.	Si desea que algún contenido específico en dicha carpeta no sea ejecutado, puede agregar una excepción en la pantalla de “Excepciones”. Bien cuando haya agregado las excepciones o si no desea realizar ninguna excepción, pulse el botón “Siguiente >”.
36.	Para finalizar deberá asignar un nombre identificativo a la regla. En el ejemplo se asignará el nombre “Permitir ejecutables en la ruta C:\aplicacion”. Pulse el botón “Crear” cuando haya asignado un nombre.



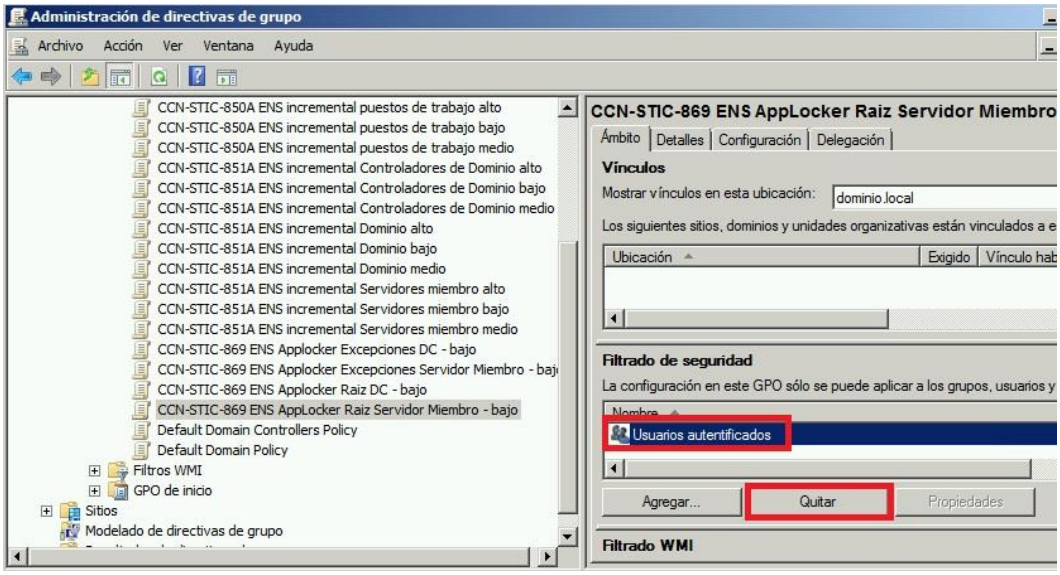
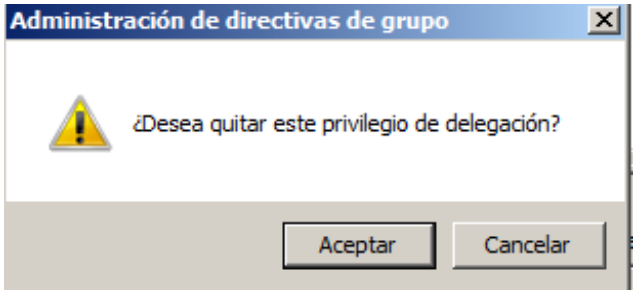
Paso	Descripción
37.	Compruebe la creación de la regla en el panel derecho del “Editor de administración de directivas de grupo”.



Una vez creadas todas las reglas necesarias para la ejecución del software del servidor, se puede proceder a la vinculación de las directivas a la unidad organizativa a la que pertenezca el servidor a securizar. Si dicha unidad contiene otros servidores que no han de recibir las reglas de AppLocker será necesario filtrar la aplicación de las dos directivas haciendo uso del filtrado de seguridad.

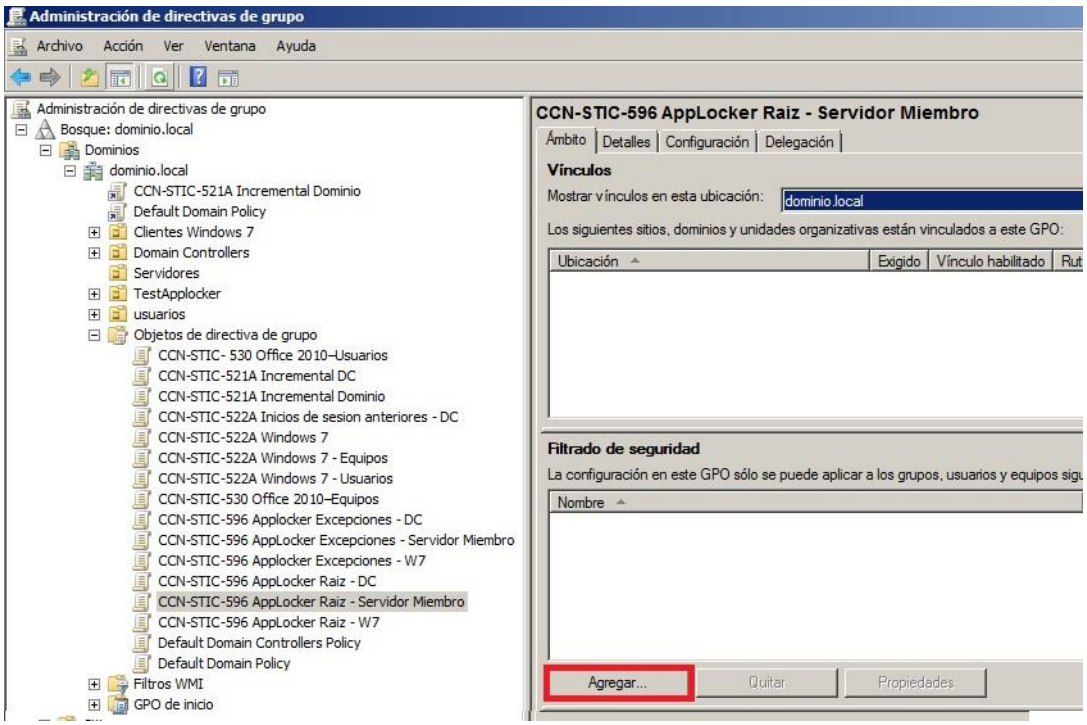
En los siguientes pasos se describe cómo vincular dichas políticas a la unidad organizativa donde resida el servidor o servidores a securizar y cómo usar el filtrado de seguridad para que sólo apliquen al servidor o servidores requeridos.

En este ejemplo, se securiza un único servidor llamado “SVR1” que reside en la unidad organizativa “Servidores”.

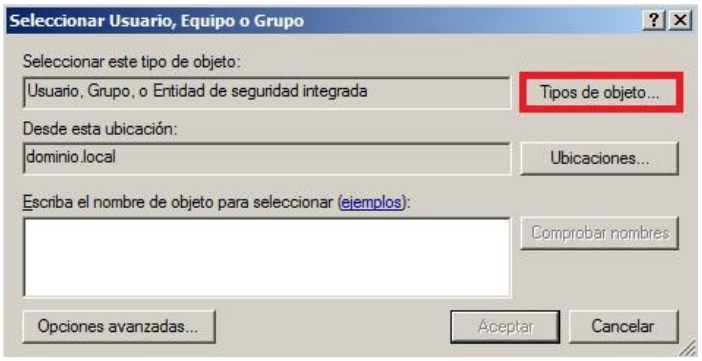
Paso	Descripción
38.	**Nota:** Si en su caso no precisa definir filtrado de seguridad (porque puede aplicar la política a todos los servidores de la Unidad Organizativa seleccionada) continúe directamente en el paso 46. Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el objeto **"Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ CCN-STIC-869 ENS Applocker Raiz Servidor Miembro – medio alto"** y elimine el grupo "Usuarios autentificados" del submenú "Filtrado de seguridad" situado en el panel derecho. 
39.	Pulse "Aceptar" en la ventana de confirmación. 

Paso	Descripción

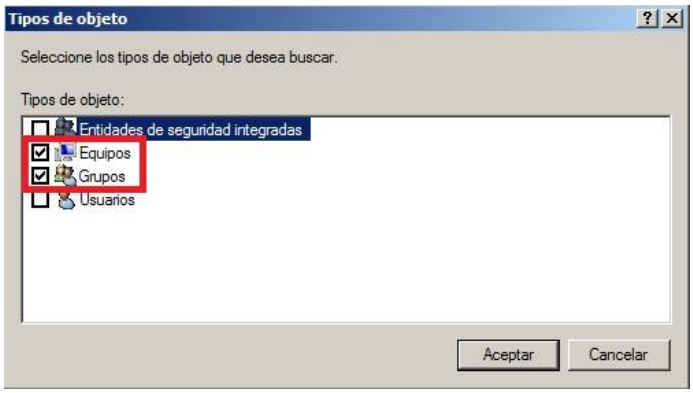
40. Agregue el servidor o grupo de servidores a los que se les vayan a aplicar las reglas de AppLocker. Para ello pulse “Agregar…” en el submenú de “Filtrado de Seguridad”.



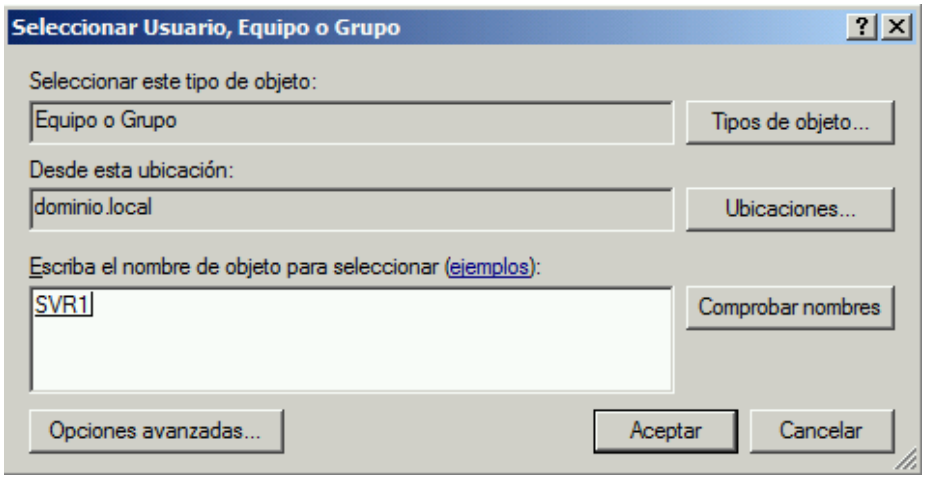
41. En la siguiente ventana, pulse “Tipos de objeto…”.



42. Seleccione “Equipos” y “Grupos” para posteriormente poder buscar por la cuenta de equipo o grupos de equipos. Pulse “Aceptar”.

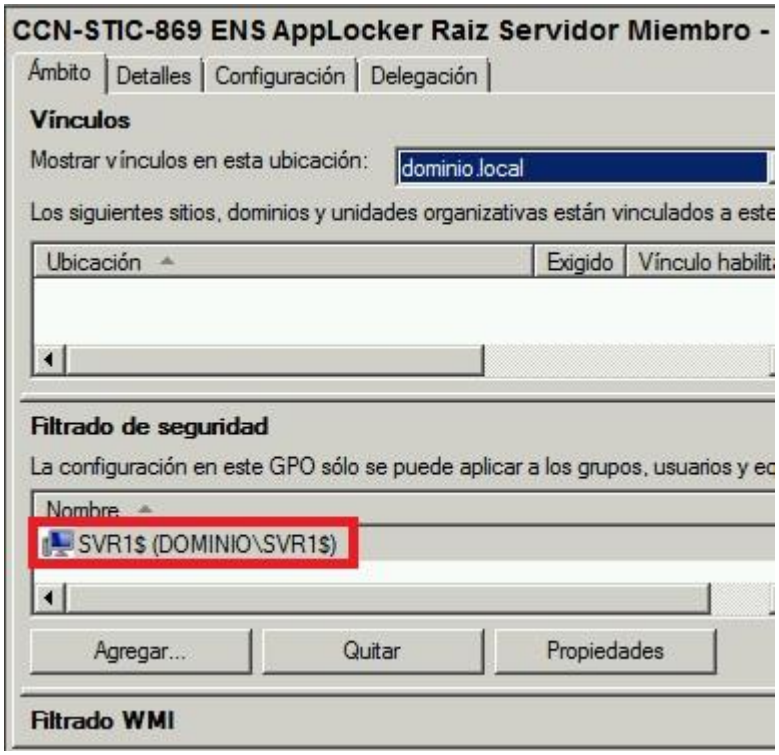


Paso	Descripción
43.	De nuevo en la ventana de “Seleccionar Usuario”, escriba el equipo, equipos, o grupos de equipos (separados por comas) a los que desee aplicar la política y pulse “Aceptar”.

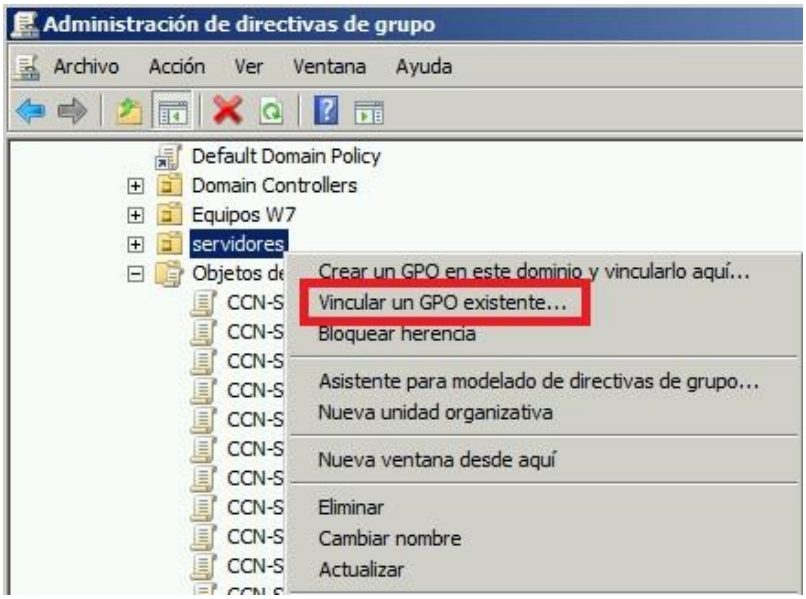
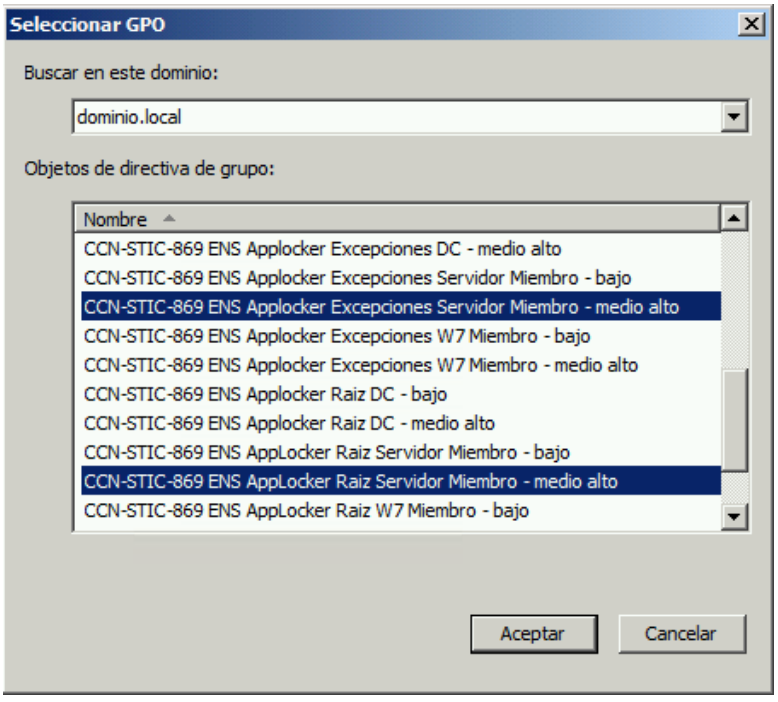


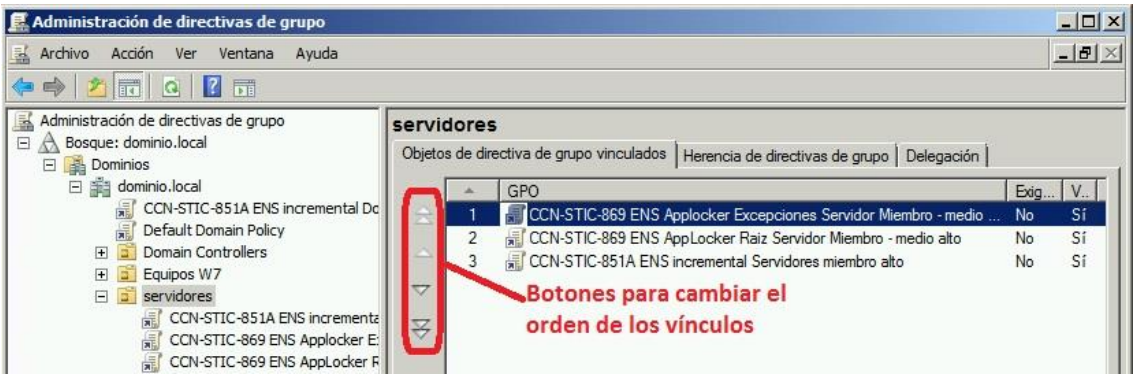
Nota: En este ejemplo únicamente se va a aplicar la política a un servidor: “SVR1”.

44.	Compruebe que el listado de servidores y/o grupos se ha actualizado en el submenú “Filtrado de Seguridad” de la consola de “Administración de directivas de grupo”.



45.	Repita los pasos del 38 al 44 para la directiva “**CCN-STIC-869 ENS Applocker Excepciones Servidor Miembro – bajo”**.
46.	Proceda a la vinculación de los dos GPO a la unidad organizativa que contenga al servidor tal y como se le indica en los siguientes pasos. En este ejemplo la OU se llama: “Servidores”.

Paso	Descripción
47.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ <OU que contenga al servidor miembro>**". Pulse botón derecho sobre la OU que contenga al servidor miembro y elija la opción "Vincular un GPO existente…" del menú contextual. En este ejemplo el nombre de la OU es "Servidores". 
48.	En el nuevo cuadro de diálogo desplegado, seleccione los GPO (haciendo uso de la tecla "CTRL"): "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto" y "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto" pulse "Aceptar". 

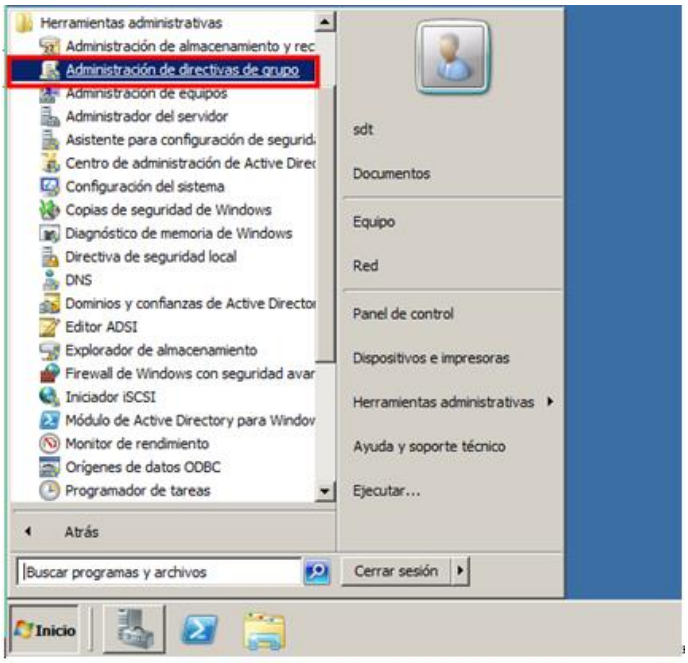
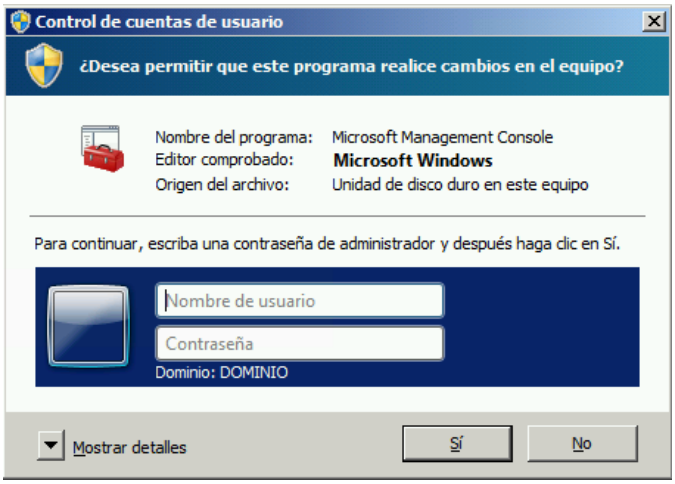
Paso	Descripción
49.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Servidores**", y observe el orden de los vínculos en la parte central de la ventana.  El orden de los vínculos ha de ser el siguiente: 1) CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto 2) CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto 3) Resto de GPOs Si el orden mostrado fuera otro, seleccione los GPOs por turnos y utilice los botones indicados en la figura para cambiar el orden de los vínculos de forma que coincida con el indicado aquí.
50.	Ya puede cerrar la consola de “Administración de directivas de grupo”.
51.	Borre la carpeta “C:\Scripts” del controlador de dominio.

3. CONFIGURACIÓN DE APPLOCKER EN CLIENTE WINDOWS 7 MIEMBRO DE DOMINIO

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

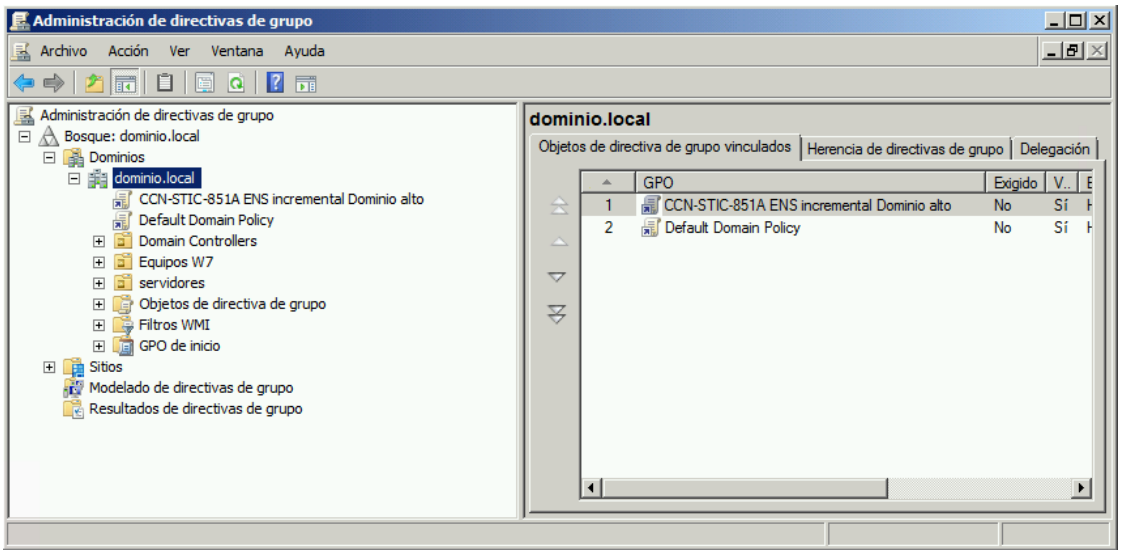
Nota: Esta guía asume que a los servidores controladores del dominio a los que va a pertenecer el equipo cliente, se les ha aplicado la configuración descrita en la guía CCN-STIC-851A para nivel medio o alto según Esquema nacional de Seguridad. También se asume que los clientes y controladores de dominio tienen aplicadas las configuraciones descritas en la guía CCN-STIC-850A.

Paso	Descripción
1.	Inicie sesión en el servidor controlador de dominio con una cuenta con derechos de administración en el dominio.
2.	Cree el directorio “Scripts” en la unidad “C:\”.
3.	Copie los ficheros y directorios que acompañan a esta guía, al directorio "C:\scripts" del controlador de dominio.
4.	Asegúrese de que al menos los siguientes directorios hayan sido copiados al directorio “C:\Scripts” del controlador de dominio: – CCN-STIC-869 AppLocker Raiz W7 miembro – medio alto – CCN-STIC-869 AppLocker Excepciones W7 miembro – medio alto

Paso	Descripción
5.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo.** 
6.	El control de cuentas de usuario le solicitará usuario y contraseña con permisos de administración. Introduzca credenciales con privilegios de administrador del dominio y pulse “Sí”. 

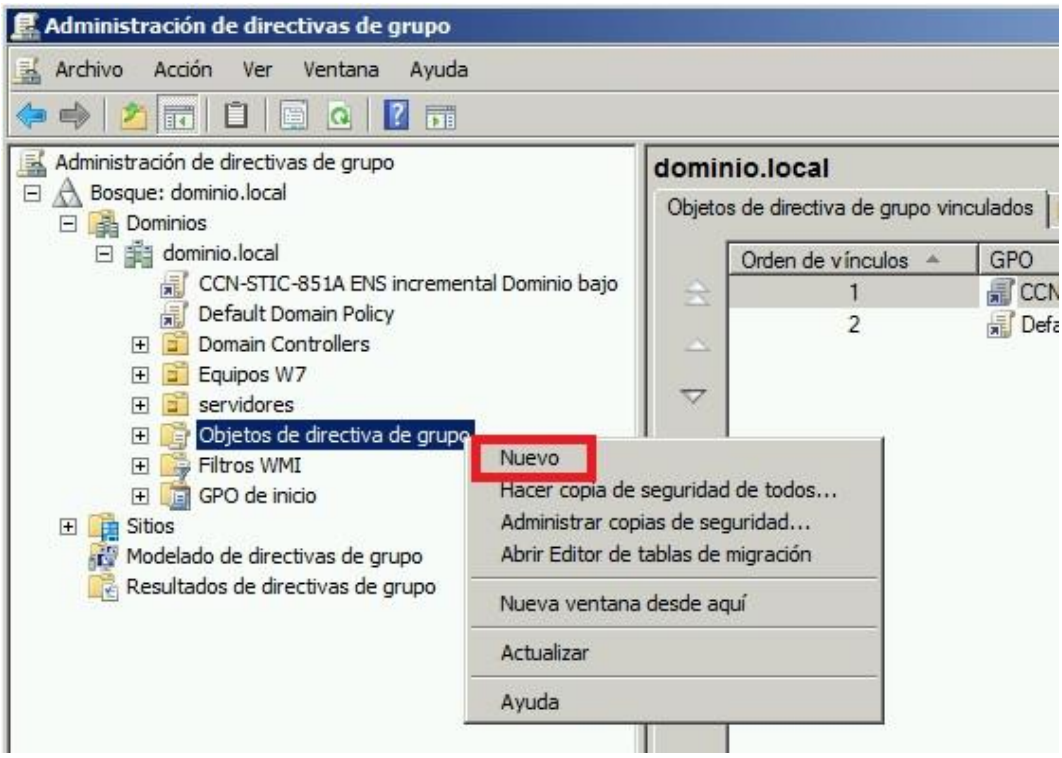
Paso	Descripción

7. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio>,** como se muestra en la siguiente imagen.

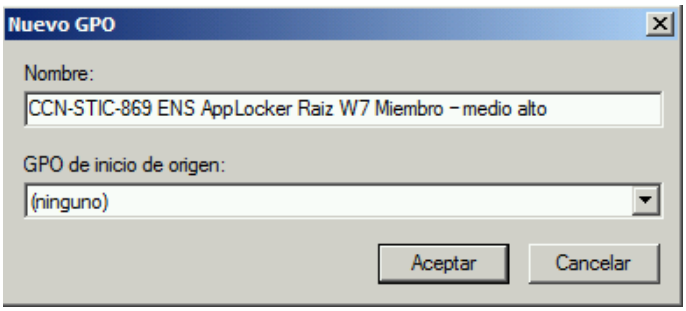


A continuación se procederá a la creación de los GPOs necesarios.

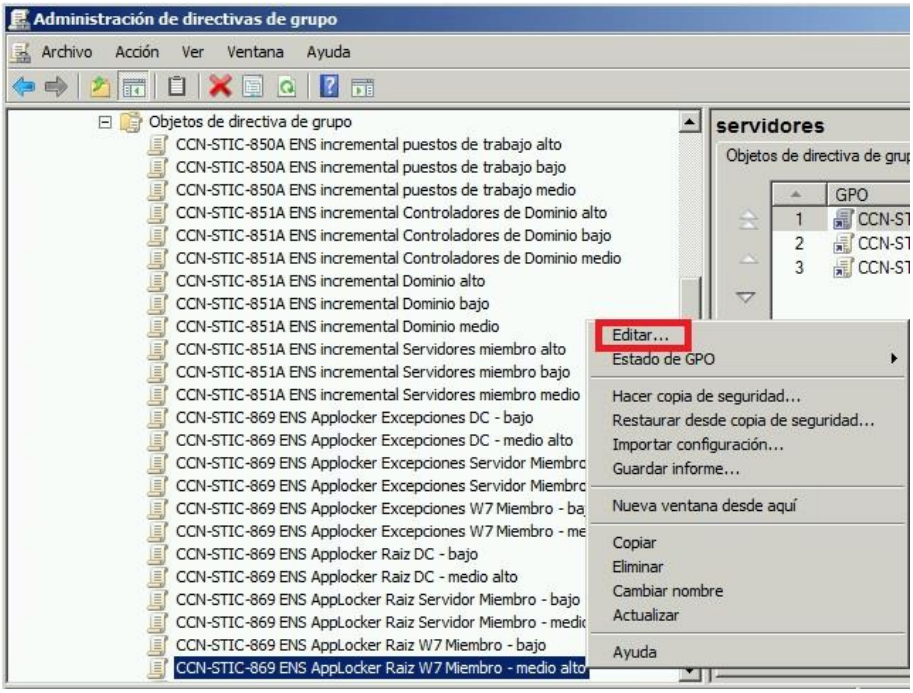
8. Expanda y seleccione el contenedor "**Objetos de directiva de grupo**" y marcando con el botón derecho sobre dicho elemento, elija la opción "Nuevo" del menú contextual que aparecerá.



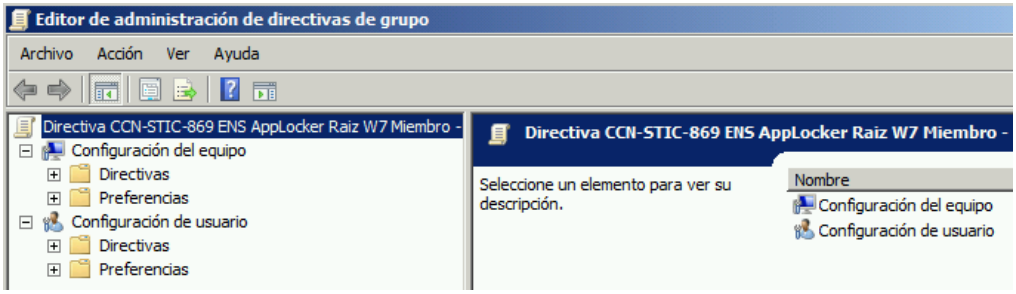
Paso	Descripción
9.	Asigne el siguiente nombre al nuevo GPO: “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto”. Pulse “Aceptar” para cerrar la ventana.



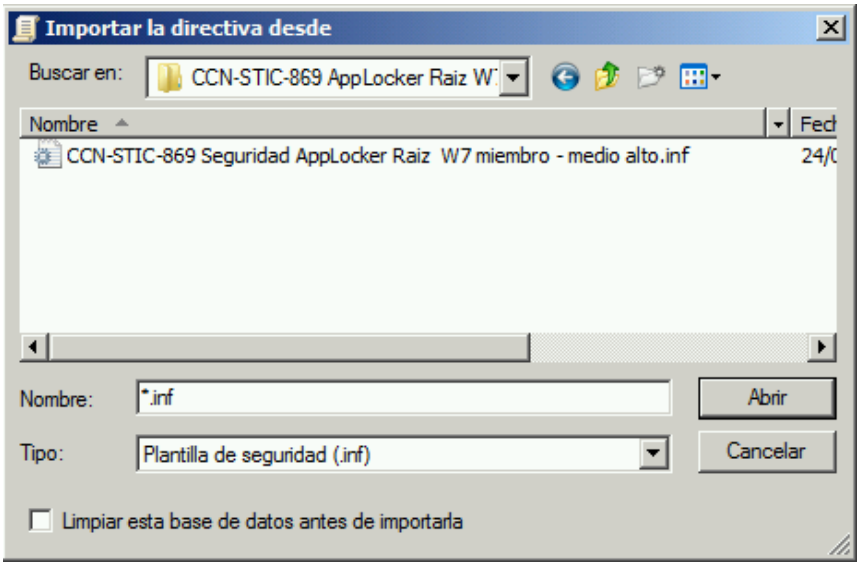
10.	Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto**", y marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.

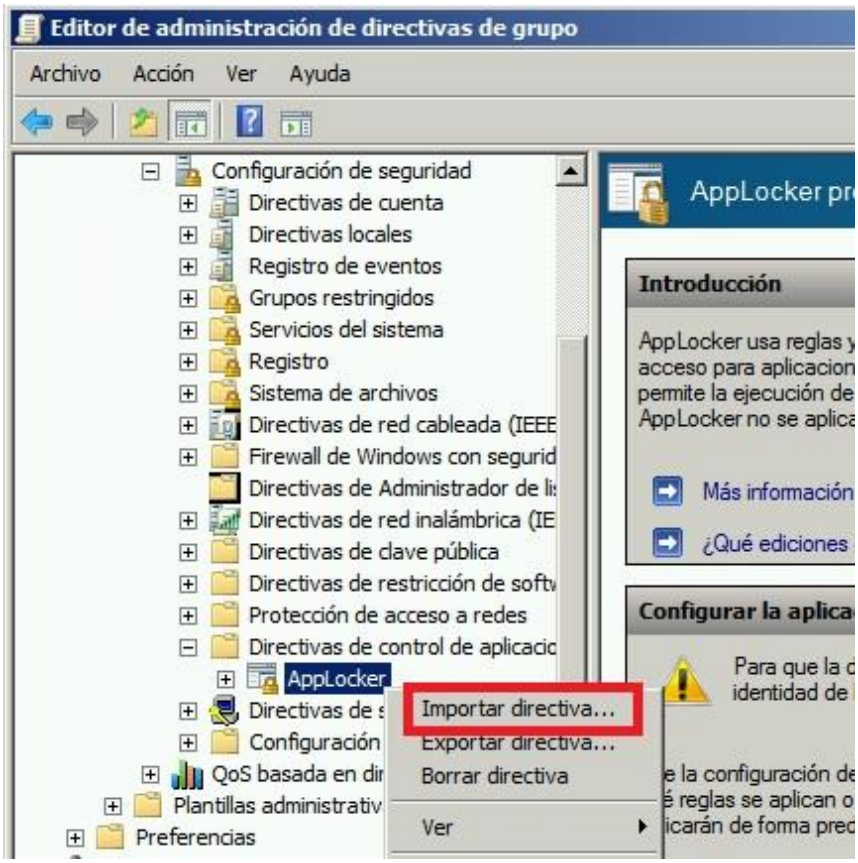
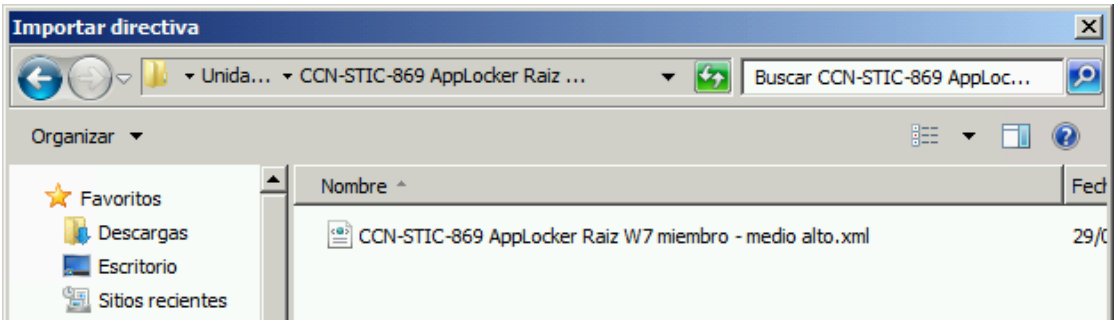


11.	Con ello se lanzará el “Editor de administración de directivas de grupo”.

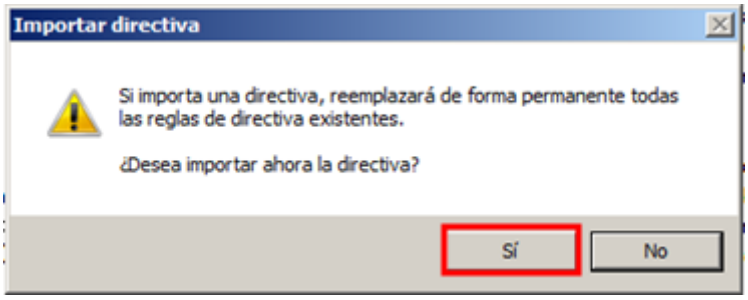


En los siguientes pasos utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando primero la configuración de la plantilla de seguridad que acompaña a esta guía, e importando posteriormente la configuración de reglas de AppLocker que aplicarán a los clientes Windows 7.

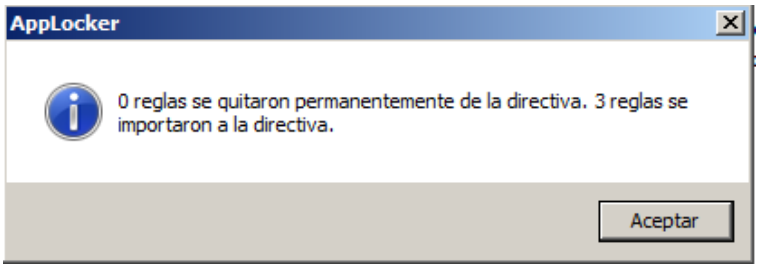
Paso	Descripción
12.	En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción “Importar directiva…” **Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad.** 
13.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz W7 – medio alto” y seleccione el fichero “**CCN-STIC-869 Seguridad AppLocker Raiz W7 Miembro – medio alto.inf**” haciendo doble clic sobre él o pulsando sobre el botón “Abrir”.  Con esto, habrá quedado importada la plantilla de seguridad en este GPO. **Nota:** No cierre todavía el “Editor de administración de directivas de grupo”, y continúe con el siguiente paso.

Paso	Descripción
14.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-ENS 869 AppLocker Raiz W7 Miembro – medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
15.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Raiz W7 – medio alto” y seleccione el fichero “**CCN-STIC-869 AppLocker Raiz W7 – medio alto.xml**” y haga doble clic sobre él o pulse “Abrir”. 

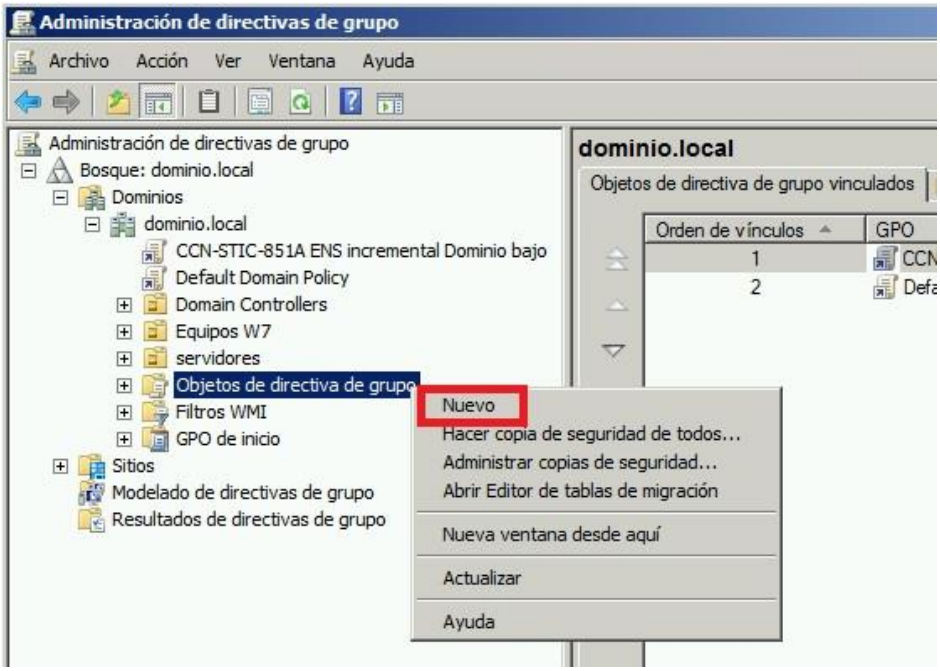
Paso	Descripción
16.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Si”.



17.	Aparecerá un nuevo mensaje informativo indicando que se importaron tres reglas a la directiva de AppLocker.

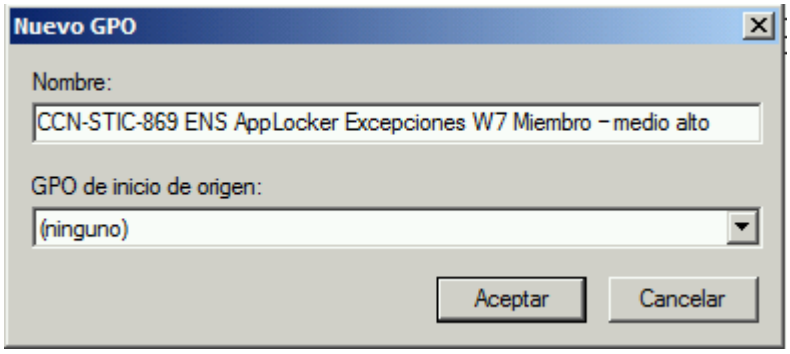


18.	El GPO "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto" está creado y configurado. Cierre la ventana del “Editor de administración de directivas de grupo”.
19.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Objetos de directiva de grupo”**, y marcando con el botón derecho sobre dicho elemento, elija la opción “Nuevo” del menú contextual que aparecerá.

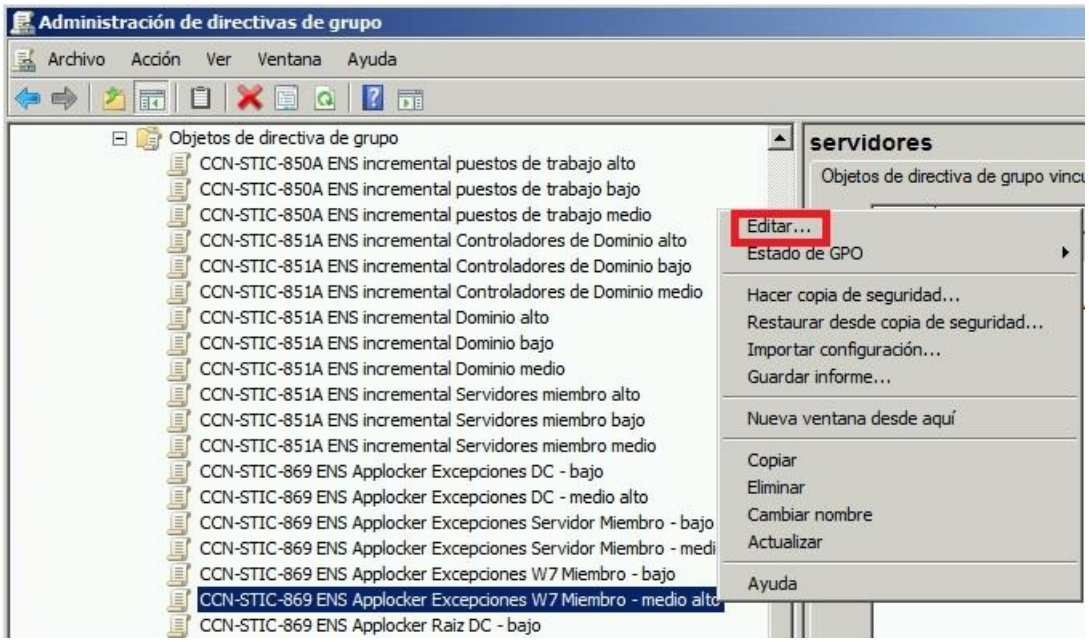


Paso	Descripción

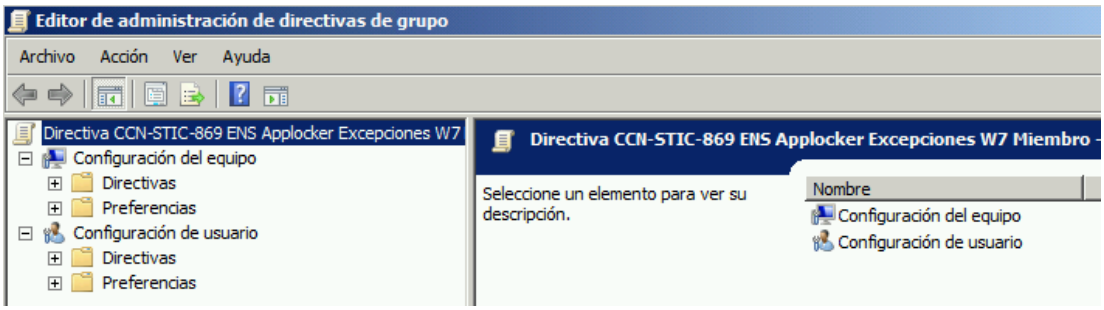
20. Asigne el siguiente nombre al GPO: “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto”. Pulse “Aceptar” para cerrar la ventana.



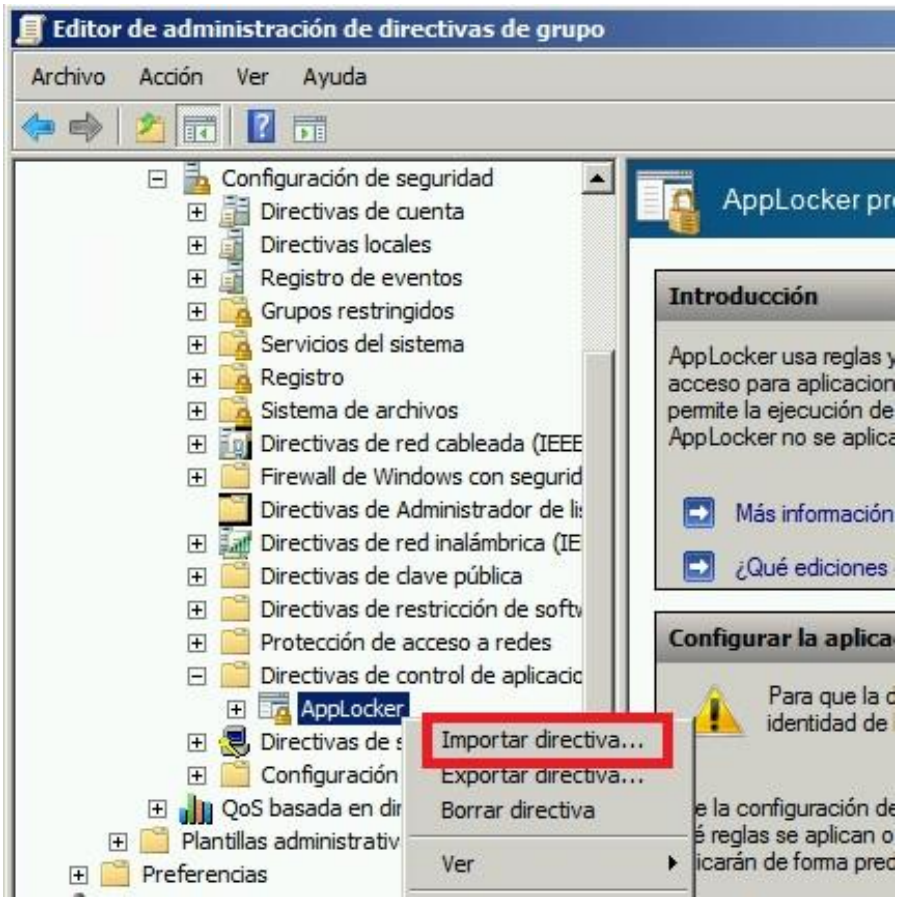
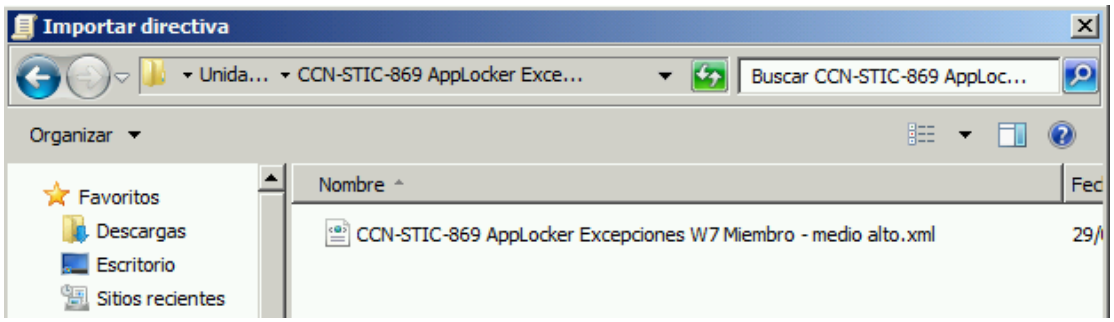
21. Seleccione el GPO recién creado, "**Objetos de directiva de grupo \ CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto**" y, marcando con el botón derecho en él, elija la opción "Editar…" del menú contextual que aparecerá.

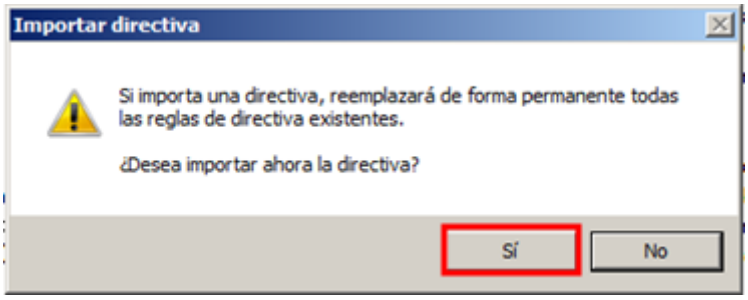
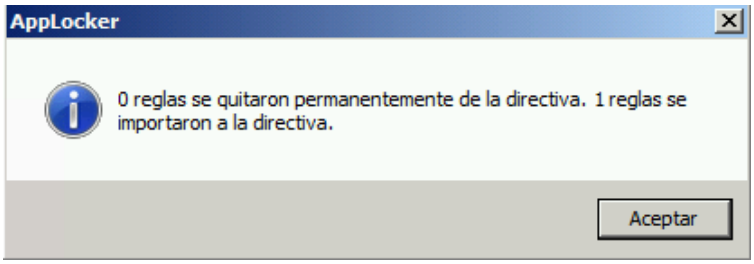


22. Con ello se lanzará el “Editor de administración de directivas de grupo”.



En los siguientes pasos, utilizará esta ventana del “Editor de administración de directivas de grupo” para modificar la configuración del GPO, importando la configuración de las reglas de AppLocker.

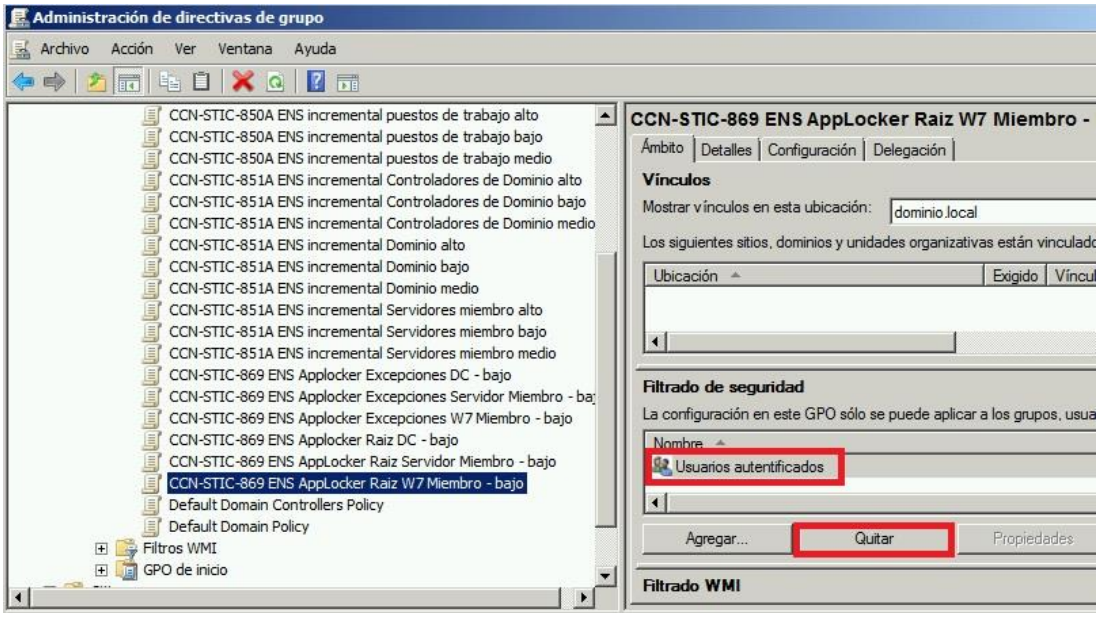
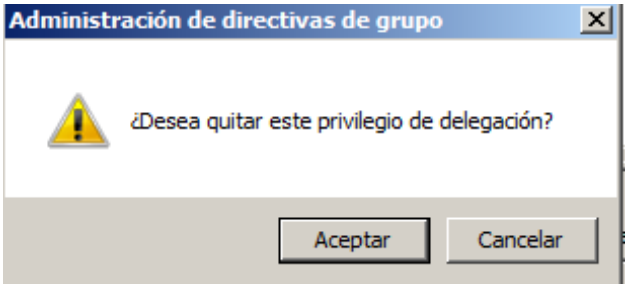
Paso	Descripción
23.	En el mismo “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
24.	En el cuadro de dialogo abierto navegue hasta el directorio “C:\Scripts\CCN-STIC-869 AppLocker Excepciones W7 Miembro –medio alto”, seleccione el fichero “**CCN-STIC-869 AppLocker Excepciones W7 Miembro – medio alto.xml**” y haga doble clic sobre él o pulse “Abrir”. 

Paso	Descripción
25.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”. 
26.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje. 
27.	El GPO recién importado contiene una única regla para permitir la ejecución de binarios desde unidades de CD o DVD. Antes de proceder a la vinculación de los GPO a las unidades organizativas donde se encuentren los clientes Windows 7, puede proceder a la edición del GPO para añadir más reglas que se ajusten al software que tengan instalado sus clientes. El GPO “CCN-STIC-869 ENS Applocker Excepciones W7 Miembro –medio alto” está diseñado para recibir las nuevas reglas que se ajusten a su organización. Edite dicho GPO. **Nota: para** más información sobre los pasos a seguir en la creación, edición y eliminación de reglas de AppLocker consulte el anexo H. Tenga en consideración que, en este caso, no será necesario realizar el procedimiento desde una máquina de referencia ya que el GPO no se encuentra vinculado a ninguna unidad organizativa.
28.	Cuando termine de adaptar la política a sus necesidades cierre la ventana del “Editor de administración de directivas de grupo”.

Una vez creadas todas las reglas necesarias para la ejecución del software en los clientes Windows 7, se puede proceder a la vinculación de las directivas a la unidad organizativa a la que pertenezcan los clientes a securizar. Si dicha unidad contiene clientes que no han de recibir las reglas de AppLocker será necesario filtrar la aplicación de las dos directivas haciendo uso del filtrado de seguridad, de tal manera que la política sólo aplicará al equipo o conjunto de equipos deseados.

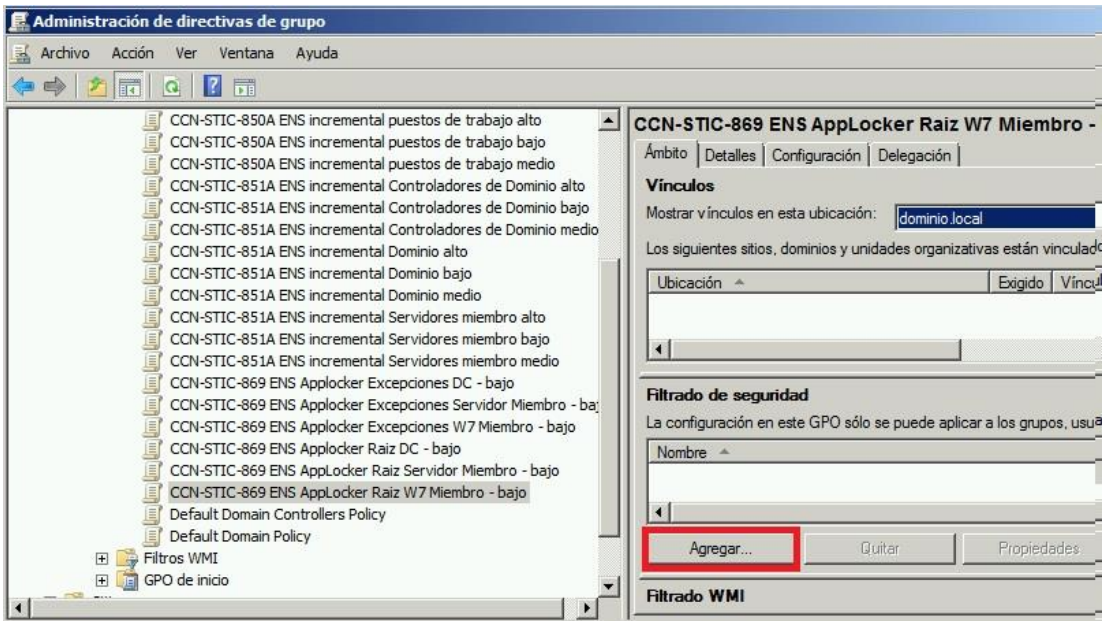
En los siguientes pasos se describe cómo vincular dichas políticas a la unidad organizativa donde residan los clientes Windows 7 y cómo usar el filtrado de seguridad para que sólo apliquen a los clientes requeridos.

En este ejemplo, se securizará un cliente llamado “CLN1” que reside en la unidad organizativa “Equipos W7”

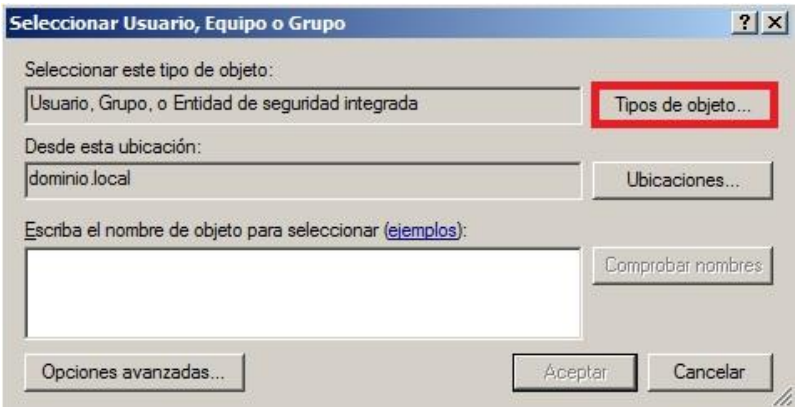
Paso	Descripción
29.	**Nota:** Si en su caso no precisa definir filtrado de seguridad (porque puede aplicar la política a todos los equipos de la Unidad Organizativa seleccionada) continúe directamente en el paso 37 Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el objeto **"Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ CCN-STIC-869 ENS Applocker Raiz W7 Miembro – medio alto"** y elimine el grupo "Usuarios autentificados" del submenú "Filtrado de seguridad" situado en el panel derecho. 
30.	Pulse "Aceptar" en la ventana de confirmación. 

Paso	Descripción

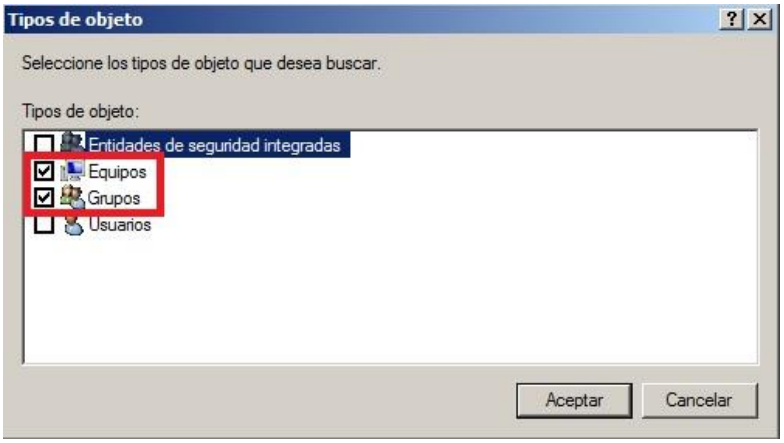
31. Agregue el equipo o grupo de equipos a los que se les vayan a aplicar las reglas de AppLocker. Para ello, pulse “Agregar…” en el submenú de “Filtrado de Seguridad”.



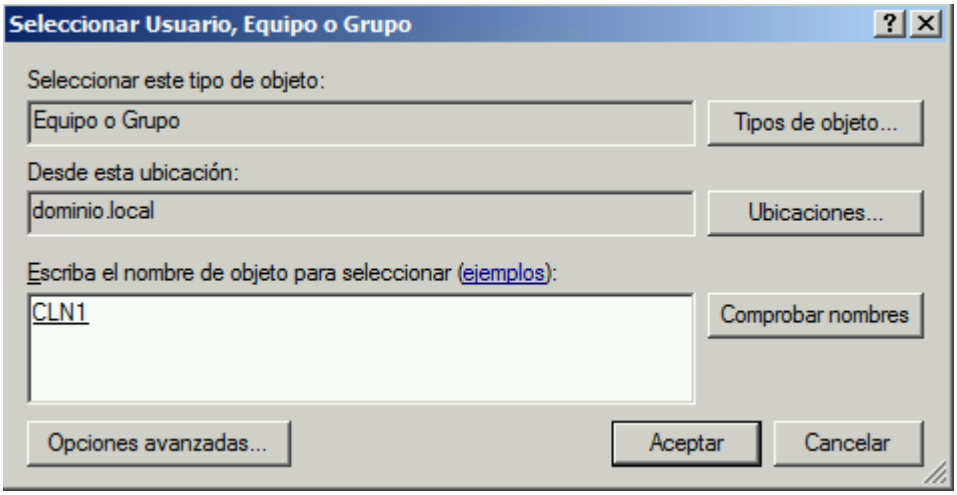
32. En la siguiente ventana, pulse “Tipos de objeto…”.



33. Seleccione “Equipos” y “Grupos” para posteriormente poder buscar por la cuenta de equipo o grupos de equipos. Pulse “Aceptar”.

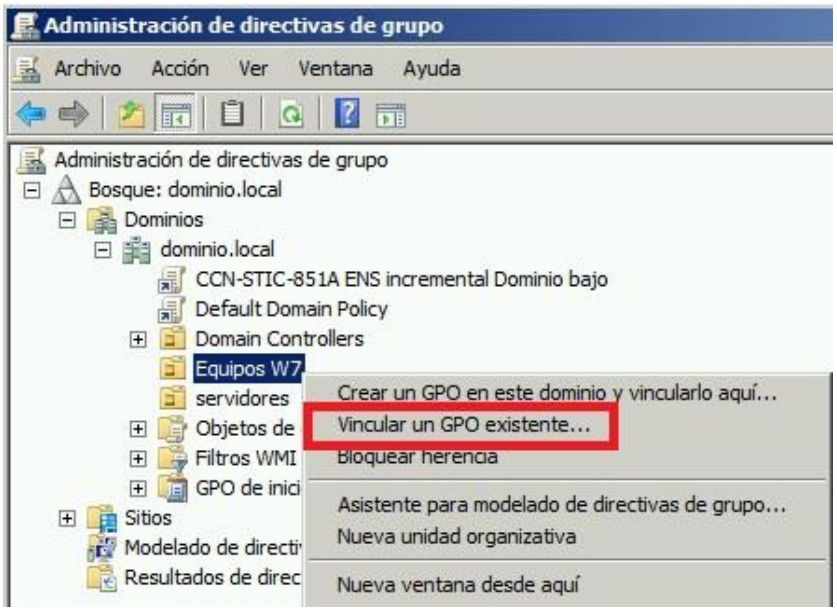
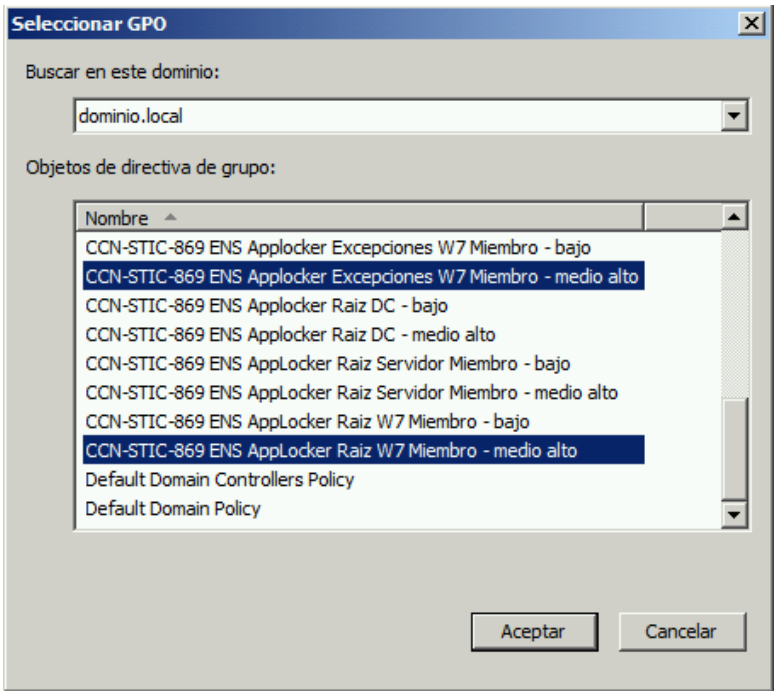


Paso	Descripción
34.	De nuevo en la ventana de “Seleccionar Usuario”, escriba el equipo, equipos, o grupos de equipos (separados por comas) a los que desee aplicar la política y pulse “Aceptar”. En este ejemplo únicamente se va a aplicar la política a un servidor: “CLN1”.

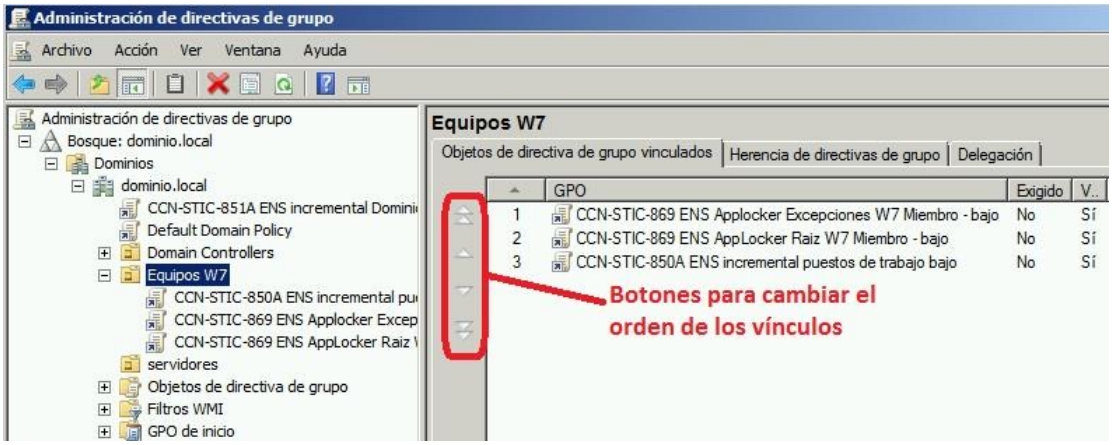


35.	Compruebe que el listado de servidores y/o grupos se ha actualizado en el submenú “Filtrado de Seguridad” de la consola de “Administración de directivas de grupo”.

36.	Repita los pasos del 29 al 35 para la directiva “**CCN-STIC-869 ENS Applocker Excepciones W7 Miembro – medio alto”**.
37.	Proceda a la vinculación de los dos GPO a la unidad organizativa que contenga al equipo cliente tal y como se le indica en los siguientes pasos. En este ejemplo la OU se llama: “Equipos W7”.

Paso	Descripción
38.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ <OU que contenga al cliente miembro>**". Pulse botón derecho sobre la OU que contenga al equipo miembro y elija la opción "Vincular un GPO existente…" del menú contextual. En este ejemplo el nombre de la OU es "Equipos W7". 
39.	En el nuevo cuadro de diálogo desplegado, seleccione los GPO (haciendo uso de la tecla "CTRL"): "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto" y "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto" pulse "Aceptar". 

Paso	Descripción
40.	Utilizando de nuevo la herramienta "Administración de directivas de grupo" (Inicio→ Herramientas administrativas → Administración de directivas de grupo), expanda y seleccione el contenedor "**Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su domino> \ Equipos W7**" y observe el orden de los vínculos en la parte central de la ventana.



El orden de los vínculos ha de ser el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto
2) CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto
3) Resto de GPOs

Si el orden mostrado fuera otro, seleccione los GPOs por turnos y utilice los botones indicados en la figura para cambiar el orden de los vínculos de forma que coincida con el indicado aquí.

41.	Ya puede cerrar la consola de “Administración de directivas de grupo”.
42.	Borre la carpeta “C:\Scripts” del controlador de dominio.

ANEXO F. GUÍA PASO A PASO PARA LA CONFIGURACIÓN DE APPLOCKER EN CLIENTES O SERVIDORES INDEPENDIENTES QUE LES SEA DE APLICACIÓN EL NIVEL BAJO DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar la implantación del servicio AppLocker en clientes independientes (tanto Windows 7 Enterprise o Ultimate como Windows Server 2008R2 o 2012R2) con una categorización de seguridad baja según los criterios del Esquema Nacional de Seguridad.

Las capturas de pantalla incluidas en los en pasos descritos en el presente anexo han sido tomadas de un sistema Windows 7 Enterprise independiente, al que previamente se le ha aplicado la guía CCN-STIC-850B. Los pasos son extensibles a servidores Windows Server 2008R2 y Windows Server 2012R2 con las guías CCN-STIC-851B y CCN-STIC-870B aplicadas a los respectivos sistemas operativos.

Para la implantación en nivel bajo según criterios del Esquema Nacional de Seguridad, las reglas de AppLocker se implementarán en modo auditoría, de tal manera que no se restringirá la ejecución de ningún binario pero se guardarán eventos de auditoría con información sobre el procesado de las reglas para cada ejecución de software. De esta manera se aprovecha AppLocker como elemento de auditoría de ejecución de software.

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.

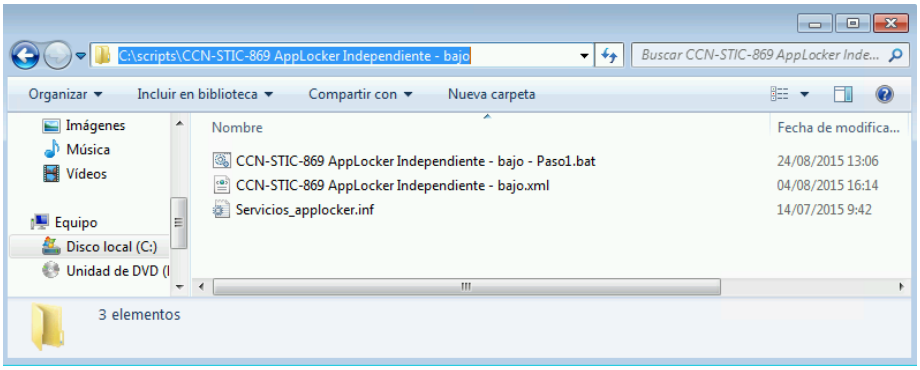
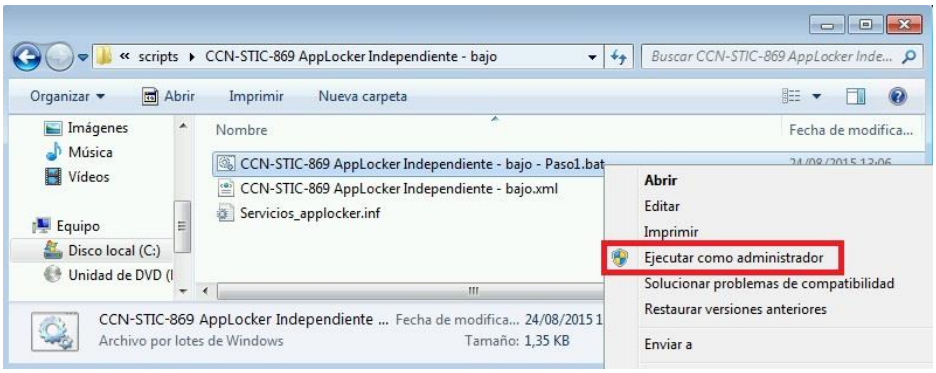
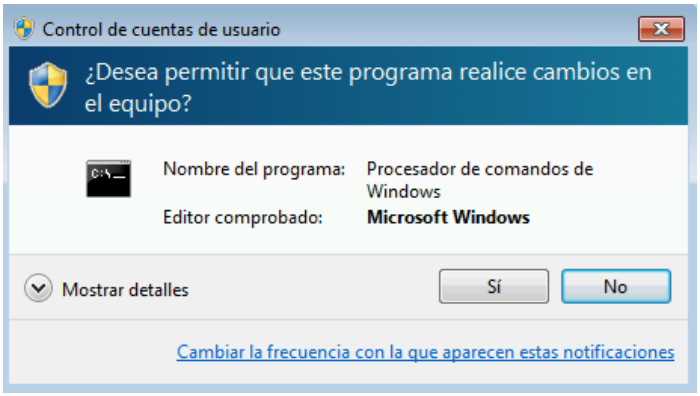
Debe tener en consideración que, antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

1. CONFIGURACIÓN DE APPLOCKER EN CLIENTE INDEPENDIENTE

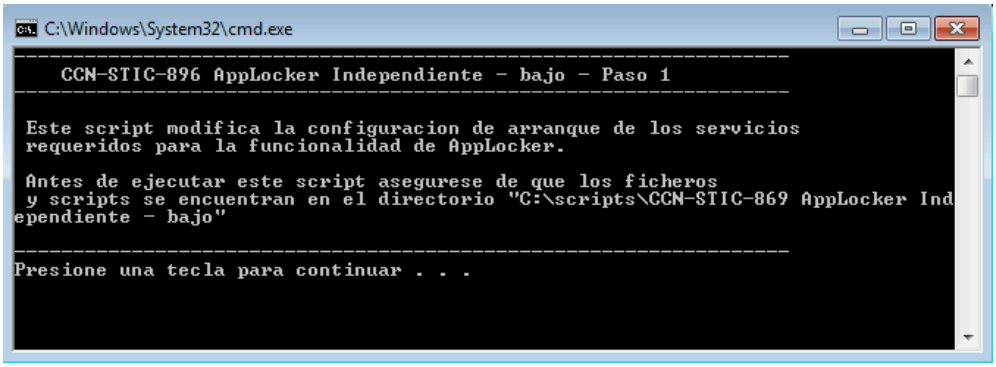
Los pasos que se describen a continuación se han diseñado para ayudar a los operadores a implementar la configuración de AppLocker en un puesto de trabajo Windows 7 que implemente servicios o información de nivel bajo y que se encuentre supeditado al cumplimiento del Esquema Nacional de Seguridad. Esto significa que previamente al cliente se le debe haber aplicado la guía CCN-STIC-850B en nivel bajo.

La aplicación de los pasos es extensible a servidores Windows Server 2008R2 y Windows Server 2012R2 con las guías CCN-STIC-851B y CCN-STIC-870B aplicadas en nivel bajo en los respectivos sistemas operativos.

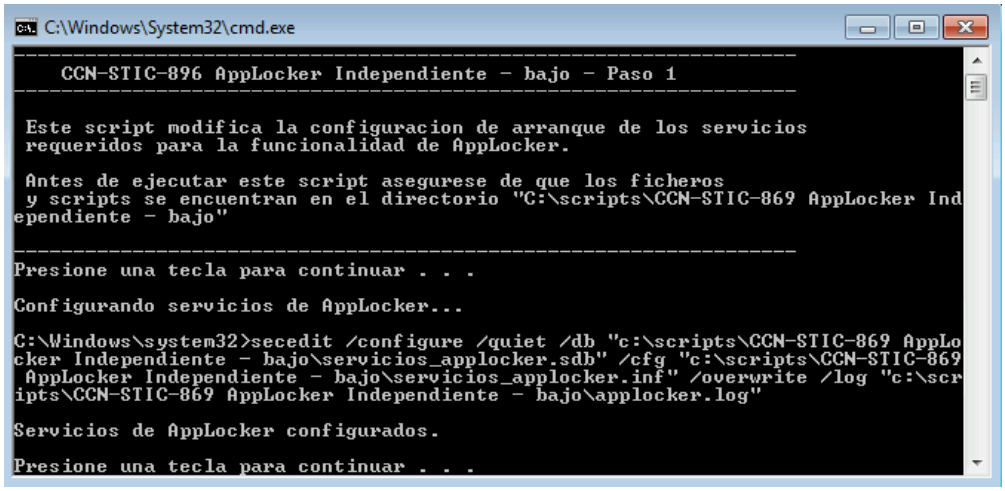
Nota: Tenga en consideración que la siguiente configuración es de tipo genérica. Es posible que sean necesarias configuraciones adicionales para agregar excepciones de permisividad de aplicaciones. Revise el punto 2 del presente anexo para conocer cómo efectuar excepciones adicionales.

Paso	Descripción
1.	Inicie sesión en el puesto de trabajo que va a configurar con un usuario con privilegios de administración local.
2.	Cree en la unidad c:\ la carpeta “scripts”.
3.	Copie la carpeta “CCN-STIC-869 AppLocker Independiente – bajo” que acompaña esta guía al directorio “C:\Scripts”.
4.	Abra la carpeta “C:\Scripts\CCN-STIC-869 AppLocker Independiente – bajo” que encontrará en la carpeta “C:\Scripts” que ha copiado. 
5.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-869 AppLocker Independiente – bajo – Paso1.bat” y seleccione la opción “Ejecutar como administrador”. 
6.	Acepte la elevación de privilegios pulsando “Si” en la ventana del Control de cuentas de usuario.  **Nota:** Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que le solicite credenciales de usuario con permisos de administración local.

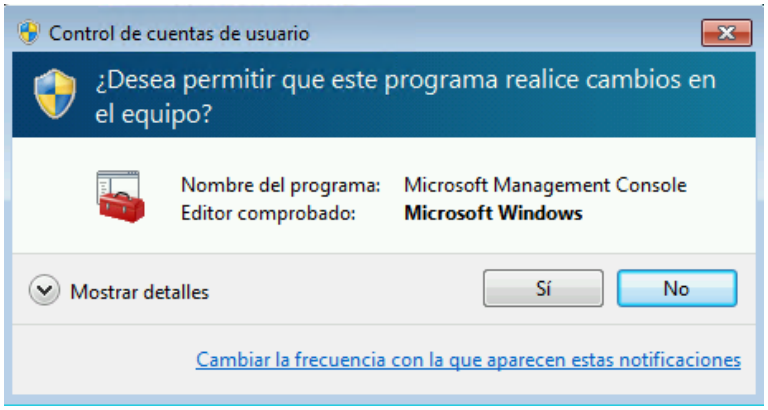
Paso	Descripción
7.	Pulse cualquier tecla para iniciar la ejecución del script que configurará el servicio de identidad de aplicación para que inicie de manera automática.



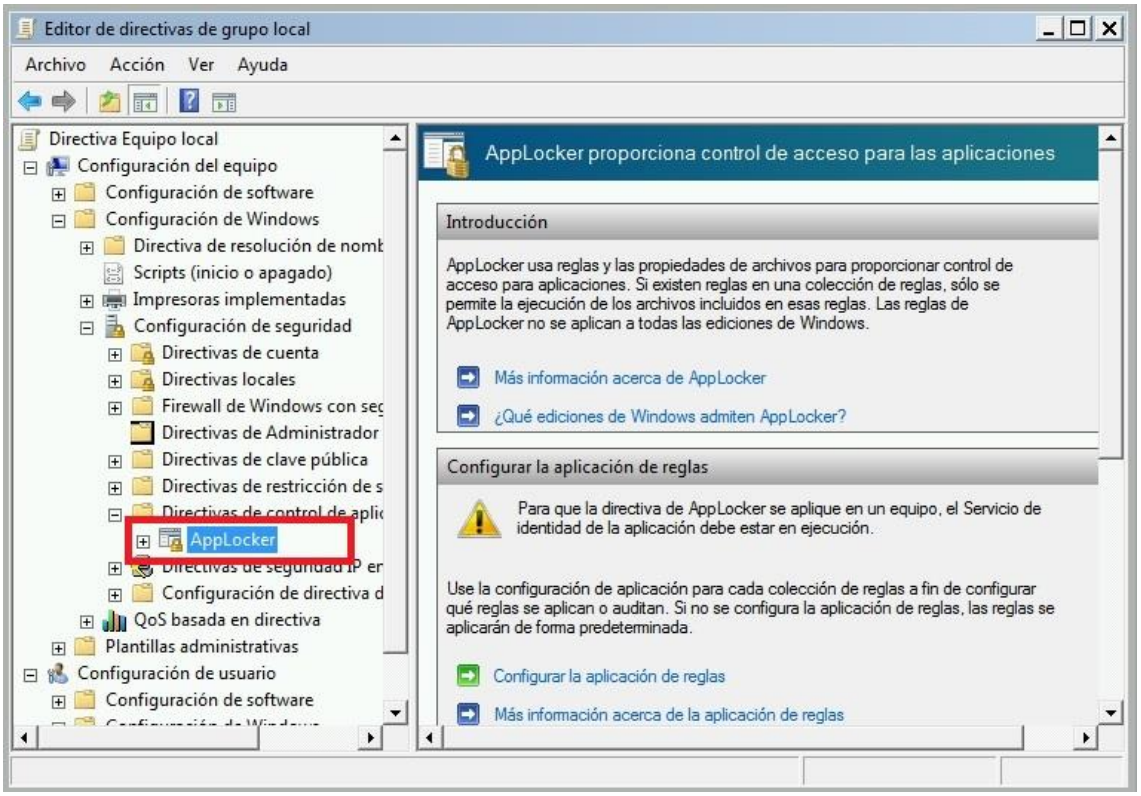
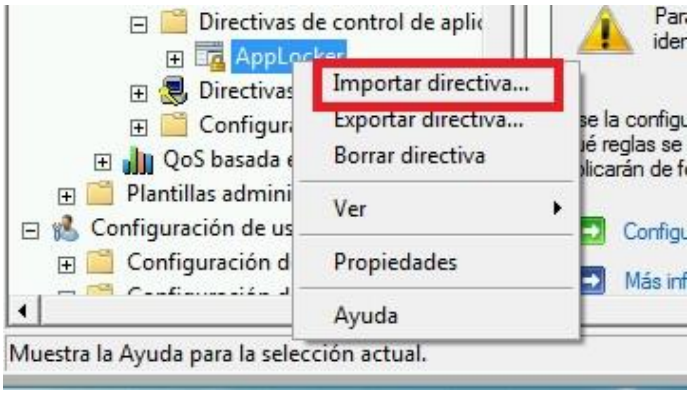
8.	Una vez completado el proceso, deberá pulsar una tecla para continuar.

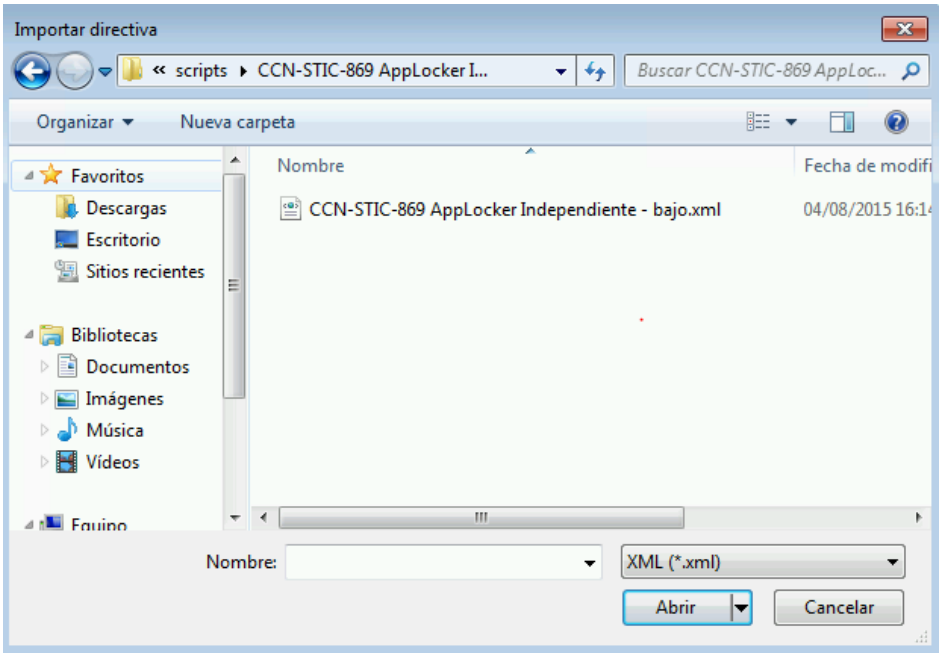
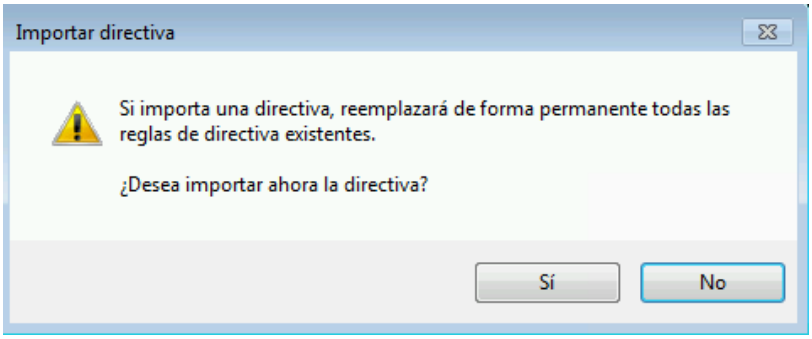
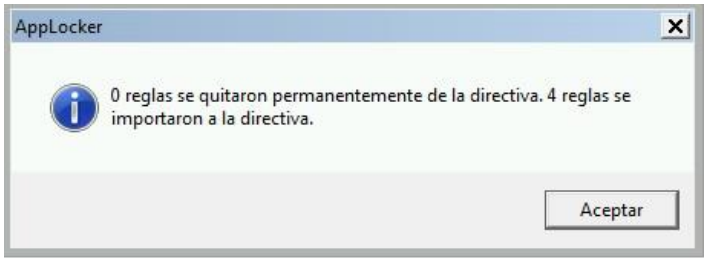


9.	La ejecución del script de configuración se habrá completado, pulse una tecla para finalizar.
10.	Pulse la combinación de teclas “Windows + R” para acceder al menú “Ejecutar”.
11.	En el menú “Ejecutar” escriba “GPedit.msc” y pulse la tecla “Enter”.
12.	Acepte el mensaje de advertencia del Control de cuentas de usuario.



Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que le solicite credenciales de usuario con permisos de administración local.

Paso	Descripción
13.	En la consola del editor de directivas de grupo local, vaya a la siguiente ruta: **Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de control de aplicaciones -> AppLocker** 
14.	Sobre “AppLocker” pulse con el botón derecho del ratón y seleccione la opción “Importar directiva…”. 

Paso	Descripción
15.	En la ventana de importación de directiva seleccione el fichero “CCN-STIC-869 AppLocker – Independiente - bajo.xml” existente en la carpeta “C:\Scripts\CCN-STIC-869 AppLocker Independiente - bajo”. Haga doble clic sobre el fichero o pulse sobre el botón “Abrir” 
16.	Pulse “Si” en la advertencia informativa. 
17.	Pulse el botón “Aceptar” en la notificación de AppLocker. 
18.	Si desea realizar alguna modificación o ampliación de reglas, sería conveniente realizarlo ahora. Para efectuarlo siga los pasos establecidos en el punto 2 del presente anexo.
19.	Puede cerrar la ventana del “Editor de directivas de grupo local”.
20.	Puede comprobar la correcta implantación de las diferentes configuraciones de seguridad aplicadas siguiendo los pasos descritos en el anexo K.
21.	Elimine la carpeta “C:\Scripts”.

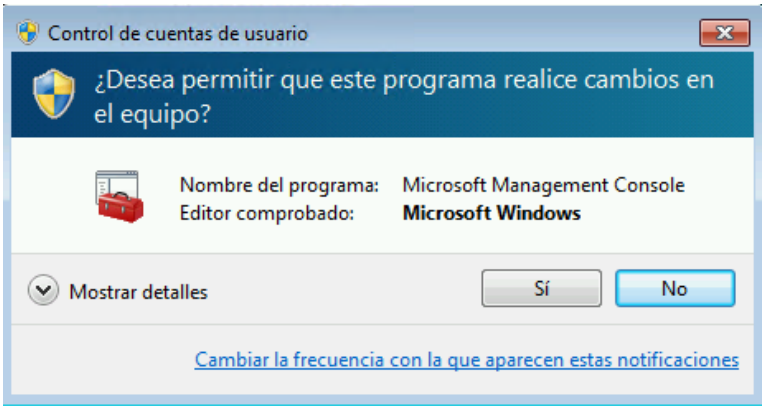
2. CREACIÓN DE EXCEPCIONES DE APPLOCKER PARA LA EJECUCIÓN DE APLICACIONES DESDE RUTAS NO ESTÁNDARES EN UN CLIENTE INDEPENDIENTE

El siguiente paso a paso describe los procesos para crear excepciones en el cliente Windows 7 independiente (con la guía CCN-STIC-850B aplicada en nivel bajo) de tal forma que se vaya a permitir ejecutar contenido desde rutas no estándares. El siguiente ejemplo simula la permisividad para la ejecución de una aplicación instalada en la carpeta "C:\Aplicacion".

La aplicación de los pasos descritos en este apartado, es extensible a servidores Windows Server 2008R2 y 2012R2 con las guías CCN-STIC-851B o CCN-STIC-870B aplicadas en nivel bajo respectivamente en cada sistema operativo.

Nota: De forma predeterminada, las aplicaciones habitualmente se instalan en el directorio de archivo de programa, pero bien por decisión del administrador del equipo o por la configuración de la propia aplicación, esta se podría realizar en una ubicación diferente. Si es así, use a modo de ejemplo el siguiente paso a paso para crear la excepción o excepciones necesarias.

Paso	Descripción
1.	Inicie sesión en el puesto de trabajo con un usuario con privilegios de administrador local.
2.	Pulse la combinación de teclas "Windows + R" para acceder al menú "Ejecutar".
3.	En el menú "Ejecutar" escriba "GPedit.msc" y pulse la tecla "Enter".
4.	Acepte el mensaje de advertencia del Control de cuentas de usuario.

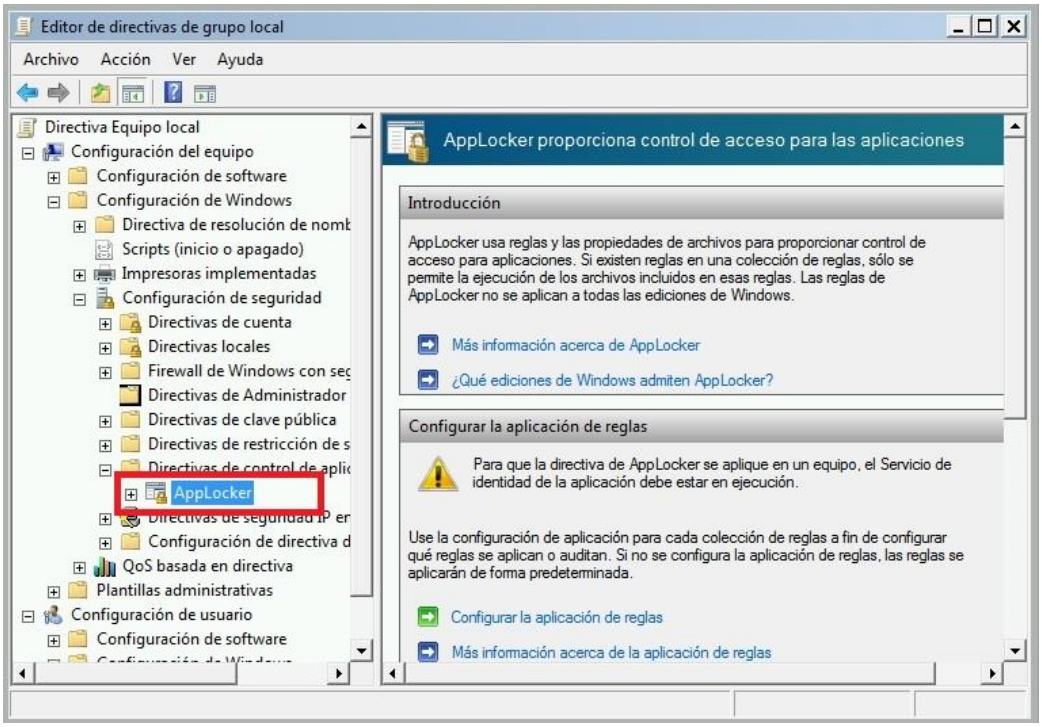


Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

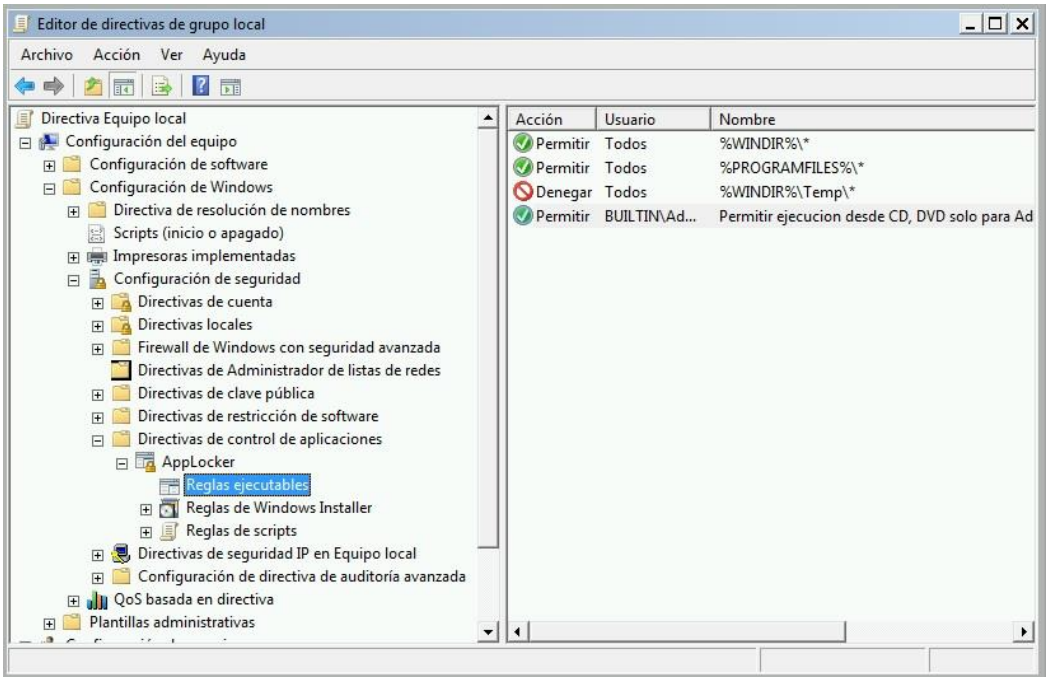
Paso	Descripción

5. En la consola del editor de directivas de grupo local, vaya a la siguiente ruta:

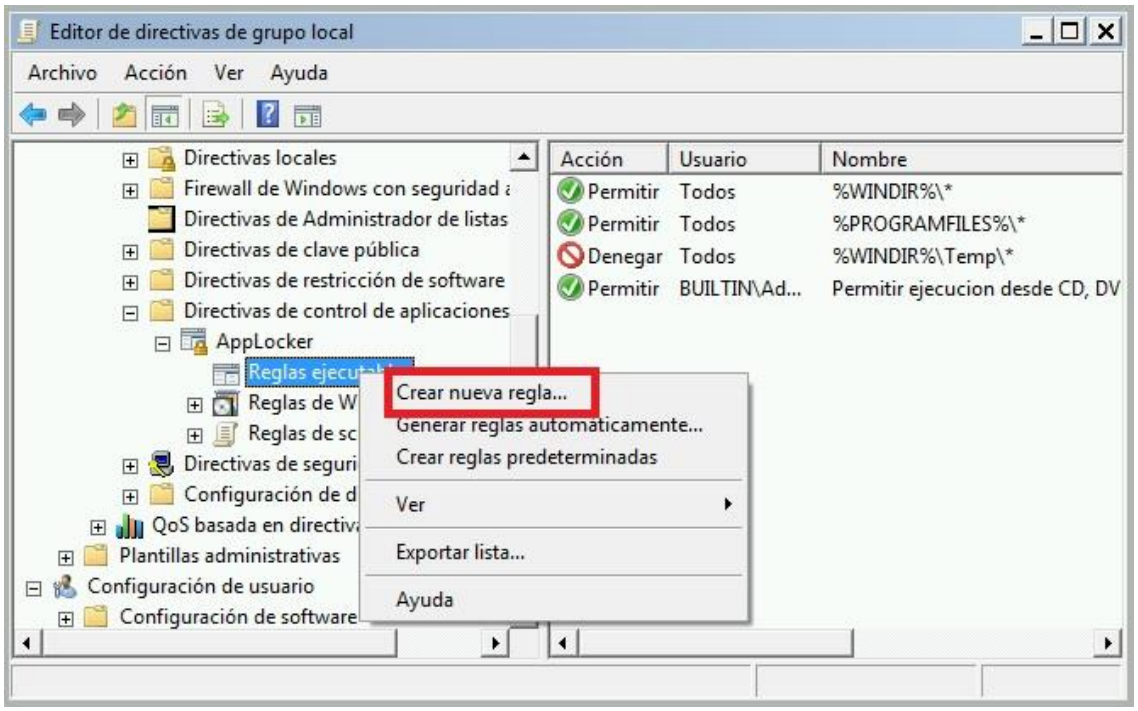
   Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de control de aplicaciones -> AppLocker



6. Despliegue el contenedor “AppLocker” y seleccione reglas ejecutables.

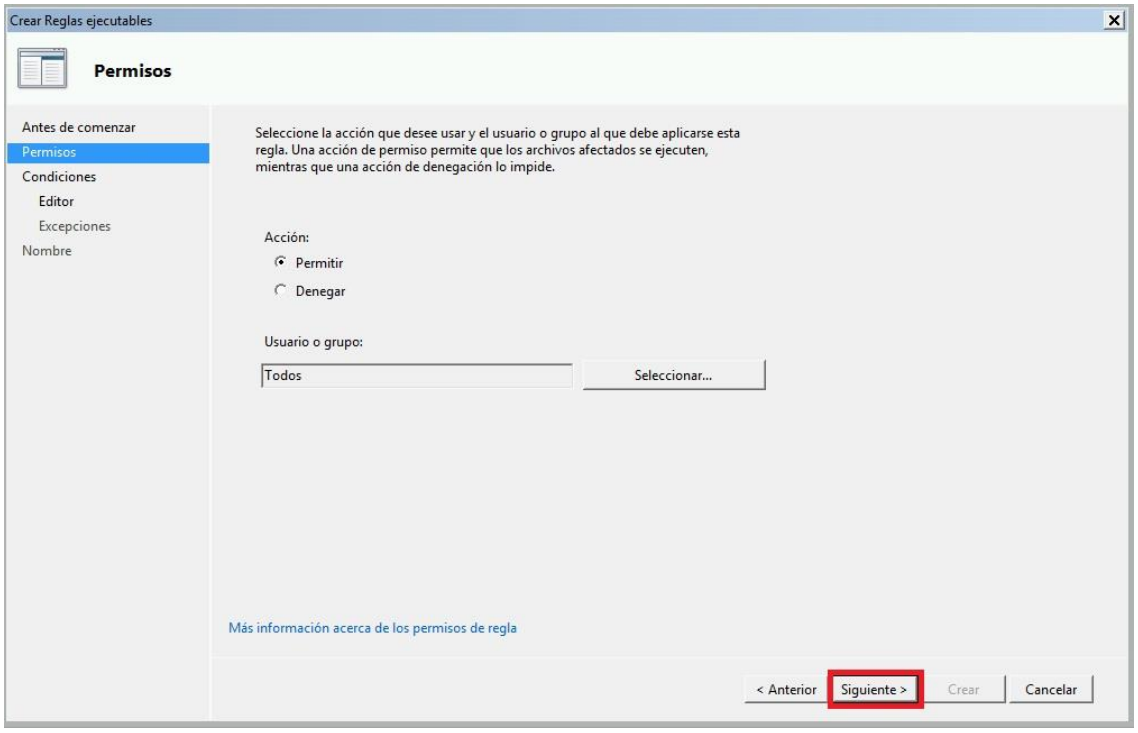


Paso	Descripción
7.	Pulse con el botón derecho del ratón sobre “Reglas ejecutables” y seleccione la opción de “Crear nueva regla”.



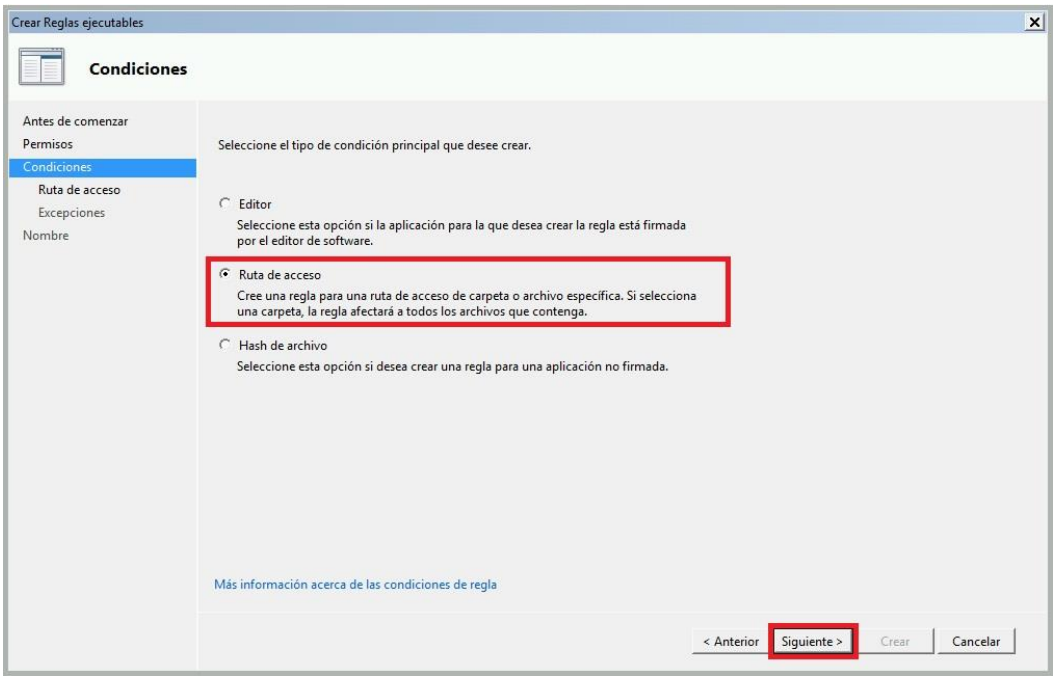
8.	En el inicio del asistente, pulse el botón “Siguiente >” para dar comienzo la creación de la regla.

9.	En permisos mantenga la configuración existente y pulse el botón “Siguiente >”.

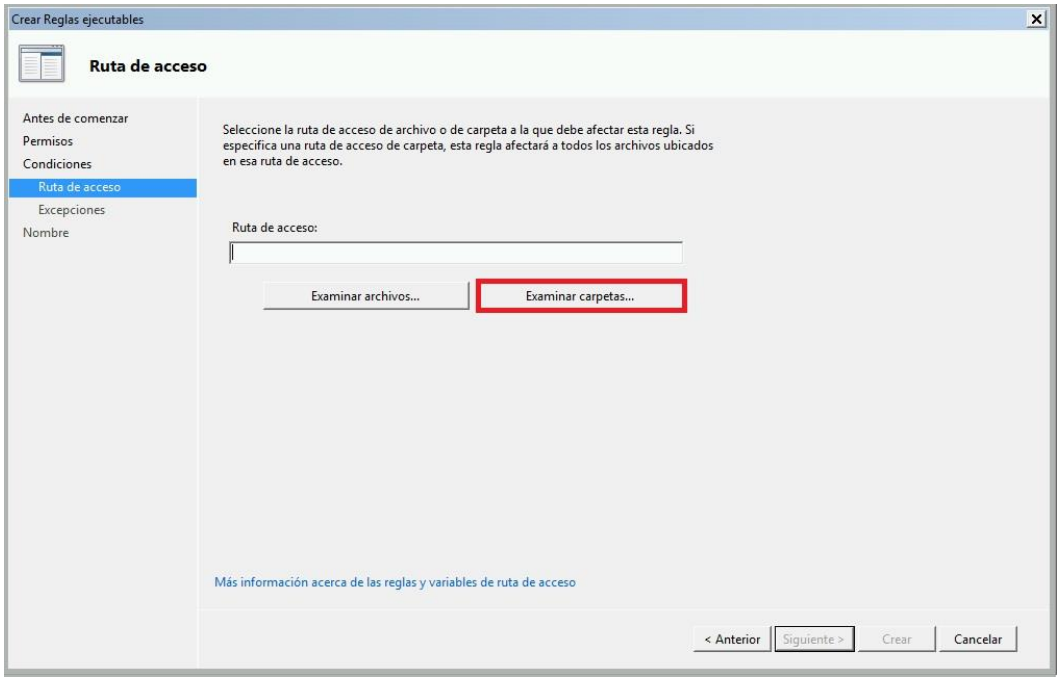


Paso	Descripción

10. En la pantalla de condiciones, seleccione la opción “Ruta de acceso” y pulse “Siguiente >”.



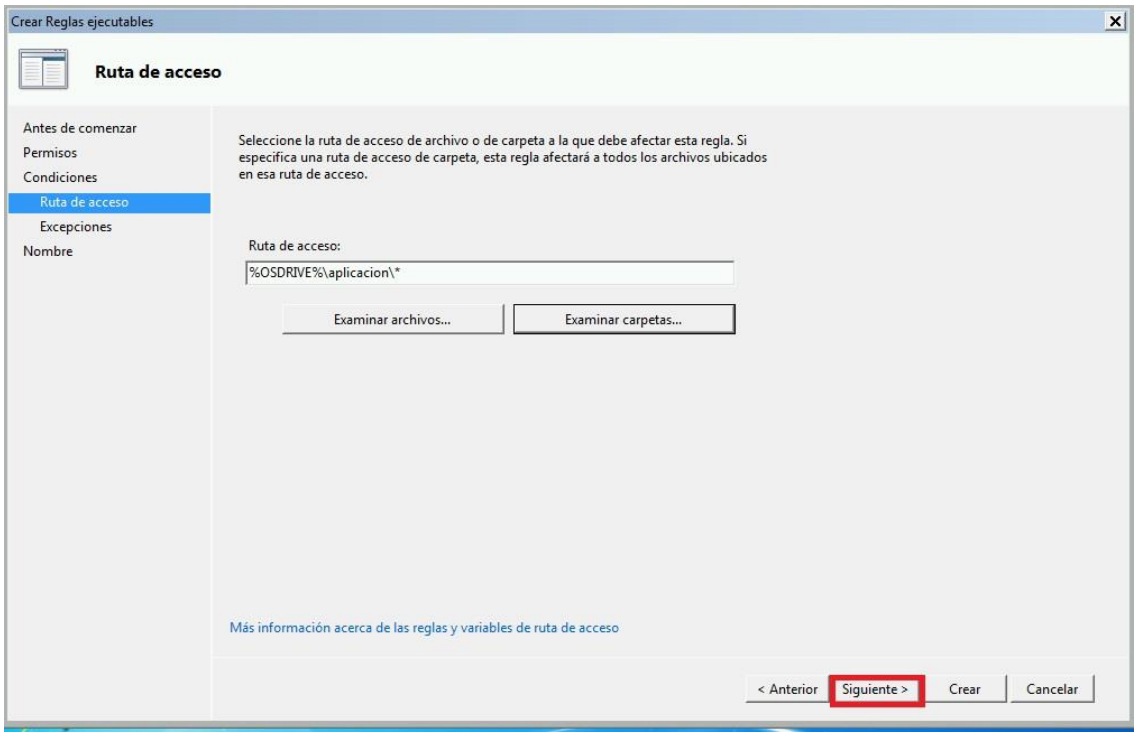
11. En la pantalla “Ruta de acceso” pulse el botón “Examinar carpetas…”.



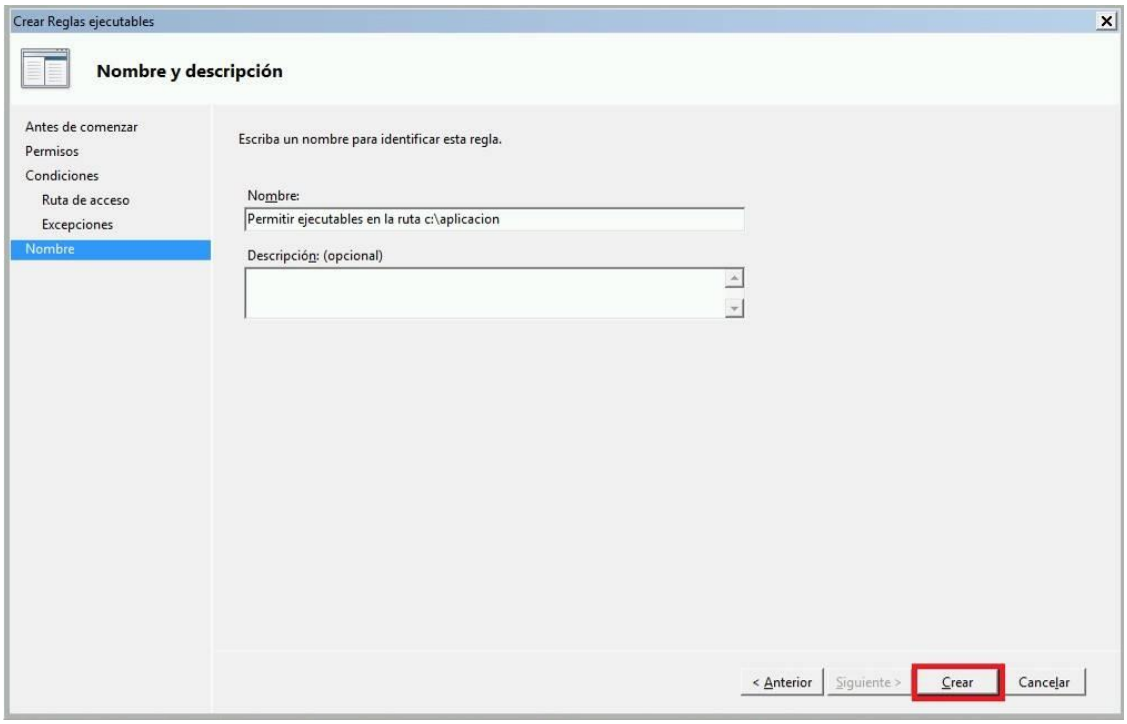
Nota: El ejemplo mostrado simula que se va a permitir la ejecución del contenido de una carpeta. Si solo fuera a ejecutar un único archivo .exe de dicha carpeta, se debería emplear la opción “Examinar archivos…” y seleccionar el único fichero ejecutable. Debe tener en consideración que las aplicaciones actuales son altamente complejas y puede que la carga de la aplicación se realice a través de un fichero .exe, pero este luego llame o dependa de otros ejecutables. Si tiene claro que la aplicación solo va a necesitar llamar a un fichero ejecutable, puede seleccionar la opción examinar archivos, de lo contrario, deberá emplear el mecanismo de examinar carpetas para permitir la ejecución de todo el contenido de dicha carpeta.

Paso	Descripción
12.	Seleccione la carpeta de la que desee crear la excepción. En el ejemplo se establece que el contenido ejecutable se encuentra en la carpeta “C:\aplicacion”.

13.	Una vez agregada la carpeta, pulse el botón “Siguiente >”.



14.	Si desea que algún contenido específico en dicha carpeta no sea ejecutado podrá agregar una excepción en la pantalla de “Excepciones”. Bien cuando haya agregado las excepciones o si no desea realizar ninguna, pulse el botón “Siguiente >”.

Paso	Descripción
15.	Para finalizar deberá asignar un nombre identificativo a la regla. En el ejemplo se asignará el nombre “Permitir ejecutables en la ruta c:\aplicacion”. Pulse el botón “Crear” cuando haya asignado un nombre. 
16.	La regla estará creada y disponible para su funcionalidad. Deberá crear tantas reglas de excepción como necesidades sean requeridas en el puesto de trabajo.
17.	Cierre la consola de editor de directivas de grupo local.
18.	Puede comprobar el correcto funcionamiento de las reglas de AppLocker aplicando los pasos descritos en la lista de comprobación del anexo K.

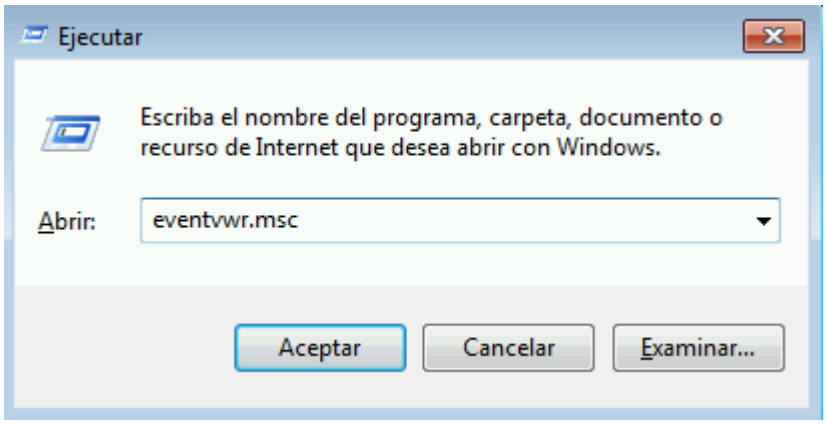
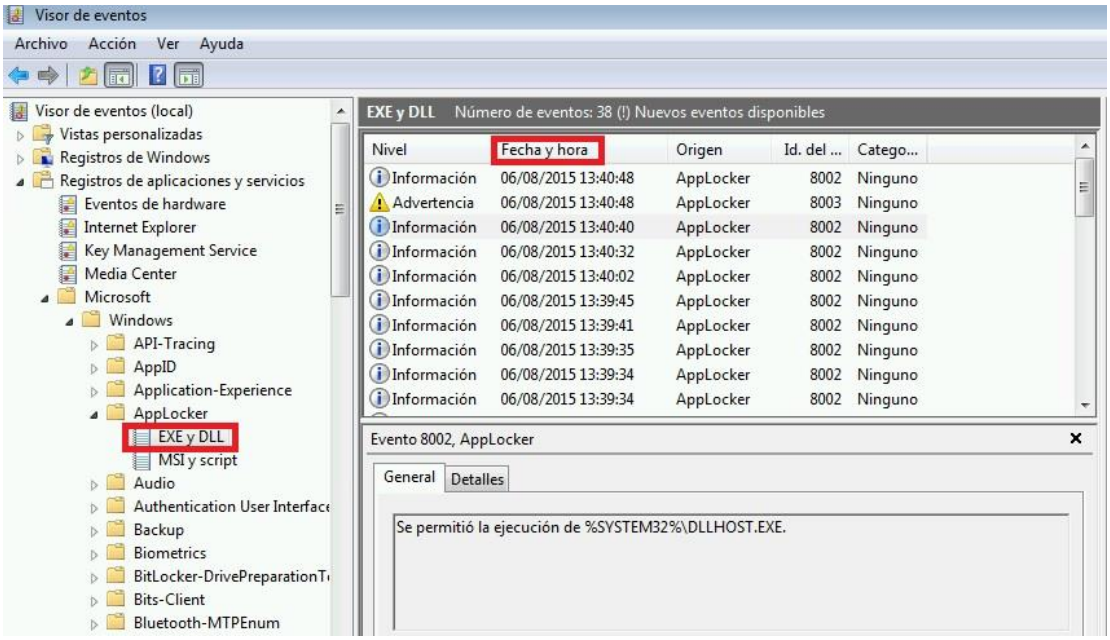
3. AUDITORÍA DE EVENTOS DE APPLOCKER

Las políticas definidas en este anexo contienen reglas de AppLocker configuradas exclusivamente en modo auditoría. No se aplican las reglas en modo forzado, por tanto, se podrá ejecutar cualquier binario sin restricción en las máquinas donde se hayan aplicado las políticas. La configuración de AppLocker se encargará de registrar logs de los eventos de permiso y restricción con el objetivo de auditar qué software se ha ejecutado en la máquina.

El presente apartado tiene como objetivo asistir a los administradores u operadores en la revisión de los eventos específicos de AppLocker.

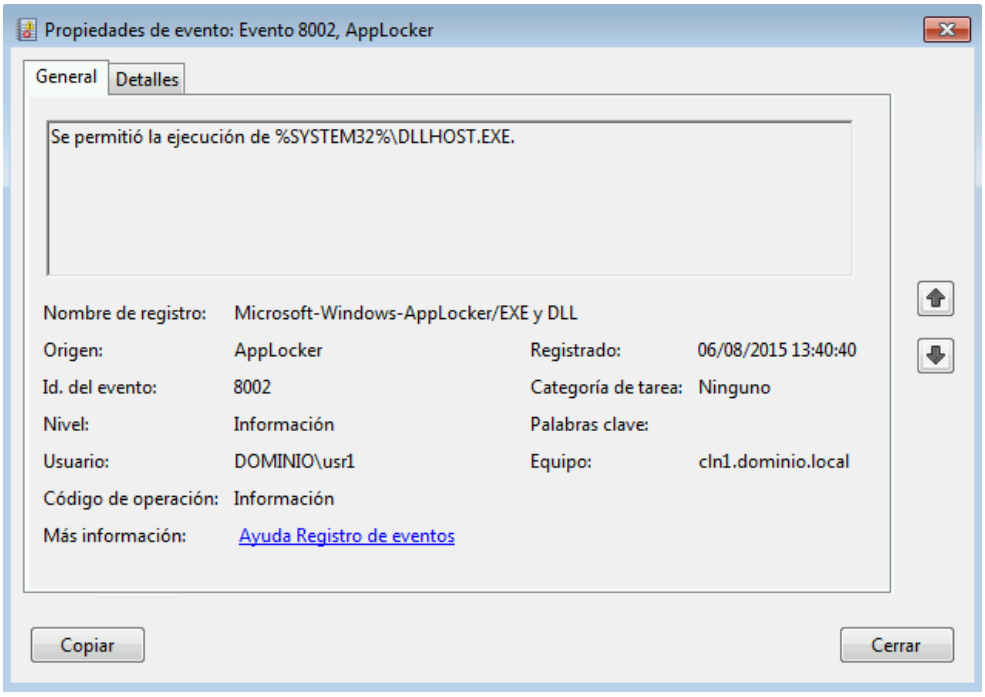
Los siguientes pasos deberán realizarse en la máquina o máquinas a revisar (pueden ser servidores o estaciones de trabajo).

El siguiente ejemplo está tomado de un cliente Windows 7 con un usuario simple (que por defecto tiene permisos de lectura sobre los eventos del equipo).

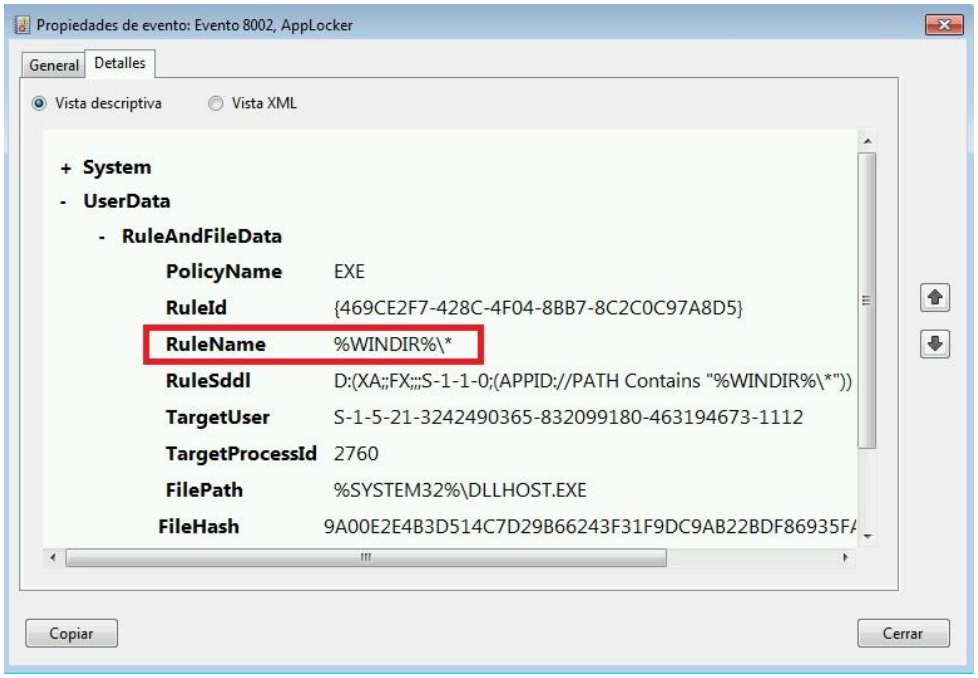
Paso	Descripción
1.	Inicie sesión en la máquina objeto del análisis de eventos. Puede iniciar sesión con un usuario sin privilegios especiales.
2.	Copie un fichero ejecutable (por ejemplo “%WINDIR%\system32\cmd.exe”) al escritorio del usuario iniciado.
3.	Ejecute el binario desde el escritorio. No tendrá problemas en ejecutar, sin embargo al estar situado en una ruta no permitida por las reglas de AppLocker definidas en éste anexo, se producirá un evento con ID 8003 que informará de que se ha ejecutado una aplicación desde una ubicación no permitida por las reglas definidas. Para comprobar dichos eventos se hará uso del visor de eventos de Microsoft.
4.	Despliegue el menú “Ejecutar” haciendo uso de la combinación de teclas “Windows + R”.
5.	En el menú “Ejecutar” escriba “eventvwr.msc” y pulse “Aceptar”. 
6.	En el “Visor de Eventos” navegue hasta la siguiente ubicación: **Visor de eventos (local) / Registros de aplicaciones y servicios / Microsoft / Windows / AppLocker / EXE y DLL** En el menú central podrá ver los eventos que se han registrado organizados por tiempo**.** 

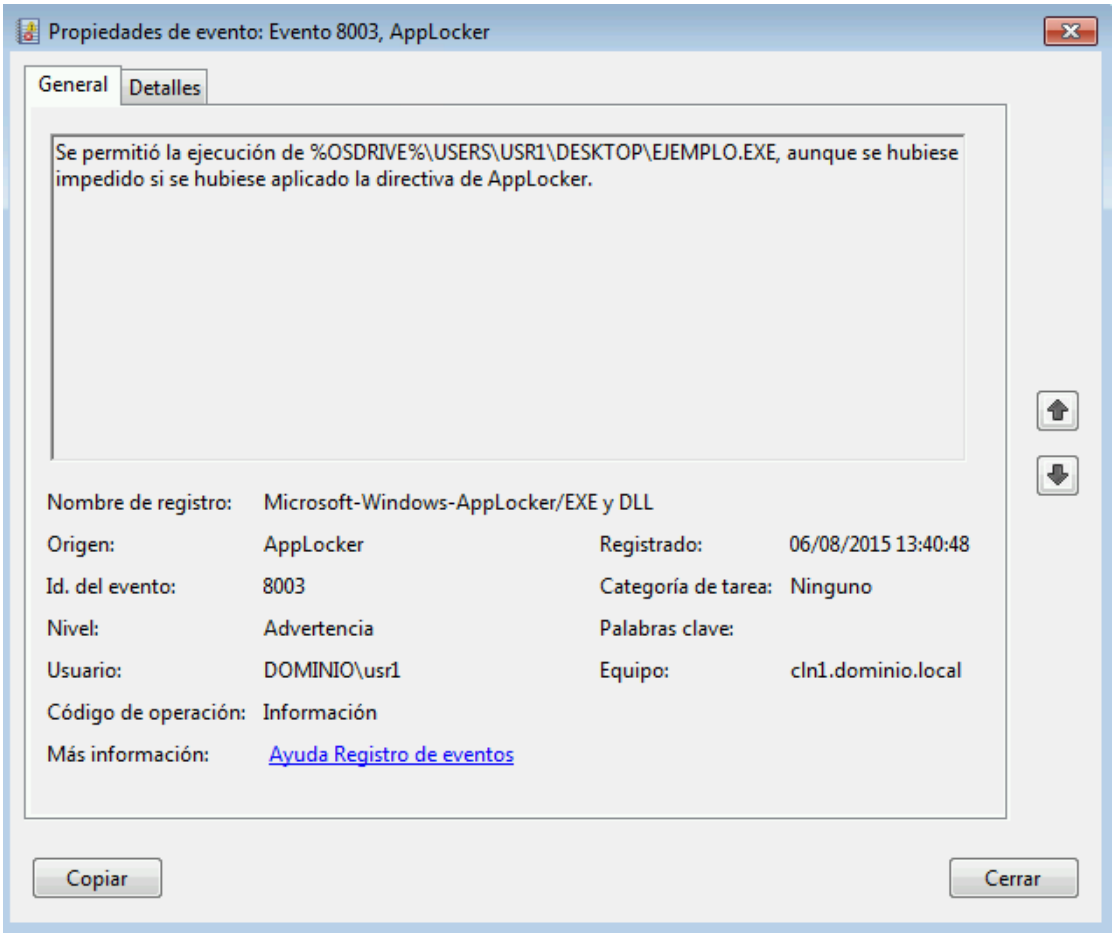
Paso	Descripción

7. Los eventos 8002 indican permisividad. Haciendo doble clic sobre un evento con ID 8002 podrá ver más información sobre el mismo. Los campos reseñables son:
   - Usuario: usuario que lanzó el ejecutable.
   - Registrado: fecha y hora de ejecución.
   - Id. Del evento: número identificativo del evento.
   - En el cuadro de texto principal se indica el nombre y ruta del ejecutable permitido.

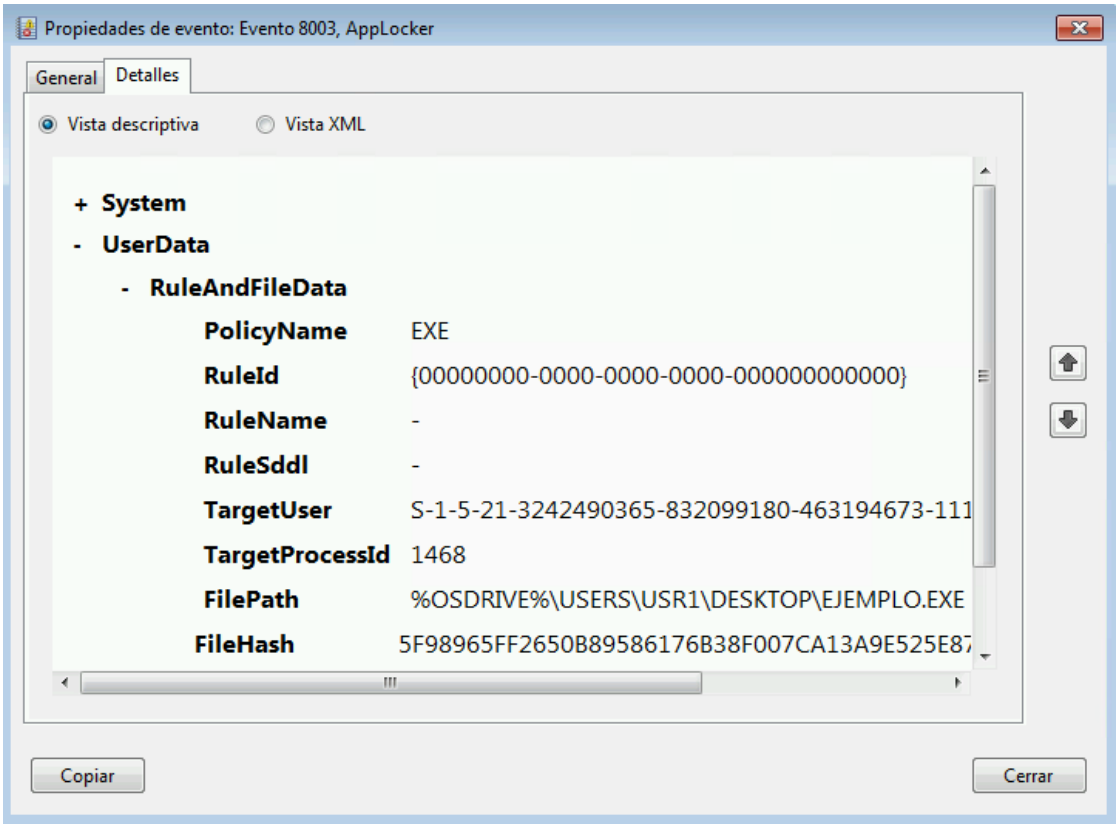


8. En la pestaña “detalles” encontramos el nombre de la regla que ha permitido la ejecución del binario además de otros campos informativos.



Paso	Descripción
9.	Los eventos 8003 indican ejecuciones de software que hubiera sido bloqueado por alguna de las reglas de AppLocker en el caso de que hubiesen estado forzadas. Haciendo doble clic sobre el evento con ID 8003 generado en el paso 3 de éste apartado podrá ver más información sobre el mismo. Los campos reseñables son: – Usuario: usuario que lanzó el ejecutable. – Registrado: fecha y hora de ejecución. – Id. Del evento: número identificativo del evento. – En el cuadro de texto principal se indica el ejecutable que se ha permitido. También se indica que dicha ejecución se habría bloqueado si las reglas de AppLocker se encontraran activas en lugar de en modo auditoría. 

Paso	Descripción
10.	En la pestaña “Detalles” se encuentra el nombre de la regla que hubiera bloqueado la ejecución del binario.



Nota: En este caso no se aprecia el nombre de la regla pero sí su identificador ({00000000-0000-0000-0000-000000000000}). Éste corresponde con la regla de negación por defecto. Si no hay una regla de permisividad para la ruta indicada, AppLocker bloquea por defecto la ejecución del binario.

ANEXO G. GUÍA PASO A PASO PARA LA CONFIGURACIÓN DE APPLOCKER EN CLIENTES O SERVIDORES INDEPENDIENTES QUE LES SEA DE APLICACIÓN EL NIVEL MEDIO O ALTO DEL ENS

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar la implantación del servicio AppLocker en clientes independientes (Windows 7 Enterprise o Ultimate así como Windows Server 2008R2 o 2012R2) con una categorización de seguridad media o alta, según los criterios del Esquema Nacional de Seguridad.

Las capturas de pantalla incluidas en los pasos, descritos en el presente anexo, han sido tomadas de un Windows 7 Enterprise independiente al que previamente se le ha aplicado la guía CCN-STIC-850B. Los pasos son extensibles a servidores Windows Server 2008R2 y 2012R2 con las guías CCN-STIC-851B y CCN-STIC-870B aplicadas respectivamente a cada sistema operativo.

Para la implantación en nivel medio o alto, según criterios del Esquema Nacional de Seguridad, las reglas de AppLocker se implementarán en modo forzado. De esta manera, se restringirá la ejecución de binarios ubicados en rutas de instalación no estándar.

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 o 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

1. CONFIGURACIÓN DE APPLOCKER EN CLIENTE INDEPENDIENTE

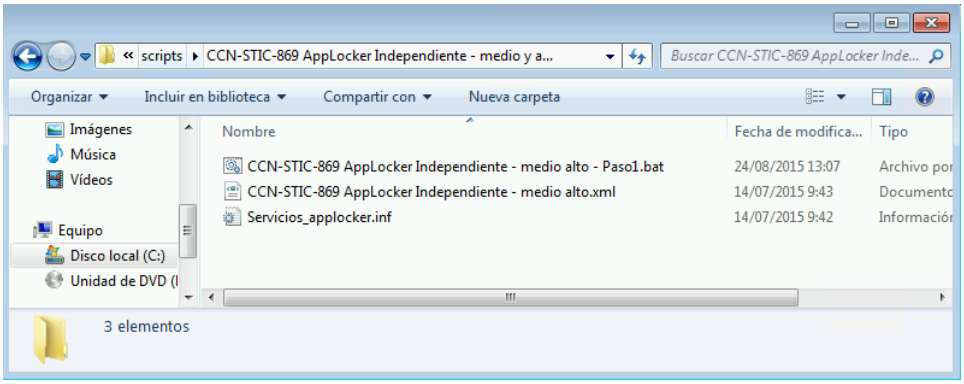
Los pasos que se describen a continuación, han sido diseñados para ayudar a los operadores a implementar la configuración de AppLocker en un puesto de trabajo Windows 7 que implemente servicios o información de nivel medio o alto y que se encuentre supeditado al cumplimiento del Esquema Nacional de Seguridad. Esto implica que, previamente, al cliente se le ha aplicado la guía CCN-STIC-850B en nivel medio o alto.

La aplicación de los pasos es extensible a servidores Windows Server 2008R2 y 2012R2 con las guías CCN-STIC-851B y CCN-STIC-870B aplicadas en nivel medio o alto respectivamente en cada sistema operativo.

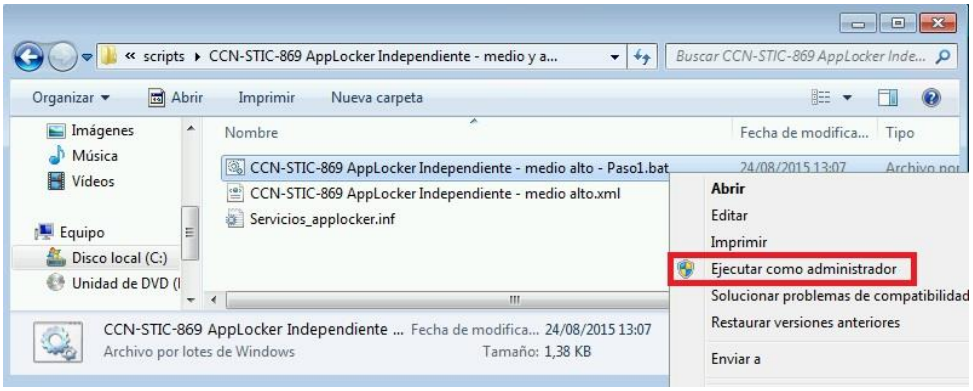
Nota: Tenga en consideración que la siguiente configuración es de tipo genérica. Es posible que sean necesarias configuraciones adicionales para agregar excepciones de permisividad de aplicaciones. Revise el punto 2 del presente anexo para conocer cómo efectuar excepciones adicionales.

Paso	Descripción
1.	Inicie sesión en el puesto de trabajo que va a configurar con un usuario con privilegios de administración local.

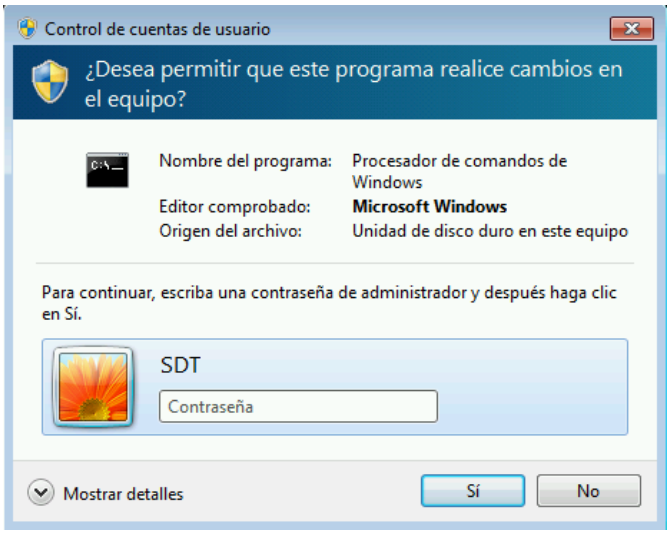
Paso	Descripción
2.	Cree en la unidad “C:\” la carpeta “Scripts”.
3.	Copie la carpeta “CCN-STIC-869 AppLocker Independiente – medio alto” que acompaña esta guía al directorio “C:\Scripts”.
4.	Abra la carpeta “C:\Scripts\CCN-STIC-869 AppLocker Independiente – medio alto” que encontrará en la carpeta “C:\Scripts” que ha copiado.



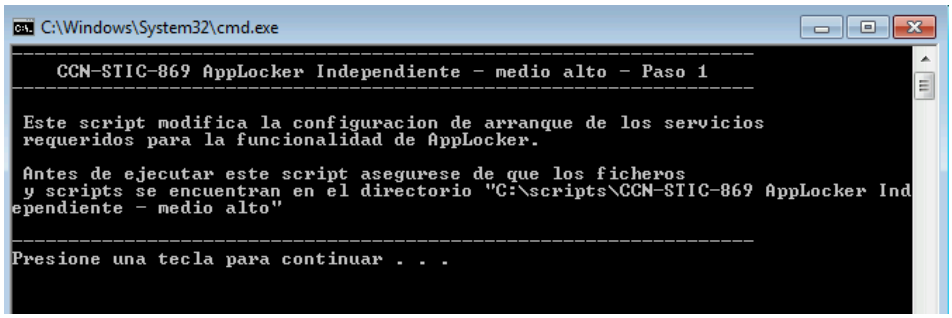
5.	Pulse con el botón derecho del ratón sobre el fichero “CCN-STIC-869 AppLocker Independiente – medio alto – Paso1.bat” y seleccione la opción “Ejecutar como administrador”.



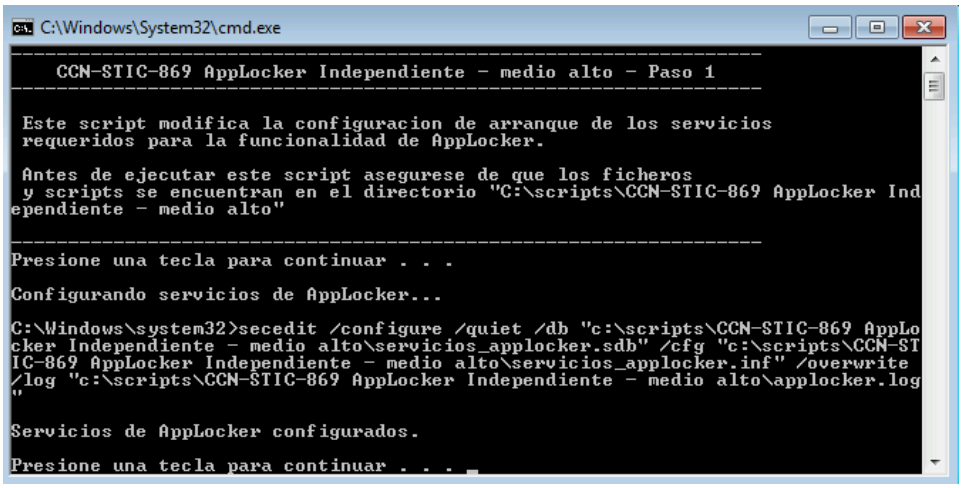
6.	Introduzca cuando se le solicite la contraseña del usuario con privilegios de administrador local para la ejecución de la aplicación.



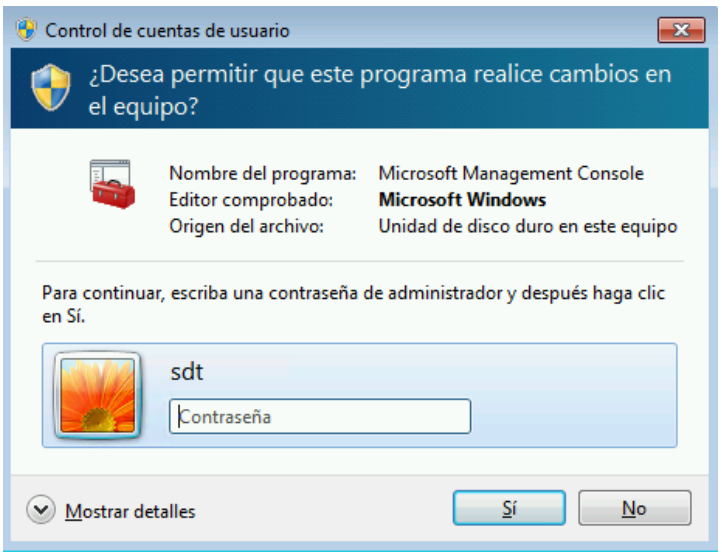
Paso	Descripción
7.	Pulse cualquier tecla para iniciar la ejecución del script que configurará el servicio de identidad de aplicación para que inicie de manera automática.

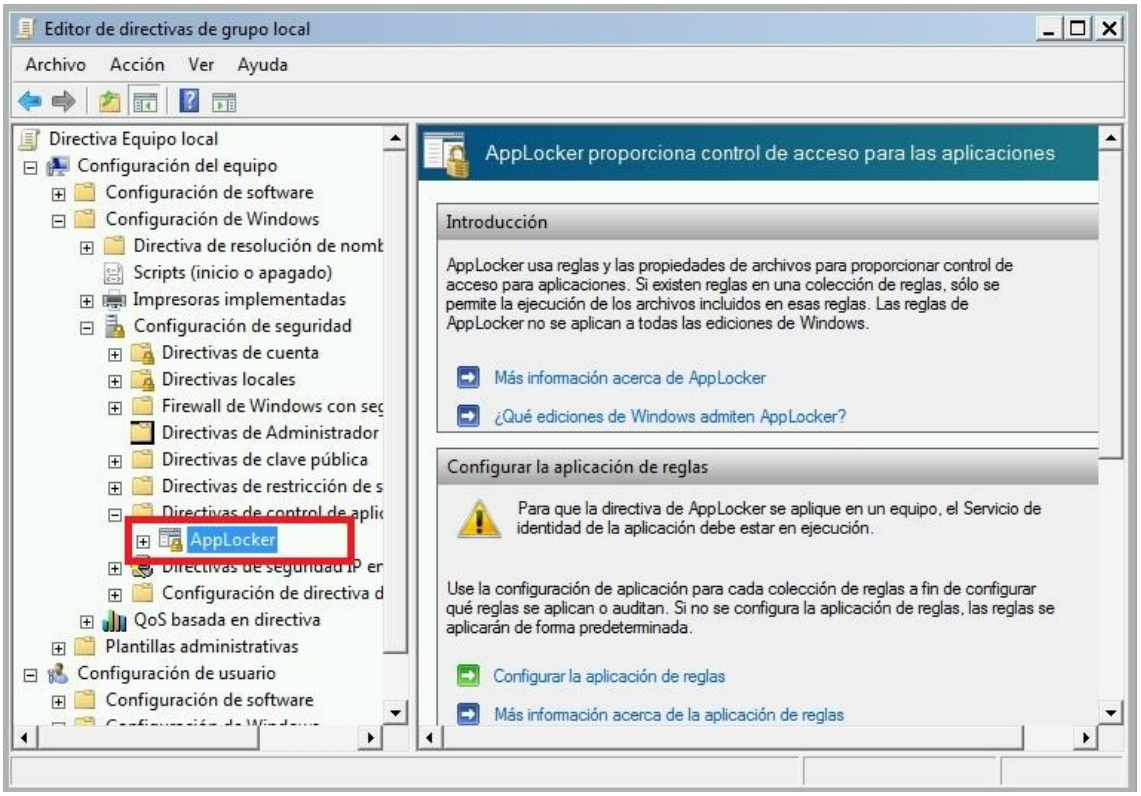
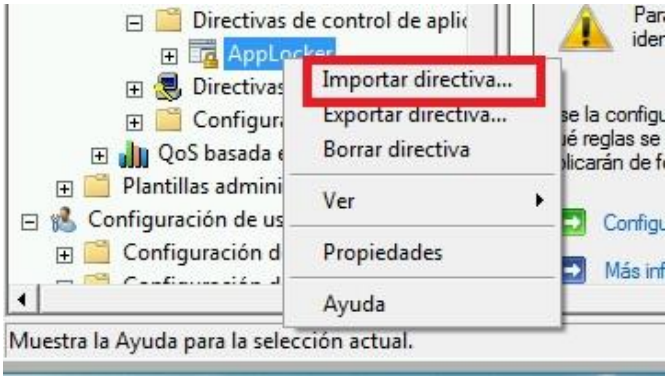


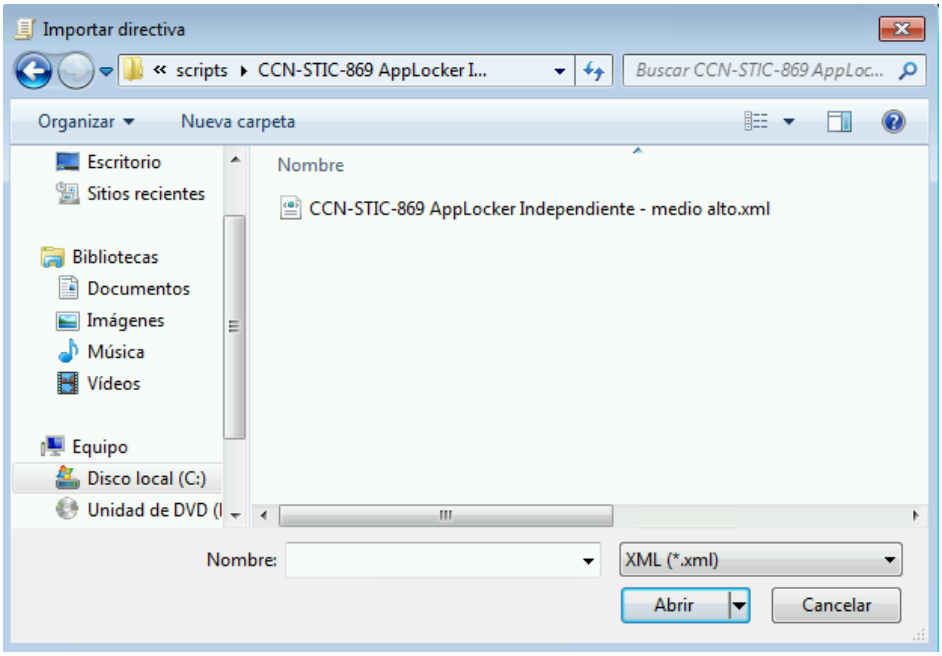
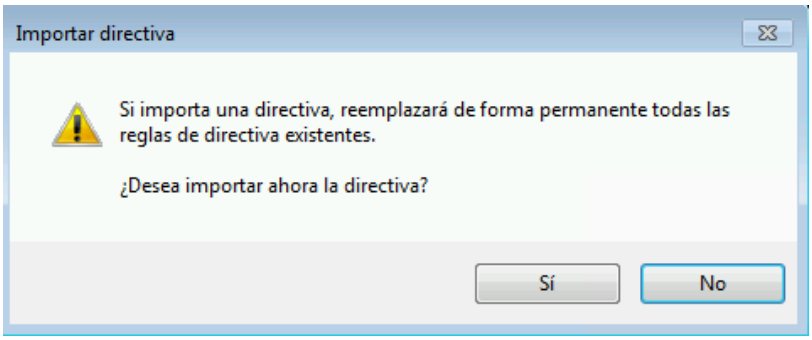
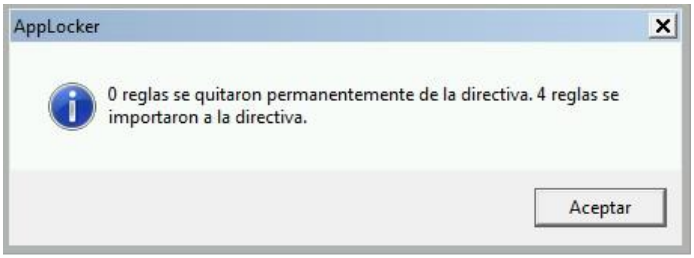
8.	Una vez completado el proceso, deberá pulsar una tecla para continuar.



9.	La ejecución del script de configuración se habrá completado, pulse una tecla para finalizar.
10.	Pulse la combinación de teclas “Windows + R” para acceder al menú “Ejecutar”.
11.	En el menú “Ejecutar” escriba “GPedit.msc” y pulse la tecla “Enter”.
12.	Introduzca la contraseña del usuario con privilegios de administrador.



Paso	Descripción
13.	En la consola del editor de directivas de grupo local, vaya a la siguiente ruta: **Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de control de aplicaciones -> AppLocker** 
14.	Sobre “AppLocker” pulse con el botón derecho del ratón y seleccione la opción “Importar directiva…”. 

Paso	Descripción
15.	En la ventana de importación de directiva seleccione el fichero “CCN-STIC-869 AppLocker – Independiente – medio alto.xml” existente en la carpeta “C:\Scripts\CCN-STIC-869 AppLocker Independiente – medio alto”. Haga doble clic sobre él o pulse sobre el botón “Abrir”. 
16.	Pulse “Si” en la advertencia informativa. 
17.	Pulse el botón “Aceptar” en la notificación de AppLocker. 
18.	Si desea realizar alguna modificación o ampliación de reglas, sería conveniente realizarlo ahora. Para efectuarlo siga los pasos establecidos en el punto 2 del presente anexo.
19.	Puede cerrar la ventana del “Editor de directivas de grupo local”.
20.	Puede comprobar la correcta implantación de las diferentes configuraciones de seguridad aplicadas siguiendo los pasos descritos en el anexo L.
21.	Elimine la carpeta “C:\Scripts”.

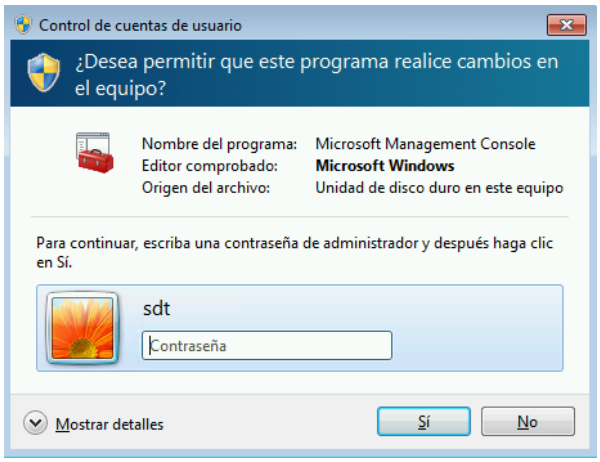
2. CREACIÓN DE EXCEPCIONES DE APPLOCKER PARA LA EJECUCIÓN DE APLICACIONES DESDE RUTAS NO ESTÁNDARES EN UN CLIENTE INDEPENDIENTE

El siguiente paso a paso describe los procesos para crear excepciones en el cliente Windows 7 independiente (con la guía CCN-STIC-850B aplicada en nivel medio o alto), de tal forma que se vaya a permitir ejecutar contenido desde rutas no estándares. El siguiente ejemplo simula la permisividad para la ejecución de una aplicación instalada en la carpeta "C:\aplicacion".

La aplicación de los pasos descritos en este apartado es extensible a servidores Windows Server 2008R2 y 2012R2 con las guías CCN-STIC-851B y CCN-STIC-870B aplicadas en nivel medio o alto respectivamente en cada sistema operativo.

Nota: De forma predeterminada, las aplicaciones se instalan habitualmente en el directorio de archivo de programa, pero bien por decisión del administrador del equipo o por la configuración de la propia aplicación, ésta se podría realizar en una ubicación diferente. Si esto es así, use a modo de ejemplo el siguiente paso a paso para crear la excepción o excepciones necesarias.

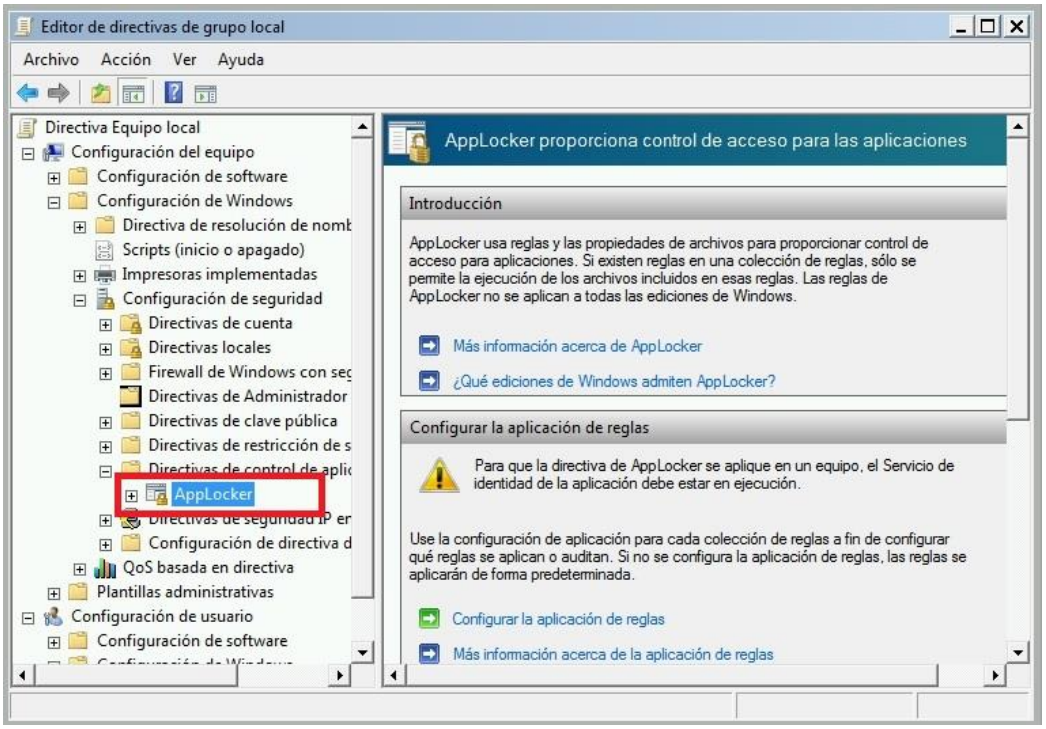
Paso	Descripción
1.	Inicie sesión en el puesto de trabajo con un usuario con privilegios de administrador local.
2.	Pulse la combinación de teclas "Windows + R" para acceder al menú "Ejecutar".
3.	En el menú "Ejecutar" escriba "GPedit.msc" y pulse la tecla "Enter".
4.	Introduzca la contraseña del usuario con permisos de administración local.



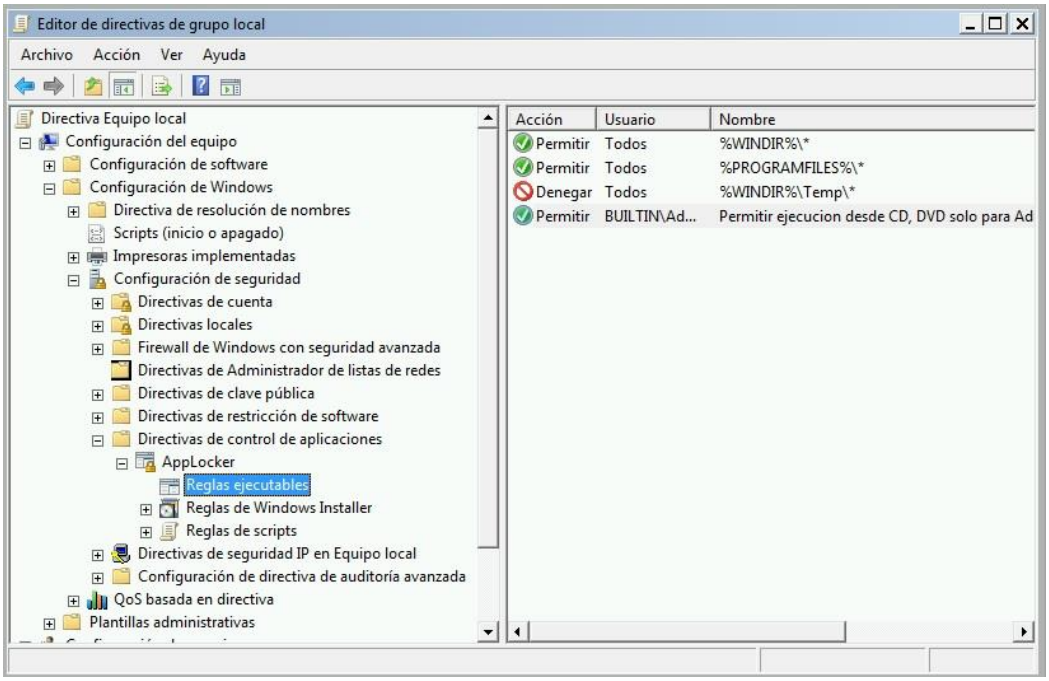
Paso	Descripción

5. En la consola del editor de directivas de grupo local, vaya a la siguiente ruta:

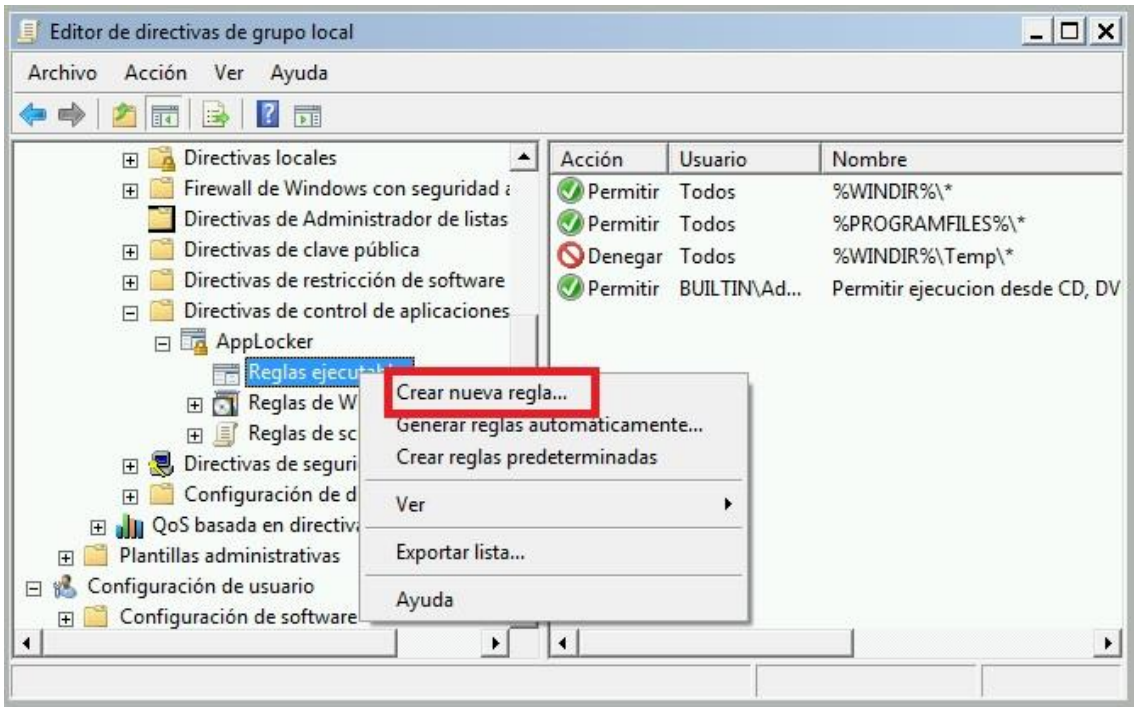
   Configuración de equipo -> Configuración de Windows -> Configuración de seguridad -> Directivas de control de aplicaciones -> AppLocker



6. Despliegue el contenedor “AppLocker” y seleccione reglas ejecutables.

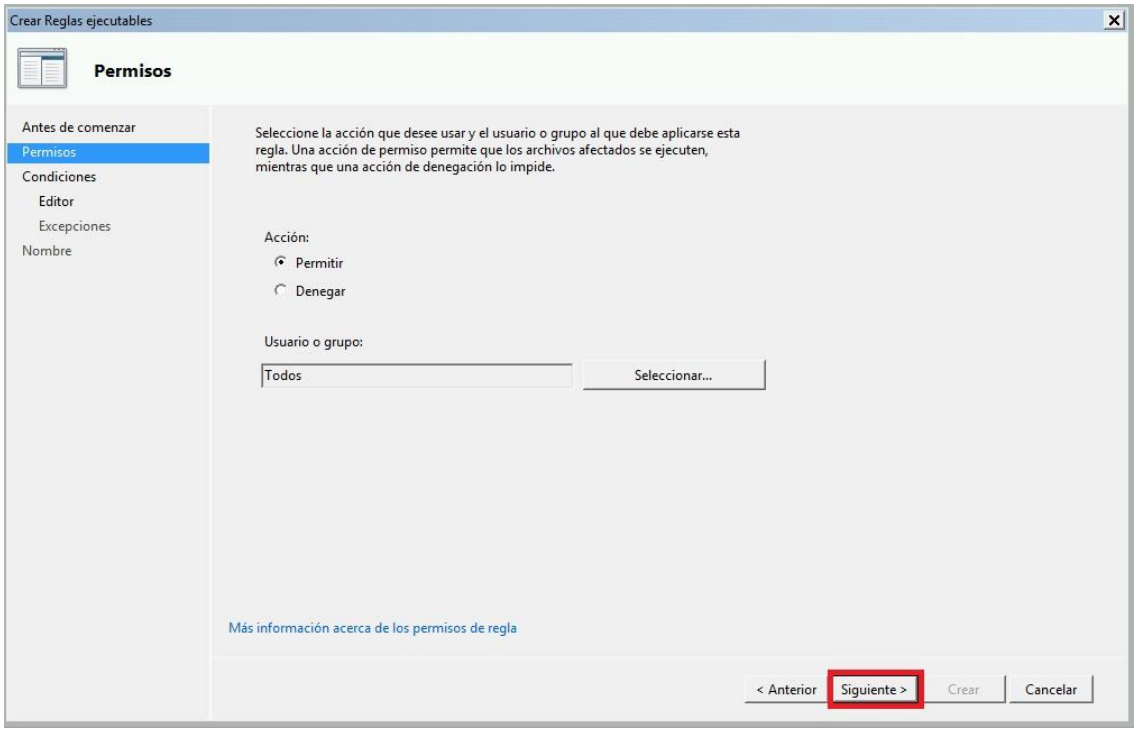


Paso	Descripción
7.	Pulse con el botón derecho del ratón sobre “Reglas ejecutables” y seleccione la opción de “Crear nueva regla”.



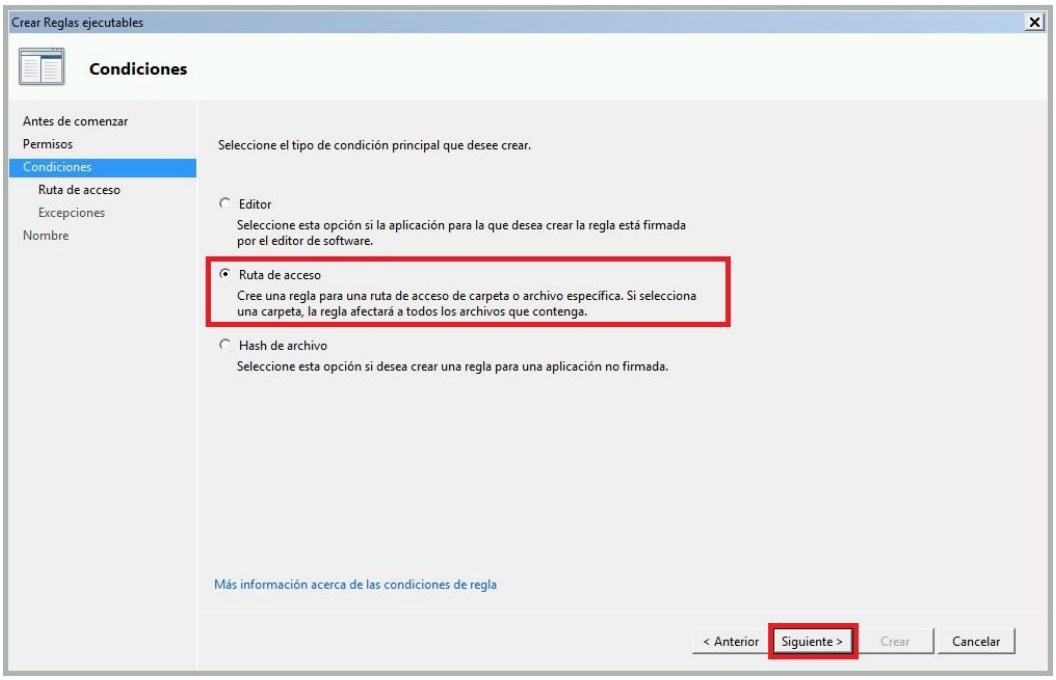
8.	En el inicio del asistente, pulse el botón “Siguiente >” para dar comienzo la creación de la regla.

9.	En “Permisos” mantenga la configuración existente y pulse el botón “Siguiente >”.

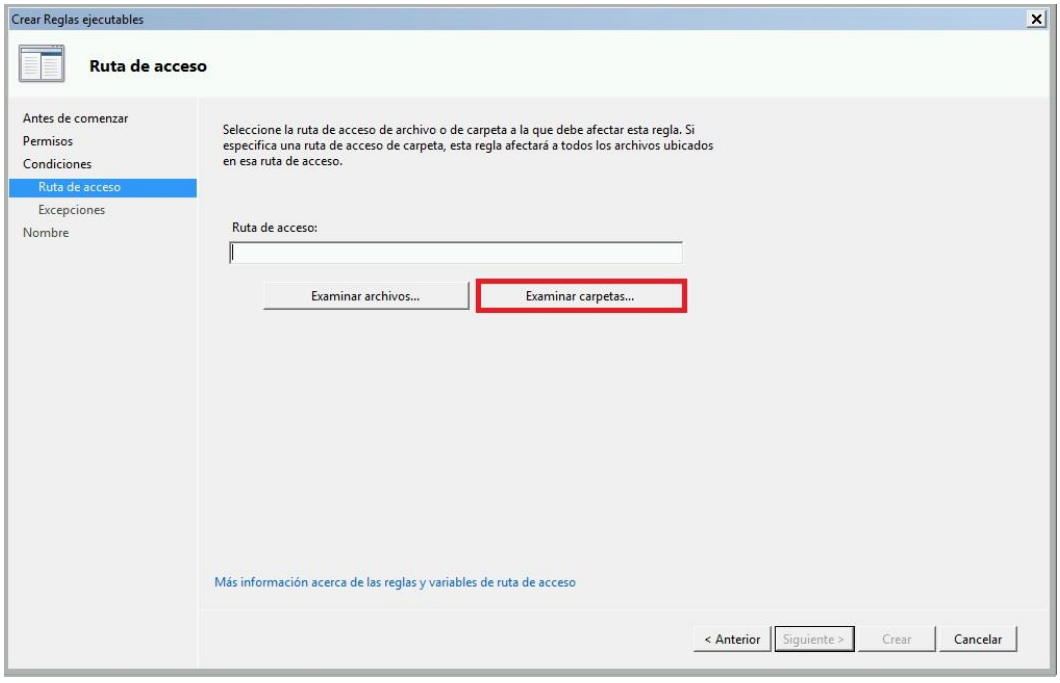


Paso	Descripción

10. En la pantalla de condiciones, seleccione la opción “Ruta de acceso” y pulse “Siguiente >”.



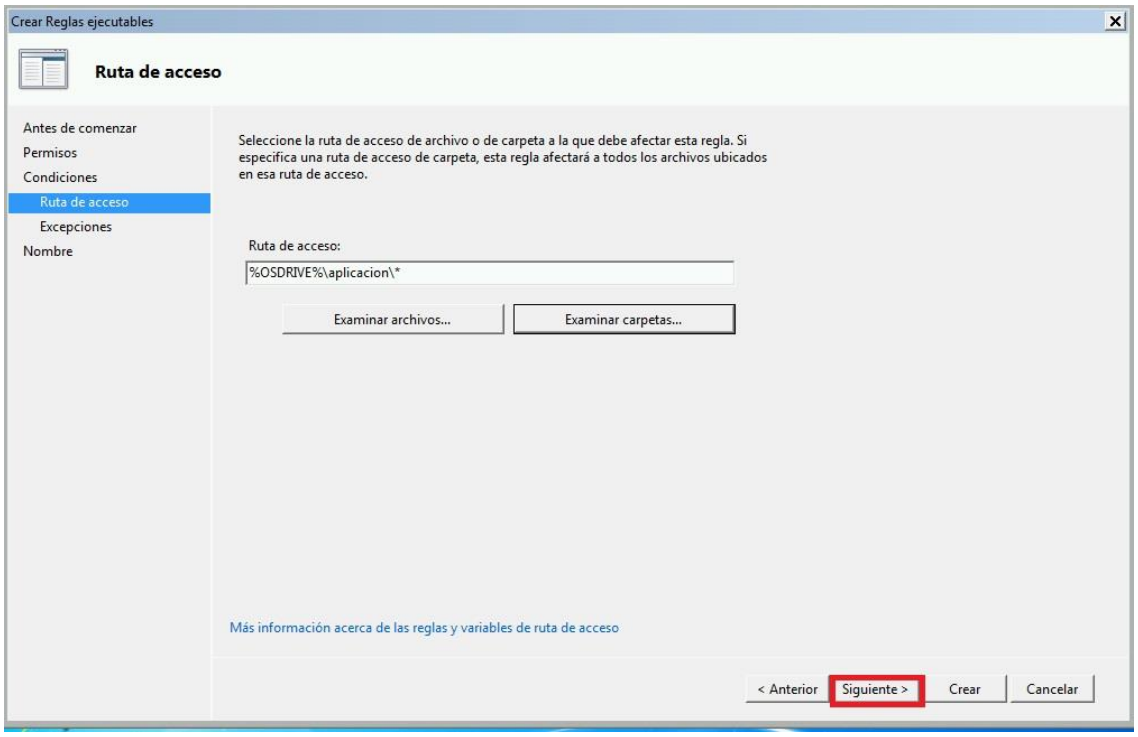
11. En la pantalla “Ruta de acceso” pulse el botón “Examinar carpetas…”.



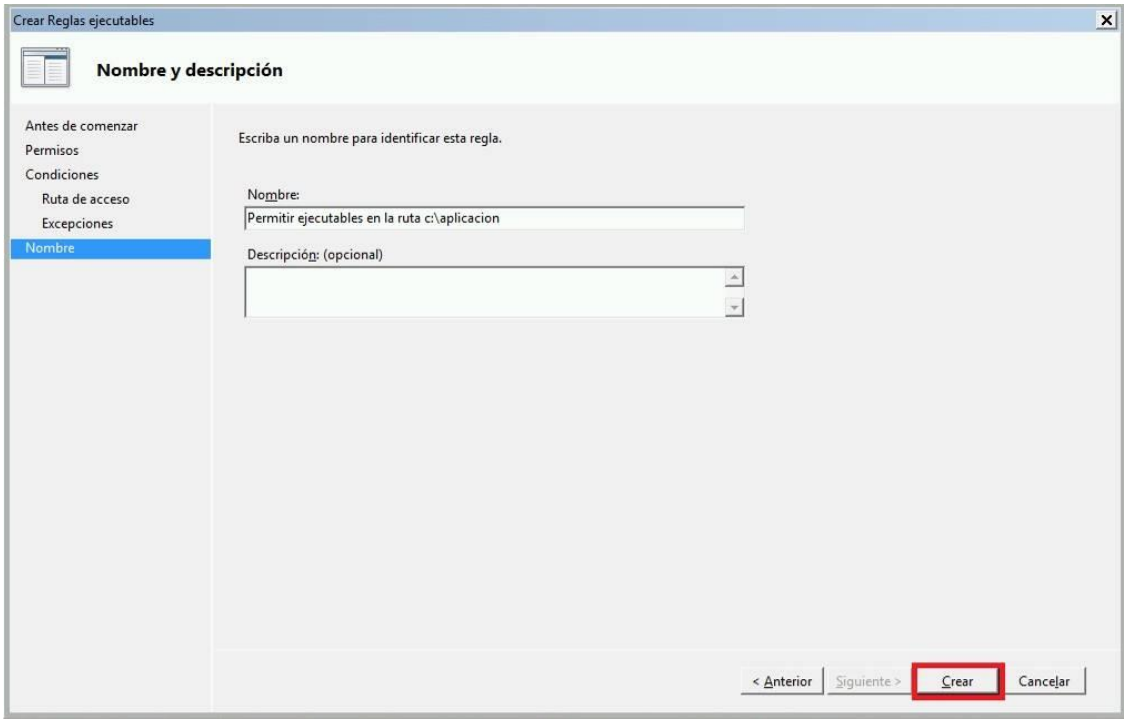
Nota: El ejemplo mostrado simula que se va a permitir la ejecución del contenido de una carpeta. Si solo fuera a ejecutar un único archivo .exe de dicha carpeta, se debería emplear la opción “Examinar archivos…” y seleccionar el único fichero ejecutable. Debe tener en consideración que las aplicaciones actuales son altamente complejas y puede que la carga de la aplicación se realice a través de un fichero .exe, pero este luego llame o dependa de otros ejecutables. Si tiene claro que la aplicación solo va a necesitar llamar a un fichero ejecutable, puede seleccionar la opción examinar archivos, de lo contrario deberá emplear el mecanismo de examinar carpetas para permitir la ejecución de todo el contenido de dicha carpeta.

Paso	Descripción
12.	Seleccione la carpeta de la que desee crear la excepción. En el ejemplo se establece que el contenido ejecutable se encuentra en la carpeta “C:\aplicacion”.

13.	Una vez agregada la carpeta, pulse el botón “Siguiente >”.



14.	Si desea que algún contenido específico de dicha carpeta no sea ejecutado, podrá agregar una excepción en la pantalla de “Excepciones”. Bien cuando haya agregado las excepciones o si no desea realizar ninguna, pulse el botón “Siguiente >”.

Paso	Descripción
15.	Para finalizar deberá asignar un nombre identificativo a la regla. En el ejemplo, se asignará el nombre “Permitir ejecutables en la ruta c:\aplicacion”. Pulse el botón “Crear” cuando haya asignado un nombre. 
16.	La regla estará creada y disponible para su funcionalidad. Deberá crear tantas reglas de excepción como necesidades sean requeridas en el puesto de trabajo.
17.	Cierre la consola de editor de directivas de grupo local.
18.	Puede comprobar el correcto funcionamiento de las reglas de AppLocker aplicando los pasos descritos en la lista de comprobación del anexo L.

ANEXO H. CREACIÓN, EDICIÓN Y ELIMINACIÓN DE REGLAS DE APPLOCKER EN RED DE DOMINIO

Este anexo ha sido diseñado para asistir a los operadores en la modificación de las políticas de AppLocker distribuidas en una red de dominio mediante GPOs. Dada la naturaleza restrictiva de las políticas aplicadas, puede darse la necesidad de que la organización precise crear excepciones temporales o permanentes para permitir ejecutar binarios desde ubicaciones que, tras la aplicación de la presente guía, no se permiten.

Microsoft no recomienda la modificación directa de las reglas de AppLocker cuando éstas sean distribuidas mediante GPO de dominio. El procedimiento que indica el fabricante pasa por realizar una exportación de las reglas (se genera un fichero XML) para luego importarlas en lo que se conoce como "equipo de referencia". En este equipo se llevará a cabo la edición de las reglas para posteriormente exportarlas e importarlas en el GPO final.

https://technet.microsoft.com/en-us/library/ee791894(v=ws.10).aspx

Para evitar problemas, el equipo de referencia ha de ser miembro del dominio pero no debe recibir políticas de AppLocker por GPO.

El proceso de importación no es aditivo, elimina las reglas anteriores y mantiene únicamente la colección importada.

Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán en modo auditoría.

1. PASO A PASO PARA LA EDICIÓN GENÉRICA DE REGLAS DE APPLOCKER EN CLIENTES O SERVIDORES MIEMBROS DE UN DOMINIO WINDOWS SERVER 2008 R2 O 2012 R2

En los siguientes pasos se detalla el procedimiento a seguir para modificar reglas de AppLocker definidas en un GPO existente. La implementación de AppLocker detallada en esta guía, para los distintos niveles del Esquema Nacional de seguridad, se ha diseñado de tal manera que las nuevas reglas, o excepciones se han de definir editando los GPO de excepciones.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel bajo del ENS son:

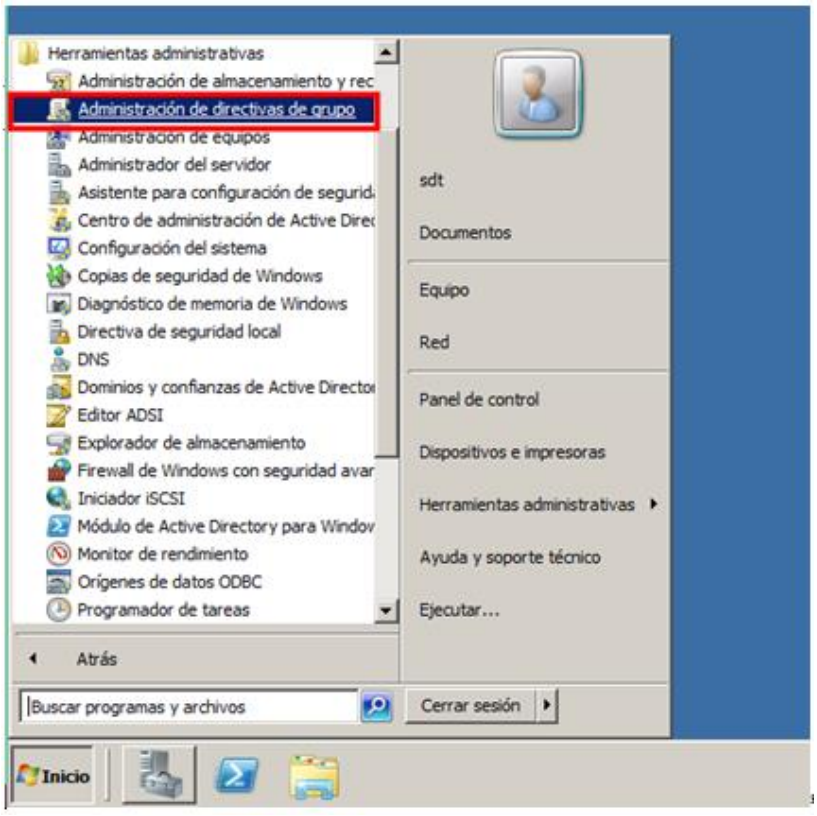
- CCN-STIC-869 ENS AppLocker Excepciones DC – bajo: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán igualmente en modo auditoría.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel medio o alto del ENS son:

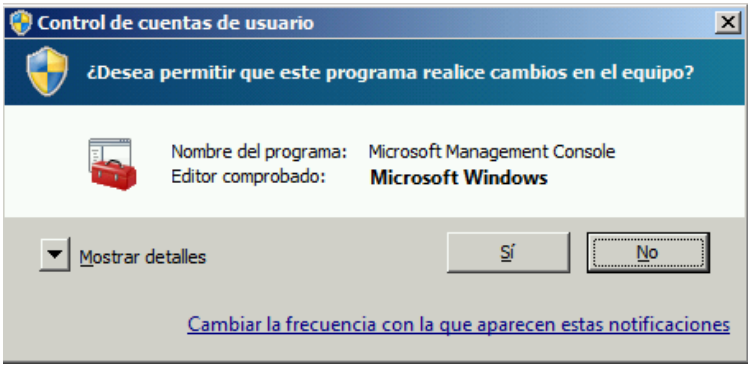
- CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio con una cuenta con derechos de administración en el dominio.
2.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio: **Inicio → Herramientas administrativas → Administración de directivas de grupo** 

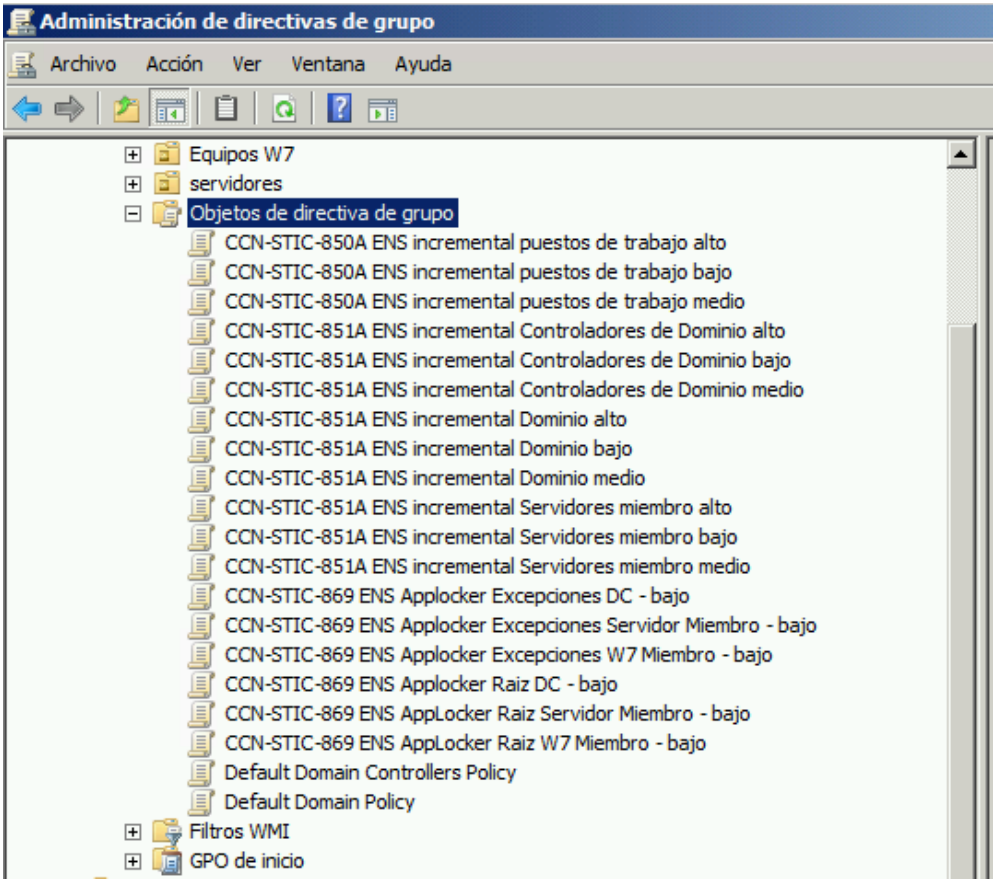
Paso	Descripción

3. Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos.



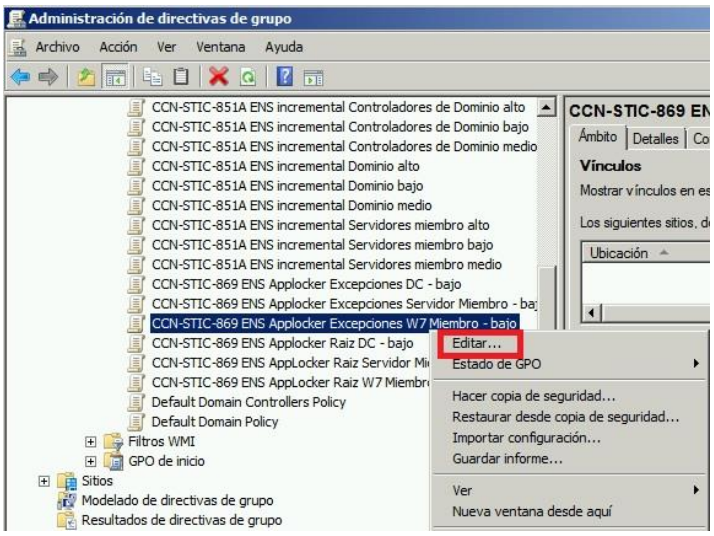
Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

4. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo,** como se muestra en la siguiente imagen.



Paso	Descripción

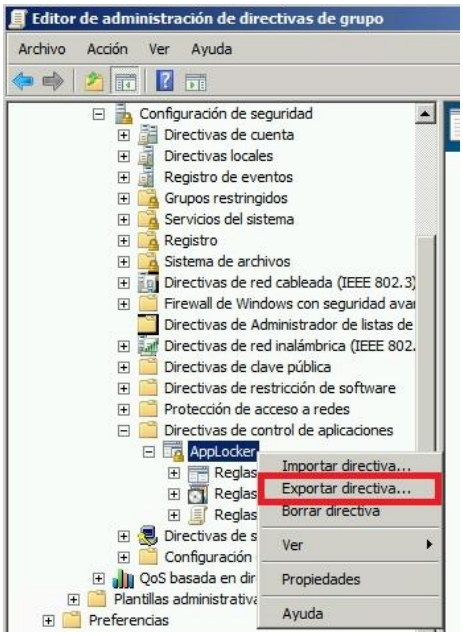
5. Seleccione el GPO de excepciones a modificar. En este ejemplo se pretende modificar la colección de reglas de AppLocker aplicadas a clientes Windows 7 a los que les aplica el nivel bajo del ENS. Por lo que se procederá a la edición del GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.



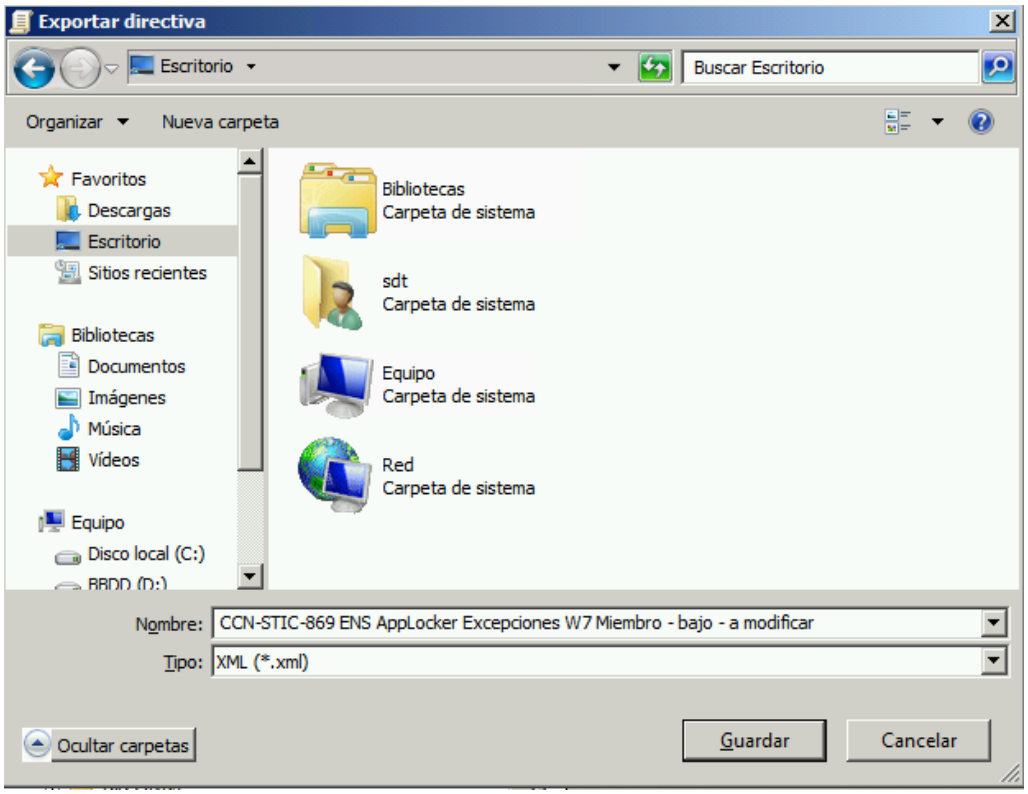
Nota: El GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" está diseñado para recibir las excepciones o nuevas reglas que se quieran aplicar a los Equipos W7 de la organización. Si necesita crear excepciones que apliquen a servidores miembros o a los controladores de dominio, seleccione el GPO adecuado según se describe al comienzo del presente anexo.

6. En el "Editor de administración de directivas de grupo" seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción "**Exportar directiva**".

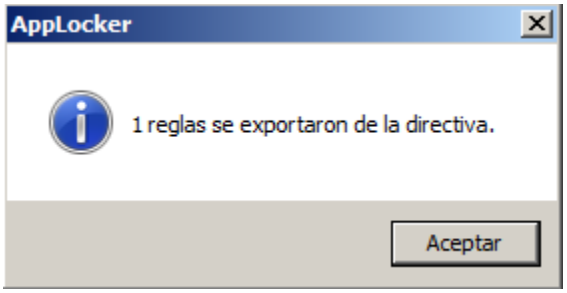
Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker



Paso	Descripción
7.	En el cuadro de dialogo abierto, navegue hasta un directorio con permisos de escritura y guarde la política exportada en formato xml. Elija un nombre reconocible.



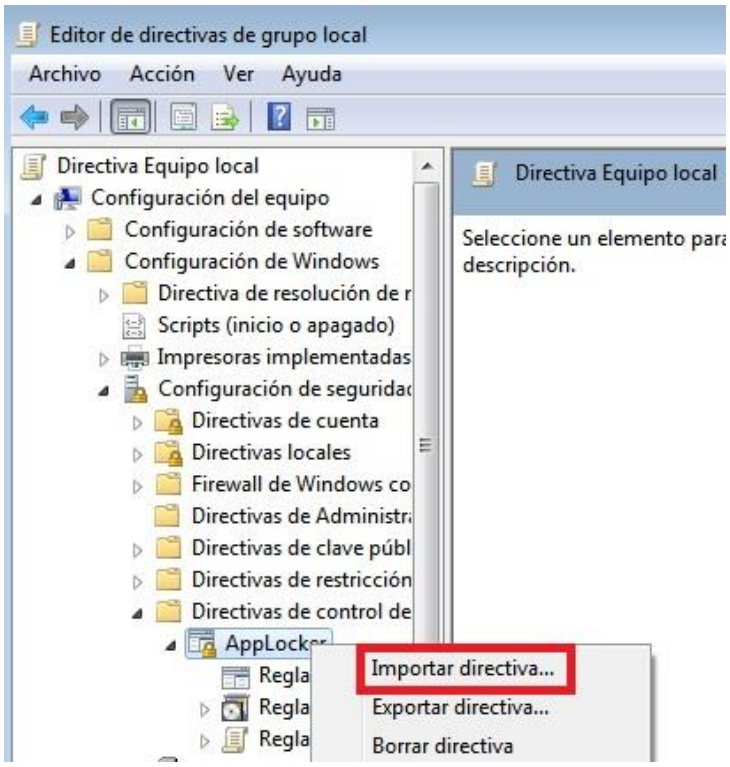
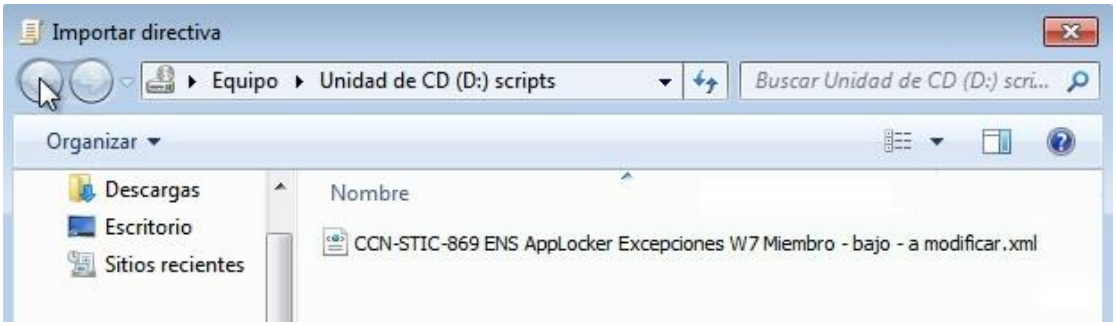
8.	Tras la exportación se presentará el siguiente mensaje informativo.



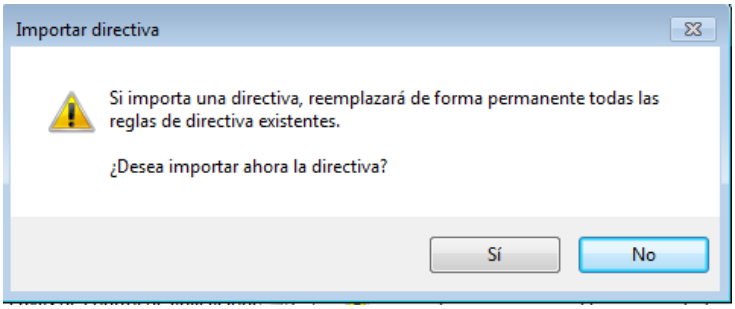
Una vez exportada la política de AppLocker definida en el GPO de excepciones seleccionado, se procederá a la importación de la misma en un equipo de referencia Windows 7 Enterprise que pertenezca al dominio y no reciba reglas de AppLocker por GPO de dominio.

Paso	Descripción
9.	Inicie sesión en la máquina de referencia con un usuario con permisos administrativos.

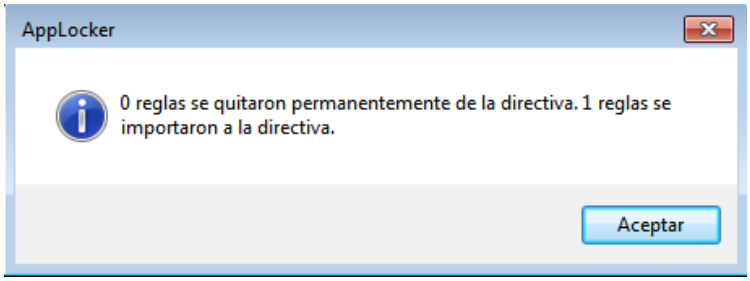
Nota: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.

Paso	Descripción
10.	Traslade el fichero XML recién exportado (CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo – a modificar.xml) a la máquina de referencia. En dicha máquina, haciendo uso de la herramienta “gpedit.msc” proceda a importar la configuración de AppLocker tal y como se indica a continuación. **Nota:** Puede lanzar “GPedit.msc” desde el menú “Ejecutar” de Windows (pulsando la combinación de teclas “Windows + R”).
11.	Una vez abierto el "Editor de administración de directivas de grupo local”, seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Escoja la opción “Importar directiva...” del menú contextual que aparece tras pulsar botón derecho sobre la ubicación señalada arriba. 
12.	En el cuadro de dialogo abierto navegue hasta el directorio donde haya depositado el XML a importar y selecciónelo. Haga doble clic sobre él o pulse sobre el botón “Abrir”. 

Paso	Descripción
13.	Puede que se le solicite confirmación ya que la importación de directivas de AppLocker sobrescribe la configuración actual. Si es así seleccione “Sí”.

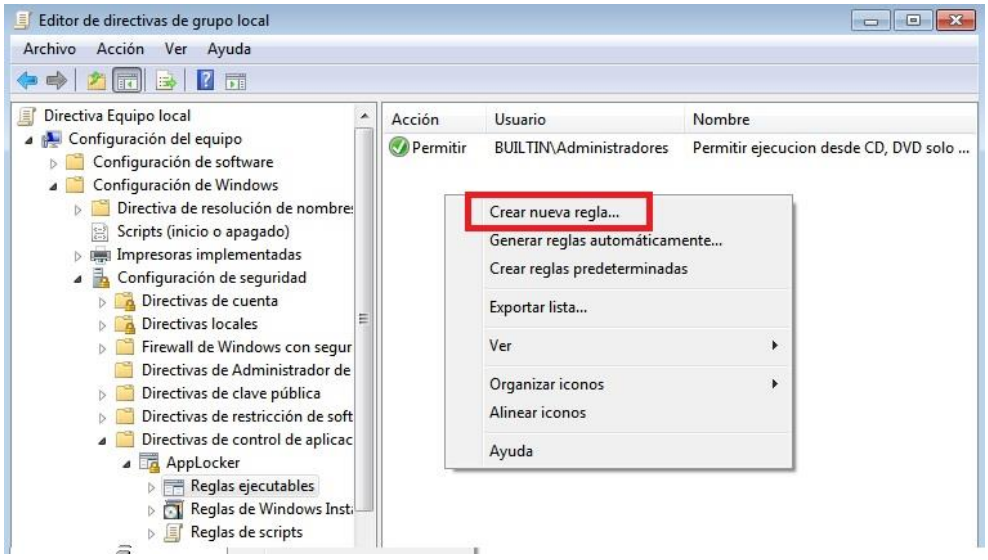


14.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.

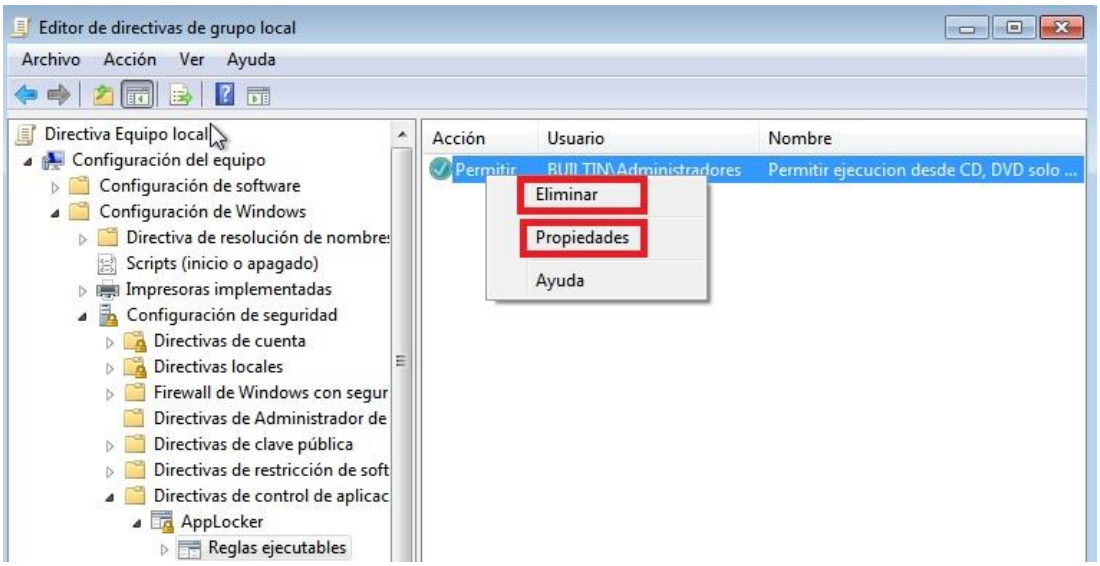


Nota: Se importa una única regla ya que se está usando la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”, que contiene una única regla de excepción para permitir ejecución de binarios ubicados en CD o DVD.

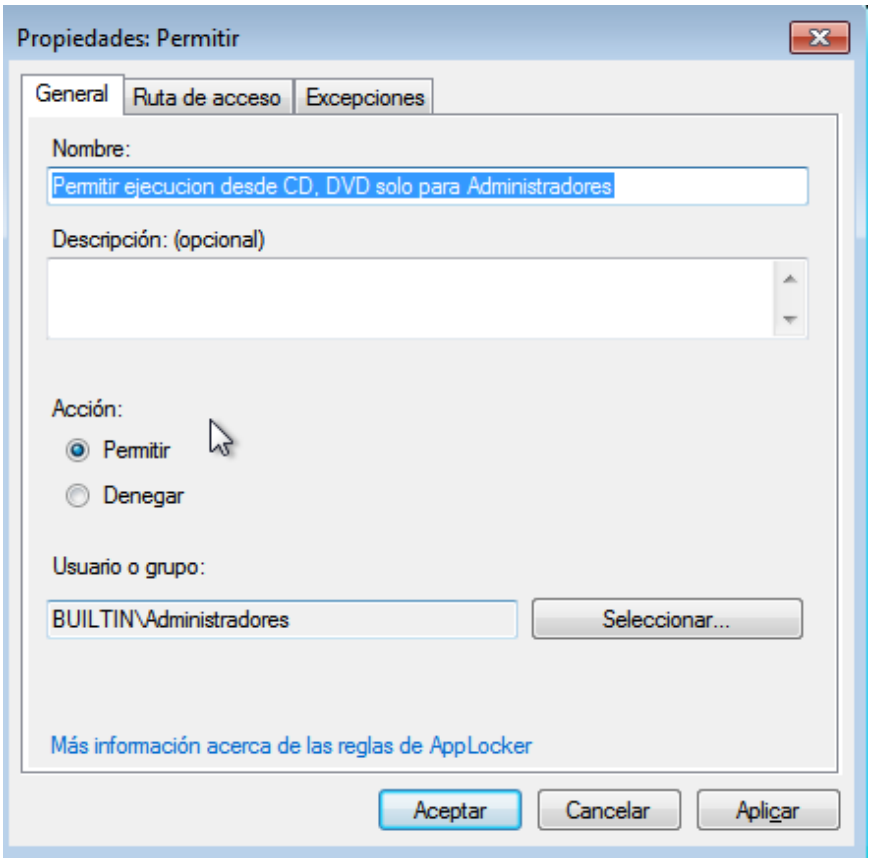
15.	Una vez importada la directiva, haciendo uso del “Editor de directivas de grupo local”, podrá crear o modificar las reglas que considere. Para crear una nueva regla, en el mismo “Editor de directivas de grupo local” navegue hasta la ubicación indicada y elija la opción “Crear nueva regla…” del menú contextual que aparece tras pulsar botón derecho en el panel derecho. **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables**



Paso	Descripción
16.	También puede editar reglas existentes seleccionando la opción “Propiedades” del menú contextual desplegado al pulsar botón derecho sobre la regla. Si quiere eliminar la regla, proceda del mismo modo pero seleccionando la opción “Eliminar”.



Las propiedades muestran una nueva ventana con tres pestañas en la que se puede editar el nombre de la regla, y sus parámetros y excepciones.



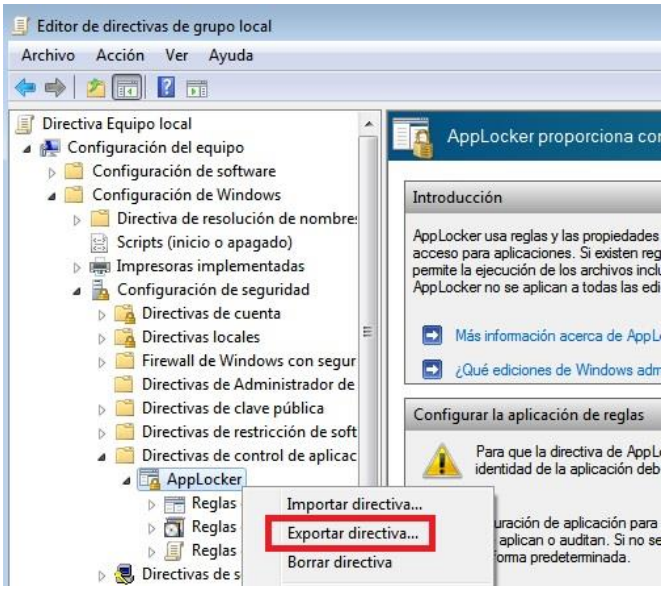
Paso	Descripción

17. Una vez modificadas o creadas las reglas necesarias, proceda a exportar la colección de reglas.

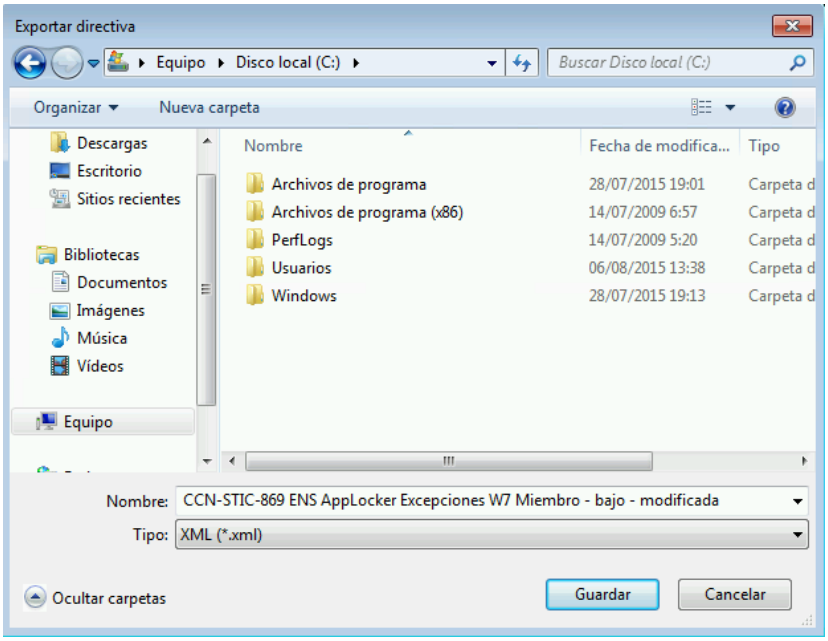
    En el mismo "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación:

    Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

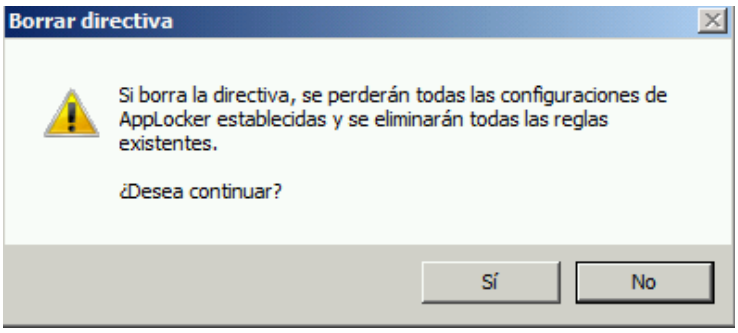
    Elija la opción "Exportar directiva…" del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.



18. En el menú de navegación, seleccione una ubicación con permisos de escritura y guarde la configuración exportada. En este caso se usa el nombre "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml". Pulse el botón "Guardar".

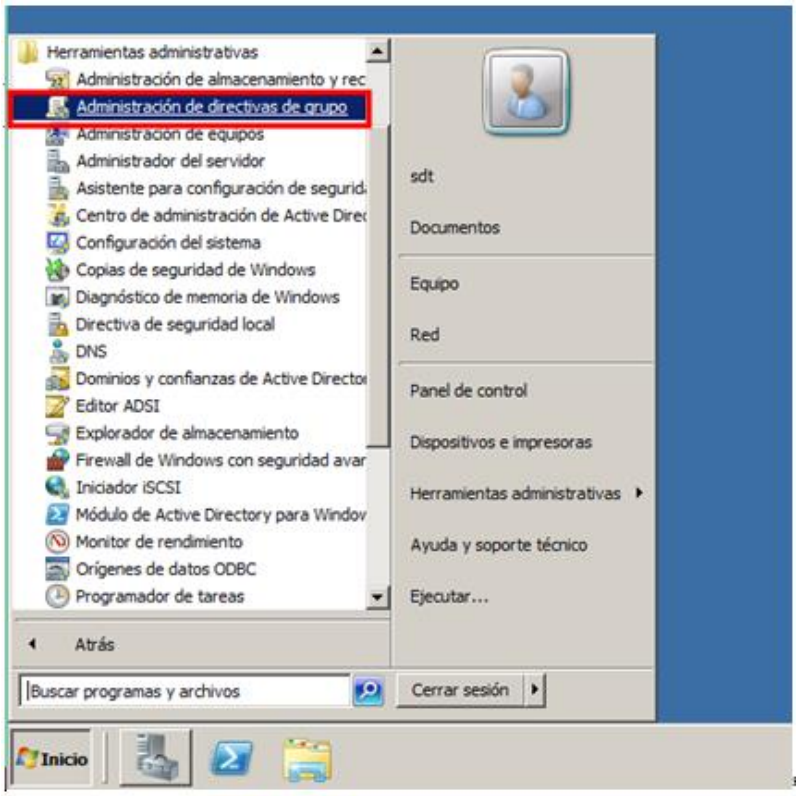


No cierre todavía el Editor de Editor de directivas de grupo local.

Paso	Descripción
19.	Haciendo uso del mismo editor de directivas de grupo local usado para modificar las reglas de AppLocker, proceda a la eliminación de la directiva para dejar así el entorno preparado para una nueva importación y edición de directivas. En el mismo "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Borrar directiva" del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
20.	Pulse "Si" en el cuadro de dialogo abierto. 

Una vez preparada la nueva directiva con las modificaciones necesarias para su entorno, se procederá a la importación de la misma en el GPO de excepciones que aplique a las máquinas que han de recibir las nuevas reglas.

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

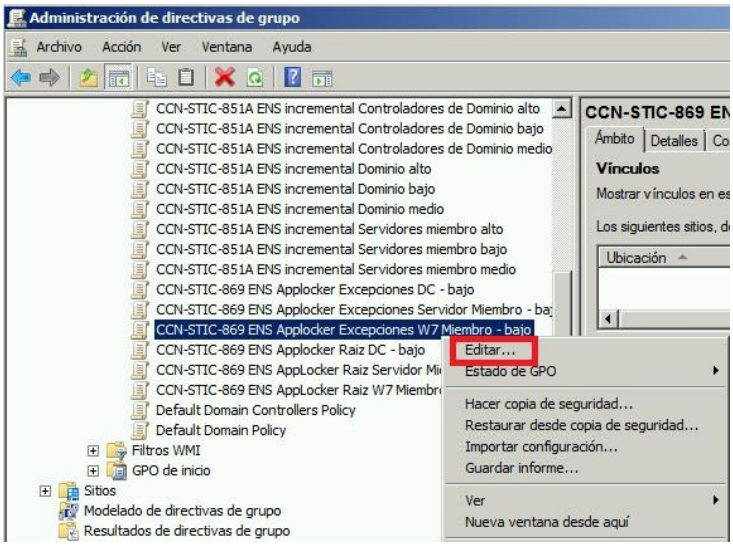
Paso	Descripción
21.	Inicie sesión en el servidor Controlador de Dominio con una cuenta que sea Administrador del Dominio.
22.	Copie el archivo XML exportado de la máquina de referencia al controlador de dominio. En el presente ejemplo se llama “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml”
23.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo** 

Paso	Descripción

24. Seleccione el GPO de excepciones a modificar. En este ejemplo se han editado las reglas de AppLocker definidas en el GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**".

    Navegue hasta el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo**

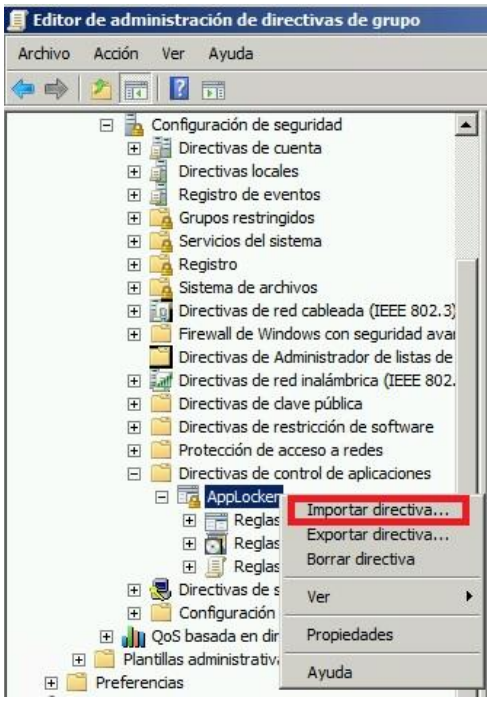
    Marcando con el botón derecho en el GPO, elija la opción "Editar..." del menú contextual que aparecerá.



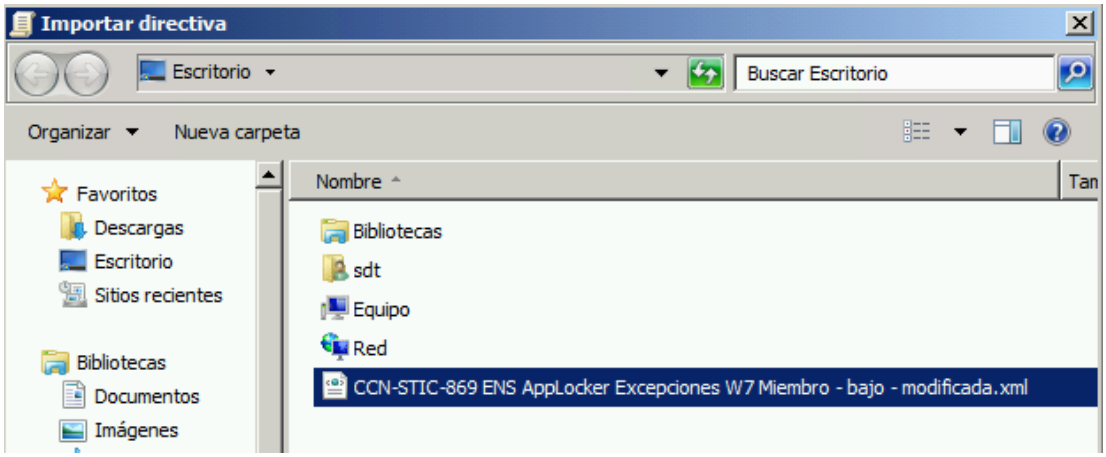
25. En el "Editor de administración de directivas de grupo", seleccione la siguiente ubicación:

    Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

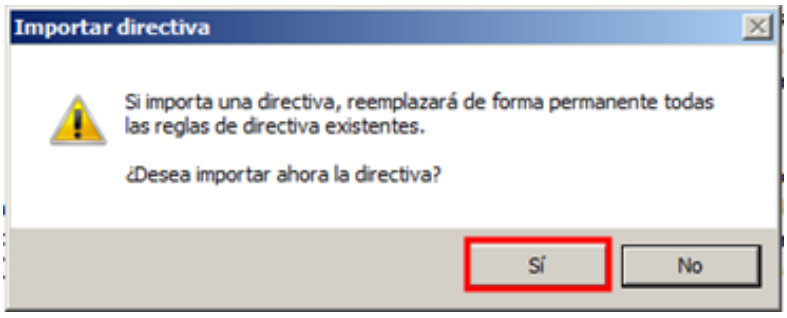
    Elija la opción "Importar directiva..." del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.



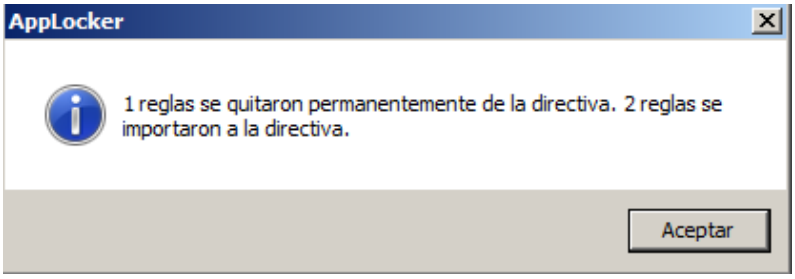
Paso	Descripción
26.	En el cuadro de diálogo abierto, navegue hasta el directorio donde haya depositado el archivo XML previamente modificado en la máquina de referencia, selecciónelo y ábralo haciendo doble clic sobre él o pulsando el botón “Abrir”.



27.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



28.	Aparecerá un nuevo mensaje informativo indicando que se importaron tantas reglas como se hayan creado/modificado reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.



29.	Ya puede cerrar el “Editor de Administración de directivas de grupo” habiendo quedado importadas al GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo**” todas las modificaciones realizadas en la máquina de referencia.

2. PASO A PASO PARA LA CREACIÓN DE REGLA QUE PERMITA EJECUCIÓN DE APLICACIONES DESDE RUTAS NO ESTÁNDARES

De manera predeterminada las aplicaciones se instalan en el directorio “Archivos de Programa”, pero pueden darse casos en los que se disponga de aplicativos instalados fuera de esa ruta, bien por decisión del administrador o por la configuración de la propia aplicación. El siguiente ejemplo simula la permisividad para la ejecución de una aplicación instalada en la carpeta “C:\aplicacion”.

En los siguientes pasos se detalla el procedimiento a seguir para modificar reglas de AppLocker definidas en un GPO existente. La implementación de AppLocker detallada en esta guía, para los distintos niveles del Esquema Nacional de seguridad, se ha diseñado de tal manera que las nuevas reglas o excepciones se han de definir editando los GPO de excepciones.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel bajo del ENS son:

- CCN-STIC-869 ENS AppLocker Excepciones DC – bajo: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán igualmente en modo auditoría.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel medio o alto del ENS son:

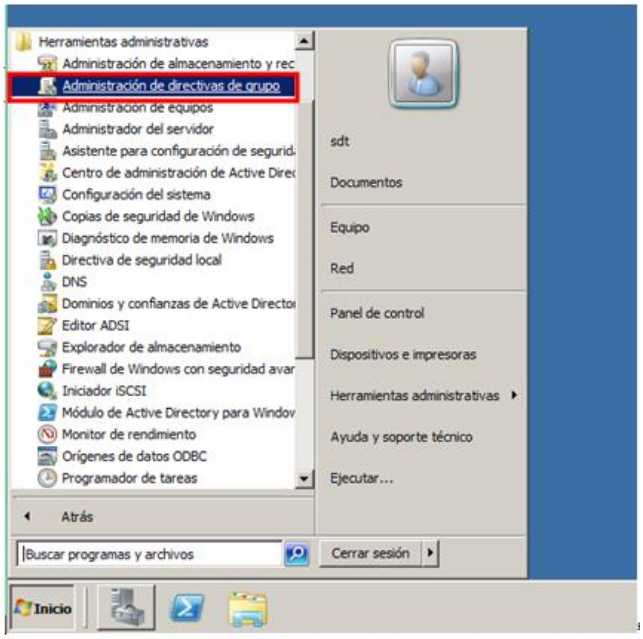
- CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Los pasos que se describen a continuación se realizarán en un controlador de dominio donde se realizará la implementación de las políticas GPO necesarias para permitir la ejecución de aplicaciones desde rutas no estándares.

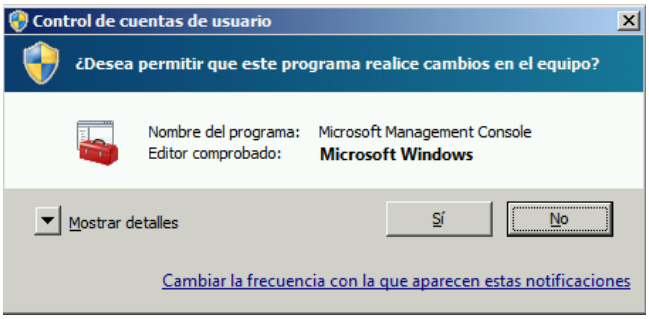
En este caso, se editará el GPO de excepciones que aplica sobre los clientes Windows 7 de la organización para una implementación del Esquema Nacional de Seguridad en nivel bajo a modo de ejemplo. Dependiendo de sus necesidades, deberá adaptar el siguiente procedimiento para que aplique a otras máquinas o niveles de implementación del Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio con una cuenta con derechos de administración en el dominio.

Paso	Descripción
2.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio: **Inicio → Herramientas administrativas → Administración de directivas de grupo**

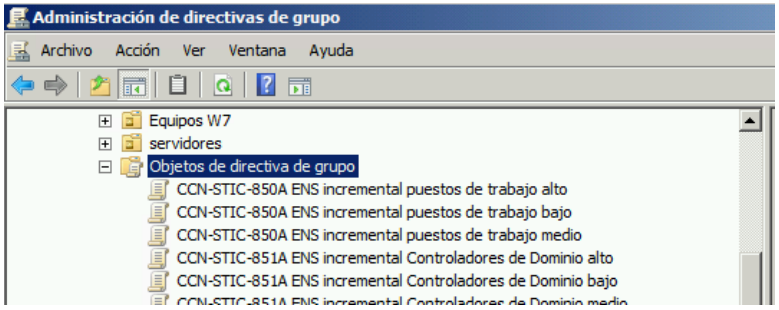


3.	Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos.



Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

4.	Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo,** como se muestra en la siguiente imagen.



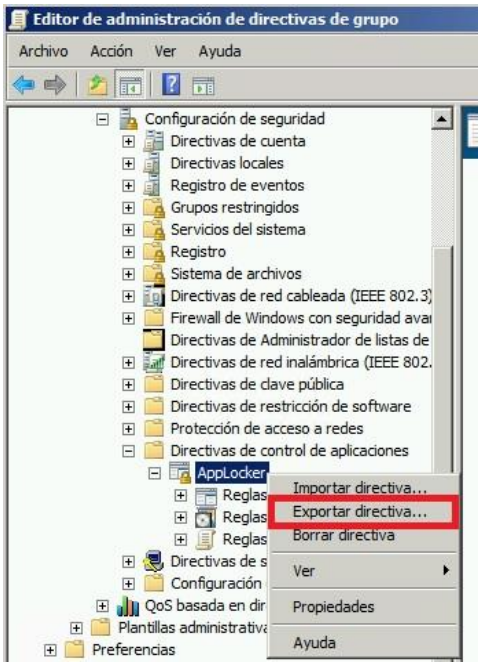
Paso	Descripción

5. Seleccione el GPO de excepciones a modificar. En este ejemplo, se pretende modificar la colección de reglas de AppLocker aplicadas a clientes Windows 7 a los que les aplica el nivel bajo del ENS. Por lo que se procederá a la edición del GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.

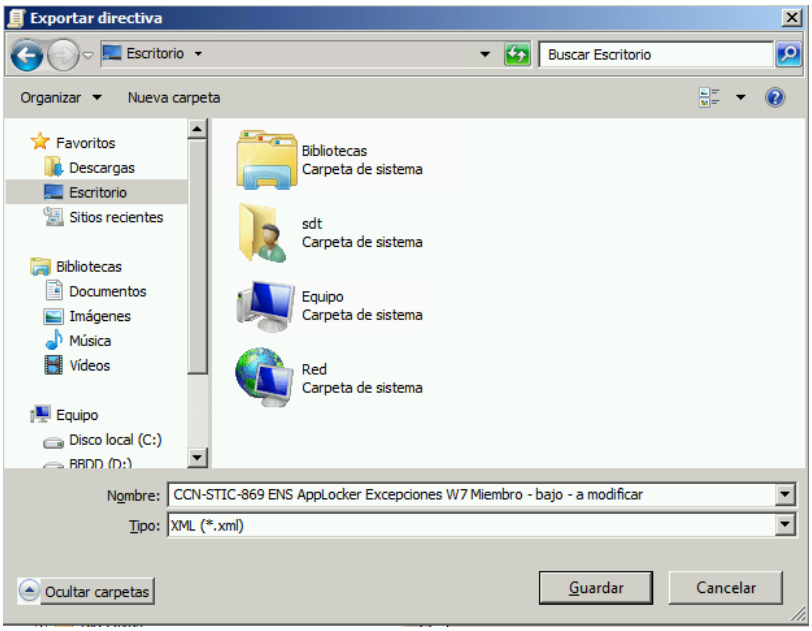
Nota: El GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" está diseñado para recibir las excepciones o nuevas reglas que se quieran aplicar a los Equipos W7 de la organización. Si necesita crear excepciones que apliquen a servidores miembros o a los controladores de dominio, seleccione el GPO adecuado según se describe al comienzo del presente apartado.

6. En el "Editor de administración de directivas de grupo", seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción "**Exportar directiva**".

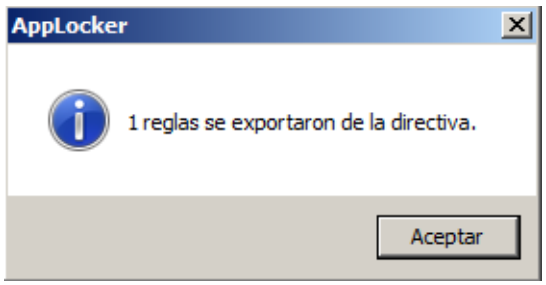
Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker



Paso	Descripción
7.	En el cuadro de diálogo abierto navegue hasta un directorio con permisos de escritura y guarde la política exportada en formato xml. Elija un nombre reconocible.



8.	Tras la exportación se presentará el siguiente mensaje informativo.



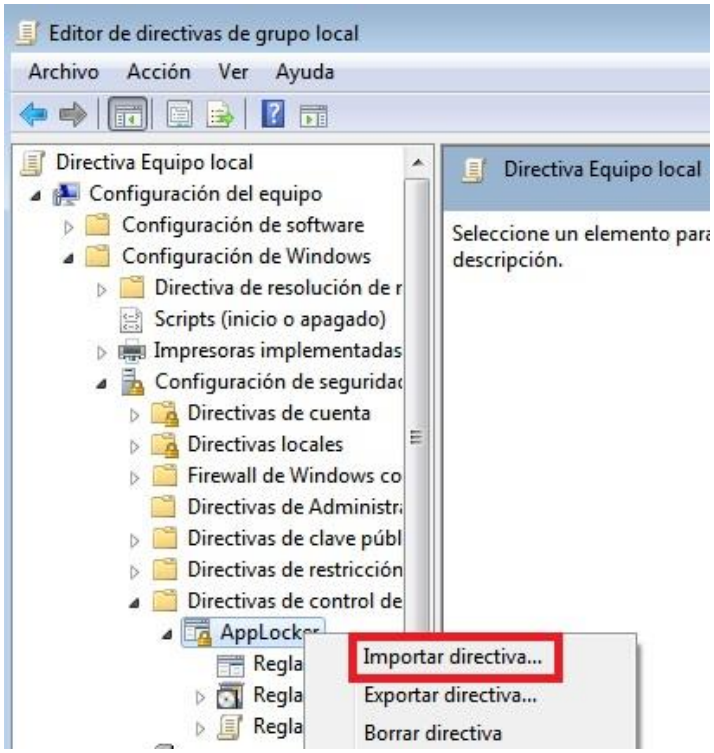
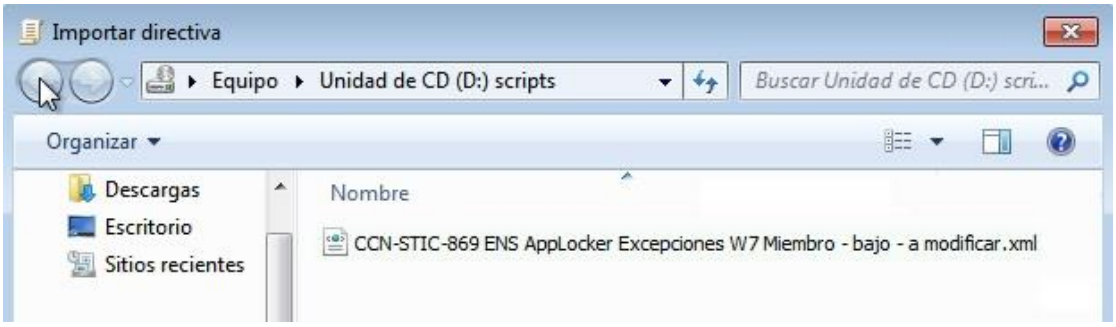
Una vez exportada la política de AppLocker definida en el GPO de excepciones seleccionado, se procederá a la importación de la misma en un equipo de referencia Windows 7 Enterprise que pertenezca al dominio pero no reciba reglas de AppLocker por GPO de dominio.

Paso	Descripción
9.	Inicie sesión en la máquina de referencia con un usuario con permisos administrativos.

Nota: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.

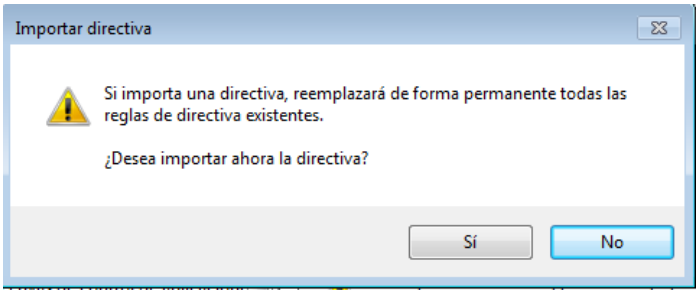
10.	Traslade el fichero XML recién exportado (CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo- a modificar.xml) a la máquina de referencia. En dicha máquina, haciendo uso de la herramienta "**GPedit.msc**" proceda a importar la configuración de AppLocker tal y como se indica a continuación.

Nota: Puede lanzar "GPedit.msc" desde el menú "Ejecutar" de Windows (pulsando la combinación de teclas "Windows + R").

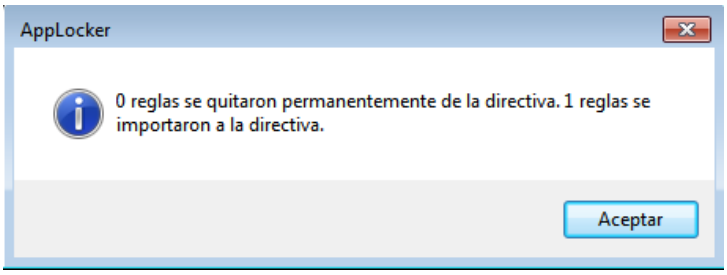
Paso	Descripción
11.	Una vez abierto el "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Escoja la opción "Importar directiva..." del menú contextual que aparece tras pulsar botón derecho sobre la ubicación señalada arriba.  **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.
12.	En el cuadro de dialogo abierto navegue hasta el directorio donde haya depositado el archivo XML a importar y selecciónelo. Haga doble clic sobre él o pulse el botón "Abrir". 

Paso	Descripción

13. Puede que se le solicite confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Si es así seleccione “Sí”.



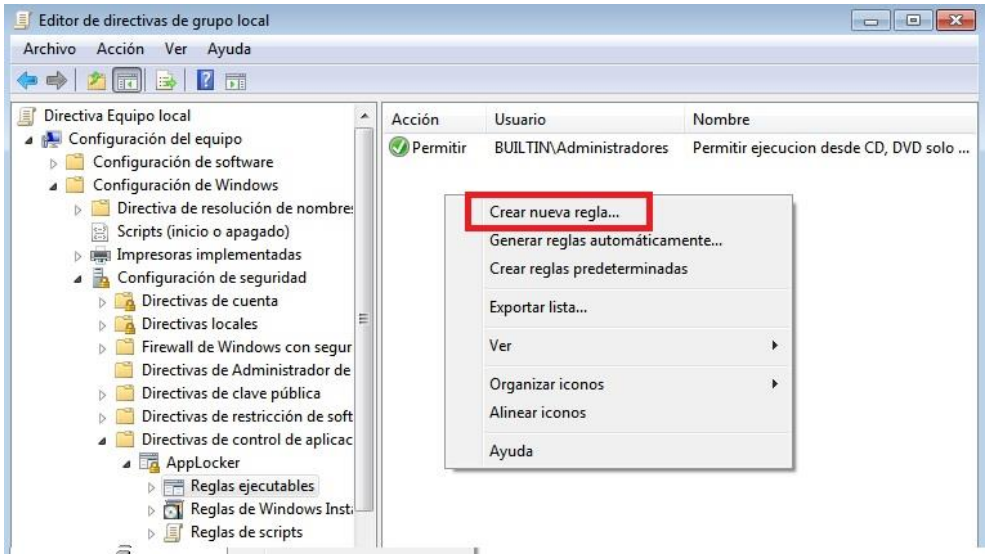
14. Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker.



Nota: Se importa una única regla ya que se está usando la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”, que contiene una única regla de excepción para permitir ejecución de binarios ubicados en CD o DVD.

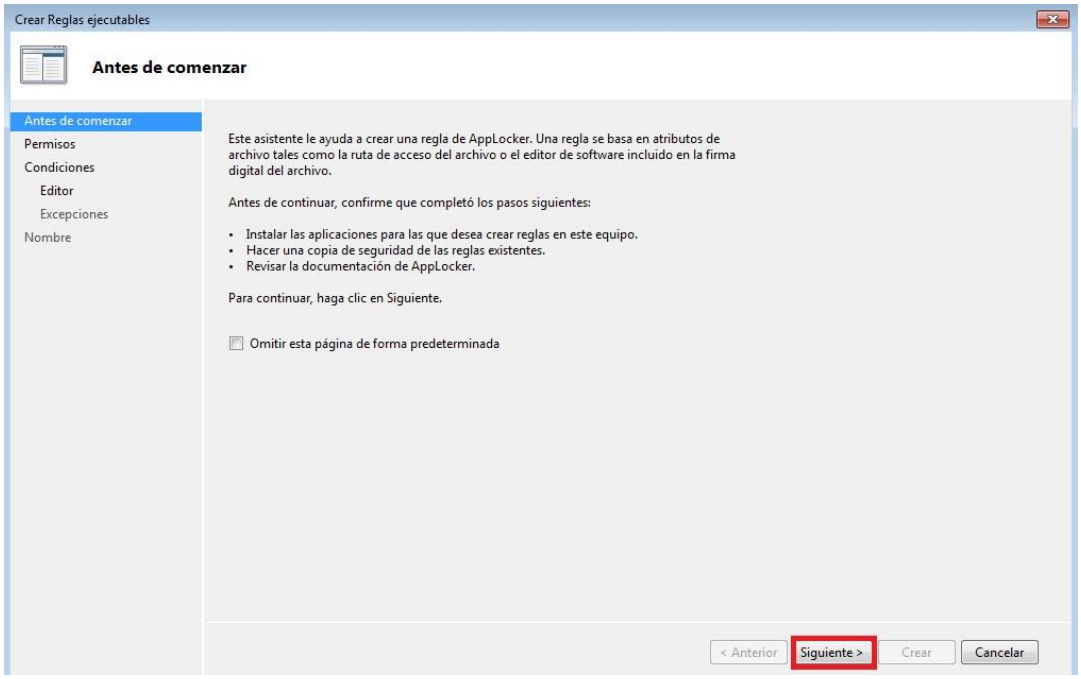
15. Para crear una nueva regla, en el “Editor de directivas de grupo local” navegue hasta la ubicación indicada y seleccione la opción “Crear nueva regla” del menú contextual que aparece tras pulsar botón derecho en el panel derecho.

Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



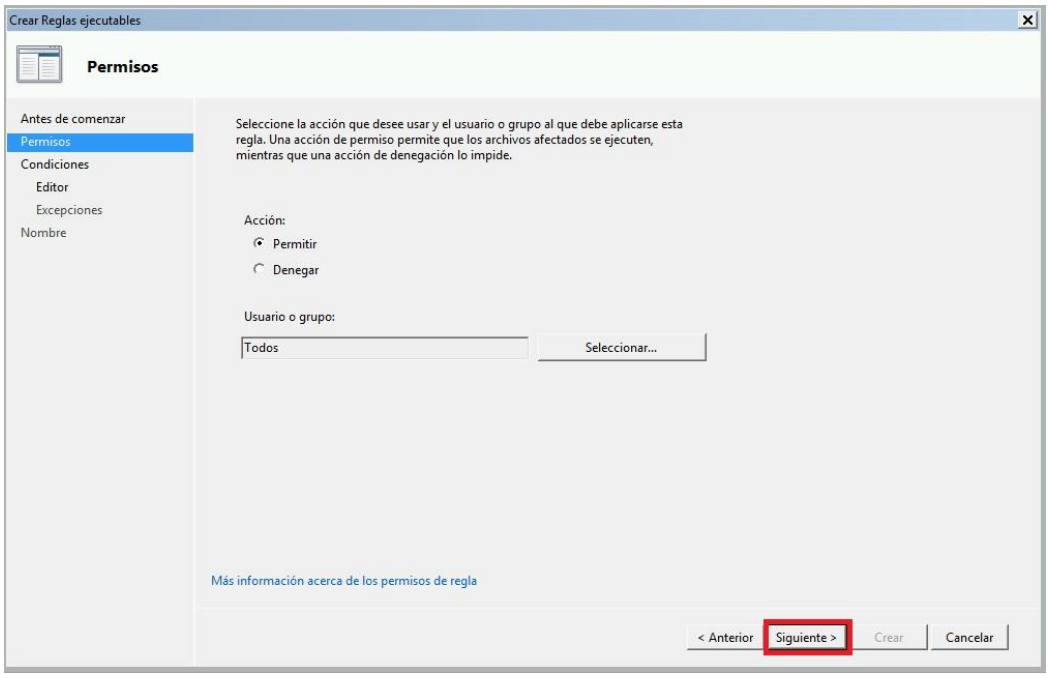
Paso	Descripción

16. En la primera pantalla del asistente desplegado pulsar sobre el botón siguiente.



17. En el siguiente menú se debe seleccionar el tipo de regla (permiso o denegación) y los usuarios o grupos de usuarios a los que aplicará.

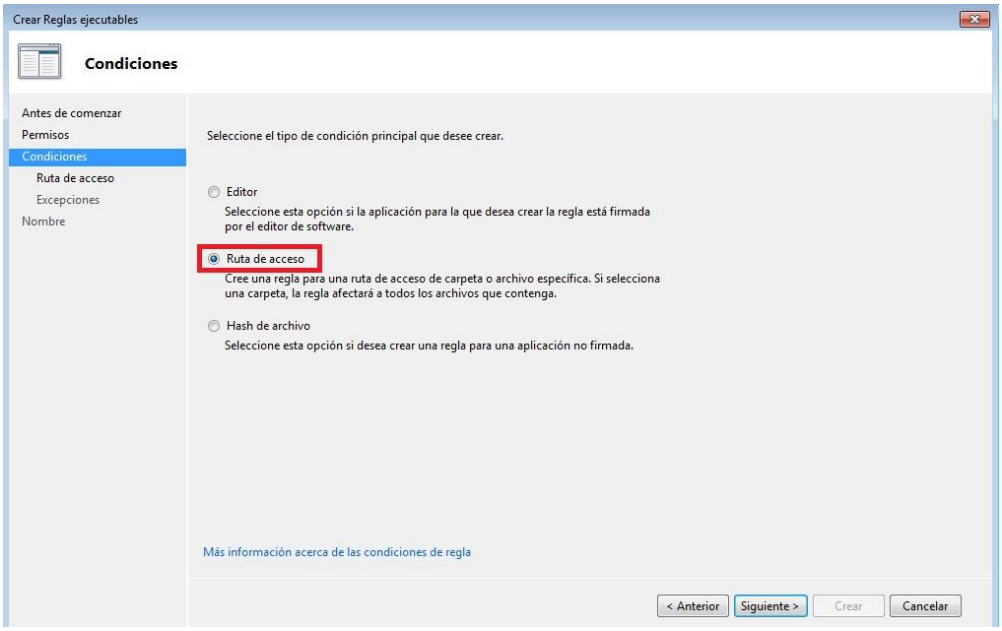
    Mantenga la configuración existente y pulse “Siguiente>”.



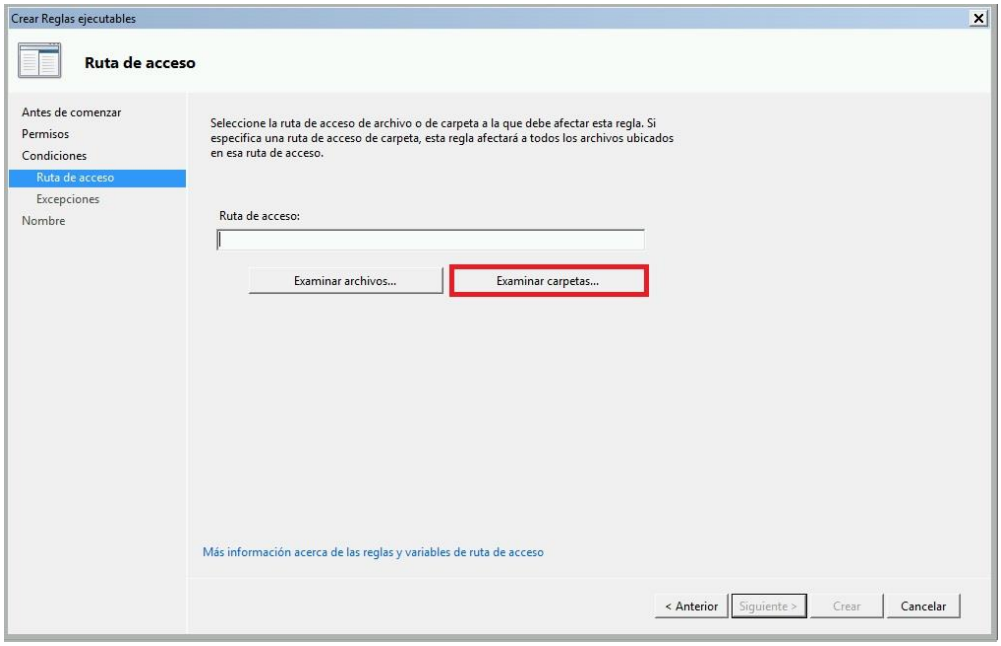
Nota: Si quiere puede restringir el permiso de ejecución a ciertos usuarios o grupos. En este caso, se mantiene el permiso para todos ya que se asume que se va a permitir una aplicación que usarán todos los usuarios de la organización.

Paso	Descripción

18. En la siguiente ventana, escoja la condición de la regla. En este caso seleccione “Ruta de acceso” y pulse “Siguiente>”.



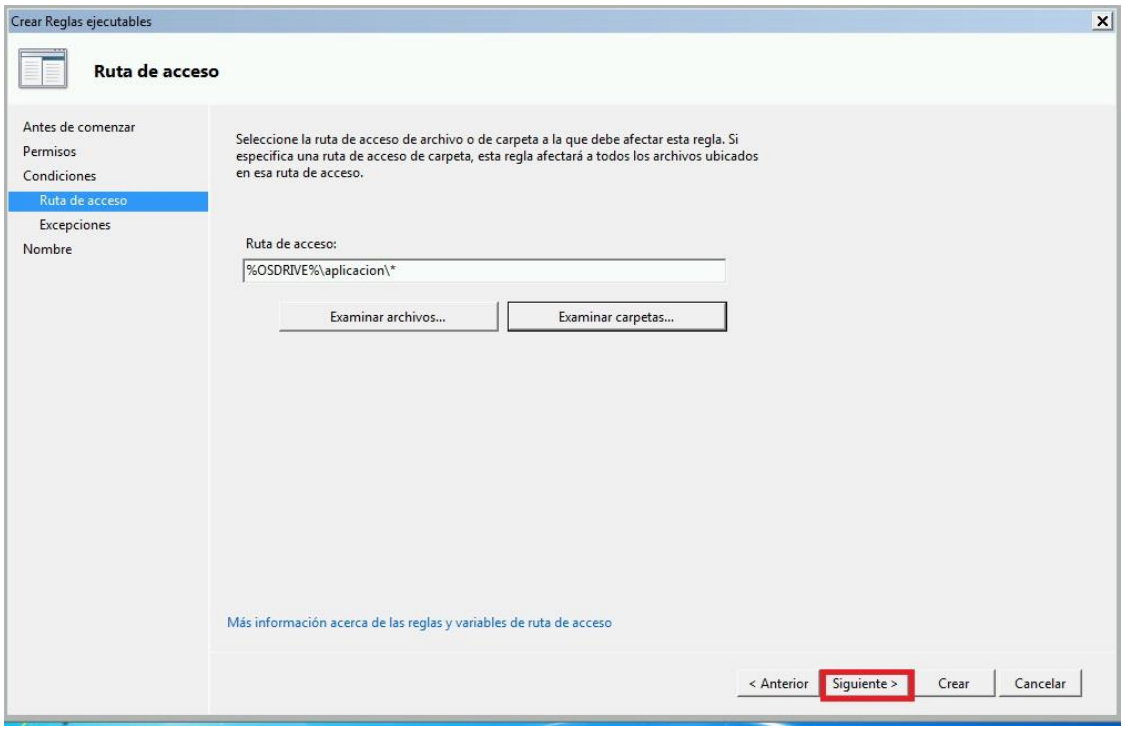
19. En la pantalla “Ruta de acceso” pulse el botón “Examinar carpetas…”.



Nota: El ejemplo mostrado simula que se va a permitir ejecutar contenido de una carpeta. Si solo fuera a ejecutar un único archivo .exe de dicha carpeta, se debería emplear la opción “Examinar archivos…” y seleccionar el único fichero ejecutable. Debe tener en consideración que las aplicaciones actuales son altamente complejas y puede que la carga de la aplicación se realice a través de un fichero .exe, pero este luego llame o dependa de otros ejecutables. Si tiene claro que la aplicación solo va a necesitar llamar a un fichero ejecutable, puede seleccionar la opción examinar archivos, de lo contrario deberá emplear el mecanismo de examinar carpetas para permitir la ejecución de todo el contenido de dicha carpeta.

Paso	Descripción
20.	Seleccione la carpeta de la que desee crear la excepción. En el ejemplo se establece que el contenido ejecutable se encuentra en la carpeta “C:\aplicacion”.

21.	Una vez agregada la carpeta, pulse el botón “Siguiente >”.

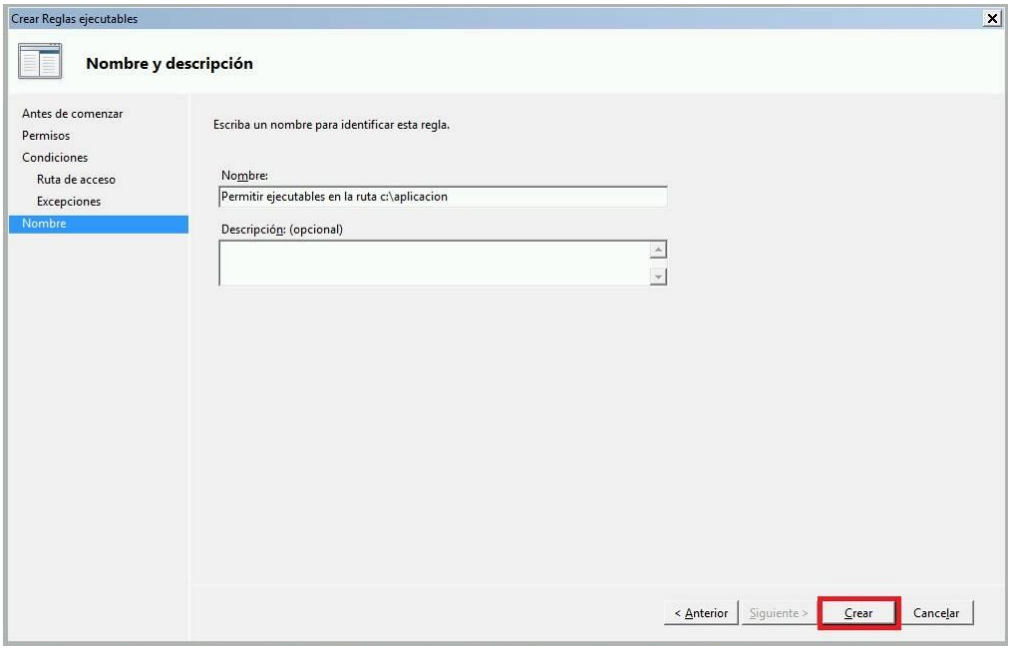


22.	Si desea que algún contenido específico en dicha carpeta no sea ejecutado, podrá agregar una excepción en la pantalla de “Excepciones”. Bien cuando haya agregado las excepciones o si no desea realizar ninguna, pulse el botón “Siguiente >”.

Paso	Descripción

23. Para finalizar, deberá asignar un nombre identificativo a la regla. En el ejemplo se asignará el nombre “Permitir ejecutables en la ruta c:\aplicacion”.

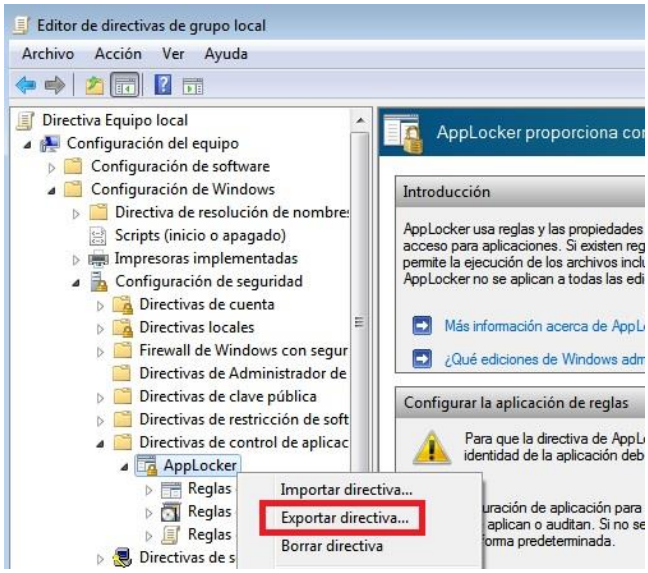
    Pulse el botón “Crear” cuando haya asignado un nombre.



24. Una vez creada la nueva regla, en el mismo "Editor de directivas de grupo local”, seleccione la siguiente ubicación:

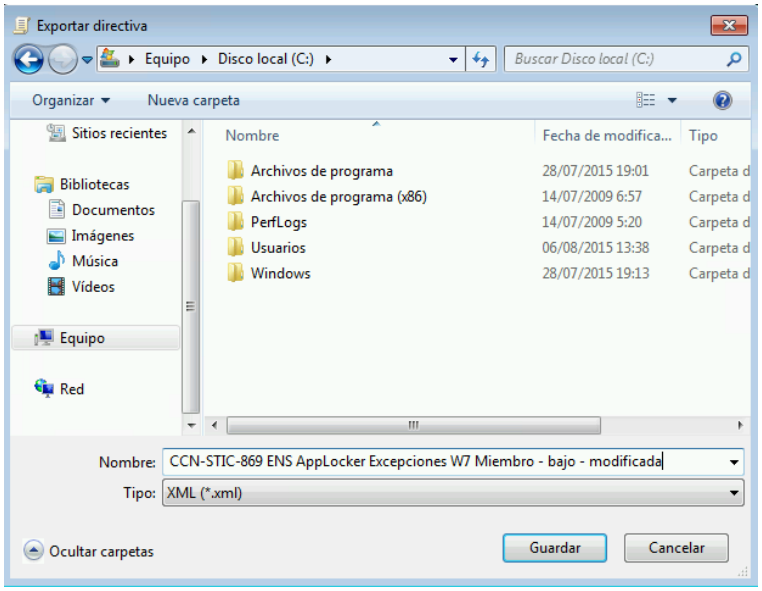
    Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

    Elija la opción “Exportar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.



Paso	Descripción

25. En el menú de navegación, seleccione una ubicación con permisos de escritura y guarde la configuración exportada. En este caso se usa el nombre “CCN-STIC-869 ENS AppLocker Excepciones W7 – bajo - modificada.xml”.



Nota: No cierre todavía el “Editor de directivas de grupo local”.

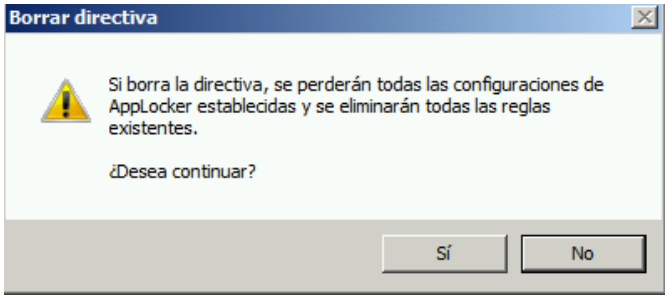
26. Haciendo uso del mismo editor de directivas de grupo local usado para modificar las reglas de AppLocker, proceda a la eliminación de la directiva para dejar así el entorno preparado para una nueva importación y edición de directivas.

    En el mismo "Editor de administración de directivas de grupo local”, seleccione la siguiente ubicación:

    Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

    Elija la opción “Borrar directiva” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.

Paso	Descripción
27.	Pulse “Si” en el cuadro de dialogo abierto.

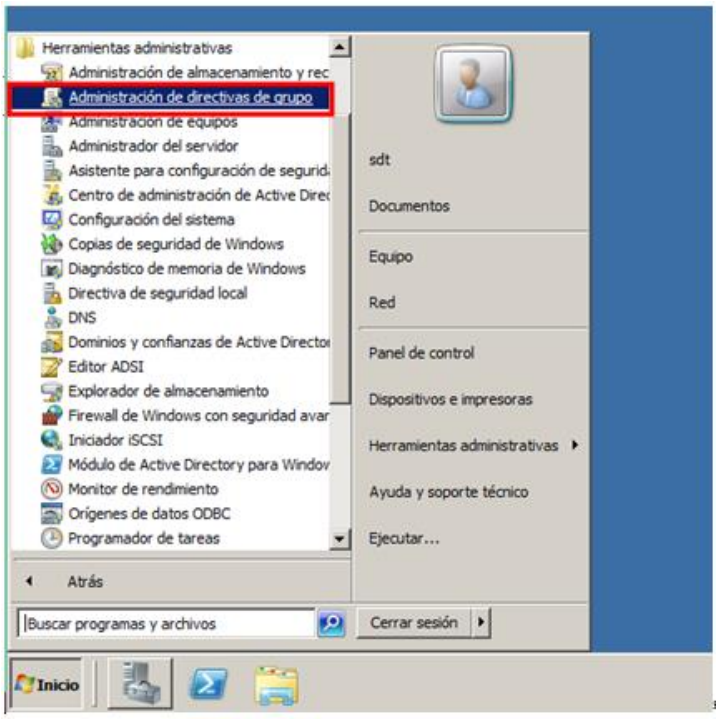


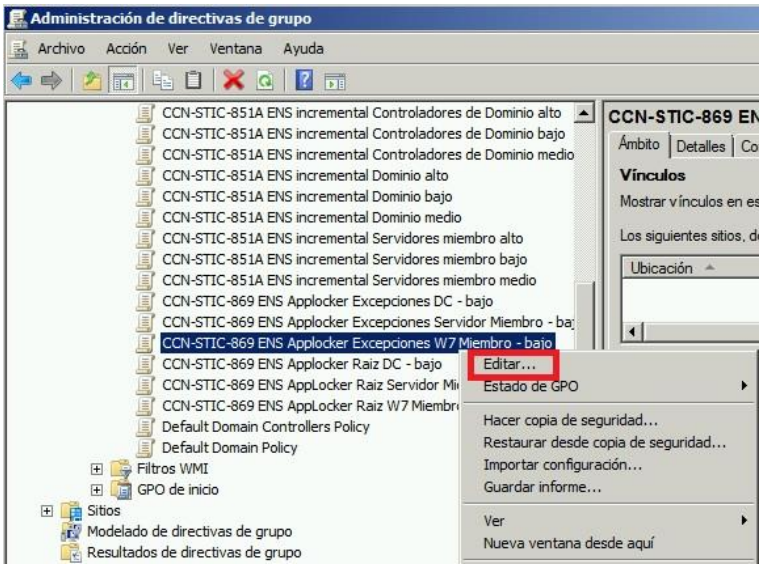
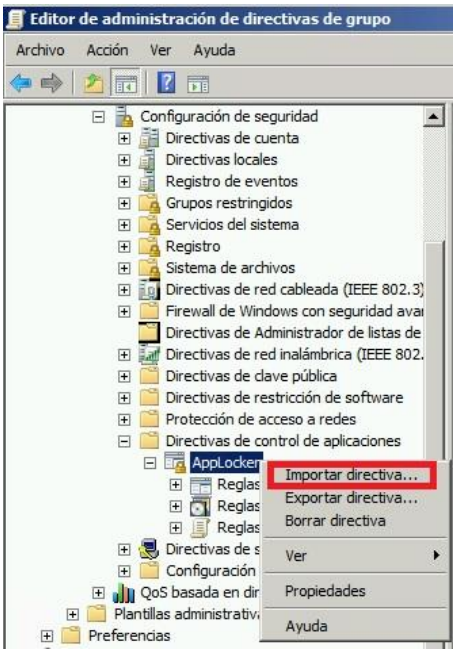
28.	Ya puede cerrar la ventana del “editor de directivas de grupo local”.

Una vez preparada la nueva directiva con las modificaciones necesarias para su entorno, se procederá a la importación de la misma en el GPO de excepciones que aplique a las máquinas que han de recibir las nuevas reglas.

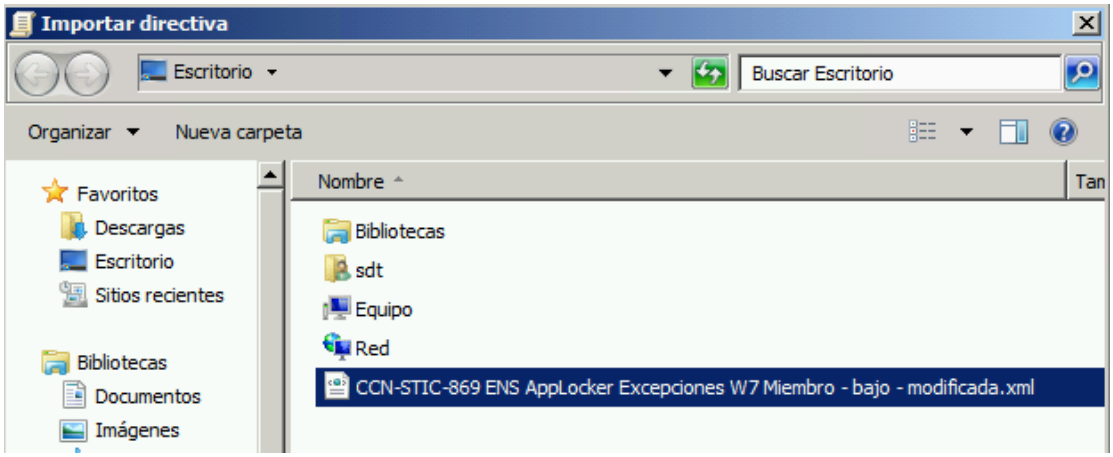
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias

Paso	Descripción
29.	Inicie sesión en el servidor Controlador de Dominio con una cuenta que sea Administrador del Dominio.
30.	Copie el archivo XML exportado de la máquina de referencia al controlador de dominio. En el presente ejemplo se llama “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml”
31.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo**

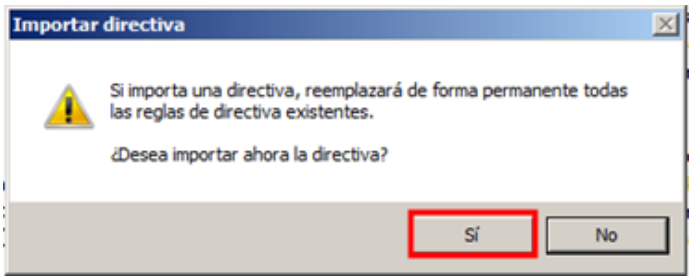


Paso	Descripción
32.	Seleccione el GPO de excepciones a modificar. En este ejemplo se han editado las reglas de AppLocker definidas en el GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Navegue hasta el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo** Marcando con el botón derecho en el GPO, elija la opción "Editar..." del menú contextual que aparecerá. 
33.	En el "Editor de administración de directivas de grupo", seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Importar directiva..." del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 

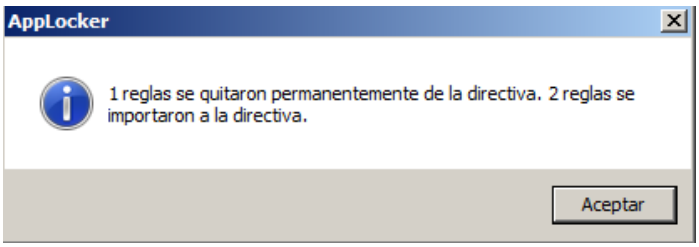
Paso	Descripción
34.	En el cuadro de diálogo abierto navegue hasta el directorio donde haya depositado el archivo XML previamente modificado en la máquina de referencia, selecciónelo y ábralo haciendo doble clic sobre él o pulsando el botón “Abrir”.

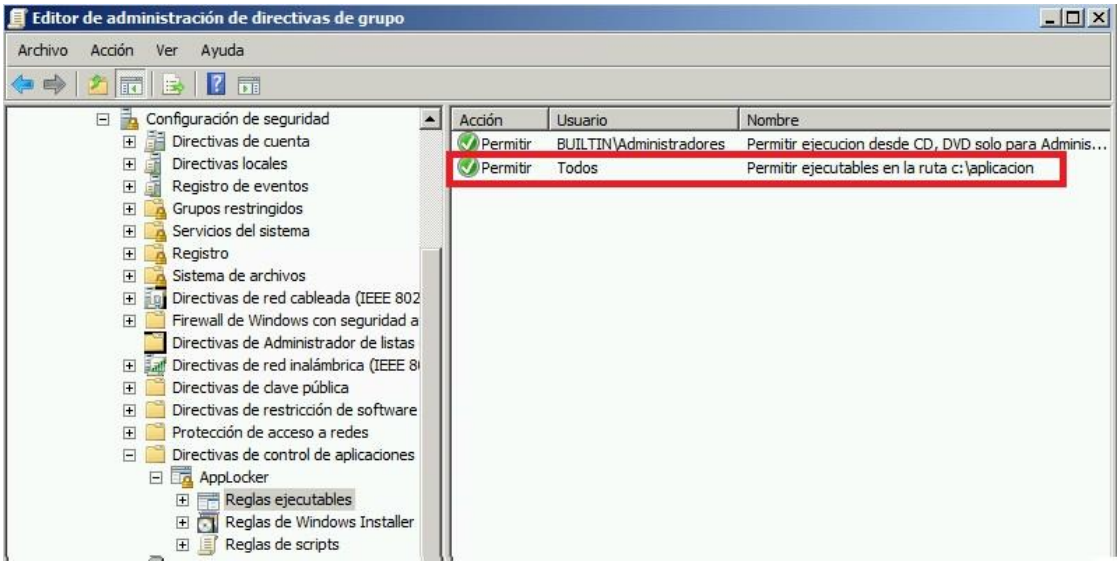


35.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



36.	Aparecerá un nuevo mensaje informativo indicando que se importaron tantas reglas como se hayan creado/modificado reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.



Paso	Descripción
37.	En el “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe en el menú que la nueva regla “Permitir ejecutables en la ruta “C:\aplicacion” se ha creado de manera correcta. 
38.	Ya puede cerrar el “Editor de Administración de directivas de grupo” habiendo quedado importadas al GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo**” todas las modificaciones realizadas en la máquina de referencia
39.	Los clientes Windows 7 recogerán la política de manera automática. No obstante puede reiniciarlos para forzar el cambio.

3. PASO A PASO PARA LA CREACIÓN DE REGLA QUE PERMITA EJECUCIÓN DESDE UNIDADES FLASH O USB

En la siguiente tabla, se detalla el procedimiento a seguir para la creación de una nueva regla que permita la ejecución de binarios desde dispositivos Flash o USB.

La implementación de AppLocker detallada en esta guía, para los distintos niveles del Esquema Nacional de Seguridad, se ha diseñado de tal manera que las nuevas reglas o excepciones se han de definir editando los GPO de excepciones.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel bajo del ENS son:

- CCN-STIC-869 ENS AppLocker Excepciones DC – bajo: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

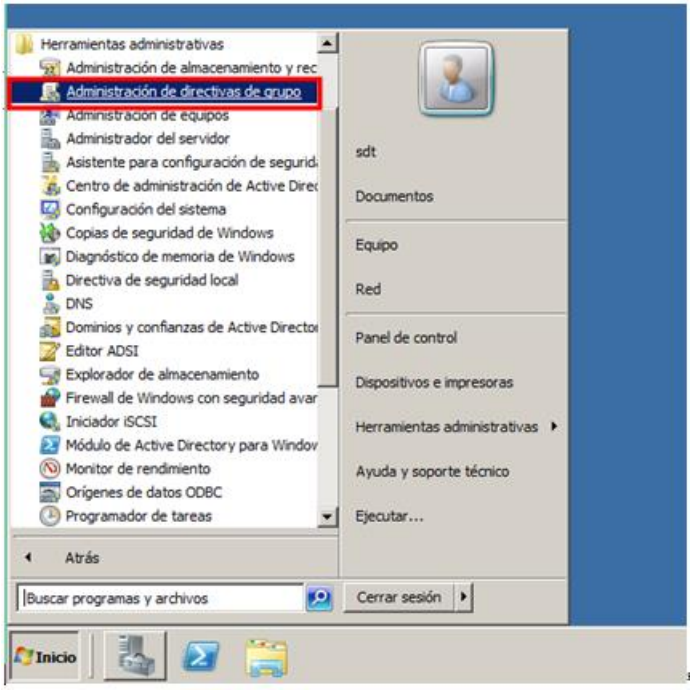
Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán igualmente en modo auditoría.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel medio o alto del ENS son:

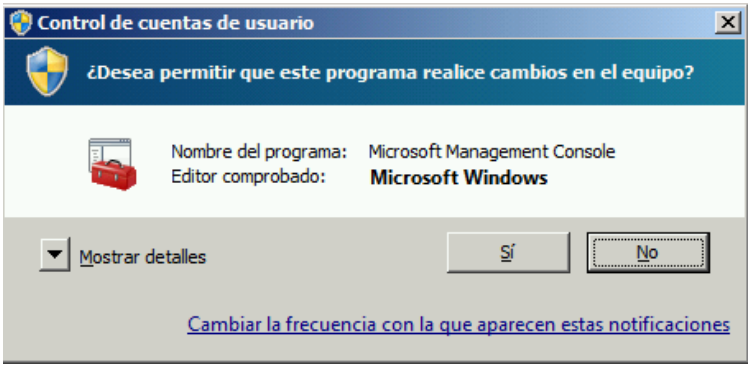
- CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Los pasos que se describen a continuación, se realizarán en un controlador de dominio donde se realizará la implementación de las políticas GPO necesarias para permitir la ejecución de aplicaciones desde rutas no estándares.

En este caso y a modo de ejemplo, se editará el GPO de excepciones que aplica sobre los clientes Windows 7 de la organización para una implementación del Esquema Nacional de Seguridad en nivel bajo. Dependiendo de sus necesidades deberá adaptar el siguiente procedimiento para que aplique a otras máquinas o niveles de implementación del Esquema Nacional de Seguridad.

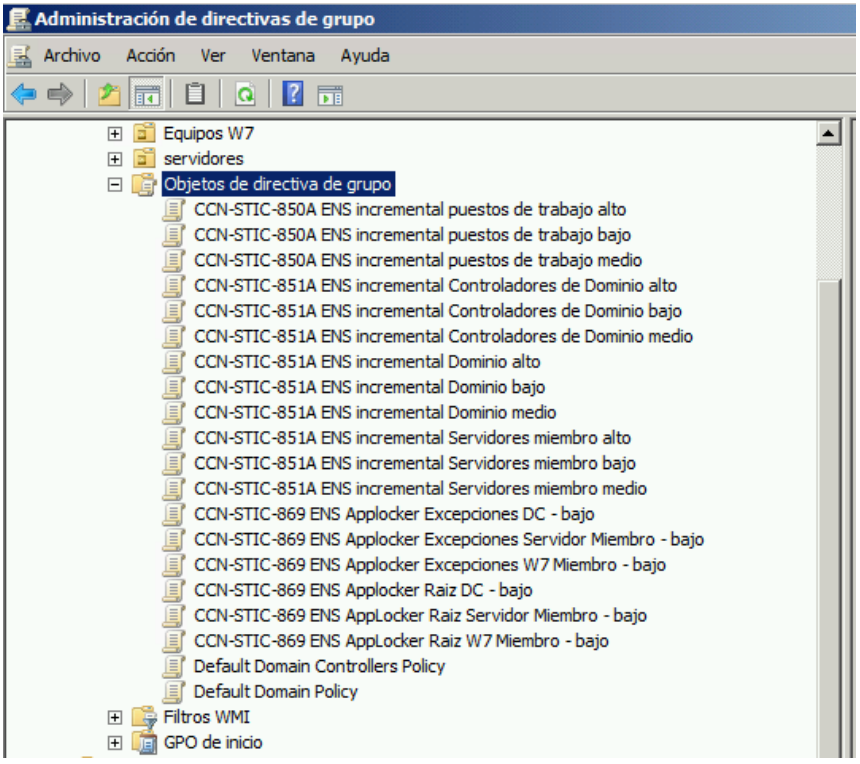
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio con una cuenta con derechos de administración en el dominio.
2.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio: **Inicio → Herramientas administrativas → Administración de directivas de grupo** 

Paso	Descripción
3.	Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos.



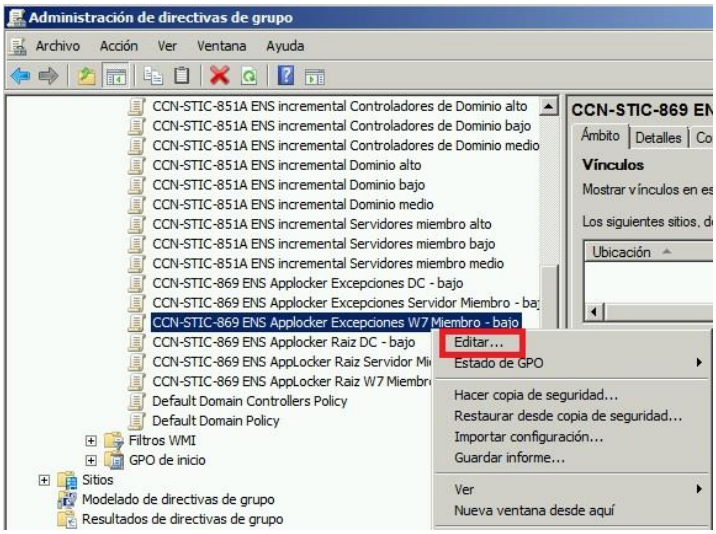
Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

4. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo,** como se muestra en la siguiente imagen.



Paso	Descripción

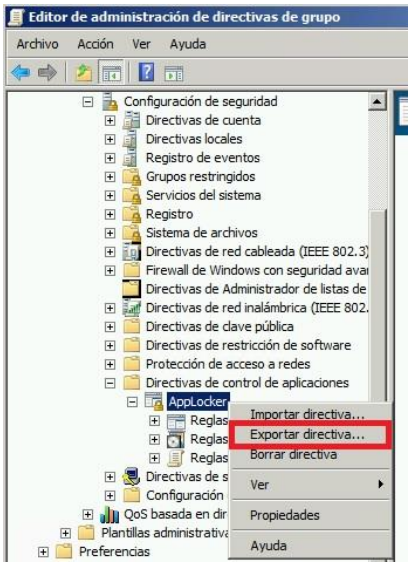
5. Seleccione el GPO de excepciones a modificar. En este ejemplo, se pretende modificar la colección de reglas de AppLocker aplicadas a clientes Windows 7 a los que les aplica el nivel bajo del ENS. Por lo que se procederá a la edición del GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.



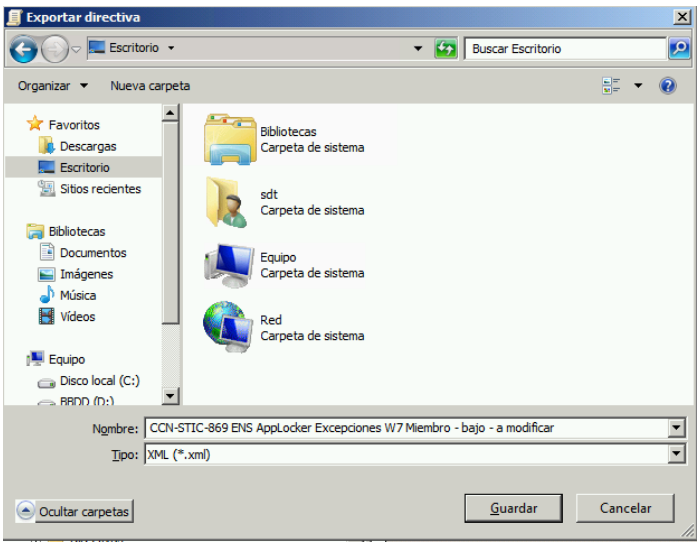
Nota: El GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" está diseñado para recibir las excepciones o nuevas reglas que se quieran aplicar a los Equipos W7 de la organización. Si necesita crear excepciones que apliquen a servidores miembros o a los controladores de dominio, seleccione el GPO adecuado según se describe al comienzo del presente apartado.

6. En el "Editor de administración de directivas de grupo" seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción "**Exportar directiva**".

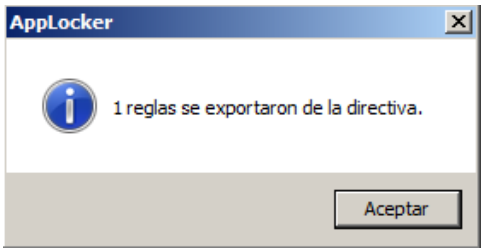
Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker



Paso	Descripción
7.	En el cuadro de diálogo abierto navegue hasta un directorio con permisos de escritura y guarde la política exportada en xml. Elija un nombre reconocible.

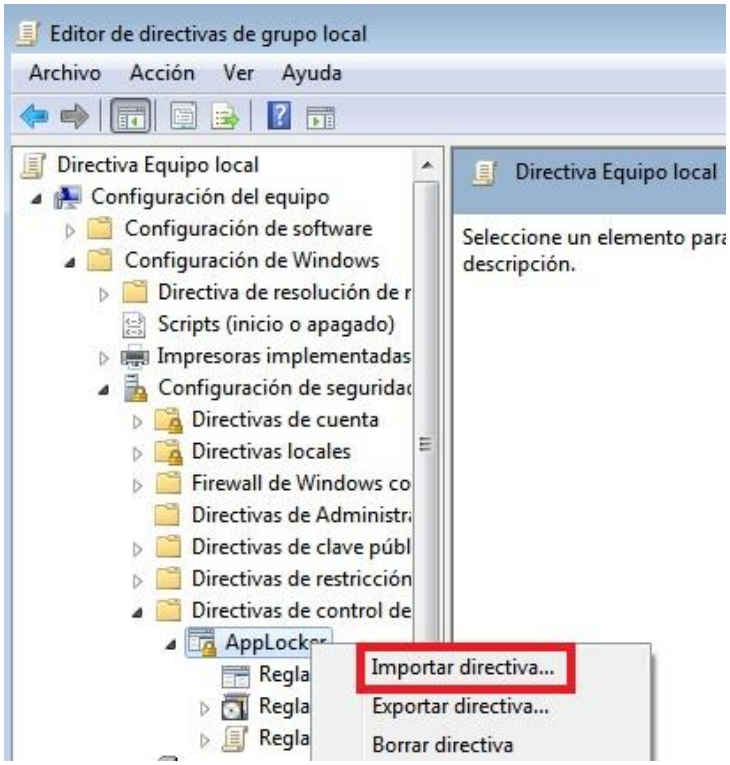
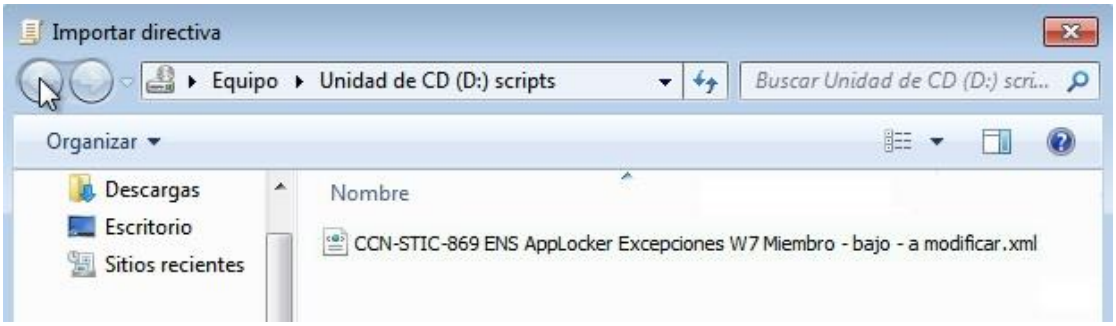


8.	Tras la exportación se presentará el siguiente mensaje informativo.



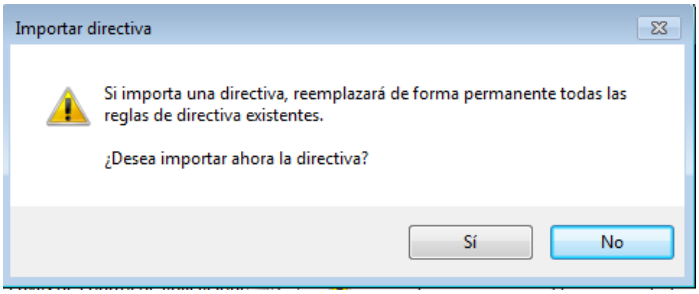
Una vez exportada la política de AppLocker definida en el GPO de excepciones seleccionado, se procederá a la importación de la misma en un equipo de referencia Windows 7 Enterprise que pertenezca al dominio pero no reciba reglas de AppLocker por GPO de dominio.

Paso	Descripción
9.	Inicie sesión en la máquina de referencia con un usuario con permisos administrativos. **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.
10.	Traslade el fichero XML recién exportado (CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo- a modificar.xml) a la máquina de referencia. En dicha máquina, haciendo uso de la herramienta "**GPedit.msc**" proceda a importar la configuración de AppLocker tal y como se indica a continuación. **Nota:** Puede lanzar "GPedit.msc" desde el menú "Ejecutar" de Windows (pulsando la combinación de teclas "Windows + R").

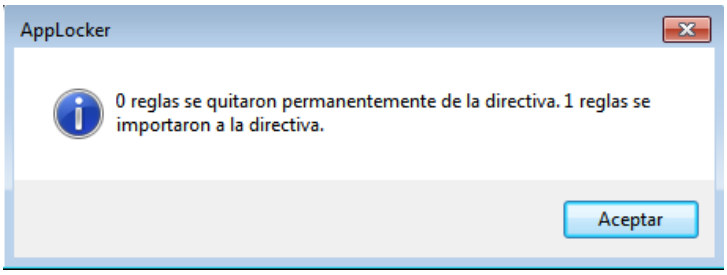
Paso	Descripción
11.	Una vez abierto el "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Escoja la opción "Importar directiva..." del menú contextual que aparece tras pulsar botón derecho sobre la ubicación señalada arriba.  **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.
12.	En el cuadro de dialogo abierto, navegue hasta el directorio donde haya depositado el archivo XML a importar y selecciónelo haciendo doble clic sobre él o pulsando el botón "Abrir". 

Paso	Descripción

13. Puede que se le solicite confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Si es así seleccione “Sí”.



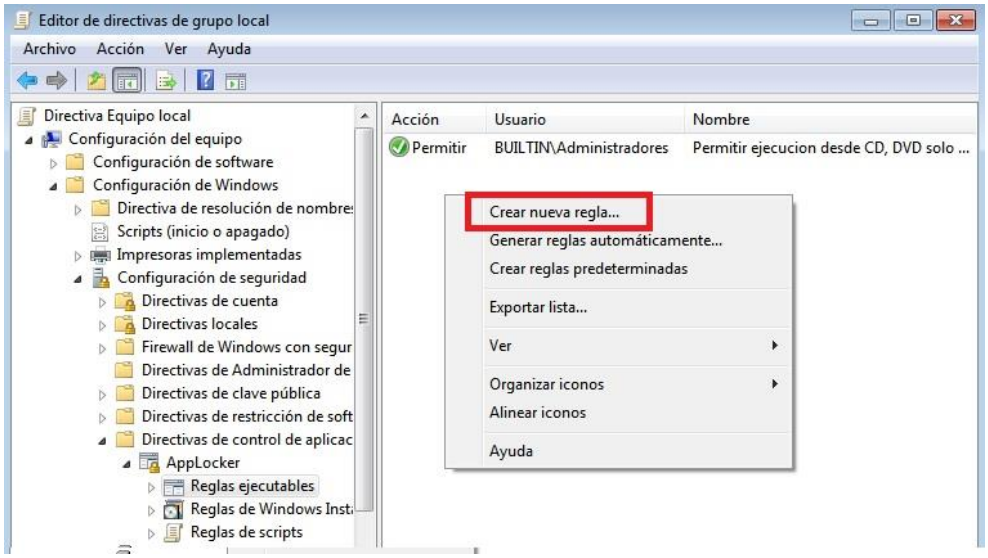
14. Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar el mensaje.



Nota: Se importa una única regla ya que se está usando la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”, que contiene una única regla de excepción para permitir ejecución de binarios ubicados en CD o DVD.

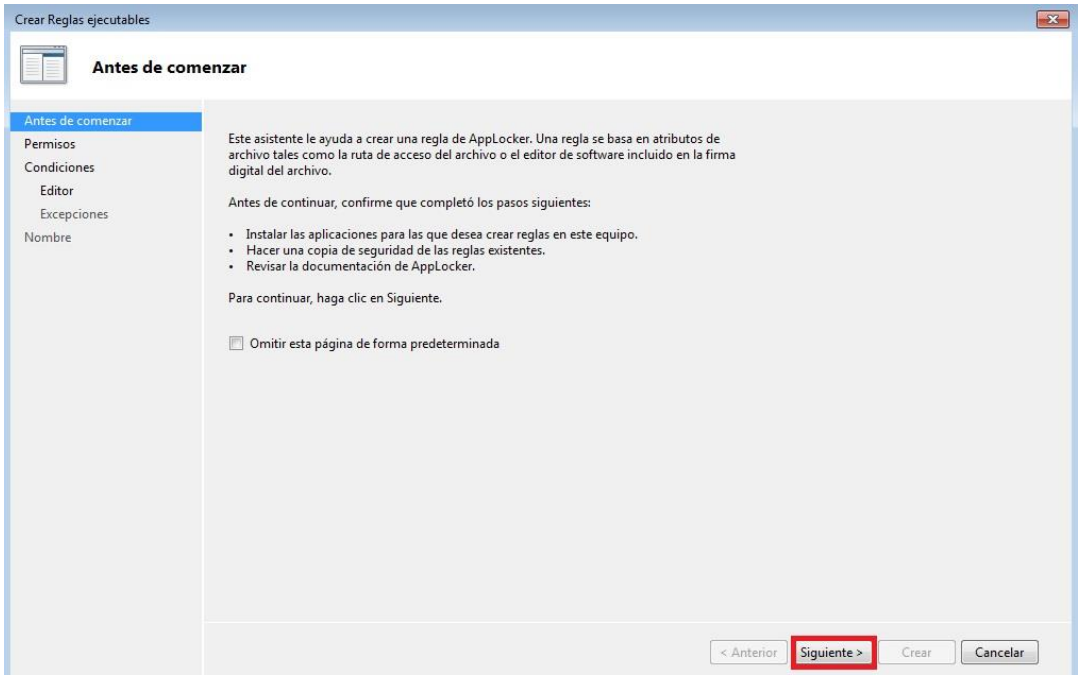
15. Para crear una nueva regla, en el “editor de directivas de grupo local” navegue hasta la ubicación indicada y seleccione la opción “crear nueva regla” del menú contextual que aparece tras pulsar botón derecho en el panel derecho.

Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



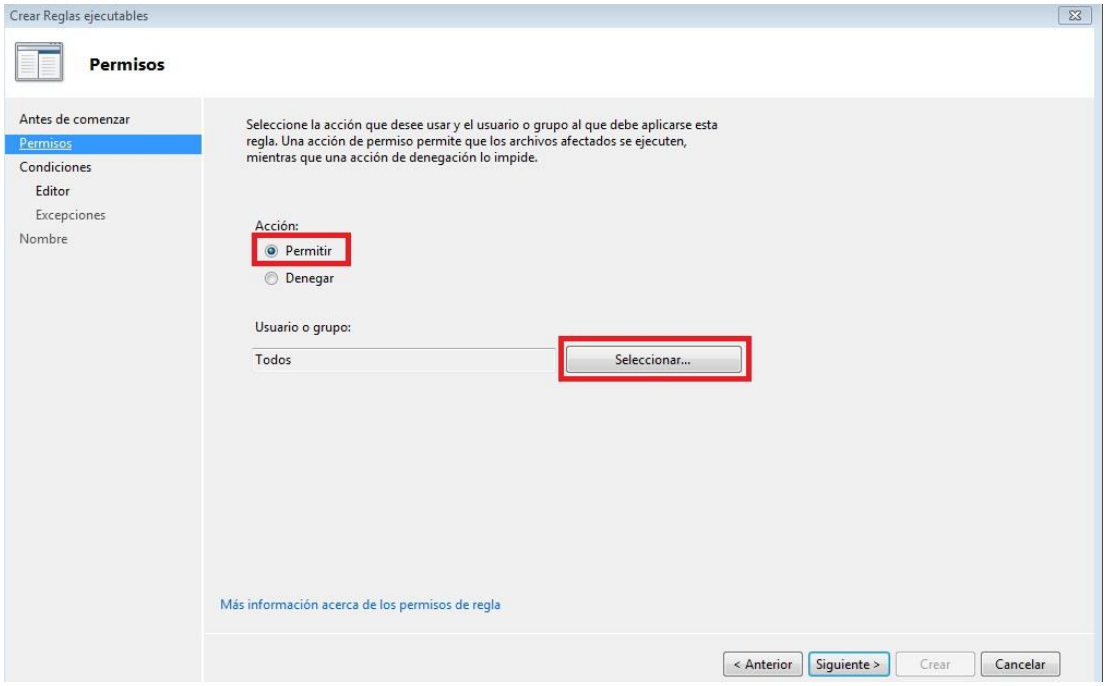
Paso	Descripción

16. En la primera pantalla del asistente desplegado pulsar sobre el botón siguiente.



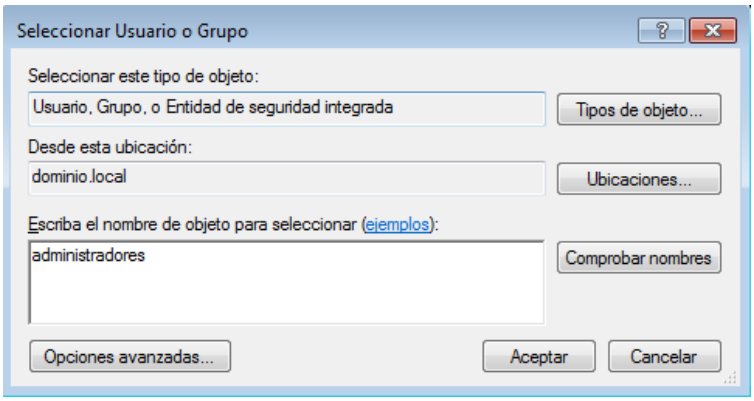
17. En el siguiente menú se debe seleccionar el tipo de regla (permiso o denegación) y los usuarios o grupos de usuarios a los que aplicará.

    En éste caso se selecciona la opción “Permitir” y a continuación se pulsa el botón “Seleccionar…” para poder elegir los usuarios a los que aplicará la nueva regla.



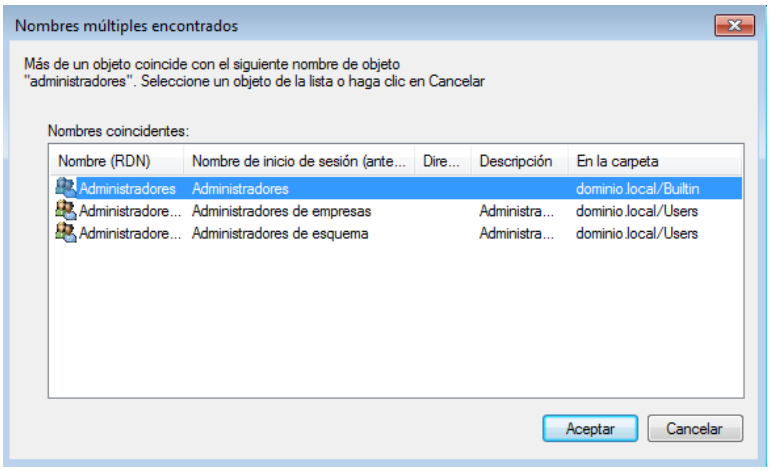
Paso	Descripción

18. En la ventana de abierta escriba “administradores” en el cuadro de texto y pulse en comprobar nombres.

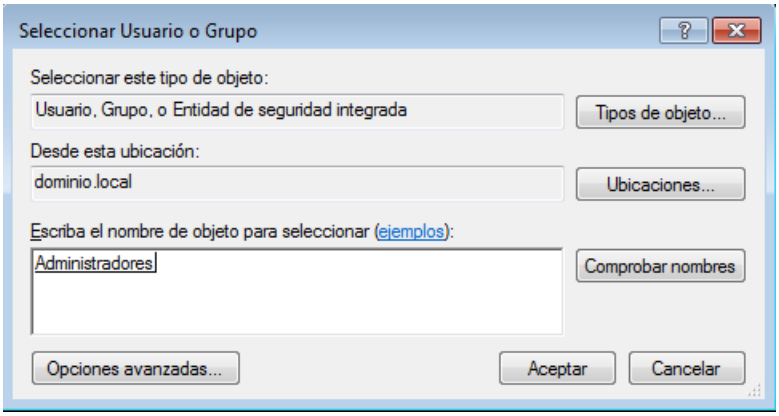


Nota: En este caso, se escoge el grupo de administradores. Elija el grupo o el usuario al que se le va a proporcionar permiso para ejecutar binarios desde USB o Flash.

19. Se abrirá una nueva ventana que mostrará todos los grupos que contienen la palabra “administradores”. Seleccione el grupo “Administradores” y pulse “Aceptar”.

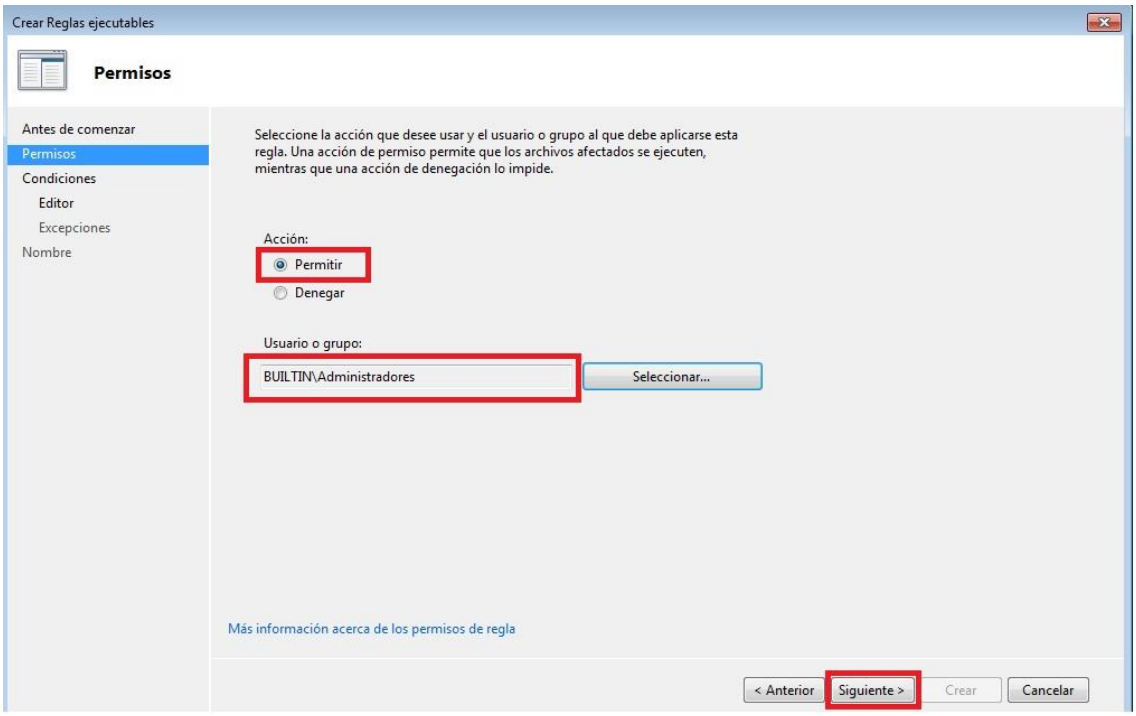


20. Pulse “Aceptar” en la ventana “Seleccionar Usuario o Grupo”.

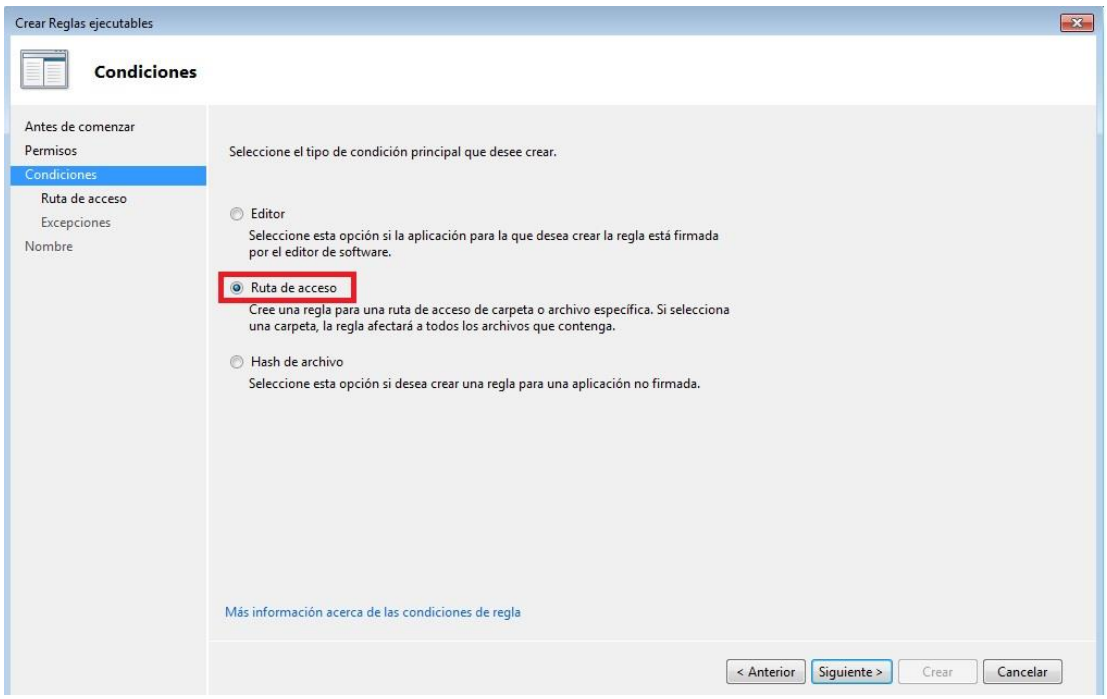


Nota: Asegúrese de que está buscando los usuarios y grupos del dominio. En el campo “Desde esta ubicación” deberá de aparecer el nombre del dominio de la organización.

Paso	Descripción
21.	En la ventana “Crear Reglas ejecutables”, compruebe que la acción seleccionada es “Permitir” y el grupo es “BUILTIN\Administradores” y si es así, pulse “Siguiente >”.

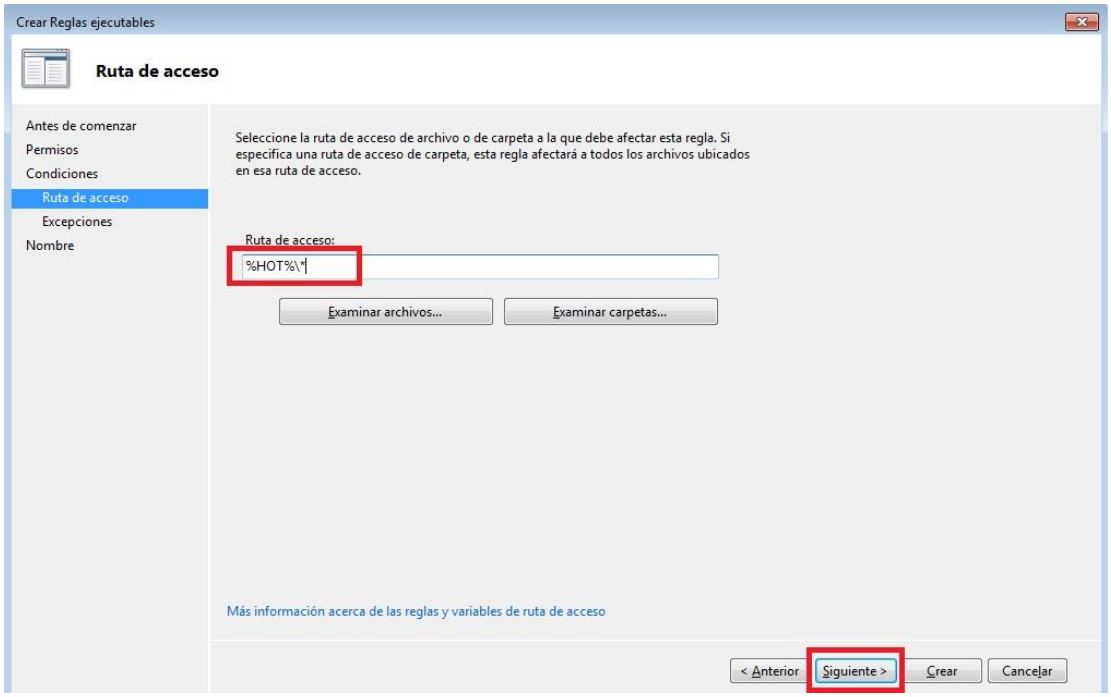


22.	En la siguiente ventana, escoja la condición de la regla. En este caso seleccione “ruta de acceso” y pulse el botón “Siguiente >”.



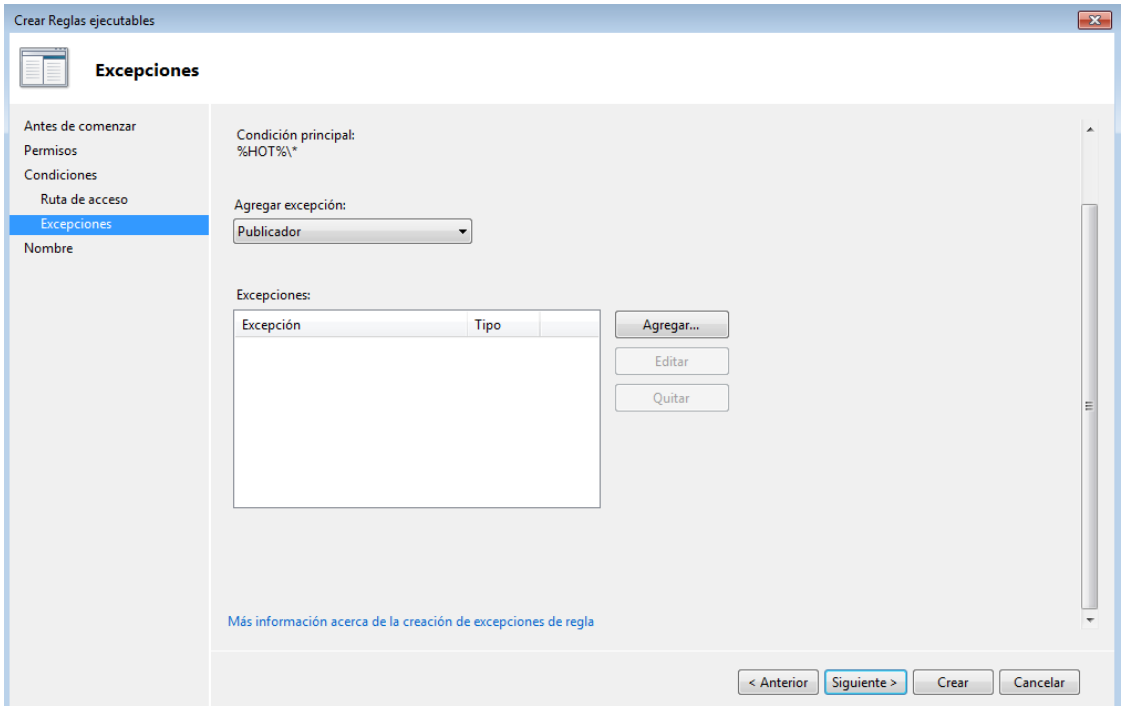
Paso	Descripción

23. En el cuadro de texto “Ruta de acceso” escriba el texto “**%HOT%***” (sin comillas) y pulse el botón “Siguiente >”.

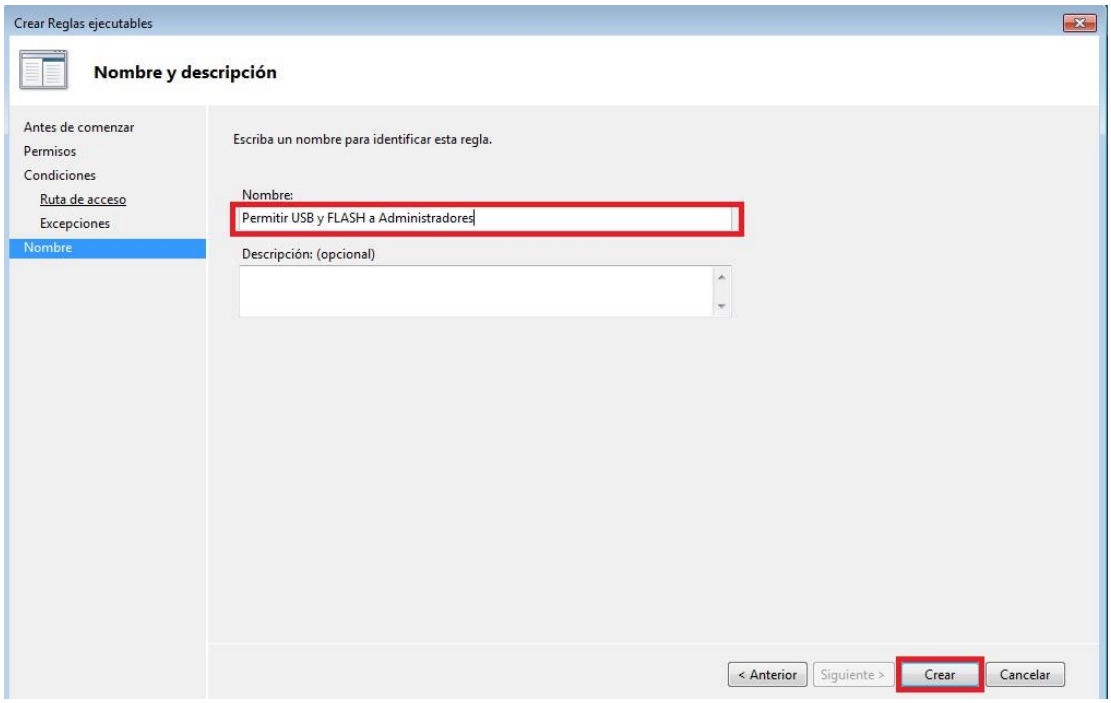


Nota: %HOT% es una variable interna de AppLocker que define todas las unidades de dispositivos de almacenamiento Flash y USB.

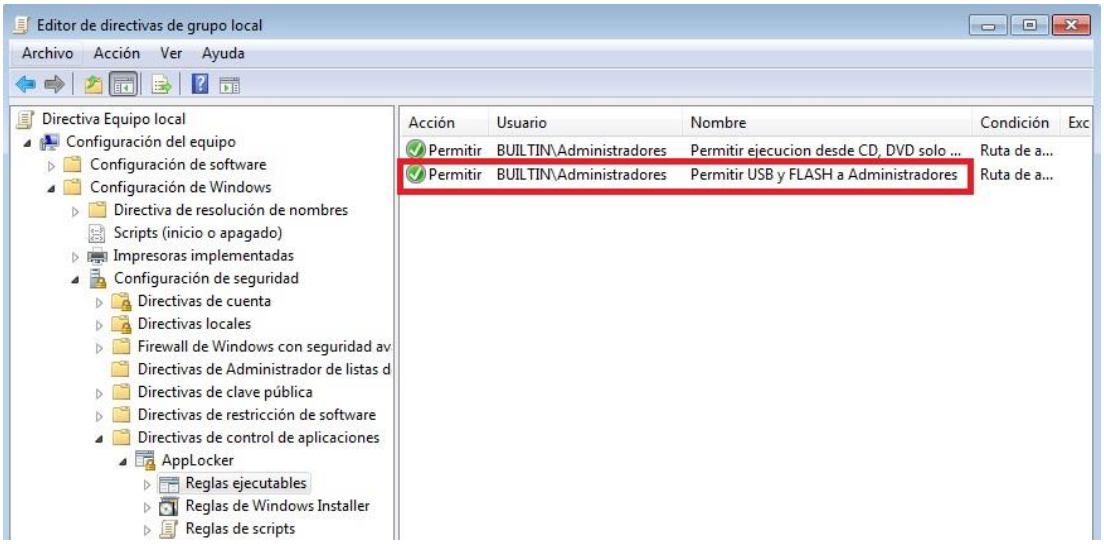
24. En la siguiente ventana se establecen las excepciones a la regla que se está creando. En este caso no se establecerá ninguna. Pulse el botón “Siguiente >”.

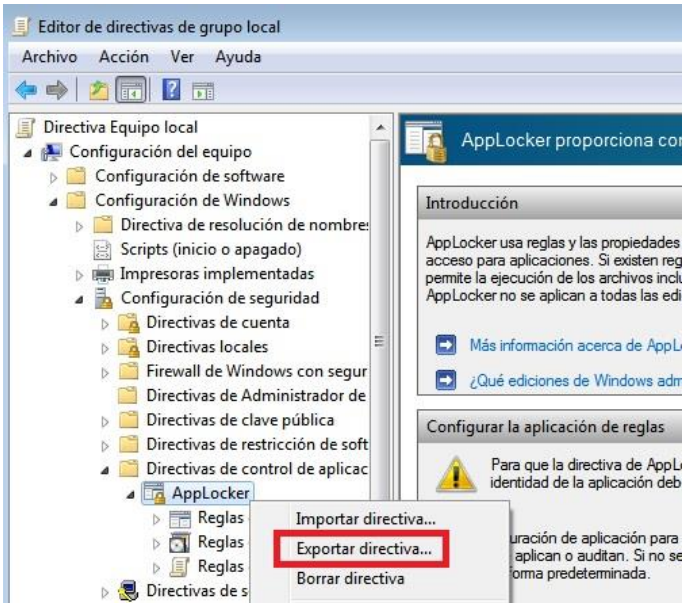
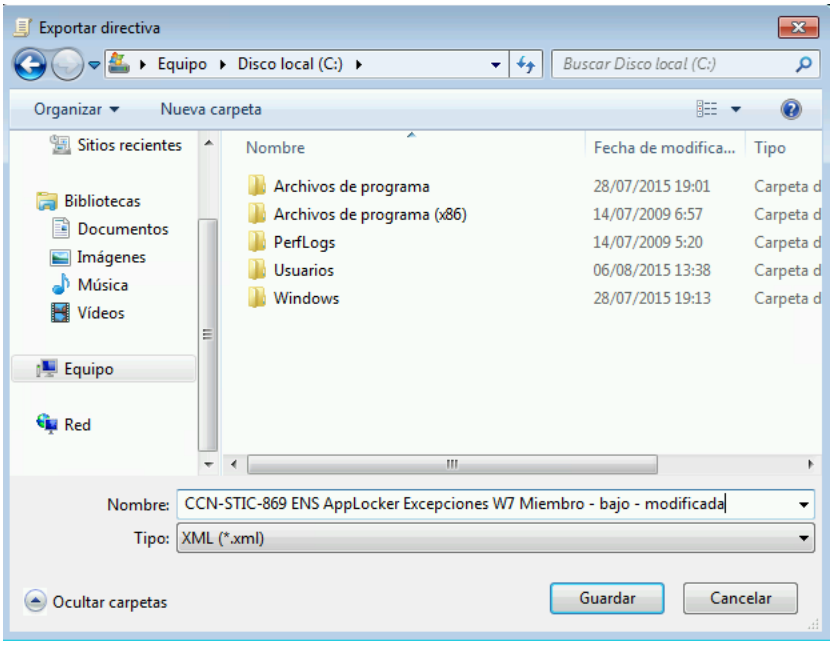


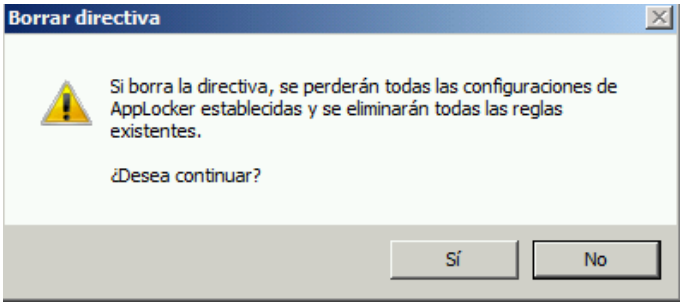
Paso	Descripción
25.	Introduzca un nombre descriptivo para la regla en el campo Nombre. En este caso se ha usado “Permitir USB y FLASH a Administradores”. Tras introducir el nombre pulse “Crear”.



26.	En el mismo "Editor de directivas de grupo local” de la máquina de referencia seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe que se ha creado la nueva regla “Permitir USB y FLASH a Administradores”.

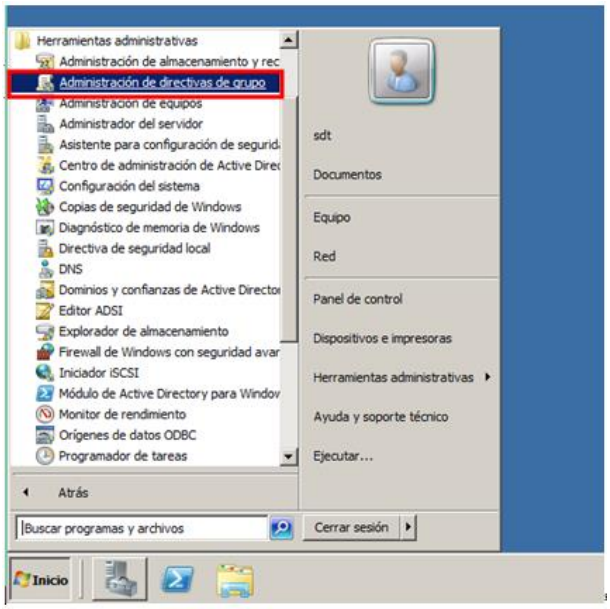


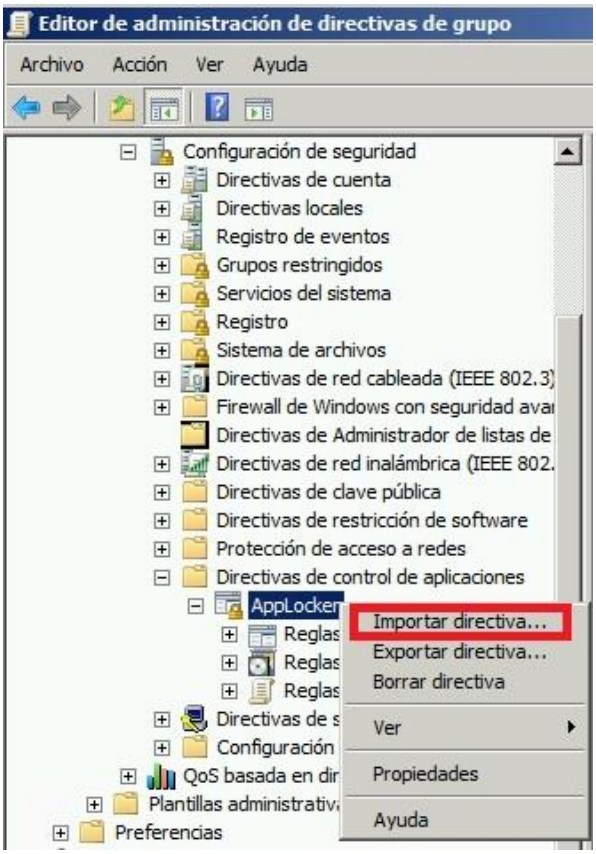
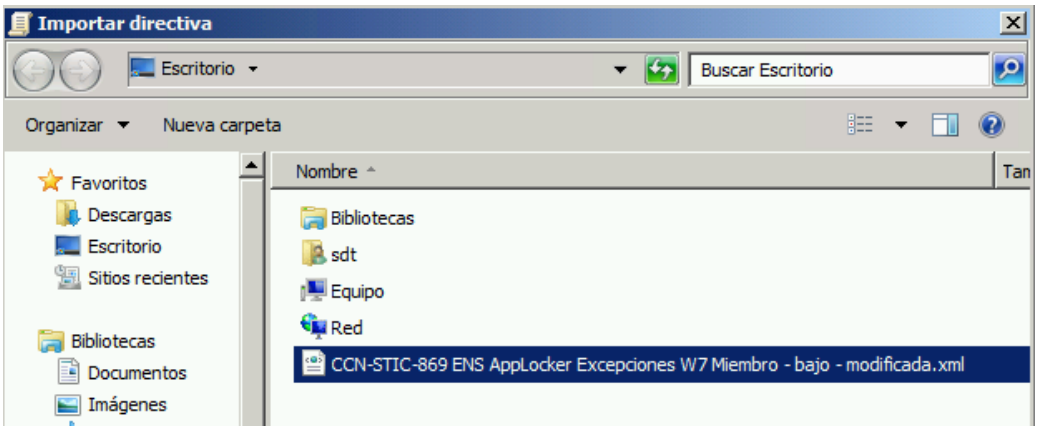
Paso	Descripción
27.	Una vez verificada la creación de la nueva regla, en el mismo "Editor de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Exportar directiva…" del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
28.	En el menú de navegación, seleccione una ubicación con permisos de escritura y guarde la configuración exportada. En este caso se usa el nombre "CCN-STIC-869 ENS AppLocker Excepciones – W7 Miembro –bajo- modificada.xml".  **Nota:** No cierre todavía el "Editor de directivas de grupo local".

Paso	Descripción
29.	Haciendo uso del mismo editor de directivas de grupo local usado para modificar las reglas de AppLocker, proceda a la eliminación de directiva para dejar así el entorno preparado para una nueva importación y edición de directivas. En el mismo "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Borrar directiva" del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
30.	Pulse "Si" en el cuadro de dialogo abierto. 
31.	Ya puede cerrar la ventana del "Editor de directivas de grupo local".

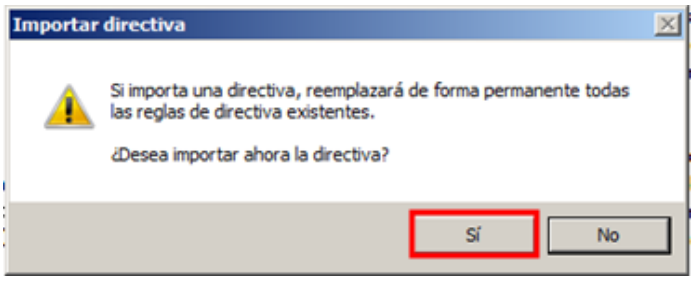
Una vez preparada la nueva directiva con las modificaciones necesarias para su entorno, se procederá a la importación de la misma en el GPO de excepciones que aplique a las máquinas que han de recibir las nuevas reglas.

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

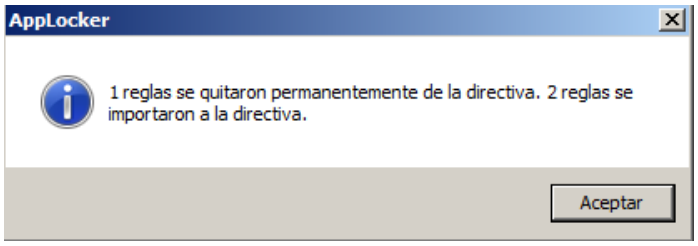
Paso	Descripción
32.	Inicie sesión en el servidor Controlador de Dominio con una cuenta que sea Administrador del Dominio.
33.	Copie el XML exportado de la máquina de referencia al controlador de dominio. En el presente ejemplo, se llama “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml”
34.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo** 
35.	Seleccione el GPO de excepciones a modificar. En este ejemplo se han editado las reglas de AppLocker definidas en el GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**”. Navegue hasta el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo** Marcando con el botón derecho en el GPO, elija la opción “Editar...” del menú contextual que aparecerá. 

Paso	Descripción
36.	En el “Editor de administración de directivas de grupo”, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva...” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
37.	En el cuadro de diálogo abierto navegue hasta el directorio donde haya depositado el XML previamente modificado en la máquina de referencia, selecciónelo y ábralo haciendo doble clic sobre él o pulsando el botón “Abrir”. 

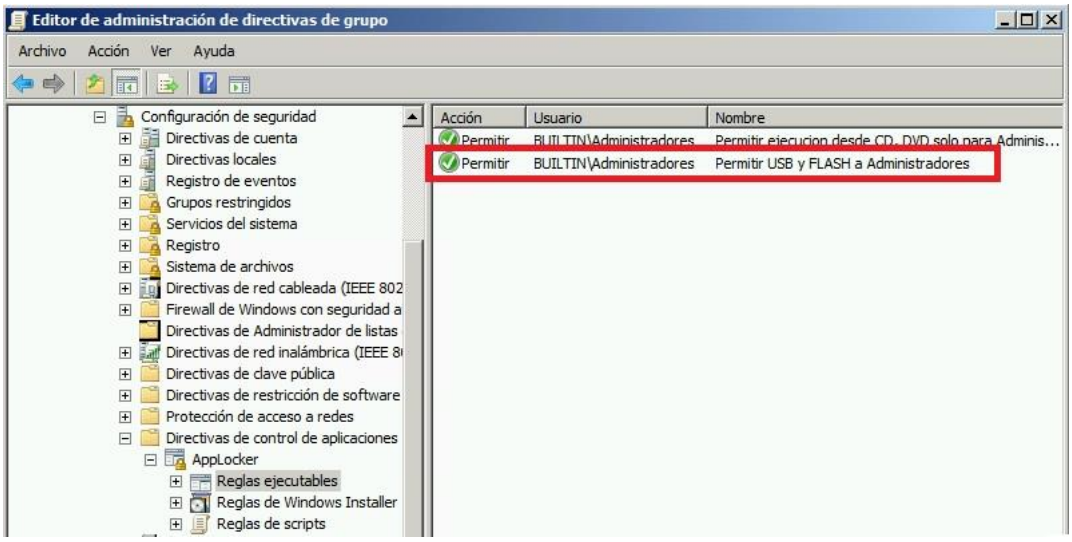
Paso	Descripción
38.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



39.	Aparecerá un nuevo mensaje informativo indicando que se importaron tantas reglas como se hayan creado/modificado reglas a la directiva de AppLocker.



40.	En el “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe en el menú que la nueva regla “Permitir USB y FLASH a Administradores” se ha creado de manera correcta.



41.	Ya puede cerrar el “Editor de Administración de directivas de grupo” habiendo quedado importadas al GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo**” todas las modificaciones realizadas en la máquina de referencia
42.	Los clientes Windows 7 recogerán la política de manera automática. No obstante, puede reiniciarlos para forzar el cambio.

4. PASO A PASO PARA LA CREACIÓN DE REGLA QUE PERMITA EJECUCIÓN DESDE DIRECTORIO TEMPORAL DEL PERFIL DE UN USUARIO

En la siguiente tabla, se detalla el procedimiento a seguir para la creación de una nueva regla que permita la ejecución de binarios desde el directorio temporal del perfil de un usuario concreto (C:\Users\%username%\AppData\Local\Temp). Esta excepción puede llegar a ser necesaria para instalaciones de software que se desempaquete de manera temporal en el perfil del usuario.

La implementación de AppLocker detallada en esta guía, para los distintos niveles del Esquema Nacional de seguridad, se ha diseñado de tal manera que las nuevas reglas o excepciones se han de definir editando los GPO de excepciones.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel bajo del ENS son:

- CCN-STIC-869 ENS AppLocker Excepciones DC – bajo: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán igualmente en modo auditoría.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel medio o alto del ENS son:

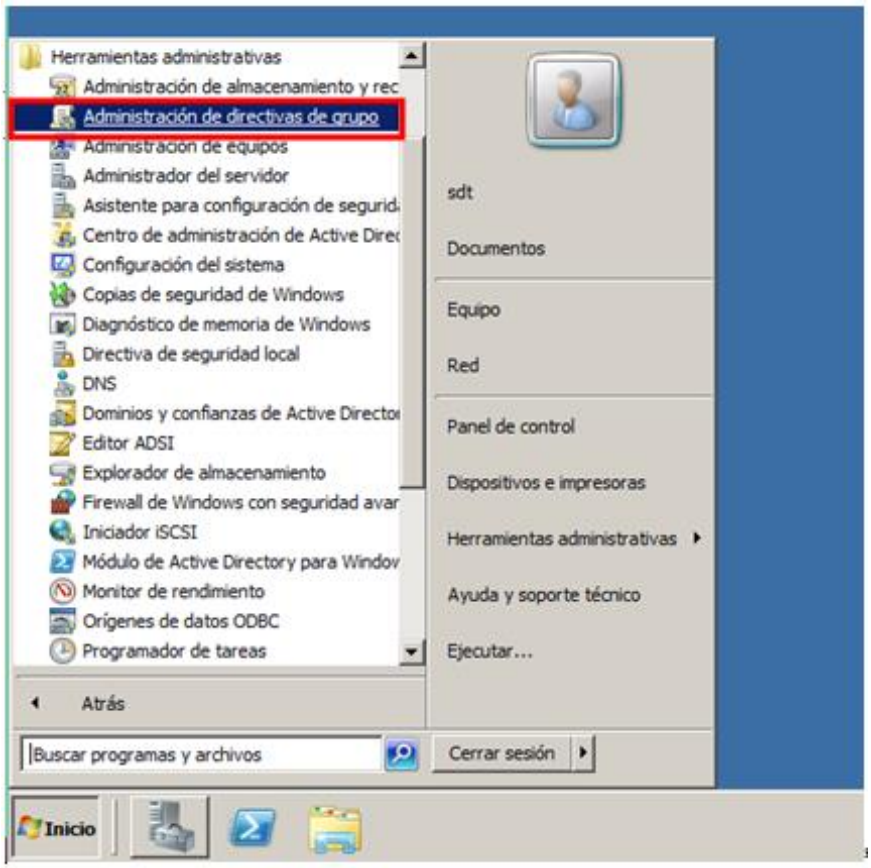
- CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.
- CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Los pasos que se describen a continuación se realizarán en un controlador de dominio donde se realizará la implementación de las políticas GPO necesarias para permitir la ejecución de aplicaciones desde rutas no estándares.

En este caso y a modo de ejemplo, se editará el GPO de excepciones que aplica sobre los clientes Windows 7 de la organización para una implementación del Esquema Nacional de Seguridad en nivel bajo. Dependiendo de sus necesidades deberá adaptar el siguiente procedimiento para que aplique a otras máquinas o niveles de implementación del Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio con una cuenta con derechos de administración en el dominio.

Paso	Descripción
2.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio: **Inicio → Herramientas administrativas → Administración de directivas de grupo**

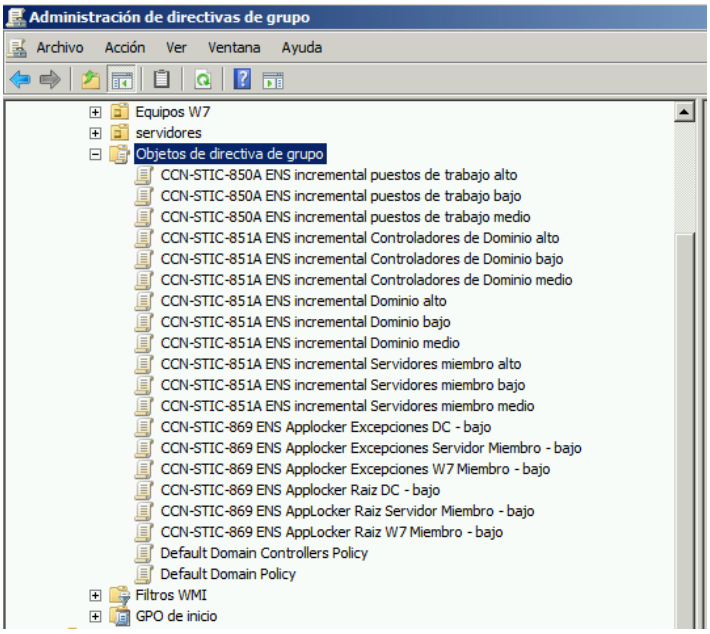


3.	Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos.

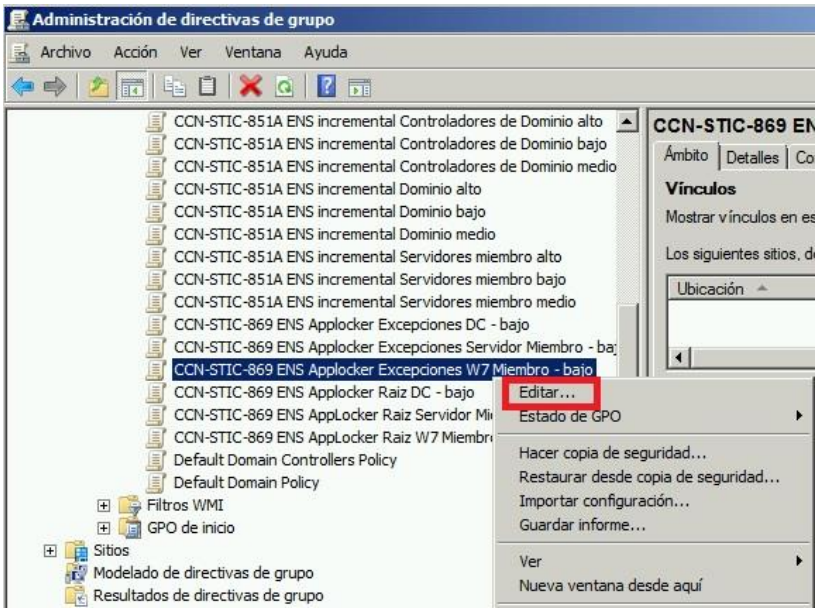
Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

Paso	Descripción

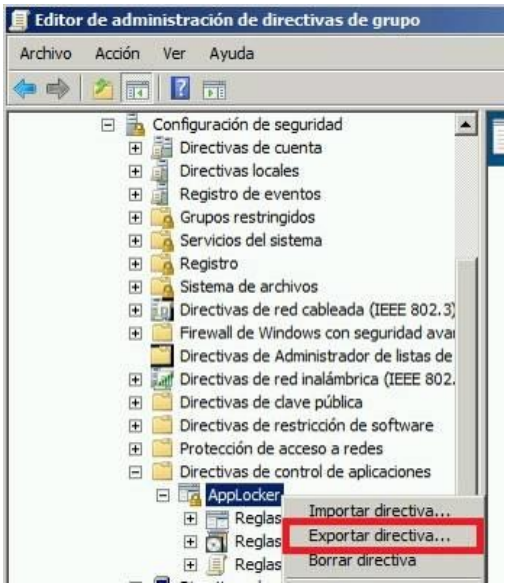
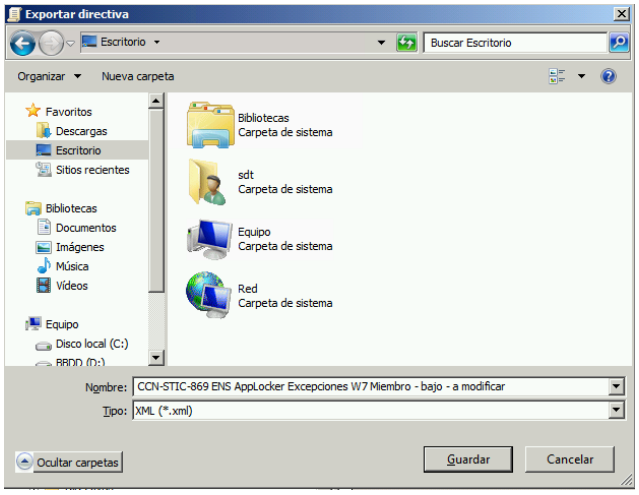
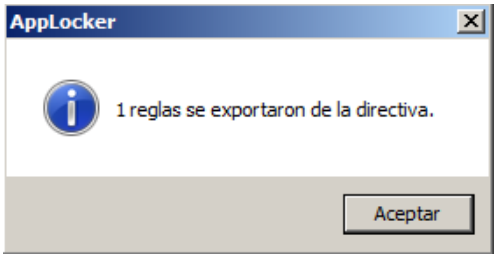
4. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo,** como se muestra en la siguiente imagen.



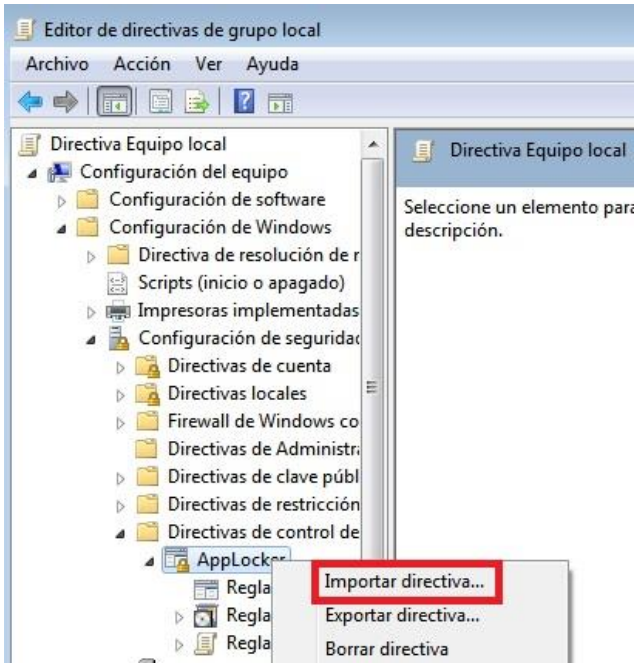
5. Seleccione el GPO de excepciones a modificar. En este ejemplo se pretende modificar la colección de reglas de AppLocker aplicadas a clientes Windows 7 a los que les aplica el nivel bajo del ENS. Por lo que se procederá a la edición del GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.



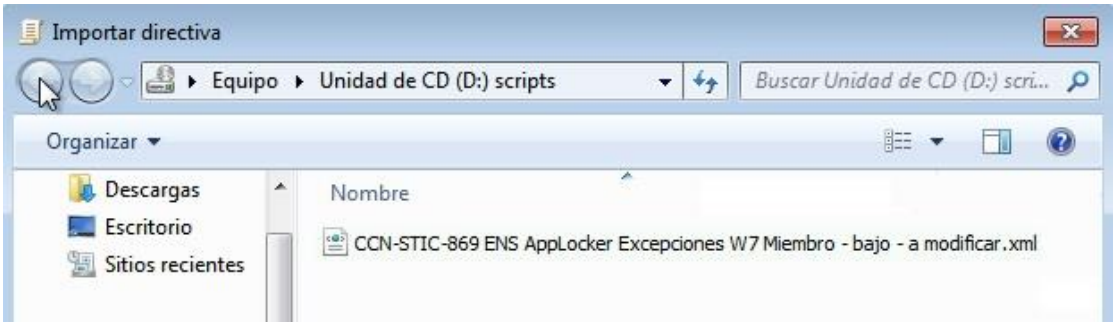
Nota: El GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" está diseñado para recibir las excepciones o nuevas reglas que se quieran aplicar a los Equipos W7 de la organización. Si necesita crear excepciones que apliquen a servidores miembros o a los controladores de dominio, seleccione el GPO adecuado según se describe al comienzo del presente apartado.

Paso	Descripción
6.	En el “Editor de administración de directivas de grupo” seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción “**Exportar directiva**”. **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** 
7.	En el cuadro de diálogo abierto navegue hasta un directorio con permisos de escritura y guarde la política exportada en formato xml. Elija un nombre reconocible. 
8.	Tras la exportación se presentará el siguiente mensaje informativo. 

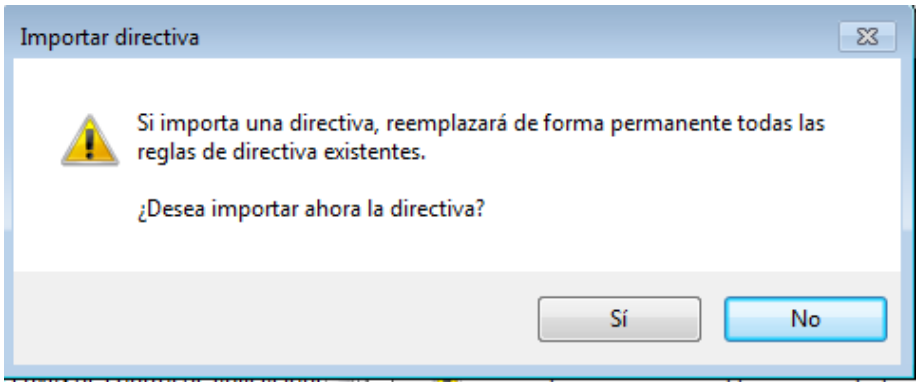
Una vez exportada la política de AppLocker definida en el GPO de excepciones seleccionado, se procederá a la importación de la misma en un equipo de referencia Windows 7 Enterprise que pertenezca al dominio pero no reciba reglas de AppLocker por GPO de dominio.

Paso	Descripción
9.	Inicie sesión en la máquina de referencia con un usuario con permisos administrativos. **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.
10.	Traslade el fichero XML recién exportado (CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo- a modificar.xml) a la máquina de referencia. En dicha máquina, haciendo uso de la herramienta "**GPedit.msc**" proceda a importar la configuración de AppLocker tal y como se indica a continuación. **Nota:** Puede lanzar "GPedit.msc" desde el menú "Ejecutar" de Windows (pulsando la combinación de teclas "Windows + R").
11.	Una vez abierto el "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Escoja la opción "Importar directiva..." del menú contextual que aparece tras pulsar botón derecho sobre la ubicación señalada arriba.  **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.

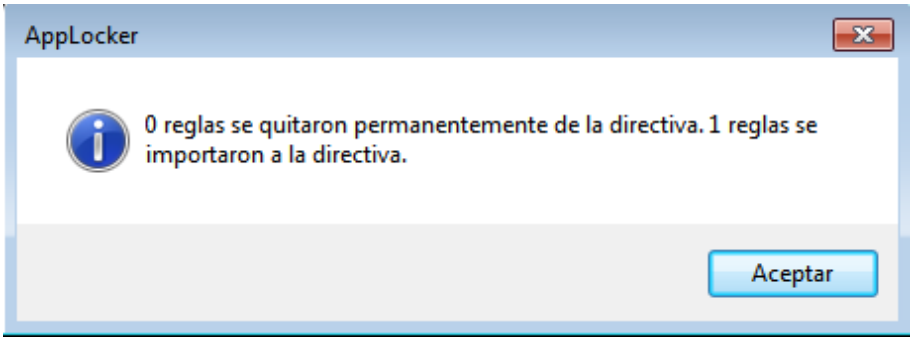
Paso	Descripción
12.	En el cuadro de dialogo abierto, navegue hasta el directorio donde haya depositado el archivo XML a importar y selecciónelo haciendo doble clic sobre él o pulsando el botón “Abrir”.



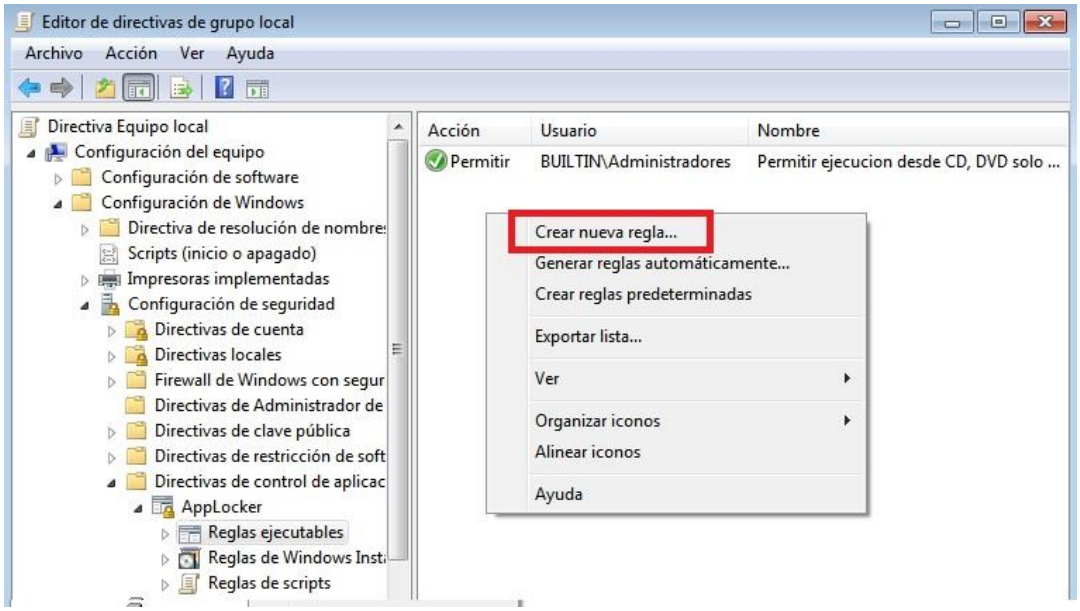
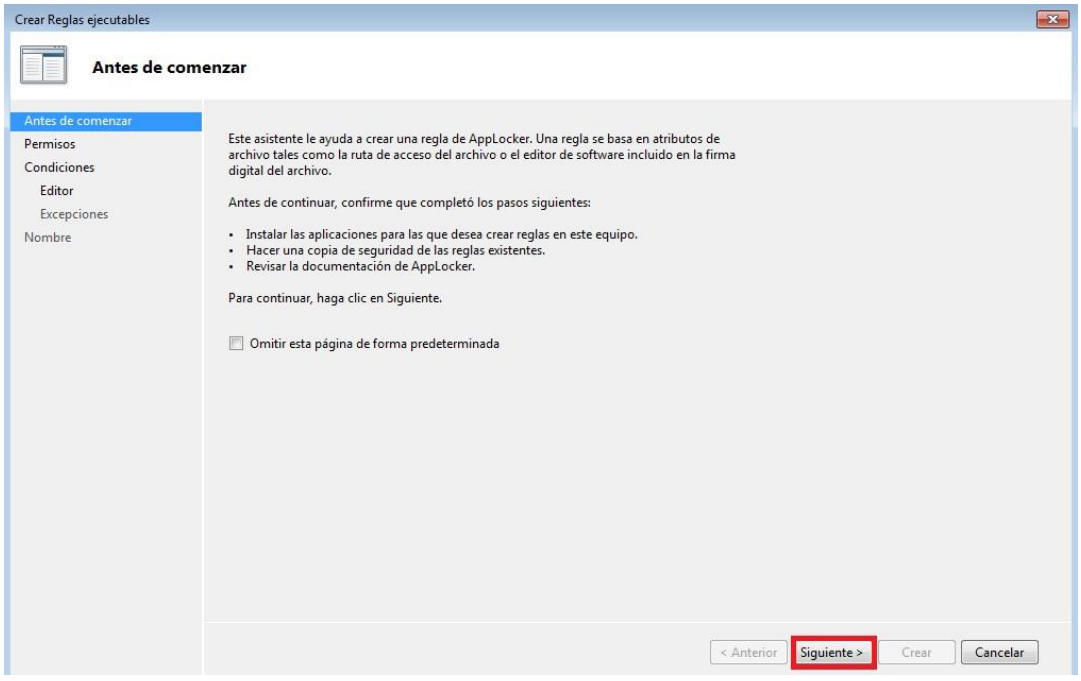
13.	Puede que se le solicite confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Si es así seleccione “Sí”.

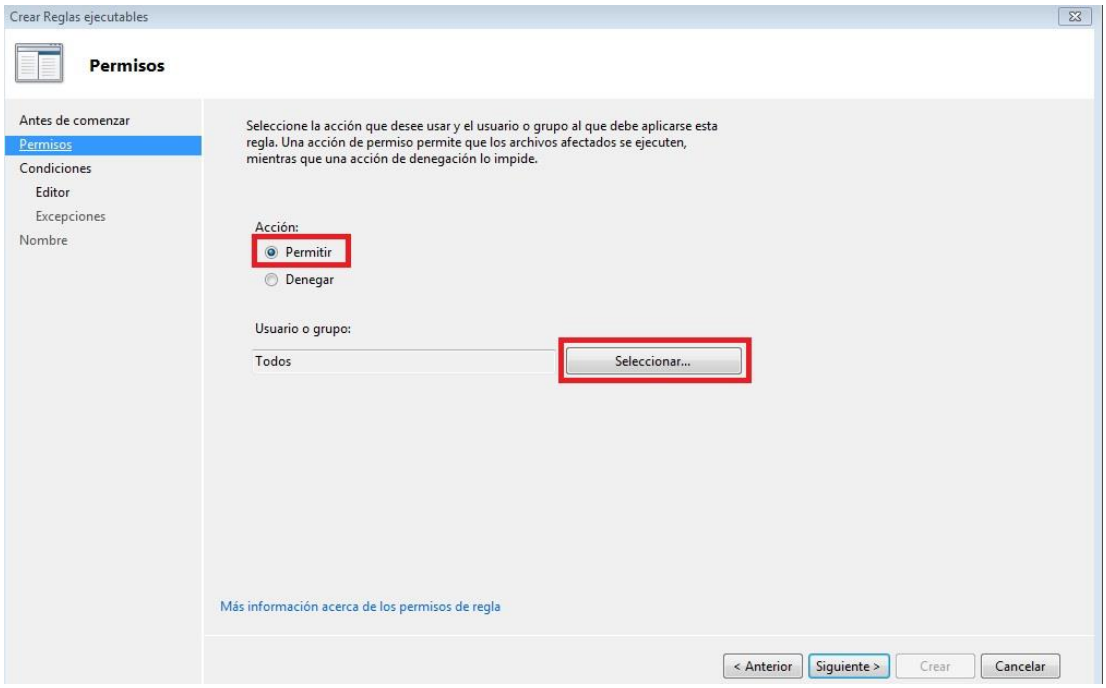
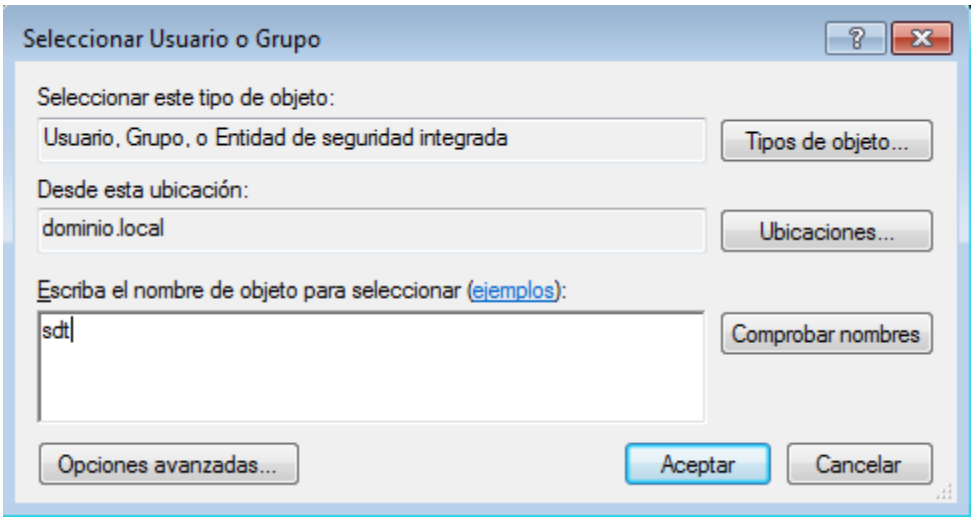


14.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.



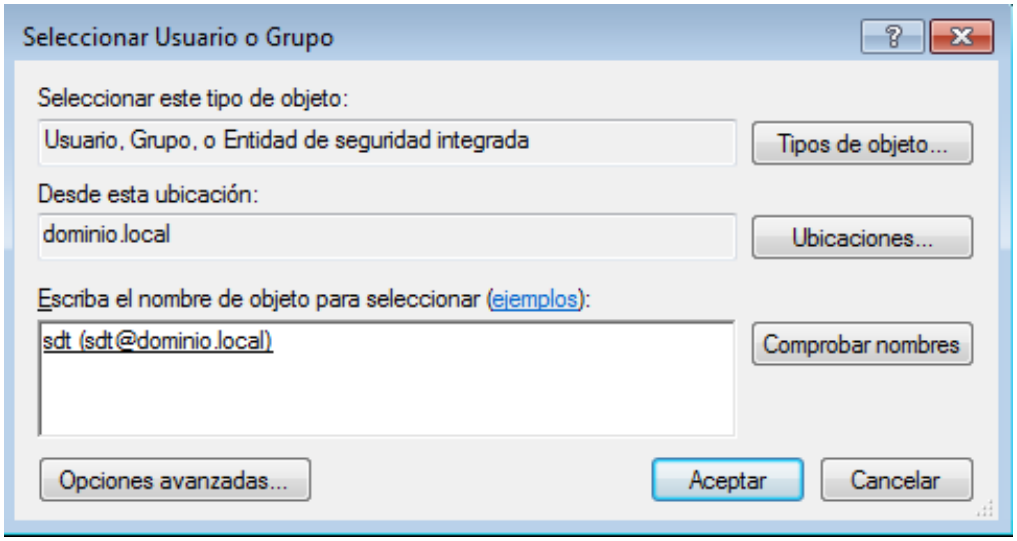
Nota: Se importa una única regla ya que se está usando la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”, que contiene una única regla de excepción para permitir ejecución de binarios ubicados en CD o DVD.

Paso	Descripción
15.	Para crear una nueva regla, en el “Editor de directivas de grupo local” navegue hasta la ubicación indicada y seleccione la opción “Crear nueva regla…” del menú contextual que aparece tras pulsar el botón derecho en el panel derecho. **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables** 
16.	En la primera pantalla del asistente desplegado pulsar sobre el botón siguiente. 

Paso	Descripción
17.	En el siguiente menú, se debe seleccionar el tipo de regla (permiso o denegación) y los usuarios o grupos de usuarios a los que aplicará. En éste caso, se selecciona la opción “Permitir” y a continuación se pulsa sobre el botón “Seleccionar…” para poder elegir los usuarios a los que aplicará la nueva regla. 
18.	En la ventana “Seleccionar Usuario o Grupo” escriba el usuario al que se le quiere permitir la ejecución de binarios desde el temporal de su perfil en el cuadro de texto y pulse en comprobar nombres.  **Nota:** En este caso se escoge el usuario "sdt". Elija el grupo o el usuario al que se le va a proporcionar permiso para ejecutar binarios desde el temporal de su perfil.

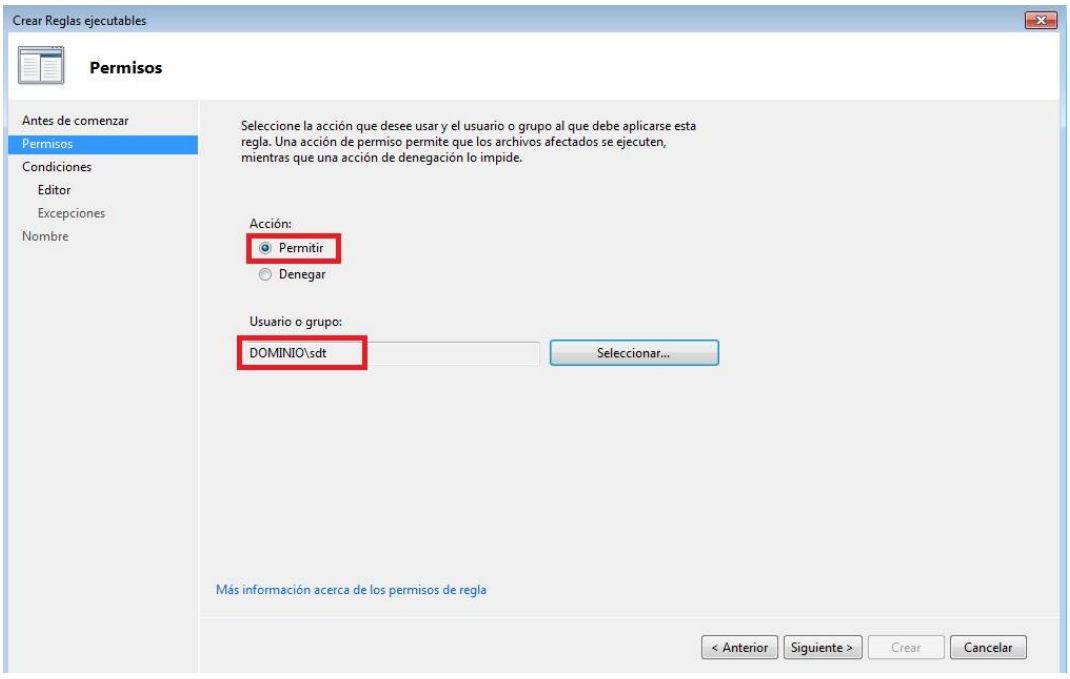
Paso	Descripción

19. Pulse “Aceptar” en la ventana “Seleccionar Usuario o Grupo”.



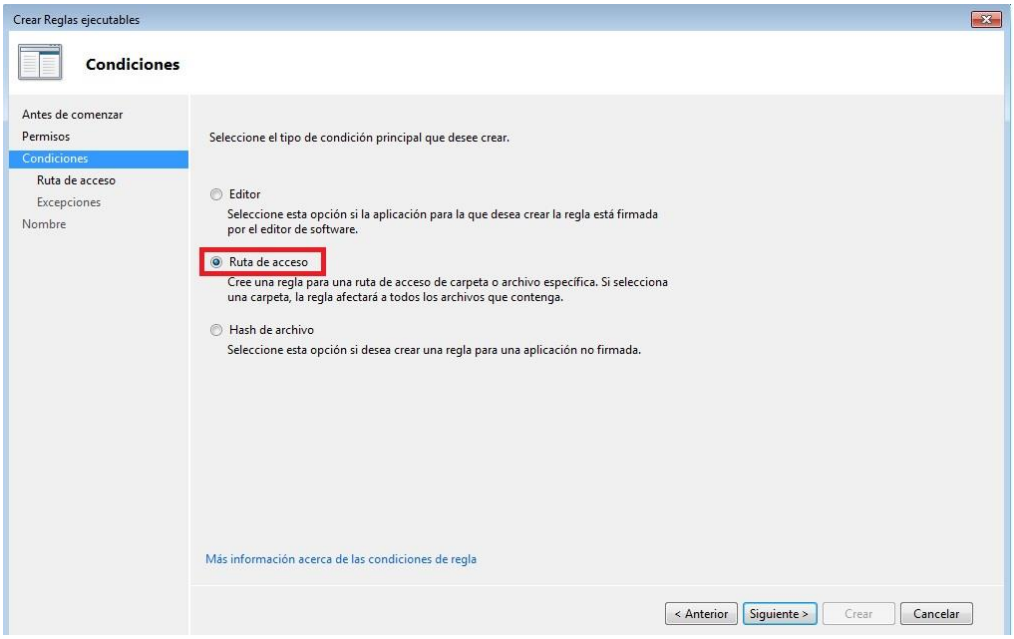
Nota: Asegúrese de que está buscando los usuarios y grupos del dominio. En el campo “Desde esta ubicación” deberá de aparecer el nombre del dominio de la organización

20. En la ventana Crear Reglas Ejecutables, compruebe que la acción seleccionada es “Permitir” y el usuario es el correcto. Si es así, pulse el botón “Siguiente >".



Paso	Descripción

21. En la siguiente ventana, escoja la condición de la regla. En este caso, seleccione “Ruta de acceso” y pulse el botón “Siguiente >”.



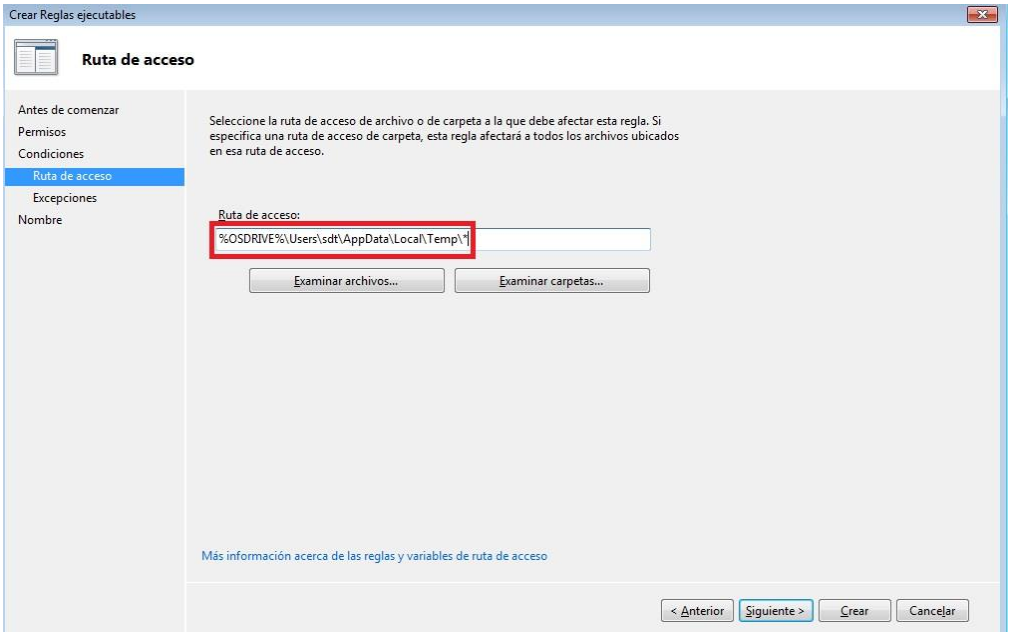
22. En el cuadro de texto “Ruta de acceso” escriba la ruta al temporal del usuario tal y como se le indica a continuación:

%OSDRIVE%\users\<carpeta de perfil>\AppData\Local\Temp*

Sustituya *<carpeta de perfil>* por el nombre de la carpeta del perfil del usuario elegido. En este caso quedaría:

%OSDRIVE%\users\sdt\AppData\Local\Temp*

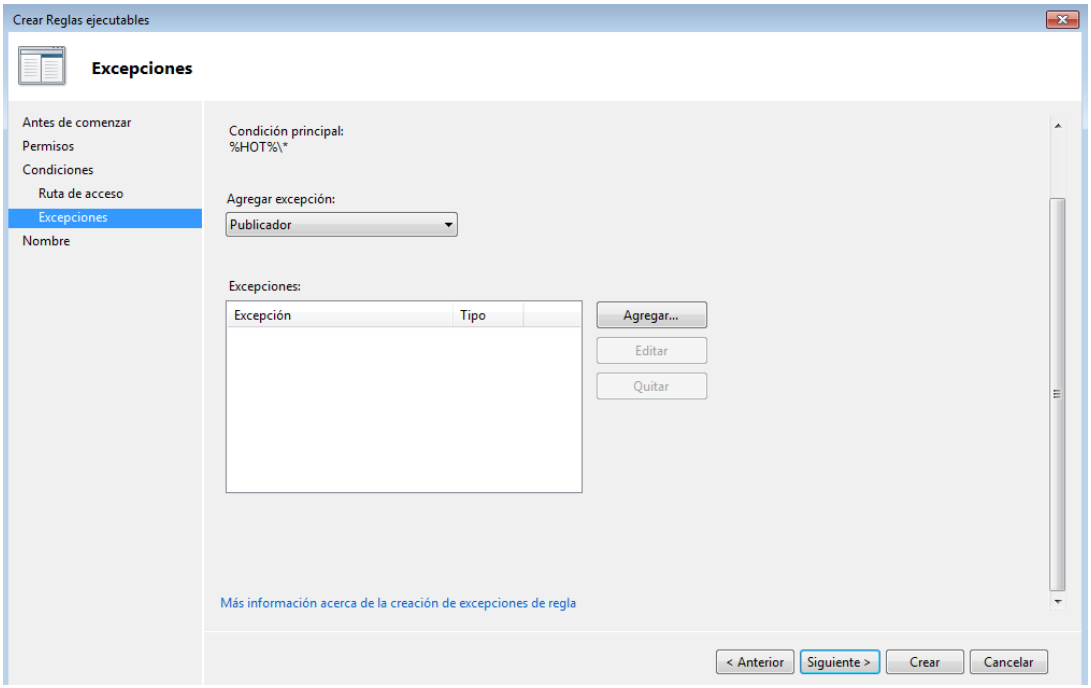
Pulse “Siguiente >” cuando termine de escribir la ruta.



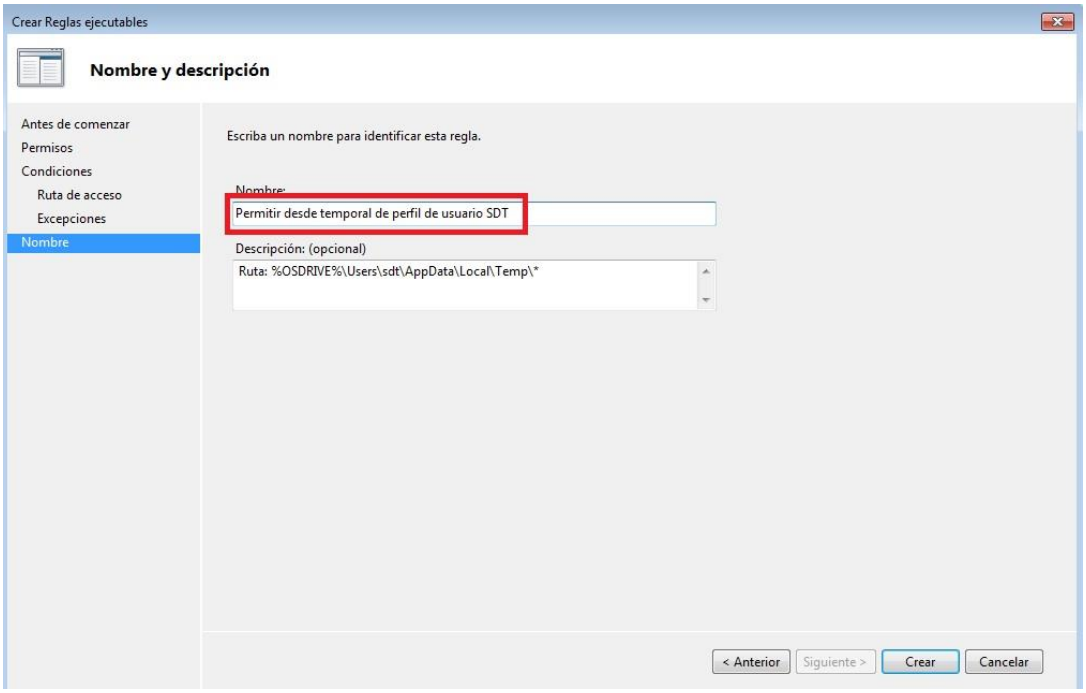
Nota: Nótese que la ruta acaba en asterisco, para así permitir todos los binarios que existan en la carpeta. %OSDRIVE% es una variable de AppLocker que, en el ejemplo, se traduce por la unidad raíz “C:\”.

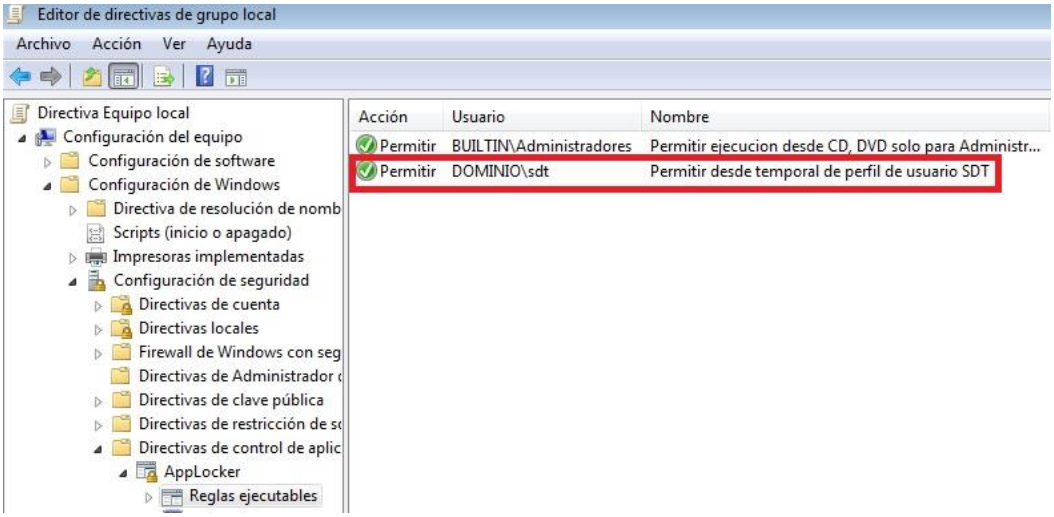
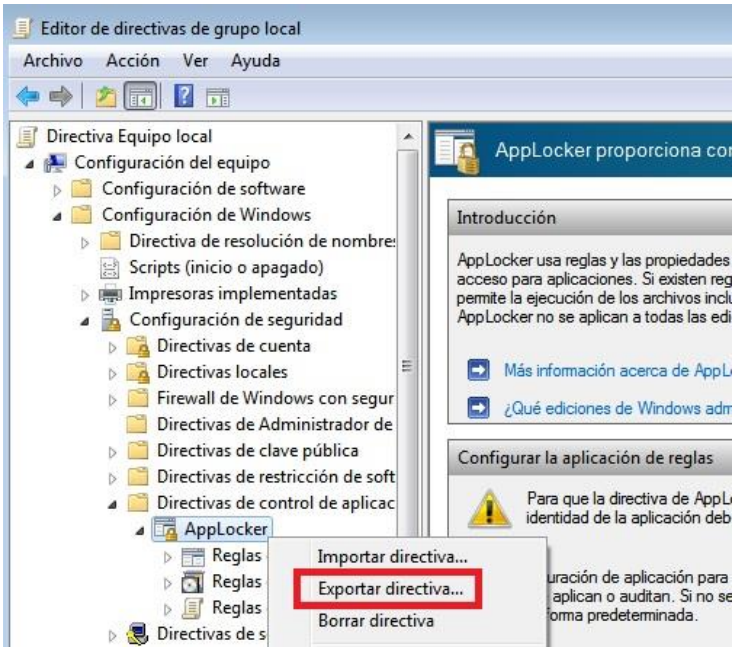
Paso	Descripción

23. En la siguiente ventana, se establecen las excepciones a la regla que se está creando. En este caso, no se establecerá ninguna. Pulse el botón “Siguiente >”.



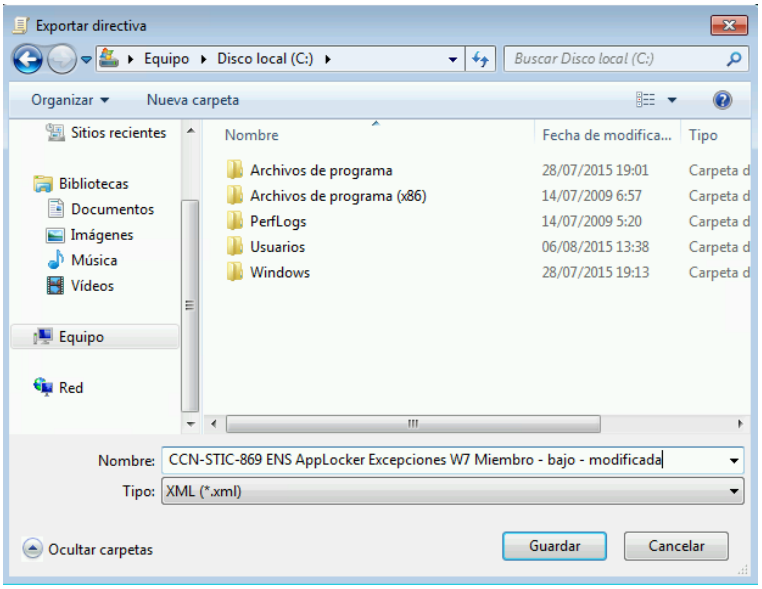
24. Introduzca un nombre descriptivo para la regla en el campo Nombre. En este caso, se ha usado “Permitir desde temporal de perfil de usuario SDT”. También puede incluir de manera opcional una descripción más detallada de la regla. Tras introducir el nombre pulse el botón “Crear”.



Paso	Descripción
25.	En el mismo "Editor de directivas de grupo local" de la máquina de referencia seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe que se ha creado la nueva regla. 
26.	Una vez verificada la creación de la nueva regla, en el mismo "Editor de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Exportar directiva…” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 

Paso	Descripción

27. En el menú de navegación seleccione una ubicación con permisos de escritura y guarde la configuración exportada. En este caso se usa el nombre “CCN-STIC-869 ENS AppLocker Excepciones – W7 Miembro –bajo- modificada.xml”.



Nota: No cierre todavía el Editor de Editor de directivas de grupo local.

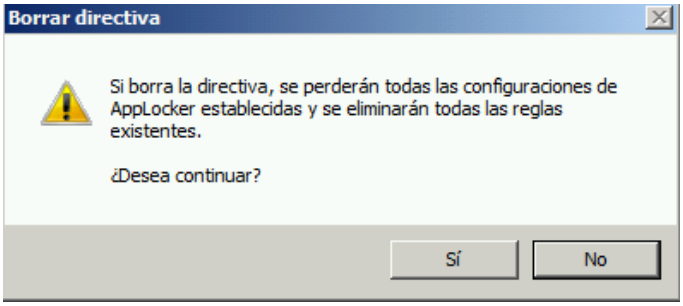
28. Haciendo uso del mismo editor de directivas de grupo local usado para modificar las reglas de AppLocker, proceda a la eliminación de directiva para dejar así el entorno preparado para una nueva importación y edición de directivas.

    En el mismo "Editor de administración de directivas de grupo local”, seleccione la siguiente ubicación:

    Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

    Elija la opción “Borrar directiva” del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada.

Paso	Descripción
29.	Pulse “Si” en el cuadro de dialogo abierto.

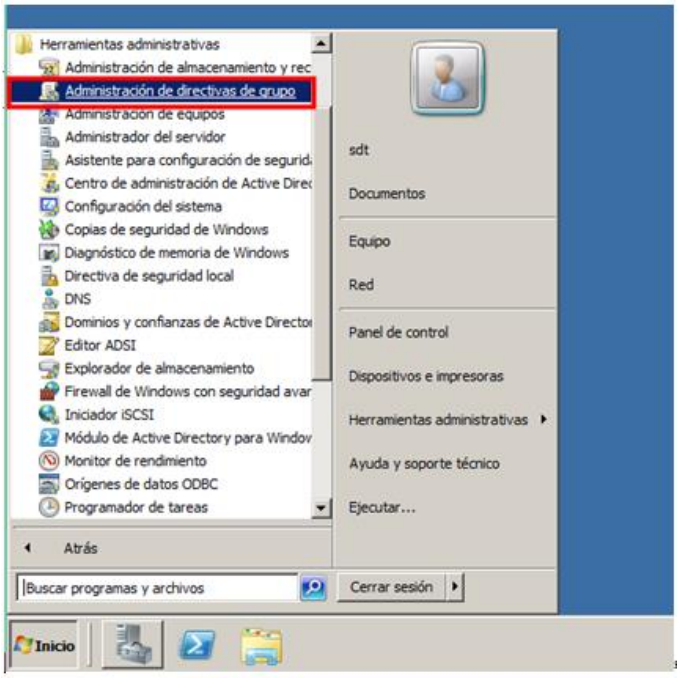


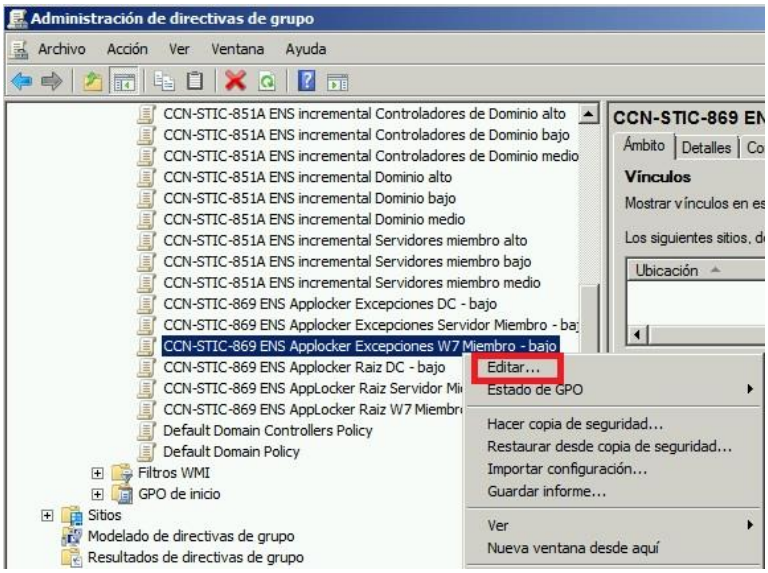
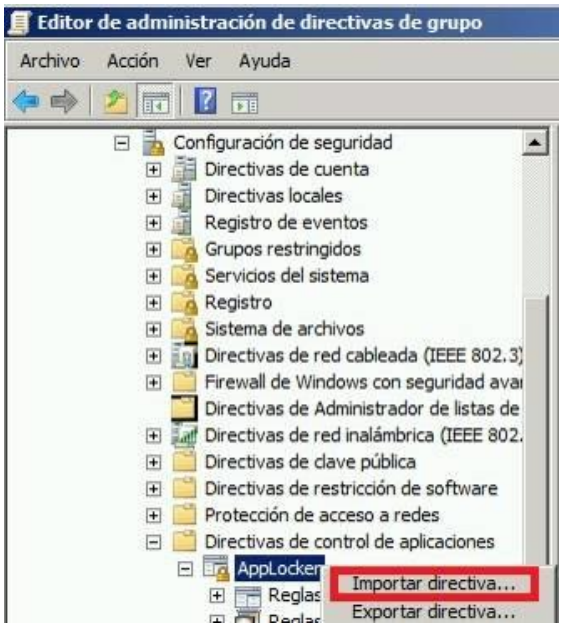
30.	Ya puede cerrar la ventana del “editor de directivas de grupo local”.

Una vez preparada la nueva directiva con las modificaciones necesarias para su entorno se procederá a la importación de la misma en el GPO de excepciones que aplique a las máquinas que han de recibir las nuevas reglas.

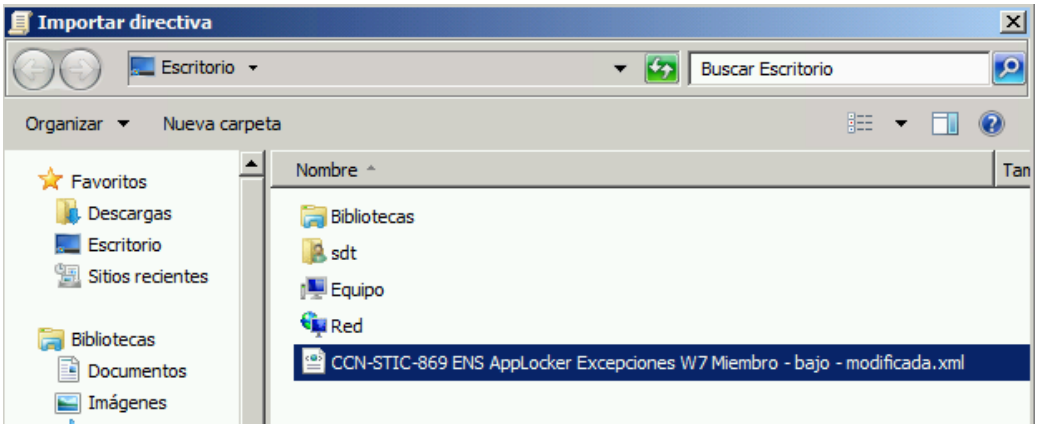
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

Paso	Descripción
31.	Inicie sesión en el servidor Controlador de Dominio con una cuenta que sea Administrador del Dominio.
32.	Copie el archivo XML exportado de la máquina de referencia al controlador de dominio. En el presente ejemplo se llama “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml”
33.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo**

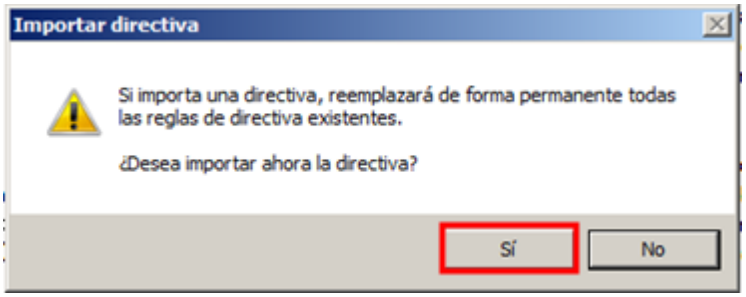


Paso	Descripción
34.	Seleccione el GPO de excepciones a modificar. En este ejemplo se han editado las reglas de AppLocker definidas en el GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Navegue hasta el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo** Marcando con el botón derecho en el GPO, elija la opción "Editar..." del menú contextual que aparecerá. 
35.	En el "Editor de administración de directivas de grupo", seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Importar directiva..." del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 

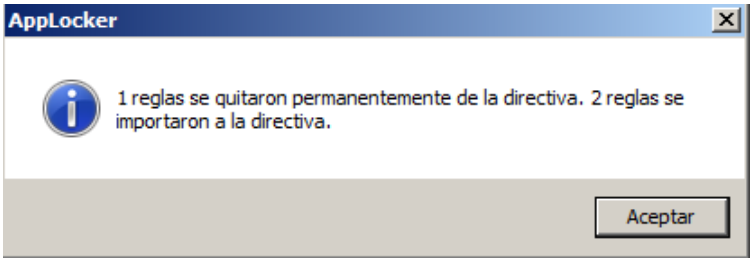
Paso	Descripción
36.	En el cuadro de diálogo abierto navegue hasta el directorio donde haya depositado el archivo XML previamente modificado en la máquina de referencia, selecciónelo y ábralo haciendo doble clic sobre él o pulsando el botón “Abrir”

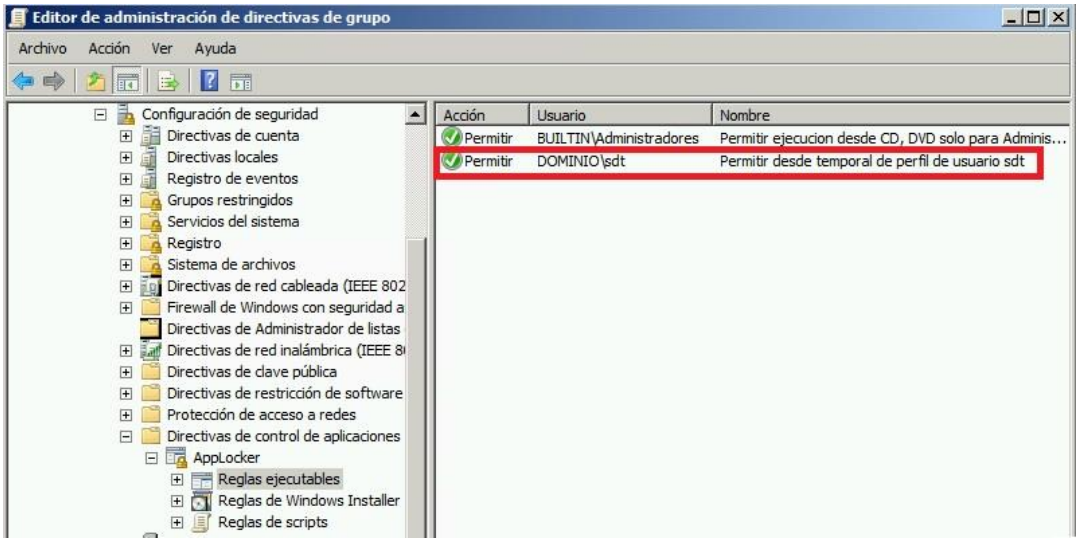


37.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



38.	Aparecerá un nuevo mensaje informativo indicando que se importaron tantas reglas como se hayan creado/modificado reglas a la directiva de AppLocker.



Paso	Descripción
39.	En el “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe en el menú que la nueva regla para permitir la ejecución desde el temporal del usuario seleccionado se ha creado de manera correcta. 
40.	Ya puede cerrar el “Editor de Administración de directivas de grupo” habiendo quedado importadas al GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo**” todas las modificaciones realizadas en la máquina de referencia
41.	Los clientes Windows 7 recogerán la política de manera automática. No obstante, puede reiniciarlos para forzar el cambio.

5. PASO A PASO PARA LA CREACION DE REGLA PARA RESTRINGIR UN BINARIO IDENTIFICADO POR HASH (FIRMA)

En la siguiente tabla se detalla el procedimiento a seguir para la creación de una nueva regla que deniega la ejecución de un binario específico identificado por su hash (firma SHA256). Esta regla puede llegar a ser necesaria si se identifican binarios maliciosos en la infraestructura y se pretende evitar su ejecución mediante el uso de políticas de dominio que implementen reglas de AppLocker.

La implementación de AppLocker detallada en esta guía para los distintos niveles del Esquema Nacional de seguridad se ha diseñado de tal manera que las nuevas reglas, o excepciones se han de definir editando los GPO de excepciones.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel bajo del ENS son:

- CCN-STIC-869 ENS AppLocker Excepciones DC – bajo: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.

– CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán igualmente en modo auditoría.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel medio o alto del ENS son:

– CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.

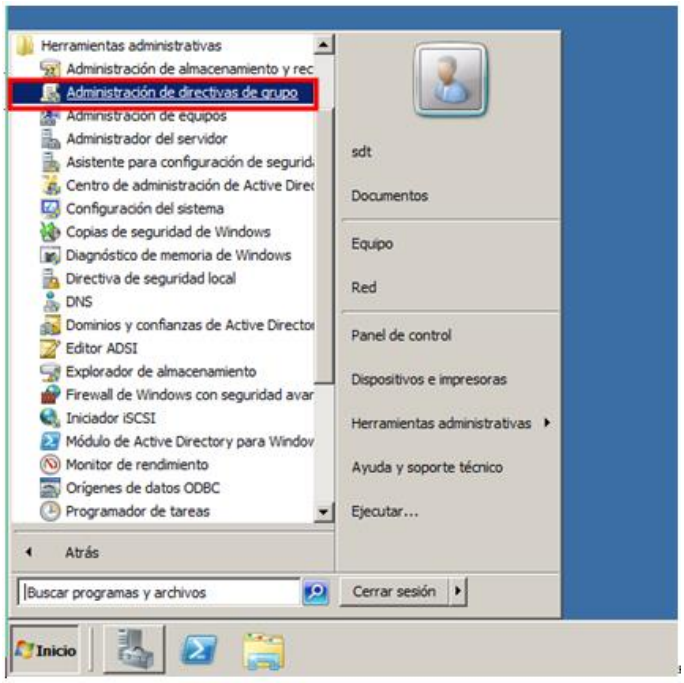
– CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.

– CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Los pasos que se describen a continuación se realizarán en un controlador de dominio donde se realizará la implementación de las políticas GPO necesarias para permitir la ejecución de aplicaciones desde rutas no estándares.

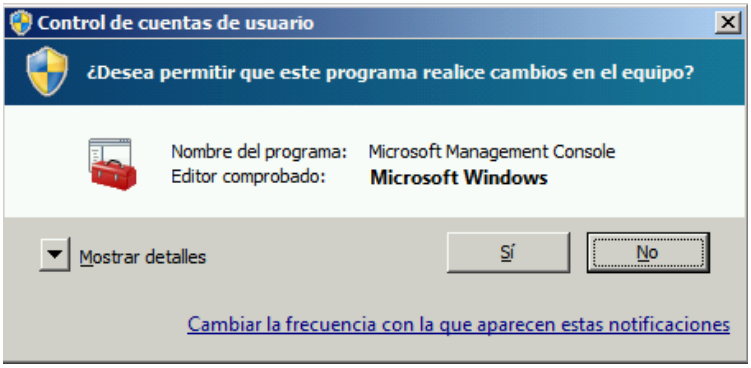
En este caso y a modo de ejemplo, se editará el GPO de excepciones que aplica sobre los clientes Windows 7 de la organización para una implementación del Esquema Nacional de Seguridad en nivel bajo. Dependiendo de sus necesidades deberá adaptar el siguiente procedimiento para que aplique a otras máquinas o niveles de implementación del Esquema Nacional de Seguridad.

Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio con una cuenta con derechos de administración en el dominio.
2.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio: **Inicio → Herramientas administrativas → Administración de directivas de grupo**



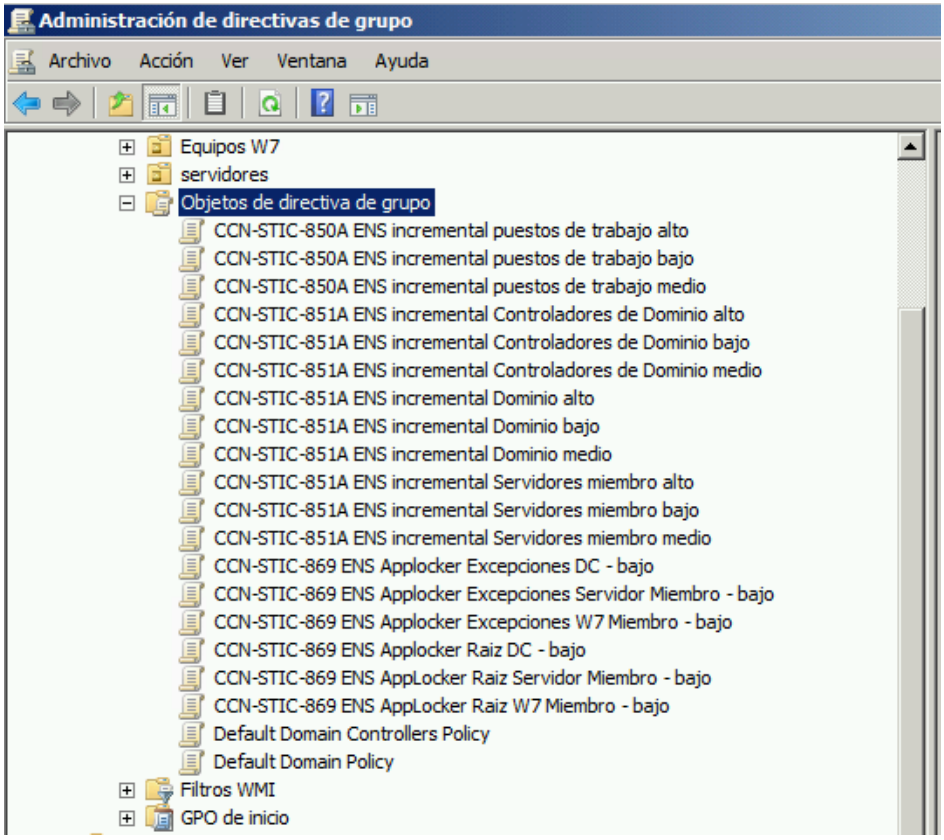
Paso	Descripción

3. Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de “Administración de directivas de grupo” con permisos administrativos.



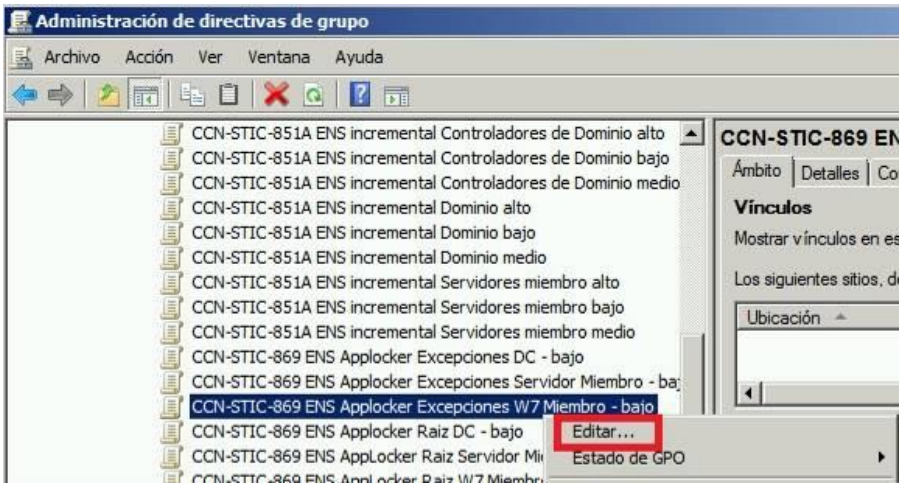
Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

4. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo,** como se muestra en la siguiente imagen.



Paso	Descripción

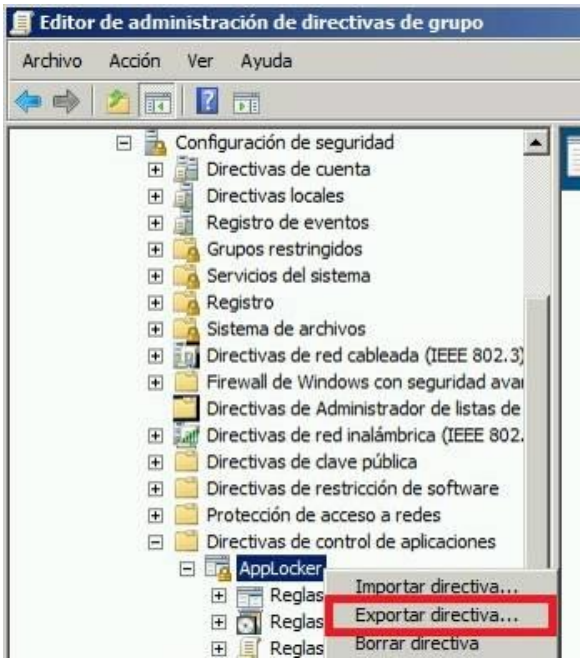
5. Seleccione el GPO de excepciones a modificar. En este ejemplo, se pretende modificar la colección de reglas de AppLocker aplicadas a clientes Windows 7 a los que les aplica el nivel bajo del ENS. Por tanto, se procederá a la edición del GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.



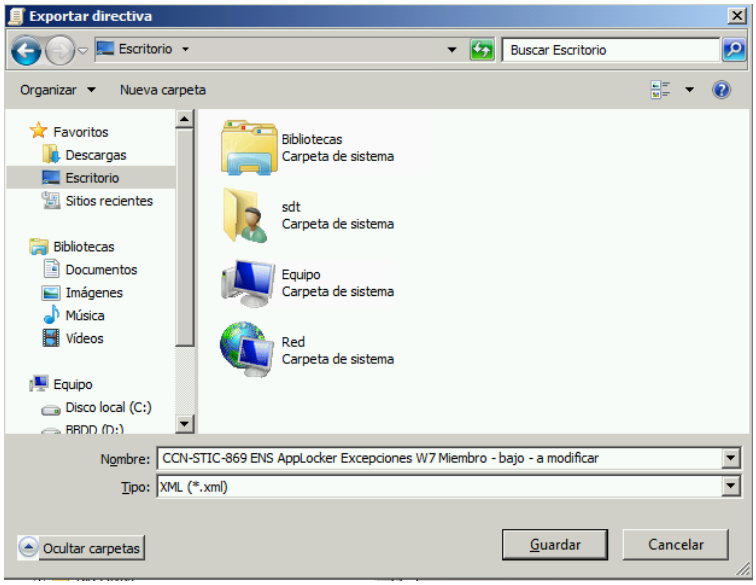
Nota: El GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" está diseñado para recibir las excepciones o nuevas reglas que se quieran aplicar a los Equipos W7 de la organización. Si necesita crear excepciones que apliquen a servidores miembros o a los controladores de dominio, seleccione el GPO adecuado según se describe al comienzo del presente apartado.

6. En el "Editor de administración de directivas de grupo" seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción "**Exportar directiva**".

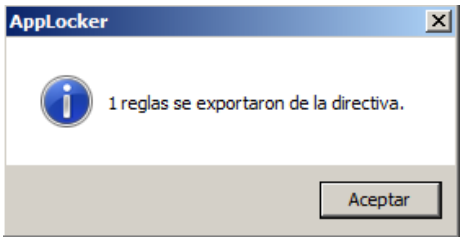
Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker



Paso	Descripción
7.	En el cuadro de diálogo abierto navegue hasta un directorio con permisos de escritura y guarde la política exportada en formato xml. Elija un nombre reconocible.



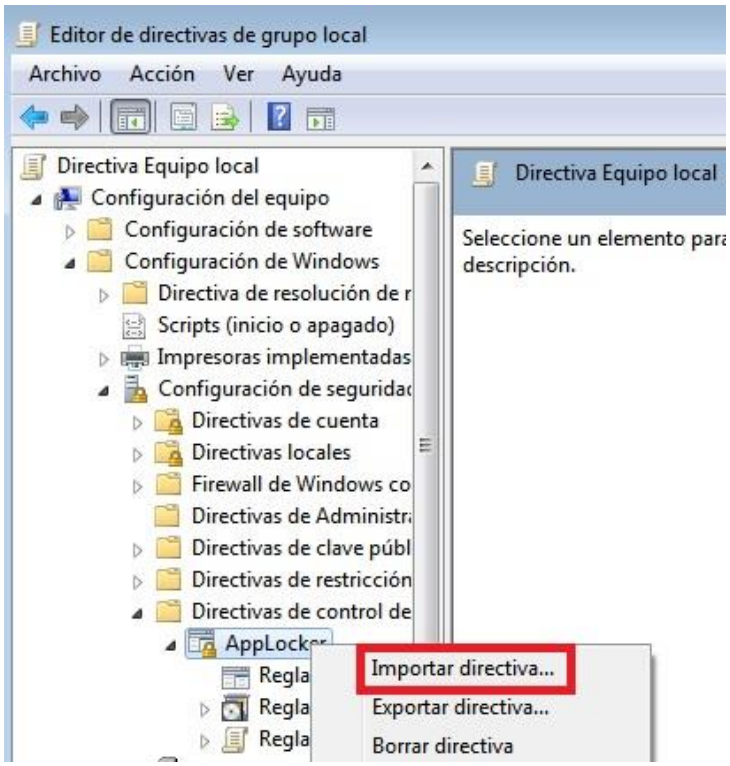
8.	Tras la exportación se presentará el siguiente mensaje informativo.



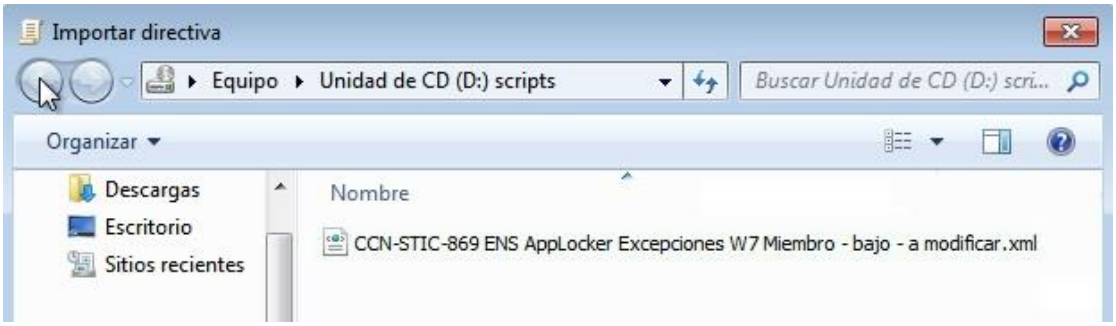
Una vez exportada la política de AppLocker definida en el GPO de excepciones seleccionado, se procederá a la importación de la misma en un equipo de referencia Windows 7 Enterprise que pertenezca al dominio pero no reciba reglas de AppLocker por GPO de dominio.

Paso	Descripción
9.	Inicie sesión en la máquina de referencia con un usuario con permisos administrativos.

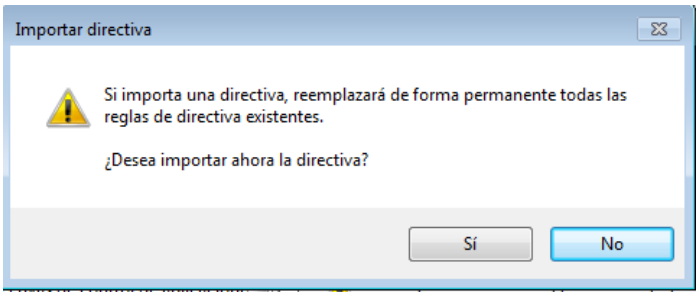
Nota: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.

Paso	Descripción
10.	Traslade el fichero XML recién exportado (CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo- a modificar.xml) a la máquina de referencia. En dicha máquina y haciendo uso de la herramienta "**GPedit.msc**" proceda a importar la configuración de AppLocker tal y como se indica a continuación. También debe trasladar a la máquina de referencia el fichero ejecutable que se desea restringir ya que durante el proceso de creación de la regla será necesario para calcular su hash. En este caso se ha usado un ejecutable de ejemplo llamado "ejemplo.exe". **Nota:** Puede lanzar "GPedit.msc" desde el menú "Ejecutar" de Windows (pulsando la combinación de teclas "Windows + R").
11.	Una vez abierto el "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Escoja la opción "Importar directiva..." del menú contextual que aparece tras pulsar botón derecho sobre la ubicación señalada arriba.  **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.

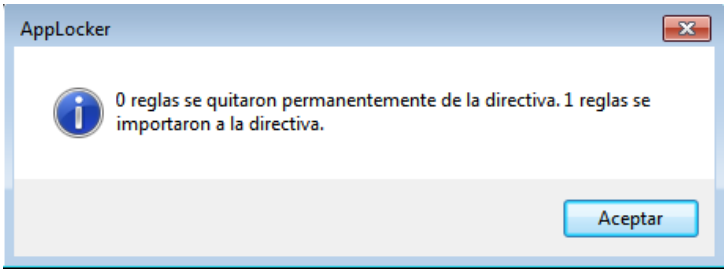
Paso	Descripción
12.	En el cuadro de dialogo abierto navegue hasta el directorio donde haya depositado el XML a importar y selecciónelo.



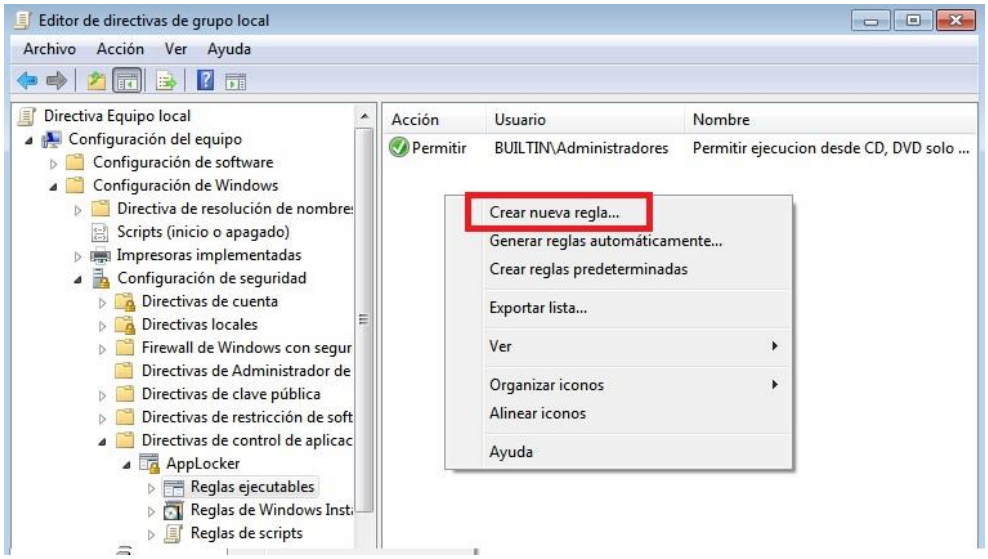
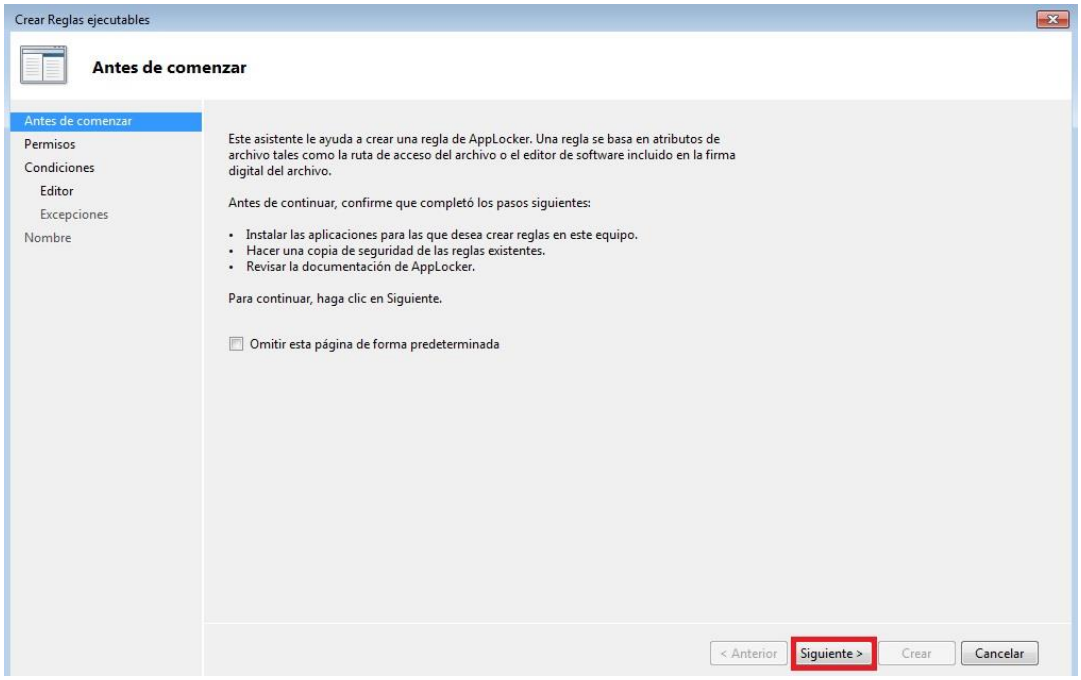
13.	Puede que se le solicite confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Si es así seleccione “Sí”.

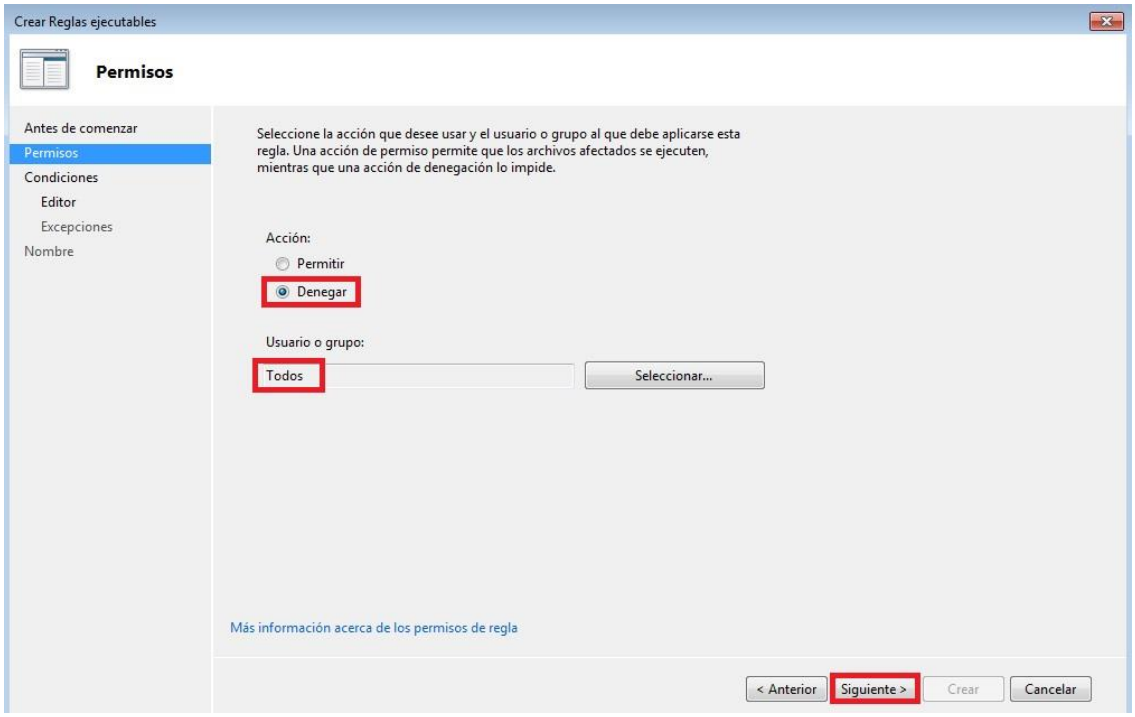
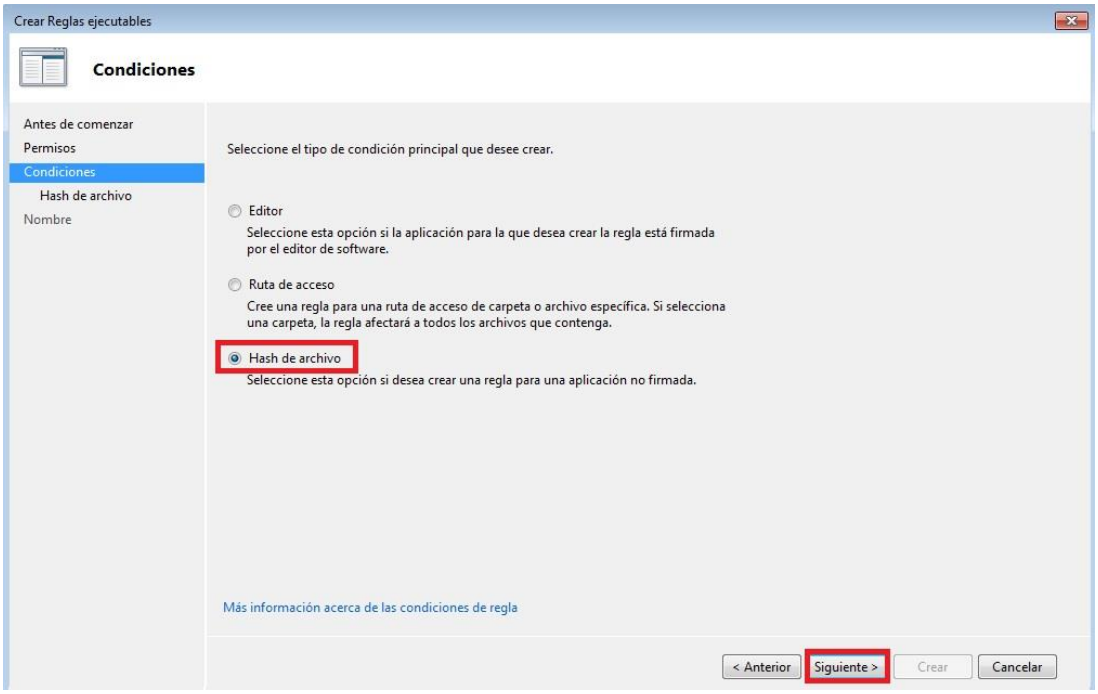


14.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.

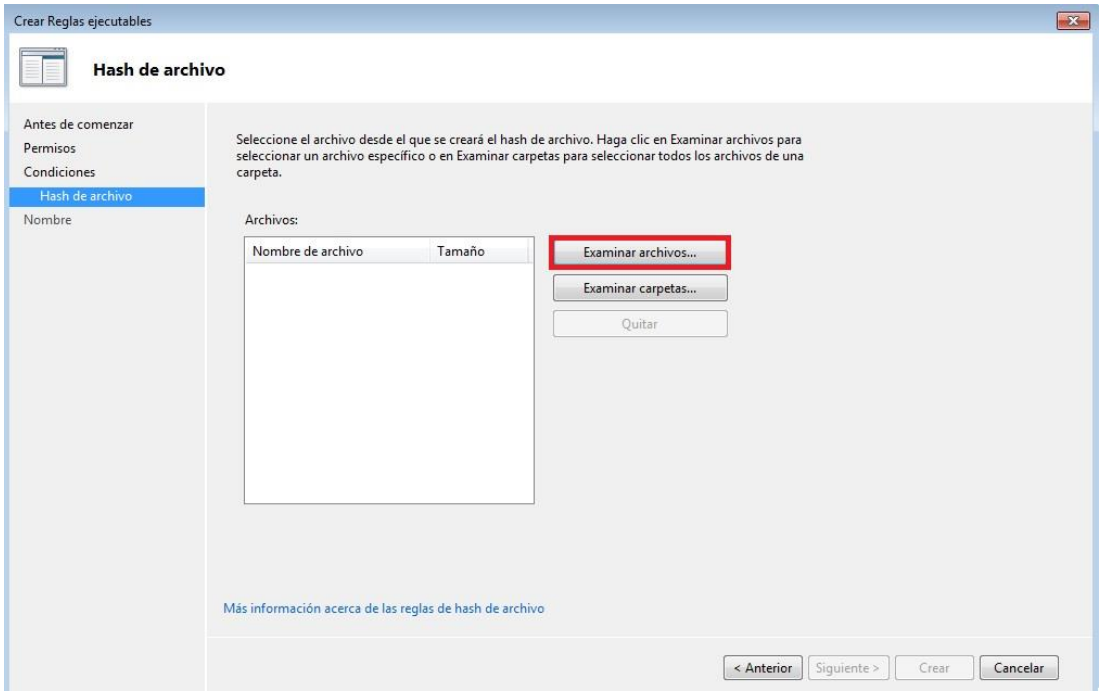


Nota: Se importa una única regla ya que se está usando la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”, que contiene una única regla de excepción para permitir ejecución de binarios ubicados en CD o DVD.

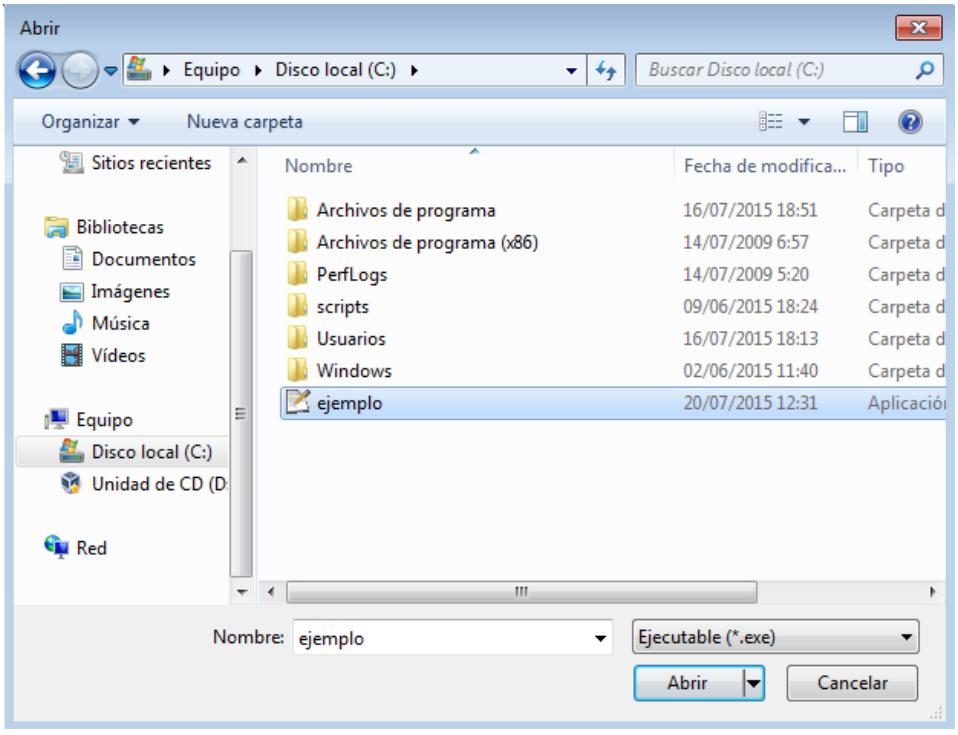
Paso	Descripción
15.	Para crear una nueva regla, en el “Editor de directivas de grupo local” navegue hasta la ubicación indicada y seleccione la opción “Crear nueva regla…” del menú contextual que aparece tras pulsar botón derecho en el panel derecho. **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables** 
16.	En la primera pantalla del asistente desplegado pulsar sobre el botón “Siguiente >”. 

Paso	Descripción
17.	En el siguiente menú se debe seleccionar el tipo de regla (permiso o denegación) y los usuarios o grupos de usuarios al que aplicará. En éste caso se debe seleccionar la opción “Denegar” y a continuación pulsar el botón “Siguiente >”. No es necesario seleccionar usuarios o grupos ya que por defecto la regla aplica al grupo “Todos”. 
18.	En la siguiente ventana se debe escoger la condición de la regla. En este caso seleccione “Hash de archivo” y pulse el botón “Siguiente >”. 

Paso	Descripción
19.	En esta ventana se debe seleccionar el archivo o archivos a los que aplicará la regla. Pulse “examinar archivos” para escoger el fichero a restringir.

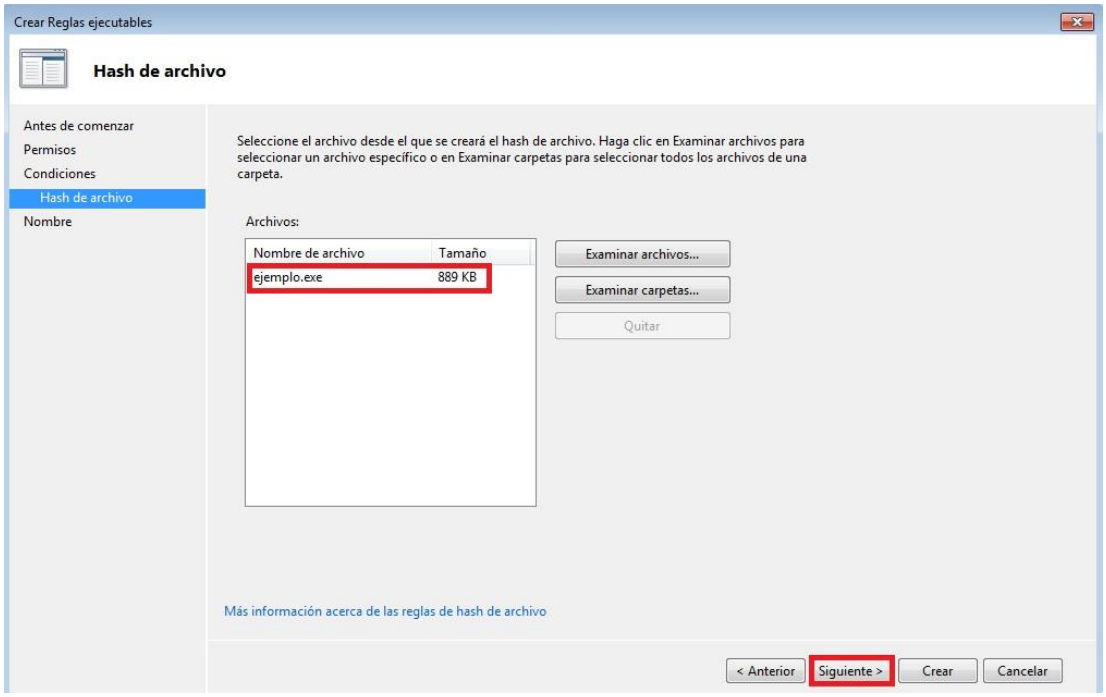


20.	En el explorador de ficheros navegue hasta la ubicación del fichero, selecciónelo y pulse “Abrir”.

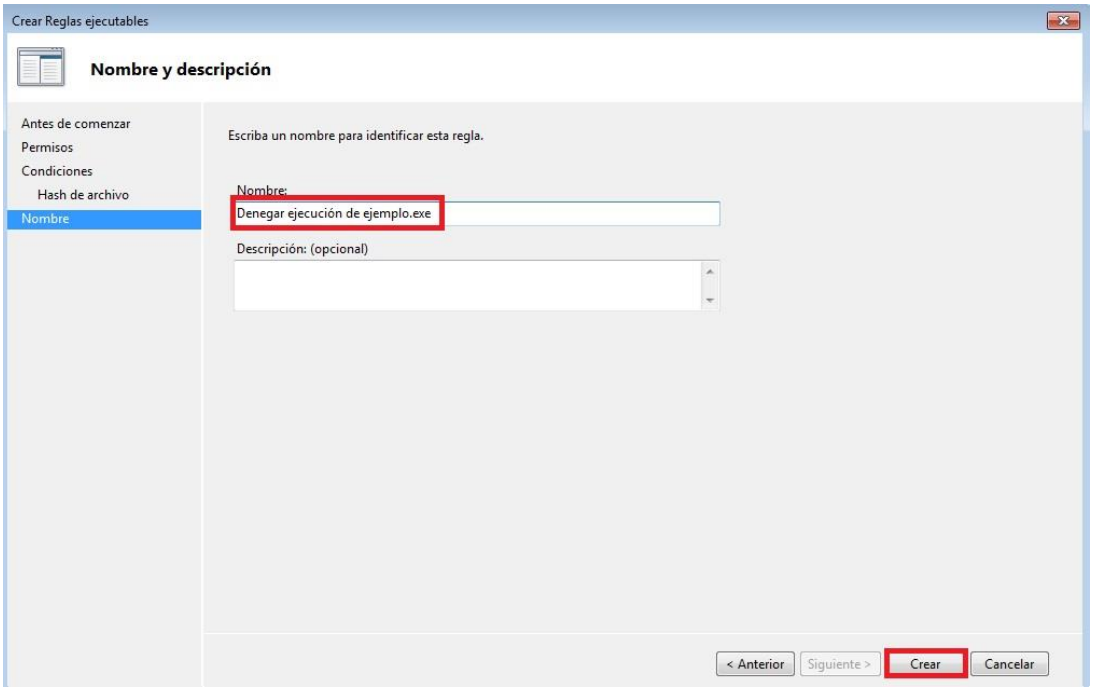


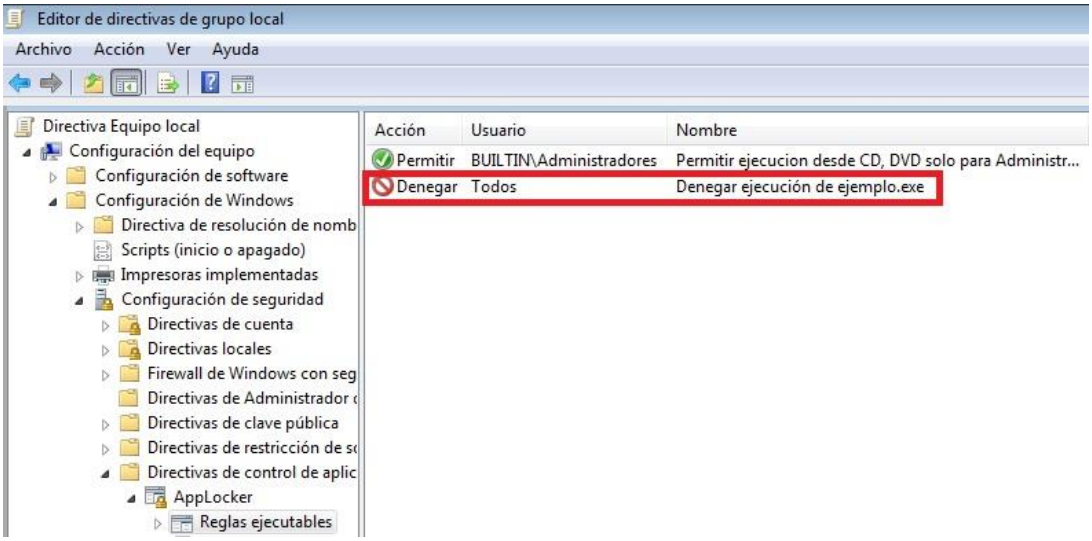
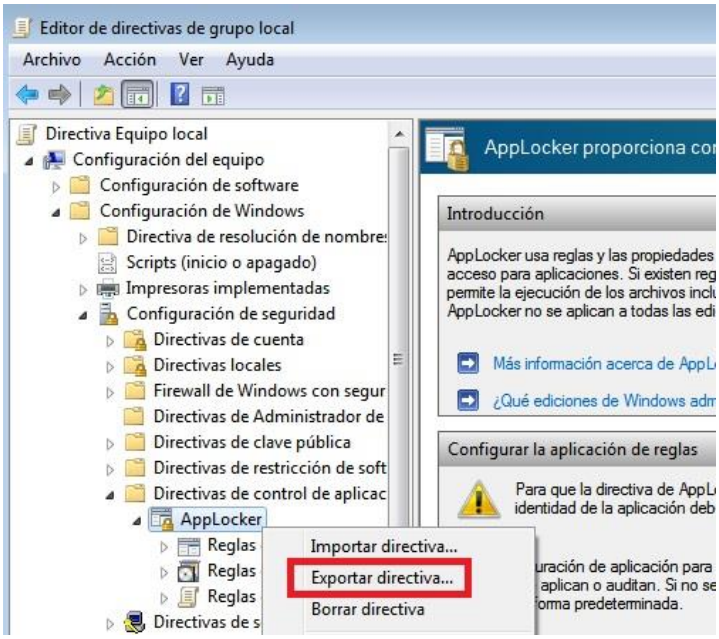
Paso	Descripción

21. En la siguiente ventana confirme que se ha seleccionado el ejecutable y pulse el botón “Siguiente >”.



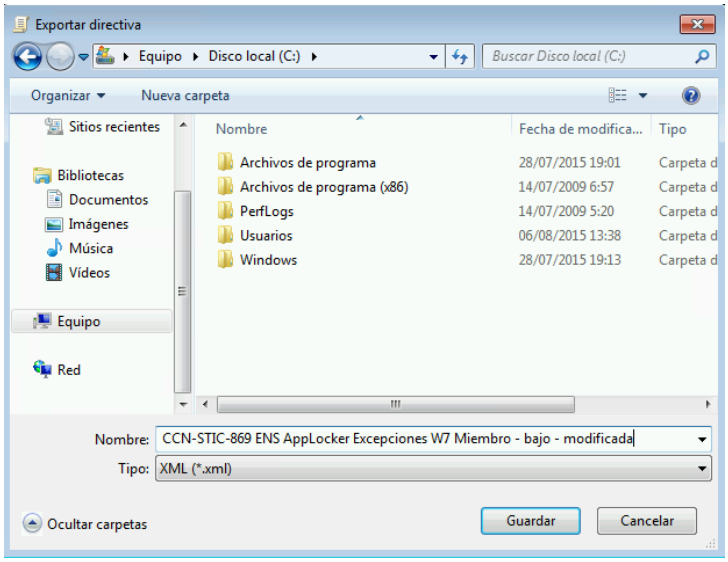
22. Introduzca un nombre descriptivo para la regla en el campo Nombre. En este caso se ha usado “Denegar ejecución de ejemplo.exe”. También puede incluir de manera opcional una descripción más detallada de la regla. Tras introducir el nombre pulse el botón “Crear”.



Paso	Descripción
23.	En el mismo "Editor de directivas de grupo local" de la máquina de referencia seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe que se ha creado la nueva regla. 
24.	Una vez verificada la creación de la nueva regla, en el mismo "Editor de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Exportar directiva…” del menú de contexto que aparece tras pulsar el botón derecho sobre la ubicación señalada. 

Paso	Descripción

25. En el menú de navegación seleccione una ubicación con permisos de escritura y guarde la configuración exportada. En este caso se usa el nombre “CCN-STIC-869 ENS AppLocker Excepciones – W7 Miembro –bajo- modificada.xml”.



Nota: No cierre todavía el Editor de directivas de grupo local.

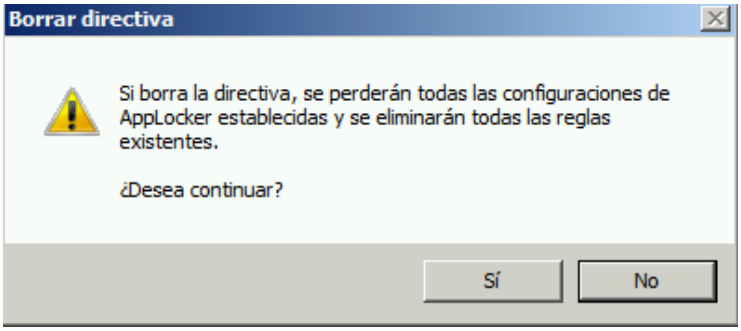
26. Haciendo uso del mismo editor de directivas de grupo local usado para modificar las reglas de AppLocker, proceda a la eliminación de directiva para dejar así el entorno preparado para una nueva importación y edición de directivas.

    En el mismo "Editor de administración de directivas de grupo local”, seleccione la siguiente ubicación:

    Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

    Elija la opción “Borrar directiva” del menú de contexto que aparece tras pulsar el botón derecho sobre la ubicación señalada.

Paso	Descripción
27.	Pulse “Si” en el cuadro de dialogo abierto.

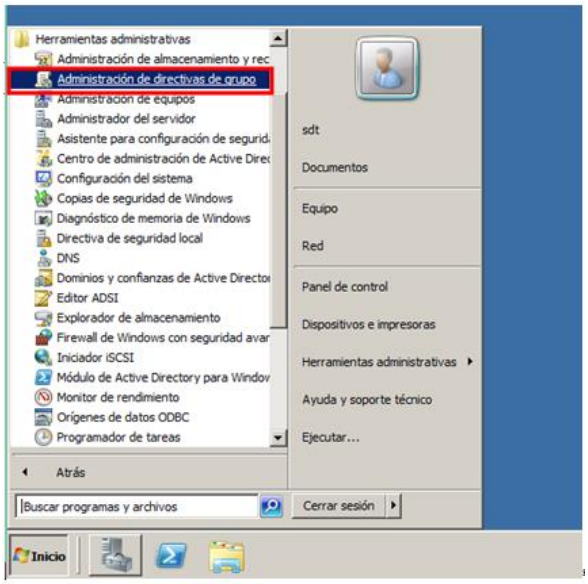


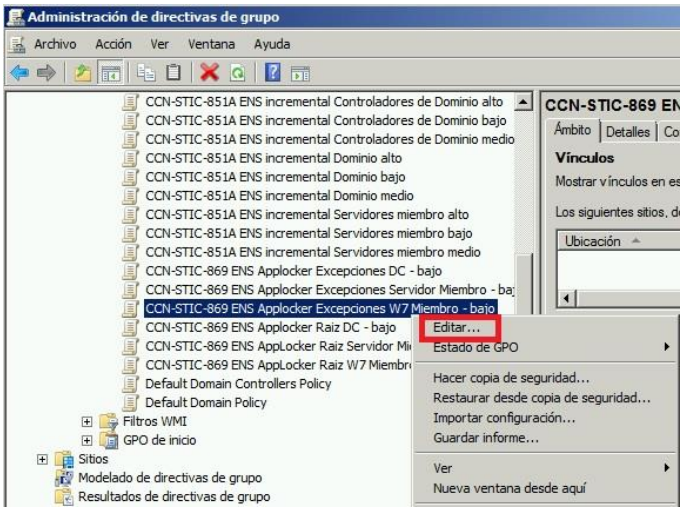
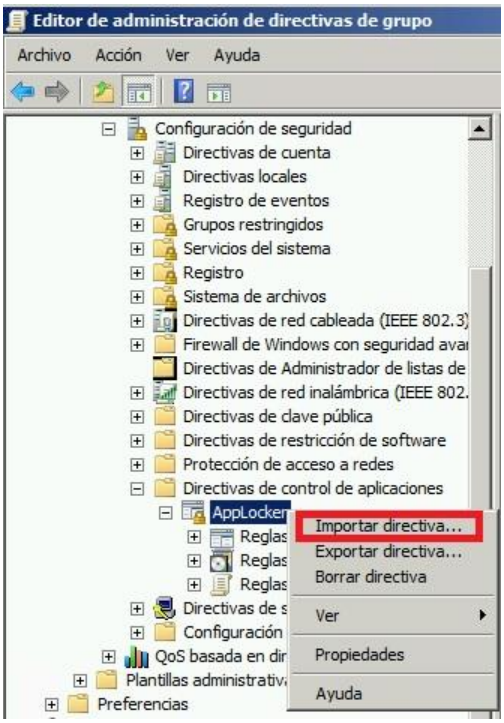
28.	Ya puede cerrar la ventana del “Editor de directivas de grupo local”.

Una vez preparada la nueva directiva con las modificaciones necesarias para su entorno, se procederá a la importación de la misma en el GPO de excepciones que aplique a las máquinas que han de recibir las nuevas reglas.

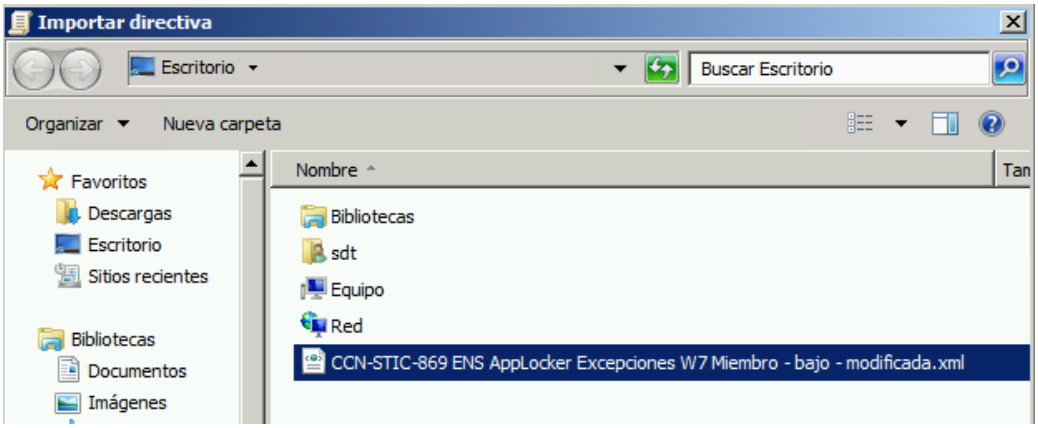
Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

Paso	Descripción
29.	Inicie sesión en el servidor Controlador de Dominio con una cuenta que sea Administrador del Dominio.
30.	Copie el archivo XML exportado de la máquina de referencia al controlador de dominio. En el presente ejemplo se llama “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml”
31.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo**

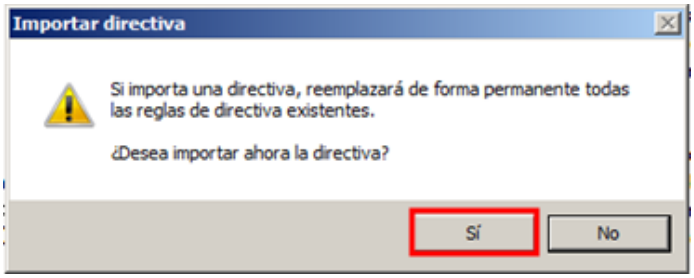


Paso	Descripción
32.	Seleccione el GPO de excepciones a modificar. En este ejemplo se han editado las reglas de AppLocker definidas en el GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Navegue hasta el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo** Marcando con el botón derecho en el GPO, elija la opción "Editar..." del menú contextual que aparecerá. 
33.	En el "Editor de administración de directivas de grupo", seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Importar directiva..." del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 

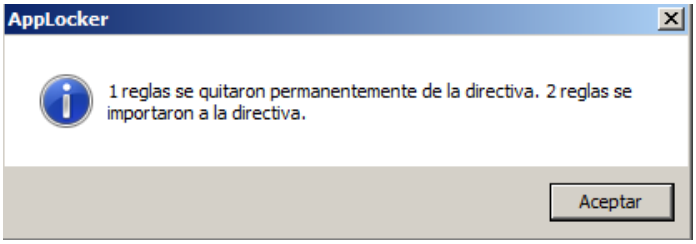
Paso	Descripción
34.	En el cuadro de diálogo abierto navegue hasta el directorio donde haya depositado el archivo XML previamente modificado en la máquina de referencia, selecciónelo y ábralo haciendo doble clic sobre él o pulsando el botón “Abrir”.

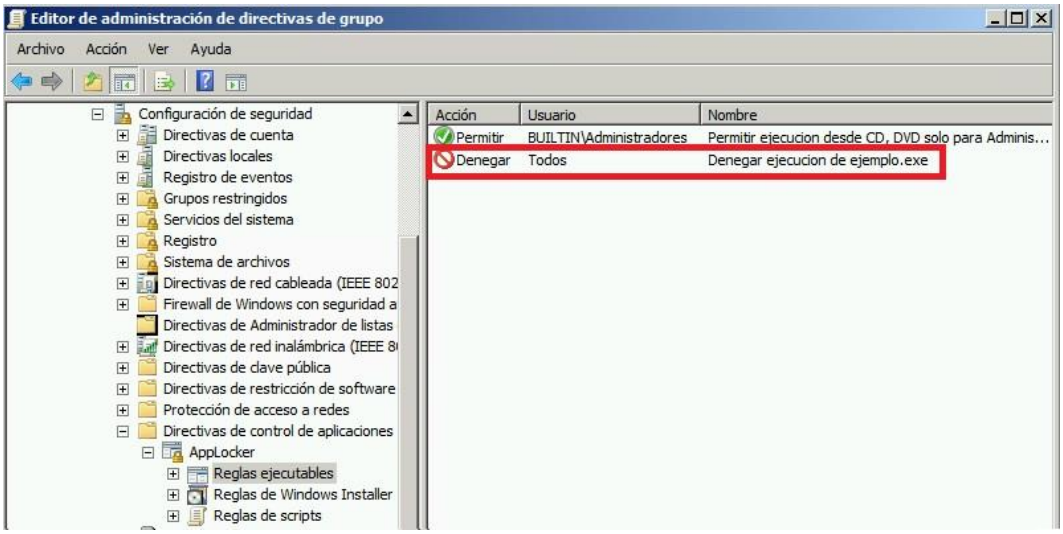


35.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



36.	Aparecerá un nuevo mensaje informativo indicando que se importaron tantas reglas como se hayan creado/modificado reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.



Paso	Descripción
37.	En el “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe en el menú que la nueva regla para denegar la ejecución del binario seleccionado se ha creado de manera correcta. 
38.	Ya puede cerrar el “Editor de Administración de directivas de grupo” habiendo quedado importadas al GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo**” todas las modificaciones realizadas en la máquina de referencia
39.	Los clientes Windows 7 recogerán la política de manera automática. No obstante, puede reiniciarlos para forzar el cambio.

6. PASO A PASO PARA LA CREACIÓN DE REGLA QUE PERMITA LA EJECUCIÓN DE BINARIOS DE INICIO DE SESIÓN DESPLEGADOS POR GPO

En la siguiente tabla se detalla el procedimiento a seguir para la creación de una nueva regla que permita la ejecución de binarios desde las carpetas compartidas donde se suelen ubicar y ejecutar los scripts de inicio (\\<nombre de dominio>\sysvol\<nombre de dominio>\policies y (\\<nombre de dominio>\NETLOGON). Esta excepción puede llegar a ser necesaria si existen políticas de equipo o usuario que lanzan ejecutables en el inicio de sesión

La implementación de AppLocker detallada en esta guía para los distintos niveles del Esquema Nacional de seguridad se ha diseñado de tal manera que las nuevas reglas, o excepciones se han de definir editando los GPO de excepciones.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel bajo del ENS son:

- CCN-STIC-869 ENS AppLocker Excepciones DC – bajo: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.
- CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.

– CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Nota: Tenga en cuenta que para el nivel bajo del ENS las reglas definidas no se encuentran aplicadas, sólo se audita la ejecución de binarios. Las excepciones o nuevas reglas que cree en los GPO para nivel bajo, se aplicarán igualmente en modo auditoría.

Los GPO destinados a albergar excepciones o nuevas reglas para el nivel medio o alto del ENS son:

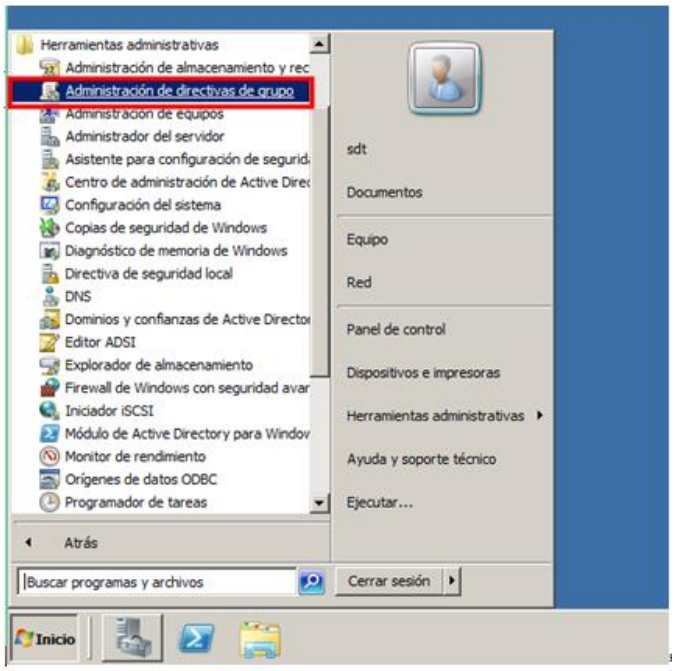
– CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre controladores de dominio.

– CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre clientes Windows 7.

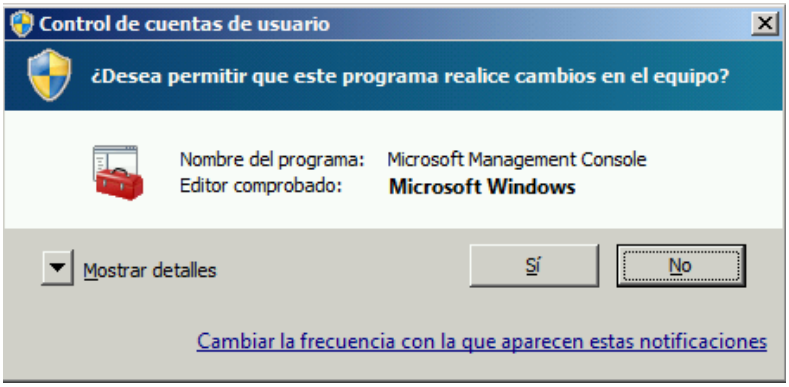
– CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto: Destinado a recibir las nuevas reglas que apliquen sobre servidores miembros del dominio.

Los pasos que se describen a continuación se realizarán en un controlador de dominio donde se realizará la implementación de las políticas GPO necesarias para permitir la ejecución de aplicaciones desde rutas no estándares.

En este caso y a modo de ejemplo, se editará el GPO de excepciones que aplica sobre los clientes Windows 7 de la organización para una implementación del Esquema Nacional de Seguridad en nivel bajo. Dependiendo de sus necesidades deberá adaptar el siguiente procedimiento para que aplique a otras máquinas o niveles de implementación del Esquema Nacional de Seguridad.

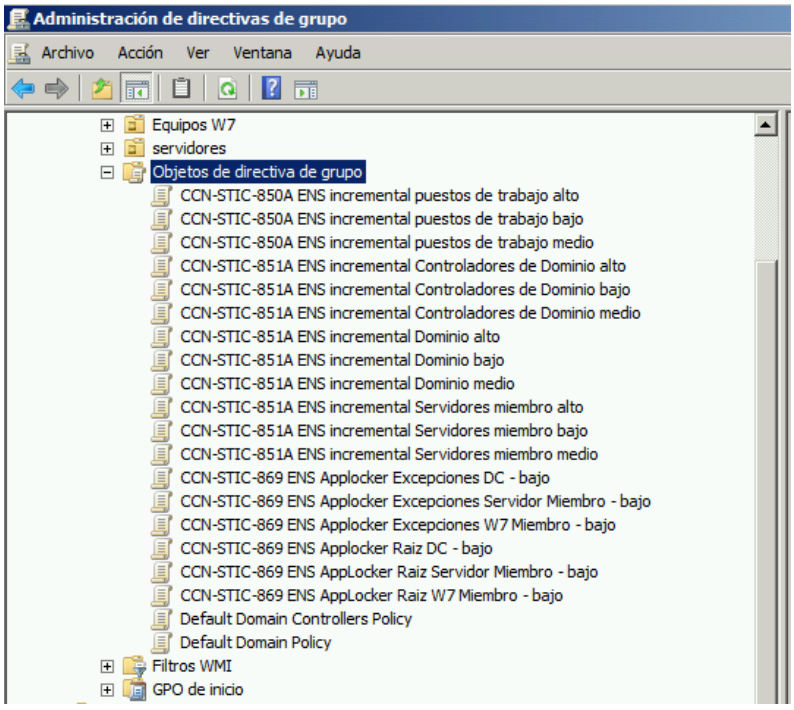
Paso	Descripción
1.	Inicie sesión en el servidor Controlador de Dominio con una cuenta con derechos de administración en el dominio.
2.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio: **Inicio → Herramientas administrativas → Administración de directivas de grupo** 

Paso	Descripción
3.	Pulse “Sí” en la ventana Control de cuentas de usuario para permitir ejecutar la consola de Administración de directivas de grupo con permisos administrativos.



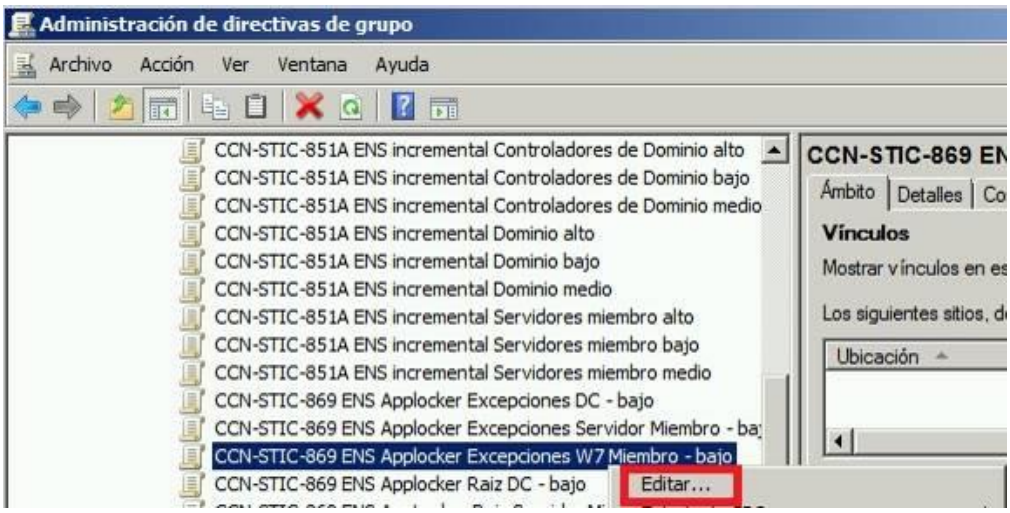
Nota: Dependiendo de la configuración del Control de Cuentas de Usuario implementada en el cliente independiente, la ventana informativa puede diferir de la aquí presentada. Puede que se le soliciten credenciales de usuario con permisos de administración local.

4. Expanda el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo,** como se muestra en la siguiente imagen.



Paso	Descripción

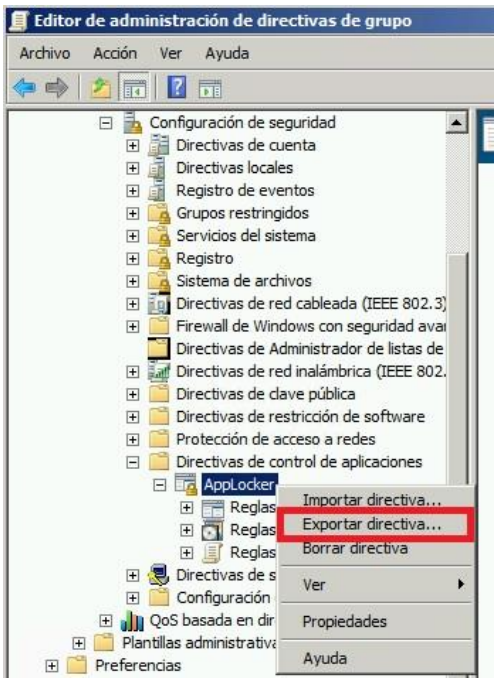
5. Seleccione el GPO de excepciones a modificar. En este ejemplo se pretende modificar la colección de reglas de AppLocker aplicadas a clientes Windows 7 a los que les aplica el nivel bajo del ENS. Por lo que se procederá a la edición del GPO "**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**". Marcando con el botón derecho en él, elija la opción "Editar..." del menú contextual que aparecerá.



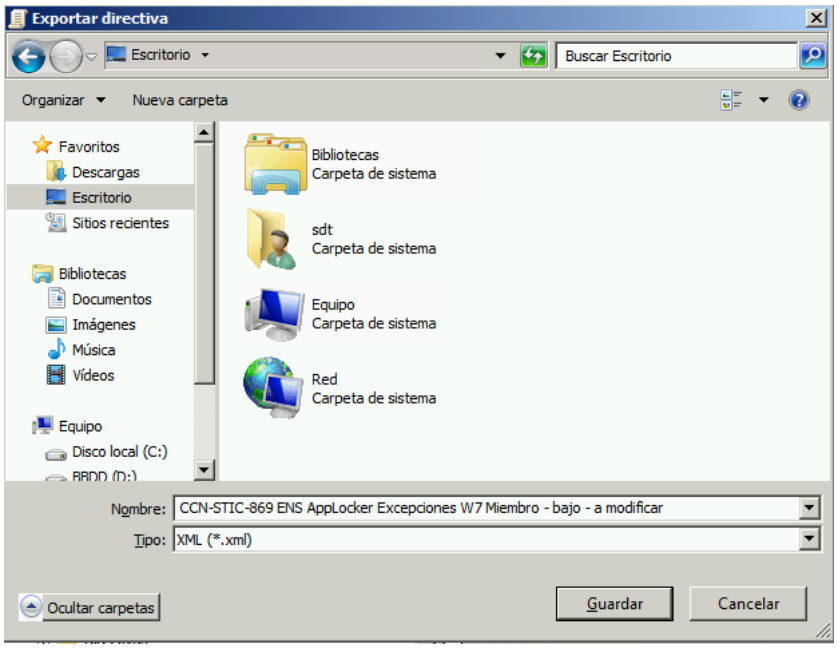
Nota: El GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo" está diseñado para recibir las excepciones o nuevas reglas que se quieran aplicar a los Equipos W7 de la organización. Si necesita crear excepciones que apliquen a servidores miembros o a los controladores de dominio, seleccione el GPO adecuado según se describe al comienzo del presente apartado.

6. En el "Editor de administración de directivas de grupo" seleccione la ubicación que se describe a continuación y marcando con el botón derecho en ella, elija la opción "**Exportar directiva**".

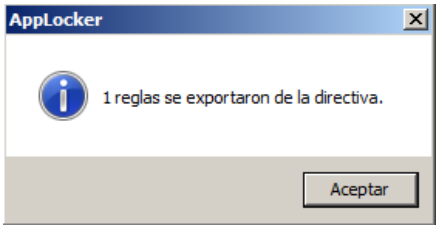
Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker



Paso	Descripción
7.	En el cuadro de diálogo abierto navegue hasta un directorio con permisos de escritura y guarde la política exportada en formato xml. Elija un nombre reconocible.

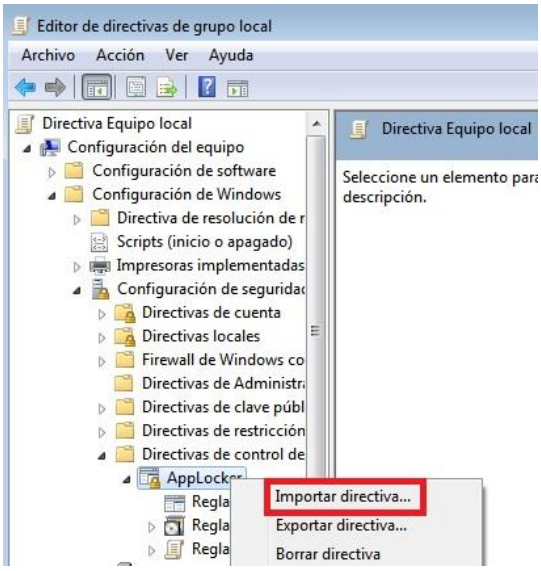
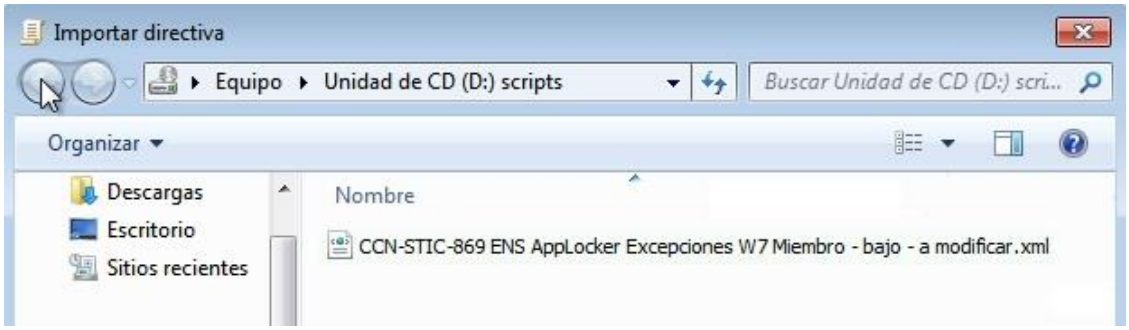
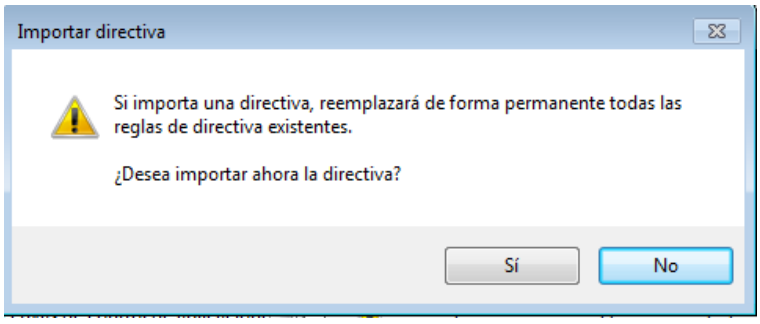


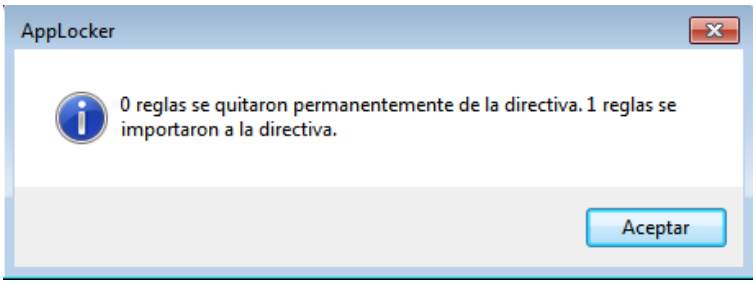
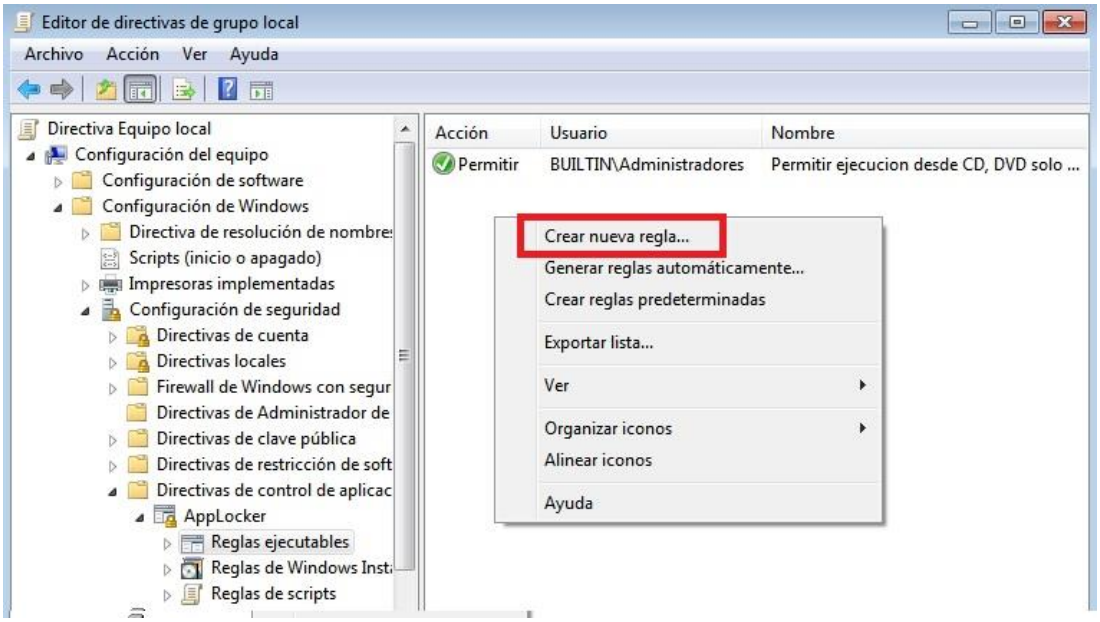
8.	Tras la exportación se presentará el siguiente mensaje informativo.



Una vez exportada la política de AppLocker definida en el GPO de excepciones seleccionado, se procederá a la importación de la misma en un equipo de referencia Windows 7 Enterprise que pertenezca al dominio pero no reciba reglas de AppLocker por GPO de dominio.

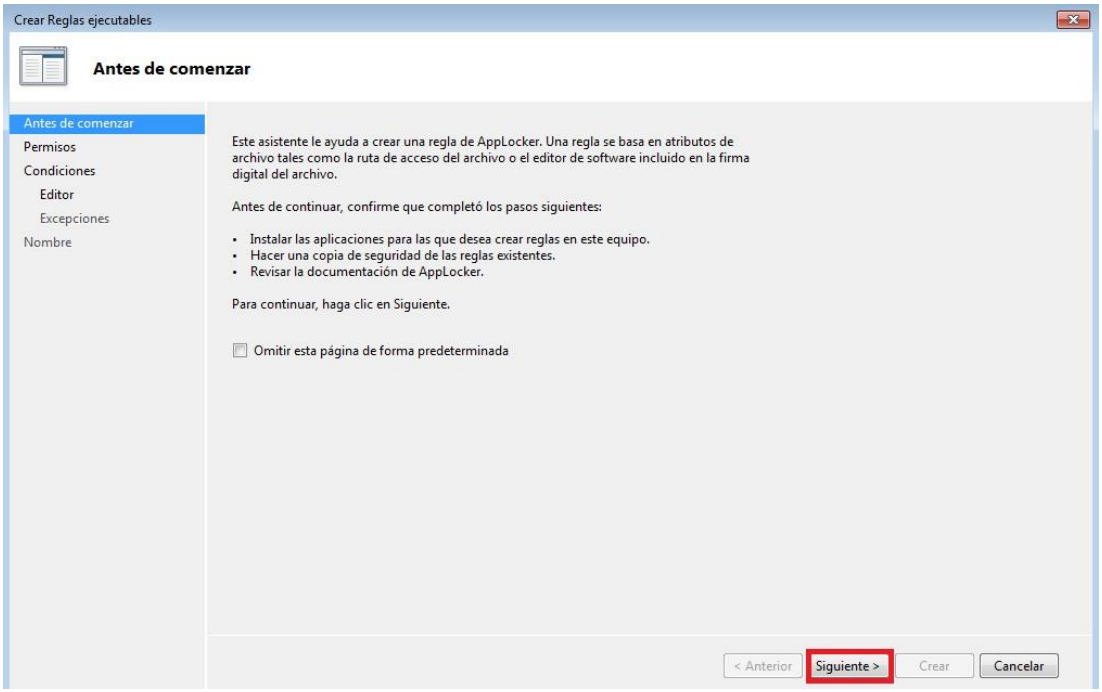
Paso	Descripción
9.	Inicie sesión en la máquina de referencia con un usuario con permisos administrativos. **Nota**: La máquina de referencia debe pertenecer al dominio (para poder seleccionar los grupos de usuarios necesarios en la edición de reglas) pero no ha de tener políticas de AppLocker activas. En este ejemplo, se ha usado un Windows 7 Enterprise al que no le aplican las GPO de AppLocker de dominio. Las operaciones de importación, edición y exportación necesitan de permisos de administración local.
10.	Traslade el fichero XML recién exportado (CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo- a modificar.xml) a la máquina de referencia. En dicha máquina, haciendo uso de la herramienta "**GPedit.msc**" proceda a importar la configuración de AppLocker tal y como se indica a continuación. **Nota:** Puede lanzar "GPedit.msc" desde el menú "Ejecutar" de Windows (pulsando la combinación de teclas "Windows + R").

Paso	Descripción
11.	Una vez abierto el "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Escoja la opción "Importar directiva..." del menú contextual que aparece tras pulsar botón derecho sobre la ubicación señalada arriba. 
12.	En el cuadro de dialogo abierto navegue hasta el directorio donde haya depositado el archivo XML a importar y selecciónelo haciendo doble clic sobre él o pulsando el botón "Abrir". 
13.	Puede que se le solicite confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Si es así seleccione "Sí". 

Paso	Descripción
14.	Aparecerá un nuevo mensaje informativo indicando que se importó una regla a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.  **Nota:** Se importa una única regla ya que se está usando la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo”, que contiene una única regla de excepción para permitir ejecución de binarios ubicados en CD o DVD.
15.	Para crear una nueva regla, en el “Editor de directivas de grupo local” navegue hasta la ubicación indicada y seleccione la opción “Crear nueva regla…” del menú contextual que aparece tras pulsar botón derecho en el panel derecho. **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables** 

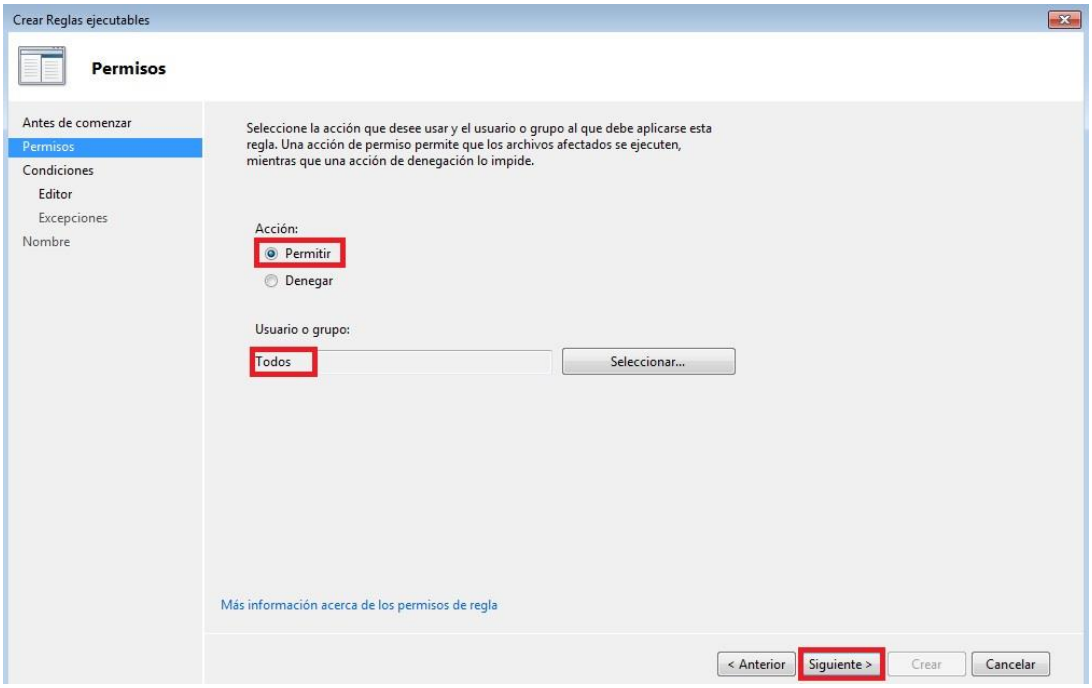
Paso	Descripción

16. En la primera pantalla del asistente desplegado pulsar sobre el botón siguiente.



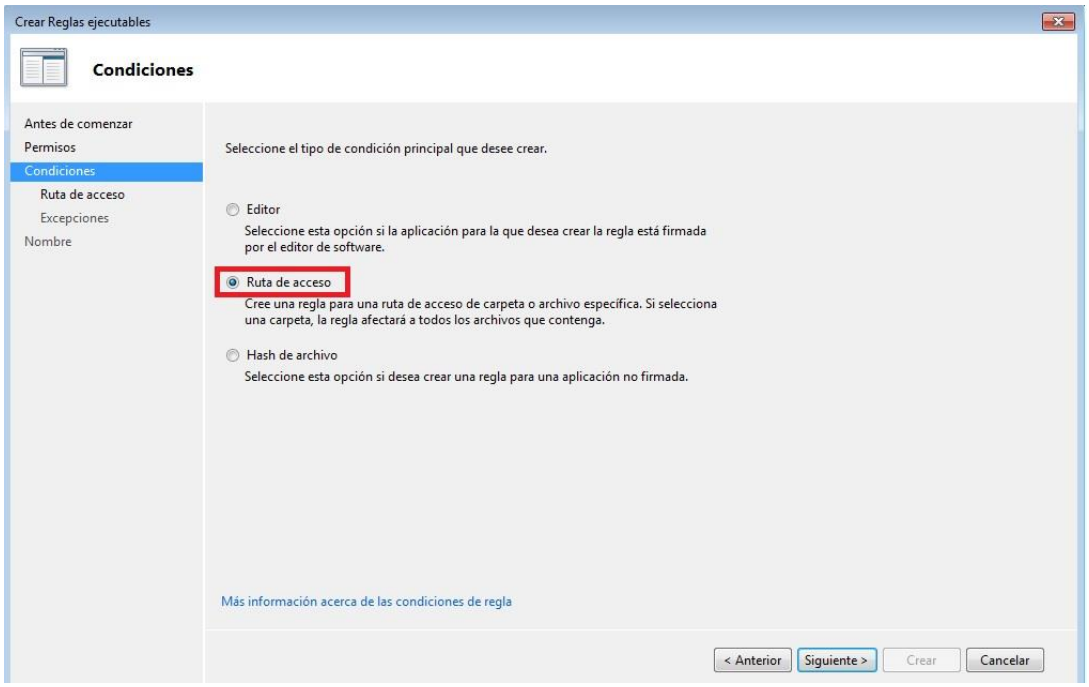
17. En el siguiente menú se debe seleccionar el tipo de regla (permiso o denegación) y los usuarios o grupos de usuarios al que aplicará.

    En éste caso se debe seleccionar “Permitir” y a continuar pulsar el botón “Siguiente >” (dejando la selección de usuarios por defecto en “Todos”).



Paso	Descripción

18. En la siguiente ventana escoger la condición de la regla. En este caso seleccione “Ruta de acceso” y pulse el botón “Siguiente >”.



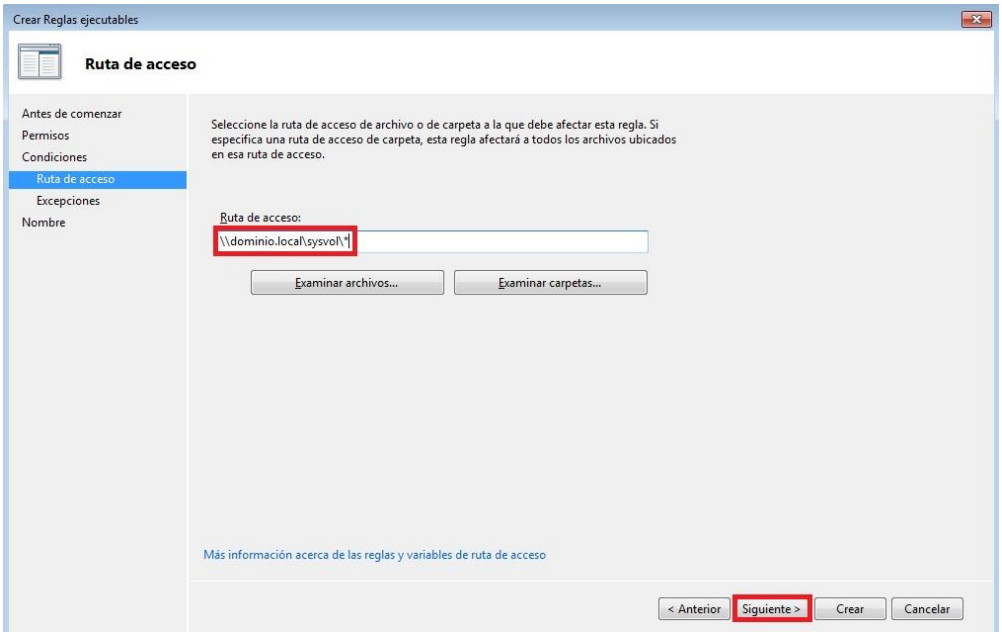
19. En el cuadro de texto “Ruta de acceso” escriba la ruta al temporal del usuario tal y como se le indica a continuación:

\\<nombre de dominio>\sysvol*

Sustituya *<nombre de dominio>* por el nombre de la carpeta del perfil del usuario elegido. En este caso quedaría:

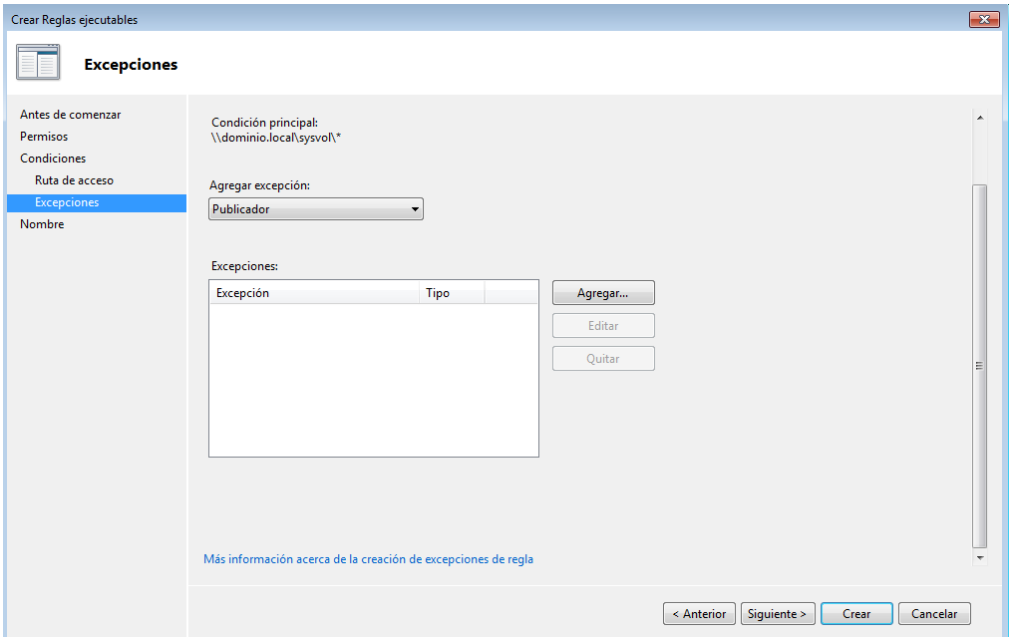
\\dominio.local\sysvol*

Pulse el botón “Siguiente >” cuando termine de escribir la ruta.

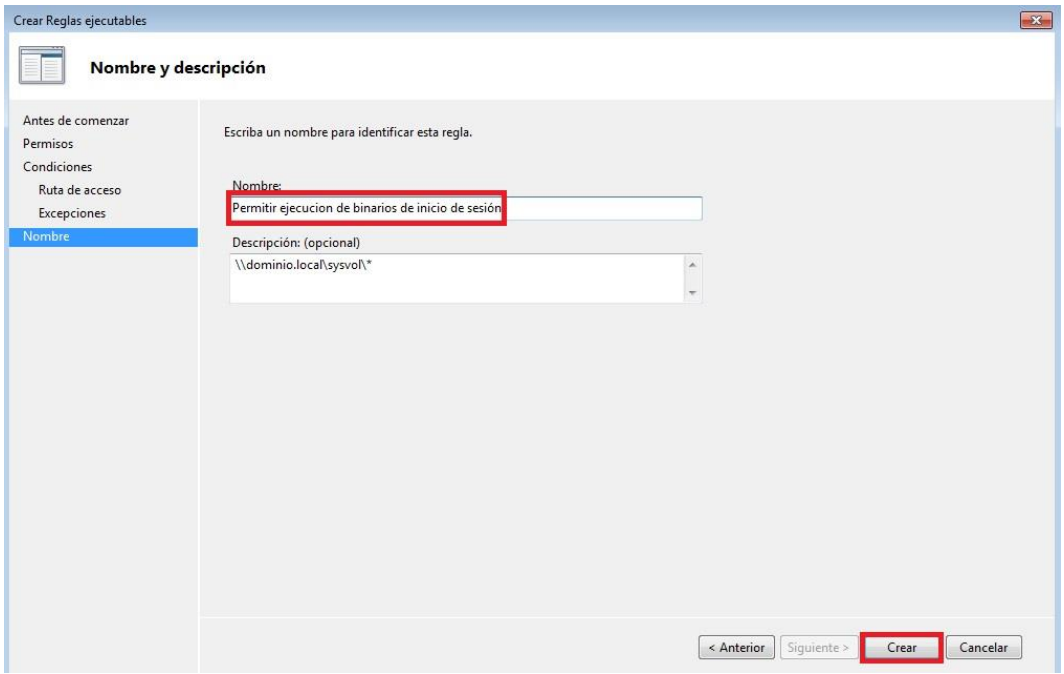


Nota: Nótese que la ruta acaba en asterisco, para así permitir todos los binarios que existan en la carpeta.

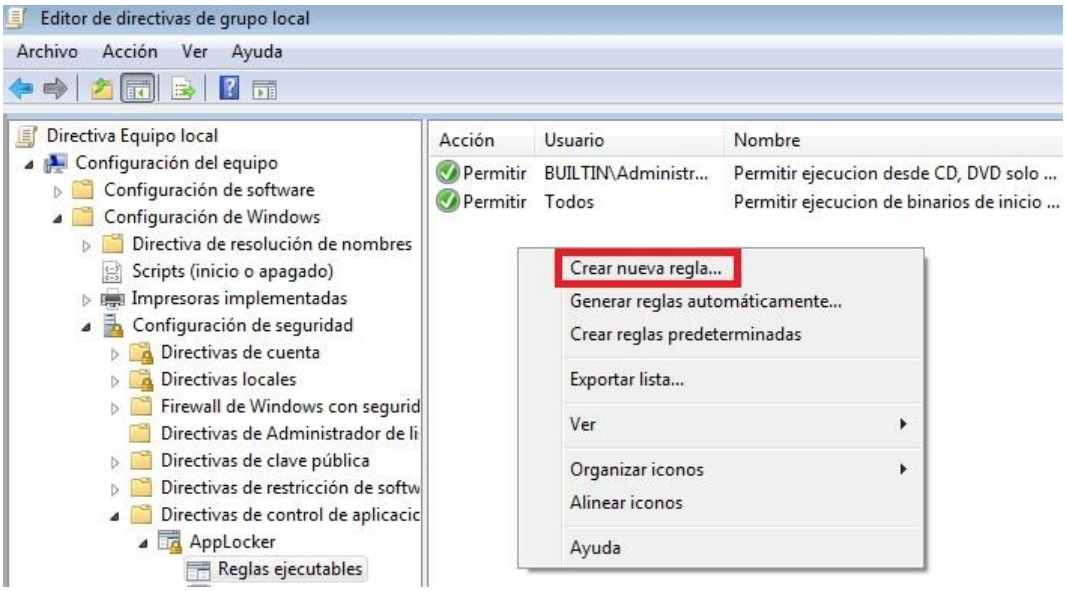
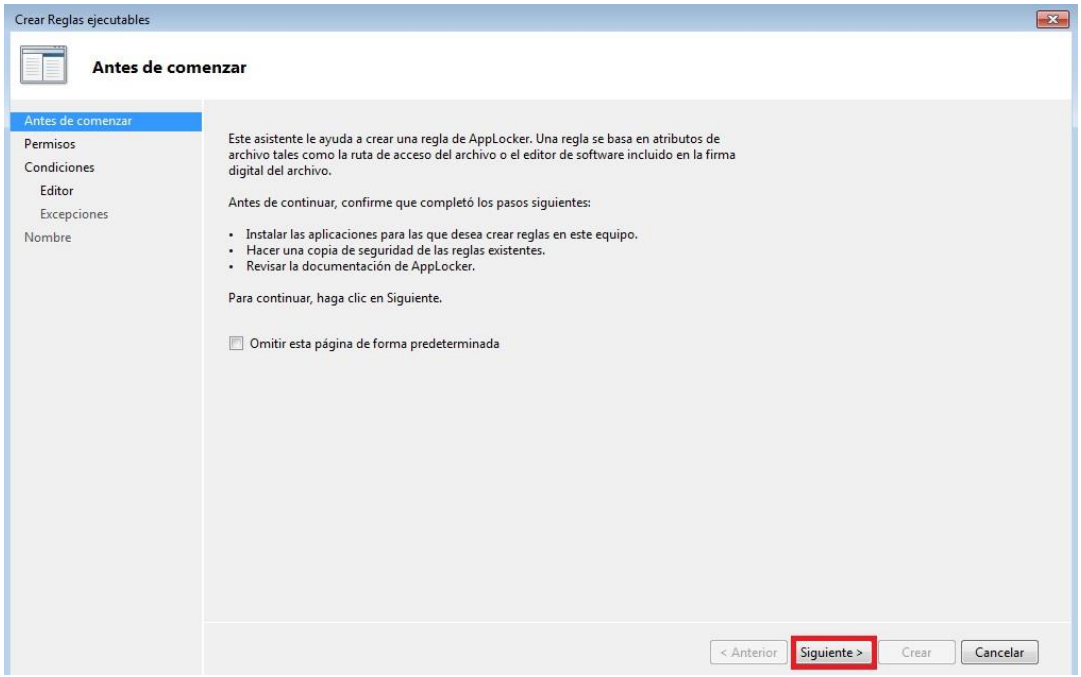
Paso	Descripción
20.	En la siguiente ventana se establecen las excepciones a la regla que se está creando. En este caso no se establecerá ninguna. Pulse el botón “Siguiente >”.



21.	Introduzca un nombre descriptivo para la regla en el campo “Nombre”. En este caso, se ha usado “Permitir ejecución de binarios de inicio de sesión”. También puede incluir de manera opcional una descripción más detallada de la regla. Tras introducir el nombre pulse el botón “Crear”.



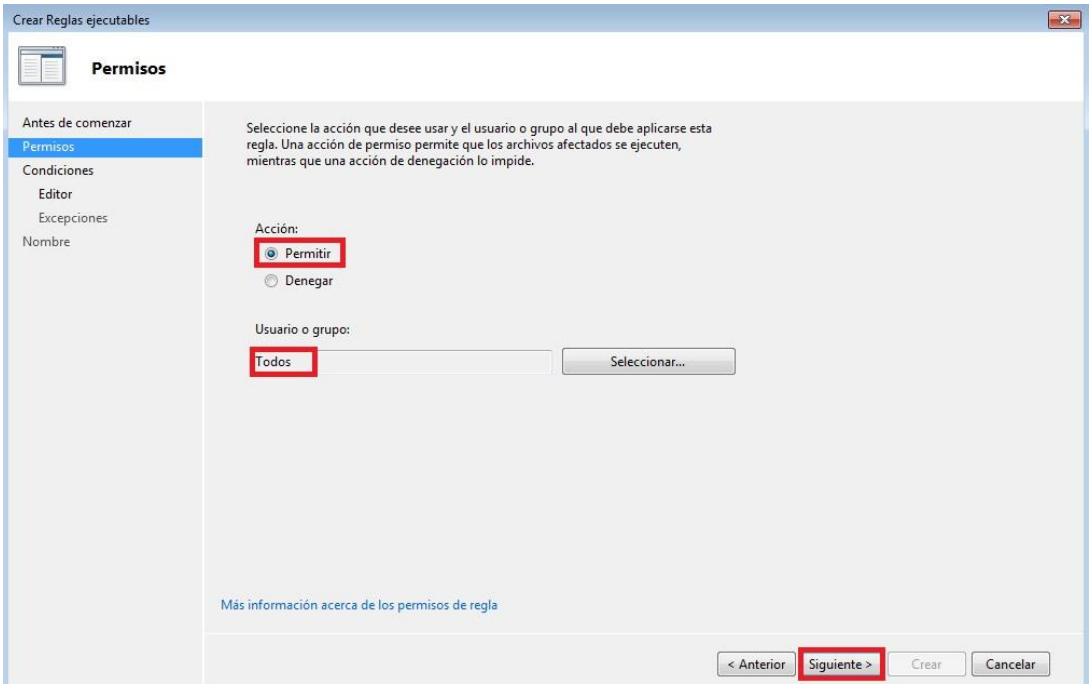
22.	Proceda a crear una segunda regla mediante el siguiente procedimiento.

Paso	Descripción
23.	Para crear una nueva regla, en el mismo “Editor de directivas de grupo local” navegue hasta la ubicación indicada y seleccione la opción “Crear nueva regla…” del menú contextual que aparece tras pulsar botón derecho en el panel derecho. **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables** 
24.	En la primera pantalla del asistente desplegado pulsar sobre el botón “Siguiente >”. 

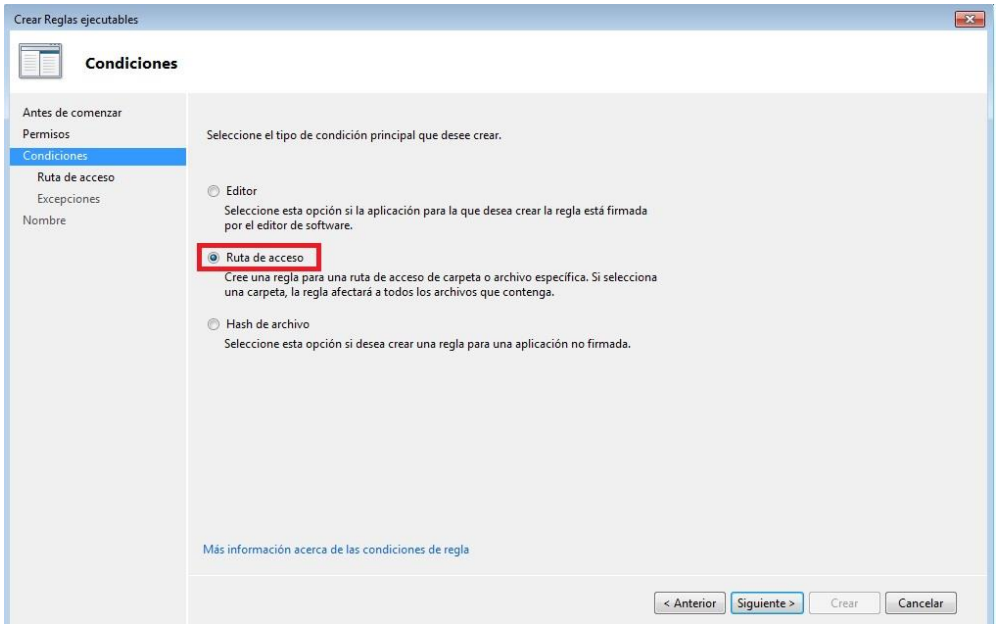
Paso	Descripción

25. En el siguiente menú, se debe seleccionar el tipo de regla (permiso o denegación) y los usuarios o grupos de usuarios a los que aplicará.

    En éste caso se debe seleccionar la opción “Permitir” y a continuación pulsar el botón “Siguiente >” (dejando la selección de usuarios por defecto en “Todos”).



26. En la siguiente ventana, escoja la condición de la regla. En este caso seleccione “Ruta de acceso” y pulse el botón “Siguiente >”.



Paso	Descripción

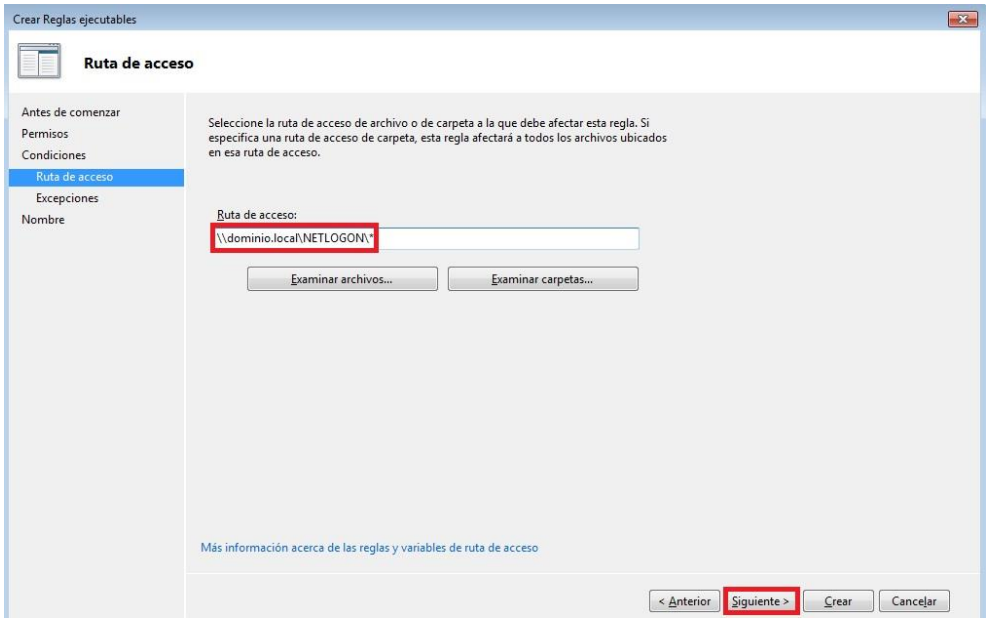
27. En el cuadro de texto “Ruta de acceso” escriba la ruta al temporal del usuario tal y como se le indica a continuación:

\\<nombre de dominio>\NETLOGON*

Sustituya *<nombre de dominio>* por el nombre de la carpeta del perfil del usuario elegido. En este caso quedaría:

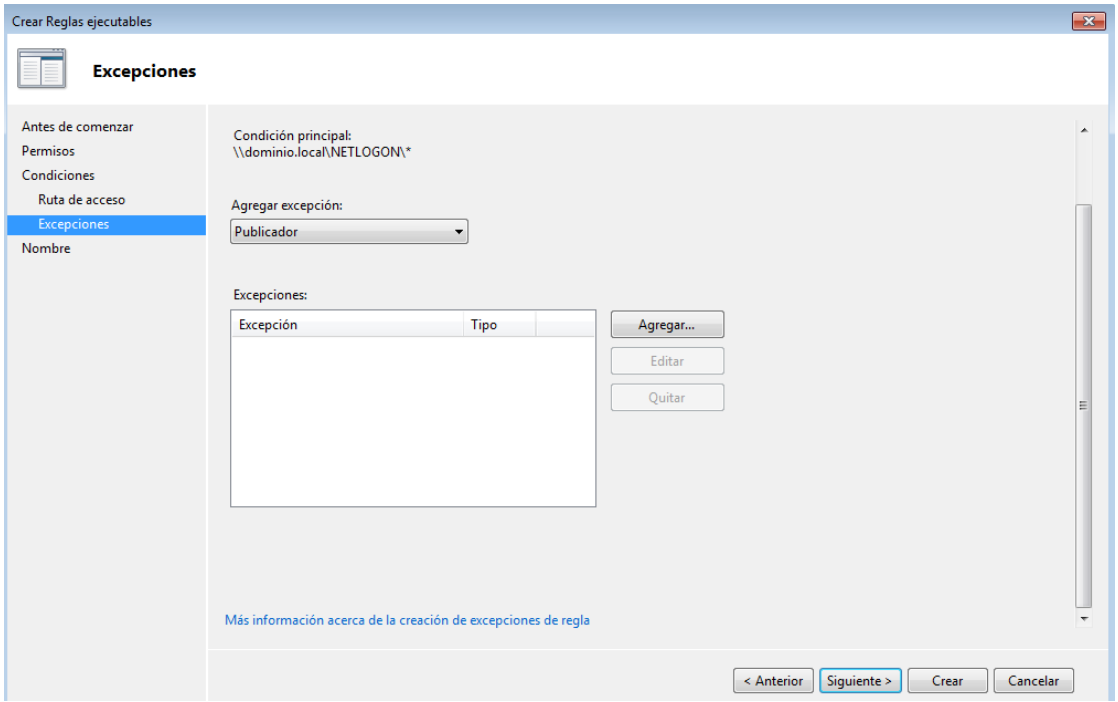
\\dominio.local\NETLOGON*

Pulse el botón “Siguiente >” cuando termine de escribir la ruta.



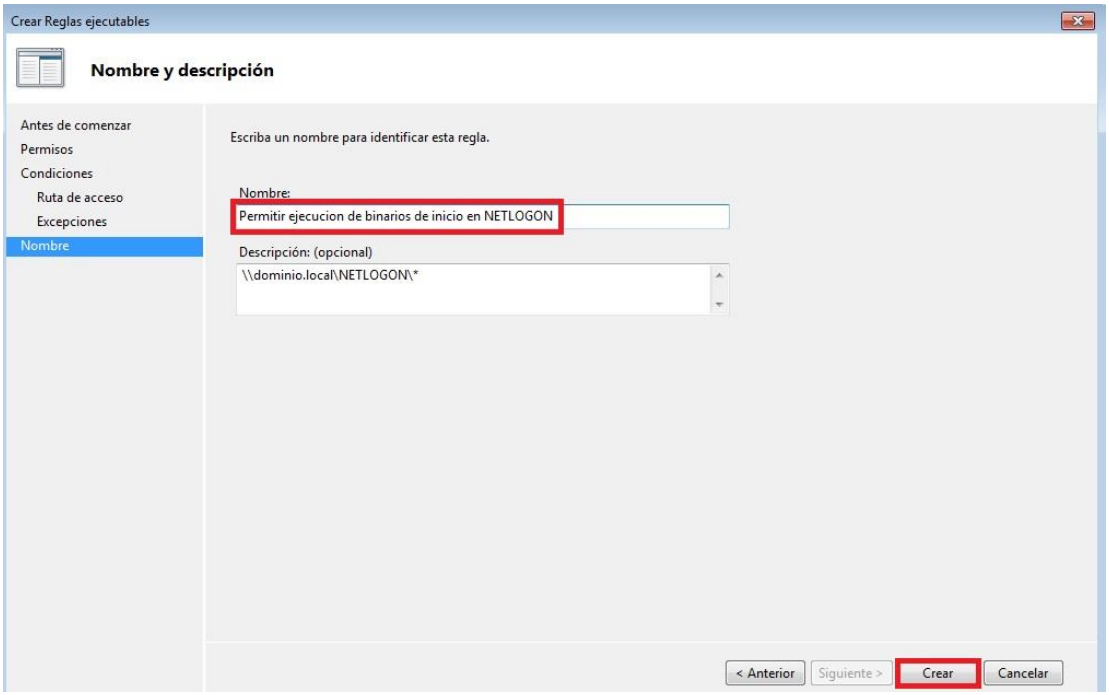
Nota: Nótese que la ruta acaba en asterisco, para así permitir todos los binarios que existan en la carpeta.

28. En la siguiente ventana se establecen las excepciones a la regla que se está creando. En este caso no se establecerá ninguna. Pulse el botón “Siguiente >”.



Paso	Descripción

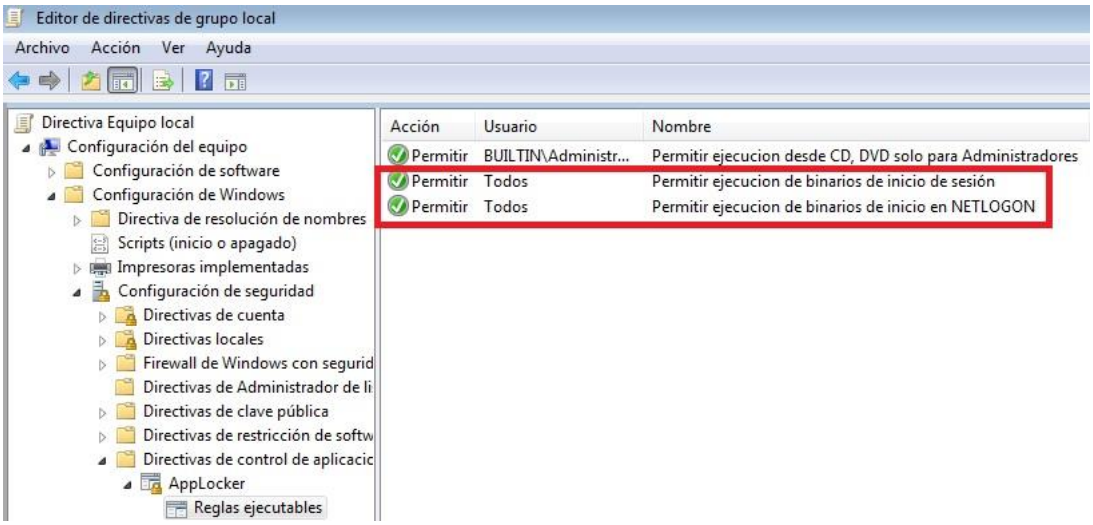
29. Introduzca un nombre descriptivo para la regla en el campo Nombre. En este caso se ha usado “Permitir ejecución de binarios de inicio en NETLOGON”. También puede incluir de manera opcional una descripción más detallada de la regla. Tras introducir el nombre pulse el botón “Crear”.



30. En el mismo "Editor de directivas de grupo local” de la máquina de referencia seleccione la siguiente ubicación:

Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables

Compruebe que se han creado las nuevas reglas.

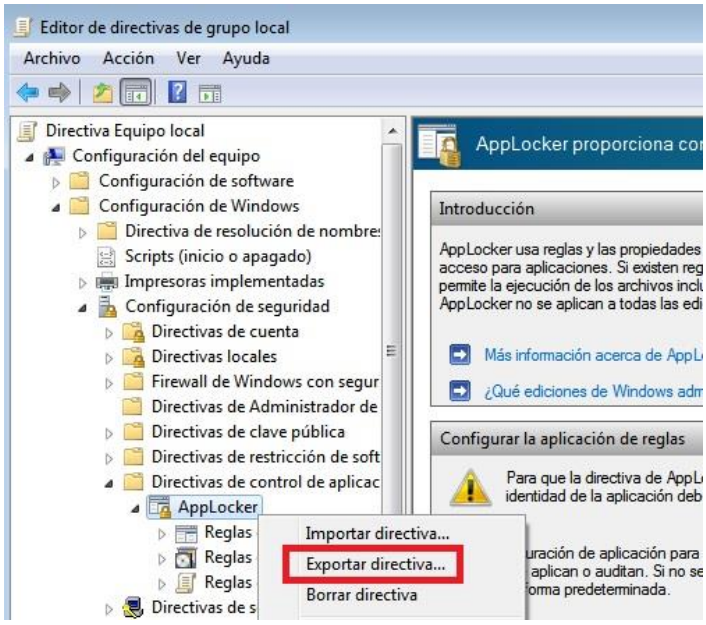


Paso	Descripción

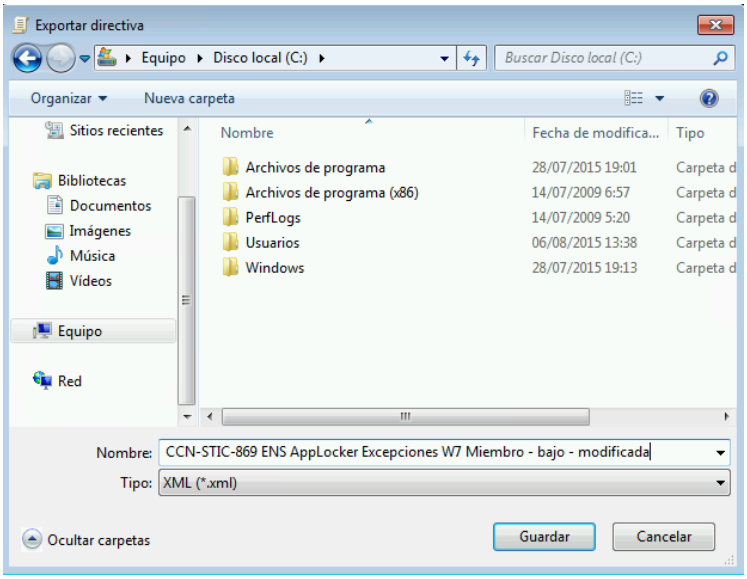
31. Una vez verificada la creación de las nuevas reglas, en el mismo "Editor de directivas de grupo local", seleccione la siguiente ubicación:

    Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker

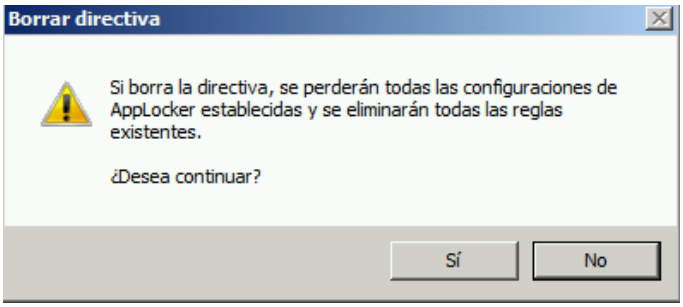
    Elija la opción "exportar directiva" del menú de contexto que aparece tras pulsar el botón derecho sobre la ubicación señalada.



32. En el menú de navegación seleccione una ubicación con permisos de escritura y guarde la configuración exportada. En este caso, se usa el nombre "CCN-STIC-869 ENS AppLocker Excepciones – W7 Miembro –bajo- modificada.xml".

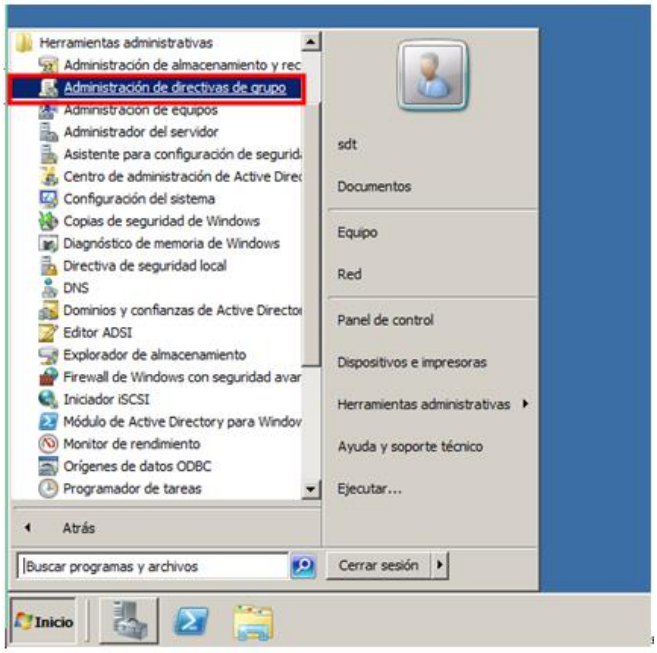
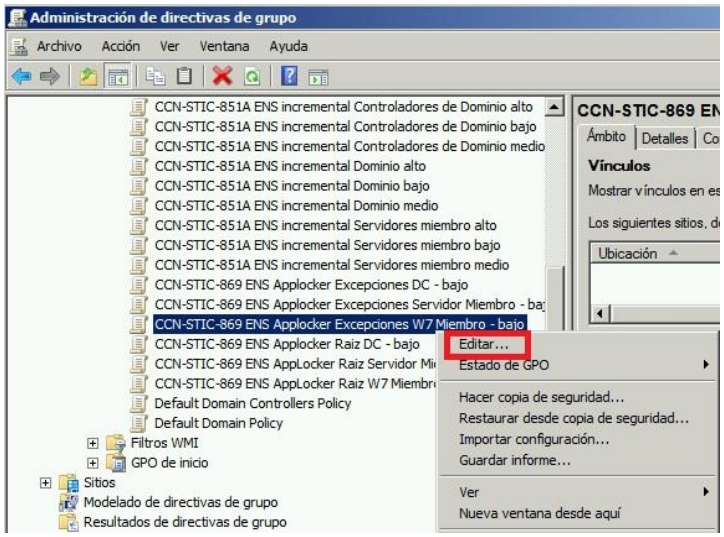


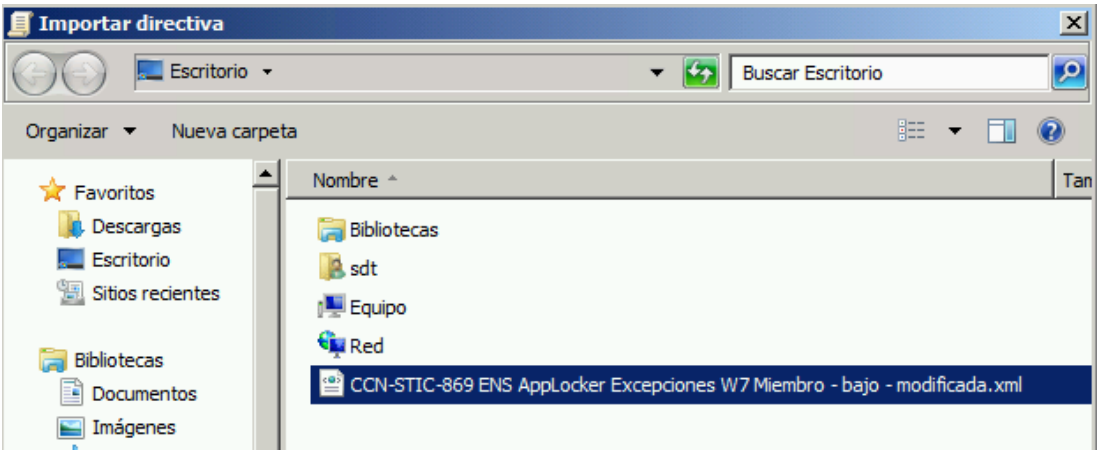
Nota: No cierre todavía el Editor de Editor de directivas de grupo local.

Paso	Descripción
33.	Haciendo uso del mismo editor de directivas de grupo local usado para modificar las reglas de AppLocker, proceda a la eliminación de directiva para dejar así el entorno preparado para una nueva importación y edición de directivas. En el mismo "Editor de administración de directivas de grupo local", seleccione la siguiente ubicación: **Directiva de Equipo Local \ Configuración de equipo \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción "Borrar directiva" del menú de contexto que aparece tras pulsar botón derecho sobre la ubicación señalada. 
34.	Pulse "Si" en el cuadro de dialogo abierto. 
35.	Ya puede cerrar la ventana del "editor de directivas de grupo local".

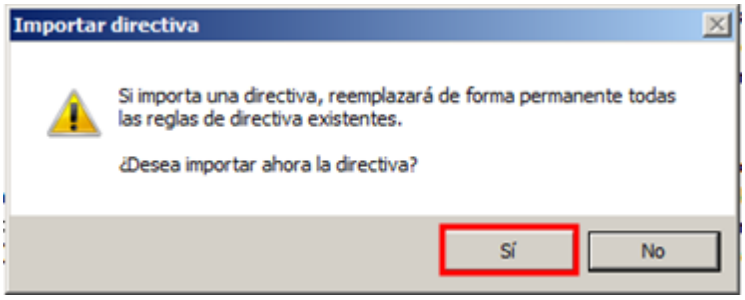
Una vez preparada la nueva directiva con las modificaciones necesarias para su entorno se procederá a la importación de la misma en el GPO de excepciones que aplique a las máquinas que han de recibir las nuevas reglas.

Los pasos que se describen a continuación se realizarán en un controlador de dominio del dominio donde se implementarán las políticas GPO necesarias.

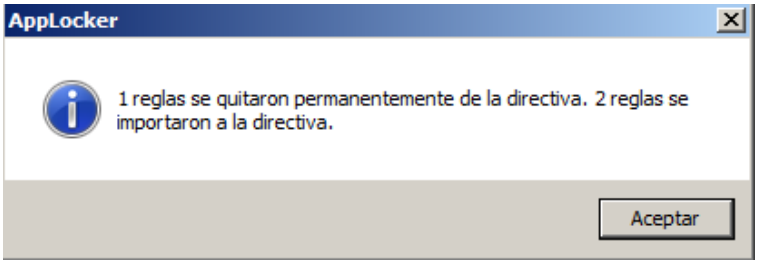
Paso	Descripción
36.	Inicie sesión en el servidor Controlador de Dominio con una cuenta que sea Administrador del Dominio.
37.	Copie el archivo XML exportado de la máquina de referencia al controlador de dominio. En el presente ejemplo, se llama “CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo - modificada.xml”
38.	Inicie la herramienta de administración de directivas de grupo a través del menú de inicio. **Inicio → Herramientas administrativas → Administración de directivas de grupo** 
39.	Seleccione el GPO de excepciones a modificar. En este ejemplo se han editado las reglas de AppLocker definidas en el GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro - bajo**”. Navegue hasta el contenedor **Administración de directivas de grupo \ Bosque:<nombre de su bosque> \ Dominios \ <nombre de su dominio> \ Objetos de directiva de grupo** Marcando con el botón derecho en el GPO, elija la opción “Editar...” del menú contextual que aparecerá. 

Paso	Descripción
40.	En el “Editor de administración de directivas de grupo”, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Elija la opción “Importar directiva...” del menú de contexto que aparece tras pulsar el botón derecho sobre la ubicación señalada. 
41.	En el cuadro de diálogo abierto navegue hasta el directorio donde haya depositado el archivo XML previamente modificado en la máquina de referencia, selecciónelo y ábralo haciendo doble clic sobre él o pulsando el botón “Abrir”. 

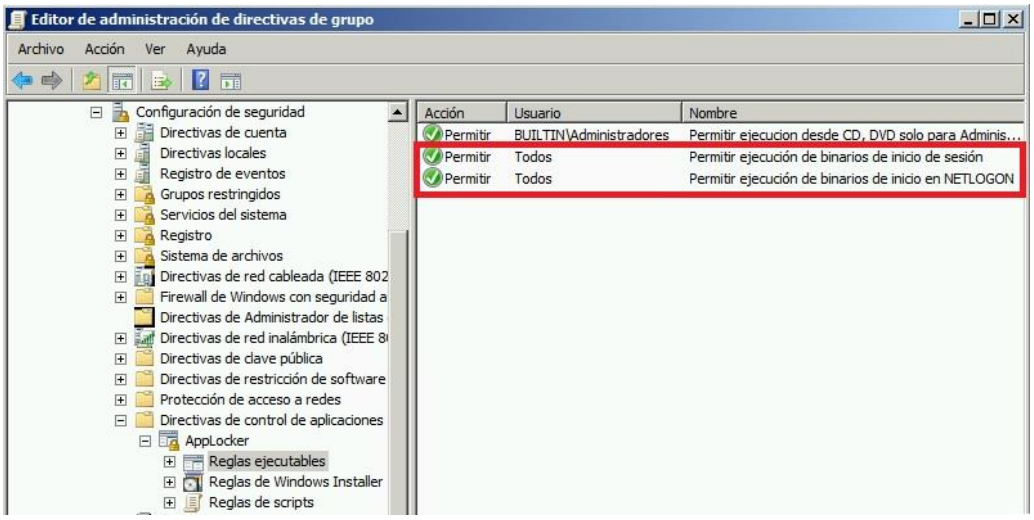
Paso	Descripción
42.	Se le solicitará confirmación ya que la importación de directivas de Applocker sobrescribe la configuración actual. Seleccione “Sí”.



43.	Aparecerá un nuevo mensaje informativo indicando que se importaron tantas reglas como se hayan creado/modificado reglas a la directiva de AppLocker. Pulse “Aceptar” para cerrar la ventana.



44.	En el “Editor de administración de directivas de grupo” del paso anterior, seleccione la siguiente ubicación: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo \ Configuración de equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas ejecutables** Compruebe en el menú que la nueva regla para denegar la ejecución del binario seleccionado se ha creado de manera correcta.



45.	Ya puede cerrar el “Editor de Administración de directivas de grupo” habiendo quedado importadas al GPO “**CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo**” todas las modificaciones realizadas en la máquina de referencia.
46.	Los clientes Windows 7 recogerán la política de manera automática. No obstante, puede reiniciarlos para forzar el cambio.

ANEXO I. LISTA DE COMPROBACIÓN DE LA CORRECTA CONFIGURACIÓN DE APPLOCKER SOBRE UN DOMINIO WINDOWS 2008 R2 O 2012 R2 CON ENS NIVEL BAJO

Este anexo ha sido diseñado para ayudar a los operadores a verificar la correcta aplicación de las distintas configuraciones de seguridad que conciernen a la implantación de AppLocker en una red de dominio categorizada como nivel bajo según los criterios del Esquema Nacional de Seguridad.

1. LISTA DE COMPROBACIÓN DE LA CONFIGURACIÓN DE APPLOCKER SOBRE UN CONTROLADOR DE DOMINIO WINDOWS SERVER 2008 R2 O 2012 R2

La siguiente tabla describe las Comprobaciónes a realizar para verificar la configuración de AppLocker para controladores de dominio Windows Server 2008 R2. Es igualmente aplicable a Windows Server 2012 R2. Para realizar ésta lista de comprobación, se deberá iniciar sesión en un controlador de dominio con una cuenta de usuario con privilegios de administración en el dominio.

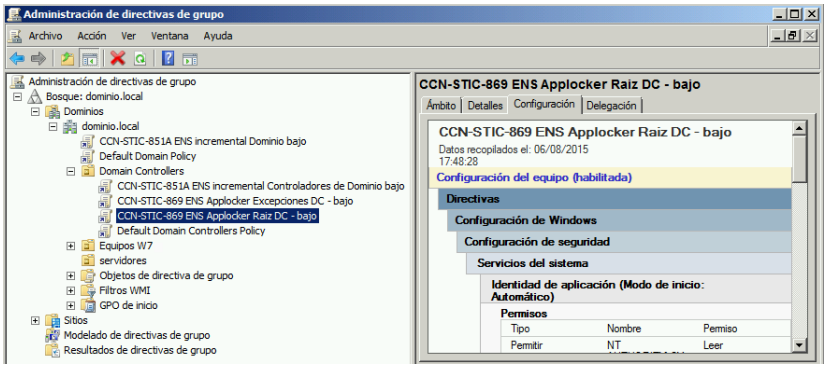
Las consolas y herramientas que se utilizarán son las siguientes:

- Administrador de directivas de grupo (gpmc.msc).
- Servicios (services.msc).
- Visor de Eventos (eventvwr.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 en este documento. 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-869 ENS AppLocker Raiz DC - bajo”.		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 “Domain Controllers”. Verifique que la política “CCN-STIC-869 ENS AppLocker Raiz DC - bajo” está creada y vinculada.

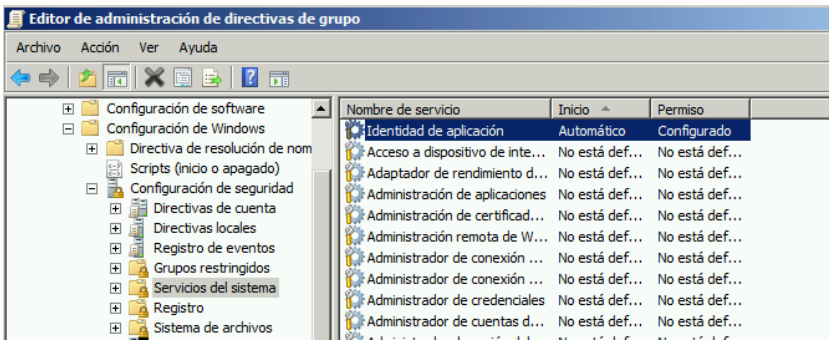
Comprobación	OK/NOK	Cómo hacerlo



3. Verifique los servicios del sistema de la directiva “CCN-STIC-869 ENS AppLocker Raiz DC - bajo”.

Utilizando el “Editor de Administración de directivas de grupo”, sobre la directiva “CCN-STIC-869 ENS AppLocker Raiz DC - bajo”, verifique que la directiva tiene los siguientes valores en servicios del sistema. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz DC - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema



Nombre de Servicio	Inicio	Permiso	OK/NOK
Identidad de aplicación	Automático	Configurado	

4. Verifique las opciones AppLocker de la directiva “CCN-STIC-869 ENS AppLocker Raiz DC - bajo”.

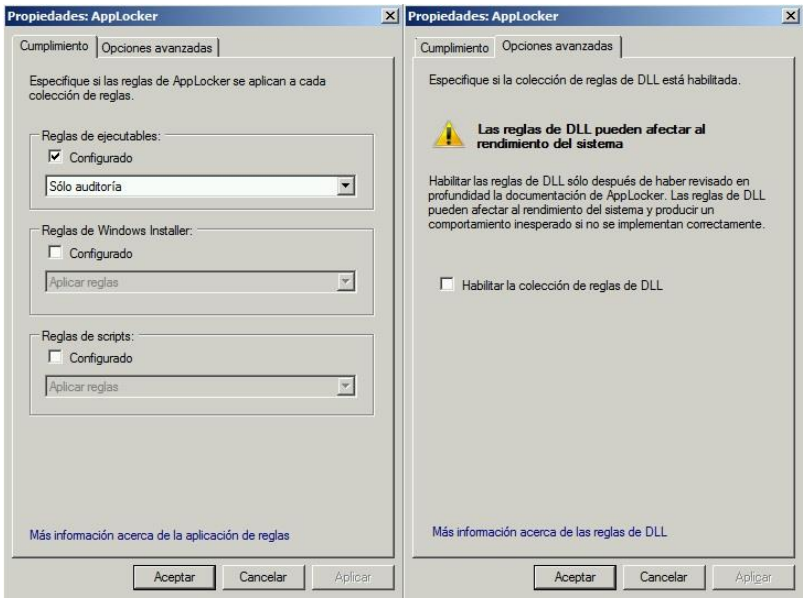
Utilizando el “Editor de Administración de directivas de grupo”, verifique que la directiva “CCN-STIC-869 ENS AppLocker Raiz DC - bajo” tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz DC - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker

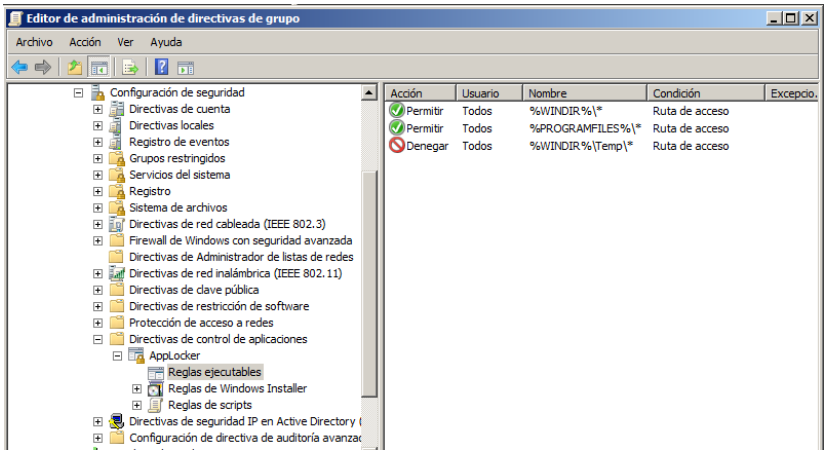
Pulse el botón derecho sobre “AppLocker” y elija el menú “Propiedades”.

Comprobación	OK/NOK	Cómo hacerlo

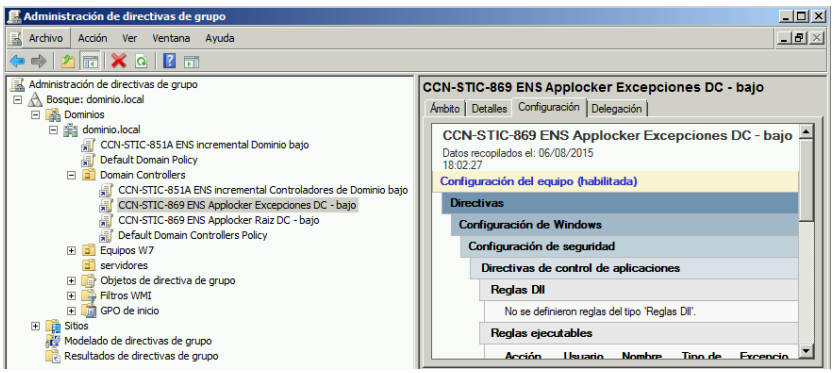
En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación.

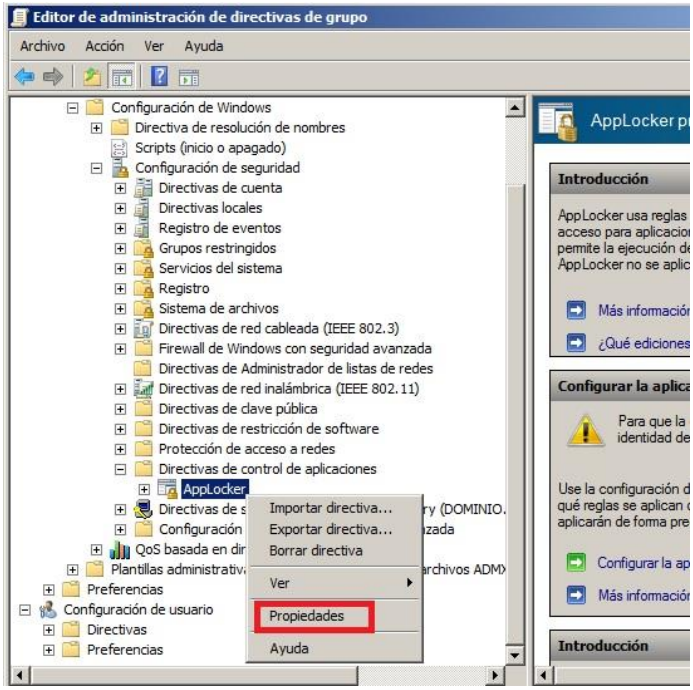
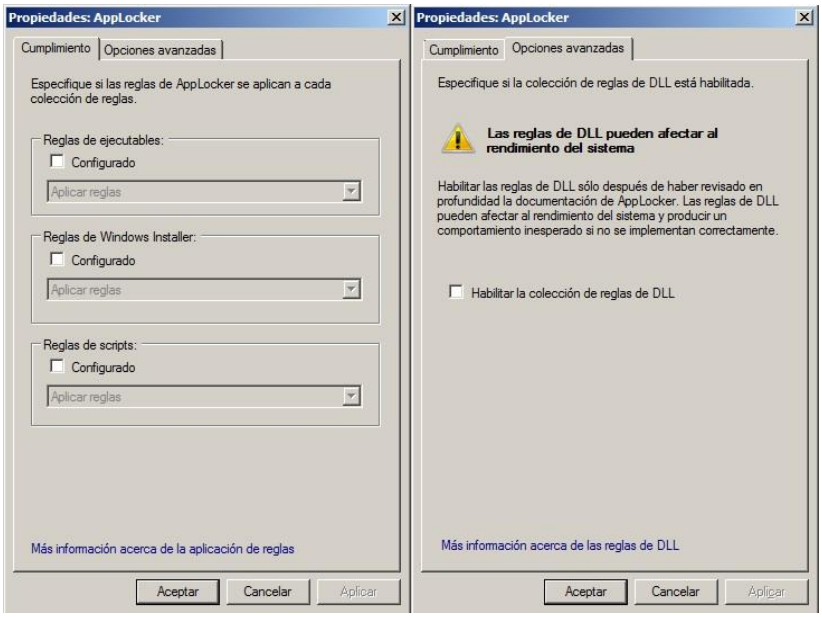


Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Sólo Auditoría	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Raiz DC - bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz DC - bajo" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz DC - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables**  Compruebe que existen las reglas que se indican a continuación:

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES%*	
Denegar	Todos	%WINDIR%\Temp*	

6. Verifique que está creada la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo".		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 "Domain Controllers". Verifique que la política "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo" está creada y vinculada. 

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones DC - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación. 

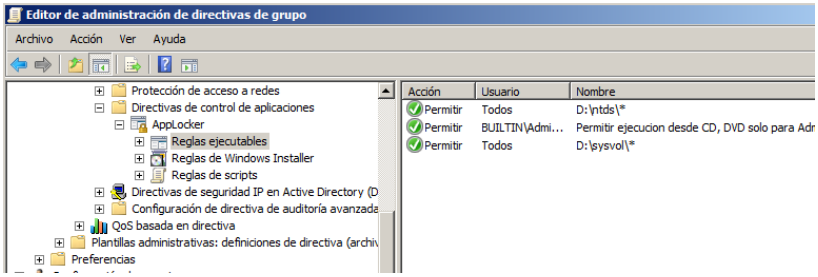
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	No configurado	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

8. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC - bajo" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Excepciones DC - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



Compruebe que existen las reglas que se muestran a continuación.

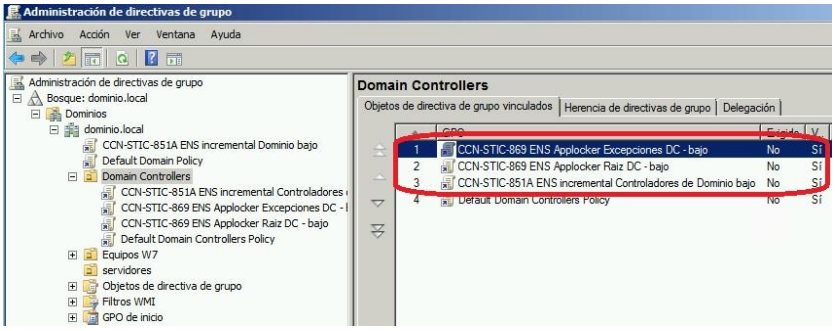
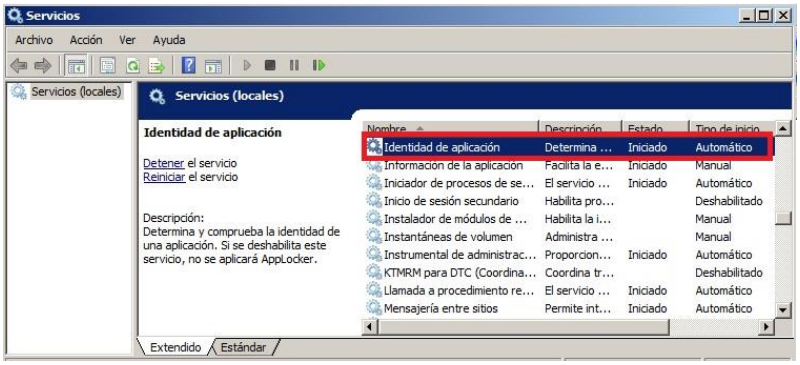
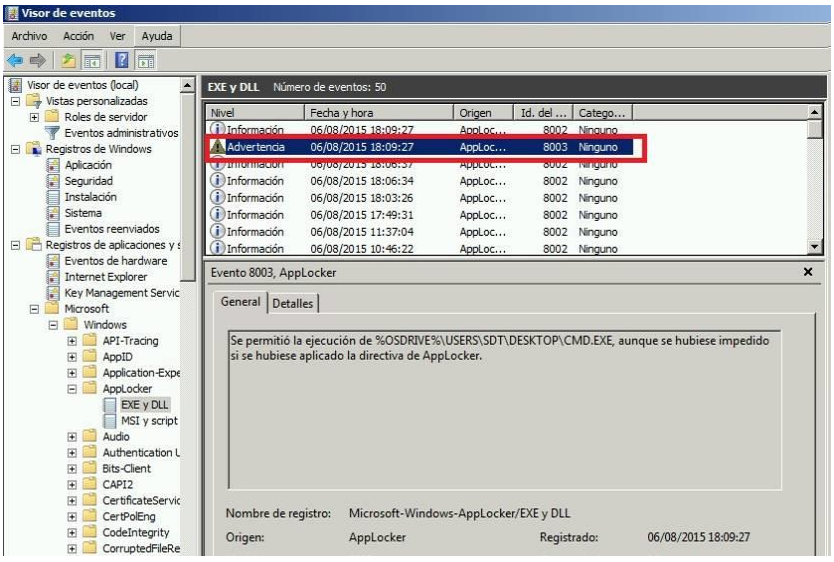
Nota: Si ha establecido excepciones (nuevas reglas) durante la fase de creación y aplicación de la política, compruebe que éstas también están aplicadas.

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	D:\ntds*	
Permitir	BUILTIN\Administradores	Permitir ejecución desde CD, DVD sólo para Administradores	
Permitir	Todos	D:\sysvol*	

9. Orden de aplicación de GPO.

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 "Domain Controllers". Verifique que el orden de aplicación es el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones DC – bajo.
2) CCN-STIC-869 ENS AppLocker Raiz DC – bajo.
3) CCN-STIC-851A ENS incremental Controladores de Dominio bajo
4) Resto de GPOs

Comprobación	OK/NOK	Cómo hacerlo
		
10. Comprobación de servicio de identidad.		Haciendo uso de la consola de servicios (Inicio → ejecutar → services.msc), compruebe que el servicio de "Identidad de Aplicación" está iniciado y configurado para que inicie automáticamente tal y como se indica en la siguiente imagen. 
11. Ejecución de prueba.		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).
12. Comprobar eventos 8003 en visor de eventos.		Abra un visor de eventos (inicio → ejecutar → eventvwr.msc) y navegue hasta: **Visor de eventos / Registros de aplicaciones y servicios / Microsoft / Windows / AppLocker** Compruebe que hay un evento con identificador 8003 que corresponde con la ejecución del binario anterior. 

2. LISTA DE COMPROBACIÓN DE LA CONFIGURACIÓN DE APPLOCKER SOBRE UN SERVIDOR WINDOWS SERVER 2008 R2 O WINDOWS SERVER 2012 R2 MIEMBRO DE UN DOMINIO

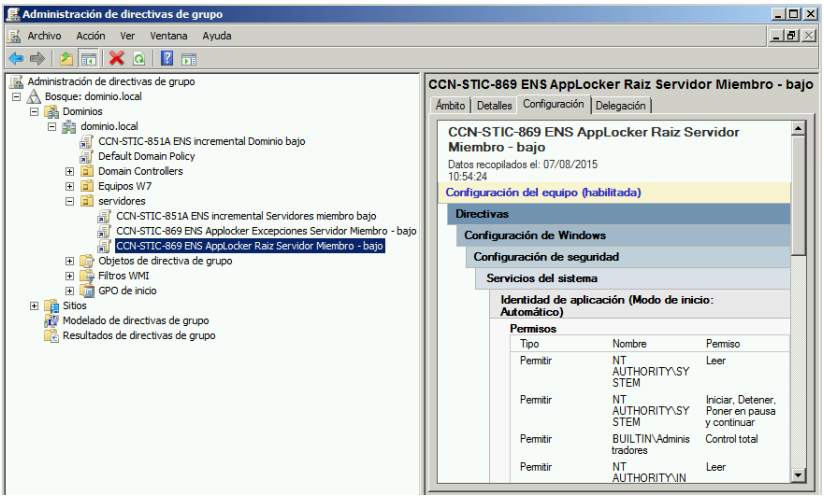
La siguiente tabla describe las Comprobaciónes a realizar para verificar la configuración de AppLocker para servidores Windows Server 2008 R2 miembros de un dominio. Es igualmente aplicable a Windows Server 2012 R2

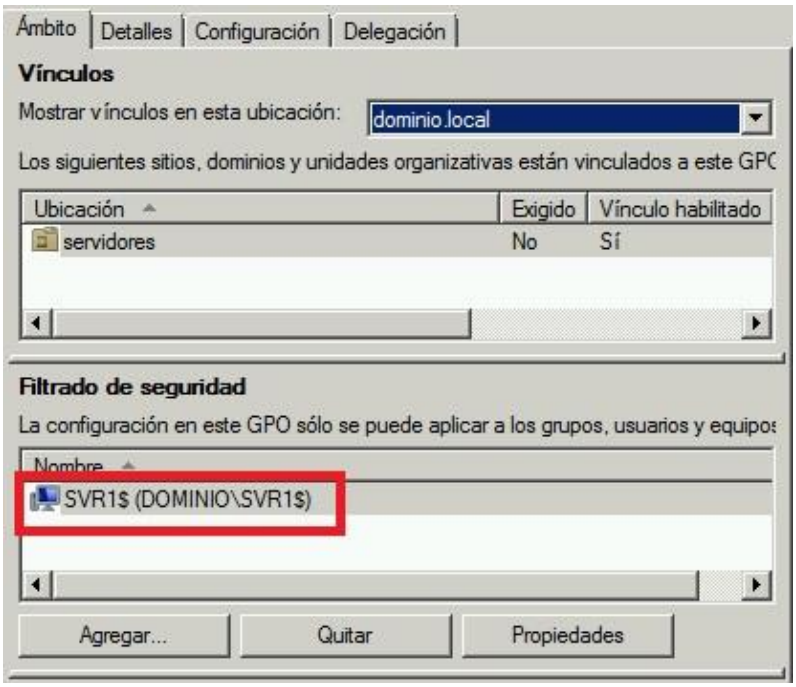
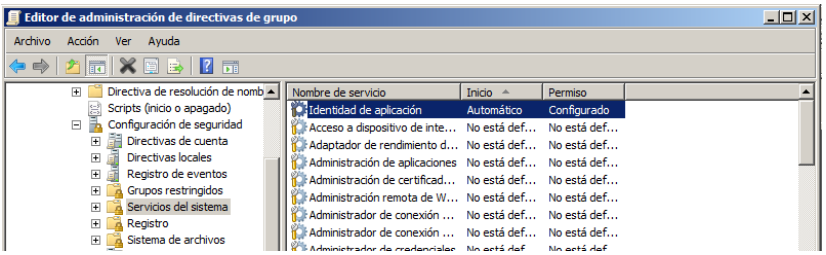
Para realizar ésta lista de comprobación, se deberá iniciar sesión en un controlador de dominio con una cuenta de usuario con privilegios de administración en el dominio.

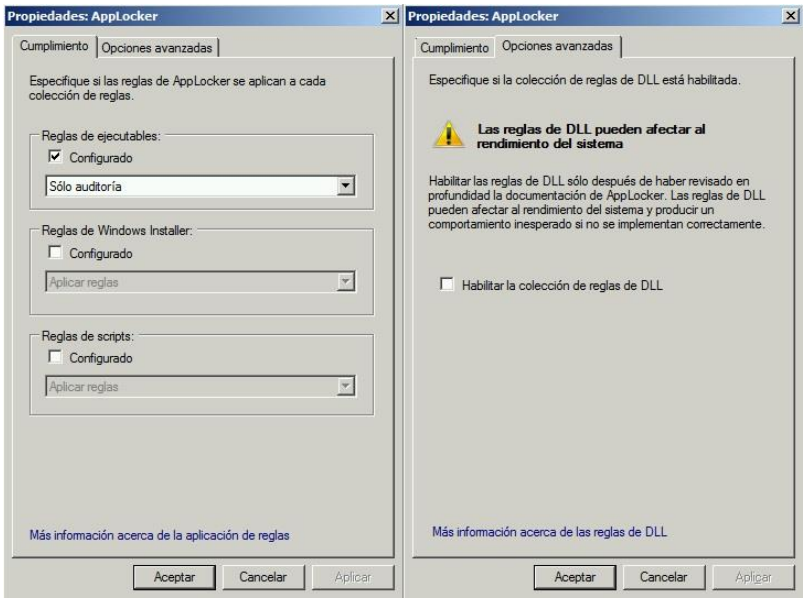
Las consolas y herramientas que se utilizarán son las siguientes:

– Administrador de directivas de grupo (gpmc.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 en este documento. 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-869 ENS AppLocker Raiz Servidor Miembro – bajo”.		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”. Verifique que está creada la política “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo”.  **Nota:** En este ejemplo, todos los servidores a los que se les aplicará la configuración residen en la OU “Servidores”. Adapte esta comprobación a la organización de su Directorio Activo.

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique, si aplica, el filtrado de seguridad del GPO “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo”		**Nota:** Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo de máquina continúe con este paso. Si no, continúe en el paso 4. Utilizando el “Administrador de directivas de grupo” (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo” y revise en el apartado “Filtrado de Seguridad” de la pestaña “Ámbito” que se encuentran los grupos o máquinas destinados a recibir la política.  **Nota:** En este ejemplo sólo se filtra por un único servidor (SVR1). Ajuste la comprobación a la organización de su entorno
4. Verifique los servicios del sistema de la directiva “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo”.		Utilizando el “Editor de Administración de directivas de grupo”, sobre la directiva “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo”, verifique que la directiva tiene los siguientes valores en servicios del sistema. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema**  | Nombre de Servicio	Inicio	Permiso	OK/NOK
---	---	---	---
Identidad de aplicación	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación: 

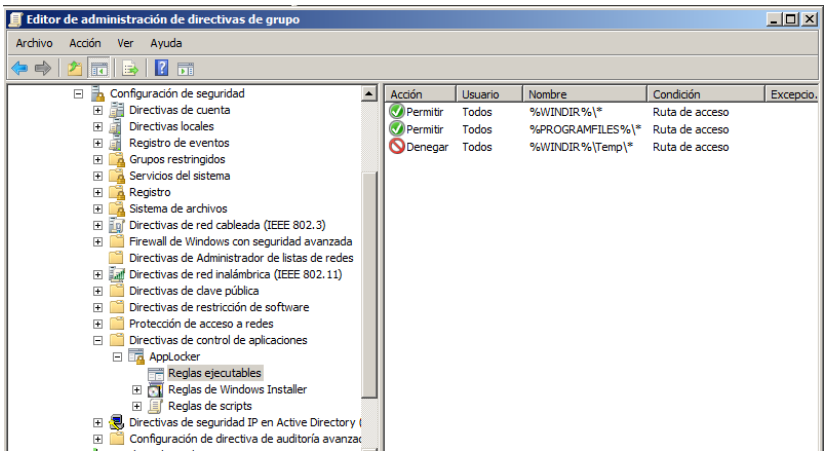
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Sólo auditoría	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

6. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



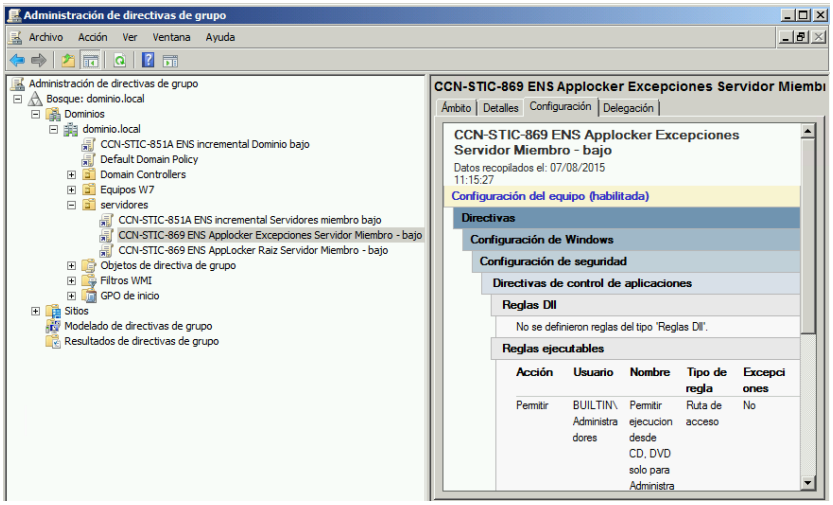
Compruebe que existen las reglas que se indican a continuación.

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES%*	
Denegar	Todos	%WINDIR%\Temp*	

7. Verifique que está creada la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo".

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". Verifique que la política "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo" está creada y vinculada.

Comprobación	OK/NOK	Cómo hacerlo

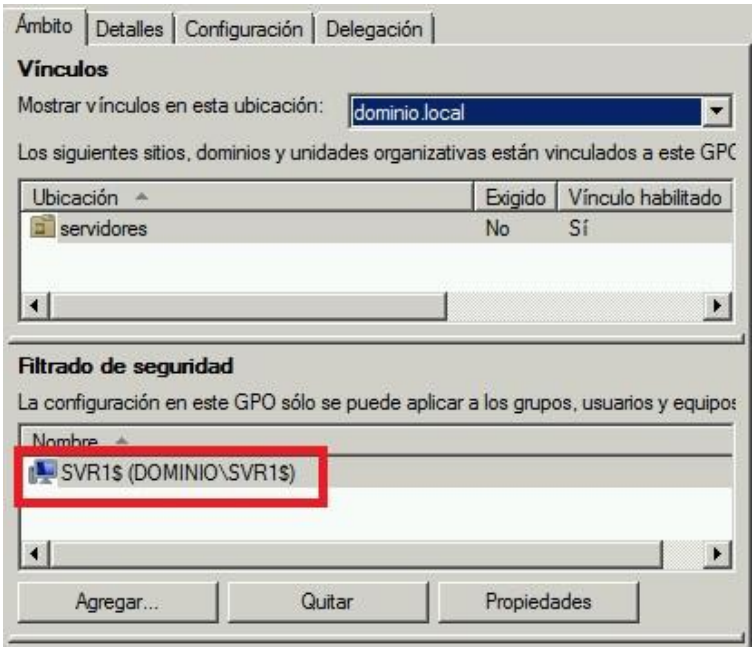


Nota: En este ejemplo, todos los servidores a los que se les aplicará la configuración residen en la OU "Servidores". Adapte esta comprobación a la organización de su Directorio Activo.

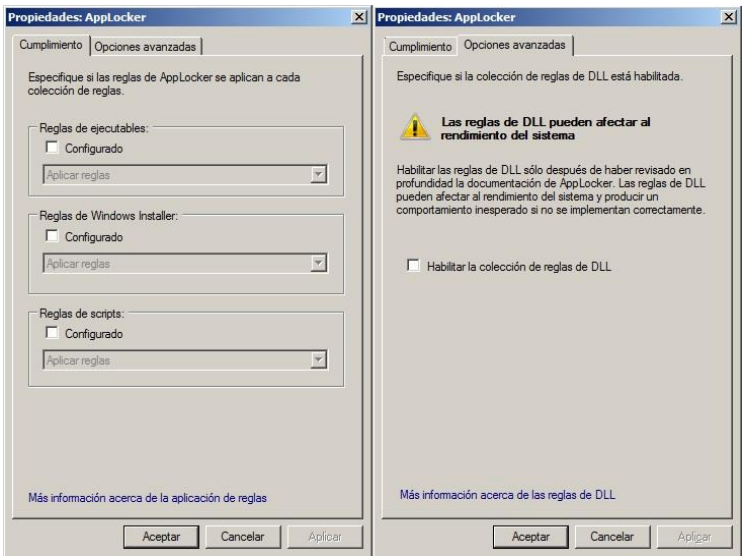
8. Verifique, si aplica, el filtrado de seguridad del GPO "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo"

Nota: Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo continúe con este paso. Si no, continúe en el paso 9.

Utilizando el "Administrador de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo" y revise en el apartado "Filtrado de Seguridad" de la pestaña "Ámbito" que se encuentran los grupos o máquinas destinados a recibir la política.



Nota: En este ejemplo sólo se filtra por un único servidor (SVR1). Ajuste la comprobación a la organización de su entorno

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación: 

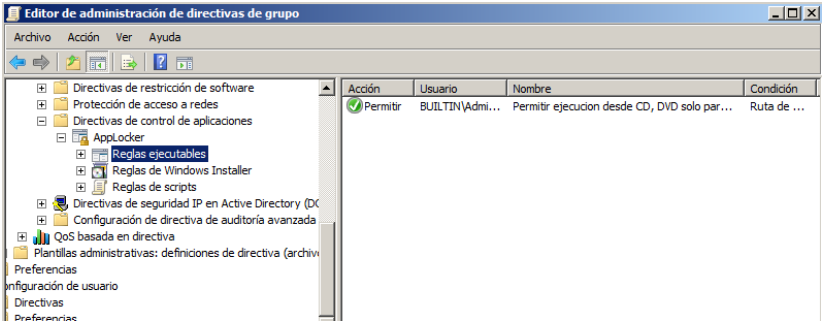
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	No configurado	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

10. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



Compruebe que existen las reglas que se muestran a continuación.

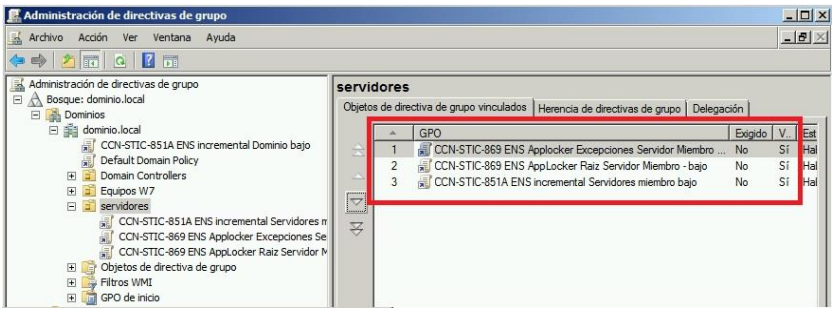
Nota: Si ha establecido excepciones (nuevas reglas) durante la fase de creación y aplicación de la política, compruebe que éstas también están aplicadas.

Acción	Usuario	Nombre	OK/NOK
Permitir	BUILTIN\Administradores	Permitir ejecución desde CD, DVD sólo para Administradores	

11. Verificar el orden de aplicación de GPOs

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". Verifique que el orden de aplicación es el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro –bajo.
2) CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro –bajo.
3) CCN-STIC-851A ENS incremental Servidores Miembro bajo
4) Resto de GPOs

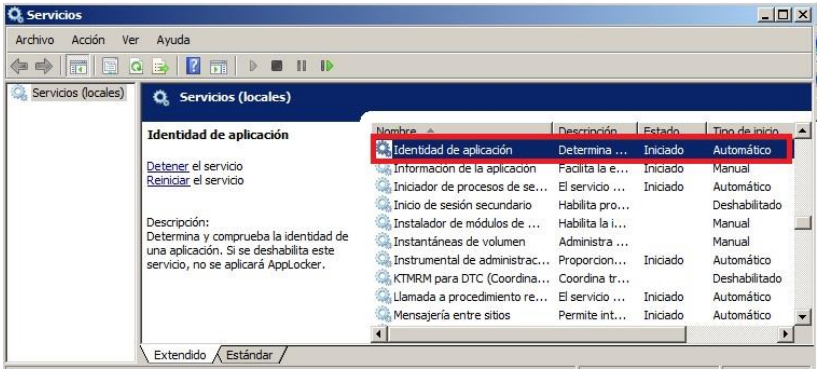
Comprobación	OK/NOK	Cómo hacerlo
		

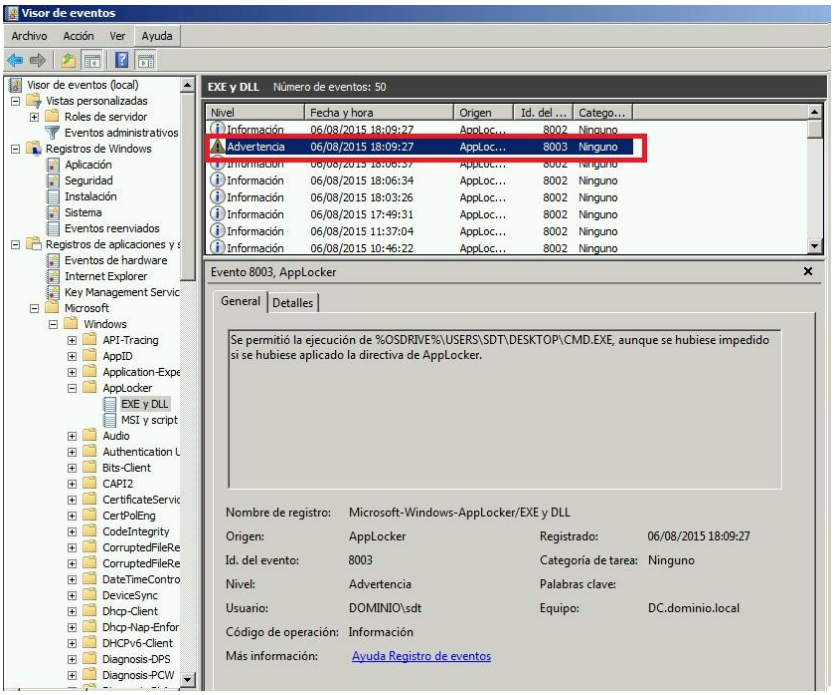
La siguiente tabla describe las Comprobaciónes a realizar para verificar el buen funcionamiento de AppLocker para servidores Windows Server 2008 R2 o Windows Server 2012 R2 miembros de un dominio.

Los siguientes pasos se realizarán desde un servidor miembro que haya recibido y aplicado las políticas “CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – bajo” y “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – bajo”. Dichas Comprobaciónes se realizarán con un usuario que tenga permisos de administración local sobre el servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

- Servicios (services.msc).
- Visor de eventos (eventvwr.msc).

Comprobación	OK/NOK	Cómo hacerlo
12. Inicie sesión en el servidor miembro		Inicie sesión en el servidor miembro del dominio con una cuenta con permisos de administración local.
13. Comprobación de servicio de identidad.		Haciendo uso de la consola de servicios (Combinación de teclas Windows + R → services.msc o Inicio → ejecutar → services.msc), compruebe que el servicio de “Identidad de Aplicación” está iniciado y configurado para que inicie automáticamente: 
14. Ejecución de binario de prueba		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).

Comprobación	OK/NOK	Cómo hacerlo
15. Comprobar eventos 8003 en visor de eventos.		Abra un visor de eventos (inicio → ejecutar → eventvwr.msc) y navegue hasta: **Visor de eventos / Registros de aplicaciones y servicios / Microsoft / Windows / AppLocker** Compruebe que hay un evento con identificador 8003 que corresponde con la ejecución del binario anterior. 

3. LISTA DE COMPROBACIÓN DE LA CONFIGURACIÓN DE APPLOCKER SOBRE CLIENTES WINDOWS 7 MIEMBROS DE UN DOMINO

La siguiente tabla describe las Comprobaciónes a realizar para verificar la configuración de AppLocker para clientes Windows 7 miembros de un dominio.

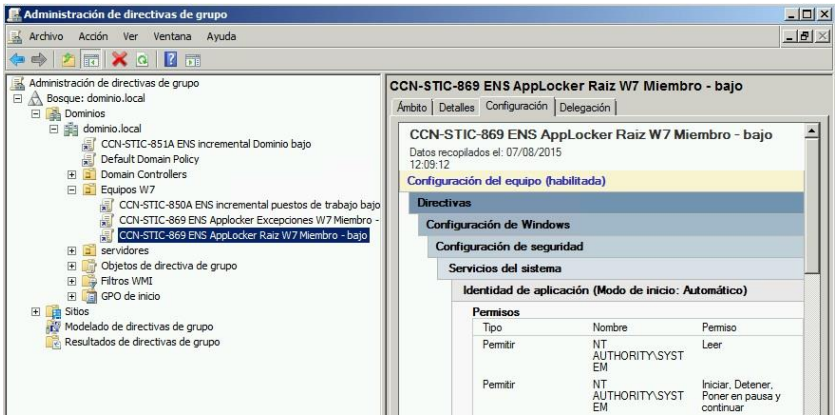
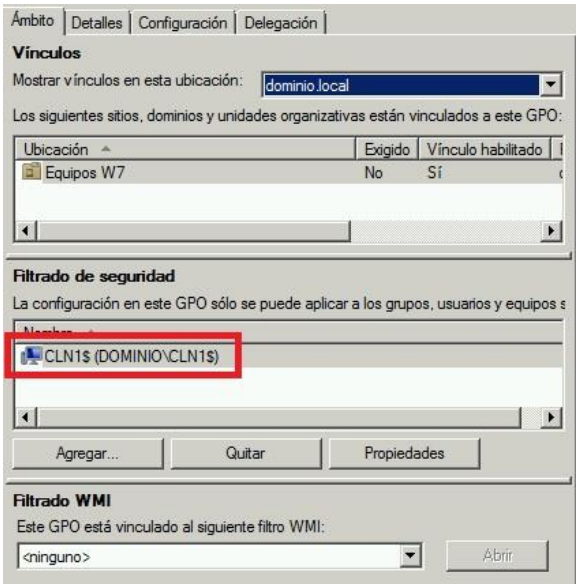
Para realizar ésta lista de comprobación, se deberá iniciar sesión en un controlador de dominio con una cuenta de usuario con privilegios de administración en el dominio.

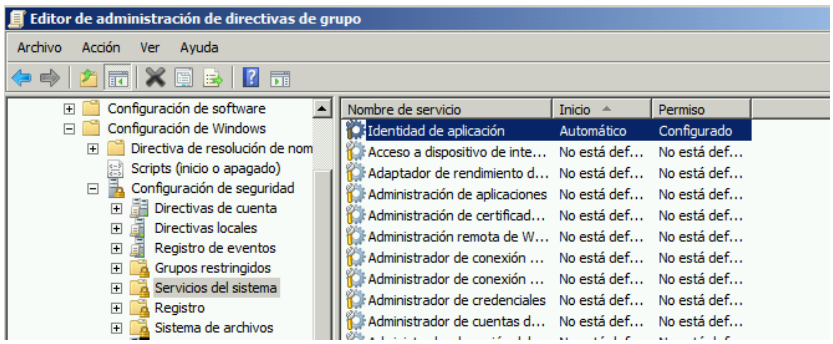
Las consolas y herramientas que se utilizarán son las siguientes:

– Administrador de directivas de grupo (gpmc.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 en este documento. 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.

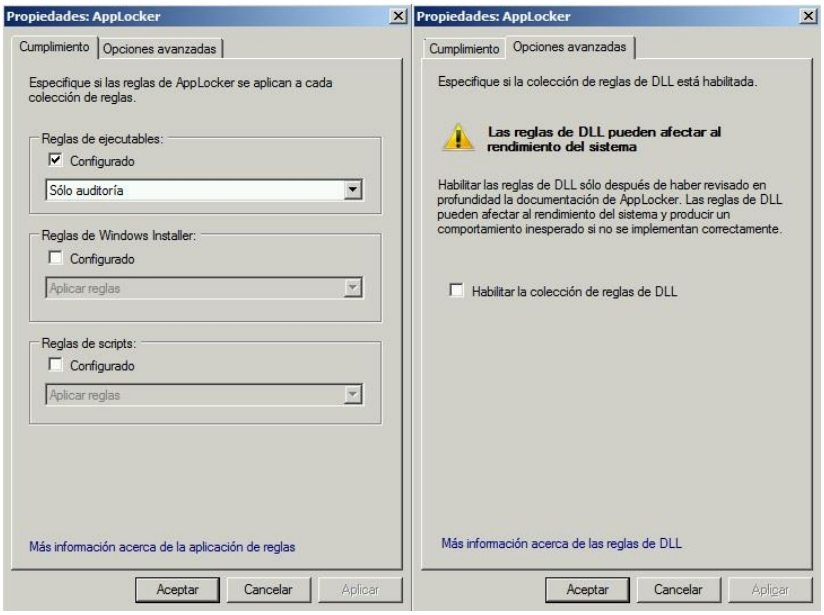
Comprobación	OK/NOK	Cómo hacerlo
2. Verifique que está creada la directiva “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo”.		Utilice el “Administrador de directivas de grupo” (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa “Equipos W7”.Verifique que está creada la política “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo”.  **Nota:** En este ejemplo, todos los clientes Windows 7 a los que se les aplicará la configuración residen en la OU “Equipos W7”. Adapte esta comprobación a la organización de su Directorio Activo.
3. Verifique, si aplica, el filtrado de seguridad del GPO “CCN-STIC-869 ENS AppLocker Raiz W7 – bajo”		**Nota:** Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo de máquina continúe con este paso. Si no, continúe en el paso 4. Utilizando el “Administrador de directivas de grupo” (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO “CCN-STIC-869 ENS AppLocker Raiz W7 – bajo” y revise que en el apartado “Filtrado de Seguridad” de la pestaña “Ámbito” se encuentran los grupos o máquinas destinados a recibir la política.  **Nota:** En este ejemplo se filtra por una única estación de trabajo (CLN1). Ajuste la comprobación a la organización de su entorno.

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique los servicios del sistema de la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo".		Utilizando el "Editor de Administración de directivas de grupo", sobre la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo", verifique que la directiva tiene los siguientes valores en servicios del sistema. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema** 

Nombre de Servicio	Inicio	Permiso	OK/NOK
Identidad de aplicación	Automático	Configurado	

5. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas aparecen como se indica a continuación.

Comprobación	OK/NOK	Cómo hacerlo

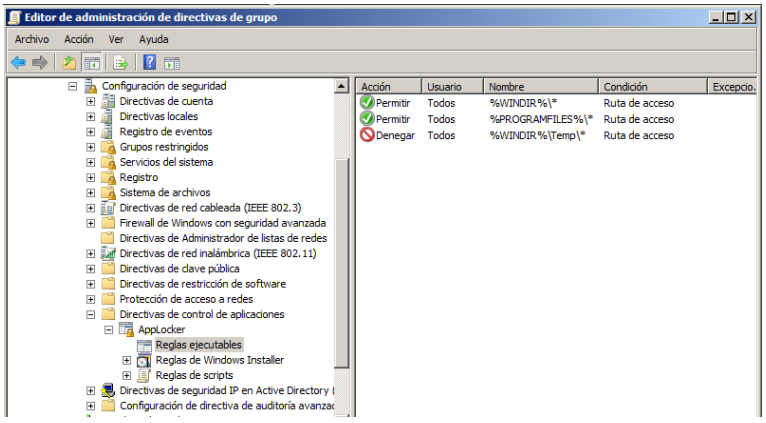


Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Sólo Auditoría	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

6. Verifique las reglas ejecutables de AppLocker en la directiva “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo”.

Utilizando el “Editor de Administración de directivas de grupo”, verifique que la directiva “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo” tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



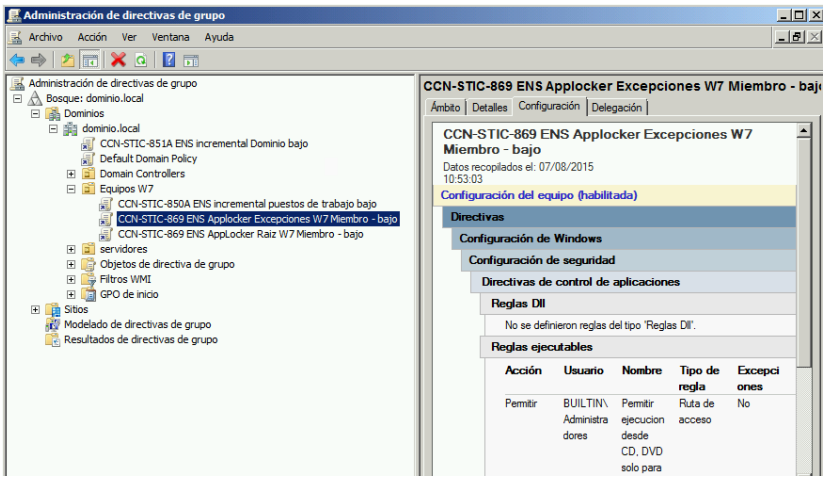
Compruebe que existen las reglas que se indican a continuación:

Comprobación	OK/NOK	Cómo hacerlo

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES%*	
Denegar	Todos	%WINDIR%\Temp*	

7. Verifique que está creada la directiva “CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo”.

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 “Equipos Windows 7”. Verifique que está creada la política “CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo”.

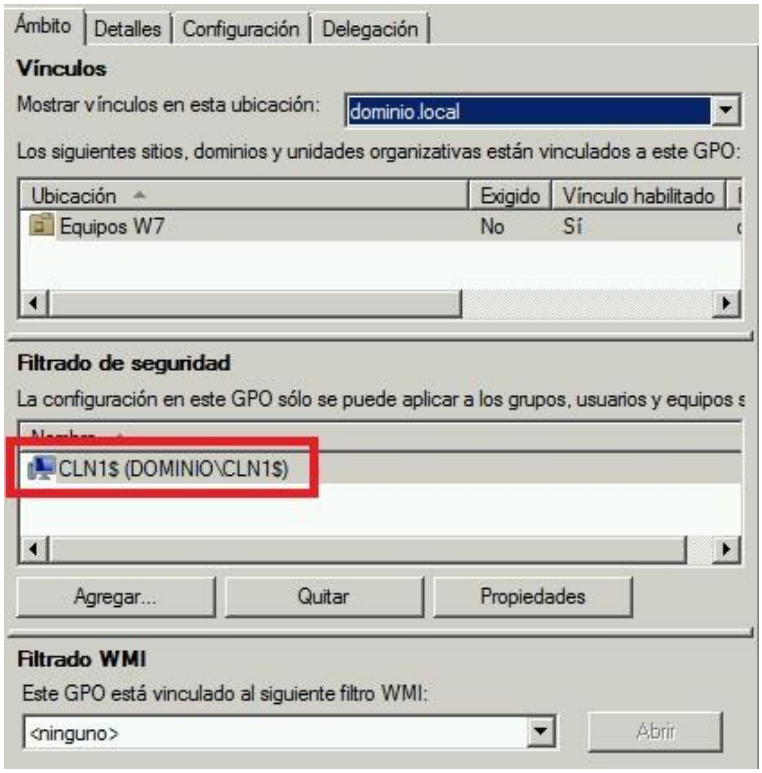


Nota: En este ejemplo, todos los clientes Windows 7 a los que se les aplicará la configuración residen en la OU “Equipos W7”. Adapte esta comprobación a la organización de su Directorio Activo.

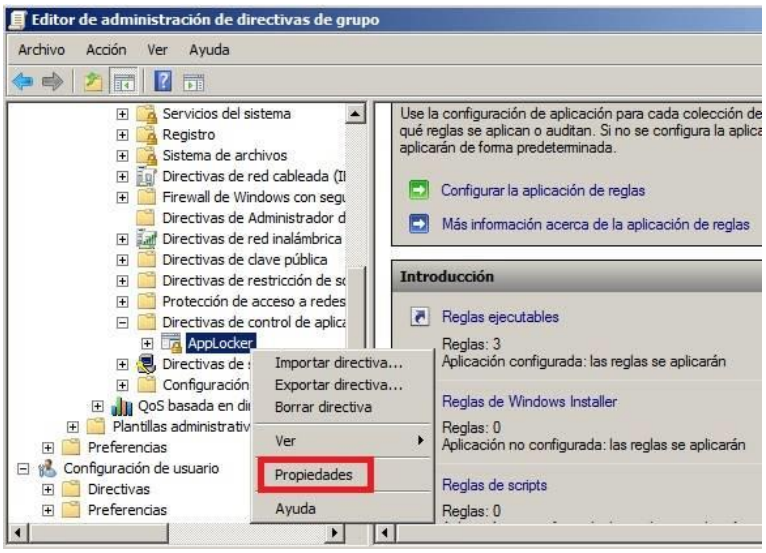
8. Verifique, si aplica, el filtrado de seguridad del GPO “CCN-STIC-869 ENS AppLocker Excepciones W7 – bajo”

Nota: Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo continúe con este paso. Si no, continúe en el paso 9.

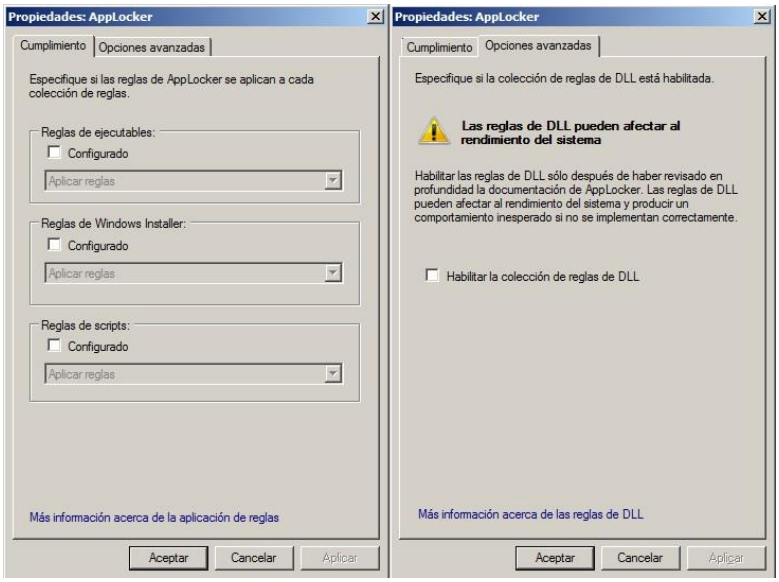
Utilizando el “Administrador de directivas de grupo” (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO “CCN-STIC-869 ENS AppLocker Excepciones W7 – bajo” y revise en el apartado “Filtrado de Seguridad” de la pestaña “Ámbito” que se encuentran los grupos o máquinas destinados a recibir la política.

Comprobación	OK/NOK	Cómo hacerlo
		 **Nota:** En este ejemplo se filtra por una única estación de trabajo (CLN1). Ajuste la comprobación a la organización de su entorno.
9. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".

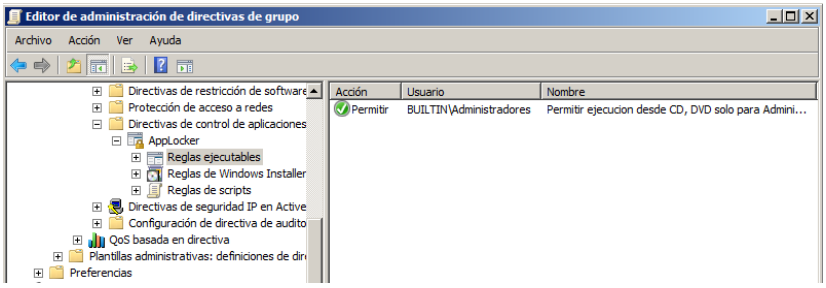
Comprobación	OK/NOK	Cómo hacerlo



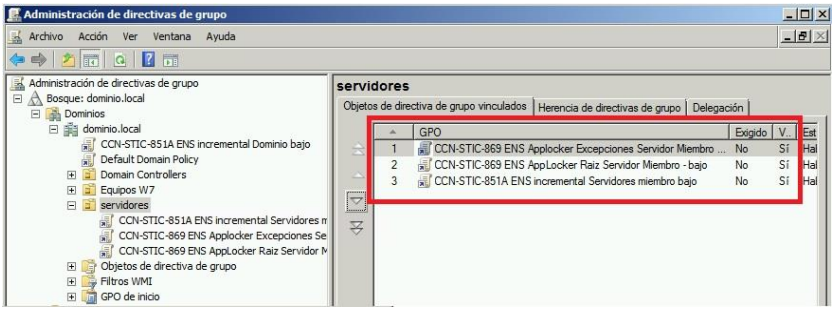
En la ventana de “Propiedades”, compruebe que las configuraciones de las dos pestañas están como se indica a continuación.



Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	No configurado	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

Comprobación	OK/NOK	Cómo hacerlo
10. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 - bajo \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables**  Compruebe que existen las reglas que se muestran a continuación. **Nota:** Si ha establecido excepciones (nuevas reglas) durante la fase de creación y aplicación de la política, compruebe que éstas también están aplicadas.

Acción	Usuario	Nombre	OK/NOK
Permitir	BUILTIN\Administradores	Permitir ejecución desde CD, DVD sólo para Administradores	

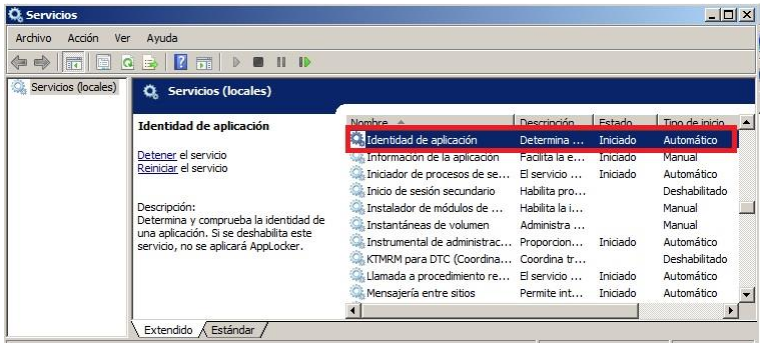
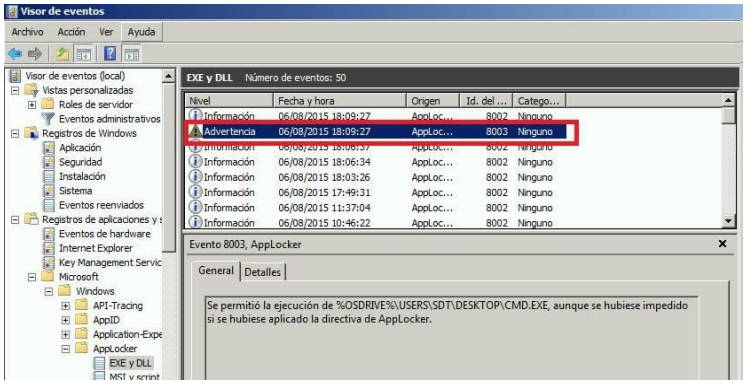
11. Verificar el orden de aplicación de GPOs		Utilice el "Administrador de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo) y despliegue el menú en árbol hasta llegar a la unidad organizativa "servidores". Verifique que el orden de aplicación es el siguiente: 1) CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo. 2) CCN-STIC-869 ENS AppLocker Raiz W7 Miembro –bajo. 3) CCN-STIC-851A ENS incremental puestos de trabajo bajo. 4) Resto de GPOs. 

La siguiente tabla describe las Comprobaciónes a realizar para verificar el buen funcionamiento de AppLocker para estaciones de trabajo Windows 7 miembros de un dominio.

Los siguientes pasos se realizarán desde un cliente Windows 7 que haya recibido y aplicado las políticas "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – bajo" y "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – bajo". Dichas Comprobaciónes se realizarán con un usuario que tenga permisos administrativos sobre la estación de trabajo.

Las consolas y herramientas que se utilizarán son las siguientes:

- Servicios (services.msc).
- Visor de eventos (eventvwr.msc).

Comprobación	OK/NOK	Cómo hacerlo
12. Inicie sesión en el cliente Windows 7.		Inicie sesión en el cliente Windows 7 del dominio con una cuenta con permisos de administración local.
13. Comprobación de servicio de identidad.		Haciendo uso de la consola de servicios (Tecla Windows + R → services.msc o Inicio → ejecutar → services.msc), compruebe que el servicio de "Identidad de Aplicación" está iniciado y configurado para que inicie automáticamente: 
14. Ejecución de binario de prueba		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).
15. Comprobar eventos 8003 en visor de eventos.		Abra un visor de eventos (inicio → ejecutar → eventvwr.msc) y navegue hasta: **Visor de eventos / Registros de aplicaciones y servicios / Microsoft / Windows / AppLocker** Compruebe que hay un evento con identificador 8003 que corresponde con la ejecución del binario anterior. 

ANEXO J. LISTA DE COMPROBACIÓN DE LA CORRECTA CONFIGURACIÓN DE APPLOCKER SOBRE UN DOMINIO WINDOWS 2008 R2 O WINDOWS 2012 R2 CON ENS NIVEL MEDIO O ALTO

Este anexo ha sido diseñado para ayudar a los operadores a verificar la correcta aplicación de las distintas configuraciones de seguridad que conciernen a la implantación de AppLocker en una red de dominio categorizada como nivel medio o alto según los criterios del Esquema Nacional de Seguridad.

1. LISTA DE COMPROBACIÓN DE LA CONFIGURACIÓN DE APPLOCKER SOBRE UN CONTROLADOR DE DOMINIO WINDOWS SERVER 2008 R2 O WINDOWS SERVER 2012 R2

La siguiente tabla describe las comprobaciones a realizar para verificar la configuración de AppLocker para controladores de dominio Windows Server 2008 R2. Es igualmente aplicable a Windows Server 2012 R2 Para realizar ésta lista de comprobación, se deberá iniciar sesión en un controlador de dominio con una cuenta de usuario con privilegios de administración en el dominio.

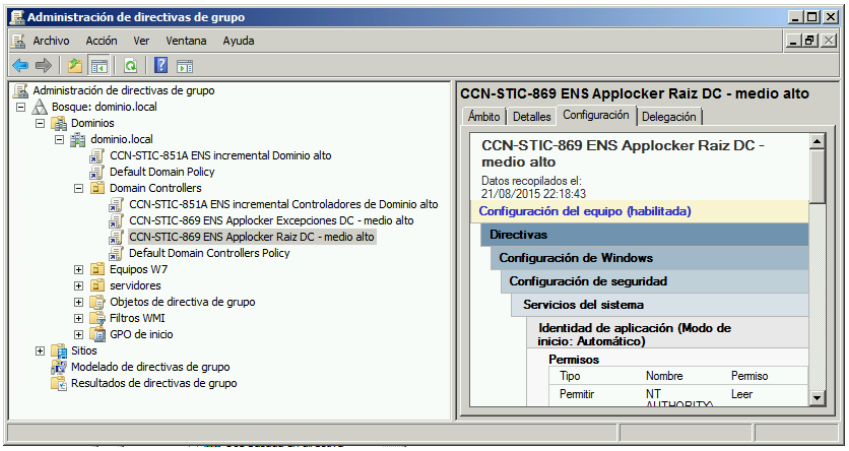
Las consolas y herramientas que se utilizarán son las siguientes:

- Administrador de directivas de grupo (gpmc.msc).
- Servicios (services.msc).
- Visor de Eventos (eventvwr.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 en este documento. 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-869 ENS AppLocker Raiz DC - medio 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 “Domain Controllers”. Verifique que está creada la política “CCN-STIC-869 ENS AppLocker Raiz DC – medio alto”.

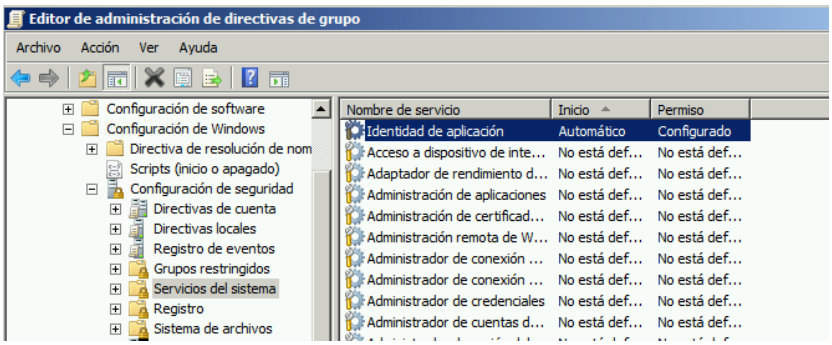
Comprobación	OK/NOK	Cómo hacerlo



3. Verifique los servicios del sistema de la directiva “CCN-STIC-869 ENS AppLocker Raiz DC - medio alto”.

Utilizando el “Editor de Administración de directivas de grupo”, sobre la directiva “CCN-STIC-869 ENS AppLocker Raiz DC - medio alto”, verifique que la directiva tiene los siguientes valores en servicios del sistema. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz DC – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema



Nombre de Servicio	Inicio	Permiso	OK/NOK
Identidad de aplicación	Automático	Configurado	

4. Verifique las opciones AppLocker de la directiva “CCN-STIC-869 ENS AppLocker Raiz DC – medio alto”.

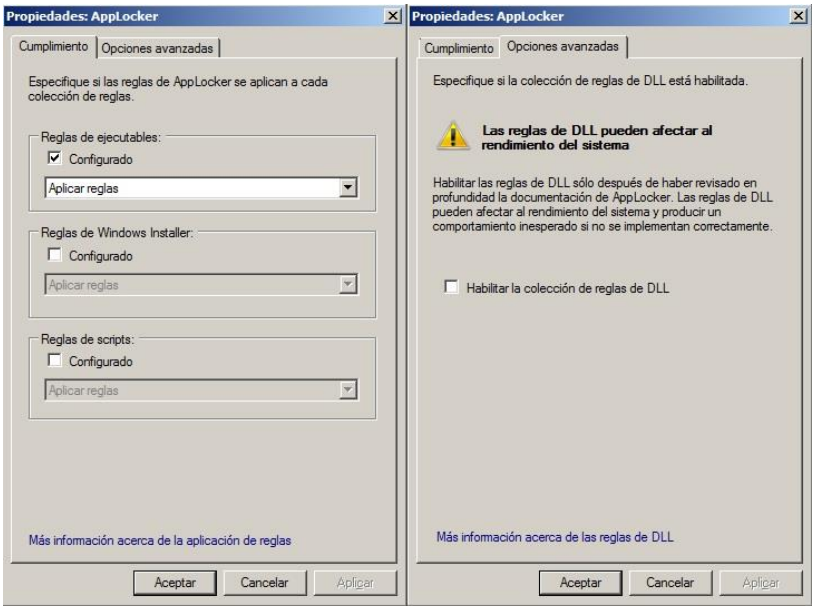
Utilizando el “Editor de Administración de directivas de grupo”, verifique que la directiva “CCN-STIC-869 ENS AppLocker Raiz DC – medio alto” tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz DC – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker

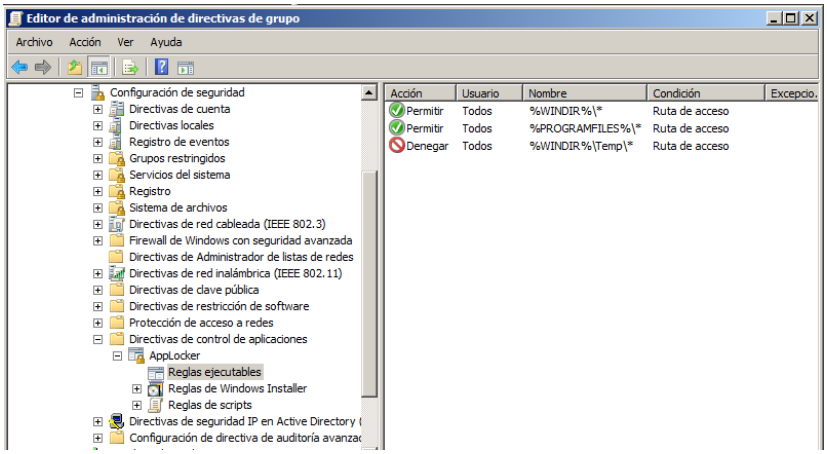
Pulse el botón derecho sobre “AppLocker” y elija el menú “Propiedades”.

Comprobación	OK/NOK	Cómo hacerlo

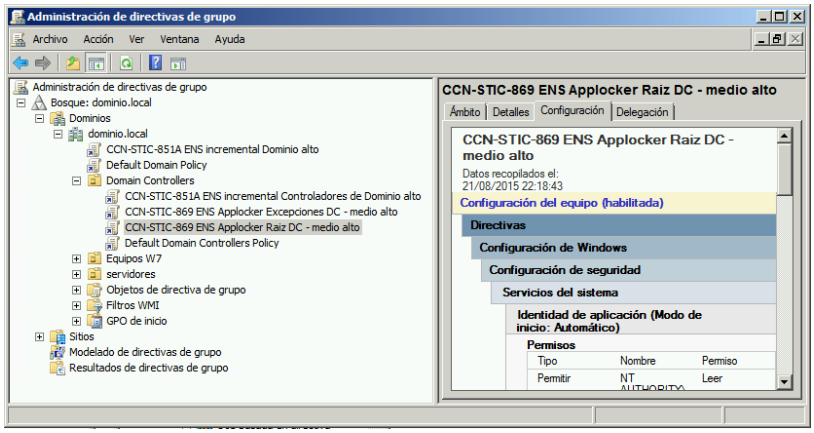
En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación.

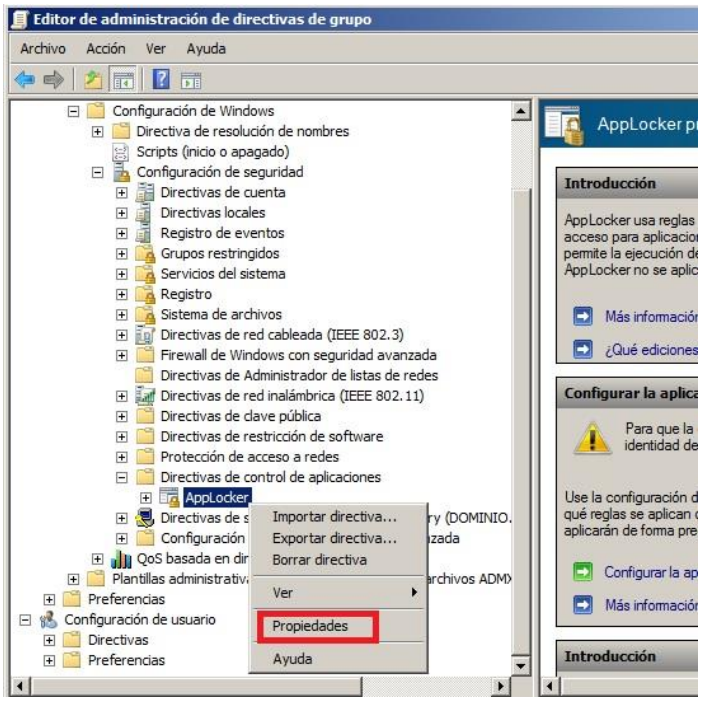
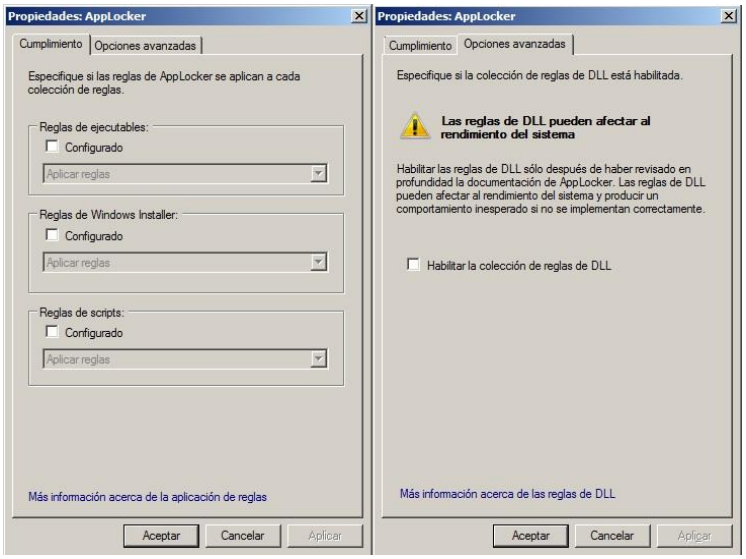


Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Aplicar reglas	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Raiz DC – medio alto".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz DC – medio alto" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz DC – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables**  Compruebe que existen las reglas que se indican a continuación:

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES%*	
Denegar	Todos	%WINDIR%\Temp*	

6. Verifique que está creada la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC – medio 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 "Domain Controllers". Verifique que está creada la política "CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto". 

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación. 

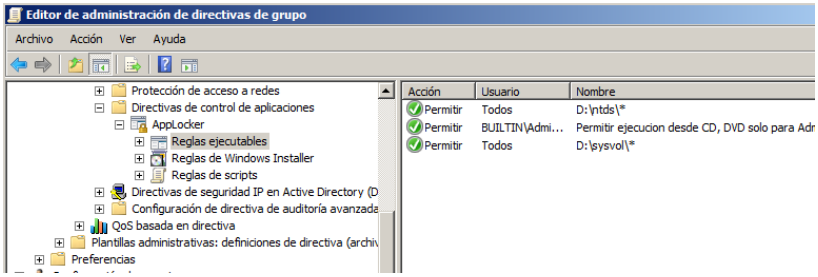
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	No configurado	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

8. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



Compruebe que existen las reglas que se muestran a continuación.

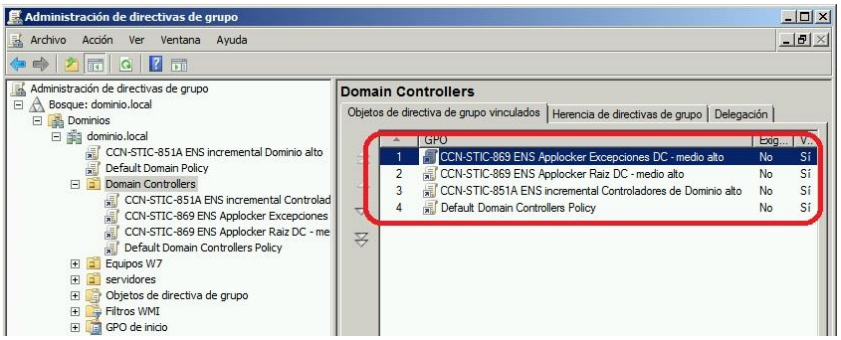
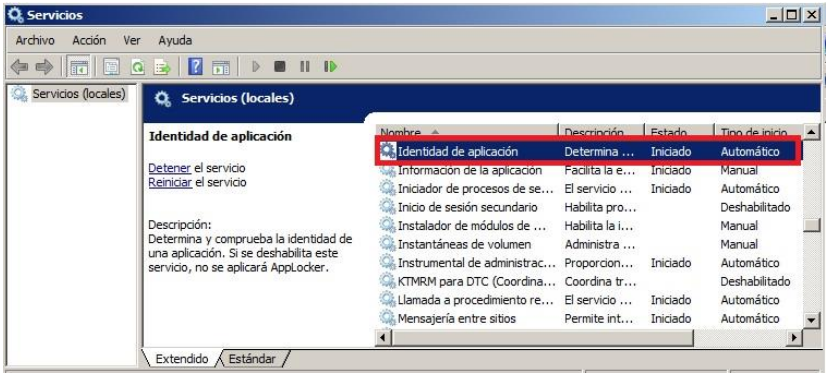
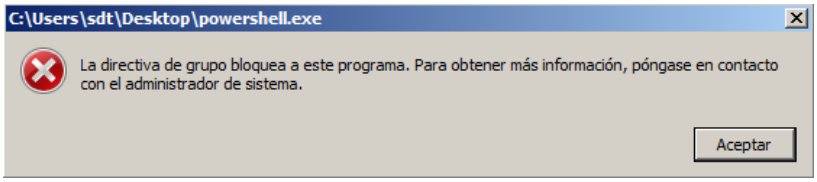
Nota: Si ha establecido excepciones (nuevas reglas) durante la fase de creación y aplicación de la política, compruebe que éstas también están aplicadas.

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	D:\ntds*	
Permitir	BUILTIN\Administradores	Permitir ejecución desde CD, DVD sólo para Administradores	
Denegar	Todos	D:\sysvol*	

9. Orden de aplicación de GPO.

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 "Domain Controllers". Verifique que el orden de aplicación es el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones DC – medio alto.
2) CCN-STIC-869 ENS AppLocker Raiz DC – medio alto.
3) Resto de GPOs

Comprobación	OK/NOK	Cómo hacerlo
		
10. Comprobación de servicio de identidad.		Haciendo uso de la consola de servicios (Inicio → ejecutar → services.msc), compruebe que el servicio de "Identidad de Aplicación" está iniciado y configurado para que inicie automáticamente tal y como se indica en la siguiente imagen. 
11. Ejecución de prueba.		Copie un ejecutable (Por ejemplo %WINDIR%\System32\cmd.exe) al escritorio del usuario y ejecútelo.
12. Comprobación de bloqueo de ejecutable.		Si la aplicación de las políticas de AppLocker es correcta deberá recibir el siguiente mensaje por pantalla. 

2. LISTA DE COMPROBACIÓN DE LA CONFIGURACIÓN DE APPLOCKER SOBRE UN SERVIDOR WINDOWS SERVER 2008 R2 O 2012 R2 MIEMBRO DE UN DOMINIO

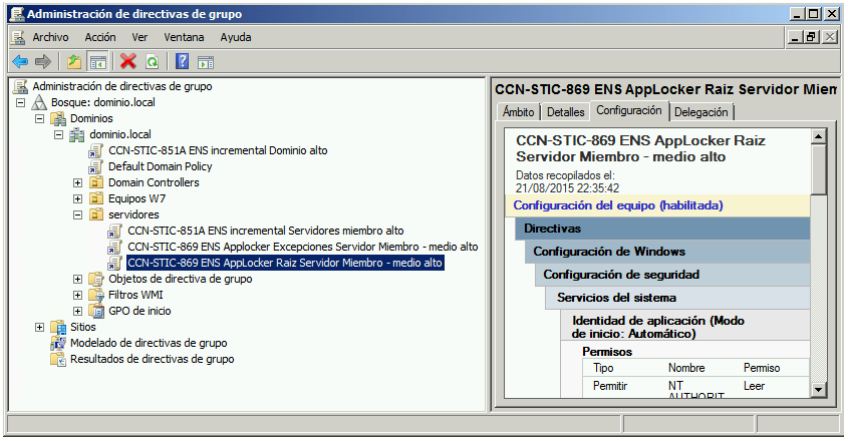
La siguiente tabla describe las Comprobaciónes a realizar para verificar la configuración de AppLocker para servidores Windows Server 2008 R2 miembros de un dominio. Es igualmente aplicable a Windows Server 2012 R2

Para realizar ésta lista de comprobación, se deberá iniciar sesión en un controlador de dominio con una cuenta de usuario con privilegios de administración en el dominio.

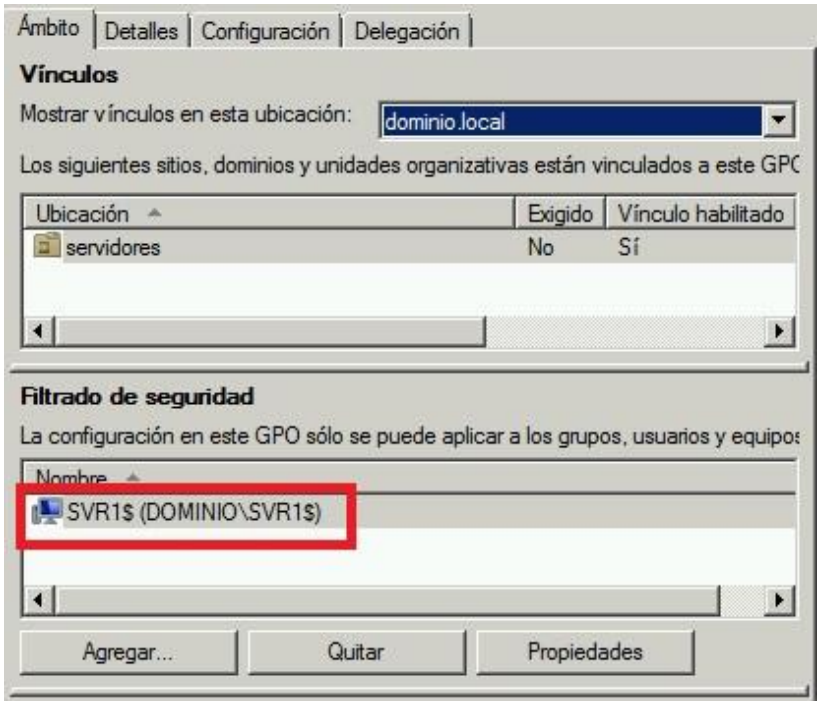
Las consolas y herramientas que se utilizarán son las siguientes:

– Administrador de directivas de grupo (gpmc.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 en este documento. 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-869 ENS AppLocker Raiz Servidor Miembro – medio 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". Verifique que está creada la política "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto".  **Nota:** En este ejemplo, todos los servidores a los que se les aplicará la configuración residen en la OU "Servidores". Adapte esta comprobación a la organización de su Directorio Activo.
3. Verifique, si aplica, el filtrado de seguridad del GPO "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto"		**Nota:** Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo de máquina continúe con este paso. Si no, continúe en el paso 4. Utilizando el "Administrador de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto" y revise en el apartado "Filtrado de Seguridad" de la pestaña "Ámbito" que se encuentran los grupos o máquinas destinados a recibir la política.

Comprobación	OK/NOK	Cómo hacerlo

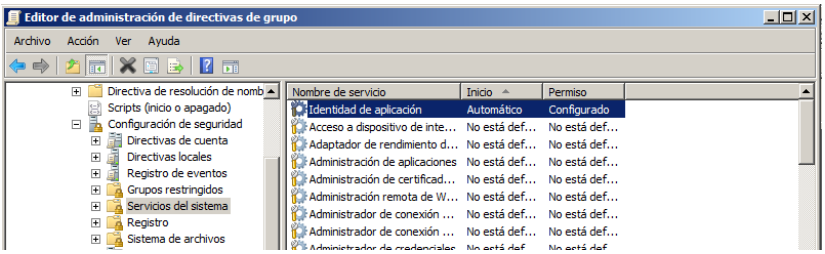


Nota: En este ejemplo sólo se filtra por un único servidor (SVR1). Ajuste la comprobación a la organización de su entorno

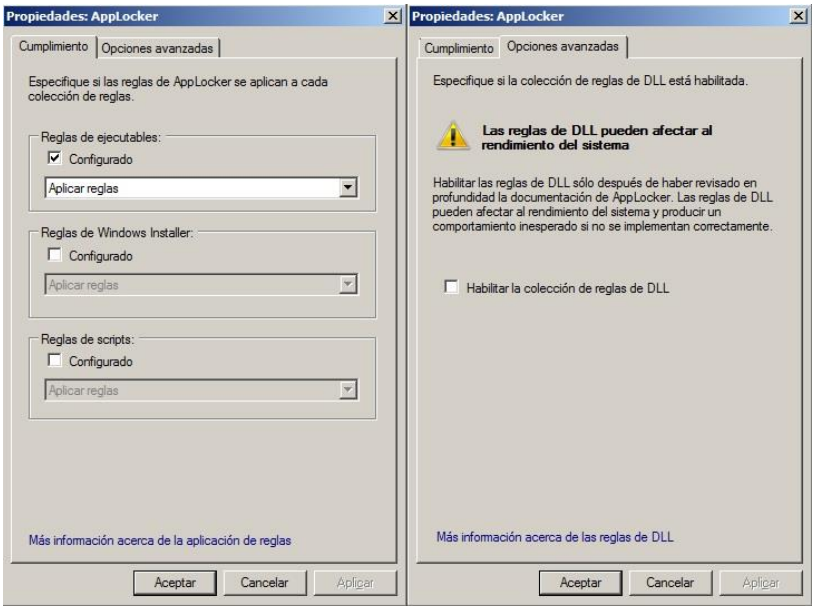
4. Verifique los servicios del sistema de la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto".

Utilizando el "Editor de Administración de directivas de grupo", sobre la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto", verifique que la directiva tiene los siguientes valores en servicios del sistema. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema



Nombre de Servicio	Inicio	Permiso	OK/NOK
Identidad de aplicación	Automático	Configurado	

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación: 

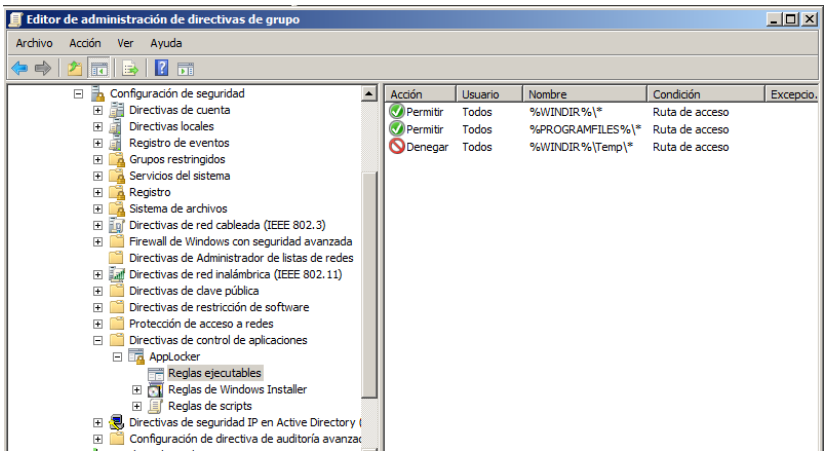
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Aplicar reglas	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

6. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto".

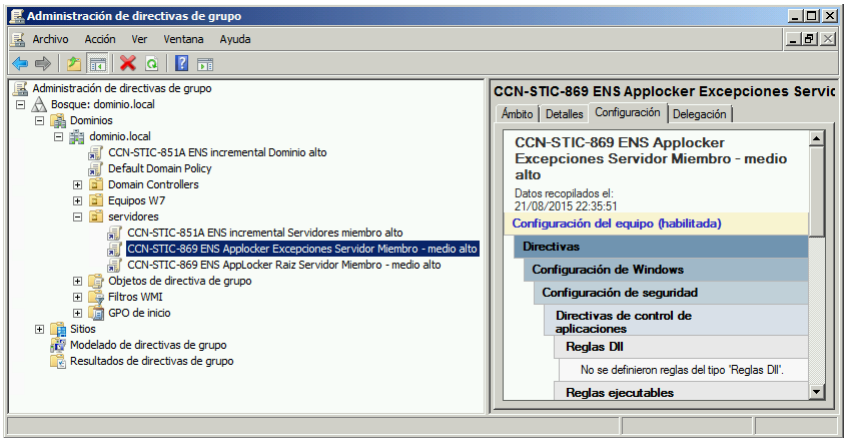
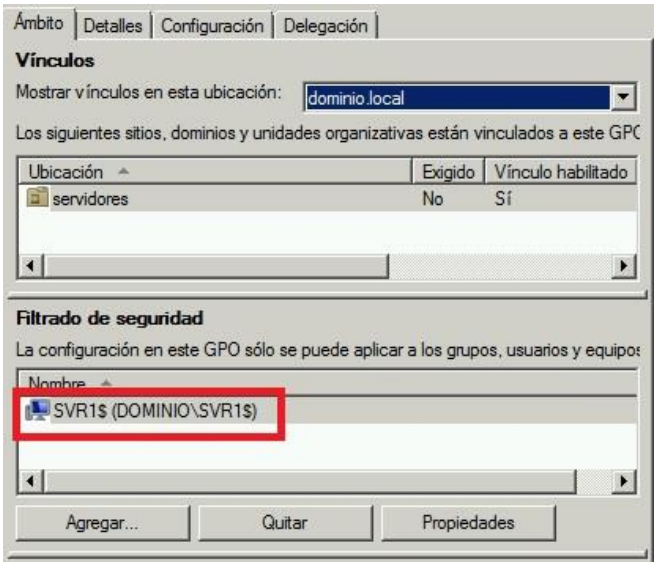
Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

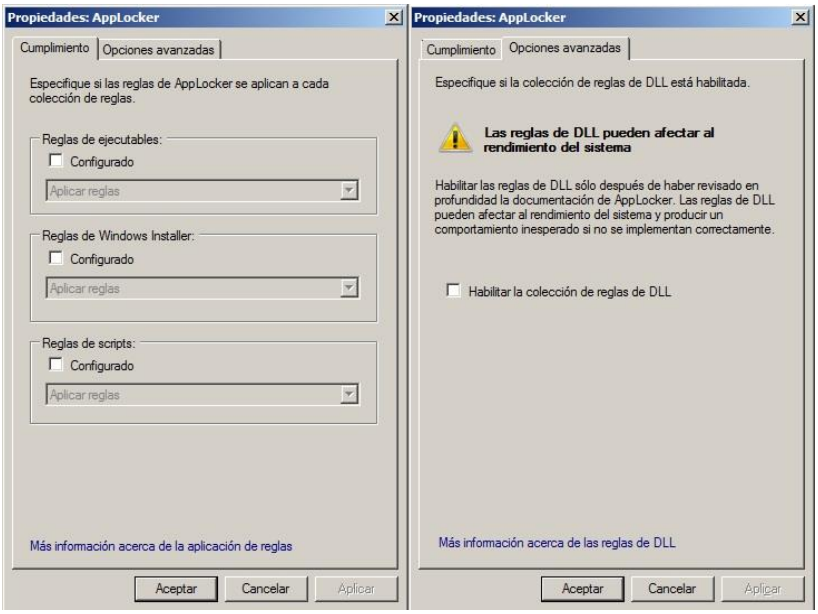
Directiva CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



Compruebe que existen las reglas que se indican a continuación.

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES%*	
Denegar	Todos	%WINDIR%\Temp*	

Comprobación	OK/NOK	Cómo hacerlo
7. Verifique que está creada la directiva “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio 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”. Verifique que está creada la política “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto”.  **Nota:** En éste ejemplo, todos los servidores a los que se les aplicará la configuración residen en la OU “Servidores”. Adapte esta comprobación a la organización de su Directorio Activo.
8. Verifique, si aplica, el filtrado de seguridad del GPO “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto”		**Nota:** Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo continúe con este paso. Si no, continúe en el paso 9. Utilizando el “Administrador de directivas de grupo” (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO “CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto” y revise en el apartado “Filtrado de Seguridad” de la pestaña “Ámbito” que se encuentran los grupos o máquinas destinados a recibir la política.  **Nota:** En este ejemplo sólo se filtra por un único servidor (SVR1). Ajuste la comprobación a la organización de su entorno

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación: 

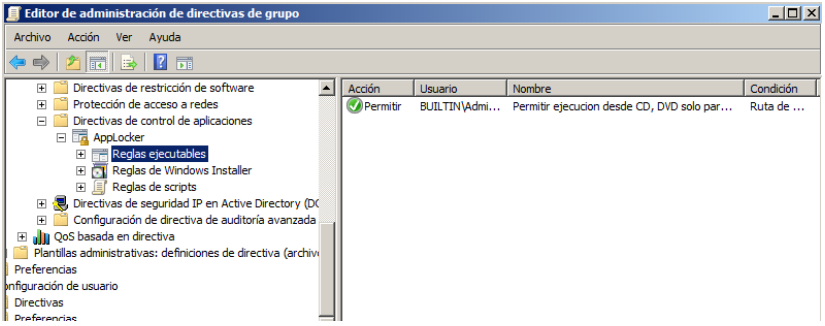
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	No configurado	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

10. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



Compruebe que existen las reglas que se muestran a continuación.

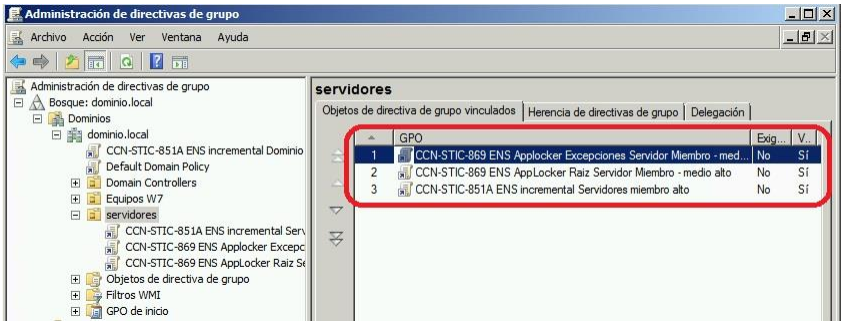
Nota: Si ha establecido excepciones (nuevas reglas) durante la fase de creación y aplicación de la política, compruebe que éstas también están aplicadas.

Acción	Usuario	Nombre	OK/NOK
Permitir	BUILTIN\Administradores	Permitir ejecución desde CD, DVD sólo para Administradores	

11. Verificar el orden de aplicación de GPOs.

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". Verifique que el orden de aplicación es el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto.
2) CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto.
3) Resto de GPOs

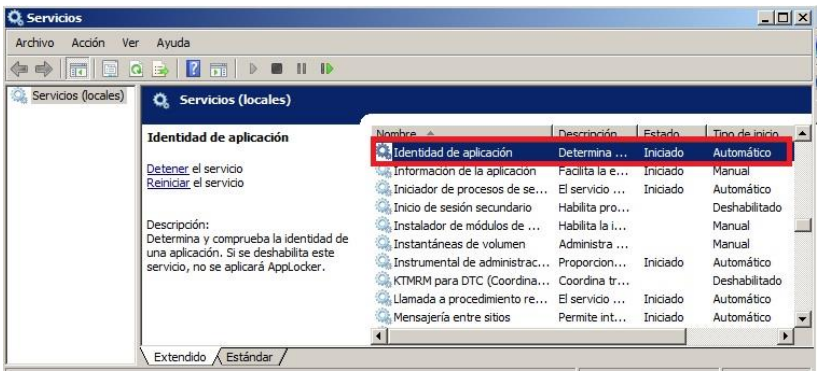
Comprobación	OK/NOK	Cómo hacerlo
		

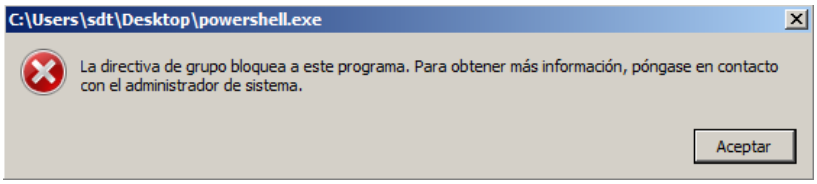
La siguiente tabla describe las Comprobaciónes a realizar para verificar el buen funcionamiento de AppLocker para servidores Windows Server 2008 R2 o Windows Server 2012 R2 miembros de un dominio.

Los siguientes pasos se realizarán desde un servidor miembro que haya recibido y aplicado las políticas "CCN-STIC-869 ENS AppLocker Raiz Servidor Miembro – medio alto" y "CCN-STIC-869 ENS AppLocker Excepciones Servidor Miembro – medio alto". Dichas Comprobaciónes se realizarán con un usuario que tenga permisos de administración local sobre el servidor.

Las consolas y herramientas que se utilizarán son las siguientes:

- Servicios (services.msc).
- Visor de eventos (eventvwr.msc).

Comprobación	OK/NOK	Cómo hacerlo
12. Inicie sesión en el servidor miembro.		Inicie sesión en el servidor miembro del dominio con una cuenta con permisos de administración local.
13. Comprobación de servicio de identidad.		Haciendo uso de la consola de servicios (Tecla Windows + R → services.msc o Inicio → ejecutar → services.msc), compruebe que el servicio de "Identidad de Aplicación" está iniciado y configurado para que inicie automáticamente: 
14. Ejecución de binario de prueba.		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).

Comprobación	OK/NOK	Cómo hacerlo
15. Comprobación de bloqueo de ejecutable.		Si la aplicación de las políticas de AppLocker es correcta deberá recibir el siguiente mensaje por pantalla. 

3. LISTA DE COMPROBACIÓN DE LA CONFIGURACIÓN DE APPLOCKER SOBRE CLIENTE WINDOWS 7 MIEMBRO DE UN DOMINO

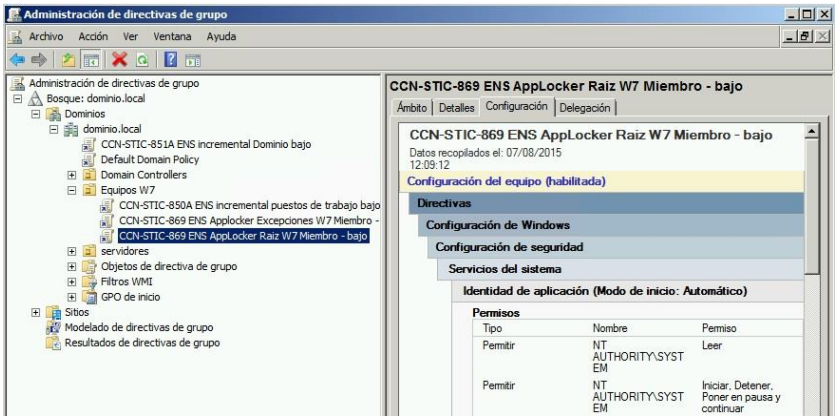
La siguiente tabla describe las Comprobaciónes a realizar para verificar la configuración de AppLocker para clientes Windows 7 miembros de un dominio.

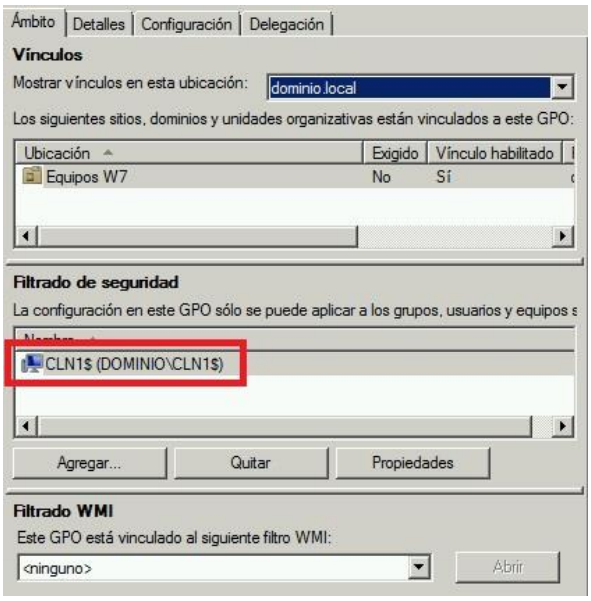
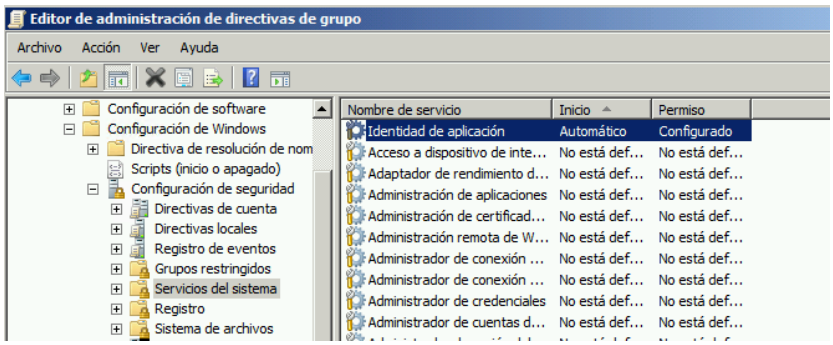
Para realizar ésta lista de comprobación, se deberá iniciar sesión en un controlador de dominio con una cuenta de usuario con privilegios de administración en el dominio.

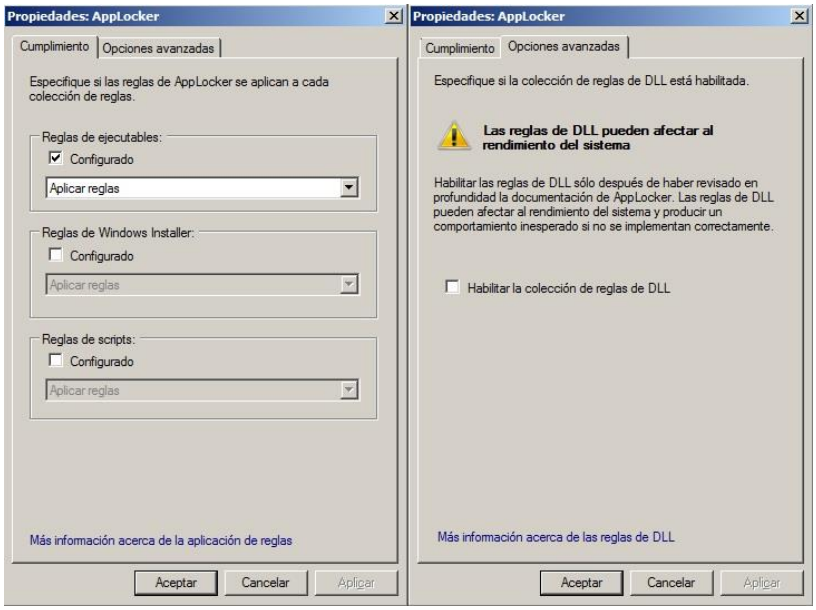
Las consolas y herramientas que se utilizarán son las siguientes:

- Administrador de directivas de grupo (gpmc.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 en este documento. 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-869 ENS AppLocker Raiz W7 Miembro - medio 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 “Equipos W7”.Verifique que está creada la política “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto”.  **Nota:** En este ejemplo, todos los clientes Windows 7 a los que se les aplicará la configuración residen en la OU “Equipos W7”. Adapte esta comprobación a la organización de su Directorio Activo.

Comprobación	OK/NOK	Cómo hacerlo
3. Verifique, si aplica, el filtrado de seguridad del GPO “CCN-STIC-869 ENS AppLocker Raiz W7 – medio alto”.		**Nota:** Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo de máquina continúe con este paso. Si no, continúe en el paso 4. Utilizando el “Administrador de directivas de grupo” (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO “CCN-STIC-869 ENS AppLocker Raiz W7 – medio alto” y revise que en el apartado “Filtrado de Seguridad” de la pestaña “Ámbito” se encuentran los grupos o máquinas destinados a recibir la política.  **Nota:** En este ejemplo se filtra por una única estación de trabajo (CLN1). Ajuste la comprobación a la organización de su entorno.
4. Verifique los servicios del sistema de la directiva “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto”.		Utilizando el “Editor de Administración de directivas de grupo”, sobre la directiva “CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto”, verifique que la directiva tiene los siguientes valores en servicios del sistema. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Servicios del Sistema**  **Nombre de Servicio** | **Inicio** | **Permiso** | **OK/NOK** Identidad de aplicación | Automático | Configurado

Comprobación	OK/NOK	Cómo hacerlo
5. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas aparecen como se indica a continuación. 

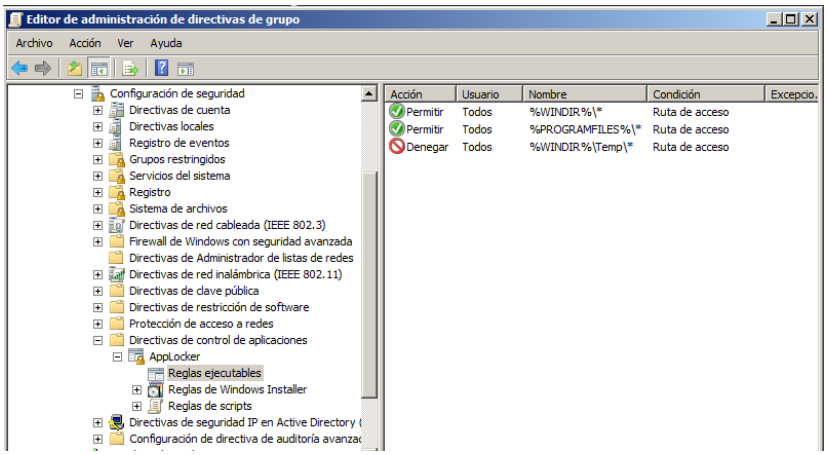
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Aplicar reglas	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

6. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



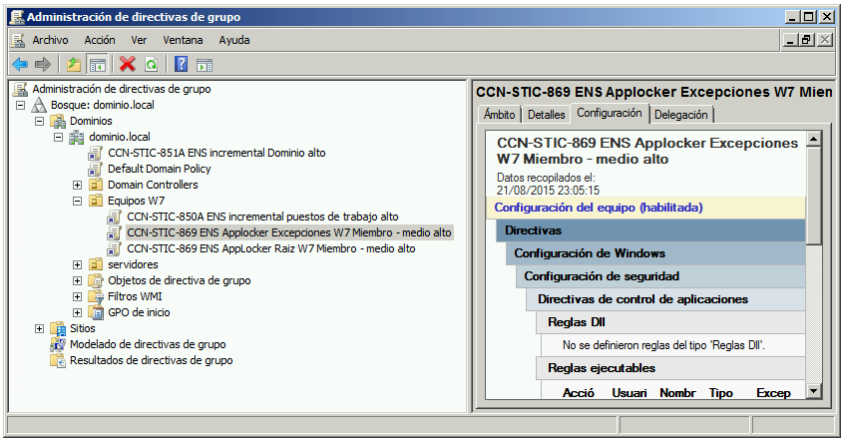
Compruebe que existen las reglas que se indican a continuación:

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES%*	
Denegar	Todos	%WINDIR%\Temp*	

7. Verifique que está creada la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio 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 "Equipos Windows 7". Verifique que está creada la política "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto".

Comprobación	OK/NOK	Cómo hacerlo

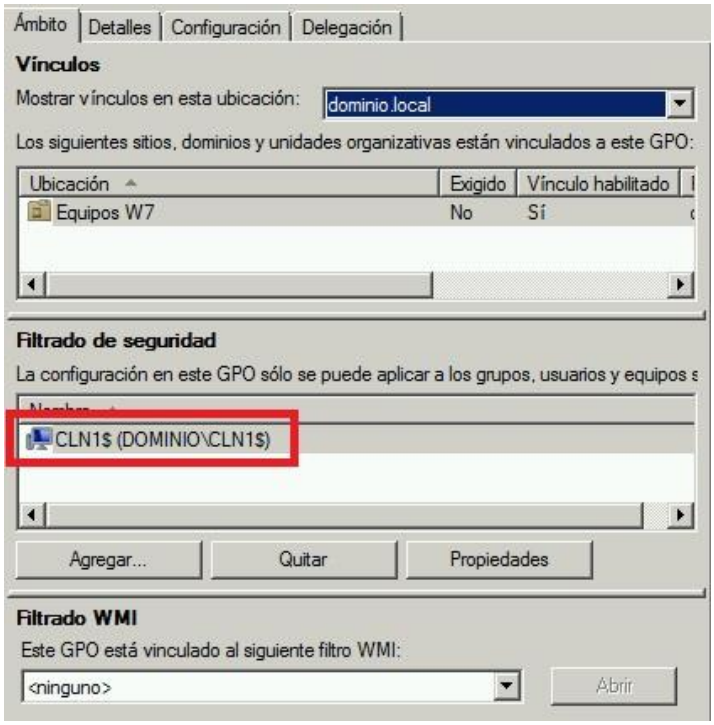


Nota: En este ejemplo, todos los clientes Windows 7 a los que se les aplicará la configuración residen en la OU "Equipos W7". Adapte esta comprobación a la organización de su Directorio Activo.

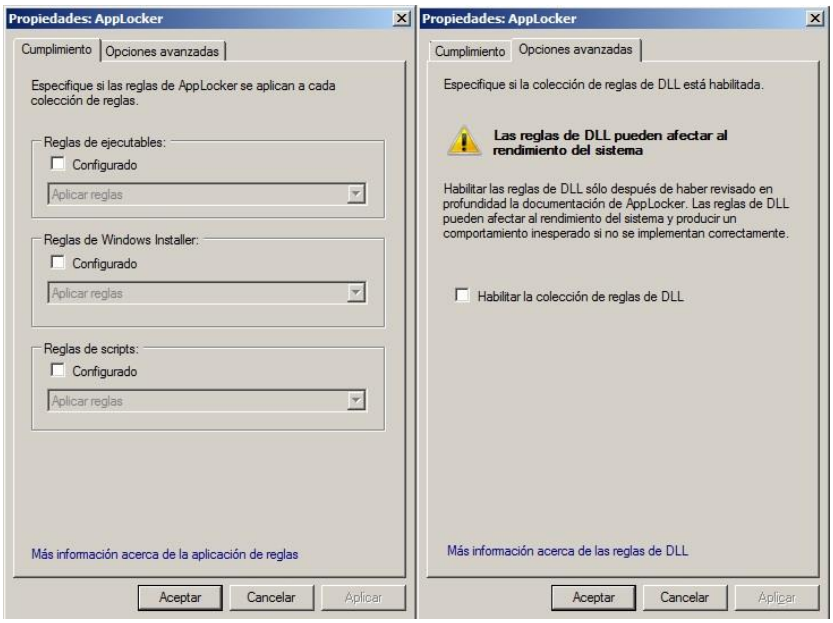
8. Verifique, si aplica, el filtrado de seguridad del GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto".

Nota: Si en la aplicación de las políticas de AppLocker ha hecho uso del filtrado por máquina o grupo continúe con este paso. Si no, continúe en el paso 9.

Utilizando el "Administrador de directivas de grupo" (Inicio → Herramientas administrativas → Administración de directivas de grupo) seleccione el GPO "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto" y revise en el apartado "Filtrado de Seguridad" de la pestaña "Ámbito" que se encuentran los grupos o máquinas destinados a recibir la política.



Nota: En este ejemplo se filtra por una única estación de trabajo (CLN1). Ajuste la comprobación a la organización de su entorno.

Comprobación	OK/NOK	Cómo hacerlo
9. Verifique las opciones AppLocker de la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto".		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto" tiene los siguientes valores en las propiedades de AppLocker. Navegue hasta: **Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker** Pulse el botón derecho sobre "AppLocker" y elija el menú "Propiedades".  En la ventana de "Propiedades", compruebe que las configuraciones de las dos pestañas están como se indica a continuación. 

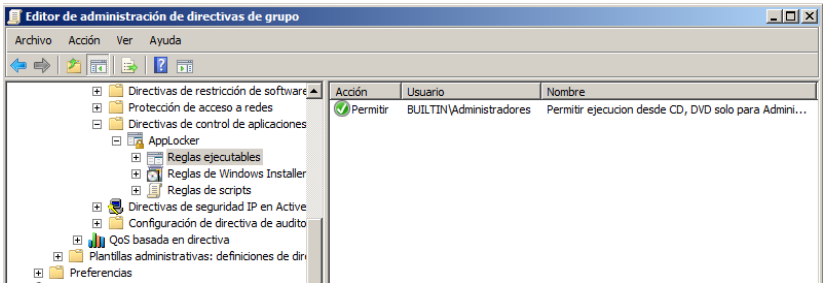
Comprobación	OK/NOK	Cómo hacerlo

Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	No configurado	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

10. Verifique las reglas ejecutables de AppLocker en la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto".

Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva "CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto" tiene los siguientes valores en las reglas de ejecutables de AppLocker. Navegue hasta:

Directiva CCN-STIC-869 ENS AppLocker Excepciones W7 – medio alto \ Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables



Compruebe que existen las reglas que se muestran a continuación.

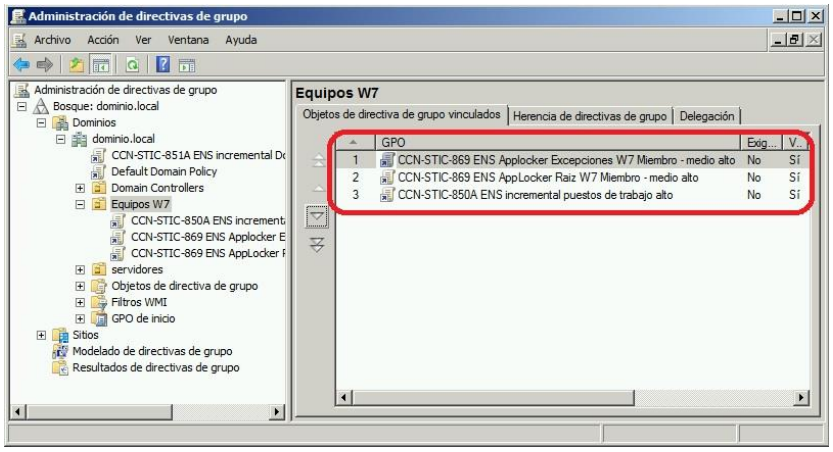
Nota: Si ha establecido excepciones (nuevas reglas) durante la fase de creación y aplicación de la política, compruebe que éstas también están aplicadas.

Acción	Usuario	Nombre	OK/NOK
Permitir	BUILTIN\Administradores	Permitir ejecución desde CD, DVD sólo para Administradores	

11. Verificar el orden de aplicación de GPOs.

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". Verifique que el orden de aplicación es el siguiente:

1) CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto.
2) CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto.
3) Resto de GPOs.

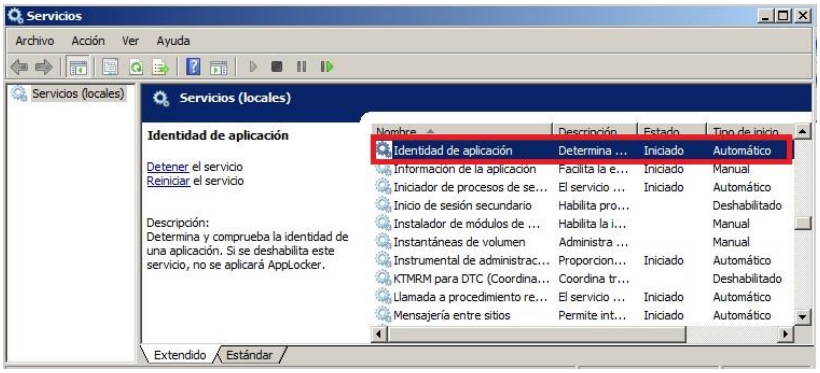
Comprobación	OK/NOK	Cómo hacerlo
		

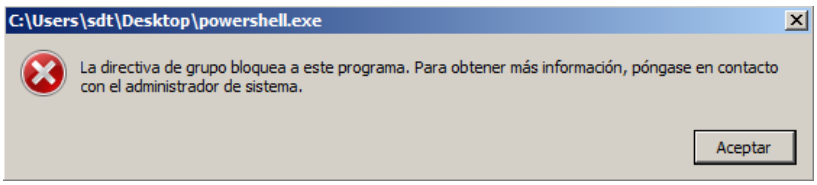
La siguiente tabla describe las Comprobaciónes a realizar para verificar el buen funcionamiento de AppLocker para estaciones de trabajo Windows 7 miembros de un dominio.

Los siguientes pasos se realizarán desde un cliente Windows 7 que haya recibido y aplicado las políticas "CCN-STIC-869 ENS AppLocker Raiz W7 Miembro – medio alto" y "CCN-STIC-869 ENS AppLocker Excepciones W7 Miembro – medio alto". Dichas Comprobaciónes se realizarán con un usuario que tenga permisos administrativos sobre la estación de trabajo.

Las consolas y herramientas que se utilizarán son las siguientes:

- Servicios (services.msc).
- Visor de eventos (eventvwr.msc).

Comprobación	OK/NOK	Cómo hacerlo
12. Inicie sesión en el cliente Windows 7.		Inicie sesión en el cliente Windows 7 con una cuenta con permisos de administración local.
13. Comprobación de servicio de identidad.		Haciendo uso de la consola de servicios (Tecla Windows + R → services.msc o Inicio → ejecutar → services.msc), compruebe que el servicio de "Identidad de Aplicación" está iniciado y configurado para que inicie automáticamente: 
14. Ejecución de binario de prueba.		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).

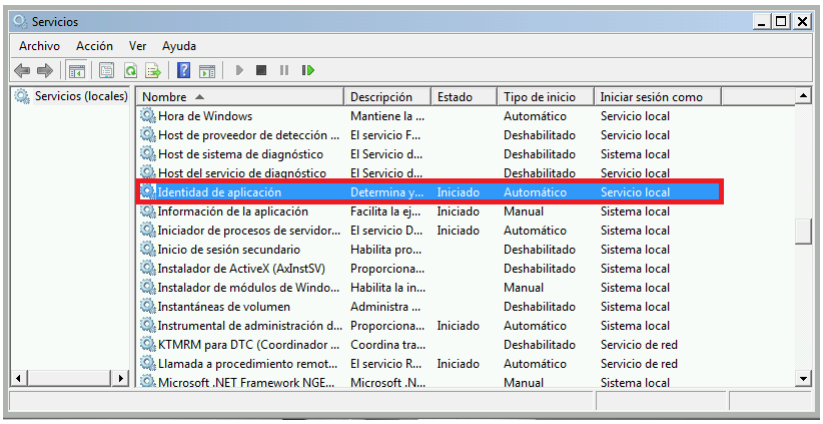
Comprobación	OK/NOK	Cómo hacerlo
15. Comprobación de bloqueo de ejecutable.		Si la aplicación de las políticas de AppLocker es correcta deberá recibir el siguiente mensaje por pantalla. 

ANEXO K. LISTA DE COMPROBACIÓN DE LA CORRECTA IMPLANTACIÓN DE APPLOCKER SOBRE CLIENTES WINDOWS 7 Y SERVIDORES INDEPENDIENTES CON ENS NIVEL BAJO

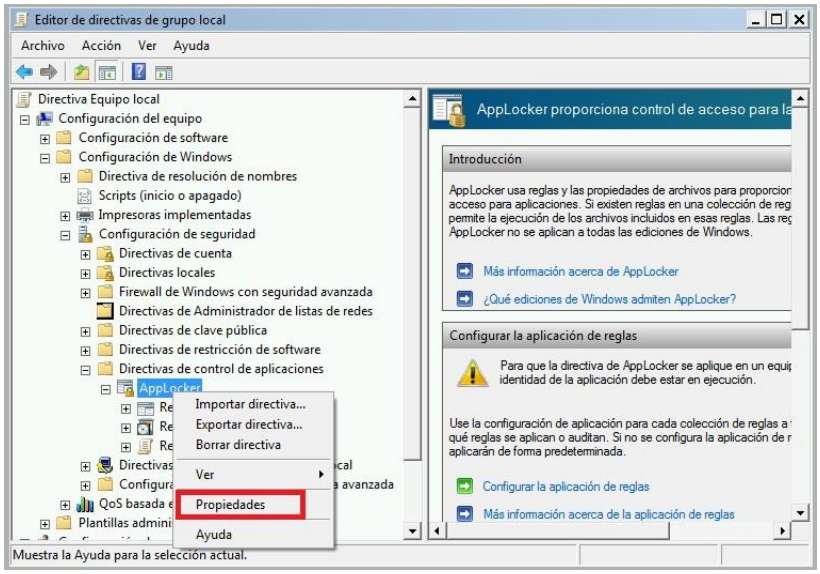
Este anexo ha sido diseñado para ayudar a los operadores a verificar la correcta aplicación de las distintas configuraciones de seguridad que conciernen a la implantación de AppLocker en clientes Windows 7 Enterprise o Ultimate y servidores Windows Server 2008R2 o 2012R2 a los que les aplique el nivel bajo según los criterios del Esquema Nacional de Seguridad.

Las consolas y herramientas que se utilizarán son las siguientes:

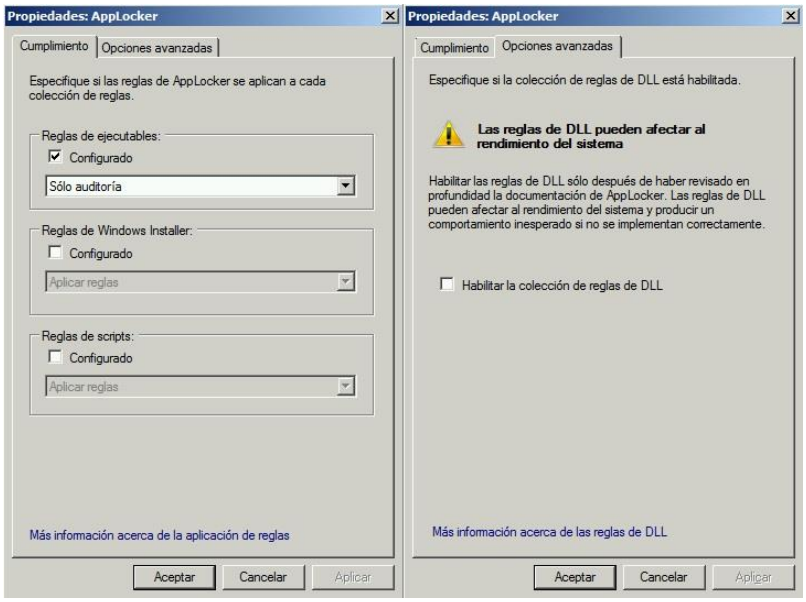
- Consola de servicios (services.msc).
- Editor de objetos de directiva de grupo (GPedit.msc).
- Visor de Eventos (eventvwr.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un cliente independiente.		Inicie sesión en el cliente con un usuario con privilegios de administrador local.
2. Verifique que el servicio de identidad de aplicaciones esté iniciado		Usando la tecla “Windows + R” inicie la consola de servicios, escribiendo “services.msc” y pulse la tecla “Enter”. Sobre la consola compruebe que el servicio “Identidad de aplicación” está iniciado y su inicio en modo “Automático”. 
3. Verifique las opciones AppLocker de la directiva local.		A través del editor de políticas locales (GPedit) vaya a la siguiente ruta: **Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker** Pulse el botón derecho sobre “AppLocker” y elija el menú “Propiedades”.

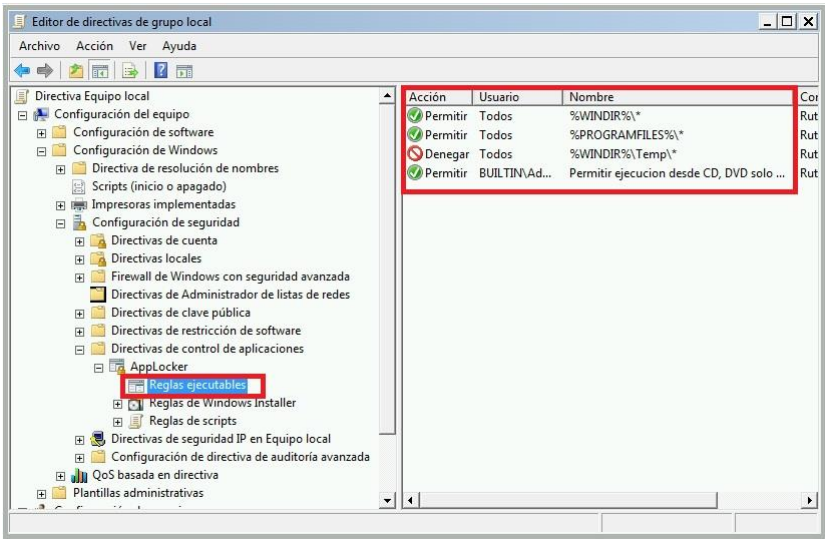
Comprobación	OK/NOK	Cómo hacerlo



En la ventana de “Propiedades”, compruebe que las configuraciones de las dos pestañas están como se muestran en las siguientes imágenes.



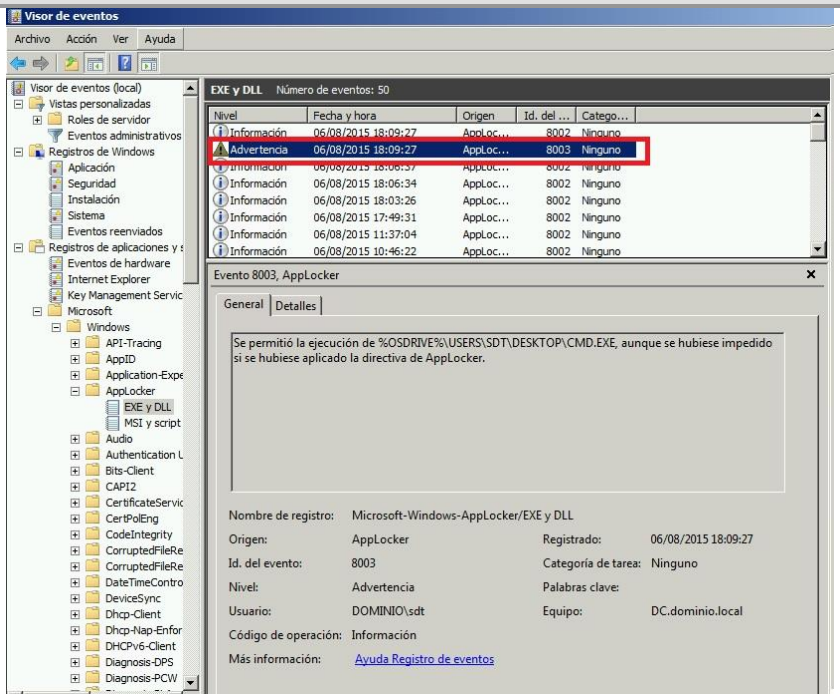
Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Sólo Auditoría	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique las reglas ejecutables de AppLocker en la directiva local.		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva de AppLocker tiene los siguientes valores en las reglas de ejecutables. Navegue hasta: **Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables**  Compruebe que existen las reglas que se indican a continuación:

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES*%	
Denegar	Todos	%WINDIR\Temp*%	
Permitir	Builtin\Administradores	Permitir ejecución de CD, DVD solo para administradores	

Nota: Si ha aplicado alguna excepción adicional a las definidas de forma predeterminada en la guía, verifique que se encuentra definida.

5. Comprobación de bloqueo de ejecutable		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).
6. Comprobar eventos 8003 en visor de eventos.		Abra un visor de eventos (inicio → ejecutar → eventvwr.msc) y navegue hasta: **Visor de eventos / Registros de aplicaciones y servicios / Microsoft / Windows / AppLocker** Compruebe que hay un evento con identificador 8003 que corresponde con la ejecución del binario anterior.

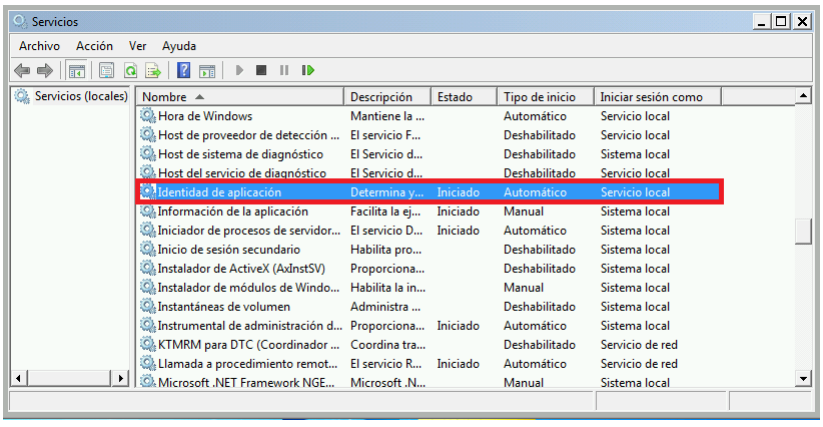
Comprobación	OK/NOK	Cómo hacerlo
		

ANEXO L. LISTA DE COMPROBACIÓN DE LA CORRECTA CONFIGURACIÓN DE APPLOCKER SOBRE CLIENTES WINDOWS 7 Y SERVIDORES INDEPENDIENTES CON ENS NIVEL MEDIO O ALTO

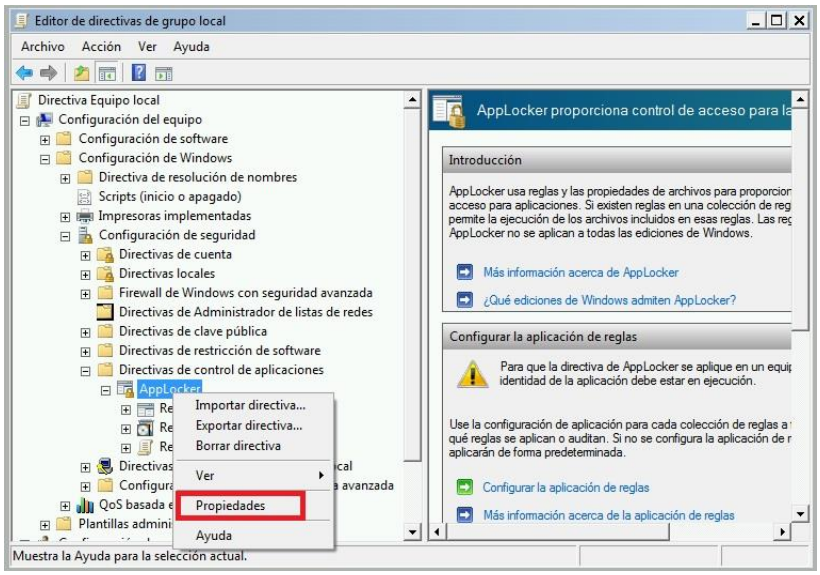
Este anexo ha sido diseñado para ayudar a los operadores a verificar la correcta aplicación de las distintas configuraciones de seguridad que conciernen a la implantación de AppLocker en clientes Windows 7 Enterprise o Ultimate y servidores Windows Server 2008R2 o 2012R2 a los que les aplique el nivel bajo según los criterios del Esquema Nacional de Seguridad.

Las consolas y herramientas que se utilizarán son las siguientes:

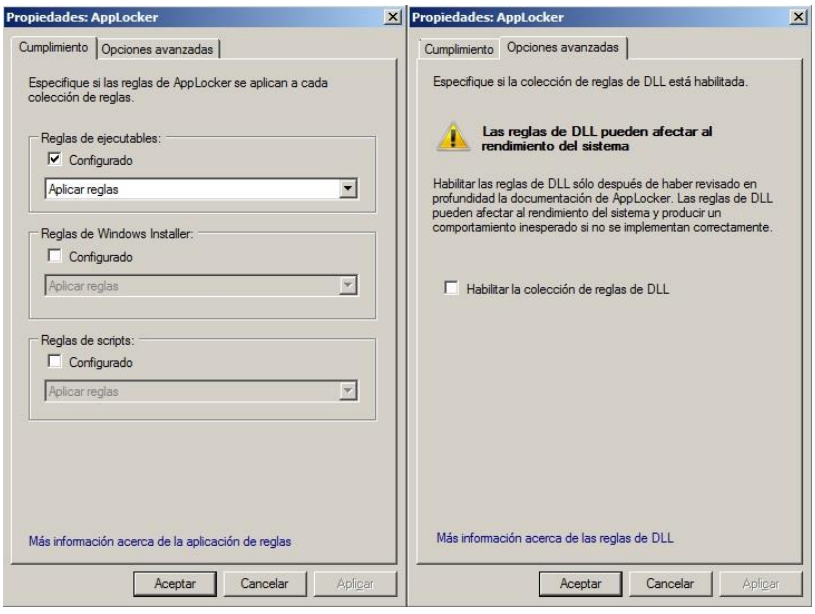
- Consola de servicios (services.msc).
- Editor de objetos de directiva de grupo (GPedit.msc).
- Visor de Eventos (eventvwr.msc).

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en un cliente independiente.		Inicie sesión en el cliente con un usuario con privilegios de administrador local.
2. Verifique que el servicio de identidad de aplicaciones esté iniciado.		Usando la tecla “Windows + R” inicie la consola de servicios, escribiendo “services.msc” y pulse la tecla “Enter”. Sobre la consola compruebe que el servicio “Identidad de aplicación” está iniciado y su inicio en modo “Automático”. 
3. Verifique las opciones AppLocker de la directiva local.		A través del editor de políticas locales (GPedit) vaya a la siguiente ruta: **Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones\AppLocker** Pulse el botón derecho sobre “AppLocker” y elija el menú “Propiedades”.

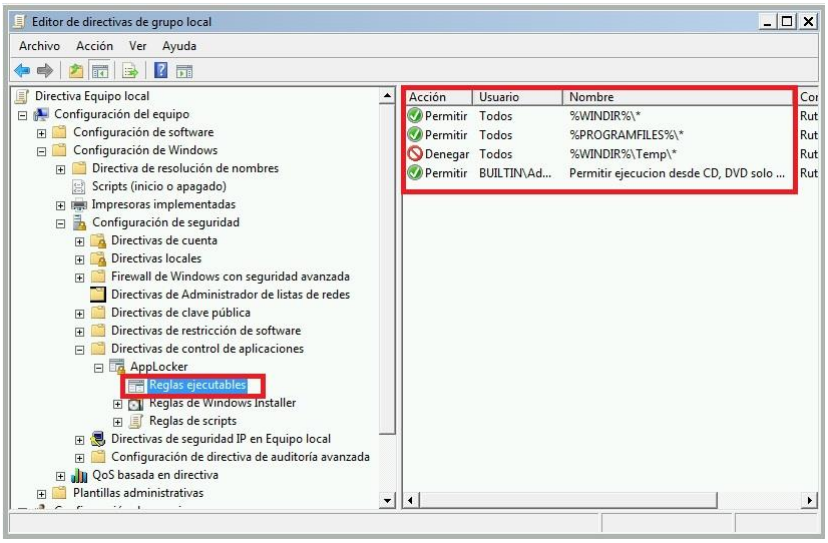
Comprobación	OK/NOK	Cómo hacerlo



En la ventana de “Propiedades”, compruebe que las configuraciones de las dos pestañas están como se muestran en las siguientes imágenes.



Pestaña / Configuración	Valor	OK/NOK
Cumplimiento / Reglas ejecutables	Configurado + Aplicar reglas	
Cumplimiento / Reglas de Windows Installer	No configurado	
Cumplimiento / Reglas de scripts	No configurado	
Opciones avanzadas / Colección de reglas de DLL	No configurado	

Comprobación	OK/NOK	Cómo hacerlo
4. Verifique las reglas ejecutables de AppLocker en la directiva local.		Utilizando el "Editor de Administración de directivas de grupo", verifique que la directiva de AppLocker tiene los siguientes valores en las reglas de ejecutables. Navegue hasta: **Configuración del equipo \ Directivas \ Configuración de Windows \ Configuración de seguridad \ Directivas de control de aplicaciones \ AppLocker \ Reglas Ejecutables**  Compruebe que existen las reglas que se indican a continuación:

Acción	Usuario	Nombre	OK/NOK
Permitir	Todos	%WINDIR%*	
Permitir	Todos	%PROGRAMFILES*%	
Denegar	Todos	%WINDIR\Temp*%	
Permitir	Builtin\Administradores	Permitir ejecución de CD, DVD solo para administradores	

Nota: Si ha aplicado alguna excepción adicional a las definidas de forma predeterminada en la guía, verifique que se encuentra definida.

5. Ejecución de un binario de prueba.		Copie un ejecutable al escritorio del usuario y ejecútelo desde el escritorio (Por ejemplo %WINDIR%\System32\cmd.exe).
6. Comprobación de bloqueo de ejecutable.		Si la aplicación de las políticas de AppLocker es correcta deberá recibir el siguiente mensaje por pantalla.